VOL 3 (2019) NO 3

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, 11134, 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 color images [1-33] 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 [3]. 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).

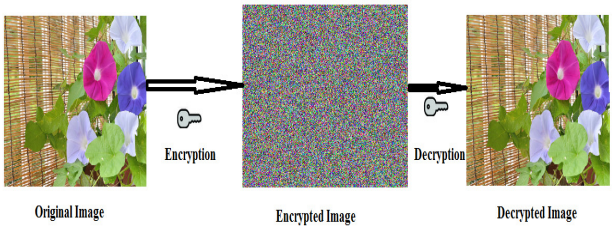


Fig 1. Encrypted and decrypted color images

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 AND METHOD / ALGORITHM

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.

**Proposed method**

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

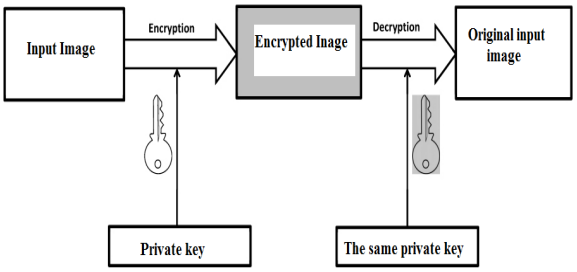


Fig 2.Encryption-decryption

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:

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

- ✓ 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

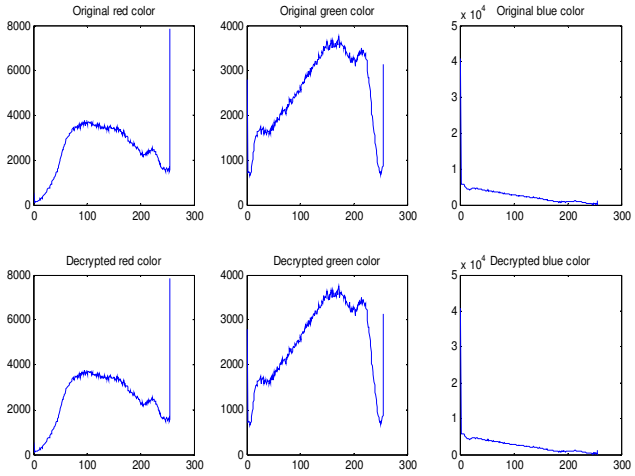


Fig 5. Original and encrypted images histograms

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

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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

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

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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

## III. Results And Discussion

The proposed method was implemented using various images(binary, gray and color images with different types), one key for all the experiments was selected and table (I) 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 | 177x284x3 | 150804 | 0.323000 | 0.312000 |
| 2 | 222x228x3 | 151848 | 0.327000 | 0.327000 |
| 3 | 186x271x3 | 151218 | 0.327000 | 0.311000 |
| 4 | 196x258x3 | 151704 | 0.323000 | 0.308000 |
| 5 | 177x284x3 | 150804 | 0.322000 | 0.310000 |
| 6 | 225x225x3 | 151875 | 0.325000 | 0.310000 |
| 7 | 177x284x3 | 150804 | 0.320000 | 0.307000 |
| 8 | 177x284x3 | 150804 | 0.321000 | 0.304000 |
| 9 | 168x300x3 | 151200 | 0.363000 | 0.347000 |
| 10 | 183x276x3 | 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 |

**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.

**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.

**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 (II):

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:

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

**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.

## IV. Conclusion

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 ] 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.**

**[2 ]** 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**

**[3 ]** Jamil S. Al Azzeh, Abdelwadood Mesleh ,Sergiy Gnatyuk and Anastasiia Abakumova, Evaluation Method for SDN Network Effectiveness in Next Generation Cellular Networks : International Journal of Communication Networks and Information Security **December 2018.**

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

[5 ] 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**.

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

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

[8 ] 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.**

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

[10 ] 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.**

[11 ] 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**.

**[12 ]** 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.**

[13 ] 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.**

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

[15 ] 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).

[16 ] 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).

[17 ] 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.**

[18 ] 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**.

[19 ] 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**

[20 ] 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**,

[21 ] 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**.

[22 ] 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**.

[23 ] 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**.

[24 ] 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**

[25 ] 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 ,

[26 ] 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**

[27 ] 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.

[28 ] 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)

[29 ] Mesleh, A. Al-Azzeh, , Abu Zneit, R., Abu Ain, A.: 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).

[30 ] Mesleh, A., Sharadqh, A., Al-Azzeh, J., Abu-Zaher, M., Al-Zabin, N., Jaber, T., Odeh, A., Hasn, M., An optical character recognition, Contemporary Engineering Sciences, vol. 5, no. 11, pp. 521-529, **2012.**

[31 ] Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi Analysis of Matrix Multiplication Computational Methods European Journal of Scientific Research Vol.121 No.3, 2014, pp.258-266.

[32 ] 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.

[33 ] Mazen Abu Zaher; Modified Least Significant Bit (MLSB) Computer and Information Science 4 (1), 60, 2010

[34 ] 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

[35 ] 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

[36 ] Mohammed Abuzalata Jamil Al-Azzeh, Ziad Alqadi;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