Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 7, July 2020, pg.77 – 85

Protecting Digital Color Image Applying Double Phase Encryption

Prof. Ziad Alqadi*[1]; Holwa Fayeq Taha[2]
[*1]Department of Computer Engineering, Faculty of Engineering Technology, Al-Balqa Applied University, Jordan
[2]Department of Physics, Faculty of Science, Al-Balqa Applied University, Jordan
natalia_maw@yahoo.com *[1], h.taha@bau.edu.jo [2]

Abstract: Digital image is one of the most important types of data used due to the large number of computerized applications that are needed for mankind. Some computerized applications that use digital images need a high level of security to protect the image, and to turn it into a vague and incomprehensible image to any third party, and that is why we have to seek a secure method of cryptography to protect the digital color images. In this paper we will introduce method based wavelet packet tree decomposition and reconstruction to generate an encrypted image, the encrypted image then will be XORed to get the final encrypted image. The method will use a complicated key which contains two parts the ordering sequences and the XORing key to form a total PK. The method will be implemented to measure the quality values such as MSE, PSNR and encryption-decryption time.

Keywords: Digital image, XORing, WPT, decomposition, level, MSE, PSNR, encryption, decryption.

Introduction

Digital color image [3], [4], [5] is one of the most important types of data [1], [2], [6], [7], for use in important human applications[8],[9],[10], including banking [14], [15], [16] and security applications and expert systems [11], [12], [13]. Mostly color image requires a high level of protection for several reasons, including [17], [18], [19]:

- The digital image can be very confidential [20], [21].
- The image may be of a personal nature [22].
- The digital image may hold or contain highly confidential data [23], [24].

And for the reasons mentioned above, it is necessary to provide a method that verifies the destruction of the original image and its distortion so that it is difficult to understand with the naked eye or difficult to retrieve it from any other party trying to spy on the image and at the same time facilitate the process of recovering the distorted image by the relevant persons or institutions [25], [26], [30].
The process of distorting the image is called the encryption process. From the name, the encryption process must be characterized by the following [27], [28], [29]:

- Full protection of the image through the use of private keys those are difficult to penetrate.
- Ease of implementation and speed to implement the encryption process.
- Maximizing the error rate (Mean square error (MSE)) between the original image and the encrypted image [27].

- Reducing the peak-to-signal-noise ratio (PSNR) value between the original image and the encrypted image [31], [32].

Cryptography is used to protect data including image, the protected image must be totally destroyed by using one or more complicated private secrete keys, these keys must highly secure in order to prevent the hacking process as shown in figure 1:

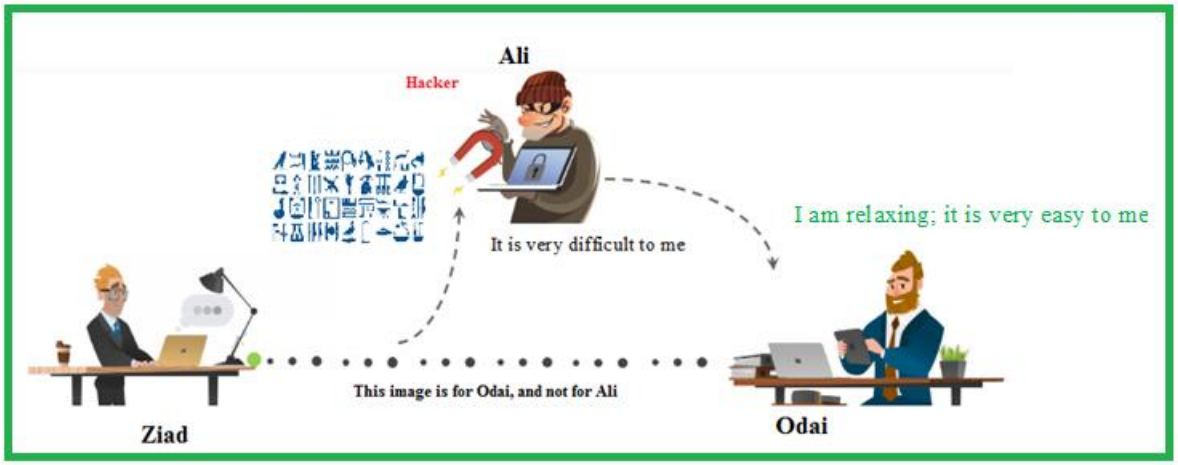


Figure 1: Preventing hacking

Many methods were proposed and used to encrypt-decrypt digital images. 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], [42].

Digital color image decomposition using WPT

Wavelet packet tree method (WPT) [39], [40], [41] can be easily used to decomposed digital speech signal into approximation and details applying the matlab function wavedec as shown in figure 2:

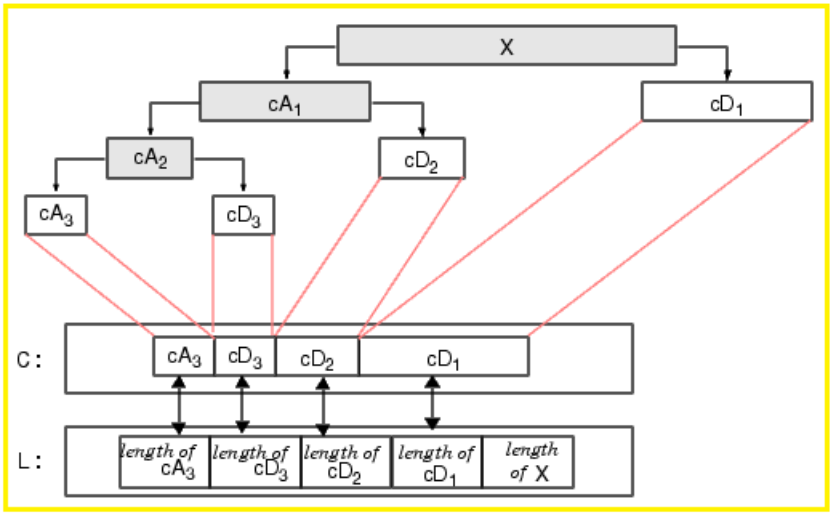


Figure 2: Signal X decomposition using WPT

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 digital color image into segment with a predefined length, these segments can be rearranged in order to generate an encrypted digital color image.

The proposed method

The proposed method as shown in figure 3 is based into two phases to generate the encrypted color image:

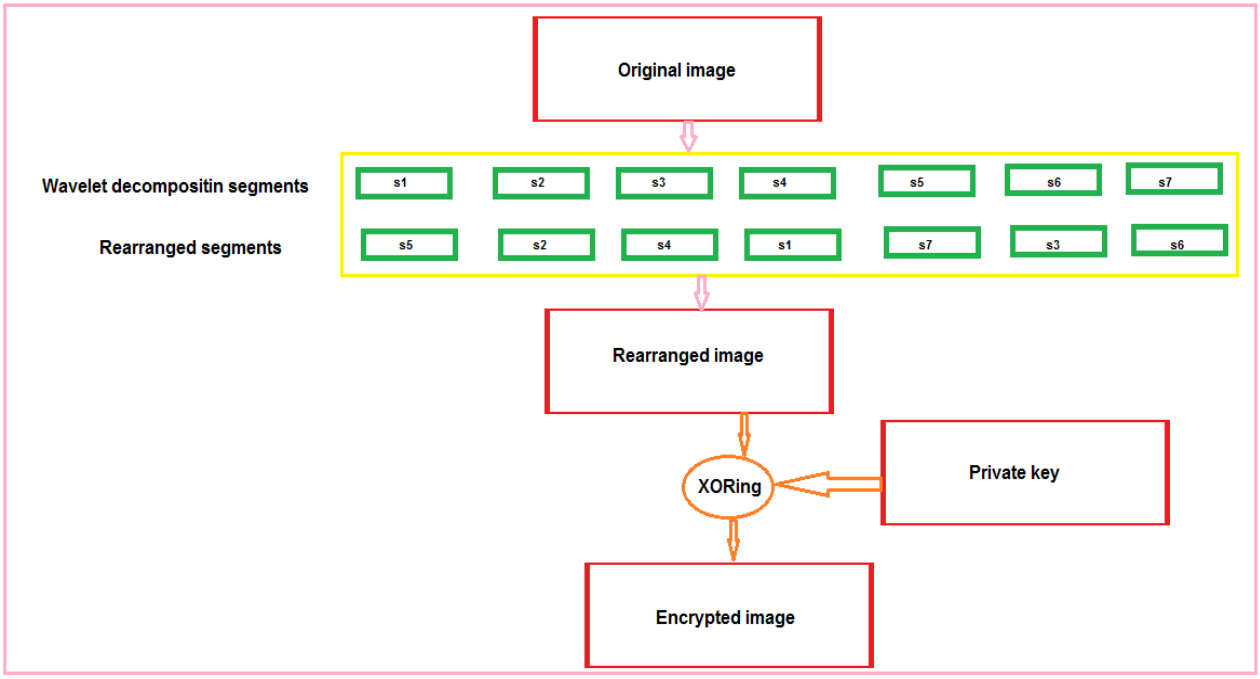


Figure 3: Encryption phase

1) Image rearrangement, by decomposition the image into segment using a selected number of key, then we use the obtained segments size to divide a one raw image matrix into segment, theses segments are to be reordered to form a new one raw matrix, the orders must be kept in secrete to be used as a part of the private key (PK).
2) The reordered image then to be used to be generated the final encrypted version by applying XORing operation using a huge 3D matrix key, this key is to be generated once, and saved to be known by the sender and receiver, this key will be used as a second part of the PK.

Figure 4 shows the image of the matrix PK.

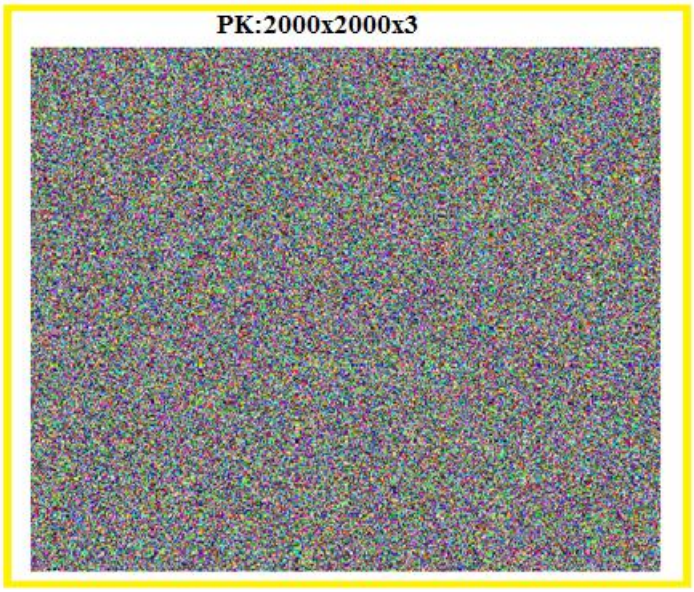


Figure 4: 3D matrix PK

Figure 5 shows an example of XORing operation, while figure 6 shows an example of data decomposition:

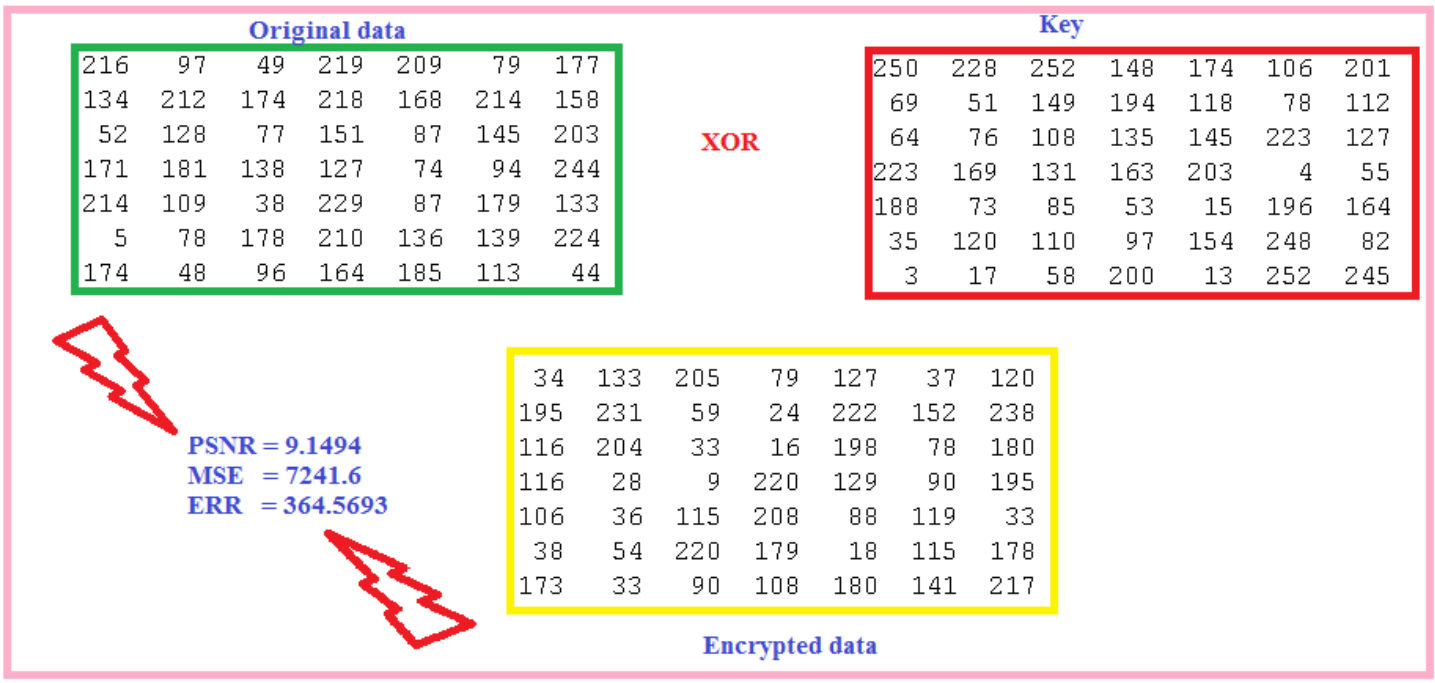


Figure 5: XORing example

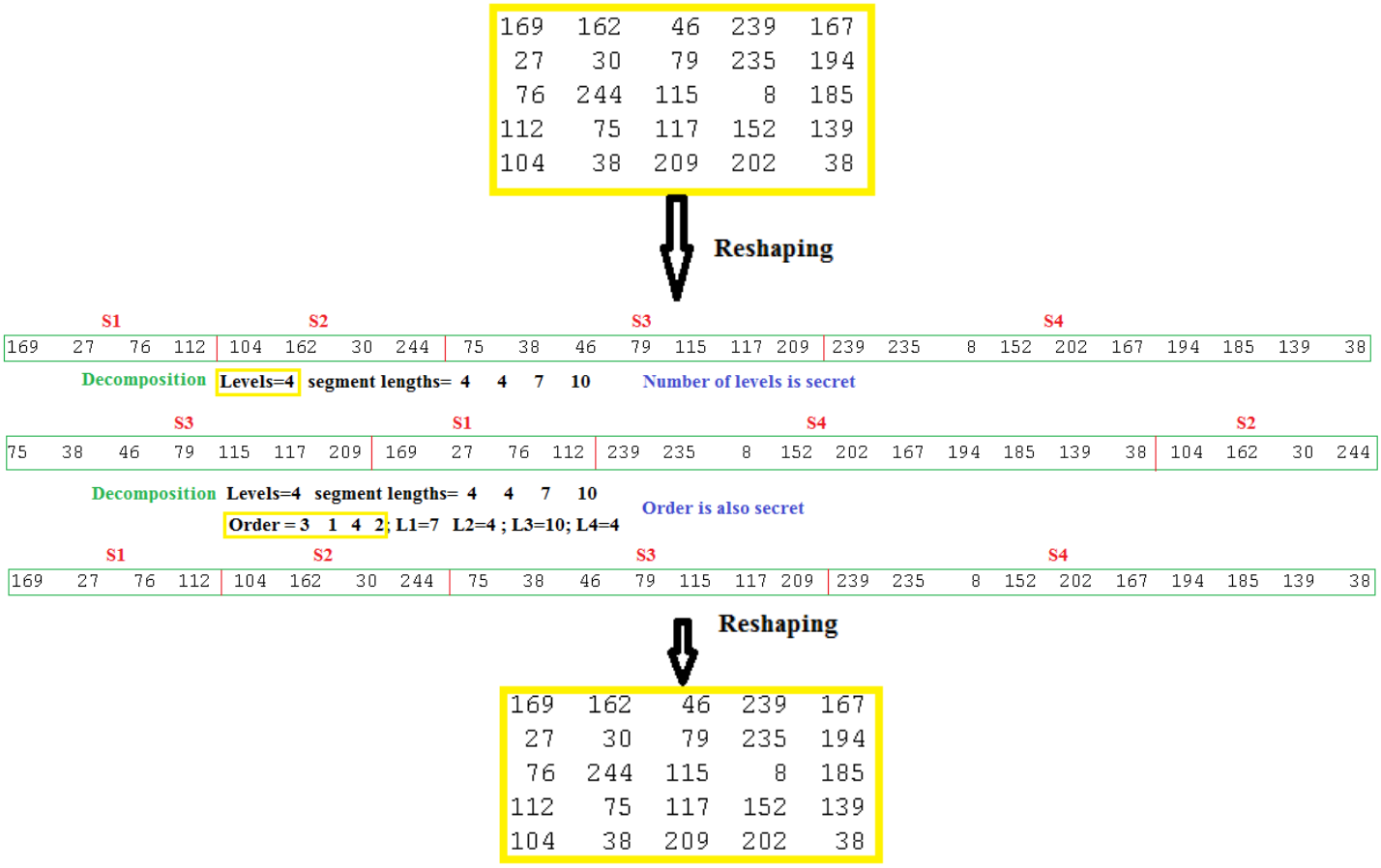
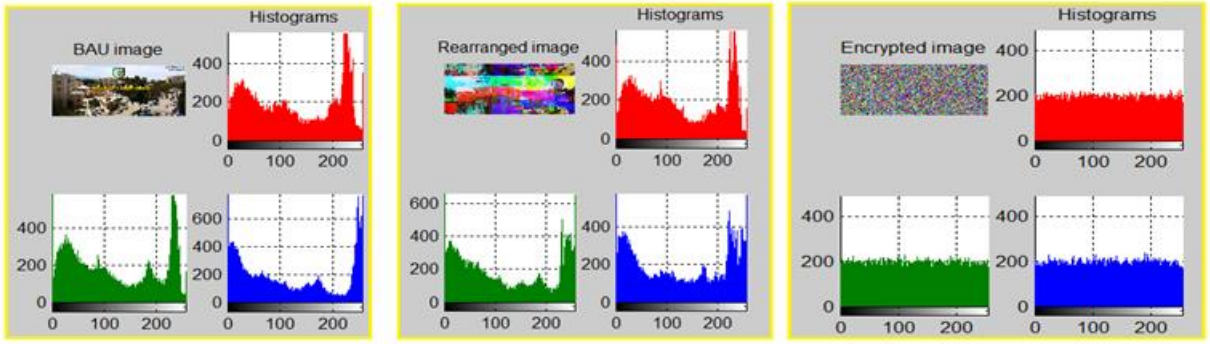


Figure 6: Decomposition and reordering example

Decryption works in the opposite way by applying XORing then reordering.

Implementation and experimental results

The proposed method was implemented using various images, figure 7 shows a sample output.



a) b) c)

Figure 7: Image example a) original b) Rearranged c) Encrypted

10 images were taken and they were encrypted decrypted using the proposed method: table 1 shows the segments lengths for each used image:

Table 1: Obtained segments lengths

Image number	Decomposed segments length							
	S1	S2	S4	S4	S5	S6	S7	S8
1	1179	1179	2358	4715	9429	18857	37713	75425
2	610	610	1219	2437	4874	9747	19494	38988
3	4050	4050	8100	16200	32400	64800	129600	259200
4	40163	40163	80325	160650	321300	642600	1285200	2570400
5	33799	33799	67598	135195	270389	540777	1081553	2163105
6	956	956	1911	3821	7642	15284	30567	61133
7	4050	4050	8100	16200	32400	64800	129600	259200
8	1180	1180	2359	4718	9436	18872	37744	75488
9	47807	47807	95614	191227	382454	764907	1529814	3059628
10	19536	19536	39072	78144	156288	312576	625152	1250304

The following order was used as a part of PK:

PK2= 7 4 7 1 8 5 2 6 3, and thus table 2 shows the reordering sequence:

Table 2: Reordering sequence

Segment number	Rearrangement order
1	4
2	7
3	1
4	8
5	5
6	2
7	6
8	3

The two phase of encryption were applied, table 3 and 4 shows the results of implementation:

Table 3: Implementation results (encryption phase)

Image number	Size(byte)	MSE	PSNR	Encryption time(second)
1	150849	15547	14.3090	0.1770
2	77976	44618	26.7922	0.1270
3	518400	71338	17.7590	0.2470
4	5140800	96352	19.0935	1.2460
5	4326210	95470	19.1854	1.0610
6	122265	83645	20.5077	0.1350
7	518400	12071	16.8397	0.2300
8	150975	11229	17.5631	0.1430
9	6119256	70923	22.1576	1.4850
10	2500608	12132	16.7890	0.7080

Table 4: Implementation results (decryption phase)

Image number	Size(byte)	MSE	PSNR	Encryption time(second)
1	150849	0	Infinite	0.1770
2	77976	0	Infinite	0.1270
3	518400	0	Infinite	0.2470
4	5140800	0	Infinite	1.2460
5	4326210	0	Infinite	1.0610
6	122265	0	Infinite	0.1350
7	518400	0	Infinite	0.2300
8	150975	0	Infinite	0.1430
9	6119256	0	Infinite	1.4850
10	2500608	0	Infinite	0.7080

From the obtained results we raise the following:

- The proposed method has a high seurity level by using two complicated keys.
- Simple to implement.
- Significant small time for encryption and decryptionn, and the has linear relationship with the image size(as shown in figure 8).
- High MSE value and low PSNR values (between the original and the encrypted images), which mean that the encryption process totally destryed the original image.
- Zero MSE value and infinite PSNR values (between the original and the deccrypted images), which mean that the decryption process recovered in image identical to theoriginal image image.
- Flixeble, ant time we can change the number of decomposition levlels, and thus we can change the number of segments and the length of each segment.

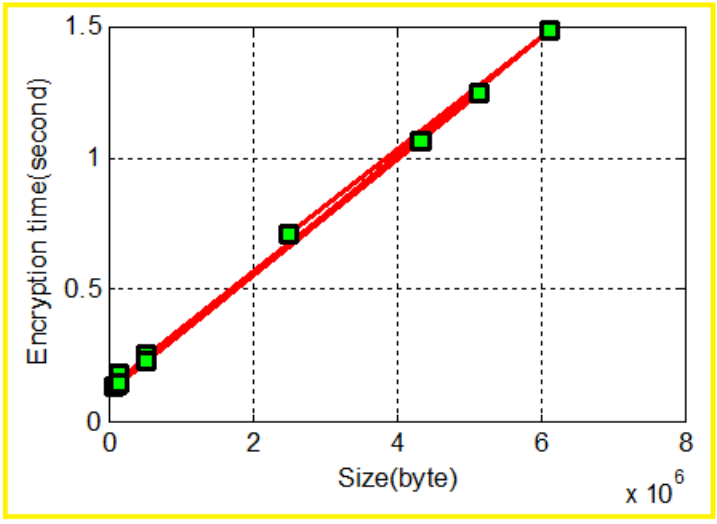


Figure 8: Encryption time and image size

Conclusion

A simple, flexible, highly secure method of color image encryption-decryption was proposed, implemented and tested. The obtained experimental results show that the proposed method satisfied the requirement of good methods of data cryptography by giving an excellent value for MSE, PSNR, encryption and decryption times, and that is why it can be highly recommended.

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.

[1] 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.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

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

[11] 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.

[12] 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.

[13] Prof. Ziad Alqadi 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.

[14] 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.

[15] 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.

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

[17]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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] Prof. Ziad Alqadi 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.

[24] 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.

[25] 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.

[26] Ziad A. AlQadi, A Highly Secure and Accurate Method for RGB Image Encryption, IJCSMC, vol. 9, issue 1, pp. 12-21, 2020.

[27] 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.

[28] 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.

[29] 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, issue 1, pp. 232-238, 2019.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] Amjad Hindi, Majed Omar Dwairi, Ziad Alqadi, Analysis of Digital Signals using Wavelet Packet Tree, IJCSMC, vol. 9, issue 2, pp. 96-103, 2020.

[42] 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 and Propagation (I.Re.C.A.P.), vol. 9, issue 6, pp. 403-408, 2019.

