Available Online at www.ijcsmc.com/journal

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. 9, September 2022, pg.11 – 28

Bits and Characters Substitutions to Increase the Security Level of Transmitted Secret Message

Prof. Ziad Alqadi
Albalqa Applied University
Faculty of Engineering Technology
Jordan Amman
DOI: https://doi.org/10.47760/ijcsmc.2022.v11i09.002

Abstract: Chaotic logistic map model is an interesting tool, it has good features, which make it capable to create chaotic keys, these keys are stable and sensitive to the selected values of chaotic parameters. In this paper research we will introduce a simple, secure and efficient method of secret message cryptography. The encryption-decryption phases will be implemented in two rounds. Two secret keys will be used; these keys will be generated by running two CLMM with a selected chaotic parameter. The first key 'CSK' will be used for message characters' substitution, while the second secret key 'BSK' will be used for message binary version bits' substitution. The two secret keys will be generated using a PK which contains the selected values of the CLMM. The PK will provide a huge key space capable to resist any hacking attack, also the generated two keys will be sensitive to any changes in the PK components, making any minor changes in these components in the decryption phase will be considered as a hacking attempt. The proposed method will be implemented using various messages, the obtained results will be analyzed using various types of data analysis method to prove the quality, security and the efficiency of the proposed method.
Keywords: Cryptography, CLMM, CLK, BSK, CSK, MSE, PSNR, CC, NSCR, throughput.

Abbreviations

The following abbreviations will be used in this paper research:
CLMM: chaotic logistic map model
CLK: chaotic logistic key
BSK: bits substitution key
CSK: characters substitution key
ET: encryption time
DT: decryption time
MSE: mean square error
PSNR: peak signal to noise ratio
CC: correlation coefficient
NSCR: number of sample change ratio
TP: throughput

Introduction

Data cryptography [40 45] is one of the most popular methods used to protect the secret transmitted messages. Cryptography can be described and explained used the following simple scenario:
Let's say there's a person named *Ziad*. Now suppose *Ziad* sends a message to his son Odai who is on the other side of the world. Now obviously he wants this message to be private and nobody else should have access to the message (see figure 1). He uses a public forum, for example, Whatsapp for sending this message. The main goal is to secure this communication.

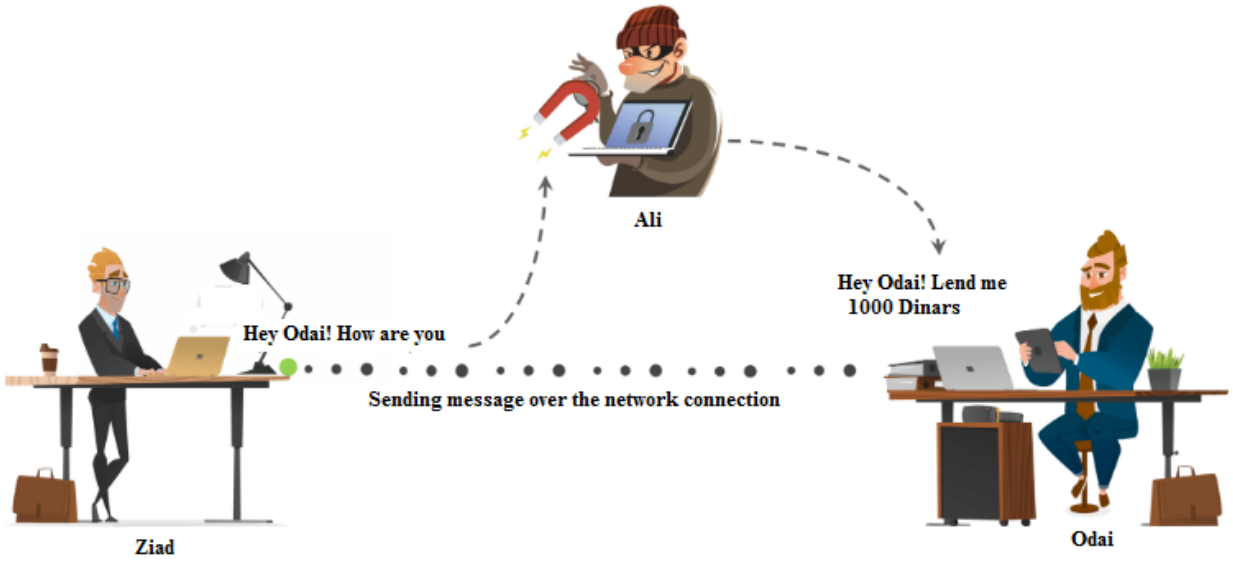

Figure 1: Unsecure message transmission

Let's say there is a smart hacker called *Ali* who secretly got access to your communication channel. Since this hacker has access to your communication, he can do much more than just eavesdropping, for example, he can try to change the message. Now, this is just a small example. What if *Ali* gets access to your private information? The result could be catastrophic [15-20].
So how can *Ziad* be sure that nobody in the middle could access the message sent to *Odai*? That's where ***Encryption or Cryptography*** comes in

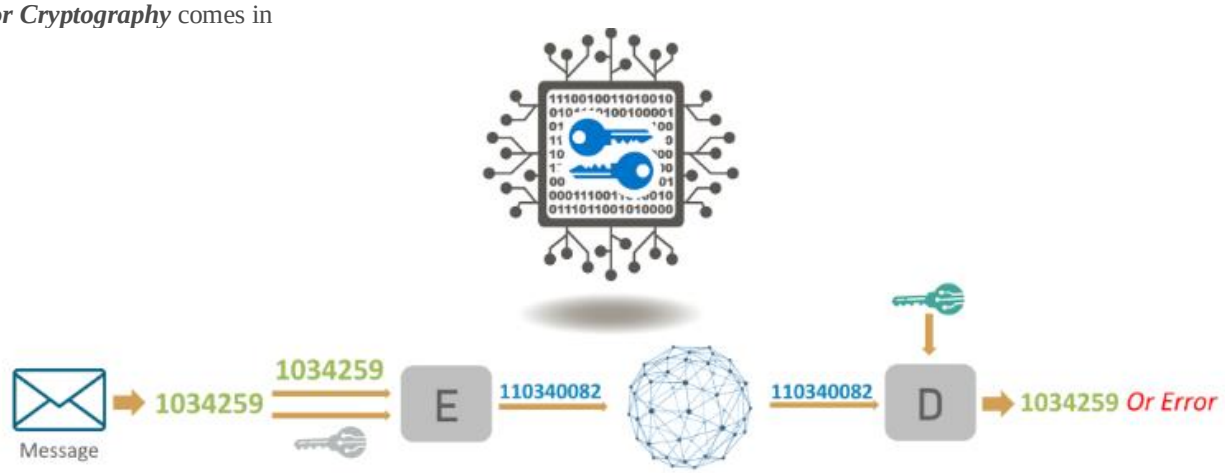

Figure 2: Using PK to secure the message

So, to protect his message, *Ziad* first convert his readable message to unreadable form. Here, he converts the message to some random numbers. After that, he uses a key to encrypt his message and **get** *cipher text (see figure 2)*.
Ziad sends this *ciphertext* [20-26]or encrypted message over the communication channel; he won't have to worry about somebody in the middle of discovering his private messages. Suppose, *Ali* here discover the message and he somehow manages to alter it before it reaches *Odai*.
Now, *Odai* would need a key to decrypt the message to recover the original plaintext. In order to convert the ciphertext into plain text, *Odai* would need to use the decryption key. Using the key, he would convert the ciphertext or the numerical value to the corresponding plain text (see figure 3).

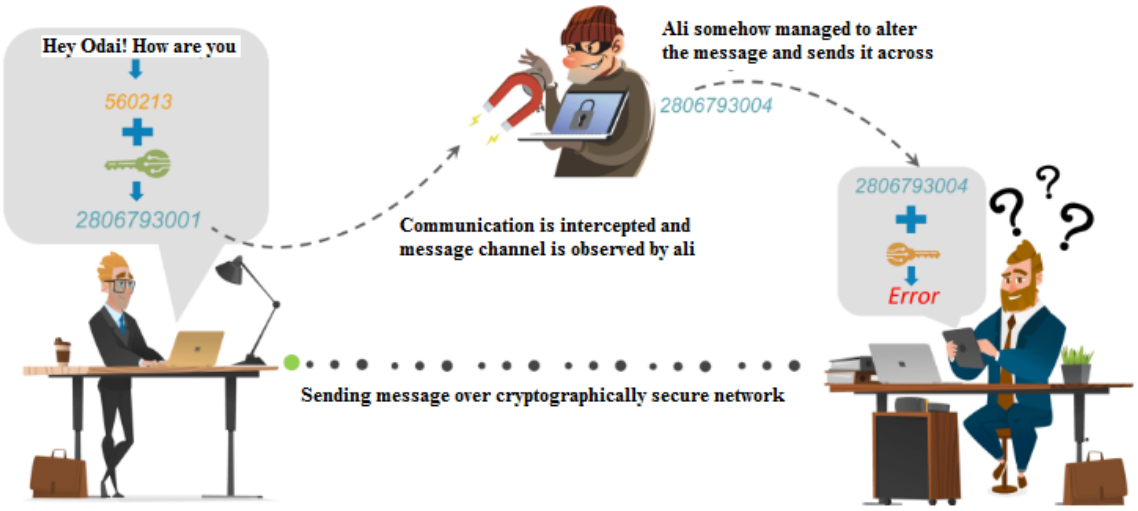

Figure 3: Secure message transmission

The model of data cryptography as shown in figure 4 contains the following components [35-40]:

- Secret message to be encrypted/decrypted
- One or more PKs
- Encryption/decryption method (algorithm)
- Encrypted/decrypted message

The encryption algorithm must destroy the secret message, making it unreadable and useless, while the decryption algorithm must recover a message identical to the source input message [30-36].

Any selected good method of message cryptography must satisfy the following requirements:

- Simplicity and flexibility, the method must be capable to treat any message with any length without the need to make any changes in the algorithm [10-15].

- Security, the PK must provide a huge key space capable to resist any kind of hacking attacks.

- Efficiency, the ET and DT must be minimized; here the method must maximize the throughput of message cryptography [26-30].

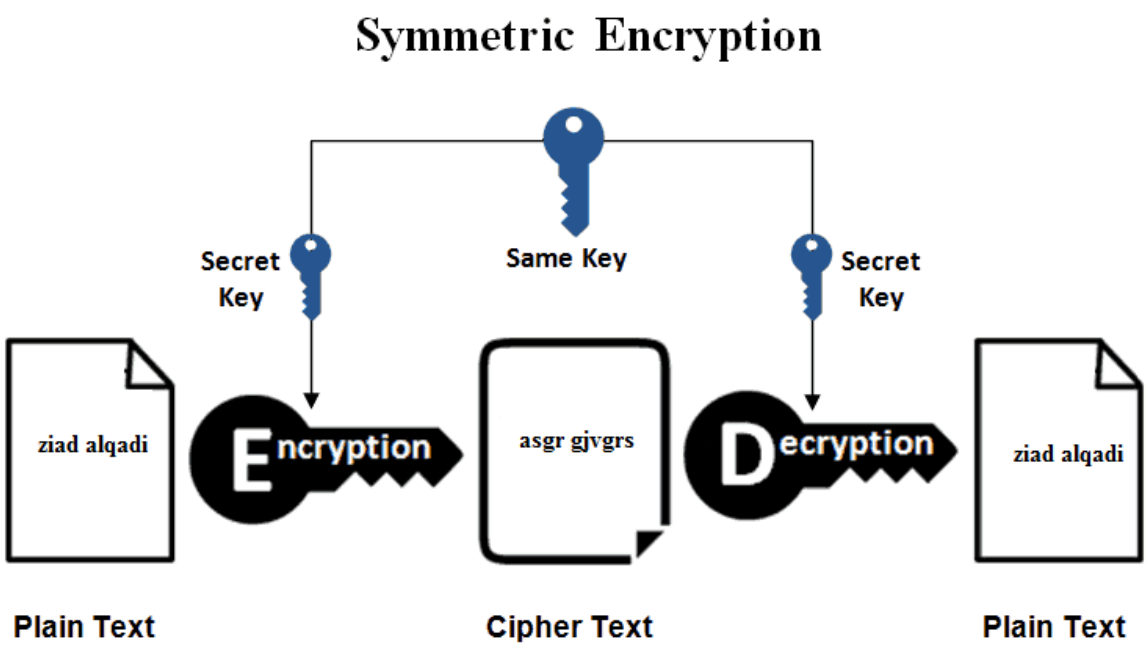

Figure 4: the model of message cryptography

- The method must provide low message quality in the encryption phase, and high quality message in the decryption phase, the quality of the message in the encryption and decryption phases can be measured by MSE, PSNR, CC and NSCR, and a good method of image cryptography must satisfy the requirements shown in table 1[26-29]:
-

Table 1: Quality requirements

Parameter	Between source and encrypted images	Between source and decrypted images
MSE	Very high	Zero
PSNR	Very low	Infinite
CC	Very low	1
NSCR	Closed to 100%	Closed to zero

Data protection is a very important matter, which prompted many researchers to provide various methods of encryption with varying values in efficiency. Some methods were based on the standards DES, AES, 3DES and BF, these methods are good for small in size data, when the data size increased (as an image), these methods became inefficient, and table 2 shows the throughputs of these standard methods [1]:

Table 2: Throughput of standard methods

	DES	3DES	AES	BF
Throughput(byte per second)	835	292	491	1038

Standard based methods of data cryptography share common features such as:

- The message must be divided into blocks with equal sizes and the block size is fixed.
- The PK is a fixed in length key and it is used to generate other sub keys.
- The cryptography is accomplished using a fixed number of rounds
- The encryption-decryption algorithms are complicated and contain a long sequence of logical and arithmetic operations.
- The low throughputs of these methods
- Some of these methods are not enough secure.

Some researchers [2-7] introduced a chaotic based method, these methods use one round of data cryptography, and for large size of input data they gave a good throughput.

The contributions of this paper research are to achieve the following:

- Eliminate the disadvantages of standard methods of message cryptography by using variable length blocks (one block can be used), using variable length of PK, and variable number of rounds.

- Enhance the performance of message cryptography by increasing the throughput of the process of cryptography.

- Improving the process of using chaotic logistic keys in message cryptography by decreasing the key generation time.

- Improving the level of message security by increasing the key space capable to resist any kind of attacks.

- Increasing the sensitivity of decryption process, making any minor changes in the private key during the decryption phase hacking attempt by producing a damaged decrypted message.

- Simplifying the process of message cryptography by minimizing the sequence of operations required for encryption and decryption phases.

The Proposed Method

The proposed method uses a complicated PK with complex structure as shown in table 3, this key can be used to apply two rounds of data cryptography, the number of rounds may be increased by adding the necessary chaotic parameters. The proposed method uses the PK to run two CLMMs to generate two CLK, theses keys can be easily converted to CSK and BSC by applying Mata lab function ‘sort’. The length of CSK must equal the message length, while the length of BSC must equal 8 (the number of column in the binary matrix, which represents the message).

Table 3: PK structure

PK	
CLMM 1 parameters	CLMM 2 parameters
r1, x1	**r2, x2**
Example	
3.99, 0.125	3.81, 0.05

The PK has 4 components each of them has a double data type, so the PK will provide a huge key space, which can resist hacking attacks (see equation 1):

$$Keyspace = 2^{64x4} = 2^{256} \quad (1)$$

BSC and CSK are generated by converting the calculated CLKs, the following is the sequence of operations required to run CLMMs to get the needed secret keys:

```
;:generation CSK (key1)
;L is message length
r1=3.91;x1=0.25;
for i=1:L
     x1=r1*x1*(1-x1);
     CLK1(i)=x1;
end
[d key1]=sort(CLK1);

;generation BSK (key2)
r2=3.77;x2=0.125;
for i=1:8
      x2=r2*x2*(1-x2);
     CLK2(i)=x2;
end
[d key2]=sort(CLK2);
```


Characters substitution can be applied the following steps (see figure 5):

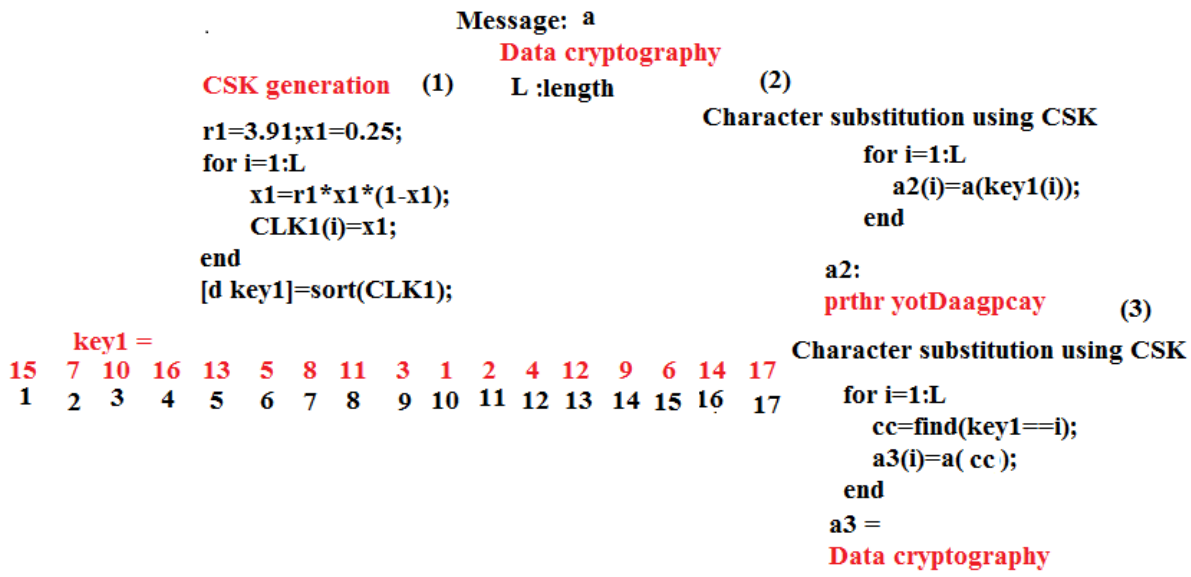

Figure 5: Using CSK

1- Get the PK parameters
2- Use r1 and x1 to run CLMM to get CLK
3- Convert CLK to CSK
4- In the encryption phase replace each character with the index in CSK
5- In the decryption phase replace each character with the content of the index in CSK.

Bits substitution can be applied using the following sequence of operations:

Encryption phase (see figure 6):

1- Get r2 and x2
2- Apply CLMM to get CLK2
3- Convert CLK2 to BSK
4- Get the message
5- Convert the message to decimal
6- Convert the decimal message to binary to get message binary matrix
7- Use the indexes of BSK to apply bits' substitution
8- Convert the binary message to decimal
9- Convert the decimal message to characters

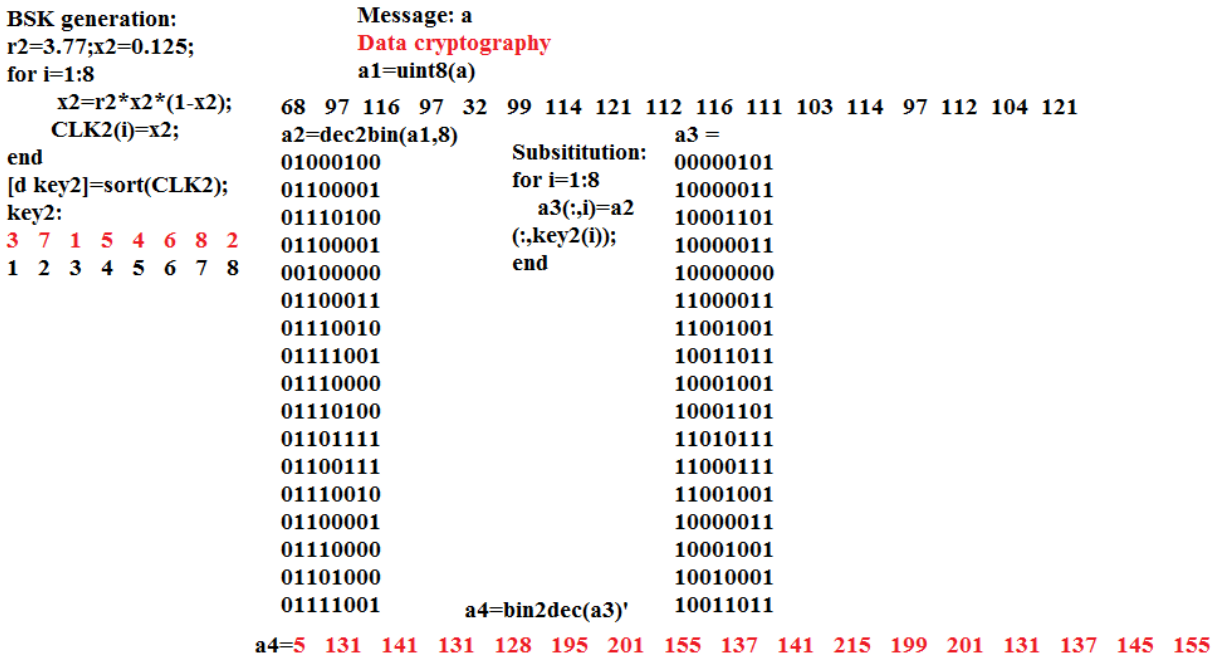

Figure 6: Using BSK in the encryption phase

Decryption phase (see figure 7):

1- Get r2 and x2

2- Apply CLMM to get CLK2

3- Convert CLK2 to BSK

4- Get the message

5- Convert the message to decimal

6- Convert the decimal message to binary to get message binary matrix

7- Use the contents of BSK indexes to apply bits' substitution

8- Convert the binary message to decimal

9- Convert the decimal message to characters


```
BSK generation:
r2=3.77;x2=0.125;
for i=1:8
      x2=r2*x2*(1-x2);
     CLK2(i)=x2;
end
[d key2]=sort(CLK2);
key2:
3  7  1  5  4  6  8  2
1  2  3  4  5  6  7  8
```

```
a4:
5  131  141  131  128  195  201  155  137  141  215  199  201  131  137  145  155
a5=dec2bin(a4,8)   bit substitution : for i=1:8
00000101                                ss=find(key2==i);
10000011       a6 =                     a6(:,i)=a5(:,ss);
10001101       01000100               end
10000011       01100001
10000000       01110100          a7=bin2dec(a6)'
11000011       01100001    68  97 116  97  32  99 114 121 112 116 111 103 114  97 112 104 121
11001001       00100000    char(a7)
10011011       01100011    Data cryptography
10001001       01110010
10001101       01111001
11010111       01110000
11000111       01110100
11001001       01101111
10000011       01100111
10001001       01110010
10010001       01100001
10011011       01110000
               01101000
               01111001
```

Figure 7: Using BSK in the decryption phase

Figures 8 and 9 show how to the sequence of applying characters and bits substitution in the encryption and decryption phases;

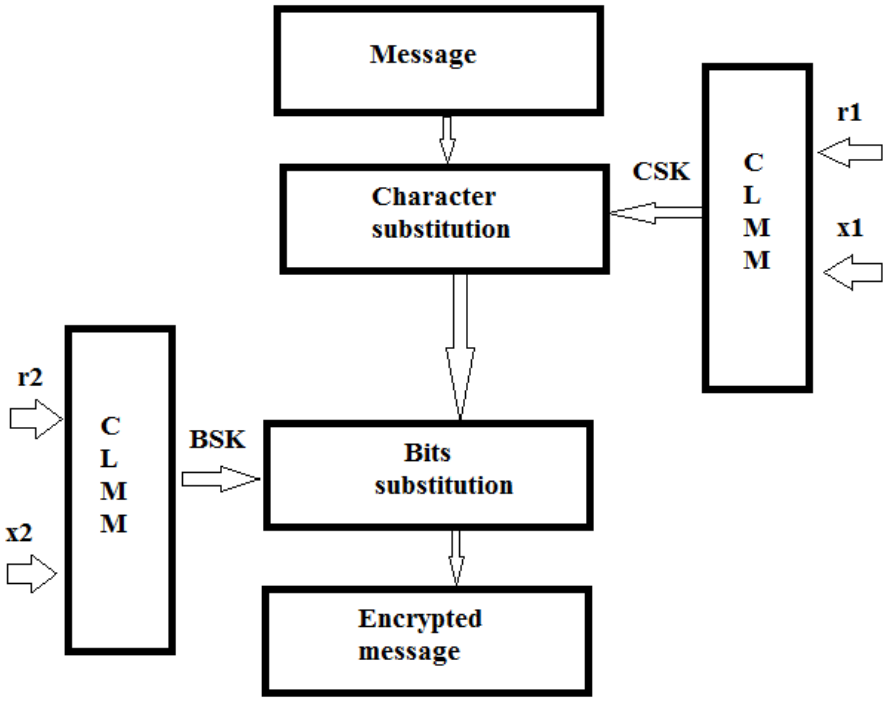

Figure 8: Encryption phase

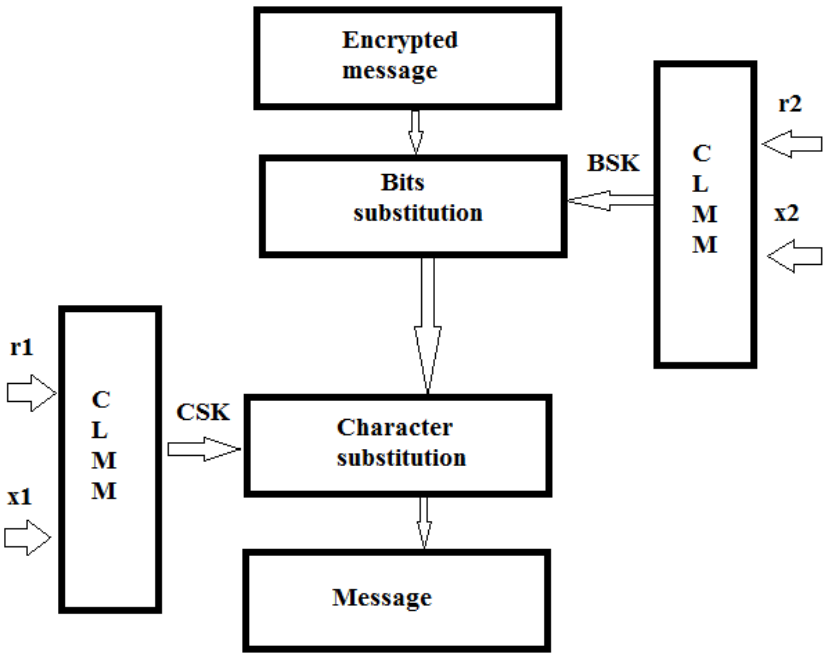

Figure 9: Decryption phase

Implementation and Results Analysis

The proposed method was implemented using various in size messages, the obtained results were analyzed using various types of data analysis methods to prove the quality and efficiency of the proposed method.

1- Visual Analysis

The encryption-decryption phase must satisfy the quality requirements by producing a damaged corrupted message in the encryption phase and producing a decrypted message which must be identical to the source message.
Several short messages were treated using the proposed method, table 4 shows the obtained encrypted and decrypted messages:

Table 4: Visual analysis

Source message	Encrypted message	Decrypted message
Data cryptography	□É□□É□□×□□□□Ç□Ã□□	Data cryptography
Characters substitution	□Õ□Ë□Ë□□□□□□□□C□É□Ë□É□Ã□Á×□	Characters substitution
Bits substitution	□□□×□□Å□□A□Ë□Ë□Ë□Õ	Bits substitution
Message protection	Õ□□É□□□□×Ë□□Ë□□ÇÃ×	Message protection
Chaotic logistic map model	□×□Ã×□□□Ã□Ë□□Ç□C□×□□□□□□□□	Chaotic logistic map model

From table 4 we can visually see that the encrypted messages are a damaged messages and the decrypted messages are identical to the source ones, this prove the quality of the proposed method.

2- Sensitivity Analysis

The generated chaotic logistic keys are very sensitive to selected values of PK parameters, any changes in one or more parameter value will lead to generate a different new key. Changing one or more parameters values in the decryption phase will be considered as a hacking attempt by producing a damaged corrupted decrypted message, table 5 shows the encrypted message using PK1 and the decrypted message using PK2:

PK1: r1=3.91; x1=0.25;

r2=3.77; x2=0.125;

PK2: r1=**3.77**; x1=**0.28**;

r2=3.77; x2=**0.145**;

Table 5: Sensitivity Analysis

Source message	Encrypted message	Decrypted message
Data cryptography	□É□□É□□×□□□□Ç□Ã□□	Hxb cxbëkqbqòpàòp
Characters substitution	□Õ□Ë□□Ë□□□□□□□□C□É□Ë□É□Ã□Á×□	b ÀâasCjqxëébszâxzqxxsc
Bits substitution	□□□×□□À□□A□Ë□Ë□Ë□Ó	Axs sxââxzxzasëéâ
Message protection	Õ□□É□□□□×Ë□□Ë□□ÇÃ×	Êssjkjjëxâcx pqëéb

From table 5 we can see that the decryption phase is very sensitive to any changes in the PK, any changes in the PK during the decryption phase will produce a damaged corrupted message.

3- MSE and PSNR Analysis

Quality between two messages can be measured by Mean square error (MSE) and peak signal to noise ratio (PSNR), high value of MSE and low value of PSNR points to the low quality, while low MSE and high PSNR points to the high quality. A good method of data cryptography must provide a low quality (high MSE and low PSNR) in the encryption phase and a high quality (low MSE and high PSNR) in the decryption phase. MSE and PSNR can be calculated using equations 2 and 3:

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \text{dB}, \quad \textbf{(2)}$$

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (x_i - y_i)^2, \quad \textbf{(3)}$$

Where: MAX is the maximum possible value of ASCII values, *N* is the total number of samples, xi and yi are the corresponding sample values of the source and encrypted/decrypted messages.

Some short messages were selected and were treated using the proposed method; MSE and PSNR were calculated between the source messages and the encrypted ones and between the source messages and the decrypted ones, table 6 shows the obtained results(MSEs between the source and decrypted messages were always zero, .while PSNRs were always infinite)

Table 6: Obtained Quality results using short messages

Message number	Length (byte)	Between source and encrypted messages			
		MSE	PSNR	CC	NSCR
1	10	8098.5	20.1934	-0.0770	100
2	20	14754	14.5960	-0.2553	100
3	50	10350	18.1410	-0.1162	98
4	75	9376.8	19.1287	0.0563	100
5	100	10708	17.9588	-0.0015	100
6	120	8819.6	19.9780	0.0902	100
7	150	11598	17.2394	-0.0354	98.6667
8	175	11829	16.8851	-0.0486	99.4286
9	180	11287	17.4326	0.0241	100
10	200	10641	18.1010	0.0153	100

The results (High MSEs and low PSNRs shown in table 6) show that the proposed method satisfy the quality requirements in the encryption phase.

.Long messages were selected and were treated using the proposed method; MSE and PSNR were calculated between the source messages and the encrypted ones and between the source messages and the decrypted ones, table 7 shows the obtained results(MSEs between the source and decrypted messages were always zero, .while PSNRs were always infinite)

Table 7: Obtained Quality results using long messages

Message number	Length (K bytes)	Between source and encrypted messages			
		MSE	PSNR	CC	NSCR
1	1	11043	17.7297	0.0201	99.8047
2	10	11005	17.7644	-0.0106	99.5996
3	20	10781	17.9698	0.0060	99.6484
4	35	10744	18.0045	0.0105	99.5703

5	40	10805	17.9479	0.0022	99.6216
6	50	10821	17.9328	0.0047	99.5781
7	60	10767	17.9829	0.0073	99.6322
8	75	10786	17.9649	-0.00020	99.6276
9	80	10877	17.8815	0.0026	99.6204
10	100	10886	17.8725	-0.0065	99.5713

The results (High MSEs and low PSNRs shown in table 7) show that the proposed method satisfy the quality requirements in the encryption phase.

4- Correlation Analysis

Measuring correlation coefficient between two messages express the dependency between their corresponding ASCII values. This is another statistical evaluation for testing the quality of the algorithm of data cryptography. Calculating correlation coefficient determines the level of correlation between two files and the correlation coefficient is always in range [−1,1]. Values between |1–0.7| is considered as strong correlation (samples from the source files are similar to samples from the encrypted file), correlation between |0.7–0.3| is considered as medium correlation and values between |0.3–0| is considered as weak correlation.

Correlation coefficient can be calculated using equation 4:

N is the total number of samples, xi and yi are the sample values of the two messages, $\bar{x}$ and $\bar{y}$ are the mean values of samples, and finally cov (x, y) is covariance between both files.

$$\mathbf{CC}_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad \textbf{(4)}$$

where

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2,$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2,$$

$$cov(x,y) = \sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}),$$

The selected short messages were treated using the proposed method, CCs were calculated between the source messages and the encrypted ones, table 6 shows the obtained results (CCs between the source messages and the decrypted one was always equal 1). The low values of CCs indicate the low quality of the encryption phase.

Long messages were also treated CCs were calculated, the low values of CCs (see table 7) prove that the proposed method satisfied the quality requirements

5- Number of Sample Change Rate

Number of sample change rate (NSCR) is robustness test for establishing the quality of data cryptography algorithms. The purpose of the test is to compare the corresponding sample values of the source and encrypted/decrypted messages and to show the difference in percent. NSCR can be calculated using equation 5:

$$NSCR = \frac{\sum_{i=1}^{N} D_i}{N} \times 100\%, \quad \textbf{(5)}$$

where

$$D_i = \begin{cases} 1, x_i \neq y_i \\ 0, Otherwise \end{cases}$$

The selected messages (short and long) were treated using the proposed method, NSCRs were calculated between the source messages and the encrypted ones, tables 6 and 7 show the obtained results (NSCR between the source and decrypted messages was always 0).

The results NSCRs showed in tables 6 and 7 showed that the proposed method satisfy the quality requirements the encryption and phase.

6- Efficiency Analysis

The selected messages were treated using the proposed method, ETs/DTs were calculated, and tables 8 and 9 show the results for short and long messages

Table 8: Speed results for short messages

Message number	ET/DT(seconds)	ETP/DTP(K byte per second)
1	0.0190	0.5140
2	0.0160	1.2207
3	0.0170	2.8722
4	0.0170	4.3084
5	0.0170	5.7445
6	0.0170	6.8934
7	0.0180	8.1380
8	0.0170	10.0528
9	0.0170	10.3401
10	0.0180	10.8507

Table 9: Speed results for long messages

Message number	ET/DT(seconds)	ETP/DTP(K byte per second)
1	0.0870	11.4943
2	0.3730	26.8097
3	0.9370	21.3447
4	1.8110	19.3263
5	2.1800	18.3486
6	3.1150	16.0514
7	4.3270	13.8664
8	7.7920	9.6253
9	9.3310	8.5736
10	16.6160	6.0183

From tables 8 and 9 we can see that the throughput of the proposed method will increase when increasing the message length, for long messages the throughput will reach the maximum value (26.8097 K byte per second) when the message length equal 10 K bytes., using messages with longer size will drop down the throughput, this because the chaotic logistic key generation process requires more time when the key length is long, figures 10 shows how the ET/DT will increase when the message is too long, the throughput will increase until the message reaches a certain length (10 K bytes in our case).

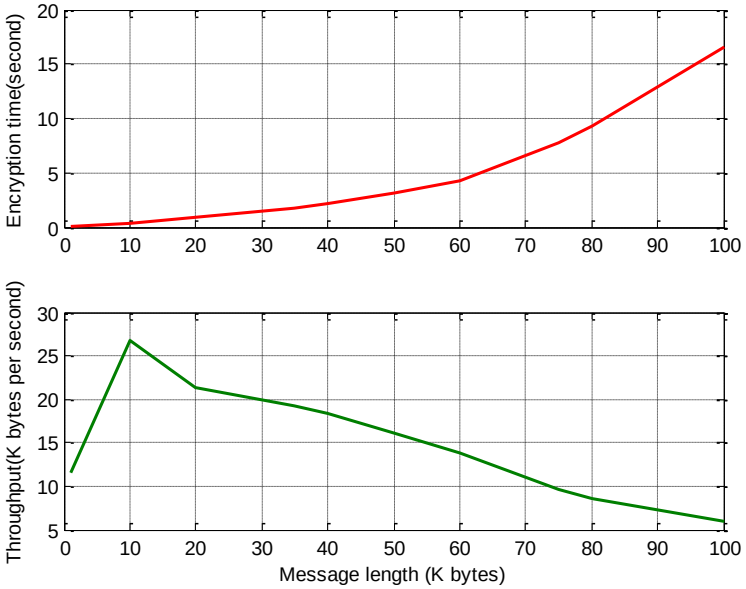

Figure 10: ET and TP vs message length

Conclusion

CLMMs were used to generate two keys, CSK for message characters substitution, and BSK for message binary version substitution; these two keys were used to apply two rounds of message cryptography. It was shown that using these two keys is very efficient in encrypting and decrypting messages with length not greater than 10 K bytes.

The proposed method used a complicated PK which provided a huge key space capable to resist hacking attacks, the decryption process is very sensitive to any minor changes in the PK parameters during the encryption phase, any minor changes here will be considered as a hacking attempt by producing decrypted damaged message.

The proposed method was implemented using short and long messages, the obtained results were analyzed using several methods of data analysis and it was proved that the proposed method satisfied the quality requirements by providing a low quality in the encryption phase and an excellent high quality in the decryption phase.

References

[1] Aamer Nadeem, Dr M. Younus Javed, A Performance Comparison of Data Encryption Algorithms, Conference Paper · September 2005 DOI: 10.1109/ICICT.2005.1598556 · Source: IEEE Xplore.

[2] 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.

[3] 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

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

[5] 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.

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

[7] 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.

[8] Liu, H.; Kadir, A.; Li, Y. Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys. *Optik* **2016**, *127*, 7431–7438.

[9] Hato, E.; Shihab, D. Lorenz and Rossler Chaotic System for Speech Signal Encryption. *Int. J. Comput. Appl.* **2015**, *128*, 09758887.

[10] Sathiyamurthi, P.; Ramakrishnan, S. Speech encryption using chaotic shift keying for secured speech communication. *EURASIP J. Audio Speech Music Process.* **2017**, *2017*, 20.

[11] Tamimi, A.A.; Abdalla, A.M. An Audio Shuffle-Encryption Algorithm. In Proceedings of the World Congress on Engineering & Computer Science, San Francisco, CA, USA, 22–24 October 2014; Volume 1.

[12] Preishuber, M.; Hütter, T.; Katzenbeisser, S.; Uhl, A. Depreciating motivation and empirical security analysis of chaos-based image and video encryption. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2137–2150.

[13] Krasimir Kordov, A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture *Electronics* 2019, *8*(5), 530; https://doi.org/10.3390/electronics805053

[14] K Matrouk, A Al-Hasanat, H Alasha'ary, Z Al-Qadi, H Al-Shalabi, World Applied Sciences Journal 31 (10), 1767-1771, 2014.

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

[16] Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications, vol. 179, issue 2, pp. 40-43, 2018.

[17] 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.

[18] 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.

[19] Jihad Nader 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.

[20] Belal Zahran Rashad J Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, B Zahran, developing new Multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 6, pp. 3228-3235, 2019.

[21] 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.

[22] 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.

[23] 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.

[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] 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.

[26] 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.

[27] 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.

[28] 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.

[29] Aws AlQaisi, Mokhled AlTarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, pp. 1220-1225, 2019.

[30] Ziad AA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Multiple Skip Multiple Pattern Matching Algorithm (MSMPMA), IAENG International Journal of Computer Science, vol. 34, issue 2, 2007.

[31] Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 21 – 37, 2020.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

