World Journal of Engineering Research and Technology
WJERT
www.wjert.org
Impact Factor Value: 5.924

SIMPLE AND EFFICIENT BASED ON SECRET POLYNOMIAL METHOD OF SPEECH CRYPTOGRAPHY

[1]*Dr. Hatim Zaini and [2]Prof. Ziad A. Alqadi

[1]Taif University, KSA.

[2]Albalqa Applied University, Jordan.

Article Received on 01/09/2021 **Article Revised on 21/09/2021** **Article Accepted on 12/10/2021**

***Corresponding Author**
Dr. Hatim Zaini
Taif University, KSA.

ABSTRACT

Protecting the audio file, which may be confidential from intruders, is a very important process. In this paper research a new method of speech cryptography will be introduced, it will be shown how this method is simple and efficient. The proposed method will be implemented to prove that this method is good to be used in data cryptography by giving good values for MSE and PSNR during the encryption and decryption phases. The obtained results of the proposed method will be compared with DES results to show how efficient is the proposed method and how it minimizes the encryption and decryption times. The proposed method will use two private keys: image_ key and secret polynomial to increase the level of security and protection of the speech signal.

KEYWORDS: Cryptography, PK, polynomial, speech, RGB, YIQ, PSNR, speedup, throughput**.**

INTRODUCTION

Color digital images[1-6] and digital speech files[13-15] are among the most widely used types of data due to their use in many important vital applications and the reason for their use is due to the ease of dealing with them. One of the reasons for the ease of dealing with digital images and digital speeches is that these types of data are represented by a matrix.[7-12] The colored digital image[20],[22] is represented by a three-dimensional matrix with one dimension for each color (red, green and blue) and the 2D matrix for each color includes a set of values indicating the value equivalent to the color of the point[37],[38], and the values are confined

between zero and 255. As for the digital speech file, it is represented by a matrix of one column (mono speech) or two columns (stereo speech), and this matrix contains a set of values that represent the amplitude at different time moments, whose values usually range between -1 and +1.[17-19]

Color digital images are processed[39-42] in different easy ways, and one of the most important operations carried out on the image is the process of converting the colored digital image to another type by changing the pixel values so that their range is from 0 to 1 to be similar to the values of the digital speech file, where can easily convert RGB image to NTSC image applying equation (1)

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1)$$

Figures 1and 2 show an example of RGB_color image and the equivalent ntsc image:

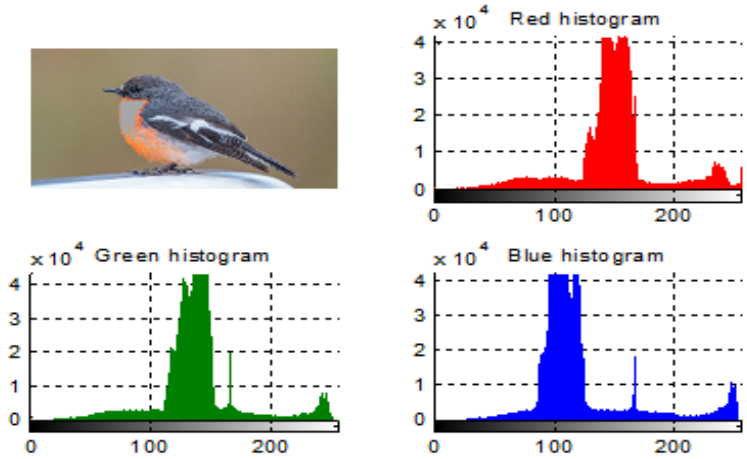

Figure 1: RGB color image example.

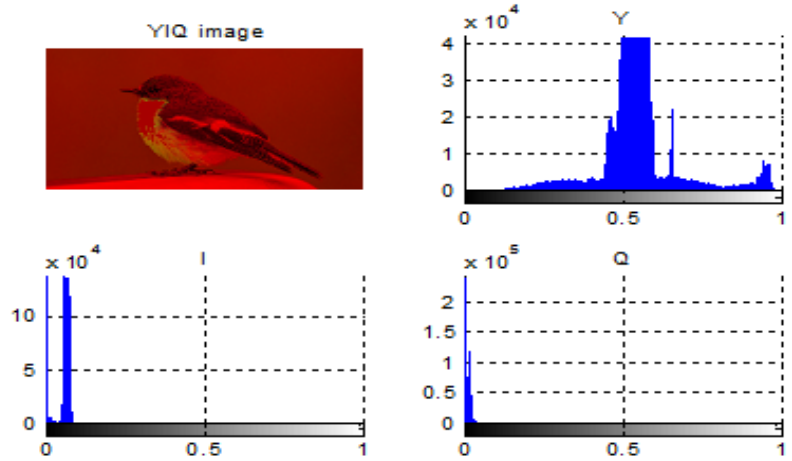

Figure 2: Equivalent YIQ image.

Another easy way to process color digital images is to reconfigure the image size so that the new size fits with the size of the audio file, and accordingly, the single color matrix can be converted into a one-column or two-column matrix with the size of the speech file, as shown in the figure 3.

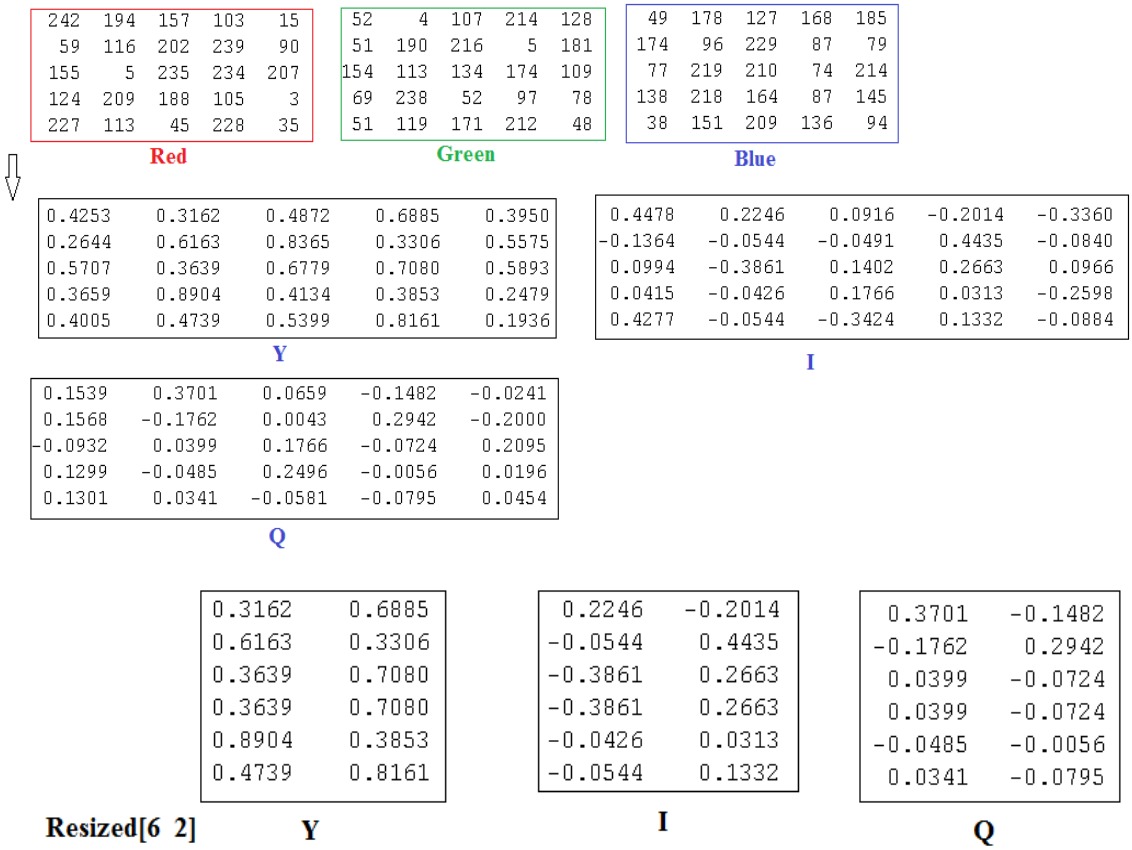

Figure 3: Image resizing.

The digital speech file[20] may be secret or contain confidential information, which requires protecting this file from theft or from the attempt of abusers to understand the file. One of the methods used to protect speech file is cryptography[16], which means encryption and decryption.[23-27]

Encryption and decryption can be done as shown in figure 4, decryption means full destruction of the original speech to be un-understood by any third party not allowed to hear the speech, while decryption means full recovery of the original speech file.[28-31]

File destruction ratio and file recovery ratio can be measured by the quality parameters MSE (mean square error) and PSNR (peak signal to noise ratio),[38] for destruction MSE must as high as possible and PSNR must be low as possible, while for recovery MSE must be low as

possible (leads to zero) and the PSNR must be high as possible (leads to infinite), the quality parameters can be calculated using equations 1 and 2.[32-36]

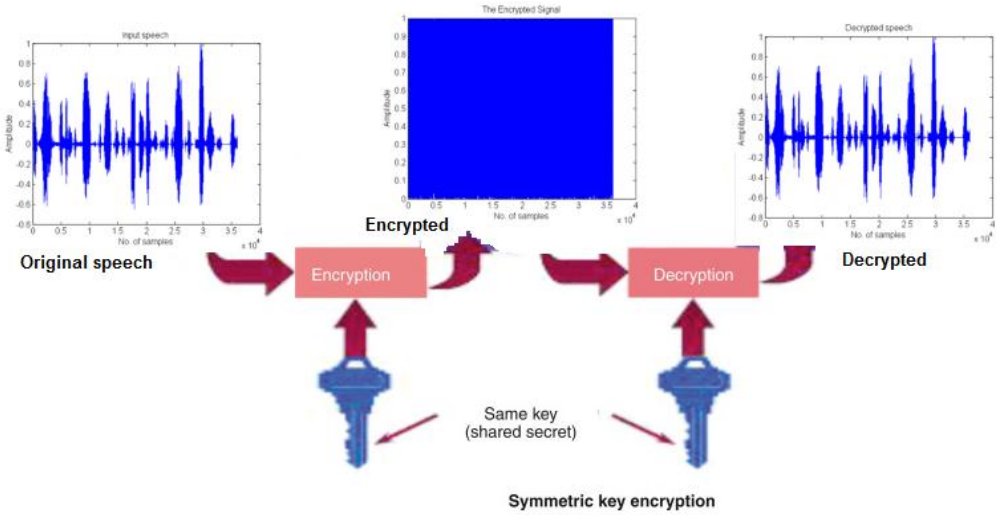

Figure 4: Speech cryptography.

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2 \quad (1)$$

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right) \quad (2)$$

Related works

Many method of data cryptography are based on DES (decryption data standard), these methods have the following characteristics[32-37]:

- They give good values for quality parameters for the both the encryption and decryption phases.
- It is better to use integer data to be encrypted-decrypted.

If the data to be encrypted-decrypted has a big size and/or if the data is double with fraction part then more programming efforts must be done to implement DES based methods and the efficiency will rapidly go down by increasing both encryption and decryption times, thus DES throughput(samples encrypted or decrypted in second) will be not applicable.

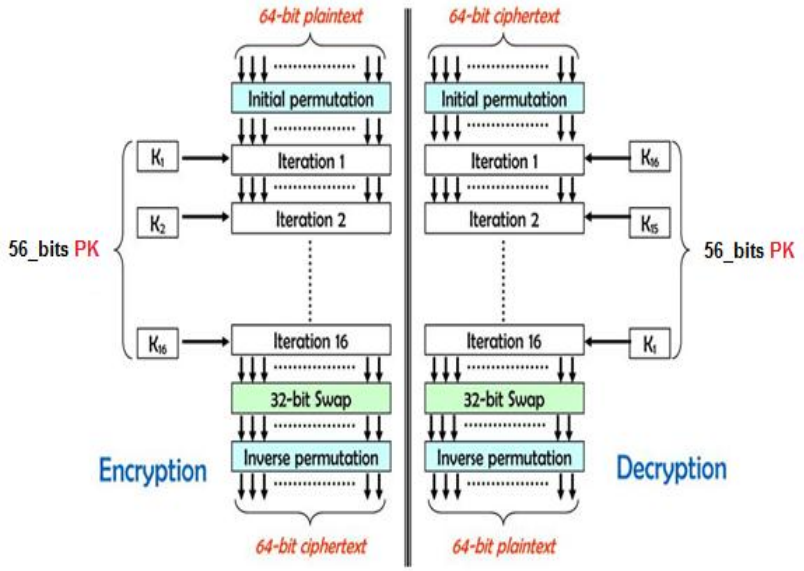

Figure 5: DES cryptography.

DES method uses 56-bits PK for encryption-decryption, this key can be easily hacked making DES method un- secure. The data to be encrypted-decrypted must be divided into blocks with 64_bits length, then applying 16 rounds with arithmetic and logical operation the data can be encrypted-decrypted as shown in figure 5.

To improve the security level and to decrease both the encryption and decryption times, a method using double private key will be introduced, the obtained results of the proposed method will be compared with DES method results to prove the efficiency improvements of the process of speech signal cryptography.

The proposed method

The proposed method uses 2 PK to perform encryption-decryption, the first one is the image_key which must be kept in secret between the sender and receiver, the second secret PK is a polynomial which is to constructed using equation 3 for encryption and equation 4 for decryption:

$$enc = s + a \cdot Y + b \cdot I - c \cdot Q - d \quad (3)$$

Where: S: Speech signal

Y, I, Q: Image channels

a, b, c, d: Coefficients

$$dec = enc - a \cdot Y - b \cdot I + c \cdot Q + d \quad (4)$$

The encryption phase as shown in figure 6 can be implemented applying the following steps:

Step 1: Get the speech file (V) and retrieve its size.

Step2: Get the image_key.

Step 3: Convert the RGB image to YIQ image.

Step 4: Resize each of Y, I, Q to match the speech file size.

Step 5: Apply equation 3 to get the encrypted speech.

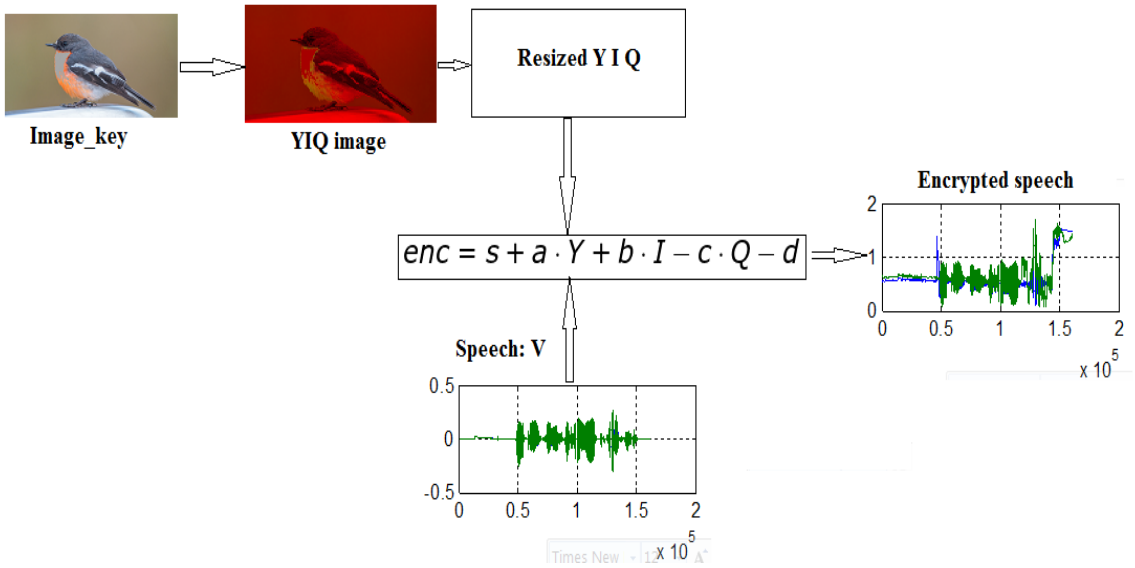

Figure 6: Proposed method encryption.

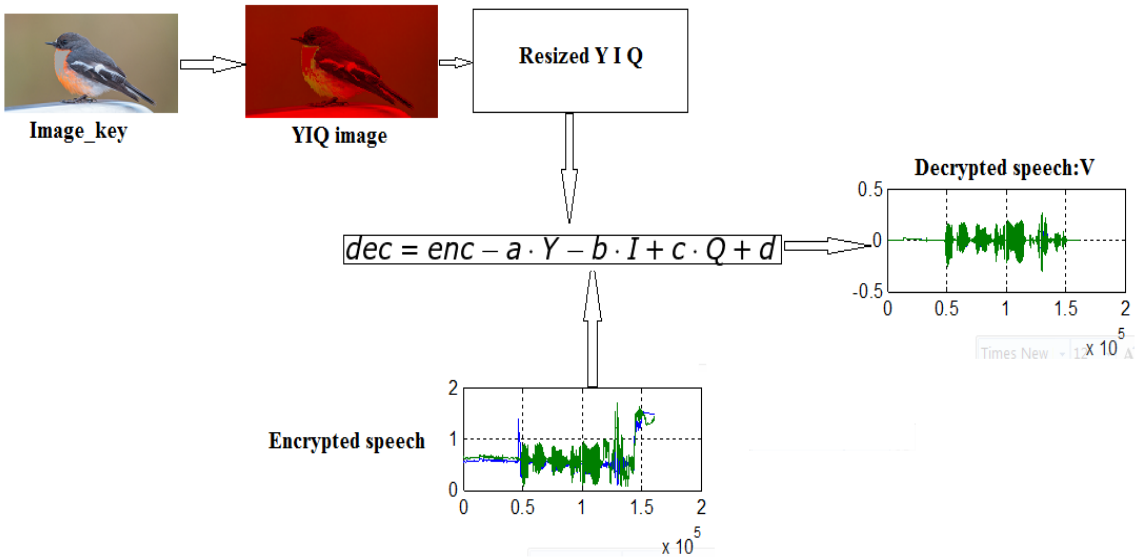

Figure 7: Proposed method decryption.

The decryption phase as shown in figure 7 can be implemented applying the following steps

Step 1: Get the encrypted speech file and retrieve its size.

Step2: Get the image_key.

Step 3: Convert the RGB image to YIQ image.

Step 4: Resize each of Y, I, Q to match the speech file size.

Step 5: Apply equation 4 to get the encrypted speech.

Implementation and experimental results

Image shown in figure 6 was used as an image_key, the following polynomial coefficients shown in tables 1 and 2 were selected to form the PK keys were.

Table 1: Encryption phase coefficients.

a	b	c	d
1.5	-3	1.6	2

Table 1: Decryption phase coefficients.

a	b	c	d
-1.5	3	-1.6	-2

12 speech files were selected, encryption-decryption phases were applied for each speech signal, and figure 8 shows example outputs of the implementation, while table 3 shows the obtained efficiency and quality parameters.

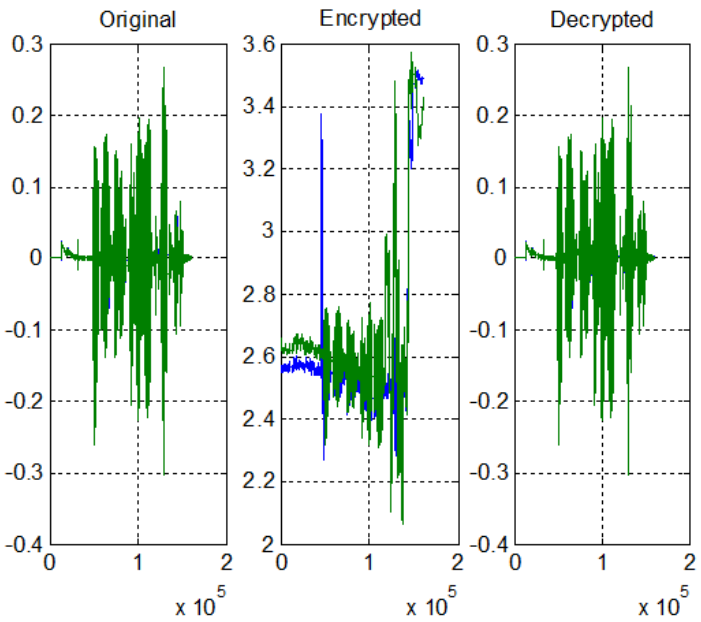

Figure 8: Implementation sample outputs.

Table 3: Obtained proposed method parameters.

Speech signal number	Size(samples)	Proposed efficiency parameters		Proposal quality parameters	
		Encryption time(second)	Decryption time(second)	PSNR(original and encrypted)	PSNR(original and decrypted)
1	272384	0.229000	0.229000	15.9971	714.0556
2	82880	0.213000	0.213000	10.8568	705.5578
3	64448	0.205000	0.205000	10.8387	704.6238
4	122816	0.244000	0.244000	11.4518	700.0822
5	138176	0.220000	0.220000	10.8740	699.5117
6	321536	0.225000	0.225000	17.5687	722.9408
7	200704	0.217000	0.217000	15.3160	720.5595
8	227328	0.216000	0.216000	15.3068	720.9661
9	430080	0.228000	0.228000	15.8144	724.1770
10	172032	0.224000	0.224000	15.3519	699.8647
11	133120	0.234000	0.234000	15.3161	693.8341
12	212992	0.235000	0.235000	15.4835	709.3856
Average	198208	0.2242	0.2242		
Throughput(samples per second)		884070	884070		

From the table 3 we can prove the following facts

- The proposed method gave excellent values For PSNR parameter in the encryption phase (very low values) and in the decryption phase (very high values), which means that the speech file was fully destructed in the encryption phase and fully recovered in the decryption phase.
- The proposed method is very efficient by providing a small times for encryption-decryption, thus the proposed method has a high cryptography throughput.
- Minimum implementation effort, it was very easy to program and implement the proposed method.

The same speech file were encrypted-decrypted using DES method, table 4 shows the obtained experimental results, and here from this table we can see the following:

- DES gave excellent values for PSNR during the encryption and decryption phases.
- The average encryption and decryption times are very low comparing with the proposed method times.
- Extra efforts are required to program DES method, because of the huge size of input data and the input data is a double fractional data type.

Table 4: DES method results.

Speech signal number	Size(samples)	DES efficiency parameters		DES quality parameters	
		Encryption time(second)	Decryption time(second)	PSNR(original and encrypted)	PSNR(original and decrypted)
1	272384	65.5740	65.5960	6.3332	Infinite
2	82880	19.4410	19.2120	6.3252	Infinite
3	64448	14.750000	14.980000	6.3284	Infinite
4	122816	29.104000	29.600000	8.6305	Infinite
5	138176	78.0480	77.2400	9.8083	Infinite
6	321536	46.7060	47.8480	8.6305	Infinite
7	200704	53.4560	53.1560	5.7842	Infinite
8	227328	107.5440	107.8880	5.7708	Infinite
9	430080	40.0840	39.9020	5.7867	Infinite
10	172032	30.8140	30.3300	5.7885	Infinite
11	133120	49.8000	50.5940	5.7536	Infinite
12	212992	78.0480	77.2400	6.3252	Infinite
Average	198208	51.1141	51.1322		
Throughput(samples per second)		3877.8	3876.4		

And by making the necessary comparison between the practical results that were obtained, we can say that the proposed method provides a tangible improvement in the efficiency of the encryption and decryption process by reducing both the encryption and decryption time, table 5 shows the speedup of the proposed method comparing with DES method.

Table 5: Speedup calculation.

Speedup1=time2/time1		
Method	**DES**	**Proposed**
DES	1	0.0044
Proposed	227.9824	1

CONCLUSION

A simple and efficient method of speech signal cryptography was proposed and implemented. The obtained experimental results showed that the proposed method is very accurate in destroying the original speech file in the encryption process and fully recovering the original speech file in the decryption phase giving excellent values for PSNR in the two phases. The proposed method is highly secure by using two private keys which are very difficult to hack. The proposed method is highly efficient and it has a significant high speedup comparing with DES method of data cryptography.

ACKNOWLEDGMENT

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).

FUNDING STATEMENT

This work was supported by the Taif University Researchers Supporting Project Number (TURSP-2020/345), Taif University, Taif, Saudi Arabia.

REFERENCES

1. Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, 2010; 8(10): 1175-1182.
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, 2016; 153(2): 31-34.
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, 2016; 5(11): 21-28.
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, 2016; 5(11): 29-36.
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, 2020; 9(2): 21–37.
7. Aws AlQaisi, Mokhled AlTarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, 2019; 17(3): 1220-1225.
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, 2019; 8(8): 50-56.
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, 2020; 9(2): 2319.

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, 2017; 6(2): 60-66.
11. Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, 2019; 14(1): 2203-2207.
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, 2019; 8(8): 50-56.
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, 2020; 4(1): 66-75.
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, 2020; 4(2): 48-55.
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), 2019; 9(5): 4092-4098.
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, 2019; 8(8): 30-48.
17. Ayman Al-Rawashdeh, Ziad Al-Qadi, Using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, 2018; 8(4): 1356-1359.
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, 2018; 8(5): 2780-2787.
19. Jihad Nader Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, 2019; 1(4): 49-55.
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, 2019; 8(3): 76-90.

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, 2019; 5(3): 82-87.
22. Musbah Aqel Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences, 2009; 6(1): 45-52.
23. Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, 2016; 5(5): 465-470.
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, 2018; 7(3): 104-107.
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, 2019; 8(6): 3228-3235.
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, 2019; 9(3): 4165-4168.
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, 2019; 11(1): 232-238.
28. Ziad A AlQadi, Accurate Method for RGB Image Encryption, International Journal of Computer Science and Mobile Computing, 2020; 9(1): 12-21.
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, 2019; 8(9): 30-48.
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, 2019; 3(3): 262-265.
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), 2020; 6(5): 6-12.
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, 2019; 9(1): 3681-3684.

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), 2016; 8(5): 125-131.
34. PROF. ZIAD A. ALQADI, A SIMPLE METHOD TO ENCRYPT-DECRYPT SPEECH SIGNAL, International Journal of Engineering Technology Research & Management, 2021; 5(2): 44-52.
35. Ziad ALQadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, 2007; 2(4): 288-298.
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, 2019; 8(3): 14-26.
37. Musbah Aqel, Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences Journal, 2009; 6(1): 45-52.
38. Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, A Novel Technique for Data Steganography, Engineering, Technology & Applied Science Research, 2019; 9(6): 4942-4945.
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), 2019; 9(5): 4092-4098.
40. Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, 2019; 14(1): 2203-2207.
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, 2009; 5(5): 355-362.
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, 2019; 8(6): 106-123.

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: Interest: Image and signal processing, parallel processing, computer applications.