ADBA Chaos and Fractals
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8951
RESEARCH ARTICLE
Vol.2 / No.2 / 2025 / pp.43-49
https://doi.org/10.69882/adba.chf.2025073

Synergistic Construction of High-Performance S-Boxes Based on Chaotic Systems: A Paradigm Shift in Cryptographic Security Design

Zaid Abdulsattar Abdulrazaq [*,1], **Harith Ghanim Ayoub** [α,2] and **Hakam Zaidan** [*,3]
[*]Technical Engineering College for Computer and AI / Mosul, Northern Technical University (NTU), Nineveh, Iraq, [α]Technical Management Institute, Northern Technical University (NTU), Nineveh, Iraq.

ABSTRACT Exchange of information between two nodes is a big issue in intenet these days. Multiple cryptosystems employed for this porpose with various mathmatical approaches. Most of these approaches uitilize subsitutions and pemutations. The subsituation S-box is a look up table that exchange x bits input with y bits output is incharge of substitution approach. The build of S-box with stong cryptographic power is important in recent cryptosystems. In this paper a novel approach for building roboust and dynamic S-box with compound multi-dimentional chaotic systems. Lorenze and henon maps employed for construction of strong S-Box with multiple security performance metrics :non-linearity(NL), Strict Avalanche Criterion (SAC), Bit-Independence Criterion (BIC), Linear-Probability (LP) and differential-Probability (LP).The results showed that proposed S_box is will be powerfull for modern cryptosystems.

KEYWORDS
Cryptography
S-box
Security
Chaotic map
Nonlinearity

INTRODUCTION

Recently, secure data communication and encryption have attracted great concern due to the rapid growth in wireless communication technology and its applications (Asghar *et al.* 2022; Al-Turjman and Zahmatkesh 2022; Sirohi *et al.* 2023; Rahman *et al.* 2023; Khoshafa *et al.* 2024). In fact, the substitutive permutation operation is one of the basic criteria in the Advanced Encryption Standard and other symmetric-key cryptosystems, namely block and stream ciphers, to resist different attacks (Ali *et al.* 2022a; Farooq *et al.* 2022; Knežević 2023). Earlier, many S-box constructions have been done using various techniques such as algebraic, cryptographic, mapping, heuristic, non-linear, chaos, and machine learning among others. It is known that designing high-performance S-boxes is a complex, challenging, and NP-hard problem (Xun *et al.* 2024; Ekwueme *et al.* 2024; Picek and Jakobovic 2022; Bavdekar *et al.* 2022). Notably, a good S-box should satisfy various cryptographic properties to enhance security without any computational overhead. Such security properties are non-linearity, differential uniformity, bit independence criterion, branch number, strict avalanche criterion, and linear approximation probability among others (Waheed *et al.* 2023; Alqahtani *et al.* 2023; Ali *et al.* 2024; Mahboob *et al.* 2023).

It is worth mentioning here that the notion of chaos is completely different from that of noise. Chaos has irregular, unpredictable deterministic dynamics, which exhibit rich and intricate patterns, while the time evolution of a chaotic system depends on its initial conditions with a positive Lyapunov exponent (Progonatı 2023; Zelinka and Senkerik 2023; Frank 2024). Due to such properties, chaos has become an evolving concept in many scientific and engineering applications. These applications include cryptography, secure communication, image processing, electrochemistry, biology, quantum mechanics, pattern formation, and control among others. Notably, chaos-based encryption reveals that a chaotic system can create a key space to improve the security between end users (Abba *et al.* 2024; Hwang *et al.* 2023; Ilyas *et al.* 2022; Rahman *et al.* 2022).

The key contributions of this work are as follows:

1. Introduction of Multi-Dimensional Chaotic Maps for S-Box Design: The proposed method introduces an S-Box constructed using multi-dimensional chaotic maps, specifically utilizing the Lorenz and Henon chaotic systems.

Manuscript received: 11 January 2025,
Revised: 22 April 2025,
Accepted: 2 May 2025.

[1]zaid.a.abdulrazzaq@ntu.edu.iq (**Corresponding author**)
[2]harithga@ntu.edu.iq
[3]hakam_m_zaidan@ntu.edu.iq

2. Enhanced Resistance Against Linear Attacks: The proposed S-Box demonstrates a high level of non-linearity, significantly improving its resistance to linear cryptanalysis attacks.

3. Comprehensive Randomness Testing:

   - NIST Test Suite: The S-Box passes the NIST randomness tests with P-values significantly greater than 0.01, indicating robust security properties.
   - Distribution Tests: Results show P-values deviating substantially from a uniform distribution, highlighting the unpredictability of the S-Box values.
   - Dieharder Tests: The generated S-Box achieves high pass percentages, further validating its randomness and suitability for cryptographic use.

4. Suitability for Modern Cryptography: The results of this research make the proposed S-Box highly suitable for modern cryptosystems, as evidenced by the strong performance in the aforementioned security tests.

5. Comparative Performance Analysis: A comparative study with existing S-Box designs demonstrates that the proposed S-Box outperforms others in terms of key performance metrics, establishing it as a superior choice for cryptographic applications.

With the advent of the big data era, wired and wireless communication technology has explosively developed. This requires more and more secure encryption and decryption algorithms and the design of S-boxes. Due to the weaknesses of S-boxes, they need to be more secure and robust (Naseer *et al.* 2024; Al-Dweik *et al.* 2022; Indumathi and Sumathi 2022; Razaq *et al.* 2023; Ye and Chen 2024). Chaotic systems as design rules for S-boxes are particularly important in the field of information security. Therefore, the excellent performance of S-boxes is of paramount significance to the building. It is also of vital significance to both the building of chaotic systems and the design of a secure and robust block cipher system (Manzoor *et al.* 2022; Farah *et al.* 2020; Alsaif *et al.* 2023; Gohar 2023; Hoseini *et al.* 2022). The Henon map and the Lorenz chaotic system are two famous chaotic systems. The study of these two systems is also very important. The construction of excellent S-boxes has always been a particularly difficult problem. A constructive framework consisting of ten corresponding operations is used to construct a novel paradigm shift method of S-boxes (Long and Wang 2021; Artuğer 2024; Wang *et al.* 2020).

The Lorenz system has been widely investigated in the field of applied science and engineering. With the advent of the big data era, encrypted communication technology becomes more and more important (Ahuja *et al.* 2023; Can *et al.* 2023; Praveen *et al.* 2023). The building and optimization of a more secure block cipher system is essential. The excellent performance of the S-box is particularly important for the block cipher system. Different methods and principles can be used to encrypt information (Zied and Ibrahim 2023; Baowidan *et al.* 2024; Ali *et al.* 2022b). Chaotic systems are particularly important in the field of information security, and the construction of secure and robust S-boxes is of paramount significance to the building of block ciphers. The performance of the Henon map can also be more excellent. The method can be used to quickly search for the best S-box. This will help resolve a long-standing complex problem of the S-box (Mahboob *et al.* 2022; Zahid *et al.* 2023b; Kuznetsov *et al.* 2024; Mishra *et al.* 2023).

RELATED WORK

Significant research attention has been devoted to the use of chaotic systems in cryptographic algorithms. One proposed algorithm utilized bit permutation and phase encoding for image encryption. Another algorithm was based on a super Henon map and iteratively generated key components such as permutation bits, discrete chaotic system sequences, ciphering bits, private key, and auxiliary value (Fang *et al.* 2023; El-Latif *et al.* 2022; Muthu and Murali 2021; Zhang *et al.* 2023; Maazouz *et al.* 2022). A unified framework and general formula for an efficient chaotic encryption algorithm with non-volatile or based chaotic ciphers were also put forward. Additionally, an entropy analysis of chaotic encryption algorithms provided statistical information for security evaluation. Finally, a reversible chaos-based encryption algorithm introduced a public key to synchronize the permutation and ciphering behavior (Man *et al.* 2024; Dua *et al.* 2022; Umar *et al.* 2024; Pourasad *et al.* 2021; Li 2024; Kaur *et al.* 2020).

A new method for collecting specific initial conditions of the Henon map was introduced, along with a multi-layer image cryptosystem based on chaos. The complexity of an image encryption algorithm using the Rossler, Lorenz, and Fractional Order Lorenz System was assessed, revealing that the key-dependent measure was practical and effective (Niu *et al.* 2024; Galias 2022; Asbroek 2023; Wu *et al.* 2024; de Hénon 2024; Hareendran *et al.* 2024; Pal and Bhattacharjee 2020; Rong *et al.* 2022; Lenci *et al.* 2024). Additionally, a symmetric cryptosystem utilizing chaotic mapping and recurrent substitution boxes was discussed, along with a novel measure to evaluate the randomness of a repeated dynamic sequence. Furthermore, a design for S-boxes using a clonal selection algorithm and crossover immune cryptosystem was proposed, incorporating memory chaotic cryptography for optimization (Ahmad *et al.* 2022; Khaja and Ahmad 2023; Zhao *et al.* 2023; Abdulrazaq 2024; Alkhateeb and Al-Khatib 2020). Finally, an image encryption algorithm using a centralized chaotic map synthesized from the logistic map and a one-dimensional piecewise linear chaotic map with cross-mapping was presented (Nejatbakhsh 2022).

PROPOSED MODEL AND USED CHAOTIC MAPS

S-Boxes are critical components of the non-linear models used in block cipher systems, ensuring the confusion property a process that obscures the relationship between plaintext and ciphertext, enhancing security (Mohamed *et al.* 2014; Shannon 1949). For an S-Box to be effective, it must exhibit high levels of non-linearity and differentiability. S-Box designs can be broadly classified into two categories: static and dynamic. Static S-Boxes, used in earlier cipher systems, are more predictable and vulnerable to attacks, as their structure remains fixed throughout the encryption process. This vulnerability has led to the development of dynamic S-Boxes, which are key-independent and provide stronger security by continuously changing, making them harder for attackers to predict or exploit.

Chaos theory has been widely applied in communication systems due to its inherent randomness, making it useful for various applications, such as voice masking (Abdullah *et al.* 2022), noise reduction (Abdullah *et al.* 2015), frequency hopping (Ayoub *et al.* 2024), and image encryption (Salih *et al.* 2024). This work introduces a novel, dynamic S-Box design based on multi-dimensional chaotic maps, aiming to achieve high security performance and improve the robustness of modern cryptographic systems.

Henon map system is a one of the most two dimensional unpredictable chaotic maps, illustrate in equations (1,2); a,b are given as the control parameters with two initial conditions x_0, y_0:

$$x(n+1) = 1 + a(x(n))^2 + y(n) \tag{1}$$

$$y(n+1) = bx(n) \tag{2}$$

Lorenz Map System is a three dimensional chaotic map system, illustrate in equations (3 - 5) with three control parameters a,b,c and initial conditions x_0, y_0, z_0:

$$x(n+1) = a(y(n) - x(n)) \tag{3}$$

$$y(n+1) = x(n)(b - z(n)) - y(n) \tag{4}$$

$$z(n+1) = x(n)y(n) - (cz(n)) \tag{5}$$

PROPOSED SUBSTITUTION BOX (S-BOX)

Several methods employed to develop strong S-Box, the recent research based on mathematic calculation of chaotic behavior. This section presents novel strong dynamic S-Box with combing Henon and Lorenz chaotic maps. the proposed S-Box represented as 16 × 16 array with 8 bit for each element ranged from 0 to 255 providing of 256! probabilities. If one bit of the keys change cause the entire change. The procedure for generating S-Box explained in Figure 1 below.

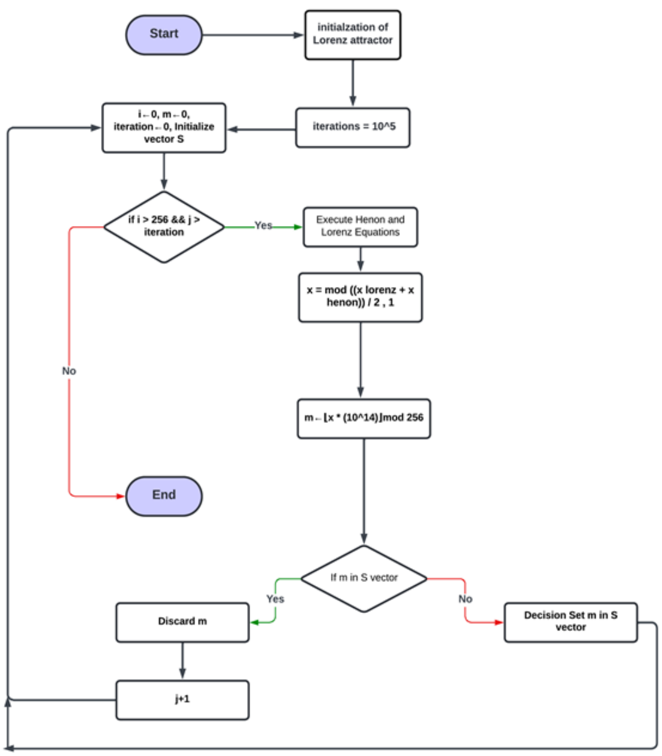

Figure 1 Flowchart of generating the proposed S-Box

S-Box Example

A complete example of a dynamic S-Box: assume $x_0 = 0.1$, $y_0 = 0$, $z_0 = 0$, $a = 10$, $b = 28$, $c = 8/3$, iterations = 100000, construction 16 × 16 S-Box with 8 bits size for each element, the elements are not repeated and random see Table 1.

Table 1 **Generated S-Box using the proposed model**

i/j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	211	67	126	207	138	182	156	251	136	152	204	155	164	111	187
2	255	228	1	210	97	108	88	31	103	66	18	147	16	222	131	134
3	2	79	245	247	109	253	4	159	248	23	153	179	176	139	225	175
4	242	209	85	68	3	37	5	40	93	112	189	105	61	81	180	46
5	205	59	100	20	198	90	213	52	128	201	73	217	49	63	158	141
6	135	71	94	191	72	11	116	82	216	56	171	14	29	254	199	36
7	47	129	25	87	224	214	208	186	96	86	197	174	32	75	188	177
8	166	183	238	167	229	77	140	130	252	70	50	60	148	65	27	84
9	200	22	123	95	178	226	146	30	250	12	190	143	133	218	54	42
10	58	151	241	19	34	196	7	236	160	33	235	119	192	24	227	57
11	26	212	234	223	202	6	240	51	17	244	230	243	181	165	249	106
12	53	170	149	110	21	48	163	114	107	142	169	124	215	41	39	239
13	232	80	122	13	28	161	43	219	127	125	237	150	98	69	203	83
14	184	206	173	104	144	154	113	145	220	172	55	89	8	233	74	62
15	10	78	118	246	45	168	64	231	76	221	15	99	185	117	101	162
16	120	91	193	157	132	35	44	9	102	121	137	195	38	194	115	92

RESULTS AND DISCUSSION

This section presented cryptographic analysis of proposed S-Box security performance in Tables 2-5.

S-Box Performance analysis

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 can be calculated using equation 6,

$$\mathrm{NL}(b) = \frac{1}{2}\left[2^n - \max_{h\in\{0,1\}^n} |WS_b(h)|\right] \tag{6}$$

The walsh spectrum of a function can be computed by the equation 7,

$$WS_{b(h)} = \sum_{x\in\{0,1\}^n} (-1)^{b(x)\oplus(h\cdot x)} \tag{7}$$

Where $h \in \{0,1\}^n$ and $h.x$ is the dot product of h and x computed by equation 8,

$$h \cdot x = (h_1 \oplus x_1) + ... + (h_n \oplus x_n) \tag{8}$$

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 the following non-linearly values with a minimum value of 112 , maximum value of 128 and average value of 125.125 shown in Table 2.

Strict-Avalanche Criterion (SAC): If an S-box's SAC value is close to 0.5 that will be considered to have sufficient randomness. Table 3 shows the mean SAC value is 0.5097, the maximum value is 0.609 and the minimum value is 0.394, and that value make the proposed S-Box satisfying for high performance.

Table 2 Non-Linearity Values of Boolean Functions of the Proposed S-Box

Boolean Function	Non-Linearity (NL)
f_1	128
f_2	120
f_3	128
f_4	120
f_5	122
f_6	126
f_7	122
f_8	112
f_9	128
f_{10}	128
f_{11}	128
f_{12}	128
f_{13}	128
f_{14}	128
f_{15}	128
f_{16}	128

Table 3 SAC Values of the Proposed S-Box

i/j	1	2	3	4	5	6	7	8
1	0.4844	0.5000	0.4844	0.5781	0.4531	0.5781	0.5312	0.5312
2	0.5312	0.5000	0.5469	0.4844	0.4844	0.4688	0.5156	0.5312
3	0.4688	0.4531	0.5469	0.6094	0.5625	0.4688	0.5469	0.5000
4	0.4844	0.5625	0.5156	0.4531	0.5156	0.5312	0.4688	0.4219
5	0.4844	0.5625	0.4844	0.4219	0.5938	0.5312	0.5469	0.5625
6	0.5312	0.4531	0.4844	0.5469	0.5469	0.5312	0.5312	0.5000
7	0.5000	0.5156	0.5312	0.5938	0.5625	0.4219	0.5000	0.5781
8	0.5000	0.5000	0.4844	0.3594	0.4062	0.5469	0.4219	0.5781

Bit-Independence Criterion (BIC)

The security of S-Box will be successful if changing one bit of its input cause changing m bits of its output. For satisfying BIC performance, the equation $((Si(x)xorSj(z)) - (Si(x)xorSj((x)))$ for all inputs of x where x, z changed by only one bit. If the average of all values is close to 0.5 it can be said that S-Box operates well in terms of BIC conditions. Table 4 shows the values of BIC for non-linearity, the average 0.503, maximum and minimum are 0.609 and 0.375 respectively, these values showed weak connection between output bits satisfying BIC property.

Table 4 BIC Values Output for SAC of the Proposed S-Box

0.4688	0.5625	0.5156	0.5156	0.5000	0.5000	0.5000	0.5781
0.4531	0.4844	0.5000	0.5000	0.5469	0.5781	0.4062	0.4688
0.5625	0.3906	0.4688	0.5469	0.5000	0.5156	0.5000	0.5000
0.5469	0.5156	0.5000	0.5312	0.5156	0.4688	0.5156	0.5156
0.5156	0.4844	0.5469	0.4531	0.4219	0.4844	0.5156	0.4844
0.5000	0.5156	0.4688	0.4688	0.5312	0.5469	0.5312	0.5000
0.4844	0.3750	0.5156	0.5000	0.5312	0.5312	0.6094	0.4688
0.5156	0.4531	0.5312	0.4844	0.6094	0.5000	0.5156	0.4844

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 9 The maximum

$$LP = \max_{a_z, b_z \neq 0} \left| \frac{\#\{z \in \mathbb{N} \mid z \cdot a_z = S(z) \cdot b_z\}}{2^n} - \frac{1}{2} \right| \tag{9}$$

value of LP is 0.123 for the proposed S-Box is indicating good resistance against linear attacks.

Differential-Probability (DP): Differential analysis is the technique of recovering the original plaintext from the encrypted ciphertext by differentiating each pairs of ciphertext from their corresponding plaintext. By this type of calculations the attacker can try to get the encryption key. The lower value of DP as shown in equation 10 indicates high level of security of cryptographic S-Box.

$$DP = \max_{\Delta_z \neq 0, \Delta_y} \left| \frac{\#\{z \in \mathbb{N} \mid S(z) \oplus S_{(z \oplus \Delta z)} = \Delta y\}}{2^n} \right| \tag{10}$$

The low differentiae is 0.0156 indicates the strength of the proposed S-Box.

Box Performance Comparison

Table 5 shows comparative study of the proposed work with other researchers in terms of performance metrics.

Table 5 Comparison of the Proposed Work with Other Studies

S-box Method	Min NL	Avg NL	Max NL	SAC	BIC	LP	DP
(Zahid *et al.* 2023a)	110	111.00	112	0.496	–	0.125	0.039
Proposed	112	125.25	128	0.509	0.503	0.123	0.015

S-box plays an important role in cryptographic operations. the proposed approach based on chaotic maps does not required calculating inverses or multiplicative mathematical operations which are complex and time consuming, the robustness was good according to performance metrics.

CONCLUSION

Information is a very important aspect in any corporation, it helps to make decision, that make the information transmission security is an essential for make profits. Cryptography is a security field that deals with information protection. This paper presents construction of strong cryptographically robust and dynamic S-box using compound chaotic maps. number of performance metrics such as non-linearity(NL), Strict Avalanche Criterion (SAC), Bit-Independence Criterion (BIC), Linear-Probability (LP) and differential-Probability (LP) for test the generated S-box and compared to recent researcher provide a satisfied strength recent cryptosystems. As a future work different hyperchaotic maps can be employed for build S_boxes enhancing cryptographic systems. Second approach is to employ this S_box for complete key generation, encryption and decryption to support overall security system performance.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Abba, A., J. S. Teh, and M. Alawida, 2024 Towards accurate keyspace analysis of chaos-based image ciphers. Multimedia Tools and Applications .

Abdullah, H. N., S. S. Hreshee, and A. K. Jawad, 2015 Noise reduction of chaotic masking system using repetition method. Unpublished .

Abdullah, H. N., S. S. Hreshee, G. Karimi, and A. K. Jawad, 2022 Performance improvement of chaotic masking system using power control method. In *International Middle Eastern Simulation and Modelling Conference 2022, MESM 2022*, pp. 19–23.

Abdulrazaq, N. N., 2024 Generating of a dynamic and secure s-box for aes block cipher system based on modified hexadecimal playfair cipher. Zanco Journal of Pure and Applied Sciences **36**: 45–56.

Ahmad, A. D. Y., I. Hussain, M. Saleh, and M. T. Mustafa, 2022 A novel method to generate key-dependent s-boxes with identical algebraic properties. Journal of Information Security and Applications **65**: 103105.

Ahuja, B., R. Doriya, S. Salunke, and M. F. Hashmi, 2023 Hdiea: high dimensional color image encryption architecture using five-dimensional gauss-logistic and lorenz system. Connection Science **35**: 123–145.

Al-Dweik, A. Y., I. Hussain, M. Saleh, and M. T. Mustafa, 2022 A novel method to generate key-dependent s-boxes with identical algebraic properties. Journal of Information Security and Applications .

Al-Turjman, F. and H. Zahmatkesh, 2022 An overview of security and privacy in smart cities' iot communications. Transactions on Emerging Telecommunications Technologies **33**: e3677.

Ali, A., M. A. Khan, R. K. Ayyasamy, and M. Wasif, 2022a A novel systematic byte substitution method to design strong bijective substitution box (s-box) using piece-wise-linear chaotic map. PeerJ Computer Science .

Ali, R., J. Ali, P. Ping, and M. K. Jamil, 2024 A novel s-box generator using frobenius automorphism and its applications in image encryption. Nonlinear Dynamics .

Ali, R. S., O. Z. Akif, S. A. Jassim, A. K. Farhan, and E. S. M. El-Kenawy, 2022b Enhancement of the cast block algorithm based on novel s-box for image encryption. Sensors **22**: 5678.

Alkhateeb, F. and R. M. Al-Khatib, 2020 A survey for recent applications and variants of nature-inspired immune search algorithm. International Journal of Computational Intelligence Systems **13**: 1234–1248.

Alqahtani, J., M. Akram, G. A. Ali, N. Iqbal, and A. Alqahtani, 2023 Elevating network security: A novel s-box algorithm for robust data encryption. In *IEEE Conference on Network Security*, IEEE.

Alsaif, H., R. Guesmi, A. Kalghoum, and B. M. Alshammari, 2023 A novel strong s-box design using quantum crossover and chaotic boolean functions for symmetric cryptosystems. Symmetry **15**: 456.

Artuğer, F., 2024 Strong s-box construction approach based on josephus problem. Soft Computing **28**: 123–145.

Asbroek, T., 2023 The hénon map. Lecture notes or unpublished work, Available upon request.

Asghar, M. Z., S. A. Memon, and J. Hämäläinen, 2022 Evolution of wireless communication to 6g: Potential applications and research directions. Sustainability **14**: 6356.

Ayoub, H. G., Z. A. Abdulrazzaq, A. F. Fathil, S. A. Hasso, and A. T. Suhail, 2024 Unveiling robust security: Chaotic maps for frequency hopping implementation in fpga. Ain Shams Engineering Journal **15**: 103016.

Baowidan, S. A., A. Alamer, and M. Hassan, 2024 Group-action-based s-box generation technique for enhanced block cipher security and robust image encryption scheme. Symmetry **16**: 45.

Bavdekar, R., E. J. Chopde, A. Bhatia, and K. Tiwari, 2022 Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. arXiv preprint arXiv .

Can, O., F. Thabit, A. O. Aljahdali, and S. Al-Homdy, 2023 A comprehensive literature of genetics cryptographic algorithms for data security in cloud computing. In *International Conference on Computing and Systems*, pp. 456–470, Taylor & Francis.

de Hénon, J. X., 2024 Hénon maps: a list of open problems. Arnold Mathematical Journal **10**: 45–60.

Dua, M., D. Makhija, P. Y. L. Manasa, and P. Mishra, 2022 3d chaotic map-cosine transformation based approach to video encryption and decryption. Open Computer Science **12**: 146–160.

Ekwueme, C. P., I. H. Adam, and A. Dwivedi, 2024 Lightweight cryptography for internet of things: A review. Endorsed Transactions on ... .

El-Latif, A. A. A., J. Ramadoss, B. Abd-El-Atty, and H. S. Khalifa, 2022 A novel chaos-based cryptography algorithm and its performance analysis. Mathematics **10**: 2736.

Fang, P., H. Liu, C. Wu, and M. Liu, 2023 A survey of image encryption algorithms based on chaotic system. The Visual Computer **39**: 2965–2983.

Farah, M. A. B., R. Guesmi, A. Kachouri, and M. Samet, 2020 A new design of cryptosystem based on s-box and chaotic permutation. Multimedia Tools and Applications **79**: 12345–12367.

Farooq, M. S., K. Munir, A. Alvi, and U. Omer, 2022 Design of a substitution box using a novel chaotic map and permutation. VFAST Transactions on Software .

Frank, E., 2024 Chaos theory, deterministic chaos, attractors, and sensitive initial conditions are key principles in chaotic encryption .

Galias, Z., 2022 Dynamics of the hénon map in the digital domain. IEEE Transactions on Circuits and Systems I: Regular Papers **69**: 1789–1800.

Gohar, Z. M. S., 2023 Securing engineering blueprints transmission using s-box and chaos theory .

Hareendran, A., B. V. Nair, S. S. Muni, and M. Lellep, 2024 Comparative analysis of predicting subsequent steps in hénon map. arXiv preprint arXiv:2403.xxxxx Preprint.

Hoseini, R., S. Behnia, S. Sarmady, and S. Fathizadeh, 2022 Construction of dynamical s-boxes based on image encryption approach. Soft Computing **26**: 12345–12360.

Hwang, J., G. Kale, P. P. Patel, and R. Vishwakarma, 2023 Machine learning in chaos-based encryption: Theory, implementations, and applications. In *IEEE Conference on Communications and Network Security*, IEEE.

Ilyas, B., S. M. Raouf, S. Abdelkader, and T. Camel, 2022 An efficient and reliable chaos-based iot security core for udp/ip wireless communication. In *IEEE International Conference on Internet of Things*, IEEE.

Indumathi, A. and G. Sumathi, 2022 Construction of key-dependent s-box for secure cloud storage. Intelligent Automation & Soft Computing .

Kaur, M., D. Singh, K. Sun, and U. Rawat, 2020 Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5d chaotic map. Future Generation Computer Systems **107**: 333–350.

Khaja, I. A. and M. Ahmad, 2023 Similarity learning and genetic algorithm based novel s-box optimization. In *International Sym-*

posium on Intelligent Informatics, pp. 456–470, Springer.

Khoshafa, M. H., O. Maraqa, J. M. Moualeu, S. Aboagye, T. M. N. Ngatched, *et al.*, 2024 Ris-assisted physical layer security in emerging rf and optical wireless communication systems: A comprehensive survey. IEEE Communications Surveys & Tutorials Accepted for publication.

Knežević, K., 2023 Machine learning and evolutionary computation in design and analysis of symmetric key cryptographic algorithms. Preprint or unpublished report.

Kuznetsov, A., S. Kandii, E. Frontoni, and N. Poluyanenko, 2024 Sbgen: A high-performance library for rapid generation of cryptographic s-boxes. SoftwareX **25**: 101595.

Lenci, S., K. C. B. Benedetti, and G. Rega, 2024 Stochastic basins of attraction for uncertain initial conditions. Journal of Sound and Vibration **568**: 118028.

Li, L., 2024 A novel chaotic map application in image encryption algorithm. Expert Systems with Applications **238**: 121932.

Long, M. and L. Wang, 2021 S-box design based on discrete chaotic map and improved artificial bee colony algorithm. IEEE Access **9**: 123456–123467.

Maazouz, M., A. Toubal, B. Bengherbia, and O. Houhou, 2022 Fpga implementation of a chaos-based image encryption algorithm. Journal of King Saud University-Computer and Information Sciences **34**: 6114–6125.

Mahboob, A., M. Asif, M. Nadeem, and A. Saleem, 2022 A cryptographic scheme for construction of substitution boxes using quantic fractional transformation. In *IEEE International Conference on Cryptography*, pp. 123–128, IEEE.

Mahboob, A., M. Nadeem, and M. W. Rasheed, 2023 A study of text-theoretical approach to s-box construction with image encryption applications. Scientific Reports .

Man, Z., J. Li, X. Di, Y. Sheng, *et al.*, 2024 Double image encryption algorithm based on neural network and chaos. Chaos, Solitons & Fractals **178**: 114328.

Manzoor, A., A. H. Zahid, and M. T. Hassan, 2022 A new dynamic substitution box for data security using an innovative chaotic map. IEEE Access **10**: 98765–98780.

Mishra, R., M. Okade, and K. Mahapatra, 2023 Novel substitution box architectural synthesis for lightweight block ciphers. IEEE Embedded Systems Letters **15**: 65–68.

Mohamed, K., M. N. M. Pauzi, F. H. H. M. Ali, S. Ariffin, and N. H. N. Zulkipli, 2014 Study of s-box properties in block cipher. In *2014 International Conference on Computer, Communications, and Control Technology (I4CT)*, pp. 362–366, IEEE.

Muthu, J. S. and P. Murali, 2021 Review of chaos detection techniques performed on chaotic maps and systems in image encryption. SN Computer Science **2**: 386.

Naseer, M., S. Tariq, N. Riaz, and N. Ahmed, 2024 S-box security analysis of nist lightweight cryptography candidates: A critical empirical study. arXiv preprint arXiv Preprint.

Nejatbakhsh, A., 2022 *Scalable Tools for Information Extraction and Causal Modeling of Neural Data*. Columbia University.

Niu, S., R. Xue, and C. Ding, 2024 A dual image encryption method based on improved hénon mapping and improved logistic mapping. Multimedia Tools and Applications **83**: 12345–12367.

Pal, A. and J. K. Bhattacharjee, 2020 The hidden variable in the dynamics of transmission of covid-19: A hénon map approach. medRxiv Preprint.

Picek, S. and D. Jakobovic, 2022 Evolutionary computation and machine learning in security. In *Proceedings of the Genetic and Evolutionary*.

Pourasad, Y., R. Ranjbarzadeh, and A. Mardani, 2021 A new algorithm for digital image encryption based on chaos theory. Entropy **23**: 341.

Praveen, S. P., V. S. Suntharam, and S. Ravi, 2023 A novel dual confusion and diffusion approach for grey image encryption using multiple chaotic maps. Computer Science **14**: 789–801.

Progonatı, E., 2023 Chaos theory and political sciences. Diplomasi Araştırmaları Dergisi .

Rahman, A., K. Hasan, D. Kundu, and M. J. Islam, 2023 On the icn-iot with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives. Future Generation Computer Systems **136**: 1–15.

Rahman, Z., X. Yi, M. Billah, M. Sumi, *et al.*, 2022 Enhancing aes using chaos and logistic map-based key generation technique for securing iot-based smart home. Electronics .

Razaq, A., G. Alhamzi, S. Abbas, M. Ahmad, *et al.*, 2023 Secure communication through reliable s-box design: A proposed approach using coset graphs and matrix operations. Heliyon .

Rong, K., H. Bao, H. Li, Z. Hua, *et al.*, 2022 Memristive hénon map with hidden neimark-sacker bifurcations. Nonlinear Dynamics **108**: 1789–1805.

Salih, A. A., Z. A. Abdulrazaq, and H. G. Ayoub, 2024 Design and enhancing security performance of image cryptography system based on fixed point chaotic maps stream ciphers in fpga. Baghdad Science Journal **21**: 1754–1754.

Shannon, C. E., 1949 Communication theory of secrecy systems. The Bell system technical journal **28**: 656–715.

Sirohi, D., N. Kumar, P. S. Rana, S. Tanwar, and R. Iqbal, 2023 Federated learning for 6g-enabled secure communication systems: a comprehensive survey. Artificial Intelligence Review **56**: 1–34.

Umar, T., M. Nadeem, and F. Anwer, 2024 Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage. Expert Systems with Applications **238**: 121656.

Waheed, A., F. Subhan, M. M. Suud, and M. Alam, 2023 An analytical review of current s-box design methodologies, performance evaluation criteria, and major challenges. Multimedia Tools and Applications .

Wang, J., Y. Zhu, C. Zhou, and Z. Qi, 2020 Construction method and performance analysis of chaotic s-box based on a memorable simulated annealing algorithm. Symmetry **12**: 788.

Wu, Y., S. Chu, H. Bao, D. Wang, *et al.*, 2024 Optimization of image encryption algorithm based on hénon mapping and arnold transformation of chaotic systems. IEEE Access **12**: 12345–12356.

Xun, P., Z. Chai, Z. Ma, L. Miao, and S. Li, 2024 Substitution box design based on improved sine cosine algorithm. In *Proceedings of the International*.

Ye, J. and Y. Chen, 2024 Sc-sa: Byte-oriented lightweight stream ciphers based on s-box substitution. Symmetry .

Zahid, A. H., M. J. Arshad, M. Ahmad, N. F. Soliman, and W. El-Shafai, 2023a Dynamic s-box generation using novel chaotic map with nonlinearity tweaking. Computers, Materials & Continua **75**.

Zahid, A. H., H. A. M. Elahi, M. Ahmad, and R. S. A. Said, 2023b Secure key-based substitution-boxes design using systematic search for high nonlinearity. In *IEEE Symposium on Security and Privacy*, pp. 456–461, IEEE.

Zelinka, I. and R. Senkerik, 2023 Chaotic attractors of discrete dynamical systems used in the core of evolutionary algorithms: state of art and perspectives. Journal of Difference Equations and Applications .

Zhang, H., H. Hu, and W. Ding, 2023 Image encryption algorithm based on hilbert sorting vector and new spatiotemporal chaotic system. Optics & Laser Technology **158**: 108859.

Zhao, M., H. Liu, and Y. Niu, 2023 Batch generating keyed strong s-boxes with high nonlinearity using 2d hyper chaotic map. Integration **90**: 123–135.

Zied, H. S. and A. G. A. Ibrahim, 2023 S-box modification for the block cipher algorithms. Przeglad Elektrotechniczny **99**: 123–128.

How to cite this article: Abdulrazaq, Z. A., Ayoub, H. G., and Ayoub, H. Synergistic Construction of High-Performance S-Boxes Based on Chaotic Systems: A Paradigm Shift in Cryptographic Security Design. *Chaos and Fractals*, 2(2), 43-49, 2025.