Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/180214

The Cryptography of Secret Messages using Block Rotation Left Operation

Mazen Alzyoud[1,*], *Saleh Alomar*[2], *Akram Mustafa*[1], *Najah Al-shanableh*[1], *Mohammad Subhi Al-Batah*[2], *Ziad A. Alqadi*[3], *and Sulieman Ibraheem Shelash Al-Hawary*[4]

[1]Department of Computer Science, Faculty Of Prince Al-Hussein Bin Abdallah II for IT, Al al-Bayt University, 25113 Mafraq, Jordan
[2]Department of Networks and Cybersecurity,The Faculty of Science and Information Technology, Jadara University, 21110 Irbid, Jordan
[3]Faculty of Engineering Technology, Al-Balqa Applied University, 11937 Amman, Jordan
[4]Department of Business, School of Business, Al al-Bayt University, 25113 Mafraq, Jordan

Received: 11 Nov. 2023, Revised: 12 Dec. 2023, Accepted: 15 Dec. 2023
Published online: 1 Mar. 2024

Abstract: Long and short text messages are widely transmitted through various communication media, and some of these messages may be very secret or of a special nature, which requires protecting them from the danger of abusers, intruders, or data hackers. Given the importance of protecting text messages, a novel method will be presented focusing on simplifying the procedures to protect data and make the hacking process difficult.A high-level protection method will be provided using the complicated variable content private key; this key can be easily changed without changing the sequence of operations used in the encryption and decryption phases.A secret color image is to be used to generate the private key;both the sender and receiver must save this image, and the selected image key can be easily resized to get a key equal to the secret message length.To increase the degree of protection, it is recommended to divide the text message into blocks with a selected size, the sender and receiver must determine the size, and the byte in each block is to be combined into one vector. This vector will be rotated left using a specified number of bits determined by the sender and receiver.The proposed method will be implemented using various color images and text messages, and the results will be compared with other methods to prove the achievements obtained by the proposed method.

Keywords: Cryptography, SMS, PK, correlation coefficient, MSE, PSNR, e throughput

1 Introduction

Recently, social media has spread widely, and the process of exchanging text messages between different parties has increased dramatically, which requires us to protect many of these messages, especially as they may be highly confidential or of a personal nature. No third, not authorized party is to view Get the text message and understand its content. One of the most important ways to protect SMS and long text messages is to use the data cryptography method [1,2,3,4,5,6,7].

Data cryptography means [8,9,10,11,12,13,14] executing two phases: encrypting the original data in the encryption phase using the private key and a sequence of operations and decrypting the encrypted data in the decryption phase using the same PK and the same sequence of operations with some minor changes, Encryption means distorting and destroying actual data which becomes ambiguous, understood unusable, while decryption means recovering the original data. Datacryptography can be implemented using the source data, as shown in Figure 1; this data must proceed using a selected method and a selected private key (PK) known by the sender and receiver [15,16,17,18,19].

The selected method of data cryptography must meet the following requirements [20,21,22,23,24,25]:

1. The data destruction degree in the encryption phase must be very high, the quality parameters can measure this, and in the research paper, we will use mean square error (MSE) shown in equation 1, peak signal-to-noise ratio (PSNR)shown in equation 2, and correlation coefficient (CC) between the original and the encrypted –decrypted data.

* Corresponding author e-mail: malzyoud@aabu.edu.jo

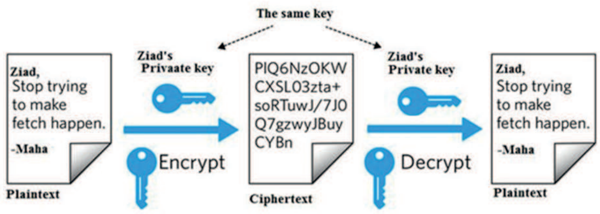

Fig. 1: Data cryptography process

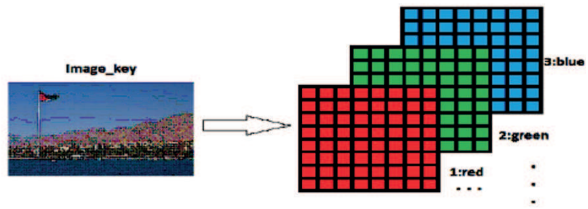

Fig. 2: Color image representation

2.In the encryption phase, the value of MSE must be very high, the PSNR value must be very low, and the CC value must be very far from 1.

3.In the decryption phase, the MSE value must be close to zero, the PSNR value must be close to infinite, and the CC value must be close to 1.

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

$$PSNR = 10\times log_{10}\frac{(MAX_1)^2}{MSE_t} \quad (2)$$

The selected method of cryptography must meet the requirements of good cryptography by achieving the following points, optimized values of the quality parameters during the encryption and decryption phases, Minimizing the encryption and decryption time to maximize the method throughput (number of bytes encrypted or decrypted in one second) and Flexibility and ease of implementation of the method and the ease of making any acceleration if necessary. The confidential data used to create the secret key is complex and difficult to decipher or hack.

The research paper uses a confidential color image as an image key to generate the necessary PK to complete the encryption and decryption process. Choosing a color image as an image key is due to the reasons [12,13,14].

1.Digital color image is a 3D matrix (one 2D matrix for each color: red, green, and blue), as shown in Figure 2. This matrix simplifies the process of color image manipulation.

2.Each pixel value of the color image matches an ASCII value of the message, and the pixel value is within the range of 0 to 255 [26,27,28,29,30,31].

3.Ease of obtaining the digital color image due to the diversity of its sources and the possibility of obtaining it without any cost.

4.The possibility of dealing with the matrix of each of the three colors separately and employing this matrix for various purposes, the most important of which is the generation of the private key [3,32,33,34,35,36,37].

5.Ease of carrying out many operations on the color matrix and the possibility of obtaining matrices of the image and the required dimensions by resizing the digital image, as shown in Figures 3, 4, and 5.

6.The possibility of replacing the image used at any time through an agreement between the recipient and the recipient without modifying the cryptographic method used [1,10,11,38,39].

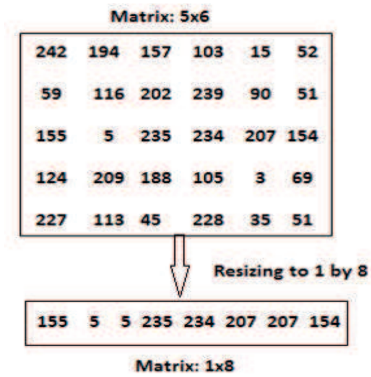

Fig. 3: Matrix resizing example

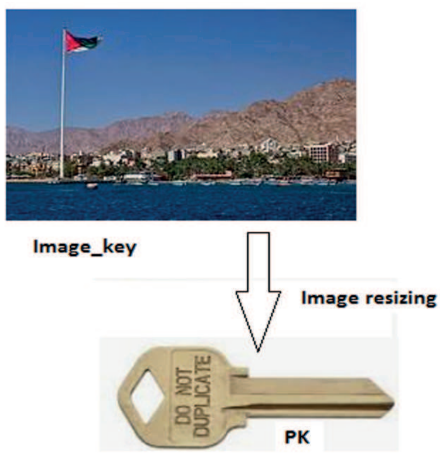

Fig. 4: PK generation

Fig. 5: Using image colors to generate PKs

Using the digital color image as an image_key in the proposed method will achieve the following benefits [29, 30, 31, 41, 42, 43, 44, 45, 46, 47, 48]:

1. The color digital image used as the key is kept secret, making it impossible to identify.
2. The possibility of using one of the colors in the image to generate the private key.
3. The possibility of employing the image to generate any private key and size.
4. The possibility of replacing the image with another without affecting the method used.

2 Methodology

Many methods of secret data cryptography and the majority of these methods were designed based on a standard DES (data encryption standard) such as 3DES, AES, and blowfish (BF) methods [49, 50, 51, 52]. These standard methods operate in the fashion using various lengths and numbers of some parameters used in each, as shown in Table 1 [53, 54, 55, 56].

The technique of Standard encryption methods have standard features that are regarded as cons:

1. For Each method used on PK, this key's length is fixed and cannot be changed.
2. The encrypted data must be divided into blocks;the block size is also fixed and cannot be changed.
3. A series of rounds must be executed;the number of rounds is fixed and cannot be changed.
4. Key generation is required. The PK is to be used to generate other required sub key [29, 30, 31, 32].
5. These methods provide excellent values quality parameters in both phases: Encryption and decryption.
6. These methods are efficient when dealing with data with small and medium sizes;when the data size increases, the throughput will rapidly drop down, and the methods will be inefficient [42, 43, 44, 45, 46, 47].
7. Increasing the number of required rounds will slow the cryptography process.
8. Most of these methods require an S-box, this box must be created and manipulated, and extra CPU time and memory space size are required [38, 39].

The proposed technique uses two logical operations: rotating left with a selected number of digits and XORing the message block generated from the image key PK. The rotation left operation is presented in Figure 6 and Figure 7.

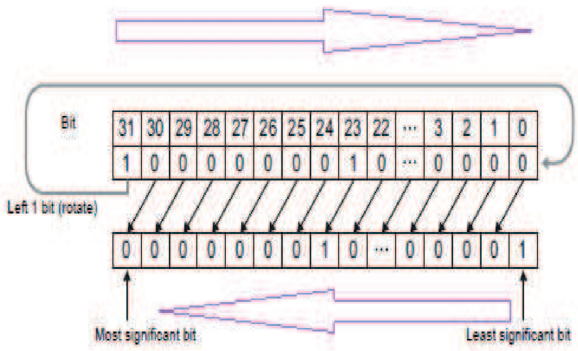

Fig. 6: Rotate left implementation

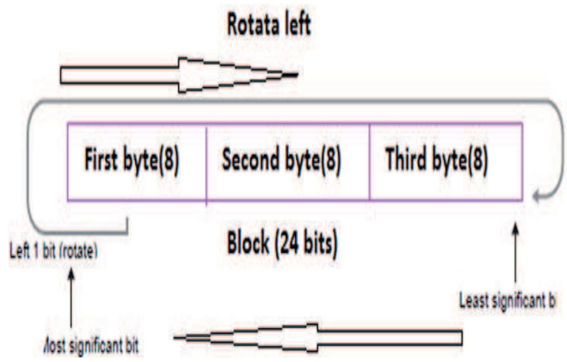

Fig. 7: Message block rotation

Fig. 8 shows an example of message block rotation during the encryption and decryption phases.

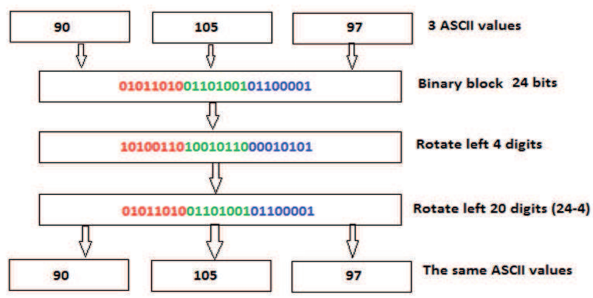

Fig. 8: Block rotation example using a selected number of digits

Table 1: Standard encryption methods characteristics

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, Know 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
Simplicity	No	No	No	No
Security level	Adequate	Adequate	Excellent	Excellent
Throughput	Low	Low	Low	Moderate

The XORing operation is to be implemented for Encryption and decryption using the message and the generated PK as shown in Fi. 9 and Fig. 10. Here, we have to notice that we can select a sequence of rotate and XORing operations to increase the level of security, in our paper research the sequence will contain rotation and XORing in the encryption phase and XORing and rotation in the decryption phase.

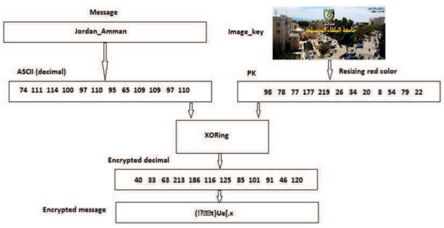

Fig. 9: Using XORing in the encryption phase example

The security level can be achieved by using the following secret information:

1. The secret image key.
2. The color matrix used to generate the PK.
3. The number of digits used for rotation left operation (RLD), from 1 to 23, in the decryption,will equal the number of digits or rotation (block size in bytes – RLD).
4. The sequence of implemented logical operations.

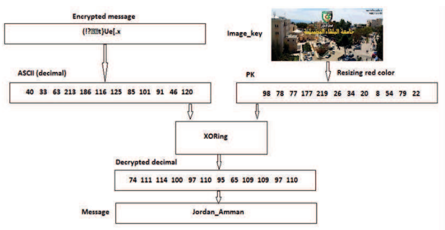

Fig. 10: Using XORing in the decryption phase example

A. The proposed algorithm for Encryption and decryption

1. Encryption Algorithm

Inputs: Secret message, color image key, Color matrix to be used to generate PK, RLD, operation sequence

Output: Encrypted message

Process:

1. Get the inputs.

2. Resize the color channel matrix to message size.

3. For every 3 bytes in the message, do the following.

Convert each byte to binary.

Merge the binary number into a one-row array.

Rotate left the block array RLD times.

Convert the array back to decimal.

Store each byte in the block in the message array.

4. Apply XORing the rotated message with PK to get the encrypted message

2. Decryption algorithm

Inputs: The encrypted message, color image key, and Color matrix to be used to generate PK, RLD, and operation sequence

Output: Decrypted message

Process:

1. Get the inputs.
2. Resize the color channel matrix to message size.
3. Apply XORing the encrypted message with PK to get a new message.
4. Do the following for every 3 bytes in the new message.

Convert each byte to binary.

Merge the binary number into a one-row array.

Rotate left the block array 24-RLD times.

Convert the array back to decimal.

Store each byte in the block in the decrypted message array.

3 Results

The proposed method was implemented using Matlab (processor 2.4 MHz, i5 with RAM size =8 G Byte) using various images and in-length messages.Figure 11 shows the used images, while Table 2 shows the basic information aboutthese images.

Fig. 11: Used images

Table 2: Images basic information

Image number	Dimension	Size(byte)
1	151 333 3	150849
2	152 171 3	77976
3	360 480 3	518400
4	1071 1600 3	5140800
5	981 1470 3	4326210
6	165 247 3	122265
7	360 480 3	518400
8	183 275 3	15075
9	183 275 3	150975
10	201 251 3	151353
11	600 1050 3	1890000
12	1144 1783 3	6119256

A message with length=240 characters was selected, and different images were selected as image keys. The parameter MSE, PSNR, CC, and Encryption (decryption) time were calculated. Table 3 shows the obtained experimental results.

From Table 3, we can see that the proposed method provides good values for the quality parameters (MSE, PSNR, and CC), and the proposed method is efficient by providing a high throughput (on average 9125.5 bytes per second (around 9 K bytes per second)). Short messages with various lengths were selected using image twoas an image key; The standard methods of data cryptography were also implemented using the same messages. Table 4 shows the obtained experimental results for a short message.

Table 3: Using various images to encrypt the same message

Image number	MA	PSNR	CC	Encryption(decryption) time (second)
1	7.1214e+003	22.1166	0.0805	0.026000
2	1.1277e+004	17.5201	-0.3739	0.025000
3	6.2011e+003	23.5005	0.1317	0.025000
4	6.1543e+003	23.5763	0.2344	0.032000
5	8.0629e+003	20.8750	0.0493	0.026000
6	4.9396e+003	25.7749	0.3281	0.024000
7	6.1054e+003	23.6560	0.0957	0.024000
8	9.5357e+003	19.1973	-0.2585	0.025000
9	6.7962e+003	22.4267	-0.0268	0.025000
10	7.4988e+003	21.6004	0.0160	0.025000
11	9.6766e+003	18.9720	-0.2448	0.033000
12	7.6899e+003	21.3487	-0.1261	0.025000
Average	7588.2	21.7	-0.0079	0.0263
Throughput(byte per second			9125.5	

From Table 4, we can see that the proposed method is more efficient than the standard method of data cryptography and decreases the encryption time, as shown in Fig. 12.

Table 4: Short messages implementation results

Message length(byte)	Encryption time (second)				
	Proposed	DES	3DES	AES	BF
24	0.005741	0.1510	0.1800	1.1160	0.0864
48	0.007389	0.3020	0.3400	2.2120	0.1528
72	0.007850	0.4580	0.5200	3.3280	0.2392
96	0.008691	0.6140	0.7100	4.4340	0.3256
120	0.010857	0.7700	0.8009	5.5600	0.4120
144	0.011261	0.9260	1.0700	6.6760	0.5084
168	0.022855	1.0820	1.2400	7.8020	0.5048
192	0.013348	1.2380	1.4200	8.8280	0.6512
216	0.014285	1.3040	1.5200	9.9440	0.6776
240	0.015784	1.4600	1.7000	10.7600	0.7640

Long messages with various lengths were selected using image 2 as an image key; the standard methods of data cryptography were also implemented using the same messages. Table 5 shows the obtained experimental results for the long messages.

From Table 5, we can see that the proposed method is more efficient than the standard method of data

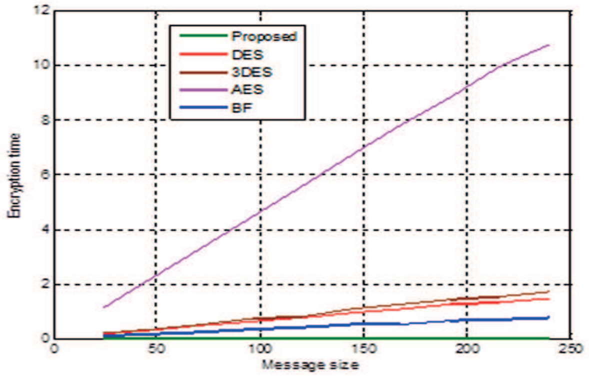

Fig. 12: Encryption time comparisons for short messages

Table 5: Long messages implementation results

Message length(K byte)	Encryption time (second)				
	Proposed	DES	3DES	AES	BF
3	0.184562	18.9680	22.0400	140.8	9.0592
6	0.443673	38.9310	44.0600	282.7	18.1184
9	0.687047	58.9030	66.1100	425.5	29.1776
12	1.035879	78.8620	90.1500	567.4	40.2368
15	1.684129	98.8200	112.1000	710.2	51.2960
18	2.233661	117.8070	135.2300	852.1	62.3552
21	2.685112	136.7750	158.2600	989.9	71.4144
24	3.157145	155.7420	180.3100	1137.8	82.4736
27	3.639037	176.7110	203.3400	1280.6	91.5328
30	4.277896	194.6700	225.2000	1421.5	101.5920

cryptography and decreases the encryption time, as shown in Fig 13.

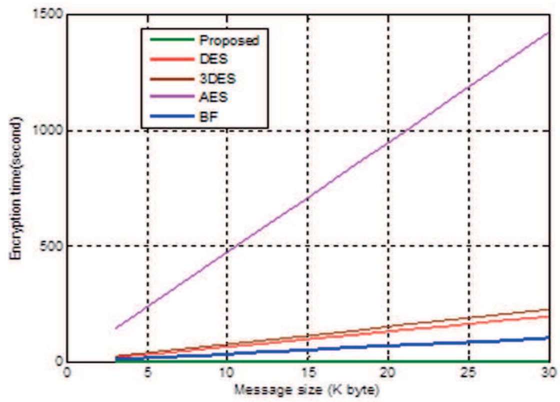

Fig. 13: Encryption time comparisons for long messages

4 Conclusion

A simple method of message cryptography was proposed and implemented. The proposed method provides good data protection by using impossible-to-guess information such as image key, generated PK, sequence of operation, and the number of digits used to rotate the data block. The experimental results showed that the proposed method meets the requirements of good methods of data cryptography by providing excellent values for the quality parameters MSE, PSNR, and CC.The proposed method is more efficient than any standard data cryptography method. It was also implemented and showed that the proposed method significantly decreases the Encryption (decryption) time. It has a better performance by maximizing the encryption (decryption) throughput. It was shown that the proposed method can use any color image regardless of the size and type ofthe image key. This image can be easily changed without needing any method modification keeping the process of message cryptography secure and efficient.

References

[1] A.A. Moustafa, Z.A. Alqadi, Color Image Reconstruction Using a New R'G'I Model, Journal of Computer Science **5**, 250-254 (2009).

[2] K. Matrouk, A. Al-Hasanat, H. Alasha'ary, Z. Al-Qadi Al-Shalabi, Speech fingerprint to identify isolated word person, World Applied Sciences Journal **31**, 1767-1771 (2014).

[3] 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 **96**, 4081-4091 (2018).

[4] Z.A. Alqadi, M.K.A. Zalata, G.M. Qaryouti, Comparative analysis of color image steganography, International Journal of Computer Science and Mobile Computing **5**, 37-43 (2016).

[5] M. Jose, Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality, International Journal of Science and Research **3**, 2281-2284 (2014).

[6] M. Juneja, P.S. Sandhu, *An improved LSB based Steganography with enhanced Security and Embedding/Extraction*, 3rd International Conference on Intelligent Computational Systems, 26-27 (2013).

[7] M. Al-Azzam, M. Al-Alwan, M. Alqahtani, S. Al-Hawary, A. Alserhan, Determinants of behavioral intention to use big data analytics (BDA) on the information and communication technologies (ICT) SMEs in Jordan, Decision Science Letters **12**, 605-616 (2023).

[8] A.A. Moustafa, Z.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**, 355-362 (2009).

[9] I.R. AlTaweel, S. Al-Hawary, The Mediating Role of Innovation Capability on the Relationship between Strategic Agility and Organizational Performance, Sustainability **13**, 7564 (2021).

[10] Z.A. Alqadi, M. Aqel, I.M. El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, World Applied Sciences Journal **5**, 211-214 (2008).

[11] A. Al-Rawashdeh, Z.A. Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research **8**, 1356-1359 (2018).

[12] Z.A. Alqadi, B. Zahran, Q. Jaber, B. Ayyoub, J. Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing **8**, 76-90 (2019).
[13] Z.A. Alqadi, M.O. Al-Dwairi, A.A. Abu Jazar, R. Abu Zneit, Optimized True-RGB color Image Processing, World Applied Sciences Journal **8**, 1175-1182 (2010).
[14] A. Waheeb, Z.A. AlQadi, Gray image reconstruction, European Journal of Scientific Research **27**, 167-173 (2009).
[15] A. AlQaisi, M. AlTarawneh, Z.A. Alqadi, A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, Telecommunication Computing Electronics and Control **17**, 1220-1225 (2018).
[16] Z.A AlQadi, A.Y Hindi, O.M Dwairi, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management **4**, 48-55 (2020).
[17] Z.A. Alqadi, M.T. Barakat, A Case Study to Improve the Quality of Median Filter, International Journal of Computer Science and Mobile Computing **10**, 19–28 (2021).
[18] H.G. Zaini, Z.A. Alqadi, High Salt and Pepper Noise Ratio Reduction, International Journal of Computer Science and Mobile Computing **10**, 88–97 (2021).
[19] N. Shamaileh, M. Eldahamsheh, S. Alneimat, R. Istaiteyeh, I. Azzam, S. Al-Hawary, The effects of smart human resources 4.0 on employee job effectiveness: The mediating role of employee job satisfaction, International Journal of Data and Network Science **7**, 801-808 (2023).
[20] H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. Aalqadi, H. Al-Shalabi, Improving Matrix Multiplication Using Parallel Computing, International Journal on Information Technology **1**, 2281-2911 (2013).
[21] B. Zahran, Z.A. Alqadi, J. Nader, A. Abu Ein, A COMPARISON BETWEEN PARALLEL AND SEGMENTATION METHODS USED FOR IMAGE ENCRYPTION-DECRYPTION, International Journal of Computer Science & Information Technology **8**, 127-133 (2016).
[22] Z.A. Alqadi, A. Abu-Jazar, Analysis of Program Methods Used for Optimizing Matrix Multiplication, Journal of Engineering **15**, 73-78 (2005).
[23] J. Al-Azzeh, B. Zahran, Z.A. Alqadi, B. Ayyoub, M. Mesleh, A Novel Based On Image Blocking Method to Encrypt-Decrypt Color, JOIV: International Journal on Informatics Visualization **3**, 86-93 (2019).
[24] J. Al-Azzeh, B. Zahran, Z.A. Alqadi, B. Ayyoub, M. Abu-Zaher, A Novel Zero-Error Method to Create a Secret Tag for an Image, Journal of Theoretical & Applied Information Technology **96**, 4081-4091 (2018).
[25] M. Al-Azzam, M. Al-Alwan, M. Alqahtani, S. Al-Hawary, A. Alserhan, Determinants of behavioral intention to use big data analytics (BDA) on the information and communication technologies (ICT) SMEs in Jordan, Decision Science Letters **12**, 605-616 (2023).
[26] J.R. Rasras, M. Abuzalata, Z. Alqadi, J. Al-Azzeh, Q. Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation, International Journal of Computer Science and Mobile Computing **8**, 14-26 (2019).
[27] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Mesleh, A Novel Based on Image Blocking Method to Encrypt-Decrypt Color, JOIV: International Journal on Informatics Visualization **3**, 86-93 (2019).
[28] B. Zahran, J. Al-Azzeh, Z. Alqadi, M.A. AL-ZOGHOUL, S. Khawatreh, A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES. Journal of Theoretical & Applied Information Technology **96**, 3014-3024 (2018).
[29] 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 **96** 4081-4091 (2018).
[30] J. AL-AZZEH, B. ZAHRAN, Z. ALQADI, Salt and Pepper Noise: Effects and Removal, International Journal on Informatics Visualization **2**, 252-256 (2018).
[31] J. Nader, Z. Alqadi, B. Zahran, Analysis of Color Image Filtering Methods, International Journal of Computer Applications **174**, 12-17 (2017).
[32] J. Al Azzeh, Z. Alqadi, Q.M. Jabber, *Statistical Analysis of Methods Used to Enhanced Color Image Histogram*, In XX International Scientific and Technical Conference, 24-26 (2017).
[33] J. Al Azzeh, H. Alhatamleh, Z. Alqadi, M.K. Abuzalata, Creating a Color Map to be used to Convert a Gray Image to Color Image, International Journal of Computer Applications**153**, 31-34 (2016).
[34] K. Matrouk, A. Al-Hasanat, H. Alasha'ary, Z. Al-Qadi, H. Al-Shalabi, Analysis of Matrix Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing **8**, 76-90 (2019).
[35] M. Abuzalata, Z. Alqadi, J. Al-Azzeh, Q. Jaber, Modified Inverse LSB Method for Highly Secure Message Hiding, International Journal of Computer Science and Mobile Computing **8**, 93-103 (2019).
[36] Q. Jaber, R.J. Rasras, M. Abuzalata, Z. Alqadi, J. Al-Azzeh, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation, International Journal of Computer Science and Mobile Computing **8**, 14-26 (2019).
[37] J. Al-Azzeh, Z. Alqadi, M. Abuzalata, Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving, International Journal of Computer Science and Mobile Computing **8**, 20-33 (2019).
[38] N. Asad, I. Shayeb, Q. Jaber, B. Ayyoub, Z. Alqadi, A. Sharadqh, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC **8**, 50–62 (2019).
[39] M.O. Al-Dwairi, A.Y. Hendi, M.S. Soliman, Z.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering **9**, 4092-4098 (2018).
[40] Z. Alqadi, B. Zahran, J. Nader, Estimation and Tuning of FIR Low pass Digital Filter Parameters, International Journal of Advanced Research in Computer Science and Software Engineering **7**, 18-23 (2017).
[41] K. Aldebei, M. Abu-Faraj, Z. Alqadi, Comparative Analysis of Fingerprint Features Extraction Methods, Journal of Hunan University Natural Sciences **48**, 177-182 (2022).
[42] M. Barakat, Z. Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering and Science **6**, 49-55 (2022).
[43] Z. Alqadi, 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 **21**, 648-656 (2021).
[44] Z. Alqadi, M. Abu-Faraj, K. Aldebei, Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study, Journal of Southwest Jiaotong University **56**, 686-694 (2021).
[45] Z. Alqadi, M. Abu-Faraj, Improving the Efficiency and Scalability of Standard Methods for Data Cryptography, International Journal of Computer Science and Network Security **21**, 451-458 (2021).
[46] M. Abu-Faraj, Z. Alqadi, Using Highly Secure Data Encryption Method for Text File Cryptography, International Journal of Computer Science and Network Security **20**, 53-60 (2021).
[47] N. Dwijendra, I. Arsana, S. Al-Hawary, A. Prakaash, R. Parra, A. Jalil, A. Hammid, Operation of the Multiple Energy System with Optimal Coordination of the Consumers in Energy Market, Environmental and Climate Technologies **27**, 1-13 (2023).
[48] D. Eleimat, M. Ebbini, L. Aryan, S. Al-Hawary, The effect of big data on financial reporting quality, International Journal of Data and Network Science **7**, 1775-1780 (2023).
[49] D.S.A. Elminaam, H.M. Abdul Kader, M. Hadhoud, Performance Evaluation of Symmetric Encryption Algorithms, IJCSNS International Journal of Computer Science and Network Security **8**, 280-286 (2008).
[50] W. Stallings, *Cryptography and Network Security* (4th Edition), Pearson Prentice Hall, United States (2006).
[51] S.S. Preet, M. Raman, Comparison of Data Encryption Algorithms, International Journal of Computer science and Communications **2**, 125-127 (2011).
[52] A. Rahamneh, S. Alrawashdeh, A. Bawaneh, Z. Alatyat, A. Mohammad, S. Al-Hawary, The effect of digital supply chain on lean manufacturing: A structural equation modelling approach, Uncertain Supply Chain Management **11**, 391-402 (2023).
[53] S. Gurjeevan, K. Ashwani, K.S. Sandha, A Study of New Trends in Blowfish Algorithm, International Journal of Engineering Research and Applications **1**, 321-326 (2011).
[54] A. Monika, M. Pradeep, A Comparative Survey on Symmetric Key Encryption Techniques, International Journal on Computer Science and Engineering **4**, 877-882 (2012).
[55] S. Mehrotra, M. Rajan, Comparative analysis of Encryption algorithm for data communication, International Journal of Computer Science and Technology **2**, 292-294 (2011).
[56] R. Alshawabkeh, H. AL-Awamleh, M. Alkhawaldeh, R. Kanaan, S. Al-Hawary, A. Mohammad, R. Alkhawalda, The mediating role of supply chain management on the relationship between big data and supply chain performance using SCOR model, Uncertain Supply Chain Management **10**, 729-736 (2022).