VOL. 17, NO. 24, DECEMBER 2022 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

IMPROVING DATA STANDARD METHODS OF CRYPTOGRAPHY

Adnan Manasreh[1], Mohammad S. Khrisat1[2], Hatim Ghazi Zaini[3], Ziad A. Alqadi[2] and Nasser Abdellatif[1]
[1]Department of Electrical Engineering, Applied Science Private University, Amman, Jordan
[2]Department of Computer Engineering, Faculty of Engineering Technology, AL-Balqa Applied University Amman, Jordan
[3]Computer and Information Technology College, Taif University, Taif, Kingdom of Saudi Arabia
E-Mail: adnan_m@asu.edu.jo

ABSTRACT

Secret messages which contain valuable confidential and private information require high-level protection to make the hacking process impossible. In this research paper, a new and simple method of data cryptography will be introduced. The proposed method will use two image_keys to generate the needed private keys. The private keys will be categorized into two sets: the first set will be used to form the RLDs required for the rotation right of each byte, while the second set will be used to apply XORing operations. The image_keys will be kept secret to avoid hacking them. The method will use a variable block size to divide the data, and it will use a variable number of rounds. The block size and the number of rounds are to be kept secret. The method will be implemented using various messages and various block sizes and a number of rounds, the obtained results will be compared with DES results to show how the proposed method will keep a high throughput when increasing the block size and increasing the number of rounds.

Keywords: cryptography, PK, image_key, XORing, RLD, MSE, PSNR, TP.

1. INTRODUCTION

Color digital images are considered one of the most important and most widespread types of digital data, and this is due to several reasons, the most important of which are [48-56]:

- The use of digital images in many vital and important applications [1-5].
- Ease of processing the digital image because it is represented by a three-dimensional matrix (a two-dimensional matrix for each of the three colors: red, green, and blue, see Figure-1), which turns the process of processing the rhyming image into an easy process for processing matrices.
- Possibility to use parts of the image [6-10].
- The possibility of using the matrix of each color independently and individually.
- The possibility of converting the matrix of each color into an available number of elements, this can be done by applying an image resizing operation as shown in the example illustrated in figure 2. Image resizing can be done to get a private key (PK) will a selected length, the contents of this PK will depend on the selected length, the selected color image (image_key), and the selected color matrix as shown in the example illustrated in Figure-3 [11-17].

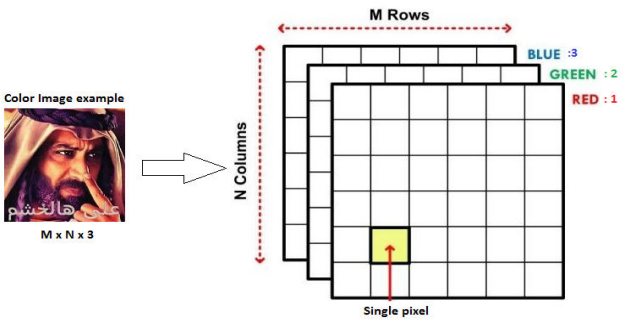

Figure-1. Color image matrices.

- The possibility of using two image-keys to generate necessary PKs, these images can be kept in secret (without transmission) and can be used to generate PKs with any needed length as shown in figure 3 [18-22].

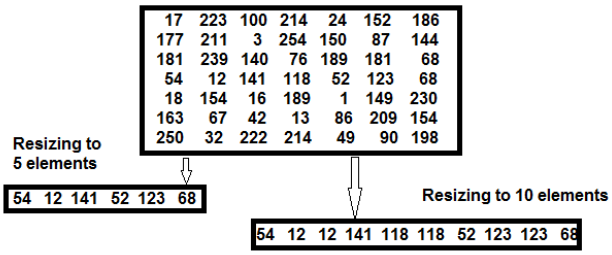

Figure-2. Matrix resizing.

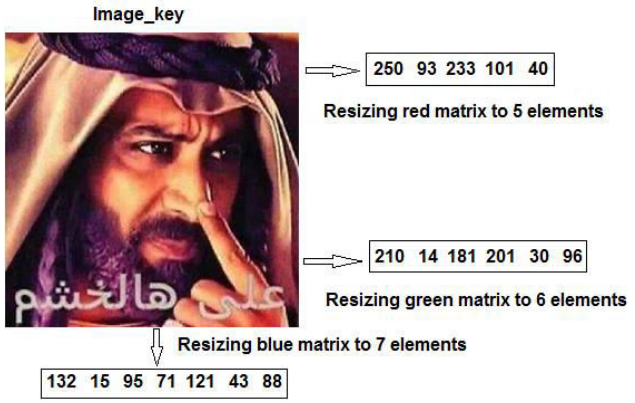

Figure-3. Image_key resizing.

- Ease of carrying out logical operations such as the left rotation process for a number of digits (using a selected number of rotated left digits (RLD)), and the process of exclusion, or where these operations can easily be used to distort the data and return it to its original, and this is what the process of data cryptography requires, [40-47] figure 4 shows how to perform rotate let operation, while Figures 5 and 6 illustrate examples of using logical operations to encrypt-decrypt a character:

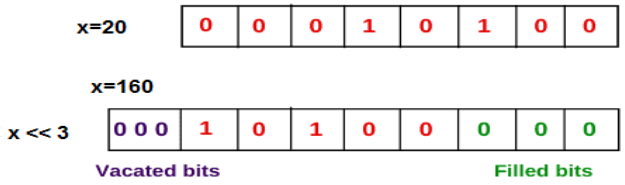

Figure-4. Rotate left operation implementation.

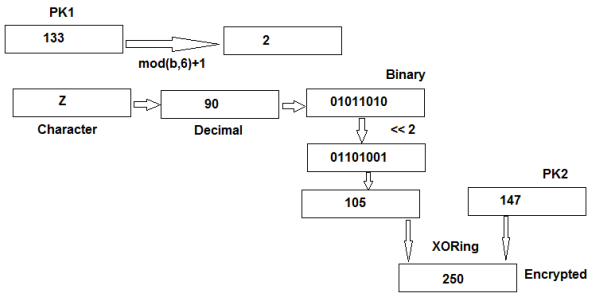

Figure-5. Using logical operations to encrypt character.

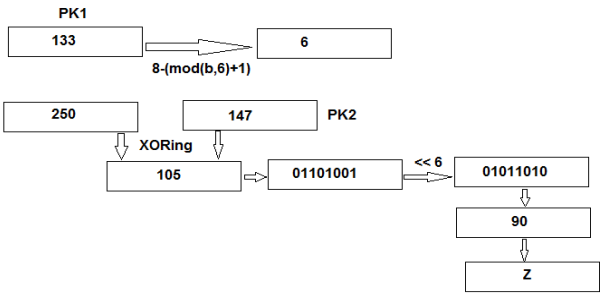

Figure-6. Using logical operations to decrypt character.

Text messages are circulated through various social media, and some of these messages are of a special personal nature or carry private or confidential information, which requires protection from penetration and from the danger of tampering and data thieves [23-28].

One of the reliable methods of secret message protection is data cryptography. Data cryptography (as shown in Figure-7) means encrypting the source data before sending while decrypting the encrypted data after receiving [29-33].

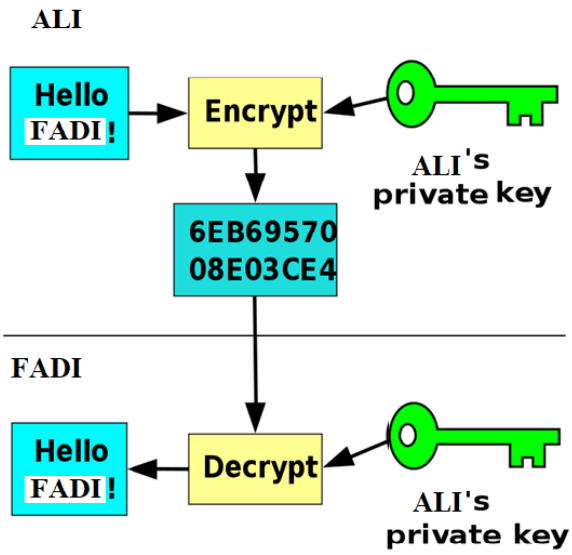

Figure-7. Data cryptography process.

A method of data cryptography is considered a good method if it satisfies the following:

- Simplicity: Easy to program and implement and easy to modify.
- Efficiency: Maximizing the method throughput (byte processed per second), this can be achieved by minimizing the encryption time (ET) and decryption time (DT) [31-34].
- Highly secure: Difficulty to hack by using a complex private key (PK) which cannot be guessed or hacked.

- Multipurpose use: Using the method to encrypt-decrypt any data including secret messages (with any length) and digital images (with any type and size) [35-40].

- Quality: The quality between two data sets can be measured by mean square error (MSE), peak signal-to-noise ratio (PSNR), and correlation coefficient (CC), these parameters can be calculated using equations 1, 2, and 3. In the encryption phase, the value of MSE must be very high, the PSNR must be very low, and also the value of CC means a full destruction of source data. In the decryption phase the value of MSE must be equal to zero, the value of PSNR must equal infinite, while the value of CC must equal 1, and this means full recovery of the source data and the decrypted data is identical to the source one [48-56].

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

2. RELATED WORKS

Many methods are used for data cryptography, in this research paper we will focus on the data encryption standard (DES) because many methods are based on DES and for many other reasons which be explained later in this section [1-10].

DES has the following features, and some of these features are considered disadvantages that we must overcome when designing a new method of data cryptography:

- Blocking:

Message to be encrypted is to be divided into equal blocks, the block size is fixed and equal to 64 bits (8 bytes) and the block length cannot be changed (see Figure-8).

- PK:

The method uses a single PK with a length equal to 56 bits; the key length is fixed and cannot be changed. PK key is to be used to generate other key nods in the process of message cryptography by applying key scheduling. The private key can be hacked and here the level of security is low, this means that DES does not provide enough protection for the transmitted secret message [50-56].

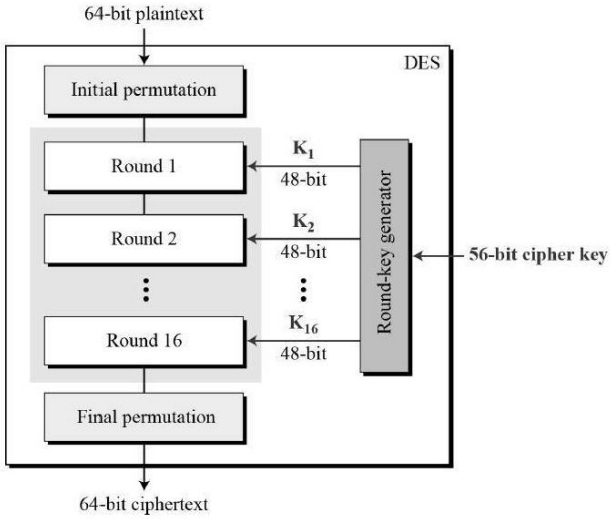

Figure-8. DES operations.

- The process of encryption/decryption is implemented in 16 rounds, this number o rounds is fixed, and each round manipulates a Feistel set of operations containing a set of logical operations (see Figure-9).

- Quality of cryptography

DES provides good values for the quality parameters MSE, PSNR, and CC in both the encryption and decryption phases.

- **Efficiency**

DES provides a good throughput, it requires a small time for encryption and decryption especially when it is used to encrypt-decrypt small in size secret message, when the message grows in size DES will be not efficient, and here DES will require much time to encrypt-decrypt big data such as digital color images.

- **Modification**

The structure of DES is a Feistel structure, it is fixed and cannot be updated, the block size and the PK size must be fixed without any changes.

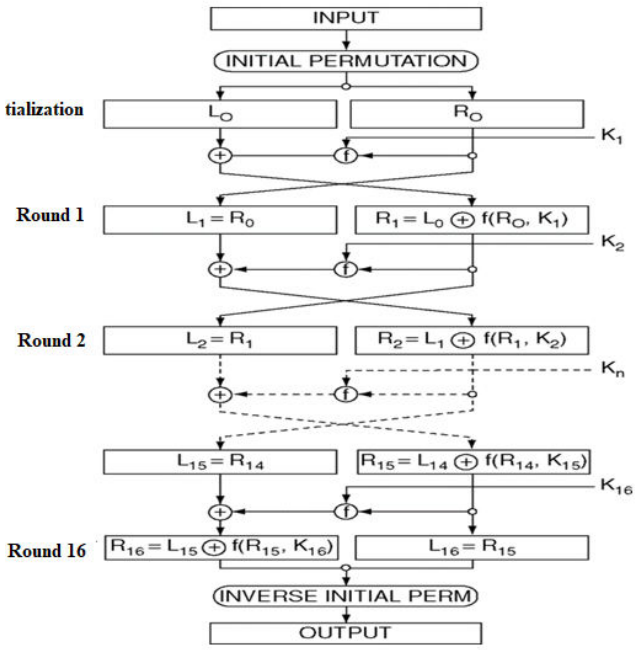

Figure-9. DES rounds.

3. THE PROPOSED METHOD

The proposed method will use two color images to generate the required secret private keys needed for message cryptography, these two images (image_keys) must be kept in secret and agree upon between the sender and receiver, one or the two image_keys can be replaced with other images any time and when the need arises without affecting the method operations.

The selected image_keys are used to generate PKs for each round of cryptography, the first set of keys are to be used to generate the number of rotating left digits (RLD) required to rotate the character value. The second set of PKs is used to maintain XORing operations.

In the proposed method the secret message (or any other data type such as a color image) is to be divided into blocks with fixed lengths. The block size can be changed at any time and it can be varied from 1 byte to the length of the secret message, this means that the proposed method is flexible, it can apply cryptography by blocking or it can take the whole message and encrypt-decrypt it in burst way.

The number of selected keys for each round depends on the block size; each byte of the message requires two keys as shown in Figure-10, the first one to calculate the RLD for the byte and the second one to implement the XORing operation. The first set of PKs is to be generated from the first image_key, while the second set of PKs is to be generated from the second image_key.

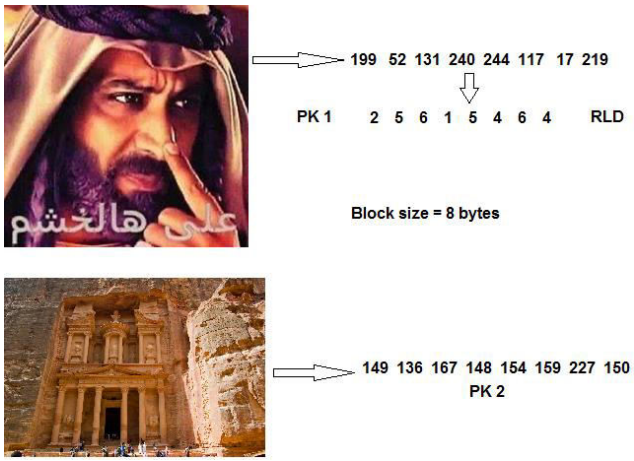

Figure-10. Using image_keys to generate PKs.

Figure-11 shows how to use the PKs to encrypt a block of 8 bytes in length, here the RLDs are to be calculated using modulus 6 + 1 operation in the encryption phase, while in the decryption phase, the calculated RLD must be subtracted from 8 as shown in Figures 11, 12, and 13.

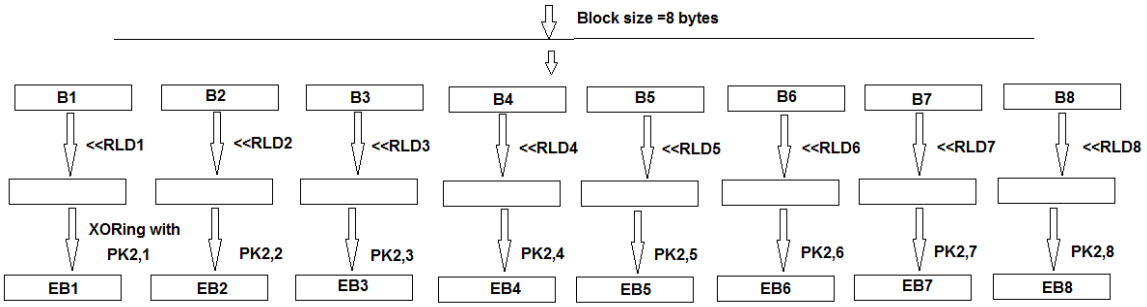

Figure-11. Encryption round of block size =8.

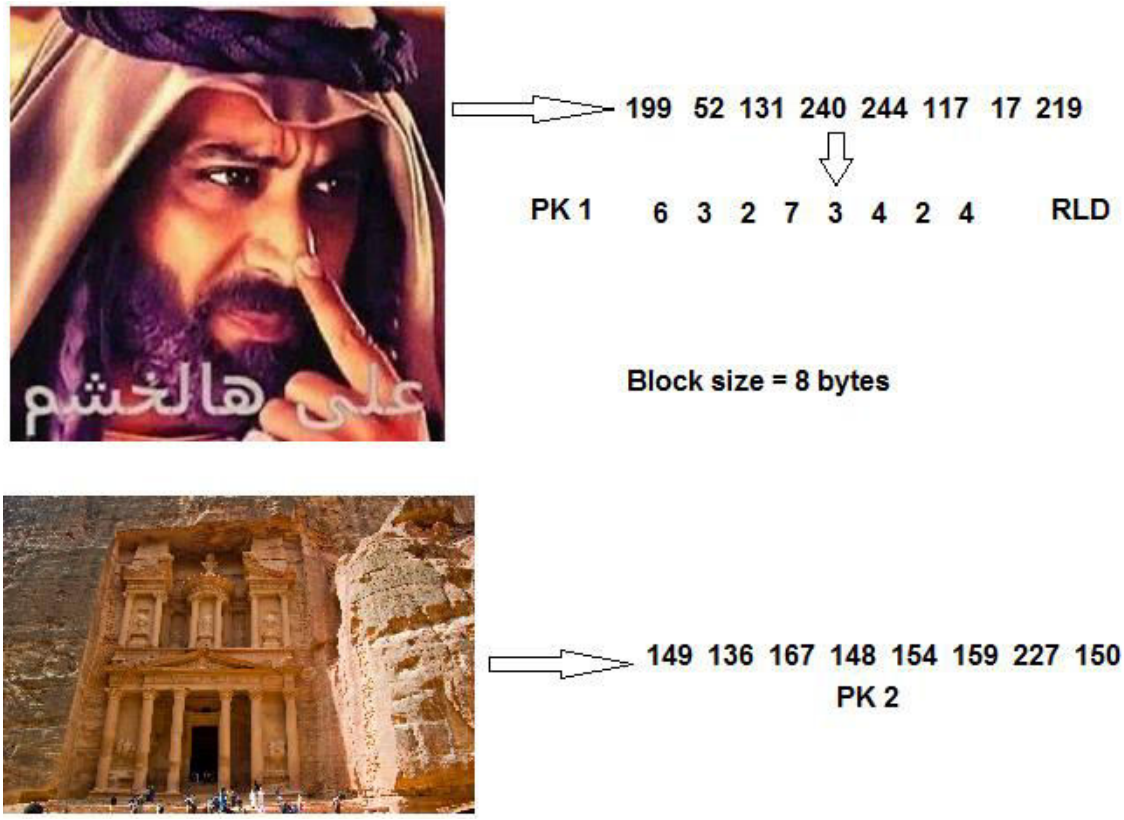

Figure-12. Using the image_keys to generate PKs for decryption.

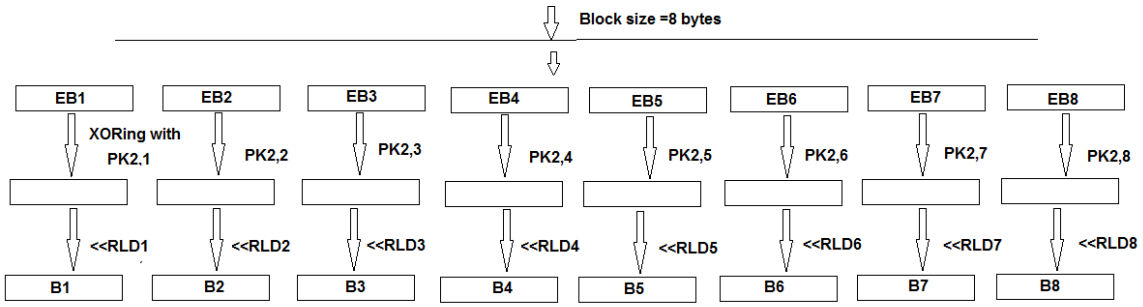

Figure-13. Decryption round of block size =8.

Below is the description of the proposed method algorithm

Encryption

Inputs:

Message to be encrypted (SM), image_key 1 (I1), image_key 2 (I2), block size (BS), number of rounds (NR).

Output:

Encrypted message (EM)

Process:

- Get the inputs
- Divide SM into blocks.
- For each block do
- Resize I1 to the block size to get PK1.
- Resize I2 to the block size to Get PK2.
- Use PK1 to calculate RLD (RLD = mod (PK1, 6+1).
- For each byte in the block do
- Rotate left the byte using the associated RLD.
- Apply XORing the resulting byte in step 8 with the associated PK from PK2.
- Repeat steps 6 to 9 for each round (if the rounds are greater than 1)

- Pad the results of step 9 to the encrypted data to get EM.

Decryption

Inputs:
Encrypted message (EM), image_key 1 (I1), image_key 2 (I2), block size (BS), number of rounds (NR).

Output:
Decrypted message (DM)

Process:
- Get the inputs
- Divide EM into blocks.
- For each block do
- Resize I1 to the block size to get PK1.
- Resize I2 to the block size to Get PK2.
- Use PK1 to calculate RLD (RLD = 8-(mod (PK1, 6+1)).
- For each byte in the block do
- Apply XORing each byte with the associated PK from PK2.
- Rotate left the resulting in step 8 byte using the associated RLD.
- Repeat steps 6 to 9 for each round (if the rounds are greater than 1)
- Pad the results of step 9 to the decrypted data to get DM.

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

For comparisons purposes, DES was implemented using various messages, Figure-14 shows a sample output , while table 1 show the obtained results:

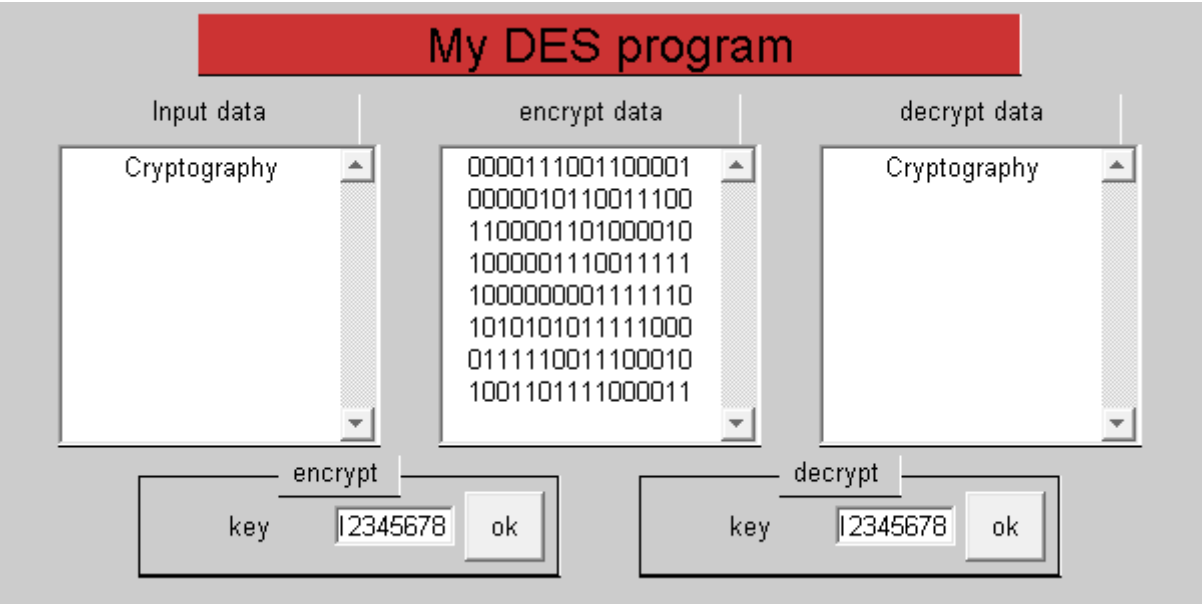

Figure-14. Sample of DES implementation.

Table-1. DES results.

Message size (byte)	ET (second)	DT (second)	ETP (byte per second)	DTP (byte per second)
100	0.2317	0.3300	431.5926	303.0303
200	0.4633	0.6900	431.6857	289.8551
300	0.7150	1.0400	419.5804	288.4615
400	0.9467	1.3100	422.5203	305.3435
500	1.1963	1.7200	417.9554	290.6977
600	1.3700	2.0200	437.9562	297.0297
700	1.6817	2.3100	416.2455	303.0303
800	1.91333	2.6900	418.1192	297.3978
900	2.1550	3.0200	417.6334	298.0132
1000	2.4067	3.3900	415.5067	294.9853
Average	1.3080	1.8520	422.8795	296.7844

The proposed method was implemented using the previous messages with Block size=8 and number of rounds =1, Table-2 shows the obtained results:

Table-2. Message cryptography: Block size=8 and number of rounds =1.

Message size	Number of blocks	ET/DT(second)	TP (byte per second)
100	13	0.0750	1333.3
200	25	0.0870	2298.9
300	38	0.1010	2970.3
400	50	0.1140	3508.8
500	63	0.1300	3846.2
600	75	0.1450	4137.9
700	88	0.1580	4430.4
800	100	0.1720	4651.2
900	113	0.1840	4891.3
1000	125	0.2270	4405.3
Average		0.1393	3647.4
Encryption speedup(DES time/proposed time)		1.3080/0.1393=9.3898	

From Tables 1 and 2 we can see that the proposed method is more efficient than DES and it will speed up the process of cryptography 9 times. From Table-2 we can show that there is a linear relationship between the ET/DT and the message size when fixing the block size, this is shown in Figure-15.

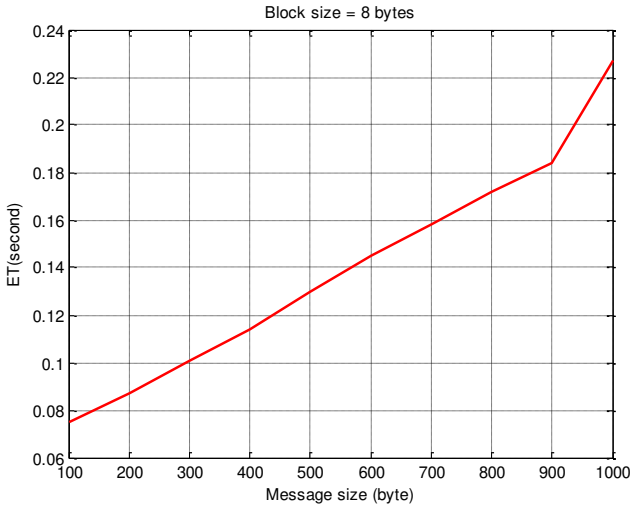

Figure-15. ET/DT vs message size.

The proposed method can use multiple rounds to accomplish the process of message cryptography, the number of rounds must be selected and agreed upon between the sender and receiver. Increasing the number of rounds will increase the method's security and at the same time will increase both the encryption and decryption times, but the proposed method will remain efficient by speeding up the process of cryptography as shown in the results shown in Table-3.

Table-3. Messages cryptography with Block size=8 and number of rounds =16.

Message size	Number of blocks	ET/DT(second)	TP(byte per second)
100	13	0.5560	179.8561
200	25	0.5350	373.8318
300	38	0.8840	339.3665
400	50	0.9310	429.6455
500	63	1.3640	366.5689
600	75	1.3870	432.5883
700	88	1.6880	414.6919
800	100	2.0380	392.5417
900	113	2.2430	401.2483
1000	125	2.2920	436.3002
Average		1.3918	376.6639

Increasing the block size and fixing the number of rounds will decrease the ET/DT, thus the throughput of cryptography will be increased, and table 4 shows the effects of increasing the block size, while Figures 16 and 17 show how varying block size will affect the method throughput.

Table-4. Method efficiency when varying the block size (Message size =1000, Rounds=4).

Block size	Number of blocks	ET/DT(second)	TP (byte per second)
8	125	0.6140	1628.7
10	100	0.4910	2036.7
12	84	0.4290	2331.0
16	63	0.3410	2932.6
20	50	0.2820	3546.1
25	40	0.2370	4219.4
30	34	0.2200	4545.5
40	25	0.1680	5952.4
50	20	0.1510	6622.5
60	17	0.1340	7462.7
Average		0.3067	4127.8

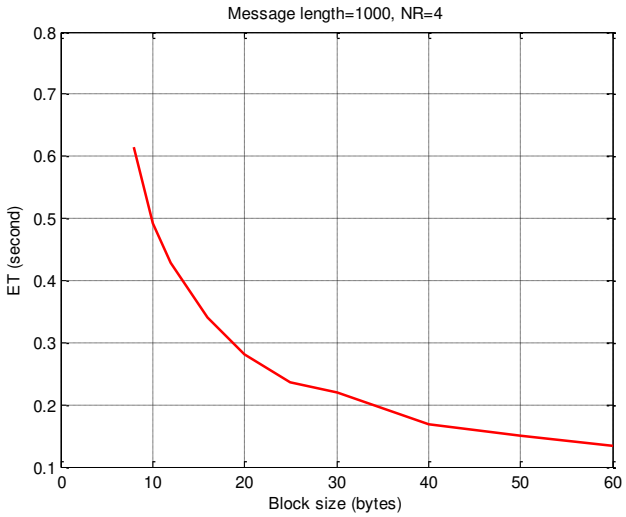

Figure-16. ET when varying block size.

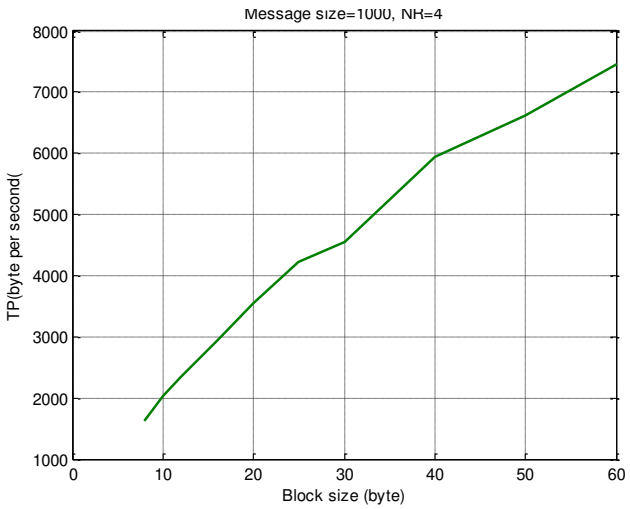

Figure-17. TP when varying block size.

Varying the number of rounds will increase the level of security providing a high level of message protection, but the throughput will drop and it remains acceptable compared with the DES method, Table-5 shows the obtained results of message cryptography when varying the number of rounds, while Figures 18 and 19 show how the number of rounds will affect ET/DT and TP.

Table-5. Method efficiency when varying number of rounds (Message length=1000, block size =64 byte).

Number of rounds	Number of blocks	ET/DT(second)	TP (byte per second)
1	16	0.0820	12195
2	16	0.0970	10309
4	16	0.1790	5586.6
6	16	0.1660	6024.1
8	16	0.2340	4273.5
9	16	0.2180	4587.2
10	16	0.2310	4329.0
12	16	0.2720	3676.5
14	16	0.3070	3257.3
16	16	0.4520	2212.4
Average		0.2238	5645.1

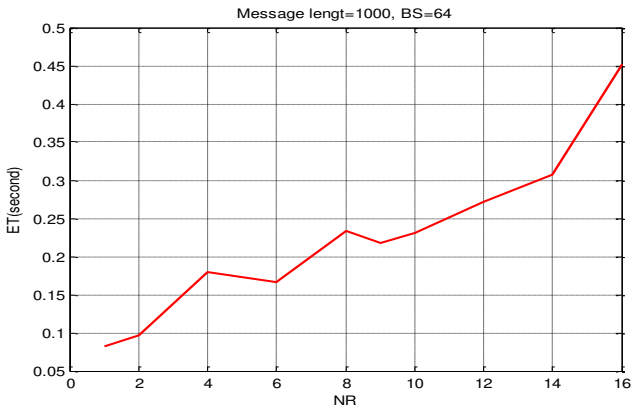

Figure-18. ET vs NR.

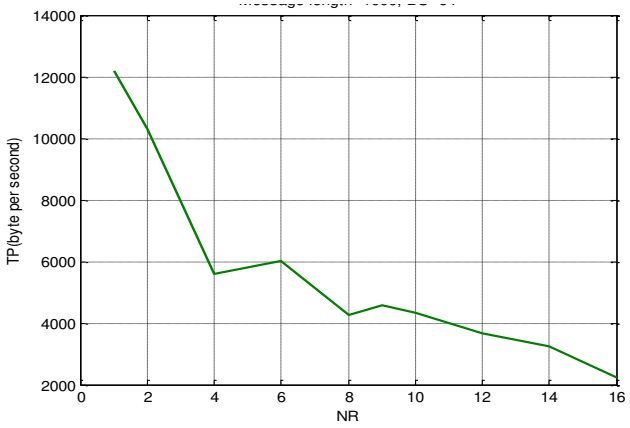

Figure-19. TP vs NR.

The proposed method was tested for quality, and the calculated MSE and PSNR were acceptable in both the encryption and decryption phases as shown in Table-6.

Table-6. Quality parameters for the proposed method.

Message length	MSE	PSNR
10	5429.9	23.2799
25	15576	14.2116
50	12342	16.6175
100	12466	16.4389
200	13047	16.0620
400	14178	15.2309
500	13244	15.9124
600	13137	15.9935
800	13406	15.7903
1000	13016	16.0855

5. CONCLUSIONS

A simple efficient and highly secure method of message cryptography was introduced. The proposed method used two image_keys to generate the required cryptography private keys, these images are to be kept secret and agreed upon between the sender and receiver, and they can be replaced when the need arises without modification to the method. The proposed method used a variable block size and a variable number of rounds to accomplish message cryptography, the block size and the number of rounds are to be determined by the sender and receiver and they are kept secret.

The proposed method was implemented using various messages and various block sizes and various numbers of rounds, the obtained results were compared with DES results and it was shown that the proposed method decreased both the encryption and decryption times, and thus increased the throughput of the process of cryptography. The proposed method destroyed the source message after encryption and recovers the original message after decryption, the obtained values of MSE and PSNR were excellent.

ACKNOWLEDGMENT

The researchers are grateful to the Applied Science Private University, Amman, Jordan, for the full financial support grated to this research project.

REFERENCES

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

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

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

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

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

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

[7] Aws Al Qaisi, Mokhled Al Tarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah. 2019. Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA. 17(3): 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. 2020. Valuable Wavelet Packet Information to Analyze Color Images

Features, International Journal of Current Advanced Research. 9(2): 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. 2019. Suggested Method to Create Color Image Features Victor. Journal of Engineering and Applied Sciences. 14(1): 2203-2207.

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

[13] Yousf Eltous Ziad A. Al Qadi, Ghazi M. Qaryouti, Mohammad Abuzalata. 2020. Analysis of Digital Signal Features Extraction Based on Kmeans Clustering. International Journal of Engineering Technology Research & Management. 4(1): 66-75.

[14] Ziad A Al Qadi Amjad Y Hindi, O Dwairi Majed. 2020. Procedures for Speech Recognition Using Lpc and Ann. International Journal of Engineering Technology Research & Management. 4(2): 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). 9(5): 4092-4098.

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

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

[18] Aws Al-Qaisi, Saleh A. Khawatreh, Ahmad A. Sharadqah, Ziad A. Alqadi. 2018. Wave File Features Extraction Using Reduced LBP. International Journal of Electrical and Computer Engineering. 8(5): 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. 2019. Enhancing the Capacity of LSB Method by Introducing LSB2Z Method. International Journal of Computer Science and Mobile Computing. 8(3): 76-90.

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

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

[23] Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi. 2022. A Technique to Encrypt-decrypt Stereo Wave File. International Journal of Computer and Information Technology. 5(5): 465-470.

[24] Musbah J. Aqel, Ziad AL Qadi, Ammar Ahmed Abdullah. 2018. RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication. International Journal of Engineering and Technology. 7(3): 104-107.

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

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

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

[28] Ziad A. Al Qadi, 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. 2019. A New Approach for Data Cryptography. International Journal of Computer Science and Mobile Computing. 8(9): 30-48.

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

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

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

[33] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein. 2016. A Comparison between Parallel and Segmentation Methods Used For Image Encryption-Decryption. International Journal of Computer Science & Information Technology (IJCSIT). 8(5): 125-131.

[34] Prof. Ziad A. Alqadi. 2021. A Simple Method to Encrypt-Decrypt Speech Signal. International Journal of Engineering Technology Research & Management. 5(2): 44-52.

[35] Ziad AL Qadi. 2007. Analysis of stream cipher security algorithm. Journal of Information and Computing Science. 2(4): 288-298.

[36] Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Qazem Jaber. 2019. Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation. International Journal of Computer Science and Mobile Computing. 8(3): 14-26.

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

[38] Amjad Y. Hindi, Majed O. Dwairi, Ziad A. Al Qadi. 2019. A Novel Technique for Data Steganography, Engineering. Technology and Applied Science Research. 9(6): 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). 9(5): 4092-4098.

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

[41] Akram A. Moustafa, Ziad A. Alqadi. 2009. 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.

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

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

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

[45] ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary. 2008. Performance analysis and evaluation of parallel matrix multiplication algorithms. World Applied Sciences Journal. 5(2): 211-214.

[46] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A. A. Alqadi. 2019. A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE). 9(5): 4092-4098.

[47] Ziad Alqadi. 2009. 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.

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

[49] M. Abu-Faraj, A. Al-Hyari and Z. Alqadi. 2022. A Dual Approach for Audio Cryptography. Journal of Southwest Jiaotong University. 57(1): 24-33.

[50] M. Abu-Faraj, A. Al-Hyari and Z. Alqadi. 2022. Complex Matrix Private Key to Enhance the Security Level of Image Cryptography. Symmetry. 14(4): 664-678.

[51] M. Abu-Faraj, K. Aldebei, and Z. Alqadi. 2022. Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography. Traitement du Signal. 39(1): 173-178.

[52] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi. 2021. Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study. Journal of Southwest Jiaotong University. 56(6): 685-694.

[53] M. Abu-Faraj, Z. Alqadi and K. Aldebei. 2021. Comparative Analysis of Fingerprint Features Extraction Methods. Journal of Hunan University Natural Sciences. 48(12): 177-182.

[54] M. Abu-Faraj and Z. Alqadi. 2021. Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography. International Journal of Computer Science and Network Security (IJCSNS). 21(12): 648-656.

[55] M. Abu-Faraj and Z. Alqadi. 2021. Improving the Efficiency and Scalability of Standard Meth- ods for Data Cryptography. International Journal of Computer Science and Network Security (IJCSNS). 21(12): 451-458.

[56] M. Abu-Faraj and Z. Alqadi. 2021. Using Highly Secure Data Encryption Method for Text File Cryptography. International Journal of Computer Science and Network Security (IJCSNS). 21(12): 53-60.