Mehran University Research Journal of Engineering and Technology

https://doi.org/10.22581/muet1982.0354

2025, 44(4) 101-119

Dynamic S-box construction based on a novel chaotic map and twitching approach

Muhammad Rehan Saleem[a], Amjad Hussain Zahid[a], and Ghulam Mustafa[a]

[a] *School of Systems and Technology, University of Management and Technology, Lahore, 54000, Pakistan*

[*] Corresponding Author: Amjad Hussain Zahid, Email: amjad.zahid@umt.edu.pk

Received: 14 May 2025, Revised: 22 September 2025, Accepted: 29 September 2025, Published: 01 October 2025

KEYWORDS

Hyperchaotic Map

Substitution Box

Twitching Mechanism

Cryptography

Cryptanalysis

Key Space

ABSTRACT

The increasing frequency of hacking and phishing assaults has made data encryption and information security as major solutions. Attackers are concentrating on breaking cryptosystems to obtain valuable data and information. Many ciphers have been created and put into use for the security of both data and information. A substitution box (S-Box), being an essential part of many symmetric-key block ciphers, provides much-needed confusion for the transmitted data. This research article offers an innovative method for creating key-dependent and dynamic S-Boxes using a new hyperchaotic map. Additionally, a dynamic twitching mechanism, that is presented first time, is applied to the initial S-Box for optimization purposes to ensure that the final S-Box adheres to the accepted cryptographic standards. Several tests, including the strict avalanche criterion, bit independence criterion, nonlinearity, fixed-point analysis, linear and differential probabilities, are performed to assess the cryptographic performance of the proposed S-Boxes. An example S-Box produced by the proposed approach is evaluated against these tests and compared with the contemporary S-Boxes. The comparative analysis reveals that the designed S-Box having average NL value of 112 and SAC value of 0.5 has the candid potential of adaptability in real-life security endeavors.

1. Introduction

Our dependence on data and information is enormous in the recent technological era. A sizeable portion of such data is automatically generated and must either be kept or sent across insecure and public communication channels [1,2]. The protection of data communicated across insecure channels is one of the major issues. The frequency of attacks on data has also increased greatly as the number of network users continues to grow and the internet usage has become more diverse [3,4]. So, the information transmitted through shared networks and protecting it becomes more important and obvious [5,6,7]. The exchange of sensitive data through public networks is increasing.

Consequently, protecting the data from intruders is a major concern, and cryptographic techniques known as ciphers must be used to ensure the security of this data. Stream and block ciphers are the two main types of ciphers that assist in the protection of data from attackers. Though stream ciphers provide good security, these are characteristically slower than block ciphers as they convert the data one bit or byte at a time [8,9]. Block ciphers are used when one has a huge volume of data and efficient encryption is needed, where stream ciphers usually underperform. To convert the data into a muddled form, permutation and substitution are the primary operations performed in these block ciphers. A substitution process substitutes a block of data with another in a nonlinear way, whereas the permutation operation exchanges the bits or bytes of plaintext with other bits or bytes of the same plaintext [10,11]. To aid in the substitution process, the majority of well-known block ciphers include substitution boxes (S-Boxes). A substitution box is a crucial part of modern block encryption methods and helps to obscure bits of data [12]. Both the static and dynamic S-Boxes are used in the cipher design. Block ciphers based on a static S-box employ

© Mehran University of Engineering and Technology 2025

an S-box that has a fixed, unique output value for a unique input, and it makes them vulnerable to attacks. A static S-box is less effective and efficient in introducing confusion than a dynamic S-box. Since static S-Boxes have flaws that can be exploited by attackers, consequently ciphers like Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are more prone to attacks. Nowadays, block ciphers employ key-dependent S-Boxes generated with the support of the cipher key and hence possess more cryptographic strength than the static S-Boxes [13,14].

Many researchers have devised a variety of methods for creating dynamic and key-dependent S-Boxes. Linear fractional transformation (LFT) is frequently employed to create strong and dynamic S-Boxes. Authors [15,16] applied the LFT concept as the basis for designing efficient and reliable S-Boxes that showed good cryptographic performance. AES cipher has some weaknesses associated with it due to the use of a static S-box based on the Galois Field (GF). Many researchers suggested various enhancements to the original AES S-box to overcome its associated weaknesses [17,18,19]. These generation techniques prove that the improved S-Boxes have shown good cryptographic properties. Authors in [20,21,22] have introduced novel and straightforward transformation techniques for the creation of dynamic S-Boxes.

To manufacture robust and dynamic S-Boxes that are also simple to produce, it is required to investigate innovative and effective strategies. The methods for building such S-Boxes that are described in the literature, however, have complexity and efficiency difficulties [23,24,25]. Numerous researchers have delved into alternative knowledge domains to create a diverse set of S-Boxes, drawing inspiration from various areas. One such domain is chaos which helps in designing chaotic map-based S-Boxes. A glimpse of such work includes chaotic map for dynamic S-box designing [26], image encryption using chaotic map and dynamic S-box [27] chaotic map and teaching-learning based optimization [28], discrete chaotic map [29], linear trigonometric transformation [30], one-dimensional discrete chaotic map [31], improved artificial bee colony algorithm and discrete chaotic map [32], the combination of chaotic map and fitness function [33], chaotic and bent functions [34], cuckoo search algorithm and discrete chaotic map [35], discrete chaotic map and multiplication of integers [36], image encryption scheme based on fractional-order differential logistic map and S-Boxes [37], and many more. Several other researchers [38–46] have introduced methodologies for S-box construction based on chaos, leveraging various conceptual frameworks.

Notwithstanding the prevalent use of chaotic maps in S-box design, it is essential to acknowledge that these maps are not without inherent limitations [47]. To establish resilient S-Boxes, a new approach in [48] is characterized by its remarkable simplicity and efficacy. In light of the continuous increase of cryptanalytic endeavours, the ongoing imperative remains the development of new substitution boxes that offer enhanced and heightened reliability [49] and provide a novel approach to S-box design through the utilization of a hyperchaotic map and a tweaking method. This paper can be regarded as a significant contribution to the field of modern cryptosystems and their data security applications. Authors [50] recommend an efficient image encryption technique based on a 4-D hyperchaotic Lorenz map, including pixel-level and bit-level permutation for improved security in the permutation phase. Researchers [51–55] presented techniques for S-box construction based on chaos, while coset graphs were utilized by the authors [56] for the same purpose.

1.1 Research gap and motivation

The approaches presented in the literature for S-Box generation using chaotic maps have associated drawbacks and limitations too. These chaotic maps do not fulfill the necessary criteria such as sensitivity to the initial conditions, Bifurcation, Lyapunov exponent, ergodicity, etc. Along with it, the resultant S-Boxes based on these chaotic maps do not meet the standard criteria such as fixed-point analysis, nonlinearity, bit independence criterion, strict avalanche criterion, linear probability, differential probability, etc. Similarly, the associated keyspace of these techniques is not enormous which must be there to defy brute force attacks. Hence, there is a critical need to design new chaotic maps for the generation of dynamic S-Boxes to assist the community in resisting the cryptanalytical efforts of the attackers.

1.2 Research contribution

The following are the key contributions of this research article:

- A new hyperchaotic map has been proposed to harness its nonlinear behaviour that is verified through bifurcation and Lyapunov criteria. The

© Mehran University of Engineering and Technology 2025

proposed hyperchaotic map is presented first time and is based on the concept of cubic polynomial.
- A method utilizing the proposed hyperchaotic map for the construction of robust and dynamic S-Boxes has been crafted.
- A novel approach is introduced that enhances the cryptographic strength of the initial S-box to generate a final S-box as ensuring data protection from potential vulnerabilities during transmission over unreliable transmission media is very important.

The rest of the paper is organized as Section 2 demonstrates the methodology including a hyperchaotic map and an innovative S-box design. Section 3 emphasizes the security analysis for the proposed S-box design, along with describing the time needed for the generation of the final S-box. Section 4 investigates the key space of the projected technique. The associated limitations of the proposed chaotic map are presented in Section 5. The conclusion given in Section 6 sums up the findings. At the end, references are stated in Section 7.

2. Proposed Methodology

In this research work, a dynamic and key-dependent S-Box based on an innovative hyperchaotic map and cipher key is designed. This approach leverages the inherent randomness, non-periodic behaviour, and sensitivity to initial conditions that characterize hyperchaotic systems, offering enhanced security for cryptographic applications. The foundation of this S-Box design is a pioneering hyperchaotic map which functions in a high-dimensional state space and enhances the complexity and unpredictability making the resultant S-Box resilient to various methods of cryptanalysis. The process of creating a final S-Box is divided into the following steps:

1. Design of a novel hyperchaotic map: The groundwork of generating a robust substitution box is based on the proposal of a novel hyperchaotic map.

2. Construction of an initial S-Box: Echoing the inherent complexity of the hyperchaotic system, this step involves the construction of an initial S-Box.

3. Nonlinearity optimization of the original S-Box: The preliminary S-Box derived from the hyperchaotic map is optimized further to boost its cryptographic strength, concentrating especially on its nonlinearity. Initial S-Box is tweaked to offer high level of protection to the data making it a perfect fit for incorporation into modern-day ciphers.

The next section covers these steps in detail.

2.1 New hyperchaotic map design

An initial S-box is generated using a novel hyperchaotic map (named as RAM−Rehan, Amjad, and Mustafa) as described in Equation (1). The suggested hyperchaotic map serves as the foundation for the initial S-box design, which promises to reduce data security breaches. Cipher key employs the values of the parameters X_n, V_1, and V_2 as stated in Eq. (1).

$$\left.\begin{aligned} Y_{n+1} &= |\left(5.0 * ((X_n)^3 + 1.3\right)) \text{ MOD } 1.0| \\ Z_{n+1} &= |\left(3.0 * \left(X_n + V_1\right)\right) \text{ MOD } 1.0| \\ \mathrm{a} &= 3.3 * \left(Y_{n+1} + V_2\right) \\ \mathrm{b} &= \mathrm{a} + V_1 + Z_{n+1} + 0.5 \\ X_{n+1} &= |\left(3.3 * \mathrm{b}\right) \text{ MOD } 1.0| \\ V_1 &= |\left(9.9 * Y_{n+1}\right) \text{ MOD } 1.0| \end{aligned}\right\} \quad (1)$$

where, $0.0 < X_n, V_1, V_2 < 1.0$ *and*

$$0.0 < a < 6.6.$$

The utilization of the proposed hyperchaotic map demonstrates a noticeable sensitivity to the initial values of the parameters and prescribed conditions, thus presenting a compelling avenue for fortifying the cryptographic robustness of the S-Box paradigm, thereby mitigating vulnerabilities to potential security breaches.

The bifurcation diagram and the Lyapunov Exponent (LE) graph identify the nonlinear behaviour of a chaotic map. A system is classified as chaotic when the bifurcation diagram covers the whole state space and the Lyapunov Exponent of its corresponding chaotic map surpasses zero. This component (LE) quantifies a system's sensitivity to initial conditions, with a positive value indicating chaotic behaviour. Greater LE values correspond to more unpredictability encapsulating the system's complex and nonlinear dynamics.

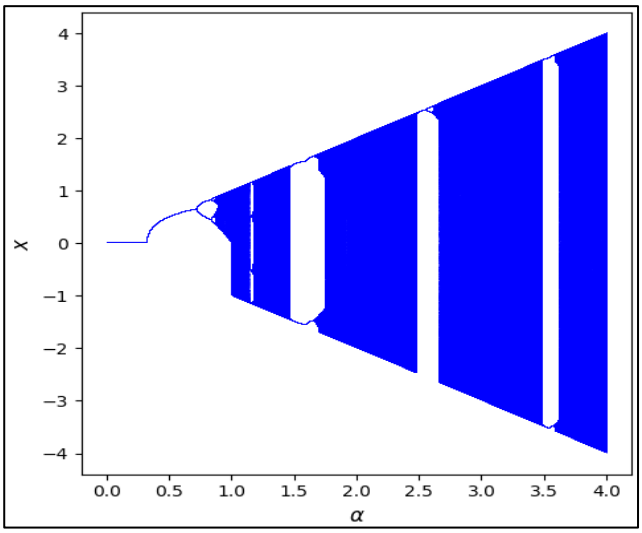
Sine map (SM), AZ map [49], Lorenz map, Chen map, and Rossler map are among the recently proposed and well-known chaotic maps. The bifurcation outcomes of these maps and the projected chaotic map (RAM) are presented and compared in Figure 1. It is evident from Figure 1 that the proposed

© Mehran University of Engineering and Technology 2025

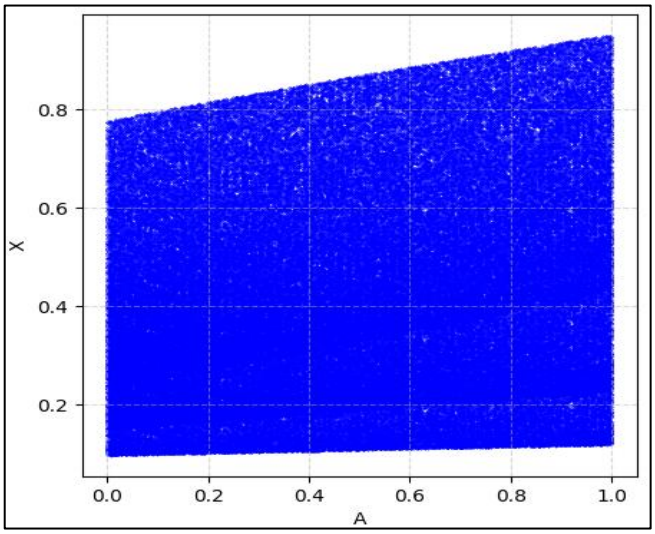
chaotic map has a more complex bifurcation pattern, covering the whole range of space compared to the other maps. As shown in Figure 2, the Lyapunov Exponent for the projected chaotic map is compatible to those of the other two 1D chaotic maps (sine and AZ maps) and three 2D chaotic maps (Lorenz, Chen, and Rossler), demonstrating its effectiveness with respect to the sensitivity and chaotic behaviour.

Similarly, 2D and 3D phase space diagrams of Lorenz map, Chen map, Rossler map, and proposed chaotic map (RAM) are depicted in Figures 3 and 4 respectively. It is very evident that the proposed chaotic map has superiority over other mentioned competitor maps.

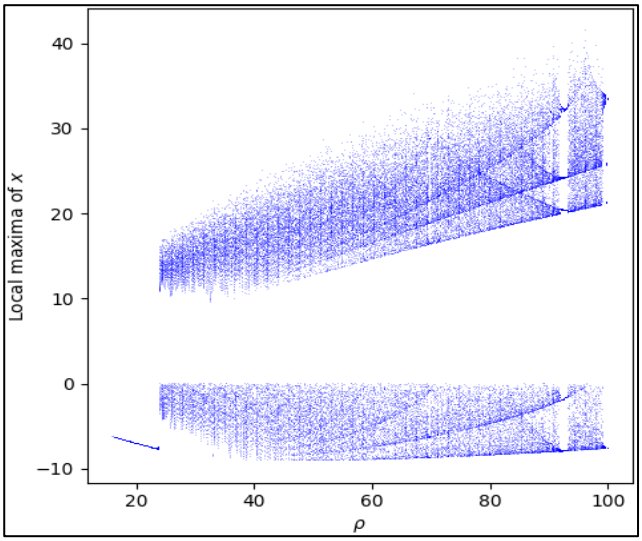
One of the necessary criteria to check the chaotic behaviour for a chaotic map along with the bifurcation and Lyapunov exponent is its sensitivity to the initial conditions. The sensitivity diagrams of the Sine Map, MAZa map [6], and the proposed chaotic map are shown in Figures 5, 6, and 7 respectively. It can be verified from Figures 5 and 6 that both the Sine and MAZa chaotic maps are not sensitive to the initial conditions even when there is a small change of order 10^{-15} in one of the parameters (X_0). Both the graphs of Figures 5 (a) and 5 (b) are identical which reflects that the Sine chaotic map has very poor sensitivity to the initial conditions. Similarly, graphs shown in Figures 6 (a) and 6 (b) are also indistinguishable which shows that the MAZa chaotic map also possesses very scarce sensitivity to the initial conditions. On the other hand, Figure 7 clearly demonstrates that the proposed chaotic map RAM is quite sensitive as even minute changes of the order 10^{-15} in the initial values of its one parameter X_0 has led to the greater unpredictability that is one of the demanding features for safeguarding the transmitted dat. Consequently, the proposed chaotic map meets the sensitivity criterion which makes it a solid candidate for its usage in the generation of innovative and robust dynamic S-Boxes.



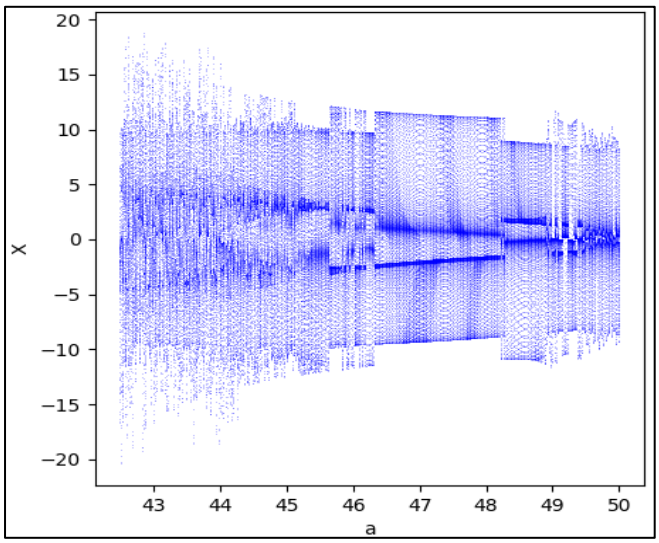
(a)



(b)

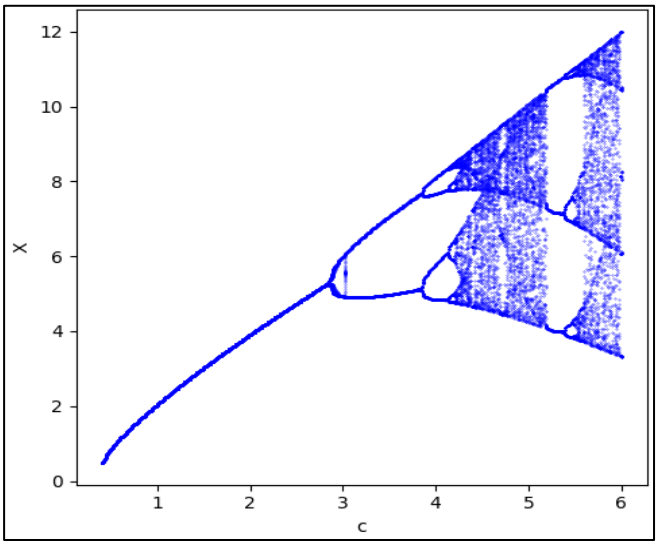


(c)

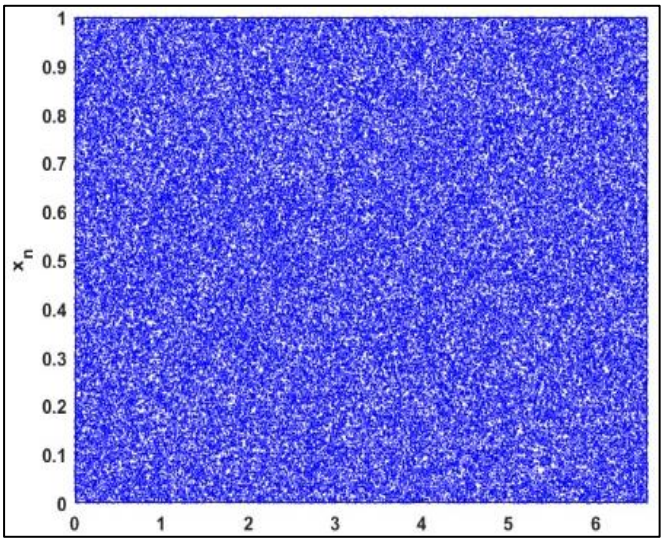


(d)

© Mehran University of Engineering and Technology 2025

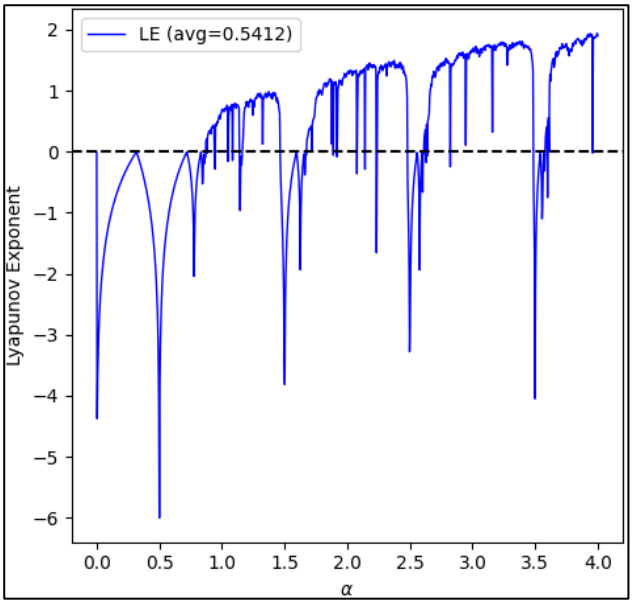


(e)

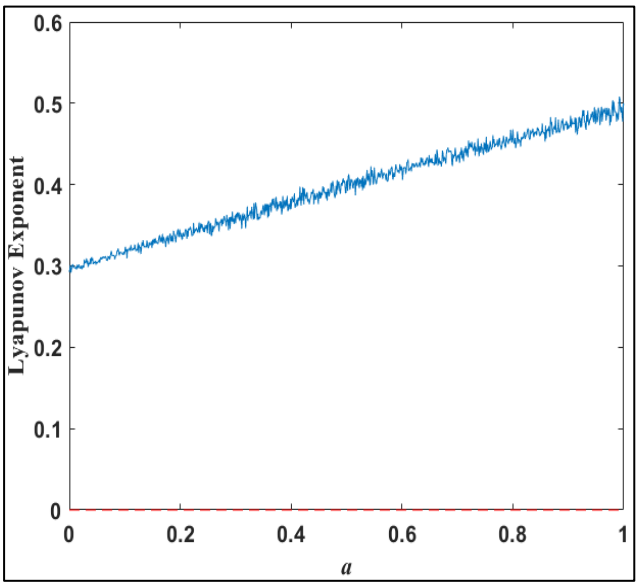


(f)

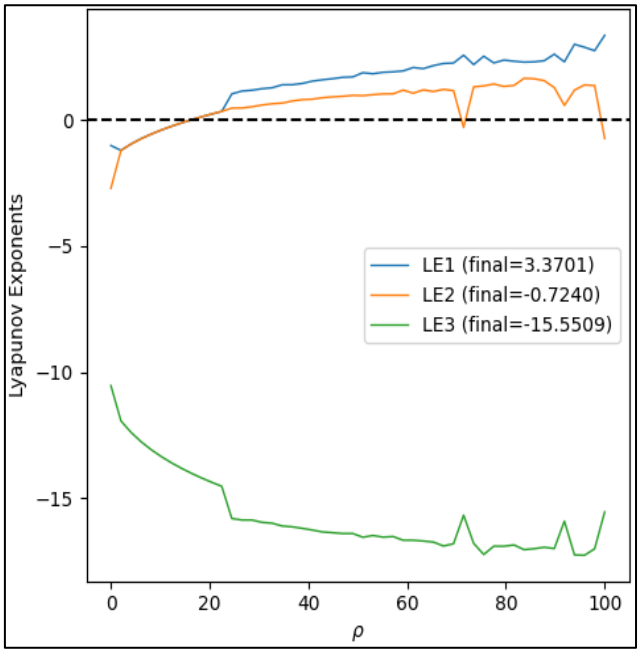
Fig. 1. Bifurcation diagrams of maps (a) Sine, (b) AZ, (c) Lorenz (d) Chen, (e) Rossler, and (f) Proposed RAM chaotic map



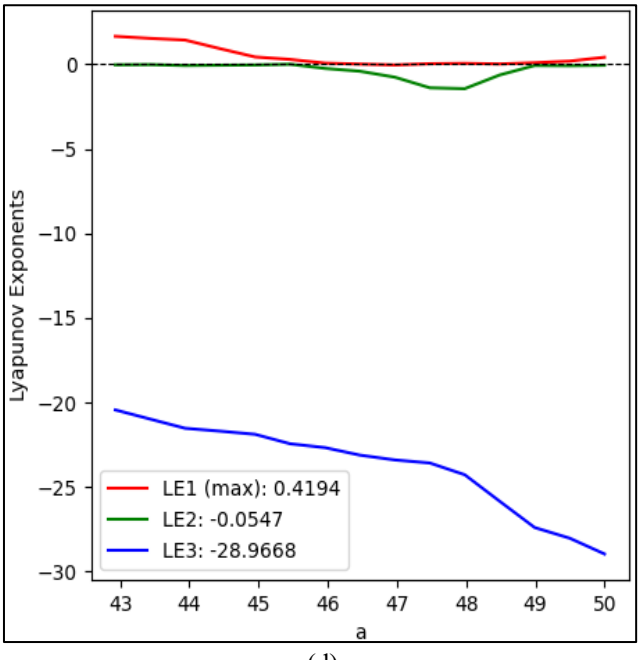
(a)



(b)

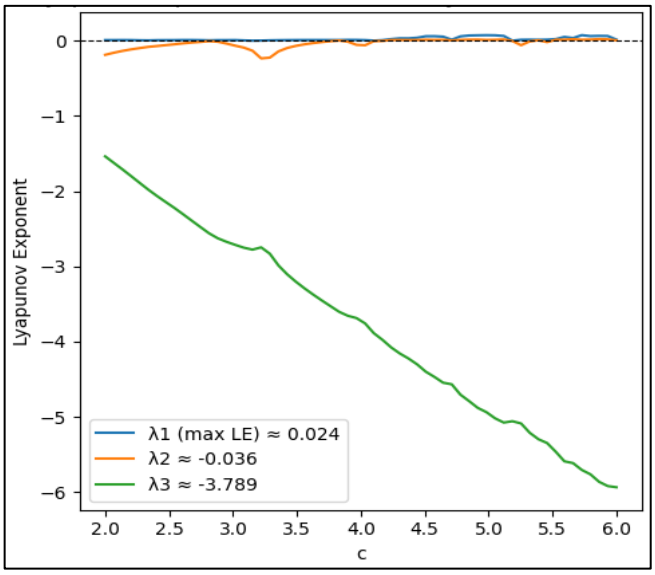


(c)

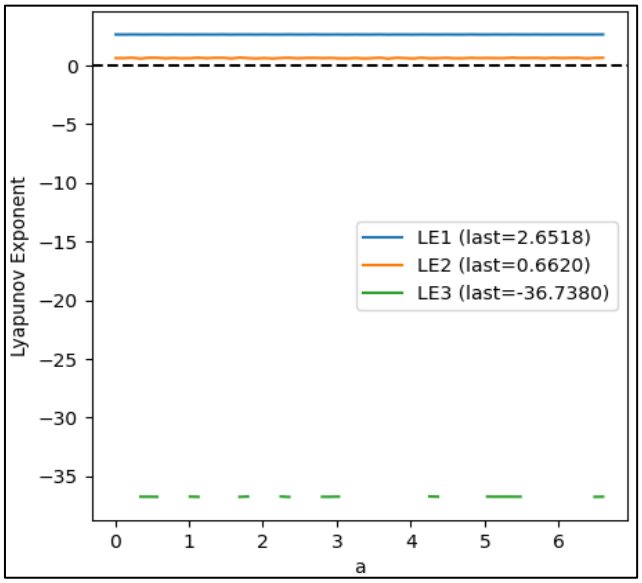


(d)

© Mehran University of Engineering and Technology 2025

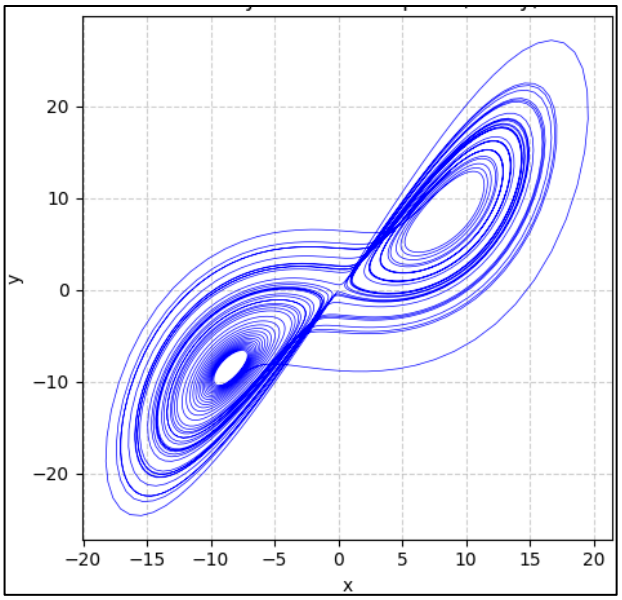


(e)

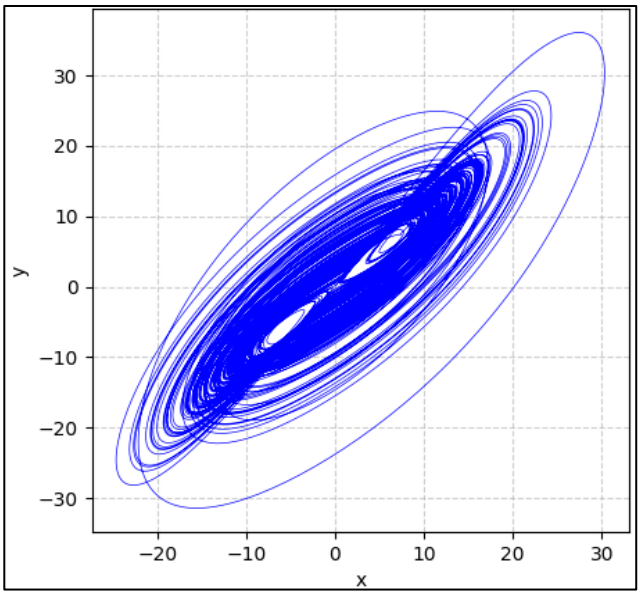


(f)

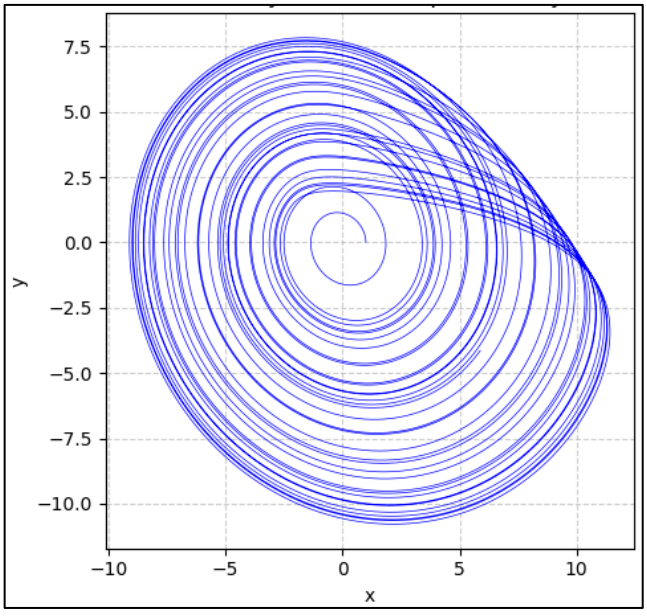
Fig. 2. LE graphs of maps (a) Sine, (b) AZ, (c) Lorenz (d) Chen, (e) Rossler, and (f) Proposed RAM chaotic map



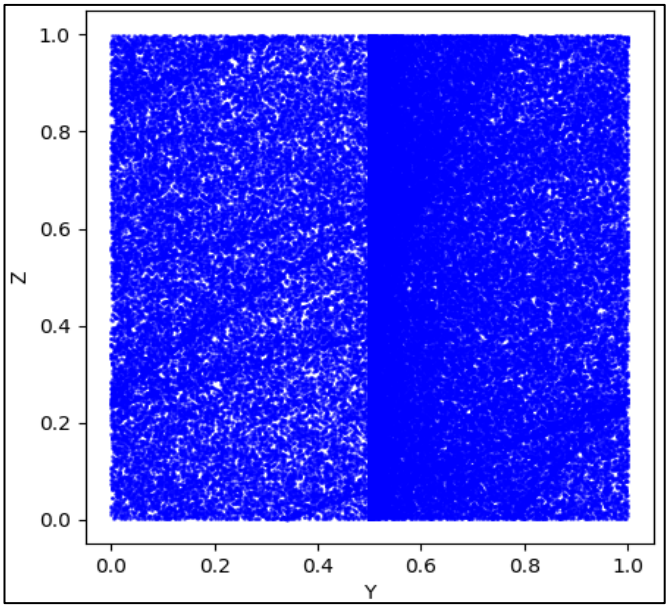
(a)



(b)



(c)



(d)

Fig. 3. 2D Phase space diagrams of maps (a) Lorenz (b) Chen, (c) Rossler, and (d) Proposed RAM chaotic map

© Mehran University of Engineering and Technology 2025

`

Another criterion to analyze the effectiveness of a chaotic map is its ergodicity. A chaotic map is said to be an ergodic one if, over time, it explores all the accessible states in its phase space uniformly. This property ensures that the map does not settle into regular or periodic behaviour but instead fully explores its range. It can be verified from Figures 1, 3, and 4 that the Sine map, AZ map, Lorenz map, Chen Map, and Rossler map do not show an ergodic behaviour as these maps do not explore the whole phase space. On the other hand, it is very much evident from the Figures 1, 3, and 4 that the proposed chaotic map fulfills the ergodicity criterion in a very decent manner as it explores all the accessible states in its phase space in a uniform way.

2.2 Initial s-box construction process

Numerous techniques have been presented by the researchers to develop strong S-Boxes. However, modern techniques for S-Box design are based on chaos theory. A novel technique proposed here for creating key-dependent S-Box is also based on this theory and uses the projected RAM chaotic map as given in Equation (1).

The procedure of constructing novel S-Boxes is illustrated through the flowchart of Figure 8. Table 1 presents an example of a preliminary S-box crafted with the assistance of Figure 8 using values of different variables as:

$X_n = 0.345380247732404$, $V_1 = 0.505155755443174$,

$V_2 = 0.668130416269544$, $V_3 = 0.803424240465076$, and, $V_4 = 10754$

Values of these variables are contributed through the cipher key making the resultant S-Box as key-dependent and dynamic.

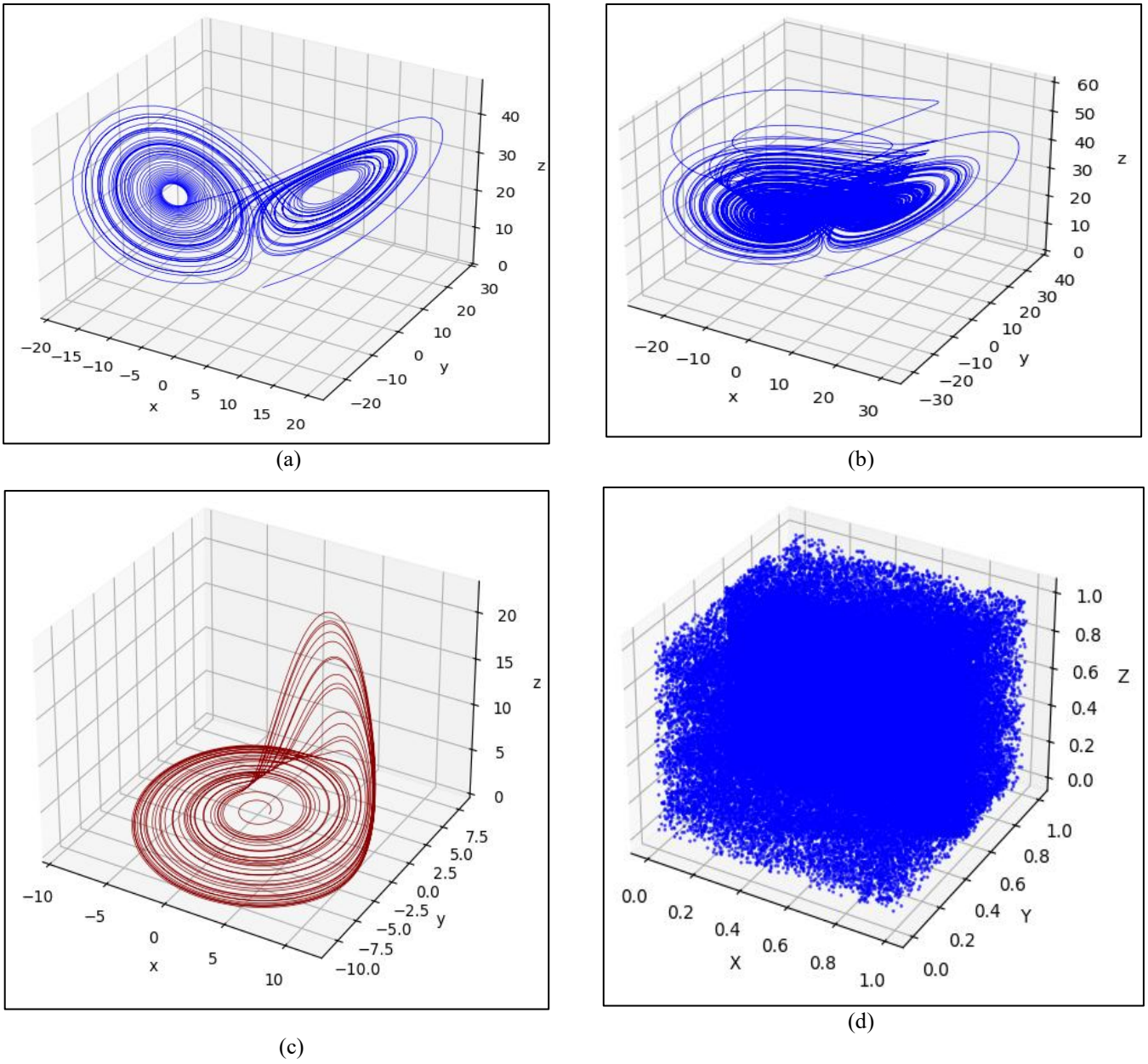
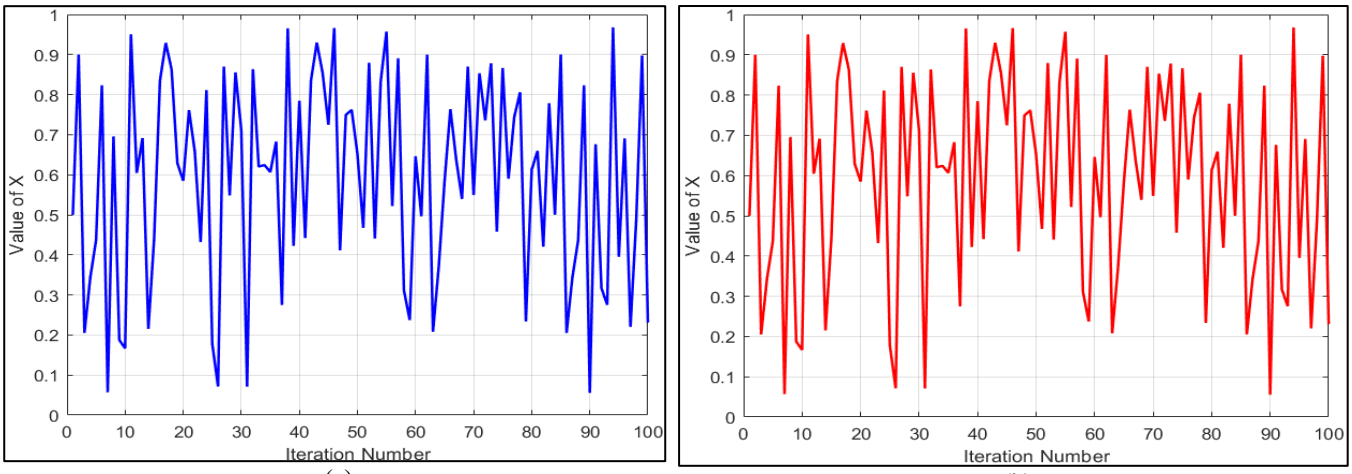
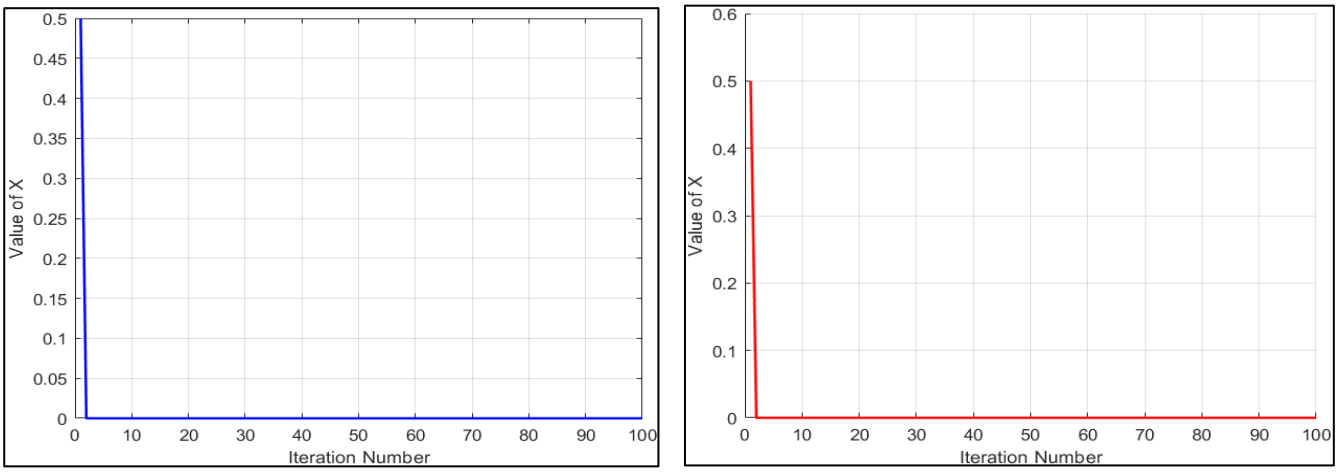


Fig. 4. 3D Phase space diagrams of maps (a) Lorenz (b) Chen, (c) Rossler, and (d) Proposed RAM chaotic map



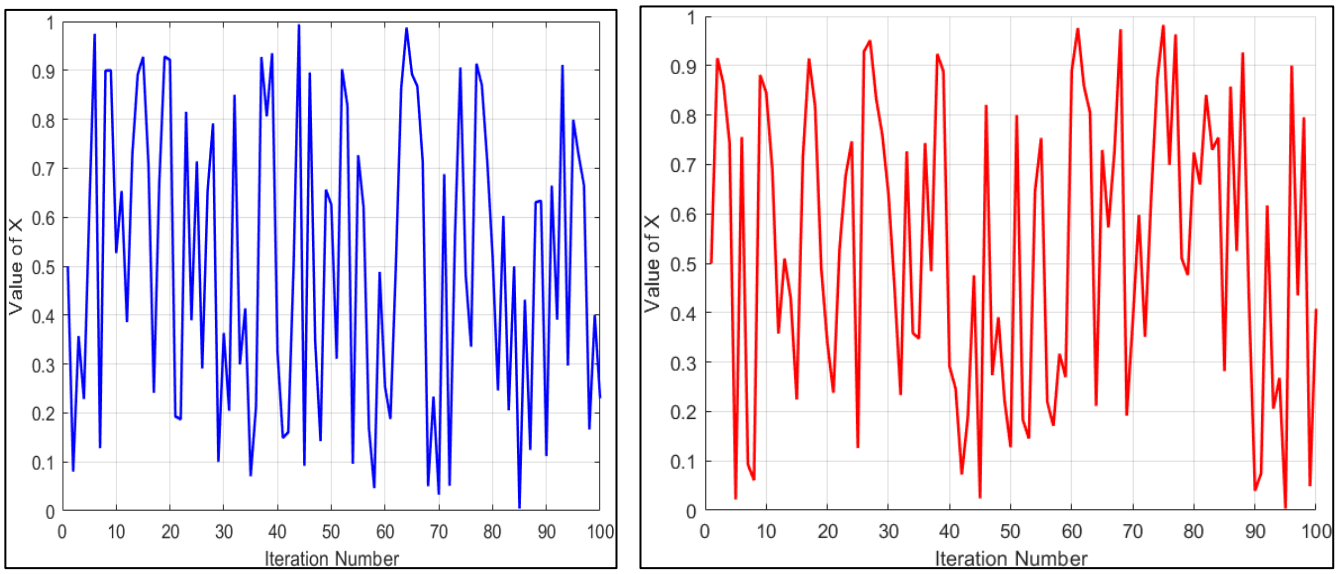
(a) (b)

Fig. 5. Graphs of Sine map with (a) r = 3.9 and X_0 = 0.500000000000000, and (b) r = 3.9 and X_0 = 0.500000000000001



(a) (b)

Fig. 6. Graphs of MAZa map with (a) r = 3.9 and X_0 = 0.500000000000000, and (b) r = 3.9 and X_0 = 0.500000000000001



(a) (b)

Fig. 7. Graphs of proposed RAM map with (a) r = 3.9, V_1 = 0.5, V_2 = 0.5, and X_0 = 0.500000000000000 and (b) r = 3.9, V_1 = 0.5, V_2 = 0.5, and X_0 = 0.500000000000001

2.3 Novel twitching approach for final s-box development

The preliminary S-Box generated using Figure 8 is evolved using a novel twitching method as illustrated in Figure 9 to render the final S-Box. The projected technique uses trigonometric and cubic transformations that assist in the permutation of initial S-Box values and yielding the final S-Box with good

© Mehran University of Engineering and Technology 2025

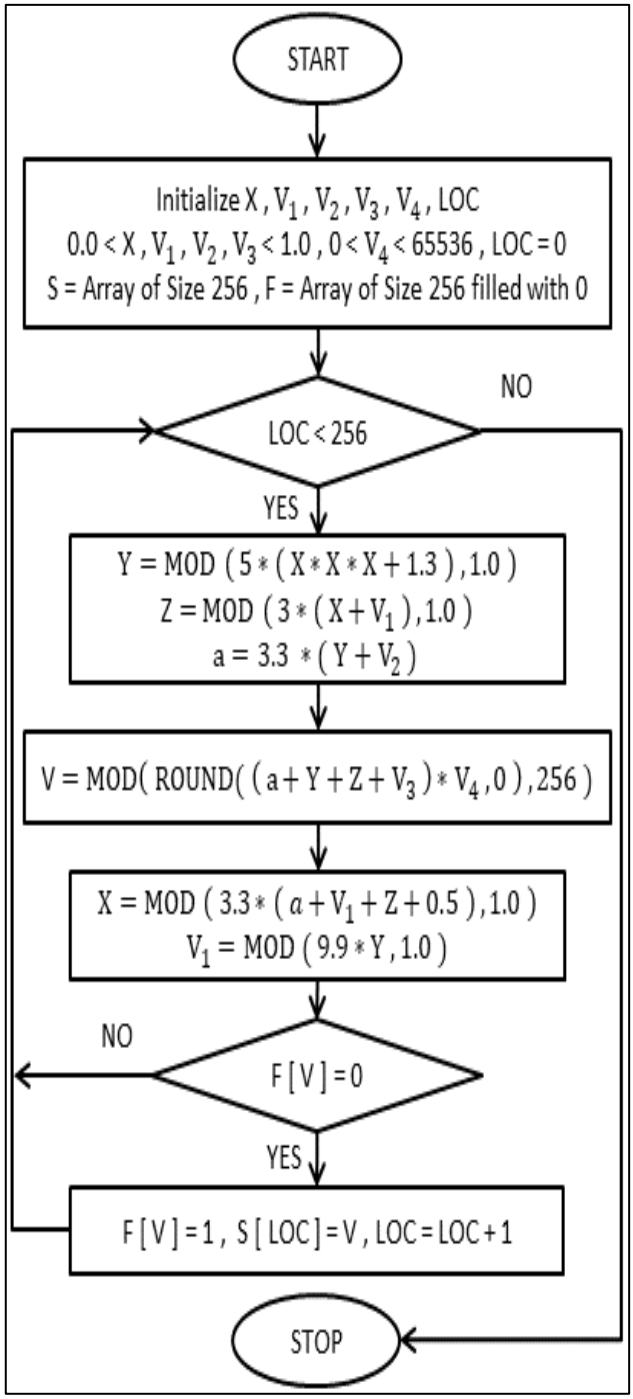


Fig. 8. Proposed Initial S-Box Creation Process

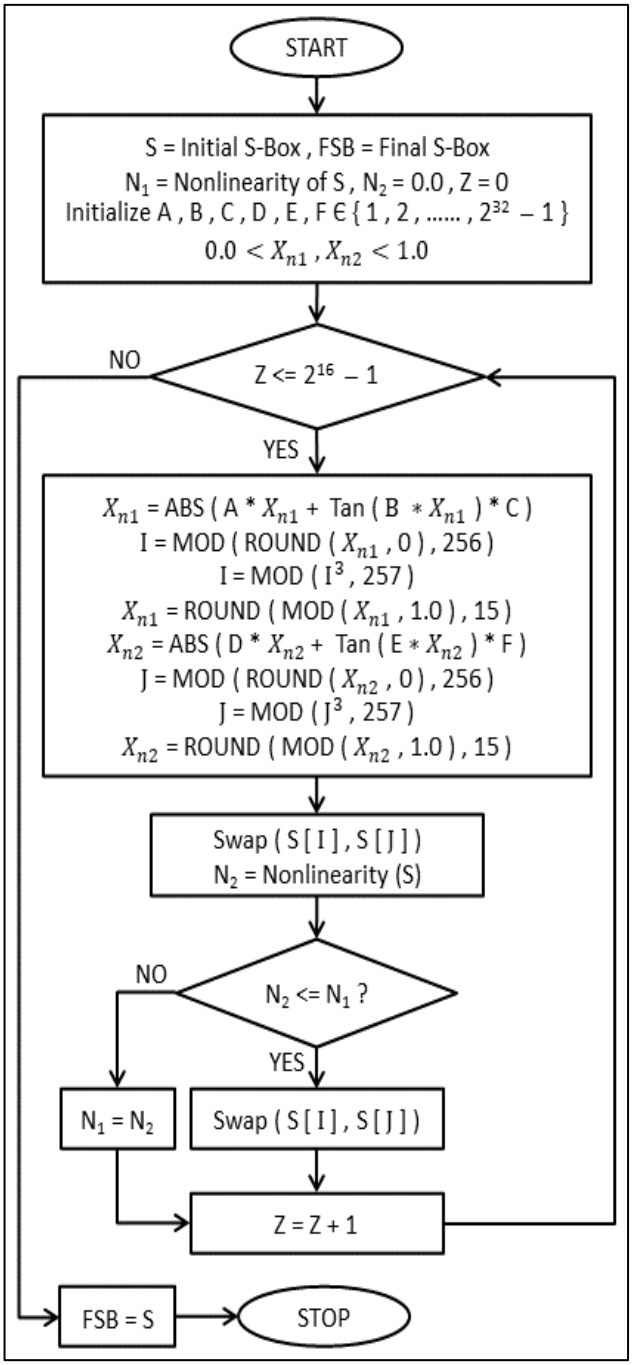


Fig. 9. Twitching Method for Final S-Box Creation

cryptographic strength against various attacks. The proposed twitching approach is dynamic in nature as it receives values of its variables from the cipher key. The proposed permutation technique applied to an initial S-Box leverages trigonometric functions combined with varying system parameters to generate dynamic and nonlinear transformations. By utilizing tangent function, cube of values, and evaluating modulus with prime number 257, the approach ensures a high degree of complexity and unpredictability in the substitution process. This mechanism significantly enhances diffusion, where minor variations in input result in substantial changes in the output. Consequently, it strengthens the cryptographic structure by mitigating predictable patterns and improving resilience against linear and differential cryptanalysis. Moreover, the method achieves this robustness while maintaining computational efficiency.

Table 2 presents an example of a final S-box created with the help of flowchart of Figure 7 using values of different variables as:

A = 57848736, B = 29739234,

C = 3471441, D = 5169737,

E = 20334563, F = 31279874,

X_{n1} = 0.653734141799598, and

X_{n2} = 0.925045503734266

Values of these variables are contributed through the cipher key making the proposed twitching approach as dynamic one.

© Mehran University of Engineering and Technology 2025

Table 1

Proposed Initial S-box

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

Table 2

Proposed Final S-box

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

3. Cryptographic Strength Evaluation of the Proposed S-Box

A significant and highly desired innovation in the field of information security is the invention of New S-Boxes. Most cryptographic algorithms include substitution boxes and contribute largely to increasing the non-linear complexity of the algorithm and its security. Hence, it is a grave challenge to develop new S-Boxes and requires ingenuity and accuracy.

Once developed, such S-Boxes are subjected to intensive and multi-level testing to establish their resistance to a large range of possible attacks. This involves theoretical examination and real-life examination to check whether they are resistant to the different kinds of cryptographic attacks, including differential cryptanalysis, linear cryptography, and algebraic attacks among others. Testing is mechanistic and harsh, and has some strict set of specifications. The

© Mehran University of Engineering and Technology 2025

screening procedure also makes sure that only the best and safest S-Boxes are created. This rigorous testing is required, because it guarantees the S-Boxes are prepared to protect confidential information within a constantly changing background of cryptography threats and malevolent intentions. These highly scrutinized S-Boxes are, therefore, required components in ensuring information systems security and integrity. Such implementation plays the key role in protecting sensitive information as they are the foundations of cryptographic functions used in the process of encryption, decryption, and other security practices. Cyber threats are continuously changing and to enhance the protection of the existing information security systems, new S-Boxes should be designed and seriously tested. Such thorough testing includes some important criteria, which are presented and explained as follows.

3.1 Bijectiveness assurance

For an $m \times n$ S-Box, where m represents the number of input bits while n represents the number of output bits, respectively, that S-Box must map each distinct m-bit input to a distinct n-bit output. This mapping should be one-to-one, i.e., every distinct input should map to a distinct output, a characteristic referred to as bijection. Here, an 8 × 8 S-Box takes an 8-bit input and produces an 8-bit output. Since 8 bits can be utilized to represent 256 values (0 to 255), the S- Box should have 256 distinct output values to attain bijectivity. The provided 8 × 8 S-Box, as shown in Table 2, is a classic example of this bijective property, where every one of the 256 possible unique inputs has a unique output, with a one-to-one relationship.

3.2 Fixed points analysis

The presence of fixed points (FP) within an S-Box is a significant aspect in determining its security. A fixed point in an S-Box B is when the input value x is equal to the output value, i.e., $B(x) = x$ [57]. The existence of fixed points can create vulnerabilities, enabling attackers to exploit the cryptographic system more easily. Fixed points can reveal clues or patterns that can be used to break the ciphertext, thus compromising the security of the encryption process. To confirm the strength and security of an S-Box, it must be tested and verified for the non-existence of fixed points. For the proposed 8 × 8 S-Box of Table 2, a detailed analysis was made to examine the existence of these points. The non-existence of fixed points was proven where no input value maps to itself throughout the entire Table 2.

The result of this thorough analysis ended with the conclusion that there are no fixed points in the S-Box proposed in Table 2. Such an absence of fixed points fully verifies the cryptographic strength of the proposed S-Box

3.3 Nonlinearity

Nonlinearity plays a decisive role in assessing the recital of a substitution box in cryptographic algorithms [20], [21], [22]. An S-Box is a nonlinear constituent used to transform input bits (plaintext) into output bits (ciphertext). The nonlinearity of a substitution box determines its confrontation to linear and differential cryptanalysis, which are common methods used by attackers to break cryptographic systems. Nonlinearity is essential for the effectiveness of S-Boxes in cryptographic algorithms [5]. A high nonlinearity value is indicative of a robust S-Box, providing strong resistance against common cryptographic attacks, thereby contributing to the overall security of the cryptographic system. Equation (2) is used to compute the nonlinearity (NL) of any Boolean function H.

$$\mathrm{NL}\,(\mathrm{H}) = \frac{1}{2}[\,2^{n} - (\,WHS_{max}\,(H\,)\,)\,] \qquad (2)$$

where,

$WHS_{max}\,(H\,)$: Walsh-Hadamard Spectrum of a Boolean function H having n bits.

Table 3

Nonlinearity Scores of the Proposed S-Box

Boolean function	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8
Nonlinearity	112	112	112	112	112	112	112	112

Table 3 shows various Boolean functions of the projected S-Box and corresponding nonlinearity values related to these functions. Table 3 confirms that the minimum, maximum, and average values of nonlinearity ($NL_{min,}$ $NL_{max,}$ and NL_{avg}) of the proposed S-Box are all equal to 112. The values of the projected S-Box are given in addition to those of recently developed S-Boxes in Table 4. An extended analysis of data in Table 4 indicates that the proposed S-Box demonstrates a significantly better resistance to cryptographic attacks, namely linear cryptanalysis. This improved security is reflected by the greater NL (nonlinear) values of the proposed S-Box compare to other S-Boxes. The greater NL score indicate that the proposed S-Box has stronger nonlinearity, which makes it harder for attackers to approximate the behaviour of the S-Box by linear functions, thus enhancing its overall cryptographic resilience.

Table 4

Comparison of Nonlinearity Scores of S-Boxes

S-Box	**NL_{Min}**	**NL_{Max}**	**NL_{Avg}**
[25]	100	108	103.8
[26]	98	106	102.3
[27]	106	110	108.0

© Mehran University of Engineering and Technology 2025

[28]	103	109	104.9
[29]	106	108	106.8
[30]	110	112	111.5
[31]	106	108	106.5
[32]	108	110	109.8
[33]	108	112	109.3
[34]	104	108	106.8
[35]	106	110	108.5
[36]	106	108	106.5
[37]	102	108	105.0
[52]	112	112	112.0
[51]	98	108	103.8
[53]	98	106	103.5
[54]	100	108	103.5
[55]	92	104	101.8
[56]	106	110	107.8
[58]	110	112	110.5
[59]	102	108	104.3
[60]	110	112	110.5
[61]	102	108	105.0
[62]	108	112	110.3
[63]	102	108	104.0
[64]	112	112	112.0
AES	112	112	112.0
Proposed	112	112	112.0

3.4 Strict avalanche criterion

Strict Avalanche Criterion (SAC) is one of the basic principles of cryptography, introduced for the first time by Tavares and Webster [65]. The SAC makes sure that a cryptographic function follows a high level of randomness and unpredictability. That is, SAC demands that a modification in the individual input bit of a function should modify half (50%) of its output bits. This property is important in ensuring the security and robustness of cryptographic algorithms since it makes it difficult for attackers to predict or manipulate the output easily. The SAC value of an S-Box can be assessed through the dependency matrix.

A substitution box is said to be secure under the SAC if its SAC value should ideally be 0.5 [24], reflecting maximum randomness and uncertainty. For the example S-Box of Table 2, the SAC value has been computed and found to be 0.5000. The value is equal to the ideal SAC value of 0.5, which means that the proposed S-Box is effective in satisfying the SAC requirements. The offset from the ideal SAC value, which is termed the SAC Offset, is 0.0. The utility of this offset even more verifies the provision of reliability and security of the suggested S-Box for cryptographic uses.

3.5 Bit independence criterion (BIC)

Webster and Tavares [65] also introduced the Bit Independence Criterion, a crucial standard for evaluating the performance of an S-Box in cryptographic systems. The BIC ensures that modification in input bits leads to alteration in output bits that are independent of each other. This independence is vital for maintaining the security and unpredictability of cryptographic functions, as it prevents patterns from emerging that could be exploited by attackers. The BIC is assessed using the BIC–NL (Bit Independence Criterion-Nonlinearity) and BIC–SAC (Bit Independence Criterion-SAC) values. These values measure how well the output bits maintain nonlinear relationship and independence when input bits are altered. High BIC-NL values and average BIC-SAC value equal to 0.5 indicate a stronger adherence to the criteria, suggesting a higher level of security and robustness.

The proposed S-Box has been evaluated for its BIC-NL and BIC-SAC values respectively. The results show an average BIC-NL score of 103.7 and an average BIC-SAC score of 0.5000. These values reflect the S-Box's capability to maintain bit independence effectively and ensures that the proposed S-Box can resist various forms of cryptanalytic attacks that rely on detecting and exploiting linear relationship and dependencies between input and output bits. These values of the projected S-Box confirm its suitability for use in security related applications, providing a robust layer of defense against potential threats and safeguarding the sensitive data and information.

3.6 Linear approximation probability

In 1993, Matsui introduced a statistical method called linear cryptanalysis to study the vulnerability and robustness of cryptographic algorithms, with the aim of attacking the Data Encryption Standard (DES) [66]. Cryptanalysis using this method exploits the probabilities of direct relationships that exist between the inputs (plaintext, key) and the output (ciphertext) of a cryptographic system. Intruders are able to recognize vulnerabilities within the cryptographic design by analyzing such linear correlations, and infer secret keys as well as breach the system's security. Hence, an S-Box's strength can be measured by the value of the probability of linear relationships (referred to as linear probability) between the input and output bits [49]. The linear probability, the more the S-Box successfully sabotage linear correlation and hence is stronger against linear cryptanalysis.

So, if the calculated linear probability is low, it indicates that the substitution box in question is secure and less vulnerable to exploitation via linear cryptanalysis. The lower probability is a good

characteristic, as it indicates that the S-Box is better able to resist cryptanalytic attacks that attempt to reveal linear dependencies in the cryptosystem. For an n × n S-Box B, its linear probability (LP) value is computed with the help of Equation (3) as described below.

$$\mathrm{LP} = \max_{m_x,\ m_y \neq 0} \left| \frac{\#\{x \in \mathrm{V} \mid \mathrm{x} \cdot \mathrm{m}_x = B(x) \cdot m_y\}}{2^n} - \frac{1}{2} \right| \quad (3)$$

Here,

m_x and m_y represent input and output masks respectively, and V = {0, 1, 2, …, $2^n - 1$}.

The proposed S-Box demonstrates strong resistance to linear cryptanalysis, as evidenced by its low linear probability (LP) value of 0.125. This low LP value indicates minimal linear relationships between input and output bits, enhancing the S-Box's security. Thus, the proposed S-Box effectively disrupts potential linear correlations, making it robust and suitable for secure cryptographic applications.

3.7 Differential approximation probability

After Matsui's linear cryptanalysis, another novel attack method (called differential cryptanalysis) for the Data Encryption Standard (DES) was proposed by Biham and Shamir [67]. This technique exploits the vulnerabilities present in the cryptosystems that utilize operations like substitution and permutation. Differential cryptanalysis is based on the study of differences between corresponding encrypted plaintexts and taking advantage of nonuniformity in the presence of differences between ciphertext and plaintext.

By seeing how small changes in the plaintext affect the ciphertext, an attacker may be able to deduce something about the encryption key. Differential probability (DP) is employed to test the resistance of a substitution box to differential cryptanalysis. Smaller value of DP indicates greater resistance to differential cryptanalysis, as they show a more uniform and random mapping, making it increasingly difficult for the attacker to identify exploitable patterns. Therefore, evaluating the DP value is necessary in determining whether a substitution box is resistant to differential cryptanalysis, thus guaranteeing the security and reliability of cryptographic systems that utilize substitution boxes within their functionality. Equation (4) is employed to compute the differential probability (DP) for an S-Box having 8 x 8 structure.

$$\mathrm{DP} = \max_{\Delta a \neq 0,\ \Delta b} [\#\{a \in \mathrm{V} \mid \mathrm{S(a)} \oplus S(a \oplus \triangle a) = \triangle b\}]/2^8 \quad (4)$$

Here, V is the set of all possible input values.

3.8 Summary of the cryptographic strength of proposed s-box

With respect to several critical criteria, a summary of comparison of the proposed S-Box of Table 2 with various recent S-Boxes is presented in Table 5. The projected S-Box bears the average NL value of 112 that reflects its sublime potential against linear cryptanalysis. A critical analysis of nonlinearity values in Table 5 clearly demonstrates that the proposed S-Box has superior average NL value than its competitors. Similarly, many of the recent S-Boxes of Table 5 have fixed points which make these S-Boxes vulnerable of attacks. On the other hand, the proposed S-Box does not have any fixed point which makes it capable to defy the cryptanalytical efforts. A comparative analysis of the S-Boxes of Table 5 clearly demonstrates that only the projected S-Box has a SAC value of 0.5000 with an offset of 0.0000. This matching of SAC value of the projected substitution box to the ideal value is an indication of the fact that the proposed S-Box has met the SAC requirements effectively. Value of SAC offset being 0.0000 authenticates the provision of security of the projected S-Box to the data. Similarly, the projected S-Box shows decent BIC values with respect to NL and SAC when equated to other recent S-Boxes in Table 5.

An evaluation of LP and DP values of S-Boxes of Table 5 also demonstrate that the proposed S-Box meets these criteria in a sophisticated manner and hence provides a strong shield against linear and differential cryptanalysis.

Table 5
Comparative Analysis of Various S-Boxes

S-Box	NL_{Avg}	FP	SAC	SAC Offset	BIC-NL	BIC-SAC	BIC-SAC Offset	LP	DP
[25]	103.8	0	0.4963	0.0037	103.1	0.4952	0.0048	0.141	0.047
[26]	102.3	1	0.4980	0.0020	103.6	0.4991	0.0009	0.148	0.039
[27]	108.0	1	0.4990	0.0010	104.3	0.4961	0.0039	0.125	0.039
[28]	104.9	3	0.4966	0.0034	103.0	0.5044	0.0044	0.133	0.039
[29]	106.8	2	0.5034	0.0034	103.8	0.5015	0.0015	0.133	0.039
[30]	111.5	0	0.5059	0.0059	104.2	0.5022	0.0022	0.125	0.039
[31]	106.5	2	0.4978	0.0022	104.2	0.5029	0.0029	0.133	0.039
[32]	109.7	0	0.5042	0.0042	109.9	0.5029	0.0029	0.086	0.023

[33]	109.3	0	0.5012	0.0012	108.2	0.5056	0.0056	0.099	0.031
[34]	106.8	0	0.4976	0.0024	103.6	0.5022	0.0022	0.133	0.039
[35]	108.5	1	0.4995	0.0005	103.9	0.5016	0.0016	0.133	0.039
[36]	106.5	0	0.5010	0.0010	104.1	0.5005	0.0005	0.133	0.039
[37]	105.0	1	0.5029	0.0029	102.9	0.5006	0.0006	0.148	0.050
[52]	112.0	1	0.5049	0.0049	112.0	0.5046	0.0046	0.063	0.016
[51]	103.8	0	0.5154	0.0154	103.9	0.4971	0.0029	0.141	0.039
[53]	103.5	3	0.4958	0.0042	103.0	0.5054	0.0054	0.133	0.055
[54]	103.5	0	0.4988	0.0012	103.0	0.4966	0.0034	0.133	0.047
[55]	101.8	1	0.5049	0.0049	103.6	0.5016	0.0016	0.141	0.039
[56]	107.8	1	0.4983	0.0017	104.1	0.5033	0.0033	0.133	0.039
[58]	110.5	2	0.5078	0.0078	103.1	0.5034	0.0034	0.133	0.047
[59]	104.3	1	0.4949	0.0051	103.6	0.5040	0.0040	0.133	0.039
[60]	110.5	2	0.5034	0.0034	103.4	0.5024	0.0024	0.164	0.047
[61]	105.0	0	0.5063	0.0063	104.1	0.5062	0.0062	0.141	0.039
[62]	110.3	0	0.4924	0.0076	110.1	0.5006	0.0006	0.086	0.023
[63]	104.0	0	0.4919	0.0081	103.0	0.5038	0.0038	0.133	0.039
[64]	112.0	1	0.5034	0,0034	112.0	0.5019	0.0019	0.063	0.016
AES	112.0	0	0.5049	0.0049	112.0	0.5046	0.0046	0.063	0.016
Proposed	112.0	0	0.5000	0.0000	103.7	0.5000	0.0000	0.125	0.039

Meeting all the above criteria of cryptographic strength described in Section III in an impressive way with a very decent computational efficiency makes the proposed substitution box a true contender for its application in today's large scale cryptographic systems to protect sensitive data and information from the intruders. Large scale cryptographic systems having many rounds may employ a different S-Box in each of its rounds. Being robust and dynamic in nature, the proposed S-Boxes generated in an efficient way have the capability to provide much needed security to the plaintext of stream ciphers as well as block ciphers which may be the core part of the large-scale cryptographic systems.

3.9 Computational efficiency

The computational efficiency of the projected method for generating the proposed S-Boxes was rigorously and meticulously evaluated on a Windows 10 system equipped with an Intel Core i7 processor (2.2 GHz) and 8GB of RAM, utilizing Visual C# as the programming framework. This innovative method operates in two distinct phases: the generation of initial S-Boxes and their transformation into the final S-Boxes, the latter being fortified through an inventive twitching mechanism designed to amplify the cryptographic strength of the initial S-Boxes. The computational efficiency of the generation of S-Boxes at both the stages was assessed thoroughly.

To validate the method, over one million (10^6) diverse initial S-Boxes were generated using a variety of parameter-driven initializations, with their respective generation times meticulously recorded to evaluate the performance. The same rigorous analysis was extended to measure the total time required for constructing the final S-Boxes to measure the overall efficiency. Insights presented in Table 6 reveal that the generation of initial S-Boxes is exceptionally swift, demonstrating the inherent efficiency of the method. However, the creation of final S-Boxes requires slightly more computational effort due to the involvement of the novel twitching approach to enhance the cryptographic forte of the initial S-Boxes. This novel twitching mechanism, presented first time, represents a transformative step in cryptographic innovation, elevating the robustness of the final S-Boxes while maintaining computational practicality-a feat made even more impressive given the processing power of modern CPUs.

The nonlinearity of the original S-Box is clearly enhanced in the final S-Box, as shown in Figure 10, and has validated the trade-off between the increased security and the computational execution through this method. Subsequently, it highlights the maturity and applicability of the suggested approach to secure confidential data in the modern digital environment.

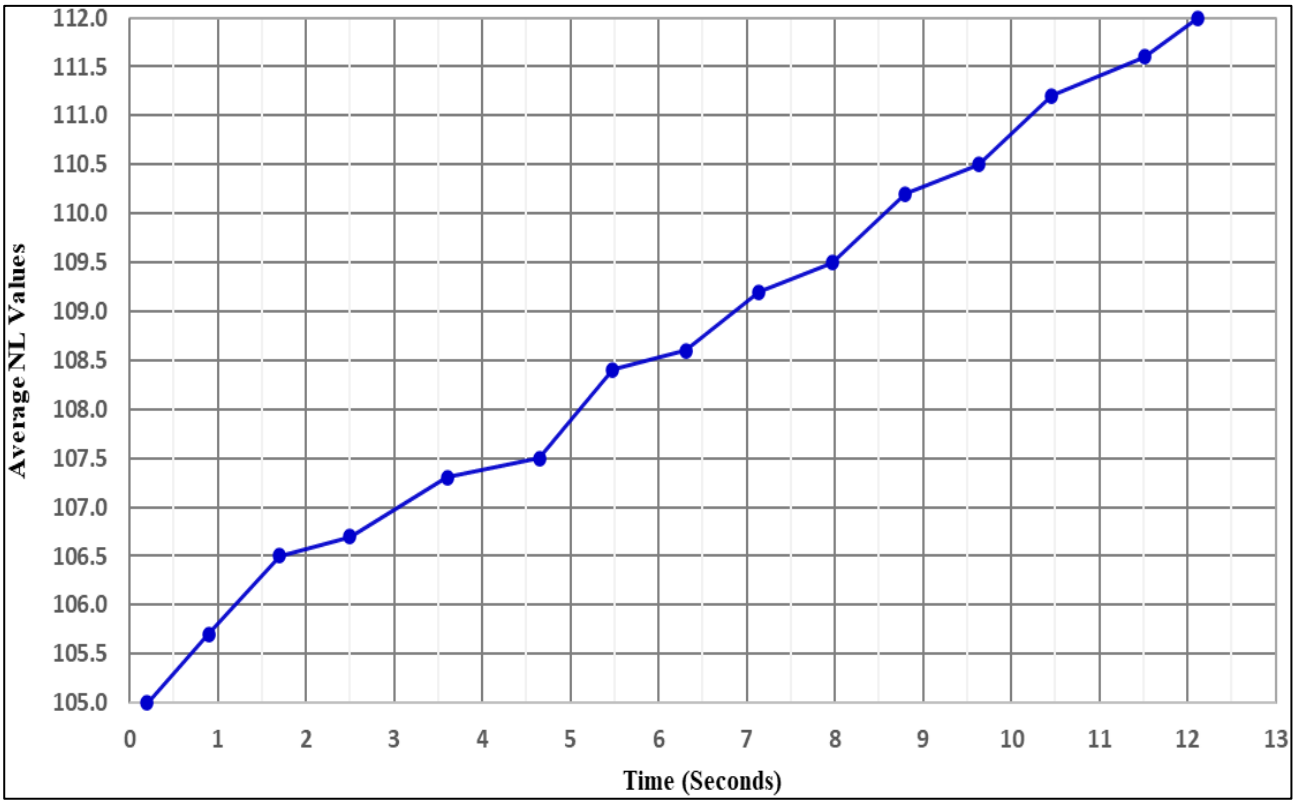


Fig. 10. Temporal Analysis of Nonlinearity Enrichment of Initial S-Box using Novel Proposed Twitching Mechanism

Table 6

Generation Time (seconds) of Various Chaotic Map-based Initial and Final S-Boxes

S-box	Initial S-box	Final S-box
[6]	0.015	13.5
[49]	0.029	12.397
[68]	0.037	13.487
Proposed	0.026	12.119

4 Key Space Investigation

The suggested design brings a key-dependent and dynamic method for S-box generation with a high level of flexibility and variability to the cryptographers. Varying the initial values of various parameters slightly, the suggested method can generate a different S-box in each implementation. Various parameters used in the suggested method, along with their corresponding ranges and key spaces, are outlined in Table 7. The total key space developed by these parameters ensures a strong and flexible S-box generation method for contemporary cryptographic needs. By enabling each parameter to range over its assigned interval, the suggested method ensures that generated S-box is distinctive with every set of values of parameters. This changing behaviour greatly boosts the security of cryptographic systems to make it highly resistant to attacks and enhance cryptographic strength in general.

The key space of our proposed method is extraordinarily vast, measured at approximately $\sim 4.08 \times 10^{152} \sim 2^{506}$. This enormous key space presents a daunting challenge for any invader attempting to crack the system through brute force methods.

Table 7

Key Space for the Proposed Technique

Parameter and Range	Key space
$0.0 < X_n < 1.0$ (15 decimal digits)	10^{15}
$0.0 < X_{n1} < 1.0$ (15 decimal digits)	10^{15}
$0.0 < X_{n2} < 1.0$ (15 decimal digits)	10^{15}
$0.0 < V_1 < 1.0$ (15 decimal digits)	10^{15}
$0.0 < V_2 < 1.0$ (15 decimal digits)	10^{15}
$0.0 < V_3 < 1.0$ (15 decimal digits)	10^{15}
$0 < V_4 < 2^{16}$	~6.55 x 10^4
$0 < A < 2^{32}$	~4.29 x 10^9
$0 < B < 2^{32}$	~4.29 x 10^9
$0 < C < 2^{32}$	~4.29 x 10^9
$0 < D < 2^{32}$	~4.29 x 10^9
$0 < E < 2^{32}$	~4.29 x 10^9
$0 < F < 2^{32}$	~4.29 x 10^9
Total key space	$\sim 4.08 \times 10^{152}$

© Mehran University of Engineering and Technology 2025

5 Conclusion

In this research article, we present an innovative technique for the generation of key-dependent and dynamic substitution box to enhance data security and resist various security attacks. Our approach effort leverages a novel hyperchaotic map and a new dynamic twitching mechanism, that is presented first time, to create a highly resilient S-Box. The inherent traits of the hyperchaotic map ensure a high degree of unpredictability and complexity, making it difficult for attackers to decipher the S-Box through analytical methods. Newly proposed dynamic twitching approach permutes the values of the initial S-Box and significantly enhances the cryptographic strength of the S-Box by ensuring that it remains unpredictable and unique for each instance. To authenticate the efficacy of the proposed substitution box, its cryptographic strength was compared with those of state-of-the-art substitution boxes that involved rigorous testing and analysis, covering a range of cryptographic metrics. The findings affirm that the proposed substitution box exhibits enhanced suitability for present-day cryptographic applications. The key space of the projected technique is particularly enormous and offers an intimidating challenge for any attacker that may attempt a cryptanalytical effort such as brute force. By employing the proposed technique, modern-day cryptographic systems can realize greater security, ensuring the integrity and confidentiality of sensitive data against various types of attacks.

6. References

[1]. E. Shannon, "Communication theory of secrecy systems," Bell Labs Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2]. C. Paar, J. Pelzl, and B. Preneel, Understanding Cryptography, 1st ed. Berlin, Germany: Springer, 2010.

[3]. A. Kadhim and S. Khalaf, "New approach for security chatting in real-time," Int. J. Emerg. Trends Technol. Comput. Sci., vol. 4, no. 3, pp. 30–36, 2015.

[4]. X. Yan, S. Wang, A. A. A. El-Latif, and X. Niu, "Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery," Multimedia Tools Appl., vol. 74, no. 9, pp. 3231–3252, May 2015.

[5]. A. H. Zahid, M. Ahmad, A. Alkhayyat, M. T. Hassan, A. Manzoor, and A. K. Farhan, "Efficient dynamic S-box generation using linear trigonometric transformation for security applications," IEEE Access, vol. 9, pp. 98460–98475, 2021.

[6]. A. Manzoor, A. H. Zahid, and M. T. Hassan, "A new dynamic substitution box for data security using an innovative chaotic map," IEEE Access, vol. 10, pp. 74164–74174, 2022.

[7]. A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," IEEE Trans. Netw. Service Manage., vol. 17, no. 1, pp. 118–131, Mar. 2020.

[8]. L. R. Knudsen and M. J. B. Robshaw, The Block Cipher Companion. Berlin, Germany: Springer-Verlag, 2011.

[9]. A. A. A. El-Latif, X. Niu, and M. Amin, "A new image cipher in time and frequency domains," Opt. Commun., vol. 285, nos. 21–22, pp. 4241–4251, Oct. 2012.

[10]. A. Belazi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Selective image encryption scheme based on DWT, AES S-box and chaotic permutation," in Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Aug. 2015, Art. no. 606610.

[11]. A. K. Farhan, R. S. Ali, H. Natiq, and N. M. G. Al-Saidi, "A new Sbox generation algorithm based on multistability behaviour of a plasma perturbation model," IEEE Access, vol. 7, pp. 124914–124924, 2019.

[12]. A. H. Zahid, A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad, H. S. Alhadawi, and A. A. Abd El-Latif, "A novel construction of dynamic S-box with high nonlinearity using heuristic evolution," IEEE Access, vol. 9, pp. 67797–67812, 2021.

[13]. A. Altaleb, M. S. Saeed, I. Hussain, and M. Aslam, "An algorithm for the construction of substitution box for block ciphers based on projective general linear group," AIP Adv., vol. 7, no. 3, Mar. 2017, Art. no. 035116.

[14]. M. Sarfraz, I. Hussain, and F. Ali, "Construction of S-box based on Mobius transformation and increasing its confusion creating ability through invertible function," Int. J. Comput. Sci. Inf. Secur., vol. 14, no. 2, pp. 187–199, 2016.

[15]. P. Agarwal, A. Singh, and A. Kilicman, "Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant," Adv. Mech. Eng., vol. 10, no. 7, pp. 1–18, 2018.

© Mehran University of Engineering and Technology 2025

[16]. S. Sahmoud, W. Elmasry, and S. Abudalfa, "Enhancement the security of AES against modern attacks by using variable key block cipher," Int. Arab J. e-Tech., vol. 3, pp. 17–26, Jan. 2013.

[17]. M. S. M. Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-Haq, S. N. M. Shah, M. Rehman, and W. Ahmad, "Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices," IEEE Access, vol. 8, pp. 35682–35695, 2020.

[18]. E. M. Mahmoud, A. Abd, T. A. E. El Hafez, and T. A. El Hafez, "Dynamic AES-128 with key-dependent S-box," Int. J. Eng. Res. Appl., vol. 3, no. 1, pp. 1662–1670, Jan./Feb. 2013.

[19]. J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, "An improved AES S-box and its performance analysis," Int. J. Innov. Comput., Inf. Control, vol. 7, no. 5, pp. 2291–2302, 2011.

[20]. A. H. Zahid, M. J. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," Entropy, vol. 21, no. 3, p. 245, May 2019.

[21]. A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," IEEE Access, vol. 8, pp. 150326–150340, 2020.

[22]. A. H. Zahid and M. J. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," Symmetry, vol. 11, no. 3, p. 437, 2019.

[23]. Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," IEEE Access, vol. 8, pp. 25664–25678, 2020, doi: 10.1109/ACCESS.2020. 2970806.

[24]. F. Riaz, "Design of an efficient cryptographic substitution box by using improved chaotic range with the golden ratio," Int. J. Comput. Sci. Inf. Secur., vol. 18, no. 1, pp. 89–94, 2020.

[25]. J. Liu, X. Tong, M. Zhang, and Z. Wang, "The design of S-box based on combined chaotic map," in Proc. 3rd Int. Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE), Apr. 2020, pp. 350–353, doi: 10.1109/AEMCSE50948.2020.00082.

[26]. A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," Eur. Phys. J. Plus, vol. 135, no. 2, pp. 1–13, Feb. 2020, doi: 10.1140/epjp/s13360-020-00187-0.

[27]. S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou, G. Muhammad, M. S. Hossain, and A. M. Abbas, "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," IEEE Access, vol. 8, pp. 160433–160449, 2020, doi: 10.1109/ACCESS.2020.3020746.

[28]. T. Farah, R. Rhouma, and S. Belghith, "A novel method for designing S-box based on chaotic map and teaching-learning-based optimization," Nonlinear Dyn., vol. 88, no. 2, pp. 1059–1074, 2017, doi: 10.1007/s11071- 016-3295-y.

[29]. D. Lambić, "A novel method of S-box design based on discrete chaotic map," Nonlinear Dyn., vol. 87, no. 4, pp. 2407–2413, 2017.

[30]. A. H. Zahid, L. Tawalbeh, M. Ahmad, A. Alkhayyat, M. T. Hassan, A. Manzoor, and A. K. Farhan, "Efficient dynamic S-box generation using linear trigonometric transformation for security applications," IEEE Access, vol. 9, pp. 98460–98475, 2021, doi: 10.1109/ACCESS.2021.3095618.

[31]. D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," J. Inf. Telecommun., vol. 2, no. 2, pp. 181–191, Apr. 2018, doi: 10.1080/24751839.2018.1434723.

[32]. M. Long and L. Wang, "S-box design based on discrete chaotic map and improved artificial bee colony algorithm," IEEE Access, vol. 9, pp. 86144–86154, 2021, doi: 10.1109/ACCESS.2021.3069965.

[33]. H. Zhu, X. Tong, Z. Wang, and J. Ma, "A novel method of dynamic S-box design based on combined chaotic map and fitness function," Multimedia Tools Appl., vol. 79, nos. 17–18, pp. 12329–12347, May 2020, doi: 10.1007/s11042-019–08478-0.

[34]. Z. Jiang and Q. Ding, "Construction of an S-box based on chaotic and bent functions," Symmetry, vol. 13, no. 4, p. 671, Apr. 2021, doi: 10.3390/sym13040671.

[35]. H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, "A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm," Multimedia Tools Appl., vol. 80, no. 5, pp. 7333–7350,

© Mehran University of Engineering and Technology 2025

Feb. 2021, doi: 10.1007/s11042-020-10048-8.

[36]. D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," Nonlinear Dyn., vol. 100, no. 1, pp. 699–711, 2020, doi: 10.1007/s11071-020-05503-y.

[37]. Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," IEEE Access, vol. 8, pp. 54175–54188, 2020.

[38]. K. M. Ali and M. Khan, "A new construction of confusion component of block ciphers," Multimedia Tools Appl., vol. 78, no. 22, pp. 32585–32604, Nov. 2019, doi: 10.1007/s11042-019-07866-w.

[39]. S. Beg, N. Ahmad, A. Anjum, M. Ahmad, A. Khan, F. Baig, and A. Khan, "S-box design based on optimize LFT parameter selection: A practical approach in recommendation system domain," Multimedia Tools Appl., vol. 79, nos. 17–18, pp. 11667–11684, May 2020.

[40]. T. S. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," Multimedia Tools and Applications, vol. 81, no. 1, pp. 20585–20609, 2022.

[41]. Z. Liu, J. Li and X. Di, "A new hyperchaotic 4D-FDHNN system with four positive Lyapunov exponents and its application in image encryption," Entropy, vol. 24, no. 7, pp. 1–28, 2022.

[42]. H. M. Heys, "A tutorial on linear and differential cryptanalysis," Cryptologia, vol. 26, no. 3, pp. 189–221, Jul. 2002, doi: 10.1080/0161- 110291890885.

[43]. M. M. Lauridsen, C. Rechberger, and L. R. Knudsen, "Design and analysis of symmetric primitive," Tech. Univ. Denmark, Lyngby, Denmark, Tech. Rep. 382, 2016.

[44]. L. Li, B. Abd-El-Atty, A. A. El-Latif, and A. Ghoneim, "Quantum color image encryption based on multiple discrete chaotic systems," in Proc. Federated Conf. Comput. Sci. Inf. Syst., Sep. 2017, pp. 555–559.

[45]. A. K. Farhan, R. S. Ali, H. R. Yassein, N. M. G. Al-Saidi, and G. H. Abdul-Majeed, "A new approach to generate multi S-boxes based on RNA computing," Int. J. Innov. Comput., Inf. Control, vol. 16, pp. 331–348, Oct. 2020.

[46]. U. Hayat, N. A. Azam, H. R. Gallegos-Ruiz, S. Naz, and L. Batool, "A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings," Arabian J. Sci. Eng., pp. 1–13, May 2021, doi: 10.1007/s13369-021-05666-9.

[47]. N. A. Azam, U. Hayat, and M. Ayub, "A substitution box generator, its analysis, and applications in image encryption," Signal Process., vol. 187, Oct. 2021, Art. no. 108144, doi: 10.1016/j.sigpro.2021.108144.

[48]. K. Mohamed, M. Nazran, M. Pauzi, F. Hani, H. M. Ali, S. Ariffin, N. Huda, and N. Zulkipli, "Study of S-box properties in block cipher," in Proc. Int. Conf. Comput. Commun. Control Technol., Langkawi, Malaysia, Sep. 2014, pp. 2–4.

[49]. A. H. Zahid, M. J. Arshad, M. Ahmad, N. F. Soliman, and W. El-Shafai, "Dynamic S-Box Generation Using Novel Chaotic Map with Nonlinearity Tweaking," Computers, Materials & Continua, vol. 75, no. 2, 2023.

[50]. K. U. Shahna, "Novel chaos-based cryptosystem using four-dimensional hyperchaotic map with efficient permutation and substitution techniques," Chaos, Solitons & Fractals, vol. 170, p. 113383, 2023.

[51]. I. Hussain, A. Anees, T. Al-Maadeed, and M. Mustafa, "Construction of S-box based on chaotic map and algebraic structures," Symmetry, vol. 11, no. 3, p. 351, Mar. 2019.

[52]. B. Idrees, S. Zafar, T. Rashid, and W. Gao, "Image encryption algorithm using S-box and dynamic Hénon bit-level permutation," Multimedia Tools Appl., vol. 79, nos. 9–10, pp. 6135–6162, Mar. 2020.

[53]. A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," Sci. Rep., vol. 10, no. 1, pp. 1–16, Feb. 2020.

[54]. N. A. Khan, M. Altaf, and F. A. Khan, "Selective encryption of jpeg images with chaotic based novel S-box," Multimedia Tools Appl., vol. 80, pp. 9639–9656, Jan. 2021.

[55]. A. H. Brahim, A. A. Pacha, and N. H. Said, "A new image encryption scheme based on

© Mehran University of Engineering and Technology 2025

a hyperchaotic system & multi specific S-boxes," Inf. Secur. J., A Global Perspective, vol. 32, no. 2, pp. 59–75, Mar. 2023.

[56]. A. Razaq, G. Alhamzi, S. Abbas, M. Ahmad, and A. Razzaque, "Secure communication through reliable S-box design: A proposed approach using coset graphs and matrix operations," Heliyon, vol. 9, no. 5, May 2023, Art. no. e15902.

[57]. R. Anjum, M. Abbas, "Fixed point property of a nonempty set relative to the class of friendly mappings." RACSAM, vol. 116, no. 32, pp. 1–10, 2022.

[58]. Artuğer F., ~~(2024)~~ "A new S-box generator algorithm based on chaos and cellular automata," Signal, Image and Video Processing, vol. 18, pp. 4731–4740, 2024.

[59]. Vijayakumar M, Ahilan A, ~~(2024)~~ "An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map," Ain Shams Engineering J, vol. 15:102620, 2024.

[60]. Artuğer F., ~~(2023)~~ "A new S-box generator algorithm based on 3d chaotic maps and whale optimization algorithm," Wireless Personal Comm, vol. 131, pp. 835–853, 2023.

[61]. Wang M, Liu H, Zhao M., ~~(2023)~~ "Construction of a non-degeneracy 3D chaotic map and application to image encryption with keyed S-box," Multimedia Tools and Appl. Vol. 82, pp. 34541–34563, 2023.

[62]. Zhao M, Yuan Z, Li L, Chen X., ~~(2024)~~ "A novel efficient S-box design algorithm based on a new chaotic map and permutation," Multimedia Tools and Appl. Vol. 83, pp. 64899–64918, 2024.

[63]. Liu H, Liu J, Ma C., ~~(2023)~~ "Constructing dynamic strong S-box using 3D chaotic map and application to image encryption," Multimedia Tools and Appl. Vol. 82, pp. 23899–23914, 2023.

[64]. Khadem B, Zade S. R., ~~(2022)~~ "Construction of side channel attack resistant S-boxes using genetic algorithms based on coordinate functions," J Electr Comput Eng Innovations, vol. 10, pp. 143–152, 2022.

[65]. A. F. Webster, and S. E. Tavares, "On the Design of S-Boxes," in Proc. Conf. Theory Appl. Crypto. Tech.," pp. 523–534, Santa Barbara, CA, USA, August 1986.

[66]. M. Matsui, "Linear Cryptanalysis Method for DES Cipher," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1994, vol. 765 LNCS, pp. 386–397.

[67]. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," J. Cryptology, vol. 4, no. 1, pp. 3–72, 1991.

[68]. A. H. Zahid, H. A. M. Elahi, M. Ahmad, L. A. Maghrabi, and R. S. A. Said, "Secure Key-Based Substitution-Boxes Design Using Systematic Search for High Nonlinearity," IEEE Access, vol. 11, pp. 139745–139758, 2023.

© Mehran University of Engineering and Technology 2025