Journal of Theoretical and Applied Information Technology
15th June 2024. Vol.102. No. 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A METHOD TO MAKE THE ENCRYPTED COLOR IMAGE INCOMPREHENSIBLE AND USELESS

MOHAMMAD IBRAHIM AHMED AL-MAR[1], BELAL GHANEM MOHAMMAD AL-ATHAMNEH[2]

[1] Faculty of Science and Information Technology , Department of Computer Networks and Cybersecurity, Jadara University, Irbid 21110, Jordan
[2] Faculty of Science and Information Technology , Department of Computer science , Jadara University, Irbid 21110, Jordan
E-mail [1] m.alomar@jadara.edu.jo , [2] b.athamneh@jadara.edu.jo

ABSTRACT

The process of protecting a digital color image is an urgent necessity due to the confidentiality of the image or the possibility of it containing high-level data. In this research paper a new method of image cryptography will be introduces, tested and implemented. The proposed method will based on selecting a sequence of rotate left and exclusive operations. This sequence can be changed from time to time to increase the security level of image cryptography. The number of rotation digits can be changed; one or more private key can be used to ensure the image protection process. Some parameters such as MSE, PSNR and correlation coefficients will be calculated to show how this method will increase the distortion degree of the encrypted images, the results will compared with the XORing image cryptography to show the added damages to the encrypted image,
Keywords: *Cryptography, MSE, PSNR, Correlation Coefficient, Rotate Left, XORing, PK, Damage*

1. INTRODUCTION

Colored digital images are considered the most important and widely used type of digital data, as they are used in important vital applications, which require protecting them from the danger of intruders and data thieves. The process of providing a secure digital image protection is very necessary for several reasons, the most important of which are [1-6]:

- The possibility of the digital image carrying confidential data.
- The possibility that the digital image is strictly confidential, and no third party is not authorized to view it and understand its contents.
- The possibility that the digital image is very private and no one else is allowed to view it [44-49].

The digital color image has important and unique features, the most important of which are [7-12]:

- Huge size of the colored digital image, where the digital image consists of a large set of pixels, and a number of pixels is assigned to you. The first represents the value of the red color, the second represents the value of the green color, and the third represents the value of the blue color, and these colors are mixed together to form the specific color of the pixel, and as shown in figure 1 [10-13].

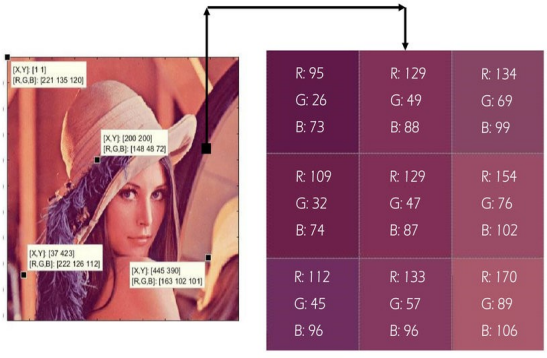

Figure 1:Pixels Values

- Ease of processing the colored digital image because it is represented by a three-dimensional matrix: the first dimension is a dual matrix dedicated to the red color, and the second dimension is a two-dimensional matrix dedicated

Journal of Theoretical and Applied Information Technology
15th June 2024. Vol.102. No. 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to the green color, and the third dimension is a dual matrix dedicated to the blue color, as shown in the figure 2, all operations Arithmetic and logical implementations on matrices can be easily performed on digital color images, all operations Arithmetic and logical implementations on matrices can be easily performed on digital color images [13-18].

- The possibility of obtaining a digital image at a lower cost due to the availability of various sources through which the digital image can be obtained.
- The possibility of processing each byte in the digital image individually, where a lot of operations can be performed on it, such as the left rotation process, by converting the decimal byte value into binary and implementing the left rotation process for a specified number of digits, as shown in the figure and implementing an operation Exclusion for a byte value with a specified private key value [19-22].

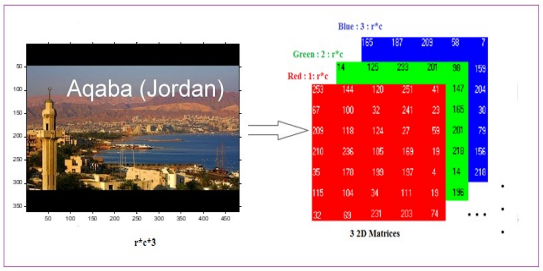

Figure 2: Color Image Matrices

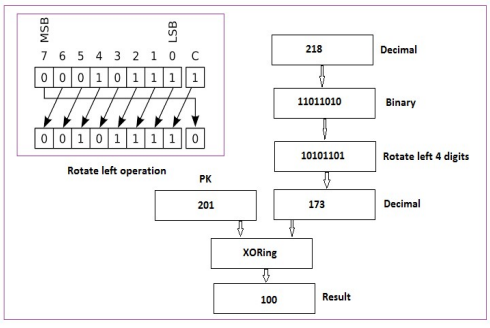

Figure 3: Rotation Left And Xoring

One of the most important ways to protect a digital color image is to use data cryptography, which means encrypting the image using a private key (PK) and some sequence of logical operations and decrypting the image using the same PK and a sequence of logical operation to get the same source image as shown in figure 4.

The encryption process should lead to the production of a destructive and distorted image that is difficult to understand or benefit from. As for the decoding process, it should return the original image without any change or loss of data.

The improved encryption method is the way to increase the distortion rate while not enabling the unauthorized parties to understand the mechanism of converting the image into an encrypted image[25-30].

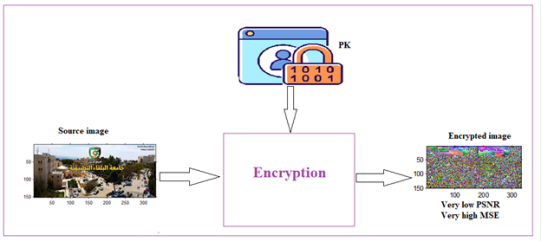

Figure 4: Encryption Process

The implementation of the encryption process must increase the degree of image distortion, and the degree of distortion can be measured using the following parameters:

- Mean square error (MSE) between the source image and the encrypted one [35-39].
- Peak signal to noise ratio (PSNR) betwwen the the souce image and the encrypted one,
- Correlection coefocients between the source color matrices and the encrypted ones,

These parameters can be calculated using equations 1 to 3 [40-43].

MSE of x channel

$$MSE_x = \frac{1}{N}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[S(i,j) - R(i,j)]^2 \ , N = m * n \quad (1)$$

Total MSE

$$MSE_t = MSE_R + MSE_G + MSE_B$$

Calculate PSNR

$$PSNR = 10 * \log_{10}\frac{(MAX_I)^2}{MSE_t} \quad (2)$$

Journal of Theoretical and Applied Information Technology
15th June 2024. Vol.102. No. 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$r = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \quad (3)$$

Where:

r = correlation coefficient

x_i = values of first image matrix

$\bar{x}$ = mean of x matrix

y_i = values of second image matrix

$\bar{y}$ = mean of y matrix

Positive correlation is measured on a 0.1 to 1.0 scale. Weak positive correlation would be in the range of 0.1 to 0.3, moderate positive correlation from 0.3 to 0.5, and strong positive correlation from 0.5 to 1.0. The stronger the positive correlation, the more likely the stocks are to move in the same direction.
Here we have to rember the ollowing[13-20]:

- Decreasing PSNR will increase the distirtion degree.
- Increasing MSE will decrease the distortion degree.Decreasing
- correlations will increase the distortion degree

2. RELATEDD WORKS

One of the most common methods used in the process of encrypting digital images is to use the logical exclusion process (XORing). This operation is executed using a private secret key, which can be an individual value used to process each byte in the digital image, or another image can be used as a special key that can be used to perform the exclusion process in one go [20-36].

XORing is a simple operation, but some times the distotion degree is not acceptable, this leads us to combine this operation with another sewuence of operations to enhance the process of encryption by decreasing the distortion degree and making the encrypted image incomprehensible and devastating features as shown in figures 5, 6, and 7[15-19]:

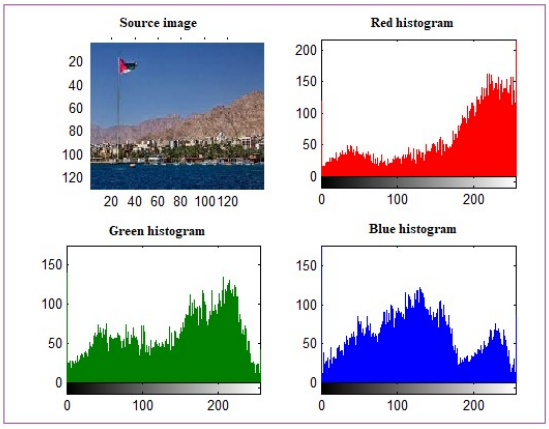

Figure 5: Source Color Image

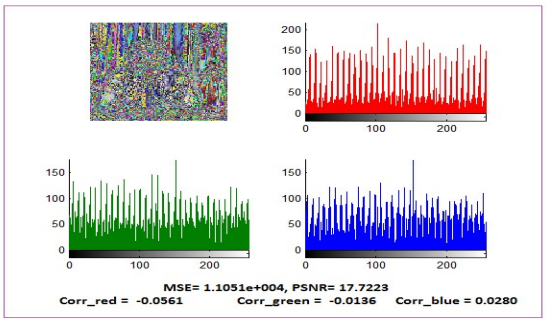

Figure 6: Encryption Using Byte Xoring And Rotation Left (More Damages)

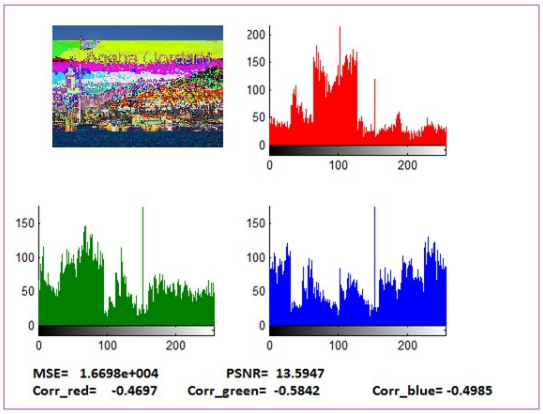

Figure 7: Encryption Using Byte Xoring (Less Damages)

3. THE PROPOSED METHOD

The proposed method is implemented by choosing a specific order for the left rotation and exclusion operations to be agreed upon between the sender and receiver, and choosing a numeric value confined between 0 and 255 to be used as a

PK. The number of rotation digits must be also determined. The order of logical operations in the decryption process is carried out in reverse, taking into account the implementation of the rotation process with a number of digits equal to eighty minus the number of rotation digits that were used in the process when executing the encryption process and as shown in table 1:

Table 1: Rotation Left Operation Examples(Source Byte = (235) Decimal =(11101011) Binary)

Encryption			Decryption		
Number of rotation digits	Binary	Decimal	Number of rotation digits	Binary	Decimal
1	11010111	215	7	11101011	235
2	10101111	175	6	11101011	235
3	01011111	95	5	11101011	235
4	10111110	190	4	11101011	235
5	01111101	125	3	11101011	235
6	11111010	250	2	11101011	235
7	11110101	245	1	11101011	235

Figures 8 and 9 show how to use a sequence : Rotate left one digit, rotate left 3 digits, rotate left 6 digits and XORing to encrypt decrypt a data byte:

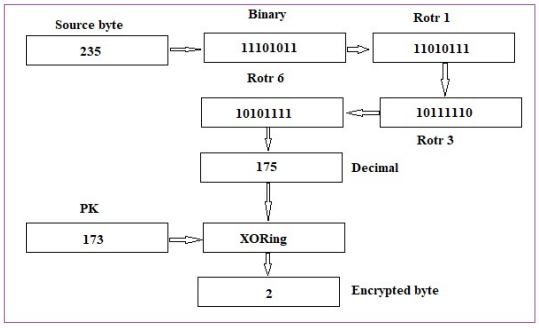

Figure 8: Encryption Using A Selected Sequence Of Operations

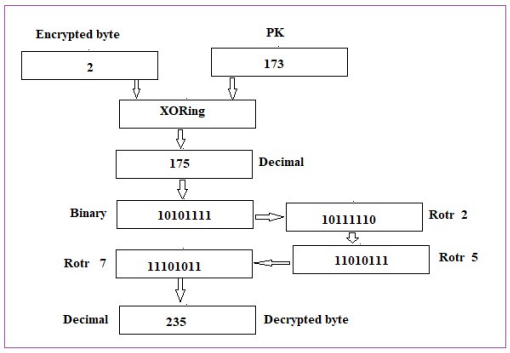

Figure 9: Decryption Using A Selected Sequence Of Operations

The proposed algorithm for encryption phase is as follows:
Input:
Source image, PK, sequences of logical operations.
Output:
Encrypted image
Process:
Implement the sequence of selected operation.
The decryption algorithm is as follows:
Input:
Encrypted image, PK, sequences of logical operations.
Output:
Decrypted image
Process:
Implement the sequence of selected operation in revers way.

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

Several images with various sizes were implemented using the proposed mehod applying various sequences of logical operations which include rotation left with a

selected number of digits and XORing, figure 10 shows the used images, while table 2 shows the basic information of these images.

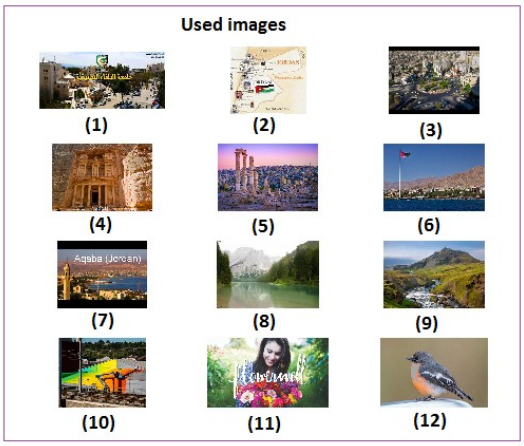

Figure 10: Used Images

Table 2: Used Images Basic Information

Image number	Dimension	Size(byte)
1	151 333 3	150849
2	152 171 3	77976
3	360 480 3	518400
4	1071 1600 3	5140800
5	981 1470 3	4326210
6	165 247 3	122265
7	360 480 3	518400
8	183 275 3	150975
9	183 275 3	150975
10	201 251 3	151353
11	600 1050 3	1890000
12	1144 1783 3	6119256

Here we have to notice the following points:

- The sequence of selected logical operation can be changed any time, the sender and reciever must agree on the sequence,
- One or private keys can be used, one PK for each XORing operation.
- The nuber of rotate left digits can be also changed.

Thes points add an extra protection increasing the proposed method level of security and making the hacking process very hard,

Several sequences were tested and MSE, PSNR and correlation coeficients were calculated, the following are the outputs of implementing these sequences (see figures 11, 12 and 13):

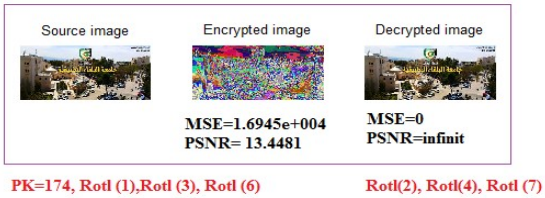

Figure 11: Using Image 1, Sequence 1

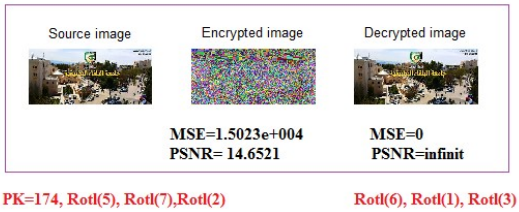

Figure 12: Using Image 1, Sequence 2

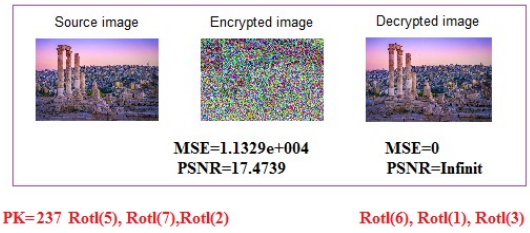

Figure 13: Using Image 5, Sequence 2

The damages obtained using the proposed method can be noticed comparing figure 11 with the results obtained by applying only XORing operation as shown in figure 12.

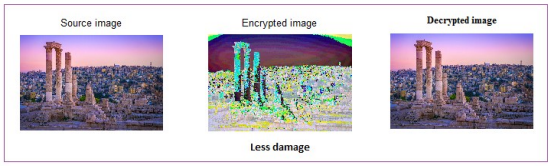

Figure 14: Less Damages Using Only Xoring Operation

The sequence: Rotl (5), Rotl (7), Rotl (2), XORing with PK= PK=237 was implemented using the proposed method, figure 15 shows an output sample of implementation, the same PK was used for XORing operation only, figure 16 shows the output sample, here we can see how the proposed method increases the damges on the encrypted image.

Journal of Theoretical and Applied Information Technology
15th June 2024. Vol.102. No. 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

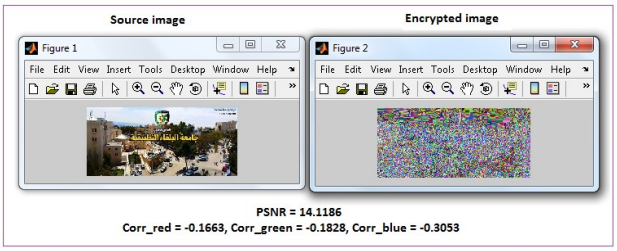

Figure 15: Encrypting Image 1 Using The Selected Sequences

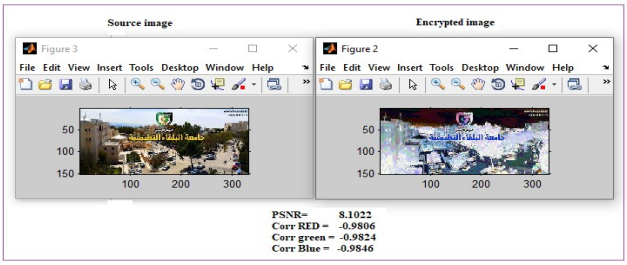

Figure 16: Encrypting Image 1 Using Only Xoring Operation

Tables 3 and 4 show the obtained experimental results using the proposed method with the selected sequence of operations:

TAble 3 MSE and PSNR using the selected sequence of operations

Image number	MSE	PSNR
1	1.5846e+004	14.1186
2	1.8190e+004	12.7390
3	1.5637e+004	14.2514
4	1.1774e+004	17.0890
5	1.1329e+004	17.4739
6	1.0435e+004	18.2957
7	2.1010e+004	11.2976
8	1.3542e+004	15.6897
9	1.1356e+004	17.4502
10	1.5791e+004	14.1531
11	1.4398e+004	15.0767
12	8.3002e+003	20.5849

TABLE 4: Correlation Coefficients Using The Selected Sequence Of Operations

Image number	Red correlation coefficient	Green correlation coefficient	Blue correlation coefficient
1	-0.1663	-0.1828	-0.3053
2	-0.1379	-0.1013	-0.0796
3	-0.3130	-0.2934	-0.2655
4	-0.1996	-0.1440	-0.1484
5	-0.1835	-0.1897	-0.1740
6	-0.1875	-0.0835	-0.2871
7	-0.5122	-0.4687	-0.4632
8	-0.2371	-0.2327	-0.2523
9	-0.1736	-0.1748	-0.1941
10	-0.2421	-0.2128	-0.2712
11	-0.2129	-0.2482	-0.2241
12	-0.1205	-0.1323	-0.1820

The sequence of operation was changed to: Rotl (2), Rotl (6), Rotl (1), XORing with PK=152
Tables 5 and 6 show the obtained experimental results:

TAble 5: MSE And PSNR Using The Selected Second Sequence Of Operations

Image number	MSE	PSNR
1	1.6741e+004	13.5692
2	1.9682e+004	11.9505
3	1.3645e+004	15.6141
4	1.1031e+004	17.7402
5	1.0796e+004	17.9559
6	7.6893e+003	21.3494
7	1.1966e+004	16.9272
8	1.3837e+004	15.4742
9	1.1468e+004	17.3520
10	1.4717e+004	14.8574
11	1.6984e+004	13.4253
12	3.5631e+003	29.0415

Table 6: Correlation Coefficients Using The Selected Second Sequence Of Operations

Image number	Red correlation coefficient	Green correlation coefficient	Blue correlation coefficient
1	-0.4652	-0.3793	-0.2930
2	-0.2068	-0.2867	-0.3837
3	-0.1946	-0.1990	-0.1886
4	0.1928	-0.0994	-0.1827
5	-0.1206	0.0634	-0.0995
6	-0.0869	-0.3127	0.5643
7	-0.1908	-0.1703	-0.1075
8	-0.3015	-0.2770	-0.3171
9	0.0063	0.0306	-0.4717
10	-0.2361	-0.2147	-0.0564
11	-0.3721	-0.3101	-0.4135
12	0.0023	0.0620	0.2553

From tables 3 to 6 we can see that the proposed method provides a good encryption quality by minimizing the values of PSNR and correlation coefficients and maximizing the values of MSE, this means that the proposed method completely destroys the source image by generated an encrypted image making this image incomprehensible and useless, thus making the process of hacking impossible.

5. CONCLUSION

A simple and highly efficient method of color image encryption-decryption was proposed and implemented. It was shown that using this method will increase the distortion degree of the encrypted image making it incomprehensible and useless, thus making the process of hacking impossible. The proposed method uses simple sequence of logical rotate left and exclusive operations with a selected primary key, one or more keys can be used to implement the XORing operations. The sequence of operations and the number of rotation left digits can be changed from time to time; this will lead to an increase in the security level of the proposed method. It was shown that the proposed method added extra damages to the encrypted image comparing with the XORing method used for image cryptography; the proposed method can be used for image cryptography (color and gray images).

6. ACKNOWLEDGMENT

I would like to acknowledge the initial support received from Jadara University under grant number Jadara-SR-Full2023. This support played a vital role in facilitating this research.

REFERENCES

[1] Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Ahmad Sharadqh, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, Vol. 8, Issue. 8, August 2019, pg.50 – 62.

[2] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2018.

[3] Akram A. Moustafa and Ziad A. Alqadi, A Practical Approach of Selecting the Edge Detector Parameters to Achieve a Good Edge Map of the Gray Image, Journal of Computer Science 5 (5): 355-362, 2009.

[4] Alomar Mhamad, Saleh Al-omar, Atef Obeidat Influence of traffic prognostic mechanism on quality of adaptive control of switchboard Contemporary Engineering Sciences, Vol. 7, 2014, no. 33, 1763-1776
http://dx.doi.org/10.12988/ces.2014.4797

[5] Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.

[6] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 76-90, 2019.

[7] 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.

[8] Waheeb, A. and Ziad AlQadi, Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173, 2009.

[9] 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.

[10] K Matrouk, A Al-Hasanat, H Alasha'ary, Z. Al-Qadi Al-Shalabi, "Speech fingerprint to

identify isolated word person", World Applied Sciences Journal, Vol. 31, No. 10, pp. 1767-1771, 2014.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. A 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.

[16] 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 2016.

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi Analysis of Matrix Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March-2019, pg. 76-90.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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)

[28] 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.

[29] Saleh Al-Omar" Method of Designing Generators of Pseudorandom Sequences for Information Protection Based on Shift Register with Non-Linear Feedback Function"Journal of Information Security Vol.5 No.4, October 29, 2014

[30] J. 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.

[31] 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.

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

[33] Akram A. Moustafa , Ziad A. Alqadi, Majed Alduari and Saleh Alomar," Practical Approach to Genetic Algorithm Cryptanalysis", International Review on Computers and Software (IRECOS), Vol. 4, No. 6, pp. 658-663, 2009

[34] Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering and Science, vol. 6, issue 1, pp. 49-55, 2022.

[35] Saleh Al-Omar, Atef Obeidat Engineering, 2012, 4, 768-773 doi:10.4236/eng.2012.411098 Published Online November 2012 (http://www.SciRP.org/journal/eng) " Burst Error Correction Method Based on Arithmetic Weighted Checksums "

[36] Saleh Al Omar, Abdelwadood Mesleh, Aws Al-Qaisi. Binary Heap Based Fair Scheduling Algorithm in Optical Burst Switching Networks", Review on Computers and Software (IRECOS), Vol 11, No 3(224-231),1/3/2016 Scopus.

[37] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Improving the Efficiency and Scalability of Standard Methods for Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp. 451-458, 2021.

[38] M. Abu-Faraj, and Z. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 53-60, 2021, doi:10.22937/IJCSNS.2021.21.12.8.

[39] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, 2018.

[40] Ziad A AlQadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

[41] Ziad A Alqadi, Mohamad Tariq Barakat, A Case Study to Improve the Quality of Median Filter, International Journal of Computer Science and Mobile Computing, vol. 10, issue 11, pp. 19 – 28, 2021.

[42] Dr. Hatim Ghazi Zaini Prof. Ziad Alqadi, High Salt and Pepper Noise Ratio Reduction, International Journal of Computer Science and Mobile Computing, vol. 10, issue 9, pp. 88 – 97, 2021.

[43] Prof. Mohamad K. Abu Zalata, Hussein N. Hatamleh, Prof. Ziad A. Alqadi, Detailed Study of Low Density Salt and Pepper Noise Removal from Digital Color Images, IJCSMC, Vol. 11, Issue. 2, PP. 56 – 67, February 2022.

[44] saleh alomar ,saleh khwatra,Comparative analysis of modern methods and algorithms of cryptographic protection of information, International Journal of Computer Science and Information Security, Vol. 15 No. 12 DEC 2017 (pp. 326-330), Thomson Reuters - Web of Science (Indexing in process) & Scopus.

[45] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022, doi.org/10.18280/ts.390117.

[46] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6, pp. 685-694, 2021, doi:10.35741/issn.0258-2724.56.6.61.

[47] M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Extraction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

[48] -"Crypto-Semantic Method of Text Data Protection" Saleh Ebrahim Alomar, Hazem Hatamleh Vol.7, No.8, 2016 (39-46) Computer Engineering and Intelligent Systems,Scopus.

[49] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 451-458, 2021, doi:10.22937/IJCSNS.2021.21.12.61.