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. 11, November 2022, pg.131 – 150

Secure Method to Protect Secret Short Messages using Rearrangement Key

Dr. Rushdi S. Abu Zneit; Prof. Ziad Alqadi
Albalqa Applied University, Faculty of Engineering Technology, Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i11.010

Abstract: An efficient, highly secure and simple method of short messages cryptography method will be introduced. The method will use a rearrangement key to encrypt-decrypt SMs, the key will be generated by running a chaotic logistic map model with a selected parameter, these parameters will form the private secret key which is known by the data sender and the data receiver. The private key will provide the necessary key space to resist hacking attacks. The SM up to I K bytes will be encrypted-decrypted using RK, if the message size is greater than 1 K bytes, the message will be divided into blocks of 1 K bytes' length, and each block can be encrypted-decrypted using its own RK. The method will be simple and easy to implement, and it can suit any message with any length, the process of encryption is based on putting the character from the SM in its position maintained in the RK, the decryption will be implemented by recovering the characters from the decrypted SM by the indexes in the RK from the index 1 to the index L (L: is the message length).

The proposed method will be implemented using various SMs, the results will be analyzed. Based on the obtained values of MSE, PSNR, CC and NSCR it will be proved that the proposed method satisfies the quality requirements in the encryption and decryption phases. The speed of the proposed method will be tested and the obtained results will be compared with other methods speed to show the improvements provided by the proposed method.

Keywords: Cryptography, PK, CLMM, CLK, RK, TP, MSE, PSNR, CC, NSCR.

Abbreviations

The following abbreviations will be used in this research paper:
PK: private key
CLK: chaotic logistic key
CLMM: chaotic logistic map model
SM: secret message
SSM: short secret message

RK: rearrangement key
ET: encryption time
DT: decryption time
TP: throughput
SM: secret message
MSE: mean square error
PSNR: peak signal to noise ratio
CC: correlation coefficient
NSCR: number of samples change ratio

Introduction

End-to-end encryption is the encryption of messages on your device and decrypted only on the device of the person you are communicating with. That is, the message is transmitted as it is sent from the sender to the recipient in encrypted form, so no one can read it except for the person who is meant to receive it.

One alternative is to transfer data in clear text, i.e. without encrypting the message at all. This is the least secure option. For example, data sent via SMS is not encrypted, which in theory means that anyone can intercept it. Fortunately, this practically requires special equipment, which somewhat limits the number of people who can eavesdrop on your messages [45-50].

There is also encryption in transit, which is when messages are encrypted from the sending end, delivered to the server, then decrypted there, re-encrypted, then delivered to the recipient and decrypted again. In-transit encryption protects information as it is sent, but allows the contents of messages to be seen by the intermediate link in the chain: the server. Perhaps this servant will deal with your secrets responsibly, and perhaps he will not. You just have to trust its owner - and this can be a problem [50-54].

But at the same time, in many cases it may be more appropriate to use in-transit encryption rather than end-to-end encryption. This is because encryption in transit allows the server to be part of the connection and thus provides a set of services that go beyond simply transferring encrypted data from one user to another. For example, the server can store your message history, connect additional conversation participants via alternate channels (such as joining a video conference call), use automatic moderation, and so on [35-40].

Messages may be private or secret, thus they require a high level of protection when using unsecure communication environment [22-26]. One of the most popular techniques to protect the secret messages is data cryptography, which means encrypting the message before sending it and decrypting the message after receiving it. Cryptography may be symmetric or asymmetric. Symmetric encryption involves the use of one secret private key (as shown in figure 1) for both encryption and decryption phases. The plaintext is read into an encryption algorithm along with a PK. The key works with the algorithm to turn the plaintext into ciphertext, thus encrypting the original sensitive data. This works well for data that is being stored and needs to be decrypted at a later date. The use of just one key for both encryption and decryption reveals an issue, as the compromise of the key would lead to a compromise of any data the key has encrypted [27-32]. This also does not work for data-in-motion, which is where asymmetric encryption comes in.

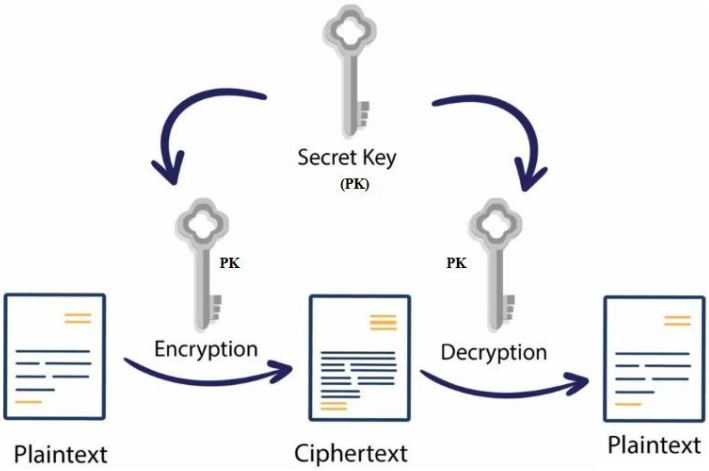

Figure 1: Symmetric data cryptography

Asymmetric encryption works with a pair of keys. The beginning of asymmetric encryption involves the creation of a pair of keys, one of which is a public key, and the other which is a private key (see figure 2) [40-50]. The public key is accessible by anyone, while the private key must be kept a secret from everyone but the creator of the key. This is because encryption occurs with the public key, while decryption occurs with the private key [11-20]. The recipient of the sensitive data will provide the sender with their public key, which will be used to encrypt the data. This ensures that only the recipient can decrypt the data, with their own private key [1-10].

To secure and protect the secret message, key size is the most important parameter in symmetric and asymmetric cryptography. The key size of symmetric cryptography is less than the asymmetric cryptography which make symmetric cryptography less secure for more sensitive data [33-39].

The encryption/decryption time of asymmetric cryptography is greater than the symmetric cryptography which makes encryption/decryption more complex for a large amount of data [3], [4]. Due to larger key size and greater key generation time of asymmetric cryptography, public key cryptography is used once for key exchange only and further encryption/ decryption is done by symmetric key cryptography [5], [6].

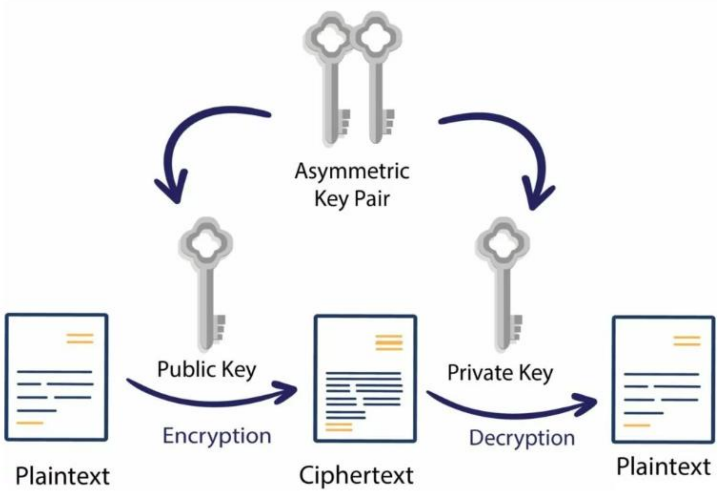

Figure 2: Asymmetric data cryptography

Many standards for message cryptography were introduced, here in this research paper we will focus on the most popular standard, the proposed method will be compared with these standard, below a brief description of these standards will be given:

- DES:

a symmetric cryptographic algorithm used for encryption and decryption of data [10]. In DES, only one secret private key is used for both encryption and decryption. The key size of DES is 56-bit (see figure 3). To encrypt-decrypt the data, the data must be divided into blocks with equal size (64 bits blocks), the encryption/decryption process is to be repeated in 16 rounds, each round performs specific logical and arithmetic operations, the key space provided by DES is small and it cannot resist hacking attacks. Another version of DES is 3DES (see figure 4), which increases the PK length to 168 bits making the process of cryptography more secure, but slowly.

- AES:

AES is the advancement of 3DES algorithm [11]. Basically, AES is based on the Rijndael cipher developed by two cryptographers, Joan Daemon and Vincent Rijmen. AES is different from DES and 3DES due to variables key sizes such as 128,192, and 256 bits [12] (see figure 5). Same like DES and 3DES, AES also performs encryption on blocks which are 128-bit [7]. AES algorithm is used in small devices for encrypting a message to send over a network. Some other applications are monetary transaction [12] and security applications [8] [13].

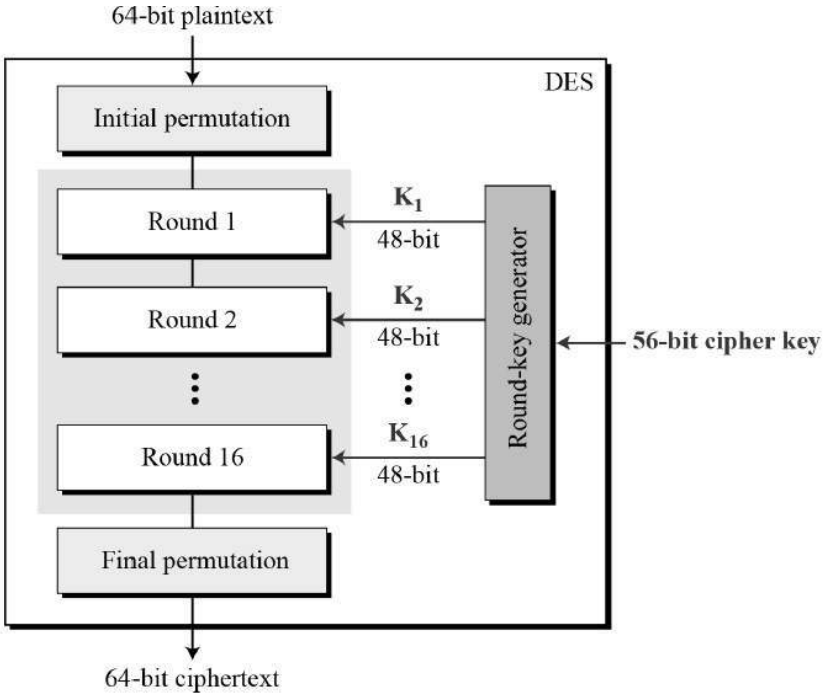

Figure 3: DES procedures

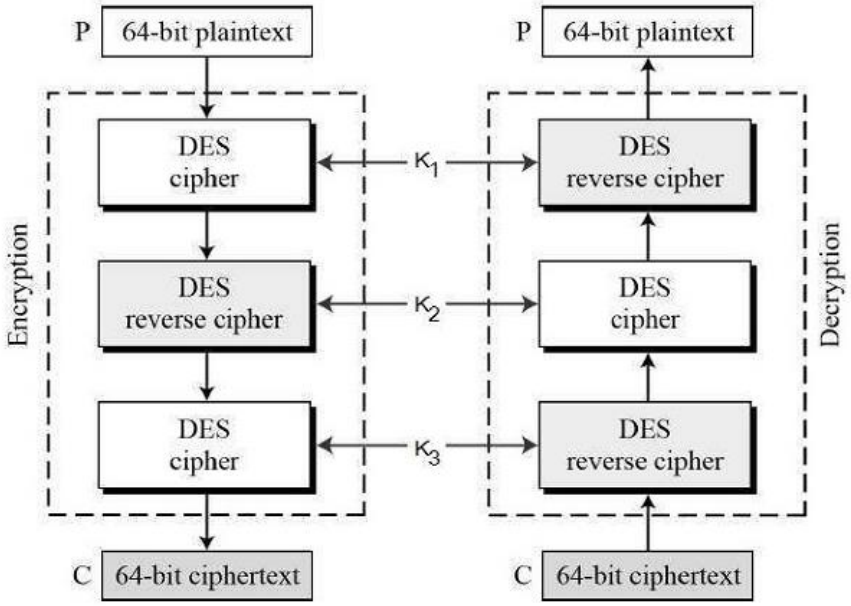

Figure 4: 3DES procedures

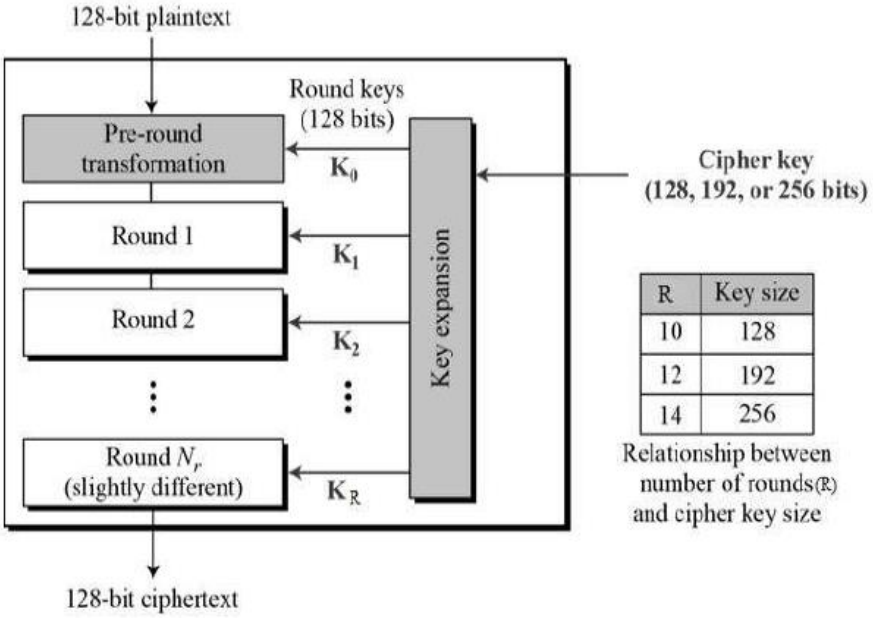

Figure 5: AES procedures

- RSA:

RSA (Rivest, Shamir and Adleman): RSA stands for Rivest, Shamir and Adleman who introduced the RSA algorithm in 1977 [14]. RSA is an asymmetric cryptographic algorithm [1] which is also used for encryption and decryption of the message. RSA (see figure 6) is widely used in transferring of keys over an in secure channel. Due to asymmetric nature, there are two keys used in the algorithm. One is public key and second is a private key. The

public key is openly accessible to everyone in the cryptosystem and the private key is kept secret by authorized person. RSA provides confidentiality, integrity, authenticity, and non-repudiation of data [15] [11]. RSA is more commonly used in electronic industry for online money transfer [9]. In future, RSA can be used in Java cards [16]
- ElGamal:

ElGamal algorithm was introduced in 1985by Taher ElGamal [16]. ElGamal is an asymmetric key encryption algorithm that is based on the Diffie-Helmankey exchange as an alternative to RSA for public key encryption. ElGamal is also used in digital signature generation algorithm called ElGamal signature scheme [10] [17]. A homomorphic algorithm named paillier used for its semantic security [2].

- Blowfish:

Designed by Bruce Schneider in 1933, this algorithm uses keys ranging from 32 to 448 bits. Its main purpose was to serve as an alternative to DES [21]. It has the well-known 16 round Feistel Structure (see figure 7), and operates on S-boxes which depend on large keys. It's large key size and range makes the cipher increase its strength and opportunities of use [21].

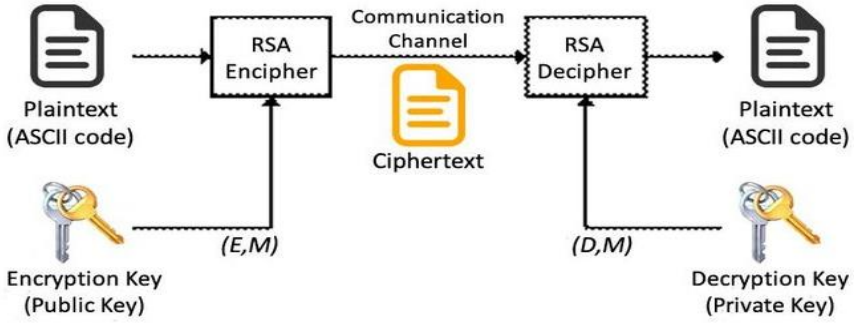

Figure 6: RSA procedures

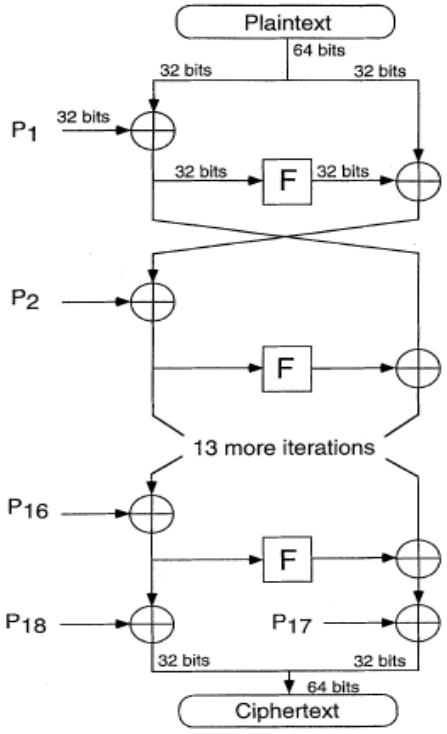

Figure 7: BF procedures

In this paper research a simple and highly secure method of message cryptography will be introduced, the method will use a variable length character PK, the objectives of the proposed method are to satisfy the following [40-45]:

- Provide a low quality encrypted message, and a high quality decrypted message, the proposed method will satisfy the quality requirement shown in table 1.

Table 1: Cryptography quality requirements

Quality parameter	Measured between encrypted and source messages	Measured between decrypted and source messages
MSE	High	0
PSNR	Low	infinite
CC	Low	1
NSCR	High	0

- Increasing the level of security by using a variable long length PK.
- Minimizing the ET/DT and maximizing the throughput of message cryptography.

Generating rearrangement key

The selected PK to be used in encryption and decryption phases must be kept in secret between the data sender and the data receiver. This key is to be used to generate the secret key (keys) needed to apply text file encryption and decryption. In this research paper the CLMM will be used to generate the SKs based on the selected chaotic parameters values, which will form the PK [30-35].
A well-known non-linear difference equation that exhibits chaos is the *logistic* map; it is characterized by equation 1 [47].

$$X_{n+1} = a.X_n(1-X_n) \qquad (1)$$

Here, X_n denotes the value of the *state* in the n^{th} iteration and is a real value in the interval [0, 1]. Also, a is a real parameter in the interval [0, 4]. The dynamics of the map can be studied by choosing a value for a, assigning an initial value x_0 to the state and iterating repeatedly, to obtain the sequence x_0, x_1, x_2, x_3... Such a sequence of states is called an *orbit*.
For a between 0 and 1, the orbit is found to converge to a fixed point x = 0. For every of a between 1 and 3, the system converges to a different non-zero point. This convergence to fixed points can be easily seen in in figure 8

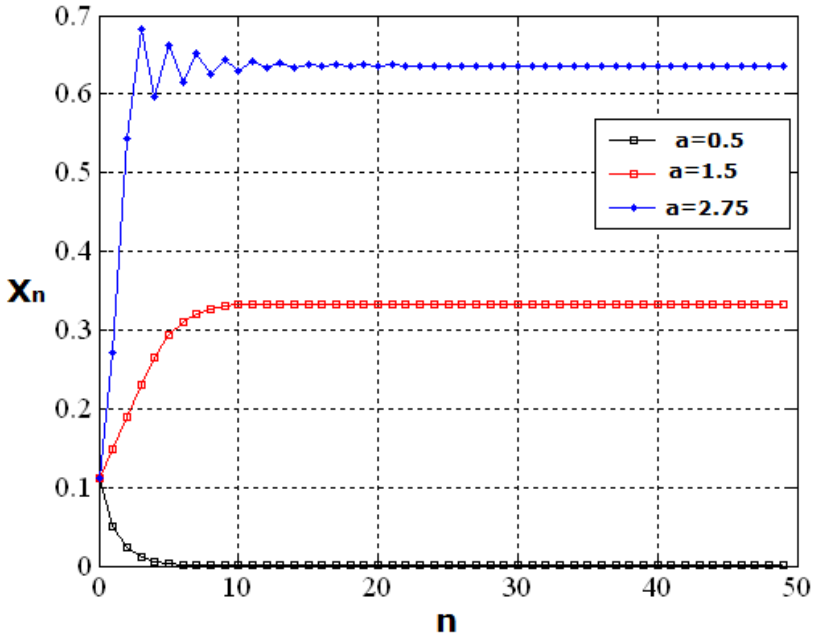

Figure 8: CLM plot for a<3

At a=3, the system undergoes what is known as a period-doubling bifurcation. It means that instead of settling to a fixed point, the system begins to oscillate between two states - a dynamics known as a 2-cycle. Further, if a is progressively increased up to about 3.57, the system undergoes a sequence of period-doubling bifurcations, encountering 4, 8, 16-cycles and so on up to infinity! This usually called a period-doubling cascade. The 2 and 4-cycles can again be seen in figure 9. The blue plot is a 2-cycle and the red plot is a 4-cycle.

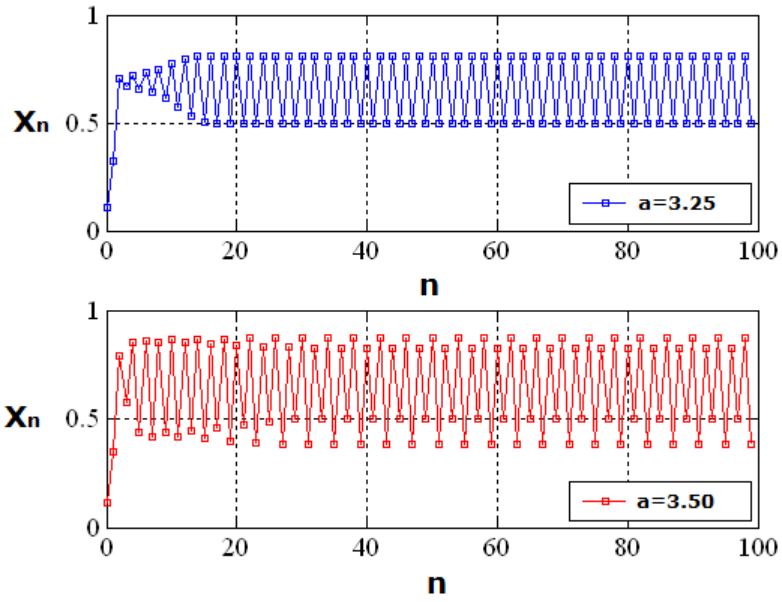

Figure 9: CLM plot for a>3

If the value of a is further increased, it is observed that the orbit neither converges to a fixed point nor oscillates between a finite number of states. Instead, it appears to behave erratically, without any apparent pattern over time. This state is called chaos. A chaotic trajectory is shown in figure 10.

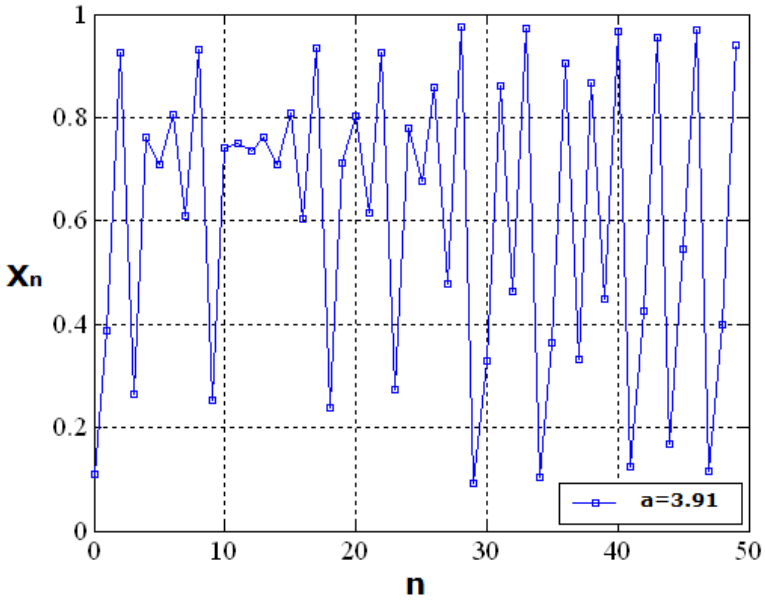

Figure 10: CLM plot for a=3.91

Chaotic systems are sensitive to initial conditions (SIC). It means that if the initial state of a chaotic system is changed by a very small amount, the resulting orbit diverges exponentially from the original orbit. In fact, the two orbits become un-correlated after the passage of a fair amount of time [1-10]. This Sickness of chaotic systems is sometimes called *the butterfly effect*. The divergence of two orbits of the logistic map can be seen in figure 11.

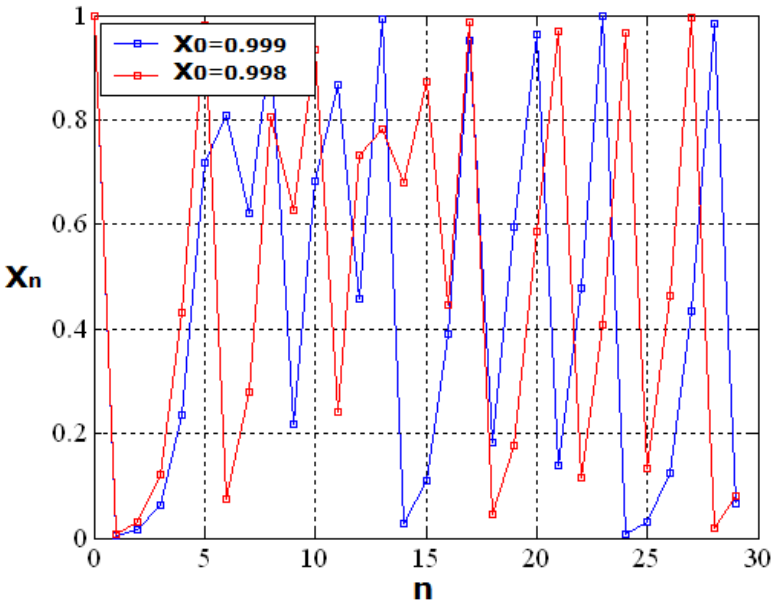

Figure 11: CLM sensitivity

CLM can be easily used to generate various secret keys which can be used in data cryptography to encrypt-decrypt secret important digital data by using chaotic private key to generate a secret key used in algorithm of cryptography. CLK can be generated based on the selected chaotic parameters values, the following sequence of operations can be used to generate CLK. The CLK can be converted to indices key using the sort function to form the RK as shown in the sequence of operations listed below:

```
r1=3.9;x1=0.35; CLMM parameters

for i=1:10                    C
    x1=r1*x1*(1-x1);          L
    CLK(i)=x1;                M
end                           M

CLK:
0.8872   0.3901   0.9279   0.2608   0.7519   0.7276   0.7729   0.6845   0.8423   0.5181
[notused,RK] = sort(CLK);

RK:
4    2   10    8    6    5    7    9    1    3
```

Using the RK in the encryption-decryption phases must be done through selecting the CLMM parameters required to run CLLM to generate the CLK, which can be converted to RK as shown in figure 12:

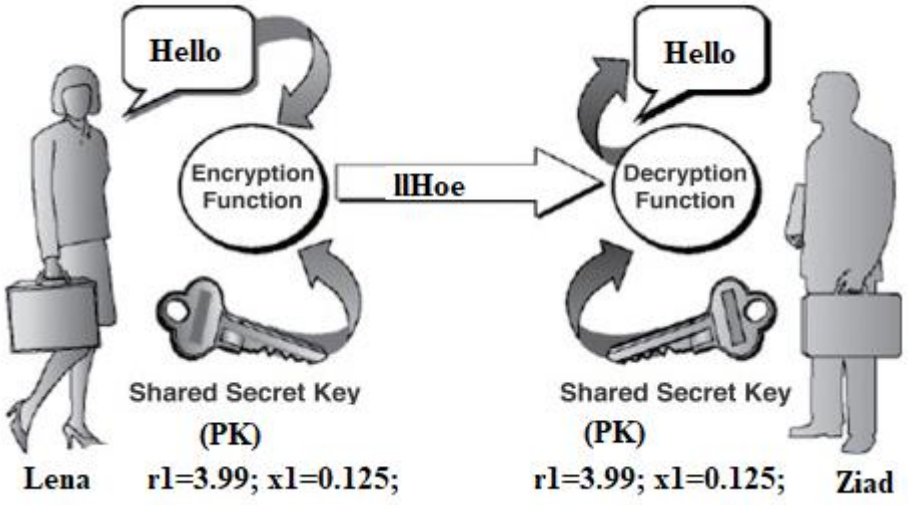

Figure 12: SM cryptography using CLK

Generating CLK requires a generation time, this time will rapidly increase when increasing the key length, table 2 shows the required generation time to produce various length CLKs, while figure 13 shows the relationship between the CLK length and the key generation time:

Table 2: RK generation time

RK length(element)	Generation time (second)	RK length(element)	Generation time (second)
100	0.000331	4000	0.007243
200	0.000319	5000	0.011068
500	0.000601	6000	0.016198
1000	**0.001024**	**7000**	**0.020535**
2500	0.003240	8000	0.026358
3000	0.004735	9000	0.033777
3500	0.005913	10000	0.051479

In the proposed method the block size 1000 bytes will be selected, the long messages with sizes greater than 1000 bytes will be divided into blocks, and each block will be encrypted- decrypted separately.

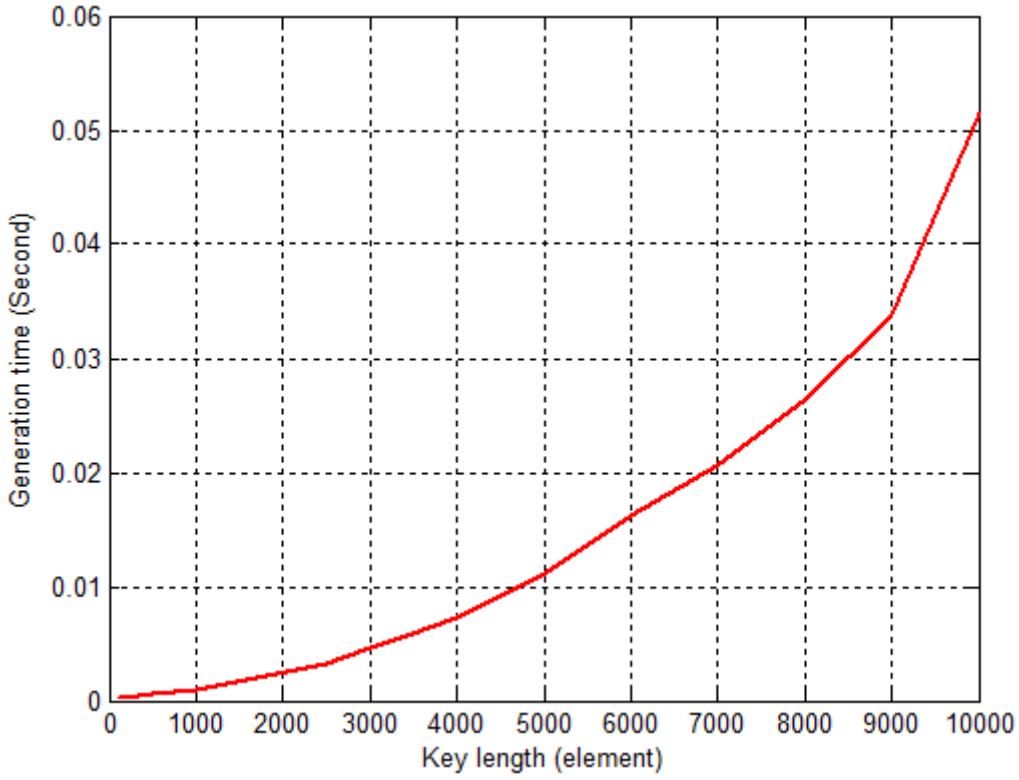

Figure 13: RK generation time vs key length

Generated RK is very sensitive to the selected values of CLMM parameters, any changes in theses parameters will lead to change the contents of RK, thus the cryptography outputs will be changed, see table 3:

Table 3: RK sensitivity

CLM parameters	Generated RK
r1=3.99; x1=0.125;	3 10 4 8 1 6 5 7 9 2
r1=3.91; x1=0.125;	6 3 7 9 1 4 8 10 2 5
r1=3.99; x1=0.325;	4 5 9 2 7 6 10 1 8 3
r1=3.89; x1=0.025;	1 6 9 2 7 4 10 3 8 5

The proposed method

The proposed method can be used to encrypt-decrypt short and long messages, long messages must be divided into equal blocks, with size equal 1000 bytes, one RK or more RKs can be used. In our method we will use different RKs, one RK for each block. The encryption phase can be implemented applying the following steps:

Step 1: Get the message and retrieve the message length (L), get PK

Step 2: if L greater than 1000 then divides the message into blocks.

Step 3: For each block do the following:

- Run CLMM to generate CLK.
- Convert CLK to RK.
- Starting from the first position of the encrypted block put the character pointed by index 1 in RK, then the second character and so on (see figure 14).

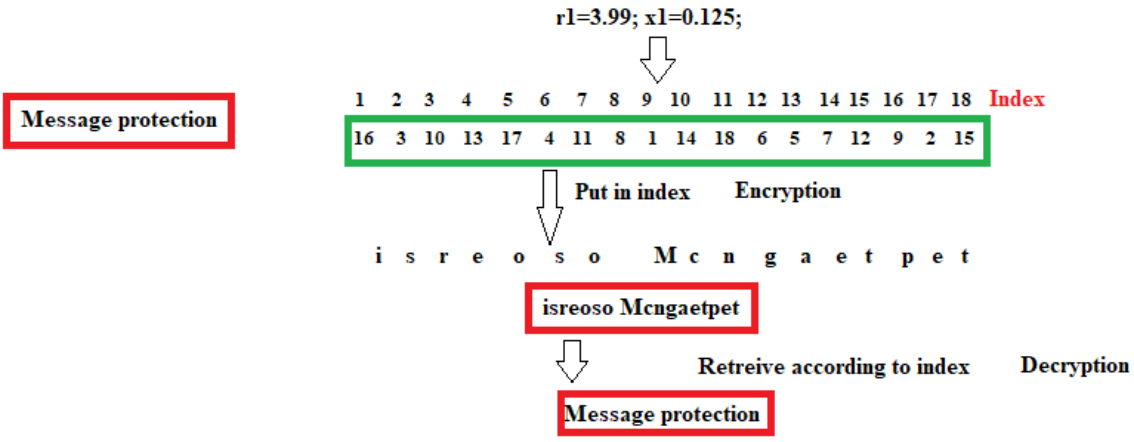

Figure 14: Encryption-decryption example

The decryption phase can be implemented applying the following steps:

Step 1: Get the encrypted message and retrieve the message length (L), get PK

Step 2: if L greater than 1000 divide the message into blocks.

Step 3: For each block do the following:

- Run CLMM to generate CLK.
- Convert CLK to RK.
- Starting from the first position of the decrypted block get the character pointed by index 1 in RK, then the second character and so on (see figure 14).

Implementation and results analysis

The proposed method was implemented using various messages, it was proved that the proposed method satisfied the quality requirements by providing a low quality message in the encryption phase (the messages were totally destroyed) and a high quality message in the decryption phase (the decrypted messages were always identical to the source messages). The quality analysis was done using the quality parameters MSE, PSNR, CC and NSCR.

The quality between two SMs [39-46] can be measured by the quality parameters MSE, PSNR, CC and NSCR, The MSE and NSCR between the source message and the encrypted one must be high, while the PSNR and CC between them must be low. The MSE and NSCR between the source message and the decrypted one must be zero, while the PSNR must be infinite, and CC must be equal 1.

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 samples values, N is the total number of samples, xi and yi are the corresponding sample values of the source and encrypted/decrypted messages.

The value of CC between two SMs expresses the dependency between their corresponding sample 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 SMs 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:

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

where

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

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

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

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

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 two SMs 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 proposed method was implemented using various SMs, the calculated values of MSE between the source SM and the encrypted one was always equal zero, the PSNR was always equal infinite, the CC value was always equal 1, while the NSCR was always equal zero, this prove that the proposed method provided a high quality in the decryption phase, table 4 shows the quality parameters measured between the source SMs and the encrypted ones, the results shown in table 4 prove that the encryption phase provided a low quality SM, thus the provided method satisfied the quality requirements of good cryptography:

Table 4: Calculated quality parameters

SSM number	Length (byte)	MSE	PSNR	CC	NSCR
1	50	90169	18.7102	0.1265	98
2	100	88021	19.7611	0.0883	97
3	200	97825	18.8632	0.1328	99.5000
4	300	10993	17.7748	0.0228	99.6667
5	500	11241	17.5524	-0.0382	99.6000

6	750	10778	17.9729	0.0567	99.6000
7	**1000**	**11439**	**17.3773**	**-0.0203**	**99.4000**
8	2000	11067	17.7077	0.0214	99.3500
9	3000	10189	18.5345	0.0375	99.5333
10	4000	10629	18.1118	0.0120	99.7750
11	5000	11036	17.7365	-0.0063	99.6200
12	10000	10908	17.8531	-0.00037434	99.6600
Remarks		High	Low	Low	High

The speed of the proposed method was tested, the ETs/DTs were measured and the TPs were calculated, table 5 shows the obtained results:

Table 5: Speed calculation results

SSM number	Length (byte)	ET/DT (second)	TP(K bytes per second)
1	50	0.00067130	72.7367
2	100	0.00070260	138.9927
3	200	0.00080310	243.1982
4	300	0.00090220	324.7271
5	500	0.0012	416.7289
6	750	0.0016	466.9867
7	**1000**	**0.0020**	**477.9340**
8	2000	0.0046	421.9142
9	3000	0.0089	329.5709
10	4000	0.0133	292.9739
11	5000	0.0189	257.8982
12	10000	0.1303	74.9382

From table 5 it is shown that the optimal speed can be achieved when the message length was equal 1000 bytes, the ET/DT rapidly increases when increasing the length of RK, and the TP will increase when increasing the message length, after reaching the message size 1000 characters the TP will drop as shown in figure 15.

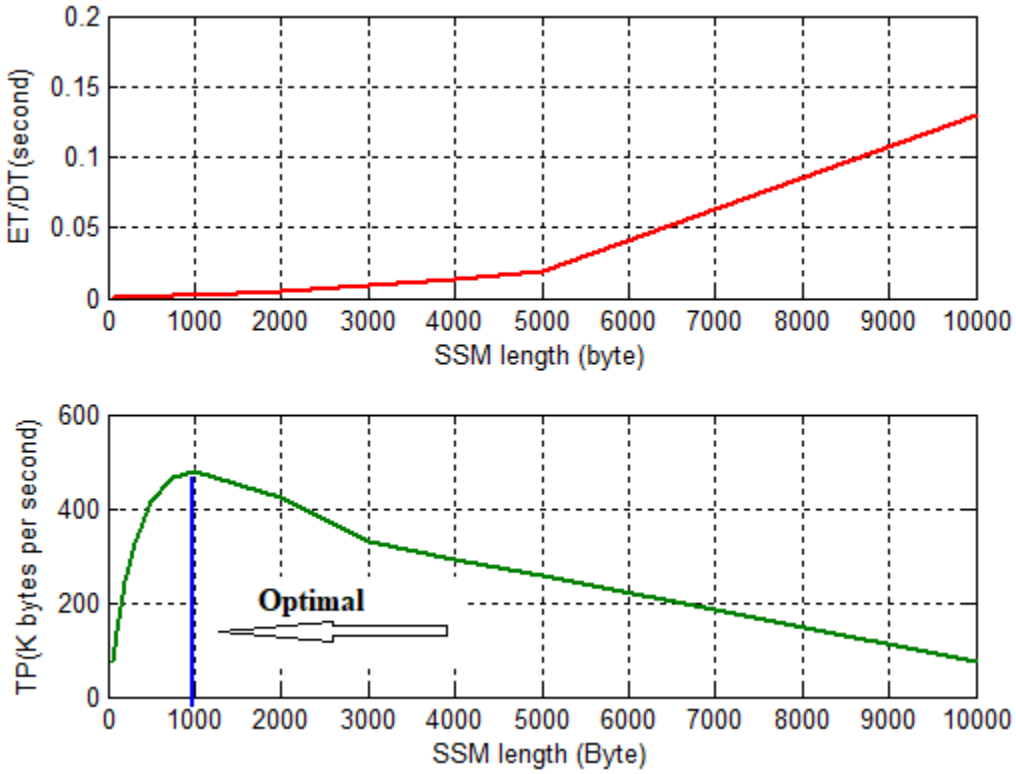

Figure 15: Speed behavior

Long messages were treated using the proposed method, ETs were measured and TPs were calculated table 6 shows the obtained speed results:

Table 6: Long messages speed results

Long message length (K bytes)	ET(second)	TP(K bytes per second)
5	0.0045	1100.5
10	0.0088	1133.5
15	0.0121	1240.7
20	0.0188	1061.2
30	0.0220	1360.7
40	0.0299	1337.1
50	0.0367	1362.0
75	0.0578	1298.7
80	0.0618	1294.2
100	0.0752	1330.2
Average		1251.9

The speed results were compared with other methods speeds, and the proposed method provided a significant speedup by increasing the TP of message cryptography as shown in table 7:

Table 7: Proposed method speedup

Method	Average encryption TP(K byte per second)	Speedup of proposed method	Average decryption TP(K byte per second)	Speedup of proposed method
DES	148.8889	8.4083	174.0260	7.1938
3DES	86.5633	14.4622	101.1779	12.3733
AES	236.4706	5.2941	255.2381	4.9048
BF	368.5200	3.3971	430.7527	2.9063
RSA	206.6838	6.0571	236.4706	5.2941
ElGamal	124.2658	10.0744	150.2804	8.3304
Non_chaotic ref. [47]	170.3906	7.3472	170.3906	7.3472
Chaotic approach ref. [47]	141.2305	8.8642	141.2305	8.8642
Proposed method	**1251.9**	**1.0000**	**1251.9**	**1.0000**

Conclusion

A simple method of message cryptography was introduced. This method was used to encrypt-decrypt short and long messages, the long messages were divided into equal blocks with sizes equal 1 K byte to enhance the speed of the proposed method. The method used simple operations to rearrange the charters in the encryption and decryption phases based on the generated RKs. CLMM was used to generate CLKs, these keys were converted to RK to be used as an indices key. The proposed method was tested and implemented using various messages and it was shown that the proposed method satisfied the quality requirements based on the calculated quality parameters MSE, PSNR, CC and NSCR in the encryption and decryption phases.

The speed of the proposed method was tested and it was shown that the proposed method provided a significant speedup comparing with other existing methods of message cryptography.

References

[1] A. Al Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," Proc. -3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008, vol. 2, no. November 2001, pp. 505–510, 2008.

[2] S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz, "An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms," Recent advances Inf. Sci., vol. 8, pp. 121–124, 2012.

[3] G. Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," Int. J. Comput. Appl., vol. 67, no. 19, pp. 975–8887, 2013.

[4] A. Patil and R. Goudar, "A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices," Int. J. Sci. Technol. Res., vol. 2, no. 8, pp. 61–65, 2013.

[5] C. Science and M. Studies, "An Efficient Password Security Mechanism Using Two Server Authentication and Key Exchange," pp. 50–53, 2015.

[6] A. Levi and E. Sava's, "Performance evaluation of public-key cryptosystem operations in WTLS protocol," Proc. - IEEE Symp. Comput. Common., pp. 1245–1250, 2003.

[7] S. S. and K. Annapurna Shetty, "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm," Int. J. Innov. Res. Comput. Commun. Eng., vol. 2, no. Special issue 5, p. 98, 2014

[8] D. Elminaam, "Performance evaluation of symmetric encryption algorithms," Int. J. Comput. Networks, vol. 8, no. 12, pp. 280–286,2008.

[9] H. Mathur and P. Z. Alam, "Cryptology Algorithm," Int. J. Emerging Trends Technol. Comput. Sci., vol. 4, no. 1, pp. 4–6, 2015.

[10] D. Sukhija, "Performance Evaluation of Cryptographic Algorithms: AES and DES," vol. 3, no. 9, pp. 582–585, 2014.

[11] M. Panda, "Performance Analysis of Encryption Algorithms for Security," pp. 840–844, 2016.

[12] E. Barker, A. Roginsky, G. Locke, and P. Gallagher, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths," NIST Spec. Publ., no. January, pp. 800–131, 2011.

[13] H. O. Alanazi, B. B. Zaidan, a. a. Zaidan, H. a. Jalab, M. Shabbir, and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," J. Comput., vol. 2, no. 3, pp. 2151–9617,2010.

[14] A. K. Mandal and C. Parakash, "Performance Evaluation of Cryptographic Algorithms: DES and AES," 2012.

[15] A. Sterbenz and P. Lipp, "Performance of the {AES} Candidate Algorithms in {Java}," Third {Advanced Encryption Stand. Candidate Conf. April 13--14, 2000, New York, NY, USA, pp. 161–168, 2000.

[16] R. L. Rivest, A. Shamir, and L. Adleman "A Method for Obtaining Digital Signatures and Public- Key Cryptosystems." Communications of the ACM, vol. 26, no. 1, pp. 96–99, 1983.

[17] M. E. Student, "Algorithms for Secure Cloud," vol. 3, no. 6, pp. 1–9,2014.

[18] G. Bernabé and N. Clarke "Study of RSA Performance in Java Cards,"2013.

[19] P. Nalwaya, V. P. Saxena, and P. Nalwaya, "A cryptographic approach based on integrating running key in feedback mode of ElGamal system," Proc. - 2014 6th Int. Conf. Comput. Intel. Commun. Networks, CICN2014, pp. 719–724, 2014.

[20] X. Li, X. Shen, and H. Chen, "ElGamal digital signature algorithm of adding a random number," J. Networks, vol. 6, no. 5, pp. 774–782, 2011.

[21] S. Sahu, A. Kushwaha, M. Scholar, Performance Analysis of Symmetric Encryption Algorithms for Mobile Ad hoc Network, Published 2014, Computer Science, Corpus ID: 13907600.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

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

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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

[45] 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.

[46] 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.

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

[48] 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.

[49] 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.

[50] 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.

[51] Ziad alqadi, Analysis of program methods used in optimizing matrix multiplication, journal of engineering, vol. 15, issue 1, 2005.

[52] Muaad Abu-Faraj, Abeer Al-Hyari, Khaled Aldebei, Ziad Alqadi, Bilal Al-Ahmad, Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography, IEEE Access, VOLUME 10, pp. 69388-69397, 2022.

[53] Prof. Ziad Alqadi, Improving Standard Methods of Message Cryptography, International Journal of Computer Science and Mobile Computing, vol. 11, issue 11, pp. 13-30, 2022.

[54] Mohamad T Barakat, Ziad A Alqadi, Securing Digital Image using Modified Chaotic Logistic Key, International Journal of Computer Science and Mobile Computing, vol. 11, issue 10, pp. 24-47, 2022.

