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. 10, Issue. 9, September 2021, pg.53 – 65

Efficient WPT Based Speech Signal Protection

Dr. Hatim Zaini; Prof. Ziad A.A Alqadi
Taif University, KSA
BAU, Jordan
DOI: 10.47760/ijcsmc.2021.v10i09.006

Abstract
Speech files are now widely circulated using various means of communication, and sometimes the speech file can be secret, which requires protecting it from any unauthorized person to hear and understand it. The methods which use DES standard for data encryption-decryption are considered ineffective because they need a long time to implement the protection of speech files due to their large size and containing double data with fractions.
In this paper research a method which uses WPT decomposition will be proposed, tested and implemented. It will be shown how the new introduced method will increase the cryptography process efficiency by minimizing the encryption-decryption times keeping at the same time excellent values for quality parameters.
Keywords: Speech, DES, WPT, throughput, cryptography, image-key, PSNR, MSE.

Introduction
Speech files [13-19] are important data for use in many vital applications. The speech file may contain important and confidential data or be of a personal nature, which requires protection from intruders and unauthorized parties so that they cannot understand the file when they hear it [39].
The process of protecting [16], [23],[24] the speech file is carried out through the implementation of the encryption and decryption process (data cryptography)[33], and this process is implemented, as shown in the figure 1, by implementing some specific operations on the data to be protected using a special secret key called the private key (PK) [26], [27].

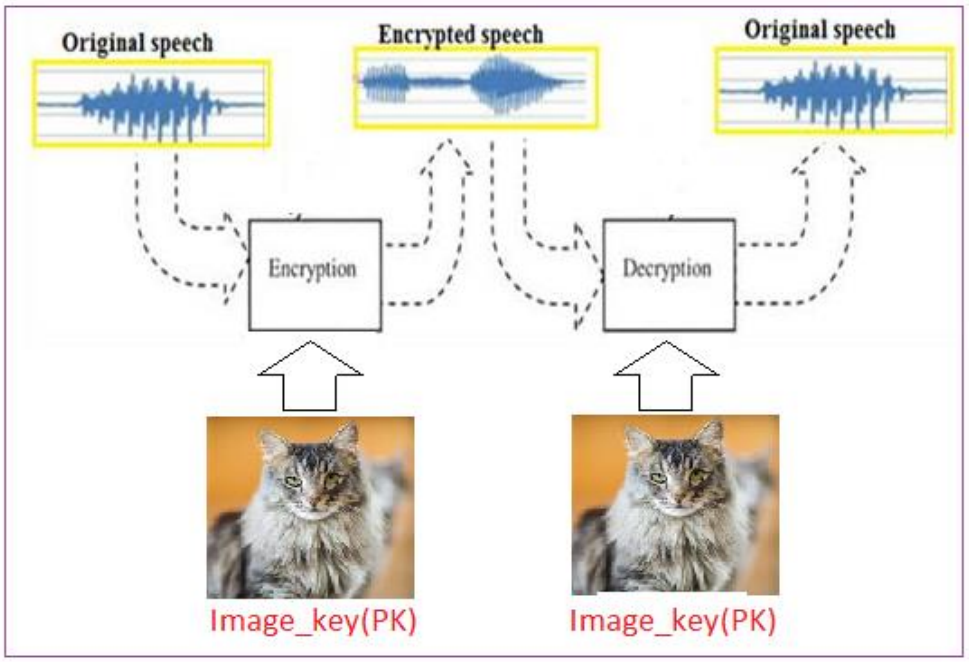

Figure 1: Data cryptography

Any method adopted to protect confidential data must achieve the following important things:

- ✓ Ease of implementation.
- ✓ The private key is difficult to hack and cannot be known or guessed.
- ✓ The method works to completely destroy the data when encrypting, so that it becomes completely incomprehensible after encryption, and that the confidential data is returned completely and uncompromised, and that the recovered data is completely identical to the original data in the process of decryption.
- ✓ The method should be effective so as to reduce the encryption time and decryption time as much as possible.

The method of data cryptography quality [38], [42] can be measured by mean square error (MSE) [31], [32] and/or peak spinal to noise ratio (PSNR) [20], [28], these parameters can be calculated by formulas 1 and 2:
The values of these parameters must be as shown in table 1

MSE between messages S and R, n: message length

$$MSE_{SR} = \frac{1}{N}\sum_{j=0}^{n-1}[S(j) - R(j)]^2 , N = n \quad (1)$$

$$PSNR_{SR} = 10 * \log_{10}\frac{(MAX_i)^2}{MSE_{SR}} \quad (2)$$

Table 1: Cryptography quality parameters

Data	Original		Encrypted		Decrypted	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
Original	-	-	Very high	Very low	Vary low (closed to zero)	Very high (closed to infinite)
Encrypted	Very high	Very low	-	-	Very high	Very low
Decrypted	Vary low (closed to zero)	Very high (closed to infinite)	Very high	Very low	-	-

The use and circulation of digital color [1-6] images has spread so that it is possible to obtain them without any cost. The digital image, as shown in the figure 2, is represented by a three-dimensional matrix (three two-dimensional matrices, one for each color), and this matrix has a huge amount of data that can be employed for multiple purposes, including using it as a private key [7-12].

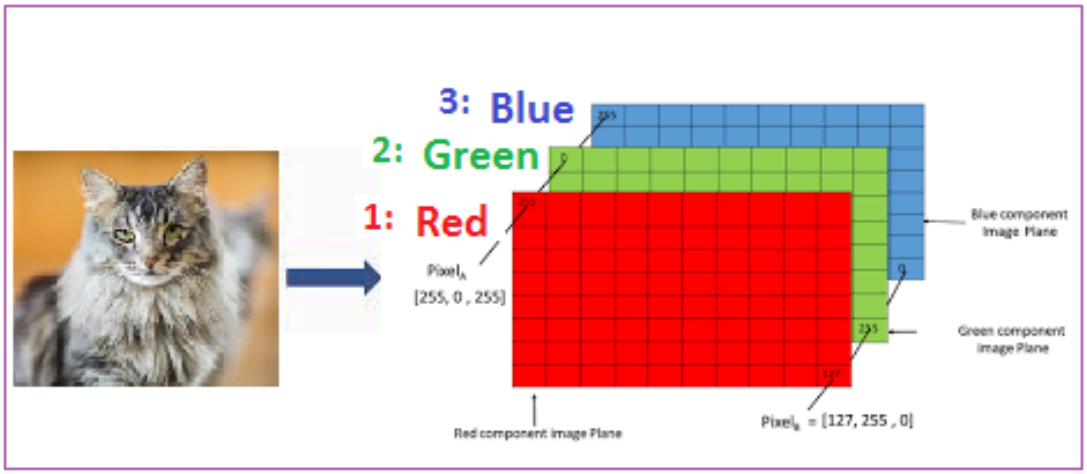

Figure 2: Color image matrix

Dealing with the color image matrix[10-12] is easy as you can easily re-form it by converting it into a one-dimensional matrix using reshaping operation (see figure 3) or changing its size, whether by reducing it or increasing it to suit the size of the speech file applying resizing operation[5-10].

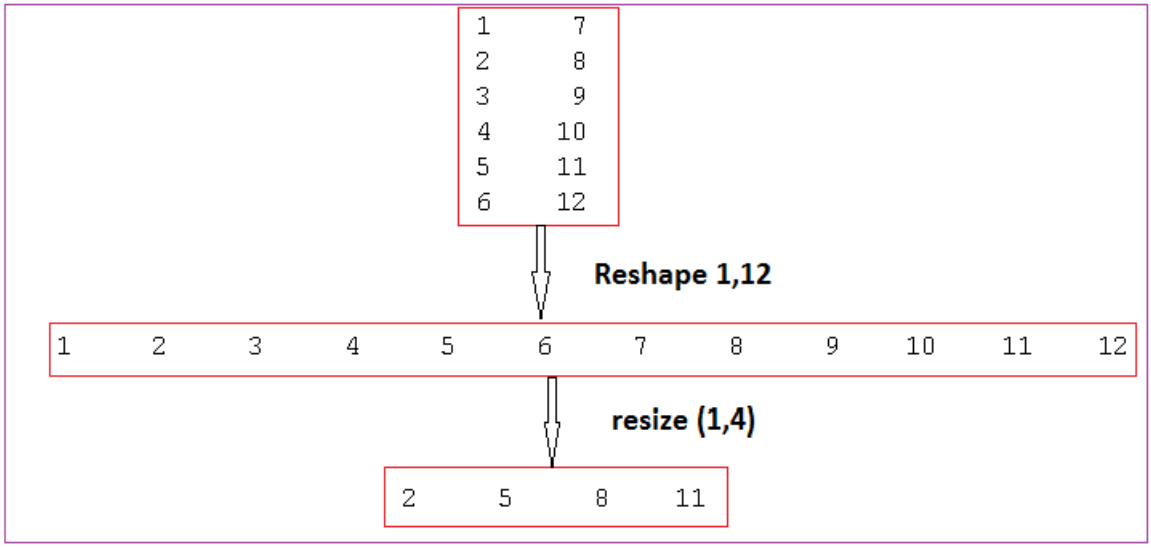

Figure 3: Reshaping and resizing operations

It is easy to convert RGB color image to YIQ image. YIQ image contains values within the range 0 to 1, these values can be easily used with the speech signal, the YIQ can be also resized to match the digital speech signal size, figure 4 illustrates an example of image converting and resizing

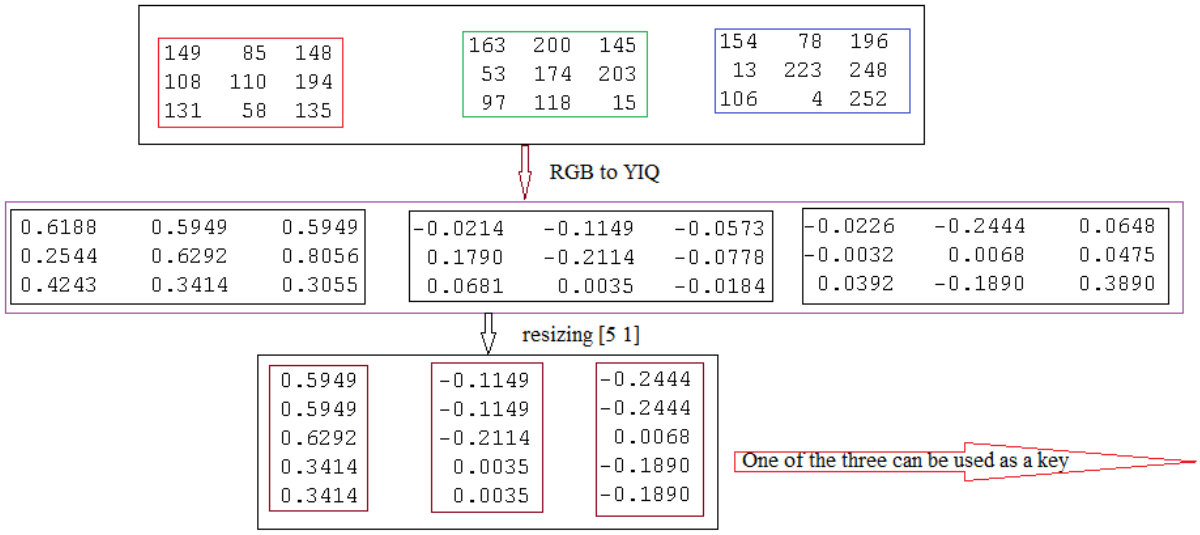

Figure 4: Converting and resizing RGB color image

Selected image_key can easily be used in whole or in part and can be easily decamped using wavelet packet tree (WPT) [9], [22] into approximations and details based on Haar equation, shown below in figure 5:

Haar scaling (low pass) function:

$$s_{j+1,i} = \frac{even_{j,i} + odd_{j,i}}{\sqrt{2}}$$ Approximation

Haar wavelet (high pass) function:

$$d_{j+1,i} = \frac{even_{j,i} - odd_{j,i}}{\sqrt{2}}$$ details

Figure 5: Haar decomposition

The image can decomposed[37], [40], [41] by reshaping it to one row matrix, then applying Haar equations we can easily get the approximation and detail, and the length of each of them will equal the root size divided by two. These approximation and detail can be used later to build the encrypted speech signal, figure 5 illustrates how to calculate the approximation and detail of an input data set.

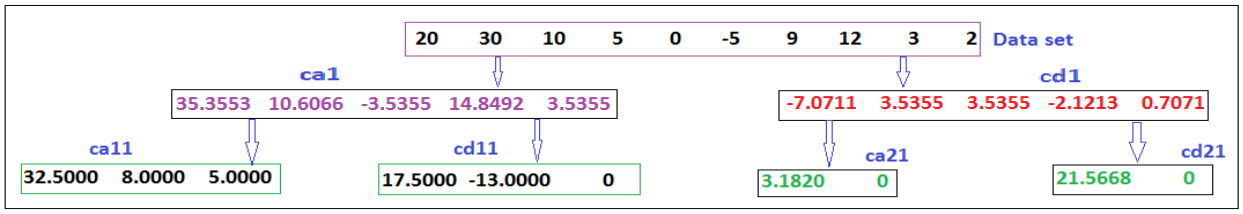

Figure 6: Approximation and detail calculation example

Related works

Various methods are used to encrypt and decrypt digital data, including speech files, and many of these methods depend on international standards DES [30], [35], [36] (data encryption standard) and AES (advanced encryption standard), all of these methods are suffering from the following disadvantages[25], [29]:

- ☒ These methods deal with valid decimal numeric data representing text messages or secret text files, and it is difficult to use them to protect data that contains fractional values such as speech files represented by a set of samples with double fractional values.
- ☒ These methods depend on dividing confidential data into blocks of fixed length (8 or 16 bytes) and they cannot deal with the data by encrypting it all at once, which requires additional time to divide the data into blocks and reassemble it again.
- ☒ These methods use a fixed-length private key (at most 256 bits) to perform the encryption and decryption process. In some cases, this key can be hacked, which in turn means that the data is not secure.
- ☒ These methods use fixed arithmetic and logical operations that are easy to know and follow.
- ☒ The private key must be processed and rescheduled to generate the other keys used in the different stages, which requires additional time.
- ☒ The encryption and decryption process is carried out in rounds with a specified number (14 or 16), and each round requires its own generated from PK keys.

The speech file is a set of samples (with double fractional values) representing the amplitudes, these samples are organized in one column array (mono speech), or two column matrix (stereo speech)(see figure 7), to use the

methods based on the known standard will require a big effort and time to encrypt_decrypt speech signal, so we have to seek another way which will satisfy the requirement of good encryption_decryption method.

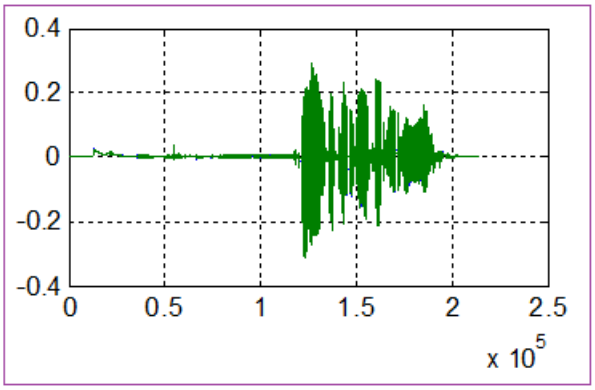

Figure 7: Speech signal wave

The proposed method

The speech file can be encrypted as shown in figure 8 applying the following steps:

Step 1: Select the image_key.
Step 2: Convert the image to YIQ image.
Step 3: Resize YIQ image to double size speech file size.
Step 4: Apply wavelet packet tree decomposition to get approximation and detail.
Step 5: Get the encrypted speech by adding speech file, approximation and constant, and subtracting the detail from the result of summation.

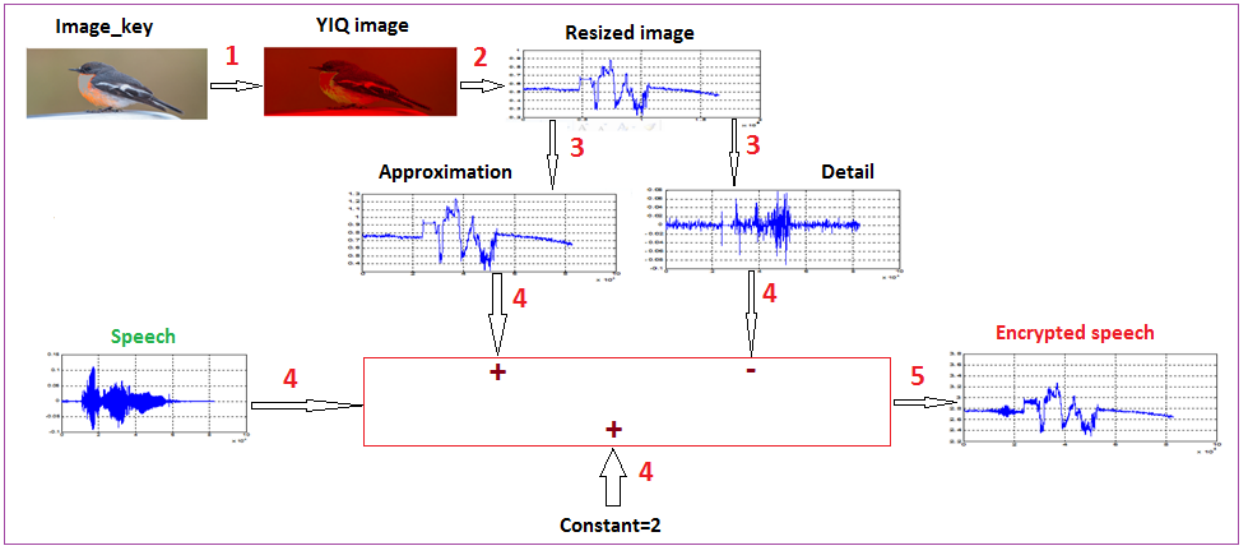

Figure 8: Proposed encryption phase

The decryption phase as shown in figure 9 can be implemented applying the following steps:

Step 1: Select the image_key.
Step 2: Convert the image to YIQ image.

Step 3: Resize YIQ image to double size speech file size.
Step 4: Apply wavelet packet tree decomposition to get approximation and detail.
Step 5: Get the decrypted speech by adding encrypted speech file, detail and subtracting constant, and approximation from the result of summation.

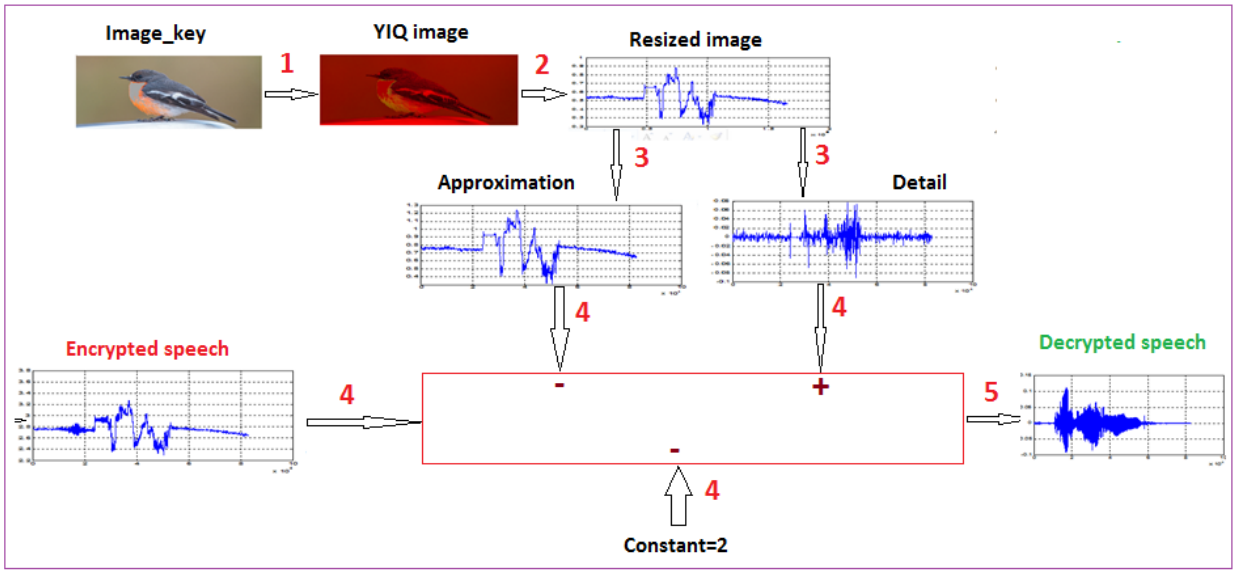

Figure 9: Proposed decryption phase

Implementation and experimental results
12 speech files were selected and encrypted-decrypted using DES, table 2 shows the obtained experimental results:

Table 2: Obtained results using DES method

Speech signal	Size(samples)	PSNR(original and encrypted)	PSNR(original and decrypted)	Encryption time(seconds)	Decryption time(seconds)
1	321536	5.7842	Infinite	78.0480	77.2400
2	200704	5.7708	Infinite	46.7060	47.8480
3	227328	5.7867	Infinite	53.4560	53.1560
4	430080	5.7885	Infinite	107.5440	107.8880
5	172032	5.7536	Infinite	40.0840	39.9020
6	133120	6.3252	Infinite	30.8140	30.3300
7	212992	4.7012	Infinite	49.8000	50.5940
8	272384	6.3332	Infinite	65.5740	65.5960
9	82880	6.3252	Infinite	19.4410	19.2120

10	64448	6.3284	Infinite	14.750000	14.980000
11	122816	8.6305	Infinite	29.104000	29.600000
12	138176	9.8083	Infinite	33.224000	33.167000
Average	198208	6.4447	Infinite	47.3788	47.4594
Throughput				4183.5	4176.4

From the obtained DES results we can see the following:

- DES satisfies the quality requirements by giving good values for PSNR in both phase's encryption and decryption.
- The DES is not efficient, it needs big times for encryption and decryption, and thus will decrease DES throughput (number of processed samples per second).

The 12 speech files encrypted-decrypted using the proposed method and using image12, table 3 shows the encryption-decryption times and the method throughput.

Table 3: Proposed method throughput calculation

Speech	Size(samples)	Encryption time(seconds)	Decryption time(seconds)	Throughput(samples per second)
1	321536	0.100000	0.100000	3215400
2	200704	0.060100	0.060100	3339500
3	227328	0.069000	0.069000	3294600
4	430080	0.237000	0.237000	1814700
5	172032	0.057100	0.057100	3012800
6	133120	0.052200	0.052200	2550200
7	212992	0.065100	0.065100	3271800
8	272384	0.071000	0.071000	3836400
9	82880	0.042500	0.042500	1950100
10	64448	0.040000	0.040000	1611200
11	122816	0.051900	0.051900	2366400
12	138176	0.053200	0.053200	2597300
Average	198208	0.0749	0.0749	2.7384 Mega samples

From table 3 we can see that the proposed method is efficient providing small times for encryption and decryption and big values for the method throughput, this is shown in figure 10, the average throughput reached 2.7 mega samples per second, which an excellent value is comparing with other methods of data cryptography based on DES and AES standards.

From table 3 we can see also that the proposed method has a big advantage comparing with DES method, the method throughput rapidly increased.

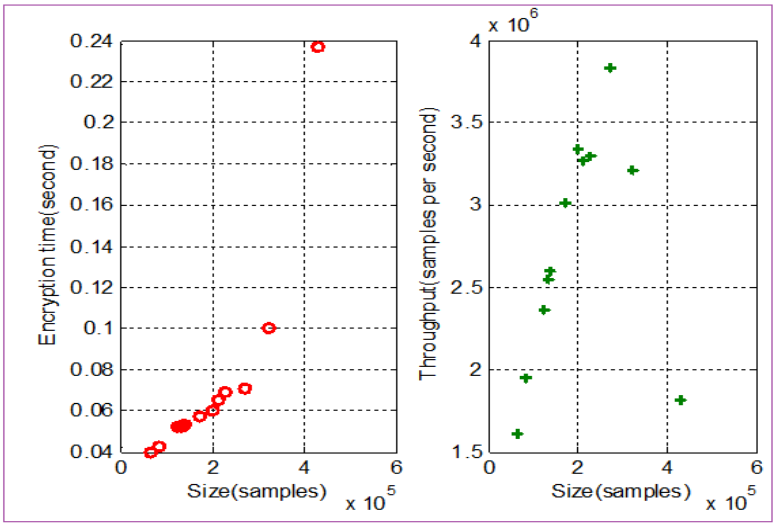

Figure 10: Measured encryption time and throughput

The proposed method provides good values for the quality parameters MSE and PSNR in phases, encryption and decryption, this is shown in table 4, and these values satisfy the requirements for quality parameters shown in table 1.

Table 4: Cryptography quality parameters

Speech	Between original and encrypted speeches		Between original and decrypted speeches	
	MSE	PSNR	MSE	PSNR
1	7.6062	3.8215	5.3359e-033	716.7873
2	7.6062	3.8215	5.4182e-033	714.4098
3	7.6062	3.8215	5.4162e-033	714.5477
4	7.6062	3.2977	5.8380e-033	717.2067
5	7.6062	3.6495	6.9084e-033	691.3076
6	7.6062	3.2487	6.5759e-033	685.7518
7	7.6062	3.4599	6.4285e-033	701.4491
8	7.6062	3.2833	6.1700e-033	706.4682

9	7.6062	3.4653	6.0779e-033	698.2704
10	7.6062	3.6508	6.0987e-033	697.2319
11	7.6062	3.3413	6.1806e-033	692.3204
12	7.6062	3.4400	5.8718e-033	692.2718

Speech 4 file was encrypted-decrypted using various image_keys, table 5 shows the obtained experimental, these results also prove that the proposed method satisfies the requirements of good encryption-decryption.

Table 5: Encrypting decrypting Speech 4

Image	Size(byte)	Between original and encrypted speeches		Between original and decrypted speeches	
		MSE	PSNR	MSE	PSNR
1	150849	6.0142	6.3380	1.0221e-032	711.6059
2	77976	10.8243	1.9401	1.1303e-032	710.5994
3	518400	6.9579	6.1435	1.0541e-032	711.2974
4	5140800	7.1457	4.8572	8.0158e-033	714.0364
5	4326210	6.2610	6.1242	8.2129e-033	713.7934
6	122265	7.4343	3.5301	6.1480e-033	716.6893
7	518400	6.9480	5.4713	8.5412e-033	713.4016
8	150975	6.0371	6.4034	8.5289e-033	713.4160
9	150975	6.9998	3.2833	5.4378e-033	717.9169
10	151353	7.2186	3.3921	7.5361e-033	714.6535
11	1890000	8.1103	4.8075	9.4546e-033	712.3855
12	6119256	7.6062	3.2977	5.8380e-033	717.2067

From table 5 we can see that using various image keys to encrypt/decrypt the speech signal does not affect the values of the quality parameters and the obtained decrypted signal remain with high quality and very closed to the original speech signal.

Conclusion

DES based method of speech signal cryptography was implemented, the obtained results showed that this method is very accurate by providing good value for quality parameters (PSNR, MSE), however, it suffers from a defect, which is its ineffectiveness by providing big times for encryption-decryption minimizing the method throughput. And to solve the defects of DES method, an alternative method was proposed, this method is based on WPT decomposition, it was tested and implemented, and the obtained results showed how this method increases the throughput by decreasing the encryption-decryption times keeping the values of quality parameters acceptable.

Acknowledgement

This work was supported by the Research Groups Program Funded by Deanship of Scientific Research, Taif University, Ministry of Education. Saudi Arabia, under Grant (TURSP-2020/345)

References

[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 be used to Convert a Gray Image to Color Image, International Journal of Computer Applications, vol. 153, issue 2, pp. 31-34, 2016.

[3]. Qazem Jaber Ziad Alqadi, Jamil azza, Statistical analysis of methods used to enhance color image histogram, XX International scientific and technical conference, 2017.

[4]. Bassam Subaih Ziad Alqadi, Hamdan Mazen, A Methodology to Analyze Objects in Digital Image using Matlab, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, pp. 21-28, 2016.

[5]. Mazen A.Hamdan Bassam M.Subaih, Prof. Ziad A. Alqadi, Extracting Isolated Words from an Image of Text, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, pp. 29-36, 2016.

[6]. Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 21 –37, 2020.

[7]. Aws AlQaisi, Mokhled AlTarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, pp. 1220-1225, 2019.

[8]. Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.

[9]. 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, 2020.

[10]. Ziad AlQadi, M Elsayyed Hussein, Window Averaging Method to Create a Feature Victor for RGB Color Image, International Journal of Computer Science and Mobile Computing, vol. 6, issue 2, pp. 60-66, 2017.

[11]. Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, pp. 2203-2207, 2019.

[12]. Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.

[13]. Yousf Eltous Ziad A. Al Qadi, Ghazi M. Qaryouti, Mohammad Abuzalata, ANALYSIS OF DIGITAL SIGNAL FEATURES EXTRACTION BASED ON KMEANS CLUSTERING, International Journal of Engineering Technology Research & Management, vol. 4, issue 1, pp. 66-75, 2020.

[14]. 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.

[15]. 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, 2019.

[16]. Ziad Alqadi, 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 8, pp. 30-48, 2019.

[17]. 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.

[18]. 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. 2780-2787, 2018.

[19]. Jihad Nader Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.

[20]. 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.

[21]. Ziad Alqadi, Ahmad Sharadqh, Naseem Asad, Ismail Shayeb, Jamil Al-Azzeh, Belal Ayyoub, 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.

[22]. Musbah Aqel Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences, vol. 6, issue 1, pp. 45-52, 2009.

[23]. 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.

[24]. 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.

[25]. Belal Zahran Rashad J Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, B Zahran, 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, 2019.

[26]. 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.

[27]. 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.

[28]. Ziad A AlQadi, Accurate Method for RGB Image Encryption, International Journal of Computer Science and Mobile Computing, vol. 9, issue 1, pp. 12-21,2020.

[29]. Ziad Alqadi, 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.

[30]. Jamil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, JOIV: International Journal on Informatics Visualization, vol. 3, issue 3, pp. 262-265, 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]. 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.

[33]. 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, issue 5, pp. 125-131, 2016.

[34]. PROF. ZIAD A. ALQADI, A SIMPLE METHOD TO ENCRYPT-DECRYPT SPEECH SIGNAL, International Journal of Engineering Technology Research & Management, vol. 5, issue 2, pp. 44-52, 2021.

[35]. Ziad ALQadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2. Issue 4, pp. 288-298, 2007.

[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 Aqel, Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences Journal, vol. 6, issue 1, pp. 45-52, 2009.

[38]. 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.
[39]. 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, 2019.
[40]. Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, pp. 2203-2207, 2019.
[41]. Akram A Moustafa, 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, vol. 5, issue 5, pp. 355-362, 2009.
[42]. Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, International Journal of Computer Science and Mobile Computing, vol. 8, issue 6, pp. 106-123, 2019.

Dr. Hatim Zaini, Associate Professor, Computer Engineering, Taif University, KSA.
Interests: Image Processing, Algorithms, Combinational Optimization, Computer Applications and Programming.

Prof. Ziad Alqadi:
Professor in Computer Engineering, Head of Computer Engineering, Department, Faculty of Engineering Technology, Albalqa Applied University. Jordan, Amman.
Interests: Image and Signal Processing, Parallel Processing, Computer Applications.

