Machine Learning for Human Intelligence
2023, Vol. 1, Issue 2

Research Article

Development of a Substitution Box through an Innovative Chaotic Map and Permutation Technique

Zubair Akbar[1], Nimra Tariq[2], and Owais Manzoor[3,⋆]

[1,2,3]Department of Computer Science, TIMES Institute Multan, 59030, Multan, Punjab, Pakistan.; Email: zubair@t.edu.pk,nimra@t.edu.pk, owais@t.edu.pk
⋆Corresponding author: Owais Manzoor (owais@t.edu.pk)

Article History

Academic Editor:
Dr. Muhammad Nabeel Asghar
Submitted: January 29, 2023
Revised: June 12, 2023
Accepted: September 1, 2023

Keywords:
Substitution-box, chaotic map, block cipher, chaotic mapping, cryptanalytic

Abstract

Data security represents a fundamental aspect in protecting information assets. Organizations require robust mechanisms to safeguard their data, which constitutes their most valuable resource. Consequently, establishing data protection stands as the primary concern for organizational operations. Cryptographic methodologies serve as essential tools for ensuring data security. In this context, chaos theory demonstrates significant importance in cryptographic applications. This research presents an innovative approach for creating a dynamic S-Box utilizing chaotic mapping techniques. The chaos generation employs a chaotic map incorporating linear equations combined with exponential functions based on specific conditions, introducing chaotic elements into plain-text to reduce vulnerability to cryptanalytic attacks. To enhance chaotic map robustness, several properties must be satisfied, including elevated non- linearity, SAC values approaching 0.5, and compliance with Linear probability, Differential uniformity, and BIC value requirements that satisfy the Bit Independence Criterion. The chaotic map produces a novel S- box that introduces uncertainty into data. Strong and robust cipher construction heavily relies on the substitution mechanism. Furthermore, the values obtained from our S-Box demonstrated superior performance compared to numerous existing S-Box designs.

1 Introduction

Cryptography represents a methodology for securing data and communication against adversarial threats [1]. This technique enables senders to transmit messages to intended recipients without concerns regarding data compromise. Cryptography concentrates on preventing unauthorized data access while ensuring only intended recipients can access content. The encryption mechanism provides information and data protection within cryptographic systems. Mathematical concepts and algorithms form the foundation of cryptographic techniques. Cryptographic methods divide into symmetric and asymmetric key cryptography. Symmetric key cryptography further branches into modern and classical approaches. Classical cryptography subdivides into substitution and transposition ciphers, while modern cryptography

separates into block and stream ciphers [2]. Block ciphers encrypt data blocks into cipher-text simultaneously, with block sizes of 64, 128, or 256 bits. Confusion and diffusion principles guide block cipher plain-text encryption [3]. Stream ciphers transform plain-text bit-by-bit or byte-by-byte into cipher-text, processing up to 8 plain-text bits equivalent to one byte. Stream ciphers employ

confusion principles for plain-text-to-cipher-text transformation. Symmetric key ciphers represent the oldest and most recognized encryption-decryption technique [4]. These systems utilize a single secret key for both encryption and decryption processes. While symmetric ciphers excel in processing speed, they present key management challenges. Notable symmetric cipher examples include DES and AES. DES constitutes a block cipher algorithm announced by NIST [5]. This algorithm processes 64-bit plain-text input and produces 64-bit cipher-text output. As a symmetric key family member, identical keys are required for encryption and decryption operations. The DES algorithm employs a 56-bit key size, removing every 8th bit from the original 64-bit key before algorithm execution. DES utilizes two fundamental cryptographic approaches: confusion and diffusion. AES represents a widely adopted symmetric key block cipher encryption algorithm [6]. This algorithm replaced DES due to DES vulnerability against powerful computational attacks. AES follows an iterative algorithm structure, implementing substitution and permutation processes through linked operations. AES processes bytes instead of bits, treating 128-bit plain-text as sixteen bytes arranged in a 4×4 matrix (four rows and four columns). Round numbers vary according to key length: AES 128-bit uses ten rounds, AES 192-bit employs twelve rounds, and AES 256-bit utilizes fourteen rounds. Asymmetric key ciphers employ two distinct keys. Public keys facilitate encryption processes, while private keys enable cipher-text decryption. Private key holders can decrypt messages, and paired keys enhance security. Private keys remain secret for message decryption, while public keys can be freely distributed for message transmission. Key relationships ensure that public key encryption requires private key decryption, while private key encryption necessitates public key decryption. The DSA algorithm, proposed by NIST in 1991 and adopted by FIPS (Federal Information Processing Standard), relies on modular exponentiation and discrete logarithm concepts. This public key cryptography foundation primarily supports digital signatures and verification.

Substitution boxes constitute essential components of symmetric key algorithms [7] -[13]. In cryptographic applications, substitution boxes (S-boxes) perform substitution functions by converting plain-text into cipher-text. AES employs 8-bit substitution boxes, while Serpent utilizes 4-bit versions. S-boxes represent the sole non-linear components concealing relationships among keys, plain-text, and cipher-text. These components generate confusion between cipher-text and keys, making information resistant to various attack types. Typically, substitution boxes consist of 16×16 tables containing 256 randomly placed data bytes. In block cipher contexts, substitution boxes obscure connections between plain-text and cipher-text. Researchers have explored various techniques and concepts for generating strong and robust substitution boxes. These investigations assess robustness using quality attributes including non-linearity, bit independence criterion, strict avalanche criterion, differential probability, and linear probability. Consequently, S-boxes must resist diverse attack types. When S-boxes possess these attributes, they provide enhanced block cipher strength. Particularly, non-linearity serves as a significant measure for evaluating S-box strength. Higher non-linearity values indicate greater resistance to various cryptanalytic methods.

Chaotic maps represent evolution maps displaying chaotic behavior [14, 15, 16]. Chaotic cryptology applies mathematical chaos theory to cryptographic applications. Cryptography efficiently utilizes chaos theory by implementing chaotic maps for entropy generation required for confusion and diffusion production. Chaotic systems possess unique characteristics enabling cryptographic applications. When chaotic parameters and cryptographic keys map symmetrically or produce functional outputs, attackers cannot predict output values without initial value knowledge. Chaos theory application in cryptography has attracted considerable interest [17, 18].

2 Related Work

Belazi et al [19] proposed an image encryption scheme based on chaos following permutation and substitution structures. The suggested technique exhibited limitations including elevated differential uniformity values. Belkhouja et al [20] developed a chaotic system for pseudo-random key formation. Identical cryptographic keys generated for both endpoints showed disappointing NIST test results. Özkaynak [21] investigated a novel hybrid random number generator scheme utilizing chaotic maps as

entropy sources. The proposed method demonstrated good performance characteristics during analysis. Authors employed existing chaotic maps with limited innovation. Acikkapi et al [22] conducted side channel analysis on two chaos-based substitution boxes and compared results with the Advanced Encryption Standard algorithm. Analysis revealed chaos-based substitution boxes showed greater resistance to side channel attacks. However, SAC and NL results were inferior to AES S-Box performance. Zaibi et al [23] introduced a new dynamic chaotic substitution box for wireless sensor network applications. The proposed scheme featured two categories: substitution boxes based on discrete chaotic maps with floating point arithmetic and those using fixed point arithmetic. Farah et al [24] suggested chaotic substitution boxes based on Ikeda maps and input value permutation. Two chaotic sequences were implemented: one for input values and another for substitution processes.

Alzaidi et al [25] presented an innovative technique generating strong substitution boxes using optimized sine-cosine algorithms. The sine-cosine algorithm combined with enhanced chaotic maps explored search spaces for optimized substitution box generation. C. Wang et al [26] proposed quadratic polynomial chaotic maps controlling new chaotic map amplitudes. The proposed scheme lacked hidden chaotic attractors in fixed point analysis for existence and stability. Ahmad et al [27] developed an algorithm constructing substitution boxes using artificial bee colony optimization and chaotic maps. The generated algorithm demonstrated excellent security strength results suitable for strong block cryptosystem construction. [28]-[33] developed chaotic substitution boxes based on block encryption algorithms utilizing baker maps, sinusoidal chaotic maps, compound chaotic maps, and linear congruence generators.

Solami et al [34] suggested bijective substitution boxes with strong cryptographic properties dependent on complex dynamics of new hyper-chaotic systems. Tanya Abdul-Sattar Jabor et al [35] proposed AES modification algorithms performing real-time encryption and decryption using identical unmodified algorithms with key generation system changes. Chebyshev polynomials generated keys with required sizes. Furthermore, substitution boxes created through meta-heuristic optimization algorithms were proposed. Non-linearity enhancement utilized chaotic maps combined with cuckoo algorithms, providing superior protection against linear attacks. Hao [36] analyzed substitution box performance enhancement using chaotic systems. Improved logistic maps obtained through fractional order differential equations created substitution boxes with enhanced performances. Singh et al [37]-[41] proposed methods using dynamic substitution boxes overcoming security drawbacks. New schemes employed dynamic irreducible polynomials and affine constants, improving security levels.

Sahmoud S. et al [41] proposed new and powerful cryptographic algorithms generating different sub- keys from original keys using AES schemes, with AES blocks encrypted using these sub-keys. Tiwari et al [42] proposed AES algorithm modifications using two secure substitution boxes mapping plaintext into ciphertext. Avalanche effects increased through dual secure substitution box implementation. Average NL values were lower than many currently proposed S-box techniques. Manjula et al [43] presented approaches constructing dynamic substitution boxes intensifying construction complexity, protecting information against various attack types. These new dynamic substitution boxes were key-dependent, increasing complexity and cryptanalytic difficulty. Static and dynamic S-Boxes represent two recognized substitution types [44]. Static substitution boxes maintain fixed value patterns independent of keys, preventing value changes due to fixed nature. Dynamic substitution boxes feature non-fixed patterns allowing value modifications. Key-dependent values change accordingly with key variations. Comparing static and dynamic substitution boxes reveals dynamic superiority, as static boxes maintain predictable fixed patterns while dynamic boxes lack fixed patterns, increasing prediction difficulty. Primary paper contributions include:

- Exploring innovative approaches constructing refined substitution boxes with numerous robust and dynamic substitution boxes obtainable through minimal transformation parameter changes.
- Applying innovative and dynamic permutation processes to S-Box values for enhanced confusion.
- Comparing developed S-boxes with current performance standards, certifying outstanding results.
- Enhancing security and optimizing substitution box robustness.

3 Materials and Methods

Substitution boxes represent crucial symmetric key algorithm components performing substitution processes. S-Boxes conceal relationships among keys, plaintext, and ciphertext. When identical substitution boxes are used across multiple algorithm rounds, they constitute static substitution boxes due to round constancy. Conversely, different substitution boxes used across multiple rounds represent dynamic substitution boxes. Primary S-Box properties include confusion characteristics making eavesdropper attacks difficult. New S-Box creation methods emerge, strengthening attack resistance. S-Box properties define strengths and weaknesses. Chaotic maps enable new substitution box proposals. Chaotic maps represent evolution maps displaying chaotic behavior. Chaotic cryptology applies mathematical chaos theory to cryptographic applications. Cryptography efficiently utilizes chaos theory through chaotic map implementation generating entropy required for confusion and diffusion production. Chaotic systems possess unique characteristics enabling cryptographic applications. When chaotic parameters and cryptographic keys map symmetrically or produce functional outputs, eavesdroppers cannot predict output values without initial value knowledge. Chaos theory application in cryptography attracts significant interest. Dynamic S-box construction involves two sequential steps:

1. An innovative chaotic map
2. Permutation process

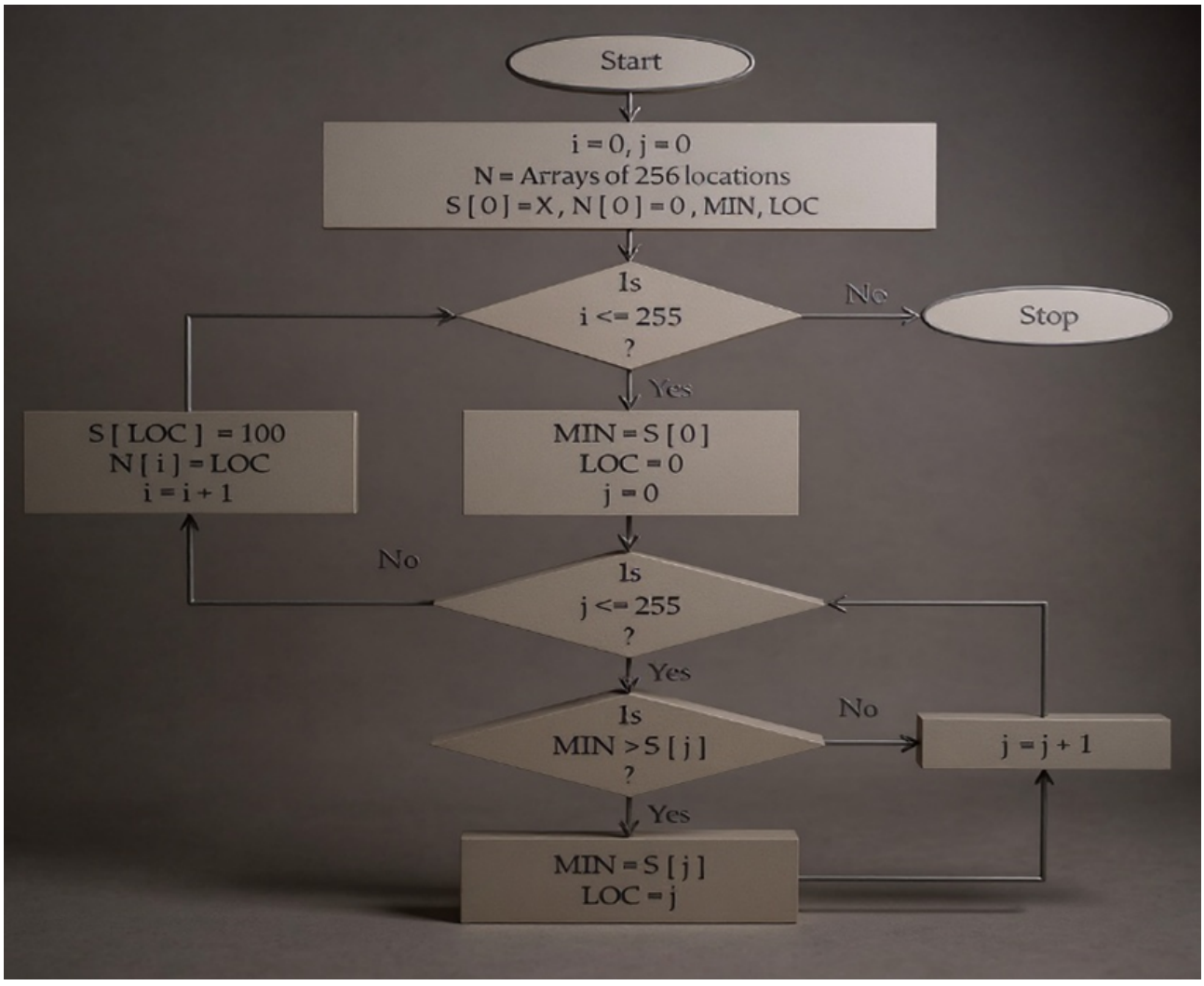

Figure 1: Working of S-Box.

3.1 Enhanced Chaotic Map Implementation

The innovative transformation practiced in S-box generation expresses mathematically as in Equation 1:

$$X_{n+1} = X_n - 1/2, if X_n > 1/2 X_n + X_n^Y, if X_n \leq 1/2 \quad (1)$$

Figure 1 illustrates substitution box functionality. Two arrays X and Y are utilized in our chaotic map formula. These variable values must range between 0 and 1, derived from keys. Two arrays with 256 possibilities were selected. S arrays store S-Box values while N arrays store indexes. Loop iterations run 255 times from 1 to 255. X values are evaluated and treated according to specified conditions. Subsequently, X results store in S with locations stored in N. Loops terminate after 256 possibilities. S-box value sorting procedures follow, with N values in sequence. S values require sorting for sequential arrangement while N values randomize.

3.2 Permutation Methodology

Value repositioning with alternative values defines permutation. Permutation also represents ordered set linear order changes. Figure 2 illustrates X and Y variables where X is dependent and Y remains independent. Y values remain static while X values change according to specified conditions. Conditions specify that X values greater than 0.5 proceed left, otherwise proceeding right. X denotes location.

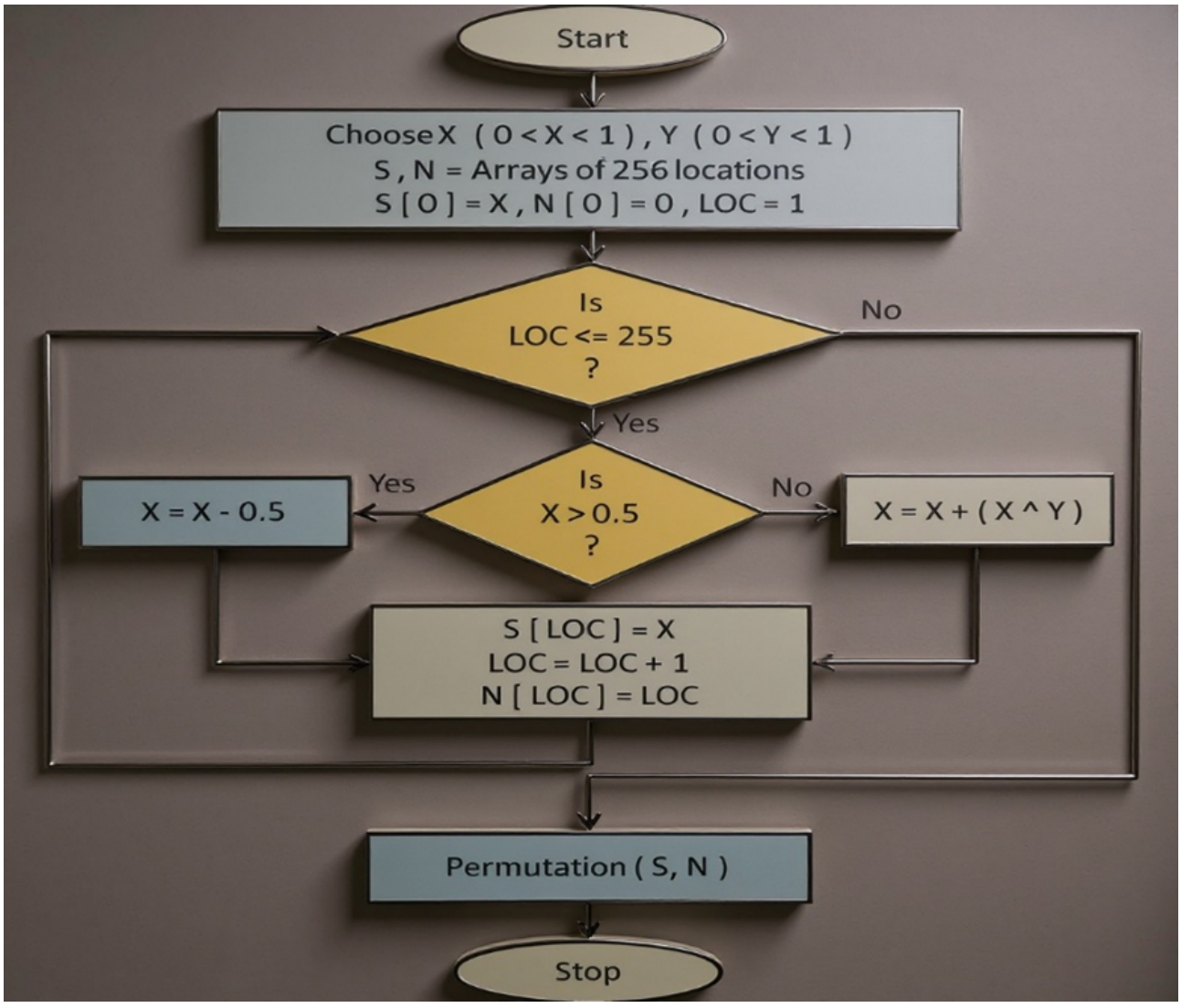

Figure 2: Permutation Process.

3.3 Security Evaluation of Suggested S-Box

This section conducts inspections assessing generated S-Box strength against standards quantifying proposed S-Box cryptographic feature compliance. These attributes must be satisfied by S-Boxes possessing powerful cryptographic characteristics:

1. Bijectiveness
2. Elevated non-linearity values
3. No fixed points
4. Strict avalanche criterion
5. Output bit independence criterion
6. Low differential uniformity
7. Low linear approximation probability

3.4 Non-Linearity Assessment

S-Boxes deliver mappings between output and input bits. Generally, non-linearity indicates absent relationships between output and input bits. Input and output bits must maintain random and non-sequential relationships. Linear mapping between output and input bits demonstrates reduced S-Box cryptographic strength. Non-linear output and input bit transformations indicate strong S-Boxes providing plain-text protection against linear cryptanalytic attacks as given in Table 1. Our Substitution

Table 1: Performance Metrics for Suggested S-Box Non-Linearity Values

Boolean Function	**BF1**	**BF2**	**BF3**	**BF4**	**BF5**	**BF6**	**BF7**	**BF8**
NL Value	108	104	108	106	106	104	108	108

Box non-linearity values are 108, 104, 108, 106, 106, 104, 108, and 108. Maximum NL value equals 108, minimum NL value equals 104, and average NL value equals 106.5 as give in Table 2.

Table 2: Comparison of Non-Linearity Performance Between Suggested S-box and Recent S-boxes

S-Box	**Min-NL**	**Max-NL**	**Average NL**
Suggested	104	108	106.5
[27]	102	108	105.2
[28]	102	108	104.5
[29]	106	108	107
[30]	110	112	111.75
[31]	108	110	109.25
[32]	108	110	107.5

3.5 Bit Independence Analysis (BIC)

BIC indicates that input bit I alterations or inversions must produce independent changes in output bits J and k. Two Bit Independence Criterion types exist: BIC-NL and BIC-SAC. Our research demonstrates average BIC-SAC values of 0.500 and average BIC-NL values of 103.5. Strict Avalanche Analysis (SAC) Webster et al. established this criterion as vital characteristics for strong S-Boxes. This criterion confirms that single input bit flips must change fifty percent of output bits correspondingly. Generally, 0.5 SAC values are considered acceptable. Our Novel S-Box demonstrates maximum SAC values of 0.5938, minimum SAC values of 0.4219, and average SAC values of 0.498.

3.6 Linear Probability Analysis (LP)

LP represents another crucial factor determining substitution box strength. Substitution boxes designed with low Linear Probability assist in various cryptanalysis methods. LP values inversely correlate with S-Box strength, meaning lower linear probability values indicate more robust substitution boxes. Our Novel S- box Linear Probability value equals 0.133. Linear Probability comparisons were made by comparing our proposed substitution box with existing substitution boxes. Furthermore, graphical representations show projected S-Box LP average values of 0.133, demonstrating comparative advantages over other present S-Boxes.

3.7 Differential Uniformity Analysis (DU)

Differential cryptanalysis provides useful tools for determining input differentials from output differentials. This method attempts collecting input data changes and output data variations. Combining both types enables attackers to deduce plaintext data or cipher keys entirely or partially. Efforts minimize differences between these numbers. Differential uniformity measurements commonly assess S-box differential uniformity. Lower differential uniformity (DU) scores provide preferable resistance against differential cryptanalytic attempts.

4 Conclusion

This research suggests simple and efficient methods generating cryptographically strong S-Boxes using novel transformation and permutation process schemes. The suggested S-Box nature is dynamic, providing greater robustness against cryptanalytic attacks. Critical evaluations assessed S-Box strength through properties including Non-Linearity, Strict Avalanche Criteria, Linear Probability, Differential Probability, and Bits Independence Criterion. Non-Linearity ensures absent connections between input and output bits. The suggested S-Box demonstrates average Non-Linearity values of 106.5. High nonlinearity values indicate fewer patterns, increasing cryptanalytic difficulty. SAC values ensure single input bit flips change half of output bits correspondingly. The suggested S-Box achieves SAC values of 0.498. Bit Independence Criterion values for the suggested S-Box include BIC-NL of 103.5 and BIC-SAC of 0.500. The suggested S-Box demonstrates LP values of 0.133. Differential probability evaluates overall input and output bit changes. The suggested S-box differential probability value equals 0.1015. Impressive suggested S-Box results compare favorably with existing S-Boxes. The novel suggested S-Box demonstrates preferable results.

Supplementary Materials

All relevant data is within the manuscript and its supporting information files.

Funding

This research received no external funding.

Data Availability Statement

Data sharing does not apply to this article as no new data were created or analyzed in this study.

Acknowledgments

We acknowledge that we did not receive any support or funding.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Gaire, R., & Nepal, S. (2019). Smart cities cybersecurity and privacy.

[2] Ellis, S. R. (2013). Computer and information security handbook (3rd ed.).

[3] Knudsen, L. R. (2011). Block ciphers. In H. C. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of cryptography and security*. Springer.

[4] Peterson, L. L., & Davie, B. S. (2012). *Computer networks* (5th ed.).

[5] Wright, R. N. (2003). Encyclopedia of physical science and technology (3rd ed.).

[6] Heron, S. (2009). Advanced Encryption Standard (AES). *Network Security*, *2009*(12), 8-12.

[7] Zahid, A. H., Al-Solami, E., & Ahmad, M. (2020). A novel modular approach based substitution-box design for image encryption. *IEEE Access*, *8*, 150326-150340. https://doi.org/10.1109/ACCESS.2020.3016401

[8] Naeem, A., Farooq, M. S., Khelifi, A., & Abid, A. (2020). Malignant melanoma classification using deep learning: datasets, performance measurements, challenges and opportunities. *IEEE Access*, *8*, 110575-110597.

[9] Obaid, I., Farooq, M. S., & Abid, A. (2020). Gamification for recruitment and job training: model, taxonomy, and challenges. *IEEE Access*, *8*, 65164-65178.

[10] Aziz, O., Farooq, M. S., Abid, A., Saher, R., & Aslam, N. (2020). Research trends in enterprise service bus (ESB) applications: A systematic mapping study. *IEEE Access*, *8*, 31180-31197.

[11] Arooj, A., Farooq, M. S., Umer, T., & Shan, R. U. (2019). Cognitive internet of vehicles and disaster management: a proposed architecture and future direction. *Transactions on Emerging Telecommunications Technologies*, e3625.

[12] Mehmood, E., Abid, A., Farooq, M. S., & Nawaz, N. A. (2020). Curriculum, teaching and learning, and assessments for introductory programming course. *IEEE Access*, *8*, 125961-125981.

[13] Zhang, X., & Cao, Y. (2014). A novel chaotic map and an improved chaos-based image encryption scheme. *The Scientific World Journal*, *2014*, 1-8.

[14] Belazi, A., Rhouma, R., & Belghith, S. (2015). A novel approach to construct S-box based on Rossler system. In *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 611-615). IEEE. https://doi.org/10.1109/IWCMC.2015.7289153

[15] Arooj, A., Farooq, M. S., Akram, A., Iqbal, R., Sharma, A., & Dhiman, G. (2021). Big data processing and analysis in internet of vehicles: architecture, taxonomy, and open research challenges. *Archives of Computational Methods in Engineering*, 1-37.

[16] Tehseen, R., Farooq, M. S., & Abid, A. (2020). Earthquake prediction using expert systems: a systematic mapping study. *Sustainability*, *12*(6), 2420.

[17] Attique, M., Farooq, M. S., Khelifi, A., & Abid, A. (2020). Prediction of therapeutic peptides using machine learning: computational models, datasets, and feature encodings. *IEEE Access*, *8*, 148570-148594.

[18] Farooq, M. S., Tahseen, R., & Omer, U. (2021). Ethical guidelines for AI: A systematic literature review.

[19] Abid, A., Ali, W., Farooq, M. S., Farooq, U., Khan, N. S., & Abid, K. (2020). Semi-automatic classification and duplicate detection from human loss news corpus. *IEEE Access*, *8*, 97737-97747.

[20] Belkhouja, T., Du, X., Mohamed, A., Al-Ali, A. K., & Guizani, M. (2018). Symmetric encryption relying on chaotic henon system for secure hardware-friendly wireless communication of implantable medical systems. *Journal of Sensor and Actuator Networks*, *7*(2).

[21] Özkaynak, F. (2014). Cryptographically secure random number generator with chaotic additional input. *Nonlinear Dynamics*, *78*(3), 2015-2020.

[22] Acikkapi, M. S., Ozkaynak, F., & Ozer, A. B. (2019). Side-channel analysis of chaos-based substitution box structures. *IEEE Access*, *7*, 79030-79043.

[23] Zaibi, G., Peyrard, F., Kachouri, A., Fournier-Prunaret, D., & Samet, M. (2014). Efficient and secure chaotic S-Box for wireless sensor network. *Security and Communication Networks*, *7*(2), 279-292. https://doi.org/10.1002/sec.728

[24] Farah, T., Rhouma, R., & Belghith, S. (2017). A novel method for designing S-box based on chaotic map and Teaching-Learning-Based Optimization. *Nonlinear Dynamics*, *88*(2), 1059-1074. https://doi.org/10.1007/s11071-016-3295-y

[25] Alzaidi, A. A., Ahmad, M., Ahmed, H. S., & Solami, E. A. (2018). Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map. *Complexity*, *2018*.

[26] Wang, C., & Ding, Q. (2019). A class of quadratic polynomial chaotic maps and their fixed points analysis. *Entropy*, *21*(7).

[27] Ahmad, M., Doja, M. N., & Beg, M. M. S. (2018). ABC optimization based construction of strong substitution-boxes. *Wireless Personal Communications*, *101*(3), 1715-1729. https://doi.org/10.1007/s11277-018-5787-1

[28] Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., & Liu, J. (2019). A novel block encryption algorithm based on chaotic S-Box for wireless sensor network. *IEEE Access*, *7*, 53079-53090. https://doi.org/10.1109/ACCESS.2019.2911395

[29] Khelifi, A., Aziz, O., Farooq, M. S., Abid, A., & Bukhari, F. (2021). Social and economic contribution of 5G and blockchain with green computing: Taxonomy, challenges, and opportunities. *IEEE Access*, *9*, 69082-69099.

[30] Vistro, D. M., Farooq, M. S., Rehman, A. U., & Malik, S. (2021, September). Smart application based blockchain consensus protocols: A systematic mapping study. In *3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)* (pp. 573-581). Atlantis Press.

[31] Farooq, M. S., & Akram, S. (2021). IoT in agriculture: challenges and opportunities. *Journal of Agricultural Research*, *59*(1), 63-87.

[32] Haafza, L. A., Awan, M. J., Abid, A., Yasin, A., Nobanee, H., & Farooq, M. S. (2021). Big data COVID-19 systematic literature review: pandemic crisis. *Electronics*, *10*(24), 3125.

[33] Rashid, A., Farooq, M. S., Abid, A., Umer, T., Bashir, A. K., & Zikria, Y. B. (2021). Social media intention mining for sustainable information systems: categories, taxonomy, datasets and challenges. *Complex & Intelligent Systems*, 1-27.

[34] Al Solami, E., Ahmad, M., Volos, C., Doja, M., & Beg, M. (2018). A new hyper-chaotic system-based design for efficient bijective substitution-boxes. *Entropy*, *20*(7), 525. https://doi.org/10.3390/e20070525

[35] Jabor, T., Tarish, H., & Raheema, A. (2018). AES with chaotic using Chebyshev polynomial. *Iraqi Journal for Computers and Informatics*, *44*, 35-40. https://doi.org/10.25195/ijci.v44i2.55

[36] Hao, J. L. (2019). A novel method for designing S-boxes based on an improved logistic map. In *2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)* (pp. 327-329). IEEE. https://doi.org/10.1109/ICITBS.2019.00086

[37] Singh, A., Agarwal, P., & Chand, M. (2017). Analysis of development of dynamic S-box generation. *Computer Science and Information Technology*, *5*, 154-163. https://doi.org/10.13189/csit.2017.050502

[38] Farooq, M. S., Arooj, A., Alroobaea, R., Baqasah, A. M., Jabarulla, M. Y., Singh, D., & Sardar, R. (2022). Untangling computer-aided diagnostic system for screening diabetic retinopathy based on deep learning techniques. *Sensors*, *22*(5), 1803.

[39] Anjum, M. J., & Farooq, M. S. (2022). SDN based V2X networks for disaster management: A systematic literature review.

[40] Shaheen, M., Farooq, M. S., Umer, T., & Kim, B. S. (2022). Applications of federated learning; taxonomy, challenges, and research trends. *Electronics*, *11*(4), 670.

[41] Sahmoud, S., Elmasry, W., & A. S. (2013). Enhancement the security of AES against modern attacks by using variable key block cipher. *International Arab Journal of E-Technology*.

[42] Tiwari, N., & Kumar, A. (2019). Security effect on AES in terms of avalanche effect by using alternate S-Box. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 26, pp. 1-14). Springer.

[43] Manjula, G., & Mohan, H. S. (2017). Constructing key dependent dynamic S-Box for AES block cipher system. In *Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology* (pp. 613-617). IEEE.

[44] Cassal-Quiroga, B. B., & Campos-Cantón, E. (2020). Generation of dynamical S-boxes for block ciphers via extended logistic map. *Mathematical Problems in Engineering*, *2020*, 1-12. https://doi.org/10.1155/2020/2702653