iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

# A SIMPLIFIED AND EFFICIENT METHOD OF SECRET MESSAGE CRYPTOGRAPHY

**Prof. Ziad Alqadi**
Albalqa Applied University, Faculty of Engineering Technology, Jordan, Amman

**ABSTRACT**
A simplified method of secret message cryptography will be introduced, the method will apply message encryption-decryption by using simple message blocking and message blocks rearrangement, and the method will eliminate the complex of logical and arithmetic operations used in other methods of data cryptography. The proposed method will use a complicated private key; this key will provide a good key space capable to resist hacking attacks. The private key components will be used to divide the message into blocks and to run a chaotic logistic map model to generate a chaotic key, which will be sorted to form the indices key required to rearrange the message blocks, the produced outputs of the method will be very sensitive to the selected values of the private key components.
The proposed method will be tested and implemented using various messages, the speed parameters will be calculated, and the speed results will be compared with other method speeds to show how the proposed method will decrease the encryption time and how it will speed up the process of message cryptography.
The quality and sensitivity of the proposed method will be examined to show that the proposed method will satisfy the requirements of good crypto method.

**Keywords**:
Cryptography, SM, block, reshaping, rearrangement, PK, CK, IK, CLMM, growth rate, population.

## INTRODUCTION

Message is a set of characters organized in one row matrix [20-25]as shown in figure 1, this row matrix can be reshaped into 2D matrix by selecting the number of rows and the number of blocks by apply a simple reshaping operation, each column in the obtained 2D matrix will be treated as a block. The number of blocks will selected by the user and it can vary from time to time (see figure 1). The block length will be a part of the used in the proposed method private key (PK) [11-19].

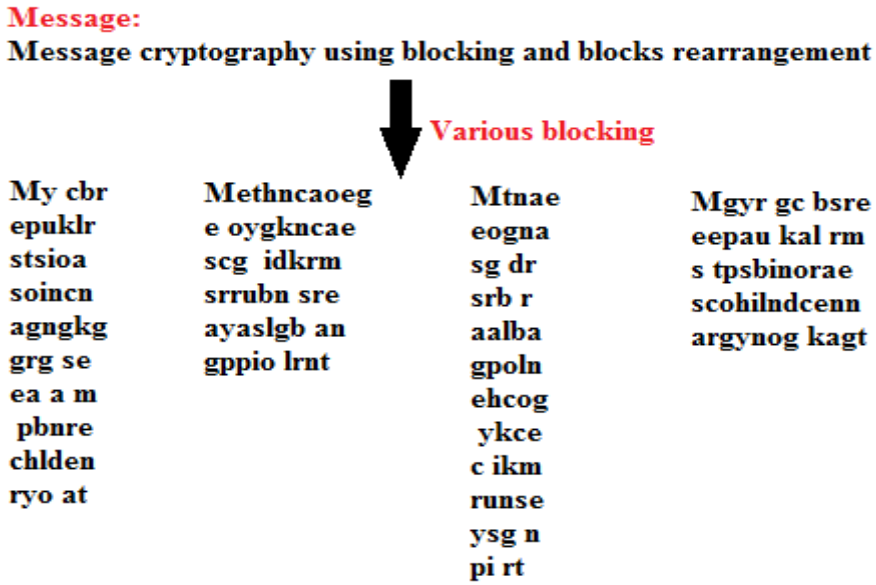


***Figure 1: Various ways of message blocking (example)***

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

The expansion of the use of the Internet and the frequent exchange of messages through it has led to an increase in the number of data hackers, which has turned the communication network into an unsafe network (see figure 2) through which the data hacker can steal the message and resend it in a way that serves his interests. In order to transform the communication network into a secure network (see figure 3), the message must be protected before it is sent and transformed into a message that cannot be read or benefited from [26-30].

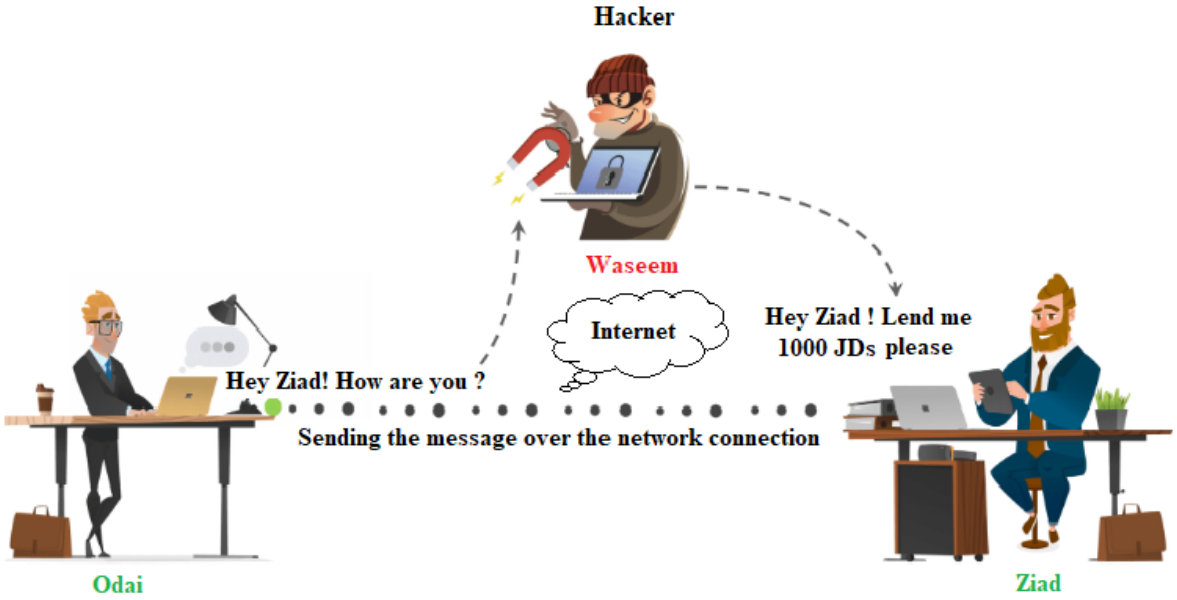


*Figure 2: Unsafe data communication network*

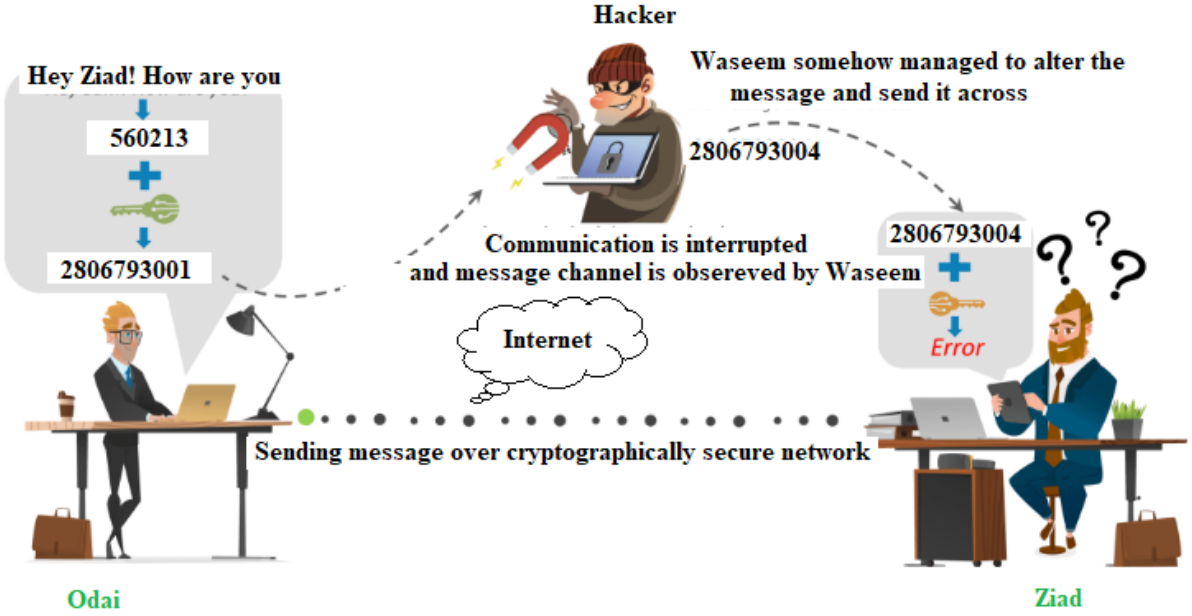


*Figure 3: Safe data communication network*

The easiest way to secure the message is message cryptography. The crypto process as shown in figure 4 contains encryption function (EF) and decryption function (DF) [31-40].

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

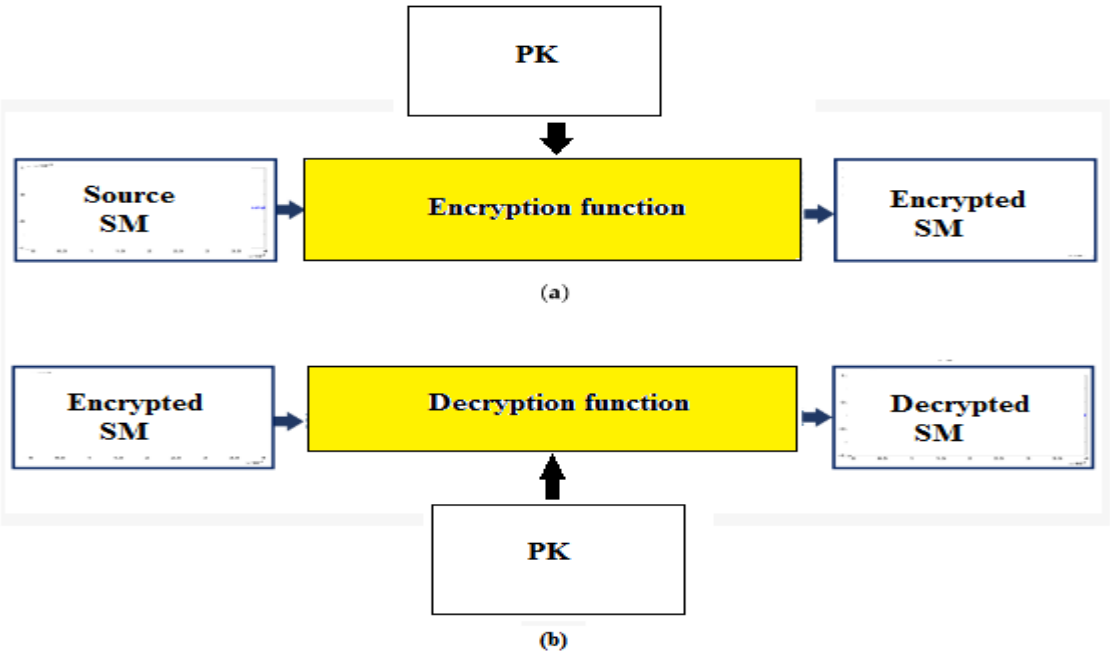


***Figure 4: Crypto process: a) encryption, b) decryption***

A good crypto method must satisfy the following requirements:

- Quality

The encrypted message must be damaged and unreadable, the mean square error (MSE) measured between the source and the encrypted messages must by high, while the peak signal to noise ratio (PSNR) must be low.

The decrypted message must be the same as the source message, the MSE measured between the source and the decrypted message must be zero, while the PSNR must be infinite [41-47].

- Speed:

The method must minimize both the encryption and decryption times, thus it must maximize the throughput of message cryptography [48-55].

- Security:

The used PK must be complicated and it must provide good entropy (entropy >128 [83]) to make the key strong enough to resist hacking attacks, the produced outputs must be sensitive to the selected values of the PK components [56-63].

- Simplicity

The method must be simple by reducing the number of rounds and reducing the number of logical and arithmetic operation required to apply key generation and message encryption –decryption. The process of key generation must be simple and does not require long time for secret key generation [64-70].

- Flexibility:

The method must be efficiently used to treat short, medium and long messages.

**The Private Key**

The PK used in the proposed method contains three components: number of blocks (NB), growth rate (r) and initial population(x). NB will be used to reshape the message into 2D matrix with NB blocks (columns), while r and x with NB are used to run a chaotic logistic map model to generate a chaotic key (CK), the CK will be sorted to form the secret indices key (IK), which will be used to rearrange the message blocks [70-77].

Chaotic logistic map (CLM) is a nonlinear difference equation (see equation 1), which maps the maps the population value at any time step to its value at the next time step [77-84].

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

$$X_{t+1}=rX_t(1-X_t) \quad (1)$$

**Where:**
**X is the papulation**
**r is the growth rate**

The calculated population values will be used as a data set to generate the secret indices key [71-80], the generated population will be sorted to get the indices key, this key will contain a set of unrepeated integer values, the first value will point to the minimum element in the data set, the second value will point to the second minimum and so on, the length of the key can be controlled by the user. The following example shows how to generate a 10 elements key with fractional values:

```
x=0.1;r=3.6;d=x;
length=12;
for i=1:length
x=r*x*(1-x);
k(i)=x;
end
[ff indices_key]=sort(k);
indices_key
indices_key =

    1   11    7    5    9    3    2   12    8    4    6   10
```

The Generated population requires time generation [77-84], this time will rapidly increase when increasing the population length, table 1 shows how the key generation time will increase when increasing the length of population:

***Table 1: key generation time***

| Population length | KGT(second) | Length | KGT(second) |
|---|---|---|---|
| 100 | 0.000001 | 15000 | 0.167000 |
| 200 | 0.000001 | 20000 | 0.250000 |
| 400 | 0.003000 | 25000 | 0.379000 |
| 500 | 0.004000 | 30000 | 0.528000 |
| 1000 | 0.017000 | 40000 | 0.976000 |
| 2000 | 0.052000 | 50000 | 1.549000 |
| 2500 | 0.054000 | 100000 | 10.599000 |
| 4000 | 0.060000 | 200000 | 57.864000 |
| 5000 | 0.064000 | 400000 | 331.892000 |
| 10000 | 0.101000 | 1000000 | 2311.878000 |

From table 1 we can see that the selected length of the population will affect the method efficiency so we have to select a length less than 5000, thus the selected number of message blocks will be less than 5000, doing this we can minimize the KGT and thus minimize the encryption time (see figure 5) .

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/


*Figure 5: KGT vs population length*

The generated populations and thus the generated secret indices key will be very sensitive to the selected values of the PK components, any minor changes in these values will lead to change the contents of the IK as shown in figue 6:

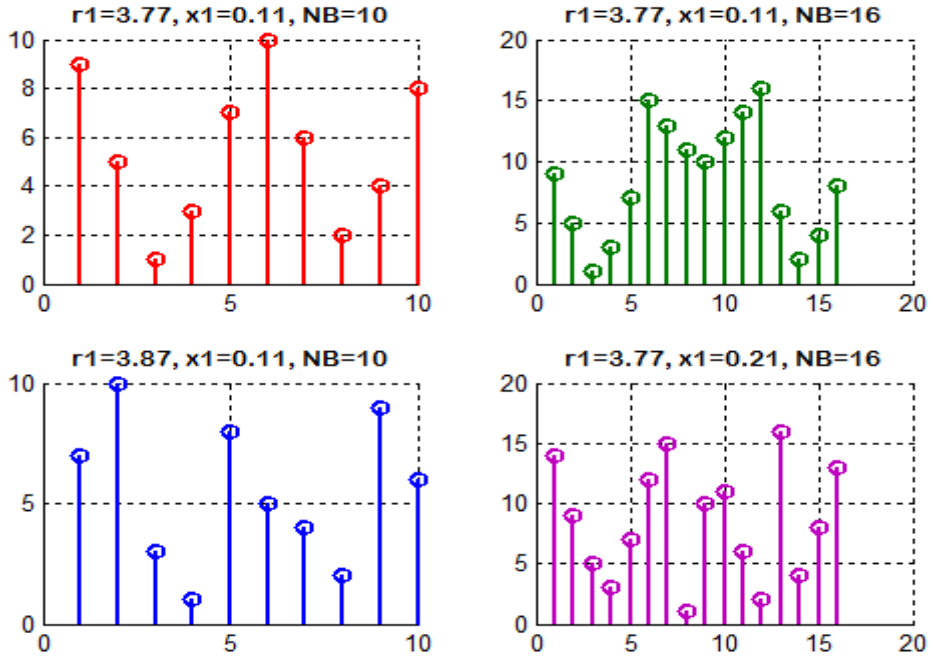


*Figure 6: Indices key sensitivity*

The PK will have a length of 192 bits, this key will provide an entropy equal 192 (greater than 128 [83]), this entropy will make the key strong enough to resist hacking attacks, the key space provided by the key will be calculated using equation 1 [11 -18]:

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

$$\text{Key space} = 2^{3x64}$$

$$= 2^{192}$$

$$= 6.277101735386680763835789423207 7x10^{57} \text{ Combinations}$$

$$\text{Entropy} = 192 \qquad (1)$$

**Related works**

Many methods for data cryptography were introduced by various authors, some of these methods were based on the standard methods DES and AES methods [1-10], other were chaotic and non chaotic methods [77-84].
The introduced methods shared the following features [1-10]:

- Data blocking:

The data to be encrypted is to divided into blocks, the block size is fixed and small.

- PK length and key space:

Mostly these methods used a long PK, and these keys provided a good key space with good entropy, making the key strong enough to resist hacking attacks.

- Rounds:

These methods were implemented using a fixed number of rounds; each round required a complex of logical operations to apply data encryption-decryption.

- Secret keys:

Each of the introduced methods required a set of secret key, the keys generation process required a complex of logical and arithmetic operations.

- Speed

These methods provided various speeds, from low speed to high (see table 2), the efficiency of these methods was decreased when increasing the data size.

- Simplicity

Mostly these methods were not simple, each method required a complex of logical and arithmetic operations to generate the required secret keys and to apply data blocks encryption and decryption.
The aim of this paper research is to introduce a new method for message cryptography, this method will use two rounds, the first round will be used to divide the message into blocks, while the second round will be used to rearrange the message blocks. The proposed method will simplify the process of cryptography and will speed up the process of message cryptography by decreasing the encryption-decryption time and increasing the throughput of message cryptography.

***Table 2: Throughputs of the introduced methods***

| Introduced method | Average ETP (K bytes per second) | Introduced method | Average ETP (K bytes per second) |
|---|---|---|---|
| DES | 86.7881 | Chaotic [77] | 141.2305 |
| 3DES | 74.6363 | Hyper chaotic [77] | 636.3379 |
| AES | 90.3135 | In [78] | 888.8867 |
| RC2 | 61.8961 | In [79] | 911.0352 |
| RC6 | 155.5953 | In [80] | 638.4082 |
| BF | 561.3837 | In [81] | 360.4102 |
| Non-chaotic [77] | 170.3906 | In [82] | 384.9609 |

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

**The proposed method**

The proposed method used a PK with three components, the first component is to be used to reshape the message into a selected number of columns, each column will be treated as a block, figure 7 shows an example of message blocking:

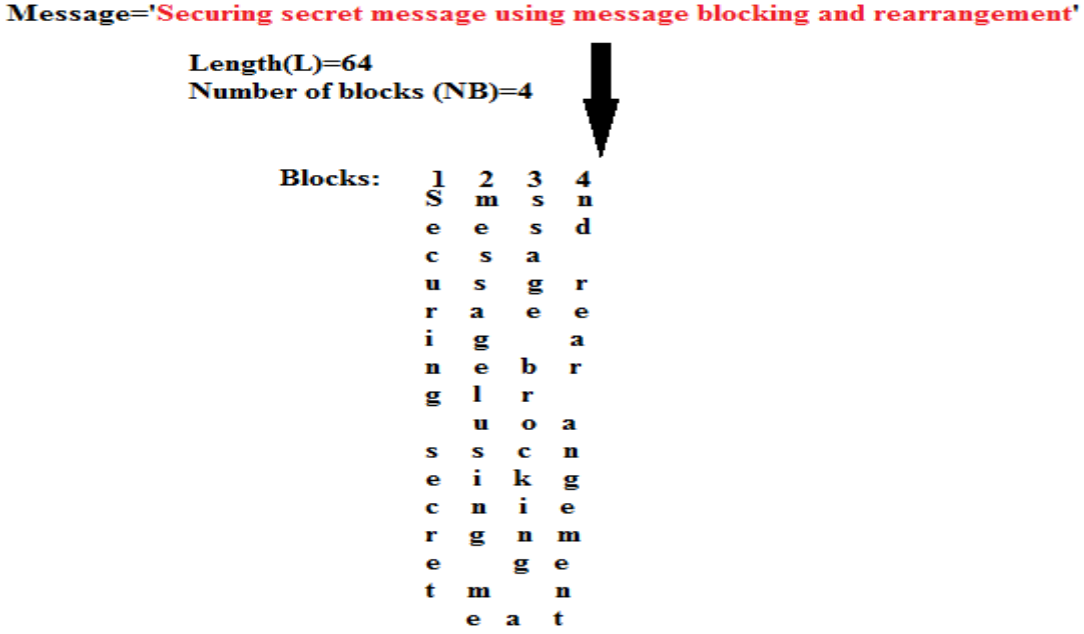


***Figure 7: Message blocking (example)***

The second and the third components in the PK are the growth rate (r) and the initial population (x), the values of these components with the value of the NB are used to run a chaotic logistic map model (CLMM) to generate a chaotic key (CK), the CK is to be sorted to form the indices key (IK) required to rearrange the message blocks, figure 8 illustrate an example of IK generation:

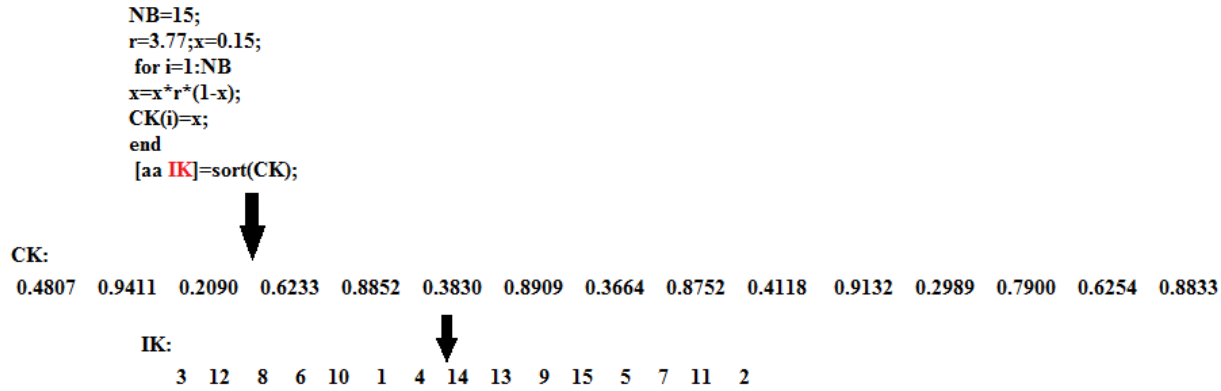


***Figure 8: IK generation (example)***

The contents of IK are used to rearrange the message blocks. In the encryption phase the blocks are to be arranged according to the contents (see figure 9 for illustration), while in the decryption phase the blocks are to arranged by finding the position of the minimum value first, then the second minimum and so on as shown in figure 10.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

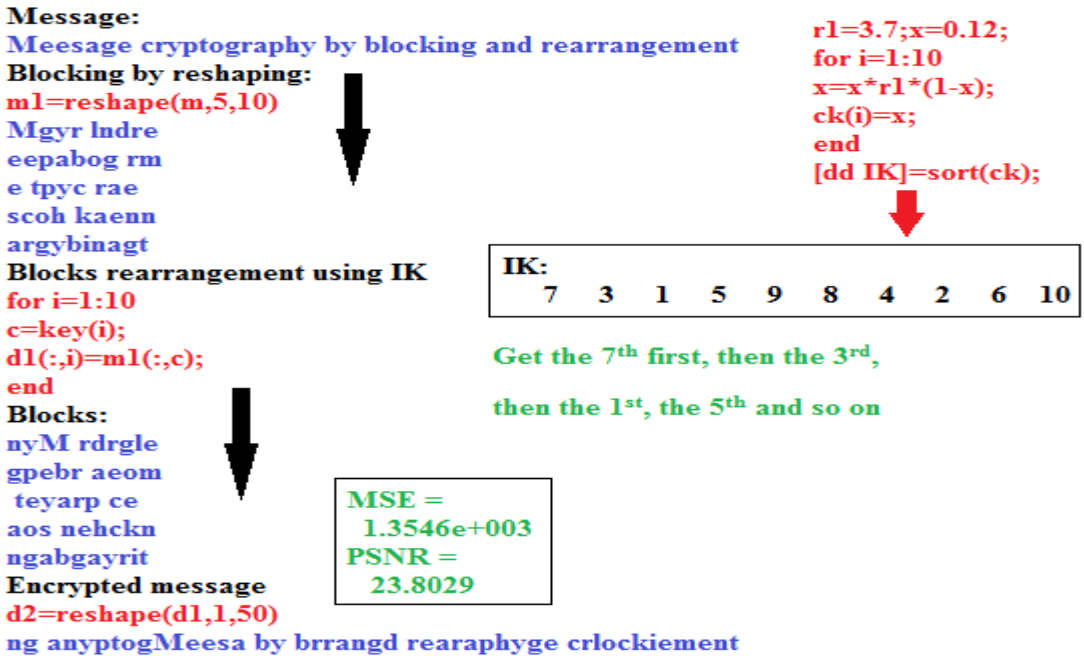


*Figure 9: Proposed method encryption phase (example)*

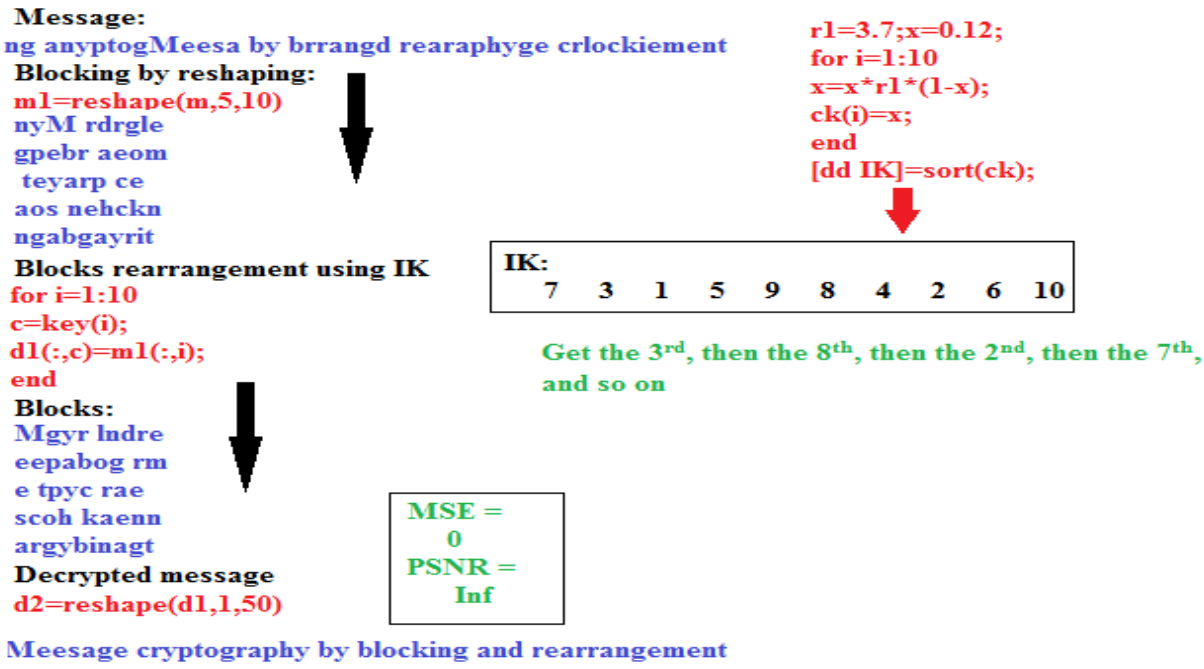


*Figure 10: Proposed method decryption phase (example)*

The encryption phase of the proposed method will be implemented applying the following steps:
Step 1: Inputs preparation:

a) Get the message.
b) Get the message length (L)
c) Get the PK: r, x and NB.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

d) Calculate the block size.

Step 2: Dividing message into blocks:
Reshape the message to 2D matrix with NB columns.
Step 3: IK generation:

a) Use r, x and NB values to run a CLMM to generate CK.
b) Sort CK to get the IK.

Step 4: Message encryption:

a) Use IK to rearrange the message blocks.
b) Reshape the message to one row matrix to get the encrypted message.

The decryption phase will be implemented using the same steps as for encryption phase using the encrypted message as an input message and by applying the decryption as shown in figure 10.
For researchers and readers, who are interested in using this method, the following mat lab code can be useful:

```
%Encryption:
m='Message cryptography by blocking and rearrangement';
m=uint8(255*rand(1,10*1024));
L=length(m);
r=3.77;x=0.12;
R=320; C=fix(L/R);
m1=reshape(m,R,C);
for i=1:C
   x=x*r*(1-x);
   CK(i)=x;
end
[dd IK]=sort(CK);
for i=1:C
   d=IK(i);
   m2(:,i)=m1(:,d);
end
m3=reshape(m2,1,R*C);
m4=char(m3);
```

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

```
%Decryption:
L=length(m4);
r=3.77;x=0.12;
R=320; C=fix(L/R);
m5=reshape(m4,R,C);
for i=1:C
   x=x*r*(1-x);
   CK(i)=x;
end
[dd IK]=sort(CK);
for i=1:C
   d=IK(i);
   m6(:,d)=m5(:,i);
end
m7=reshape(m6,1,R*C);
m8=char(m7);
```

**Implementation and results discussion**

The proposed method was implemented using mat lab 7 and using a computer with the following specifications:

| | |
|---|---|
| Processor: | Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz 2.50 GHz |
| Installed memory (RAM): | 4.00 GB |
| System type: | 64-bit Operating System |
| Pen and Touch: | No Pen or Touch Input is available for this Display |

Increasing the number of blocks will increase the size of generated IK, thus the CLMM running time will be increased, thus the efficiency of the method will negatively affected, so it is required to select the optimal value for NB. To show this fact a message of 10 K characters was selected and treated using the proposed method by varying the NB value, the encryption time (ET) in seconds was calculated and the encryption throughput (ETP) in K bytes per second also was calculated and table 3 shows the obtained results.

***Table 3: Speed results when varying NB***

| NB | Block size (byte) | ET(second) | ETP(K bytes per second) |
|---|---|---|---|
| 2048 | 5 | 0.1180 | 84.7458 |
| 1024 | 10 | 0.0480 | 208.3333 |
| 640 | 16 | 0.0260 | 384.6154 |
| 512 | 20 | 0.0210 | 476.1905 |
| 320 | 32 | 0.0150 | 666.6667 |
| 256 | 40 | 0.0140 | 714.2857 |
| 128 | 80 | 0.0090 | 1111.1 |
| 64 | 160 | 0.0060 | 1666.7 |
| **32** | **320** | **0.0050** | **2000.0** |
| **Optimal** | | **Min ET** | **Max. ETP** |
| 16 | 640 | 0.0060 | 1666.7 |
| | | | |

From table 3 we can see that the optimal ET and the optimal ETP was achieved when using 32 blocks, it is also seen that choosing NB within the range 32 to 128 will optimize the speed of message cryptography (see figure 11).

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

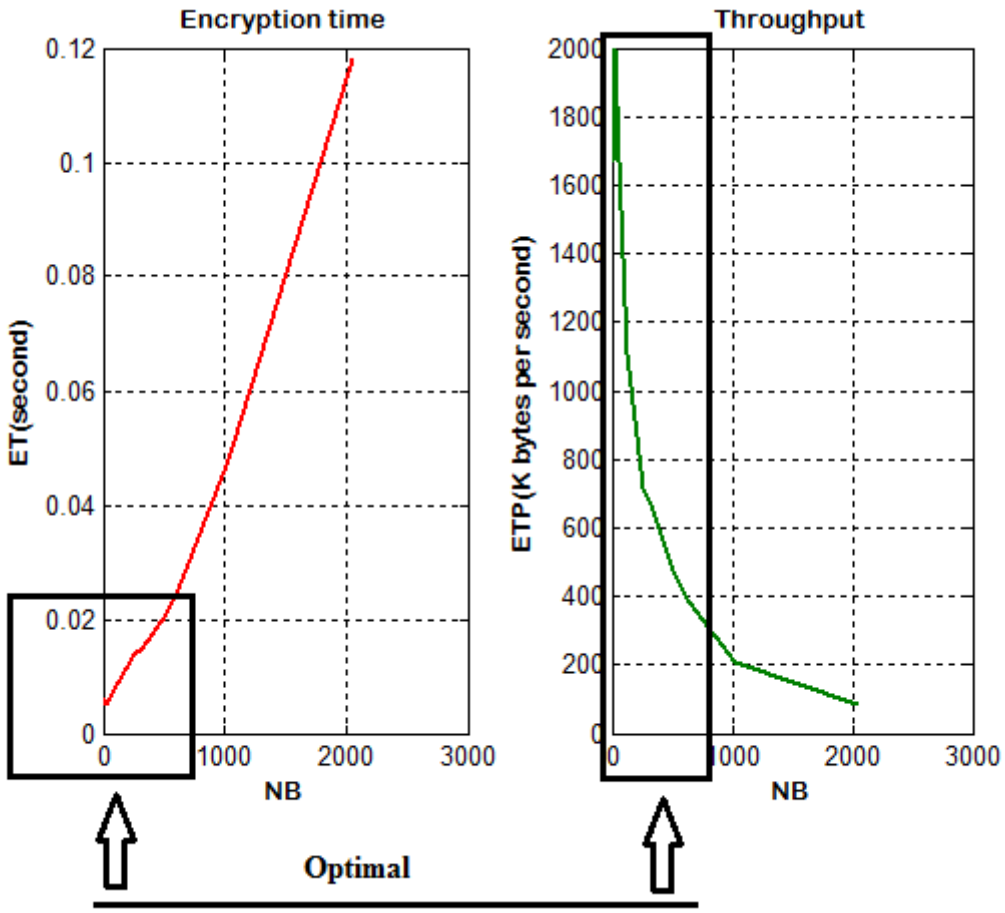


***Figure 11: ET and ETP vs NB***

A set of messages were selected and processed using the proposed method, block sizewas fixed to 256, the ET and the ETP were calculated and table 4 shows the obtained speed results:

***Table 4: Speed results for various messages (block size=256 bytes)***

| Message length(K bytes) | NB | ET(second) | ETP(K bytes per second) |
|---|---|---|---|
| 0.5 | 2 | 0.0050 | 100.0000 |
| 1 | 4 | 0.0050 | 200.0000 |
| 2 | 8 | 0.0040 | 500.0000 |
| 4 | 16 | 0.0050 | 800.0000 |
| 5 | 20 | 0.0060 | 833.3333 |
| 10 | 40 | 0.0050 | 2000.0 |
| 25 | 100 | 0.0080 | 3125.0 |
| 50 | 200 | 0.0120 | 4166.7 |
| 100 | 400 | 0.0260 | 3846.2 |
| 200 | 800 | 0.0830 | 2409.6 |
| 500 | 2000 | 0.4740 | 1054.9 |
| Average | | | 1730.5 |

From table 4 we can see the following facts:

- Increasing the message size will increase the ETP.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

- The maximum ETP will be achieved when reaching a 50 K bytes message length and this is the optimal ETP.
- Increasing the message size for messages with length greater than 50 K bytes will decrease the ETP 9see figure 12)..
- Changing the block size and the message length will change the optimal ETP.
- The method provided a good average of ETP, which is equal 1730.5 K bytes per second..
- The method provided a speed up in message cryptography comparing with other existing methods (see table 5), the proposed method significantly increased the throughput of message cryptography.

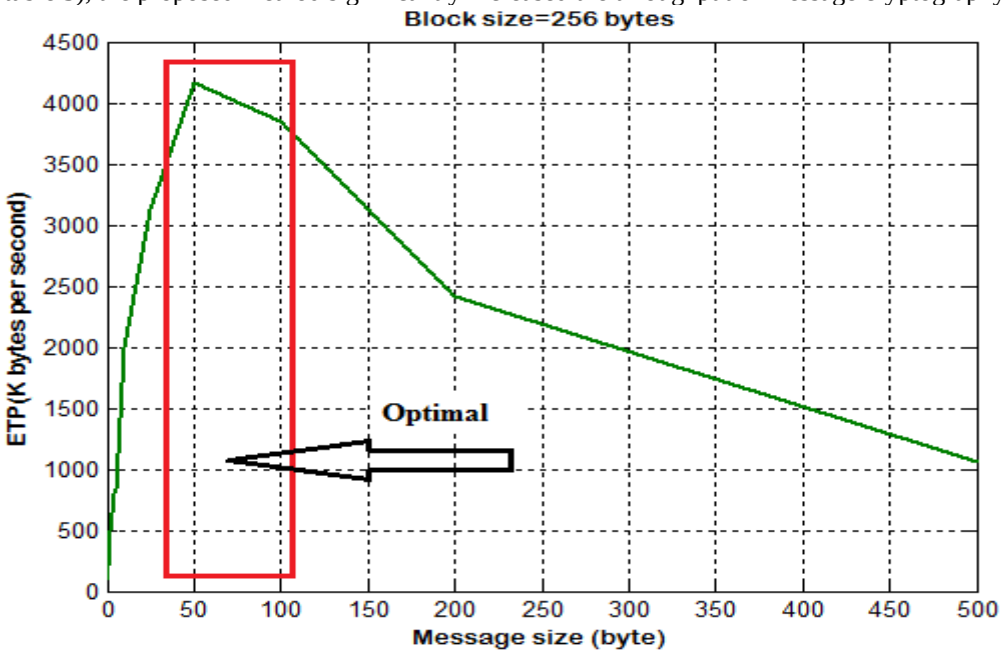


***Figure 12: ETP ns message length (block size =256 bytes)***

***Table 5: Proposed method speed up***

| Introduced method | Average ETP (K bytes per second) | Speed up of the proposed method | Introduced method | Average ETP (K bytes per second) | Speed up of the proposed method |
|---|---|---|---|---|---|
| DES | 86.7881 | 19.9394 | Chaotic [77] | 141.2305 | 12.2530 |
| 3DES | 74.6363 | 23.1858 | Hyper chaotic [77] | 636.3379 | 2.7195 |
| AES | 90.3135 | 19.1610 | In [78] | 888.8867 | 1.9468 |
| RC2 | 61.8961 | 27.9581 | In [79] | 911.0352 | 1.8995 |
| RC6 | 155.5953 | 11.1218 | In [80] | 638.4082 | 2.7106 |
| BF | 561.3837 | 3.0826 | In [81] | 360.4102 | 4.8015 |
| Non-chaotic [77] | 170.3906 | 10.1561 | In [82] | 384.9609 | 4.4953 |

The quality of the proposed method was tested, the decrypted messages were always identical to the source messages, while the encrypted messages were always damaged.
The previous selected messages were again processed by the proposed method, the obtained High values of MSE measured between the source and the encrypted messages and the low values of PSNR prove the fact that the proposed method satisfied the encryption quality requirements (see table 6):

***Table 6: Encryption quality parameters(block size 256 bytes)***

| Message length(K bytes) | NB | MSE | PSNR |
|---|---|---|---|
| 1 | 4 | 11305 | 17.4949 |
| 2 | 8 | 10902 | 17.8579 |

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

| | | | |
|---|---|---|---|
| 4 | 16 | 10058 | 18.6637 |
| 5 | 20 | 10447 | 18.2843 |
| 10 | 40 | 10920 | 17.8415 |
| 25 | 100 | 10732 | 18.0150 |
| 50 | 200 | 10858 | 17.8986 |
| 100 | 400 | 10765 | 17.9851 |
| 200 | 800 | 10770 | 17.9803 |
| 500 | 2000 | 10841 | 17.9147 |

The sensitivity of the proposed method was tested, the message '10.6+7*5/2+12+23=63.1000' was encrypted using the following PK, the encrypted message was decrypted by adding some changes to the PK, the obtained results shown in table 7 prove that the method is very sensitive to the selected values of the PK.

**PK:**
**r=3.77;x=0.12;**
**NB=4;**

***Table 7: Proposed method sensitivity***

| Changes | Decrypted message |
|---|---|
| No changes | 10.6+7*5/2+12+23=63.1000 |
| NB=3 | 5/10+16+3.1*0002.2+273=6 |
| r=3.87 | 10.6+7*5/0002+12+23=63.1 |
| x=0.22 | 2+26+7*5/3=63.10002+110. |

## CONCLUSION

A simple and easy to implement method of message cryptography was proposed, the method used a simple message blocking and blocks rearrangements to replace the complex of logical and arithmetic operations used in other methods of data cryptography, the method used a simplified procedure to generate the secret indices by running a chaotic logistic map model. The proposed method provided a good security level, the entropy of the key is acceptable and it provide a strong enough key space capable to resist hacking attacks, the produced outputs were very sensitive to the selected values of the private key. The private key was used to apply message blocking and message blocks rearrangements based on the contents of the generated secret indices key. The message block size and the number of blocks were examined tp provide an optimal efficiency.
The speed of the proposed method was examined by implementing the proposed method using various messages, and it was shown that the proposed method was efficient when processing short, medium and long messages. The proposed method provided a good average speed, and the speed results of the proposed method were compared with other existing methods speeds, and it was shown that the proposed method provided a significant speed up, it reduced the encryption time and increased the throughput of message cryptography.
The quality and sensitivity of the proposed method were tested and it was shown that the proposed method satisfied the requirements of good crypto method.

## 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/

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[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] 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.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[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.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[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.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[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.