VOL 4 (2020) NO 1

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

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images

Jamil Al-Azzeh[#], Ziad Alqadi[#], Qazem Jaber[#]

[#] *Computer Engineering Department, Al Balqa'a Applied university, Amman, Jordan*
E-mail: azzehjamil@gmail.com, natalia_maw@yahoo.com, qazemjaber@gmail.com

***Abstract*— The digital image may be important and has a secret character, which requires not understanding it when looking at the naked eye or not understanding the contents. So seeking a method of digital image encryption-decryption is a very important task. In this paper we will introduce a new method of digital image encryption-decryption, which will be very simple, highly secure and accurate and highly efficient.**

***Keywords*— Encryption, decryption, private key, speedup, throughput.**

I. INTRODUCTION

Digital image encryption is the process of encoding an image in such a way that only authorized parties can access it and those who are not authorized cannot. The decryption process is to return back the original image without losing any piece of information from the original image.

Digital colour images [1], [2] are one of the most important types of data currently in the process of messaging through the Internet, which leads us to resort to the use of multiple ways to protect them from parasitism. The digital image may be important and has a secret character, which requires not understanding it when looking at the naked eye or not understanding the contents [1-60]. In order to do this, we must use a safe and efficient way to encrypt and re-encrypt them so that we can obtain a new image that matches the original image as shown in figure (1).

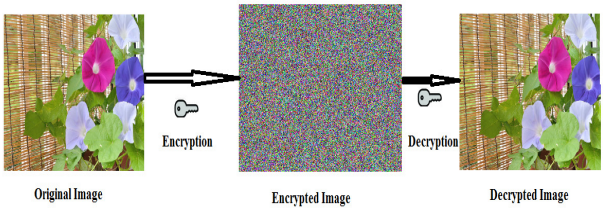

Fig. 1 Encrypted and decrypted colour images

Digital images are treatment (and here encryption=decryption) is different from text encryption-decryption due to some valuable features of the digital image, such as bulk data capacity and high correlation among pixels. [4], [5], [6].

In order to solve the problem of image encryption-decryption, we introduced a simple one key which can be used to encrypt-decrypt any image (binary, gray color) with any size.

II. THE MATERIAL

The digital image may be important and has a secret character, which requires not understanding it when looking at the naked eye or not understanding the contents, many different digital image encryption-decryption methods and techniques have been investigated tested and proposed for enhancing the security of images. In [7] an encryption technique for encryption=decryption using the Hill cipher method was proposed. In [8] a comparative analysis was introduced and different methods of image encryption decryption were tested and compared.

In [9] a New Chaotic Algorithm for Image Encryption-decryption was proposed this method was tested and implemented and it gave a 0.5 second encryption time to encrypt an RGB color image with size 256x256x3.

In [10] A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps was proposed this method was tested and implemented and it gave a 0.4 second encryption time to encrypt an RGB color image with size 256x256x3.

In [11] An Image Scrambling Encryption using Chaos-controlled Poker Shuffle Operation was proposed this method was tested and implemented and it gave a 0.56 second encryption time to encrypt an RGB color image with size 256x256x3.

III. METHOD/ ALGORITHM

The sender and receiver must use the same key for encryption-decryption as shown in figure (2).

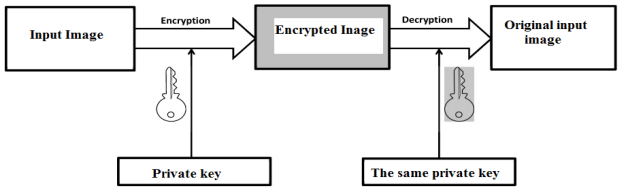

Fig. 2 Encryption-decryption

The proposed method can be implemented applying the following phases:

Phase 1: Private-key generation

To increase the security of the proposed method and to suit any image size a large 3D matrix with random values will be generated, the generated key must be saved for later use to encrypt or decrypt any image.

The following key was generated and used here in this paper:

$$key = uint8(255 * rand(5000, 5000, 3))$$

Figure (3) shows a sample part of the generated key:

$$key(1:10, 1:10, 1) =$$

127	19	223	76	1	183	253	127	9	55
211	41	197	75	226	226	209	242	94	250
39	84	249	52	87	182	225	20	142	38
49	143	106	104	4	223	63	71	68	173
165	53	211	61	2	138	91	89	129	127
98	167	26	87	87	75	80	225	214	13
222	162	208	90	201	49	127	24	129	149
57	209	169	86	35	126	202	42	191	218
107	224	237	111	166	117	189	124	187	105
88	42	159	99	64	192	240	228	123	13

Fig. 3 Sample of the generated key

Phase 2: Image encryption

This phase can be implemented applying the following steps:

- ✓ Get the original input image.
- ✓ Find the input image dimensions as follows:

$$[rows, colomns, colors] = size(originalimage)$$

- ✓ Load the key.
- ✓ Adjust the key to suit the input image size by extracting a used_key as follows:

$$Usedkey = key(1:rows, 1:columns, 1:colors)$$

- ✓ Find the encrypted image by applying the following formula:

$$Encryptedimage = Originalimage \oplus Usedkey$$

- ✓ Save the encrypted image.

Phase 3: Image decryption

This phase can be implemented applying the following steps:

- ✓ Get the encrypted image.
- ✓ Find the encrypted image dimensions as follows:

$$[rows, colomns, colors] - size(Encryptedimage)$$

- ✓ Load the key.
- ✓ Adjust the key to suit the encrypted image size by extracting a used key as follows:

$$[rows, colomns, colors] = size(Encryptedimage)$$

- ✓ Find the decrypted image by applying the following formula:

$$Decryptedimage = Encryptedimage \oplus Usedkey$$

- ✓ Save the decrypted image

The proposed method was implemented and the decrypted image was always the same as the original input image, some experimental samples are shown in figures (4) through (8):

Fig. 4 Sample image encryption-decryption

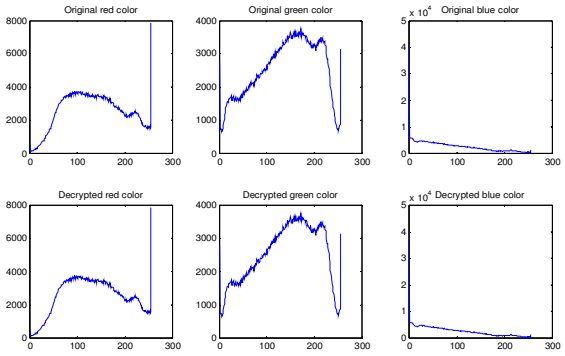

Fig. 5 Original and encrypted images histograms

$$original(100:110, 100:110, 1) =$$

75	74	73	72	71	44	64	90	113	126	127
80	79	79	78	80	55	57	63	73	89	104
82	86	87	89	90	84	73	61	58	70	91
84	90	95	99	100	106	90	74	68	75	90
86	92	99	103	106	111	100	87	81	84	90
81	99	110	107	100	98	99	102	106	111	114
93	98	101	100	99	103	107	115	125	138	149
102	95	91	92	97	108	111	117	125	134	141
100	92	86	89	96	104	104	103	105	106	105
89	88	89	90	92	95	95	95	95	96	97
84	89	92	92	89	95	95	95	97	98	98

Fig. 6 Samples from the original image

$$encrypted(100:110,100:110,1) =$$

28	249	43	110	160	101	150	246	71	16	8
248	48	27	134	33	141	124	193	193	26	60
179	91	0	39	1	137	94	183	220	46	200
149	78	211	183	214	148	168	57	192	7	33
155	244	193	33	226	1	63	161	32	193	116
116	182	83	129	46	168	196	6	226	68	52
191	67	144	179	32	17	97	215	92	163	83
230	86	96	169	43	237	65	35	91	39	79
4	123	110	48	157	93	194	158	225	159	207
36	218	10	205	214	136	51	211	55	45	138
225	63	105	25	178	234	97	246	77	146	3

Fig. 7 Samples from the decrypted image

$$decripted(100:110,100:110,1) =$$

75	74	73	72	71	44	64	90	113	126	127
80	79	79	78	80	55	57	63	73	89	104
82	86	87	89	90	84	73	61	58	70	91
84	90	95	99	100	106	90	74	68	75	90
86	92	99	103	106	111	100	87	81	84	90
81	99	110	107	100	98	99	102	106	111	114
93	98	101	100	99	103	107	115	125	138	149
102	95	91	92	97	108	111	117	125	134	141
100	92	86	89	96	104	104	103	105	106	105
89	88	89	90	92	95	95	95	95	96	97
84	89	92	92	89	95	95	95	97	98	98

Fig 8 Samples from the decrypted image

IV. Results And Discussion

The proposed method was implemented using various images (binary, gray and colour images with different types), one key for all the experiments was selected and table (1) shows some results samples of the performed experiments:

TABLE I
SAMPLES OF THE EXPERIMENTAL RESULTS

Image number	Image size	Size in pixels	Encryption time(seconds)	Decryption time(seconds)
1	177 x 284 x 3	150804	0.323000	0.312000
2	222 x 228 x 3	151848	0.327000	0.327000
3	186 x 271 x 3	151218	0.327000	0.311000
4	196 x 258 x 3	151704	0.323000	0.308000
5	177 x 284 x 3	150804	0.322000	0.310000
6	225 x 225 x 3	151875	0.325000	0.310000
7	177 x 284 x 3	150804	0.320000	0.307000
8	177 x 284 x 3	150804	0.321000	0.304000
9	168 x 300 x 3	151200	0.363000	0.347000
10	183 x 276 x 3	151524	0.325000	0.311000
Average		151260	0.3276	0.3147
Time per pixel(microseconds)			2.1658	2.0805
Throughput(Byte per second)			2 165800	2080500

4-1 Simplicity issues

It is very simple to generate the encryption-decryption key, this key can be generated once and it can be used for any image type with any size by adjusting the key size to suite the image size. Also an XORring operation used is very simple and fast to implement.

4-2 Security issues

The generated encryption-decryption key is very huge and contains 750000 values each of them within the range 0 to 255, thus making the process of guessing the key very difficult; this key must be known only by the image sender and the receiver. In bad cases (if the key was hacked) it is very easy to generate a new one.

4-3 Efficiency issues

From table (1) we can see that the average encryption time is around 0.3276 seconds which give us a high throughput which is in average around 2 Mbyte per second. The throughput was calculated using the following formula:

$$Throughput = \frac{Imagesizeinbits}{encryptiontimeinseconds}$$

The excremental results were compared with other methods result and the results of comparisons gave a good speedup as show in table (2):

TABLE II
COMPARISON RESULTS

Method	Encryption time (seconds)	Decryption time (seconds)	Total time	Speedup of the proposed method
Proposed	0.3276	0.3147	0.6423	1.0000
Ref[9]	0.5	0.5	1.0000	1.5569
Ref[10]	0.4	0.4	0.8000	1.2455
Ref[11]	0.56	0.56	1.1200	1.7437

The speedup was calculated using the following formula:

$$Speedup = \frac{Othermethodtime}{proposedmethodtime}$$

4-4 Accuracy issues

The obtained decrypted image was always the same as the original image for all experiments and the value of the mean square error (MSE) [12] was always zero and the value of peak signal to noise ratio (PSNR)[12] was always infinite which means the 100 % of encryption-decryption process.

V. Conclusions

A method of image encryption-decryption process was produced, the experimental results showed that the proposed method has the following important features:

- ✓ Very simple to use.
- ✓ High secure making hacking impossible.
- ✓ Very accurate by minimizing MSE to zero.
- ✓ Very efficient by increasing the speedup and increasing the method throughput.

REFERENCES

[1] Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, Optimized True-RGB color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, ISSN 1818-4952, 2010.

[2] A. A. Moustafa, Z. A. Alqadi, "Color Image Reconstruction Using A New R'G'I Model", Journal of Computer Science, Vol.5, No. 4, pp. 250-254, 2009.

[3] K Matrouk, A Al-Hasanat, H Alasha'ary, Z. Al-Qadi,H Al-Shalabi, "Speech fingerprint to identify isolated word person", World Applied Sciences Journal, Vol. 31, No. 10, pp. 1767-1771, 2014

[4] 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, Vol . 96. No. 13, pp. 4081-4091, 2018.

[5] Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.

[6] M. Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", International Journal of Science and Research, Vol. 3, No. 9, pp. 2281-2284, 2014.

[7] R. M. Patel, D. J. Shah, "Conceal gram :Digital image in image using LSB insertion method", International Journal of Electronics and Communication Engineering & Technology, Vol. 4, No.1, pp. 230-2035, 2013,

[8] N. Akhtar, P. Johri, S. Khan, "Enhancing the security and quality of LSB based image steganography", 5th International Conference on Computational Intelligence and Communication Networks, Mathura,India, Seprember 27-29, 2013.

[9] M. Juneja, P. S. Sandhu, "An improved LSB based Steganography with enhanced Security and Embedding/Extraction", 3rd International Conference on Intelligent Computational Systems, Hong Kong China, January 26-27, 2013.

[10] H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. A lqadi, H. Al-Shalabi (2013), Improving Matrix Multiplication Using Parallel Computing, International Journal on Information Technology (I.RE.I.T.) Vol. 1, N. 6 ISSN 2281-2911

[11] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein A COMPARISON BETWEEN PARALLEL AND SEGMENTATION METHODS USED FOR IMAGE ENCRYPTION-DECRYPTION, International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5, October 201.

[12] Z.A. Alqadi, A. Abu-Jazzar (2005), Analysis Of Program Methods Used For Optimizing Matrix Multiplication, Journal of Engineering, vol. 15 n. 1, pp. 73-78.

[13] Z.A. Alqadi, M. Aqel, I.M. El Emary, (2008) "Performance Analysis and Evaluation of Parallel Matrix Multiplication Algorithms" , World Applied Sciences Journal, vol. 5 (2):, ISSN 1818-4952, 2008

[14] H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. Alqadi, H. Al-Shalabi (2013), Improving Matrix Multiplication Using Parallel Computing, International Journal on Information Technology(I.RE. I.T.) Vol. 1, N. 6 ISSN 2281-2911

[15] Ziad Al-Qadi, Musbah Aqel, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences Journal, vol. 6, issue 1, pp 45-52, 2009.

[16] Jamil Al-Azzeh, Bilal Zahran and Ziad Alqad, Salt and Pepper Noise: Effects and Removal International Journal on Electrical Engineering and Informatics 2(4),

[17] T. Vimala, "Salt and Pepper Noise Reduction Using Mdbutm Filter With Fuzzy Based Refinement", Volume 2, Issue 5, May 2012.

[18] F. A. Jassim, "Image Denoising Using Interquartile Range Filter with Local Averaging", International Journal of Soft Computing and Engineering (IJSCE), vol. 2, Issue 6, pp: 424 –428, January 2013.

[19] Jamil S. AL-Azzeh: Distributed Mutual Inter-Unit Test Method For D-Dimensional Mesh-Connected Multiprocessors With Round-Robin Collision Resolution: Jordanian Journal of Computers and Information Technology April 2019.

[20] Jamil AL-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh : A Novel Based On Image Blocking Method To Encrypt-Decrypt Color JOIV: International Journal on Informatics Visualization, 2019

[21] Jamil AL-Azzeh, Evaluation Method for SDN Network Effectiveness in Next Generation Cellular Networks : International Journal of Communication Networks and Information Security December 2018.

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

[23] Jamil AL-Azzeh: A Novel Zero-Error Method to Create a Secret Tag for an Image; Journal of Theoretical and Applied Information Technology 15th July 2018.

[24] Jamil AL-Azzeh, Qualitative risk analysis of software development ; Asian Journal of Information Technology July 2018.

[25] Bilal Zahran , Jamil AL-Azzeh, A Modified LBP Method To Extract Features From Color Images : Journal of Theoretical and Applied Information Technology May 2018.

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

[27] Jamil 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.

[28] Jamil 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.

[29] Jamil AL-Azzeh, Analysis of Self-Similar Traffic Models in Computer Networks; International Review on Modelling and Simulations; October 2017 Volume 10, Number 5.

[30] Jamil AL-Azzeh: Statistical Analysis of Methods Used to Enhanced Color Image Histogram; XX International Scientific and Technical Conference; Russia May 24-26, 2017.

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

[32] Jamil AL-Azzeh: ZigBee, Bluetooth and Wi-Fi Complex Wireless Networks Performance Increasing; International Journal On Communications Antenna and Propagation, vol 7 No 1 February 2017.

[33] Jamil AL-Azzeh ,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).

[34] Jamil AL-Azzeh, 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.

[35] 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.

[36] 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

[37] Jamil S. Al-Azzeh, Adaptive Regulation of Radiated Power Radio Transmitting Devices in Modern Cellular Network Depending on Climatic Conditions. Contemporary Engineering Sciences, Vol. 9, 2016,

[38] Mazin Al Hadidi, Jamil AL-Azzeh, 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.

[39] 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.

[40] Jamil AL-Azzeh, 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.

[41] Jamil AL-Azzeh; an approach to achieving increased fault-tolerance and availability of multiprocessor-based computer systems"; Australian Journal of Basic and Applied Sciences. Apr. 2014

[42] Jamil AL-Azzeh, Computer simulation of vibration robot created for the wall movement; Research Journal of Applied Sciences.; 2014 , Issue: 9, Page No.: 597-602 ,

[43] Jamil AL-Azzeh, 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

[44] Jamil AL-Azzeh, Fastest Color Model for Image Processing Using Embedded Systems Australian Journal Of Basic And Applied Sciences. Dec 2013, Vol. 7 Issue 14, p83-89. 7p.

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

[46] Jamil AL-Azzeh, Detection of eyes using FCM, International Review on Computers and Software (IRECOS), Praise Worthy Prize, Part A, vol. 7, no. 4, pp.1428-1434, Jul. 2012 (impact factor = 6.14).

[47] Jamil AL-Azzeh, An optical character recognition, Contemporary Engineering Sciences, vol. 5, no. 11, pp. 521-529, 2012.

[48] Jamil AL-Azzeh, Analysis of Matrix Multiplication Computational Methods European Journal of Scientific Research Vol.121 No.3, 2014, pp.258-266.

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

[50] 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, February- 2019, pg. 93-103

[51] Qazem Jaber, Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019/3

[52] Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata; Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019

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

[54] Jamil Al-Azzeh#, Bilal Zahran# , Ziad Alqadi#, Belal Ayyoub#, Muhammed Mesleh ;A Novel Based on Image Blocking Method to Encrypt-Decrypt Color; INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION VOL 3 (2019) NO 1

[55] Jamil Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub and M. Mesleh," A Novel Based On Image Blocking Method To Encrypt-Decrypt Color",International Journal on Informatics Visualization, Vol 3, No 1. 2019.

[56] B. Zahran, J. AL-Azzeh, Z. Al Qadi, M. Al Zoghoul and S. Khawatreh,"A Modified LBP Method to Extract Features from Color Images", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 10, 2018.

[57] 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(JATIT), Vol.96. No 13, 2018.pp: 4081-4091.

[58] Jamil AL-AZZEH, B. ZAHRAN, Z. ALQADI," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.

[59] Jihad Nader, Ziad Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", International Journal of Computer Applications (IJCA), Volume 174, issue 8, 2017, pp:12-17.

[60] Ziad Alqadi, Bilal Zahran, Jihad Nader, " Estimation and Tuning of FIR Lowpass Digital Filter Parameters", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 2, 2017, pp:18-23.