ESP IJAST
ESP International Journal of Advancements in Science & Technology
ISSN: 2583-9233 / Volume 3 Issue 3 July 2025 / Page No: 15–23
Paper Id: IJAST-V3I3P103 / Doi: 10.56472/25839233/IJAST-V3I3P103

Original Article

Enhancing AES Encryption with Chaotic Maps for Improved Network Security

Zaid A. Abdulrazaq
Computer Techniques Engineering, Northern Technical University, Mosul, Iraq.

Received Date: 07 May 2025 Revised Date: 24 June 2025 Accepted Date: 08 July 2025

Abstract: *This paper presents an enhanced chaotic AES encryption algorithm with a diffusion mechanism for secure image encryption. The approach combines a dynamically generated chaotic S-box, derived from a logistic map, with a key-dependent diffusion phase to strengthen encryption performance. The chaotic S-box ensures high non-linearity, while the diffusion process introduces randomness and resistance to statistical attacks. Experimental results demonstrate the effectiveness of the proposed method, achieving high entropy values (7.9974), significantly low correlation coefficients (0.0021), and successful decryption with no data loss. These results validate the algorithm's robustness, reliability, and applicability in secure image transmission. Potential applications include sensitive fields such as medical imaging, defense, and IoT. The proposed scheme highlights the synergy between chaos theory and cryptographic techniques, offering a promising direction for future research in advanced encryption mechanism.*

Keywords: *AES, Cryptographic, Networks, S-Box, Security.*

I. INTRODUCTION

In the highly technological world that embraces the so-called fourth industrial revolution, network security is more significant than ever before . This is because most of the newly introduced technologies are based on interconnected networks, where security is a considerable concern [1-3]. To protect the network from vulnerabilities and attacks within the network, the data exchange in the network must be highly secured. In order to establish the security of any network, the main concern is the privacy and integrity of the data sent and received between the communication devices[4-5]. There are two ways to protect data during communication: encryption and the use of secure protocols or algorithms in the network. In this context, secure transmission of data and the measures applied to do so are investigated more closely. The Advanced Encryption Standard (AES) is broadly used as a secure and efficient encryption standard for transferring confidential information across vulnerable channels. The large number of known vulnerabilities of traditional AES algorithms is offered over others [6-7]. The abuse of secure channels of AES encryption is facilitated by the consequences of gaining unauthorized access to confidential or especially encrypted data. To cope with this issue, chaos-based cryptosystems are utilized to improve the strength of symmetric encryption. Here the effectiveness of selecting a chaotic map in AES encryption is evaluated so the encryption process can be further strengthened against various types of attacks. To effectively cope with various types of potential threats, the selected chaotic map's unpredictability, non-linearity, and dependency on the secret key are essential [3][4]. The introduction of chaotic values generated by the selected map, which are used to update the S-Box, can protect the encryption process from attacks effectively. Frequent testing of the dynamic S-Box of the chaotic map during decryption ensures that the encryption process confronts the highest level of security possible. It potentially broadens the spectrum of AES in terms of enhanced security by exploring new insights. The potential of chaotic maps used in the traditional AES method to strengthen the encryption process is experimentally verified and successfully realized [8-10]. Furthermore, the characterization of the chaotic SDM to a deeper analysis of the substitution mechanism in the above chaos-based S-Box is extended. This detailed chaotic S-Box analysis is useful for the development of more effective security mechanisms. With the advancement of secure communication in contemporary society, the development of innovative security solutions is currently of great interest. In light of this phenomenon, secure information exchange or transmission is broadly and continuously addressed in both academia and industry [11-12]. The secure channels for exchanging confidential data across networks are opened to some extent to ensure that it is not intercepted or altered by unauthorized parties. With this approach, initially, the most widely accepted secure channel is AES encryption, which is a benchmark widely employed to improve the symmetric encryption strength of confidential data. With the continuous introduction of new algorithms and computational resources, traditional AES encryption cunningly performed some kind of attack by decrypting encrypted data. For the described reasons, chaotic maps may be useful tools for developing sophisticated cryptosystems [13-15]. Besides their sensitive dependence on original conditions and their pseudo-random or random-like nature, chaotic maps have a large holder exponent, which can be easily tailored. A secure communication system has been proposed with encryption based on the multiplication of the original message with the output of a chaotic operands generator map. To obtain the plain message, the chaotic product undergoes a process consisting of discrete wavelet transformation decomposition along with various

wavelet functions and decomposition levels. Subsequently, a partition is supplied to parse the detailed coefficients by a segmented block of bits and specify the same coefficients for each block [16- 18].

II. RELATED WORKS

Cryptographic systems play a significant role in the present security scenario due to the data that is transmitted over the internet. The primary goal is security, which is essential to prevent intruders from accessing the data. Cryptographic algorithms such as the Advanced Encryption Standard (AES) have been most commonly used to protect confidential data during transmission [19]. The security of the AES algorithm is based on its key length, the more bits the key length, the stronger the AES encryption security. Recently, the security of the AES algorithm has become a major concern, contributing to a significant increase in the number of researchers focusing on this particular issue [20]. Researchers must discover multiple methods to strengthen this algorithm. Providing an additional supporting system in the form of chaotic maps to enhance the security of the AES algorithm is one of the decryption approaches [21-22]. A plethora of previous researchers concentrated on applying chaotic maps to various encryption techniques. Researchers used these maps in ways such as generating keys, shuffling, and substituting their locations to amplify the encryption performance of cryptographic algorithms . The data ciphering speed, avalanche effect, encryption time, and key sensitivity of the chaotic systems were analyzed by these technics [23-25]. The proposed methodology has not been used on the AES decryption algorithm previously. The undocumented utilization of the chaotic maps as a supportive technology would unmistakably enrich the encryption algorithm's security, broaden the understanding of these functions, and inspire supplementary research in this domain. Nonetheless, since the AES algorithm is the most secure algorithm, it is critical to find alternatives that are more secure in order to fulfill this purpose. So, devising an innovative system using chaotic maps and the AES algorithm to be employed as an extra layer of network information security is highly recommended [26]. Furthermore, because hackers' techniques and sensitivities have improved, installing additional layers of security will be more difficult to expose in the event of an assault. The above system can be incorporated as an additional layer of security.

The research proposed improved AES with randomization of S-BOX using logistic chaotic map because of the minimum information exchanged between transmitter and receiver then diffusion approach with for each round of AES improving security performance.

III. THEORETICAL FRAMEWORK

The launch of the Advanced Encryption Standard (AES) has quadrupled the adoption of encryption worldwide. Under the Competition for Advanced Encryption Standard, the authors of the Rijndael algorithm have emerged. Successfully, they have steadily improved its algorithm efficiency and resistance to cryptanalysis through a combination of greater algebraic complexity of its operations and a greater number of rounds [27-30]. Due to its success, the security and efficiency of the AES algorithm are no longer to be distrusted. Opponents of the AES algorithm must rely on time-consuming and challenging cryptanalysis. As a result, misleading and unrealistic exhaustive search time assessments have persisted since its inception. With exponentially increasing complexities, for the first time, previous study methodologically and theoretically estimates practical and 'truly safe' search times for partial and full AES keys [30- 31].

In recent years, chaotic systems have been applied in computer security for their ergodic mix of statistical properties. Given the importance of securing the transmission of sensitive information across a public channel, there is a growing interest in secure communication systems. Consequently, increasing attention has been paid to new strange attractors discoveries capable of holding a significant number of chaotic transforms useful in secure communications. Despite the success of the Rijndael method, selected as the Advanced Encryption Standard (AES) and the greatest competitive candidate since its invention, there has been a tremendous endeavor to improve its safety and efficiency through both hardware and software implementations [32- 33].

A. Basics of AES Encryption

Advanced Encryption Standard (AES) in Figure 1 comprises of a number of changes, which connected on the information piece iteratively in a settled number of rounds. The number of rounds depends on the length of the encryption key; 10 rounds for a 128-bit key, 12 rounds for 192-bit key and 14 rounds for a 256-bit key. For a 10 circular (128-bit AES) emphasis, nine rounds are comparable with four changes specifically Sub Bytes, Shift Rows, Mix Columns and Include Round Key but the tenth circular has as it were three changes short the Mix Columns encryption method to develop an encryption system. effectiveness of the proposed system to secure sensitive data over network traffic. A detailed made system was informed in each part to ease better understanding of the system operation. Moreover, the test outcomes are shown with insightful explanations of selected test settings. This research conducted establishes that predicted and robust encryption mechanisms can be developed [34].

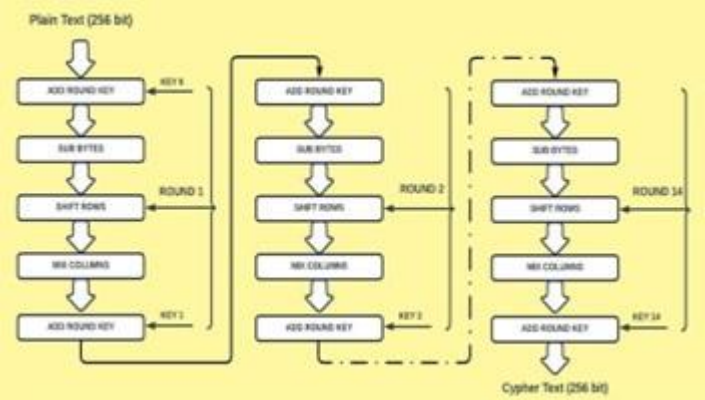

Figure 1 : AES Structure

IV. ROBLEM STATEMENT WITH PROPOSED APPROACH

The research proposed improved the randomization of S-BOX using chaotic as shown in Fig. 2 maps with the Objective of Progress the encryption productivity and security of the AES calculation by joining chaos-based S- box era. The Inventive Angle was Utilize Logic chaotic system to powerfully produce an S-box for AES, guaranteeing: Tall haphazardness within the substitution step.

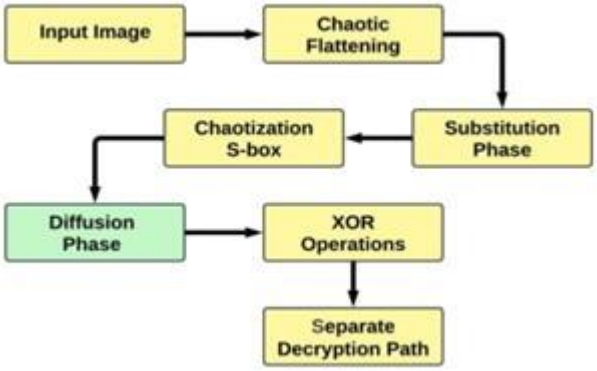

Figure 2 : Proposed Algorithm

More grounded resistance to cryptanalysis. Improved torrential slide impact (Strict Torrential slide Basis). The steps of implementation were :

- Use a chaos-based generator to produce dynamic S- boxes.
- Replace the static AES S-box with the dynamic S- box.
- Apply the enhanced AES algorithm to encrypt multiple images such as cameraman (as an example of normal image), brain image (as an example of medical image), surface compositional mapping (as an example of hyperspectral image).
- Analyze the performance metrics (entropy, correlation).

V. CHAOTIC SYSTEM DESIGN

A. Step 1 : Logistic Maps

$$x_{n+1} = \ . x_n \ . (1 \ - \ x_n) \quad \text{.....1}$$

r: control parameter (typically $3.57 \leq r \leq 4$)., initial value x_0 should be random and secret.

B. Step 2 : Generating Dynamic S-box

Use the chaotic system to generate substitution values for the AES S-box:

a) Generate a Sequence of Chaotic Numbers.

- Normalize the sequence to fit the range [0,255][0, 255][0,255] for an 8-bit S-box.

b) Remove Duplicate Values to Ensure Bijection (A Requirement for S-Boxes)

c) Apply Scrambling Techniques to Enhance Randomness.

d) Validate the S-Box Using Metrics:

- Non-linearity: Check resistance to linear attacks.

- Strict Avalanche Criterion (SAC): Evaluate diffusion properties.

C. Step 3 : Enhanced AES Integration

a) Substitution Layer: Replace the Static S-Box of AES with the Chaotic Dynamic S-Box.

b) Key Scheduling: Use Another Chaotic Sequence to Enhance the Key Expansion Phase.

c) Encryption Process:

d) Test on Image Datasets Such as:

- Standard images: Lena, Cameraman.
- Specialized datasets: Medical images, hyperspectral images

D. Step 4: Performance Analysis

Evaluate and compare the enhanced AES algorithm to the standard AES. Metrics include:

a) Security Metrics:

- Entropy: Ideal value is close to 8 for 8-bit images.
- Pixel Correlation: Should be near o for encrypted images.
- Histogram Analysis: Uniformity indicates strong encryption.
- Key Sensitivity: Test small variations in the key.
- Avalanche Effect: Measure the effect of flipping a single bit on ciphertext.

b) Efficiency Metrics:

- Encryption Time: Time taken to encrypt the dataset.
- Throughput: Measure the data processing rate.

i) Input Image

- The image is taken as input.

ii) Chaotic Flattening

- The image is flattened into a vector using a chaotic sequence.

iii) Substitution Phase

- A substitution process is applied using a chaotic S- box.

iv) Chaotization S-box

- Further transformation occurs using a chaotic S-box.

v) Diffusion Phase

- The modified image undergoes a diffusion phase to enhance security.

vi) XOR Operations

- XOR operations are applied with a chaotic key to enhance diffusion.

vii) Separate Decryption Path

- The decryption path follows an inverse process to reconstruct the original image.

VI. DYNAMIC S-BOX PERFORMANCE ANALYSIS

A. Non-linearity

To reduce the possibility of linear cryptanalysis attacks and keeps the plaintext confidentiality there is a high need for ensure the non-linearity property of S-Box. The non- linearity of an n-bit S-Box calculated using the equation (2):

$$N(b) = \frac{1}{2}\left[2^n - \left(max_{h\in\{0,1\}^n}\right)\left|W\ \bar{S_b}\ (h)\right|\right] \ldots\ldots\ldots 2$$

The Walsh spectrum of a function computed by the equation (3):

$$W\ S(h) = \Sigma_{x\in\{0,1\}^n}(-1)^{b(x)\ \oplus\ h.x} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 3$$

Where h ∈ $\{0,1\}^n$ and h.x is the dot product of h and x computed by equation (4) :

$$h.x = (h_1 \oplus \quad 1) + \ldots + (h_n \oplus \quad x_n) \ldots\ldots\ldots\ldots\ldots\ldots 4$$

The non-linearity degree can be calculated by computing its Walsh spectrum and that will be necessary for high performance S-Box for cryptography application. The proposed S-Box has non-linearly value 128.

B. Linear-Probability (LP)

Linear probability if a metric of correlation between S-Box inputs and outputs. The lower value of LP indicates high-level cryptographic power. From equation (5), the Value of LP is (0.5) for the proposed S-Box is indicating good resistance against linear attacks.

$$LP = max_{a_z, b_z \neq 0} \left| \frac{\#\{Z \in N | Z.a_z = s(z).b_z\}}{2^N} \right| \ldots\ldots\ldots\ldots\ldots\ldots 5$$

VII. SECURITY ANALYSIS

Security analysis is an important process to examine the results of the proposed encryption/decryption system. The images illustrated in Figure 3 used for tests.

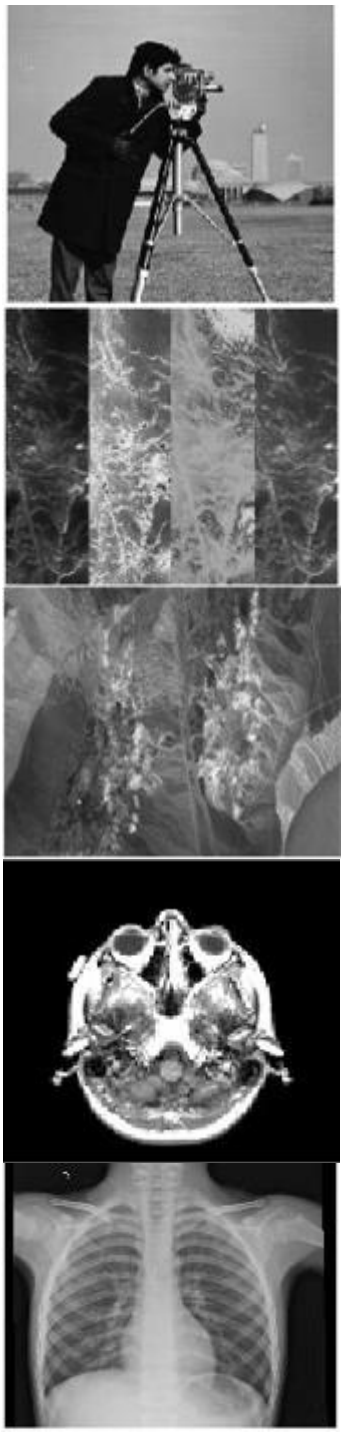

Figure 3 : Used Images in Proposed Work

A. Histogram Analysis

Histogram is the distribution of the pixels through the image inside a statistical curve. For a grayscale image, the x-

axis of the histogram represents pixel intensity values (from 0 = black to 255 = white), and the y-axis shows how many pixels have each intensity value. For a color image, histograms can be generated for each color channel (Red, Green, Blue).

Histogram analysis is a common statistical attack method.

- A non-uniform histogram of an encrypted image may leak information to attackers.
- A flat histogram means the image encryption is likely statistically secure.

Figure 4 show the histogram of the chosen images versus it encrypted form. It can be observed that each encrypted histogram of an image very different from its original histogram form that is indication that no statistical attack can be done to retrieve the original image from the encrypted image.

B. Entropy Analysis

In information theory, entropy measures the amount of uncertainty or randomness in data. It was introduced by Claude Shannon, and it tells us how unpredictable the information is. For an image:

- Entropy gives us an idea of how much information is stored in the image.
- In the context of encryption, higher entropy = higher randomness = better security.

In a securely encrypted image, the entropy should be close to the maximum value:

For an 8-bit image (values from 0–255), the maximum entropy is 8. An ideal encrypted image should have entropy very close to 8 (e.g., 7.99+).

- This indicates the pixel values are uniformly random, with no detectable patterns.
- This is a key sign that the encryption is effective and the image is resistant to information leakage.

To test the randomness manner of an image the Shannon entropy takes turn. Which defined by the following equation:

$$E(I) = \sum_{1}^{N}[P(I_i)\log_2(P(I_i))] \quad \text{.....6}$$

Table 1 presents the entropy results of the source and images that must be highly near to identical value 8 that indicates that the image is random and there is no statistical information to retrieve the original image from the ciphered image proving the effectiveness of the encryption system.

Table 1 : Entropy Results

Image	Encrypted image channels
Camera man	7.9974
CT-Scan	8.0000
Hyperspectral 1	7.9995
Hyperspectral 1	7.9997
MRI	7.9899

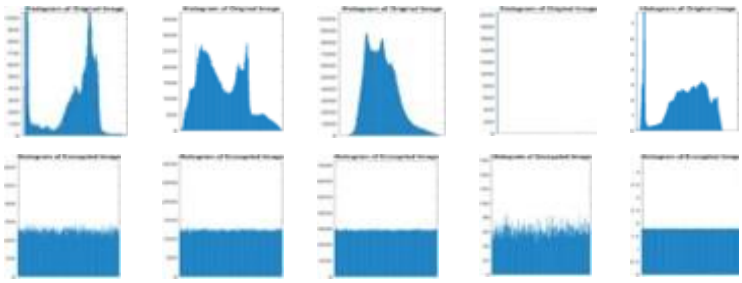

Figure 4 : Histogram Analysis

C. Correlations Coefficient Analysis

The correlation analysis used to examine the relation between pixels of images as shown in the following equation.

$$p_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad \text{.....7}$$

The equation added in multiple directions: horizontal (H), vertical (V), diagonal (D) for each channel of the two

images original and encrypted red, green, blue for chosen images presented in table. 2 if the distribution of the pixels of the image symmetric the value of correlation coefficient high close to 1 but if else the distribution of the pixels is not uniformed the correlation coefficient is far away from 1 then the value close to 0 or -1. So, for high performance image encryption system the second choice is the best from table. 2 it can be observed that values are indication to the success of encryption process.

Table 2 : Correlations Results

Image	Source image	Encryption image
Camera man	0.9333	0.0021
CT-Scan	0.9989	0.0001
Hyperspectral 1	0.9291	0
Hyperspectral 1	0.9555	0.0013
MRI	0.9059	0.0088

VIII. CONCLUSION AND FUTURE WORK

This paper presented a novel, enhanced AES encryption algorithm incorporating a dynamic diffusion mechanism using chaotic maps for secure image encryption. The strength of a dynamic chaotic S-Box and a key-dependent diffusion phase dramatically improves the quality and robustness of the encryption process.

The performance evaluation metrics offered several points:

- High entropy values (close to 8), indicating strong randomness in encrypted images.
- Low correlation coefficients between adjacent pixels, confirming effective decorrelation and resistance to statistical attacks.
- Successful decryption of the original image, validating the correctness and reliability of the algorithm.

In terms of cryptographic strength:

- The proposed S-Box achieves a non-linearity value of 128 and a linear probability (LP) of 0.5, reflecting strong resistance to linear and differential cryptanalysis.

Compared to conventional AES, the proposed approach offers enhanced security by leveraging the properties of chaos theory, making it highly suitable for protecting sensitive visual data.

The results highlight the potential of chaotic-based cryptographic schemes in applications such as medical imaging, military systems, and Internet of Things (IoT) environments:

A. Real-Time Implementation

Optimize the algorithm for real-time processing on hardware platforms such as FPGAs, GPUs, or embedded systems to meet the needs of latency-sensitive applications like video streaming and live surveillance.

B. Video Encryption

Extend the algorithm to handle video data, exploring its efficiency and effectiveness in encrypting multi-dimensional datasets while maintaining low computational overhead.

C. Chaotic Map Diversity

Investigate other chaotic maps, such as 3D logistic maps or hybrid chaotic systems, to further strengthen the randomness properties of the S-box and enhance security against cryptanalysis.

D. Adaptive Encryption

Develop an adaptive mechanism where the chaotic parameters or keys are updated dynamically during encryption to resist chosen-plaintext and known-plaintext attacks.

E. Compression Compatibility

Explore the integration of the encryption algorithm with compression standards (e.g., JPEG, MPEG) to maintain security while optimizing storage and transmission efficiency.

F. Quantum-Resistant Enhancements

Study the incorporation of quantum-resistant cryptographic techniques to ensure the algorithm remains secure

against potential threats posed by quantum computing.

G. Statistical and Security Analysis

Conduct an in-depth analysis of NPCR (Number of Pixel Change Rate), UACI (Unified Average Changing Intensity), and key sensitivity under various attack models, such as brute force and differential attacks, to solidify the algorithm's robustness.

H. Multi-Layer Cryptographic Framework

Explore the integration of the proposed algorithm into a multi-layer encryption framework for heightened security in applications requiring multi-level protection.

By addressing these directions, the proposed method can evolve into a comprehensive solution for secure data encryption across diverse fields, including healthcare, defense, and IoT ecosystem

- **Conflict of Interest** : "The author declare no conflict of interest".

IX. REFERENCES

[1] SALIH, Ahmed Amir; ABDULRAZAQ, Zaid Abdulsattar; AYOUB, Harith Ghanim. Design and enhancing security performance of image cryptography system based on fixed point chaotic maps stream ciphers in FPGA. Baghdad Science Journal, 2024, 21.5 (SI): 1754-1754.

[2] AYOUB, Harith G., et al. Unveiling robust security: Chaotic maps for frequency hopping implementation in FPGA. Ain Shams Engineering Journal, 2024, 15.11: 103016.

[3] S. A. Baker, S. J. Rashid, and O. I. Alsaif. Fog Computing: A Comprehensive Review of Architectures, Applications, and Security Challenges. Northern Technical University Journal for Engineering and Technology (NTU-JET), 2023.

[4] ARROYO, David; DIAZ, Jesus; RODRIGUEZ, F. B. Cryptanalysis of a one round chaos-based substitution permutation network. Signal Processing, 2013, 93.5: 1358-1364.

[5] HWANG, Jinha, et al. Machine learning in chaos-based encryption: Theory, implementations, and applications. IEEE Access, 2023, 11: 125749-125767.

[6] ZEGHID, MEDIEN; AHMED, HASSAN YOUSIF; KHAN, AKHTAR NAWAZ. High-Level Design and Implementation of a Configurable Cryptosystem with a Novel Chaos-Enhanced Function. IEEE Access, 2025.

[7] ALTAMEEM, Ayman, et al. A hybrid AES with a chaotic map-based biometric authentication framework for IoT and industry 4.0. Systems, 2023, 11.1: 28.

[8] KUMAR, Sanjay; SHARMA, Deepmala. Image scrambling encryption using chaotic map and genetic algorithm: a hybrid approach for enhanced security. Nonlinear Dynamics, 2024, 112.14: 12537-12564.

[9] ALAWIDA, Moatsum. A novel image encryption algorithm based on cyclic chaotic map in industrial IoT environments. IEEE Transactions on Industrial Informatics, 2024.

[10] HABBAL, Adib; ALI, Mohamed Khalif; ABUZARAIDA, Mustafa Ali. Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. Expert Systems with Applications, 2024, 240: 122442.

[11] KAMALOV, Firuz, et al. Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective. Sustainability, 2023, 15.4: 3317.

[12] MANIKANDAPRABHU, P.; SAMREETHA, M. A review of encryption and decryption of text using the AES algorithm. International Journal of Scientific Research & Engineering Trends, 2024, 10.2.

[13] SARKAR, Bikramjit, et al. A Survey on the Advanced Encryption Standard (AES): A Pillar of Modern Cryptography. 2024.

[14] MOURA, Ricardo, et al. MultiTLS: using multiple and diverse ciphers for stronger secure channels. Computers & Security, 2023, 132: 103342.

[15] KUMAR, Chanumolu Kiran; RAMACHANDRAN, Nandhakumar. Intrusion Detection Model Using Chaotic MAP for Network Coding Enabled Mobile Small Cells. Computers, Materials & Continua, 2024, 78.3.

[16] NASR, Marwa A., et al. A robust audio steganography technique based on image encryption using different chaotic maps. Scientific Reports, 2024, 14.1: 22054.

[17] KENT, Robert M.; BARBOSA, Wendson AS; GAUTHIER, Daniel J. Controlling chaos using edge computing hardware. Nature Communications, 2024, 15.1: 3886.

[18] ADENIYI, A. E., et al. Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach. Multimedia Tools and Applications, 2023, 82.13: 20537-20551.

[19] HADJ BRAHIM, A.; ALI PACHA, A.; HADJ SAID, N. An image encryption scheme based on a modified AES algorithm by using a variable S-box. Journal of Optics, 2024, 53.2: 1170-1185.

[20] ABDUL HUSSIEN, Farah Tawfiq; ALDEEN KHAIRI, Teaba Wala. Performance Evaluation of AES, ECC and Logistic Chaotic Map Algorithms in Image Encryption. International Journal of Interactive Mobile Technologies, 2023, 17.10.

[21] LI, Lizong. A novel chaotic map application in image encryption algorithm. Expert Systems with Applications, 2024, 124316.

[22] LIU, Lingfeng; WANG, Jie. A cluster of 1D quadratic chaotic map and its applications in image encryption. Mathematics and Computers in Simulation, 2023, 204: 89-114.

[23] ALEXAN, Wassim, et al. Color image encryption through chaos and kaa map. IEEE Access, 2023, 11: 11541-11554.

[24] SHUKUR, Wisam Abed; QURBAN, Luheb Kareem; ALJUBOORI, Ahmed. Digital data encryption using a proposed W-method based on AES and DES algorithms. Baghdad Science Journal, 2023, 20.4: 1414-1414.

[25] R. H. Joudah and M. E. Manaa. A New Approach to Improving the Security of the 5G-AKA Using Crystals-Kyber Post-Quantum Technologies and ASCON Algorithm. International Journal of Safety & Security, 2024.
[26] F. Shen, L. Shi, J. Zhang, C. Xu, Y. Chen, and Y. He. BMSE: Blockchain-based multi-keyword searchable encryption for electronic medical records. Computer Standards & ..., 2024.
[27] P. Duan, Z. Ma, H. Gao, and T. Tian. Multi-Authority Attribute-Based Encryption Scheme With Access Delegation for Cross Blockchain Data Sharing. IEEE Transactions on ..., 2024.
[28] J. Gong, L. Xiong, F. Zhang, and M. Pu. Integrated Quad-Color Nanoprinting and Tri-Channel Holographic Encryption Meta-Marks with Printable Metasurfaces. Laser & Photonics, 2025.
[29] A. Bedi, J. Ramprabhakar, R. Anand, and U. Kumaran. A Novel Blockchain Supported Hybrid Authentication and Handshake Algorithm for Smart Grid. IEEE, 2024.
[30] S. K. Gochhi, S. Sahoo, and P. K. Samanta. Blockchain-Based Comparative Analysis of E-Voting Systems: A Review. In Smart, Secure ..., 2024.
[31] M. Alawida. Enhancing logistic chaotic map for improved cryptographic security in random number generation. Journal of Information Security and Applications, 2024.
[32] MNE Farandi, A Marjuni, and N Rijati. Enhancing image encryption security through integration multi-chaotic systems and mixed pixel-bit level. The Imaging Science, 2024.
[33] T. Umar, M. Nadeem, and F. Anwer. Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage. Expert Systems with Applications, 2024.
[34] X. Fang, C. Guyeux, Q. Wang, and J. M. Bahi. Randomness and disorder of chaotic iterations. Applications in information security field. 2016.
[35] M. Shariatzadeh, M. Javad Rostami, and M. Eftekhari. An Adaptive Image Encryption Scheme Guided by Fuzzy Models. 2022.