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. 13, Issue. 8, August 2024, pg.86 – 98

Message Cryptography using Two Round of Message Reordering

Prof. Ziad Al Qadi

Albalqa Applied University, Faculty of Engineering Technology, Amman Jordan

DOI: https://doi.org/10.47760/ijcsmc.2024.v13i08.010

Abstract:

A highly secure method of message cryptography will be introduced, the method will use a complicated PK, which will provide a high entropy space capable to resist hacking attempts, and the produced decrypted message will be very sensitive to the selected values of the PK components. The PK will be used to generate two chaotic keys; these keys will be converted to indices key to be used to reorder the message contents at the character level and at the bit level. The encryption-decryption process will be implemented in two rounds: the first round will be used to reorder the message characters, while the second round will be used to reorder the message blocks of bits. The PK will be also used to divide the message array of bits to equal blocks.

The introduced method will simplify the process of message cryptography by applying simple reordering operations and eliminating the need to use a complex og logical operations used in other methods of message cryptography.

The proposed method will be implemented and tested using various short, medium and long messages, the obtained results will be analyzed to prove the enhancements provided by the proposed method in: speed, quality and sensitivity of message cryptography.

Keywords: Cryptography, cipher message, MAC, MAD, MBM, MAB, PK, CK, IK.

Abbreviations

EF: Encryption function.
DF: Decryption function.
ET: Encryption time.
ETP: Encryption throughput.
DTP: Decryption throughput.
MAC: Message array of characters.
MAD: Message array of decimals.
MBM: Message binary matrix.

MAB: Message array of bits.
PK: Private Key.
CK: Chaotic key.
IK: Indices key.
CLMM: Chaotic logistic map model.
MSE: Mean square error.
PSNR: Peak signal to noise ratio.

Introduction

1. Text message

Text message [1-10] is an array of characters; it can be easily converted to decimal to form the message array of decimals (MAD). MAD can be easily converted to binary to form the message binary matrix (MBM). MBM is a 2D matrix with 8 columns and one row for each character. MBM can be also easily reshaped one row matrix to form the message array of bits (MAB) as shown in figure 1 [11-15].

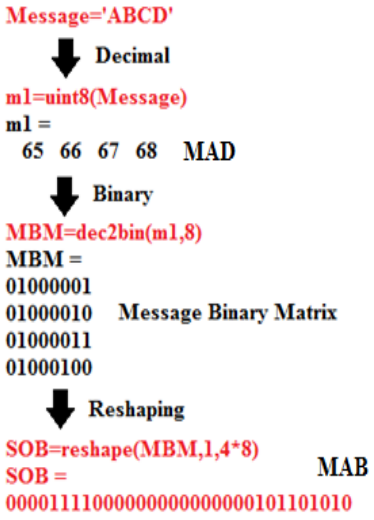

Figure 1: Converting message to MAB

Reversing the previous operations we can easily convert MAB to characters as shown in figure 2:

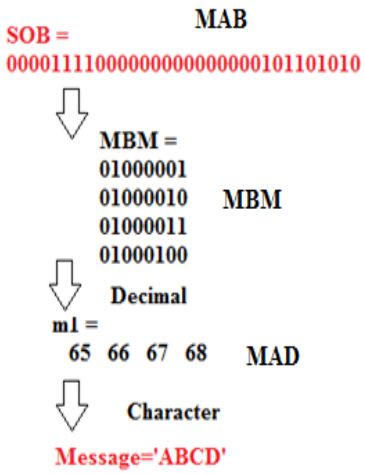

Figure 2: Converting MAB to characters

2. Indices keys generation

The indices key is a set of decimal unsigned non repeated values, and it can be obtained by sorting a set of another values. In the proposed method a chaotic logistic array will be used to form the indices key [16-20].

The PK will contain two sets of chaotic logistic parameters (r1, x1, r2 and x2), these parameters will used to run CLMM to generate two CKs. CKs will be sorted to get two indices keys. The length of the IKs will equal the message length, while the length of the second IKs will equal the number of blocks obtained by dividing the length of MBM by the block size [21-27],

CK has the following features:

- Easy to generate, applying the chaotic equation using the values of r and x parameters and the length of CK we can get the CK, sorting this key will produce the IK as shown in the sequence of mat lab operations shown in figure 3 [28-32]:

```
r1=3.77;x1=0.11;
r2=3.68;x2=0.17;
for i=1:messagelength
    x1=r1*x1*(1-x1);  Chaotic logistic equation
    CK1(i)=x1;
end
[ff IKEY1]=sort(CK1);
for i=1:numberofblocks
    x2=r2*x2*(1-x2);   Chaotic logistic equation
    CK2(i)=x2;
end
[ff IKEY2]=sort(CK2);
```

Figure 3: IK generation sequence of operations

- IK is very sensitive to the selected values of the PK, any minor changes in the PK components will change the generated IK as shown in figure 4 [33-40]:

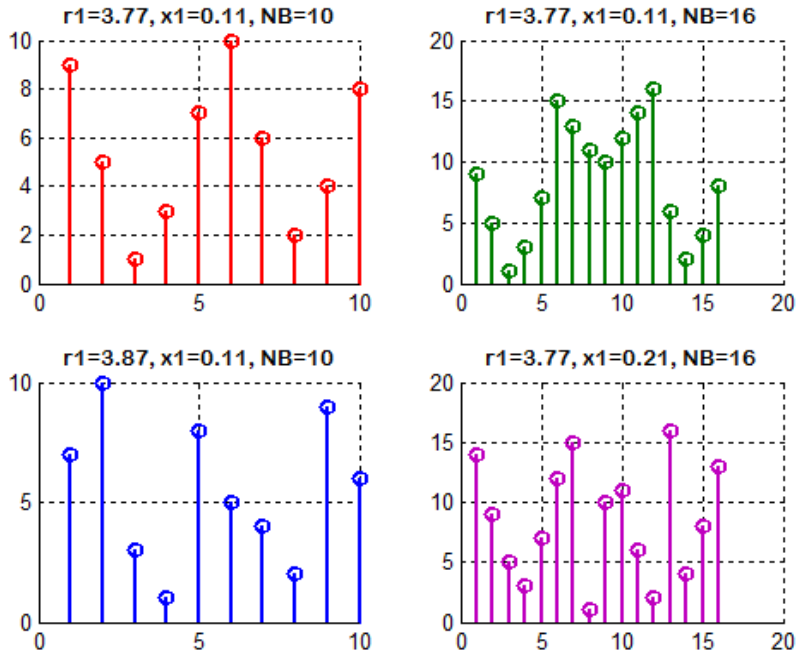

Figure 4: Changing the PK will change the generated IKs

3. Message reordering

The message reordering process will applied at the characters and the bits level. At the character level the encrypted message can be obtained by reordering the message characters based on the contents of IK1, the content of the IK1 points to the index where to put the associated character, while the decrypted message can be obtained based on the content of the IK1 [41-46], the content will point to the position where to get the associated character as shown in figure 5.

```
m='ABCDEFGHIJ';                          IKEY1= 9  5  1  3  7  10  6  2  4  8

for i=1:LM
c=IKEY1(i);       Encryption       Put 1 in 9, 2 in 5, and so on
m1(c)=m(i);
end
m1=CHDIBGEJAF ;   Encrypted message
for i=1:LM
c=IKEY1(i);     Decryption       Get from 9 , get from 5 and so on
m2(i)=m1(c);
end
m2=ABCDEFGHIJ   ; Decrypted message
```

Figure 5: Message reordering at the character level

The message reordering at the bit level requires converting the message to MAB, this array must be devided into equal blocks, the blocks will be reordered based on the contents of IK2 using the same procedures as in message reordering at the character level, figure 6 illustrate an example of MAB reordering [47-52]:

```
BS=6; NB=6
 B1     B2     B3     B4     B5     B6                          IKEY= 3  4  1  2  6  5
00001  11100  00000  00000  00010  11010  10     m3
e1=m3;
for i=1:6          Encryption   Put in 3, then put in 4 and so on
   c=IKEY(i);
      e1(1,1+BS*(i-1):i*BS)=m3(1,1+BS*(c-1):c*BS);
end
00000  00000  00001  11100  11010  00010  10          Encrypted
d1=e1
for i=1:6          Decryption   Get from 3, then get from 4 and so on
   c=IKEY(i);
      d1(1,1+BS*(c-1):c*BS)=m3(1,1+BS*(i-1):i*BS);
end
00001  11100  00000  00000  00010  11010  10          Decrypted
```

Figure 6: Message reordering at the bit level

4. Message cryptography

Message cryptography means encrypting and decrypting the message [53-60]. The encryption process as shown in figure 7 is implemented using the encryption function, which processes the source message and the PK to produce a cipher encrypted message. The decryption process as shown in figure 8 is implemented using the decryption function, which processes the cipher message and the PK to produce a decrypted message [61-70].

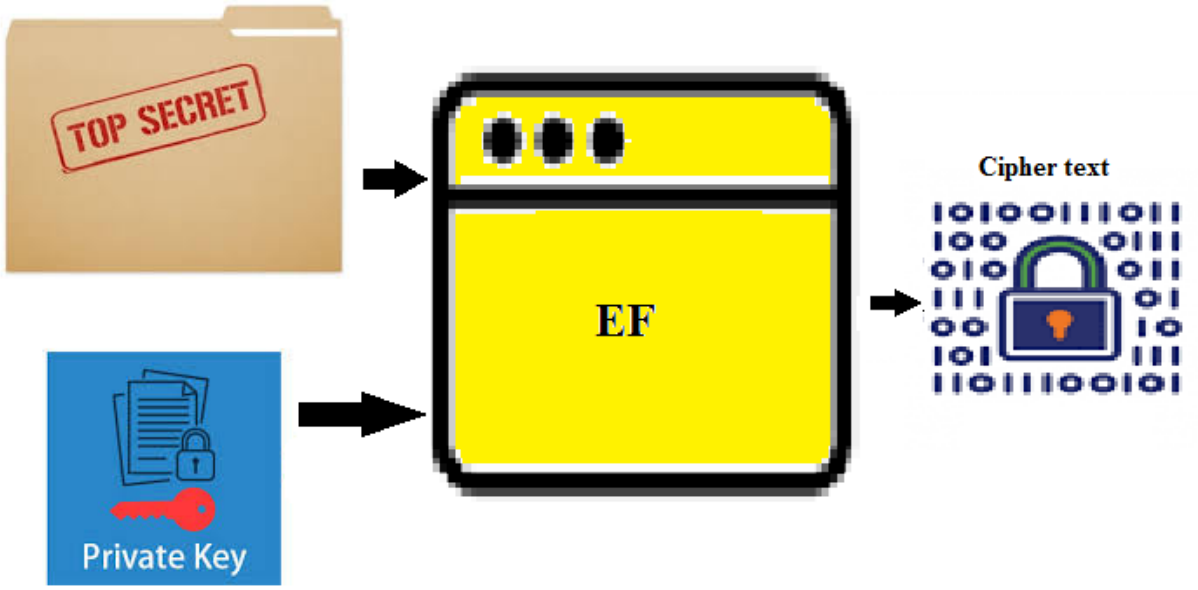

Figure 7: Encryption process diagram

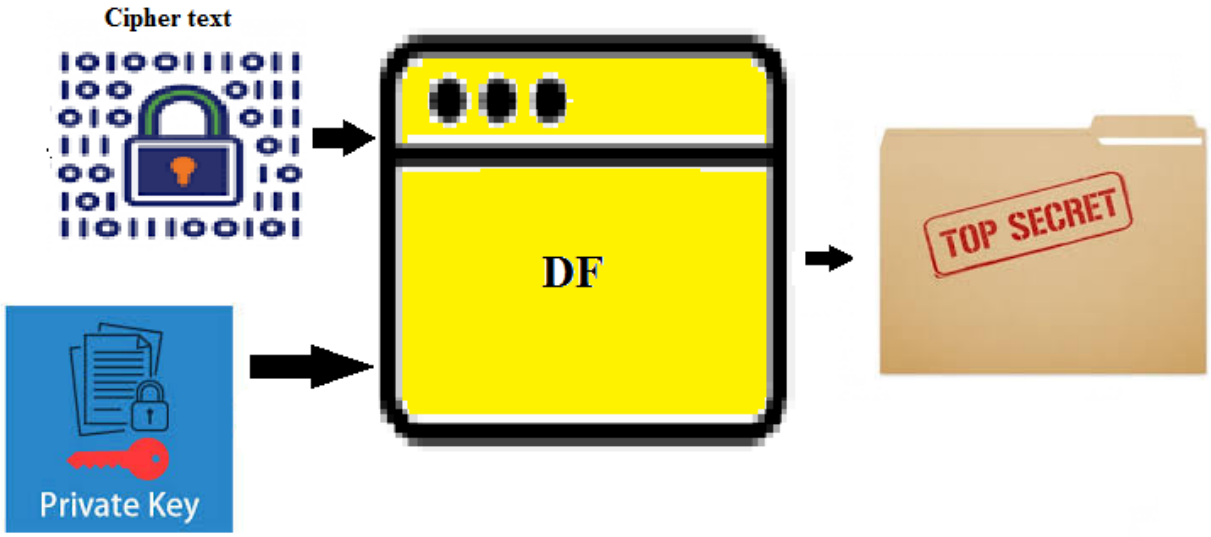

Figure 8: Decryption process diagram

A good crypto system must satisfy the following requirements:

- Encrypted message quality [71-75]:
  The encrypted message must be damaged, corrupted and unreadable, MSE measured between the source and the encrypted messages must be high, while PSNR must be low.
- Decrypted message quality[76-80]:
  The decrypted message must be identical to the source message, MSE measured between the source and the decrypted message must be zero, while the PSNR must be infinite.
- Speed :
  The crypto system must provide a high speed by reducing both the encryption and decryption times and increasing both the encryption and decryption throughputs.

- Security [81-84]:
  The system must use a complicated PK, this key must provide a huge key space, the entropy of the space must be greater than 128 [83], the produced decrypted message must be sensitive to the selected values of the PK.
- Simplicity:
  The crypto system must simplify the process of secret key generation, and it must simplify the process of encryption-decryption by reducing or eliminating the sequence of needed logical operations, and reducing the number of rounds.
- Flexibility:
  The crypto system must be capable to process any message (short, medium and long) efficiently, changing the message must not require any changes in the encryption and decryption functions.

5. Related works

A lot of methods for message cryptography were introduced, many of these methods were based on DES (data encryption standard) and AES (advanced encryption standard) methods, and table 1 summarizes the expected enhancements provided by the proposed method comparing with standard based methods:

Table 1: Comparisons between the proposed method and the standard methods [1-10]

Feature	Standard methods	Proposed method
Simplicity	Not simple, require a complex of logical operations	Simple, only reordering operations are required
Principle	Message is divided into blocks at the character level, block size is fixed	Massage is divided into blocks at the bit level, block size is variable and changeable
PK	56 to 256 bits	320 bits
Security	Entropy key space up to 256	Entropy key space equal 320
Rounds	10 to 16	2
Required secret keys	10 to 16	2
Quality of encrypted message	Satisfy requirements	Satisfy requirements
Quality of decrypted message	Satisfy requirements	Satisfy requirements
Speed	Moderate	Good

The Proposed Method

The proposed method encryption process can be implemented applying the following task:

Task1: Message preparation

a) Get the message.
b) Retrieve the message length (LM).
c) Convert the message to decimal.

Task2: Secret keys (IK1 and IK2) generation:

a) Get the PK.
b) Calculate the number of blocks by dividing LM by the block size (BS) included in the PK.
c) Run the first CLMM using r1, x1 and LM values to generate CK1, and then sort this key to get IK1.
d) Run the second CLMM using x2, r2 and NB values to generate CK2, and then sort this key to get IK2.

Task3: Message encryption

a) Apply round 1 to reorder the message characters using IK1.
b) Convert the message to binary to get the MBM.
c) Reshape MBM to one row to get the MAB.
d) Apply round 2 to reorder the blocks.

e) Reshape back MAB to get MBM.
f) Convert MBM to decimal.
g) Convert the decimals to characters to get the cipher message.

The decryption process can be implemented applying the same tasks as for encryption process, but the decryption task must be implemented by applying round2 first.

For researchers and readers who are interested in testing and running the proposed method, the following mat lab code can be useful:

```
%Encryption process:
a='Message cryptography';
a1=uint8(a); LM=length(a1);
BS=10; r1=3.77;x1=0.11; r2=3.68;x2=0.17;
NB=fix(LM*8/BS);
for i=1:LM
    x1=r1*x1*(1-x1);      CK1(i)=x1;
end
[ff IKEY1]=sort(CK1);
for i=1:NB
    x2=r2*x2*(1-x2);      CK2(i)=x2;
end
[ff IKEY2]=sort(CK2);
aa1=a1;
for i=1:LM
  c=IKEY1(i);
  aa1(1,i)=a1(1,c);
end
a2=dec2bin(aa1,8);
a3=reshape(a2,1,LM*8);
e1=a3;
for i=1:NB
  c=IKEY2(i);
    e1(1,1+BS*(i-1):i*BS)=a3(1,1+BS*(c-1):c*BS);
end
en1=reshape(e1,LM,8);en=bin2dec(en1)'; enc=char(en) ;
```

```
%Decryption process:
LM=length(enc);en1=uint8(enc);
BS=10;r1=3.77;x1=0.11; r2=3.68;x2=0.17;NB=fix(LM*8/BS);
for i=1:LM
    x1=r1*x1*(1-x1);      CK11(i)=x1;
end
[ff IKEY1]=sort(CK11);
for i=1:NB
    x2=r2*x2*(1-x2);      CK22(i)=x2;
end
[ff IKEY2]=sort(CK22);
aa2=dec2bin(en1,8);
aa3=reshape(aa2,1,LM*8);
d1=aa3;
for i=1:NB
  c=IKEY2(i);
    d1(1,1+BS*(c-1):c*BS)=aa3(1,1+BS*(i-1):i*BS);
end
d2=reshape(d1,LM,8);
d3=bin2dec(d2)';
de=d3;
for i=1:LM
  c=IKEY1(i);
  de(1,c)=d3(1,i);
end
char(de);
```


Implementation and Results Discussion

The proposed method uses a PK, which contains the values of 4 chaotic parameters(r1, x1, r2 and x2) and the BS value, thus the key space provided by this key will be calculated by equation1;

$$\text{Key space} = 2^{5*64} = 2^{320} \approx 2.13598703592091008239502170616 96 \times 10^{96}$$

$$\text{Entropy} = 320 \quad (1)$$

The entropy of the key space equal 320 (greater than 128 [83]), this means that the key is very strong and capable to resist any hacking attempt.

The produced decrypted messages are very sensitive to the selected values of the PK, any changes in the PK in the decryption process will lead to produce damaged message, to show this fact the message "Two rounds of message reordering" was encrypted using PK1, the encrypted message was decrypted using each of the following PK2, the obtained results (see table 2) show that the method is very sensitive to the selected PK.

PK1:
BS=17;
r1=3.77;x1=0.11;
r2=3.68;x2=0.17;
PK2:
BS=27;
r1=3.77;x1=0.11;
r2=3.68;x2=0.17;
PK3:
BS=17;
r1=3.87;x1=0.11;
r2=3.68;x2=0.17;
PK4:
BS=17;
r1=3.77;x1=0.21;
r2=3.68;x2=0.17;
PK5:
BS=17;
r1=3.77;x1=0.11;
r2=3.78;x2=0.17;
PK6:
BS=17;
r1=3.77;x1=0.11;
r2=3.68;x2=0.27;

Table 2: Proposed method sensitivity

Used PK in the decryption process	Decrypted message	Remarks
PK1	Two rounds of message reordering	Correct
PK2	¬e□□<Y>-¸üy:¸□8□↳<14□z¯]8-Šš<□8□	Damaged
PK3	soueegrf T gdrin saondreo remwos	Damaged
PK4	in T rndsergdmwoesreo feosaougr	Damaged
PK5	□e□D□^□iB□□Kî-ïkè□□K□□ïJàLà(û ûM	Damaged
PK6	r□□□U□□$□□^ZLzù@□□Nè¢□K□J□¶è□L□□	Damaged

The quality of the decrypted messages was tested and the obtained results showed that the decrypted message was always identical to the source message.
The quality of the encrypted messages was also tested, several messages were processed using the proposed method and the MSE and PSNR between the encrypted and source messages were calculated and table 3 shows the obtained results. The high values of MSE and the low values of PSNR prove the fact that the proposed method satisfies the quality requirement of the encrypted messages.

Table 3: Quality parameters between the source and the encrypted messages

Message length (byte)	MSE	PSNR
10	3693.2	27.1342
50	11756	16.7877
100	10427	18.3038
250	10771	17.9793
500	10912	17.8490
1000	10542	18.1938
2000	10670	18.0730
2500	11114	17.6656
5000	10932	17.8306
10000	10991	17.7766

A message 0f 5000 characters was processed varying the block size, the encryption time (ET) and the encryption throughput (ETP) were calculated, and table 4 shows the obtained speed results:

Table 4: Speed results for a message of 5000 characters when varying BS

BS (bits)	NB	ET (second)	ETP (K bytes per second)
10	4000	0.1530	31.9138
20	2000	0.1420	34.3860
30	1333	0.1140	42.8317
40	1000	0.1060	46.0643
100	400	0.0940	51.9448
200	200	0.0920	53.0740
300	133	0.0900	54.2535
400	100	0.0930	52.5034
500	80	0.0910	53.6573
750	53	0.0910	53.6573
1000	40	0.0920	53.0740

From table 4 we can see that using BS greater than 100 bytes will provide a good speed of message cryptography, thus it is recommended to use a suitable block size to reduce the number of blocks, this will minimize the encryption time and will maximize the encryption throughput (see figure 9).

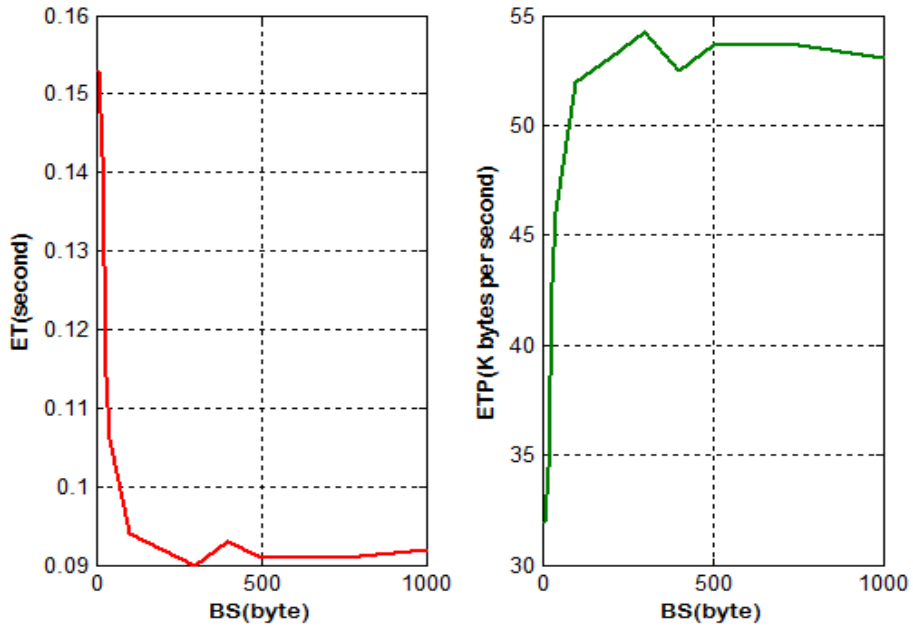

Figure 9: ET and ETP vs block size

Conclusion

A two rounds method of message cryptography was proposed, the first round was used to reorder the message at the character level, while the second round was used to reorder the message at the bit level. Two secret keys were used, one for each round of message cryptography. The private key contained 5 components, one value from the private key was used to set the block size, and the other four values were used to run two chaotic logistic map models to generate two chaotic keys, these two keys were sorted to form two indices keys, which were used as a secret rounds keys. The private key provided a good space entropy and it was capable to resist hacking attacks, the produced output messages were very sensitive to the selected values of the private key.

The proposed method simplified the process of message cryptography by using simple reordering operations, the method eliminate the complex of logical operations used in standard methods of message cryptography. The second round of the proposed method was used to reorder the message at the bit level, the message bits were divided into equal blocks, the required block size was investigated and it was shown that increasing the block size (decreasing the number of blocks) will minimize the encryption time and will maximize the encryption throughput.

The proposed method was tested and implemented using various messages and it was shown that the proposed method satisfied the requirements of good crypto system in the sensitivity, quality and speed.

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, &EijiKawaguchi,"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]. M. Bala Kumara, P. Karthikkab , N. Dhivyac , T. Gopalakrishnan, A Performance Comparison of Encryption Algorithms for Digital Images, International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 2, February – 2014.

[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.

[64]. Alqadi, Z. (2019). A new method for voice signal features creation. International Journal of Electrical and Computer Engineering (IJECE), 9(5): 4092-4098.https://doi.org/10.11591/ijece.v9i5.pp4092-4098.

[65]. Alqadi, Z. (2009). A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image. Journal of Computer Science, 5(5): 355-362.

[66]. Zaini, H., Alqadi, Z.A. (2021). Efficient WPT based speech signal protection. IJCSMC, 10(9): 53-65.https://doi.org/10.47760/ijcsmc.2021.v10i09.006.

[67]. Zneit, R.A., Khrisat, M.S., Khawatreh, S.A., Alqadi, Z.(2020). Two ways to improve WPT decomposition used for image features extraction. European Journal of Scientific Research, 157(2): 195-205.

[68]. Hindi, A., Qaryouti, G.M., Eltous, Y., Abuzalata, M.,Alqadi, Z. (2020). Color image compression using linear prediction coding. International Journal of Computer Science and Mobile Computing, 9(2): 13-20.

[69]. Zaidan, A.A., Majeed, A., Zaidan, B.B. (2009). High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World Academy of Science Engineering and Technology(WASET), 54: 468-479.

[70]. Zaidan, A.A., Zaidan, B.B. (2009). Novel approach for high secure data hidden in MPEG video using public key infrastructure. International Journal of Computer and Network Security, 1(1): 1985-1553.

[71]. Khalifa, O.O., Naji, A.W., Zaidan, A.A., Zaidan, B.B.,Hameed, S.A. (2010). Novel approach of hidden data inthe (unused area 2 within EXE file) using computation between cryptography and steganography. Int. J. Comput.Sci. Netw. Secur, 9(5): 294-300.

[72]. Majeed, A., Mat Kiah, M.L., Madhloom, H.T., Zaidan,B.B., Zaidan, A.A. (2009). Novel approach for high secure and high rate data hidden in the image using image texture analysis. International Journal of Engineering and technology, 1(2): 63-69.http://eprints.um.edu.my/id/eprint/4951.

[73]. Zaidan, A.A., Othman, F., Zaidan, B.B., Raji, R.Z.,Hasan, A.K., Naji, A.W. (2009). Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In Proceedings of the World Congress on Engineering, 1: 1-7.

[74]. Aos, A.Z., Naji, A.W., Hameed, S.A., Othman, F.,Zaidan, B.B. (2009). Approved undetectable-antivirussteganography for multimedia information in PE-file. In 2009 International Association of Computer Science and Information Technology-Spring Conference, pp. 437-444. https://doi.org/10.1109/IACSIT-SC.2009.103.

[75]. Zaidan, A.A., Zaidan, B.B., Abdulrazzaq, M.M., Raji,R.Z., Mohammed, S.M. (2009). Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen,Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, 19: 482-489.

[76]. Naji, A.W., Zaidan, A.A., Zaidan, B.B., Muhamadi, I.A.(2010). Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard. Proceeding of World Academy of Science Engineering and Technology (WASET), 56(5): 498-502.

[77]. M. Bala Kumara, P. Karthikkab , N. Dhivyac , T. Gopalakrishnan, A Performance Comparison of Encryption Algorithms for Digital Images, International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 2, February – 2014.

[78]. Lee Mariel Heucheun Yepdia, Alain Tiedeu, and Guillaume Kom, A Robust and Fast Image Encryption Scheme Based on a Mixing Technique, Security and Communication Networks, Volume 2021 |Article ID 6615708 | https://doi.org/10.1155/2021/6615708.

[79]. Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," Information Sciences, vol. 480, pp. 403–419, 2019.

[80]. M. Asgari-chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," Signal Processing, vol. 157, p. 1, 2019.

[81]. X. Zhang and X. Wang, Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System, Springer, New York, NY, USA, 2019.

[82]. J. S. Zhenjun and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," Optics and Lasers in Engineering, vol. 80, pp. 1–11, 2016.

[83]. Pleacher, D. (n.d.), Calculating password entropy. Retrieved February 16, 2023, from https://www.pleacher.com/mp/mlessons/algebra/entropy.htmlPotter,

[84]. Shaza D. Rihan, Ahmed Khalid Saife, Eldin F. Osman, A Performance Comparison of Encryption Algorithms AES and DES, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS120227 www.ijert.org (This work is licensed under a Creative Commons Attribution 4.0 International License.) Vol. 4 Issue 12, December-2015.