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

MULTI ROUNDS BASED ON CHAOS THEORY TO PROTECT SECRET MESSAGES

Akram Nacer Adam Mousa[1]
Talal L.M. Bukewitin[2]
Amna M.M Salem[3]
[1,2,3]Libyan Authority for Scientific Research

ABSTRACT

Protecting circulated via various transmission Medias secret messages from being hacked is vital issue. In this paper research an easy to implement and flexible to use method of message cryptography will be introduced. This method will be used efficiently to encrypt-decrypt short and long messages, changing the message and or changing the private key will not require any changes in the encryption and decryption functions. The method will secure the transmitted secret message base on using a private key with complicated structure, this key will use four values with double data type, thus the key space will be high and capable to resist hacking attacks. The produced decrypted message will be very sensitive to the selected PK values, changes in one or more values during the decryption will be considered as a hacking attempt by producing a damaged decrypted message. The private key will be used to generate a 2D chaotic logistic key, each row of the key will be used to generate a secret key required to encrypt-decrypt the message in the associated round, the number of selected rounds will be included in the private key and it will be used to control the quality of the encrypted message, increasing the number of rounds will increase the decree of encrypted message destruction. The proposed method will enhance the performance of message cryptography by decreasing the encryption time and increasing the throughput of message cryptography.

The proposed method will be tested and implemented using various messages; the obtained results will be discussed to prove the quality, sensitivity and performance of the proposed method.

Keywords:
Health Care, Delivery System, Rural Health, GIDA, Philippine Health Agenda, Case Study

INTRODUCTION

Text messages are widely circulated through various means of communication [1-5], and the text message may be:

It is strictly confidential and no one who is unauthorized is allowed to view it [21]. The text message may be of a private nature and may not be circulated by tampering persons. For the above reasons, it is necessary to protect the text message and prevent its penetration [12-17]. When the communication environment is not secure, the possibility of hacking the message and rewriting it by the hacker and then re-sending it with incorrect information to the sender is easy [18-24]. To protect the text message and to transform the communication environment into a safe environment for messaging, private keys can be used to encrypt the message before sending it and decrypt it after receiving it, where the sender and receiver agree on the key to be used to protect the secret message and prevent hackers and intruders from penetrating it. One of the easiest, most widely used and least expensive ways to protect text messages is message cryptography. Cryptography means processing the secret message by turning it into a destructive, unreadable and useless message before sending and recovering the same source message after receiving, destroying the message is called encryption, while recovering the message is called decryption. The crypto system as shown in figure 1 contains: original message to be sent, which os called plain message; encrypted (cipher) message, decrypted (plain) message, encryption function, decryption function and a private key (PK).

The encryption and decryption functions use the PK to generate the required secret keys to apply message encryption and decryption [25-30].

Vol-08 Issue 11, November -2024 ISSN: 2456-9348
Impact Factor: 7.936

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

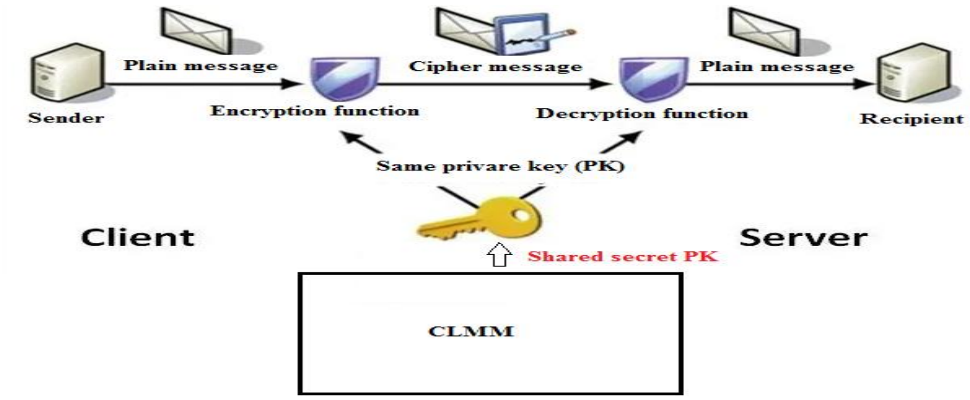

Figure 1: Crypto system components

OBJECTIVES

The aim of this paper research is to introduce a method of message cryptography, which will meet the following requirements:

- Low quality of the encrypted message, the encrypted message must be damaged and unreadable and the quality parameters measured between the sources and the encrypted messages must satisfy the following:
  - High value of mean square error (MSE).
  - Low value of peak signal to noise ratio (PSNR).
  - Low value of correlation coefficient (CC).
  - Closed to 100% value of number of characters changed ratio (NCCR) [30-33].
- High quality of decrypted message, the decrypted message must be identical to the source one and the quality parameters measured between the decrypted message and the source one must satisfy the following requirements:
  - Zero value of MSE.
  - Infinite value of PSNR.
  - Value 1 of CC.
  - Zero value of NCCR [30-33].
- High speed of cryptography, the method must increase the throughput of message cryptography.
- Secure, the PK must provide a better key space capable to resist hacking attacks.
- Efficient use for short and long messages.
- Sensitive, the encryption and decryption functions must use the same PK, any changes in the PK in the decryption function must produce a damaged message, and these changes must be considered as a hacking attempt.

METHODOLOGY

The encryption and decryption algorithm will be implemented using mat lab 7, the programs will be executed using I3 PC with 8 M bytes RAM, and several short and long messages will be tested.

RELATED WORKS

Many methods were introduced for secret message cryptography, and many of these methods were based on standard methods of data cryptography such as: DES, 3DES, AES, RC2, RC6 and blowfish (BF) [1-4]. Standard methods of data cryptography share some features, many of these features can be considered as disadvantages, these features include:

- The message to be encrypted-decrypted is to be divided into small blocks with a fixed length.
- Each of these methods uses a PK with fixed length.
- A lot of time is spent to generate the secret keys required for various rounds of encryption-decryption.
- Some of these methods are not secure by using a short in length PK.

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

- All these method provide a low quality of encrypted messages and an excellent quality of decrypted messages.
- These methods are efficient to encrypt-decrypt short messages, when the message length increases the speed of cryptography (throughput) decreases, table 1 shows the average speed parameters of these methods when they were used to encrypt-decrypt messages with average size equal 1366.7 K bytes:

Table 1: Speed parameters for standard methods of data cryptography [1-4]

Method	Encryption time(second)	Throughput(K bytes per second)
DES	128.3360	85.1968
3DES	149.1840	73.2904
AES	123.2800	88.6912
RC2	179.9200	60.7704
RC6	71.5680	152.7752
BF	19.8560	550.6552

The speed of encoding and decoding is one of the most important factors that determine the efficiency of the method [5-11]. Therefore, some authors have tried to improve the speed of presenting multiple and varied methods. Table 2 shows the most important of these proposed methods and their speed of implementation.

Table 2: Throughputs of some of the introduced methods of message cryptography

Introduced method-reference	Throughput (K byte per second)
Non chaotic method [5-6]	170.3940
Chaotic method [5-6]	141.2336
Hyper chaotic[5-6]	636.3379
Reference [7]	888.867
Reference [8]	638.4082
Reference [9]	911.0352
Reference [10]	360.4102
Reference [11]	384.9609

THE PROPOSED METHOD

The proposed method uses a PK with the structure shown in table 3:

Table 3: PK structure

PK			
Size of chaotic logistic key (rows and columns)		CLMM parameters	
R (number of rounds)	**C** (message length for short messages)	**r1**	**x1**
Example			
6	15	3.77	0.1

The PK is to be used to generate a chaotic logistic key (CLK) by running a chaotic logistic map model (KLMM) [12-17] using the chaotic parameters r1 and x1 [4-11]. The generated CLK is a 2D matrix, the row are defined by the number of rounds R and the columns are defined by the message length C. The generated CLK must be converted to decimal integers, and each row will be used as a secret key to apply round encryption-decryption by applying XOR operation between the message and the secret key.
One of the disadvantages of CLK is that when increasing the key size, the key generation time will rapidly increases as shown in table 4, to avoid this problem and for long messages we can select a smaller value for the parameter C instead of selecting the message length, the obtained CLK can be resized to match the message length, thus we can save time for key generation and optimize the throughput of the method.

Table 4: Optimizing the speed of the proposed method cryptography(R=6)

Message length (K bytes)	Without resizing		With resizing(C=80)	
	Key generation time(second)	Encryption time(second)	Key generation time(second)	Encryption time(second)
500	2017.4	2017.6	0.0050	0.1530
100	74.6510	74.7250	0.0050	0.0850

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

75	39.9740	40.0410	0.0040	0.0730
50	17.1030	17.1690	0.0040	0.0680
25	4.3770	4.4350	0.0040	0.0640
10	0.7650	0.8200	0.0040	0.0620
5	0.2270	0.2830	0.0040	0.0670
1	**0.0250**	**0.0800**	**0.0040**	**0.0600**
0.5	0.0100	0.0660	0.0040	0.0590
0.25	0.0060	0.0610	0.0040	0.0580
0.1	0.0050	0.0620	0.0040	0.0580

Referring to the obtained results shown in table 4 we will consider a message with length greater than 1 K bytes as a long message, which requires key resizing by fixing the C parameter to 1000.
The generated secret key is very sensitive to the selected values of the PK components, any minor changes in one or more value will generate a new key, thus results of decryption will negatively affected, to show this the following PKs shown in figure 2 were taken, A CLMM was run using each of these keys, figure 3 shows the obtained secret keys:

PK1:
R1=6;C1=15;
r1=3.77;x1=0.1;
PK2:
R1=6;C1=15;
r1=3.92;x1=0.1;

PK3:
R1=6;C1=15;
r1=3.77;x1=0.25;
PK4:
R1=6;C1=15;
r1=3.62;x1=0.19;

PK5:
R1=6;C1=10;
r1=3.77;x1=0.1;

Figure 2: Selected PKs

Generated key using PK1

87 216 126 240 52 157 228 92 221 110 236 66 185 192 179
202 159 226 98 227 93 222 107 234 72 194 175 207 147 235
70 191 181 197 168 216 124 240 53 157 227 94 223 104 232
77 203 156 229 89 219 117 239 58 168 216 124 240 53 158
227 94 224 103 232 80 207 146 235 69 190 183 195 172 211
137 239 57 166 218 118 239 56 165 220 115 238 60 173 210

Generated key using PK2

90 228 94 233 80 216 130 250 20 73 203 161 232 81 217
128 250 20 71 201 168 225 103 241 53 164 230 89 227 96
235 72 203 163 230 88 225 103 240 54 167 226 100 238 61
181 206 156 237 65 189 191 188 193 183 202 164 229 91 230
88 227 99 238 64 187 195 179 209 147 244 41 135 249 23
81 217 126 250 20 71 201 166 227 98 236 68 195 179 209

Generated key using PK3

180 199 164 220 113 237 62 177 204 154 230 86 215 127 240
52 156 228 91 220 113 237 63 178 202 158 227 95 225 101
230 86 215 126 240 52 156 228 91 221 112 237 64 181 199
165 219 116 238 59 170 213 131 240 53 158 227 95 225 101
230 85 214 131 240 53 158 227 94 224 103 232 80 207 147
235 71 193 178 203 156 228 90 220 115 238 60 172 211 137

Generated key using PK4

142 228 88 209 137 229 83 203 150 224 100 220 110 226 92
213 128 231 79 198 160 215 121 230 81 200 156 219 111 227
90 211 131 231 80 199 159 217 117 229 84 204 149 224 97
218 115 229 86 206 143 227 89 210 134 230 81 200 156 219
112 227 89 210 134 230 81 200 156 219 111 227 90 211 131
231 80 199 159 217 117 229 84 203 149 224 98 219 113 228

Generated key using PK5

87 216 126 240 52 157 228 92 221 110
236 66 185 192 179 202 159 226 98 227
93 222 107 234 72 194 175 207 147 235
70 191 181 197 168 216 124 240 53 157
227 94 223 104 232 77 203 156 229 89
219 117 239 58 168 216 124 240 53 158

Figure 3: Generated secret keys using various PKs

The encryption process of the proposed method can be implemented by performing the following sequence of steps:

Step 1:

Get the message to be encrypted: Get the message, retrieve the message length and convert the message to decimal (get the ASCII values of the message characters); this step can be implemented by executing the following mat lab operations:

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

```
mes='Data protection';
m1=uint8(mes);k=0.25;
L=length(m1);
```

Step 2:
Get the PK; this step can be implemented by executing the following mat lab operations:

```
R1=6;C1=10;
r1=3.77;x1=0.1;
```

Step 3:
CLK generation: use the chaotic logistic parameters included in the PK to run CLMM to get the 2D CLK, change this key to decimal integers; this step can be implemented by executing the following mat lab operations:

```
for i=1:R1
   for j=1:C1

      x1=r1*x1*(1-x1);
     CLK1(i,j)=x1;

   end
end
key=uint8(255*CLK1);
```

Step 4:
Encryption: for each round: get the row key, resize the key to message length, apply XORing of the message and the key; this step can be implemented by executing the following mat lab operations:

```
e=m1;
for i=1:R1
   d=key(i,:);
   d1=imresize(d,[1,L]);
   e=bitxor(e,d1);
end
```

The decryption process can be implemented using the same steps as for encryption process, but the input message must be the encrypted message.

RESULTS DISCUSSION

The proposed method was implemented using various short and long messages; the selected number of rounds was 6.

The proposed method satisfied the quality requirements in the encryption and the decryption phases, the calculated quality parameters between the source and decrypted messages were always as follows: MSE=0, PSNR=infinite, CC=1, and NCCR=0. Visually we can test the quality of the method, 5 short messages were treated using the proposed method, table 5 shows the obtained messages, while table 6 shows the quality parameters between the source and the encrypted messages:

Table 5: Source and encrypted messages

Message number	Message	Encrypted message	Decrypted message
1	Data protection	□±¤Hm=U ·¬z□□ SR	Data protection
2	Secure message transmission	□□û¥¢L D(>>F@½□¬m~q□□□□□USR	Secure message transmission
3	Using Chaotic keys	□ë ¹¾NM□OF ·¬v|□¢¬EO	Using Chaotic keys
4	Efficient method	□□¶@J$BI¬□r□□□SX	Efficient method

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

5	Data cryptography		□ù¤H .?^¨¬pxŸ□¹TE	Data cryptography

Table 6: Quality parameters between the source and encrypted messages

Message number	MSE	PSNR	CC	NCCR
1	3891.7	25.2065	-0.1040	100
2	5668.1	24.2416	-0.0414	100
3	5745.9	22.6293	0.0426	100
4	7428.6	21.6158	-0.0527	100
5	4392.6	26.4723	0.2065	100
Remarks	**High**	**Low**	**Low**	**High**

The proposed method also satisfied the encryption quality when dealing with long messages, the results shown in table 7 proved this fact:

Table 7: Encryption quality parameters for long messages(C=200)

Message length (K bytes)	MSE	PSNR	CC	NCCR
5	11521	17.3057	-0.0497	100
10	11404	17.4083	-0.0468	100
25	1152.0	17.3066	-0.0526	100
50	11474	17.3465	-0.0525	100
100	11426	17.3892	-0.0508	100
Remarks	**High**	**Low**	**Low**	**High**

The proposed method was tested for sensitivity, the pervious short messages shown in table 5 were encrypted using PK1 shown in figure 4 and the encrypted messages were decrypted using PK4 shown in the same figure, table 8 shows the obtained decrypted messages and the quality parameters between the source and the decrypted messages:

Table 8: Decryption results using different PK

Message number	Decrypted message	MSE	PSNR	CC	NCCR
1	ô□_p□□-C□ɜ*¾¦3#	6461.3	22.2075	-0.0549	100
2	□□□□Yt1>8I□□dw':§£¼/5"#	6675.8	22.7629	-0.2099	100
3	□□BEv□87MC□□*ê¤□‰>	9551.4	18.0515	-0.0552	100
4	□□Mxù□:BX□(,¾§3)	7599.0	20.9913	-0.0492	100
5	ô□_p1ù &\□ÿ.¸«□44	6057.2	23.2590	-0.1314	100
Remarks	**Damaged**	**High (instead of low)**	**Low (instead of high)**	**Low instead of 1**	**High instead of 0**

As we can see from table 8, changing the PK in the decryption phase will be considered as a hacking attempt by producing damaged decrypted messages.
The proposed method uses a variable number of rounds, this number can be included in the PK, increasing the round number (R) will increase the degree of the encrypted message destruction, this can be shown in table 9, the same messages shown in tables 5 and 6 which were encrypted using 6 rounds, the used number of rounds was 16. As we can see from table 9 the values of the quality parameters became worse.

Table 9: Quality parameters between the source and encrypted messages(R=16)

Message number	MSE	PSNR	CC	NCCR
1	7520.3	20.9341	0.00068870	100
2	8311.8	20.0948	0.001428	100

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

3	9828.3	18.5789	-0.01135	100
4	8169.1	20.5075	0.02176	100
5	9431.9	18.8305	-0.02951	100
Remarks	**High**	**Low**	**Low**	**High**

The speed of the proposed method was tested; the actual speed can be tested when dealing with long messages. A selected set of long messages were processed using the proposed method, the encryption (decryption) time was measured and the throughput was calculated, table 10 and 11show the obtained speed parameters:

Table 10 speed results(R=6)

Message length(K bytes)	Encryption time (second)	Throughput (K bytes per second)
5	0.0590	84.7458
10	0.0630	158.7302
50	0.0880	568.1818
100	0.1010	990.0990
300	0.1270	2362.2
400	0.1530	2614.4
500	0.2000	2500.0
1366.7	0.4330	3156.3

Table 11 speed results(R=16)

Message length(K bytes)	Encryption time (second)	Throughput (K bytes per second)
5	0.0630	79.3651
10	0.0700	142.8571
50	0.0840	595.2381
100	0.1190	840.3361
300	0.2410	1244.8
400	0.2980	1342.3
500	0.3600	1388.9
1366.7	0.8740	1563.7

From tables 10 and 11 we can see the following:

- Significantly increasing the length of a text message will slowly increase the encryption time (see figure 6).
- Significantly increasing the length of a text message will exponentially increase the permeability (throughput) of the encryption (see figure 4).
- Increasing the number of cycles will reduce the efficiency of the method, but it remains good and acceptable.

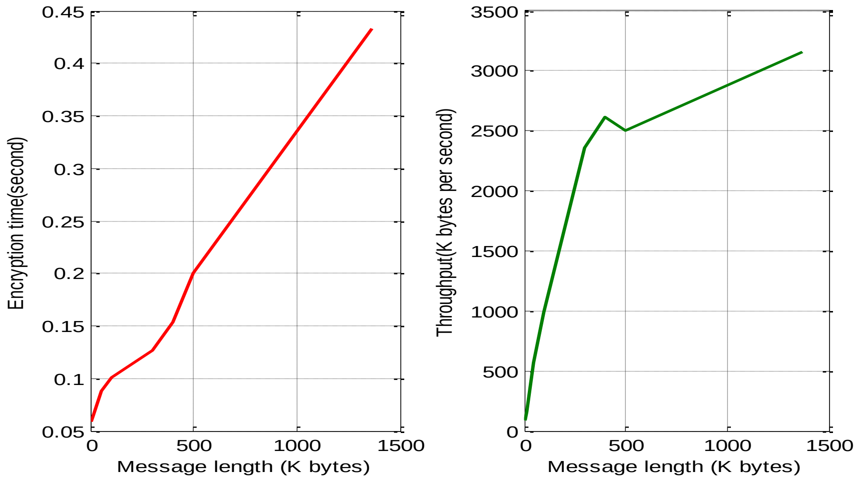

Figure 4: Encryption time, throughput vs message length

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

The speed of the proposed method was compared with other method speed, the results of comparisons shown in table 12 shows that the proposed method provided a significant speed up by increasing the cryptography throughput (speed up of the proposed method equal throughput of the proposed method divided by other method throughput).

Table 12: Method speed up

Method	Throughput(K bytes per second)	Speed up of the proposed method
DES	85.1968	**18.3540**
3DES	73.2904	**21.3357**
AES	88.6912	**17.6308**
RC2	60.7704	**25.7313**
RC6	152.7752	**10.2353**
BF	550.6552	**2.8397**
Non chaotic method [5-6]	170.3940	**9.1770**
Chaotic method [5-6]	141.2336	**11.0717**
Hyper chaotic[5-6]	636.3379	**2.4573**
Reference [7]	888.867	**1.7592**
Reference [8]	638.4082	**2.4494**
Reference [9]	911.0352	**1.7164**
Reference [10]	360.4102	**4.3387**
Reference [11]	384.9609	**4.0620**
Proposed (R=16)	1563.7	**1.0000**

CONCLUSION

A simple and flexible method of message cryptography was proposed, it was easily to used this method to encrypt-decrypt short and long messages, changing the message or/and changing the PK did not require any changes in the encryption and decryption functions. The proposed method provided a good level of message security based on using a complicated PK, this key provided a good key space and the decrypted message were very sensitive to the selected PK, any minor changes in the PK during the process of decryption was considered as a hacking attempt by producing a damage decrypted message. The PK was used to generate a 2D chaotic logistic key, which was converted to integer decimals. The rows of the chaotic key determined the required key for the associated round of message encryption-decryption. The selected number of rounds was variable and it was included in the PK. It was shown that increasing the number of rounds will decrease the quality of the encrypted message keeping the method performance acceptable.
The proposed method was tested using various short and long messages and the obtained results proved the quality and sensitivity of the method. The speed of the proposed method was tested and it was shown that the proposed method provided a significant speed up comparing with other methods, and the proposed method increased the throughput of secret message cryptography.

REFERENCES

[1] Sadkhan Sattar B. and Abbas Nidaa A., "Performance Evaluation of Speech Scrambling Methods Based on Statistical Approach" ATTI DELLA “Fonazione GiorgioRonchi” Anno Lxvi, No. 5 PP. 601-6014 (2011).
[2] Ambika D. and Radha V., "Secure Speech communication – A Review International Journal of Engineering Research and Applications (IJERA), Vol. 2Issue 5 PP. 1044-1049 (2012).
[3] Mosa E.; Messiha N.W.; Zahran O. and Abd El-SamieF.E. "Encryption of Speech Signal with Multiple Secret Keys in Time Transform Domains " Int. J Speech Technol., Vol. 13 PP. 231-242 (2010).
[4] Mua’ad M. Abu-Faraj, Khaled Aldebei2, Ziad A. Alqadi, Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography, Traitement du Signal, vol. 39, issue 1, pp. 173-178, 2022.
[5] 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.
[6] 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.

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

[7] 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
[8] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019.
[9] 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.
[10] X. Zhang and X. Wang, *Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System*, Springer, New York, NY, USA, 2019.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Pur- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.
[16] 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.
[17] 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.
[18] Rashad J. Rasras1, Mutaz Rasmi Abu Sara2, Ziad A. AlQadi3, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3 ,2019, https://doi.org/10.30534/ijatcse/2019/64832019
[19] Musbah J. Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering & Technology, 7(3.13) (2018) 104-107.https://doi.org/10.14419/ijet.v7i3.13.16334
[20] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein,A COMPARISON BETWEEN PARALLEL ANDSEGMENTATIONMETHODS USED FOR IMAGE ENCRYPTION-DECRYPTION International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5,October 2016.
[21] Musbah J. Aqel , Ziad A. Alqadi, Ibraheim M. El Emary, Analysis of Stream Cipher Security Algorithm, Journal of Information and Computing Science Vol. 2,No. 4, 2007, pp. 288-298.
[22] 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.
[23] 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.
[24] Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Modified Inverse LSB Method for Highly Secure Message Hiding, IJCSMC, Vol. 8, Issue.2, February 2019, pg.93 – 103
[25] Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Engineering, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages Engineering Technology & Applied Science Research, Vol.9 Issue 1, Pages 3681-3684, 2019.
[26] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- ods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.
[27] 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.

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

[28] 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.
[29] 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.
[30] 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.
[31] 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.
[31] 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.
[33] 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.