VOL 3 (2019) NO 1

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

A Novel Based on Image Blocking Method to Encrypt-Decrypt Color

Jamil Al-Azzeh[#], Bilal Zahran[#] , Ziad Alqadi[#], Belal Ayyoub[#], Muhammed Mesleh[#]

[#] Computer Engineering Department, Al Balqa'a Applied university, Amman, 11134, Jordan
E-mail: azzehjamil@gmail.com, zahranb@bau.edu.jo, natalia_maw@yahoo.com, belal_ayyoub@hotmail.com, meslehmuh@gmail.com

***Abstract*— Encryption of digital color image is the process of conversion original digital color image into an encrypted one to protect the image from hacking or to prevent an authorized person to get the valuable information located in the color image. The process of color image encryption-decryption is very important issue in human activities and here in this paper we will introduce a new simple, efficient and highly secure method to be used for color image encryption-decryption. The proposed method will be tested and implemented, the efficiency parameters of the proposed method will be calculated and will be compared with other methods parameters to prove the efficiency issues of the proposed method.**

***Keywords*— Encryption Time, Decryption Time, Throughput, MSE, PSNR, Speedup**

I. Introduction

Digital RGB color image can be represented by a 3D matrix, which is consisted of 3 2D matrixes, the first one as shown in figure refers to the red channel (component), and the second refers to the green channel, while the third refers to the blue channel [1][7][8].

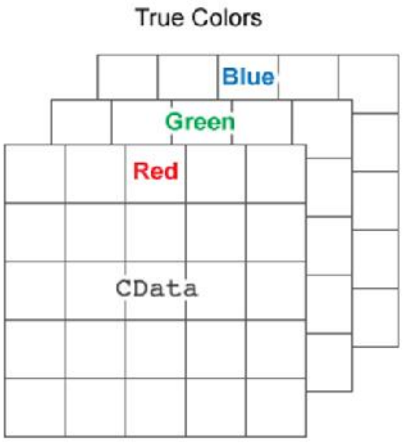


Fig 1. 3d Color Image Matrix.

Combining the three matrices to gather will give the appropriate color for each individual pixel.

Encryption of RGB color image [19] is the process of conversion original digital color image into an encrypted one to protect the image from hacking or to prevent an authorized person to get the valuable information located in the color image [2],[3]. While, the decryption process is considered as the reverse of encryption process that includes of converting back the encrypted color image into its original image without losing any piece of information, which means that the error between the original image and the decrypted one must equal zero. In RGB color images, the encryption process should be carried out before transmitting the image over the internet securely and to ensure that no any unauthorized user can perform any decryption process for this image. The encryption process for image, video and other chaos based techniques have many applications in many areas like medical imaging, internet communication, transmission, military Communication, etc. The progress in encryption techniques is moving towards a future of endless possibilities and applications. The image data have special features such as a huge capability, high correlation between the pixels, and a high redundancy. Encryption techniques are very useful tools to protect private information [4].

Data encryption is the main technique that used to secure the data resources over the internet, intranets and extranets and to provide an authentication process for the users' data resources from integrity, accuracy and safety perspectives [5].

There are many ways to encrypt-decrypt digital color images, and when talking about the efficiency of a particular method, the following important factors must be taken into account:

- Encryption time: time in seconds needed to implement the selected method to convert the original image to encrypted one, this time must be as small as possible.

- Decryption time: time in seconds needed to implement the selected method to convert the encrypted image to the original one, this time must be as small as possible.
- Throughput: number of bits encrypted or decrypted per a second, yjis parameter must be maximized.
- Mean square error: mean square error (MSE) is the error between 2 images [6], it is calculated using the following equation:

  Where: X, Y are the color images; r: number of rows; c: number of columns; p: number of colors (p=3).

  In the encryption process MSE between the original image and the encrypted one must be high, but in the decryption process, MSE between the decrypted image and the original one must be closed to zero.
- Peak signal to noise ratio: peak signal to noise ratio (PSNR) is most commonly used to measure the quality of reconstruction of loss information, and it is calculated using the following formula:

$$d= \max(\max(X), \max(Y))$$

The value of PSNR between the original image and the encrypted one must be small, but between the decrypted image and the original one must by high, by these values we can measure the image quality.

II. Related works

Recently, many methods have been used for data encryption and decryption. Many of these methods rely on the use of encryption standards like the data encryption standard Many works were done in image encryption decryption (DES)[9], these methods suffer from low throughput causes by a high time of encryption-decryption , which make these methods un efficient[10],[11].

In [12], the author proposed a method of encryption-decryption by reshaping the 3D color matrix to 2D matrix, squaring the matrix, generating a secret key with size equal image size, then applying matrix multiplication to get the decrypted image. This method provides a good throughput but the size of the encryption-decryption key is very huge, and it must equal the original image size, so it is very difficult to remember the key, and thus the method require more memory space for storing and more time for transferring, thus negatively affecting the proposed here method efficiency.

In [13] an image encryption-decryption method was proposed, this method used a double logistic maps, in which the image matrix was confused from row and column respectively. This method is efficient but the confusion effect is carried out by the substitution stage and Chen's system is employed to diffuse the gray value distribution. In [14] a method of encryption-decryption was proposed, this method is based on matrix reordering and it has a medium throughput. In [15] a method of image encryption-decryption was suggested by a Chaotic Algorithm applying using the power and tangent functions instead of linear function. The process of encryption is one-time-one-password system and is more secure (but not enough) than the DES algorithm, also it has low efficient parameters with big encryption-decryption time and low throughput. In [16], An Asymmetric image encryption-decryption method was introduced, this method is based on matrix transformation but it has high encryption-decryption time and thus low throughput. In [17] a method based on Rubik's Cube Principle was proposed it has a good security level but the throughput is low. In [18] a method of encryption-decryption was presented, this method is based on using Chaos-controlled Poker Shuffle Operation, both variants of this method (A-I and A-II) have a poor throughput.

III. The proposed method

The proposed method for encryption the color image can be implemented applying the following steps:

1) Get the original color image.
2) Reshape the 3D color image matrix to 2D gray image as shown in figure (2).
3) Divide the 2D image matrix into blocks with equal sizes as shown in figure (3).
4) Select a secret key with size equal block size (each element in the key matrix must be within the range 0 to 255).
5) Save the secret key to be used in decryption phase.
6) Get the encrypted block by applying XOR operation between the original block and the key.
7) Reshape back the encrypted 2D matrix to 3D matrix to get the encrypted color image.

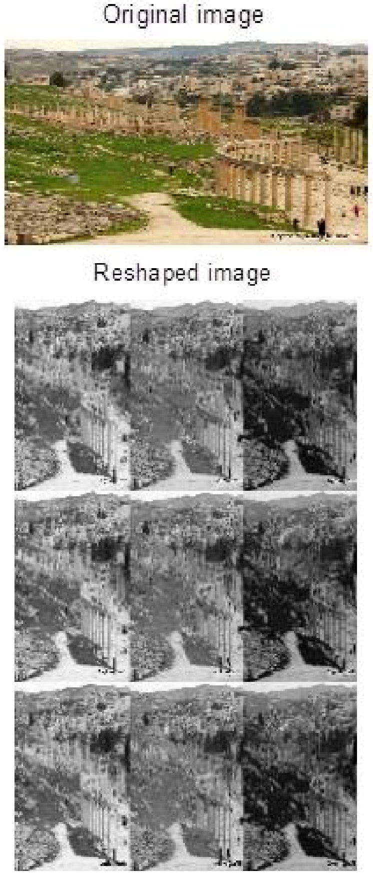
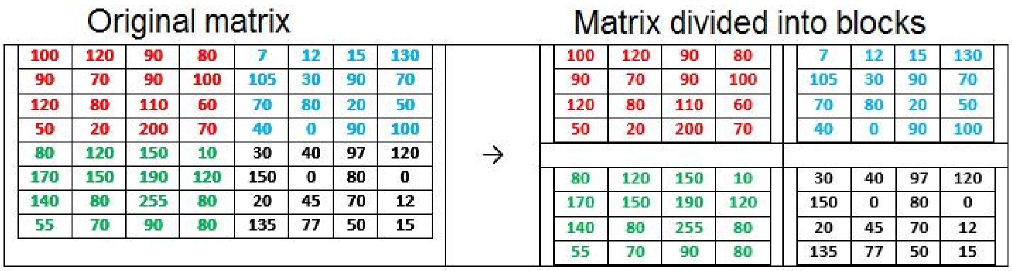


Fig 2. Color Image Reshaping



Original matrix

100	120	90	80	7	12	15	130
90	70	90	100	105	30	90	70
120	80	110	60	70	80	20	50
50	20	200	70	40	0	90	100
80	120	150	10	30	40	97	120
170	150	190	120	150	0	80	0
140	80	255	80	20	45	70	12
55	70	90	80	135	77	50	15

→

Matrix divided into blocks

100	120	90	80
90	70	90	100
120	80	110	60
50	20	200	70

7	12	15	130
105	30	90	70
70	80	20	50
40	0	90	100

80	120	150	10
170	150	190	120
140	80	255	80
55	70	90	80

30	40	97	120
150	0	80	0
20	45	70	12
135	77	50	15

Fig 3. Dividing 2d Image To Blocks

The proposed method for decryption the color image can be implemented applying the following steps:

1) Get the encrypted color image.
2) Reshape the 3D color image matrix to 2D gray image.
3) Divide the 2D image matrix into blocks with equal sizes.
4) Use the secret key.
5) Get the decrypted block by applying XOR operation between the encrypted block and the key.
6) Reshape back the decrypted 2D matrix to 3D matrix to get the encrypted original color image.

IV. Implementation and Experimental Results

The proposed method of color image encryption-decryption based on 2D matrix blocking was implemented and all the obtained results showed that MSE between the original image and the decrypted one was always zero (PSNR=infinite), which means that there is no loss of information and the decrypted image is the same as original image. Figures (4), (5), and (6) show some of the obtained results.

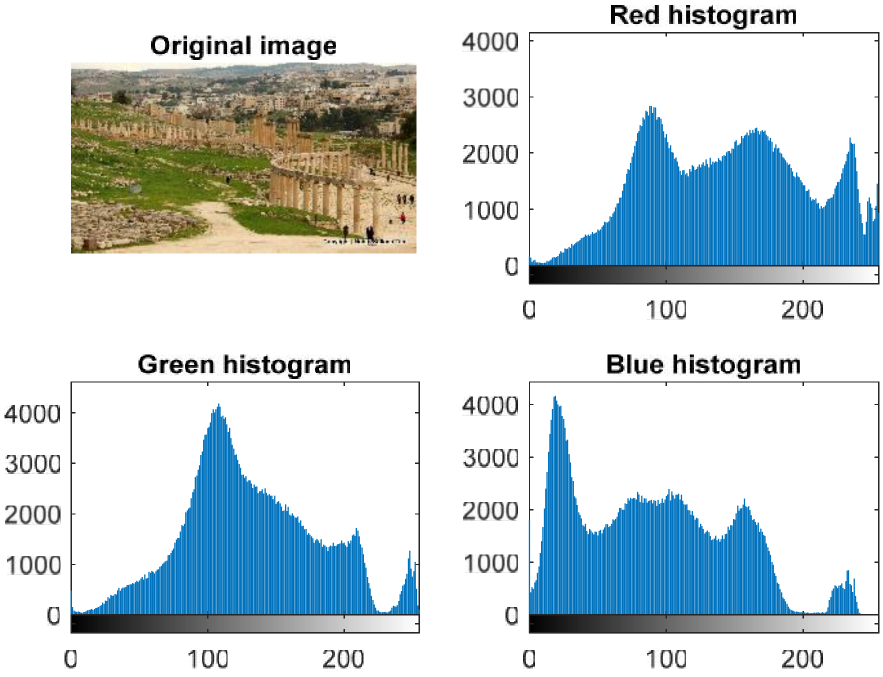


Fig 4. Original Color Image

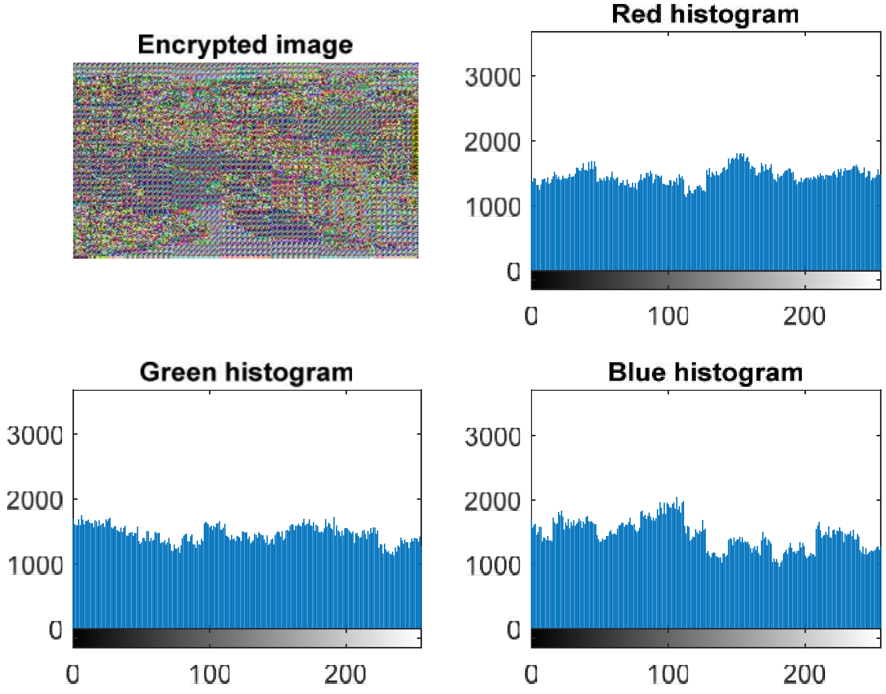


Fig 5. Encrypted Color Image

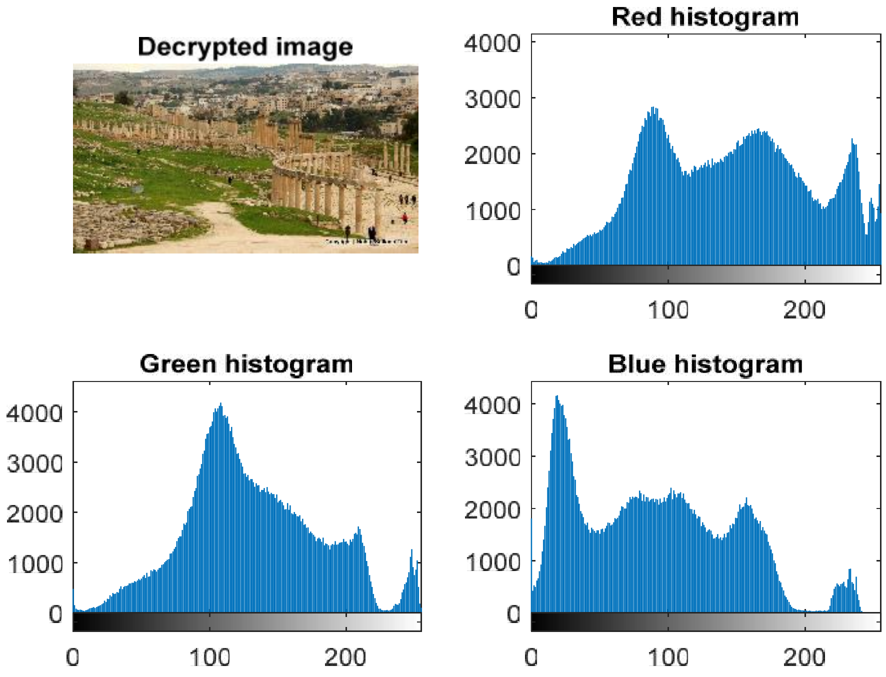


Fig 6. Decrypted Color Image

1. MSE between the original image and the encrypted one was very high (very low value of PSNR), which means that the encrypted image was differ and it is impossible to guess the image or recognize it by human eyes as shown in figure (5).

2. The proposed method uses a key of at least 16 element (4 by 4 matrix with values from 0 to 255, this make it difficult to guess the key and will increase the number of combinations to 256 raised to the power 10, thus will extremely increase the security level of the proposed method.

3. The experimental results showed that increasing the block size will decrease the encryption-decryption times (increase the method throughput which is measured in M bits and obtained by dividing the image size in Mbits by the encryption time in seconds. Table (1) shows the experimental results of applying the method for an image with size equal 8.5876 Mbits using various block sizes, from this table we can see that selecting a 4 by 4 key will give an acceptable performance using a simple small key.

TABLE 1
METHOD PARAMETERS WITH FIXED IMAGE SIZE AND VARIABLE BLOCK SIZE

Block size	Encryption time	Throughput	PSNR between original and encrypted images
2x2	0.5630	15.2534	22.6542
3x3	0.2700	31.8061	20.6512
4x4	0.1470	58.4194	21.6316
5x5	0.0970	88.5324	23.8235
6x6	0.0690	124.4586	25.7486

The proposed method was implemented using various color images in type and size fixing the block size to 4 by 4 and the results of this experiment are shown in table 2

TABLE 2
ENCRYPTION-DECRYPTION VARIOUS IMAGES WITH FIXED BLOCK SIZE

Image size	Encryption time	throughput	MSE between the original and the encrypted images	PSNR between original and encrypted images
0.3750	0.0060	62.5000	6.9494e+003	22.3612
1.1494	0.0190	60.4971	7.5959e+003	21.4716
1.1536	0.0190	60.7139	7.2026e+003	22.0034
1.1539	0.0190	60.7332	8.6048e+003	20.2245
1.1547	0.0190	60.7754	7.2832e+003	21.8921
1.1559	0.0200	57.7972	1.0213e+004	18.5113
1.1587	0.0200	57.9357	7.3874e+003	21.7499
2.0599	0.0360	57.2205	8.2597e+003	20.6338
2.0672	0.0360	57.4214	9.0620e+003	19.7069
3.2959	0.0560	58.8553	7.5507e+003	21.5313
4.1199	0.0710	58.0264	8.5676e+003	20.2679
7.0862	0.1280	55.3608	8.1219e+003	20.8021
8.5876	0.1470	58.4194	7.4877e+003	21.6151
16.7370	0.2870	58.3170	7.6785e+003	21.3635
18	0.3160	56.9620	8.7233e+003	20.0877
25.9100	0.4530	57.1964	8.4783e+003	20.3726
94.6241	1.6440	57.5572	7.8238e+003	21.1760
AV=11.1641	AV= 0.1939	Av= 58.6052		

From table (2) we can see that the average encryption time is significantly small, which means good performance for the proposed method, also we can see that MSE always has a high value, and PSNR has a small value, meaning that the image was really encrypted.

From table (2) we can see that increasing the image size will lead to increasing the encryption time and the relationship between the encryption (decryption) time and the image size is closed to linear relation as shown in figure (7).

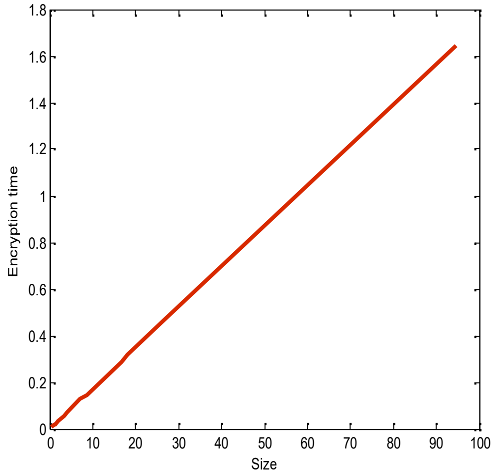


Fig 7. Relationship Between Encryption Time And Image Size

Color image matrix is consisted of three 2D matrices, the first one for the red color, the second for the green color, and the third one for the blue color, So we can extract the matrix of each color, then encrypt it and after that reconstruct again the encrypted three 2D matrices to get the encrypted color image.

The proposed method was implemented several times using various images, the two approaches were used and the experimental method showed that reshaping approach gave better results than the extraction-reconstructing approach as shown in table (3).

TABLE 3
COMPARISONS BETWEEN RESHAPING AND RECONSTRUCTING APPROACHES

Image size	Using reshaping(1)			Encrypting each color matrix(2)		
	Encryption time(3)	Throughput (4)	PSNR between original and encrypted images	Encryption time(5)	Throughput (6)	PSNR between original and encrypted images
0.3750	0.0060	62.5000	22.3612	0.0130	28.8462	23.2592
1.1494	0.0190	60.4971	21.4716	0.0210	54.7355	20.3607
1.1536	0.0190	60.7139	22.0034	0.0210	54.9316	20.1369
1.1539	0.0190	60.7332	20.2245	0.0220	52.4514	19.6534
1.1547	0.0190	60.7754	21.8921	0.0220	52.4878	19.2049
1.1559	0.0200	57.7972	18.5113	0.0210	55.0450	15.4151
1.1587	0.0200	57.9357	21.7499	0.0210	55.1769	21.7436
2.0599	0.0360	57.2205	20.6338	0.0380	54.2089	20.1402
2.0672	0.0360	57.4214	19.7069	0.0420	49.2183	16.6103
3.2959	0.0560	58.8553	21.5313	0.0620	53.1597	20.0086
4.1199	0.0710	58.0264	20.2679	0.0760	54.2089	19.0847
7.0862	0.1280	55.3608	20.8021	0.1320	53.6832	18.6809
8.5876	0.1470	58.4194	21.6151	0.1650	52.0463	21.6408
16.7370	0.2870	58.3170	21.3635	0.3130	53.4728	19.1448
18	0.3160	56.9620	20.0877	0.3370	53.4125	17.9348
25.9100	0.4530	57.1964	20.3726	0.4890	52.9856	17.6283
94.6241	1.6440	57.5572	21.1760	1.7880	52.9218	19.0916
AV=11.1641	AV= 0.1939	Av= 58.6052		AV= 0.2108	AV= 51.9407	
Speedup of (1) over (2)=(5)/(3)	1.0872		Enhancement level of (1) comparing with(2)= 1.1283 =(4)/(6)			

For performance analysis the encryption-decryption methods listed in table (4) were implemented and compared with the proposed method results, these results showed that the proposed method has a better parameter and using the proposed method will enhance the encryption-decryption process and the proposed method always has the smallest value of encryption-decryption time and the biggest value of method throughput

TABLE 4
COMPARISON RESULTS

Image size=256x256x3x8=1572864bit=1.5000M bits					
Method	Encryption time(seconds)	Decryption time(seconds)	Throughput(M Bits)	Speedup of the proposed method	Order
Proposed	**0.02500**	**0.02500**	**60.0000**	**1**	**1**
Ref[12]	0.06469	0.062727	23.1876	2.5876	2
Ref[14]	0.23	0.23	6.52170	9.2001	4
Ref[15]	0.5	0.5	3.0000	20.000	6
Ref[16]	0.4	0.4	3.7500	16.000	5
Ref[17]	0.12	0.12	12.5000	4.8000	3
Ref[18 version A-I]	0.56	0.56	2.6786	22.3998	7
Ref[18 version A-II]	1.01	1.01	1.4852	40.3986	8

V. CONCLUSION

A novel method of color image encryption-decryption process was proposed, implemented and tested. The obtained experimental results proved the following facts:

- The proposed method can be used to encrypt-decrypt any color image with any type and any size.
- The proposed method has a higher efficiency parameters comparing with parameters of existing methods of color image encryption-decryption.
- The proposed method is highly secure, and the high level of security can be achieved depending on the private key complicity.
- The private key is not fixed in size, and the key size depends on the block size.
- Reshaping the color image to be used in the proposed method will give better performance.

REFERENCES

[1] Jamil S. AL-Azzeh: Improved testability method for mesh-connected VLSI multiprocessors: Jordanian Journal of Computers and Information Technology August 2018.

[2] Jamil AL-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub and Mazen Abu-Zaher: A Novel Zero-Error Method to Create a Secret Tag for an Image; Journal of Theoretical and Applied Information Technology **15th July 2018**.

[3] Jamil AL-Azzeh, Bilal Zahran and Ziad Alqadi: Salt and Pepper Noise: Effects and Removal; International Journal on Informatics Visualization **July 2018.**

[4] Jamil AL-Azzeh, Oleksandr Kovalenko , Oleksii Smirnov Anna Kovalenko , Serhii Smirnov : Qualitative risk analysis of software development ; Asian Journal of Information Technology **July 2018.**

[5] Bilal Zahran, Jamil Al-Azzeh ,Ziad Alqadi, Mohd-Ashraf Al Zoghoul : A Modified Lbp Method To Extract Features From Color Images : Journal of Theoretical and Applied Information Technology **May 2018.**

[6] Jamil AL-Azzeh, Information Technologies for Supporting Administrative Activities of Large Organizations; DESIDOC Journal of Library & Information Technology, Vol. 38, No. 3, **May 2018.**

[7] Jamil S. AL-Azzeh: A Distributed Multiplexed Mutual Inter-Unit in-Operation Test Method for Mesh-Connected VLSI Multiprocessors; Jordan Journal of Electrical Engineering; **2017 Volume 10, Number 5.**

[8] Jamil S. AL-Azzeh: Fault-Tolerant Routing in Mesh-Connected Multicomputer based on Majority-Operator-Produced Transfer Direction Identifiers; Jordan Journal of Electrical Engineering **Volume 3, Number 2, April 2017**.

[9] Jamil S. AL-Azzeh, Mazin Al Hadidi, R. Odarchenko,S. Gnatyuk, Z. Shevchuk :Analysis of Self-Similar Traffic Models in Computer Networks; International Review on Modelling and Simulations; October **2017 Volume 10, Number 5.**

[10] Jamil Al Azzeh, Ziad Alqadi Qazem, M. Jabber: Statistical Analysis of Methods Used to Enhanced Color Image Histogram; XX **International** Scientific and Technical Conference; Russia **May 24-26, 2017.**

[11] Mazen Abuzaher, Jamil AL-Azzeh: JPEG Based Compression Algorithm; International Journal of Engineering and Applied Sciences Volume 4, Number 4, **2017**

[12] Mazin al hadidi, Jamil s. Al-azzeh, oleg p. Tkalich,roman s. Odarchenko,sergiy o. Gnatyuk and yulia ye. Khokhlachova2: Zigbee, Bluetooth and Wi-Fi Complex Wireless Networks Performance Increasing; International Journal On Communications Antenna And Propagation, **vol 7 No 1 February 2017**. (SJR indicator = 0.620).

[13] Jamil Al Azzeh, Daniel Monday Afodigbokwu ,Denis Olegovich Bobyntsev, Igor Valerievich Zotov: Implementing Built-In Test in Analog and Mixed-Signal Embedded-Core-Based System-On-Chips; Asian Journal of Information Technology, Medwell Journals ,**2016.** (SJR indicator = 0.11).

[14] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata : Creating a Color Map to be used to Convert a Gray Image to Color Image; International Journal of Computer Applications (0975 – 8887).Volume 153 – No2, **November 2016.**

[15] Jamil Al-Azzeh: Analysis of Second Order Differential Equation Coefficients Effects on PID Parameters International Journal on Numerical and Analytical Methods in Engineering (IRENA) Vol 4, No 2 **2016**.

[16] Dmitriy Skopin and Jamil Al-Azzeh; Automated Demodulation of Amplitude Modulated Multichannel Signals with Unknown Parameters Using 3D Spectrum Representation Research Journal of Applied Sciences, Engineering and Technology, Maxwell Scientific Publication June 05, **2016**; (SJR indicator = 0.15).

[17] Mazin Al Hadidi, Jamil S. Al-Azzeh, R. Odarchenko, Sergiy Gnatyu,k and A. A bakumova Adaptive Regulation of Radiated Power Radio Transmitting Devices in Modern Cellular Network Depending on Climatic Conditions. Contemporary Engineering Sciences, Vol. 9, **2016**, no. 10, 473 - (impact factor= 0.193) **2016**. 485

[18] Mazin Al Hadidi, Jamil S. Al-Azzeh, B. Akhmetov, O. Korchenko,S. Kazmirchuk, M. Zhekambayeva: Methods of Risk Assessment for Information Security Management International Review on Computers and Software (I.RE.CO.S.), Vol. 11, N. 2 ISSN 1828-6003 (impact factor = 6.14). February **2016**.

[19] Jamil Al Azzeh, Bidirectional Virtual Bit-slice Synchronizer: A Scalable Solution for Hardware-level Barrier Synchronization. Research Journal of Applied Sciences, Engineering and Technology,

11(8): 902-909. Maxwell Scientific Publication Corp November **2015**. (SJR indicator = 0.16)

[20] Jamil Al Azzeh, Michael E. Leonov. Dniitriy E. Skopm. Evgeny A. Titenko, Isor V Zotov; The Organization of Built-in Hardware-Level Mutual Self-Test in Mesh-Connected VLSI Multiprocessors; International Journal on Information Technology (I.RE.I.T.) Vol. 3, Praise Worthy Prize, March **2015**.

[21] Jamil Al Azzeh, Dmitriy B. Borzov2, Igor V. Zotov3 and Dmitriy E. Skopin'; an approach to achieving increased fault-tolerance and availability of multiprocessor-based computer systems" ; Australian Journal of Basic and Applied Sciences. Apr. **2014**. (SJR indicator = 0.18).

[22] Jamil Al -Azzeh,S. F. Yatsun, A.A. Cherepanov, I.V. Lupehina4 and V.S. Dichenko; Computer simulation of vibration robot created for the wall movement; Research Journal of Applied Sciences.; **2014** , Issue: 9, Page No.: 597-602 , (SJR indicator = 0.36).

[23] AL-Azzeh Jamil, Review of Methods of Distributed Barrier Synchronization of Parallel Processes in Matrix VLSI Systems, International Review on Computers and Software (IRECOS), Praise Worthy Prize, Part A, vol. 8, no. 4, pp.42- 46, April **2013** ISSNJS2S-6003 (impact factor = 6.14).

[24] Skopin Dmitriy, Al-Azzeh Jamil, Nader Jihad And Abu-Ein Ashraf, Australian Journal Of Basic And Applied Sciences. Dec **2013**, Vol. 7 Issue 14, p83-89. 7p. Fastest Color Model For Image Processing Using Embedded Systems. (SJR indicator = 0.18).

[25] Jamil Al-Azzeh, Mazin Al Hadidi , Using Virtual Network to Solve Freight Company Problems; World Applied Sciences Journal 27 (6): 754-758, **2013**; (SJR indicator = 0.17