IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 4, April 2020

A Novel Method to Encrypt-Decrypt Digital Speech Signal (EDDSS)

Dr. Saleh A. Khawatreh[1], Dr. Mohammad S. Khrisat[2], Dr. Amjad Hindi[3], Dr. Majed Omar Dwairi[4], Prof. Ziad Alqadi[5]

Al-Ahliyya Amman University, Jordan, Amman[1]

Albalqa Applied University, Faculty of Engineering Technology, Jordan, Amman[2, 3, 4, 5]

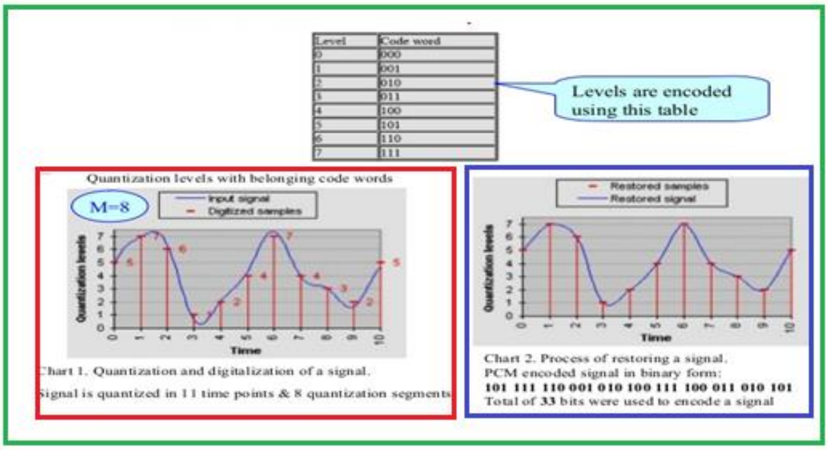
Abstract: Digital speech signal is very famous and important data type; it is used in many important vital applications such as banking systems, protection and security systems, so speech protection is required. In this research paper we will introduce a simplified method of digital speech signal image encryption-decryption; the method will be tested and implemented using various digital speech signals. The proposed EDDSS will change the frequency and amplitude of the original signal, the issues of security, efficiency and accuracy will be discussed; the obtained experimental results will be analysed in order to raise some judgments.

Keywords: DSS, encryption, EDDSS, decryption, FS, SFS, secret range, encryption time, efficiency measures, speedup, throughput, MSE, PSNR.

I. INTRODUCTION

Digital signal such as digital color images [1], [2], [3], [4] and digital speech signals (DSS) 5], [6] are a very important data types used over the internet, they are used in many vital applications such as computer security application [7]. DSS is a two column matrix (stereo speech), or one column matrix (mono speech) [32], [33], [34], the values in each column represent the signal amplitude taken in various times of sampling [7].

DSS can be received from the analogue version of the signal using analogue to digital converter [8], [9], [10]which applies the sampling and quantization operations as shown in figure 1[35],[36].



Level	Code word
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Chart 1. Quantization and digitalization of a signal.
Signal is quantized in 11 time points & 8 quantization segments

Chart 2. Process of restoring a signal.
PCM encoded signal in binary form:
101 111 110 001 010 100 111 100 011 010 101
Total of **33** bits were used to encode a signal

FIGURE 1: SPEECH SAMPLING AND QUANTIZATION.

The number of generated samples in second depends on the sampling frequency (FS) (rate), figure 2 shows the digitize speech using various values of FS [37], [38], [39].

DOI 10.17148/IJARCCE.2020.9419

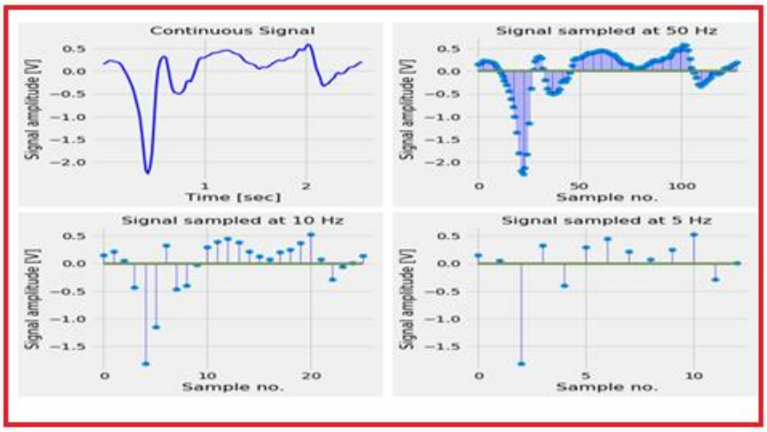


FIGURE 2: DIGITIZE SPEECH USING VARIOUS FS

DSS signal can be manipulated in time or in frequency domains, in time domain we can access the speech amplitude, and in frequency domain we can access both the frequency and the angle magnitudes, figure 3 shows a sample representation of DSS in both amplitude and frequency domains[40], [41], [42].

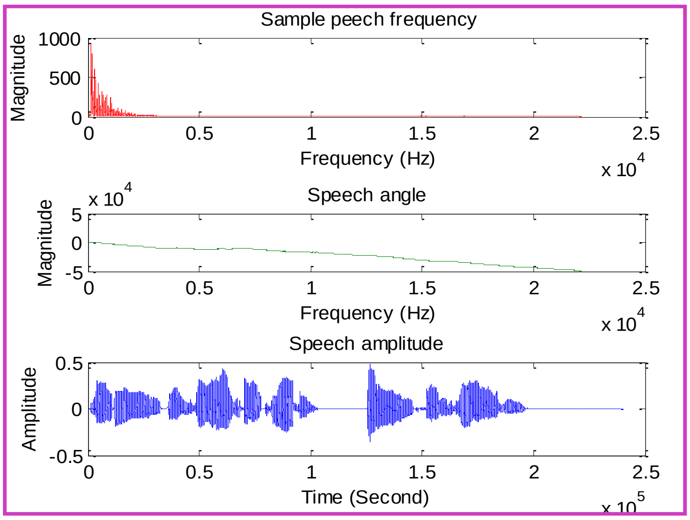


FIGURE 3: DSS IN TIME AND FREQUENCY DOMAINS

II. SPEECH SIGNAL ENCRYPTION DECRYPTION

Digital signals including DSS may be used in some application which requires security, and some time DSS may contain valuable information, which needs good protection, so here the encryption-decryption process is a must. DSS encryption is the process of encoding a speech signal in such a way that only authorized parties can access it and those who are not authorized cannot. The decryption process is to return back the original speech signal without losing any piece of information from the original speech. DSSs are one of the most important types of data currently in the process of messaging through the Internet, which leads us to resort to the use of multiple ways to protect them from parasitism. DSS may be important and has a secret character, which requires not understanding it when hearing it by human ears. In order to do this, we must use a safe and efficient way to encrypt and re-encrypt them so that we can obtain a new DSS that matches the original; figure 4 shows the process of encryption-decryption.

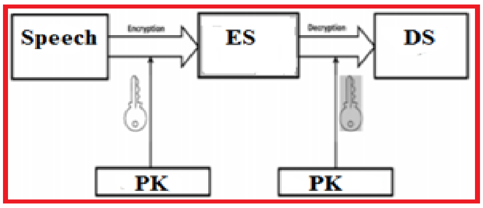


Figure 4: Encryption-decryption process

The efficiency of any encryption-decryption method can be measured by an encryption time (ET) and decryption time (DT) [11], [12], here we can also use a throughput to measure the number of samples encrypted in a second , the protection level can be measured by the damage factors between the original speech and the encrypted one, here we can use mean square error (MSE), or peak-to-signal-noise-ratio (PSNR) , good protection can be achieved when minimizing MSE and maximizing (PSNR) values[13], [14], [15]. Here we can also use the total number of samples in the encrypted signal which were changed.

Any good method for DSS encryption-decryption must have the following features [16], [17], [18]:

- Efficient by minimizing the encryption-decryption times, and maximizing the method throughput and speedup.
- Simple by using simple procedures to handle the process of encryption-decryption.
- Accurate by minimizing mean square error (MSE) and maximizing peak-signal-to-noise-ratio (PSNR) between the original image and the decrypting one, so the decrypted image is completely identical to the original image [20].
- Secure to make it impossible or very difficult to hack the encrypted image, and destroying the original image, so the encrypted image not became understandable to seeing with the eye, here the method must provide a maximum MSE value and a minimum PSNR value [19], [21].

Many methods of digital signals encryption-decryption[23], [24], [25] were proposed, some methods were based on matrix multiplication [22], other methods used blocking feature and xoring [26], [27], in [31] a method based on signal scrambling was introduced, while in [26], [28] the authors used logistic maps to encrypt-decrypt the signal. In [27] the authors used matrix reordering principle, while in [31] the encryption was based on based on 3D Chaotic Cat Maps. In [30] the authors introduced a method based on Rubik's Cube principle; these methods will be implemented to make comparisons with the proposed here method.

III. THE PROPOSED METHOD

The proposed EDDSS method applies encryption-decryption based on the following changes in the original speech signal:

a) Changing the signal frequency:

Here we have to record the speech using a secret sampling frequency (SFS), after reading this signal it must be rewritten by another new frequency sampling (NFS), this rate will be known for the sender and receiver.

b) Changing the speech amplitude:

Here we have to select one or more secret ranges, and according to these ranges the speech signal will be divided into various length segments, each segment samples must be reordered by inverting the samples, figure 5 shows a block diagram of the proposed method.

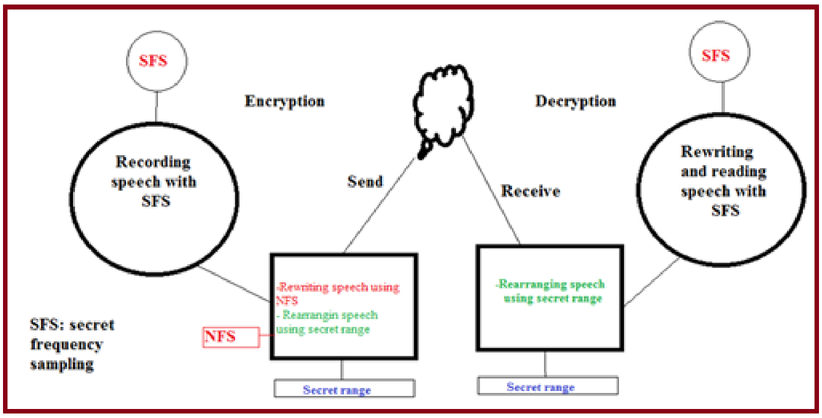

SFS
Encryption
Decryption
SFS
Recording speech with SFS
Send
Receive
Rewriting and reading speech with SFS
-Rewriting speech using NFS
- Rearrangin speech using secret range
-Rearranging speech using secret range
SFS: secret frequency sampling
NFS
Secret range
Secret range

Figure 5: EDDSS operations

So taking the above into consideration the encryption phase will be implemented applying the following steps:

1) Get the original speech signal recorded by SFS.
2) Rewrite the signal using NFS.
3) Get the length of the signal.
4) Reshape the signal into one raw.
5) Decide a secret range.
6) Divide the signal into segment.
7) Invert each segment sample
8) Combine the segments into one signal to form the encrypted signal.

DOI 10.17148/IJARCCE.2020.9419

9) Write the signal using NFS.

The decryption phase will be implemented applying the following steps:

1) Read the encrypted signal.
2) Get the signal length.
3) Reshape the signal into one raw.
4) Get the secret range.
5) Divide the signal into segments according to the ranges.
6) Invert the samples in each segment.
7) Combine the segments into one signal
8) Write the signal using SFS to get the decrypted signal.

IV. Implementation and Experimental Results

The proposed EDDSS was implemented, figures 6, 7, 8 and 9 shows a sample outputs of the implementation:

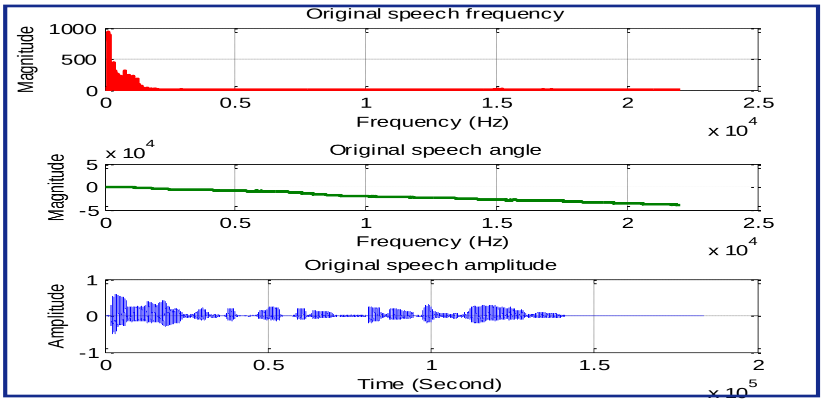


Figure 6: Original speech example

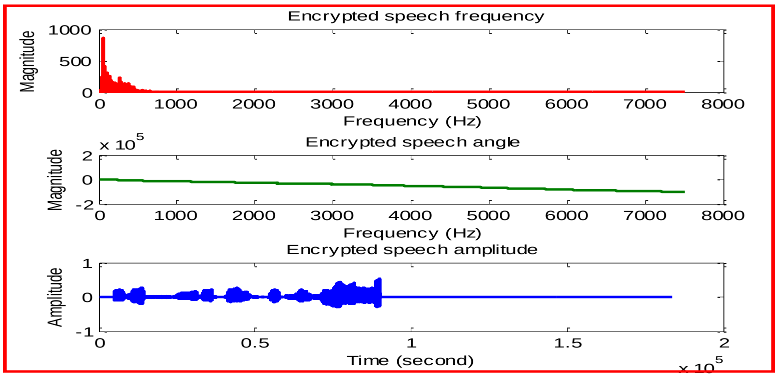


Figure 7: Encrypted speech

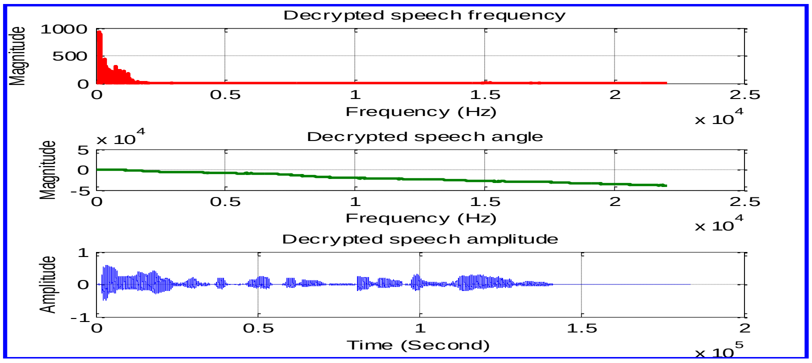
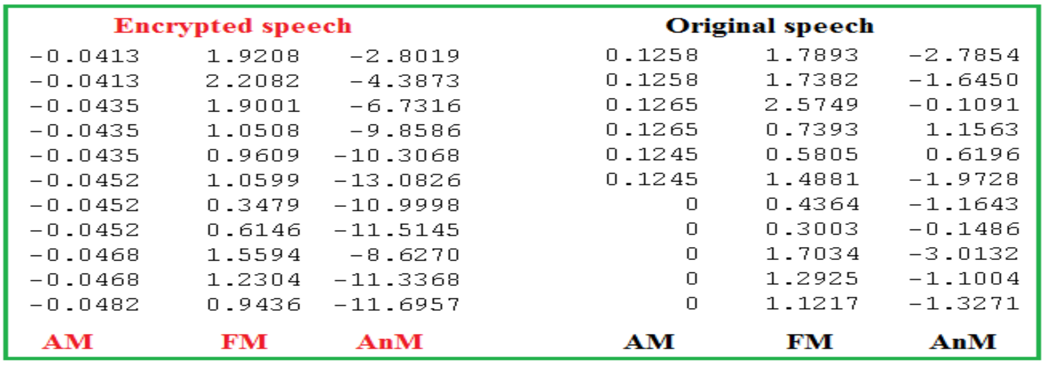


Figure 8: Decrypted signal



```
        Encrypted speech                            Original speech
 -0.0413    1.9208    -2.8019          0.1258    1.7893    -2.7854
 -0.0413    2.2082    -4.3873          0.1258    1.7382    -1.6450
 -0.0435    1.9001    -6.7316          0.1265    2.5749    -0.1091
 -0.0435    1.0508    -9.8586          0.1265    0.7393     1.1563
 -0.0435    0.9609   -10.3068          0.1245    0.5805     0.6196
 -0.0452    1.0599   -13.0826          0.1245    1.4881    -1.9728
 -0.0452    0.3479   -10.9998               0    0.4364    -1.1643
 -0.0452    0.6146   -11.5145               0    0.3003    -0.1486
 -0.0468    1.5594    -8.6270               0    1.7034    -3.0132
 -0.0468    1.2304   -11.3368               0    1.2925    -1.1004
 -0.0482    0.9436   -11.6957               0    1.1217    -1.3271
   AM         FM        AnM             AM        FM         AnM
```

Figure 9: Samples from the encrypted and original signals

From the output figures we can see a minor changes between the original speech signal and the encrypted one, the decrypted signal remain the same as original signal, also when listening to the encrypted signal we see that the encrypted signal was completely damaged and destroyed.

To measure the various factors for the proposed method we implemented the following experiments:

Experiment one: Varying NFS (SFS=44100, range 1000-50000)

Here we took the spoken sentence "My name is Ziad alqadi, i am from Jordan", and run the method by changing NFS, table 1 shows the results of this experiment (file size =238997 samples):

Table 1: Experiment 1 results

NFS	ET	DT	MSE between original and encrypted signals	MSE between original and decrypted signals
1000	0.040000	0.041000	0.0091	0
2000	0.035000	0.046000	0.0091	0
50000	0.040000	0.037000	0.0091	0
10000	0.043000	0.048000	0.0091	0
20000	0.040000	0.041000	0.0091	0
40000	0.040000	0.041000	0.0091	0
60000	0.040000	0.041000	0.0091	0

From table 1 we can see that the method provides a significant small times for encryption-decryption, MSE remain the same for any selected NFS, and the total samples changed in the encrypted speech was around 2175 samples, the obtained decrypted speech was the same as the original one.

Experiment one: Varying NFS (SFS=44100, range 1000-50000)

Here we took the spoken sentence "My name is Ziad alqadi, i am from Jordan", and run the method by changing the range, NFS=10000, table 2 shows the results of this experiment (file size =238997 samples):

Table 2: Experiment 2 results

Range	ET	DT	MSE between original and encrypted signals	MSE between original and decrypted signals
500-10000	0.040000	0.041000	0.0089	0
1000-15000	0.044000	0.033000	0.0089	0
20000-45000	0.047000	0.041000	0.0092	0
500-80000	0.046000	0.037000	0.0092	0
20000-80000	0.037000	0.040000	0.0090	0
40000-60000	0.042000	0.047000	0.0093	0
30000-100000	0.039000	0.038000	0.0092	0

From table 2 we can see that the method provides significant small times for encryption-decryption, changing the range will affect MSE and all the time the encrypted file will be a destroyed version of the original speech.

Experiment 3: We used the speech signals illustrated in table 3, and apply the proposed method using various ranges, and various NFS.

Table 3: Tested speech files

Speech #	Spoken sentence	SFS	Size in samples
1	My name is Ziad AlQadi	8000	43360
2	Amman is the capital city of Jordan	11025	45892
3	Aqaba is a Jordanian city, it is located on red sea	12000	70614
4	Albalqa applied university	16000	56181
5	Faculty of engineering technology	22050	86546
6	Computer engineering department	24000	80779
7	Stay home stay safe	32000	91052
8	Good morning	44100	86627
9	Happy birth day	48000	110944
10	Be healthy, good bye and good luck	48000	197280
Average size			86928
Average time			0.047000
Throughput	47000/86928=0.5407 microsecond for each sample		

The obtained average encryption time was equal 0.041 second and average MSE of 0.009 between the original speech and the encrypted one.

The obtained results were compared with other methods result, and the proposed method has a good improvement as shown in table 4:

Table 4: Methods comparisons

Method	Encryption time (s)	Throughput (M bits)	Speedup of the proposed method	Order
Proposed **EDDSS**	0.047000	64.3117	`1	1
Ref. [22]	0.0513	29.2398	1.0915	2
Ref. [24]	0.06469	23.1876	1.3764	3
Ref. [26]	0.23	6.5217	4.8936	5
Ref. [27]	0.5	3	10.6383	7
Ref. [28]	0.4	3.7500	8.5106	6
Ref. [29]	0.12	12.5000	2.5532	4
Ref. [30] v.1	0.56	2.6786	11.9149	8
Ref [30] v.2	1.01	1.4852	21.4894	9

V. CONCLUSION

A simple, efficient, secure and accurate method of speech signal encryption-decryption was proposed, tested and implemented. The obtained experimental results showed that the proposed methods improves the efficiency factor by decreasing the required times for encryption-decryption and increasing the method throughput, the method destroys the speech signal when encryption and retrieve the same original speech when decryption, the proposed method has some advantages comparing with some existing and has a speedup greater than 1.

REFERENCES

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

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

[3]. 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, issue 1, pp. 86-93, 2019.

[4]. Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7. Issue 3.13, pp. 104-107. 2018.

[5]. Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 465-470, 2016.

[6]. Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications, vol. 975, pp. 8887, 2018.

[7]. 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 9, pp. 4092-4098, 2019.

[8]. Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8. Issue 5, pp. 2780-2787, 2018.

[9]. 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.

[10]. Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, 2016.

DOI 10.17148/IJARCCE.2020.9419

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

[12]. Jihad Nader Ahmad Sharadqh , Ziad Al-Qadi, Bilal Zahran, Experimental Investigation of Wave File Compression-Decompression, International Journal of Computer Science and Information Security, vol. 14m issue 10, pp. 774-780, 2016.

[13]. Ziad A AlQadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

[14]. Majed O Al-Dwairi, A Hendi, Z AlQadi, An efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology & Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.

[15]. Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, A novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp, 232-238, 2019.

[16]. Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, USING SPEECH SIGNAL HISTOGRAM TO CREATE SIGNAL FEATURES, International Journal of Engineering Technology Research & Management, vol. 4, issue 3, pp. 144-153, 2020.

[17]. Majed O Al-Dwairi, A Hendi, Z AlQadi, An efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology & Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.

[18]. Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, A novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp. 232-238, 2019.

[19]. Ziad Alqadi, Ahmad Sharadqh, Naseem Asad, Ismail Shayeb, Jamil Al-Azzeh, Belal Ayyoub, A highly secure method of secret message encoding, International Journal of Research in Advanced Engineering and Technology, vol. 5, issue 3, pp. 82-87, 2019.

[21]. Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, IJCSMC, Vol. 8, Issue 6, pp. 106 –123, 2019.

[21]. Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation, IJCSMC, vol. 8, issue 3, pp. 14-26, 2019.

[22]. 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, issue 1, pp. 86-93, 2019.

[23]. Jamil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION, VOL 3 (2019) NO 3, pp. 262-265.

[24]. S. Wang, Y. Zheng, Z. Gao, “A New Image Scrambling Method through Folding Transform”, IEEE International Conference on Computer Application and System Modelling, Taiyuan, China, October 22-24, 2010.

[25]. J. N. Abdel-Jalil, “Performance analysis of color image encryption\decryption techniques”, International Journal of Advanced Computer Technology, Vol. 5, No. 4, pp. 13-17, 2016.

[26]. G. Ye, “An Efficient Image Encryption Scheme based on Logistic maps”, International Journal of Pure and Applied Mathematics, Vol. 55, No. 1, pp. 37-47, 2009.

[27]. T. Sivakumar, R. Venkatesan, “A Novel Image Encryption Approach using Matrix Reordering”, WSEAS Transactions on Computers, Vol. 12, No. 11, pp. 407-418, 2013.

[28]. H. Gao, Y. Zhang, S. Liang, D. Li, “A New Logistic maps for Image Encryption”, Chaos- Solutions & Fractals, Vol. 29, No. 2, pp. 393- 399, 2006.

[29]. G. Chen, Y. Mao, C. K. Chui, “A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps”, Chaos, Solutions & Fractals, Vol. 21, No. 3, pp. 749–761, 2004.

[30]. K. Loukhaoukha, J. Y. Chouinard, A. Berdai, “A Secure Image Encryption Algorithm Based on Rubik's Cube Principle”, Journal of Electrical and Computer Engineering, Vol. 2012, Article ID 173931, pp. pp. 1-13, 2012.

[31]. X. Wang, J. Zhang, “An Image Scrambling Encryption using Chaos-controlled Poker Shuffle Operation”, IEEE International Symposium on Biometrics and Security Technologies, Islamabad, Pakistan, April 23-24, 2008.

[32]. Ziad Alqadi, Bilal Zahran, Jihad Nader, Estimation and Tuning of FIR Lowpass Digital Filter Parameters, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, issue 2, pp. 18-23, 2017.

[33]. Amjad Y. Hindi, Majed O. Dwairi, Ziad A. AlQadi, Analysis of Digital Signals using Wavelet Packet Tree, IJCSMC, vol. 9, issue 2, pp. 96-103, 2020.

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

[35]. Prof. Yousif Eltous, Dr. Ghazi M. Qaryouti, Prof. Mohammad Abuzalata, Prof. Ziad Alqadi, Evaluation of Fuzzy and C_mean Clustering Methods used to Generate Voiceprint, IJCSMC, vol. 9, issue 1, pp. 75 -83, 2020.

[36]. Prof. Yousif Eltous Dr. Amjad Hindi, Prof. Ziad Alqadi, Dr. Ghazi M. Qaryouti, Prof. Mohammad Abuzalata, Using FIR Coefficients to Form a Voiceprint, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, vol. 8, issue 1, pp. 1-6, 2020.

[37]. Dr. Ghazi M. Qaryouti, Prof. Mohammad Abuzalata, Prof. Yousf Eltous, Prof. Ziad Alqadi, Comparative Study of Voice Signal Features Extraction Methods, *IOSR* Journal of Computer Engineering (IOSR-JCE), vol. 22, issue 1, pp. 58-66, 2020.

[38]. Amjad Y. Hindi, Majed O. Dwairi, Ziad A. AlQadi, Creating Human Speech Identifier using WPT, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 117 – 123, 2020.

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

[40]. Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8, issue 5, pp. 2780, 2018.

[41]. Ziad Alqad, Prof. Yousf Eltous Dr. Ghazi M. Qaryouti, Prof. Mohammad Abuzalata, Analysis of Digital Signal Features Extraction Based on LBP Operator, International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 1, pp. 1-7, 2020.

[42]. Ziad Alqadi, Aws Al-Qaisi, Adnan Manasreh, Ahmad Sharadqeh, Digital Color Image Classification Based on Modified Local Binary Pattern Using Neural Network, IRECAP, vol. 9, issue 6, pp. 403-408, 2019.

DOI 10.17148/IJARCCE.2020.9419