IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 May 2022, accepted 7 June 2022, date of publication 17 June 2022, date of current version 19 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3184012

A New Dynamic Substitution Box for Data Security Using an Innovative Chaotic Map

ATIF MANZOOR, AMJAD HUSSAIN ZAHID, AND MALIK TAHIR HASSAN
School of Systems and Technology, University of Management and Technology, Lahore 54700, Pakistan
Corresponding author: Amjad Hussain Zahid (amjad.zahid@umt.edu.pk)

ABSTRACT As the motivations and capabilities of threat actors continue to evolve, providing data security has become more important than ever. For this purpose, different ciphers using various techniques are being developed. Currently, chaotic maps are designed and applied in the development of these ciphers. Modern ciphers utilize a substitution box (S-Box) as a core module to provide data security. In this article, an innovative chaotic map is suggested for the design of new and dynamic S-Box. Criteria like Bijectiveness, Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), Linear Approximation Probability (LP), and Differential Approximation Probability (DP) are used to critically analyze and evaluate the proposed S-Box performance against various attacks. The cryptanalytic strength of the proposed S-Box is equated with freshly designed S-Boxes for its customization in real-life security applications. The comparative analysis gratifies the true potential of the proposed S-Box for its solicitation in data security domain.

INDEX TERMS Chaotic map, substitution-box, cryptography, security applications, threat actors.

I. INTRODUCTION

Data and information communication performs a very active part in this era for everyone. Businesses must share data and information online for their working and day-to-day operations. Secure communication in the public network is the primary concern of every business in the modern era. It has become very necessary to make the data and information resources protected from unauthorized access. Recently, a sudden rise in security incidents on the networks and web has been seen [1]. The need to protect systems, data, and information becomes more critical and evident when data is resident on shared networks [2]. As sensitive data and information are increasingly being communicated over the networks, it requires cryptographic algorithms to ensure the security of these assets. Using encryption, users share their data securely over an insecure network. Attackers try to break the security, and hence different cryptographic algorithms have been designed and implemented to protect the data and information [3], [4]. Cryptanalysis techniques compromise this security and attack the ciphertext to get the original data from it. Systems that use encryption techniques must prevent cryptanalysis. Modern block ciphers having permutation and substitution operations in encryption and decryption phases.

A substitution operation replaces the characters of plaintext with other characters to create meaningless data (ciphertext). This transformation of given data into new data is done in a nonlinear way. With the help of the permutation operation, character positions are changed. A substitution box is a core component of an encryption algorithm and has a key role in encryption of data. It helps in performing confusion of bits using nonlinear transformation [5]. A block cipher based on static S-Box(es) uses the same S-Box(es) every time for the input data. A static S-Box is weak in characteristics that allows attackers to inspect the properties of the captured ciphertext. A dynamic S-Box depends on the key and is stronger and more effective in terms of confusion as compared to a static S-Box [6], [7].

Over the years, cryptography researchers developed many S-Boxes which have used different models like dynamic random growth technique [8], DNA computing [9], [10], optimization techniques [11]–[14], linear fractional transformation (LFT) [15]–[17], cellular automata [18], elliptic curve [19]–[22], etc. Recently, chaotic maps have become extensively pragmatic in the design of novel S-boxes for secure communication [23]–[25]. In [26], authors proposed

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

a new chaos dependent method which is based on affine transformation and rotation of matrices for the construction of sturdy S-Boxes. In [27], an algorithm has been designed consisting of two stages; design of a static S-Box and then dynamic S-Box optimization. The fitness function and the chaotic map are combined to design a robust S-box. Using a chaotic system, a static S-box is generated while using fitness function, it is transformed to a dynamic S-box.

Qing *et al.* [28] proposed a Logistic Sine System (LSS) chaotic map-based S-Box for a secure and efficient image encryption algorithm. This chaotic map provides a wider range of chaos and better properties of the chaotic map. Alghafis *et al.* [29] projected a S-Box which is built on a continuous chaotic system and quantum chaotic map. For improving data randomness efficiency, the quantum logistic map and Rossler chaotic system have been used.

Liu *et al.* [30] anticipated a new chaotic map using an improved coupling quadratic map (ICQM) and backtracking for the design of an S-Box. An improved coupling quadratic map has been designed for good ergodicity and randomness which is tested by using a bifurcation diagram. Riaz [31] proposed an improved chaotic range with a golden ratio for designing an efficient S-Box. The proposed algorithm consists of two functions of a chaotic map with initial parameters and is used for image encryption. Tanyildizi and Ozkaynak [32] proposedf a method using a one-dimensional chaotic map for the production of S-Box. Although, the chaotic maps are being intensively used in the S-box design methodologies, these maps have associated drawbacks too [33].

The quantity of generated S-boxes and performance can be enhanced by transformation methods and optimization algorithms. Zahid *et al.* [34], [35] proposed innovative polynomial techniques along with the novel permutation processes for the development of resilient S-Boxes. These permutation techniques are very simple and efficient.

There is always a need to design new substitution boxes with better and more robust performance. This research article presents the design of a new substitution box for data security to encounter the security attacks using an innovative chaotic map.

The key contributions of this research article are as trails:

- An algorithm based on an innovative chaotic map has been designed to develop an initial substitution-box.
- A new dynamic permutation operation is applied on the initial S-Box for further confusion and better security. Consequently, the permutation process strengthens the security of the encrypted text.
- The cryptographical vigor of the projected S-Box is compared with the cryptographical vigor of the best-known substitution boxes to justify its suitability in modern ciphers.

The rest of the research paper has the description in the following sequence. Section II defines the proposed chaotic map approach for the design of S-Box. Section III narrates a comparison of S-Boxes based on different constructions and respective security analysis. Section IV narrates the limitations of the proposed chaotic map. Section V clarifies the conclusion part.

II. PROPOSED APPROACH FOR S-BOX DESIGN

Recently, chaotic maps have been extensively pragmatic in designing novel S-boxes with good cryptographic characteristics. The main features of a chaotic map are sensitivity of initial conditions, random-like behavior, and non-periodicity. These properties confirm the confusion and diffusion which are the main requirements of cryptographic security. Here, we design an innovative chaotic map for the production of dynamic S-boxes that can be employed in the development of new ciphers. The overall procedure for generating the proposed dynamic and key-dependent S-boxes consists of following three modest steps:

- Ingenious Chaotic Map Design
- Preliminary S-Box Development
- Novel Heuristic Method for Final S-Box Generation

These steps are explained in the following section.

A. INGENIOUS CHAOTIC MAP DESIGN

For the creation of n × n S-boxes, an ingenious chaotic map named as MAZa (Malik, Atif, and Zahid) is designed that is mathematically stated in Equation (1).

$$F(X_n) = X_{n+1} = |MOD(Z * Sin(Y * Sin(W)), 4.0)| \quad (1)$$

where:

$$\begin{aligned} W &= \pi * (1 - X_n) \\ Y &= \pi * (90 * X_n) \\ 0.0 < Z &< 4.0, \text{ and} \\ \pi &= 3.14159265358979 \end{aligned}$$

Cipher key is used to provide the values of the variables X_n and Z as described in Eq. (1). The proposed chaotic map (MAZa) uses these variables as parameters to maximize the power of S-box to minimize the security attacks and is sensitive to initial condition (initial values of variables). Performance of the proposed chaotic map is equated with those of the logistic map and the sine map. We verified that the projected chaotic map has tremendous chaotic complexity using subsequent exploration and comparison.

1) BIFURCATION

Bifurcation is the study of the qualitative and topological change of a system's phase space that arises because of parameters variations and has serious threshold. Stable values are denoted by a solid line and the dotted line shows unstable values. Most of the time, a slight change in parameters origins a severe variation in system performance with phase space topologically altered [36]. Logistic map (LM) is a commonly used 1-D chaotic map that shows bifurcation and chaos. It is

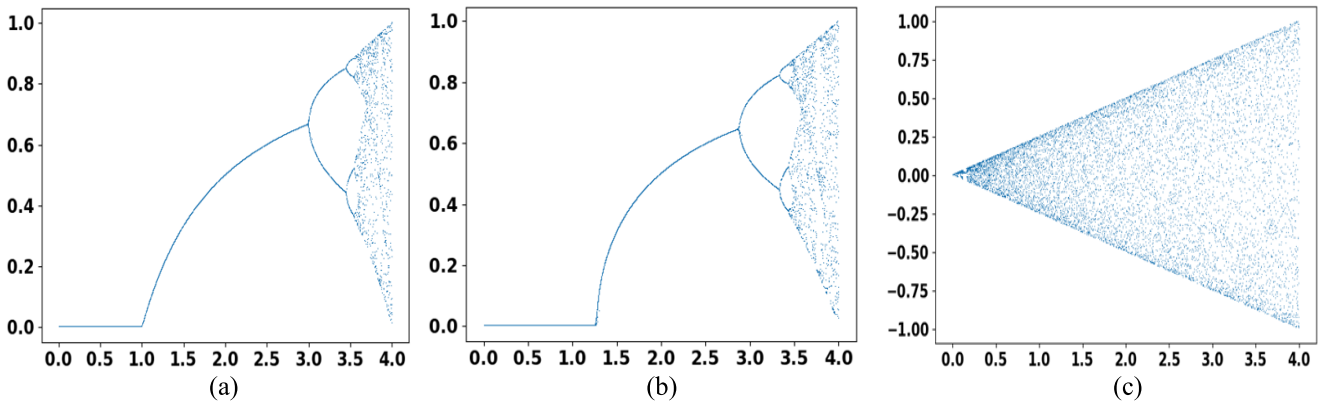

FIGURE 1. Bifurcation results of (a) LM, (b) SM, and (c) Proposed chaotic map.

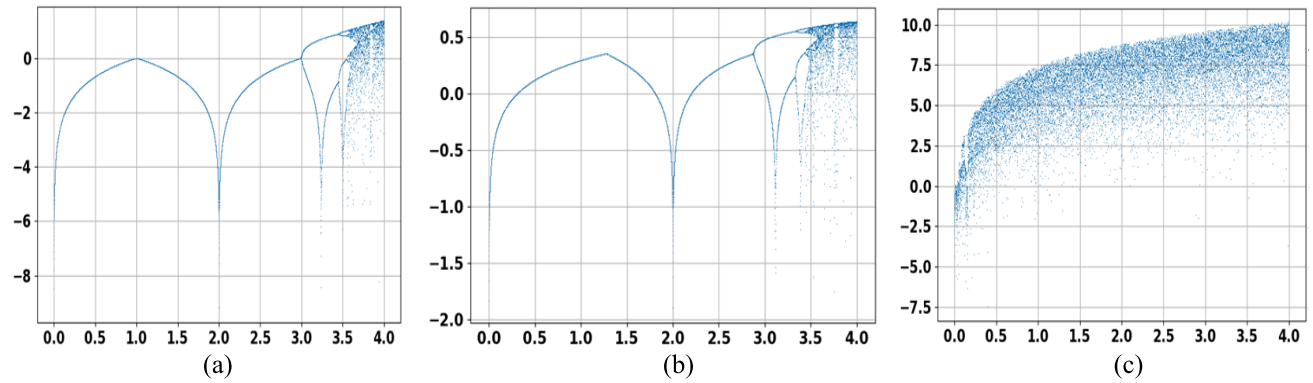

FIGURE 2. Lyapunov exponent results of (a) LM, (b) SM, and (c) Proposed chaotic map.

defined in Equation (2) as:

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

Here, n counts the number of iterations, and the control parameter is r with a limit between [0, 4]. Similarly, Sine map (SM) is a one-dimensional chaotic map that also shows bifurcation and is defined in Equation (3) as:

$$x_{n+1} = S_\alpha (x_n) = \alpha * Sin (\pi * x_n) \tag{3}$$

Here, α is the control parameter in the sine map having a range of [0, 4]. The bifurcation results of all three chaotic maps (LM, SM, and proposed chaotic map) are compared and shown in Figure 1. It is discovered that the bifurcation behavior of the proposed chaotic map is multifaceted and insurances more regions of space than the Logistic and Sine maps.

2) LYAPUNOV EXPONENT

The Lyapunov-Exponent (LE) is an analytical metric that helps to characterize chaos. A system is in a chaotic state if the Lyapunov Exponent of the chaotic map of that system is greater than 0. The larger the value of LE is, the more chaotic behaviour that system exhibits. LE tells us about the rate of convergence or separation of invisibly close trajectories [37], [38]. The Lyapunov Exponent of a chaotic map is calculated using Equation (4).

$$\lim_{t\to\infty} \frac{1}{t} \sum_{i=0}^{t-1} \text{Log} \frac{df}{dx} |x = xi| \tag{4}$$

The derivative equation of the proposed chaotic map as described above is given in Equation (5).

$$F' (X_n) = -\left(\frac{A * D}{4.0}\right) * (C * cos (B) - sin (B)) \tag{5}$$

where:

$$A = 90 * \pi * Z$$
$$B = 90 * (1 - X_n)$$
$$C = 90 * X_n$$
$$D = cos (C * \pi * sin (B))$$

The proposed chaotic mop is more sensitive as compared to the Logistic-map and Sine-map because a minor variation in initial values of the proposed chaotic map has better unpredictability. The Lyapunov Exponent of the proposed chaotic map grows better with an escalation in parameters. It may be observed that LE of the proposed chaotic map is

Algorithm 1 Construction of an Initial S-Box

Input Parameters:
X // $0 < X < 1.0$
Z // $0 < Z < 4.0$
Output:
S, *B* // *Arrays of size 256 each*
Initializations:
Pi ← *3.14159265358979*
Loc ← *0*
Procedure:
WHILE (*Loc* <= *255*) *DO*
W ← PI * (1 − X)
Y ← PI * (X * 90)
X ← ABS (Z * MOD (Sin (Y * Sin (W)), 4.0))
S[Loc] ← X
Loc ← Loc + 1
END WHILE
i ← *0*
WHILE (*i* <= 255) *DO*
MAX ← S [0]
LOC ← 0
j ← 1
WHILE (j <= 255) DO
IF (*MAX* < *S*[*j*]) *THEN*
MAX ← S[j]
LOC ← j
END IF
j ← *j* + *1*
END WHILE
B [i] ← LOC
S [LOC] ← −1.0
i ← i + 1
END WHILE

Algorithm 2 Heuristic Method for Final S-Box Generation

Input Parameters:
A, *C* // $A, C \in \{1, 3, \ldots, 2^{16} - 1\}$
B, *D* // $B, D \in \{1, 2, \ldots, 2^{16} - 1\}$
SB // *Initial S-Box*
Output:
F // *Final S-Box*
Initializations:
Z ← *0*
N_1 ← *Nonlinearity (SB)*
N_2 ← *0.0*
Procedure:
WHILE ($Z <= 2^{16} - 1$) *DO*
I ← ((A * Z^3 + B) MOD 257) + A * Z) MOD 256
J ← ((C * Z^3 + D) MOD 257) + C * Z) MOD 256
SB[I] ←→ SB[J] // Swap values of SB[I] and SB[J]
N_2 = Nonlinearity (SB)
IF (N_2 <= N_1) THEN
SB[I] ←→ SB[J]
ELSE
N1 ← *N2*
END IF
Z = Z + 1
END WHILE
F ← *SB*
RETURN (*F*)

superior to those of the Logistic and Sine maps as shown in Figure 2.

B. PRELIMINARY S-BOX DEVELOPMENT

Algorithm 1, presented below, based on Eq. (1) produces a preliminary S-Box.

Figure 3 depicts the flowchart for construction of an initial S-Box. An example initial S-Box is given in Table 1.

C. NOVEL HEURISTIC METHOD FOR FINAL S-BOX GENERATION

An initial S-Box produced through Algorithm 1 and Figure 3 is processed through a novel heuristic approach presented in Algorithm 2 is used to produce the concluding S-Box. The proposed heuristic approach is dynamic and depends on the parameters' values provided through the cipher key. For the purpose of calculation and demonstration, A = 53591, B = 13555, C = 11379, and D = 46328 are chosen. Using the heuristic process, initial result of S-box is permuted, and the final S-Box is obtained. Algorithm 2 is used for the permutation process for the construction of the final S-Box as given in Table 2.

III. SECURITY ANALYSIS OF PROPOSED S-BOX

A major research contribution in data and information security field revolves around the design of new S-boxes. Once an S-box is designed, it is analyzed to check its capabilities to decides its strength against different attacks (linear and differential).

Evaluation tests for the cryptanalytic of an S-Box is calculated with the predefined criteria that include:

- Bijectiveness
- Nonlinearity (NL)
- Fixed Points (FP)
- Strict Avalanche Criterion (SAC)
- Bit Independence Criterion (BIC)
- Linear Approximation Probability (LP)
- Differential Approximation Probability (DP)

The description of these tests and results for the projected S-Box is as follows.

A. BIJECTIVENESS

This property has the requirement of mapping an input of 8 bits to a unique output of 8 bits for an 8 × 8 S-Box. There must be a one-to-one mapping in the structure of S-Box [39]. There are a total of 256 unique values in the 8 × 8 S-Box table

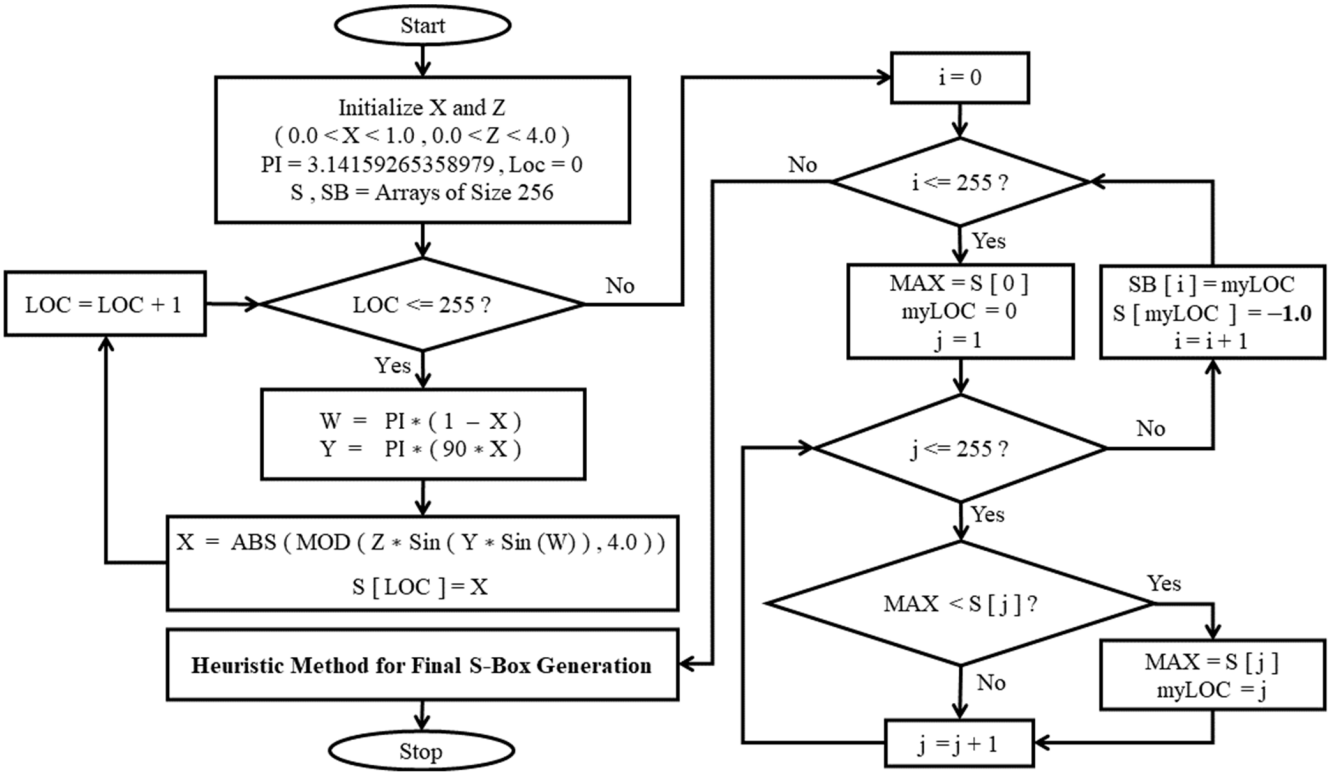

FIGURE 3. S-Box construction process.

TABLE 1. Initial S-Box for proposed technique.

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

TABLE 2. Final S-Box after heuristic method.

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

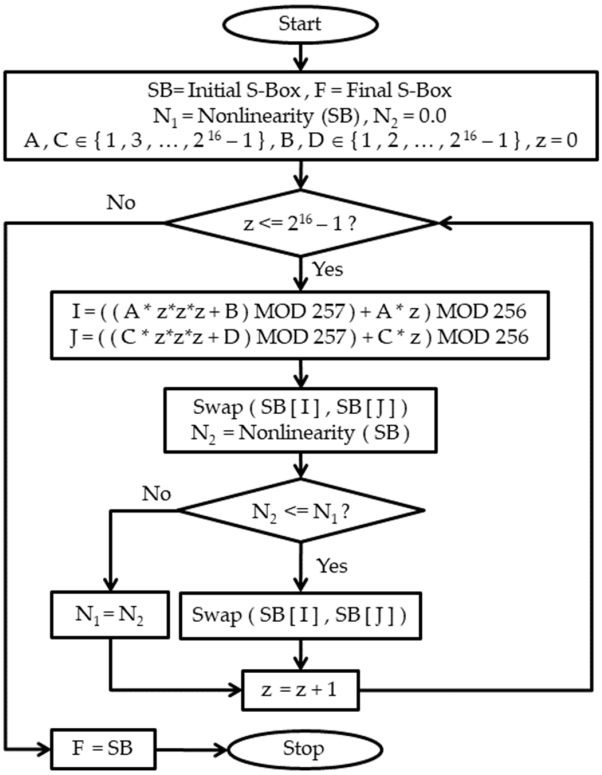

FIGURE 4. Heuristic method for generation of final S-Box.

from {0 to 255}. The proposed S-Box meets this criterion and has all the possible values from 0 to 255.

B. NONLINEARITY (NL)

Nonlinearity is a core parameter in evaluating the performance of substitution boxes [40], [41]. An S-Box is a nonlinear module of any cryptographic algorithm. If an S-Box is constructed in which the relationship amongst plaintext and ciphertext is linear then the S-Box strength against different attacks (linear and differential) is weak. Nonlinearity value must be high for strong confrontation against such attacks [42].

TABLE 3. Nonlinearity values of the proposed S-Box.

Boolean Function	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8
Nonlinearity	110	110	110	110	110	110	112	108

The nonlinearity value of any Boolean function R is calculated using the Equation (6) below.

$$N_L(R) = \frac{1}{2}\left[2^n - (W_{max}(R))\right] \tag{6}$$

Here, W_{max} (R) represents the Walsh-Hadamard transformation spectrum of an n-bit Boolean function R. Boolean functions and nonlinearities values of the projected S-Box are mentioned in Table 3.

Results of nonlinearity test show that $NL_{MIN} = 108$, $NL_{MAX} = 112$, and $NL_{AVG} = 110$ are attained. Table 4 equates NL values of the projected S-Box and recently designed S-Boxes. It can be observed that the average NL value (NL_{AVG}) of the proposed S-Box is higher than the average NL values of most of the other S-Boxes and hence provides a strong defense against the linear cryptanalytic attacks.

C. FIXED POINTS (FP)

An attacker may get the secret data from the captured ciphertext in case of the existence of any fixed point in a

TABLE 4. Nonlinearity (NL) comparison with recent S-Boxes.

S-Box	Minimum	Maximum	Average
Proposed	108	112	110.0
[28]	104	110	106.30
[31]	104	108	105.25
[43]	104	110	106.25
[44]	104	110	107.0
[45]	106	110	108.0
[46]	104	110	106.5
[47]	106	108	106.8
[48]	112	110	111.50
[49]	106	108	106.50
[50]	108	110	109.75
[51]	112	114	112.25
[52]	106	108	106.8
[53]	104	108	106.75
[54]	106	110	108.50
[55]	106	108	106.0

TABLE 5. SAC dependency matrix of proposed substitution box.

0.4844	0.4219	0.5000	0.5000	0.5469	0.4063	0.5156	0.4844
0.4688	0.5000	0.5156	0.5000	0.5313	0.4844	0.4844	0.5313
0.5156	0.5469	0.5313	0.4844	0.4688	0.5313	0.5000	0.5313
0.5469	0.5313	0.4844	0.5156	0.4531	0.4688	0.5469	0.4688
0.5000	0.5313	0.5313	0.5313	0.5156	0.4844	0.5156	0.5625
0.5156	0.5156	0.4531	0.5000	0.5469	0.5625	0.5313	0.5156
0.5313	0.5469	0.5625	0.4531	0.5000	0.5469	0.3750	0.5156
0.4688	0.4844	0.5000	0.4844	0.4844	0.5000	0.4375	0.5156

TABLE 6. BIC-NL values of proposed S-Box.

-	106	106	102	104	100	102	102
106	-	106	104	106	102	106	102
106	106	-	106	96	102	102	104
102	104	106	-	102	106	100	106
104	106	96	102	-	102	106	104
100	102	102	106	102	-	104	104
102	106	102	100	106	104	-	106
102	102	104	106	104	104	106	-

TABLE 7. Comparison of SAC and BIC values of S-Boxes.

S-Box	SAC	SAC Offset	BIC-NL
Proposed	0.5034	0.003	103.5
[28]	0.507	0.007	103.9
[31]	0.5000	0.000	104.2
[43]	0.4977	0.002	104.1
[44]	0.5101	0.010	106.25
[45]	0.4990	0.001	104.29
[46]	0.4995	0.001	104.57
[47]	0.5034	0.003	103.8
[48]	0.506	0.006	104.2
[49]	0.4978	0.002	104.21
[50]	0.5042	0.004	110.6
[51]	0.4995	0.001	106.35
[52]	0.5034	0.003	103.79
[53]	0.4976	0.002	102.85
[54]	0.4995	0.001	103.85
[55]	0.5010	0.001	100

substitution box. As a result, fixed points must not be found in the ultimate S-Box [56]. For security purposes, the proposed S-Box was tested against fixed points criterion. Table 2 shows none of the fixed points in the proposed S-Box.

D. STRICT AVALANCHE CRITERION (SAC)

Strict Avalanche Criterion (SAC) was first introduced by Tavares and Webster [57]. To meet this standard, if one input bit of any cryptographic function is changed, then 50% of the output bits must change. SAC value of SBox can be calculated by the dependence matrix. The dependency matrix of the proposed S-Box is specified in Table 5. The 0.5 is the ideal SAC value for better cryptographic uncertainty. The SAC value of the proposed S-Box is 0.5034 is near to 0.5. Table 7 compares the SAC values of other S-Boxes with the SAC values of the proposed S-Box. It may be observed from Table 7 that the SAC Offset value of our S-box is 0.003 that is very small and hence authenticates the use of the proposed S-box in security related applications.

E. BIT INDEPENDENCE CRITERION (BIC)

Another principle for S-Box performance evaluation is the Bit Independence Criterion (BIC) that was formulated by Tavares and Webster [57]. According to this criterion, if any change occurs in input bits, then output bits should change

TABLE 8. Differential uniformity values of projected S-Box.

8	6	6	6	6	6	6	6	8	6	6	6	8	8	6	6
6	6	8	6	6	6	8	6	10	6	8	6	8	6	6	6
6	6	8	6	8	6	6	6	6	6	6	8	6	6	6	6
6	6	6	8	6	6	8	6	6	6	6	6	6	8	8	8
4	6	6	8	6	6	6	6	6	6	6	10	6	6	6	6
8	8	6	6	6	6	6	6	8	8	6	6	8	8	6	8
6	6	10	6	6	6	8	8	8	6	6	8	6	10	8	6
6	6	8	6	6	6	8	6	10	6	8	6	8	8	6	6
8	6	6	6	6	6	6	6	6	8	6	6	8	8	6	6
8	8	6	6	6	8	6	8	6	8	6	8	6	6	8	6
6	8	6	8	6	6	8	6	6	10	10	8	8	6	6	8
6	8	6	10	8	6	6	10	8	6	10	6	6	6	8	6
6	6	8	6	6	6	6	6	8	6	6	6	6	8	6	6
6	6	8	8	6	8	8	6	8	6	6	8	6	10	6	6
6	8	6	6	10	6	6	6	6	4	4	10	6	4	6	6
8	8	6	8	6	8	8	6	6	6	8	8	8	6	8	0

TABLE 9. LP and DP values of different S-Boxes.

S-Box	LP	DP
Proposed	0.133	0.039
[28]	0.133	0.039
[31]	0.132	0.039
[43]	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

independently. Table 6 demonstrates BIC-NL results of the proposed S-Box. The proposed S-Box average BIC-NL value is 103.5. A comparison of SAC and BIC-NL values of different S-Boxes is given in Table 7.

F. LINEAR APPROXIMATION PROBABILITY (LP)

In 1993, Matsui proposed linear cryptanalysis as a theoretical attack against Data Encryption Standard (DES) [58]. This is a cryptanalysis technique pragmatic to the symmetric-key block ciphers. This method provides a linear approximate expression for a given cipher. Advanced Encryption Standard (AES) was designed by the National Institute of Standards and Technology (NIST) to inhibit linear and such other attacks [59]. If the linear probability (LP) value of an S-Box is found to be low, it indicates that the respective S-Box is resilient to linear cryptanalysis attacks, and vice versa. Linear Probability (LP) value related to a Substitution box is computed by Equation (7).

$$LP = \max_{r_x, r_y \neq 0} \frac{1}{2} \left| \frac{\#\left\{x \in A \mid x \cdot r_x = S\left(x\right) \cdot r_y\right\}}{2^{n-1}} - 1 \right| \tag{7}$$

where:

$$\mathrm{r_x \text{ and } r_y} = \text{Input and output masks}$$
$$\mathrm{A} = \{0, \ldots, 2^{\mathrm{n}} - 1\}$$

LP value of the proposed S-Box is very low, and hence shows its effectiveness against linear attacks. Table 9 gives a comparison of LP values of different S-Boxes.

G. DIFFERENTIAL APROXIMATION PROBABILITY (DP)

Differential cryptanalysis was revealed by Biham and Shamir in 1990 as a new type of attack on the Data Encryption

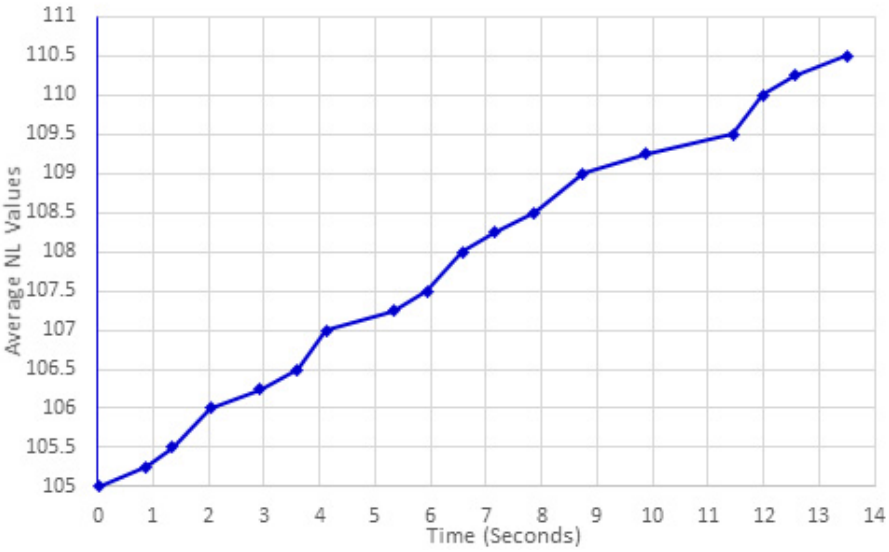

FIGURE 5. Nonlinearity enrichment of preliminary S-box using heuristic technique w.r.t. time.

Standard (DES) [60]. This attack applies to all the ciphers which use DES like substitution and permutation. Differential uniformity (DU) and differential probability (DP) values are used for evaluation of strength of an S-Box against this attack. Equation (8) calculates the differential uniformity (DU) of a given S-Box.

$$DU = Max_{\Delta g \neq 0, \Delta y} \left[\#\{g \in N | S(g) \oplus S(g \oplus \Delta g) = \Delta y\} \right] \quad (8)$$

where 'N' denotes all the possible inputs.

Results of DU of given S-Box are enumerated in Table 8. Proposed S-Box DU value is 0.039 which indicates that the proposed S-Box offers high confrontation against cryptanalysis attacks. A comparison of DP values of different S-Boxes is given in Table 9.

H. EFFICIENCY ANALYSIS

To spectate the computational efficiency of the proposed S-box technique, simulation was done in Visual C# on a system running Windows 8, having 4GB RAM, and 2.2 GHz Intel core i7 CPU (2.2 GHz). Computational efficiency of the proposed method was spectated for both the S-boxes (initial and final). Erection of the final S-box depends on an innovative and heuristic approach to extemporize cryptographic strength of an S-box that is generated initially. 100000 different initial S-boxes were generated to measure their time complexity and the time taken to produce final S-boxes using different initial values of the parameters. Average time complexity of these initial and final S-box constructions is quantified in Table 10.

It may be observed from Table 10 that the construction time of preliminary S-box is handsomely inspirational. However, the final S-box construction time by the proposed technique is a bit higher. Heuristic technique employed in the suggested method has significant contribution to boost the cryptographic strength of the resultant S-box. The protection of one's data is really imperative and a real concern, this requirement of safeguarding data should not be compromised sighting modern-day CPUs' speed. Figure 5 portrays the enrichment in nonlinearity of preliminary S-box by employing innovative heuristic technique against computational time.

TABLE 10. Construction time (seconds) for S-Boxes using proposed technique.

Initial S-Box	Final S-Box
0.015	13.5

TABLE 11. 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}
Z	0 < Z < 4.0 (15 decimal digits)	$4x10^{15}$
A	1, 3, … …, $2^{16} - 1$	~ $3.2x10^{4}$
B	1, 2, … …, $2^{16} - 1$	~ $6.5x10^{4}$
C	1, 3, … …, $2^{16} - 1$	~ $3.2x10^{4}$
D	1, 2, … ….., $2^{16} - 1$	~ $6.5x10^{4}$

I. KEY SPACE

As our proposed technique is key dependent and dynamic, the selection of different initial values of the parameters helps in the generation of new S-box each time. Parameters used in our technique along with their respective range are described in Table 11. Key space for each parameter is also mentioned.

It may be observed that the overall key space of the proposed method is $\sim 1.7 \times 10^{49} \sim 2^{164}$ which is a huge space for any attacker. Consequently, our proposed technique is very much resistant to brute force attempts by invaders.

IV. LIMITATIONS OF PROPOSED CHAOTIC MAP

An innovative chaotic map has been designed for the production of dynamic S-boxes to be employed in the development of new ciphers. One limitation of this chaotic map is that the dimensionality of the map is static (i.e., 1). Consequently, no inferences are made about the scalability of the impacts of chaotic maps on recital with respect to more dimensions. Similarly, a comparison of the proposed chaotic map has been made only with Logistic and Sine maps. A detailed comparison with other chaotic maps may lead to an improvement in this map to yield better results.

V. CONCLUSION

In this paper, a dynamic and key-dependent substitution box has been proposed using an innovative chaotic map and permutation process. Both the chaotic map and the permutation processes are introduced first time and are dynamic in nature. Different parameters used in these processes take their values from the cipher key. A minute change in the set of values always generates a new S-Box. We verified that the proposed chaotic map has tremendous chaotic complexity using subsequent exploration and comparison. The designed S-Box has been evaluated for its cryptographic strength using typical criteria. Along with it, proposed S-box performance is equated with newly developed S-Boxes based on chaotic maps. The comparison ensures that the designed S-Box is suitable for cryptographic applications.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security Principles and Practices*. London, U.K.: Pearson, 2017.

[2] 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, doi: 10.1109/TNSM.2020.2969863.

[3] M. Tanveer, G. Abbas, Z. H. Abbas, M. Waqas, F. Muhammad, and S. Kim, "S6AE: Securing 6LoWPAN using authenticated encryption scheme," *Sensors*, vol. 20, no. 9, pp. 1–23, 2020, doi: 10.3390/s20092707.

[4] L. R. Lauridsen, M. M. Rechberger, and C. Knudsen, "Design and analysis of symmetric primitives," Ph.D. dissertation, Tech. Univ. Denmark, Lyngby, Denmark, 2016.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[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)*, Sep. 2014, pp. 362–366, doi: 10.1109/I4CT.2014.6914206.

[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, doi: 10.1109/ACCESS.2021.3077194.

[8] 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, doi: 10.1109/ACCESS.2020.3016401.

[9] F. A. Kadhim, G. H. A. Majeed, and R. S. Ali, "Proposal new S-box depending on DNA computing and mathematical operations," in *Proc. Al-Sadeq Int. Conf. Multidisciplinary IT Commun. Sci. Appl. (AIC-MITCSA)*, May 2016, pp. 142–147, doi: 10.1109/AIC-MITCSA.2016.7759926.

[10] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "A new DNA-based S-box," *Int. J. Eng. Tech.*, vol. 15, no. 4, pp. 1–9, 2015.

[11] A. A. Alzaidi, M. Ahmad, H. S. Ahmed, and E. A. Solami, "Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map," *Complexity*, vol. 2018, pp. 1–16, Dec. 2018, doi: 10.1155/2018/9389065.

[12] Y. Wang, K.-W. Wong, C. Li, and L. Yang, "A novel method to design S-box based on chaotic map and genetic algorithm," *Phys. Lett. A*, vol. 376, nos. 6–7, pp. 827–833, 2012, doi: 10.1016/j.physleta.2012.01.009.

[13] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7201–7210, 2019, doi: 10.1007/s00521-018-3557-3.

[14] M. Ahmad, M. N. Doja, and M. M. S. Beg, "ABC optimization based construction of strong substitution-boxes," *Wireless Personal Commun.*, vol. 101, no. 3, pp. 1715–1729, 2018, doi: 10.1007/s11277-018-5787-1.

[15] L. C. Nizam Chew and E. S. Ismail, "S-box construction based on linear fractional transformation and permutation function," *Symmetry*, vol. 12, no. 5, p. 826, May 2020, doi: 10.3390/sym12050826.

[16] A. Qureshi and T. Shah, "S-box on subgroup of Galois field based on linear fractional transformation," *Electron. Lett.*, vol. 53, no. 9, pp. 604–606, Apr. 2017, doi: 10.1049/EL.2017.0194.

[17] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic S-boxes based on Mobius transformation and chaotic Tent-Sine system," *IEEE Access*, vol. 7, pp. 173273–173285, 2019.

[18] B. R. Gangadari and S. R. 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, 2016, doi: 10.1049/htl.2016.0033.

[19] 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, doi: 10.1007/s11277-018-5698-1.

[20] N. A. Azam, U. Hayat, and I. Ullah, "An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Dec. 2018, doi: 10.1155/2018/3421725.

[21] 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, doi: 10.1155/2021/3367521.

[22] 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.*, vol. 46, no. 9, pp. 8887–8899, Sep. 2021, doi: 10.1007/s13369-021-05666-9.

[23] M. M. Dimitrov, "On the design of chaos-based S-boxes," *IEEE Access*, vol. 8, pp. 117173–117181, 2020, doi: 10.1109/ACCESS.2020.3004526.

[24] W. Yan and Q. Ding, "A novel S-box dynamic design based on nonlinear-transform of 1D chaotic maps," *Electronics*, vol. 10, no. 11, pp. 1–11, 2021, doi: 10.3390/electronics10111313.

[25] A. Manzoor, M. Hussain, and S. Mehrban, "Performance analysis and route optimization: Redistribution between EIGRP, OSPF & BGP routing protocols," *Comput. Standards Interfaces*, vol. 68, Feb. 2020, Art. no. 103391, doi: 10.1016/j.csi.2019.103391.

[26] 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, doi: 10.1109/ACCESS.2020.2973679.

[27] I. A. Shoukat, U. Iqbal, A. Rauf, and M. R. Faheem, "Randomized substitution method for effectively secure block ciphers in I.O.T environment," *Arabian J. Sci. Eng.*, vol. 45, no. 12, pp. 11019–11036, Dec. 2020, doi: 10.1007/s13369-020-04919-3.

[28] 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.

[29] A. Alghafis, N. Munir, M. Khan, and I. Hussain, "An encryption scheme based on discrete quantum map and continuous chaotic system," *Int. J. Theor. Phys.*, vol. 59, no. 4, pp. 1227–1240, Apr. 2020.
[30] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-box based on chaotic map and backtracking," *Appl. Math. Comput.*, vol. 376, Jul. 2020, Art. no. 125153, doi: 10.1016/j.amc.2020.125153.
[31] 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.
[32] E. Tanyildizi and F. Ozkaynak, "A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838, 2019, doi: 10.1109/ACCESS.2019.2936447.
[33] I. Gagnon, A. April, and A. Abran, "An investigation of the effects of chaotic maps on the performance of metaheuristics," *Eng. Rep.*, vol. 3, no. 8, Feb. 2021, Art. no. e12369, doi: 10.1002/eng2.12369.
[34] 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, pp. 1–13, 2019, doi: 10.3390/e21030245.
[35] 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, doi: 10.1109/ACCESS.2021.3086717.
[36] G. Zhang, W. Ding, and L. Li, "Image encryption algorithm based on tent delay-sine cascade with logistic map," *Symmetry*, vol. 12, no. 3, p. 355, Mar. 2020, doi: 10.3390/sym12030355.
[37] 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, doi: 10.1155/2014/713541.
[38] 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, doi: 10.1007/s11071-020-06098-0.
[39] M. Ahmad, E. Al-Solami, A. M. Alghamdi, and M. A. Yousaf, "Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures," *IEEE Access*, vol. 8, pp. 110397–110411, 2020, doi: 10.1109/ACCESS.2020.3001868.
[40] 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.
[41] 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, doi: 10.1007/s11042-019-08464-6.
[42] Y. Wang, Z. Zhang, L. Y. Zhang, J. Feng, J. Gao, and P. Lei, "A genetic algorithm for constructing bijective substitution boxes with high nonlinearity," *Inf. Sci.*, vol. 523, pp. 152–166, Jan. 2020, doi: 10.1016/j.ins.2020.03.025.
[43] 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.
[44] 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.
[45] 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.
[46] 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.
[47] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, 2017.
[48] 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.
[49] 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.
[50] 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.
[51] 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.
[52] 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.
[53] 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.
[54] 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, doi: 10.1007/s11042-020-10048-8.
[55] 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.
[56] 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, doi: 10.1109/ACCESS.2020.2979827.
[57] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, Santa Barbara, CA, USA, Aug. 1986, pp. 523–534.
[58] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 765, 1994, pp. 386–397, doi: 10.1007/3-540-48285-7_33.
[59] 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.
[60] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991.