JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 11 Issue 02
2026
Research Article
https://doi.org/10.56979/1102/2026/1462

Creating an S-Box Using Chaotic Map for Improved Data Security: A Design Approach

Zarsha Nazim[1], Tayyaba Anees[2], Syed Baqar Hussain[2], Amber Sultan[2*], Wajeeha Khalil[3], and Amjad Hussain Zahid[2]

[1]Lahore Garrison University, Lahore, Pakistan.
[2]University of Management and Technology, Lahore, Pakistan.
[3]University of Engineering and Technology, Peshawar, Pakistan.
[*]Corresponding Author: Amber Sultan. Email: amber.sultan@umt.edu.pk

Received: March 03, 2026 **Accepted:** July 20, 2026

Abstract: In this era of digitization, data security is an inherent requirement over public internet. Due to advancement of Artificial Intelligence based attacks, data secuirty has become a challenge. For this purpose, substitution boxes (S-Box) with ciphers are used. Most of the existing S-Boxes use block ciphers that are currently created through chaotic maps. This article presents a dynamic novel technique of creating block ciphers that use innovative chaotic map approach to provide data security and integrity. This approach is initially designed and then tested against recently projected S-Box in fields of Nonlinearity (NL), Bijectiveness, Bit Independence Criterion (BIC), Strict Avalanche Criterion (SAC), Differential Approximation Probability (DP), and Linear Approximation Probability (LP). Time complexity analysis is also performed to evaluate the computational overhead of the proposed S-Box. The results of these Standard Evaluation Criteria signifies this approach to be particularly robust in the act of protection against attempts to cryptanalyze and proves its forte in data encryption and security.

Keywords: S-Box; Cryptography; Chaotic Map; Security

1. Introduction

In this modern era data and information is continuously expanding. Every day new data is being recorded and information is processed [1]. With this rapid expansion of data they are also widely communicated between networks. These networks may be public and there is always a threat of data being stolen and use for malicious acts over these unprotected networks. Sensitive data and information is needed to be protected from attackers while transferring so a number of ways are applied to make this data unreadable or inaccessible for these integrity violators. One of the ways to imply this protection is to use cryptography.

Cryptography is a way to protect data by encrypting it in a form that is not understood using sturdy algorithms called ciphers [2]. These ciphers are further extended into two main categories called stream ciphers and block ciphers. Stream ciphers work by converting the data in a byte by byte / bit by bit manner whereas a block cipher does the same operation in a block or a chunk manner [3]. Stream ciphers are mostly used where the efficiency is not a major concern because this type is slow and has a greater time complexity. While if efficiency is required and quick, secured cryptography is needed block ciphers are the main resource. Block ciphers are widely used these days because of its efficiency, simplicity and ease in implementation. Most popular ciphers like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, RC5, etc. use Block ciphers [4], [5].

A Block cipher employs two of the main ways one is called the Feistel structure and the other one is the substitution and permutation operations. Feistal structure works by dividing the data in parts and performing cryptography on these parts differently. Blowfish, DES, RC5 and RC6 are some example

ciphers that employ the feistal structured manner [6]. The other technique is substitution and permutation which transforms the data/plaintext into a puzzling form not understood by the intruders. A permutation operation is performed when the cipher shuffles or swaps the bit/bytes of the text with each other and a substitution operation works by substituting the bits/bytes with other random bits/bytes that can be a part of the text or not. Some worth mentioning block ciphers that use this method are SHARK, SQUARE, AES, and PRESENT [7].

Those ciphers involving the substitution method often uses more than substitution boxes also called the S-Boxes). A substitution box is one of the vital constituent of a block cipher. It creates mystification between the given simple given text and the ciphertext in a nonlinear fashion. Other components work in a linear fashion whereas an S-Box is the only part of a block cipher that shows nonlinearity. The robustness of an S-Box is directly proportional to the strength of the cryptography. The stronger an S-Box the stronger cryptography it employs and as a result more protected ciphertext is generated. Bit Independence criteria, Resistance to linearity (NL), Differential Linearity (DP) are some of the important properties to be employed in an S-Box that defines its strength. An S-Box having more of these properties the more strength it possesses. A substitution box is further categorized into two main types i.e. static S-Boxes and the dynamic S-Boxes

Static S-Box has fixed information bits and bytes that are replaced every time for the same bits and bytes in the text. The downside of this type is that once an intruder or attacker gets an access of the S-Box it gets the key and can easily decode the text and can take malicious advantage. Some incidents have happened where the attackers got the access of the key of the static S-Box and the integrity of the data was compromised [8]. Such examples include the DES and AES.

To overcome this drawback researchers, encourage the use of dynamic S-Boxes. This type includes a key that is random and hence, this type provides more security to the cipher and greater protection against cryptanalysis. An example that uses this way of producing ciphertext is blowfish. Experts, scientists, researchers are investigating and creating new techniques and ways to generate a more random key fashions for dynamic S-Boxes to increase its robustness and strengthen the cryptography. For this purpose, different algebraic concepts and algorithms are introduced.

One of these algebraic concepts to employ more random key for a stronger, more robust dynamic S-Box is Linear Fractional Transformation (LFT) [9]-[12]. Many researchers have suggested the use of this technique employing Galois Field (GF) [13]. But this technique can be proved inefficient as to calculate the multiplicative inverse of a value using the GF is time consuming and makes the algorithm complex and complicated [14].

Another way to make S-Boxes more dynamic and stronger is to use the chaos system [15]-[22]. It generates randomness in the key of the S-Box hence, creating a robust and non-periodical dynamic S-Box [23]. Hyperchaotic methods creates more studier and vigorous S-Boxes than simple chaotic techniques [24]. It combines chaotic maps with other chaotic algorithms to provoke more cryptography and make cryptanalysis difficult for the attackers [25], [26].

DNA computing is another useful and nowadays more employed technique to create robust dynamic S-Boxes. Their testing has proved efficient in creating strong and secure ciphers and can be a possible solution to achieve cryptographic forte.

Cubic Fractional Transformation (CFT) and Cubic Polynomial Transformation (CPT) are the techniques also suggested by researchers to implement in creation of decent robust dynamic S-Boxes. These transformational techniques are simple, efficient and effective ones to use [27], [28].

Some other ways including the optimization techniques [44], [30]-[32], elliptic curve [33], [34] cellular automata [35] graph theory [36], [37] backtracking, etc. are also methods suggested by analysts and investigators to be considered possible solutions to the drawback of static S-Boxes and in creation of effective dynamic ones.

These are some of the ways to induce strength in dynamic S-Boxes by creating randomness, transformations etc. But these methods are either inefficient or very complex to employ. The main objective of this article to present a simple and efficient way to create robust block ciphers that are secure and difficult to perform cryptanalysis on.

Some criteria was considered while defining the way to create such S-Boxes. It is given as follows:

- Data security enhancement and resistance to cryptanalysis for block ciphers;

- A simple and easy to implement S-Box;
- A dynamic key dependent S-Box that uses sub-keys when encrypting data;
- A substitution box that employs the essential properties like Non-Linearity, Strict Avalanche Criteria, Bit Independence Criteria, Linear Probability, Differential Probability, etc.

2. Projected S-Box

A lot of methods are followed to design secure ciphers that provide the best in cryptographic forte. One of these methods are chaotic mapping. This approach is used to design robust block ciphers that excel in their forte by following the characteristics provided that they are sensitive to initial conditions, random generative behavior, and non-recurrence. On these terms creates an S-Box that shows primary behavior in one of its essential fields i.e. security enhancement of initial input text. Hence, we use this technique to create novel S-Box that provides best of the security to the text. For creation of such S-Box we follow three steps:

- Innovative Chaotic Map Design
- Elementary S-Box Development
- Heuristic Method to create a Final S-Box

These methods and their results are explained in the given sections.

2.1. Innovative Chaotic Map Design

A mathematical equation is given in equation 1 used to design an n x n S-Box using the ingenious method of chaotic map approach:

$$X = (A+X*(3-X)) \text{ MOD } 1 \quad (1)$$

Where, $0 < X<1$ and $1.5<A<2.5$. The values of X and A are provided using a cipher key. This method used for S-Box is subtle to the primary values of the variables provided by the key and hence it's certain in its maximum security against cryptanalytical attacks and its forte in data encryption.

2.1.1. Bifurcation

Bifurcation is the study of the quality and topology change in a system mainly due to change in initial parameters. Dotted lines represents the unstable values whereas, solid lines a representation for stable ones. Usually, a subtle variation in the input variables results in a huge variation in the system's working and an alteration in phase space topology. A comparison of projected work with two commonly used 1-D chaotic maps is given in Figure 1. The first is Logistic map (LM) it gives bifurcation and chaos using the equation 2.

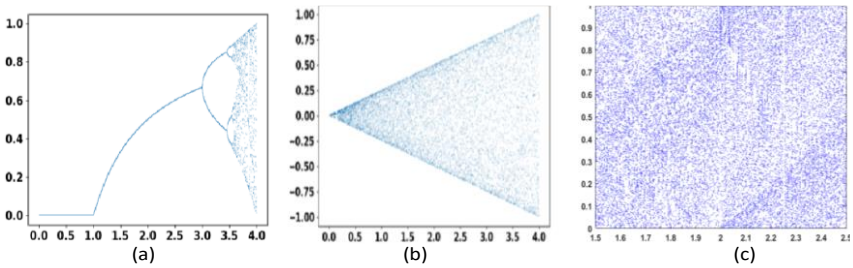

Figure 1. Comparison of Bifurcation diagram of (a) and (b) with projected S-Box (c)

$$x_{n+1} = r * x_n(1 - x_n) \quad (2)$$

Whereas, n gives the iterating number and r provides the control parameter having the limit of [0, 4]. Likewise, another projected map is the Sine Map (SM) given in the equation 3.

$$x_n + 1 = S_\alpha(x_n) = \alpha + sin(\pi * x_n) \quad (3)$$

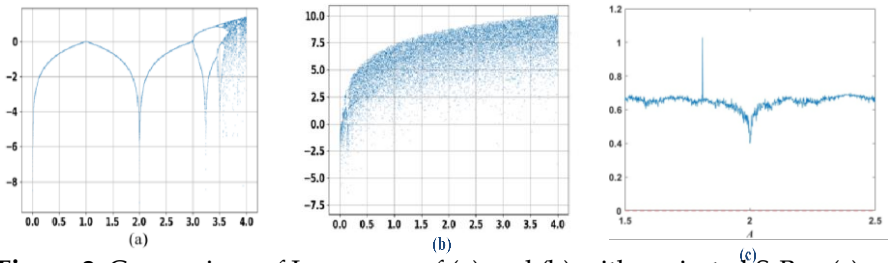

Figure 2. Comparison of Lyapunov of (a) and (b) with projected S-Box (c)

Here, α gives the control parameter within the limit [0, 4]. The comparison of resultant graphs of these two chaotic map designs with the projected one in the following figure shows that the projected one offers more chaos in the field and gives more regions of space than the other two.

Algorithm 1: Construction of initial S-Box

Input:
X // 0< X <1
A // 1.5<A<2.5
Output:
SB //Array of size 256
Initialization:
X,A,B and Loc=0
Procedure:
*WHILE (*Loc <= 255*) DO*
X=(A+X*(3-X)) MOD 1
V=(X*B)MOD 256
S[Loc] ← *X*
Loc ← *Loc + 1*
END WHILE
F[X]=0
S[Loc]=X
F[X]=1
Loc=Loc+1

Algorithm 2 Heuristic Method for Final S-Box Generation

Input Parameters:
$\mathbf{0 < X_n < 1}$
z=0
SB=Array of size 256
Output:
F // Final S-Box
Initialization:
Z<=$\mathbf{2^{16}}$-1
Procedure;
WHILE (Z<=$\mathbf{2^{16}}$*-1) DO*
I ← *MOD (Round(Xn * (A1 * B1) + C1, 0)) , 256)*
J ← *MOD (Round(Xn * (D1 * E1) + F1, 0)) , 256)*
SB[I] ←→ *SB[J]* // Swap values
N1=Non Linearity(SB)
N2=0
IF (N2 <= N1) THEN
SB[I] ←→ *SB[J]*
ELSE N1 ← *N2*
END IF Z = Z + 1
END WHILE
F ← *SB*
RETURN *(F)*

2.1.2. Lyapunov Exponent

This exponent is employed to characterize the degree of chaos in an S-Box. A system is considered to be in a state of chaos if this exponent of a chaotic map is greater than zero. So higher degree of this exponent indicates more chaos, is more secure and harder to perform cryptanalysis on. The value for this variable is calculated through the equation 4:

$$\lim_{t\to\infty} \frac{1}{t} \sum_{i=0}^{t-1} \text{Log} \frac{df}{dx} |X = Xi| \quad (4)$$

Figure 2 gives a comparison of graphs produced of the le factor of projected S-Box with recent LM and SM [38], [39]. Through the calculations performed using this equation it becomes evident that the LE of presented S-Box is much more than as of the ones put in comparison and this is an indication of chaos in the system. And as a conclusion it can be stated that projected technique of S-Box provides greater security and more chaos in encrypted for. The algorithm given below is for constructing the presented S-Box. Firstly, the input and output parameters are indicated in the algorithm then further step of process are defined with initial beginning with defining the number of iterations and the last one proposing a creation of 8 x 8 table representing the S-Box.

2.2. Elementary S-Box Development

A preliminary S-Box was initially developed. Given algorithm 1 above, based on the original equation produces an elementary S-Box. The flowchart is projected in figure 3 below that explains the construction of an elementary S-Box. An example for values generated by the initial S-Box by considering Z = 2.210257908194450, B = 943401158 and Xn = 0.931900959430216.

2.3. Novel Heuristic Method for Final S-Box Generation

The elementary S-Box given is applied using the heuristic method and concluded in algorithm 2 and it is employed to create the final S-Box. Using the cipher key values are included. Here the values are supposedly taken for the sake of calculations, A = 45673, B = 43201, c = 19327, and D = 41237 and Xn = 0.357399447531846. The heuristic method was then used to process the previously drawn results of the elementary S-Box and a final S-Box is concluded. Figure 4 shows the final s-box construction in flowchart.

3. Security Assessment of Projected S-Box

An S-Box needs to be proved secure enough to defy attackers and all such attempts of illegal cryptanalysis. An S-Box in order to excel its forte has to fulfill a checklist of standard evaluation criteria

(SEC). This criteria is used globally to appraise the security of concerned S-Boxes. A list of recently presented S-Box methodologies is reviewed and compared with cryptographic properties of the projected s- box in this article.

3.1. Bijectiveness

This evaluation property of S-Boxes requires a map of initial values provided as input of 8 bits to a distinctive result of 8 bits for a S-Box of 8x8. This means there should be one-to-one mapping, no key for bits of input should be similar to the key for bits of output. This demands uniqueness. So, for the 8x8 projected S-Box all the inputs of 256 bits has a key of 256 all unique bits of output [0,1,……..,255]. The presented S-Box fulfills this criterion of bijectiveness. The resultant Total Fixed Points and Total Opposite Fixed Points turn out to be zero.

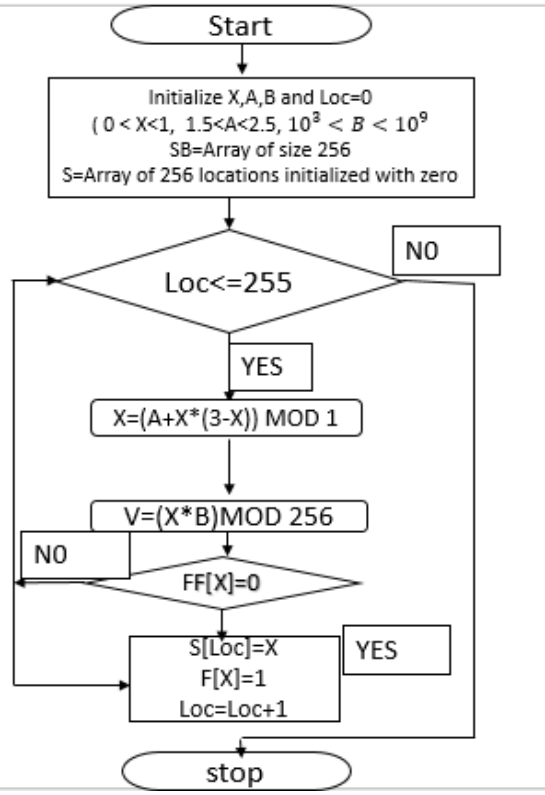

Figure 3. Flowchart of initial S-Box

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

Figure 4. Initial S-Box for projected technique

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

Figure 5. Heuristic Method of S-Box for projected technique

3.2. Non linearity (NL)

An S-Box should convert the n-bits of input into n-bits of output in a highly nonlinear fashion to prove its cryptographic strength. The more the non-linearity the stronger cipher text is generated and more resilient it is against linear cryptanalytical attacks. Walsh-Hadamard Transformation ($W_{max}B$) provides the equation 5 for non-linearity comparison i.e.

$$NL(B) = \left[2^n - \left(W_{max}(B)\right)\right]\frac{1}{2} \quad (5)$$

Here B is an n-bit Boolean function. Non-linearity score is generated using this equation. If an S-Box has high score it means, it's highly nonlinear and provides good protection to the data.

Table 1. Nonlinearity (NL) values of projected S-Box

Bool Function	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**
Non Linearity	104	110	100	106	108	108	108	104

Table 2. Nonlinearity (NL) comparison with recent S-Boxes.

S-BOX	**Average**
Projected	109.75
[19]	106.8
[22]	106.8
[32]	106.5
[44]	106.30
[45]	105.25
[46]	108.50
[47]	109.75
[48]	107.0
[49]	111.50
[50]	106.75
[51]	106.50
[52]	108.0
[53]	106.0
[54]	106.25
[55]	112.25

0.5156	0.5313	0.5156	0.4375	0.4844	0.5000	0.4375	0.5156
0.4219	0.4531	0.4688	0.4844	0.5000	0.4688	0.5156	0.5156
0.4375	0.4688	0.5156	0.5313	0.5313	0.5313	0.5313	0.4844
0.5000	0.4844	0.5000	0.4688	0.5313	0.5313	0.4531	0.5000
0.5000	0.5156	0.5469	0.5469	0.5313	0.5000	0.4844	0.5469
0.4688	0.5000	0.4063	0.5313	0.5313	0.4531	0.5313	0.4531
0.5938	0.4688	0.4688	0.5156	0.5156	0.4688	0.4375	0.4844
0.5469	0.5000	0.4531	0.5000	0.5156	0.4688	0.4844	0.5000

Figure 6. Strict Avalanche Criterion (SAC) dependency matrix of projected S- box.

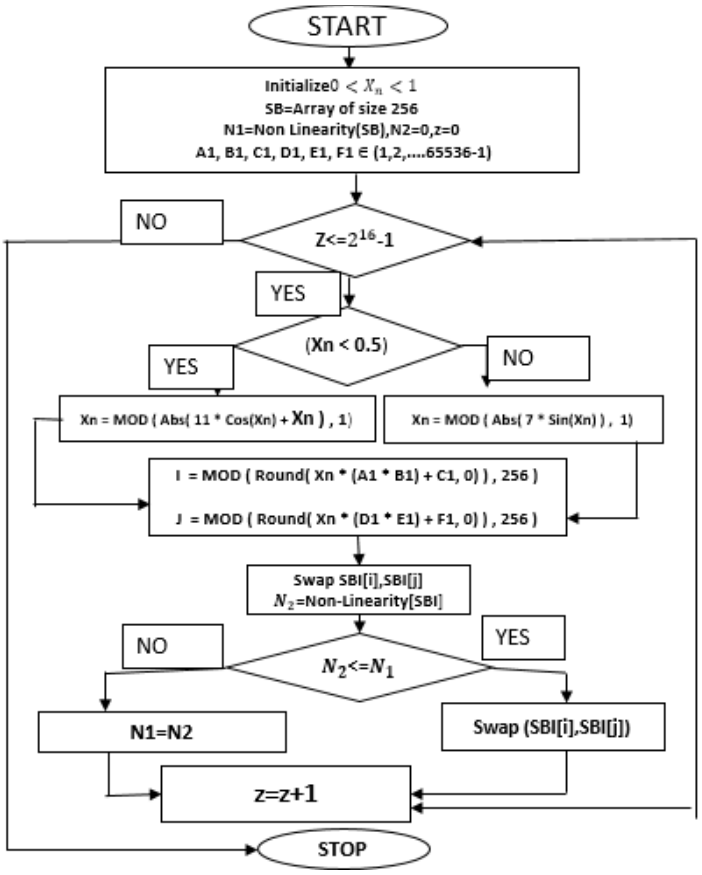

Figure 7. Flowchart of Final S-Box

Table 3. Comparison of SAC and BIC values of S-Boxes

S-BOX	SAC	BIC-NL
Projected	0.4958	103.5000
[19]	0.507	103.9
[22]	0.5000	104.2
[32]	0.4977	104.1
[44]	0.5101	106.25
[45]	0.4990	104.29
[46]	0.4995	104.57
[47]	0.5034	103.8
[48]	0.506	104.2
[49]	0.4978	104.21

[50]	0.5042	110.6
[51]	0.4995	106.35
[52]	0.5034	103.79
[53]	0.4976	102.85
[54]	0.4995	103.85
[55]	0.5010	100

The results given in table 3 provided with an average NL of 109.75 that is considered quite impressive in the factor. The comparison of nonlinearity conclusions in bool functions of presented in table 4 shows given S-Box with the scores of selected S-Boxes revealed about the projected S-Box that it has greater average score than most of the already presented. So, it becomes apparent that projected S-Box checks the box of non-linearity in SEC.

Table 4. BIC-NL values of projected S-Box

0	**102**	**104**	**102**	**108**	**98**	**108**	**98**
102	0	102	106	98	102	104	104
104	102	0	102	102	94	106	104
102	106	102	0	106	106	106	108
108	98	102	106	0	102	108	106
98	102	94	106	102	0	102	104
108	104	106	106	108	102	0	106
98	104	104	108	106	104	106	0

3.3. Strict Avalanche Criterion (SAC)

This criterion presented by Websters says that if a sole bit of data is altered within the input key it produces changes in the 50% of the output key of bites. If an S-Box shows approximate SAC score of 0.5 then it is considered a decently robust. The average SAC value of the projected S-Box turned out to be 0.4871 that is considered a quite good score and proves to be robust one. A SAC score comparison of projected S-Box with is done in table 7 with recently presented S-Boxes and it shows to be quite effective in its robustness than most of them.

3.4. Bit Independence Criterion (BIC)

This criterion given by Websters and Tavares says that the two bit values changed in the output should not be dependent on the single bit change in the initial map of keys. Bit Independence Criterion-nonlinearity (BIC-NL) and Bit Independence Criterion- Strict Avalanche Criterion (BIC-SAC) of the projected S-Box is given in table 5 and table 6 and giving an average score of 103.5000 and 0.4958 as shown in table 7. It shows that there is little to no dependency of the output bits on the changed input bit.

3.5. Linear Approximation Probability (LAP)

A strong cipher creates muddled ciphertext that is almost impossible for the attackers to track and get an access to the input that is the plain text. Every S-Box developer wants to achieve this jumble of output from plain input and is created through a nonlinear conversion of input to output. The more non-linearity the more it is difficult for the attackers to perform linear cryptanalysis on the data and this forte assessment for low probability of linearity is given by equation 6:

$$LP = \max_{rx,ry\neq 0} \frac{1}{2}\left|\frac{\#\{x \in A | x.r_x = S(x).r_y|\}}{2^{n-1}}\right| - 1 \quad (6)$$

Where R= {0, 1, . . . , $2^n - 1$} and r_x, r_y= input and output mask.

3.6. Differential Uniformity (DU)

There should be a uniformed changed in the respective output if there is a change made in the input/ plaintext this is called differential uniformity. If there is some non-uniformity or evident variations in the output key the attackers might capture it and upon careful analysis they can easily get an access to the original data and exploit it. S-Box developers attempts to reduce the difference among the two variations and make it uniform. This difference is calculated through evaluation of DU value given in table 8 for the projected S-Box. To keep from invaders performing the differential analysis, the results of DU of an S-Box

should be minimized to a possible greater extent. The DU of an S-Box can be calculated through the equation 7.

$$DU = \max_{\Delta g \neq 0, \Delta f} [\#\{g \in K \mid S(g) \oplus S(g \oplus \Delta g) = \Delta f\}] \quad (7)$$

Where Δg is the input differential while Δf is the output differntial and here K = {0, 1, ..., 254, 255}. The DU value 0.0469 of presented S-Box suggests that it might be a better solution to cryptography problems and crypt-analytical attacks on text. A comparison of DU value of projected S-Box is done with that of other recent ones in table 9.

Table 5. Differential uniformity values of projected S-Box

6	**6**	**8**	**4**	**8**	**6**	**6**	**6**	**6**	**6**	**6**	**8**	**6**	**6**	**8**	**6**
8	6	6	6	8	6	6	6	6	8	6	6	6	6	6	8
8	6	6	6	8	8	4	6	8	10	8	6	6	6	6	10
6	6	6	8	8	6	6	6	6	6	8	6	6	8	4	6
6	8	6	8	8	6	8	6	8	6	6	6	6	6	6	6
6	8	8	6	8	6	6	8	6	6	6	6	8	6	6	8
8	6	6	8	6	8	6	6	8	6	8	8	8	8	6	8
8	6	6	8	8	6	6	10	6	8	6	6	6	6	10	8
6	6	8	6	8	10	6	6	6	6	6	6	6	10	10	6
8	6	6	6	6	8	6	6	8	6	6	10	6	8	8	6
6	8	6	8	8	6	6	6	6	10	10	6	8	8	8	6
8	6	6	6	8	6	6	6	8	6	6	8	8	8	6	6
6	6	10	8	8	8	8	6	8	6	6	6	8	6	6	6
6	6	6	8	6	6	6	6	8	8	10	10	6	6	6	8
6	6	6	6	6	8	6	6	6	6	8	8	10	8	12	6
6	8	6	6	8	6	8	6	6	6	6	6	6	8	6	0

Table 6. LP and DP values of different S-Boxes

S-BOX	**LP**	**DP**
Projected	0.1328	0.0469
[19]	0.133	0.039
[22]	0.132	0.039
[32]	0.132	0.046
[44]	0.105	0.030
[45]	0.125	0.039
[46]	0.117	0.039
[47]	0.133	0.039
[48]	0.125	0.039
[49]	0.133	0.039
[50]	0.085	0.039
[51]	0.128	0.039
[52]	0.133	0.039
[53]	0.132	0.039
[54]	0.109	0.039
[55]	0.070	0.039

Table 7. Construction time (seconds) for S-Boxes using proposed technique.

Initial s-box	**Final s-box**
0.0469	12.0

Table 8. Range and key space of parameters of proposed technique.

Parameter	**Parameter and Range**	**Key Space**
X	0<X<1.0 (15 decimal digits)	10^15

A	1<A<65536	4.5 x 10^3
B	1<B<65536	4.3 x 10^3
C	1<C<65536	1.9 x 10^3
D	1<D<65536	4.1 x 10^3

3.7. Efficiency Analysis

The efficiency analysis of projected S-box was performed on Microsoft Visual Studio using C# as the coding language. The C# program was run on Windows 8 (64-bit) operating system, having Intel core i7 processor with 4GB RAM. Fair comparison was ensured by using the same software environment and hardware for measuring the execution time.

The efficiency was computed for both initial and final s-box after heuristic evaluation. Firstly, analysis were performed for the cryptographic properties and the execution time of the S-box. Secondly, the final S-box was computed and tested after the application of heuristic approach. Approximately ten thousand initial versions of proposed S-box were generated and their execution time and cryptographic strength was evaluated. Table 10 gives the average value of time complexity tested for both initial and final versions.

It is observed that the time complexity of the initial S-box indicates less execution time as compared to that of final S-box. As the heuristic method is employed the data security is enhanced, which indicates increased cryptographic strength of the proposed S-box, which is the primary goal of any encryption device. Therefore, it is noted that the privacy of the data should not be compromised especially when it contrasts with the factors like CPU speed and time.

Figure 5 gives us the graph that portrays how the cryptographic strength of primary S-box gradually increases in field of nonlinearity as we employ the heuristic approach.

3.8. Key Space

The key space given in our proposed technique helps us to create a new s-box each time due to its property of heavily dependence on external key. It can be observed in table 11 that each key has a parameter range and a specific key space. This huge difference makes the s-box more heavily dependent and on the key and more dynamic in its working.

4. Limitations of Projected Method

A dynamic approach to create a dynamic substitution box was presented in this paper. The technique was also verified across multiple analytical criteria. However, there is always a possibility of mistake and error. This proposed method was compared with recently proposed ones but this comparison only includes Sine and Logistic maps and also it is limited. Extensive comparison always leaves a room for improvement in the proposed method. Also this novel method is a 1-D proposed technique that can limit in functionality for other dimensions of data.

5. Conclusion

This research paper presents a new modular scheme to create dynamic key-dependent S-Boxes. This way of designing S-Boxes of block ciphers is further assessed and analyzed using standard evaluation criteria. The results prove that the method of S-Box creation in this article elegantly fulfills these SEC's that include the DU, FPA, BIC, SAC, LAP and bijectiveness. The projected method of creating a robust S-Box provides decent result figures that fulfills this criterion and it's evident that the projected method is effective in creating strong encrypted output that is difficult to perform cryptanalysis on and hence, provide great security to the data. A comparison of this S-Box created using the projected methodology is also given at points with other recent techniques to create S-Boxes and the statistics are the evidence of the cryptographic strength of the projected one. Moreover, light weight encryption algorithms and real-time secure communication systems can be integrated with the proposed S-box to evaluate its performance in real life applications.

Supplementary Materials: Not Applicable.
Funding: Not Applicable.
Data Availability Statement: Not Applicable.
Acknowledgments: Not Applicable.
Conflicts of Interest: The authors declare no conflict of interest.

References

1. W. Stallings, Cryptography and Network Security Principles and Practices. London, U.K.: Pearson, 2017.
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. K. Mohamed, M. N. M. Pauzi, F. H. H. M. Ali, S. Ariffin, and N. H. N. Zulkipli, ''Study of S-Box properties in block cipher,'' in Proc. Int. Conf. Comput., Commun., Control Technol. (I4CT), Sep. 2014, pp. 362–366
5. M. M. Lauridsen, C. Rechberger, and L. R. Knudsen, ''Design and analysis of symmetric primitive,'' Tech. Univ. Denmark, Kgs. Lyngby, Denmark, Tech. Rep. 382, 2016.
6. K. Mohamed, M. N. M. Pauzi, F. H. H. M. Ali, S. Ariffin, and N. H. N. Zulkipli, ''Study of S-Box properties in block cipher,'' in Proc. Int. Conf. Comput., Commun., Control Technol. (I4CT), Kedah, Malaysia, Sep. 2014, pp. 2–4.
7. A. H. Zahid, A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad, H. S. Alhadawi, and A. A. A. El-Latif, ''A novel construction of dynamic S-Box with high nonlinearity using heuristic evolution,'' IEEE Access, vol. 9, pp. 67797–67812, 2021.
8. A. Alabaichi and A. I. Salih, ''Enhance security of advance encryption standard algorithm based on key-dependent S-Box,'' in Proc. 5th Int. Conf. Digit. Inf. Process. Commun. (ICDIPC), Sierre, Switzerland, Oct. 2015, pp. 7–9.
9. S. Farwa, T. Shah, and L. Idrees, ''A highly nonlinear S-Box based on a fractional linear transformation,'' SpringerPlus, vol. 5, no. 1, Dec. 2016, Art. no. 1658.
10. I. Hussain, T. Shah, M. A. Gondal, M. Khan, and W. A. Khan, ''Construction of new S-Box using a linear fractional transformation,'' World Appl. Sci. , vol. 14, no. 2, pp. 1779–1785, 2011.
11. 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.
12. 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.
13. K. Kobayashi, N. Takagi, and K. Takagi, ''An algorithm for inversion in GF(2m) suitable for implementation using a polynomial multiply instruction on GF(2),'' in Proc. 18th IEEE Symp. Comput. Arithmetic (ARITH), Jun. 2007, pp. 105–112.
14. M. Saeed and M. S. Mian, ''Methods of finding multiplicative inverses in GF(28),'' Comput. Commun., vol. 31, no. 17, pp. 4117–4123, Nov. 2008.
15. S. Garg and D. Upadhyay, ''S-Box design approaches: Critical analysis and future directions,'' Int. J. Adv. Res. Comput. Sci. Electron. Eng., vol. 2, no. 4, pp. 426–430, 2013.
16. G. Jakimoski and L. Kocarev, ''Chaos and cryptography: Block encryption ciphers based on chaotic maps,'' IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol. 48, no. 2, pp. 163–169, Feb. 2001.
17. F. Özkaynak, ''Construction of robust substitution boxes based on chaotic systems,'' Neural Comput. Appl., vol. 31, no. 8, pp. 3317–3326, Aug. 2019.
18. M. Ahmad, H. Haleem, and P. M. Khan, ''A new chaotic substitution box design for block ciphers,'' in Proc. Int. Conf. Signal Process. Integr. Netw., Delhi, India, Feb. 2014, pp. 255–258.
19. D. Lambić, ''A novel method of S-Box design based on discrete chaotic map,'' Nonlinear Dyn., vol. 87, no. 4, pp. 2407–2413, Mar. 2017.
20. A. A. A. EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, ''A novel image steganography technique based on quantum substitution boxes,'' Opt. Laser Technol., vol. 116, pp. 92–102, Aug. 2019.
21. A. A. Alzaidi, M. Ahmad, M. N. Doja, E. A. Solami, and M. M. S. Beg, ''A new 1D chaotic map and β-hill climbing for generating substitutionboxes,'' IEEE Access, vol. 6, pp. 55405–55418, 2018.
22. D. Lambić, ''A novel method of S-Box design based on chaotic map and composition method,'' Chaos, Solitons Fractals, vol. 58, pp. 16–21, Jan. 2014
23. E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, ''A new hyperchaotic system-based design for efficient bijective substitution-boxes,'' Entropy, vol. 20, no. 7, p. 525, Jul. 2018.
24. M. M. Dimitrov, ''On the design of chaos-based S-Boxes,'' IEEE Access, vol. 8, pp. 117173–117181, 2020
25. J. Peng, S. Jin, L. Lei, and R. Jia, ''A novel method for designing dynamical key-dependent S-Boxes based on hyperchaotic system,'' Int. J. Adv. Comput. Technol., vol. 4, no. 18, pp. 282–289, Oct. 2012.
26. E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, ''A new hyperchaotic system-based design for efficient bijective substitution-boxes,'' Entropy, vol. 20, no. 7, p. 525, Jul. 2018.

27. A. H. Zahid, H. Rashid, M. M. U. Shaban, S. Ahmad, E. Ahmed, M. T. Amjad, M. A. T. Baig, M. J. Arshad, M. N. Tariq, M. W. Tariq, M. A. Zafar, and A. Basit, ''Dynamic S-Box design using a novel square polynomial transformation and permutation,'' IEEE Access, vol. 9, pp. 82390–82401, 2021.
28. A. Zahid, M. Arshad, and M. Ahmad, ''A novel construction of efficient substitution-boxes using cubic fractional transformation,'' Entropy, vol. 21, no. 3, p. 245, Mar. 2019.
29. A. Zahid and M. Arshad, ''An innovative design of substitution-boxes using cubic polynomial mapping,'' Symmetry, vol. 11, no. 3, p. 437, Mar. 2019.
30. A. A. Alzaidi, M. Ahmad, H. S. Ahmed, and E. A. Solami, ''Sinecosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map,'' Complexity, vol. 2018, pp. 1–16, Dec. 2018.
31. Y. Wang, K.-W. Wong, C. Li, and Y. Li, ''A novel method to design Sbox based on chaotic map and genetic algorithm,'' Phys. Lett. A, vol. 376, nos. 6–7, pp. 827–833, Jan. 2012.
32. F. Özkaynak, ''On the effect of chaotic system in performance characteristics of chaos based S-Box designs,'' Phys. A, Stat. Mech. Appl., vol. 550, Jul. 2020, Art. no. 124072.
33. 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, Apr. 2017.
34. U. Hayat, N. A. Azam, and M. Asif, ''A method of generating 8 × 8 substitution boxes based on elliptic curves,'' Wireless Pers. Commun., vol. 101, no. 1, pp. 439–451, Jul. 2018.
35. G. Murtaza, N. A. Azam, and U. Hayat, ''Designing an efficient and highly dynamic substitution-box generator for block ciphers based on finite elliptic curves,'' Secur. Commun. Netw., vol. 2021, pp. 1–14, Dec. 2021.
36. B. R. Gangadari and S. Rafi Ahamed, ''Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications,'' Healthcare Technol. Lett., vol. 3, no. 3, pp. 177–183, Sep. 2016.
37. B. N. Tran, T. D. Nguyen, and T. D. Tran, ''A new S-Box structure based on graph isomorphism,'' in Proc. Int. Conf. Comput. Intell. Secur., Beijing, China, Dec. 2009, pp. 463–467.
38. A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shuaib, W. Aslam, and M. Alawida, ''A novel method for generation of strong substitutionboxes based on coset graphs and symmetric groups,'' IEEE Access, vol. 8, pp. 75473–75490, 2020.
39. X. Zhang and Y. Cao, ''A novel chaotic map and an improved chaos-based image encryption scheme,'' Sci. World J., vol. 2014, pp. 1–8, Jan. 2014.
40. P. Zhou, J. Du, K. Zhou, and S. Wei, ''2D mixed pseudo-random coupling PS map lattice and its application in S-Box generation,'' Nonlinear Dyn., vol. 103, no. 1, pp. 1151–1166, Jan. 2021
41. 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.
42. A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, ''Quantuminspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications,'' Sci. Rep., vol. 10, no. 1, p. 116, Dec. 2020.
43. 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, Mar. 2020, Art. no. 118131.
44. A. Belazi and A. A. A. El-Latif, ''A simple yet efficient S-Box method based on chaotic sine map,'' Optik Int. J. Light Electron Opt., vol. 58568, pp. 1–11, 2016.
45. 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
46. 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.
47. 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, Feb. 2021
48. 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
49. 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,
50. 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.

51. 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
52. 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
53. 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
54. 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, 2021
55. 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