VOL. 18, NO. 13, JULY 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

SPEECH FILES CRYPTOGRAPHY USING IMAGE KEY AND INDICES KEY

Adnan Manasreh[1], Nasser Abdellatif[1] and Ziad A. Alqadi[2]
[1]Department of Electrical Engineering, Applied Science Private University, Amman, Jordan
[2]Department of Computer Engineering, Faculty of Engineering Technology, AL-Balqa Applied University
Amman, Jordan
E-Mail: adnan_m@asu.edu.jo

ABSTRACT

Protecting speech files from being hacked is a vital issue. In this paper's research, a new and simple method of speech files cryptography will be introduced. The method will simplify the encryption and decryption functions by using a simple replacement operation. The method will provide a high level of security based on using two secret private keys: the image_key and the image position, these two keys will be used to generate an indices key, which will be used to apply speech sample replacements in the encryption and decryption phases. The introduced method will be efficiently used to encrypt-decrypt mono and stereo speeches. The method will be very flexible; the changes of the private keys will be an easy process, without the need to make any changes in the method algorithm. The proposed meth will be tested and implemented using various speech files, the obtained results will be used to prove the sensitivity quality, and efficiency of the proposed method.

Keywords: cryptography, speech file, image_key, position, index key, sensitivity, quality, replacement.

Manuscript Received 13 April 2023; Revised 20 August 2023; Published 13 September 2023

1. INTRODUCTION

Verbal communication is closely related to daily life, such as education, commerce, politics, the military, e-learning, telephone banking, and news broadcasting. With the advancement of modern communication and multimedia technologies, a huge amount of sensitive speech data travels in daily routines on open and shared networks. To maintain security, sensitive data must be protected before it is sent or distributed. To protect speech when it is transmitted over any unsecured channel, certain coding techniques are required to convert the clear form of speech into sound before transmission (encoding) [10-20].

The speech signal is a set of double values representing the amplitudes taken in periodic intervals of times, these values are usually within the range -1 to +1, The digital speech values are organized in a column matrix (mono speech) and two column matrix (stereo speech) as shown in Figures 1 and 2 [5-9].

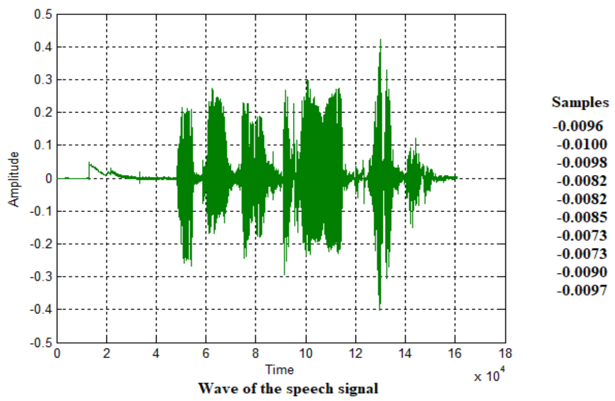

Figure-1. Mono speech signal wave.

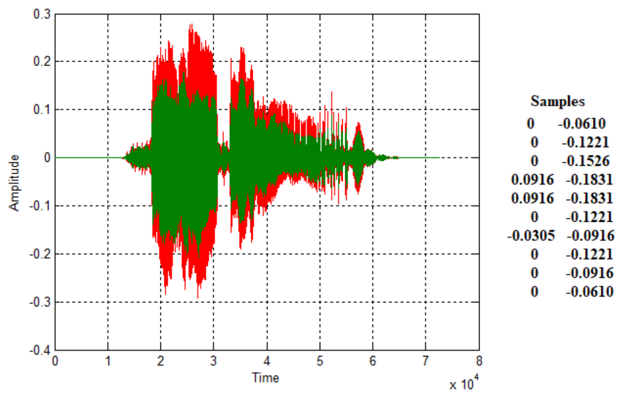

Figure-2. Stereo speech signal wave.

Digital color images can be used as a good source of data to generate a key to be used in data cryptography for the following reasons [21-25]:

- It is very easy to process the image because it is represented as shown in Figure 3 by a 3D matrix (one 2D matrix for each color: red, green, and blue) [26-31].
- The image has a huge size, which can be deployed for any application.
- It is easy to get and store the image because a lot of resources are freely available and it is very easy to generate the image because a lot of equipment is available [32-40].
- It is very easy to get apart from the image to be used to implement a selected application [41-45].

 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.

www.arpnjournals.com

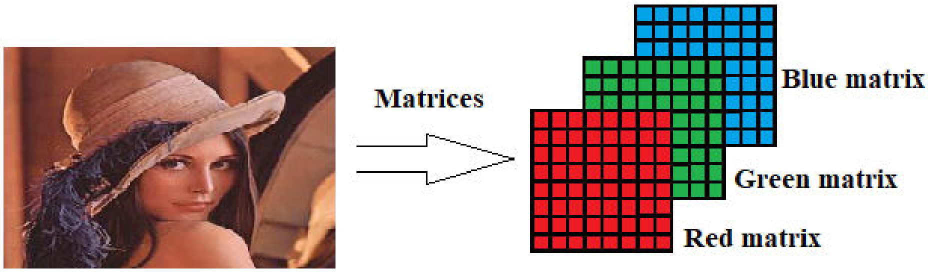

Figure-3. Digital color image matrices.

One of the most popular methods of speech file protection is speech cryptography, which means encrypting the speech file before sending it and converting it into a damaged file, and decrypting the speech file after receiving it by converting the damaged speech file into a speech identical to the source speech. Usually, encryption and decryption processes are implemented using one or more private keys, these keys must be kept secret between the sender and receiver [53-60].

This paper research aims to present a method of speech cryptography, which must provide the following advantages:

- Simplicity, The method will simplify the encryption and decryption function by minimizing the required number of operations and using a simple replacement operation to apply encryption and decryption.
- The method will be used to process any speech file with any size and type, and it will be used to encrypt-decrypt mono and stereo speech files.
- Low quality of the encrypted speech file, the quality parameters (mean square error (MSE), peak signal to noise ratio (PSNR), correlation coefficient (CC) and number of samples change ratio (NSCR)) must satisfy the quality requirements listed in table 1 [46-54].
- High quality of the encrypted speech file, the quality parameters of the decrypted speech file must satisfy the quality requirements listed in Table-1.
- High speed of encryption and decryption, the method will provide a high throughput of encryption and decryption.
- High security level, the method will increase the degree of speech file protection by using two private keys, the color image as an image_key and the starting location in the image where to start getting the required part of the image.

Table-1. Quality requirements of speech cryptography [4-10].

Quality parameters	MSE	PSNR	CC	NVCR(%)
Measured between source and encrypted speeches	High	Low	Low	High
Measured between source and decrypted speeches	0	Infinite	1	0

Many methods [1-4] were produced for data cryptography, most of them were based on standard methods of data cryptography, these methods provided good quality but they have the following disadvantages:

- They are good at processing data with small sizes.
- It is difficult to use them for speech cryptography.
- They use a fixed-length private key.
- The use to divide the data to be encrypted into equal blocks.
- Encryption and decryption processes are implemented in a fixed number of rounds.
- A lot of time is required to generate the required keys.
- Some of these methods are not enough secure.
- The speeds of these methods are very low; Table-2 shows the speed results of some of the standard methods of data cryptography.

Table-2. Standard methods speed.

Speech size(sample)	Encryption time (second)					
	DES	3DES	AES	RC2	RC6	BF
321536	29.54	34.34	28.38	41.41	16.47	4.57

©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.

200704	17.01	19.78	16.34	23.85	9.49	2.63
133120	11.24	13.06	10.79	15.75	6.26	1.74
47315	7.83	9.10	7.52	10.98	4.37	1.21
172030	14.59	16.96	14.02	20.46	8.14	2.26
Average						
174941	16.0420	18.6480	15.4100	22.4900	8.9460	2.4820
Average throughput (K samples per second)	10.6496	9.1613	11.0864	7.5963	19.0969	68.8319

2. PROPOSED METHOD

The proposed method is very secure; it uses two private keys to apply encryption-decryption. The first key is an image_key, which must be kept secret between the sender and receiver, the second private key is a starting position, where to start getting apart from the image.

The two keys are easily used, and they can be replaced at any time without affecting the encryption and decryption algorithms.

The image_key and the starting position are used to get a part from the image_key with a length equal to the speech file length, this part is to be converted to an indices key, which will be used to apply the requirement replacements in the encryption and decryption processes. The conversion of the image part to the indices key is very simple to implement, and we can use the mat lab sort function with the image part. Figure-4 shows an example of encrypting-decrypting 10 samples of a speech file:

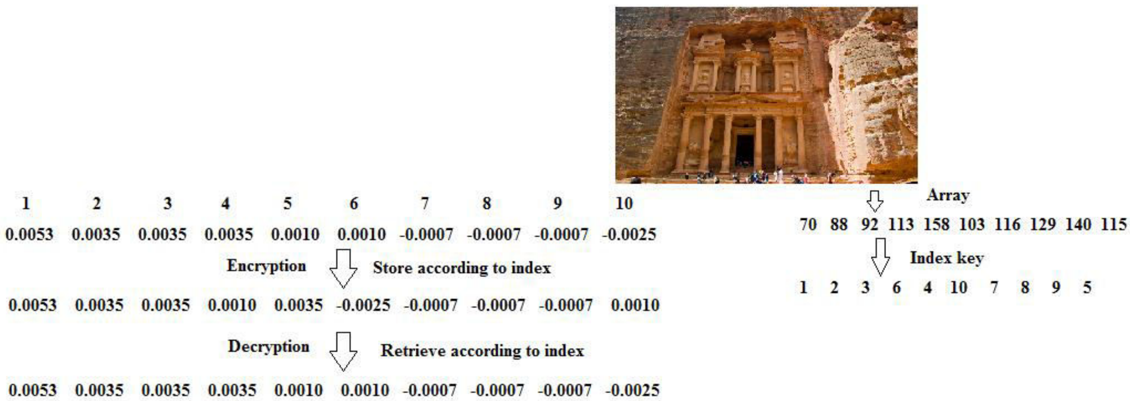

Figure-4. Encryption-decryption example.

The encryption process is implemented by putting the character in a position pointed by the index key, while the decryption is implemented by retrieving the characters according to the indexes in the index key.

Encryption and decryption functions must use the same private keys, changing the image_key or/and the starting position will lead to producing a damaged decrypted speech file and these changes will be considered as a hacking attempt, Figures 5 and 6 show how the index key will change, and how the decrypted speech samples are differing from the source samples when changing the image_key:

VOL. 18, NO. 13, JULY 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

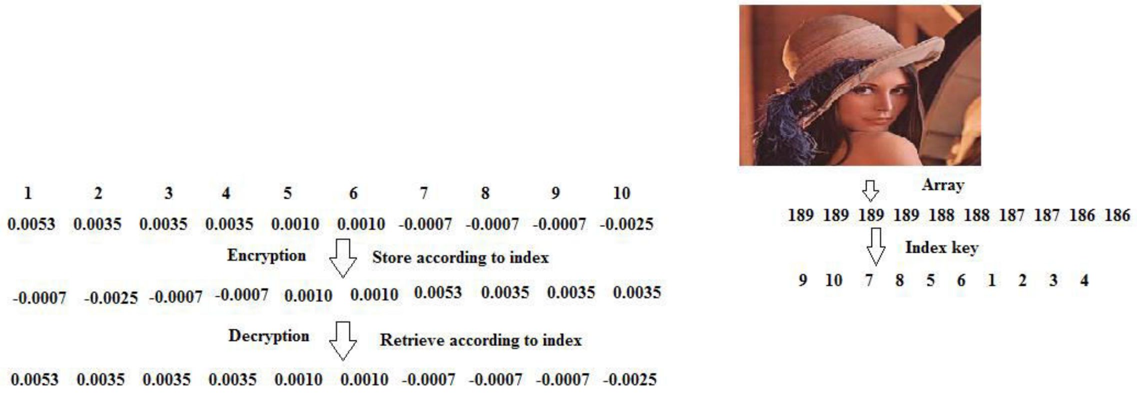

Figure-5. Changing image_key changes the index key.

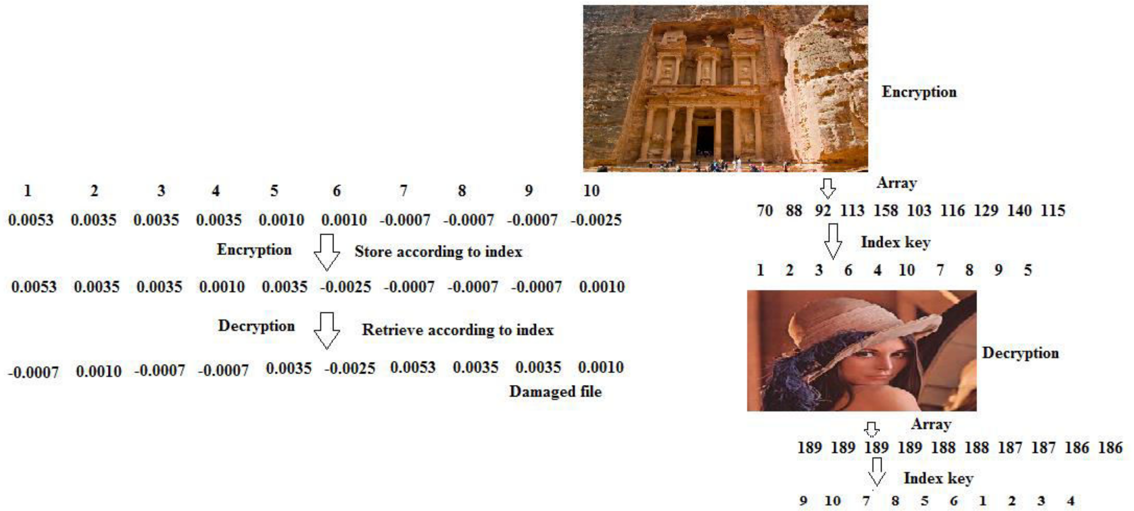

Figure-6. Using another image_key in the decryption produces a damaged speech file.

The encryption phase of the proposed method can be implemented by applying the following steps:

Step 1:

Speech file preparation: get the speech file, retrieve the speech file size, and reshape the speech file into the one-row matrix, this step can be implemented using the following sequence of mat lab operations:

```
[a1 fs]=wavread('C:\Users\Dr.Tayseer\Desktop\voices\a11.wav');
[n1 n2]=size(a1);
a2=reshape(a1,[1,n1*n2]);
s=n1*n2;
```

Step 2:

Key generation: get the image_key, get the position, retrieve the image size, reshape the image into a one-row matrix, calculate the starting location, retrieve a part from the image with a size equal to speech file size, sort the part to get the index key, this step can be implemented using the following sequence of mat lab operations:

```
ikey=imread('C:\Users\Dr.Tayseer\Desktop\drziad\MAVAV\a12.jpg');
[nn1 nn2 nn3]=size(ikey);
ikey1=reshape(ikey,1,nn1*nn2*nn3);
kk=ikey1(1,1:s);
[dd key]=sort(kk);
```

Step 3:

Encryption: for each sample in the speech file, store the sample in the position pointed by the index key, this step can be implemented using the following sequence of mat lab operations:

```
for i=1:s

        ff=key(i);
        a2(i)=a1(ff);

end
```

The decryption process can be implemented using the same steps but step 3 must perform the decryption by retrieving the samples using the indexes in the index key, and applying the following sequence of mat lab operations:

 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.


```
for i=1:s
        ff=find(key==i);
        a4(i)=a2(ff);
end
```

3. IMPLEMENTATION AND RESULTS DISCUSSIONS

Several speech files were selected and processed using the proposed method, and the results showed that the proposed method satisfied the quality requirements, Figure-7 shows sample outputs, and from this figure, it is shown that the encrypted speech was damaged, and the decrypted speech was identical to the source speech file.

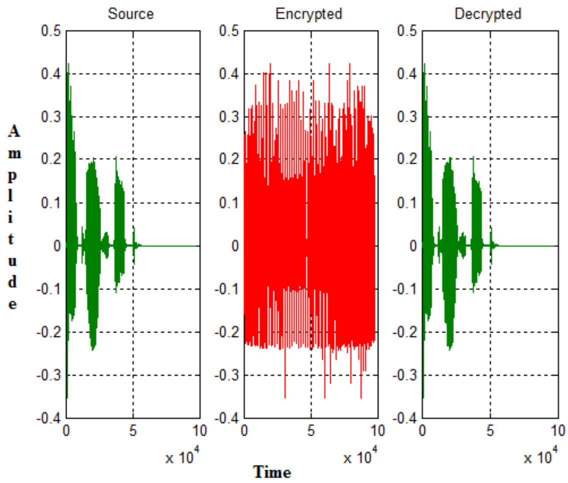

Figure-7. Sample outputs.

The proposed method satisfied the quality requirements listed in Table-1 and the results shown in Table-3 prove the quality of the proposed method:

Table-3. Quality parameters of the encrypted speeches.

Speech signal	MSE	PSNR	CC	NSCR
1	0.0048	36.1394	-0.00086194	79.7704
2	0.0117	26.4477	0.0047	79.4398
3	0.0072	35.6637	-0.0055	74.4837
4	0.0097	35.8873	0.0094	91.1075
5	0.0021	35.4564	0.0021	99.5553
6	0.0013	38.2164	0.0012	98.4679
7	0.0015	36.6604	0.0015	98.3720
8	0.0131	34.0167	0.0026	97.8881
9	0.0066	33.0669	0.0021	99.1783
10	0.0055	26.5240	-0.0056	98.4464
Remarks	High	Low	Low	High

The decrypted speeches are very sensitive to the selected private keys, any changes in them in the decryption phase will produce a damaged decrypted speech signal. Figure-8 shows a sample image_keys, while Figures 9 and 10 show the obtained outputs when using each of these private keys:

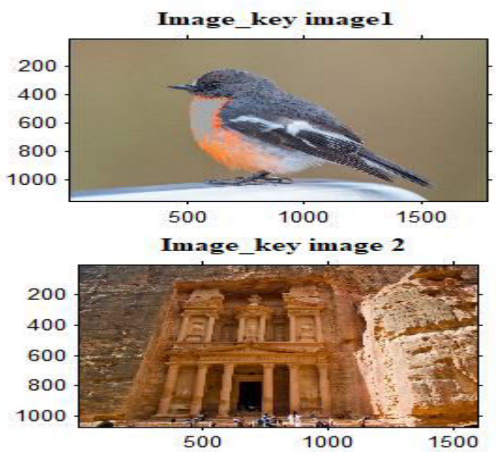

Figure-8. Selected image_keys.

ARPN Journal of Engineering and Applied Sciences
©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

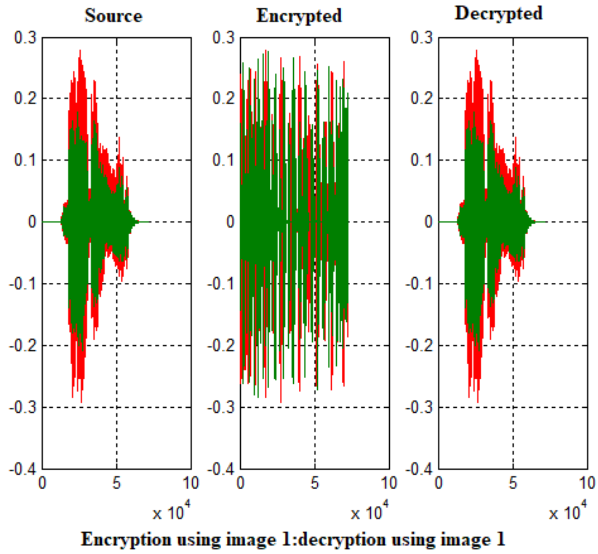

Figure-9. Sample outputs using the same image_key.

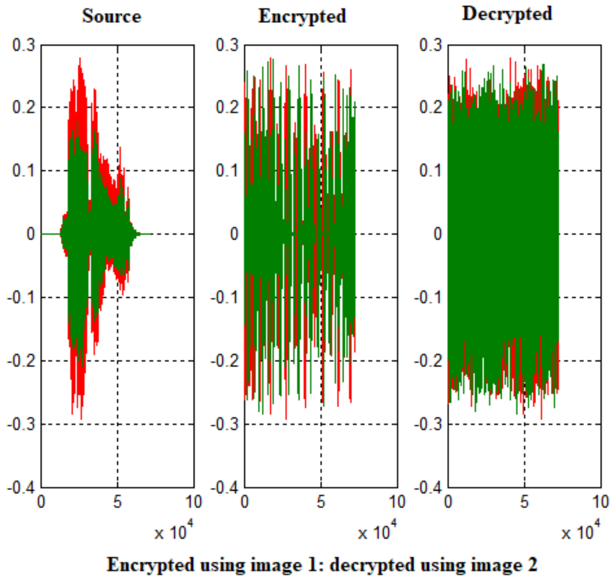

Figure-10. Sample outputs using different image_keys.

The speed of the proposed method was tested, the selected speech files were implemented and the encryption time was measured for each speech file, the throughput was calculated, Table-4 shows the obtained results:

Table-4. Speed results of the proposed method.

Speech signal	Size (sample)	Encryption time(second)	Throughput (K samples per second)
1	98015	0.0049	19559
2	94819	0.0042	21805
3	84691	0.0036	22939
4	157413	0.0064	24153
5	321536	0.0140	22491
6	200704	0.0097	20307
7	227328	0.0097	22859
8	134144	0.0057	22896
9	160768	0.0068	23124
10	145408	0.0059	23877
Average			
	162480	0.0071	22401

From Table-8 we can see that the speed results are better than the results provided by the standard methods (shown in Table-2), the proposed method enhanced the speed of data cryptography by significantly decreasing the encryption time and increasing the throughput of data cryptography.

4. CONCLUSIONS

A simple method of speech cryptography was introduced, it simplified the encryption and decryption function by replacing the encryption and decryption processes with a simple replacement operation. The proposed method can be efficiently used to encrypt-decrypt mono and stereo speeches.

The proposed method provided a high level of security and speech protection based on using two secret keys: the image_key and the position, these keys cannot be hacked because they are kept secret. The two private keys were used to generate the index key, which was used to apply character replacements in the encryption and decryption phases.

©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.

The proposed method was implemented using various speech files and the obtained results proved the sensitivity, quality, and efficiency of the proposed method.

ACKNOWLEDGMENT

The researchers are grateful to the Applied Science Private University, Amman, Jordan, for the full financial support grated to this research project.

REFERENCES

[1] Sadkhan Sattar B. and Abbas Nidaa A. 2011. Performance Evaluation of Speech Scrambling Methods Based on Statistical Approach ATTI DELLA Fonazione GiorgioRonchi Anno Lxvi. (5): 601-6014.

[2] Ambika D. and Radha V. 2012. Secure Speech communication - A Review International Journal of Engineering Research and Applications (IJERA). 2(5): 1044-1049.

[3] Mosa E., Messiha N. W., Zahran O. and Abd El-Samie F. E. 2010. Encryption of Speech Signal with Multiple Secret Keys in Time Transform Domains. Int. J Speech Technol. 13: 231-242.

[4] Mua'ad M. Abu-Faraj, Khaled Aldebei2, Ziad A. Alqadi. 2022. Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography, Traitement du Signal. 39(1): 173-178.

[5] Alqadi Z. 2019. A new method for voice signal features creation. International Journal of Electrical and Computer Engineering (IJECE), 9(5): 4092-4098.https://doi.org/10.11591/ijece.v9i5.pp4092-4098.

[6] Alqad Z. 2009. A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image. Journal of Computer Science. 5(5): 355-362.

[7] Zaini H., Alqadi Z. A. 2021. Efficient WPT based speech signal protection. IJCSMC, 10(9): 53-65. https://doi.org/10.47760/ijcsmc.2021.v10i09.006.

[8] Zneit R. A., Khrisat M. S., Khawatreh S. A., Alqadi, Z. 2020. Two ways to improve WPT decomposition used for image features extraction. European Journal of Scientific Research. 157(2): 195-205.

[9] Hindi A., Qaryouti G. M., Eltous Y., Abuzalata M., Alqadi Z. 2020. Color image compression using linear prediction coding. International Journal of Computer Science and Mobile Computing. 9(2): 13-2

[10] Prof. Qazem Jabber Prof. Ziad Alqadi, Digital Image Cryptography using Index Keys. International Journal of Computer Science and Mobile Computing. 12(2): 26-37.

[11] Hatim Zaini, Ziad Alqadi. 2023. Improving Average and Median Filters. International Journal of Computer Science and Mobile Computing. 12(2): 1-13.

[12] Hatim Zaini, Ziad Alqadi. 2023. Long Messages Segmentation for Efficient Message Cryptography. IJCSMC. 12(1): 59-693.

[13] Ziad A. Alqadi and Nasser Abdellati Adnan Manasreh, Mohammad S. 2023. Khrisat, Hatim Ghazi Zaini, Improving Data Standard Methods of Cryptography. Arpn Journal of Engineering and Applied Sciences. 17(24): 2077-2088.

[14] Zaid Alqadi and Basel J. A. Ali Mua'ad Abu-Faraj, Abeer Al-Hyarib, Ismail Altaharwaa. 2023. Increasing the security of transmitted text messages using chaotic key and image key cryptography. International Journal of Data and Network Science. 7: 1-12.

[15] Abdullah N Olimat, Ali F Al-Shawabkeh, Ziad A Al-Qadi, Nijad A Al-Najdawi, Ahmed Al-Salaymeh. 2023. Experimental study and computational approach prediction on thermal performance of eutectic salt inside a latent heat storage prototype. Thermal Science and Engineering Progress. 37: 101606.

[16] Mohammad S. Khrisat, Ziad A. Alqadi. 2022. Enhancing LSB Method Performance Using Secret Message Segmentation, IJCSNS. 22(7): 1-6.

[17] F. Omar and Z. A. Alqadi, M. M. Al-Laham. 2022. Digital Image Slicing to Strengthen the Security of LSB Technique of Encrypting Text Messages. 2022 International Arab Conference on Information Technology (ACIT). pp. 1-6.

[18] Hatim Ghazi Zaini and Ziad A. Alqadi Adnan Manasreh, Mohammad S. Khrisat. 2022. Color Images Steganography by Implementing Simple Logical Operations Using Aselected Steganographic Factor. Arpn Journal of Engineering and Applied Sciences. 17(17): 1602-1610.

©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.

[19] Aamer Nadeem, Dr M. Yuns Javed, A Performance Comparison of Data Encryption Algorithms, Conference Paper · September 2005 DOI: 10.1109/ICICT.2005.1598556 · Source: IEEE Explore.

[20] Prof. Ziad Alqadi. 2022. Modified LSB2 Steganography Method to Secure the Embedded Secret Message. International Journal of Computer Science and Mobile Computing. 11(8): 22-44.

[21] Dr. Dojana, Prof. Ziad Alqadi, Digital Image Cryptography using Lookup Table, International Journal of Computer Science and Mobile Computing, vol. 11, issue 11, pp. 180 – 199, 2022.

[22] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi. 2018. A new method for voice signal features creation. International Journal of Electrical and Computer Engineering (IJECE). 9(5): 4092-4098.

[23] Akram A. Moustafa and Ziad A. Alqadi. 2009. A Practical Approach of Selecting the Edge Detector Parameters to Achieve a Good Edge Map of the Gray Image. Journal of Computer Science. 5(5): 355-362.

[24] ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary. 2008. Performance analysis and evaluation of parallel matrix multiplication algorithms. World Applied Sciences Journal. 5(2): 211-214.

[25] Ayman Al-Rawashdeh, Ziad Al-Qadi. 2018. Using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research. 8(4): 1356-1359.

[26] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh. 2019. Enhancing the Capacity of LSB Method by Introducing LSB2Z Method. International Journal of Computer Science and Mobile Computing. 8(3): 76-90.

[27] Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, Optimized True-RGB color Image Processing. World Applied Sciences Journal 8(10): 1175-1182, ISSN 1818-4952, 2010.

[28] Waheeb A. and Ziad AlQadi. 2009. Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173.

[29] A. A. Moustafa, Z. A. Alqadi. 2009. Color Image Reconstruction Using a New R'G'I Model. Journal of Computer Science. 5(4): 250-254.

[30] K. Matrouk, A. Al-Hasanat, H. Alasha'ary, Z. Al-Qadi Al-Shalabi. 2014. Speech fingerprint to identify isolated word person. World Applied Sciences Journal. 31(10): 1767-1771.

[31] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Abu-Zaher. 2018. A Novel zero-error method to create a secret tag for an image. Journal of Theoretical and Applied Information Technology. 96(13): 4081-4091.

[32] Prof. Ziad A. A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti. 2016. Comparative Analysis of Color Image Steganography, JCSMC. 5(11): 37-43.

[33] M. Jose. 2014. Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality. International Journal of Science and Research. 3(9): 2281-2284.

[34] M. Juneja, P. S. Sandhu. 2013. An improved LSB based Steganography with enhanced Security and Embedding/Extraction, 3rd International Conference on Intelligent Computational Systems, Hong Kong China, and January 26-27.

[35] H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. A. Alqadi, H. Al-Shalabi. 2013. Improving Matrix Multiplication Using Parallel Computing. International Journal on Information Technology (I.RE.I.T.). 1(6), ISSN 2281-2911.

[36] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein. 2016. A Comparison between Parallel and Segmentation Methods Used For Image Encryption-Decryption. International Journal of Computer Science & Information Technology (IJCSIT). 8(5).

[37] Z.A. Alqadi, A. Abu-Jazar. 2005. Analysis of Program Methods Used for Optimizing Matrix Multiplication. Journal of Engineering. 15(1): 73-78.

[38] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh. 2019. A Novel Based On Image Blocking Method to Encrypt-Decrypt Color JOIV: International Journal on Informatics Visualization.

[39] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub and Mazen Abu-Zaher. 2018. A Novel Zero-Error Method to Create a Secret Tag for an Image. Journal of Theoretical and Applied Information Technology 15th July.

©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.

[40] Jamil Al Azzeh, Ziad Alqadi Qazem, M. Jabber. 2017. Statistical Analysis of Methods Used to Enhance Color Image Histogram. XX International Scientific and Technical Conference; Russia May 24-26.

[41] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata. 2016. Creating a Color Map to be used to convert a Gray Image to Color Image. International Journal of Computer Applications (0975-8887). 153(2).

[42] Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi. 2019. Analysis of Matrix Ziad Alqadi *et al*. International Journal of Computer Science and Mobile Computing. 8(3): 76-90.

[43] [42] Mohammed Abuzalata; Ziad Alqadi, Jamil Al-Azzeh; Qazem Jaber. 2019. Modified Inverse LSB Method for Highly Secure Message Hiding: International Journal of Computer Science and Mobile Computing. 8(2): 93-103.

[44] Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh. 2019. Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation. International Journal of Computer Science and Mobile Computing. 8(2): 3.

[45] Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata. 2019. Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing. 8(2).

[46] Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Qazem Jaber. 2019. Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation International Journal of Computer Science and Mobile Computing. 8(3): 14-26.

[47] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh. 2019. A Novel Based On Image Blocking Method to Encrypt-Decrypt Color; International Journal on Informatics Visualization. Vol. 3.

[48] B. Zahran, J. AL-Azzeh, Z. Al Qadi, M. Al Zoghoul and S. Khawatreh. 2018. A Modified Lbp Method to Extract Features from Color Images. Journal of Theoretical and Applied Information Technology (JATIT). 96(10).

[49] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Abu-Zaher. 2018. A novel Zero-error Method to Create a Secret Tag for an Image. Journal of Theoretical and Applied Information Technology (JATIT). 96(13): 4081-4091.

[50] J. AL-Azzeh, B. Zahran, Z. Alqadi. 2018. Salt and Pepper Noise: Effects and Removal. International Journal on Informatics Visualization. 2(4): 252-256.

[51] Jihad Nader, Ziad Alqadi, Bilal Zahran. 2017. Analysis of Color Image Filtering Methods. International Journal of Computer Applications (IJCA). 174(8): 12-17.

[52] Ziad Alqadi, Bilal Zahran, Jihad Nader. 2017. Estimation and Tuning of FIR Low pass Digital Filter Parameters. International Journal of Advanced Research in Computer Science and Software Engineering. 7(2): 18-23.

[53] Khaled Aldebei, Mua'ad M. Abu-Faraj, Ziad A. Alqadi. 2022. Comparative Analysis of Fingerprint Features Extraction Methods. Journal of Hunan University Natural Sciences. 48(12): 177-182.

[54] Dr. Mohamad Barakat Prof. Ziad Alqadi. 2022. Highly Secure Method for Secret Data Transmission. International Journal of Scientific Engineering and Science. 6(1): 49-55.

[55] M. Abu-Faraj, A. Al-Hyari and Z. Alqadi. 2022. A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography. Symmetry, 14(4): 664-678, doi.org/10.3390/sym14040664.

[56] M. Abu-Faraj, K. Aldebei and Z. Alqadi. 2022. Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography. Traitement du Signal. 39(1): 173-178, doi.org/10.18280/ts.390117.

[57] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi. 2021. Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study. Journal of Southwest Jiaotong University, 56(6): 685-694, doi:10.35741/issn.0258-2724.56.6.61.

[58] M. Abu-Faraj, Z. Alqadi, and K. Aldebei. 2021. Comparative Analysis of Fingerprint Features

ARPN Journal of Engineering and Applied Sciences
©2006-2023 Asian Research Publishing Network (ARPN). All rights reserved.

Extraction Methods. Journal of Hunan University Natural Sciences. 48(12): 177-182.

[59] M. Abu-Faraj and Z. Alqadi. 2021. Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography. International Journal of Computer Science and Network Security (IJCSNS), 21(12): 648-656, doi: 10.22937/IJCSNS.2021.21.12.89.

[60] M. Abu-Faraj and Z. Alqadi. 2021. Improving the Efficiency and Scalability of Standard Methods for Data Cryptography. International Journal of Computer Science and Network Security (IJCSNS), 21(12): 451-458, doi:10.22937/IJCSNS.2021.21.12.61.

[61] M. Abu-Faraj and Z. Alqadi. 2021. Using Highly Secure Data Encryption Method for Text File Cryptography. International Journal of Computer Science and Network Security (IJCSNS), 21(12): 53-60, doi:10.22937/IJCSNS.2021.21.12.8.