IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 November 2023, accepted 27 November 2023, date of publication 4 December 2023,
date of current version 15 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3339389

RESEARCH ARTICLE

Secure Key-Based Substitution-Boxes Design Using Systematic Search for High Nonlinearity

AMJAD HUSSAIN ZAHID[1], HAFIZ ALI MANSOOR ELAHI[2], MUSHEER AHMAD[3], LOUAI A. MAGHRABI[4], (Member, IEEE), AND RAMY SAID AGIEB SAID[5]

[1]School of Systems and Technology, University of Management and Technology, Lahore 54700, Pakistan
[2]Industrad Engineering Services, Lahore 54700, Pakistan
[3]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[4]Department of Software Engineering, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia
[5]Department of Electrical Engineering, Faculty of Engineering, Modern University for Technology and Information (MTI), Cairo 11585, Egypt

Corresponding author: Musheer Ahmad (mahmad9@jmi.ac.in)

ABSTRACT The significance of data security has become more critical due to the ever-changing goals and capabilities of attackers. As a result, many cryptosystems employing diverse approaches are being developed to safeguard sensitive data. A Substitution box (S-box) plays a vigorous role in modern cryptosystems because of its credence for inducing confusion during the encryption process and ultimately protecting the data. Currently, chaotic maps are being developed and widely employed to yield S-Boxes as the use of chaotic maps aids in the randomness and resistance to mitigate many cryptanalytic attacks. In this paper, a novel chaotic map and an inventive systematic search method are proposed for the generation of key-dependent dynamic and highly nonlinear S-boxes. A variety of standard cryptographic tests such as fixed-point analysis, nonlinearity (NL), strict avalanche criterion (SAC), bit independence criterion (BIC), linear probability (LP), differential probability (DP), etc.) are applied to assess and analyze the cryptographic strengths of S-boxes generated using the proposed method. The findings from experimental and comparative analyses show that the proposed S-box provides stronger and better cryptographic features (no fixed point, no opposite fixed point, average NL = 111.75, SAC offset = 0.0000, BIC-NL = 103.9, LP = 0.125, and DP = 0.039) than many of the existing S-boxes studies presented in recent years. Hence, the proposed S-box construction technique has a lot of potential and genuine prospects for its utilization in cryptographic applications to protect sensitive data from attackers.

INDEX TERMS Key-based substitution-box, chaotic map, cryptosystem.

I. INTRODUCTION

The importance of information in all aspects of our daily lives is clearly transforming the globe along with technological advancements. For running day-to-day business operations, it is need of time to store data somewhere and transmit it over public networks through the Internet. Public networks are always good targets for intruders to grasp the transmitted data and misuse it later on to harm the communicating parties. Before storage and transmission, digital data must be transformed into a form that is meaningless for attackers and hence useless [1]. Cryptography assists in achieving this objective to safeguard the data from intruders. As a result, a large number of researchers are exploring and designing novel cryptographic systems to provide security to sensitive data [2].

These cryptographic solutions allow users to securely communicate data and information in a secure manner via an insecure network by making the transmission more and more meaningless for the attackers. On the other hand, intruders try to use various cryptanalytical efforts and approaches to weaken data fortification. Consequently, cryptographers design robust cryptosystems (ciphers) to resist such malicious techniques [3]. Modern block ciphers employ a substitution operation that assists in achieving meaninglessness in the stored or transmitted data. Characters in the original

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

data (plaintext) are substituted with other characters making the resultant data (ciphertext) much meaningless for the intruders. A substitution process is nonlinear in nature as compared to other operations of a cipher which are generally linear. This nonlinear nature of a substitution operation makes the job of an attacker very difficult in getting the original data from the captured ciphertext via insecure networks. The substitution process is carried out with the help of a substitution table generally known as a substitution box (S-box). An S-box is the most central constituent of modern block ciphers as it assists in achieving the confusion property that is one of the basic requirements of an encryption algorithm [4].

Well-known ciphers like Data Encryption Standard (DES), Advanced Encryption Standard (AES), etc. employed static S-boxes in the encryption and decryption processes. Such S-boxes have associated weaknesses and drawbacks that assist the attackers in reaching the original data from the ciphertext [5], [6]. Modern block ciphers use dynamic S-boxes which are designed with the assistance of the cipher key. Such S-boxes have the capability to provide more protection to the data by creating more confusion in the ciphertext as compared to the static S-boxes and are difficult to be guessed by the attackers due to the use of cipher key in their construction [7], [8]. The overall cryptographic forte of a block cipher is highly reliant on the S-box employed in that cipher and consequently, the cryptographic robustness of an S-box has been the primary motivation and concern of cryptosystem designers. As a result, many cryptographers have proposed diverse techniques for S-box design over time including the use of elliptic curves [9], [10], [11], [12], DNA computing [13], [14], optimization techniques [15], [16], [17], [18], cellular automata [19], linear fractional transformation [20], [21], [22], compressive sensing [23], [24], [25], [26].

Chaotic maps have gained the worthwhile attention of cryptosystem designers to construct robust and dynamic S-boxes due to their inherent characteristics such as simple implementation, controlling of results through parameters, initial condition sensitivity, randomness, unpredictable behavior, etc. As randomness and unpredictability are among the major traits of a cryptosystem, chaos theory is one of the most promising fields today used for the generation of dynamic S-boxes. Riaz et al. [27] proposed an S-box design method based on two chaotic maps and utilized the resultant S-box in image encryption. Comparative analysis proved the effectiveness of the proposed methodology against cryptanalytical efforts. Lu et al. [28] proposed an S-box design technique using another compound chaotic map that is computationally efficient and offers enough chaotic behaviour. Alghafis et al. [29] introduced a three-dimensional chaotic map-based S-Box creation approach. The resulting S-Box is used for image encryption alongside other chaotic systems, and the results indicate the resilience of the substitution box against different attacks. Liu et al. [30] developed an efficient quadratic map and a dynamic S-Box was constructed using this map. S-box analysis proved the feasibility of the proposed S-box design technique for security applications.

With the help and usage of the Logistic chaotic map, matrix rotation, and affine transformation, authors in [31] presented an innovative approach for generating dynamic S-boxes. Different researchers [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], and [44] have generated S-boxes using well-known and innovative chaotic maps along with other novel ideas. Hyperchaotic systems are gaining popularity due to the dynamic complexities and the resistance offered against cryptanalysis. Hence, these systems have been used for the construction of robust S-boxes by authors in [45], [46], [47], [48], [49], and [50].

A. MOTIVATION FOR THE PROPOSED TECHNIQUE

Although the use of chaotic maps for the generation of S-Boxes is on an increasing side, these maps also demonstrate a number of drawbacks associated with them [51]. Consequently, cryptographers try to explore, design, and apply new and novel optimization, heuristic, and transformation methodologies to increase the number of potential S-boxes and improvise the associated cryptographic forte. Zahid et al. [5], [52], [53] presented simple and novel improvisation and effective heuristic techniques to initial S-boxes to produce more robust S-boxes to defy the efforts of the attackers. However, these techniques lack huge key space, chaotic range, etc.

As cryptanalytic attempts grow, there is a dire need to design new techniques on a regular basis for generating S-boxes having enhanced and more dependable performances. In this paper, a pioneering technique for constructing dynamic S-boxes is proposed that uses an innovative chaotic map and a novel systematic search approach for improvising the cryptographic forte of the initial S-boxes.

B. CONTRIBUTIONS OF THE PROPOSED TECHNIQUE

The following are the significant contributions made in this paper:

- A novel one-dimensional chaotic map is put forward that possesses upright dynamics and incredible chaotic features as compared to state-of-the-art chaotic maps.
- The novel chaotic map is employed in the design of an algorithm that yields an initial S-box with the help of the cipher key.
- A novel systematic search approach is applied to the basic S-box to create a highly nonlinear one. The systematic search method improves the final S-box's security strength, particularly its nonlinearity.

The rest of this research article is organized as follows. Section II describes a new chaotic map-based S-Box construction approach in detail. The suggested method's distinctive advantages in creating S-Boxes for cryptographic applications are described in this section. Section III analyzes the suggested method's S-Box performance and comparisons. It examines how parameters affect S-Boxes. This section also includes security evaluations to evaluate the created S-Boxes' cryptographic strength and resilience. The proposed method's efficacy and acceptability are assessed through rigorous examination and comparison. Section IV

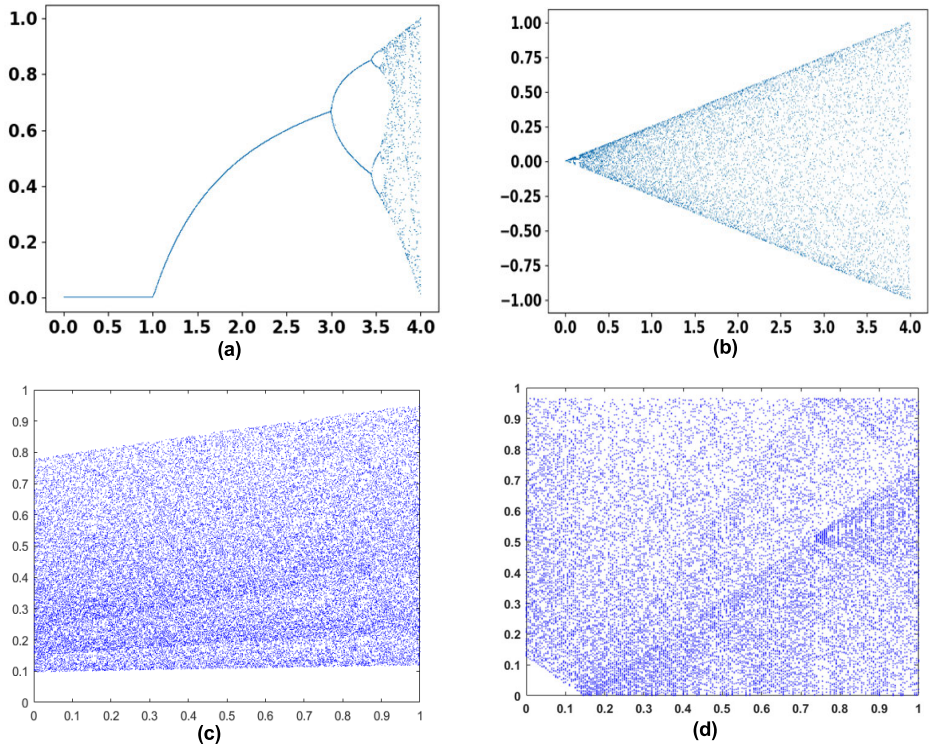

FIGURE 1. Bifurcation diagrams of (a) Logistic Map, (b) MAZa Map, (c) AZ Map, and (d) Proposed TCP Chaotic Map.

presents the conclusion of this research work, summarizing the key findings, contributions, and implications.

II. PROPOSED METHOD FOR S-BOX DESIGN

In recent years, numerous researchers have used chaotic maps in the design of robust S-Boxes as these maps offer randomness and unpredictable behavior which are among the major traits needed from a cryptosystem. These characteristics of chaotic maps assist a cryptosystem in achieving diffusion and confusion features needed for the data security. These features of chaotic maps are the motivation behind the design of a novel chaotic map for the generation of key-dependent S-boxes which may then be used for putting forward novel cryptosystems. The procedure of creating dynamic S-boxes using a cipher key is comprised of following simple phases with brief description:

- A novel Chaotic map design.
- Formulation and generation of an initial S-Box.
- Systematic search approach for nonlinearity improvement of the final S-Box.

A. NOVEL CHAOTIC MAP

A novel chaotic map using trigonometric functions and a cubic polynomial (named TCP Map) for the inception of an 8 × 8 S-box is stated in Equation (1) as follows.

$$X_{n+1} = \begin{cases} 0.33 * X_n + 1.67 * \text{Sin}\,(X_n) & 0.0 < X_n < 0.5 \\ R * Cos(X_n) - (X_n)^3 & else \end{cases} \tag{1}$$

where $X_n \in (-1.0, 1.0)$, $R \in (0.0, 1.0)$.

As the proposed TCP map of Equation (1) employes two variables, X_n and R, cipher key assists in the provision of values to these variables. The proposed chaotic map is 1-D in nature and bears the sensitivity to the initial values of the variables (X_n and R) and stated conditions. Use of variables R and X_n in the chaotic map of Equation (1) assists the cryptographers in designing more secure cryptosystems to minimize the attacks on the captured data by the attackers.

A chaotic map $x_{n+1} = f(x_n)$ is said to have a fixed point (equilibrium point) for which $x_{n+1} = x_n = x^* = f(x^*)$. The absence of a fixed point in a chaotic map is a fundamental property of chaotic systems and the map's trajectory may continue to explore different regions of its state space indefinitely. It signifies the intricate and unpredictable nature of the map's dynamics, where points in the system's trajectory continue to evolve in a complex and ever-changing manner. The proposed chaotic map of Equation (1) does not have any fixed point in the range $0.0 < X_n < 1.0$, and thus possesses an unpredictable behaviour that is needed in present-day cryptosystems. Along with it, Bifurcation diagram and Lyapunov exponent are the two well-established standards to evaluate the performance of a given chaotic map [52]. Bifurcation diagrams of well-known Logistic chaotic map, recently published in [52] and [53] chaotic maps, and the proposed TCP chaotic map are compared in Figure 1. Similarly, Lyapunov exponents of these mentioned chaotic maps are compared in Figure 2. Careful analysis of these standards clearly gratifies that the proposed TCP chaotic map holds a noteworthy amount of chaotic sophistication as it covers more spatial areas in comparison to Logistic, and chaotic maps in [52]

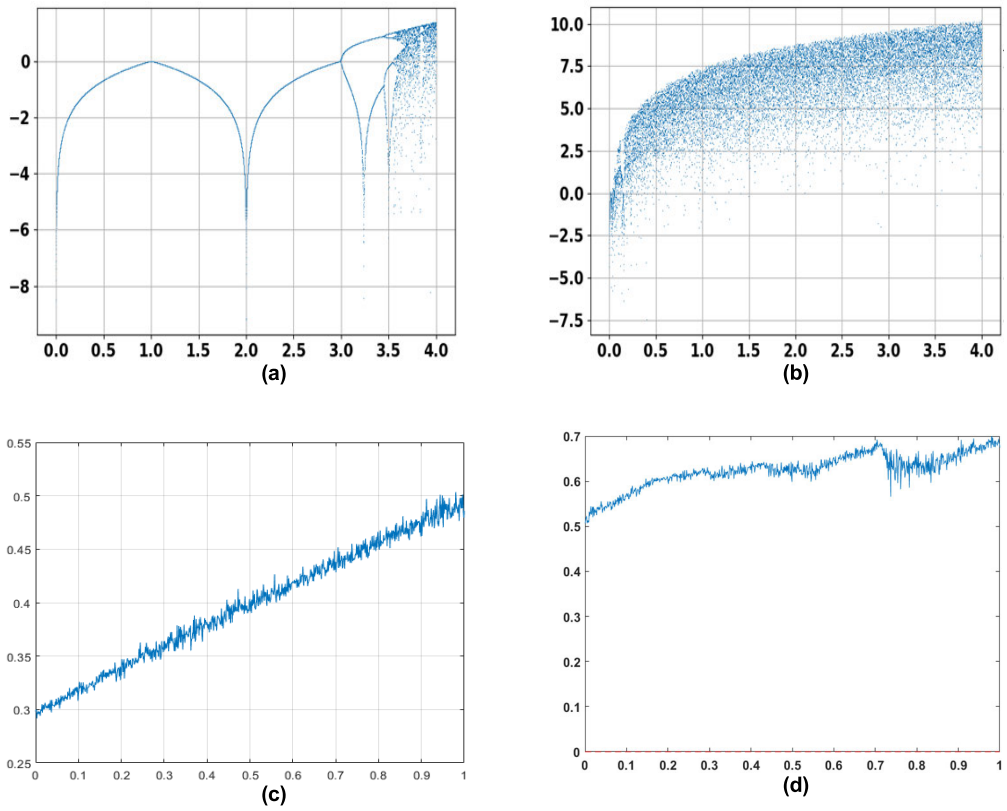

FIGURE 2. Lyapunov exponents of (a) Logistic map, (b) MAZa map, (c) AZ map, and (d) Proposed TCP Chaotic map.

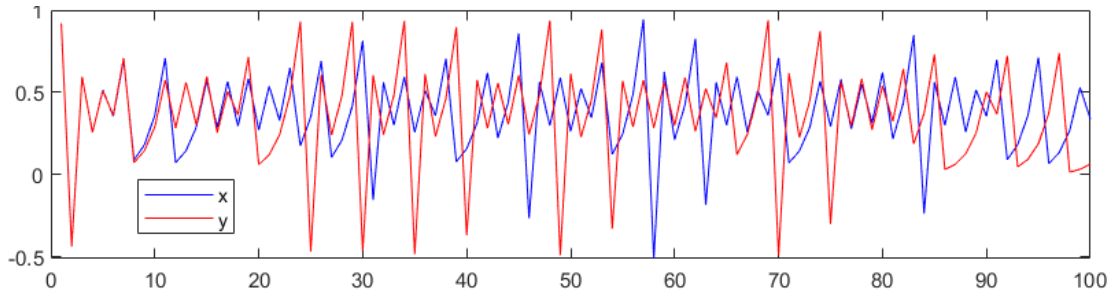

FIGURE 3. Sensitivity test of proposed chaotic map where initial values of state variables x and y difference by 0.001 only.

and [53]. Moreover, we have also performed the sensitivity test shown in Figure 3. The diagram shows that our map is quite sensitive to a minor difference in the initial values and both the trajectories are somewhat different and non-overlapping.

B. PRELIMINARY S-BOX CONCEPTION

A preliminary S-Box is generated using the proposed chaotic map (TCP) specified in Equation (1) and Algorithm 1.

Figure 4 illustrates the flowchart depicting the step-by-step process involved in the generation of an initial substitution box (S-Box). Furthermore, Table 1 showcases a specimen example of an initial S-box.

C. SYSTEMATIC SEARCH APPROACH

A substitution-box with candid cryptographic properties especially the nonlinearity provides a candid defense to protect the data against the cryptanalytical efforts. Permuting elements of a given S-box having low cryptographic forte may assist in strengthening it. Here, a final S-box is generated after permuting values of initial S-box of Table 1 with the help of an innovative tweak method, presented first time, bearing its description given in Algorithm 2 and pictorial representation in Figure 5. The proposed systematic search approach uses different parameters (A, B, C, D, E, F, and X) which receive values from the cipher key and hence is dynamic in nature. This dynamic nature of the search approach makes the

Algorithm 1 Formulation of Initial S-Box

Input:
X_n // $-1.0 < X < 1.0$
R // $0.0 < R < 1.0$
Output:
F, SBox // *Arrays of size 256 each*
Procedure:
POS $\leftarrow 0$ // *a loop variable goes from 0 to 255*
F $\leftarrow 0$ // *F has 0 in ALL locations*
WHILE (POS <= 255) DO
IF ($0 < X_n < 0.5$) THEN
$X_n = 0.33 * X_n + 1.67 * Sin\ (X_n)$
ELSE
$X_n = R * Cos\ (X_n)$ - $(X_n)^3$
END IF
VAL = ROUND ((10^6 / ABS (X_n)), 0) % 256
IF (F [VAL] = 0) DO
SBox [POS] = VAL
F [VAL] = 1
POS = POS + 1
END IF
END WHILE

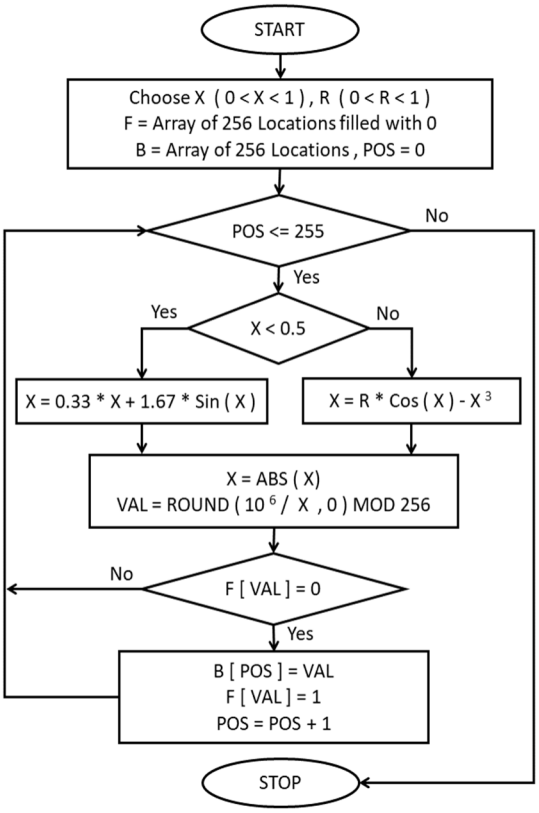

FIGURE 4. Chaos-based initial S-Box formulation.

job of an assailant very ineffective and inefficient to get the original data. A specimen final S-box yielded as a result of the application of the proposed novel search approach given in Algorithm 2 is shown in Table 2.

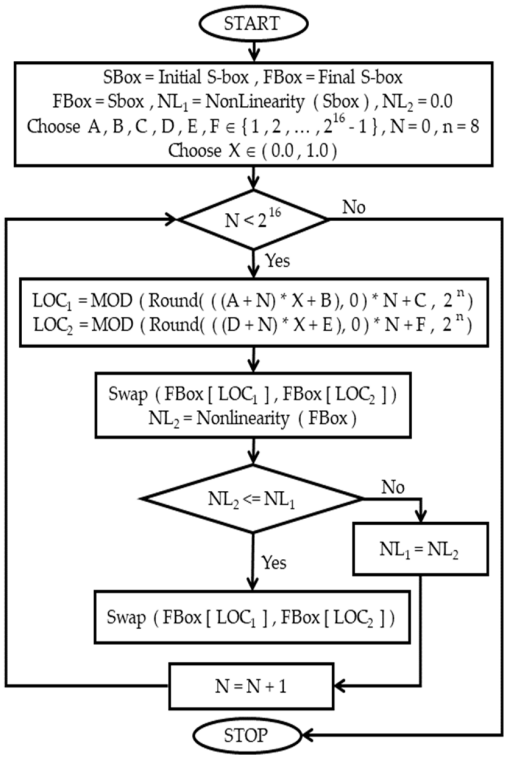

FIGURE 5. Systematic search process for nonlinearity improvement of S-box.

Values 35467, 53646, 25962, 18377, 20344, 37437, and 0.473823507891357 are used for parameters A, B, C, D, E, F, and X respectively for the creation of specimen final S-Box.

III. SECURITY ASSESSMENT OF PROPOSED S-BOX

The innovation of novel S-Boxes stands as a paramount and highly esteemed research contribution within the realm of information security. Subsequent to their creation, comprehensive evaluations are conducted to ascertain their resilience against a wide range of attacks. Employing a methodical and comprehensive approach, the projected S-Box's strength has been rigorously assessed through the following carefully curated and well-defined set of evaluation criteria. This meticulous evaluation process ensures that only the most formidable and impervious S-Boxes are designed which are suitable for deployment in information security systems to safeguard sensitive data from ever-evolving threats.

- Bijectiveness Analysis (BA)
- Fixed Points Investigation (FP)
- Opposite Fixed Points Investigation (OFP)
- Nonlinearity (NL)
- Strict avalanche criterion (SAC)
- Bit Independence Criterion (BIC)
- Linear Probability (LP)
- Differential Probability (DP)

The subsequent subsections present a comprehensive elucidation of the conducted tests and their respective outcomes for the proposed S-Box, offering a meticulous and comprehensive analysis.

TABLE 1. Initial S-Box for X = 0.632000214248896, R = 0.474008403007876.

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

TABLE 2. Final S-Box using proposed method.

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

A. BIJECTIVENESS

A fundamental characteristic of an m×n S-Box is its capability to ensure a one-to-one correspondence between distinct m-bit inputs and unique n-bit outputs. This critical requirement, as emphasized by reference [54], is paramount in preserving the integrity of data transformations. In the case of the 8 × 8 S-Box presented in Table 2, encompassing a comprehensive range of 256 distinct values spanning

Algorithm 2 Systematic Searching for High NL S-Box

Input:
A, B, C, D, E, F // *A, B, C, D, E, F*∈ *{1, 2, …, <* 2^{16}*- 1 }*
X // *X* ∈ *(0.0, 1.0)*
SBox // *Initial Substitution Box*
Output:
FBox // *Final Substitution Box*
Procedure:
N ← *0*
FBox ← *SBox*
NL_1 ← *Nonlinearity (FBox)*
NL_2 ← *0.0*
n ← *8*
WHILE (N < 2^{16} *) DO*
LOC_1 = MOD (Round(((A + N) ∗ X + B), 0) ∗ N + C, 2^n)
LOC_2 = MOD (Round(((D + N) ∗ X + E), 0) ∗ N + F, 2^n)
Swap (FBox [LOC_1], FBox [LOC_2])
NL_2 = Nonlinearity (FBox)
IF (NL_2 <= NL_1) THEN
Swap (FBox [LOC_1 *], FBox [* LOC_2 *])*
ELSE
NL_1 ← NL_2
END IF
N = N + 1
END WHILE
RETURN (FBox)

from 0 to 255, the projected S-Box demonstrates an exceptional compliance with this bijectiveness criterion. It meticulously associates each possible unique input with an exclusive and individualized output, exhibiting exemplary adherence to the principles of cryptographic functionality. This further substantiates the efficacy and reliability of the projected S-Box in achieving robust cryptographic objectives.

B. FIXED POINTS (FP)

The presence of fixed points (FP) within an S-Box raises concerns regarding a potential vulnerability, as it allows adversaries to potentially decipher the captured ciphertext. Consequently, the existence of any fixed points significantly undermines the security strength of an S-Box [5]. In the case of the projected S-Box outlined in Table 2, a comprehensive evaluation was conducted to meticulously examine this criterion, resulting in the observation that no fixed points were discovered across the entire table. This absence of fixed points serves as a testament to the robustness and resilience of the projected S-Box, reassuring its efficacy in preserving the confidentiality and integrity of sensitive information.

C. OPPOSITE FIXED POINTS (OFP)

An opposite fixed point (OFP) is present when an S-Box output is the complement of its input. The analysis of opposite fixed points in an S-Box is crucial in assessing the security and robustness of cryptographic algorithms. By identifying and examining these opposite fixed points, researchers can uncover potential vulnerabilities or weaknesses that may exist within the algorithm. The presence of opposite fixed points in a cryptographic algorithm can be problematic as it may introduce a level of predictability or redundancy that attackers can exploit. Such vulnerabilities can compromise the confidentiality and integrity of the cryptographic system. S-Box given in Table 2 was examined against this criterion and no opposite fixed points were identified. This absence of OFPs serves as a mitigation of potential security risks.

D. NONLINEARITY

The nonlinearity of a substitution box (S-box) serves as a fundamental criterion in assessing its efficacy within modern block ciphers [52], [53]. As the sole nonlinear component, an S-box plays a pivotal role in bolstering the security of cryptographic systems making it vital in defending against various attacks. When constructing an S-box, it is crucial to ensure that the transformation from original data to scrambled data is not linear in order to enhance its resistance against linear and differential attacks. Therefore, in order to effectively protect against such malicious efforts, it is imperative to construct an S-box with a substantial level of nonlinearity [54].

Equation (2) is employed for evaluating the value of nonlinearity exhibited by a Boolean function B. This quantitative measure aids in assessing the effectiveness and robustness of a function against various attacks and malicious attempts.

$$N_L(B) = \frac{1}{2}[2^n - WH_{max}(B)] \tag{2}$$

where, $WH_{max}(B)$ denotes the Walsh-Hadamard Spectrum for a Boolean function B having n bits.

Table 3 presents nonlinearity values associated with eight Boolean functions incorporated into the proposed substitution box.

TABLE 3. Final S-Box nonlinearity values.

Boolean Function	BF_1	BF_2	BF_3	BF_4	BF_5	BF_6	BF_7	BF_8
NL Value	112	112	112	112	112	112	110	112

Table 4 presents a comprehensive analysis of the nonlinearity scores for the projected S-Box, highlighting key metrics including the minimum, maximum, and average values at 110, 112, and 111.75, respectively. In order to evaluate its performance, a comparative assessment is conducted against recently designed S-Boxes, as delineated in Table 4. The results explicitly demonstrate that the proposed S-Box exhibits superior resilience against attacks such as linear cryptanalysis. The observed higher nonlinearity scores (minimum, maximum, and average) of the proposed S-Box, in relation to the majority of other S-Boxes analyzed, substantiate its enhanced resistance against adversarial assaults. This finding emphasizes the efficacy of the proposed S-Box design in bolstering security measures, particularly in the face of sophisticated attacks like linear cryptanalysis.

TABLE 4. Recent S-Boxes and nonlinearity values.

S-Box	Nonlinearity		
	Minimum	Maximum	Average
Proposed	**110**	**112**	**111.75**
[53]	110	112	110.75
[55]	108	110	109.75
[56]	106	108	106.8
[57]	106	108	106.8
[58]	106	108	106
[59]	104	110	106.5
[60]	112	110	111.5
[61]	106	110	108
[62]	106	110	108.5
[63]	106	108	106.5
[64]	112	114	112.25
[65]	104	110	106.25
[66]	104	108	106.75
[67]	104	110	107

E. STRICT AVALANCHE CRITERION (SAC)

The seminal work of authors [68] introduced the Strict Avalanche Criterion, which establishes a stringent requirement for ciphers. In order to satisfy this criterion, any modification to a single input bit must induce a 50% alteration in the resulting ciphertext. To assess the adherence of a substitution box to the SAC, a meticulous analysis involves the utilization of a dependency matrix for computation. In the present study, a comprehensive evaluation of the proposed S-Box has been conducted, yielding valuable insights into its compliance with the SAC. The process entailed the careful calculation of the dependency matrix, which has been quantified and presented in Table 5, providing a comprehensive assessment of the proposed S-Box's SAC score.

An ideal SAC score for an S-Box is conventionally represented by a value of 0.5, indicating a balanced and desirable behavior. Remarkably, the proposed S-Box exhibits a commendable average SAC score of 0.5000, which is exactly equal to the ideal benchmark. This match of the SAC score of the proposed substitution box to the desired value and an offset of 0.0000 from the ideal value accentuates its efficacy in meeting this stringent cryptographic requirement. Moreover, a SAC offset of 0.0000 reinforces the viability and effectiveness of the proposed S-Box and solidifies its standing as a promising candidate for its deployment in real-life scenarios that demand high-security standards for safeguarding sensitive data.

TABLE 5. SAC dependence values of projected S-Box.

0.4688	0.4688	0.5312	0.5469	0.4844	0.4844	0.5156	0.5156
0.4844	0.5312	0.4688	0.4688	0.4375	0.5156	0.4688	0.5312
0.4844	0.5000	0.5625	0.5000	0.4844	0.5000	0.5000	0.5312
0.4844	0.4844	0.5625	0.4375	0.5156	0.5000	0.5938	0.5156
0.5156	0.5312	0.5000	0.5625	0.5000	0.4688	0.4375	0.5000
0.4844	0.4688	0.5000	0.5156	0.5625	0.5000	0.4219	0.5156
0.4844	0.4375	0.5312	0.4688	0.5312	0.4375	0.5000	0.5625
0.4844	0.5312	0.4844	0.5000	0.4844	0.5156	0.4844	0.5000

F. BIT INDEPENDENCE CRITERION (BIC)

The Bit Independence Criterion, pioneered by Tavares and Webster [68], serves as another standard for evaluating the performance of S-Boxes. This criterion mandates that any change in the input bits should yield independent alterations in the corresponding output bits, ensuring a lack of correlation between them. In order to assess the adherence of the proposed S-Box to the BIC, the BIC-NL values have been meticulously computed and are presented in Table 6. Notably, the average BIC-NL score for the proposed S-Box is quantified at 103.9. Table 7 provides a detailed descriptive comparison of BIC-NL and SAC values for various S-Boxes. This comparative analysis helps evaluate the suggested S-Box's performance against its counterparts and reveals its robustness and applicability for real applications.

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

-	104	102	104	106	104	108	104
104	-	100	100	106	100	104	104
102	100	-	104	106	104	106	104
104	100	104	-	106	106	98	100
106	106	106	106	-	106	102	102
104	100	104	106	106	-	106	106
108	104	106	98	102	106	-	106
104	104	104	100	102	106	106	-

G. LINEAR PROBABILITY (LP)

Matsui pioneered linear cryptanalysis to assess Data Encryption Standard's weaknesses [69]. A novel theoretical attack approach finds linear connections between cryptosystem inputs like the key and plaintext and their output, the ciphertext. Linear cryptanalysis assesses cipher security and robustness using statistical patterns and biases. Linear cryptanalysis has become more popular for block cipher analysis. Block cipher resilience and cryptographic algorithm improvement

to survive sophisticated attacks in today's threat scenario require this technology. After linear cryptanalysis, the DES cipher showed severe flaws and compromises, necessitating increased security.

In response to these findings, the development of the Advanced Encryption Standard was led by the National Institute of Standards and Technology (NIST) [70]. The primary objective behind the creation of AES was to withstand potential malicious efforts exerted by attackers exploiting the weaknesses exposed through linear cryptanalysis of its predecessor.

The linear probability, which measures the likelihood of a linear relationship between inputs and the corresponding output of a substitution box, serves as an important indicator of robustness against linear cryptanalysis. When the computed linear probability value for a substitution box is found to be small, it indicates a reduced probability of linear relationships between the inputs and outputs and signifies a higher degree of resilience offered by an S-Box against linear cryptanalytic attempts.

The Linear Probability for a substitution box S is computed with the help of Equation (3).

$$LP = \max_{m_x, m_y \neq 0} \left| \frac{1}{2} \left(\frac{\#\left\{x \in N \mid x.m_x = S\,(x)\,.m_y\right\}}{2^{n-1}} - 1 \right) \right| \quad (3)$$

In Equation (3), m_x and m_y denote the masks with respect to the input and output respectively, and $N = \{0, 1, 2, \ldots, 2^n - 1\}$. The projected S-Box exhibits a notably low LP value of 0.125, highlighting its remarkable worth in thwarting linear cryptanalysis attacks. The achievement of a low LP value by the proposed S-Box emphasizes its suitability for enhancing the security of cryptographic systems. Table 9 provides a comprehensive comparison of the LP values for the proposed S-Box and few other recently designed S-Boxes. The significantly low LP value highlights its potential for secure application in real-world cryptographic scenarios, where protection against linear cryptanalysis is crucial.

H. DIFFERENTIAL PROBABILITY (DP)

Biham and Shamir invented differential cryptanalysis to challenge the Data Encryption Standard [71]. This novel strategy worked for several cryptosystems that use substitution and permutation operations like DES. Differential cryptanalysis is a major innovation in cryptanalysis that allows attackers to exploit cryptographic system flaws. Cryptanalysts can discover the secret key by carefully examining the differences between input and output values. The values of differential uniformity (DU) and differential probability (DP) determine an S-Box's resistance to differential cryptanalysis. Quantitative measures are essential for assessing S-Box strength and security. A smaller DU value indicates limited input difference propagation through the S-Box, making differential cryptanalysis more difficult. Differential probability (DP) calculates the probability of an output difference given an input difference. Smaller DP values reduce the possibility of deriving a definite output difference from an input difference, strengthening the S-Box against differential cryptanalysis. Equation (4) calculates substitution box S differential uniformity.

$$DU = \max_{\Delta i \neq 0, \Delta j} \left[\#\left\{i \in I | S\,(i) \oplus S\,(i \oplus \Delta i) = \Delta j\right\}\right] \quad (4)$$

Equation (4) uses I to represent the whole range of input values for an S-Box S. Table 8 shows that the proposed S-Box has a very low differential uniformity (DU) score of 10. This score indicates that the S-Box can withstand differential cryptanalysis. Table 9 compares S-Box differential probability (DP) values for a complete evaluation. One can simply determine if the proposed replacement box can withstand differential cryptanalysis by comparing these values across S-Boxes.

I. GENERATION TIME ANALYSIS

A thorough computational time efficiency evaluation of the projected S-Box generation method is done. The test was done on a Visual C# and Windows 10 system with a 2.2 GHz Intel Core i7 CPU and 8GB RAM. The approach was analyzed for its computing efficiency for both preliminary and final substitution boxes. A novel search approach is used to shape the final S-Box in this scheme to improve its cryptographic strength. The time taken to generate each of these preliminary S-Boxes was recorded. Similarly, the overall time

TABLE 7. SAC and BIC-NL scores of different S-Boxes.

S-Box	SAC Score	SAC Offset	BIC-NL
Proposed	**0.5**	**0.000**	**103.9**
[53]	0.496	0.004	102.9
[55]	0.5042	0.004	110.6
[56]	0.5034	0.003	103.79
[57]	0.5034	0.003	103.8
[58]	0.501	0.001	100
[59]	0.4995	0.001	104.57
[60]	0.506	0.006	104.2
[61]	0.499	0.001	104.29
[62]	0.4995	0.001	103.85
[63]	0.4978	0.002	104.21
[64]	0.4995	0.001	106.35
[65]	0.4977	0.002	104.1
[66]	0.4976	0.002	102.85
[67]	0.5101	0.01	106.25

TABLE 8. Differential uniformity scores of proposed S-Box.

6	8	8	8	8	6	8	6	4	8	6	8	6	4	6	6
6	6	8	6	6	8	6	6	8	8	6	6	6	8	8	8
10	6	6	8	8	8	6	6	10	6	6	8	6	4	6	8
8	6	8	6	6	6	8	6	6	6	8	6	6	6	6	8
6	8	8	6	6	8	6	6	8	8	6	6	8	8	6	6
8	6	6	8	6	8	6	6	8	6	8	6	6	10	8	6
6	6	6	6	6	8	8	6	6	6	8	6	6	8	6	6
6	6	6	6	6	6	6	6	6	6	8	6	6	6	6	8
6	6	8	6	8	6	8	6	6	8	6	8	6	6	6	6
6	6	6	8	8	6	6	6	6	10	8	10	8	8	6	8
6	6	6	6	8	8	8	8	6	6	6	6	6	8	8	6
6	6	8	6	8	6	8	6	6	10	6	8	8	6	6	10
6	6	6	6	6	6	6	8	6	6	8	6	6	8	6	8
8	6	6	6	8	8	6	6	8	6	8	8	8	8	8	6
4	8	8	8	6	6	6	8	8	6	6	6	6	10	8	8
6	6	8	8	10	8	6	6	6	6	8	8	6	8	6	-

TABLE 9. Linear and differential probability scores of some recent S-Boxes.

S-Box	Probability	
	Linear (LP)	Differential (DP)
Proposed	**0.125**	**0.039**
[53]	0.125	0.039
[55]	0.085	0.039
[56]	0.133	0.039
[57]	0.133	0.039
[58]	0.07	0.039
[59]	0.117	0.039
[60]	0.125	0.039
[61]	0.125	0.039
[62]	0.109	0.039
[63]	0.133	0.039
[64]	0.128	0.039
[65]	0.132	0.046
[66]	0.132	0.039
[67]	0.105	0.039

required for the generation of the final S-Boxes was also measured. The average times taken for the generation of both the initial and final S-Boxes are presented in Table 10. From the table, it is evident that the construction time for the initial S-Boxes is highly promising, indicating good computational efficiency. However, the proposed approach, which incorporates the novel tweak approach, requires very small amount of time to yield the final S-Box as can be seen in Table 10. This additional time is justified by the significant improvement in the cryptographic forte of the final substitution box, as confirmed by our analysis. It is crucial to emphasize the importance of data protection and the need to safeguard sensitive information. The requirement for robust cryptographic measures cannot be understated although increasingly powerful CPUs are available today. Figure 6 illustrates how the nonlinearity (NL) values of initial substitution boxes were substantially amplified while maintaining the computational efficiency.

TABLE 10. Example S-Box's construction time (seconds).

Initial Substitution Box	Final Substitution Box
0.037	13.487

J. KEY SPACE ANALYSIS

The proposed method is characterized by its dynamic and key-dependent nature, which enables the generation of unique S-boxes with each implementation. To achieve this, distinct initial values are employed for the parameters involved in the method. This dynamic nature ensures that the resulting S-boxes are not fixed or predetermined, and the respective cryptanalysis of each S-box becomes very difficult. Table 11 provides a comprehensive listing of the

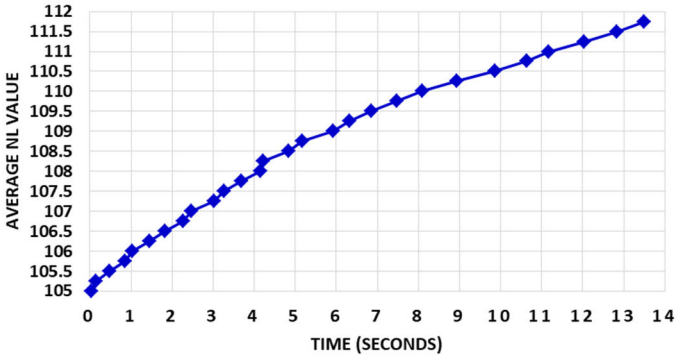

FIGURE 6. Nonlinearity improvement versus time of initial S-Box using proposed method.

parameters employed in the proposed method of S-box creation, along with their corresponding ranges and key spaces.

TABLE 11. Parameters, respective range, and key space.

Parameter Name	Range of Parameter	Key Space
X_n	$0 < X_n < 1$ (15 decimal places)	10^{15}
R	$0 < R < 1$ (15 decimal places)	10^{15}
X	$0 < X < 1$ (15 decimal places)	10^{15}
A	1, 2, 3, … …, $2^{16} - 1$	~ 6.6 x 10^4
B	1, 2, 3, … …, $2^{16} - 1$	~ 6.6 x 10^4
C	1, 2, 3, … …, $2^{16} - 1$	~ 6.6 x 10^4
D	1, 2, 3, … …, $2^{16} - 1$	~ 6.6 x 10^4
E	1, 2, 3, … …, $2^{16} - 1$	~ 6.6 x 10^4
F	1, 2, 3, … …., $2^{16} - 1$	~ 6.6 x 10^4

The magnitude of the key space offers a significant protection against unauthorized access attempts [72], [73]. The sheer number of possible keys makes it highly improbable for an attacker to stumble upon the correct key by random guessing or exhaustive search. Even with the most powerful computing resources at their disposal, the likelihood of successfully discovering the correct key within this gigantic key space is infinitesimally small. One notable and crucial aspect of the proposed method is the extensive key space it encompasses. The estimated size of this key space is approximately 8.3×10^{73} or $\sim 2^{242}$, that represents an overwhelmingly large number of possible key combinations. This huge key space poses a formidable barrier for potential attackers attempting to employ brute force techniques.

K. SECURITY APPLICATION

For decades, Image-based communication is popular today due to social media and quick communication. To evaluate proposed S-box for encryption. The proposed S-box is used to

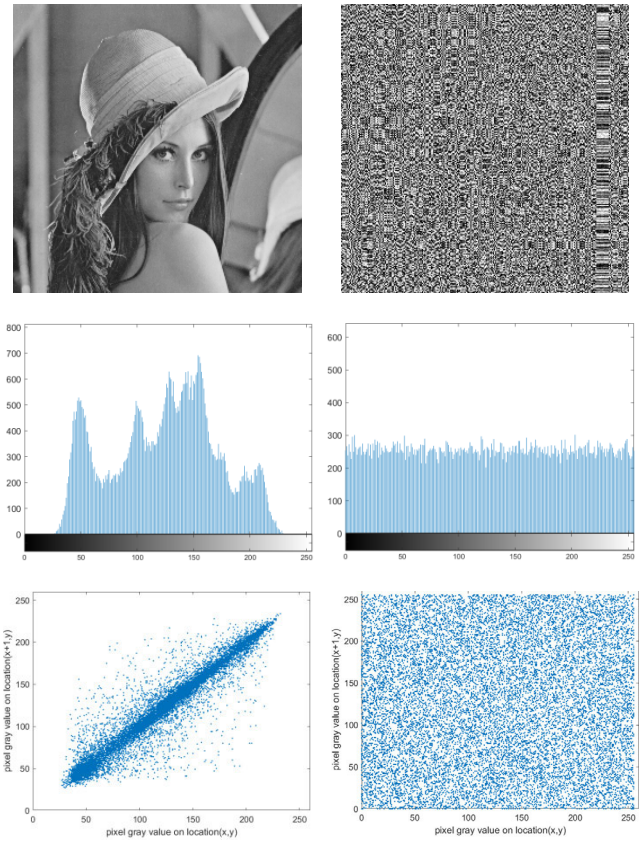

FIGURE 7. Visual description of encryption content through proposed S-box.

encrypt the standard gray-scale Lena plain-image. The two-way S-box substitution process involves forward substitution from first to last pixel, followed by backward substitution from last to first pixel. The plain-image, its histogram, and correlation of adjacent pixels in the image are available in first column of Figure 7. However, the second column shows the encrypted image, its histogram, and correlation plot. The encrypted image and histogram show that the S-box can provide strong encryption because the image is indistinguishable and its pixels distribution is fairly uniform compared to the plain-image content. Moreover, the adjacent pixels are not

correlated to their neighboring pixels in the encrypted image unlike plain-image. In addition, the famous Majority Logic Criteria is adopted to quantify the encryption effect. MLC suite statistical tests include entropy, correlation, contrast, energy, and homogeneity [22]. Table 12 shows MLC test scores for Figure 3's plain-image and encrypted picture. The Table scores show that the suggested S-box for multimedia encryption performs well when compared with Ref. [22].

TABLE 12. Image encryption performance for *Lena* test image.

Test Image	Entropy	Correlation	Contrast	Energy	Homogeneity
Plain-image	7.4439	0.90249	0.44825	0.11273	0.8622
Encrypted	7.9967	-0.03949	10.1184	0.01572	0.40322
Ref. [22]	7.9968	-0.00114	10.51509	0.015647	0.389625

IV. CONCLUSION

This research article introduces a construction method for a novel and secure substitution box (S-Box) aimed at protecting data from security assaults. The method incorporates several key features to enhance its cryptographic strength, including its innovative, key-dependent, and dynamic nature, which are achieved through the utilization of a novel chaotic map. A significant contribution of this method is the introduction of a dynamic tweak approach that permutes the values of the initial S-Box. This dynamic nature allows for adaptability and variability in the generated S-Box, strengthening its resistance against security attacks. The values of the tweak approach are determined based on the parameters used in the method, which themselves are dynamic and presented for the first time in this research. Notably, even a slight variation in the values of these parameters leads to the creation of a completely different and unique S-Box. This property highlights the method's versatility and its ability to generate diverse S-Boxes, enhancing the overall security of the cryptographic system.

Through thorough analysis, comparison, and exploration, the research confirms that the proposed chaotic map exhibits a significant level of chaotic complexity. This characteristic is desirable in cryptographic systems, as it augments the randomness and unpredictability of the resultant substitution boxes. To evaluate the cryptographic strength of the final S-Box, well-defined criteria are used. A comparative analysis is performed, comparing the strength of the resultant S-Boxes with state-of-the-art substitution boxes commonly employed in contemporary ciphers. This assessment demonstrates that the substitution boxes engendered using the proposed technique possess a high level of cryptographic aptitude, making them suitable for applications in the field of cryptography. Although the proposed 1-D chaotic map serves as a building block for an S-box generation technique, dealing with real-world systems and complex phenomena require higher-dimensional maps for precise representation and analysis. Limited dimensionality restricts the capability to model complex systems. Another limitation is the use of a smaller number of parameters (R and X_n) in the proposed chaotic map. Future research using the proposed approach may find its root using a hyperchaotic map offering more dimensions and unpredictable behaviour that is needed to protect sensitive data from attackers. Coupling of the proposed chaotic map with other 1-D maps may lead to the emergence of good unpredictable behaviour and complex spatiotemporal designs.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security Principles and Practices*. London, U.K.: Pearsons, 2017.
[2] A. H. Zahid, M. Ahmad, A. Alkhayyat, M. J. Arshad, M. M. U. Shaban, N. F. Soliman, and A. D. Algarni, "Construction of optimized dynamic S-boxes based on a cubic modular transform and the sine function," *IEEE Access*, vol. 9, pp. 131273–131285, 2021.
[3] 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 Manag.*, vol. 17, no. 1, pp. 118–131, Mar. 2020.
[4] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019.
[5] 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.
[6] K. Mohamed, M. N. M. Pauzi, F. H. H. Mohd 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.
[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. 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] 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. 1–6.
[14] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "A new DNA-based S-box," *Int. J. Engg. Tech.*, vol. 15, no. 4, pp. 1–9, 2015.
[15] 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.
[16] Y. Wang, K.-W. Wong, C. Li, and Y. Li, "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, Jan. 2012.

[17] 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, Nov. 2019.

[18] M. Ahmad, M. N. Doja, and M. M. S. Beg, "ABC optimization based construction of strong substitution-boxes," *Wireless Pers. Commun.*, vol. 101, no. 3, pp. 1715–1729, Aug. 2018.

[19] 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.

[20] L. Chew, N. Chew, and E. S. Ismail, "S-box construction based on linear fractional transformation and permutation function," *Symmetry*, vol. 12, no. 5, p. 826, 2020.

[21] 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.

[22] 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.

[23] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105837.

[24] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018.

[25] Y.-G. Yang, B.-W. Guan, J. Li, D. Li, Y.-H. Zhou, and W.-M. Shi, "Image compression-encryption scheme based on fractional order hyper-chaotic systems combined with 2D compressed sensing and DNA encoding," *Opt. Laser Technol.*, vol. 119, Nov. 2019, Art. no. 105661.

[26] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Process.*, vol. 155, pp. 218–232, Feb. 2019.

[27] 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.

[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.

[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.

[31] 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.

[32] W. Yan and Q. Ding, "A novel S-box dynamic design based on nonlinear-transform of 1D chaotic maps," *Electronics*, vol. 10, no. 11, p. 1313, May 2021.

[33] E. Tanyildizi and F. Özkaynak, "A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838, 2019.

[34] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3317–3326, Aug. 2019.

[35] F. Özkaynak, V. Çelik, and A. B. Özer, "A new S-box construction method based on the fractional-order chaotic Chen system," *Signal, Image Video Process.*, vol. 11, no. 4, pp. 659–664, May 2017.

[36] M. A. Khan, A. Ali, V. Jeoti, and S. Manzoor, "A chaos-based substitution box (S-box) design with improved differential approximation probability (DP)," *Iranian J. Sci. Technol., Trans. Electr. Eng.*, vol. 42, no. 2, pp. 219–238, Jun. 2018.

[37] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and S_8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.

[38] X. Wang, A. Akgul, U. Cavusoglu, V.-T. Pham, D. Vo Hoang, and X. Nguyen, "A chaotic system with infinite equilibria and its S-box constructing application," *Appl. Sci.*, vol. 8, no. 11, p. 2132, Nov. 2018.

[39] Ü. Çavusoglu, A. Zengin, I. Pehlivan, and S. Kaçar, "A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear Dyn.*, vol. 87, no. 2, pp. 1081–1094, Jan. 2017.

[40] X. Wang and Q. Wang, "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos," *Nonlinear Dyn.*, vol. 75, no. 3, pp. 567–576, Feb. 2014.

[41] Z. Hua and Y. Zhou, "Dynamic parameter-control chaotic system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3330–3341, Dec. 2016.

[42] H. Liu, F. Wen, and A. Kadir, "Construction of a new 2D Chebyshev-sine map and its application to color image encryption," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 15997–16010, Jun. 2019.

[43] X. Wang, Ü. Çavusoglu, S. Kacar, A. Akgul, V.-T. Pham, S. Jafari, F. Alsaadi, and X. Nguyen, "S-box based image encryption application using a chaotic system without equilibrium," *Appl. Sci.*, vol. 9, no. 4, p. 781, Feb. 2019.

[44] Ü. Çavusoglu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-box," *Chaos, Solitons Fractals*, vol. 95, pp. 92–101, Feb. 2017.

[45] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyper-chaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018.

[46] Y. Tian and Z. Lu, "S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm," *J. Syst. Eng. Electron.*, vol. 27, no. 1, pp. 232–241, Feb. 2016.

[47] T. Ye and L. Zhimao, "Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling," *Nonlinear Dyn.*, vol. 94, no. 3, pp. 2115–2126, Nov. 2018.

[48] 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. Advancements Comput. Technol.*, vol. 4, no. 18, pp. 282–289, Oct. 2012.

[49] M. Ababneh, "A new four-dimensional chaotic attractor," *Ain Shams Eng. J.*, vol. 9, no. 4, pp. 1849–1854, Dec. 2018.

[50] L. Liu, Y. Zhang, and X. Wang, "A novel method for constructing the S-box based on spatiotemporal chaotic dynamics," *Appl. Sci.*, vol. 8, no. 12, p. 2650, Dec. 2018.

[51] 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, Aug. 2021, Art. no. e12369.

[52] 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.

[53] A. Hussain Zahid, M. Junaid Arshad, M. Ahmad, N. F. Soliman, and W. El-Shafai, "Dynamic S-box generation using novel chaotic map with nonlinearity tweaking," *Comput., Mater. Continua*, vol. 75, no. 2, pp. 3011–3026, 2023.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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, Mar. 2020.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] 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.
[64] 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.
[65] 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.
[66] 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.
[67] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," *Eur. Phys. J. Plus*, vol. 135, no. 2, p. 194, Feb. 2020.
[68] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Crypto. Tech.*, Santa Barbara, CA, USA, Aug. 1986, pp. 523-534.
[69] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 765. Berlin, Germany: Springer-Verlag, 1994, pp. 386–397.
[70] H. M. Heys, "A tutorial on linear and differential cryptanalysis," *Cryptologia*, vol. 26, no. 3, pp. 189–221, Jul. 2002.
[71] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991.
[72] R. A. Muhajjar, N. A. Flayh, and M. Al-Zubaidie, "A perfect security key management method for hierarchical wireless sensor networks in medical environments," *Electronics*, vol. 12, no. 4, p. 1011, Feb. 2023.
[73] M. Al-Zubaidie and G. S. Shyaa, "Applying detection leakage on hybrid cryptography to secure transaction information in e-commerce apps," *Future Internet*, vol. 15, no. 8, p. 262, Aug. 2023.

AMJAD HUSSAIN ZAHID received the Ph.D. degree in computer science (Information Security) from the University of Engineering and Technology, Lahore. He is currently working as an Assistant Professor with the University of Management and Technology (UMT), Lahore, Pakistan. He is also the Program Advisor for B.S. (IT) program and member of many academic bodies. He has been an active member of Higher Education Commission (HEC) National Curriculum Revision Committee (NCRC), Pakistan. He has more than 23 years of qualitative experience in teaching. He is vigorous in academic research and his research interests include information security, programming languages, algorithm design, enterprise architecture, technology management, IT infrastructure, blockchain. He is serving as an efficient and effective Reviewer in several reputed International Research Journals of high impact factor in the domain of Information Security. He possesses quality monitoring and maintaining capabilities along with the strong interpersonal, leadership and team management skills. He has been an active member of faculty board of studies for Punjab University College of Information Technology (PUCIT) and Virtual University of Pakistan.

HAFIZ ALI MANSOOR ELAHI received the M.Phil. degree in computer science from The Institute of Management Sciences, Lahore, Pakistan. He is a multi-skilled IT Professional with above 12 years of experience, good supervisory, technical expertise, and excellent academic and practical knowledge in the IT Security domain. He is currently working as an IT Manager in a private limited company. He is an Internationally Certified Ethical Hacker. He has conducted many international and professional pieces of training and did certifications like CEH, CPT, CHFI, CISCO, MICROSOFT, RFID, DevOps along with his professional career. His professional experience has given him a strong foundation in the Information Security domain and has developed a reputation as a strategic thinker and problem solver.

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he has worked in the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor in the Department of Computer Engineering, Jamia Millia Islamia. He has published over 110 research papers in internationally reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. He has more than 3400 citations of his research works with an H-index of 34, i-10 index of 81, and cumulative impact factor of more than 275. He has been consecutively listed three times among World's Top 2% researchers in studies conducted by Elsevier and Stanford University in 2021, 2022 and 2023. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has served as a reviewer and a technical program committee member of many international conferences. He has also served as referee of some renowned journals, such as Information Sciences, Signal Processing, *Journal of Information Security and Applications*, IEEE JSAC, IEEE TCYB, IEEE TCSVT, IEEE TII, IEEE TPAMI, IEEE TNNLS, IEEE TITS, IEEE TNSE, IEEE TNB, IEEE TCAS, IEEE TBD, IEEE TR, IEEE IOTJ, IEEE MULTIMEDIA, IEEE Access, Expert Systems with Applications, Wireless Personal Communications, Neural Computing and Applications, Multimedia Tools & Applications, *International Journal of Bifurcation and Chaos*, Chaos Solitons & Fractals, Physica A, Signal Processing: Image Communication, Neurocomputing, IET Information Security, IET Image Processing, Security and Communication Networks, Optik, Optics and Laser Technology, Complexity, Computers in Biology and Medicine, Computational and Applied Mathematics, and Concurrency and Computation.

LOUAI A. MAGHRABI (Member, IEEE) received B.Sc. degree in computer science from Lebanese American University, Beirut, Lebanon, M.Sc. degree in information technology from the University of West of England, Bristol, U.K., and the Ph.D. degree in cybersecurity from Kingston University, London, U.K. He is currently an Assistant Professor in the Department of Software Engineering, College of Engineering, University of Business & Technology, Jeddah, Saudi Arabia. His research interests include cybersecurity, risk assessment, cryptography, artificial intelligence, machine learning, IoT, blockchain, drones, metaverse, quantum computing and game theory.

RAMY SAID AGIEB SAID born in June 1982. He received the Ph.D. degree from Ain-Shams University in 2014. He is an accomplished academic and cyber security expert. He became a respected Lecturer, sharing his knowledge in electronics, communications, artificial intelligence, and cyber security across various universities. He influence extends to the realms of artificial intelligence, wireless communications, and security, where his published works have advanced both theory and practice. Notably, he specializes in mobile application security testing, enhancing digital safety. His legacy is one of education, innovation, and safeguarding the digital world.