ISSN: 2454-1907
International Journal of Engineering Technologies and Management Research
July 2020, Vol 7(07), 71 – 79
DOI: https://doi.org/10.29121/ijetmr.v7.i7.2020.727

SPEECH SIGNAL CRYPTOGRAPHY USING WPT

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

DOI: https://doi.org/10.29121/ijetmr.v7.i7.2020.727

Article Citation: Prof. Ziad Alqadi, and Holwa Fayeq Taha. (2020). SPEECH SIGNAL CRYPTOGRAPHY USING WPT. International Journal of Engineering Technologies and Management Research, 7(7), 71-79. https://doi.org/10.29121/ijetmr.v7.i7.2020.727

Published Date: 26 July 2020

Keywords:
Speech
WPT
Decomposition
Level
Approximations
Details
Encryption
Decryption
Error

ABSTRACT

Digital speech signal 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 signals need a high level of security to protect the signal, and to turn it into a vague and incomprehensible signal to any third party, and that is why we have to seek a secure method of cryptography to protect the speech signal. In this research paper we will introduce a method based wavelet packet tree decomposition and reconstruction to generate an encrypted speech, the method will reorder the original speech using a secret number of decomposition levels, the obtained wavelet decomposition sizes will be used to form a speech segments, which must be rearranged in a secret order to get the encrypted speech, the introduced method will be implemented and evaluated to prove the security issues.

1. INTRODUCTION

The digital signal [3], [4], [5] such as sound [1] and digital image [2], [6], [7] is considered one of the most important types of data currently used and one of the most widely circulated data [8], [9], [10]. The digital audio signal may be confidential, it may be of a personal nature, or it may contain important data [11], [12], [13] which requires distortion and making it incomprehensible to any third party that is not authorized to deal with this signal. Digital signals are very important because they are used in vital applications such as in fingerprint recognition [14], [15], [16] systems and facial recognition systems [15], [16] to identify specific person.

Cryptography means encryption-decryption. The process of data encryption [17], [18] 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. 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].

© 2020 The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

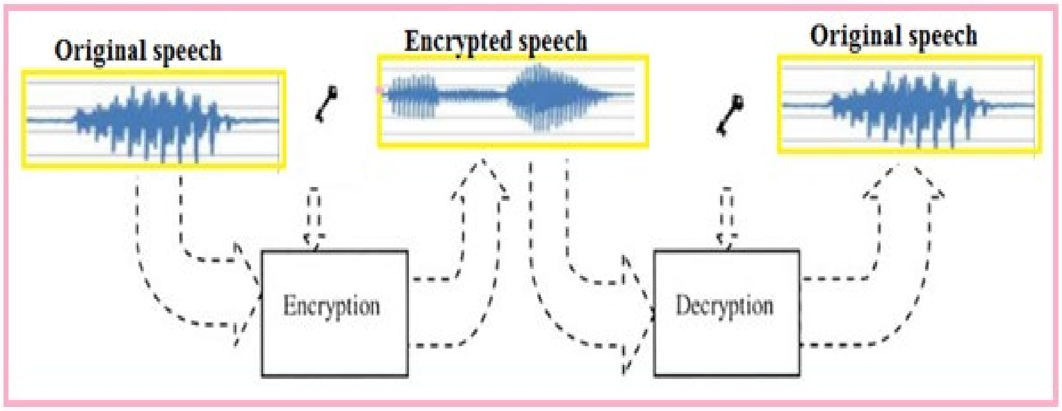

Figure 1: Speech encryption-decryption

The encryption and decryption method is good if you achieve the following things [26], [27], [28], [29], [42]:

- Security and protection so that it is difficult for any third party to penetrate data.
- Achieve a high level of distortion so that the error value between the original data and the encoded data is high.
- Achieving a very high percentage of correspondence between the original data and the data that was decoded so that the error ratio between them falls to zero.
- Do not lose or lose any part of the information during encryption and decryption.
- Ease of implementation.
- The speed of the encryption and decryption process.

For data protect [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];

2. SIGNAL 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:

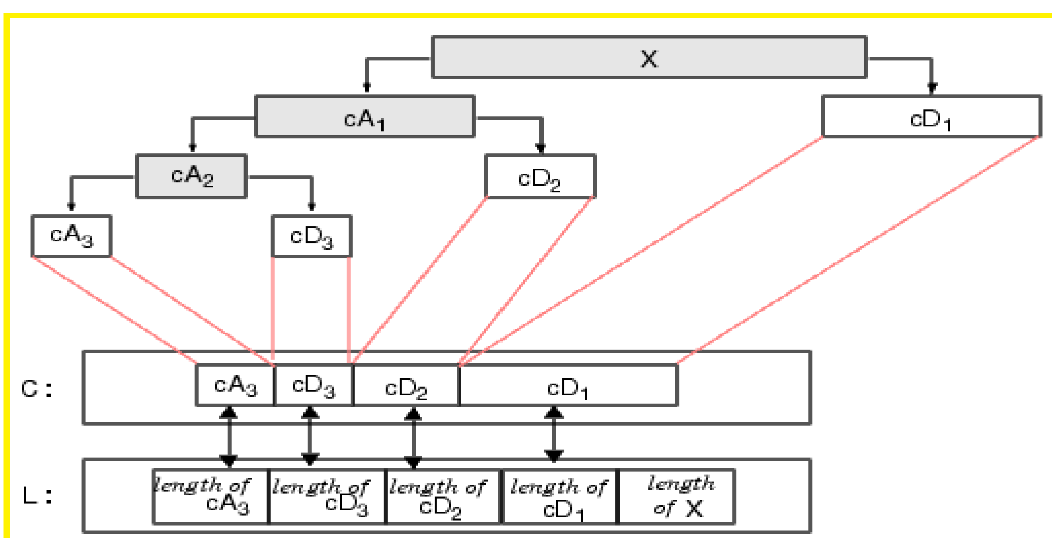

Figure 2: Signal X decomposition using WPT

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 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:

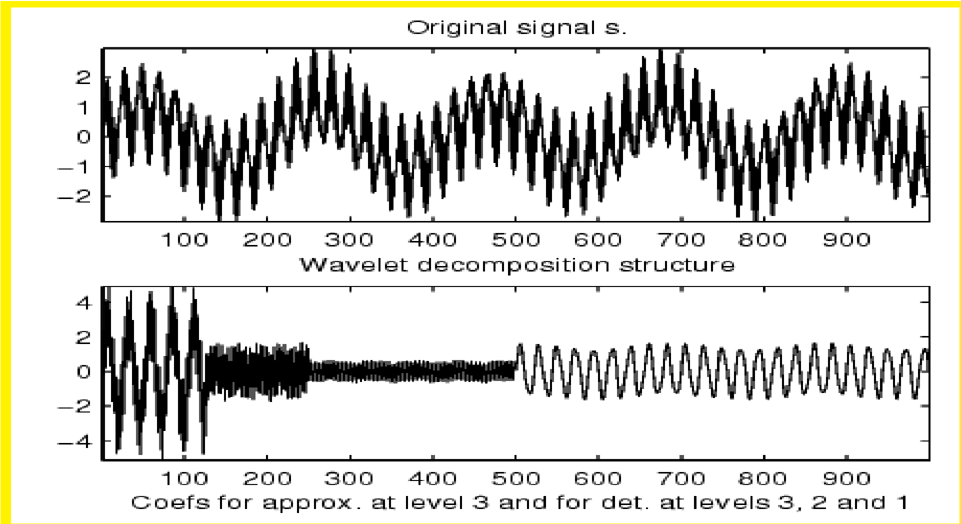

Figure 3: Speech signal decomposition example

3. THE PROPOSED METHOD

The proposed method of encryption-decryption is based on WPT decomposition, and the encryption phase as shown in figure 4 can be implemented applying the following steps:

1) Get the original speech signal.
2) Reshape the signal matrix (whether it is mono or stereo) to one row matrix.
3) Select a level of decomposition to be used as private key (PK1).
4) Apply wavedec
5) Get the length of each approximation.
6) Use the length to divide the speech matrix into segments.
7) Select a rearrangement order to rearrange the segment (this is to be used as PK2).
8) Rearrange the speech matrix to get the encrypted one.
9) Reshape back the matrix to get the encrypted speech signal.

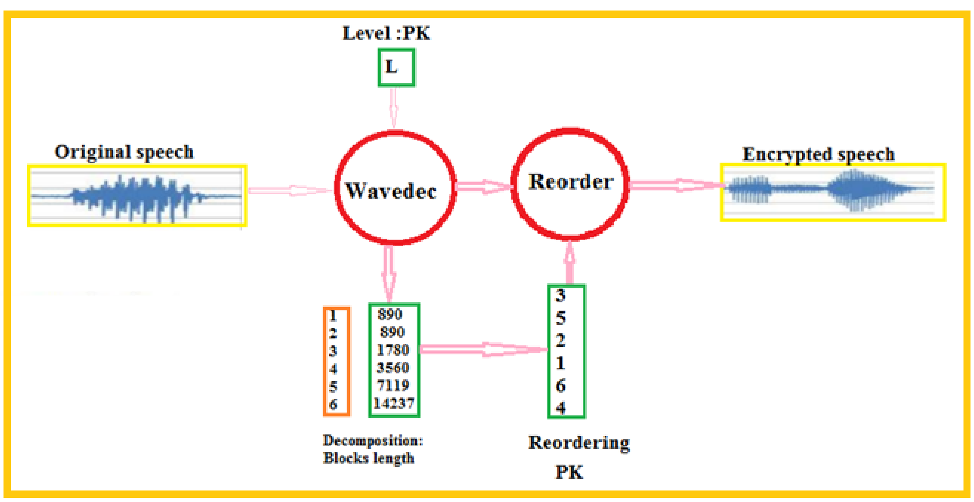

Figure 4: Encryption phase

The decryption phase as shown in figure 5 can be implemented applying the following steps:

1) Get the encrypted speech signal.
2) Reshape the signal matrix (whether it is mono or stereo) to one row matrix.
3) Retrieve the level of decomposition to be used as private key (PK1).
4) Apply wavedec
5) Get the length of each approximation.
6) Use the length to divide the speech matrix into segments.
7) Retrieve the rearrangement order to rearrange the segment (this is to be used as PK2).
8) Rearrange the speech matrix to get the decrypted one.
9) Reshape back the matrix to get the decrypted speech signal.

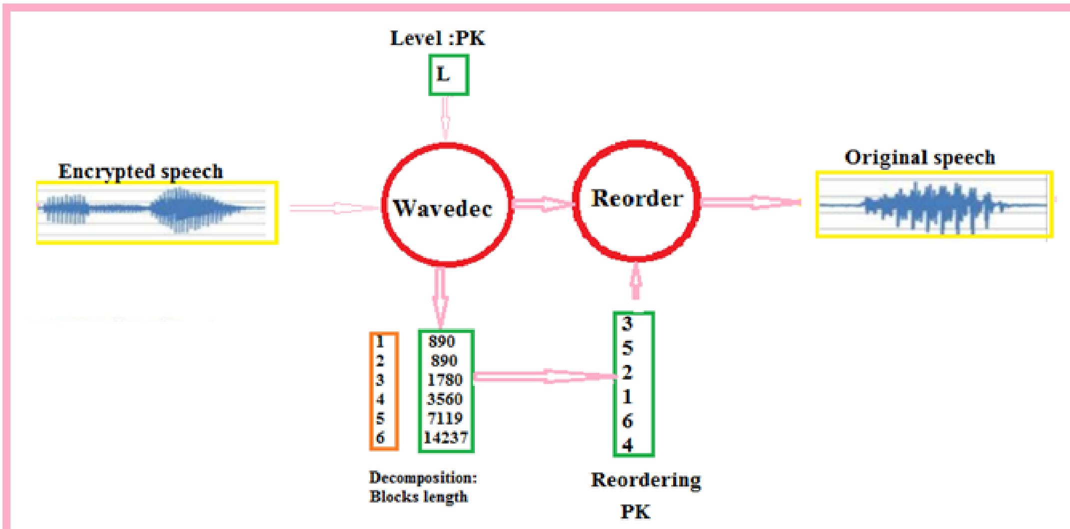

Figure 5: Decryption phase

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The following speeches shown in table 1 were recorded using sampling frequency 44100 samples per second; these speeches were used in our experiments:

Table 1: Used speeches

Speech number	Recorded speech	Size(sample)
1	Al-Balqa Applied University is a Jordanian university	260635
2	Speech encryption decryption method	181102
3	Amman is the capital city of Jordan	183544
4	Ziad Abdel kareem Alqadi	171261
5	Mohammad Khrisat	110368
6	Yousif Eltous	135114
7	Jihad Nader	96690
8	Saleh Khawatreh	109474
9	Aqaba is a wonderful city located on the red sea	223861
10	May God protect Jordanians and all mankind	220897

Figure 6 shows the plot of speech 1 and the encrypted version of this speech.

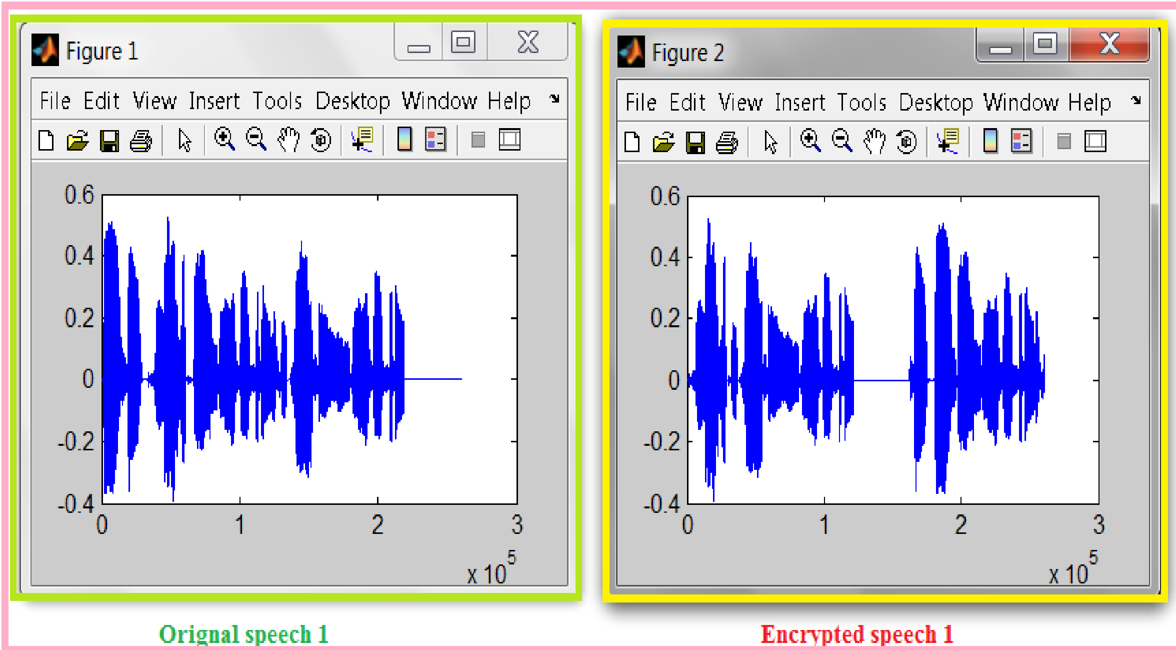

Figure 6: Speech 1 encryption.

We selected a level of decomposition equal 6(PK 1=5), then we applied decomposition for each of the used speech signal, table 2 shows the obtained segment length for each speech signal:

Table 2: Speech segments length

Speech number	Segments length					
	1	2	3	4	5	6
1	8145	8145	16290	32580	65159	130318
2	5660	5660	11319	22638	45276	90551
3	5736	5736	11472	22943	45886	91772
4	5352	5352	10704	21408	42816	85631
5	3449	3449	6898	13796	27592	55184
6	4223	4223	8445	16890	33779	67557
7	3022	3022	6044	12087	24173	48345
8	3422	3422	6843	13685	27369	54737
9	6996	6996	13992	27983	55966	111931
10	6904	6904	13807	27613	55225	110449

The segments were rearranged using the rearrangement order (PK 2) shown in table 3:

Table 3: Rearrangement order

Segment order	New order (PK2)
1	4
2	6
3	3
4	1
5	2
6	5

Using the new order the speeches were encrypted decrypted, table 4 shows the obtained results:

The error was calculated using formula 1:

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

Where x1 is the original signal; And x2 is the encrypted/decrypted signal

Table 4: Experimental results

Speech number	Error between original and encrypted speeches	Error between original and decrypted speeches	Encryption time(seconds)	Decryption time (Seconds)
1	68.1420	0	0.148000	0.148000
2	38.0654	0	0.131000	0.131000
3	41.7242	0	0.146000	0.146000
4	43.6924	0	0.129000	0.129000
5	29.9639	0	0.121000	0.121000
6	30.1948	0	0.128000	0.128000
7	34.0084	0	0.119000	0.119000
8	38.2777	0	0.124000	0.124000
9	41.0847	0	0.141000	0.141000
10	43.8856	0	0.155000	0.155000

From the obtained experimental results we can raise the following facts:

- It is easy to use WPT decomposition for signal encryption-decryption.
- It is easy to change the number of levels and the number of segments.
- The encryption-decryption method is secure by using 2 private keys.
- It is easy to change PK2.
- The proposed method provides a good quality of encryption by providing a high error between the original and the encrypted signal.
- The proposed method is efficient by providing significantly small time for encryption-decryption.

5. CONCLUSION

A method based on WPT decomposition for speech signal encryption-decryption was proposed, implemented and tested. The obtained experimental results showed that this method is flexible in selecting the decomposition level, and in selecting the new segments order. It was shown that this method has a high quality and it was efficient in performing encryption-decryption without losing any piece of information.

SOURCES OF FUNDING

None.

CONFLICT OF INTEREST

None.

ACKNOWLEDGMENT

None.

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