IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 3, 2020, accepted June 8, 2020, date of publication June 12, 2020, date of current version June 25, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3001868

Bijective S-Boxes Method Using Improved Chaotic Map-Based Heuristic Search and Algebraic Group Structures

MUSHEER AHMAD[1], EESA AL-SOLAMI[2], AHMED MOHAMMED ALGHAMDI[3], AND MUHAMMAD AWAIS YOUSAF[4]

[1]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[2]Department of Information Security, University of Jeddah, Jeddah 21493, Saudi Arabia
[3]Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 21493, Saudi Arabia
[4]Department of Mathematics, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan

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

ABSTRACT This paper presents a hybrid method for the construction of cryptographically strong bijective substitution-boxes by utilizing the merits of chaotic map and algebraic groups. The hybrid method first generates the key-dependent dynamic S-boxes using chaotic heuristic search strategy and then the S-boxes are evolved with the help of potent proposed algebraic group structures. This paper proposes a new improved combination chaotic map to operate initial search strategy. To augment the strength of generated S-boxes, the algebraic group structures are discovered which have the power to improve their cryptographic strength. The performance assessments using standard criterions are rendered to quantify the strengths of proposed bijective S-boxes. The experimental results and comparisons with recent S-box research findings justify the effectiveness and competence of the proposed bijective S-boxes and anticipated hybrid generation method.

INDEX TERMS Bijective substitution-boxes, improved chaotic map, heuristic search, algebraic groups.

I. INTRODUCTION

Due to open and insecure nature of internet and networking technologies, security of sensitive information and multimedia data has been crucial issue since decades. Over the years, different types of data security techniques have been suggested the cryptographers [1], [2]. Depending upon how data is processed, the cryptographic algorithms can be classified as block ciphers and stream ciphers. A block cipher is a method of encrypting text in which a cryptographic key and algorithm are applied to a block of data at once as a group, called blocks, with an unvarying transformation [3]–[5]. The block ciphers employ the layers of permutation and substitution for strong design capable of exhibiting strong confusion and diffusion properties. The Fiestal network and Substitution-Permutation (S-P) network are the two much studied architecture that are engaged to build block cryptosystems [6]. The substitution-boxes are crucial constituents for such networks intended to convey requisite nonlinear transformation of data which in turn brings desired confusion along with robustness to different cryptographic assaults. Substitution and permutation are two important building blocks of a block cipher algorithm and they are purely mathematical blocks [7], [8]. Substitution process takes block of bits as input and nonlinearly transforms them to generate other block of bits as output. Whereas, permutation process applies shuffling, this is a linear transformation on the input pattern. A P-box takes the results of S-box of one round, applies permutations and feeds back to S-boxes for another rounds. The combination of S-boxes and P-boxes across multiple rounds makes the cipher strong and powerful [9]. It is recommended to have cryptographic strong S-boxes so as to satisfy Shannon's confusion and diffusion properties [10]. These nonlinear transformation components are usually deployed as lookup tables known as substitution-boxes.

It has been well-studied that the chaotic dynamical systems hold many features that are consistent with the need of cryptography. They have the features of high sensitivity to initial conditions and system parameters, rapid attainment of auto-correlation and random-like behaviour of generated sequences, high entropy and prediction complexity, etc.

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran Tariq.

These characteristics of chaotic systems have made them suitable for the construction of strong cryptographic algorithms. Consequently, they have been utilized to construct multimedia data encryption, substitution-boxes design, steganography, watermarking, hash functions algorithms, etc, [3], [4], [11], [12] for the last decade. However, the security of these cryptographic algorithms heavily relies on the use of rich dynamics of digital chaotic maps and systems. It is need not necessary that all chaotic maps and systems are suitable to realize strong chaos-based cryptosystems. A chaotic system shouldn't have the frail performance to avoid weak security in the system. It has been highlighted in research findings that some of the existing discrete 1-D chaotic maps such as chaotic logistic map, chaotic sine map, chaotic cubic map, chaotic tent map, etc., suffer from one or more demerits that discourage their use to develop a security system [12]. Hence, the employed digital chaotic map should have cryptographic suited features such as large lyapunov exponent, wide-spread and uniform bifurcation, high chaotic range, high complexity, etc.

Fundamentally, a substitution-box of size $n \times m$ receives n input bits and nonlinearly transforms to m output bits. It is a representation from Galois field GF(2^n) $\rightarrow$ GF(2^m), that performs replacements secretly the n-bit input data to m-bit output cipher data [13], [14]. It would be a one-to-one mapping if $n = m$, i.e. when each n-bit input is uniquely mapped to a single n-bit output. Such S-boxes are termed as bijective S-boxes and are of much significance for the S-P network based block cipher design paradigms. Bijectivity entails that all possible 2^n input words each of length n-bit map to distinct outputs of same size. As s result, the $n \times n$ S-box can be viewed as a permutation of the sequence from 0 to 2^n - 1.They can also be viewed as vectorial Boolean functions that are multi-input and multi-output functions. A small 8×8 S-box inherently comprises of eight Boolean functions, where each takes 8-bit input and yields 1-bit as output, thereby all 8 functions collectively gives output bit-stream of size 8-bit. The performance metrics used to appraise Boolean functions are also used to measure the strength of S-boxes. The secure S-boxes have a dominant part to decide the forte of block ciphers. The security features of S-boxes are of vast significance for the security of cryptosystems [15]. Henceforth, the progress of tough S-boxes is of supreme impact for researchers aspiring in planning strong modern day ciphers. Of late, the S-boxes have been smeared in various security application areas such as image encryption, watermarking, steganography, etc., [16]–[20]. The designs of variable sized key-dependent S-boxes have not been considered significantly in literature. There are few proposals that have investigated the design and construction of variable sized $n \times n$ S-boxes restricted to sizes for $5 \leq n \leq 8$ in [21].

The successes of AES block cipher and its S-box is mainly responsible for the progress and development of proposals devoted to the creation of S-boxes [22]. All of them are balanced and whose designs are primarily based on concepts such as algebraic techniques, optimization, chaotic maps and systems, etc, [23]–[30]. Lambić proposed a simple search methodology for yielding S-boxes which is based on chaotic system and composition methods in [31]. In [32], the authors have constructed an S-box using method based on the 3D four-wing autonomous chaotic system. Khan and Asghar came up with a unique method of designing S-boxes by using S8 symmetry group and Gingerbreadman chaotic map in [33]. The S8 permutations and Gingerbreadman chaotic maps combinations proved to be useful for encryption of images. A new S-box design was proposed in [34] which is honorable. Their design aided with rich dynamic features of new scaled Zhongtang chaotic system. A method to construct bijective S-box based on discrete chaotic map is investigated in [35]. The outcomes of the method showed that the S-boxes have good cryptographic properties. As an advantage, the method has a large key space and suitability to generate random S-boxes. In [36], it has been shown that a good S-box can be obtained by using fractional-order chaotic Chen system. The work done in [37] leads to a new block cipher using Duffing chaotic systems. This block cipher is easy to gather and is appropriate for secure communications. Moreover, the authors in [38] proposed a new scheme for constructing substitution box which has in its base the linear fractional transformation. Analytically, the generated S-box is easy to device in software and hardware. The statistical outcomes proved the confusion capableness of their S-box is acceptable. It is researched that S-boxes tend to deal high safety to the ciphers and better resistivity to prevalent assaults.

The designing efficient and variable sized S-boxes is a complex and an open issue. One of the elementary causes of this complication is the size of massively bulky search space. The possible search space for configuration of an $n \times n$ S-box is $2^n!$, which is exhaustively large like it is $(2^5 = 32)! \approx 10^{35}$ for 5×5, $(2^6 = 64)! \approx 10^{89}$ for 6×6, $(2^7 = 128)! \approx 10^{215}$ for 7×7, $(2^8 = 256)! \approx 10^{506}$ for 8×8 S-box [39]. Therefore, with an aim to draw a proficient structure of an S-box whose size is variable, a chaos-based heuristic method is framed which can construct efficient $n \times n$ ($5 \leq n \leq 8$) S-boxes. In this paper, a general and effective approach based on improved chaos and group action based method is proposed for constructing strong bijective S-boxes with minor alteration in the input parameters of proposed algorithm. The main contributions made in this paper include the following.

- ⋆ An improved one-dimensional chaotic map is proposed based on novel combination mechanism of sine and logistic functions.
- ⋆ The improved chaotic map has better dynamics, complexity and chaotic behaviour as compared to conventional chaotic Logistic map in terms of lyapunov exponent, bifurcation behavior and complexity.
- ⋆ A systematic $n \times n$ S-boxes generation procedure using improved chaos based heuristic search is suggested which gives key-dependent dynamic bijective S-boxes.

- ⋆ Some specific algebraic group structures for each initial bijective S-box are proposed whose actions improvise the cryptographic strength of S-boxes.
- ⋆ The performance of proposed bijective S-boxes are found considerably respectable over many existing S-boxes.
- ⋆ Remarkably, the nonlinearity of 114 is achieved for the S-box of size 8×8 which is larger than well known AES S-box nonlinearity bound of 112.

The organization of rest of the paper is as follows: Section 2 provides the details of improved 1-D chaotic map. Where as, the dynamical behaviour of proposed map is analyzed and compared in Section 3. The proposed method of bijective S-boxes generation using improved chaos based heuristic search and algebraic group actions are detailed in Section 4. The performance of different sized proposed bijective S-boxes are evaluated and compared with state of the art methods in Section 5. At last, the conclusions of the research work are presented in Section 6.

II. IMPROVED 1-D CHAOTIC MAP

It has been well studied that the conventional discrete one-dimensional chaotic maps suffered from many problems that affect their degree of chaoticity and usage in security applications [40]–[42]. Specifically, the chaotic logistic map, govern by the Equation (1), possesses limitations such as: non-uniform coverage of whole bounded space in bifurcation behaviour, limited chaotic range for parameter L which is restricted to 3.57 to 4, low value of largest lyapunov exponent, and low value of approximate entropy [43]. The security and robustness of many chaos-based cryptographic algorithms primarily rely on the dynamics of employed chaotic maps. To develop strong security algorithm, it is necessary to have chaotic maps which holds excellent and rich dynamical features [44]. Instead of relying on any existing chaotic map, we develop a new combinational chaotic map which found to have better dynamical performance compared to chaotic logistic map and other recent chaotic map. The proposed improved chaotic map is defined as follows:

$$\begin{aligned} x_{n+1} &= f_{chaos}(x_n, r) \\ &= \begin{cases} (r100sin(\pi x_n)(1-sin(\pi x_n)))mod(1) & if\ x_n \geq 0.5 \\ (r100sin(\pi 3^{10+x_n}))mod(1) & if\ x_n < 0.5 \end{cases} \end{aligned} \tag{1}$$

where, r is its system parameter, and x_n indicates state variable bounded to space (0, 1). The much-studied conventional chaotic logistic map is as follows [45].

$$x_{n+1} = rx_n\,(1 - x_n) \tag{2}$$

The dynamics of logistic-sine system (LSS) map investigated in [46] is defined as.

$$x_{n+1} = (rx_n\,(1 - x_n) + ((4 - r)/4)\sin(\pi x_n))\ \text{mod}\ (1) \tag{3}$$

The 1-D sine-powered (DSP) chaotic map is recently suggested in [47] is governed by.

$$x_{n+1} = ((\alpha + 1)x_n)^{\sin(\beta\pi + x_n)} \tag{4}$$

The dynamical characteristics of these 1-D chaotic maps are analyzed and examined in what follows.

III. DYNAMIC BEHAVIOUR OF IMPROVED 1-D CHAOTIC MAP

In this section, the dynamical behaviour of proposed improved 1-D chaotic map is determined and compared with recent 1-D chaotic maps.

A. LYAPUNOV EXPONENT

Lyapunov exponent is one of the prominent quantifiable measures of degree of chaotic behaviour in any chaotic map or system. It represents the rate of separation of two minutely close trajectories. Mathematically, it is expressed as.

$$LE = \lim_{N\to\infty}\left[\frac{1}{N}\sum_{n=1}^{N}\log\left|\frac{d}{dx}\,(x_{n+1}))\right|\right]$$

A positive exponent confirms the existence of chaos in the system. More positive the exponent, better the chaotic phenomenon in the map [40]. The LE of chaotic maps are determined and shown in first column of Figure 1. The improved map starts to show the chaotic behaviour for $r > 0$. The LE for proposed map gets larger with increase in parameter r. It can be seen that the LE of improved map is larger and better as compared to chaotic logistic map, LSS map, and DSP map as well.

B. BIFURCATION ANALYSIS

It is the study of qualitative changes in behaviour of a dynamical system when the changes in system parameters are made. This helps to understand the existence of any fixed points, quasi-fixed points, periodic or chaos phenomenon, etc, in the system [43]. The bifurcation diagrams of the four 1-D chaotic maps are depicted in second column of Figure 1. The bifurcation behaviour of improved map looks more complex and covers entire region of space (0, 1) better than all three chaotic maps.

The phase attractors of the dynamical maps under analysis are also determined and their projections in 2D/3D are shown in third/fourth column in Figure 1. It is evident from the Figure that the proposed map shows uniform coverage of entire state space in better way unlike rest of the three 1-D maps including recent DSP chaotic map.

C. COMPLEXITY ANALYSIS

Among various complexity measures pertinent to chaotic systems, approximate entropy is one of the potential complexity criteria as suggested in [39], [40]. It quantifies the irregularities in a given time series. Higher value of ApEn indicates high complexity content and randomness in the anticipated time series from chaotic system. We followed the

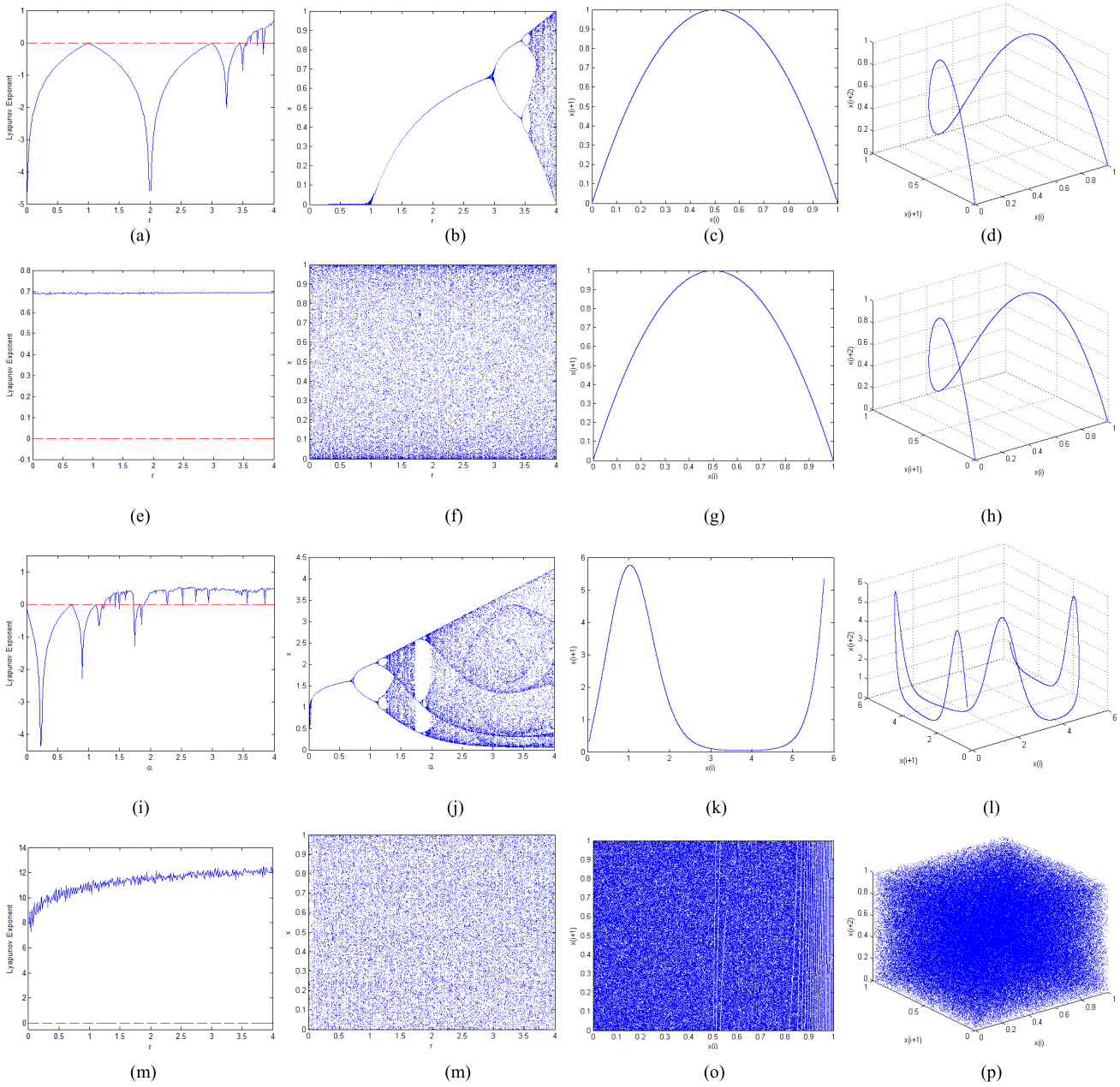

FIGURE 1. Lyapunov exponent diagram (first column) and bifurcation behavior (second column), phase attractor in 2D (third column), and phase attractor in 3D (fourth column) of (a)-(d) logistic map, (e)-(h) LSS map, (i)-(l) DSP map for $\beta = 0.3306$, and (m)-(p) proposed improved map.

procedure of its computation for the generated time series from our chaotic map and chaotic maps [45]–[48] under analysis over 10000 points. The obtained ApEn for proposed improved chaotic map comes out as 1.1995 which is considerably higher than the logistic map [45], LSS map [46], DSP map [47], and TLS map [48] as evident from the ApEn comparison plot shown in Figure 2 for bifurcation parameter in [0, 4].

The outcomes of three mentioned analyses to study the dynamics of 1-D chaotic maps of Eqn.(1)-(4) are summarized in Table 1 for comprehensible comparison of their relative performances. The Table clearly shows that the proposed chaotic map possesses better dynamical performance and complexity which are desirable for chaos-based cryptographic applications.

IV. PROPOSED S-BOXES CONSTRUCTION

In what follows, we discuss the proposed general technique for creating strong bijective S-boxes of different sizes ranging from 5×5 to 8×8. The hybrid method makes use of both the chaos-based approach and algebraic technique to solve the purpose.

TABLE 1. Dynamical performance comparison of 1-D chaotic maps.

Measure	Logistic map	LSS map[46]	DSP map[47]	Proposed map
Chaotic range	$3.57 < r \leq 4$	$0 < r \leq 4$	$\alpha > 2$	$r > 0$
Largest LE	0.6919	0.6981	0.5395	12.495
ApEn	0.4473	0.6053	0.5237	1.3314

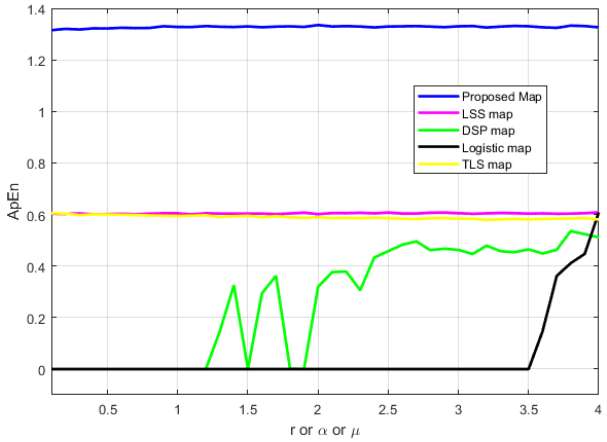

FIGURE 2. Comparison of ApEn complexity of 1-D chaotic maps.

A. CHAOTIC HEURISTIC SEARCH

The proposed hybrid method explores the features of chaos-based construction and algebraic group-based techniques which inherits most of the merits of the two approaches of S-boxes design. The first half of proposed method is dedicated to generation of key-dependent dynamic S-boxes of required size using improved chaotic map. It is done with the help of proposed heuristic search technique. The working steps of chaotic heuristic search for generation of key-dependent dynamic $n \times n$ S-boxes are as follows:

a) Choose initial values of X_0, Δ, N and size of S-box $n \in [5, 8]$.
b) Iterate new chaotic map (1) for Δ times and die out all values except the last
c) Take S_1, S_2, S_3 as empty arrays of size 2^n
d) Further iterate chaotic map (1) to get next chaotic value X
e) Get w such that $0 \leq w \leq 2^n$ -1 from current value X, If it doesn't belong to array S_1 then add w to S_1, else-if check for S_2, else check for S_3
f) Go for Steps-e until all three S_i are completely filled up.
g) Decide S_L which is best of all three S in terms of nonlinearity.
h) Update as $S_G = S_L$ if S_L has higher nonlinearity over S_G
i) Repeat Steps e to h for N generations.

TABLE 2. $A_1 = 5 \times 5$ S-box from heuristic search.

4	6	28	5	19	0	16	2
31	17	13	10	18	30	24	21
29	20	12	27	23	11	14	22
1	15	25	8	9	7	26	3

TABLE 3. $A_2 = 6 \times 6$ S-box from heuristic search.

7	43	27	33	29	39	3	23
37	4	42	32	61	62	12	20
24	56	31	2	21	16	5	53
26	59	41	22	50	57	49	17
36	1	8	48	19	28	35	0
13	14	34	25	40	6	55	58
30	15	46	44	63	11	52	60
51	54	9	18	45	38	47	10

The suggested chaos-based heuristic search is simulated for parameter settings of $X_0 = 0.234$, $r = 3.9$, $\Delta = 250$ and $N = 1000$ for different n. The S-boxes A_1 to A_4 obtained using suggested heuristic search after the given experimental setup are shown in Tables 2 to 5, respectively. The anticipated method is simulated using MATLAB on Intel Core i7 2.2 GHz, 4GB RAM, Windows 8 OS. In order to have an idea of the time complexity of proposed chaotic heuristic search method, we estimated the time taken to generate the initial S-box. It is found that the search takes 2.6s for 5×5, 6.154s for 6×6, 14.383s for 7×7, and 33.039s for 8×8 initial S-box generation. The time consumption of the proposed heuristic searching approach is satisfactorily nominal.

B. PROPOSED GROUP STRUCTURES AND ACTIONS

The algebraic based construction of S-boxes has been rigorously investigated in literature [49]–[52]. The second half of the proposed hybrid method involves the algebraic group based cryptographic features improvisation of S-boxes generated in previous section III.A. This step includes the determining the suitable groups whose action augments the S-box strength. This group finding approach needs to be exclusively carried out for each S-box. After rigorous experiments and simulations, the following algebraic groups are found to be

TABLE 4. $A_3 = 7 \times 7$ S-box from heuristic search.

5	79	93	11	1	115	63	57	125	12	50	27	91	40	65	47
97	16	23	58	67	107	78	59	92	110	68	55	72	122	15	90
22	35	87	7	62	74	99	8	111	73	28	51	114	44	54	18
119	94	121	96	95	70	103	20	10	4	0	69	13	76	116	36
3	89	106	83	2	75	104	38	112	118	101	43	88	60	48	33
14	64	42	105	113	25	34	109	86	41	82	126	117	6	127	108
81	37	19	84	30	32	61	39	56	124	53	24	102	49	45	9
98	123	77	46	85	29	66	21	100	31	17	26	80	52	120	71

TABLE 5. $A_4 = 8 \times 8$ S-box from heuristic search.

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

significant for the purpose. The determined algebraic groups with their actions are as follows:

The group $G_5 =< x : x^{32} = 1 >$ of order 32 with only one generator, that is, $x :=$ (27,24,28,21,3,11,5,25,17,9,23,26,8, 12,18,20,7,30,22,14,19,29,15,6,1,10,4,2,32,31,13,16); acts naturally on the index set $I_{\Omega i}$ of A_1 that is, 5×5 S-box from chaos-based search. This action can be defined as: $G_5 \times I_{\Omega i} \rightarrow I_{\Omega i}$, where $i = 1, 2, 3, \ldots, 32$; defined as for fixed g defined as, for fixed $g \epsilon\ G_5$, $\mu(g, \omega) = (\omega)\sigma_g$, $\omega \epsilon I_{\Omega i}$. The action of each element/permutation of the cyclic group G_5 on the index set of A_1 generates a distinct S-box. After thorough analysis and research, it has been revealed that the S-box related to the element $x^{27} \epsilon G_5$ offers the highest average value of non-linearity. Hence, through bijection from $I_{\Omega i}$ to A_1, we get S-box S_1 which is shown in Table 6.

The finite group $G_6 =< x, y, z : \mathrm{x}^4 = \mathrm{y}^{54} = \mathrm{z}^6 = [\mathrm{x}, \mathrm{y}] = [\mathrm{x}, \mathrm{z}] = 1 >$ of order 1296 with three generators, in terms of permutations defined on a set of 64 elements. Where

$x :=$ (1, 38, 17, 51)

$y :=$ (2, 48, 18, 57, 30, 61, 41, 32, 44, 22, 35, 43, 34, 62, 11, 16, 58, 37, 53, 10, 46, 47, 29, 45, 24, 56, 20, 8, 6, 14, 39, 52, 55, 50, 13, 31, 33, 60, 19, 23, 4, 64, 21, 59, 25, 9, 27, 54, 36, 28, 26, 15, 7, 63)

$z :=$ (3, 12, 40, 5, 42, 49)

TABLE 6. Proposed 5×5 S-box after G_5 group action.

22	24	18	0	25	19	15	1
14	3	5	4	10	17	20	27
28	2	11	31	13	9	12	26
8	21	30	29	23	6	16	7

where, $[x, y]$, $[x, z]$ are the commutators. The group G_6 acts naturally on the index set $I_{\Omega i}$ of A_2, that is, 6×6 S-box from chaos-based search. This action can be defined as: $G_6 \times I_{\Omega i} \rightarrow I_{\Omega i}$, where $i = 1, 2, 3, \ldots, 64$; defined as for fixed g defined as, for fixed $g \epsilon G_6$, $\mu(g, \omega) = (\omega)\sigma_g$, $\omega \epsilon I_{\Omega i}$. The action of each element/permutation of the cyclic group G_6 on the index set of A_2 generates a distinct S-box. After thorough analysis and research, it has been revealed that the S-box related to the element $x^3 y^{47} z^5 \epsilon\ G_6$ offers the highest average value of

TABLE 7. Proposed 6 × 6 S-box after G_6 group action.

40	30	5	15	53	58	24	21
18	41	34	23	4	3	26	28
59	11	43	60	19	35	7	32
55	45	12	42	38	54	31	33
62	10	22	14	9	63	47	61
44	29	20	16	27	51	37	6
0	25	2	8	17	13	46	39
1	48	49	56	36	57	52	50

non-linearity. Hence, through bijection from $I_{\Omega i}$ to A_2, we get S-box S_2 which is shown in Table 7.

The algebraic group $C_{57876} \times C_4 \times C_2$ of order 463008 having following finite representation:

$$G_7 = \left\langle x, y, t, u, v \,|x^{53}, y^{52}, t^{14}, u^4, v^3, [x, y], [x, t], [x, u], [x, v], [y, t], [y, u], [y, v], [t, u], [u, v] \right\rangle$$

with five generators which are as follows:

$x :=$ (1, 83, 101, 22, 98, 71, 44, 122, 31, 36, 47, 105, 80, 58, 17, 85, 89, 128, 84, 5, 108, 11, 4, 23, 118, 77, 41, 99, 18, 50, 25, 34, 35, 48, 82, 86, 93, 2, 55, 32, 121, 15, 12, 107, 6, 125, 74, 91, 72, 27, 24, 40, 30)

$y :=$ (3, 102, 67, 115, 103, 68, 37, 78, 92, 97, 8, 10, 109, 53, 20, 100, 29, 127, 95, 52, 61, 38, 64, 45, 90, 124, 19, 16, 126, 56, 14, 13, 116, 79, 69, 94, 73, 110, 112, 62, 123, 33, 87, 42, 26, 7, 43, 113, 49, 111, 63, 60)

$t :=$ (9, 120, 81, 28, 59, 88, 51, 46, 114, 76, 65, 117, 96, 57)

$u :=$ (21, 75, 39, 106)

$v :=$ (66, 104, 70)

The group G_7 acts as right multiplication on the index set $I_{\Omega i}$ of A_3, that is, 7 × 7 S-box from chaos-based search. This action can be defined as: $G_7 \times I_{\Omega i} \rightarrow I_{\Omega i}$, where $i = 1, 2, 3, \ldots, 128$; defined as for fixed g defined as, for fixed $g \epsilon G_7$, $\mu(g, \omega) = (\omega)\sigma_g$, $\omega \epsilon I_{\Omega i}$. The action of each element or permutation of the cyclic group G_7 on the index set of A_3 generates a distinct S-box. After thorough analysis and research, it has been revealed that the S-box related to the element $x^{27}y^{11}t^3u^3v^2 \epsilon G_7$ offers the highest average value of non-linearity. Hence, through bijection from $I_{\Omega i}$ to A_3, we get S-box S_3 which is shown in Table 8.

The algebraic group $G_8 = C_{32075600} \times C_2 \times C_2$ of order 128302400 with six generators $G_8 =< a, b, c, d, e, f >$. The algebraic group G_8 can be generated by generators with cycles 106, 89, 25, 16, 17 and 2. Where,

$a :=$ (1, 26, 109, 163, 104, 230, 145, 231, 223, 172, 37, 126, 92, 67, 97, 140, 232, 22, 59, 214, 180, 113, 237, 12, 226, 51, 128, 215, 233, 90, 105, 219, 149, 52, 221, 70, 244, 17, 242, 179, 68, 176, 120, 134, 56, 222, 194, 9, 63, 116, 110, 169, 256, 196, 240, 117, 198, 18, 254, 49, 189, 123, 31, 64, 224, 69, 160, 143, 228, 108, 167, 20, 152, 182, 208, 130, 129, 171, 19, 141, 84, 99, 54, 165, 14, 142, 199, 6, 8, 124, 212, 173, 119, 250, 48, 91, 207, 33, 197, 177, 154, 2, 87, 50, 55, 57)

$b :=$ (3, 159, 16, 131, 112, 30, 193, 7, 93, 203, 44, 146, 190, 137, 21, 103, 243, 164, 132, 72, 247, 42, 118, 4, 60, 74, 216, 249, 35, 192, 95, 220, 166, 71, 191, 88, 65, 170, 202, 81, 210, 83, 38, 89, 28, 62, 27, 148, 186, 248, 151, 82, 75, 236, 122, 85, 168, 34, 86, 133, 10, 121, 61, 147, 229, 66, 239, 136, 111, 114, 181, 24, 187, 150, 178, 138, 175, 40, 76, 5, 115, 36, 23, 80, 184, 106, 96, 255, 25)

$c :=$ (11, 174, 43, 156, 125, 41, 213, 135, 211, 45, 206, 77, 225, 13, 188, 205, 218, 39, 201, 253, 238, 94, 101, 234, 153)

$d :=$ (15, 209, 78, 144, 185, 157, 245, 200, 102, 46, 29, 158, 217, 227, 79, 235)

$e :=$ (32, 127, 251, 252, 241, 195, 53, 183, 58, 47, 139, 246, 204, 100, 107, 98, 161)

$f :=$ (73, 155)

The group G_8 acts as right multiplication on the index set $I_{\Omega i}$ of A_3, that is, 8 × 8 S-box from chaos-based search. This action can be defined as: $G_8 \times I_{\Omega i} \rightarrow I_{\Omega i}$, where $i = 1, 2, 3, \ldots, 256$; defined as for fixed g defined as, for fixed $g \epsilon G_8$, $\mu(g, \omega) = (\omega)\sigma_g$, $\omega \epsilon I_{\Omega i}$. The action of each element or permutation of the cyclic group G_8 on the index set of A_3 generates a distinct S-box. After thorough analysis and research, it has been revealed that the S-box related to the element $a^{37}b^{54}c^4d^{31}e^7f \epsilon G_8$ offers the highest average value of non-linearity. Hence, through bijection from $I_{\Omega i}$ to A_4, we get S-box S_4 which is shown in Table 9.

The general perspective of the proposed method for bijective S-boxes generation is described through the schematic diagram shown in Figure 3.

V. PERFORMANCE ANALYSES

This section evaluates the performance of created S-boxes using suggested method. The standard criterions are adopted to assess and evaluate the features of S-boxes. The security performance of our proposed method and S-boxes are also compared with recently available S-boxes in the literature.

A. NONLINEARITY

Linearity is curse in cryptography and nonlinearity assure that the output is not the linear combination of input vectors. The nonlinearity measure of a Boolean function f is computed by knowing the least distance of f to the set of all affine functions [53]. Thus, the constituent functions of S-box should have standing nonlinearities scores. The nonlinearity NL_f of

TABLE 8. Proposed 7 × 7 S-box after G_6 group action.

42	103	69	78	24	80	110	81	85	57	11	53	40	20	27	23
113	94	26	95	101	37	29	8	35	73	59	125	84	5	7	100
17	87	18	54	83	13	124	122	19	34	63	31	36	0	56	64
98	92	55	127	102	70	90	52	3	97	21	116	96	9	45	74
44	39	32	61	48	89	51	68	6	82	99	121	111	62	46	4
10	25	30	1	86	117	22	14	71	114	38	60	79	2	120	43
126	104	16	58	107	93	77	75	33	67	115	50	12	112	119	49
28	109	106	91	123	88	66	108	65	15	76	41	118	47	72	105

TABLE 9. Proposed 8 × 8 S-box after G_6 group action.

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

any Boolean function f is computed as:

$$NL_f = \frac{1}{2}(2^n - S_{\max}(f))$$

where, $S_{\max}(f)$ is the Walsh-Hadamard transform of Boolean function f [54]. A Boolean function is deemed frail if it tends to have poor nonlinearity. The maximization of nonlinearity of balanced Boolean functions is considered one of the prominent measures responsible for providing power against the any type of linear attacks [16], [54]. The nonlinearity scores of all component Boolean functions inherent to proposed four $n \times n$ S-boxes are provided in Table 10. It can be seen that the group actions improvise the nonlinearity feature of all four S-boxes. The average nonlinearity score is 12, 24.33, 54, and 114 for S-boxes of size 5×5, 6×6, 7×7, and 8×8, respectively, which show excellent nonlinearity performance.

TABLE 10. Nonlinearities of proposed bijective S-boxes.

Proposed S-box	nl_1	nl_2	nl_3	nl_4	nl_5	nl_6	nl_7	nl_8
5×5	12	12	12	12	12			
6×6	24	24	24	26	24	24		
7×7	54	54	54	54	54	54	54	
8×8	114	116	114	114	112	114	114	114

B. STRICT AVALANCHE CRITERIA

The strict avalanche criterion is dealt with sensitivity of slightest possible change in the input data. The idea of SAC was described by Tavares and Webster, which gets its base on the completeness effect's notion and the avalanche [55]. This criterion measures that by making a single change in input bits, how much output bits get altered. The SAC assumed as satisfied when all the output bits are changed with a likelihood of 0.5, when only one input bit is flipped. The calculated average SAC scores for all four S-boxes are shown in Table 11. The outcomes show that proposed S-boxes found to satisfy the strict avalanche criterion quite well as their values are quite close to ideal value.

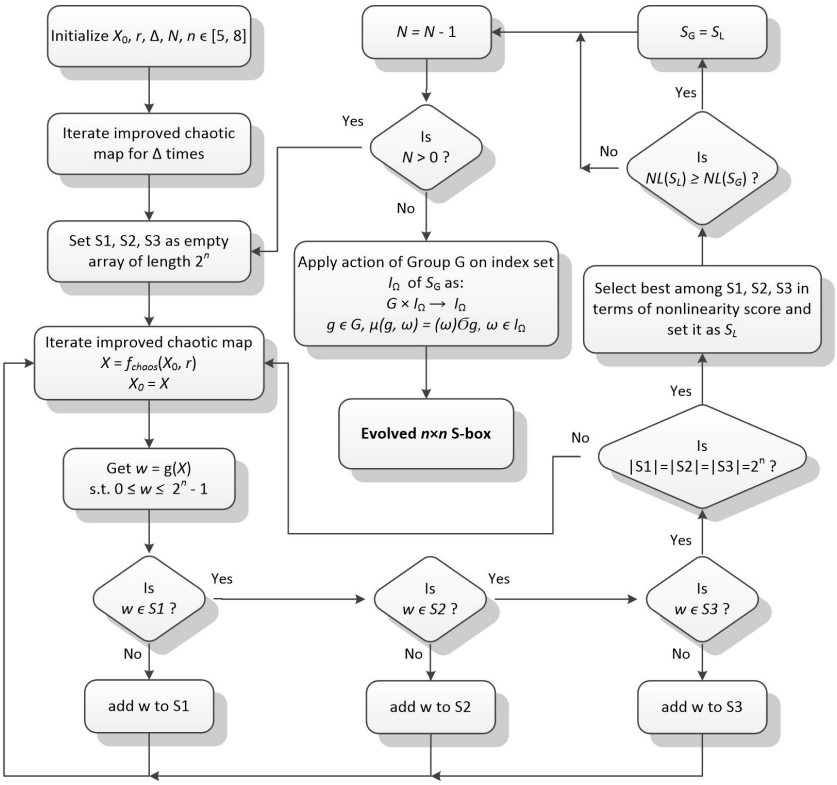

FIGURE 3. Schematic diagram of S-box generation using proposed hybrid method.

TABLE 11. SAC and BIC outcomes of our bijective S-boxes.

Proposed S-box	SAC	BIC-SAC	BIC-NL
5×5	0.5600	0.4975	9.4
6×6	0.5104	0.5042	21.73
7×7	0.5006	0.4987	48.09
8×8	0.4978	0.4979	103.86

TABLE 12. Differential and linear approximation probabilities of proposed S-boxes.

Proposed S-box	DP	LAP
5×5	0.1875	0.1325
6×6	0.09375	0.2188
7×7	0.0625	0.1718
8×8	0.04687	0.125

C. BITS INDEPENDENCE CRITERIA

The input bits which remain unchanged are explored under bits independence criterion. The revamping of independent performance of pairwise variables of avalanche vectors and unaltered input bits are the assets of this measure. It is an effective criterion in symmetric cryptosystem, because by augmenting independence between bits, the recognition and prediction of patterns of the system is not possible [56]. The average BIC outcomes with respect to SAC and nonlinearity are delivered in Table 11. The BIC analysis results verifies the acceptable performance of proposed method as the BIC-SAC are close to ideal value and BIC-NL are quite higher as desired for strong security.

TABLE 13. Comparison of nonlinearities of bijective S-boxes.

S-box	Ref. [21]	Ref. [39]	Ref. [59]	Ref. [60]	Proposed
5×5	11.2	11.2	10	10	12
6×6	23.67	23.67	22	22	24.33
7×7	51.14	51.71	48	48	54
8×8	108.5	109.5	98	104	114

D. DIFFERENTIAL PROBABILITY

The differential probability measures the resistivity of an S-Box against the differential cryptanalysis. The attack procedure of cryptanalysis was given by Biham and Shamir; it is related with developing imbalance on the input/output dissemination to assault block ciphers and S-boxes [57]. Confrontation to this cryptanalysis can be consummate if the EX-OR of each output has identical probability with the EX-OR value of each input. If an S-box is uniform in input/output distribution, then it is said to be resistant. It is

TABLE 14. Comparison of DP and LAP of bijective S-boxes.

S-box	Differential probability			Linear approximate probability		
	Ref. [21]	Ref. [39]	Proposed	Ref. [21]	Ref. [39]	Proposed
5×5	0.1875	0.1875	0.1875	0.3125	0.25	0.3125
6×6	0.09375	0.125	0.09375	0.2188	0.25	0.2188
7×7	0.0625	0.0781	0.0625	0.1875	0.1875	0.1718
8×8	0.0391	0.0391	0.04687	0.1328	0.1328	0.125

preferred that the largest value of differential probability (DP) in EX-OR table should be as small as possible. The differential probability for a S-box S is measured as:

$$DP = \max_{\delta a \neq 0, \delta b} \left(\frac{\#\{a \in A | S(a) \oplus S(a \oplus \delta a) = \delta b\}}{2^n} \right)$$

where, set A holds all probable input values and the figure of its elements is 2^n. The largest value of EX-OR table for an S-box should be as small enough to resist the cryptanalysis. The largest DP for our bijective S-boxes are shown in Table 12. The differential probabilities of suggested S-boxes are obtained as low as 0.1875, 0.09375, 0.0625, and 0.04875 for S-boxes of size 5×5, 6×6, 7×7, and 8×8, respectively, which are considerably pretty.

E. LINEAR APPROXIMATION PROBABILITY

The method of linear approximation probability (LAP) is helpful in calculating the imbalance of an incident. The largest value of imbalance of an event is measured with the help of the analysis introduced by Matsui in [58]. There must be no difference between output and input bits uniformity. Each of the input bits with its results in output bits is examined individually. If all the input elements are 2^n, the class of all possible inputs is d and the masks applied on the equality of output and input bits are respectively m_a and m_b, then maximum linear approximation is the maximum number of same results and calculated as:

$$LAP = \max_{m_a, m_b \neq 0} \left| \frac{\#\{a \in A | a.m_a = b.m_b\}}{2^n} - 0.5 \right|$$

A lower value of this probability indicates that S-box is more capable to fight against linear cryptanalysis attack. The outcomes of this crucial analysis acquired for proposed S-boxes are listed in Table 12.

F. COMPARISON ANALYSIS

This section provides comparison of experimental results and cryptographic features of proposed S-boxes with some recent and state of the art S-box studies. The nonlinearity scores of bijective S-boxes are compared in Table 13. It is clear from the comparison Table that the proposed four bijective S-boxes offers considerably better resistance to linear attacks and offer high nonlinear transformation of input data to ciphertext data as compared to other S-boxes investigated in [21], [39], [59], [60]. The differential probabilities and linear approximation probabilities of proposed S-boxes and other similar kind of S-boxes are compared in Table 14. Again, the proposed S-boxes found to have better resistance to differential and linear cryptanalysis to attack S-boxes and block ciphers. This is because; our S-boxes have lower values of these two indicators as compared to other similar bijective S-box studies.

The design of S-boxes of size 8×8 has its own significance, therefore most of the S-boxes proposals are particularly dedicated to 8×8 sizes. It is fair to assess and scrutinize the proposed 8×8 S-box against some recent S-boxes proposals. The comparison Table 15 is maintain for the purpose which provides the average nonlinearity, average SAC, average BIC-NL, differential uniformity, and linear probability of different 8×8 S-boxes. The comparison analysis reveals the following facts about the proposed 8×8 S-box in terms of performance strength and features.

- The nonlinearity has been considered as main (maximization) target while designing strong S-boxes. Reason being, it is mainly liable for mitigating all linear approximation based assaults. The remarkable achievement of our proposed research finding is that with proposed method we are able to get the S-box having nonlinearity of 114 which is pretty higher than all 8×8 S-boxes available in literature [19], [22], [29], [40], [42], [61]–[83] including AES S-boxes where it's bound is 112. Thus, the proposed S-box holds excellent nonlinearity performance compared to all competitor S-boxes. It is worth mention the proposed method holds the significant merit over the existing S-box methods previously investigated in [40], [42], [61], [67], [69], [77]–[83] in terms of nonlinearity performance as minimum NL of 112, maximum NL of 116 and average NL of 114 is achieved with the proposed method.
- The SAC score of 0.4978 is quite close to ideal value of 0.5 and have an offset of only 0.0022 which is negligible. The SAC performance of our 8×8 S-box is found to be comparable and acceptable.
- The proposed S-box also has satisfactory BIC performance like other S-boxes as it has been found that all avalanche variable pairs are quite independent to each other.

TABLE 15. Comparison of cryptographic features of recent 8 × 8 S-boxes.

S-box	NL_{min}	NL_{max}	NL_{avg}	SAC	BIC-NL	DP	LAP
Proposed	112	116	114	0.4978	103.86	0.04687	0.125
Ref. [19]	96	106	102.5	0.5037	103.9	0.0391	0.125
Ref. [22]	112	112	112	0.5058	112	0.01563	0.0625
Ref. [30]	106	108	107.5	0.4943	104.36	0.0391	0.125
Ref. [40]	110	112	110.25	0.5	105.2	0.0391	0.125
Ref. [42]	100	110	106.75	0.5002	104	0.1172	0.125
Ref. [61]	104	110	106.25	0.5032	103.9	0.0391	0.1328
Ref. [62]	104	110	107	0.5101	106.25	0.0391	0.1484
Ref. [63]	106	108	106.5	0.5009	104.07	0.0391	0.1328
Ref. [64]	106	110	108	0.4988	102.86	0.04687	0.1406
Ref. [65]	110	112	110.25	0.4953	104.07	0.0391	0.125
Ref. [66]	100	108	105	0.5002	103	0.04687	0.125
Ref. [67]	106	110	107.75	0.4976	105.07	0.0391	0.125
Ref. [68]	104	108	106.25	0.5009	103.64	0.0391	0.1328
Ref. [69]	104	110	106	0.4978	103.92	0.04687	0.1563
Ref. [70]	104	108	106.75	0.5031	103.64	0.04687	0.1484
Ref. [71]	100	108	104.7	0.4982	103.1	0.0391	0.1406
Ref. [72]	106	108	106.5	0.5046	104.14	0.0391	0.1328
Ref. [73]	106	108	106.7	0.4941	103.5	0.0391	0.125
Ref. [74]	98	110	105.5	0.4937	105.7	0.125	0.1172
Ref. [75]	108	110	108.75	0.4946	102.78	0.0391	0.1328
Ref. [76]	100	108	105	0.5007	104.14	0.0391	0.1328
Ref. [77]	102	108	105	0.5029	102.9	0.04687	0.14844
Ref. [78]	112	112	112	0.4956	112	0.01563	0.0625
Ref. [79]	96	106	102.5	0.5178	102.5	0.21094	-
Ref. [80]	102	112	110	0.5066	109	0.03125	0.1093
Ref. [82]	98	106	103.5	0.4958	103.5	0.05469	0.1328
Ref. [83]	96	104	100.5	0.4973	102.78	0.0391	0.15625

- For our S-box, the imbalance on the input/output EX-OR distribution is calculated as differential probability whose maximum value is 0.04687 which is capable to resist the differential cryptanalysis in better way as compared to the S-boxes found in [22], [74], [82] and comparable to other findings. But, the S-boxes available in [40], [42], [61], [78], [80] have merits over our S-box due to better I/O EX-OR differential distribution.
- The low value of linear approximation probability is essential to withstand the attack suggested by Mitsui [58]. The LAP value of 0.125 is lower and thus better than S-boxes investigated in [61]–[64], [68]–[72], [75], [76], [82], [83]. However, the S-boxes

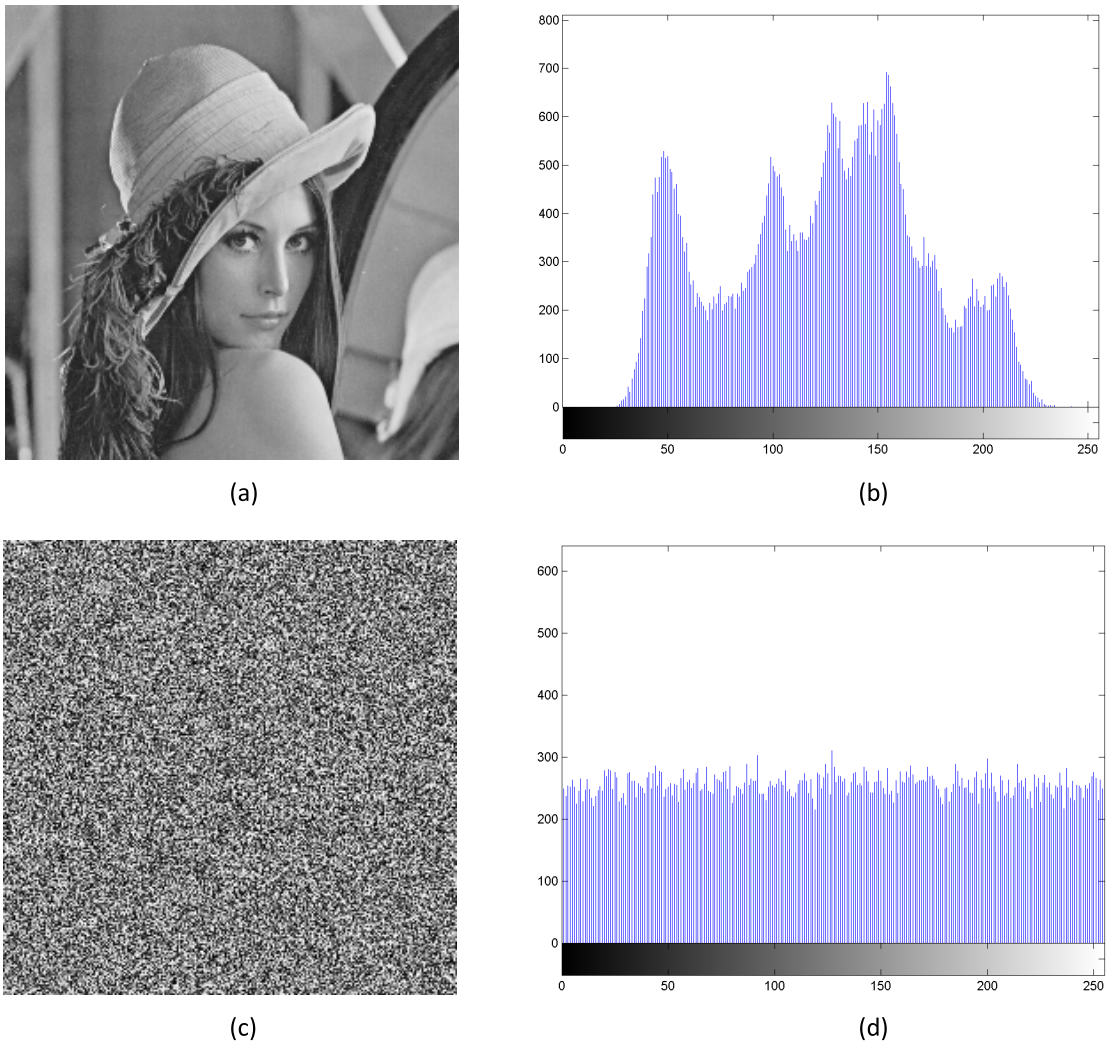

FIGURE 4. Lena plain-image and encrypted image using proposed S-box substitution with histograms.

TABLE 16. MLC statistical encryption performance results for 256 × 256 *Lena* image.

Lena image	Entropy	Correlation	Contrast	Energy	Homogeneity
Plain-image	7.4439	0.902495	0.448254	0.112748	0.862215
Encrypted	7.9969	-0.001496	10.42533	0.015635	0.390185
Ref. [42]	7.9968	-0.00114	10.51509	0.015647	0.389625

of [22], [74], [78], [80] have advantage of having better LAP performance.

G. ENCRYPTION APPLICATION OF S-BOX

Information encryption has always been a mechanism to protect and secure the information from the illegal usage and access for decades. In today's era of social media and fast communication facilities, the image based communication is one of the preferred means [84], [85]. to check the suitability of proposed S-box for encryption applications. We apply our proposed 8×8 S-box shown in Table 9 to encrypt the standard 8-bit encoded gray-scale *Lena* plain-image of size 256×256 using the two-way S-box substitution process; where the S-box substitution of image is done in forward direction starting from first pixel to last, and then the same S-box is applied to perform the backward substitution of image starting from last pixel to first. The *Lena* plain-image and its histogram are shown in Figure 4(a)-(b). The obtained encrypted image and its histogram are also depicted in Figure 4(c)-(d). Its clear from the encrypted image and its histogram that the S-box can offer good visual encryption effect as the encrypted image is highly indistinguishable and the distribution of

its pixels is fairly uniform. The encryption effect is also quantified through the well-known Majority Logic Criteria (MLC). The different statistical tests available under MLC suite are *entropy*, *correlation*, *contrast*, *energy*, and *homogeneity* whose details are available in [15], [23], [42]. The scores of MLC tests for plain -image and encrypted image available in Figure 4 are listed in Table 16. The scores shown in Table show the satisfactory performance of proposed S-box for the multimedia information encryptions.

VI. CONCLUSION

The algebraic group theory based and chaos-based are the two prominent design methods for constructing S-boxes. These design paradigms have their own set of merits for security applications. In this paper, the two approaches are explored to propose a hybrid method for constructing not bijective S-boxes. The hybrid method makes use of proposed improved chaotic map to execute the chaotic heuristic searching of initial S-boxes. The security strengths of generated bijective S-boxes are augmented with the help of proposed potent algebraic groups which are constructed after rigorous experiments. The algebraic group actions improvise the cryptographic features of S-boxes. The experimental results show the proposed S-boxes satisfied the standard criterions for the competent S-boxes well. The proposed S-box generation method has the advantageous capability of constructing highly nonlinear variable sized $n \times n$ (for $5 \leq n \leq 8$) S-boxes. Moreover, another merit of our method is that the nonlinearity score of 114 is achieved for 8×8 S-box using the proposed method which is highest among all available 8×8 S-boxes in literature including [40], [42], [61], [67], [69], [77]–[80]. Moreover, the comparative study is also carried out with S-boxes of recent proposals to assess over all standing. It has been found that the proposed bijective S-boxes have better nonlinearity, SAC, and linear approximation probability features as compared to most of the available S-boxes.

REFERENCES

[1] F. A. Kadhim, G. H. Abdul-Majeed, and R. S. Ali, "Enhancement CAST block algorithm to encrypt big data," in *Proc. Annu. Conf. New Trends Inf. Commun. Technol. Appl. (NTICT)*, Mar. 2017, pp. 80–85.

[2] A. K. Farhan and M. A. A. J. Ali, "Database protection system depend on modified hash function," in *Proc. 2nd Int. Conf. Cihan Univ.-Erbil Commun. Eng. Comput. Sci.*, 2017, p. 84.

[3] H. S. Alhadawi, M. F. Zolkipli, S. M. Ismail, and D. Lambić, "Designing a pseudorandom bit generator based on LFSRs and a discrete chaotic map," *Cryptologia*, vol. 43, no. 3, pp. 190–211, May 2019.

[4] U. A. Waqas, M. Khan, and S. I. Batool, "A new watermarking scheme based on Daubechies wavelet and chaotic map for quick response code images," *Multimedia Tools Appl.*, vol. 79, pp. 6891–6914, Dec. 2019.

[5] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, vol. 21, no. 10, p. 958, Sep. 2019.

[6] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2005.

[7] A. M. Ali and A. K. Farhan, "A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-document," *IEEE Access*, vol. 8, pp. 80290–80304, 2020.

[8] A. M. Ali and A. K. Farhan, "Enhancement of QR code capacity by encrypted lossless compression technology for verification of secure E-document," *IEEE Access*, vol. 8, pp. 27448–27458, 2020.

[9] L. R. Knudsen and M. Robshaw, *The Block Cipher Companion*. Springer, 2011.

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

[11] M. Ahmad, E. Al Solami, X.-Y. Wang, M. N. Doja, M. M. Beg, and A. A. Alzaidi, "Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos," *Symmetry*, vol. 10, no. 7, p. 266, 2018.

[12] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Process.*, vol. 164, pp. 249–266, Nov. 2019.

[13] A. Rafiq and M. Khan, "Construction of new S-boxes based on triangle groups and its applications in copyright protection," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 15527–15544, Jun. 2019.

[14] 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.

[15] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar, and A. Razaq, "Comparison of pre and post-action of a finite Abelian group over certain nonlinear schemes," *IEEE Access*, vol. 8, pp. 39781–39792, 2020.

[16] 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.

[17] I. Shahzad, Q. Mushtaq, and A. Razaq, "Construction of new S-box using action of quotient of the modular group for multimedia security," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, Nov. 2019.

[18] I. Hussain, N. A. Azam, and T. Shah, "Stego optical encryption based on chaotic S-box transformation," *Opt. Laser Technol.*, vol. 61, pp. 50–56, Sep. 2014.

[19] A. A. A. El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019.

[20] A. Belazi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Selective image encryption scheme based on DWT, AES S-box and chaotic permutation," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, pp. 606–610.

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

[22] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-the Advanced Encryption Standard*. Springer, 2013.

[23] A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shuaib, W. Aslam, and M. Alawida, "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," *IEEE Access*, vol. 8, pp. 75473–75490, 2020.

[24] M. Ahmad, D. Bhatia, and Y. Hassan, "A novel ant colony optimization based scheme for substitution box design," *Procedia Comput. Sci.*, vol. 57, pp. 572–580, Jan. 2015.

[25] M. Ahmad, H. Chugh, A. Goel, and P. Singla, "A chaos based method for efficient cryptographic S-box design," in *Proc. Int. Symp. Secur. Comput. Commun.* Berlin, Germany: Springer, Aug. 2013, pp. 130–137.

[26] H. Isa, N. Jamil, and M. R. Z'Aba, "Construction of cryptographically strong S-boxes inspired by bee waggle dance," *New Gener. Comput.*, vol. 34, no. 3, pp. 221–238, Aug. 2016.

[27] M. Ahmad and M. Malik, "Design of chaotic neural network based method for cryptographic substitution box," in *Proc. Int. Conf. Electr., Electron., Optim. Techn. (ICEEOT)*, Mar. 2016, pp. 864–868.

[28] M. Ahmad, N. Mittal, P. Garg, and M. M. Khan, "Efficient cryptographic substitution box design using travelling salesman problem and chaos," *Perspect. Sci.*, vol. 8, pp. 465–468, Sep. 2016.

[29] N. Nedjah and L. D. M. Mourelle, "Designing substitution boxes for secure ciphers," *Int. J. Innov. Comput. Appl.*, vol. 1, no. 1, pp. 86–91, 2007.

[30] 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.

[31] 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.

[32] G. Liu, W. Yang, W. Liu, and Y. Dai, "Designing S-boxes based on 3-D four-wing autonomous chaotic system," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1867–1877, Dec. 2015.

[33] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and S8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.
[34] Ü. Çavuşoğlu, 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.
[35] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, 2017.
[36] F. Özkaynak and A. B. Özer, "A method for designing strong S-boxes based on chaotic lorenz system," *Phys. Lett. A*, vol. 374, no. 36, pp. 3733–3738, Aug. 2010.
[37] M. Khan and T. Shah, "A construction of novel chaos base nonlinear component of block cipher," *Nonlinear Dyn.*, vol. 76, no. 1, pp. 377–382, Apr. 2014.
[38] I. Hussain, T. Shah, M. A. Gondal, W. A. Khan, and H. Mahmood, "A group theoretic approach to construct cryptographically strong substitution boxes," *Neural Comput. Appl.*, vol. 23, no. 1, pp. 97–104, Jul. 2013.
[39] 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.
[40] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. A. Solami, and M. M. S. Beg, "A new 1D chaotic map and β-Hill climbing for generating substitution-boxes," *IEEE Access*, vol. 6, pp. 55405–55418, Oct. 2018.
[41] M. Alawida, A. Samsudin, and J. S. Teh, "Enhancing unimodal digital chaotic maps through hybridisation," *Nonlinear Dyn.*, vol. 96, no. 1, pp. 601–613, Apr. 2019.
[42] 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.
[43] M. Alawida, A. Samsudin, and J. S. Teh, "Enhanced digital chaotic maps based on bit reversal with applications in random bit generators," *Inf. Sci.*, vol. 512, pp. 1155–1169, Feb. 2020.
[44] M. Alawida, A. Samsudin, J. S. Teh, and W. H. Alshoura, "Digital cosine chaotic map for cryptographic applications," *IEEE Access*, vol. 7, pp. 150609–150622, 2019.
[45] Ashish, J. Cao, and R. Chugh, "Chaotic behavior of logistic map in superior orbit and an improved chaos-based traffic control model," *Nonlinear Dyn.*, vol. 94, no. 2, pp. 959–975, Oct. 2018.
[46] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, pp. 172–182, Apr. 2014.
[47] A. Mansouri and X. Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," *Inf. Sci.*, vol. 520, pp. 46–62, May 2020.
[48] Q. Lu, C. Zhu, and G. Wang, "A novel S-box design algorithm based on a new compound chaotic system," *Entropy*, vol. 21, no. 10, p. 1004, Oct. 2019.
[49] N. Munir and M. Khan, "A generalization of algebraic expression for nonlinear component of symmetric key algorithms of any characteristic p," in *Proc. Int. Conf. Appl. Eng. Math. (ICAEM)*, Sep. 2018, pp. 48–52.
[50] A. Razaq, H. A. Al-Olayan, A. Ullah, A. Riaz, and A. Waheed, "A novel technique for the construction of safe substitution boxes based on cyclic and symmetric groups," *Secur. Commun. Netw.*, vol. 2018, Oct. 2018, Art. no. 4987021.
[51] M. Khan and N. A. Azam, "Right translated AES gray S-boxes," *Secur. Netw. Commun.*, vol. 8, no. 9, pp. 1627–1635, 2015.
[52] A. Razaq, A. Ullah, and A. Waheed, "A novel technique to improve nonlinearity of substitution box without disturbing its mathematical properties," *Wireless Pers. Commun.*, vol. 111, pp. 2091–2105, Nov. 2019.
[53] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Amsterdam, The Netherlands: Elsevier, 2009.
[54] 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.
[55] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology* (Lecture Notes in Computer Science). 1985, pp. 523–534.
[56] C. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," *J. Cryptol.*, vol. 3, no. 1, pp. 27–41, Jan. 1990.
[57] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," in *Advances in Cryptology* (Lecture Notes in Computer Science). 1990, pp. 2–21.
[58] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology* (Lecture Notes in Computer Science). 1993, pp. 386–397.
[59] E. Laskari, G. Meletiou, and M. Vrahatis, "Utilizing evolutionary computation methods for the design of S-boxes," in *Proc. Int. Conf. Comput. Intell. Secur.*, Nov. 2006, pp. 1299–1302.
[60] P. Tesař, "A new method for generating high non-linearity S-boxes," *Radioengineering*, vol. 19, pp. 23–26, Apr. 2010.
[61] 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.
[62] 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.
[63] 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, pp. 699–711, Jan. 2020, doi: 10.1007/s11071-020-05503-y.
[64] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A new design of cryptosystem based on S-box and chaotic permutation," *Multimedia Tools Appl.*, Mar. 2020.
[65] 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, Jun. 2020.
[66] 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.
[67] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu, and J. Liu, "A novel block encryption algorithm based on chaotic S-box for wireless sensor network," *IEEE Access*, vol. 7, pp. 53079–53090, 2019.
[68] M. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dyn.*, vol. 99, pp. 3041–3064, Dec. 2019.
[69] A. K. Farhan, R. S. Ali, H. Natiq, and N. M. G. Al-Saidi, "A new S-box generation algorithm based on multistability behavior of a plasma perturbation model," *IEEE Access*, vol. 7, pp. 124914–124924, 2019.
[70] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, "A novel construction of substitution box involving coset diagram and a bijective map," *Secur. Commun. Netw.*, vol. 2017, Nov. 2017, Art. no. 5101934.
[71] 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.
[72] N. A. Azam, U. Hayat, and I. Ullah, "Efficient construction of a substitution box based on a mordell elliptic curve over a finite field," *Frontiers Inf. Technol. Electron. Eng.*, vol. 20, no. 10, pp. 1378–1389, Oct. 2019.
[73] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3317–3326, Aug. 2019, doi: 10.1007/s00521-017-3287-y.
[74] M. Khan and T. Shah, "A novel construction of substitution box with zaslavskii chaotic map and symmetric group," *J. Intell. Fuzzy Syst.*, vol. 28, no. 4, pp. 1509–1517, 2015.
[75] T. Zhang, C. L. P. Chen, L. Chen, X. Xu, and B. Hu, "Design of highly nonlinear substitution boxes based on I-ching operators," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3349–3358, Dec. 2018.
[76] 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.
[77] 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.
[78] 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.
[79] M. Ş. Açikkapi, F. Özkaynak, and A. B. Özer, "Side-channel analysis of chaos-based substitution box structures," *IEEE Access*, vol. 7, pp. 79030–79043, 2019, doi: 10.1109/ACCESS.2019.2921708.
[80] M. F. Khan, A. Ahmed, K. Saleem, and T. Shah, "A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system," *IEEE Access*, vol. 7, pp. 84980–84991, 2019.
[81] 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.
[82] A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Sci. Rep.*, vol. 10, no. 1, pp. 1–16, Dec. 2020.

[83] 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.
[84] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran, A. K. Bashir, O.-Y. Song, and W. Mazurczyk, "Providing end-to-end security using quantum walks in IoT networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020.
[85] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. A. El-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci.*, vol. 515, pp. 191–217, Apr. 2020.

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. Since 2011, he has been an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia, New Delhi. He has published over 70 research papers in international reputed refereed journals and conference proceedings. His research interests include, but not limited to, multimedia security, chaos-based cryptography, cryptanalysis, image processing, and optimization techniques.

EESA AL-SOLAMI received the bachelor's degree in computer science from King Abdulaziz University, Saudi Arabia, in 2002, and the master's degree in information technology and the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2008 and 2012, respectively. He is currently an Assistant Professor with the Department of Information Security, University of Jeddah, Saudi Arabia. His major research interests include information security and biometric technology.

AHMED MOHAMMED ALGHAMDI received the B.Sc. degree in computer science and the M.Sc. degree in business administration from King Abdulaziz University, Jeddah, Saudi Arabia, in 2005 and 2010, respectively, the master's degree in Internet computing and network security from Loughborough University, U.K., in 2013, and the Ph.D. degree in computer science from King Abdulaziz University. He is currently an Assistant Professor with the Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia. He has also over 11 years of working experience before attending the academic carrier. His research interests include high-performance computing, big data, distributed systems, programming models, software engineering, and software testing.

MUHAMMAD AWAIS YOUSAF received the Ph.D. degree in combinatorial group theory from the Department of Mathematics, Quaid-i-Azam University, Islamabad, in 2015. He is currently working as an Assistant Professor with The Islamia University of Bahawalpur. His main research interests include theory of group graphs, chemical graph theory, algebraic cryptography, homomorphic public-key cryptosystems over groups, and algorithms development over galois fields.