Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation

Rashad Rasras
Al-Balqa' Applied University

Mohammed Abuzalata
Al-Balqa Applied University

Ziad Alqadi
Al-Balqa' Applied University

Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 8, Issue. 3, March 2019, pg.14 – 26

Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation

Rashad J. Rasras[1]; Mohammed Abuzalata[2]; Ziad Alqadi[3]; Jamil Al-Azzeh[4]; Qazem Jaber[5]

[1]Computer Engineering Department, Al Balqa'a Applied University, Amman, 11134, Jordan
E-mail: Rashad.Rasras@bau.edu.jo
[2]Computer Engineering Department, Al Balqa'a Applied University, Amman, 11134, Jordan
E-mail: abuzalata@bau.edu.jo
[3]Computer Engineering Department, Al Balqa'a Applied University, Amman, 11134, Jordan
E-mail: Natalia_maw@yahoo.com
[4]Computer Engineering Department, Al Balqa'a Applied University, Amman, 11134, Jordan
E-mail: azzehjamil@gmail.com
[5]Computer Engineering Department, Al Balqa'a Applied University, Amman, 11134, Jordan
E-mail: qazemjaber@gmail.com

Abstract: Color image encryption-decryption is an important issue, because it is used in many important applications. This paper will introduce 3 methods of image encryption-decryption, these methods will be implemented and tested, and the obtained experimental results will be compared with experimental results of the proposed method in order to do some judgment regarding the efficiency and the security of the proposed method.

Keywords: Encryption time, decryption time, MSE, PSNR, private key, window.

1- Introduction

True color image is a 3D matrix, the first dimension represents the red color, the second one represents the green color, while the third one represents the blue color [1-41] . Digital color image is one of the most popular data type used in the internet as a result of data communication between the sender and receiver over the internet [4]. Color images are widely used by different users, and several applications need certain and consistent 'security in data communication and security in storing' [5], [6], such as medical imaging systems, pay-TV, confidential video conferences, and military image communications, so the need for image encryption-decryption must have a priority with highest level.

Color encryption methods act as shown in figure (1) by selecting a private secret key and manipulating the original image in such a way to get the encrypted image.

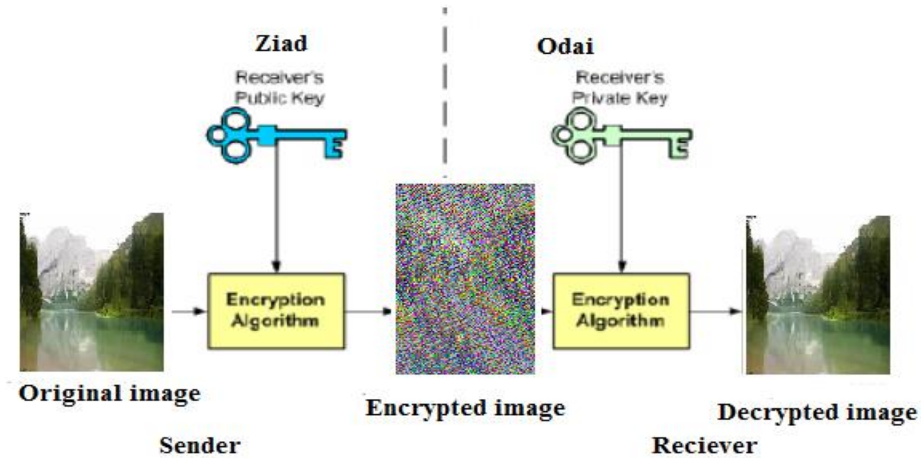

Figure (1): Encryption-decryption process

The used method of encryption must destroy the original image in order to make it impossible to be understand by a third party or by unauthorized person, thus un understanding level will be measured by the mean square error (MSE), or a peak signal to noise ratio (PSNR) between the original image and the encrypted one [7], [8], Where the value of the large error indicates the effectiveness of the method used and vice versa the small value of PSNR indicates the effectiveness of the method of encryption-decryption method, MSE between the original image and the decrypted one must lead to zero [7], [8] as shown in figure (2) and (3):

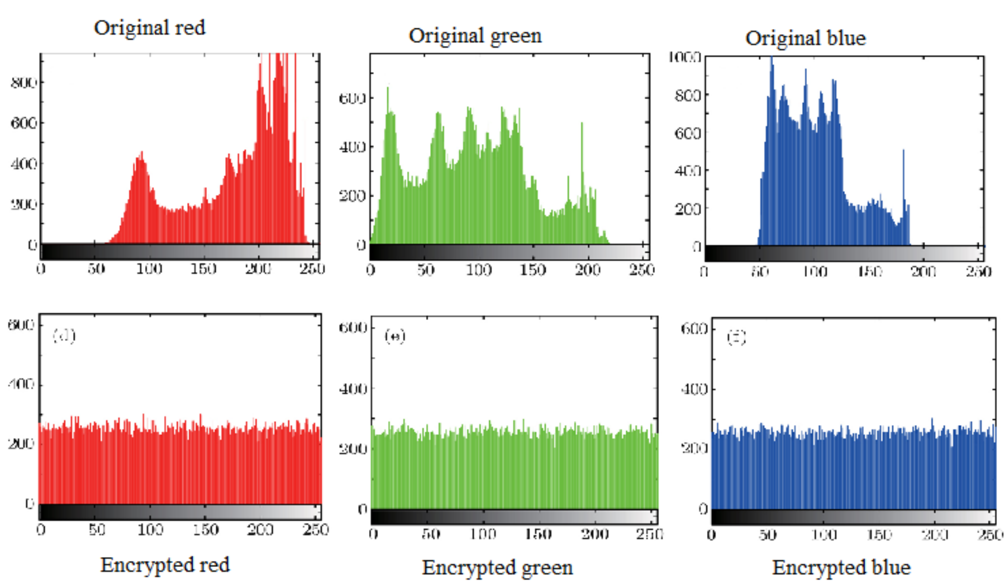

Figure (2): Destroying the encrypted image

Figure (3): Getting the decrypted image the same as original one

Many methods of encryption-decryption are based on matrix multiplication [10, 11, 12, and 13], if we multiply the original image matrix by a secret key then we can get the encrypted image, and if multiply the encrypted image by the key inverse we can get the decrypted original matrix as shown in figures (4) and (5)[10], [11]:

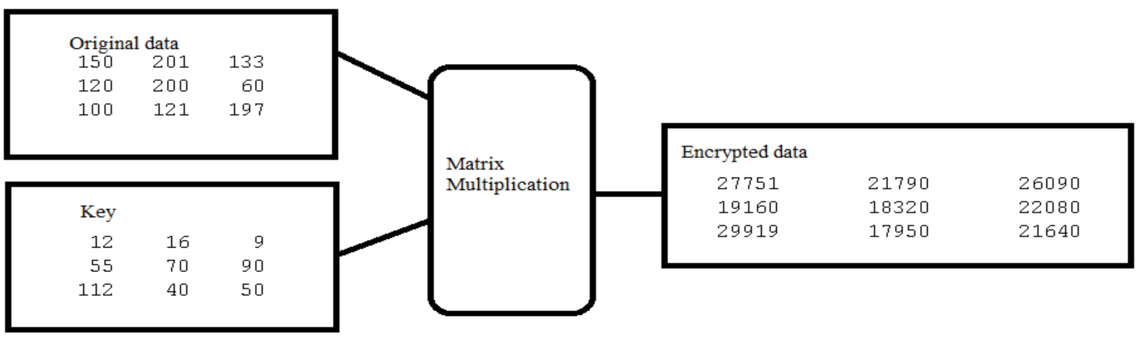

Figure (4): Encryption process

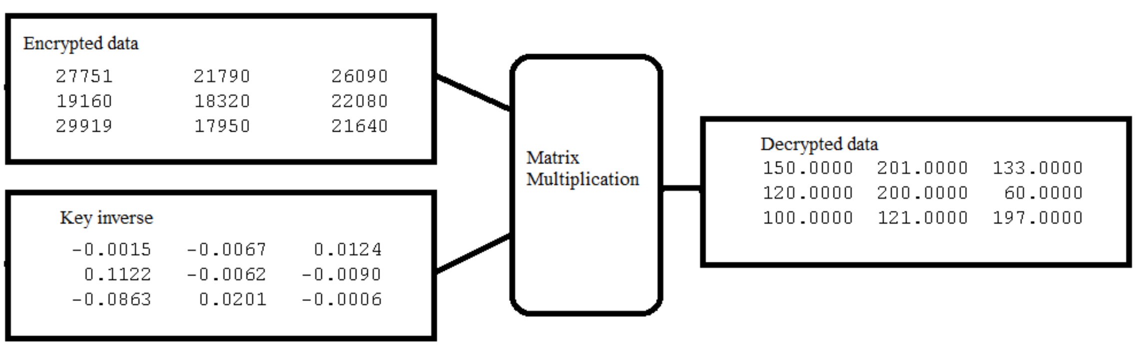

Figure (5): Decryption process

Colors from color images can be extracted, and each color may be encrypted, then the encrypted color image cab constructed from the 3 encrypted colors as shown in figure (6) [12], [13].

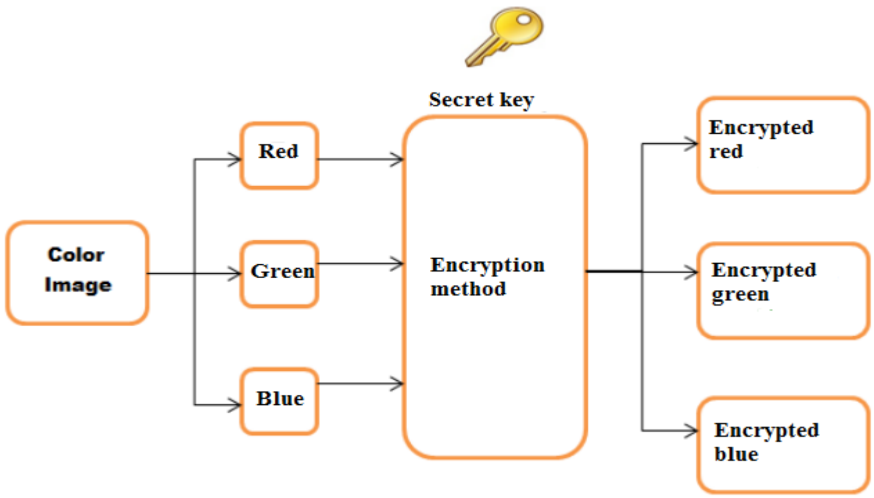

Figure (6): Encrypting each color of the color image.

2- *The Studied Methods*

Here we will describe 3 methods [14] which are used for color image encryption-decryption, and will a new one, this method will be tested and implemented and a comparative analysis between the four methods will be done.

Method 1: Encryption individual color component:

To do this we have to apply the following phases:

1) Phase 1: Private key generation
   This phase is to be implemented one time and it includes the following tasks:
   A. Generate a huge 2D matrix which is to be called key.
   B. Save the key.
2) Phase 2: Image encryption
   To do this we have to implement the following tasks:
   A. Get the original image.
   B. Extract the color components (Red, Green, and Blue).
   C. Load the key.
   D. Adjust the key to suit the 2D matrix.
   E. Get the encrypted Redenc, Greenenc, and Blueenc applying matrix multiplication of the key and each one of the 2D matrices.
   F. Compose the encrypted color image from the three encrypted components.
   G. Save the encrypted image.
3) Phase 3: Image decryption
   This phase can be implemented applying the following tasks:

A. Get the encrypted image.
B. Extract the color components (Red, Green, and Blue).
C. Load the key.
D. Adjust the key to suit the 2D color matrix.
E. Get the decrypted Red, Green, and Blue applying matrix multiplication of the inverse key and each one of the 2D matrices?
F. Compose the decrypted color image from the three decrypted components.

Method 2: Encryption using the reshaped 3D to 2D color image.

To do this we have to apply the following phases:

1) Phase 1: Private key generation

This phase is to be implemented one time and it includes the following tasks:

A. Generate a huge 2D matrix which is to be called key.

B. Save the key.

2) Phase 2: Image encryption

To do this we have to implement the following tasks:

A. Get the original image.

B. Reshape the 3D color matrix to 2D matrix

C. Load the key.

D. Adjust the key to suit the 2D matrix.

E. Get the encrypted 2D matrix by applying matrix multiplication of the key and 2D matrix.

F. Reshape the encrypted 2D image to 3D color matrix.

G. Save the encrypted image.

3) Phase 3: Image decryption

This phase can be implemented applying the following tasks:

A. Get the encrypted image.

B. Reshape the 3D color matrix to 2D matrix

C. Load the key.

D. Adjust the key to suit the 2D matrix.

E. Get the decrypted 2D matrix by applying matrix multiplication of the inverse of the key and 2D matrix.

F. Reshape the decrypted 2D image to 3D color matrix.

Method 3: Color image encryption by XORING the image with private secret key.

To do this we have to apply the following phases:

1) Phase 1: Private key generation

This phase is to be implemented one time and it includes the following tasks:

A. Generate a huge 3D matrix which is to be used as a private key.
B. Save the key.

2) Phase 2: Image encryption

To do this we have to implement the following tasks:

A. Get the original image.
B. Retrieve the image size.
C. Load the key.
D. Adjust the private key dimensions to match the 3D image matrix size.
E. Get the encrypted 3D matrix by applying matrix XORING of the private key and 3D matrix.
F. Save the encrypted image.

3) Phase 3: Image decryption

This phase can be implemented applying the following tasks:

A. Get the encrypted image.
B. Retrieve the image size.
C. Load the key.
D. Adjust the private key dimensions to match the 3D image matrix size.
E. Get the decrypted 3D matrix by applying matrix XORING of the private key and 3D matrix.

Method 4: The proposed method

Color image encryption by applying XORING operation between the image blocks with private secret key.

To do this we have to apply the following phases:

1) Phase 1: Private key generation

This phase is to be implemented one time and it includes the following tasks:

A. Generate a huge 1D array which is to be used as a private key.
B. Save the key.

C. Generate a block (window) size.

D. Save the window size.

2) Phase 2: Image encryption

To do this we have to implement the following tasks:

A. Get the original image.

B. Reshape the 3D image to 1D array.

C. Load the key.

G. Adjust the private key dimensions to match the 1D image matrix size.

H. Get the window size

I. Get the encrypted 1D matrix by applying XORING of the private key and each block in the 1D array.

J. Reshape 1D array back to 3D matrix to form the encrypted color image

K. Save the encrypted image.

3) Phase 3: Image decryption

This phase can be implemented applying the following tasks:

A. Get the decrypted image.

B. Reshape the 3D image to 1D array.

C. Load the key.

D. Adjust the private key dimensions to match the 1D image matrix size.

E. Load the window size

F. Get the decrypted 1D matrix by applying XORING of the private key and each block in the 1D array.

G. Reshape 1D array back to 3D matrix to form the decrypted color image

3- Implementation and Experimental Results

Diffident color images in sizes and types were implemented applying each of the above mentioned methods of color image encryption-decryption, a matlab code was written for each method, and the codes were implemented using the selected images.

Encryption and decryption times were calculated by the programs.

Table (1) and (2) show the experimental results:

Table (1): Results for methods 1 and 2

Color image size(Mbyte)	**Method1:** Encryption each color alone(matrix multiplication)		**Method2:** Encryption reshaped color image to 2D matrix(matrix multiplication)	
	Encryption time(seconds)	Decryption time(seconds)	Encryption time(seconds)	Decryption time(seconds)
0.1345	0.0250	0.0630	0.0210	0.0360
0.1440	0.0260	0.0650	0.0220	0.0380
0.1443	0.0290	0.0780	0.0240	0.0430
1.8024	1.1630	3.3100	1.0910	1.8100
2.3848	1.4690	3.6910	1.4000	2.1570
3.6403	3.2520	9.2910	3.1100	5.1560
5.8358	6.0160	16.1220	5.8810	9.3280
Average=2.0123	**1.7114**	**4.6600**	**1.6499**	**2.6526**

Table (2): Results for methods 3 and 4

Color image size(Mbyte)	**Method3:** Xoring image with secret key		**Method4:** Xoring image blocks with secret key Block size(window)=40	
	Encryption time(seconds)	Decryption time(seconds)	Encryption time(seconds)	Decryption time(seconds)
0.1345	0.276000	0.275000	0.007000	0.008000
0.1440	0.272000	0.273000	0.008000	0.008000
0.1443	0.279000	0.276000	0.008000	0.008000
1.8024	0.274000	0.275000	0.089000	0.093000
2.3848	0.266000	0.272000	0.120000	0.123000
3.6403	0.269000	0.273000	0.178000	0.184000
5.8358	0.277000	0.277000	0.287000	0.297000
Average=2.0123	**0.2733**	**0.2744**	**0.0996**	**0.1030**

From these tables we can see that the proposed method gave the best efficiency parameters by decreasing both the encryption decryption times as shown in figure(7) and (8)

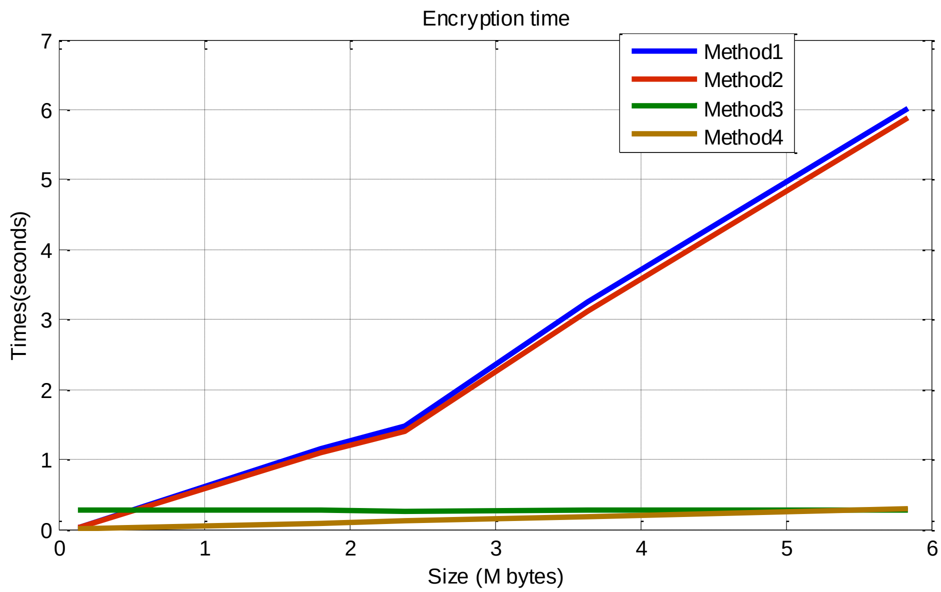

Figure (7): Encryption time comparisons

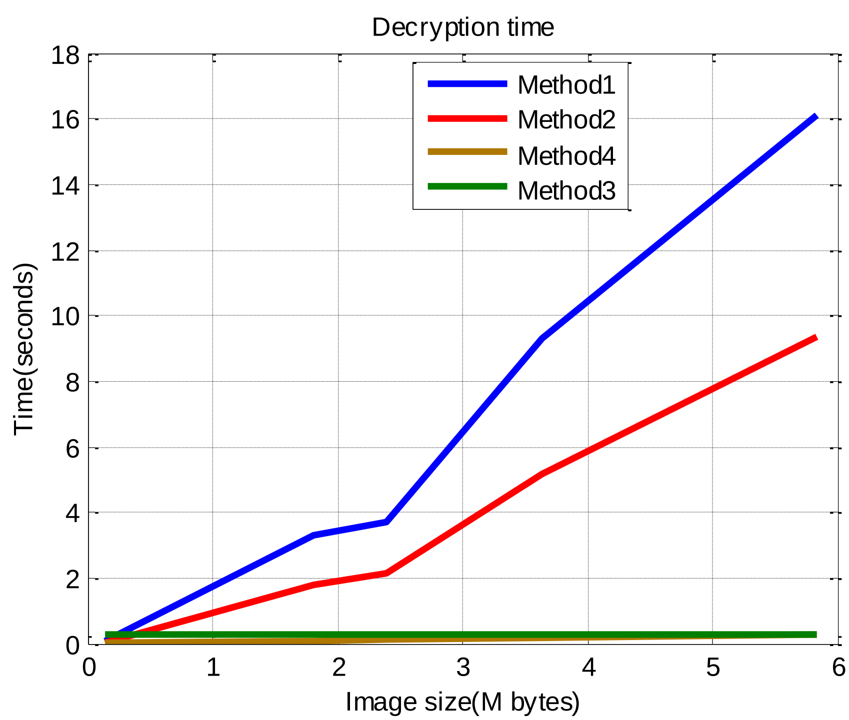

Figure (8): Decryption time comparisons

The proposed method gave the parameters values:

MSE between the original image and encrypted one= 1.0155e+004

PSNR between the original image and encrypted one= 18.5679

MSE between the original image and Decrypted one= 0

PSNR between the original image and Decrypted one= infinite.

Which are an excellent parameters and as shown in figures (9), (10) and (11)

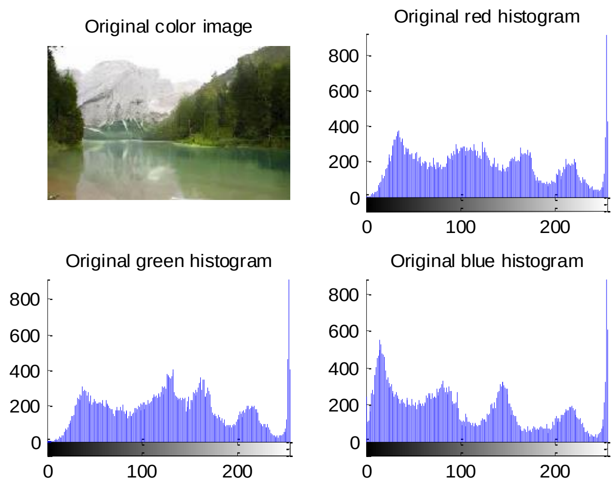

Figure (9): Original color image

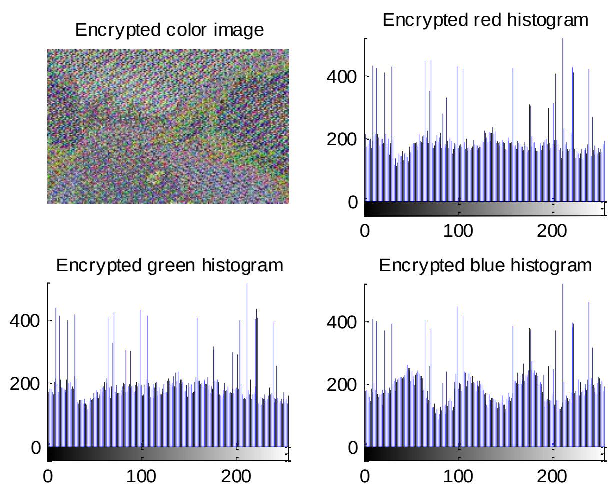

Figure (10): Encrypted color image

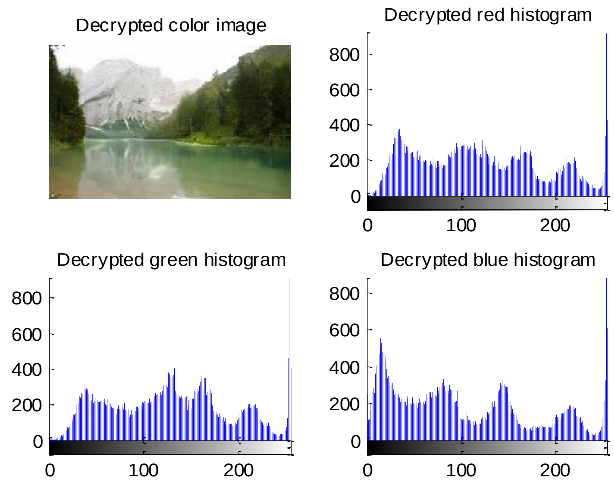

Figure (11): Decrypted color image

Conclusion

Four methods of color image encryption-decryption were studied and all these methods gave efficient parameters. The fourth proposed method gave the best parameters by decreasing encryption-decryption time.

The proposed method gave acceptable values for MSE and PSNR, and it is highly secure because of:

- The private key has several values and the number of values is variable and changeable.
- The window size is variable and changeable.

References

1. Akram A. Moustafa and Ziad A. Alqadi, Color Image Reconstruction Using A New R'G'I Model, Journal of Computer Science 5 (4): 250-254, 2009.
2. Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abu Zalata, Creating a Color Map to be used to Convert a Gray Image to Color Image, International Journal of Computer Applications 153(2):31-34,2016.
3. Gupta, Sunny Gupta, Anuradha Signals, Importance and Techniques of Information Hiding: A Review, International Journal of Computer Trends and Technology (IJCTT) –volume 9number5–Mar 2014.
4. S.N Wawale, Prof A Dasgupta, Review of Data Hiding Techniques, International Journal for Advance Research in Engineering and Technology, Vol. 2, Issue II, Feb 2014
5. H Kayarkar, Sugata Sanyal, A Survey of Data Hiding Techniques and their Comparative Analysis, arxiv.org.
6. *Jamil Azzeh*, *Bilal Zahran, Ziad Alqadi*, Salt and Pepper Noise: Effects and Removal, International Journal on Informatics Visualization, vol. 2, Issue 4, Pages 252-256, 2018.
7. R. Kaur, Jagriti, H.Singh and R.Kumar, Multilevel Technique to improve PSNR and MSE in Audio Steganography. International Journal of Computer Applications, Vol.103, No.5, 1-4, (2014).
8. Mutaz Rasmi Abu Sara Rashad J. Rasras, Ziad A. AlQadi, Engineering, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages Technology & Applied Science Research, Vol.9 Issue 1, Pages 3681-3684, 2019.
9. K. Matrouk, A. A. Hasanat and H. Alashalary, Prof. Ziad Al-Qadi and Prof. Hasan Al-Shalabi, "Speech fingerprint to identify isolated word person", World Appl. Sci. J., vol. 31, no. 10, pp. 1767-1771, 2014.
10. Emam, M. M., Aly, A. A., & Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science & Applications,1(7), pp. 361-366, (2016).
11. Kaur, G., & Kochhar, A. A steganography implementation based on LSB & DCT. International Journal for Science and Emerging Technologies with Latest Trends,4(1), pp.35-41, (2012).

12. Saher Manaseer, Asmaa Aljawawdeh and Dua Alsoud, A New Image Steganography Depending On Reference & LSB, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9 (2017) pp. 1950-1955.
13. Jamil S. AL-Azzeh: Improved testability method for mesh-connected VLSI multiprocessors: Jordanian Journal of Computers and Information Technology August 2018.
14. 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**.
15. Jamil AL-Azzeh, Bilal Zahran and Ziad Alqadi: Salt and Pepper Noise: Effects and Removal; International Journal on Informatics Visualization **July 2018.**
16. Jamil AL-Azzeh, Oleksandr Kovalenko , Oleksii Smirnov Anna Kovalenko , Serhii Smirnov : Qualitative risk analysis of software development ; Asian Journal of Information Technology **July 2018.**
17. 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.**
18. Jamil AL-Azzeh, Information Technologies for Supporting Administrative Activities of Large Organizations; DESIDOC Journal of Library & Information Technology, Vol. 38, No. 3, **May 2018.**
19. 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.**
20. 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**.
21. 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.**
22. 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.**
23. Mazen Abuzaher, Jamil AL-Azzeh: JPEG Based Compression Algorithm; International Journal of Engineering and Applied Sciences Volume 4, Number 4, **2017**
24. 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).
25. 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).
26. 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.**
27. 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**.
28. 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**.
29. 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
30. 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 february **2016**.
31. 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**.
32. 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**.
33. 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**.
34. 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 .
35. 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
36. 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.
37. 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
38. Jamil Al-Azzeh, Mohammed Abuzalata Ziad Alqad; Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing 20198 2.
39. Mohammed Abuzalata ; Ziad Alqadi ; Jamil Al-Azzeh ; Qazem Jaber : Modified Inverse LSB Method for Highly Secure Message Hiding, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2.

