

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. 11, Issue. 7, July 2022, pg.18 – 36

Multiple CLMMs Keys to Secure Message Transmission

Prof. Ziad Alqadi; Prof. Qazem Jaber

Albalqa Applied University, Faculty of Engineering Technology, Jordan – Amman

DOI: <https://doi.org/10.47760/ijcsmc.2022.v11i07.003>

Abstract: A simple, flexible and efficient method of message cryptography will be introduced. The method will suit any message with any length, it can use one or more rounds to apply encryption-decryption. The PK key will have a complicated structure that cannot be hacked. The PK will contain information about chaotic parameters, these parameters will be used to run a CLMMs to generate the needed number of CLKs, the generated CLKs will be converted to induces keys, which are to be used as a lockup tables in the encryption and decryption phases. The generated key will sensitive to any minor changes in the PK, and using another PK in the decryption phase will produce a damaged decrypted message. The method will be implemented and the obtained results will be used to calculate the method throughput. The obtained throughputs will be compared with DES method throughput to show how the proposed method speedup the process of message cryptography.

Keywords: Cryptography, PK, CLMM, CLK, IK, lockup table, throughput.

Abbreviations

The following abbreviation was used in this research paper:

PK: private key

IK: indices key

CLK: chaotic logistic key

CLMM: chaotic logistic map model

ET: encryption time

DT: decryption time

TP: throughput

Introduction

Encryption is the method by which information is converted into a secret code that hides the true meaning of the information. The science of coding and decoding information is called cryptography [13-20].

In computing, unencrypted data is also known as common text, and encrypted data is called cipher text. The formulas used to encrypt and decrypt messages are called cipher algorithms or ciphers [55-62].

To be effective, encryption includes a variable as part of the algorithm. The variable, called the key, is what makes the code's output unique. When an encrypted message is intercepted by an unauthorized entity, the hacker has to guess the identity of the sender used to encrypt the message, as well as the keys that were used as variables. The time it takes to guess this information is what makes encryption a valuable security tool [16-20].

At the beginning of the encryption process, the sender must decide what encryption will hide the meaning of the message and the best variable to use as a key to make the encrypted message unique. The most commonly used types of ciphers fall into two categories: symmetric and asymmetric.

Symmetric ciphers, also referred to as secret key ciphers, use a single key. The key is sometimes referred to as a shared secret because the sender or the computing system doing the encryption must share the secret key with all entities authorized to decrypt the message. Symmetric key encryption is usually much faster than asymmetric encryption. The most commonly used symmetric cipher is the Advanced Encryption Standard (AES), which is designed to protect government classified information [30-39].

Asymmetric ciphers, also known as public key cryptography, use two different - but logically related - keys. This type of cipher often uses primes to generate keys because they are difficult to compute with large primes and the reverse design of the cipher. The Rivest-Shamir-Adleman (RSA) encryption algorithm is currently the most widely used public key algorithm. With RSA, the public or private key can be used to encrypt a message; Whichever is not used for encryption becomes the decryption key (see figure 1) [40-50].

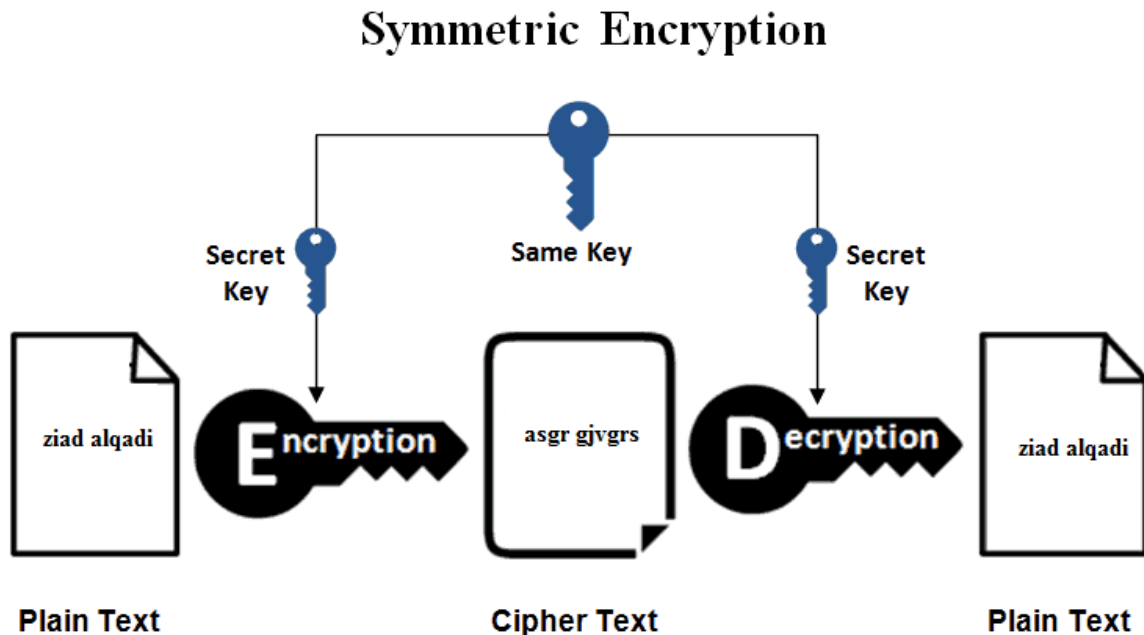


Figure 1: Process of data cryptography

Today, many cryptographic processes use a symmetric algorithm to encrypt data and an asymmetric algorithm for secure secret key exchange [55-62].

Cryptography plays an important role in securing many types of IT assets. It provides the following:

- Confidentiality encodes the content of the message.
- Authentication verifies the origin of the message.
- Integrity proves that the contents of the message have not changed since it was sent.
- Failure to reply prevents senders from refusing to send the encrypted message.

Encryption is commonly used to protect data in transit and data at rest. Every time someone uses an ATM or buys something online using a smartphone, encryption is used to protect the information being transmitted. Companies are increasingly relying on encryption to protect applications and sensitive information from reputational damage in the event of a data breach [25-31].

There are three main components to any encryption system: the data, the encryption engine, and the key management. In laptop encryption, all three components are run or stored in the same place: on the laptop.

However, in application architectures, the three components are usually run or stored in separate places to reduce the chance that a compromise of any single component will compromise the entire system.

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over the Internet or any other computer network [31-37].

In addition to security, encryption adoption is often driven by the need to meet compliance regulations. A number of standards organizations and bodies recommend or require that sensitive data be encrypted in order to prevent unauthorized third parties or threatening actors from gaining access to the data. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires merchants to encrypt customers' payment card data when it is stored at rest and transmitted over public networks [22-28].

A good method of message cryptography must provide the following [12-20]:

- Quality, the quality of the decrypted message must be very low, the message must be totally destroyed and corrupted to make it useless to any third party. Here the quality between the source and the encrypted messages can be measured by MSE and PSNR, the value of MSE must be high, while the value of PSNR must be low. The quality of the decrypted message must be high, and the decrypted message must be identical to the source message, here MSE must be equal zero, while PSNR must be infinite.
- Security, the method must provide a high level of security, this can be achieved by using a complicated PK, which must provide a huge key space that can resist any attack, also the process of cryptography must be sensitive to any minor changes in the PK components.
- Speed, the method must provide small times for encryption-decryption, thus it must maximize the throughput (speed) of the process of cryptography.
- Simplicity, the method must be simple and easy to implement, it must suit any message with any length, changing the message, or changing the PK must not require any changes in the method algorithm [55-62].

Related Work

Many methods [55-62] were introduced for data cryptography, many of them were based on data encryption standard (DES), mostly these methods share the following characteristics (some of the characteristics are considered as a disadvantages which need solving (see table 2)) [1-11]:

Table 1: Standard encryption methods features [1-11]

Method parameter	DES	3DES	AES	Blowfish
PK length(bit)	56(fixed)	112, 168(fixed)	128, 192, 256(fixed)	32-448(fixed)
Block size(bit)	64(fixed)	64(fixed)	128(fixed)	64(fixed)
Ability to deal with images	Difficult	Difficult	Difficult	Difficult
Encryption quality	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR
Decryption quality	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR
Efficiency	Slow	Slow	Slow	Moderate
Attack	Brute force attack	Brute force attack, Known plaintext, Chosen plaintext	Side channel attack	Dictionary attack
Structure	Feistel	Feistel	Substitution-Permutation	Feistel
Block cipher	Binary	Binary	Binary	Binary
Rounds	16(fixed)	48(fixed)	10,12,14(fixed)	16(fixed)
Flexibility to modification	no	yes	yes	yes

Methods based on DES technique have common features, some of the features are considered as disadvantages, below is the main features of these methods:

- Private Key (PK): PK has a fixed length (some times it can be hacked), this key is used in generation other sub keys to be used in various rounds [12-20].
- Block size: Data is divided into equal blocks, block size usually fixed and small [21-30].
- Rounds: The process of cryptography (encryption-decryption) is accomplished using a fixed number of rounds, each round uses its own sub key and Feistel functions, the number of executed rounds negatively affect the efficiency of data cryptography (see figure 2) [31-40].
- Data size: Increasing the data size will rapidly decrease the cryptography process efficiency [41-50].
- Simplicity: It is difficult to change the sequence of operations required to perform encryption and decryption phases, the number of rounds is fixed and cannot be changed, also the block size and the PK size are fixed and cannot be changed [51-55].

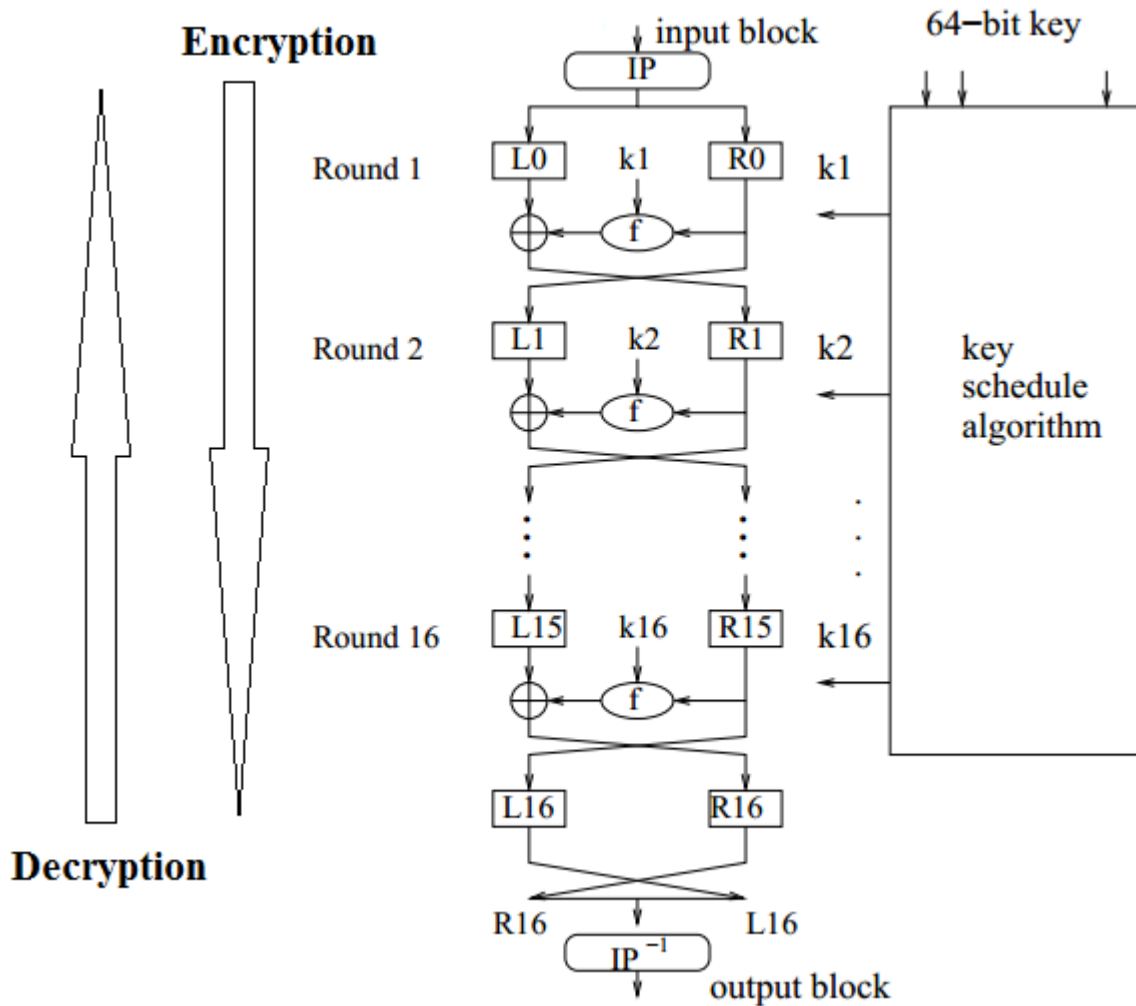


Figure 2: DES rounds

Indices keys generation

The proposed method uses a complicated PK, which has a complex structure as shown in figure 3:

PK								
R1	r1	x1	r2	x2	r3	x3	r4	x4
Example								
26	3.9	0.01	3.99	0.3	3,78	0.125	3.8	0.215

Figure 3: PK structure

The PK contains the chaotic parameters values required to run four CLMM to generate four chaotic logistic keys, these key then must be converted to indices keys to be used in the four rounds of message encryption-decryption, the

following sequence of operations uses 4 CLMM to generate the required secret keys to be used in 4 rounds of encryption-decryption:

```

R1=26;
r1=3.9;x1=0.325;
r2=3.8;x2=0.125;
r3=3.85;x3=0.065;
r4=3.79;x4=0.097;
for i=1:R1
    x1=r1*x1*(1-x1);
    x2=r2*x2*(1-x2);
    x3=r3*x3*(1-x3);
    x4=r4*x4*(1-x4);
    key1(i)=x1;
    key2(i)=x2;
    key3(i)=x3;
    key4(i)=x4;
end
[notused,kk1] = sort(key1);
[notused,kk2] = sort(key2);
[notused,kk3] = sort(key3);
[notused,kk4] = sort(key4);

```

CLMM parameters

CL keys

Keys with values: 1:26

Figure 4 shows an example of generated IKs using various values of chaotic parameters, while figure 5 shows the plots of these keys.

CLMM parameters	Generated keys
r1=3.9;x1=0.325;	4 21 24 9 17 5 15 7 22 2 25 19 13 11 10 12 18 1 6 14 16 8 23 20 3 26 Key 1
r2=3.8;x2=0.125;	11 26 14 3 1 24 9 12 22 7 20 5 18 16 15 17 4 19 6 21 8 23 2 13 25 10 Key 2
r3=3.85;x3=0.065;	19 25 22 6 14 1 9 20 26 17 23 4 12 7 15 2 10 11 3 16 8 13 5 21 24 18 Key 3
r4=3.79;x4=0.097;	5 21 16 8 24 1 14 3 26 19 6 22 12 17 10 9 11 18 25 2 13 23 7 15 20 4 Key 4

Figure 4: Generated IKs

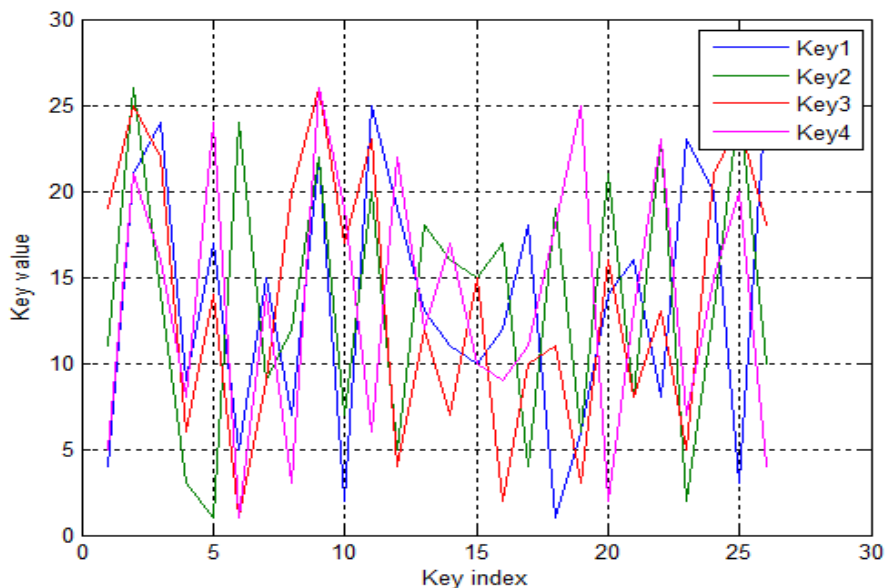


Figure 5: Plots of the generated IKs

From the figures 4 and 5 it is seen that any minor changes in the parameters r and x will lead to generate a new different IK. The generated CLK will remain fixed when fixing the chaotic parameters values, and the generated CLK are different from the random generated keys, the random keys must be saved because they will be change from run to run as shown in figure 6:

First run		Second run	
0.8556	0.2904	0.8556	0.0336
0.4819	0.6171	0.4819	0.0688
0.9737	0.2653	0.9737	0.3196
0.0998	0.8244	0.0998	0.5309
0.3503	0.9827	0.3503	0.6544
0.8876	0.7302	0.8876	0.4076
0.3892	0.3439	0.3892	0.8200
0.9271	0.5841	0.9271	0.7184
0.2636	0.1078	0.2636	0.9686
0.7570	0.9063	0.7570	0.5313
0.7174	0.8797	0.7174	0.3251
0.7906	0.8178	0.7906	0.1056
0.6456	0.2607	0.6456	0.6110
0.8924	0.5944	0.8924	0.7788
0.3746	0.0225	0.3746	0.4235
0.9137	0.4253	0.9137	0.0908
0.3075	0.3127	0.3075	0.2665
0.8305	0.1615	0.8305	0.1537
0.5489	0.1788	0.5489	0.2810
0.9657	0.4229	0.9657	0.4401
0.1293	0.0942	0.1293	0.5271
0.4391	0.5985	0.4391	0.4574
0.9605	0.4709	0.9605	0.8754
0.1479	0.6959	0.1479	0.5181
0.4915	0.6999	0.4915	0.9436
0.9747	0.6385	0.9747	0.6377
CLMM	Random	CLMM	Random
key	key	key	key

Figure 6: CLK vs random keys

The generated CLK s are converted to IKs using a built in matlab function 'sort', this function will return a key which can be used as a lockup table, the character ASCII value of the message is to be replaced by the index of the IK in the encryption phase, while the character of the encrypted message is to be replaced by the contents of the index, this will be explained in the following worked example:

Let us take the following chaotic parameters and run the CLMM:

$r1=3.9; x1=0.325;$

Figure 7 shows the CLK and the associated IK:

CLK	index	IK	
0.8556	1:	4	Character = f
0.4819	2:	21	Decimal =102
0.9737	3:	24	102-96=6
0.0998	4:	9	Encrypted =5,
0.3503	5:	17	5+96=101, Encrypted character: e
0.8876	6:	5	Decimal =101
0.3892	7:	15	101-96=5
0.9271	8:	7	5 is index 6 so decrypted =6
0.2636	9:	22	6+96=102
0.7570	10:	2	Decrypted =f
0.7174	11:	25	
0.7906	12:	19	
0.6456	13:	13	
0.8924	14:	11	
0.3746	15:	10	
0.9137	16:	12	
0.3075	17:	18	
0.8305	18:	1	
0.5489	19:	6	
0.9657	20:	14	
0.1293	21:	16	
0.4391	22:	8	
0.9605	23:	23	
0.1479	24:	20	
0.4915	25:	3	
0.9747	26:	26	

Figure 7: Using IK in cryptography

The Proposed Method

The proposed method uses the PK explained earlier to generate four IKs, which are used to apply four rounds of encryption in the encryption phase, and four rounds of decryption in the decryption phase.

The encryption phase as shown in figure 8 can be implanted applying the following algorithm:

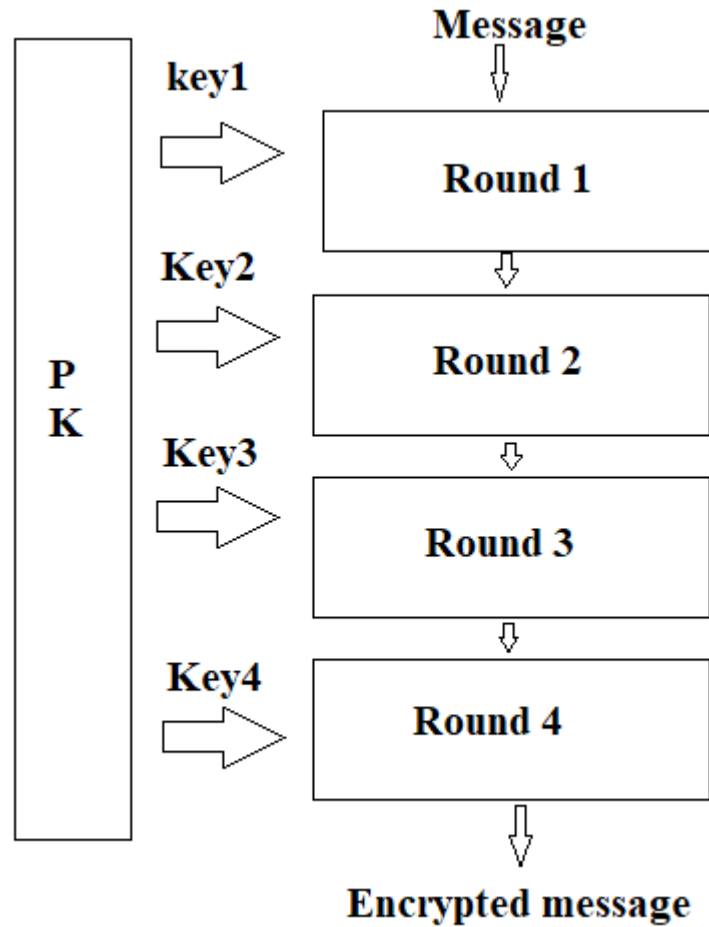


Figure 8: Encryption phase diagram

Inputs

Message to be encrypted, PK

Output

Encrypted message

Process

1. *Get the message.*
2. *Get the message length*
3. *Convert the message to decimal*
4. *Subtract 96 from each character value*
5. *Get the PK*

6. *Run the CLMMs to generate 4 CLKs*
7. *Convert CLKs to IKs*
8. *For each round starting from IK1 do*
9. *For each character value do*
10. *If the character value is less than 1 or greater than 26 proceed to the next character*
11. *Replace the character value by its index in the associated IK*
12. *Add 96 to the value obtained in step 11 to get the encrypted value*
13. *Convert the encrypted message back to characters*

The decryption phase can be implemented a similar way, figure 9 shows the decryption phase diagram, and this phase can be implemented applying the following algorithm:

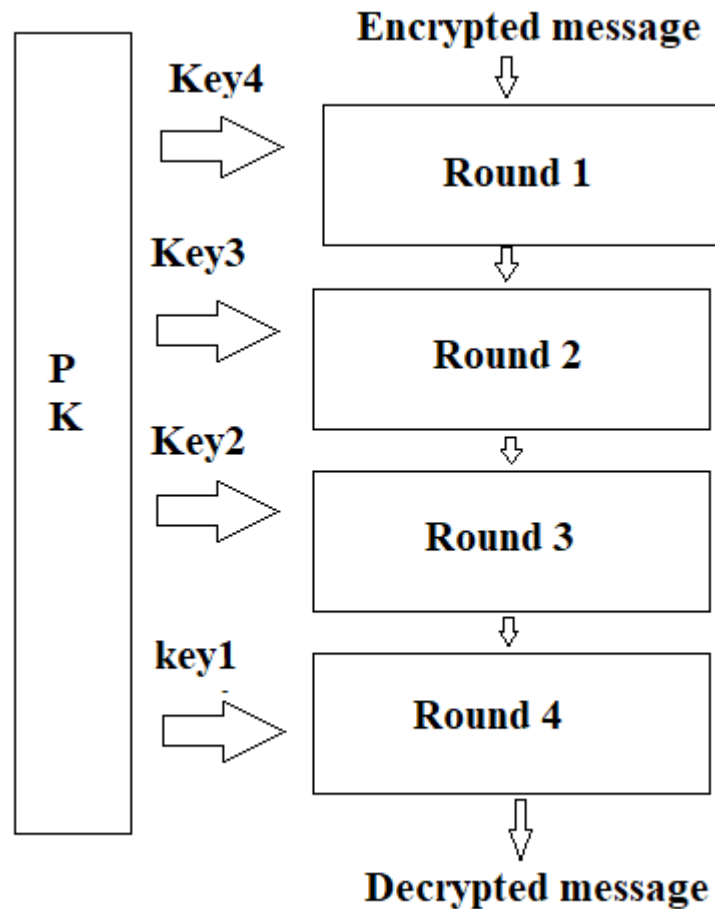


Figure 9: Decryption phase diagram

Inputs

Encrypted message, PK

Output

Decrypted message

Process

1. *Get the encrypted message.*
2. *Get the message length*
3. *Convert the message to decimal*
4. *Subtract 96 from each character value*
5. *Get the PK*
6. *Run the CLMMs to generate 4 CLKs*
7. *Convert CLKs to IKs*
8. *For each round starting from IK4 do*
9. *For each character value do*
10. *If the character value is less than 1 or greater than 26 proceed to the next character*
11. *Replace the character value by its index in the associated IK*
12. *Add 96 to the value obtained in step 11 to get the decrypted value*
13. *Convert the decrypted message back to characters*

Implementation and Experimental Results

The proposed method was implemented using various short messages; the messages were also encrypted-decrypted using DES method to make comparisons and to show how the proposed method increases the efficiency of message cryptography.

The short messages shown in table 2 encrypted-decrypted using DES method of data cryptography, table 3 shows the obtained performance results for DES.

Table 2: Used short messages

Message number	Length (byte)	Message
1	35	Amman is the capital city of Jordan
2	27	Secret message cryptography
3	33	Using color image as an image_key
4	48	Aqaba is a beautiful city located on the red see
5	71	Aqaba is a beautiful city located on the red see in the south of Jordan
6	17	Mean square error
7	26	Peak signal to noise ratio

8	29	Three levels of data security
9	35	Encryption: Fully image destruction
10	32	Decryption: Fully image recovery
Average	35.3000	

Table 3: Times results using DES (short messages)

Message number	Encryption time(second)	Decryption time(second)	Decryption throughput(byte per second)	Decryption throughput(byte per second)
1	0.0690	0.0820	507.2464	426.8293
2	0.0550	0.0810	490.9091	333.3333
3	0.0670	0.0810	492.5373	407.4074
4	0.0940	0.1070	510.6383	448.5981
5	0.1320	0.1460	537.8788	486.3014
6	0.0410	0.0710	414.6341	239.4366
7	0.0540	0.0760	481.4815	342.1053
8	0.0560	0.0780	517.8571	371.7949
9	0.0540	0.0760	648.1481	460.5263
10	0.0530	0.0750	603.7736	426.6667
Average	0.0675	0.0873	520.5104	394.2999

The same selected short messages were encrypted-decrypted using the proposed method; table 4 shows the obtained results:

Table 4: Times results using proposed method

Message number	ET(second)	DT(second)	Encryption Throughput (byte per second)	Decryption throughput (byte per second)
1	0.0160	0.0160	2187.5	2187.5
2	0.0120	0.0120	2250.0	2250.0
3	0.0100	0.0100	4800.0	4800.0
4	0.0170	0.0170	4176.5	4176.5
5	0.0160	0.0160	1062.5	1062.5
6	0.0160	0.0160	1625.0	1625.0
7	0.0150	0.0150	1933.3	1933.3
8	0.0160	0.0160	2250.0	2250.0
9	0.0150	0.0150	2333.3	2333.3
10	0.0150	0.0150	2133.3	2133.3
Average			2475.1	2475.1

As we can see from table 4, the proposed method is more efficient than DES method and it provides a significant speedup.

The encryption and decryption phases are very sensitive to any minor changes in the values of the PK components, any changes in the PK during the decryption phase will be considered as a hacking attempt by producing a damaged decrypted message. The message 'ziad alqadi' was taken and encrypted using PK1 shown below, the encrypted message was decrypted using various PKs, table 5 shows how changing the key will affect the decryption results:

PK1

R1=26;
r1=3.9; x1=0.325;
r2=3.8; x2=0.125;
r3=3.85; x3=0.065;
r4=3.79; x4=0.097;

PK2

R1=26;
r1=3.88; x1=0.325;
r2=3.8; x2=0.125;
r3=3.85; x3=0.065;
r4=3.79; x4=0.097;

PK3

R1=26;
r1=3.72; x1=0.325;
r2=3.8; x2=0.125;
r3=3.85; x3=0.065;
r4=3.79; x4=0.097;

PK4

R1=26;
r1=3.9; x1=0.725;
r2=3.8; x2=0.125;
r3=3.85; x3=0.065;
r4=3.79; x4=0.097;

PK5

R1=26;
r1=3.9; x1=0.725;
r2=3.8; x2=0.125;
r3=3.85; x3=0.165;
r4=3.79; x4=0.097;

PK6

R1=26;

r1=3.9; x1=0.725;

r2=3.8; x2=0.125;

r3=3.85; x3=0.065;

r4=3.79; x4=0.197;

Table 5: Using various PKs in the decryption phase

PK used in the encryption phase	PK used in the decryption phase	Encrypted message	Decrypted message
PK1	PK1	kxwl wepwlx	ziad alqadi
PK1	PK2	kxwl wepwlx	kfbo bazbof
PK1	PK3	kxwl wepwlx	ohfb fktfbh
PK1	PK4	kxwl wepwlx	jaew efzewa
PK1	PK5	kxwl wepwlx	wmsd sfqsdm
PK1	PK6	kxwl wepwlx	dhen exwenh

The private key contains 8 chaotic parameters values, each of them has a double data type (64 bits are used for value presentation), thus the number of combinations provided by the PK is very huge, so the PK will provide a huge key spaces which is equal 2 raised the power of $8*64=512$, this space will resist any type of attacks.

This method was design to replace a message character with another message, the IK size was equal 26, the method can be modified by using an IK with 256 length to replace the character with any other ASCII character.

For researchers who want to reproduce the method outputs the following codes may be useful:

Key generation

```

R1=26;
r1=3.9;x1=0.325;
r2=3.8;x2=0.125;
r3=3.85;x3=0.03;
r4=3.79;x4=0.197;
for i=1:R1
    x1=r1*x1*(1-x1);
    x2=r2*x2*(1-x2);
    x3=r3*x3*(1-x3);
    x4=r4*x4*(1-x4);
    key1(i)=x1;
    key2(i)=x2;
    key3(i)=x3;
    key4(i)=x4;
end

[notused,kk1] = sort(key1);
[notused,kk2] = sort(key2);
[notused,kk3] = sort(key3);
[notused,kk4] = sort(key4);
    
```

Encryption round operation (1 round)

```

numbers = double(lower(in)-96);
codednumbers = zeros(1,length(numbers));
for i = 1:length(numbers)
    if numbers(i) >= 1 & numbers(i) <= 26
        codednumbers(i) = kk1(numbers(i));
    else
        codednumbers(i) = numbers(i);
    end
end
coded1 = char(codednumbers+96);
    
```

Decryption round operation (1 round)

```

numbers = double(lower(en))-96;
decodednumbers = zeros(1,length(numbers));
for i = 1:length(numbers)
    if numbers(i) >= 1 & numbers(i) <= 26
        decodednumbers(i) = find(kk4==numbers(i));
    else
        decodednumbers(i) = numbers(i);
    end
end
de4 = char(decodednumbers+96);

```

Conclusion

A simple and efficient method of message cryptography was proposed. This method can be easily used to encrypt-decrypt any message with any length, the number of rounds can be changed, each round will require an IK. The method used a complicated PK, this key provided a huge key space and it is very sensitive to any minor changes, changing the PK in the decryption phase will produce a damaged decrypted image. The PK contained 8 chaotic parameters to run 4 CLMMs to get a CLKs, these keys were converted to indices key to be used as a lookup table in the encryption and decryption phases. The proposed method was implemented and it was shown that the method provided a significant speedup comparing with DES method of data cryptography.

References

- [1] Diao Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.
- [2] W. Stallings, Cryptography and Network Security, 4th Edition, Pearson Prentice Hall, 2006.
- [3] Singh S Preet, Mani Raman, "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communications, Vol. 2, No.1, January-June 2011, pp. 125-127.
- [4] Singh Gurjeevan, Kumar Ashwani, Sandha K.S. "A Study of New Trends in Blowfish Algorithm" International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326.
- [5] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSSE), Vol. 4 No. 05 May 2012, pp. 877-882.
- [6] Seth Shashi Mehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.
- [7] Mandal Pratap Chandra, "Superiority of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.
- [8] Apoorva, Kumar Yogesh, "Comparative Study of Different Symmetric Key Cryptography", IJAIEEM, vol. 2, Issue 7, July 2013, pp. 204-206.
- [9] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.
- [10] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.
- [11] Thakur Jawahar, Kumar Nagesh. "DES, AES and Blowfish Symmetric Key Cryptography algorithm Simulation Based Performance Analysis", IJETAE, vol. 1, Issue 2, DEC. 2011, pp. 6-12.

- [12]Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Ahmad Sharadqh, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, Vol. 8, Issue. 8, August 2019, pg.50 – 62.
- [13]Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2018.
- [14]Akram A. Moustafa and Ziad A. Alqadi, 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, 2009.
- [15]ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, World Applied Sciences Journal, vol. 5, issue 2, pp. 211-214, 2008.
- [16]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.
- [17]Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 76-90, 2019.
- [18]Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, Optimized True-RGB color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, ISSN 1818-4952, 2010.
- [19]Waheeb, A. and Ziad AlQadi, Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173, 2009.
- [20]A. A. Moustafa, Z. A. Alqadi, "Color Image Reconstruction Using a New R'G'I Model", Journal of Computer Science, Vol.5, No. 4, pp. 250-254, 2009.
- [21]K Matrouk, A Al-Hasanat, H Alasha'ary, Z. Al-Qadi Al-Shalabi, "Speech fingerprint to identify isolated word person", World Applied Sciences Journal, Vol. 31, No. 10, pp. 1767-1771, 2014.
- [22]Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi , A Novel Methodology to Extract Voice Signal Features , International Journal of Computer Applications, Volume 179 – No.9, January 2018.
- [23]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.
- [24]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.
- [25]M. Juneja, P. S. Sandhu, An improved LSB based Steganography with enhanced Security and Embedding/Extraction, 3rd International Conference on Intelligent Computational Systems, Hong Kong China, January 26-27, 2013.
- [26]H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. A alqadi, H. Al-Shalabi (2013), Improving Matrix Multiplication Using Parallel Computing, International Journal on Information Technology (I.RE.I.T.) Vol. 1, N. 6 ISSN 2281-2911.
- [27]Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein A COMPARISON BETWEEN PARALLEL AND SEGMENTATION METHODS USED FOR IMAGE ENCRYPTION-DECRYPTION, International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5, October 2016.
- [28]Z.A. Alqadi, A. Abu-Jazar (2005), Analysis of Program Methods Used for Optimizing Matrix Multiplication, Journal of Engineering, vol. 15 n. 1, pp. 73-78.
- [29]Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh: A Novel Based On Image Blocking Method to Encrypt-Decrypt Color JOIV: International Journal on Informatics Visualization, 2019.
- [30]Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub and Mazen Abu-Zaher: A Novel Zero-Error Method to Create a Secret Tag for an Image; Journal of Theoretical and Applied Information Technology 15th July 2018.
- [31]Jamil Al Azzeh, Ziad Alqadi Qazem, M. Jabber: Statistical Analysis of Methods Used to Enhanced Color Image Histogram; XX International Scientific and Technical Conference; Russia May 24-26, 2017.
- [32]Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata: Creating a Color Map to be used to Convert a Gray Image to Color Image; International Journal of Computer Applications (0975 – 8887). Volume 153 – No2, November 2016.
- [33]Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi Analysis of Matrix Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 76-90.
- [34]Mohammed Abuzalata; Ziad Alqadi, Jamil Al-Azzeh; Qazem Jaber Modified Inverse LSB Method for Highly Secure Message Hiding: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019, pg. 93-103.

- [35] Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019/3.
- [36] Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata; Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019.
- [37] Rashad J. Rasras, Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 14-26.
- [38] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad , Analysis of Color Image Features Extraction using Texture Methods , TELKOMNIKA, vol. 17, issue 3, 2018.
- [39] B. Zahran, J. AL-Azzeh, Z. Al Qadi, M. Al Zoghoul and S. Khawatreh, "A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 10, 2018.
- [40] J. AL-AZZEH, B. ZAHARAN, 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(JATIT), Vol.96. No 13, 2018.pp: 4081-4091.
- [41] J. AL-AZZEH, B. ZAHARAN, Z. ALQADI," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.
- [42] Jihad Nader, Ziad Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", International Journal of Computer Applications (IJCA), Volume 174, issue 8, 2017, pp:12-17.
- [43] Ziad Alqadi, Bilal Zahran, Jihad Nader, " Estimation and Tuning of FIR Low pass Digital Filter Parameters", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 2, 2017, pp:18-23.
- [44] Khaled Aldebei, Mua'ad M. Abu-Faraj, Ziad A. Alqadi, Comparative Analysis of Fingerprint Features Extraction Methods, Journal of Hunan University Natural Sciences, vol. 48, issue 12, pp. 177-182, 2022.
- [45] Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering and Science, vol. 6, issue 1, pp. 49-55, 2022.
- [46] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp. 648-656, 2021.
- [47] Ziad Alqadi Mua'ad Abu-Faraj , Khaled Aldebei, DEEP MACHINE LEARNING TO ENHANCE ANN PERFORMANCE: FINGERPRINT CLASSIFIER CASE STUDY, JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY, vol. 56, issue 6, pp. 686-694, 2021.
- [48] Ziad A. Alqadi Mua'ad M. Abu-Faraj, Improving the Efficiency and Scalability of Standard Methods for Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp. 451-458, 2021.
- [49] Mua'ad M. Abu-Faraj Prof. Ziad Alqadi, Using Highly Secure Data Encryption Method for Text File Cryptography, International Journal of Computer Science and Network Security, vol. 20, issue 11, pp. 53-60, 2021.
- [50] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, 2018.
- [51] 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.
- [52] Ziad A Alqadi, Mohamad Tariq Barakat, A Case Study to Improve the Quality of Median Filter, International Journal of Computer Science and Mobile Computing, vol. 10, issue 11, pp. 19 – 28, 2021.
- [53] Dr. Hatim Ghazi Zaini Prof. Ziad Alqadi, High Salt and Pepper Noise Ratio Reduction, International Journal of Computer Science and Mobile Computing, vol. 10, issue 9, pp. 88 – 97, 2021.
- [54] Prof. Mohamad K. Abu Zalata, Hussein N. Hatamleh, Prof. Ziad A. Alqadi, Detailed Study of Low Density Salt and Pepper Noise Removal from Digital Color Images, IJCSMC, Vol. 11, Issue. 2, PP. 56 – 67, February 2022.
- [55] M. Abu-Faraj, A. Al-Hyari, K. Aldebei, B. Al-Ahmad, and Z. Alqadi, "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography," IEEE Access, vol. 10, pp. 69388- 69397, 2022, doi:10.1109/ACCESS.2022.3187317.

- [56] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Experimental Analysis of Methods Used to Solve Linear Regression Models," *CMC-Computers, Materials & Continua*, vol. 72, no. 3, pp. 5699-5712, 2022, doi:10.32604/cmc.2022.027364. (Web of Science Indexed, Scopus Indexed).
- [57] 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, doi:10.3390/sym0664. (Web of Science Indexed, Scopus Indexed)
- [58] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography," *Traitement du Signal*, vol. 39, no. 1, pp. 173-178, 2022, doi:10.18280/ts.390117. (Web of Science Indexed, Scopus Indexed)
- [59] M. Abu-Faraj, and Z. Alqadi, "Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 21, no. 12, pp. 648-656, 2021, doi: 10.22937/IJCSNS.2021.21.12.89. (Web of Science Indexed)
- [60] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 21, no.12, pp. 451-458, 2021, doi:10.22937/IJCSNS.2021.21.12.61. (Web of Science Indexed)
- [61] M. Abu-Faraj, and Z. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 21, no.12, pp. 53-60, 2021, doi:10.22937/IJCSNS.2021.21.12.8. (Web of Science Indexed)
- [62] M. Abu-Faraj, and M. Zubi, "Analysis and Implementation of Kidney Stones Detection by Applying Segmentation Techniques on Computerized Tomography Scans," *Italian Journal of Pure and Applied Mathematics*, iss. 43, pp. 590-602, 2020. (Scopus Indexed)