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. 8, August 2023, pg.45 – 57

Comparative Analysis of using SIK for Message Cryptography

Prof. Ziad Alqadi
Albalqa Applied University, Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2023.v12i08.006

Abstract:

The process of selecting the private key, which is used in the process of generating the secret key to encrypt messages, is one of the most important processes used in the encryption process, which determines the efficiency of the method used in terms of security and speed of implementation, because part of the encryption time is consumed in generating the secret key. In this paper research we will introduce two methods of using private keys to generate a secret index key, the first key will be used a chaotic logistic map model to generate a chaotic key, the chaotic key will be converted to secret index key. The second way is using a color image as an image_key, an array will be extracted from this image, and the array will be converted to secret index key. A simple procedure of message encryption-decryption will be used, this procedure is based on the secret index key, this key will be used to rearrange the message characters' binary bits.

The two approaches of generating secret index key will be implemented using various messages, the obtained results will be analyzed, and the results of analysis will be used to raise some recommendations regarding the message length, security, quality and the speed of message cryptography.

Keywords: Cryptography, CK, CLMM, image_key, SIK, MBM, rearrangement.

Introduction

Text messages are considered one of the most widely circulated types of data through the various means of communication [1-10]. These messages may be private or confidential so that unauthorized persons or entities may not view or understand them, which require providing the necessary protection for them, for the following reasons [11-15]:

- The text message may be confidential and contain highly confidential information, or it may be private and must be hidden from intruders and data thieves.

- Recently, and with the expansion of various communication technologies, the number of data hackers has increased, and their experience in the process of decoding secret messages has increased, and since some communication environments are insecure (see figure 1), data hackers may be able to decipher the message, modify it, and then redirect it to the receiver so that it can It constitutes damage to the future, which requires transforming the communication environment from an insecure environment to a secure environment (see figure 2)that prevents the risk of data hackers [16-21].
- There are a lot of protection tools available in the various means of communication, but there are no bulletins or special information about these tools, which could lead to doubts about the ineffectiveness of these tools.

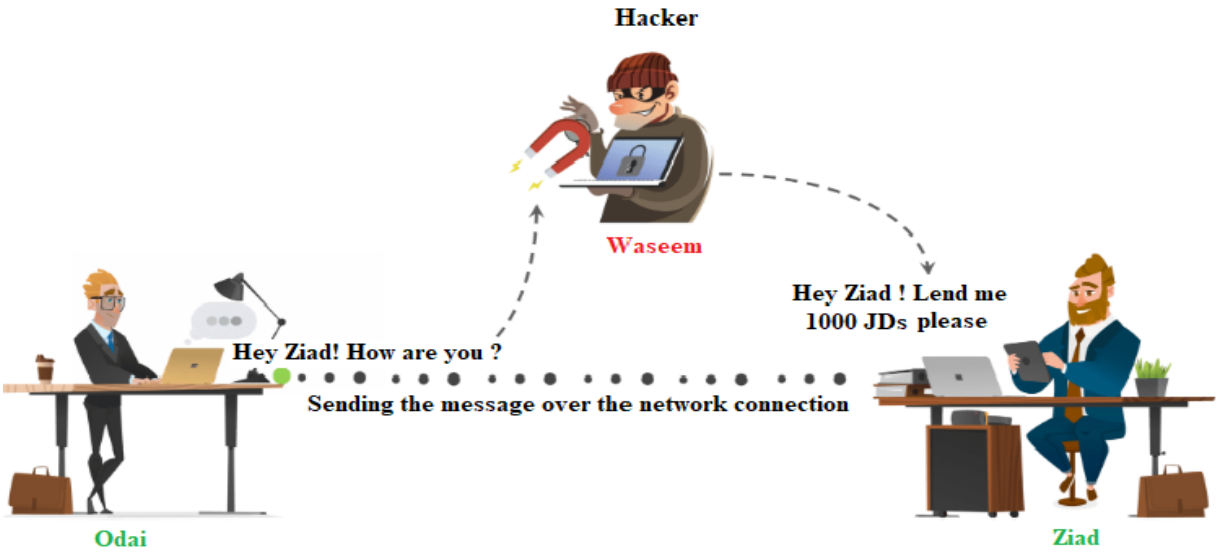

Figure 1: Unsafe communication environment

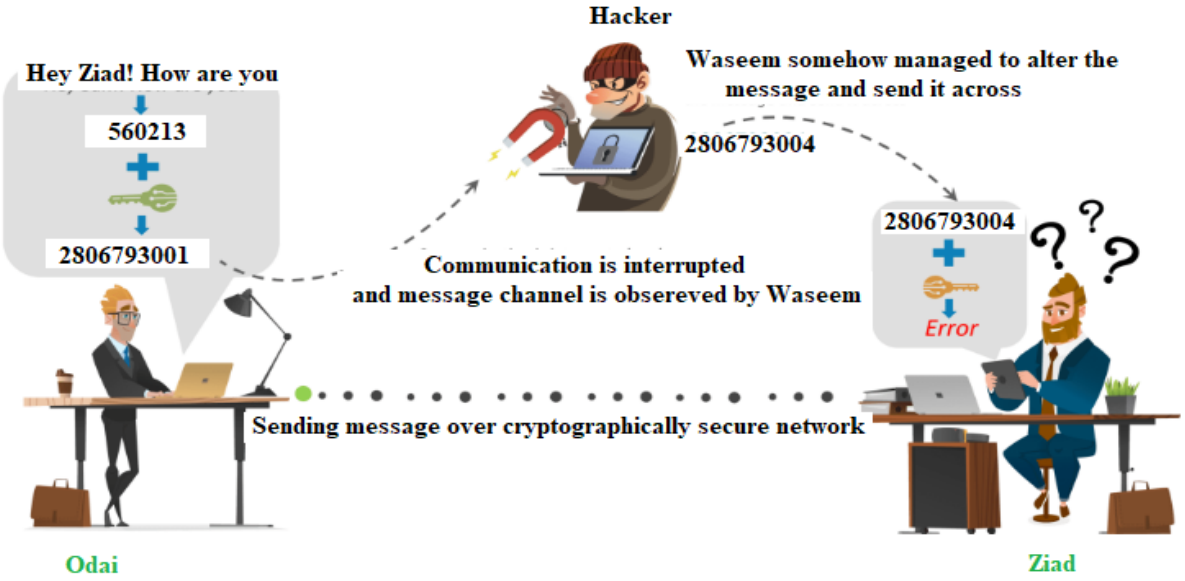

Figure 2: Safe communication environment

One of the easiest and popular methods used to protect secret messages from being hacked is message cryptography [22-30]. Cryptography means encoding the message and converting this message to unreadable corrupted damaged

message in the encryption phase and retrieving a message which is identical to the source message in the decryption phase.

The crypto system as shown in figure 3 contains two parts: the sending part and the receiving part. The sending part uses the encryption function to manipulate the secret message (plain message) and the private key (PK) to produce the encrypted message (cipher message), while the receiver part uses the decryption function to manipulate the cipher message and the PK to produce a decrypted message [31-40].

A good method of message cryptography must meet the following requirements:

- Low quality of the encrypted message, the encrypted message must be corrupted and damaged and unreadable, the quality parameters measured between the source and the encrypted messages must meet the quality requirements listed table 1 [35-40].
- High quality of the decrypted message, the decrypted message must be identical to the source message, the quality parameters measured between the source and the decrypted messages must meet the quality requirements listed table 1 [40-50].
- High speed of cryptography, the method of cryptography must reduce the encryption-decryption time, thus it must increase the throughput of encryption and decryption processes.
- Security, the method must use a PK that provides a huge key space to resist hacking attacks, the results of decryption phase must be sensitive to the selected PK, any changes in the PK in the decryption phase must be considered as a hacking attempt by producing a damaged decrypted message.
- Simplicity and flexibility, the encryption and decryption functions must be simplified, these functions must remain without any changes when changing the input data needed to be encrypted.

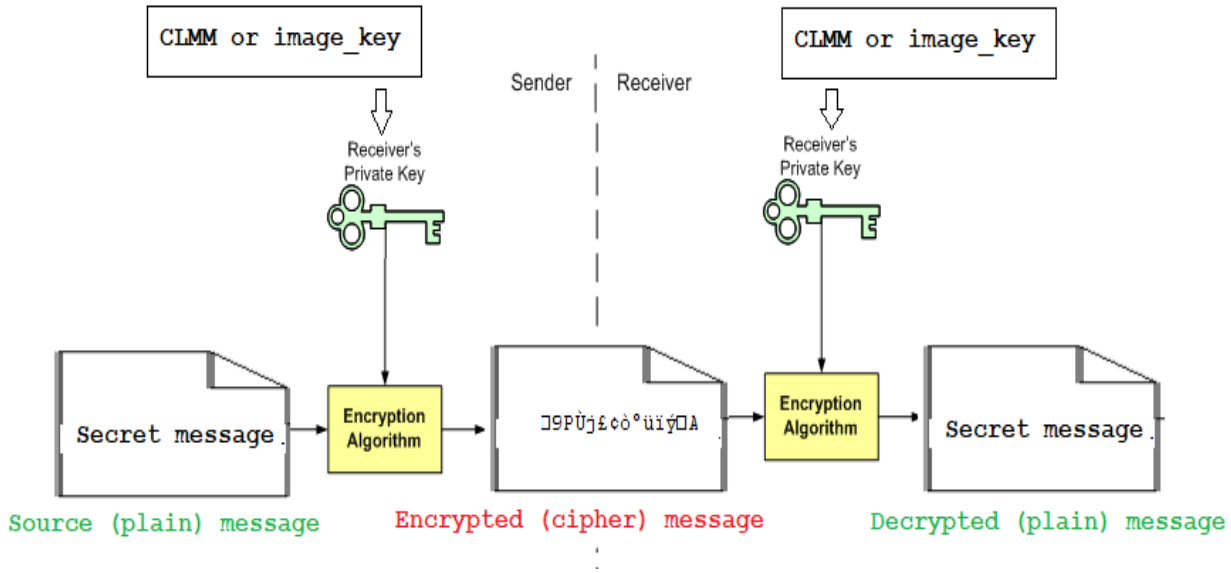

Figure 3: Crypto system components

Table 1: Quality requirements [40-47]

Quality parameter	Measured between source and encrypted messages	Measured between source and decrypted messages
Mean square error (MSE)	High	0
Peak signal to noise ratio (PSNR)	Low	Infinity
Correlation coefficient (CC)	Low	1
Number of characters change rate (NCCR)	High	0

The Proposed Method

The proposed method will use a simplified encryption and decryption functions. Each of these functions will apply message bits' replacement base on the generated secret index key (SIK), the message to be rearranged (replaced) must be treated as follows:

a) Get the message.
b) Retrieve the message length.
c) Convert the message to decimal.
d) Convert the decimal message to binary to get the character's binary matrix (CBM).
e) Reshape CBM to one row matrix.
f) Use the SIK to rearrange the message binary bits.
g) Reshape the message back to 8 column matrix.
h) Convert the message to decimal, then to characters to get the encrypted message.

Figure 4 illustrate an example of producing an encrypted message.

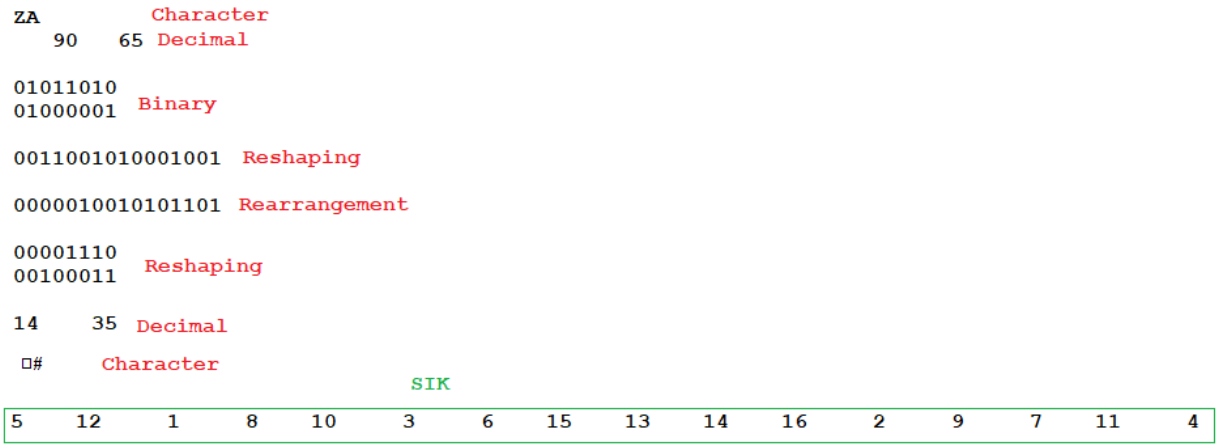

Figure 4: Encryption example

The encrypted message can be converted to decrypted message applying similar steps, figure 5 illustrates an example of decrypting the encrypted message:

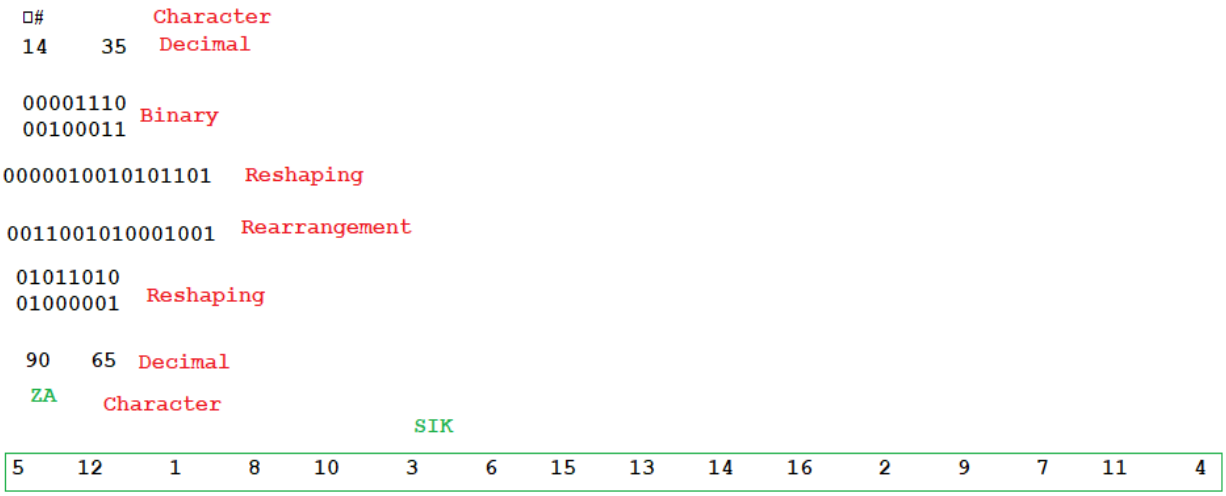

Figure 5: Decryption example

The proposed method uses SIK to apply message binary bits' rearrangement; in this research paper we will analyze two ways of generating this key: the first way is using a color image [55-63] as a PK; the second way is using a chaotic logistic parameter as a PK.

It is very easy to use a color image as an image_key, this image must be kept in secret between the sender and receiver, the key_image must be reshaped to one row matrix, and a part from this image with a size equal the message length multiplied by 8 must extracted from the image, this part must be sorted to get SIK [48-54].

The method can use any image, changing the image will not require any changes in the method. The generated SIK will be very sensitive to the selected image, changing the image will lead to change the SIK contents as shown in figures 6 and 7:

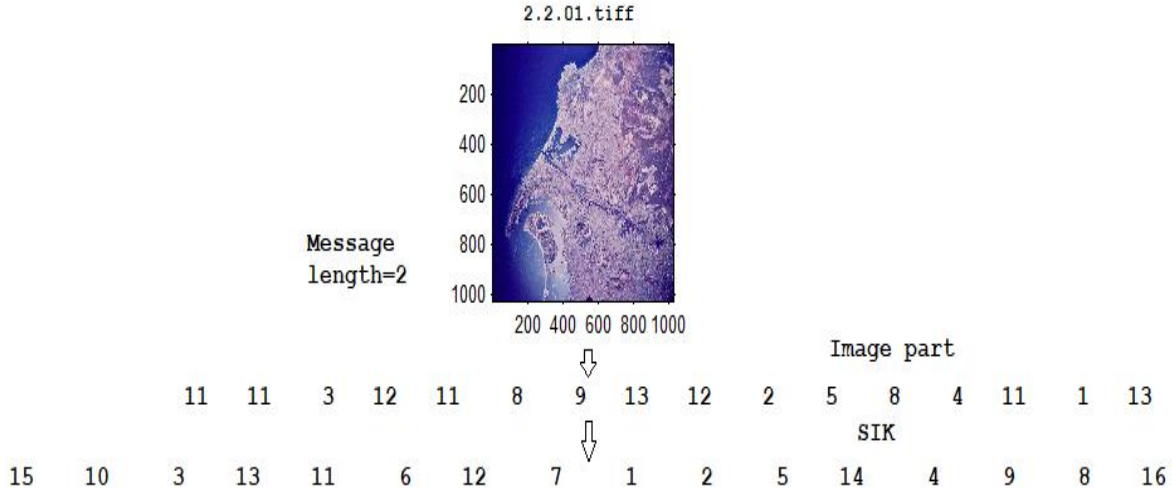

Figure 6: Using image to generate SIK

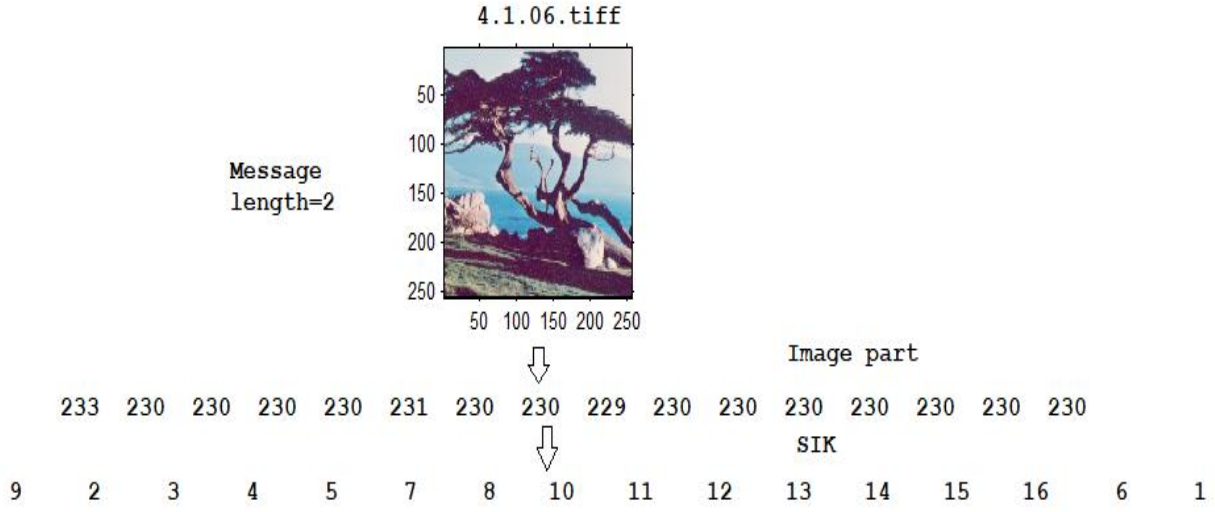

Figure 7: Changing the image_key changes SIK

The second way of generating SIK is using chaotic logistic map model (CLMM), the PK here will contain the chaotic parameters r1 and x1 and the message length, the parameters values are to be used to run a CLMM to generate a chaotic key (CK), this key will be sorted to get the SIK.

The generated SIK using CLMM is also very sensitive to the selected values in the PK.

Implementation and Results Discussion

The proposed method was implemented using various short and long messages, the two ways of SIK generations were tested, below the obtained results will be discussed.

Speed Analysis

One of the most important factors of evaluating a method of message cryptography is a speed of cryptography, the method must increase the speed by increasing the method throughput (number of characters encrypted-decrypted per second), this can be achieved by decreasing both the encryption and decryption times.

A set of long messages were selected and processed using CLMM to generate SIK, table 2 shows the obtained speed parameters:

Table 2: Long messages speed parameters using CK

Message length(characters)	KGT	ET	TET	TP
50000	263.3691	0.5784	263.9475	189
20000	33.6054	0.2404	33.8458	591
15000	15.4202	0.1798	15.6000	962
10000	6.3972	0.1233	6.5205	1534
7500	3.2270	0.0933	3.3202	2259
5000	0.9964	0.0651	1.0615	4710
2500	0.1617	0.0458	0.2075	12048
2000	0.1045	0.0303	0.1347	14848
1000	0.0369	0.0193	0.0561	17825
750	0.0179	0.0165	0.0343	21866
500	0.0090	0.0128	0.0217	23041
400	0.0062	0.0123	0.0185	21622

The same messages were processed using an image_key to generate SIK, table 3 show the obtained results:

Table 3: Long messages speed parameters using image_key

Message length(characters)	KGT	ET	TET	TP
50000	0.0294	0.5949	0.6243	80090
20000	0.0124	0.2449	0.2573	77731
15000	0.0093	0.1844	0.1937	77423
10000	0.0066	0.1245	0.1312	76229
7500	0.0053	0.0980	0.1033	72575
5000	0.0048	0.0660	0.0709	70552
2500	0.0028	0.0362	0.0390	64161
2000	0.0029	0.0304	0.0333	60119
1000	0.0022	0.0180	0.0203	49283
750	0.0023	0.0151	0.0174	43137
500	0.0020	0.0122	0.0142	35186
400	0.0020	0.0111	0.0131	30438

From tables 2 and 3 we can raise the following facts:

- Increasing the message size will require a SIK with big size, generating long CK with big size require a lot of time, and thus the encryption-decryption time will rapidly increase, and her the method will be inefficient (see figure 8).

- It is better to use an image_key to generate SIK when dealing with long message, here we can save a lot of time for key generation and the obtained throughput will be better and the performance of the cryptography process will be enhanced.

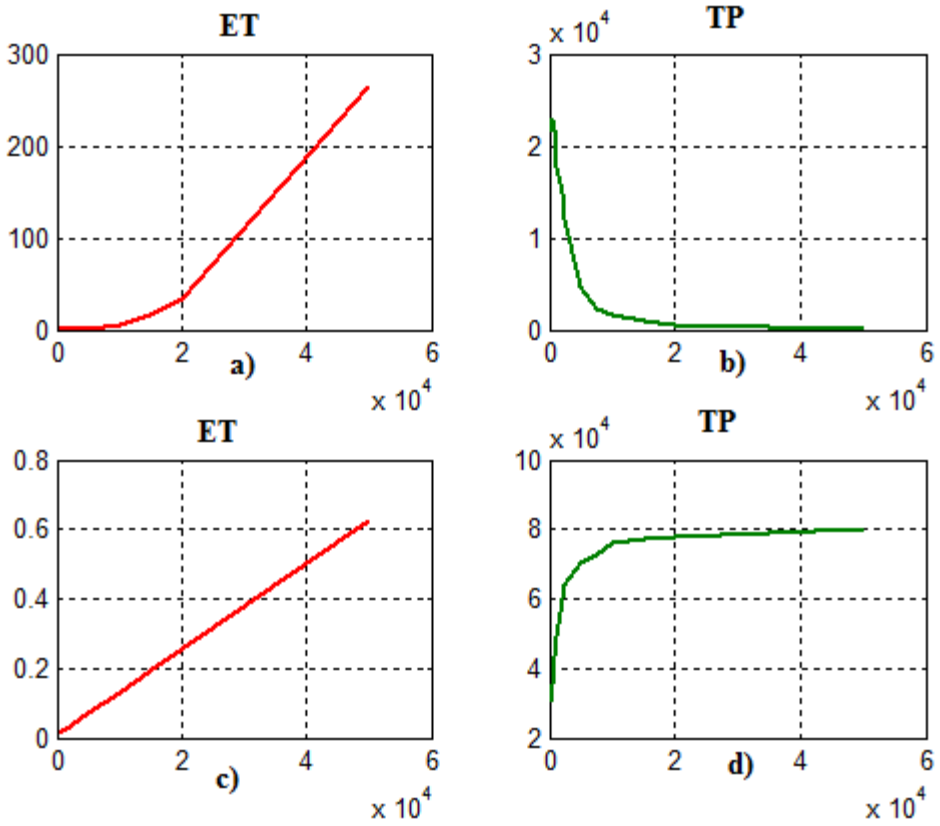

Figure 8: a) ET using CK, b) TP using CK, c) ET using image_key, d) TP using image_key

The previous experiment was repeated for short messages, tables 4 and 5 show the obtained speed parameters values:

Table 4: Short messages speed parameters using CK

Message length (characters)	KGT(seconds)	ET(seconds)	TET(seconds)	TP(characters per second)
10	0.0030	0.0100	0.0130	769.2308
50	0.0050	0.0110	0.0160	3125
100	0.0110	0.0120	0.0230	4347.8
150	0.0230	0.0120	0.0350	4285.7
200	0.0360	0.0130	0.0490	4081.6
300	0.0560	0.0130	0.0690	4347.8
400	0.0580	0.0150	0.0730	5479.5
500	0.0660	0.0160	0.0820	6097.6
750	0.0760	0.0180	0.0940	7978.7
800	0.0770	0.0180	0.0950	8421.1
1000	0.0910	0.0200	0.1110	9009

Table 5: Short messages speed parameters using Image_key

Message length (characters)	KGT(seconds)	ET(seconds)	TET(seconds)	TP(characters per second)
10	0.00100	0.0100	0.0110	909
50	0.00100	0.0120	0.0130	3846
100	0.00100	0.0122	0.0132	7576
150	0.00100	0.0130	0.0140	10714
200	0.00100	0.0135	0.0145	13793
300	0.00100	0.0147	0.0157	19108
400	0.00100	0.01530	0.0163	24540
500	0.00100	0.01610	0.0171	29240
750	0.00100	0.01760	0.0186	40323
800	0.00100	0.0180	0.0190	42105
1000	0.00100	0.0200	0.0210	47619

Here the performance of the method using CK to generate SIK was enhanced but the method performance using image_key still better as shown in figure 9.

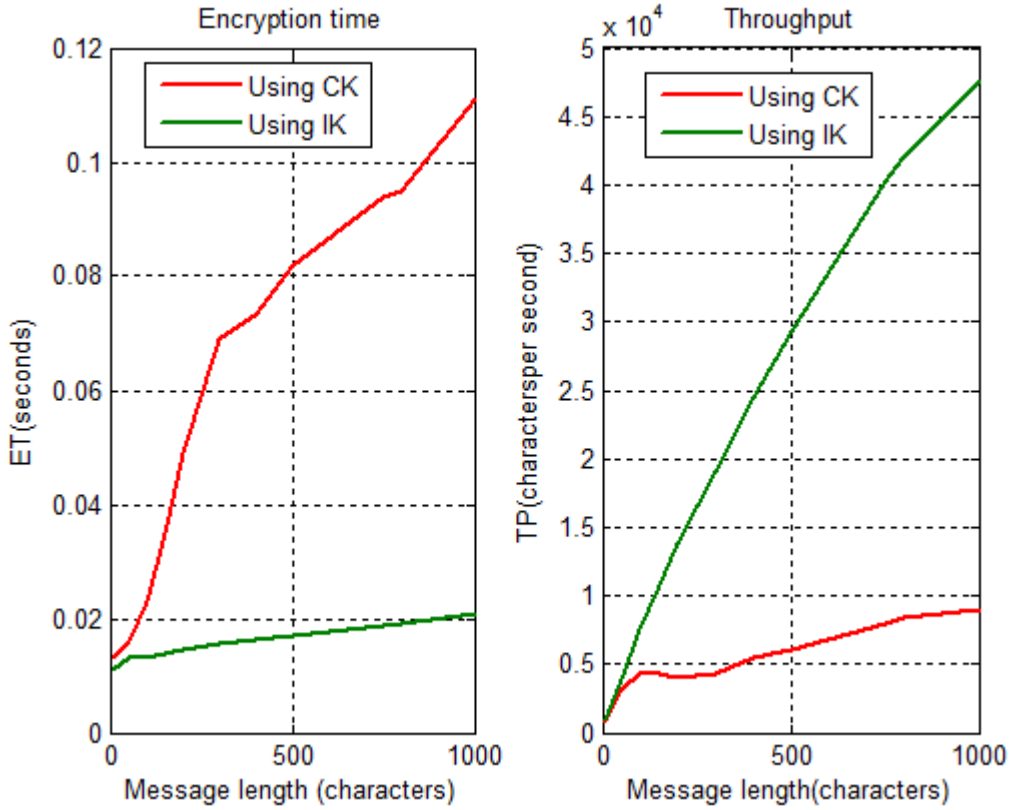

Figure 9: Performances comparisons

Based on the obtained results we can strongly recommend the way of using image_key to generate SIK when dealing with short and long messages. Using CK to generate SIK will give a poor efficiency, and this efficiency can be enhanced when dealing with short messages, but here the method using image_key will give better speed results and it provides a speed up comparing with the method which uses CLMM to generate SIK as shown in table 6, for long messages it is recommended to use image_key and ignore CK as shown in table 7.

Table 6: Speed up of using image_key (for short messages)

Message length	TP using CK	TP using IK	Speed up of using IK
10	769.2308	909	1.1817
50	3125	3846	1.2307
100	4347.8	7576	1.7425
150	4285.7	10714	2.4999
200	4081.6	13793	3.3793
300	4347.8	19108	4.3949
400	5479.5	24540	4.4785
500	6097.6	29240	4.7953
750	7978.7	40323	5.0538
800	8421.1	42105	4.9999
1000	9009	47619	5.2857

Table 7: Speed up of using image_key (for long messages messages)

Message length(characters)	TP using CK	TP using IK	Speed up of using IK
50000	189	80090	423.7566
20000	591	77731	131.5245
15000	962	77423	80.4813
10000	1534	76229	49.6930
7500	2259	72575	32.1270
5000	4710	70552	14.9792
2500	12048	64161	5.3254
2000	14848	60119	4.0490
1000	17825	49283	2.7648
750	21866	43137	1.9728
500	23041	35186	1.5271
400	21622	30438	1.4077

Quality Analysis

The method using each of the two ways of generating SIK was tested for quality, the two ways gave an acceptable results of quality as shown in table 8:

Table 8: Quality parameters measured between source and encrypted messages

Message length(characters)	Used SIK	MSE	PSNR	CC	NCCR
10	CK	**11590**	**15.3562**	**-0.7200**	**100**
	IK	**50575**	**25.5390**	**0.6238**	**100**
50	CK	**12370**	**16.4377**	**-0.0865**	**100**
	IK	**10185**	**18.2222**	**0.1134**	**100**
100	CK	**10320**	**18.4066**	**0.0193**	**100**
	IK	**10181**	**18.5421**	**18.5421**	**100**
1000	CK	**10816**	**17.9375**	**0.0150**	**99.6000**
	IK	**1.0475**	**18.2581**	**0.0217**	**99.5000**
2500	CK	**10953**	**17.8114**	**0.0116**	**99.6800**
	IK	**10768**	**17.9823**	**0.0079**	**99.5600**

5000	CK	**11002**	**17.7670**	**-0.0021**	**99.3200**
	IK	**10822**	**17.9315**	**0.0135**	**99.4200**
Remarks		High	Low	Low	High

Sensitivity Analysis

The method using any of the two ways of SIK generation was tested for sensitivity, changing the chaotic PK parameters in the decryption phase will be considered as a hacking attempt by producing a damaged decrypted message, to show this fact the following message was encrypted using the PK shown below, the encrypted message was decrypted using the changes listed in table 9, as shown in this any changes in the PK will lead to produce a corrupted decrypted message.

The message "Message protection using SIK"

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

Table 9: PK sensitivity using CK

Changing	Changes	Decrypted message
No	-	Message protection using SIK
Yes	r1=3.87	*£□□³¨ú4vÙ□u©s□0&i§å9_□L «QÃ
Yes	x1=.19	□µ□§tf2X□þ□□óG7 i□O¦vÙ¹□ÙT
Yes	r1=3.78; x1=0.11	□□ò}QÈÑ□□®»ë§□s□□□»□Ò□□□□□□□

The same message was processed using image_key, the PK was the image 2.2.01.tiff, the encrypted message was decrypted using other image_keys in the decryption phase, the obtained results show in table 10 shows that the decrypted message is sensitive to the selected PK

Table 10: PK sensitivity using image_key

Used image_key in the decryption phase	Decrypted message
2.2.01.tiff	Message protection using SIK
4.1.05.tiff	WêY&□¥□Ïè□UÀtÖ¦ã·□□78ÐT□ßyB
4.1.06.tiff	IC□i□□Å□a□□9oüAXD P¤Óe÷^ßKÛë
4.2.06.tiff	óØTO´HÒ \Âêëþ2¦ä(o&° □f.ñÑû□
House.tiff	W-Fi^¦□à□i□□ß□×·RAWÂ`6Vz□·Ê

Conclusion

A simple and easy to implement method of message cryptography was presented; the encryption and decryption functions were simplified and used a simple rearrangement of message binary bits based on the generated secret index key, the method was flexible and it was used to process short and long messages, changing the message and/or changing the PK did not require any changes in the encryption and decryption functions. Two ways of SIK generation were tested and implemented, and for speed of cryptography it was shown that using image_key to generate SIK was better than using chaotic key, the CK generation require a lot of time and this will negatively affect the performance of the process of cryptography, for long messages it was recommended to use image_key instead of chaotic key to generate SIK, for short message the use of CK to generate SIK will give a good performance butt also here using image_key will speed up the process of cryptography.

Both ways of SIK generation were tested for quality and sensitivity, and both ways gave good results.

References

[1]. Kaur, R. Dhir, & G. Sikka,"A new image steganography based on first component alteration technique", International Journal of Computer Science and Information Security (IJCSIS), 6, pp.53-56, 2009.http://arxiv.org/ftp/arxiv/papers/1001/1001.1972.pdf

[2]. Alvaro Martin, Guillermo Sapiro, &GadielSeroussi,"Is Steganography Natural", IEEE Transactions on Image Processing, 14(12), pp.2040-2050, 2005.doi: 10.1109/TIP.2005.859370

[3]. Bhattacharyya, A. Roy, P. Roy, & T. Kim,"Receiver compatible data hiding in color image", International Journal of Advanced Science and Technology, 6, pp.15-24, 2009.http://www.sersc.org/journals/IJAST/vol6/2.pdf

[4]. EE. KisikChang, J. Changho, & L. Sangjin,"High Quality Perceptual Steganographic Techniques", Springer. 2939, pp.518-531, 2004.doi: 10.1007/978-3-540-24624-4_42, http://www.springerlink.com/content/c6guuj5xnyy4wj3c/

[5]. C. Kessler,"Steganography: Hiding Data within Data" An edited version of this paper with the title "Hiding Data in Data", Windows & .NET Magazine, 2001. [Online] Available: http://www.garykessler.net/library/steganography.html (October 4,2011)

[6]. Gandharba Swain, &S.K.lenka,"Steganography-Using a Double Substitution Cipher", International Journal of Wireless Communications and Networking. 2(1), pp.35-39, 2010. ISSN: 0975-7163. http://www.serialspublications.com/journals1.asp?jid=436&jtype

[7]. Hideki Noda, MichiharuNimi, &Eiji Kawaguchi,"High- performance JPEG steganography using Quantization index modulation in DCT domain", Pattern Recognition Letters, 27, pp.455-46, 2006.http://ds.lib.kyutech.ac.jp/dspace/bitstream/10228/450/1/repository6.pdf

[8]. Kathryn, "A Java Steganography Tool", 2005.http://diit.sourceforge.net/files/Proposal.pdf

[9]. Motameni, M.Norouzi, M.Jahandar, & A. Hatami,"Labeling method in Steganography", Proceedings of world academy of science, engineering and technology, 24, pp.349-354, 2007. ISSN 1307-6884. http://www.waset.org/journals/waset/v30/v30-66.pdf

[10]. Mohammed A.F Al Husainy, "Message Segmentation to Enhance the Security of LSB Image Steganography", International Journal of Advanced Computer Science and Applications, 3(3): 57-62, 2012.http://www.ijacsa.thesai.org

[11]. Mohammed A.F Al Husainy, "Developed Segmented LSB Image Steganography", International Science and Technology Conference (ISTEC 2012), Dubai, December 13-15, 2012. http://www.iste-c.net

[12]. Afjal H. Sarower; Rashed Karim; Maruf Hassan, An Image Steganography Algorithm using LSB Replacement through XOR Substitution, Computer Science:2019 International Conference on Information and Communications Technology (ICOIACT), DOI:10.1109/icoiact46704.2019.8938486.

[13]. Rashad J. Rasras1, Mutaz Rasmi Abu Sara2, Ziad A. AlQadi3, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3 ,2019, https://doi.org/10.30534/ijatcse/2019/64832019

[14]. 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 Journal8 (10): 1175-1182, ISSN 1818-4952.

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

[16]. Akram A. Moustafa and Ziad A. Alqadi, Color Image Reconstruction Using A New R'G'I Model, Journal of Computer Science 5 (4): 250-254, 2009 ISSN 1549-3636.https://doi.org/10.3844/jcs.2009.250.254

[17]. Musbah J. Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering & Technology, 7(3.13) (2018) 104-107.https://doi.org/10.14419/ijet.v7i3.13.16334

[18]. Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein,A COMPARISON BETWEEN PARALLEL ANDSEGMENTATIONMETHODS USED FOR IMAGE ENCRYPTION-DECRYPTION International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5,October 2016.

[19]. Khaled Matrouk, Abdullah Al- Hasanat, HaithamAlasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi, Analysis of Matrix Multiplication Computational Methods, European Journal of Scientific Research, ISSN 1450-216X / 1450-202X Vol.121 No.3, 2014, pp.258-266.

[20]. Ziad A.A. Alqadi, Musbah Aqel, and Ibrahiem M. M. ElEmary, Performance Analysis and Evaluation ofParallel Matrix Multiplication Algorithms, World Applied Sciences Journal 5 (2): 211-214, 2008.

[21]. Z Alqadi, A Abu-Jazzar, Analysis of program methods used in optimizing matrix multiplication, Journal of Engineering, 2005.

[22]. Musbah J. Aqel , Ziad A. Alqadi, Ibraheim M. El Emary, Analysis of Stream Cipher Security Algorithm, Journal of Information and Computing Science Vol. 2,No. 4, 2007, pp. 288-298.

[23]. 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.

[24]. 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.

[25]. 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.

[26]. Emam, M. M., Aly, A. A., & Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science &Applications,1(7), pp. 361-366, (2016). https://doi.org/10.14569/IJACSA.2016.070350

[27]. Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Modified Inverse LSB Method for Highly Secure Message Hiding, IJCSMC, Vol. 8, Issue.2, February 2019, pg.93 – 103

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

[29]. Zhou X, Gong W, Fu W, Jin L. 2016An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15thInt. Conf. on Computer and Information Science (ICIS), Okayama, Japan, pp. 1–4 .https://doi.org/10.1109/ICIS.2016.7550955

[30]. Wu D-C, Tsai W-H. A stenographic method for images by pixel value differencing. Pattern Recognition. Lett. 24, 1613–1626. 2003https://doi.org/10.1016/S0167-8655(02)00402-6

[31]. Das R, Das I. Secure data transfer in IoT environment: adopting both cryptography and steganography techniques. In Proc. 2nd Int. Conf. on Research in Computational Intelligence and Communication Networks, Kolkata, India, pp. 296–301, 2016.https://doi.org/10.1109/ICRCICN.2016.7813674.

[32]. M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.

[33]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

[34]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022.

[35]. M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Pur- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.

[36]. 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.

[37]. M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

[38]. M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- ods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.

[39]. Abdullah N. Olimat, Ali F. Al-Shawabkeh, Ziad A. Al-Qadi, Nijad A. Al-Najdawi, Forecasting the influence of the guided flame on the combustibility of timber species using artificial intelligence, Case Studies in Thermal Engineering, Volume 38, 2022, 102379, ISSN 2214-157X, https://doi.org/10.1016/j.csite.2022.102379.

[40]. M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.

[41]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

[42]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022.

[43]. M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purr- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.

[44]. 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.

[45]. M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- odds for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.

[46]. J. Vilkamo and T. Bäckström, "Time-Frequency Processing: Methods and Tools," in Parametric Time-Frequency Domain Spatial Audio, V. Pulkki, S. Delikaris-Manias, and A. Politis, Eds. Wiley, 2017, pp. 3–24.

[47]. 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.

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

[49]. 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.

[50]. 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.

[51]. 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.

[52]. 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.

[53]. 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.

[54]. 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.

[55]. 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.

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

[57]. 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.

[58]. 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.

[59]. 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.

[60]. 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.

[61]. 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.

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

[63]. M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

