iJETRM
International Journal of Engineering Technology Research & Management

SPEECH SIGNAL ENCRYPTION-DECRYPTION USING NOISE SIGNAL AND PMT

Prof. Yousif Eltous
Dr. Akram Moustafa Hamarchi
Dr. Mohammad S. Khrisat
Dr. Saleh A. Khawatreh
Prof. Ziad Alqadi
Albalqa Applied University, Al Al-Bayt University, Al-Ahliyya Amman University
yousifeltous@yahoo.com
jamarchi@yahoo.com
mkhrisat@bau.edu.jo
skhawatreh@ammanu.edu.jo
natalia_maw@yahoo.com

ABSTRACT
Digital signals, and those including the audio signal, are among the most important types of digital data circulating in the Internet and through various social media.

The digital audio signal may contain confidential information, or the signal may be of a personal nature, which requires preventing its understanding from unauthorized entities or persons and therefore this signal must be encrypted.
In this paper, we will discuss a new method for encrypting the audio signal based on redistributing the signal range values and on adding a specific noise signal.

The method will be run to measure its efficiency and the extent to which it achieves the level of security and protection. We will compare this method with other methods used to indicate the preference of the proposed method.

Keywords:
Speech, PMT, MSE, PSNR, encryption time, decryption time, throughput, speedup, noise.

INTRODUCTION

Digital signals [1], [2], [3], among them the sound [4], [5] and color digital picture[17], [18], are among the most important types of data circulating between people and different institutions because of these types of importance and wide use in many important and vital applications [6], [7], [8].
The digital signal may carry confidential information [22], [23], [24] or it may be of a personal nature [9], [10]. In these cases, it is necessary to prevent people and unauthorized parties from understanding this signal[33], [34] or deciphering it to know the content of the digital signal [35], [36], 37], which requires us to provide a safe way to protect this signal [25], [26], [38].
The audio signal is an analogue signal that is converted into a digital signal through the use of an analogue to digital converter[19]m [20], [21], which applies as shown in figure 1 sampling and quantization operations to get the speech signal samples values [11], [12], [13].

iJETRM
International Journal of Engineering Technology Research & Management

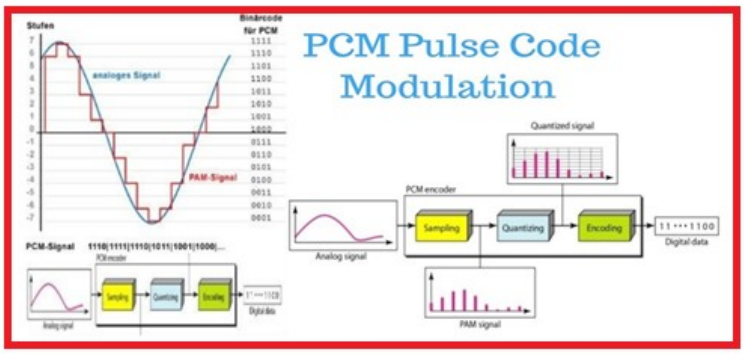

Figure 1: Converting speech analogue signal to digital

Based on the foregoing, the digital audio signal can be dealt with as a single-column array (mono speech) or an array of two columns (stereo speech) consisting of a set of values that indicate the signal range (amplitude) in different time periods [13], [14], and the number of these values (samples) is determined by the frequency ratio (sampling frequency) used in the process of conversion [15], [16].

Signal encryption-decryption methods

Signal encrypting means obtaining a destructive and incomprehensible signal from the original signal [25[, [26], [27]. As for decrypting, it means obtaining a signal that is completely identical to the original signal and without losing any information from it [28], [29]. Many existing method of cryptography are based on using a private key and some arithmetic and logic operations to implement encryption-decryption as shown in figure 2 [30], [31], [32].

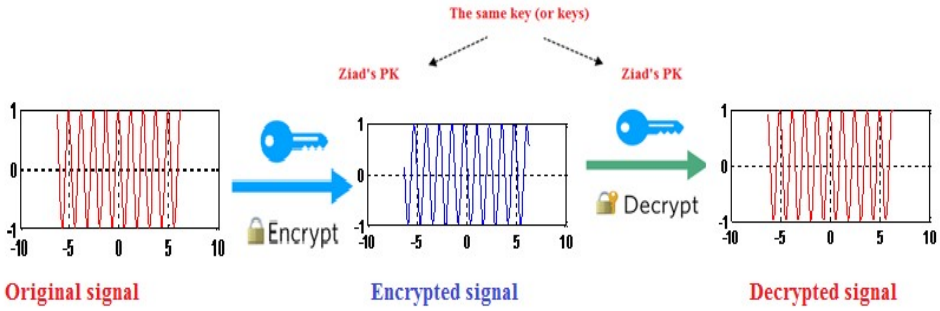

Figure 2: Encryption-decryption process

When using a specific method, the following must be taken into consideration [33], [34], [35]:

- The peak-to-signal ratio between the original signal (PSNR) and the encrypted one must be very low (Mean square error (MSE)) must very high.
- PSNR value between the original signal and the decrypted one must be very high (MSE must be closed to zero).
- Encryption, decryption time must be very small, making the process to increase the throughput (number of samples manipulated in a unit of time (second)) [36], [37], [38].
- The method must provide a high level of security and protection by making the process of hacking impossible or even very difficult [39], [40].

Many methods were introduced to encrypt-decrypt color image, some of these methods were based on image blocking and XORING the created blocks by a private key [31], [32], [33], [35], [41], [45]. In [36], a method based on matrix multiplication of the original image and a special generated private key matrix [30]. In [41] the

iJETRM
International Journal of Engineering Technology Research & Management

authors used matrix reordering principle, while in [43] the encryption was based on based on 3D Chaotic Cat Maps. In [44] the authors introduced a method based on Rubik's Cube principle; these methods will be implemented to make comparisons with the proposed here method.

The proposed method

The proposed method of speech signal encryption-decryption as shown in figure 3 is based on the following:

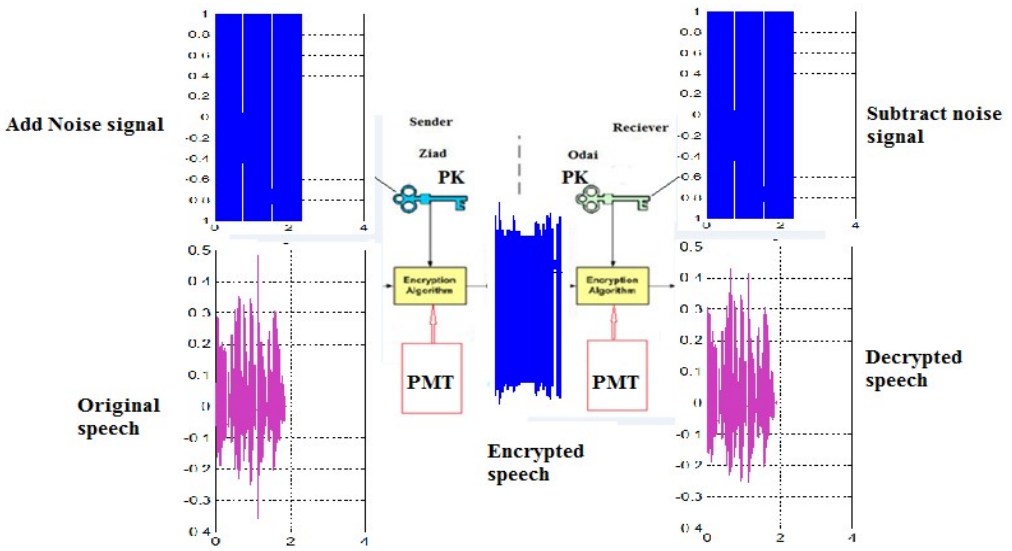

Figure 3: Proposed method block diagram

1) A noise signal of huge number of samples is to be generated, this signal must be saved and it will be used as a private key.
2) From the noise signal we have to extract a segment with size equal the speech signal size, this segment must be added to the original signal.
3) A partition map table (PMT) must be created, this table is to be used as another private key, and it is used to divide the signal into partitions, then the partitions must reordered to get the encrypted signal, table 1 shows an example of used PMT in our experiments:

Table 1: PMT example

Partition number	Location	Size	Order after rearrangement
1	1	2000	3
2	2001	5500	5
3	7501	27500	2
4	35001	60000	4
5	95001	Variable depending on speech size	1

Figure 4 shows how add/subtract a noise signal to/from a simple signal, while figure 5 illustrates the effect of using PMT.

iJETRM
International Journal of Engineering Technology Research & Management

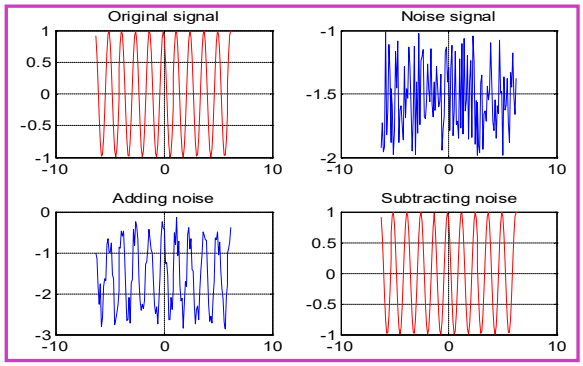

Figure 4: Adding/subtracting noise signal

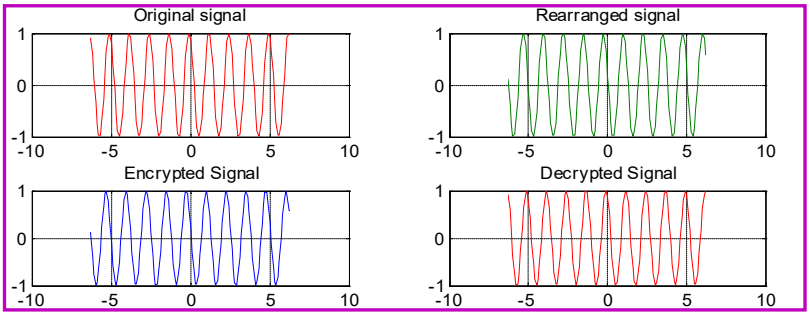

Figure 5: Rearranging the signals using PMT

The proposed method requires an initialization step, in this step we have to generate a noise signal of huge size to cover any treated speech signal, this noise signal is to be saved and kwon for the sender and receiver.

The encryption phase can be implemented applying the following steps:

a) Get the speech signal.
b) Retrieve the signal size.
c) Reshape the signal into one raw matrix.
d) Load the noise signal.
e) Extract a segment from the noise signal with size equal to the speech signal size.
f) Add the extracted noise to the speech signal.
g) Select the partitions (location and size of each partition) by creating PMT.
h) Reorder the partitions and update PMT
i) Save PMT
j) Combine the encrypted signal and reshape it to the original.

The decryption phase can be implemented applying the following steps:

a) Get the encrypted speech signal.
b) Retrieve the signal size.
c) Reshape the signal into one raw matrix.
d) Get PMT

iJETRM
International Journal of Engineering Technology Research & Management

e) Reorder the signal according to PMT.
f) Load the noise signal.
g) Extract a segment from the noise signal with size equal to the speech signal size.
h) Subtract the extracted noise to the speech signal.
i) Combine the decrypted signal and reshape it to the original.

Implementation and experimental results

The proposed method was implemented using various speech signals, figure 6 shows a sample output of one implementation, while figure 7 shows selected set values of each speeches.

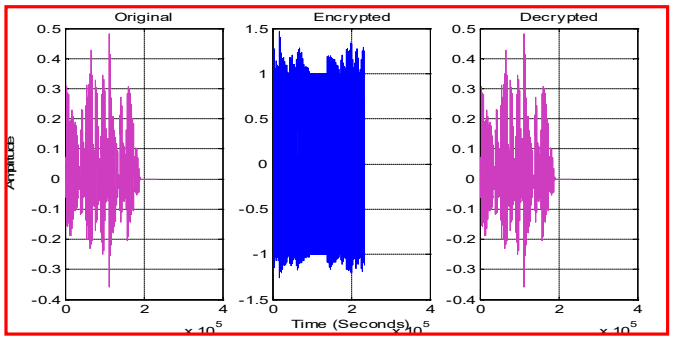

Figure 6: Implementation sample outputs

Original	Encrypted speech signals	Decrypted
-0.0001	0.4983	-0.0001
-0.0001	0.0531	-0.0001
-0.0001	0.1005	-0.0001
-0.0001	0.9336	-0.0001
-0.0000	-0.4309	-0.0000
-0.0000	0.9190	-0.0000
-0.0000	-0.5023	-0.0000
-0.0000	0.2518	-0.0000
-0.0000	1.0328	-0.0000
-0.0000	0.4833	-0.0000
0	-0.3624	0
0	1.0686	0
0	0.7041	0
0.0000	-0.6448	0.0000

Figure 7: Outputs sample values

The proposed method was implemented using the speech files recorded with sampling frequency equal to 48000 samples per second; these speeches represent different spoken sentences, table 2 shows the used in the implementation process speech signals.

Table 2: The used speech signals

Speech number	Spoken sentence	Size (samples)
1	My name is ziad alqadi and I am from Jordan	250809

iJETRM
International Journal of Engineering Technology Research & Management

2	Stay home stay safe	136566
3	Amman is the capital city of Jordan	199778
4	Good morning every one	144600
5	Good evening ladies and gentles men	181909
6	Albalq Applied University	160994
7	Faculty of engineering technology	188378
8	Computer engineering department	161539
9	Communication technology department	173328
10	Digital signal processing, human speeches	245301
Average		184320

During the encryption-decryption processes each speech signal was divided into 5 partitions as shown in the PMT in table 1, the number of partitions can be varied and it is not fixed, but the same partitions must be used in the encryption and decryption phases.

Tables 3 and 4 show the results of implementation:

Table 3: Encryption phase results

Speech #	ET(seconds)	MSE between original and encrypted speeches	PSNR between original and encrypted speeches	Throughput (samples per second)
1	0.0150	0.3447	52.7906	15646000
2	0.0040	0.3441	52.7982	34142000
3	0.0140	0.3442	52.7961	14270000
4	0.0050	0.3430	52.8118	28920000
5	0.0130	0.3431	52.8110	13993000
6	0.0110	0.3458	52.7760	14636000
7	0.0130	0.3419	52.8254	14491000

iJETRM
International Journal of Engineering Technology Research & Management

8	0.0060	0.3422	52.8216	26923000
9	0.0120	0.3415	52.8310	14444000
10	0.0170	0.3442	52.7963	14429000
Average	0.0110	0.3435	52.8058	19189400

Table 4: Decryption phase results

Speech #	ET(seconds)	MSE between original and encrypted speeches	PSNR between original and encrypted speeches	Throughput (samples per second)
1	0.0150	6.6754e-035	389.9200	15646000
2	0.0040	5.0453e-035	391.1359	34142000
3	0.0140	5.6269e-035	390.6621	14270000
4	0.0050	5.4640e-035	390.7897	28920000
5	0.0130	5.7121e-035	390.5969	13993000
6	0.0110	5.9182e-035	390.4429	14636000
7	0.0130	4.9074e-035	391.2563	14491000
8	0.0060	5.2802e-035	390.9383	26923000
9	0.0120	4.4161e-035	391.7144	14444000
10	0.0170	5.6580e-035	390.6382	14429000
	0.0110	5.3365e-035	390.8095	19189400

From the obtained experimental results shown in tables 3 and 4 we can see the following:

- PSNR value between the original speech signal and the encrypted one is low (High MSE), which means that the encryption process destroys the original signal and made it destructive and incomprehensible signal.
- PSNR value between the original speech signal and the decrypted one is high (low MSE), which means that the decryption process generates a signal identical to the original.
- The encryption decryption times are very low, thus the provide method provides a high throughput.

iJETRM
International Journal of Engineering Technology Research & Management

- The provide method provide a high security and protection level by using two keys the noise signal and PMT and it is difficult to know or guess them.
- The propose method has some advantages comparing with other methods results by increasing the process throughput, and it has a speedup always greater than one as shown in table 5

Table 5: Results comparisons

Method	Encryption time (s)	Decryption time (s)	Speedup of the proposed method	Order
Proposed SSEAM	0.0110	0.0110	`1	1
Ref. [29]	0.0513	0.0513	4.6636	2
Ref. [39]	0.06469	0.062727	5.8809	3
Ref. [40]	0.23	0.23	20.9091	5
Ref. [41]	0.5	0.5	45.4545	7
Ref. [42]	0.4	0.4	36.3636	6
Ref. [43]	0.12	0.12	10.9091	4
Ref. [44] v.1	0.56	0.56	50.9091	8
Ref [45] v.2	1.01	1.01	91.8182	9

Conclusion

A simple method of speech signal encryption-decryption was proposed, this method is highly secure and protected by using two keys; the noise signal and PMT. The proposed method was implemented using various speech signals, and the obtained experimental results showed that the proposed is very efficient and it satisfies the requirement of encryption-decryption process.

References

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

[2] Jamil Azzeh, Bilal Zahran, Ziad Alqadi, Salt and Pepper Noise: Effects and Removal, International Journal on Informatics Visualization, vol. 2, issue 4, pp. 252-256, 2018.

[3] 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.

[4]] Ziad AA Alqadi, Investigation and analysis of mat lab models used to solve second order linear ODE, International Journal on Numerical and Analytical Methods in Engineering, vol. 2, issue 1, 2014.

[5] 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.

[6] 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.

[7] 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.
[8] 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.

[9] 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.

[10] 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.

iJETRM
International Journal of Engineering Technology Research & Management

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2019.

[16] Dr. Amjad Hindi Dr. Majed Omar Dwairi Prof. Ziad Alqadi, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

[17] Haitham Alasha'ary, Abdullah Al-Hasanat, Khaled Matrouk, Ziad Al-Qadi, Hasan Al-Shalabi, A Novel Digital

Filter for Enhancing Dark Gray Images, European Journal of Scientific Research , pp. 99-106, 2014.

[18] Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, vol. 8, issue 10, pp. 1175-1182, 2010.

[19] 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, vol. 153, issue 2, pp. 31-34, 2016.

[20] Musbah J. Aqel, Ziad A. Alqadi, Ibraheim M. El Emary, Analysis of Stream Cipher Security Algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.

[21] 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, pp. 20 – 33, 2019.

[22] Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, A Novel Technique for Data Steganography, Engineering, Technology & Applied Science Research, vol. 9, issue 6, pp. 4942-4945, 2019.

[23] Mutaz Rasmi Abu Sara Rashad J. Rasras, Ziad A. AlQadi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, Engineering, Technology & Applied Science Research, vol. 9, issue 1, pp. 3681-3684, 2019.

[24] Dr. Amjad Hindi, Dr. Ghazi M. Qaryouti, Prof. Yousif Eltous, Prof. Mohammad Abuzalata, Prof. Ziad Alqadi, Color Image Compression using Linear Prediction Coding, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 13 – 20, 2020.

[25] 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.

[26] Ziad A. AlQadi, A Highly Secure and Accurate Method for RGB Image Encryption, IJCSMC, vol. 9, issue 2, pp. 12-21, 2020.

iJETRM
International Journal of Engineering Technology Research & Management

[27] Belal Zahran Rashad J. Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, Developing new Multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 6, pp. 3228-3235, 2020.

[28] Ziad Alqad, Majid Oraiqat, Hisham Almujafet, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.

[29] 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.

[30] 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.

[31] 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.

[32] Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Simple and Highly Secure, Efficient and Accurate Method (SSEAM) to Encrypt-Decrypt Color Image, International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, issue 4, pp. 64-69, 2020.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

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

[40] 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.

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

iJETRM
International Journal of Engineering Technology Research & Management

[42] 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.

[43] 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.

[44] 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.

[45] 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.