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. 12, Issue. 3, March 2023, pg.22 – 33

Speech Files Cryptography using Indices Keys and Blocking

Prof. Ziad Alqadi; Dr. MOHAMAD-TARIQ BARAKAT
Albalqa Applied University
Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2023.v12i03.003

Abstract: Protecting speech file is a vital issue. In this paper research a simple method of speech cryptography will be introduced. The method will use indices key to perform simple replacement operations to apply speech encryption and decryption, the replacement operation will use the indexes and the indexes contents to apply speech cryptography. The proposed method will protect the speech signal by increasing the security level, the method will use a color image as an image_key, this key will be kept in secret between the sender and receiver and it will be used to generate the indices key. The proposed will sensitive to the selected image_key, changing this image will be considered as a hacking attempt by producing a damaged decrypted speech signal. The proposed method will be flexible, changing the image_key will not cause any changes in the proposed method algorithms. To increase the efficiency of the proposed method by decreasing the processing time the speech file will be divided into blocks, and each block will be treated separately. The proposed method will be tested and implemented using various speech files, the obtained results will be used to prove the quality, sensitivity and efficiency of the proposed method.

Keywords: Cryptography, image_key, indices key, quality, sensitivity, flexibility.

Introduction

Digital speech file is a set of amplitude values taken in a period of time and they are organized in one column matrix (mono speech) or 2 column matrix (stereo speech) as shown in figure 1 [1-10].

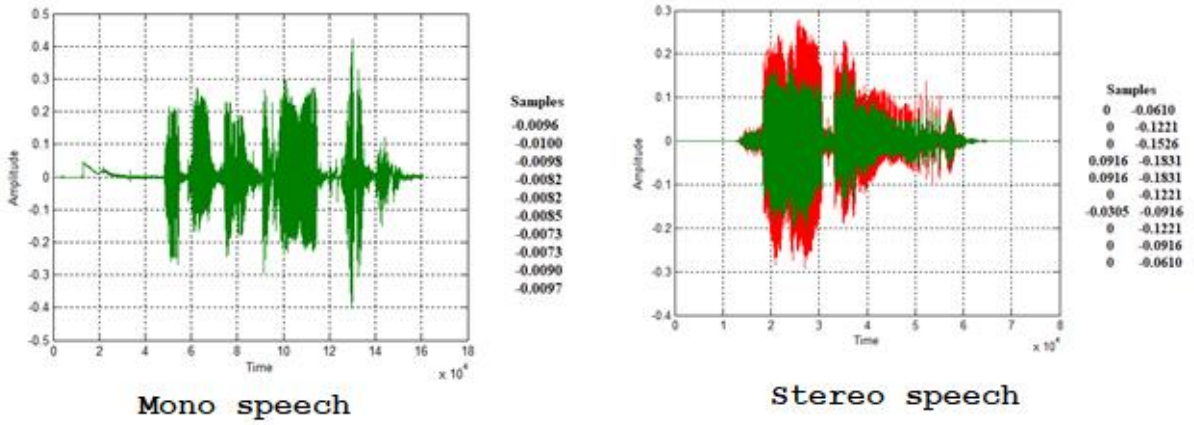

Figure 1: Speech signal wave

Speech file may be secret or may be contains valuable secret information [1-10]. This speech requires protection from being hacked. Cryptography is one way to protect speech file and make it secure. Cryptography means encryption the speech file before sending, making the speech file damaged and un understandable, and decryption after receiving the decrypted speech by producing a decrypted file which is 100% identical to the source file [11-20]. Speech encryption and decryption as shown in figure 2 are applied by using an encryption/decryption function and one or more private keys [21-30].

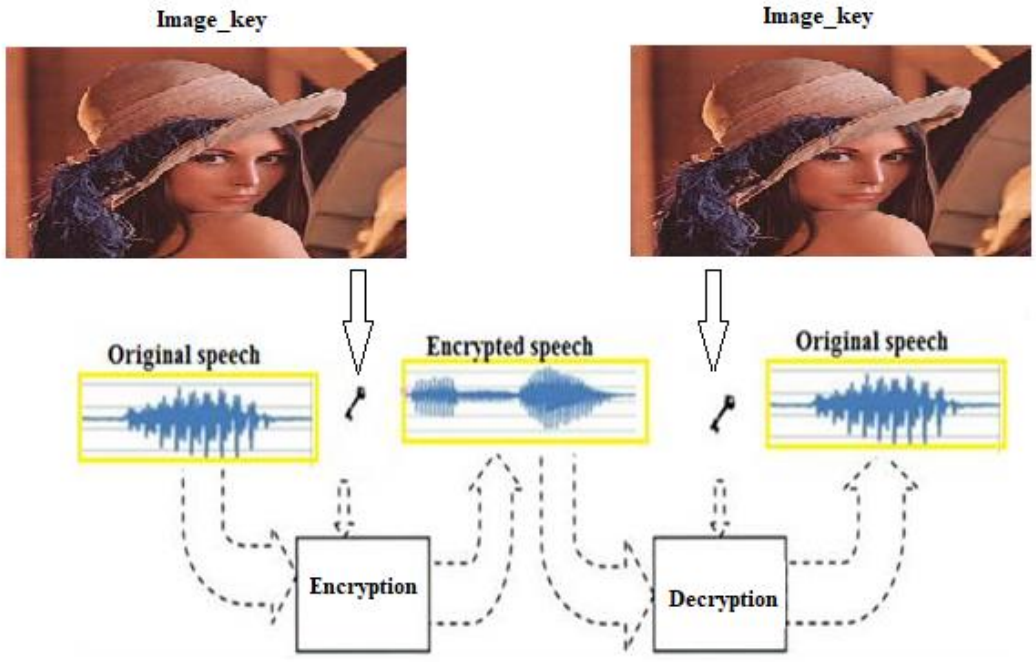

Figure 2: Speech cryptography process

The objective of this research paper is to introduce a method of speech cryptography, which will provide the following features [31-40]:

- High level of security by providing a high degree of speech file protection [11-20]. This can be achieved by using a digital color image as an image_key. The key image must be kept confidential by the sender and the receiver, and an agreement must be reached between them to specify this image, provided that it is not communicated. Using the color image as an image_key has the following advantages:
    1) Easy to implement. The color image is represented by a 3D matrix (one 2D matrix for each color (red, green and blue)) as shown in figure 3, and using this matrix will simplify the private key processing [41-45].
    2) Easy to use any part of the image to be used to generate the indices keys required to apply speech encryption and decryption.
    3) Easy to reshape the image from 3D to one row matrix [46-50].
    4) Image has a huge size, and it can be deployed to apply many applications [15-22].
    5) Easy to get and save, there are a lot of resources available to get the image from, and a lot of equipment's, which can be easily used to generate the image.

- Flexibility, it is easy to change the image_key without affecting the algorithms of the proposed method.

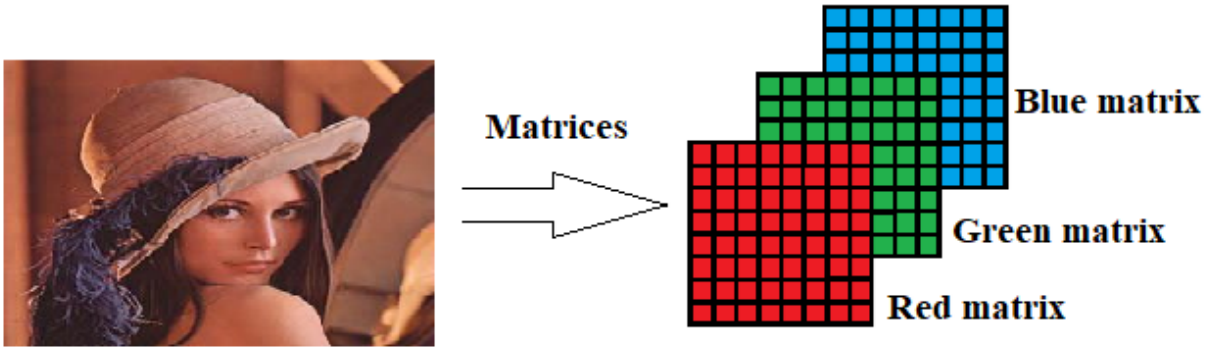

Figure 3: Color image matrices

- Low encrypted speech quality [1-6], the generated encrypted speech must be damaged, and the quality parameters measured between the source and the encrypted speeches must satisfy the requirements listed in table 1 (mean square error (MSE), peak signal to noise ratio (PSNR), correlation coefficient (CC) and number of samples change ratio (NSCR)) [51-60].

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

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

- High quality of the decrypted speech file, the quality parameters measured between the source and the decrypted speeches must satisfy the quality requirements listed in table 1.
- Sensitivity, the encryption and decryption functions must use the same private key, any changes in the image_key during the decryption phase must be considered as a hacking attempt by producing a damaged decrypted speech file.
- High speed of speech cryptography, the method must minimize both the encryption and decryption times (processing time), thus it must maximize the throughput of speech cryptography [1-10].

The Proposed Method

The proposed method uses a huge in size private key, this key must be kept in secret and it is impossible to hack it. A color image is used as an image_key, this image-key is to be used to extract a part with a selected size (block size), and the extracted array is to be used to generate an indices key needed to apply simple replacement operation to apply speech sample encryption and decryption. The extracted array is to be sorted to get the indices key, and the replacement operations are simply applied as shown in figure 4. The encryption and decryption functions will maintain only one operation making theses function very simple by minimizing the required operations of these functions:

1	2	3	4	5	6	7	8	9	10
0.0053	0.0035	0.0035	0.0035	0.0010	0.0010	-0.0007	-0.0007	-0.0007	-0.0025

Encryption ⇩ Store according to index

0.0053	0.0035	0.0035	0.0010	0.0035	-0.0025	-0.0007	-0.0007	-0.0007	0.0010

Decryption ⇩ Retrieve according to index

0.0053	0.0035	0.0035	0.0035	0.0010	0.0010	-0.0007	-0.0007	-0.0007	-0.0025

⇩ Array

70	88	92	113	158	103	116	129	140	115

⇩ Index key

1	2	3	6	4	10	7	8	9	5

Figure 4: Replacement operations in the encryption and decryption functions

The proposed method is very sensitive to the selected image_key, changing the image_key as shown in figure 5 will change the indices key, thus the encrypted speech file will be changed.

1	2	3	4	5	6	7	8	9	10
0.0053	0.0035	0.0035	0.0035	0.0010	0.0010	-0.0007	-0.0007	-0.0007	-0.0025

Encryption ⇩ Store according to index

-0.0007	-0.0025	-0.0007	-0.0007	0.0010	0.0010	0.0053	0.0035	0.0035	0.0035

Decryption ⇩ Retrieve according to index

0.0053	0.0035	0.0035	0.0035	0.0010	0.0010	-0.0007	-0.0007	-0.0007	-0.0025

⇩ Array

189	189	189	189	188	188	187	187	186	186

⇩ Index key

9	10	7	8	5	6	1	2	3	4

Figure 5: Changing the image_key produces a new indices key

The search operation in the decryption function will take a time, this time will rapidly increase when increasing the sizes of the data to be decrypted, so the speech file must be divided into equal blocks and each block must be treated separately, this process will totally decrease the decryption time (this will be shown in the implementation part by dividing the speech file into 16 blocks).
Replacing the image_key in the decryption phase will produce a damaged speech file as shown in figure 6:

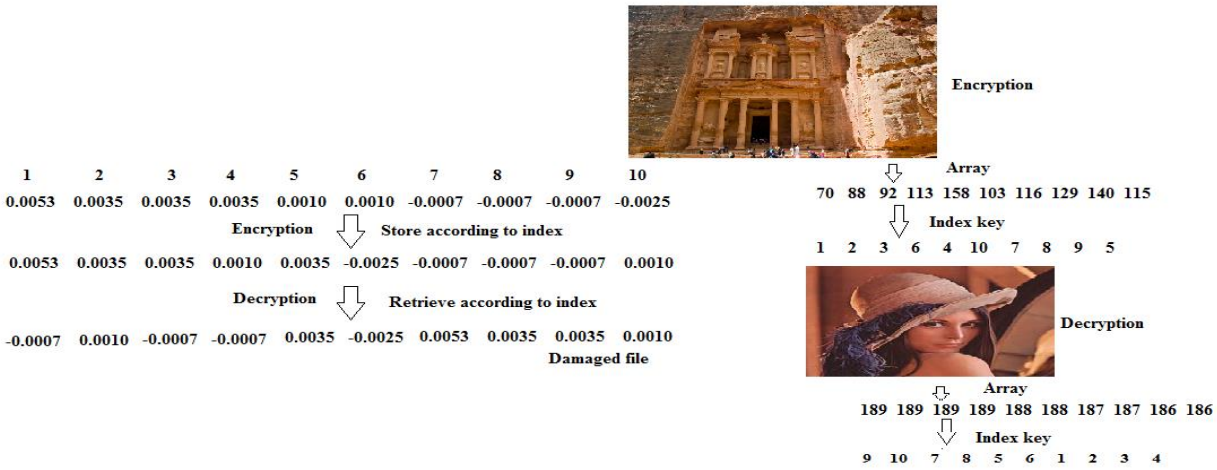

Figure 6: Effects of replacing the image_key in the decryption phase

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

Step 1:

Speech file preparation: Get the speech file, retrieve the speech file size, reshape the file into one row matrix, divide the speech file into 16 blocks, this step can be implemented applying the following sequence of mat lab operations:

```
[a1 fs]=wavread('C:\Users\Dr.Tayseer\Desktop\voices\tts4.wav');
[n1 n2]=size(a1);
a=reshape(a1,1,n1*n2);
row=0.06;
s=n1*n2;
R=fix(s*row);
b1=a(1,1:R);b2=a(1,R+1:2*R);b3=a(1,2*R+1:3*R);b4=a(1,3*R+1:4*R);
b5=a(1,4*R+1:5*R);b6=a(1,5*R+1:6*R);b7=a(1,6*R+1:7*R);b8=a(1,7*R+1:8*R);
b9=a(1,8*R+1:9*R);b10=a(1,9*R+1:10*R);b11=a(1,10*R+1:11*R);b12=a(1,11*R+1:12*R);
b13=a(1,12*R+1:13*R);b14=a(1,13*R+1:14*R);b15=a(1,14*R+1:15*R);b16=a(1,15*R+1:s);
w=prod(size(b16));
```

Step 2:

Indices key generation: Get the image_key, retrieve the image size, reshape the image into one row matrix, get two parts from the image, the first one to be used to generate the indices key for each of the first 15 blocks, the second one to be used to generate the indices key for the last block (block 16), this step can be implemented applying the following sequence of mat lab operations:


```
ikey=imread('C:\Users\Dr.Tayseer\Desktop\drziad\MAVAV\a4.jpg');
[nn1 nn2 nn3]=size(ikey);
ikey1=reshape(ikey,1,nn1*nn2*nn3);
kk1=ikey1(1,1:R);
[dd key1]=sort(kk1);
kk2=ikey1(1,15*R+1:s);
[dd key2]=sort(kk2);
```

Step 3:

Encryption: Encrypt each block of the first 15 blocks, then encrypt the last block. For encrypting each block of the first 15 blocks the following sequence of operations can be used (by using the associated block):

```
for i=1:R

        ff=key1(i);
        e1(i)=b1(ff);

end
```

The last block can be encrypted using the following sequence of operations:

```
for i=1:w

        ff=key2(i);
        e16(i)=b16(ff);

end
```

Step 4:

Getting the encrypted speech: Combine the encrypted blocks in one row matrix, reshape the matrix to the speech file size, this step can be implemented applying the following sequence of mat lab operations:

```
en1=[e1 e2 e3 e4 e5 e6 e7 e8 e9 e10 e11 e12 e13 e14 e15 e16];
en=reshape(en1,n1,n2);
```

The decryption phase can be implemented applying the same steps by changing the encryption to decryption applying the following:

```
for i=1:R

        ff=find(key1==i);
        d1(i)=e1(ff);

end
```


Implementation and Results Discussion

Several speech files were selected, the speech files were encrypted-decrypted using one block division (the speech file without division), the encryption time, decryption time were measured, and the processing time was calculated (Processing time is the summation of encryption and decryption times), table 2 shows the obtained results:

Table 2: Speed result without speech file division

Speech number	Size (samples)	Encryption time (seconds)	Decryption time (seconds)	Processing time (seconds)
1	347858	0.0170	0.0170	318.2684
2	212552	0.0097	116.5690	116.5787
3	170944	0.0077	72.3859	72.3936
4	321536	0.0169	266.7623	266.7792
5	200704	0.0092	100.5777	100.5868
6	227328	0.0134	132.9138	132.9272
7	98015	0.0044	21.7122	21.7166
8	94819	0.0041	20.2591	20.2636
9	84691	0.0037	15.9214	15.9251
10	157413	0.0073	59.8649	59.8722

From table 2 we can see the following facts:

- The encryption time is low and it is acceptable.
- The decryption time is very high and it requires enhancement.
- Increasing the speech file size will rapidly increase the decryption time and thus the processing time will be very high as shown in figure 7

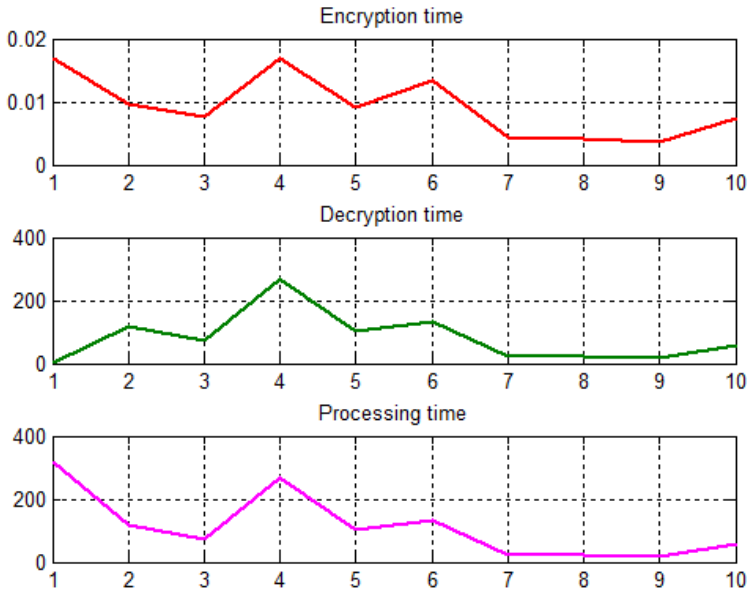

Figure 7: cryptography times without speech file blocking

The decryption time requires a lot of time, because searching the index in the indices key require a lot of time, and this time will rapidly increase when increasing the speech file size. To reduce the decryption time, the speech file must be small in size, so it must be divided into small blocks, each block is to be treated separately, table 3 shows the cryptography times when dividing each speech signal into 16 blocks:

Table 3: Cryptography times when dividing speech file into 16 blocks

Speech number	Encryption time (seconds)	Decryption time (seconds)	Processing time (seconds) using 16 blocks	Processing time (seconds) using 1 block	Speed up of blocking
1	2.8524	13.2685	16.1209	318.2684	19.7426
2	1.0136	5.0786	6.0922	116.5787	19.1357
3	0.6787	3.3872	4.0659	72.3936	17.8051
4	2.3039	11.3085	13.6124	266.7792	19.5982
5	0.9185	4.4826	5.4012	100.5868	18.6230
6	1.1592	5.7640	6.9232	132.9272	19.2003
7	0.2294	1.1970	1.4264	21.7166	15.2248
8	0.2213	1.1100	1.3313	20.2636	15.2209
9	0.1801	0.9193	1.0995	15.9251	14.4839
10	0.5749	2.9289	3.5038	59.8722	17.0878

From table 3 we can see that blocking the speech file will enhance the efficiency of speech cryptography and will speed up the process of speech cryptography as shown in table 3.

The proposed method was tested for sensitivity, a speech file was encrypted using the image_key shown in figure 6 and the encrypted speech was decrypted using the other image shown in figure 6, figure 8 shows the obtained speech files, from this figure we can see that the decrypted speech is a damaged file and it is not identical to the source speech file, which prove the sensitivity of the proposed method:

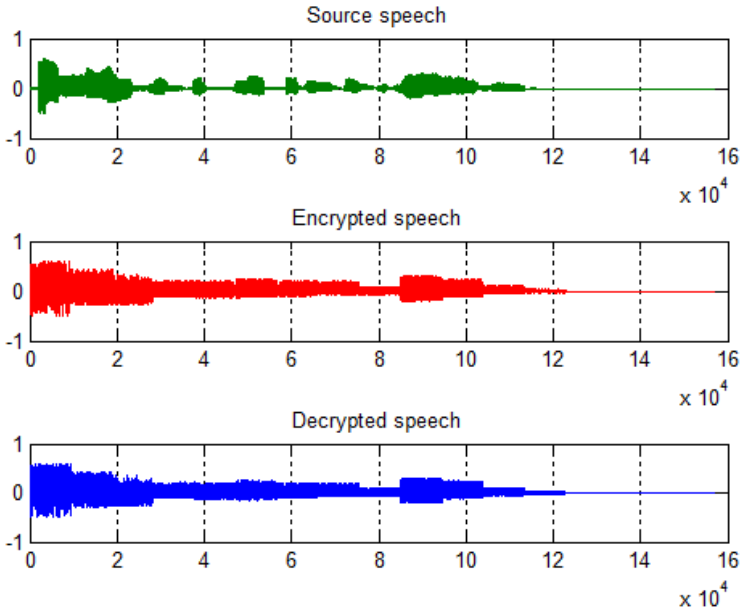

Figure 8: Example of the method sensitivity

The proposed method was tested for quality, an image_key was selected as a private key in both the encryption and decryption phases, figure 9 shows an example of speech files implementation:

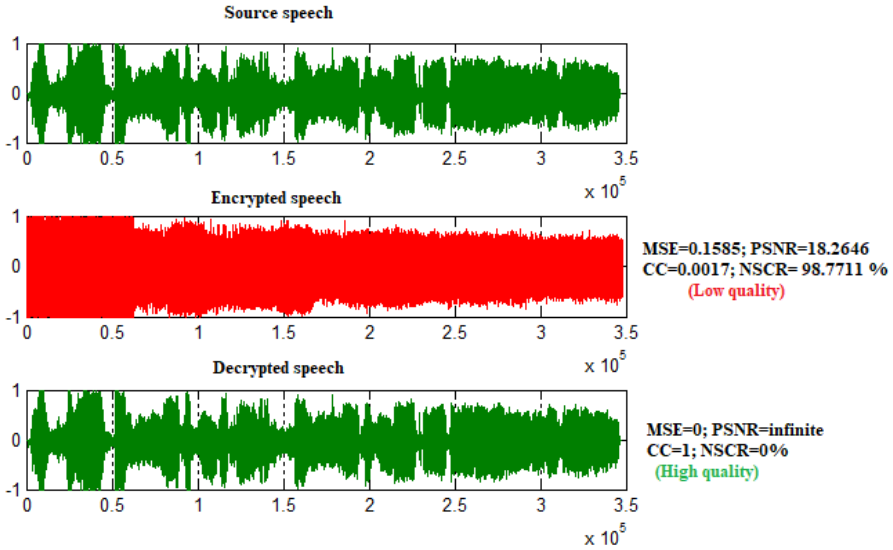

Figure 9: Quality of speech cryptography

From figure 9 we can see that the proposed method satisfied the quality requirement in the encryption and decryption phases by satisfying the requirements listed in table 1.

Conclusion

A simple, flexible, qualitied, sensitive, secure and efficient method of speech file cryptography was proposed. The method simplified the encryption and decryption functions by using a simple replacement operation in each function. The private key can be easily changed and replaced with another key without the need to change the method algorithm. The method used a color image as a private key, this key was used to generate an indices key required to apply the replacement operation in the encryption and decryption function. The proposed method was very sensitive to the selected private key, any changes in this key in the decryption phase were considered as a hacking attempts by producing a damaged decrypted speech files.

To enhance the speed of decryption the speech file was divided into blocks, using blocks speed up the process of speech cryptography. The proposed method was tested for quality and the obtained results proved the quality of the encrypted and decrypted speeches.

References

[1] Sadkhan Sattar B. and Abbas Nidaa A., "Performance Evaluation of Speech Scrambling Methods Based on Statistical Approach" ATTI DELLA "Fonazione GiorgioRonchi" Anno Lxvi, No. 5 PP. 601-6014 (2011).
[2] Ambika D. and Radha V., "Secure Speech communication – A Review International Journal of Engineering Research and Applications (IJERA), Vol. 2Issue 5 PP. 1044-1049 (2012).
[3] Mosa E.; Messiha N.W.; Zahran O. and Abd El-SamieF.E. "Encryption of Speech Signal with Multiple Secret Keys in Time Transform Domains " Int. J Speech Technol., Vol. 13 PP. 231-242 (2010).
[4] Mua'ad M. Abu-Faraj, Khaled Aldebei2, Ziad A. Alqadi, Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography, Traitement du Signal, vol. 39, issue 1, pp. 173-178, 2022.
[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] Alqadi, 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, vol. 12, issue 2, pp. 26 – 37, 2023.
[11] Hatim Zaini, Ziad Alqadi, Improving Average and Median Filters, International Journal of Computer Science and Mobile Computing, Vol. 12, Issue. 2, pg.1 – 13, 2023.
[12] Hatim Zaini, Ziad Alqadi, Long Messages Segmentation for Efficient Message Cryptography, IJCSMC, vol. 12, issue 1, pp. 59-69, 2023.
[13] Ziad A. Alqadi and Nasser Abdellati Adnan Manasreh, Mohammad S. Khrisat, Hatim Ghazi Zaini, IMPROVING DATA STANDARD METHODS OF CRYPTOGRAPHY, ARPN Journal of Engineering and Applied Sciences, vol. 17, issue 24, pp. 2077-2088, 2023.
[14] Zaid Alqadi and Basel J. A. Ali Mua'ad Abu-Faraj, Abeer Al-Hyarib, Ismail Altaharwaa, Increasing the security of transmitted text messages using chaotic key and image key cryptography, International Journal of Data and Network Science, vol. 7, pp. 1-12, 2023.
[15] Abdullah N Olimat, Ali F Al-Shawabkeh, Ziad A Al-Qadi, Nijad A Al-Najdawi, Ahmed Al-Salaymeh, Experimental study and computational approach prediction on thermal performance of eutectic salt inside a latent heat storage prototype, Thermal Science and Engineering Progress, Volume 37, 101606, 2023.
[16] Mohammad S Khrisat, Ziad A Alqadi, Enhancing LSB Method Performance Using Secret Message Segmentation, IJCSNS, vol. 22, issue 7, pp. 1-6, 2022.

[17] F. Omar and Z. A. Alqadi, M. M. Al-Laham, 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, 2022.
[18] Hatim Ghazi Zaini and Ziad A. Alqadi Adnan Manasreh, Mohammad S. Khrisat, COLOR IMAGES STEGANOGRAPHY BY IMPLEMENTING SIMPLE LOGICAL OPERATIONS USING ASELECTED STEGANOGRAPHIC FACTOR, ARPN Journal of Engineering and Applied Sciences, vol. 17, issue 17, pp. 1602-1610, 2022.
[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, Modified LSB2 Steganography Method to Secure the Embedded Secret Message, International Journal of Computer Science and Mobile Computing, vol. 11, issue 8, pp. 22 – 44, 2022.
[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, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2018.
[23] Akram A. Moustafa and 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 5 (5): 355-362, 2009.
[24].ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, World Applied Sciences Journal, vol. 5, issue 2, pp. 211-214, 2008.
[25] 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.
[26] 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.
[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, Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173, 2009. [20].A. A. Moustafa, Z. A. Alqadi, "Color Image Reconstruction Using a New R'G'I Model", Journal of Computer Science, Vol.5, No. 4, pp. 250-254, 2009.
[29] K Matrouk, A Al-Hasanat, H Alasha'ary, Z. Al-Qadi Al-Shalabi, "Speech fingerprint to identify isolated word person", World Applied Sciences Journal, Vol. 31, No. 10, pp. 1767-1771, 2014.
[30] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Abu-Zaher, "A Novel zero-error method to create a secret tag for an image", Journal of Theoretical and Applied Information Technology, Vol. 96. No. 13, pp. 4081-4091, 2018.
[31] Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.
[32] M. Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", International Journal of Science and Research, Vol. 3, No. 9, pp. 2281-2284, 2014.
[33] M. Juneja, P. S. Sandhu, An improved LSB based Steganography with enhanced Security and Embedding/Extraction, 3rd International Conference on Intelligent Computational Systems, Hong Kong China, January 26-27, 2013.
[34] 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.) Vol. 1, N. 6 ISSN 2281-2911.
[35] 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, No 5, October 2016.
[36] Z.A. Alqadi, A. Abu-Jazar (2005), Analysis of Program Methods Used for Optimizing Matrix Multiplication, Journal of Engineering, vol. 15 n. 1, pp. 73-78.
[37] 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, 2019.
[38] 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 15th July 2018.
[39] Jamil Al Azzeh, Ziad Alqadi Qazem, M. Jabber: Statistical Analysis of Methods Used to Enhanced Color Image Histogram; XX International Scientific and Technical Conference; Russia May 24-26, 2017.

[40] 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 (0975 – 8887). Volume 153 – No2, November 2016.
[41] Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi Analysis of Matrix Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 76-90.
[42] Mohammed Abuzalata; Ziad Alqadi, Jamil Al-Azzeh; Qazem Jaber Modified Inverse LSB Method for Highly Secure Message Hiding: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019, pg. 93-103.
[43] Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019/3.
[44] Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata; Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019.
[45] 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, March- 2019, pg. 14-26.
[46] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh; A Novel Based on Image Blocking Method to Encrypt-Decrypt Color; INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION VOL 3, (2019).
[47] B. Zahran, J. AL-Azzeh, Z. Al Qadi, M. Al Zoghoul and S. Khawatreh, "A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 10, 2018.
[48] J. AL-AZZEH, B. ZAHRAN, Z. ALQADI, B. AYYOUB, M. ABU-ZAHER, "A novel Zero-error Method to Create a Secret Tag for an Image", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 13, 2018.pp: 4081-4091.
[49] J. AL-AZZEH, B. ZAHRAN, Z. ALQADI," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.
[50] Jihad Nader, Ziad Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", International Journal of Computer Applications (IJCA), Volume 174, issue 8, 2017, pp:12-17.
[51] Ziad Alqadi, Bilal Zahran, Jihad Nader, " Estimation and Tuning of FIR Low pass Digital Filter Parameters", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 2, 2017, pp:18-23.
[52] Khaled Aldebei, Mua'ad M. Abu-Faraj, Ziad A. Alqadi, Comparative Analysis of Fingerprint Features Extraction Methods, Journal of Hunan University Natural Sciences, vol. 48, issue 12, pp. 177-182, 2022.
[53] Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering and Science, vol. 6, issue 1, pp. 49-55, 2022.
[54] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022, doi.org/10.3390/sym14040664.
[55] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022, doi.org/10.18280/ts.390117.
[56] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6, pp. 685-694, 2021, doi:10.35741/issn.0258-2724.56.6.61.
[57] M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Extraction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.
[58] M. Abu-Faraj, and Z. Alqadi, "Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no. 12, pp. 648-656, 2021, doi: 10.22937/IJCSNS.2021.21.12.89.
[59] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 451-458, 2021, doi:10.22937/IJCSNS.2021.21.12.61.
[60] M. Abu-Faraj, and Z. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 53-60, 2021, doi:10.22937/IJCSNS.2021.21.12.8.

