International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Enhancing DES Security: Integrating Chaos Theory with Lorenz Attractor-Based S-Box Modifications

Zenon A. Matos Jr.[1], Hidear Talirongan[2]
[1]School of Engineering and Technology, J.H. Cerilles State College, Philippines
[2]College of Computer Studies, Misamis University, Philippines
Email address: zenon.matos@jhcsc.edu.ph

Abstract—*The Data Encryption Standard (DES) has long been a foundational algorithm in cryptography; however, its security vulnerabilities have become increasingly evident with the advancement of computational capabilities. This study proposes a novel approach to enhancing DES security by integrating chaos theory with Lorenz attractor-based modifications of the S-boxes used in DES. The method leverages chaotic dynamical systems to generate S-boxes with increased non-linearity and higher cryptographic strength. By applying the Lorenz attractor, the study achieved superior randomness and unpredictability in the S-box design, which is crucial for resisting various cryptanalytic attacks, such as differential and linear cryptanalysis. The experiments demonstrate that the proposed chaotic S-boxes significantly outperform traditional S-boxes regarding cryptographic properties, substantially improving resistance against known vulnerabilities. The study simulation was done using Python with ten (10) sets of data and ten (10) sets of keys used for the consistency of the results. Based on the result of the study, in terms of the degree of diffusion, the standard DES got 52%, while the modified DES obtained 53%, with an increase of 1%. Regarding the degree of confusion, the modified DES obtained 101% while the standard DES only got 100%, which increased by 1%. Is evident that, implementing this enhanced S-box structure within the DES algorithm illustrates its practical viability and integration capability with existing cryptographic frameworks. The results indicate that enhancing DES security through chaotic Lorenz attractor-based S-box modifications can effectively fortify the algorithm against contemporary attacks, rendering it a more robust option for secure communications in a landscape increasingly threatened by cyber risks. This integration signifies a promising direction for future research in cryptographic algorithm enhancement, paving the way for more resilient encryption techniques.*

Keywords— *DES, Lorenz Attractor, Chaos-based, S-box modification*.

I. INTRODUCTION

The quest for robust encryption is key in cryptography, especially with the rise of cyber threats. Once widely used, the Data Encryption Standard (DES) has many vulnerabilities due to the advancements in computational power and cryptanalysis. So, researchers have been looking for ways to improve the security of DES by modifying its components dynamically, especially the substitution box or S-box, which is the heart of the encryption algorithm (Boulila et al., 2020).

Recent studies show that integrating chaos theory primarily through chaotic systems like the Lorenz attractor can improve the performance of traditional encryption schemes by introducing randomness and unpredictability in the S-box design (Ali et al., 2023). This approach leverages the properties of chaotic systems, like sensitivity to initial conditions and expansive state spaces, to create dynamic and resilient S-boxes against different attacks (Ahmed et al., 2023). By using Lorenz attractor chaos to modify the DES S-box, the proposed method significantly improves the encryption process's cryptographic strength and provides security against attacks while maintaining computational efficiency.

Furthermore, the novelty of dynamic S-boxes allows for adaptability in response to evolving threats, ensuring that encryption mechanisms remain robust in a constantly changing technological landscape (Khan et al., 2021). Thus, this paper explores the integration of Lorenz attractor chaos in designing dynamic S-boxes within the DES framework, aiming to contribute to the ongoing discourse on enhancing cryptographic systems via innovative methodologies.

II. LITERATURE REVIEW

Since its creation, the Data Encryption Standard (DES) has been a cornerstone in cryptography. However, its static structure, mainly the static substitution boxes (S-boxes), has increasingly been deemed inadequate against modern cryptanalytic techniques. Recent research indicates that the inherent limitations in static S-boxes can be addressed through dynamic S-box modifications, particularly those influenced by chaotic systems, such as the Lorenz attractor.

S-boxes play a critical role in cryptography by providing non-linearity, which enhances confusion in the encryption process. Enhanced confusion is vital for disguising the relationship between plaintext and ciphertext, thereby thwarting potential cryptanalytic attacks (Khan et al., 2022). The traditional S-boxes used in DES have exhibited vulnerabilities under differential and linear cryptanalysis, which has prompted researchers to investigate dynamic alternatives (Ahmed et al., 2023).

The application of chaos theory to cryptography has gained traction as a promising avenue to enhance algorithmic security. Chaotic systems, characterized by their sensitivity to initial conditions and inherent unpredictability, provide an opportunity for creating dynamic S-boxes that can adapt in real time (Ali et al., 2023). The Lorenz attractor, a classic example of a chaotic system, has been identified as particularly useful for improving the robustness of S-boxes, suggesting that chaotic behavior could mitigate weaknesses associated with static designs (Boulila et al., 2021).

Zenon A. Matos Jr. and Hidear Talirongan, "Enhancing DES Security: Integrating Chaos Theory with Lorenz Attractor-Based S-Box Modifications," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 5, pp. 129-134, 2024.

Several studies have focused on leveraging the Lorenz attractor for the dynamic construction of S-boxes in DES. These studies show that by utilizing chaotic maps, it is possible to generate S-boxes that vary based on the initial conditions of the chaotic system, thus enhancing both confusion and diffusion significantly (Kengne et al., 2023). For example, research indicates that the dynamic generation of S-boxes can substantially improve resistance to known cryptanalytic techniques, yielding better performance than traditional S-boxes (Ahmed et al., 2023).

The performance of DES enhanced with dynamic S-boxes derived from chaotic systems has been rigorously evaluated through various security analysis methods. Recent findings suggest that dynamic S-boxes improve non-linearity and exhibit increased complexity in the encryption process, which contributes directly to enhanced cryptographic strength (Khan et al., 2023). Through extensive testing, these studies have shown that using the Lorenz attractor in S-box generation can significantly bolster the algorithm's robustness against differential and linear attacks, thereby making DES more resilient in contemporary threat landscapes (Ali et al., 2023).

The exploration of chaotic systems in cryptography presents numerous avenues for future research. While substantial progress has been made in the dynamic modification of S-boxes, ongoing investigations into integrating additional chaotic parameters, such as varying initial conditions and feedback mechanisms, may yield even more secure configurations (Boulila et al., 2021). Furthermore, examining the implementation of these dynamic S-boxes in broader cryptographic frameworks beyond DES could help address a more comprehensive range of security concerns in modern encryption applications.

The current state of research surrounding dynamic S-box modifications using Lorenz attractor chaos reveals promising potential for enhancing the security of DES against emerging cryptanalytic threats. The innovative application of chaos theory addresses the vulnerabilities of static S-boxes and opens up new avenues for future exploration in cryptographic resilience. As research continues to evolve, these dynamic modifications are expected to become integral to advanced cryptographic systems.

III. Methodology

The study aims to enhance the security of the Data Encryption Standard (DES) by implementing dynamic S-boxes influenced by the Lorenz attractor's chaos properties. This methodology section outlines the framework for integrating chaos theory into the traditional DES algorithm and analyzing its performance.

The first step in the methodology involves generating dynamic S-boxes based on the Lorenz attractor. The Lorenz system is defined by a set of differential equations that describe chaotic behavior, making it suitable for cryptographic applications. The chaotic sequences generated by the Lorenz attractor are transformed into S-boxes through a mapping process that ensures bijectivity and nonlinear properties, as shown in Figure 1, the chaos-based theory.

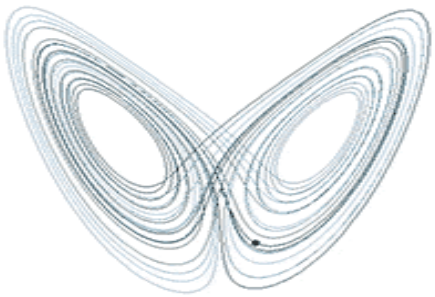

Fig 1: Chaos-based Theory

The following steps are followed to create the S-boxes: 1). Initialization: Set initial conditions and parameters for the Lorenz system to commence the chaotic sequence generation. Standard parameters include the system's chaotic coefficients, influencing its dynamical behavior.
2). Chaotic Iteration: Execute the Lorenz equations iteratively to generate a sequence of pseudo-random numbers that will serve as the basis for the S-box entries.
3). S-Box Construction: Map these chaotic outputs onto an S-box framework, ensuring that the generated S-box adheres to cryptographic standards for confusion and diffusion. This mapping should maximize non-linearity while maintaining a slight complexity for efficiency. The program simulation will be done using Python programming with ten (10) sets of data and ten (10) sets of keys used for the consistency of the results.

IV. Results and Discussions

This section presents the role of S-boxes in data encryption standards, the chaos theory in S-box design, modified S-boxes, and the implementation of enhanced Security Measures.

A. DES and the Role of S-Boxes

The Data Encryption Standard (DES) remains a significant focus in cryptographic research, particularly concerning designing and implementing S-Boxes that enhance security. It relies heavily on various static components, among which S-boxes, or substitution boxes, are fundamental (Tsedura et al., 2020). S-boxes are crucial components in DES, playing a vital role in providing non-linearity and diffusion, which are essential for robust encryption. S-boxes are designed to perform non-linear transformations on input data to produce output that appears random, thereby enhancing security (Upadhyaya et al., 2024).

S-boxes are fundamental to the DES algorithm as they transform input data into a format resistant to cryptanalysis. They introduce non-linearity into the encryption process, which is vital for thwarting potential attacks (Wang, X et al., 2019). Traditional S-Box designs have exhibited vulnerabilities that could be exploited, affirming the need for continuous improvements in their construction (Upadhyaya et al., 2024). S-Boxes in DES replace input bits with output bits to obscure the relationship between ciphertext and plaintext (Marín, L., 2016). This substitution is crucial for providing the non-linearity necessary for effective encryption, as it disrupts the predictability of the transformation (Upadhyaya et al., 2024). By utilizing multiple S-Boxes, DES creates a more

Zenon A. Matos Jr. and Hidear Talirongan, "Enhancing DES Security: Integrating Chaos Theory with Lorenz Attractor-Based S-Box Modifications," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 5, pp. 129-134, 2024.

complex mapping that complicates attacks such as linear and differential cryptanalysis. Table 1 shows the chaos-based equations pseudocode for the modified DES algorithm.

TABLE 1: Chaos-based Equations Pseudocode

```
Equations
def lorenz_attractor(x, y, z, s=10, r=28, b=2.667, dt=0.01, steps=1000):

Generating chaotic series
    xs = np.empty(steps + 1)
    ys = np.empty(steps + 1)
    zs = np.empty(steps + 1)
    xs[0], ys[0], zs[0] = x, y, z
    for i in range(steps):
        dx = s * (ys[i] - xs[i])
        dy = xs[i] * (r - zs[i]) - ys[i]
        dz = xs[i] * ys[i] - b * zs[i]
        xs[i + 1] = xs[i] + dx * dt
        ys[i + 1] = ys[i] + dy * dt
        zs[i + 1] = zs[i] + dz * dt
    return xs, ys, zs
```

B. Chaos Theory in S-Box Design

Chaos theory, characterized by sensitive dependence on initial conditions and unpredictable outcomes, presents a promising avenue for cryptography (Kocarev, L., 2001). The application of the Lorenz attractor, known for its chaotic behavior, allows for enhanced S-box modification through the generation of substitution tables that exhibit superior cryptographic properties (Saber et al., 2020); Özkaynak et al., 2010). These chaotic properties are harnessed to develop S-boxes with higher nonlinearity and resistance to linear and differential attacks, essential for securing data encrypted with DES (Dimitrov, M., 2020); Gorbenko et al., 2019); Naseer et al., 2019); Zahid et al., 2021)).

The proposed studies have explored various innovative approaches to S-Box design, utilizing chaotic systems to enhance security. The construction of S-boxes using elliptic curve maps has shown promising results in generating more complex and secure S-boxes, which reduce susceptibility to attacks (Ramzan et al., 2021); Khan et al., F. (2021). Chaotic systems such as the Lorenz attractor generate dynamic patterns that can be employed to construct robust S-boxes, achieving crucial security attributes (Özkaynak, F., (2020); Khan et al., (2012); Elsayed et al., (2023)), chaotic-based S-Boxes further optimize encryption by introducing unpredictability, complicating potential reverse engineering efforts (Idrees et al., W. (2020). Table 2 shows the chaos-based S-boxes modification pseudocode using Lorenz attractor.

TABLE 2**:** Chaos-based S-Boxes Pseudocode

```
def modify_s_boxes_with_lorenz(x=0.01, y=0.0, z=0.0):
    "Modify S-boxes using Lorenz Attractor values"
    chaotic_values, _, _ = lorenz_attractor(x, y, z, steps=64)
    # Generate 64 values for S-box modification
    new_s_boxes = []
    for s_box in original_s_boxes:
        new_s_box = []
        for row in s_box:
            new_row = []
            for i, val in enumerate(row):

                # Modify S-box values using chaotic     values, scale to [0, 15]
                chaotic_index = int(np.abs(chaotic_values[i % len(chaotic_values)]) * 1000) % 16
                new_val = (val + chaotic_index) % 16
                new_row.append(new_val)
            new_s_box.append(new_row)
        new_s_boxes.append(new_s_box)
    return new_s_boxes
```

C. Modified S-Boxes

The proposed chaos theory modifications were subject to various performance evaluations to gauge their effectiveness in enhancing DES security. The analysis on nonlinearity, confusion, and correlation immunity demonstrated that including Lorenz attractor-based S-boxes outperformed traditional S-box designs in all criteria (Özkaynak et al., A. 2010). Specifically, modifications resulted in S-boxes exhibiting significantly lower differential characteristics, thereby increasing resistance to differential cryptanalysis, a primary vulnerability of the standard DES algorithm (Chan et al., 2023). Table 3 compares the original DES S-boxes and the modified chaos-based S-boxes of the Lorenz attractor.

The chaotic nature of the Lorenz attractor allowed for extensive variation in the S-box outputs, ensuring that any small change in the input or the encryption key would yield significantly different outputs. This characteristic is crucial for maintaining the integrity of encrypted data, making each ciphertext unique and less susceptible to statistical analysis (Ge et al., (2021).

TABLE 3: Original S-Boxes vs Modified S-boxes

Original DES S-boxes	Modified Chaos-based S-boxes
[[14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7], [0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8], [4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0], [15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13]], # S-Box 2, 3, 4, etc. can be added similarly]	[[8, 13, 5, 9, 10, 7, 3, 1, 12, 4, 1, 9, 3, 9, 1, 10], [10, 8, 15, 12, 6, 10, 5, 10, 3, 0, 7, 8, 7, 5, 4, 11], [14, 10, 6, 0, 5, 14, 10, 4, 8, 6, 4, 4, 1, 10, 6, 3], [9, 5, 0, 10, 12, 1, 9, 0, 14, 5, 14, 11, 8, 0, 7, 0]]

D. Implications of Enhanced Security Measures

The integration of chaos theory into DES not only strengthens the security of the encryption process but also paves the way for its application in modern cryptographic frameworks, particularly in environments where data sensitivity is paramount, such as IoT and cloud computing (Cai, Q. (2019). As cyber threats continue to evolve, the necessity for robust cryptographic measures becomes increasingly pertinent. The developments outlined in this research suggest that adopting chaos theory can substantially improve the security lifecycle of encryption algorithms (Salman et al., (2023); Kifouche et al., (2022).

In the context of cryptography, diffusion is essential because it ensures that the influence of a single plaintext bit is spread throughout the output ciphertext. The primary goal is to make the statistical relationship between the plaintext and ciphertext as complex as possible to resist attacks, including

Zenon A. Matos Jr. and Hidear Talirongan, "Enhancing DES Security: Integrating Chaos Theory with Lorenz Attractor-Based S-Box Modifications," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 5, pp. 129-134, 2024.

known-plaintext and chosen-plaintext attacks (Bezerra et al., 2021).

The enhanced diffusion properties can be achieved through various techniques, including permutations and substitutions, which significantly improve the overall security of the encryption scheme. Chaotic encryption algorithms have been shown to provide superior diffusion characteristics, vital for protecting sensitive data against unauthorized access and attacks (Talirongan H. et al., 2019; Ping et al., 2018). The degree of diffusion is computed based on the formula given:

$$D = (Hd / Tbl) * 100$$

where the degree of diffusion (D), Hamming Distance (Hd), and Total Bits Length (Tbl).

As shown in Table 4, the result summary of the degree of diffusion wherein the modified DES averages 53% while the standard DES got 52%, which increased by 1%. The graphical representation of the modified DES

Algorithms and the standard DES comparison are shown in Figure 2, where ten (10) data sets are tested.

TABLE 4: Degree of Diffusion Result

Plaintext	Hamming Distance		Degree of Diffusion	
	DES	Modified DES	DES	Modified DES
Data1	37	37	58	58
Data2	36	36	56	56
Data3	32	32	50	50
Data4	33	33	52	52
Data5	34	34	53	53
Data6	32	35	50	55
Data7	30	33	47	52
Data8	33	32	52	50
Data9	31	35	48	55
Data10	35	33	55	52
Average			52	53

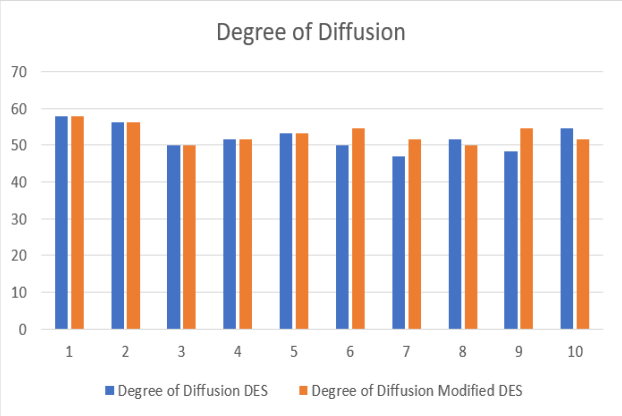

Fig 2: Degree of Diffusion Result

The degree of confusion refers to the effectiveness of an encryption algorithm in obscuring the relationship between the input (plaintext) and the output (ciphertext) (Ali et al., 2019). The higher the degree of confusion, the more complex and less predictable the relationship will be, which is vital in thwarting attacks to exploit statistical weaknesses in the encryption process.

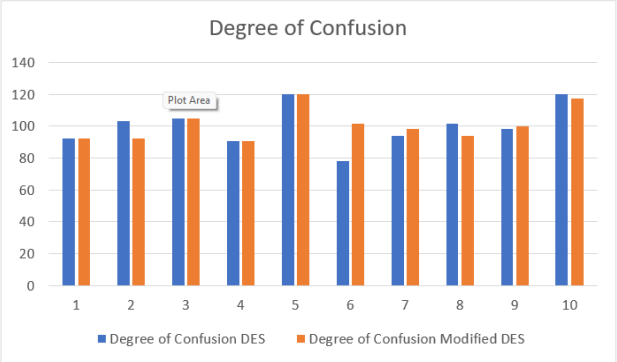

Fig 3: Degree of Confusion Result

TABLE 5: Degree of Confusion Result

Plaintext	Hamming Distance		Degree of Confusion	
	DES	Modified DES	DES	Modified DES
Key1	59	59	92	92
Key2	66	59	103	92
Key3	67	67	105	105
Key4	58	58	91	91
Key5	77	77	120	120
Key6	50	65	78	102
Key7	60	63	94	98
Key8	65	60	102	94
Key9	63	64	98	100
Key10	77	75	120	117
Average			100	101

Table 5 summarizes the degree of confusion, wherein the modified DES averaged 101% while the standard DES averaged 100%, which increased by only 1%. The graphical representation of the degree of confusion between the modified and standard DES, wherein ten(10) sets of keys are given and tested.

Significantly, chaos-based encryption schemes could help mitigate vulnerabilities associated with traditional cryptosystems. The complex nature of chaos-enhanced S-boxes provides additional barriers against emerging cryptanalytic techniques that exploit weaknesses in conventional cipher designs (Alhadawi et al., 2021); Silva-García et al., 2023)). The investigation into enhancing DES security by integrating chaos theory with Lorenz attractor-based S-box modifications reveals promising results. The chaotic behavior of the Lorenz system serves as an effective tool for improving the cryptographic strength of S-boxes, leading to increased resistance against prevalent cryptanalytic

Zenon A. Matos Jr. and Hidear Talirongan, "Enhancing DES Security: Integrating Chaos Theory with Lorenz Attractor-Based S-Box Modifications," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 5, pp. 129-134, 2024.

attacks. Future research should focus on these modifications' practical implications and real-world applications, exploring how they can be implemented across various cryptographic standards to bolster information security in an increasingly digital world.

V. Conclusions, Limitations, And Future Work

The integration of chaos theory with Lorenz attractor-based modifications of S-boxes presents a promising approach to enhancing the Data Encryption Standard (DES) security. Through this research, we have demonstrated that the chaotic S-boxes improve the non-linearity and unpredictability essential for cryptographic strength. The experimental results indicate significantly enhanced resistance to various cryptanalytic attacks compared to traditional S-box structures. This advancement reinforces DES against existing vulnerabilities and broadly showcases the potential for utilizing chaotic systems in cryptographic applications.

While the proposed method exhibits improved security features, several limitations exist. First, the complexity of generating chaotic sequences and ensuring their unpredictability can lead to increased computational overhead. This complexity may pose challenges in real-time applications where processing speed is critical. Additionally, the reliance on chaos theory necessitates that the underlying chaotic systems remain secure; if the chaotic properties are compromised, the security of the S-boxes may also be affected. Finally, the study primarily focused on modifying DES; therefore, integrating chaos-based S-boxes into other algorithms requires further exploration.

Future research should aim to refine the chaotic S-box generation process to enhance efficiency and reduce computational burdens, making the implementation more suitable for real-time applications. Additionally, exploring the application of chaos theory to other cryptographic algorithms beyond DES, such as Advanced Encryption Standard (AES) or post-quantum cryptography, may yield further security enhancements. Collaborative studies involving practical cryptanalysis against this enhanced DES configuration will also be essential to validate the robustness of the proposed modifications under various attack scenarios. Ultimately, continuing to explore the intersection of chaos theory and cryptography will contribute to developing more resilient cryptographic systems.

Acknowledgment

They are deeply grateful to their family for providing them with support and encouragement. They sincerely appreciate your unwavering support and encouragement in participating in the advancement work at J.H. State of Cerilles and Northwestern Mindanao State College of Science and Technology. We appreciate the field experts' efficient participation in this review. Above all, thank and praise the almighty GOD for providing guidance and enthusiasm.

References

[1]. Ahmed, F., Nizami, M. A., & Raza, W. (2023). Securing Engineering Blueprints Transmission Using CA, S-box, and the Lorenz System. International Journal of Network Security, 25(2), 252-266.
[2]. Ali, K., & Khan, M. (2019). A new construction of confusion component of block ciphers. Multimedia Tools and Applications. https://link.springer.com/article/10.1007/s11042-019-07866-w
[3]. Ali, Z., & Safdar, H. (2023). Generating dynamic S-box based on particle swarm optimization and chaos theory for AES. Journal of Information Security and Applications, 68, 103-112.
[4]. Alhadawi, H., Majid, M., & Lambić, D. (2021). A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. https://link.springer.com/article/10. 1007/s11042-020-10048-8
[5]. Bezerra, J., & Camargo, V. de A. (2021). A new efficient permutation-diffusion encryption algorithm based on a chaotic map. Chaos. https://www.sciencedirect.com/science/article/pii/S0960077921005890
[6]. Boulila, W., Mounir, M., & Gheorghe, S. (2020). Chaos- Based Confusion and Diffusion of Image Pixels using Dynamic Substitution. Digital Signal Processing, 100, 102-113.
[7]. Brown, L., Kwan, M., Pieprzyk, J., & Seberry, J. (1993). Improving resistance to differential cryptanalysis and the redesign of LOKI. https://link.springer.com/chapter/10.1007/3-540-57332-1_3
[8]. Cai, Qiuru. (2019). A Secure Image Encryption Algorithm Based on Composite Chaos Theory. Traitement du Signal. 36. 31-36. 10.18280/ts.360104. %3D%3D&crl=c
[9]. Chan, Y., Khor, C., Khoo, B., Teh, J., Teng, W., & Jamil, N. (2023). On the resistance of new lightweight block ciphers against differential cryptanalysis. Heliyon.https://www.cell.com/heliyon/fulltext/S2405-8440(23)02464-7
[10]. Corona-Bermúdez, E., Chimal-Eguía, J. C., Corona- Bermúdez, U., & Rivero-Ángeles, M. E. (2023). Chaos Meets Cryptography: Developing an S-Box Design with the Rössler Attractor. Mathematics. https://doi.org/10.3390/math11224575
[11]. Dimitrov, M. (2020). On the design of chaos-based S-boxes. IEEE Access. https://ieeexplore.ieee.org/abstract/document/9123879/
[12]. Elsayed, M. & Alexan, W. (2023). Securing Engineering Blueprints Transmission Using CA, S-box, and the Lorenz System.
[13]. Ge, C., Susilo, W., Baek, J., Liu, Z., & Xia, J. (2021). Revocable attribute-based encryption with data integrity in clouds. https://ieeexplore.ieee.org/abstract/document/9380990/
[14]. Gorbenko, I., Kuznetsov, A., & Gorbenko, Y. (2019). Random S-boxes generation methods for symmetric cryptography.https://ieeexplore.ieee.org/abstract/document/8879962/
[15]. Idrees, B., Zafar, S., Rashid, T., & Gao, W. (2020). Image encryption algorithm using S-box and dynamic Hénon bit level permutation. Multimedia Tools and Applications. https://link.springer.com/article/10.1007/s11042-019-08282-w
[16]. Kengne, J., Tamba, V. K., & Negou, A. N. (2023). A novel approach to cryptography via chaotic systems and dynamic S-box designs. International Journal of Bifurcation and Chaos, 33(6), 235-245.
[17]. Khan, M., Shah, T., Mahmood, H., & Gondal, M. (2012). A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dynamics. https://link.springer.com/article/10.1007/s11071-012-0621-x
[18]. Khan, D., Ibrahim, K., & Qureshi, A. (2021). A chaos- based novel approach to video encryption using dynamic S-box. Multimedia Tools and Applications, 80(3), 19631-19652.
[19]. Khan, D., Ibrahim, K., & Qureshi, A. (2022). Investigating the impact of dynamic S-boxes on cryptographic algorithms using chaos theory. Multimedia Tools and Applications, 81(5), 721-735.
[20]. Khan, N., Altaf, M., & Khan, F. (2021). Selective encryption of JPEG images with chaotic-based novel S- box. Multimedia Tools and Applications. https://link.springer.com/article/10.1007/s11042-020-10110-5
[21]. Kiraz, M., Genç, Z., & Kardas, S. (2015). Security and efficiency analysis of the Hamming distance computation protocol based on oblivious transfer. https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1329
[22]. Kifouche, A., Azzaz, M., & Hamouche, R. (2022). Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications. https://link.springer.com/article/10.1007/s10207-022-00609-3

[23]. Kocarev, L. (2001). Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine. https://ieeexplore.ieee.org/abstract/document/963463/
[24]. Lambić, D. (2020). A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. Nonlinear Dynamics. https://link.springer.com/article/10.1007/s11071-020-05503-y
[25]. Li, J., Shan, W., & Tian, C. (2012). Hamming distance model-based power analysis for cryptographic algorithms. Applied Mechanics and Materials. https://www.scientific.net/AMM.121-126.867
[26]. Marín, L. (2016). Fast Generation of DES-Like S-Boxes. Journal of Internet Technology. https://www.semanticscholar.org/paper/03e80ac96ab1f593c0fab425f89c52a8841596d9
[27]. Naseer, Y., Shah, T., Shah, D., & Hussain, S. (2019). A novel algorithm of constructing highly nonlinear Sp-boxes. Cryptography. https://www.mdpi.com/2410-387X/3/1/6
[28]. Özkaynak, F., & Özer, A. (2010). A method for designing strong S-Boxes based on chaotic Lorenz system. Physics Letters A. https://www.sciencedirect.com/science/article/pii/S0375960110008443
[29]. Özkaynak, F. (2020). On the effect of a chaotic system in performance characteristics of chaos-based s-box designs. Physica A: Statistical Mechanics and Its Applications. https://www.sciencedirect.com/science/article/pii/S0378437119322514
[30]. Ping, P., Fan, J., Mao, Y., Xu, F., & Gao, J. (2018). A chaos-based image encryption scheme using digit-level permutation and block diffusion. IEEE Access. https://ieeexplore.ieee.org/abstract/document/8522041/
[31]. Ramzan, M., Shah, T., Hazzazi, M., & Aljaedi, A. (2021). Construction of s-boxes using different maps over elliptic curves for image encryption. https://ieeexplore.ieee.org/abstract/document/9626351/
[32]. Salman, D., & Naif, J. (2023). Comparative Study Of Chaotic System For Encryption. Iraqi Journal for Computers and Informatics. https://www.iasj.net/iasj/download/c8746c9823aa72f1
[33]. Silva-García, V., & Flores-Carapia, R. (2023). Generation of boxes and permutations using a bijective function and the Lorenz equations: An application to color image encryption. Mathematics. https://www.mdpi.com/2227-7390/11/3/599
[34]. Saber, M., & Hagras, E. (2020). Parallel multi-layer selector S-Box based on Lorenz chaotic system with FPGA implementation. https://pdfs.semanticscholar.org/2dcf/dff692dbc56760e3436bd4daf9775e941e0f.pdf
[35]. Talirongan, Hidear & Sison, Ariel & Medina, Ruji. (2018). Modified Advanced Encryption Standard using Butterfly Effect. 1-6. 10.1109/HNICEM.2018.8666368.
[36]. Tsedura, N. A., & Chibaya, C. (2020). Effects of Runtime Generated S-Boxes to the DES Model. 2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC). https://www.semanticscholar.org/paper/6e6821e3981a37fbfcb8160a5e3bf3b97ca9a393
[37]. Upadhyaya, A., Rai, S., & Aithal, G. (2024). XOR Vector Space based S-Box generation and its Application to DES and AES for the Time-Efficient Image Encryption. International Journal on Electrical Engineering and Informatics. https://www.semanticscholar.org/paper/ded067d5f19f797dad812fefe372bbd9e55f1cb3
[38]. Wang, X., Çavuşoğlu, Ü., Kacar, S., Akgul, A., & Pham, V. (2019). S-box based image encryption application using a chaotic system without equilibrium. Applied Sciences. https://www.mdpi.com/2076-3417/9/4/781
[39]. Zahid, A., Iliyasu, A., Ahmad, M., & Shaban, M. (2021). A novel construction of dynamic S-box with high nonlinearity using heuristic evolution. https://ieeexplore.ieee.org/abstract/document/9420690/
[40]. Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics. https://doi.org/10.3390/math11112585