IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

Two WPT Levels Decomposition for Color Image Cryptography

Prof. Ziad Alqadi*[1], Holwa Fayeq Taha[2]

Department of Computer Engineering, Faculty of Engineering Technology, Al-Balqa Applied University, Jordan*[1]

Department of Physics, Faculty of Science, Al-Balqa Applied University, Jordan[2]

Abstract: Digital color image is one of the most important types of data used due to the large number of computerized applications that are needed for mankind. The importance of digital color image force use to seek a good method of cryptography to protect the image from any unauthorized party. In this paper research we will introduce a method of color image cryptography, this method will be implemented and tested, we will show the main positive characteristics of this method and we will prove that this method satisfies the requirement of good methods of cryptography.

Keywords: Cryptography, WPT, Decomposition, Level, PSNR, Error, Encryption Time.

I. INTRODUCTION

Digital signals [1] , [6], [7] including color digital images [3], [4], [5] are among the most important types of data circulating between different people and institutions and one of the most used data in data communication networks and in various social media [8], [9], [10].
The importance of digital images is due to their use in many vital applications such as security [14], [15], [16], banking [17], [18], health, industrial applications, and many other essential applications for humans [2].
The color digital image may be of a personal nature [11], [12], [13], or it may be very confidential, or it may carry very important confidential data, which requires not understanding it with the naked eye and protecting it from the intrusion of unauthorized people. For these reasons, it is necessary to search for a safe and effective way to protect the image by distorting it at a very high rate so that it becomes unclear and difficult to return to its original image without knowing the mechanism of distortion. The process of deforming the image is called encryption, while the process of returning the image to its original form is called decryption (see figure 1).

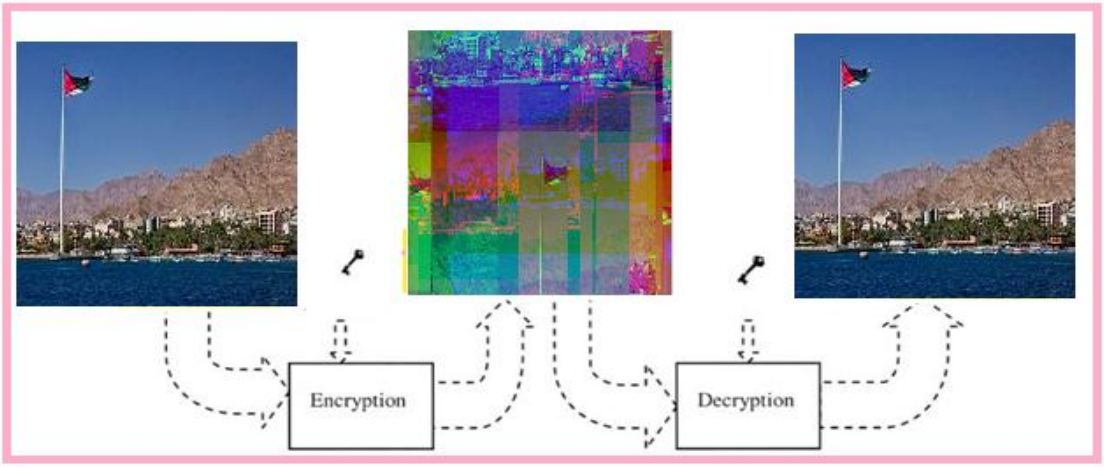

Figure 1: Color image encryption-decryption

The process for selecting the particular method of encryption depends on the extent to which this method fulfils the following conditions:

- Achieve a high degree of security so that the image is completely protected from the penetration process by using one or more private secret keys that are difficult to know or guess by any unauthorized third party.
- Ease of implementation.
- Increased speed of execution by reducing encryption and decryption times.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

- Increasing the percentage of distortion in the encoded image so that the error rate between the original image and the encoded image is very high or minimize the value of peak-signal-to-noise-ratio between the original and encrypted images.
- Retrieve the original image from the encrypted image without losing any information, meaning that the error rate between the original image and the decrypted image is zero or is close to zero.
-

II. IMAGE CRYPTOGRAPHY

For data security and protection [30], many methods were introduced to encrypt-decrypt digital signals. Some methods were based on signal segmentation [31], [32], others were based on adding and subtracting fixed noise to the signal [33], [34]. Some proposed methods were based on matrix multiplication and XORING Using huge private key [35], [36], [37], while others were based on signal blocking, dividing the original signal into blocks then each block was encrypted alone [38].
Cryptography means encryption-decryption [19], [20]. The process of data encryption [17], [18] , [42] is only the process of destroying the original data so that this data becomes distorted and incomprehensible to any third party who is not authorized [19], [20] and this process is usually carried out by carrying out specific processing operations on the original data and by using a secret key (as shown in figure 1) [21], [22] that is known only by the sender and its recipient[21], [22]. As for the decryption process, it is executed on the encrypted data using the secret key and the specific processing operations to obtain data identical to the original without losing or losing any part of the information [23], [24], [25].
In our research paper we will concentrate on Wavelet packet tree method (WPT) [39], [40], [41], this method can be easily used to decomposed color image into approximation and details applying the matlab function wavedec as shown in figure 2:

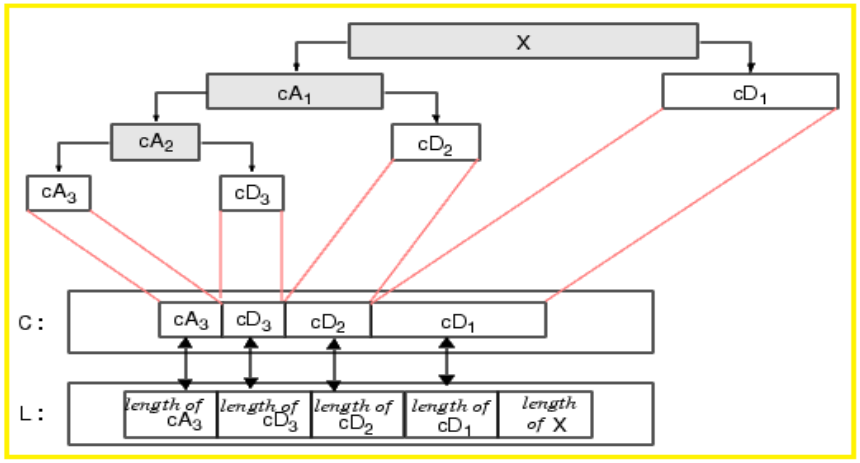

Figure 2: Decomposition signal x using WPT

Here by selecting the decomposition level we can obtain a set of approximations and details (C in the figure) with a specified length of each (L in the figure), these components can be used to divide a speech signal into segment with a defined length, these segments can be rearranged in order to generate an encrypted speech signal, figure 3 shows an example of signal decomposition using WPT:

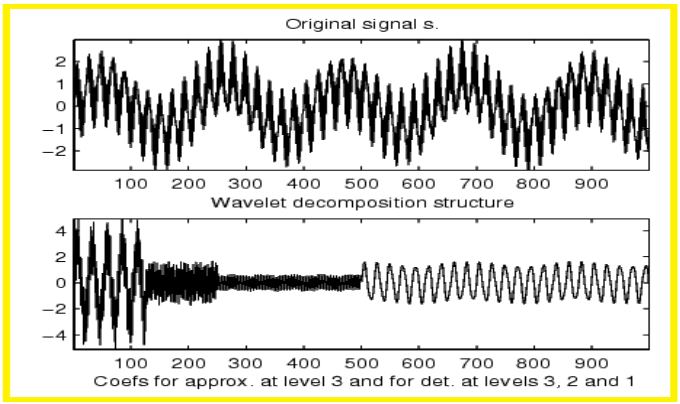

Figure 3: One row image decomposition example

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

The input data set in the WPT must be a row image so we have to reshape each color image matrix [18], [19] from 3D matrix to one row matrix as shown in figures 4 and 5.

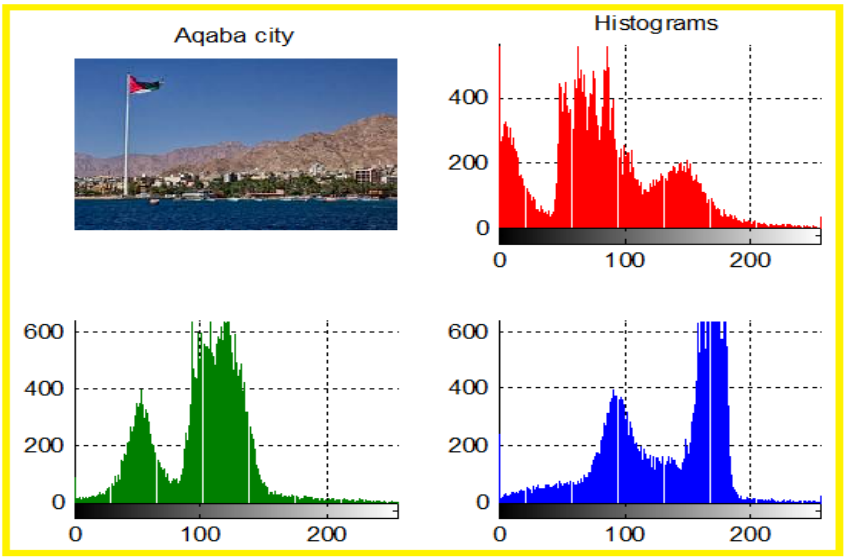

Figure 4: Original color image example

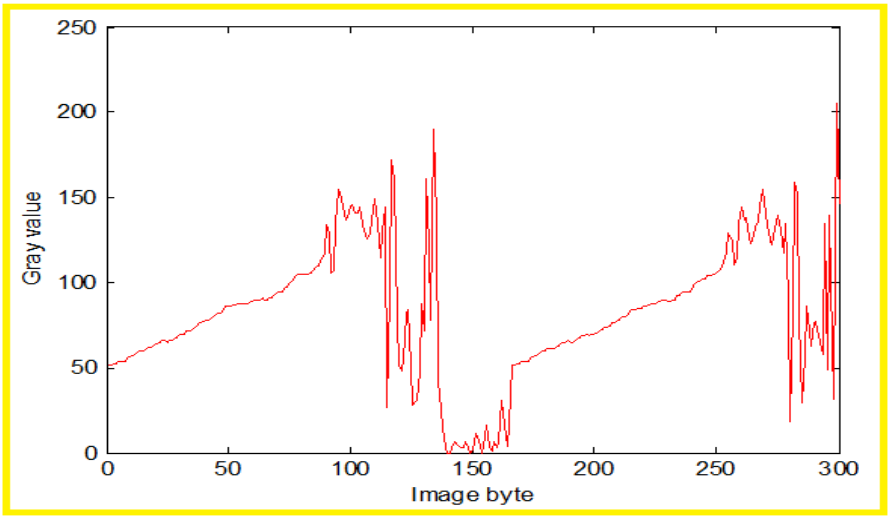

Figure 5: Part of the one row matrix (1 to 300 bytes).

III. THE PROPOSED METHOD

The proposed method of cryptography is based on WPT decomposition and it can be implemented applying the following steps:

Encryption phase:

- Reshape the color image matrix from 3D matrix to one row matrix.
- Select the levels of the first phase decomposition (the number of levels must be kept in secrete as a part of the private key).
- Decompose the row matrix into segments (using matlab wavedec function) as shown in figure 6.
- Select the largest segment.
- For the largest segment select a levels of decomposition (the number of levels must be kept in secrete as a second part of the private key).
- Apply decomposition.
- Rearrange the segments and use the results of reordering to form the encrypted image (the order sequence must also be kept in secret as a third part of the private key (PK)).
- The decryption phase can be implemented in the manner knowing the PK.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

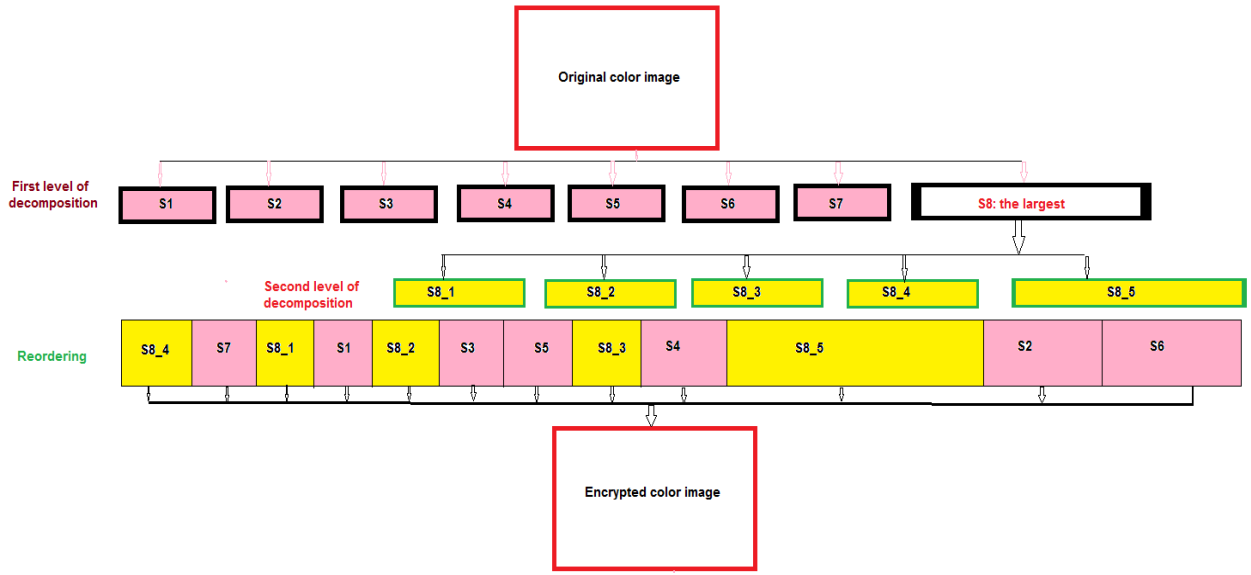

Figure 6: Encryption phase

Figure 7 shows the encrypted image for the image shown in figure 4:

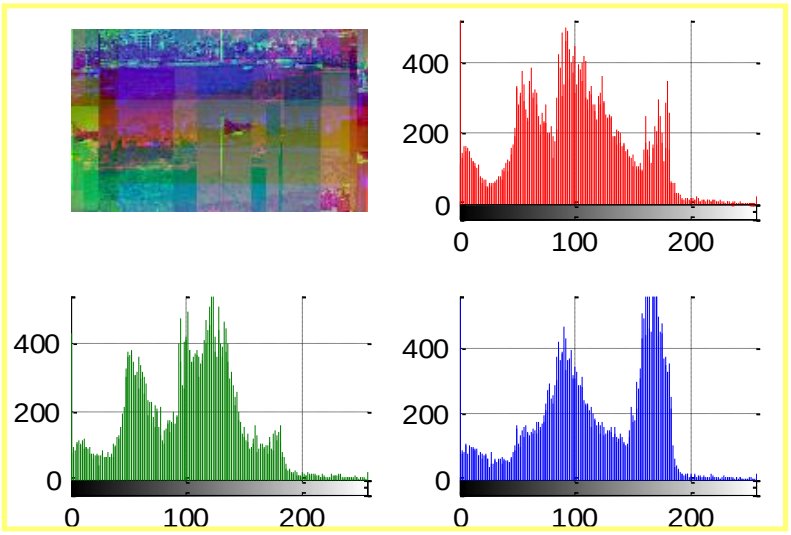

Figure 7: Encrypted image example

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

Different color images with various sizes were taken, and encrypted decrypted using the proposed method: The private key components were selected as follows:

- Levels of first decomposition were set to 9.
- Levels of second decomposition were set to 5.
- The rearrangement order was taken as shown in table 1:

Table 1: Rearrangement order

Segment number from the original image	Segments in the encrypted image
S1	S10_2
S2	S8
S3	S10_4
S4	S 5
S5	S10_1
S6	S3

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

S7	S10_5
S8	S1
S9	S9
S10_1	S10_3
S10_2	S4
S10_3	S7
S10_4	S2
S10_5	S10_6
S10_6	S6

The selected images were encrypted decrypted using the proposed method, tables 2, 3 and 4 shows the obtained experimental results:

Table 3: First round of decomposition

Image #	Size(byte)	Segments of first level of decomposition									
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
1	150849	295	295	590	1179	2358	4715	9429	18857	37713	75425
2	77976	153	153	305	610	1219	2437	4874	9747	19494	38988
3	518400	1013	1013	2025	4050	8100	16200	32400	64800	129600	259200
4	5140800	10041	10041	20082	40163	80325	160650	321300	642600	1285200	2570400
5	4326210	8450	8450	16900	33799	67598	135195	270389	540777	1081553	2163105
6	122265	239	239	478	956	1911	3821	7642	15284	30567	61133
7	518400	1013	1013	2025	4050	8100	16200	32400	64800	129600	259200
8	150975	295	295	590	1180	2359	4718	9436	18872	37744	75488
9	6119256	11952	11952	23904	47807	95614	191227	382454	764907	1529814	3059628
10	2500608	4884	4884	9768	19536	39072	78144	156288	312576	625152	1250304
Average	**1962600**										

Table 4: Second round of decomposition

Image #	S10 decomposition					
	S10-1	S10-2	S10-3	S10-4	S10-5	S10-6
1	2357	2357	4714	9428	18855	37709
2	1219	1219	2437	4873	9746	19492
3	8100	8100	16200	32400	64800	129600
4	80325	80325	160650	321300	642600	1285199
5	67597	67597	135194	270388	540775	1081550
6	1911	1911	3821	7641	15282	30564
7	8100	8100	16200	32400	64800	129600
8	2359	2359	4718	9436	18872	37743
9	95614	95614	191227	382454	764907	1529813
10	39072	39072	78144	156288	312576	625152

Table 5: Calculated parameters

Image #	Encryption time(seconds)	PSNR	Error
1	0.0154	14.7493	47373
2	0.0132	27.6740	17848
3	0.0330	23.6358	56315
4	0.3451	23.6769	17698
5	0.2925	20.1964	19321
6	0.0139	27.4418	22610
7	0.0368	23.6603	56246
8	0.0153	18.9766	38364
9	0.4153	30.3820	13809
10	0.1660	19.8691	14932
Average	**0.1346**	**23.0262**	**30452**
Throughput(byte/second)	**1962600/0.1346=14581000**		

DOI 10.17148/IJARCCE.2020.9629

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

Here the error was calculated using formula (1):

$$err = \sum_{i=1}^{n} \sqrt{(x1_i - x2_i)^2} \quad (1)$$

From the obtained experimental results we can see the following important points:

- The proposed method is flexible; it is easy to change the levels of decomposition and the rearrangement order.
- Segments have diffident sizes for the same image, and the segments length changes from image to another.
- The proposed method is highly secure because it uses a complex PK of thee parts.
- The proposed method satisfies the requirements of good method of cryptography by providing a high error and low PSNR between the original and the encrypted images, and vice versa between the original and the decrypted images.
- The proposed method has a good average of encryption-decryption time.
- The proposed method provides a high value of throughput.

V. CONCLUSION

An easy and flexible method of color image cryptography was proposed, implemented and tested using various color images, it was shown that this method provides a high level of security by using a complex and complicated private key, the proposed method satisfies the requirements of good method of cryptography by totally destroying the original image to get the encrypted one, and by generating the decrypted image which is identical to the original one without losing any piece of information.

REFERENCES

[1]. Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8, issue 5, pp. 2780, 2018.

[2]. Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, vol. 8, issue 10, pp. 1175-1182, 2010.

[3]. 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, vol. 153, issue 2, pp. 31-34, 2016.

[4]. 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.

[5]. Mohammed Ashraf Al Zudool, Saleh Khawatreh, Ziad A. Alqadi, Efficient Methods used to Extract Color Image Features, IJCSMC, vol. 6, issue 12, pp. 7-14, 2017.

[6]. Akram A. Moustafa and Ziad A. Alqadi, Reconstructed Color Image Segmentation, Proceedings of the World Congress on Engineering and Computer Science, WCECS 2009, vol. II, 2009.

[7]. 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, vol. 96, issue 13, pp. 4081-4091, 2018.

[8]. Bilal zahran, jamil al-azzeh, ziad alqadi, mohd–ashraf alzoghoul, saleh khawatreh, a modified lbp method to extract features from color images, journal of theoretical and applied information technology, vol. 96, issue 10, pp. 3014-3024, 2018.

[9]. Waheeb Abu Ulbeh, Akram Moustafa, Ziad A Alqadi, Gray image reconstruction, European Journal of Scientific Research, vol. 27, issue 2, pp. 167-173, 2009.

[10]. Dr Rushdi S Abu Zneit, Dr Ziad alqadi, Dr Mohammad Abu Zalata, A Methodology to Create a Fingerprint for RGB Color Image, IJCSMC, vol. 6, issue 1, pp. 205-212. 2017.

[11]. RA Zneit, Ziad Alqadi, Dr Mohammad Abu Zalata, Procedural analysis of RGB color image objects, IJCSMC, vol. 6, issue 1, pp. 197-204, 2017.

[12]. Amjad Y Hindi, Majed O Dwairi, Ziad A alqadi, A Novel Technique for Data Steganography, Engineering, Technology & Applied Science Research, vol. 9, issue 6, pp. 4942-4945, 2019.

[13]. Mutaz Rasmi Abu Sara Rashad J. Rasras, Ziad A. Alqadi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, Engineering, Technology & Applied Science Research, vol. 9, issue 1, pp. 3681-3684, 2019.

[14]. Prof. Ziad Alqad i Prof. Yousif Eltous, Dr. Majed Omar Dwairi, Dr. Mohammad S. Khrisat, Dr. Saleh A. Khawatreh, Secure Secret Message Steganography (SSMS), International Journal of Computer Science and Mobile Computing, vol. 9, issue 6, pp. 1-9, 2020.

[15]. Prof. Ziad Alqadi Dr. Mohammad S. Khrisat, Prof. Yousif Eltous, Dr. Saleh A. Khawatreh, Dr. Majed Omar Dwairi, Building Face Recognition System (FRS), International Journal of Computer Science and Mobile Computing, vol. 9, issue 6, pp. 15-24, 2020.

[16]. Jamil Al-Azzeh Naseem Asad, Ziad Alqadi, Ismail Shayeb, Qazem Jaber, Simple Procedures to Create HSCS, International Journal of Engineering Research And Management (IJERM), vol. 7, issue 5, pp. 6-10, 2020.

[17]. Ziad Alqadi, Mohammad Abuzalata, Yousf Eltous, Ghazi M Qaryouti, Analysis of fingerprint minutiae to form fingerprint identifier, International Journal on Informatics Visualization, vol. 4, issue 1, pp. 10-15, 2020.

[18]. Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 465-470, 2016.

[19]. Belal Zahran Rashad J. Rasras , Ziad Alqadi, Mutaz Rasmi Abu Sara, Developing new Multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 6,pp. 3228-3235, 2020.

[20]. Ziad Alqad, Majid Oraiqat, Hisham Almujafet, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.
[21]. Jamil Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, JOIV: International Journal on Informatics Visualization, vol. 4, issue 2, pp. 40-44, 2020.
[22]. Prof. Yousif Eltous Prof. Ziad Alqadi , Dr. Mohammad S. Khrisat ,Dr. Jihad Nader, Securing LSB2 Message Steganography, International Journal of Computer Science and Mobile Computing, vol. 9, issue 6, pp. 156 – 164, 2020.
[23]. Dr. Jihad Nader Prof. Ziad Alqadi , Dr. Mohammad S. Khrisat, A Survey of RGB Color Image Encryption Methods, IJCSMC, vol. 9, issue 6, pp. 106 – 113, 2020.
[24]. Prof. Ziad Alqad i Prof. Yousif Eltous, Dr. Majed Omar Dwairi, Dr. Mohammad S. Khrisat, Dr. Saleh A. Khawatreh, Secure Secret Message Steganography (SSMS), International Journal of Computer Science and Mobile Computing, vol. 9, issue 6, pp. 1-9, 2020.
[25]. Prof. Ziad Alqadi Dr. Saleh A. Khawatreh, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, A Novel Method to Encrypt-Decrypt Digital Speech Signal (EDDSS), International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 4, pp. 117-123, 2020.
[26]. Dr. Majed Omar Dwairi Prof. Ziad Alqadi , Dr. Mohammad S. Khrisat , Dr. Amjad Hindi, Simple and Highly Secure, Efficient and Accurate Method (SSEAM) to Encrypt-Decrypt Color Image, International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 4, pp. 64-69, 2020.
[27]. Ziad A. Alqadi, A Highly Secure and Accurate Method for RGB Image Encryption, IJCSMC, vol. 9, issue 1, pp. 12-21, 2020.
[28]. Belal Ayyoub Ziad Alqadi, Ahmad Sharadqh, Naseem Asad Ismail Shayeb, Jamil Al-Azzeh, A highly secure method of secret message encoding, International Journal of Research in Advanced Engineering and Technology, vol. 5, issue 3, pp. 82-87, 2019.
[29]. Majed O Al-Dwairi, A Hendi, Z alqadi, An efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology & Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.
[30]. Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, A novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, iss.1, pp. 232-238, 2019.
[31]. Mutaz Rasmi Abu Sara Rashad J. Rasras, Ziad A. Alqadi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, Engineering, Technology & Applied Science Research, vol. 9, issue 1, pp. 3681-3684, 2019.
[32]. Dr. Saleh A. Khawatreh Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Digital color image encryption-decryption using segmentation and reordering, International Journal of Latest Research in Engineering and Technology (IJLRET), vol. 6, issue 5, pp. 6-12, 2020.
[33]. Dr. Saleh Prof. Ziad Alqadi , Dr. Mohammad S. Khrisat , Dr. Amjad Hindi , Dr. Majed Omar Dwairi, color image encryption-decryption using SMT, International Journal of Engineering Technology Research & Management, vol. 4, issue 5, pp. 32-40, 2020.
[34]. Prof. Ziad Alqadi Prof. Yousif Eltous, Dr. Akram Moustafa Hamarchi, Dr. Mohammad S. Khrisat, Dr. Saleh A. Khawatreh, Color Image Encryption-Decryption using RANDOM Noise and PMT, International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 5, pp. 1-7, 2020.
[35]. Prof. Ziad Alqadi Prof. Yousif Eltous, Dr. Akram Moustafa Hamarchi, Dr. Mohammad S. Khrisat, Dr. Saleh A. Khawatreh, speech signal encryption-decryption using noise signal and PMT, International Journal of Engineering Technology Research & Management, vol. 4, issue 5, pp. 49-59, 2020.
[36]. 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, pp. 14-26, 2019.
[37]. Musbah J Aqel, Ziad alqadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7, issue 3, pp. 104-107, 2018.
[38]. Jihad Nadir, Ziad Alqadi, Ashraf Abu Ein, Classification of Matrix Multiplication Methods Used to Encrypt-decrypt Color Image, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 459-464, 2016.
[39]. 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, vol. 3, issue 1, pp. 86-93, 2019.
[40]. Prof. Ziad Alqadi, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Dr. Mohammad S. Khrisat, Features Analysis of RGB Color Image based on Wavelet Packet Information, IJCSMC, vol. 9, issue 3, pp. 149 – 156, 2020.
[41]. Ziad Alqadi Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, valuable wavelet packet information to analyze color images features, International Journal of Current Advanced Research, vol. 9, issue 2, pp. 2319-6505, 2020.
[42]. Amjad Hindi, Majed Omar Dwairi, Ziad Alqadi, Analysis of Digital Signals using Wavelet Packet Tree, IJCSMC, vol.9, iss.2, pp.96-103, 2020.
[43]. Aws Al-Qaisi, A. Manasreh, A. Sharadqeh, Z. Alqadi, Digital Color Image Classification Based on Modified Local Binary Pattern Using Neural Network, International Journal on Communications Antenna & Propagation (I.Re.C.A.P), vol.9, iss.6, pp.403-408, 2019