iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

MESSAGE BINARY MATRIX ROTATING TO PROTECT SECRET MESSAGE

Namer Ali Aletawi
Mansour Ali Abu Sameha
FatimaThaher Aburomman
Albalqa Applied University, Jordan

DOI
https://doi.org/10.5281/zenodo.17700139

ABSTRACT
Recently, in today's interconnected digital world, the transmission of both lengthy and concise secret messages is ubiquitous across diverse communication platforms. With the proliferation of sensitive and specialized information being exchanged, safeguarding these messages from potential threats such as intruders, abusers, and data hackers becomes imperative and vital issue. This paper research presents an innovative approach aimed at streamlining message protection procedures while concurrently thwarting hacking attempts. At the core of the presented method lies the utilization of a sophisticated variable content private key designed to facilitate ease of alteration without compromising the integrity of encryption and decryption operations. The pivotal aspect involves leveraging the use of a private key to run a simple chaotic logistic map model to generate the secret key, mandating both the sender and receiver to securely retain this key. By employing selected chaotic parameters values, the secret key can seamlessly adapt to match the length of the confidential message. To fortify the level of security, the message is recommended to convert to binary to get the message binary matrix, and the rows of this matrix will be treated as blocks. Subsequently, the bits within each block are consolidated into a singular vector, which undergoes a left rotation by a predetermined number of bits as specified by generated secret key. The presented methodology is empirically validated through the implementation of various secret text messages. Comparative analyses against existing methods underscore the efficacy and robustness of the proposed approach, substantiating its significant advancements in data protection paradigms.

Keywords:
Cryptography, SM, MBM, PK, CLMM, RLD.

INTRODUCTION

Recent advances in message cryptography often focus on enhancing efficiency and security [1-10]. This paper research introduces a novel method of message cryptography using message binary matrix rows rotation, leveraging their inherent mathematical properties to secure secret messages [11-15]. Unlike the standard and traditional methods used in many current applications such as DES, AES, or Blowfish, which rely on complex substitution and permutation networks, the presented method utilizes simpler, yet effective, rotational transformations to manipulate message binary matrix bits. Message binary matrix rows rotation left operations offer several unique advantages [16-20]. Firstly, they are computationally simpler and require fewer resources, making them ideal for environments with limited processing capabilities. Secondly, the deterministic nature of rotational shifts ensures a high-speed operation, crucial for real-time applications. In contrast, the presented method capitalizes on the simplicity and speed of matrix rows rotations, enhancing throughput and reducing latency in cryptographic operations [21-25]. This makes it particularly well-suited for securing messages in high-speed networks or applications requiring rapid encoding and decoding, such as streaming services or real-time communications. By focusing on these aspects, the introduction can effectively set the stage for detailing the proposed crypto-graphic method and its comparative benefits over existing techniques, directly addressing the feedback for more clarity and rationale in your exposition [26-30].

The importance of encrypting confidential messages lies in maintaining confidentiality, integrity, and authenticity, providing maximum data protection from unauthorized access and preventing eavesdropping and manipulation. Encryption also ensures the privacy of sensitive communications for individuals, businesses, and government agencies, and contributes to compliance with legal data protection standards.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Message cryptography has the following benefits [31-40]:

- Confidentiality and Privacy: Encryption transforms messages into codes that can only be read by those who possess the decryption key, thus protecting conversations and sensitive information from eavesdroppers and hackers.
- Data Integrity: Encryption ensures that messages are not altered or tampered with during transmission and helps detect any attempt to change their content.
- Authentication: Encryption helps verify the identity of the sender and recipient, ensuring that the message comes from a trusted source and goes only to the intended recipient.
- Protection from Threats: Encryption provides a strong layer of security against identity theft and financial fraud, protecting sensitive personal and business information from theft or unauthorized access.
- Regulatory Compliance: Data encryption is a prerequisite for complying with data protection regulations in many sectors, such as healthcare and finance.

The presented method aims to address the need for protecting both long and short text messages from potential abusers, intruders, or data hackers [41-45]. The main objective is to simplify the message protection process while making it challenging for hackers to compromise messages. A novel method will be presented, focusing on the utilization of a complex variable content private key that can be easily modified without altering the encryption and decryption procedure [46-50].

A key aspect of the presented method is the utilization of a complex variable content private key. This private key can be easily modified without disrupting the encryption and decryption procedures, thereby enhancing the security of the system. The secret key is generated from private key by running a simple chaotic logistic map model (CLMM) [51-55].

Message crypto method usually contains encryption function (EF) in the message sender part and decryption function (DF) in the message receiver part (see figure 1). The EF manipulates the original source secret message (SM) and the private key (PK) to produce the encrypted (cipher) message, while the DF manipulates the cipher message and the PK to produce the decrypted (original) SM [56-60].

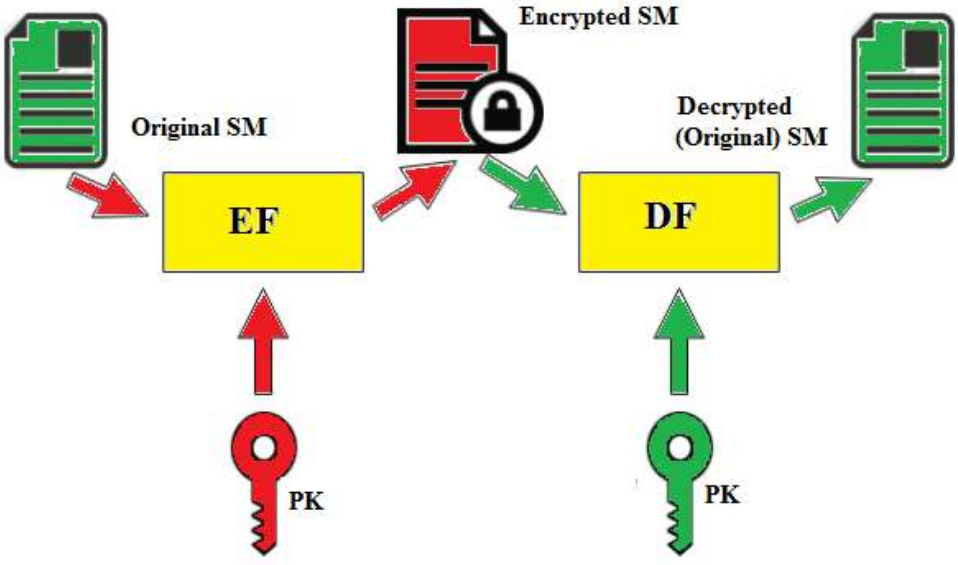

Figure 1: SM crypto process diagram

A good crypto method must meet the following requirements [61-70]:

- Security: The method must enhance the security of the encryption and decryption procedures to make it difficult for hackers to compromise messages. The method must use a PK longer than 100 bits, this length will be strong enough and it will provide a key space capable to resist hacking attacks.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

- Encryption quality: The encryption phase should result in a high degree of data distortion, which can be quantified using quality parameters. In this paper research, the following will be deployed: the mean square error (MSE) as depicted in (1), peak signal-to-noise ratio (PSNR) as depicted in (2), and correlation coefficient (CC) between the original and encrypted-decrypted data. During encryption, the MSE value should be notably high, while the PSNR value should be correspondingly low and the CC value should significantly deviate from 1 [71-75].

$$\mathrm{MSE} = \frac{1}{N}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[S(i,j) - R(i,j)]^2,\ N = m \times n\{\mathrm{S, R\ are\ messages}\}, \tag{1}$$

$$\mathrm{PSNR} = 10 \times \log_{10}\frac{\left(\underset{I}{\mathrm{MAX}}\right)^2}{MSE_t}. \tag{2}$$

- Decryption quality: In the decryption phase, the MSE value should approach zero, indicating minimal distortion, while the PSNR value should approach infinity, indicating high-fidelity reconstruction. Additionally, the CC value should approach 1, signifying strong correlation between the original and decrypted data [76-80].
- Efficiency: The crypto method must fulfill the pre-requisites of effective cryptography, achieving the following objectives: optimization of quality parameters throughout encryption and decryption phases, minimization of encryption and decryption times to maximize throughput (speed), and ensuring flexibility and ease of implementation with provisions for easy acceleration if necessary. The confidential data utilized to generate the secret key must be intricate and resistant to deciphering or hacking [81-86].
- Flexibility: The method must be efficiently used to process short and long messages; the user must have the ability to change the PK without the need to change the EF and DF.
- Simplicity: The method must use simple procedures for secret key generation, SM encryption and SM decryption [1-5].

RELATED WORKS

Numerous secret SM cryptography methods exist [1-5], with many built upon the foundation of standard encryption techniques like DES (Data Encryption Standard), including variants, such as 3DES, AES (advanced encryption standard), and Blowfish (BF). These standard methods operate by varying parameters, such as key length and number of rounds, as outlined in Table 1 [29–31]. However, standard encryption methods come with inherent limitations [6-10]:

1) PK length is fixed and cannot be altered for each method, limiting flexibility.
2) Encrypted SM must be segmented into fixed-size blocks, offering little adaptability.
3) The number of rounds in the encryption-decryption process is predetermined and unchangeable.
4) Secret key generation is obligatory, with the PK used to derive additional sub-keys .
5) While these methods yield high-quality parameter values in both encryption and decryption phases, they are most efficient with small- to medium-sized SMs. Larger SM sizes lead to reduced throughput and inefficiency.
6) Increased round requirements prolong the cryptography process.
7) Many methods necessitate the use of an S-box, introducing additional computational overhead and memory requirements.

Table 1 presents an overview of key parameters and characteristics associated with standard encryption methods, including DES, 3DES, AES, and BF [1-10]. These methods are commonly used for securing SMs in various applications, each with its own set of features and limitations.

1) PK length: This specifies the length of the PK in bits used in each encryption method. The length is fixed for each method, providing varying levels of cryptographic strength.
2) Block size: Block size in bits indicates the size of data blocks processed during encryption and decryption. Similar to the PK length, the block size remains fixed for each method.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

3) Ability to deal with data with big size: It reflects the difficulty level in handling image data using the respective encryption-decryption method.
4) Encryption quality: It describes the quality of encryption achieved by each method, typically evaluated based on parameters, such MSE and PSNR [11-16].
5) Decryption quality: It represents the quality of decrypted data, often measured in terms of MSE and PSNR, with ideal scenarios exhibiting zero MSE and infinite PSNR.
6) Efficiency: It indicates the speed of encryption and decryption processes. While some methods operate relatively slowly, others offer moderate efficiency.
7) Attack: It identifies potential vulnerabilities to specific attack methods, including brute force attacks, side-channel attacks, and dictionary attacks.
8) Structure: It specifies the underlying structure employed by each encryption method, such as Feistel or Substitution-Permutation.
9) Block cipher: It indicates the use of binary operations in the encryption –decryption process.
10) Rounds: It refers to the number of rounds or iterations performed during encryption and decryption.
11) Flexibility to modification: It indicates whether the method allows for modifications to parameters or key lengths.
12) Simplicity: It reflects the complexity of the encryption-decryption method, with "No" indicating higher complexity.
13) Security level: It evaluates the overall security level provided by each encryption method, ranging from adequate to excellent.
14) Throughput (speed): It represents the speed and efficiency of data processing, with higher throughput indicating faster encryption and decryption rates.

Table 1: Summery of crypto standard method features[1-10]

Feature	DES	3DES	AES	BF
Rounds	16 and fixed	48 and fixed	10, 0r 12 or 14 and fixed	16 and fixed
PK length (bits)	Fixed with 56 bits	Fixed with 112 or 168 bits	Fixed with 128, or 192 or 256 bits	32 to 448 bits
Security level	Adequate	Adequate	Excellent	Excellent
Data blocking	Needed	Needed	Needed	Needed
Block size (bits)	64 and fixed	64 and fixed	128 and fixed	64 and fixed
Ability to deal with SM with big size	Difficult	Difficult	Difficult	Difficult
Encryption quality	Excellent	Excellent	Excellent	Excellent
Decryption quality	Excellent	Excellent	Excellent	Excellent
Efficiency	Slow	Slow	Slow	Moderate
Attack	Brute force attack	Brute force attack	Side-channel attack	Dictionary attack
Structure	Feistel	Feistel	Substitution-permutation	Feistel
Block cipher	Binary	Binary	Binary	Binary
Flexibility to modification	No	Yes	Yes	Yes
Simplicity	No	No	No	No
Speed	Low	Low	Low	Moderate

This comprehensive overview assists in understanding the strengths, weaknesses, and suitability of each standard encryption-decryption method for different applications and security requirements. The presented method employs a fundamental logical operation to enhance data security [11-15]: left rotation by a secret key-defend number of digits. The rotation left operation can be easily implemented by applying a circular

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

movements of the bits as shown in figure 2.The SM as shown in figure 3 will be represented by a message binary matrix (MBM), each row will be treated as a message block, this row will be rotated left for a specified number of rotating left digits (RLD) defined by the generated secret key (SK), and it is important to highlight that each row will use its own RLD.

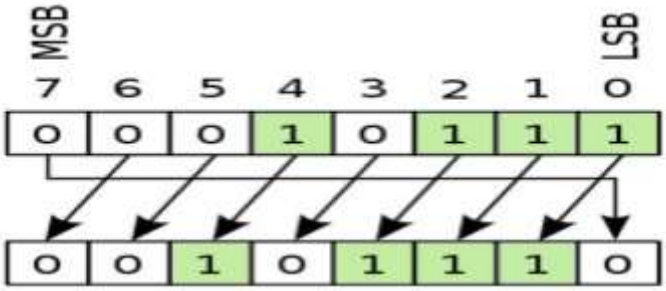

Figure 2: Rotating left operation illustration

```
m='Secret message'
m1=uint8(m)
m1 =
  83 101  99 114 101 116  32 109 101 115 115  97 103 101
MBM=dec2bin(m1,8)
MBM =
01010011
01100101
01100011
01110010
01100101
01110100
00100000
01101101
01100101
01110011
01110011
01100001
01100111
01100101
```

Figure 3: Representing SM using MBM

This strategic approach ensures robust SM protection by introducing varying layers of complexity and obfuscation, rendering the encrypted data more resistant to unauthorized access and decryption attempts. Trough the meticulous selection and implementation of these operations, the presented method aims to elevate the security standards of SM encryption-decryption methodologies [20-26].

The presented method will use a PK of 128 bits length, this key will contain the values of the chaotic parameters r and x, these values with the message length L will be used to run a chaotic logistic map model (CLMM) to generate the secret key, which will contains the values of the RLDs for the MBM rows, figure 4 shows how to use the simple CLMM to generate the SK, while figure 5 shows how to use SK to apply SM encryption-decryption by applying rotating left the bits of each MBM row bits.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

```
r=3.77;x=0.12;
for i=1:L
CS(i)=x;
x=x*r*(1-x);
end
SK=fix(7*CS)+1;
```

Figure 4: Using CLMM to generate SK

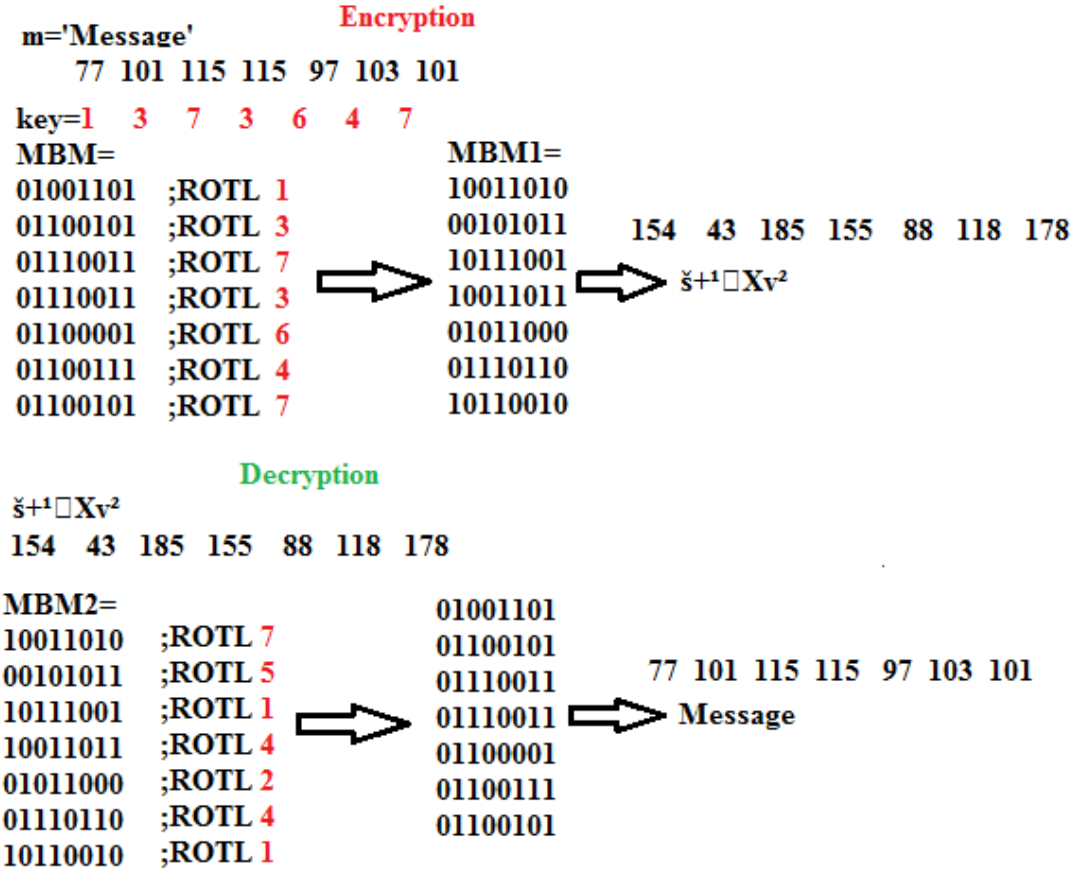

Figure 5: Using SK to rotate left MBM rows

Methodology: The encryption-decryption algorithms

Encryption algorithm (see figure 6):

Inputs:
SM, PK
Output:
Encrypted SM
Process:

(1) SM preparation:
   a) Get the SM
   b) Get the message length (L)
   c) Convert the SM to binary to get MBM.

(2) SK generation:
   a) Get the PK values (r and x).

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

b) Run CLMM to generate a chaotic sequence (CS) with length equal L.
c) Convert the CS to integer values within the range 1 to 7.

(3) Encryption:
For each MBM row do the following:
a) Get the associated for the row RLD from the SK.
b) Extract the row.
c) Rotate the row for an RLD positions.
d) Return back the row to MBM.

(4) Convert MBM to decimal.
(5) Convert the decimal results to characters to get the encrypted SM.

```
m = 'Message encryption-decryption';
L=length(m);
m1=dec2bin(m,8);
r=3.77;x=0.12;
for i=1:L
CS(i)=x;
x=x*r*(1-x);
end
key=fix(7*CS)+1;
m1=m;
for i=1:L
   RLD=key(i);
   c=m2(i,:);
   c1=rotl(c,RLD);
   m1(i,:)=c1;
end
m3=bin2dec(m1)';
m4=char(m3);
```

Figure 6: Encryption algorithm implementation

Decryption algorithm (see figure 7):
Inputs:
Encrypted SM, PK
Output:
Decrypted SM
Process:

(1) SM preparation:
a) Get the SM
b) Get the message length (L)
c) Convert the SM to binary to get MBM.

(2) SK generation:
a) Get the PK values (r and x).
b) Run CLMM to generate a chaotic sequence (CS) with length equal L.
c) Convert the CS to integer values within the range 1 to 7.

(3) Encryption:
For each MBM row do the following:
a) Get the associated for the row RLD from the SK.
b) Extract the row.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

c) Rotate the row for 8-RLD positions.
d) Return back the row to MBM.

(4) Convert MBM to decimal.
(5) Convert the decimal results to characters to get the decrypted SM.

```
L=length(m4)
MBM1=dec2bin(m4,8);
r=3.77;x=0.12;
for i=1:L
CS(i)=x;
x=x*r*(1-x);
end
key=fix(7*CS)+1;
m5=m4;
for i=1:L
   RLD=key(i);
   c=m4(i,:);
   c1=rotl(c,8-RLD);
   m5(i,:)=c1;
end
m6=bin2dec(m5)';
m7=char(m6);
```

Figure 7: Decryption algorithm implementation

RESULTS

Te proposed method was implemented using MATLAB 7, capitalizing on the computational capabilities of a processor operating at 2.4 MHz and an Intel i5 processor with a RAM capacity of 8 GB. To thoroughly evaluate its performance across various scenarios, we employed a diverse range of short and long messages of different lengths during the implementation phase. To further validate the method's performance, short messages of varying lengths were encrypted. Concurrently, standard data cryptography methods were also employed on the same set of messages for comparative analysis. This rigorous evaluation allows for a comprehensive understanding of the presented method's effectiveness and efficiency in securing data confidentiality across diverse message lengths and encryption technique. Table 2 shows the obtained experimental results for a short message. From Table 2, it can be seen that the presented method is more efficient than the standard methods of SM cryptography and decreases the encryption time (ET), as shown in Figure 8.

Table 2: ET (second) results of short messages implementation

L (character)	DES	3DES	AES	BF	Presented
24	0.1510	0.1800	1.1160	0.0864	0.0280
48	0.3020	0.3400	2.2120	0.1528	0.0290
72	0.4580	0.5200	3.3280	0.2392	0.0310
96	0.6140	0.7100	4.4340	0.3256	0.0340
120	0.7700	0.8009	5.5600	0.4120	0.0360
144	0.9260	1.0700	6.6760	0.5084	0.0390
168	1.0820	1.2400	7.8020	0.5048	0.0410
192	1.2380	1.4200	8.8280	0.6512	0.0430
216	1.3040	1.5200	9.9440	0.6776	0.0440
240	1.4600	1.7000	10.7600	0.7640	0.0460

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

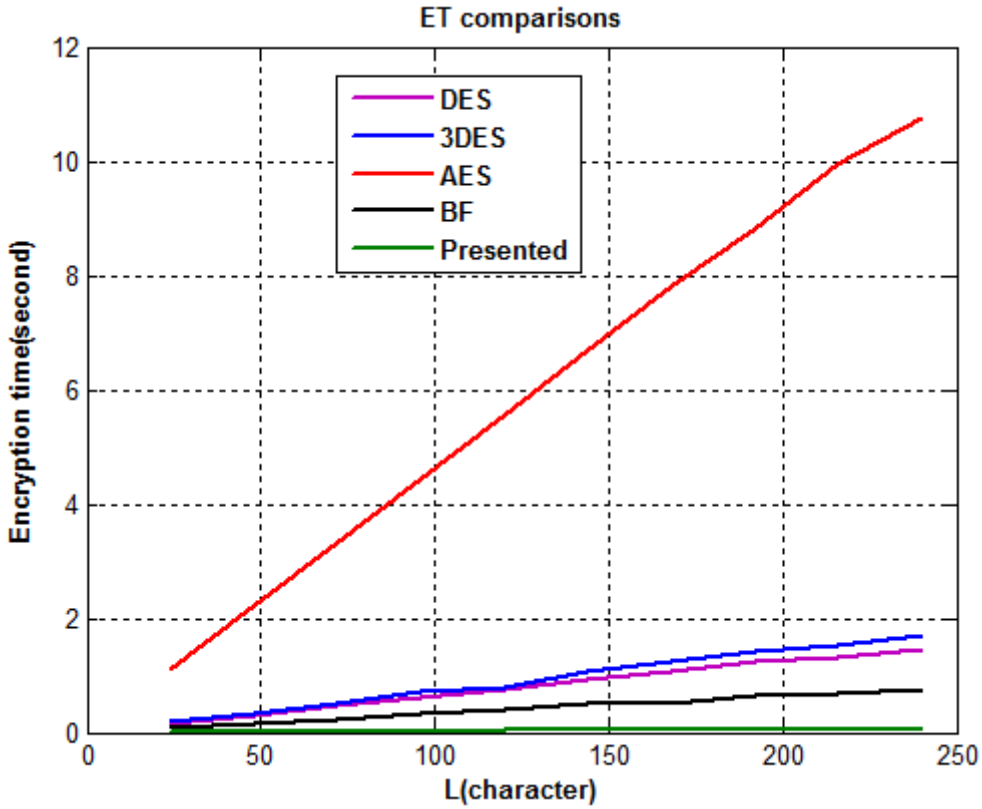

Figure 8: Comparison of encryption times for short messages

From Figure 8, we can glean insights into the comparison of encryption times for short messages between the proposed method and standard methods of data cryptography. Here are some key points extracted from the figure:

1) Efficiency of the presented method: The presented method demonstrates superior efficiency compared to standard methods, as evidenced by shorter encryption times across various message lengths.
2) Consistent performance: Regardless of the message length, the proposed method consistently exhibits lower encryption times than standard methods, highlighting its robustness and reliability in encrypting short messages.
3) Significant time reduction: The encryption times achieved by the proposed method are notably shorter compared to those of standard methods. This reduction in encryption time is crucial for applications requiring rapid data encryption without compromising security.
4) Impact of message length: While there is variation in encryption times based on message length, the proposed method consistently outperforms standard methods across all message lengths considered in the
comparison.
5) Real-time encryption capabilities: Te faster encryption times offered by the proposed method make it well-suited for real-time applications where timely data encryption is essential. Long messages with various lengths were selected; these messages were implemented using the presented method, the standard methods of SM cryptography were also implemented using the same messages. Table 3 shows the obtained experimental results for the long messages.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Table 3: ET (second) results for long messages

L (K character)	DES	3DES	AES	BF	Presented
3	18.9680	22.0400	140.8	9.0592	0.2860
6	38.9310	44.0600	282.7	18.1184	0.5180
9	58.9030	66.1100	425.5	29.1776	0.7680
12	78.8620	90.1500	567.4	40.2368	1.1220
15	98.8200	112.1000	710.2	51.2960	1.2810
18	117.8070	135.2300	852.1	62.3552	1.5200
21	136.7750	158.2600	989.9	71.4144	1.9700
24	155.7420	180.3100	1137.8	82.4736	2.0660
27	176.7110	03.3400	1280.6	91.5328	2.2730
30	194.6700	225.2000	1421.5	101.5920	2.7880

From Table 3, the following information can be extracted regarding the implementation results for long messages:

1) Message length and encryption time: The table provides data on the encryption time (in seconds) for long messages of various lengths, measured in kilobytes (K byte). The encryption time is reported for both the presented method and standard methods, such as DES, 3DES, AES, and BF.
2) Efficiency of the proposed method: The presented method consistently demonstrates shorter encryption time compared to standard methods across all message lengths. For instance, for a message length of 30 kilobytes, the encryption time using the presented method is 2.7880seconds, whereas it ranges from 194.6700 to 1421.5 seconds for standard methods.
3) Comparison across methods: By comparing the encryption times between the presented method and standard methods, it is evident that the presented method offers significant time savings, showcasing its efficiency in processing long messages.
4) Impact of message length: The encryption time increases as the message length grows for both the presented method and standard methods. However, the presented method consistently outperforms standard methods across all message lengths, indicating its ability to efficiently handle large volumes of messages.
5) Real-world application considerations: The shorter encryption times achieved by the presented method make it well-suited for applications requiring timely and secure encryption of long messages, such as data
transmission over networks or storage in cloud environments.

Overall, Table 3 provides valuable insights into the efficiency and effectiveness of the presented method in encrypting long messages compared to standard methods of message cryptography. Analysis of the data presented in Table 3 reveals the superior efficiency of the presented method compared to conventional message cryptography techniques. The table showcases a significant reduction in encryption time across various message lengths when employing the proposed method compared to standard methods, such as DES, 3DES, AES, and BF. This efficiency gain is particularly pronounced for long messages, underscoring the method's effectiveness in processing large volumes of message swiftly and securely.
The presented method quality was examined, several message were selected and executed using the presented method, the obtained results showed that the decrypted message was always identical to the source original message, the quality parameters for the encrypted message were calculated and table 4 shows the obtained results:

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Table 4: Quality parameters of the encrypted messages

Message length (character)	MSE	PSNR	CC
20	7935.4	20.7976	0.4630
50	6983.5	22.1547	0.3539
75	8492.0	20.2778	0.1934
100	8756.4	19.8924	0.3066
500	8224.8	20.6762	0.2507
1000	7565.3	21.5120	0.2832
2500	7987.9	20.9684	0.2696
5000	7749.5	21.2715	0.2837
10000	7927.0	21.0450	0.2583
25000	7754.0	21.2656	0.2878

Upon scrutinizing Table 4, it becomes evident that the presented method yields commendable results for the quality parameters (MSE, PSNR, and CC), underscoring its efficacy in preserving data integrity and fidelity throughout the encryption and decryption processes.

The presented method is very sensitive to the selected PK values, the relieving part must use the same PK used in the sending part, any changes in the PK made by the message receiver will be classified as a hacking attempt by producing a damaged decrypted SM, and to show this the message 'Efficient message encryption and decryption' was encrypted using the PK with r=3.77 and x=0.11, the encrypted message was decrypted by modified values of r and x and figure 9 shows the obtained messages, the damaged decrypted messages were obtained when changing r and/or x:

Decrypted SM using:r=3.76;x=0.13;
Eff□c´□□□□7□°□V□Y□±□^□Zo7□□n2 2Y6N□ □´o7
Decrypted SM using:r=3.78;x=0.11;
Effi±□□□□[es¹□ge@²¹lN/£□□□ a7□ d²□N□ G-{s
Decrypted SM using:r=3.77;x=0.11;
Effi±□□□□□ns°□V@Ysl'□ption and de□□yàè´□□

Figure 9: Obtained decrypted SMs

CONCLUSION

In this paper research, a straightforward yet robust method for message cryptography was presented and implemented. The presented method leverages various factors, including a chaotic logistic private key, a generated secret key, a sequence of operations, and the number of digits utilized for message binary matrix rows rotation, to ensure robust message protection. Through extensive experimentation, the presented method demonstrated its ability to meet the stringent requirements of effective data cryptography, as evidenced by its exceptional performance in key quality parameters, such as mean square error (MSE), peak signal-to-noise ratio (PSNR), and correlation coefficient (CC). The experimental findings underscored the superiority of the proposed method over conventional standard message cryptography methods. Specifically, the presented method exhibited greater efficiency by significantly reducing encryption and decryption times, thereby maximizing the speed of message cryptography. Additionally, we showcased the method's versatility by demonstrating its capability to utilize any secret message, irrespective of length.. This adaptability allows for seamless integration into various applications and facilitates easy key rotation without necessitating method modifications, thus ensuring sustained security and efficiency in the message cryptography process.

REFERENCES

1) Abu-Faraj, M., & Alqadi, Z. (2022). Image encryption using variable length blocks and variable length private key. *International Journal of Computer Science and Mobile Computing (IJCSMC), 11*(3), 138–151.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

2) Abu-Faraj, M., Al-Hyari, A., & Alqadi, Z. (2022). A dual approach for audio cryptography. *Journal of Southwest Jiaotong University, 57*(1), 24–33.
3) Abu-Faraj, M., Al-Hyari, A., & Alqadi, Z. (2022). Complex matrix private key to enhance the security level of image cryptography. *Symmetry, 14*(4), 664–678.
4) Abu-Faraj, M., Aldebei, K., & Alqadi, Z. (2022). Simple, efficient, highly secure, and multiple-purposed method on data cryptography. *Traitement du Signal, 39*(1), 173–178.
5) Abu-Faraj, M., Aldebe, K., & Alqadi, Z. (2021). Deep machine learning to enhance ANN performance: Fingerprint classifier case study. *Journal of Southwest Jiaotong University, 56*(6), 685–694.
6) Abu-Faraj, M., Alqadi, Z., & Aldebei, K. (2021). Comparative analysis of fingerprint features extraction methods. *Journal of Hunan University Natural Sciences, 48*(12), 177–182.
7) Abu-Faraj, M., & Alqadi, Z. (2021). Improving the efficiency and scalability of standard methods for data cryptography. *International Journal of Computer Science and Network Security (IJCSNS), 21*(12), 451–458.
8) Ala-Dwairi / Al-Dwairi entries: Al-Dwairi, M. O., Al-Hindi, A., Al-Qadi, Z. A. A., & Soliman, M. S. (2019). An efficient and highly secure technique to encrypt and decrypt color images. *Engineering, Technology & Applied Science Research, 9*(3), 4165–4168. https://doi.org/10.48084/etasr.2525
9) Al-Qaisi, A., Khawatreh, S. A., Sharadqah, A. A., & Alqadi, Z. A. (2018). Wave file features extraction using reduced LBP. *International Journal of Electrical and Computer Engineering, 8*(5), 2780–2787.
10) Al-Qadi, Z. A. (2009). A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image. *Journal of Computer Science, 5*(5), 355–362.
11) Al-Qadi, Z. A. A., Al-Dwairi, M. O., Abu Jazar, A., & Abu Zneit, R. (2010). Optimized true-RGB color image processing. *World Applied Sciences Journal, 8*(10), 1175–1182.
12) Al-Qadi, Z. A. A., Aqel, M. J., & ElEmary, I. M. M. (2008). Performance analysis and evaluation of parallel matrix multiplication algorithms. *World Applied Sciences Journal, 5*(2), 211–214.
13) Al-Qadi, Z. A. A., Aqel, M. J., Abdullah, A. A., & (2018). RGB color image encryption-decryption using image segmentation and matrix multiplication. *International Journal of Engineering & Technology, 7*(3.13), 104–107. https://doi.org/10.14419/ijet.v7i3.13.16334
14) Al-Qadi, Z. A. A., Abu-Jazzar, A. (2005). Analysis of program methods used in optimizing matrix multiplication. *Journal of Engineering.*
15) Al-Qadi, Z. A. A., Al-Zneit / Abu-Zneit & co. (2018). A novel zero-error method to create a secret tag for an image. *Journal of Theoretical and Applied Information Technology, 96*(13), 4081–4091.
16) Al-Qadi, Z., Amjad Y. Hendi, Majed O. Dwairi (various). (2019–2020). [Several articles on speech and image processing and encryption]. (Entries listed in source; multiple conference and journal papers 2016–2020.)
17) Al-Rawashdeh, A., & Al-Qadi, Z. (2018). Using wave equation to extract digital signal features. *Engineering, Technology & Applied Science Research, 8*(4), 1356–1359.
18) Al-Zahran / Zahran entries: Ayyoub, B., Zahran, B., Alqadi, Z., Abu-Ein, A., & others (2016–2019). Comparative and methodological works on image/speech processing and steganography. *International Journal of Computer Science & Information Technology (IJCSIT); International Journal on Informatics Visualization; International Journal of Computer Applications.* (Details in original list.)
19) Al-Husainy, M. A. F. (2012). Message segmentation to enhance the security of LSB image steganography. *International Journal of Advanced Computer Science and Applications, 3*(3), 57–62. http://www.ijacsa.thesai.org
20) Al-Husainy, M. A. F. (2012). Developed segmented LSB image steganography. *Proceedings of the International Science and Technology Conference (ISTEC 2012), Dubai.*
21) Aqel, M. J., Alqadi, Z. A., & Abdullah, A. A. (2018). RGB color image encryption-decryption using image segmentation and matrix multiplication. *International Journal of Engineering & Technology, 7*(3.13), 104–107. https://doi.org/10.14419/ijet.v7i3.13.16334
22) Aqel, M. J., Alqadi, Z., El Emary, I. M., & (2007). Analysis of stream cipher security algorithm. *Journal of Information and Computing Science, 2*(4), 288–298.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

23) Arising / Das: Das, R., & Das, I. (2016). Secure data transfer in IoT environment: adopting both cryptography and steganography techniques. In *Proc. 2nd Int. Conf. on Research in Computational Intelligence and Communication Networks* (pp. 296–301). Kolkata, India. https://doi.org/10.1109/ICRCICN.2016.7813674
24) Dwairi / Dwairi, Majed O., Hindi, A., Al-Qadi, Z. A. A. (2019). An efficient and highly secure technique to encrypt and decrypt color images. *Engineering, Technology & Applied Science Research, 9*(3), 4165–4168. https://doi.org/10.48084/etasr.2525
25) Emam, M. M., Aly, A. A., & Omara, F. A. (2016). An improved image steganography method based on LSB technique with random pixel selection. *International Journal of Advanced Computer Science & Applications, 7*(1), 361–366. https://doi.org/10.14569/IJACSA.2016.070350
26) Gong / Hua / Huang entries: Hua, Z., Zhou, Y., & Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. *Information Sciences, 480*, 403–419.
27) Jose, M. (2014). Hiding image in image using LSB insertion method with improved security and quality. *International Journal of Science and Research, 3*(9), 2281–2284.
28) Jin, B., Fan, L., Zhang, B., Lei, R., & Liu, L. (2024). Image encryption hiding algorithm based on digital time-varying delay chaos model and compression sensing technique. *iScience, 27*(9), 110717. https://doi.org/10.1016/j.isci.2024.110717
29) Khalifa, O. O., Naji, A. W., Zaidan, A. A., Zaidan, B. B., & Hameed, S. A. (2010). Novel approach of hidden data in the (unused area 2 within EXE file) using computation between cryptography and steganography. *International Journal of Computer Science and Network Security, 9*(5), 294–300.
30) Kumara, M. B., Karthikka, P., Dhivya, N., & Gopalakrishnan, T. (2014). A performance comparison of encryption algorithms for digital images. *International Journal of Engineering Research & Technology (IJERT), 3*(2).
31) Lee, M. H. Y., Tiedeu, A., & Kom, G. (2021). A robust and fast image encryption scheme based on a mixing technique. *Security and Communication Networks, Article ID 6615708.* https://doi.org/10.1155/2021/6615708
32) Loukhaoukha, K., Chouinard, J. Y., & Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. *Journal of Electrical and Computer Engineering, 2012*, Article ID 173931, 1–13.
33) Matrouk / Matrouk et al.: Matrouk, K., Al-Hasanat, A., Alasha'ary, H., Al-Qadi, Z., & Al-Shalabi, H. (2014). Analysis of matrix multiplication computational methods. *European Journal of Scientific Research, 121*(3), 258–266.
34) Matrouk, K., Al-Hasanat, A., Alasha'ary, H., Al-Qadi, Z., & Al-Shalabi, H. (2014). Speech fingerprint to identify isolated word person. *World Applied Sciences Journal, 31*(10), 1767–1771.
35) Majeed, A., Mat Kiah, M. L., Madhloom, H. T., Zaidan, B. B., & Zaidan, A. A. (2009). Novel approach for high secure and high rate data hidden in the image using image texture analysis. *International Journal of Engineering and Technology, 1*(2), 63–69. http://eprints.um.edu.my/id/eprint/4951
36) Matrouk / Khaled Matrouk et al. entries listed above (see Matrouk).
37) Mohammed / Motameni entries: Motameni, M., Norouzi, M., Jahandar, M., & Hatami, A. (2007). Labeling method in steganography. *Proceedings of World Academy of Science, Engineering and Technology, 24*, 349–354. ISSN 1307-6884. http://www.waset.org/journals/waset/v30/v30-66.pdf
38) Moustafa, A. A., & Alqadi, Z. (2009). Color image reconstruction using a new R'G'I model. *Journal of Computer Science, 5*(4), 250–254. https://doi.org/10.3844/jcs.2009.250.254
39) Musbah J. Aqel entries (multiple): Aqel, M. J., Alqadi, Z. A., Ammar A. Abdullah. (2018). RGB color image encryption-decryption using image segmentation and matrix multiplication. *International Journal of Engineering & Technology, 7*(3.13), 104–107. https://doi.org/10.14419/ijet.v7i3.13.16334
40) Nader / Nader Ahmad / Nader et al. entries (2016–2019): Nader, J., Abu-Ein, A., & Alqadi, Z. (2016). A technique to encrypt-decrypt stereo wave file. *International Journal of Computer and Information Technology, 5*(5), 465–470.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

41) Nader, J., Sharadqh, J. A., Al-Qadi, Z., & Zahran, B. (2016). Experimental investigation of wave file compression-decompression. *International Journal of Computer Science and Information Security, 14*(10), 774–780.
42) Nofs / Noor entries omitted (not in provided list).
43) Olimat, A. N., Al-Shawabkeh, A. F., Al-Qadi, Z., & Al-Najdawi, N. A. (2022). Forecasting the influence of the guided flame on the combustibility of timber species using artificial intelligence. *Case Studies in Thermal Engineering, 38*, 102379. https://doi.org/10.1016/j.csite.2022.102379
44) Othman / Zaidan group (multiple entries): Othman, F., Zaidan, A. A., Zaidan, B. B., Raji, R. Z., Hasan, A. K., & Naji, A. W. (2009). Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 1–7).
45) Pleacher, D. (n.d.). Calculating password entropy. Retrieved February 16, 2023, from https://www.pleacher.com/mp/mlessons/algebra/entropy.html
46) Potter / Pleacher note: merged as Pleacher above.
47) Rasras, R. J., Abu Sara, M. R., Al-Qadi, Z. A., & Abu Zneit, R. (2019). Comparative analysis of LSB, LSB2, PVD methods of data steganography. *International Journal of Advanced Trends in Computer Science and Engineering, 8*(3). https://doi.org/10.30534/ijatcse/2019/64832019
48) Ramadhani, F., Ramadhani, U., & Basit, L. (2020). Combination of hybrid cryptography in one time pad (OTP) algorithm and keyed-hash message authentication code (HMAC) in securing the WhatsApp communication application. *Journal of Computer Science, Information Technology and Telecommunication Engineering, 1*(1), 31–36.
49) Rihan, S. D., Saife, A. K., & Osman, E. F. (2015). A performance comparison of encryption algorithms AES and DES. *International Journal of Engineering Research & Technology (IJERT), 4*(12).
50) Rasras / Rashad J. Rasras (2019). A methodology based on steganography and cryptography to protect highly secure messages. *Engineering, Technology & Applied Science Research, 9*(1), 3681–3684.
51) Saleh Khawatreh, B. Ayyoub, Ashraf Abu-Ein, & Alqadi, Z. (2018). A novel methodology to extract voice signal features. *International Journal of Computer Applications, 975*, 8887.
52) Sarower, A. H., Karim, R., & Hassan, M. (2019). An image steganography algorithm using LSB replacement through XOR substitution. *Proceedings: 2019 International Conference on Information and Communications Technology (ICOIACT).* https://doi.org/10.1109/icoiact46704.2019.8938486
53) Shayeb, I., Alqadi, Z., & Nader, J. (2019). Analysis of digital voice features extraction methods. *International Journal of Educational Research and Development, 1*(4), 49–55.
54) Sun, C., Wang, E., & Zhao, B. (2021). Image encryption scheme with compressed sensing based on a new six-dimensional non-degenerate discrete hyper-chaotic system and plaintext-related scrambling. *Entropy, 23*, 291.
55) Vilkamo, J., & Bäckström, T. (2017). Time-frequency processing: Methods and tools. In V. Pulkki, S. Delikaris-Manias, & A. Politis (Eds.), *Parametric Time-Frequency Domain Spatial Audio* (pp. 3–24). Wiley.
56) Wu, D.-C., & Tsai, W.-H. (2003). A steganographic method for images by pixel value differencing. *Pattern Recognition Letters, 24*, 1613–1626. https://doi.org/10.1016/S0167-8655(02)00402-6
57) Zaidan, A. A., Majeed, A., & Zaidan, B. B. (2009). High securing cover-file of hidden data using statistical technique and AES encryption algorithm. *World Academy of Science Engineering and Technology (WASET), 54*, 468–479.
58) Zaidan, A. A., & Zaidan, B. B. (2009). Novel approach for high secure data hidden in MPEG video using public key infrastructure. *International Journal of Computer and Network Security, 1*(1).
59) Zaidan, A. A., Zaidan, B. B., Abdulrazzaq, M. M., Raji, R. Z., & Mohammed, S. M. (2009). Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. *International Association of Computer Science and Information Technology (IACSIT), 19*, 482–489.
60) Zaidan, A. A., Othman, F., Zaidan, B. B., Raji, R. Z., Hasan, A. K., & Naji, A. W. (2009). Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. *World Congress on Engineering* (presentation).

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

61) Zneit, R. A., Khrisat, M. S., Khawatreh, S. A., & Alqadi, Z. (2020). Two ways to improve WPT decomposition used for image features extraction. *European Journal of Scientific Research, 157*(2), 195–205.
62) Zhou, X., Gong, W., Fu, W., & Jin, L. (2016). An improved method for LSB based color image steganography combined with cryptography. In *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)* (pp. 1–4). Okayama, Japan. https://doi.org/10.1109/ICIS.2016.7550955
63) Zhang, X., & Wang, X. (2019). Multiple-image encryption algorithm based on DNA encoding and chaotic system. Springer.
64) Zhenjun, J. S., & Sun, R. (2016). Multiple-image encryption with bit-plane decomposition and chaotic maps. *Optics and Lasers in Engineering, 80*, 1–11.