VOL. 18, NO. 23, DECEMBER 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A DETAILED STUDY OF SPEECH SIGNAL CRYPTOGRAPHY USING SIMPLE PUT _OPERATION AND GET_OPERATION

Nasser Abdellatif[1,2], Adnan Manasreh[1,2], Ziad A. Alqadi[3], Mohammad S. Khrisat[3], Maryam Akhozahieh[1,2] and Dmitry Manasreh[4]
[1]Department of Electrical Engineering, Applied Science Private University, Amman, Jordan
[2]Department of Electrical Engineering, Middle East University, Amman, Jordan
[3]Department of Computer Engineering, Faculty of Engineering Technology, AL-Balqa Applied University Amman, Jordan
[4]Center for Smart, Sustainable and Resilient Infrastructure (CSSRI), University of Cincinnati, Ohio
E-Mail: nasser_abdellatif@asu.edu.jo

ABSTRACT

Protecting digital speech files is an important issue. In this paper's research, a simplified method of speech file cryptography will be provided, and the encryption and decryption functions will require a reduced number of operations. The encryption function will perform a put_operation to reorder the speech sample to get the encrypted file, while the decryption function will perform a get_operation to reorder the encrypted samples to get the decrypted speech file; these operations will be implemented based on the generated secret indices key. The Put and get operations will affect the speech file by recording the samples keeping the histograms of the speech files (source, encrypted, and decrypted) the same and without any changes. The secret key generation phase will be analyzed for efficiency purposes, and two methods will be presented: The first one will use the chaotic logistic map model to generate the secret indices key, while the second method will use a selected secret image to generate the secret indices key, both methods will be tested and examined to give some recommendations for the users. Each of the introduced methods will provide a high level of security, the private keys will provide a huge key space and they will be very sensitive to resist any hacking attacks. The quality, sensitivity, security, and speed of the proposed methods will be examined, the method will be tested and implemented, and the obtained results will be analyzed to prove the achievements provided by the proposed method.

Keywords: speech, cryptography, put_operation, get_operation, PK, SIK, CLMM, quality, security, sensitivity, speedup.

Manuscript Received 24 October 2023; Revised 19 January 2024; Published 10 February 2024

1. INTRODUCTION

A digital speech file [28] is a set of samples (representing the amplitude values) taken over some time**,** each sample has a double data type and usually falls within the range -1 to 1, the size of the speech file depends on the recording time and the sampling frequency (FS), and it is calculated by multiplying the recording time by FS, figure 1 show a sample of a speech file waveform [43-45].

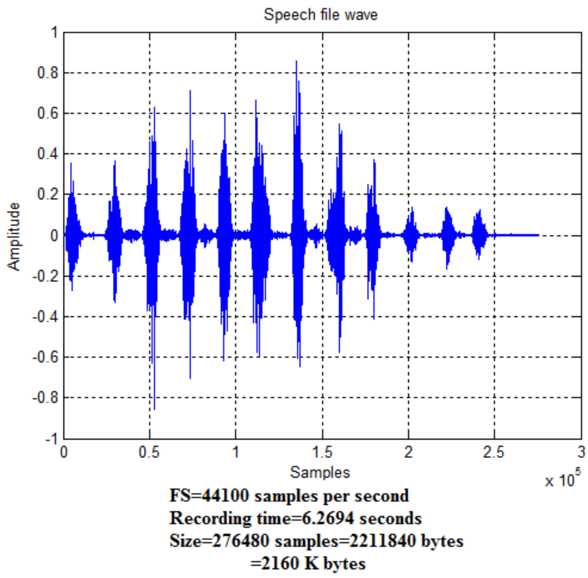

Figure-1. Speech file wave example.

Digital speech files are very important data types, that are used in various computer applications, they are circulated through different communication Media, and they may contain secret or private information, so protecting them from being hacked is a vital issue [46-47]. Speech cryptography [20-27] is one of the easiest and most efficient techniques used to protect speech files. The

ARPN Journal of Engineering and Applied Sciences

sender must encrypt the speech before sending, while the receiver must decrypt the encrypted speech after receiving it. The sender part of the crypto system as shown in Figure-2 contains a source speech file, private key (PK), encrypted speech file, secret key generation function, and encryption function. The decryption part of the crypto system, as shown in Figure 3, contains Encrypted speech, PK, decrypted speech, secret key generation function, and decryption function [29-.35]

The decryption function must destroy the source speech file, making it damaged and un understandable, here the encrypted speech must have low quality, and the quality parameters measured between the source and the encrypted speeches must be as follows: High MSE (mean square error, low PSNR (peak signal to noise ratio), low CC (correlation coefficient) and closed to 100% NSCR (number of samples changed rate). The decryption function must produce a decrypted speech identical to the source speech, the quality parameters measured between the source and the decrypted speeches must be as follows: 0 MSE, infinite PSNR, 1 CC, and 0% NSCR [36-42].

This paper research aims to introduce an efficient method of speech cryptography that will meet the cryptography requirements listed in table 1 [16-24]:

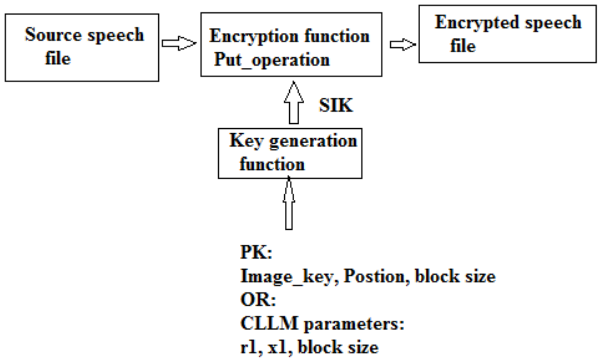

Figure-2. Encryption process.

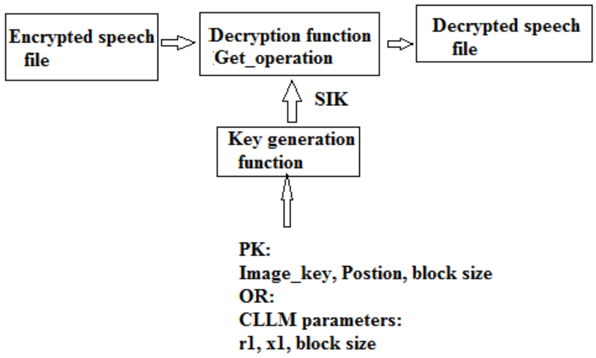

Figure-3. Decryption process.

Table-1. Speech files cryptography requirements.

Requirement	Description
Low encrypted file quality	High MSE, low PSNR, low CC, and high NSCR
High decrypted file quality	MSE=0, PSNR-infinite, CC=1 and NSCR=0%(No data loss)
PK	Complex with complicated structure
Security	Huge key space, High value of NSCR (for the encrypted speech), and PK sensitive
Secret key	Variable length secret key(length selected by the user as a part of the PK), small time of generation, sensitive to any changes in the PK.
Speed	High speed of cryptography: reduced time for key generation, reduced time for encryption-decryption. Provide blocking to minimize the encryption-decryption time, block size is variable.
Simplicity	Reduced operations for the key generation function and the encryption-decryption functions

Many methods were introduced for speech cryptography; some of these methods were based on the standards of cryptography such as AES standard [1-10], and others were based on using a chaotic logistic map model (CLMM) to generate the secret key. These methods provide good quality, various levels of security, and various speeds of cryptography, and here we will select an AES based method [2], and a chaotic based method [1] to show how the proposed methods will speed up the process of speech cryptography.

2. PROPOSED METHOD

Using chaotic keys to generate secret indices keys (SIK) is a simple procedure [1-5], the PK parameters (r1 and x1 with key length) can be used to run the chaotic logistic map model (CLMM) to get an array (chaotic key: CK), the CK can be sorted to get the SIK (6-17), the generated SIK is very sensitive to the selected PK, any minor changes in the PK will lead to change the SIK, figure 4 shows the sensitivity of the generated SIK using CLMM.

VOL. 18, NO. 23, DECEMBER 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

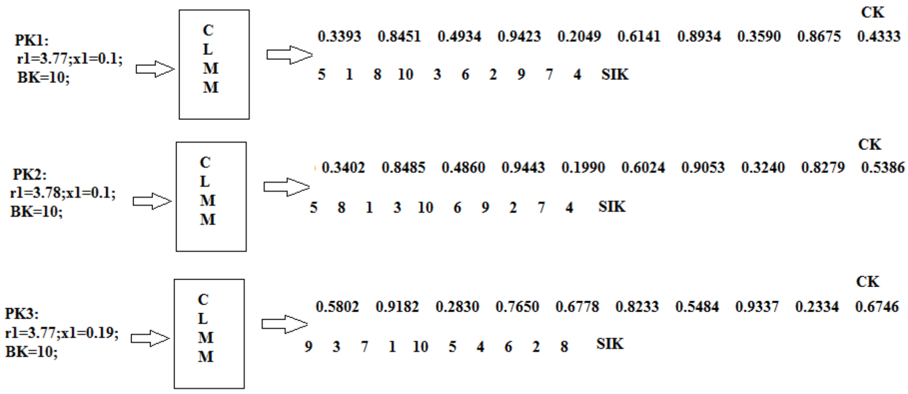

Figure-4. Generated SIK using CLMM sensitivity.

For the first proposed method, the SIK generation (key generation phase) will use the CLMM parameters and the speech file block size, these parameters will be used in the executed CLMM to get the chaotic key, this key will changed to SIK by sorting the CK, this phase will be required in the encryption and decryption phases and will be applied implementing the following steps:

Step1

Get the chaotic parameters r1, x1, and block size.

Step 2:

Run CLMM to get the CK.

Step 3:

Convert the CK to SIK by sorting the CK.

The SIK generation phase using CLMM can be implemented using the following sequence of matlab operations:

```
r1=3.77;x1=0.1;
for i=1:BS

    x1=r1*x1*(1-x1);
    CLK1(i)=x1;
end
[d1d k2]=sort(CLK1);
```

Increasing the size of the CK will rapidly increase the key generation time, thus the encryption time will be increased, to avoid this disadvantage, we can use blocking operation by dividing the speech file into blocks with small lights, or use a color image[10-16] as an image_key, an array from this image can be extracted and sorted to generate SIK., this key generation method will be proposed for method 2 of speech cryptography, here the PK will contain the image key and a fractional parameter to be used to calculate the starting position in the image_key where to start extracting the array, the block size must be included in the PK. Here the generated SIK will be very sensitive to the selected PK, any changes in the PK will lead to a change in the generated SIK as shown in Figures 5 and 6.

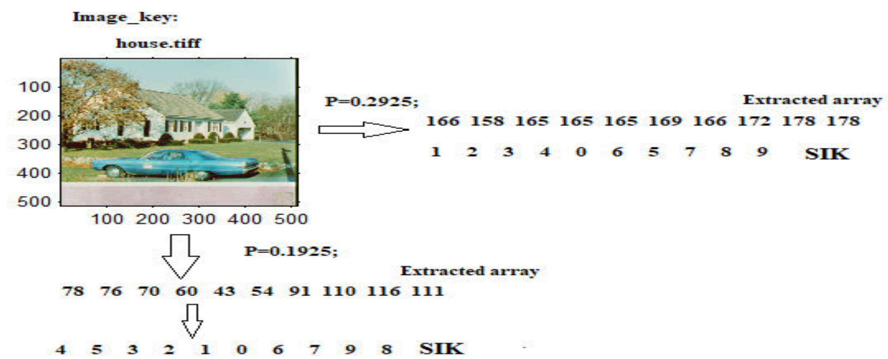

Figure-5. Changing the position fraction changes the SIK.

ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

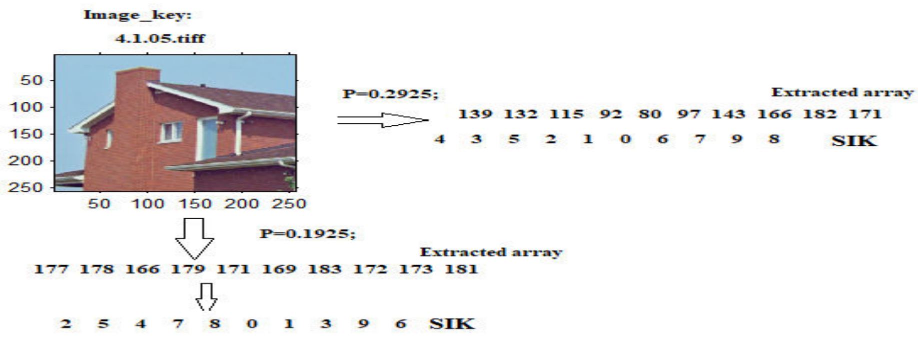

Figure-6. Changing the image_key changes the SIK.

The key generation phase for method 2 can be implemented by applying the following steps:

Step 1:

Data preparation: Get the PK: image_key, P, and block size.

Step 2:

Generating SIK: retrieve the image_key size, reshape the image matrix into one row matrix, use P to calculate the starting point, extract the array with a length equal to BS, and sort the array to get SIK.

This phase can be implemented by applying the following sequence of matlab operations:

The proposed method 1 and 2 use the same encryption and decryption functions.

The decryption function (Put_operation) will put the sample value in the index pointed by the SIK. While the decryption function (Get_operation) will retrieve the sample using its location in the SIK, Figures 7 and 8 show how to implement the Put_operation and the Get_operation for both methods.

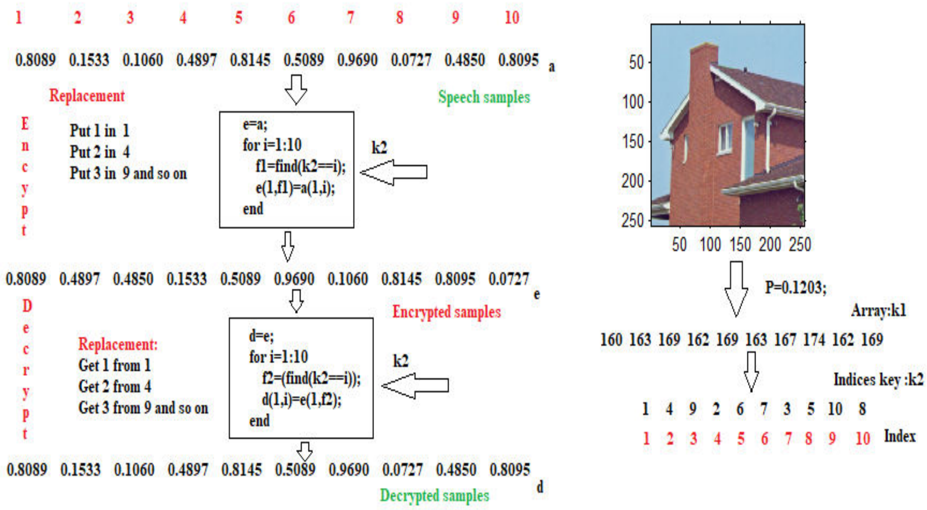

Figure-7. Encryption-decryption for method 2.

VOL. 18, NO. 23, DECEMBER 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

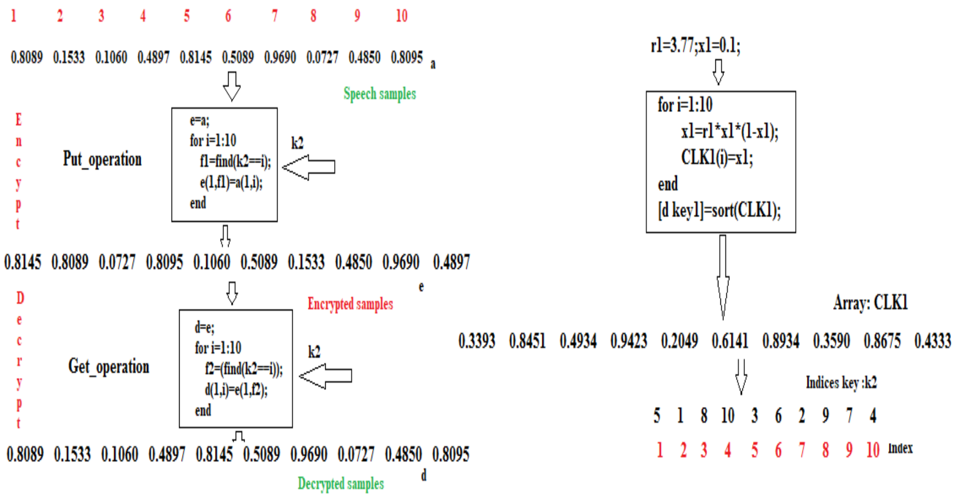

Figure-8. Encryption-decryption for method 1.

The Put_operation (encryption phase) can be implemented by applying the following sequence of matlab instructions:

```
NB=fix(L/BS);
LBS=L-NB*BS;
P=0.1203;
ST=fix(s*P);
 %NB:number of bocks, LBS:last block size
for h=1:NB
   block=sp(1,(h-1)*BS+1:h*BS);
for i=1:BS
   f1=find(k2==i);              %Put_operation
   e1(1,f1)=block(1,i);
end
e(1,(h-1)*BS+1:h*BS)=e1;
end
Lblock=sp(1,NB*BS+1:NB*BS+LBS);
LB1=Lblock;
for i=1:LBS
   f2=find(k4==i);              %Put_operation
   LB1(1,f2)=Lblock(1,i);        for last block
end
e(1,NB*BS+1:NB*BS+LBS)=LB1;
 e1=reshape(e,ddd1,ddd2);
```

The Get_operation (decryption phase) can be implemented by applying the following sequence of matlab instructions:

```
for h=1:NB
   block=e(1,(h-1)*BS+1:h*BS);
for i=1:BS
   f1=find(k2==i);            %Get_operation
   d1(1,i)=block(1,f1);
end
d(1,(h-1)*BS+1:h*BS)=d1;
end
Lblock=e(1,NB*BS+1:NB*BS+LBS);
for i=1:LBS
   f2=find(k4==i);                 %Get_operation
   LB1(1,i)=Lblock(1,f2);          %for the last block
end
d(1,NB*BS+1:NB*BS+LBS)=LB1;
dt=toc;
d1=reshape(d,ddd1,ddd2);
```

3. IMPLEMENTATION AND RESULTS DISCUSSION

The proposed two methods (method1 (using CLMM to generate secret indices key), method2 (Using image_key to generate secret indices key)) were implemented using various selected speech files, the obtained results were analyzed, below the discussion of results analysis will be provided.

a) Speed analysis

The speed of speech cryptography is an important factor used to evaluate the efficiency of cryptography, the speed can be measured by the encryption-decryption time (ET-DT) or by the throughput (TP), which is equal to the number of samples processed in one second (speech size in samples divided by ET in seconds).

Method1 or method2 ET includes key generation time and Put_operation (Get_operation) time. The Put_operation and the Get_operation for the two methods are fixed, but the indices keys used different procedures to generate the indices keys, so the indices key step will be

VOL. 18, NO. 23, DECEMBER 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

analyzed to raise some recommendations regarding method1 and method2.

Several indices keys were generated with various lengths, Table-1 shows the obtained results:

Table-2. Indices key generation time.

Key length (block length in samples)	Indices key generation time using CLMM (second)	Indices key generation time using image_key(second)
100	0.001000	0.028000
500	0.004000	0.029000
1000	0.015000	0.029000
5000	0.069000	0.031000
10000	0.104000	0.031500
25000	0.366000	0.032000
50000	1.425000	0.033000
75000	4.747000	0.036000
100000	11.435000	0.040000
120000	18.219000	0.041000
165670	39.817000	0.047000
315224	171.070000	0.071000

As we can see from Table-2, the key generation time in method1 (using CK) will rapidly increase when increasing the SIK length (see Figure-9), and for speech files (usually, speech file size is big) using this method will be inefficient, here the key generation time will be high and the speed of speech cryptography will be low.

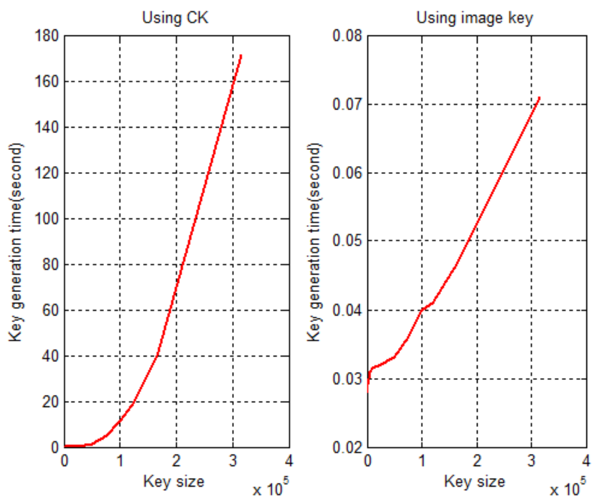

Figure-9. SIK generation time vs key length.

To overcome the problem of a long time of key generation using CLMM, the speech file can be divided into small blocks, and each block will be encrypted-decrypted separately using smaller length SIK. The alternative solution to the previous problem is to switch to the method by using image_key to generate SIK, here even for speech files with big sizes the key generation time will be short (see red and green in Table-2, and see Figure-9).

The Put_operation (encryption phase) and the Get_operation (decryption phase) require an execution w will increase when increasing the block size, so using blocks with small sizes will decrease the encryption-decryption time (key generation time plus encryption-decryption execution time).

Tables 3 and 4 show how using blocking decreases the encryption time and increases the encryption throughput, as is shown in Tables 3 and 4 the speed parameters of method one are very close to the speed parameters of method 2 (see Figure-10), so selecting any of these methods will achieve a good choice.

VOL. 18, NO. 23, DECEMBER 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

Table-3. Method 1 speed parameters (BS=400 samples).

Speech file size(Samples)	Without blocking (method 2)		With blocking(block size=400 samples):method 1	
	ET(second)	TP(Samples per second)	ET(second)	TP(Samples per second)
500	0.0060	83333	0.0060	83330
1000	0.0140	71429	0.0100	100000
5000	0.2670	18727	0.0360	138890
10000	1.0220	9785	0.0700	142860
25000	4.7450	5269	0.1620	154320
50000	18.3520	2724	0.3210	155760
75000	40.9380	1832	0.4730	158560
100000	72.7780	1374	0.7470	133870
120000	104.4460	1149	0.8540	140520
165670	200.0310	828	1.0330	160380
315224	750.5380	420	1.9460	161990
Average	108.4670	17897	0.5144	139130

Table-4. Speed parameters comparisons (method 1 with method 2:BS=400 samples).

Speech file size(Samples)	Using image_key (method 1)		Using CLMK (method 2)	
	ET(second)	TP(Samples per second)	ET(second)	TP(Samples per second)
500	0.0060	83330	0.0100	50000
1000	0.0100	100000	0.0140	71430
5000	0.0360	138890	0.0410	121950
10000	0.0700	142860	0.0730	136990
25000	0.1620	154320	0.1670	149700
50000	0.3210	155760	0.3220	155280
75000	0.4730	158560	0.4780	156900
100000	0.7470	133870	0.6330	157980
120000	0.8540	140520	0.7500	160000
165670	1.0330	160380	1.0360	159910
315224	1.9460	161990	1.9610	160750
Average	0.5144	139130	0.4986	134630

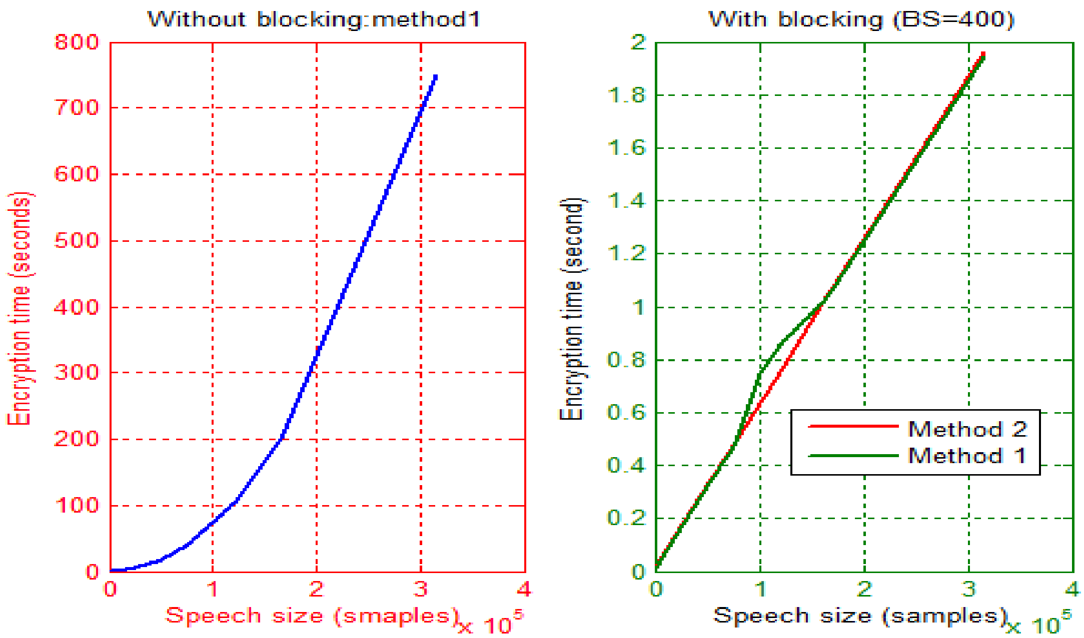

Figure-10. Encryption time comparison.

For both methods it is recommended to use a block with size between 10 and 200 samples, this range will give the best performance, to prove this fact a speech file with 315224 samples was processed by method 1 and method 2 varying the block size, Table-5 shows the obtained speed parameters, while Figure-11 shows how rapidly the encryption time will increase when increasing the block size.

Table-5. Speed parameters when varying block size.

	Method1:Using image_key		Method2:Using CLMM	
Block size	**ET(second)**	**ETP(samples per second)**	**ET(second)**	**ETP(samples per second)**
10	0.5180	608540	0.5410	582670
50	0.5340	590310	0.5270	598150
100	0.6710	469780	0.6470	487210
200	0.8800	358210	0.9050	348310
400	2.0470	153990	2.2210	141930
1000	4.0350	78120	4.1010	76870
2000	7.1260	44240	7.3810	42710
5000	16.6580	18920	16.4310	19180
10000	32.2620	9770	32.2690	9770
20000	46.6120	6760	46.8540	6730
40000	91.0470	3460	91.8040	3430
50000	111.3320	2830	112.9030	2790

VOL. 18, NO. 23, DECEMBER 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

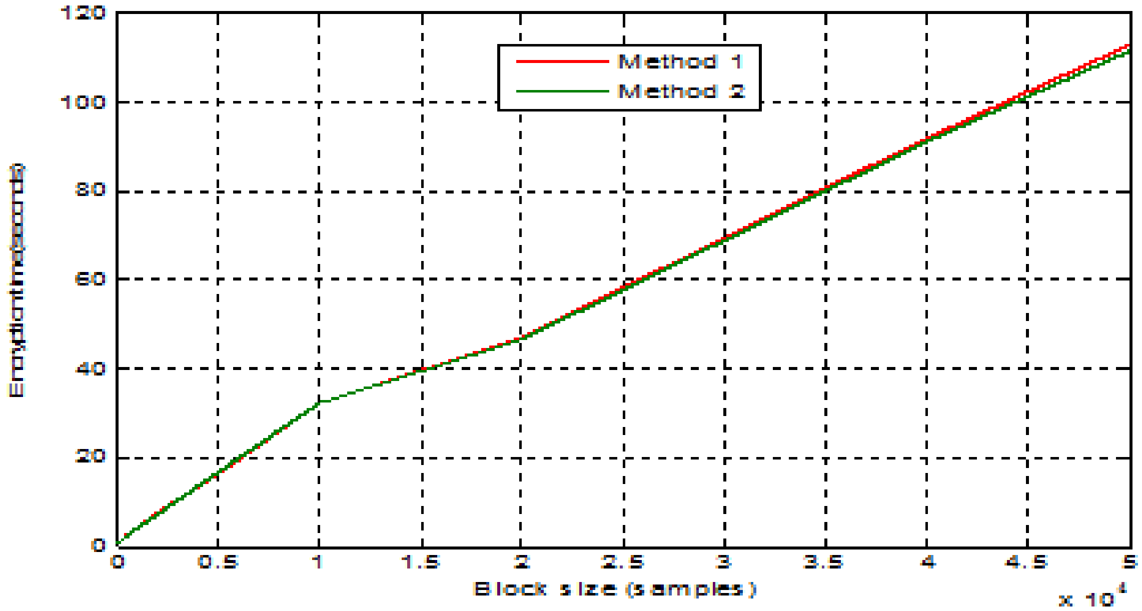

Figure-11. Encryption time VS block size.

Several speech files were selected and processed using method1 and method2, table 6 shows the obtained speed parameters (BS=100:

Table-6. Speed results for method 1 and method 2.

Speech file	Size (samples	Method1		Method2	
		ET(seconds)	**TPT(samples per second)**	**ET(seconds)**	**TPT(samples per second)**
file_example_WAV_1MG.wav	536474	0.6525	822150	0.6542	819990
AMBForst_Forest (ID 0100)_BSB.wav	5218062	5.8454	892670	5.9708	873930
ANMLDog_Barking dog 2 (ID 2954)_BSB.wav	890162	1.0002	889950	1.0307	863680
cat_fight (1).wav	347858	0.4398	790900	0.4196	829040
mix kit-animated-small-group-applause-523.wav	364452	0.4323	843010	0.4180	871800
Average		1.6740	847736	1.6987	851688

AS it is shown in Table-6 method1 and method2 provide a good speed of speech file cryptography, the speed results of these methods were compared with other methods speed, and the results of comparisons show that the proposed methods provided a speedup by decreasing the encryption time, the results shown in Table-7 prove this fact.

VOL. 18, NO. 23, DECEMBER 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

Table-7. Speeds comparisons.

Speech file size (samples)	Lorenz Map [1]	AES (256) [1-2]	Method 2:Using CLMM(block size=100)	Method 1:Using image_key (block size=100)
218880	0.933	4.376	0.4560	0.6480
217150	0.759	4.051	0.4470	0.4450
192380	0.702	3.519	0.3940	0.3960
205630	0.998	3.799	0.4300	0.4730
203900	0.730	4.965	0.4140	0.4180
Average	0.8244	4.1420	0.4282	0.4760
Speed up of method 1	1.9253	9.6730	1.0000	1.1116
Speed up of method 2	1.7319	8.7017	0.8996	1.0000
Speed up of x equals encryption time of y divided by encryption time of x				

b) Quality analysis

Method 1 and method 2 satisfied the quality requirements by producing a damaged encrypted speech file and by producing a decrypted speech file identical to the source speech file. To prove the quality requirements of method 1 we can visually examine the source, encrypted and decrypted file, the speech file 'file_example_WAV_1MG.wav' was encrypted-decrypted using method 1, Figure-12 shows the obtained speech files (blocks size =5000 samples):

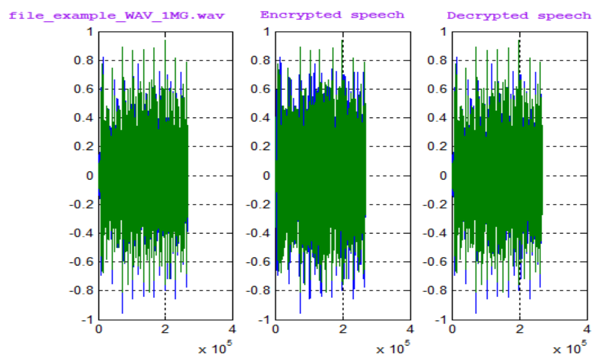

Figure-12. Sample outputs.

As we can see from Figure-12, the wave of the encrypted speech signal was changed. The histograms of the three speech file must be the same, because the samples values do not change in the encryption and decryption files, they are reordered and remain the same, so the histograms will not change, this is shown in Figure-13:

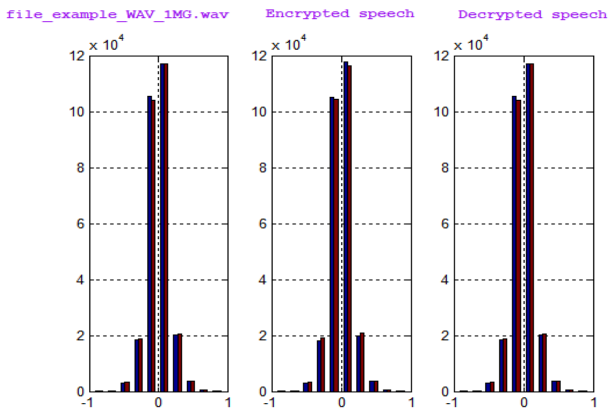

Figure-13. Sample outputs histograms.

The same results were obtained when using method2. The quality of the encrypted and decrypted speeches can be also examined by the calculated quality parameters, Tables 8 and 9 show the obtained encryption quality parameters using method1 and method 2 (BS=5000 samples) (for decryption the quality parameters were always: PSNR=infinite, MSE=0, and CC=1):

Table-8. Obtained quality parameters (method 1).

Speech file	MSE	CC	PSNR
file_example_WAV_1MG.wav	0.0448	-0.00081247	29.8563
AMBForst_Forest (ID 0100)_BSB.wav	0.00037701	0.00042917	51.3686
ANMLDog_Barking dog 2 (ID 2954)_BSB.wav	0.0066	0.0091	43.7216
cat_fight (1).wav	0.1586	0.0010	18.2575
mix kit-animated-small-group-applause-523.wav	0.0655	-0.0019	27.0189
Remarks	High	Low	Low

Table-9. Obtained quality parameters (method 2).

Speech file	MSE	CC	PSNR
file_example_WAV_1MG.wav	0.0448	-0.0013	29.8513
AMBForst_Forest (ID 0100)_BSB.wav	0.00037741	-0.00064118	51.3579
ANMLDog_Barking dog 2 (ID 2954)_BSB.wav	0.0067	43.5988	43.5988
cat_fight (1).wav	0.1588	-0.00022961	18.2450
mix kit-animated-small-group-applause-523.wav	0.0655	-0.0016	27.0220
Remarks	High	Low	Low

c) Sensitivity analysis

In both methods the encryption and decryption functions must use the same PK, any minor changes in the PK in the decryption phase is be considered as a hacking attempt by producing a damaged decrypted speech. To show this the speech file "cat_fight (1).wav" was encrypted using PK1, the encrypted speech was decrypted varying some components of the PK, Table-10 shows the obtained quality parameters of the decrypted speeches:

```
PK1:
Image_key:house.tiff
P=0.1203;
BS=100;
```

Table-10. Method 1 sensitivity.

Changed parameter	Changes	MSE	CC	PSNR	Remarks
No changes	No changes	0	1	Infinite	Correct
Image_key	4.1.05.tiff	0.1563	0.0154	18.4028	Damaged
P	P=0.2203;	0.1510	0.0489	18.7486	Damaged
BS	BS=300	0.1506	0.0515	18.7758	Damaged

For method 2 the following PK was used to encrypt the same speech file, the encrypted speech file was decrypted using the changes shown in Table-1, the obtained decrypted files were damaged when changing the PK.

```
PK:
r1=3.77;x1=0.1;
BS=100
```

Table-11. Method 2 sensitivity.

Changed parameter	Changes	MSE	CC	PSNR	Remarks
No changes	No changes	0	1	Infinite	Correct
r	r=3.87	0.0663	-0.0140	26.8987	Damaged
x	x=0.19	0.0658	-0.0061	26.9775	Damaged
BS	300	0.0668	-0.0206	26.8340	Damaged

d) Security analysis

The method of speech cryptography should be capable of resisting a differential attack. It is one of the most commonly and efficiently used methods by hackers to come across significant information between the plain source data and the cipher encrypted data. NSCR (number of samples changed rate) [1-6]is used to quantify the ability of an encryption method to test the effectiveness of being sensitive when the plain-text data is changed or modified during transmission or any stage by different hacking processes. NSCR determines the change rate in several data items between two data sets, the source data set and the encrypted data set, here NSCP must be closed to 100% [7-16]. This value of NSCR was achieved when dealing with all the tested data sets, results shown in table 1 2, and 3 prove this fact.

Table-12. Calculated NSCR.

Speech file	Calculated NSCR between source and encrypted speeches	Calculated NSCR between source and encrypted speeches
	Method 1	**Method 2**
file_example_WAV_1MG.wav	97.9814	97.9887
AMBForst_Forest (ID 0100)_BSB.wav	96.8128	96.9117
ANMLDog_Barking dog 2 (ID 2954)_BSB.wav	97.0753	97.1832
cat_fight (1).wav	95.5407	95.5108
mix kit-animated-small-group-applause-523.wav	97.7459	97.7739

In addition to NSCR, the proposed method1 and method2 used a complicated PK, the image_key is to be kept in secret and it is impossible to guess or hack. Trying to hack SIK directly will be very difficult, SIK contains BS elements, each of them is an unsigned integer 8 value, and this key will provide a huge key space, which is equal to the factorial of BS. Method 2 PK contains 3 values of double data type and these values provide a key space equal to AES key space which is considered as a secure method of data cryptography.

4. CONCLUSIONS

Two simplified methods of speech cryptography were introduced, the SIK generation required a short sequence of operations, and the Put_operation and the Get operations reduced the number of instructions in the encryption and decryption functions. The generated SIK were very secure and very sensitive, changing the PK in each method changed the generated SIK, and the obtained output speeches were affected.

The speed of the two methods was analyzed and it was recommended to divide the speech file to be encrypted-decrypted into blocks, the block size must be small to achieve a good performance.

The two methods provided good speed values, the results of this two method were compared with other method speed results and it was shown that the two methods provided a speed up by decreasing the encryption-decryption time and increasing the throughput of speech cryptography.

A sensitivity and quality analysis were performed and it was shown that the two methods were very sensitive and satisfied the quality requirements in the encryption and decryption phases.

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] Mahmood K. Ibrahem, Hussein Ali Kassim. 2017. Implementation of VoIP Speech Encryption System Using Stream Cipher with Lorenz map Key Generator, International Journal of Scientific & Engineering Research. 8(7).

[2] P. M. A. S. S. M. M. Ashtiyani. 2012. Speech Signal Encryption Using Chaotic Symmetric Cryptography. Journal of Basic and Applied Scientific Research. 2(2): 1668-1674.

[3] Modified and Efficient Image Encryption Algorithm Based on Chaos Theory. 2016. DNA Complementary Rules and SHA-256, Holmgatan: Master's Thesis to Computer Engineering in Mid Sweden University.

[4] F. M. M. R. A. G. P. G. Alvarez. 2000. Cryptanalysis of a chaotic encryption system. Physics Letters. 276(1): 1- 13.

[5] A. D. S. Eman Hato. 2015. Lorenz and Rossler Chaotic System for Speech Signal Encryption. International Journal of Computer Applications. 128(11): 25-33.

[6] M. Abu-Faraj, A. Al-Hyari, K. Aldebei, B. Al-Ahmad and Z. Alqadi. 2022. Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography. IEEE Access, 10: 69388- 69397, doi:10.1109/ACCESS.2022.3187317.

[7] M. Abu-Faraj, A. Al-Hyari, I. Al-taharwa, B. Al-Ahmad and Z. Alqadi. 2022. CASDC: A Cryptographically Secure Data System Based on Two Private Key Images. IEEE Access, 10: 126304-126314, doi:10.1109/ACCESS.2022.32263

[8] M. Abu-Faraj, A. Al-Hyari and Z. Alqadi. 2022. Experimental Analysis of Methods Used to Solve Linear Regression Models. CMC-Computers, Materials & Continua, 72(3): 5699-5712, doi:10.32604/cmc.2022.027364.

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

[10] 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:10.18280/ts.390117.

[11] M. Abu-Faraj and M. Zubi. 2020. Analysis and Implementation of Kidney Stones Detection by Applying Segmentation Techniques on Computerized Tomography Scans. Italian Journal of Pure and Applied Mathematics. (43): 590-602.

[12] M. Abu-Faraj, Z. Alqadi and M. Zubi. 2022. Creating Color Image Features Based on Morphology Image Processing. Traitement du Signal, 39(3): 797-803, doi:10.18280/ts.390304.

[13] M. Abu-Faraj, Z. Alqadi, B. Al-Ahmad, K. Aldebei and B. Ali. 2022. A Novel Approach to Extract Color Image Features using Image Thinning. Applied Mathematics & Information Sciences (AMIS), 16(5): 665-672, doi:10.18576/amis/160501.

[14] M. Abu-Faraj, A. Al-Hyari, B. Al-Ahmad, Z. Alqadi, B. Ali and A.Alhaj. 2022. Building a Secure Image Cryptography System using Parallel Processing and Complicated Dynamic Length Private Key. Applied Mathematics & Information Sciences (AMIS), 16(6): 1017-1026, 2022,doi:10.18576/amis/160619

[15] M. Abu-Faraj, A. Al-Hyari, I. Al-taharwa, Z. Alqadi and B. Ali. 2023. Increasing the Security of Transmitted Text Messages Using Chaotic Key and Image Key Cryptography. International Journal of Data and Network Science, 7(1): 1-12, doi:10.5267/j.ijdns.2023.1.008.

[16] M. Abu-Faraj, A. Al-Hyari, B. Al-Ahmad, Z. Alqadi, B. Ali and K. Aldebe. 2023. Improving the Efficiency of Median Filters Using Two Rounds of Generated Windows Processing. Applied Mathematics & Information Sciences (AMIS), 17(1): 187-200, doi:10.18576/amis/170119.(Scopus indexed)

[17] Prof. Qazem Jabber Prof. Ziad Alqadi. 2023. Digital Image Cryptography using Index Keys. International Journal of Computer Science and Mobile Computing. 12(2): 26-37.

[18] Hatim Zaini, Ziad Alqadi. 2023. Long Messages Segmentation for Efficient Message Cryptography, IJCSMC. 12(1): 59-69.

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

[20] 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.

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

[22] 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.

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

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

[25] 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.

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

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

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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).

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

[34] 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.

[35] 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.

[36] 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.

[37] 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).

[38] 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.

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

[40] 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).

[41] 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.

[42] 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.

[43] 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).

[44] 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.

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

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

[47] 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.

[48] 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.

[49] Musbah J. Aqel, Ziad Al Qadi, Ammar Ahmed Abdullah. 2018. RGB color image encryption-decryption using image segmentation and matrix multiplication, International Journal of Engineering & Technology. 7(3.13): 104-107.