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. 2, February 2019, pg.93 – 103

Modified Inverse LSB Method for Highly Secure Message Hiding

Mohammed Abuzalata[1]; Ziad Alqadi[2]; Jamil Al-Azzeh[3]; Qazem Jaber[4]

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

Abstract: The data may be very important and very confidential and when sent in an insecure environment may be stolen or being snatched on them, which eliminates the importance and confidentiality, so the need for data hiding becomes a very important issue to protect the data and prevent unauthorized party seeing or reading it. In this paper we will investigate a methodology to increase the security level of LSB method of data hiding. The process of data hiding and data extracted will tested in order to obtain an acceptable parameters, which allow us to adopt this methodology.

Keywords: LSB, steganography, hiding time, extracting time, reference, PSNR, MSE, Covering image, holding image, secret message.

1- Introduction

True color image can be represented by a 3D matrix [1-40], and mostly for a high resolution images the matrices are very huge and the can be easily used to hold secret message or to hold another image which carries the secret message.

Steganography is the process of hiding data into another data as shown in figure (1), in this study we will insert (hide) a secret message in a color image, then the holding color image will be hidden in another bigger color image.

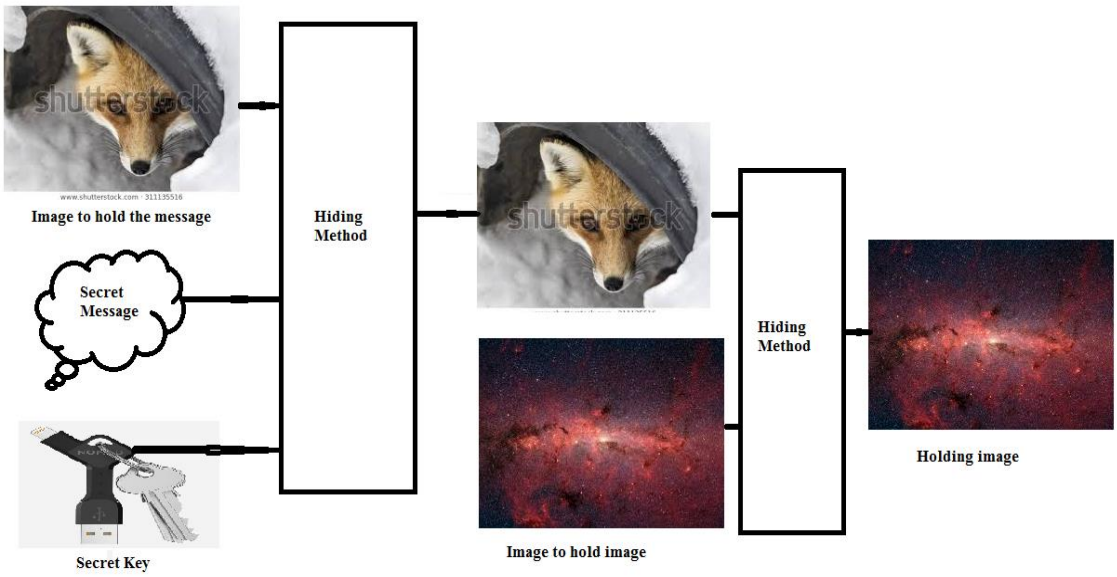

Figure (1): Data steganography

Steganography is very useful and applicable process for the following reasons [3], [4], [5]:

a. Personal data are private and sometimes are very confidential.
b. Data are very sensitive
c. Confidential data and trade secrets
d. Misuse of data is not acceptable.
e. Data does not bear unintentional damage, or human error and accidental deletion.
f. Data should not be exposed monetary and blackmail purposes
g. Data does not deal with hiding traces of crime

Any data hiding technique shall express certain features such as:

- Capacity, which refers to the amount of data that can be hidden in cover medium [3].
- Security, the data hiding method should provide security such that only the intended user can gain access to it. In other words, it refers to the inability of un-authorized user to detect hidden information. This is very crucial to protect the confidentiality and sensitivity of information being sent [3], [4].
- Robustness, which refers to the amount of data that can be hidden without showing any negative effects and destroying hidden information [1]. In other words making it difficult to distinguish them with the naked eye

- Perceptibility, the data hiding method should hide data in such a manner that the original covering data and the hidden data are perceptually indistinguishable.[5]

True color image is a three dimensional matrix [1], [2], the firs dimension is reserved for the red color; the second dimension is reserved for the green color, while the third one is reserved for the blue color.

High intensity color image usually has a huge size, thus it can be used as a good medium to cover and hold the secret message and to make it very difficult to distinguish them with the naked eye. So using a huge color image as a covering media will reduce mean square error(MSE) and will maximize peak signal to noise ratio(PSNR) [6], [7],avoiding destroying covering image.

2- Proposed Methodology

The proposed methodology is based on least significant bit (LSB) method of data hiding [8]. This method is very simple to implement and provides a high PSNR value and a low MSE value, but it is not secure because of the known procedures [9], [10].

LSB method sometimes added minor changes to covering image due to the following reasons [11], [12]:

a. If the least bit of the byte in the covering image equal the corresponding bit of the message byte then the byte of the covering image will not change.

b. If the least bit of the byte in the covering image equal 1 and the corresponding bit of the message byte equal 0 then the byte of the covering image will be reduced by 1 and still closed to the original value .

c. If the least bit of the byte in the covering image equal 0 and the corresponding bit of the message byte equal 1 then the byte of the covering image will be increased by 1 and still closed to the original value .

Each byte from data to be hidden requires 8 bytes from the covering image, so the maximum size of the hidden data must not exceed the size of the holding image divided by 8 [1].

Table (1) shows how to hide 'Ziad' in covering image bytes:

Table (1): LSB example

Message= Ziad = **90 105 97 100**

Binary=**01011010 01101001 01100001 01100100**

Red pixel	Decimal	Covering binary	Holding binary	Decimal	Red pixel	Decimal	Covering binary	Holding binary	Decimal
1	**249**	**11111001**	1111100**0**	**248**	**17**	**249**	**11111001**	1111100**0**	**248**
2	**249**	**11111001**	1111100**1**	**249**	**18**	**249**	**11111001**	1111100**1**	**249**
3	**249**	**11111001**	1111100**0**	**248**	**19**	**249**	**11111001**	1111100**1**	**249**
4	**249**	**11111001**	1111100**1**	**249**	**20**	**249**	**11111001**	1111100**0**	**248**
5	**249**	**11111001**	1111100**1**	**249**	**21**	**249**	**11111001**	1111100**0**	**248**
6	**249**	**11111001**	1111100**0**	**248**	**22**	**249**	**11111001**	1111100**0**	**248**

7	249	11111001	11111001	249	23	249	11111001	11111000	248
8	249	11111001	11111000	248	24	249	11111001	11111001	249
9	249	11111001	11111000	248	25	249	11111001	11111000	248
10	249	11111001	11111001	249	26	249	11111001	11111001	249
11	249	11111001	11111001	249	27	249	11111001	11111001	249
12	249	11111001	11111000	248	28	249	11111001	11111000	248
13	249	11111001	11111001	249	29	249	11111001	11111000	248
14	249	11111001	11111000	248	30	249	11111001	11111001	249
15	249	11111001	11111000	248	31	249	11111001	11111000	248
16	249	11111001	11111001	249	32	249	11111001	11111000	248

The proposed methodology can be applied implementing the following phases:

1) Hiding message in color image (a1).

   This phase can be implemented applying the following steps:

   A. Get the original covering image.

   B. Get the message to be hidden.

   C. Convert each of the image and the message into one column arrays.

   D. Select a reference (position) in the image array where to start hiding (save this reference let us say ref1).

   E. Apply LSB method starting from ref1 and back toward the beginning to hide each byte of the message.

   F. Get the decimal values of the image.

   G. Save message length

   H. Save image a1 size.

   I. Reshape the resulting image back to 3D matrix and save the holding image (a1).

2) Hiding a1 in another bigger color image.

   This phase can be implemented applying the following steps:

   A. Get the new bigger covering image.

   B. Get the image a1.

   C. Convert each of the two images into one column arrays.

   D. Select a reference (position) in the image array where to start hiding a1 (save this reference let us say ref2).

   E. Apply LSB method starting from ref2 and back toward the beginning to hide each byte of the image a1.

F. Get the decimal values of the holding image (a2).

G. Reshape the resulting image back to 3D matrix and save the holding image (a2).

3) Extracting the image a1 from image a2.

This phase can be implemented applying the following steps:

A. Load image a2.

B. Load reference ref2.

C. Load the size of image a1.

D. Convert image a2 to one column array and convert the values to binary.

E. For each value in a1 take the LSB of 8 bytes.

F. Repeat the previous step for a number of bytes equal a1 size.

G. Reshape a1 to the original size.

4) Extracting message from image a1.

This phase can be implemented applying the following steps:

H. Load image a1.

I. Load reference ref1.

J. Load the size of message.

K. Convert image a1 to one column array and convert the values to binary.

L. For each value in message take the LSB of 8 bytes.

M. Repeat the previous step for a number of bytes equal message size.

The reference contains (k1, k2, k3), where k1 is the row where to start, k2 is the column number, and k3 is the color number, this reference must be converted to location using the following formula:

$$ref = (k3 - 1) \cdot \times n1 \cdot \times n2 + (k1 - 1) \cdot \times n2 + k2$$

Where: n1, n2, and n3 are image matrix dimensions.

3- Experimental Implementation

In this part we will experimentally investigate the above mentioned phases, in order to get some parameters which can be used to judge the advantages of the proposed methodology. Figures (2) and (3) show the original image and a holding image after hiding a message of 100 characters length, and here we can see that the holding image is very closed to original covering image and the changes cannot be noticed by human eyes.

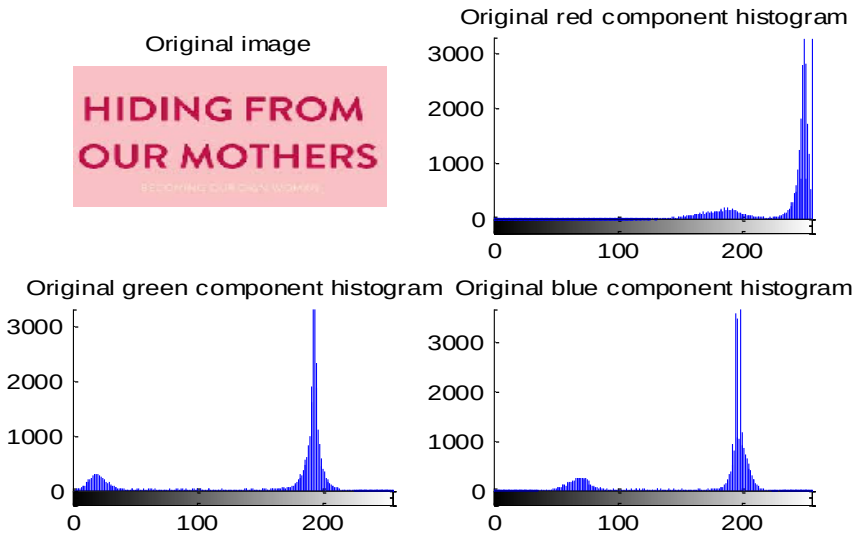

Figure (2) : Original covering image

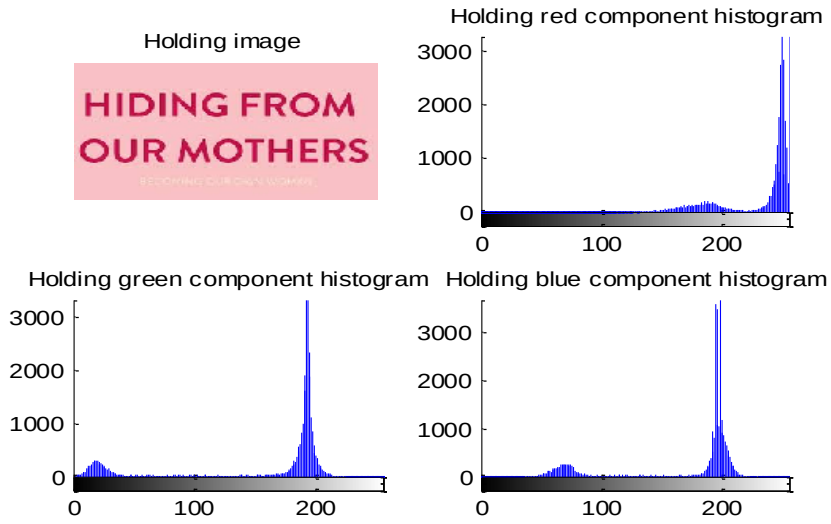

Figure (3): Holding image

Now we will perform some experiments to measure some parameters of the process of steganography.

Experiment 1:

Hiding message (100 character length) in various image.

The results of this experiment are shown in table (2):

Table (2) : Experiment 1 results

Image size(byte)	Hiding time(seconds)	Extraction time(seconds)	PSNR	MSE
284x160x3=136320	0.0240	0.2040	170.4450	0.0026
284x260x3=221520	0.0290	0.2050	170.4450	0.0026
320x207x3=198720	0.0290	0.2090	171.4452	0.0023
314x280x3=263760	0.0295	0.2120	171.4921	0.0023
450x351x3=473850	0.0270	0.2110	171.4595	0.0023
477x268x3=383508	0.0260	0.2300	171.4810	0.0023
550x367x3=605550	0.0260	0.2140	169.2277	0.0023
560x315x3=529200	0.0280	0.2790	171.4810	0.0023
590x310x3=548700	0.0240	0.2320	171.2701	0.0023
600x340x3= 612000	0.0270	0.2130	171.4735	0.0023
660x330x3=653400	0.0280	0.2330	171.5131	0.0023
1271x2048x3=7809024	0.0280	0.2520	171.4899	0.0023
4500x3000x3=40500000	0.0280	0.2150	171.4661	0.0023
Average	**0.0272**	**0.2238**	**171.1299**	**0.0024**

Here for the covering images with size range 133 Kbytes to 39551 Kbytes the average hiding time was equal 0.0272 seconds, the average extraction time was equal 0.2238 seconds and the average PSNR was equal 171.1299 which are good hiding parameters.

Experiment 2:

Hiding holding image with 560x315x3 bytes in other bigger images:

Figures (4), (5), and (6) show the images: Image which holds the message, original covering image, image which holds image.

Figure (4): Image holding the message

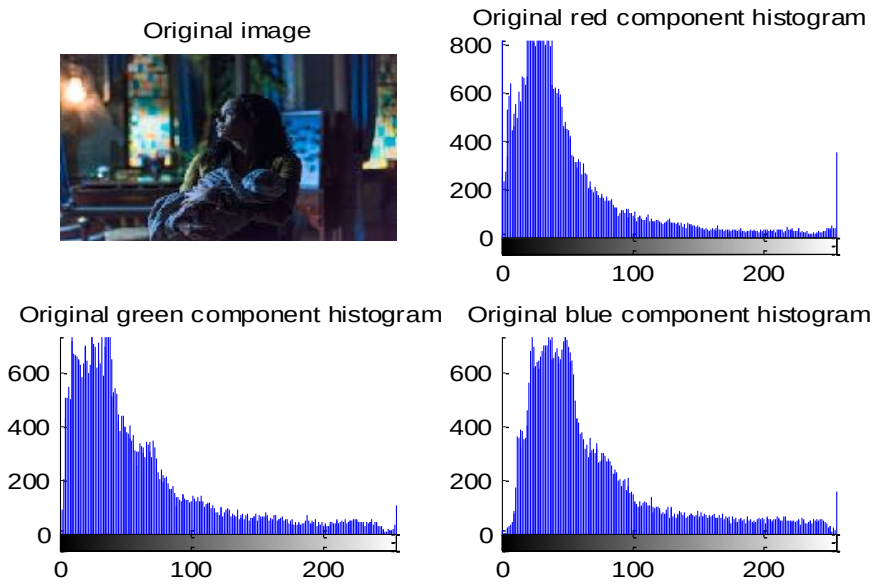

Figure (5): Original covering image

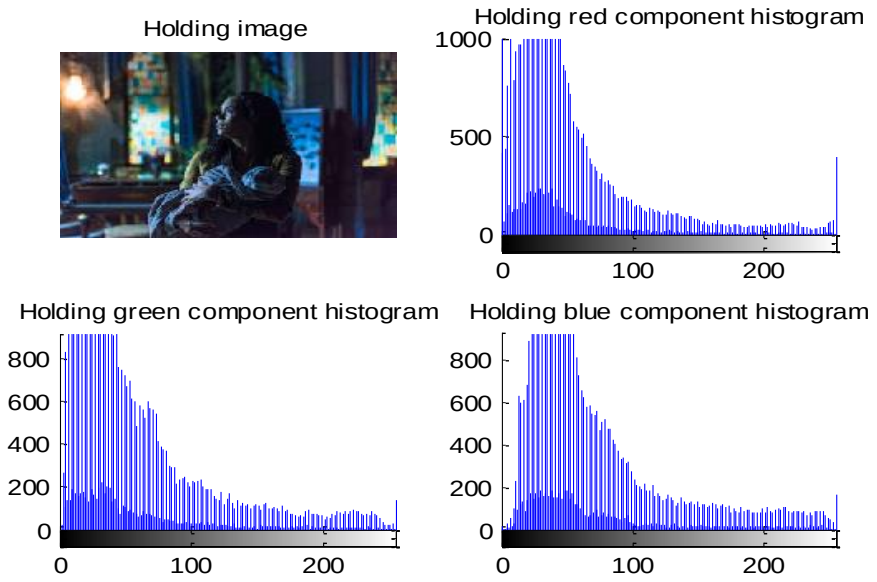

Figure (6): Image which holds another image

Table (3) shows the results of this experiment:

Table (3): Experiment 2 results

Image size(byte)	Hiding time(seconds)	Extraction time(seconds)	PSNR	MSE
4500x3000x3=40500000	0.3410	0.2330	120.5734	0.3773
1500x1102x3=4959000	0.3200	0.2470	120.9807	0.3622
1300x957x3=3732300	0.3370	0.2300	121.1922	0.3546
1271x2048x3=7809024	0.3310	0.2140	120.5538	0.3780
1280x720x3=2764800	0.3270	0.2100	120.3233	0.3868
Average	**0.3312**	**0.2268**	**120.7247**	**0.3718**

From table (3) we can see that the average hiding time was equal **0.3312** seconds, the average extraction time was equal **0.2268** seconds and the average PSNR was equal **120.7247** which are good hiding and extracting parameters.

From tables (3) and (4) we can see that the total average hiding time equal 0.3584 seconds and the total extraction time equal 0.4506 with a high average of PSNR values for the phase of hiding a message into an image, and hiding an image into another image.

Conclusion

A methodology based on LSB method was proposed, implemented and tested.

The proposed methodology increases the security level of LSB method by using secret references ref1 and ref2 as a private keys. The experimental results showed that the obtained values for hiding time, extracting time, PSNR and MSE are acceptable and optimal.

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.

