IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 31, 2020, accepted April 20, 2020, date of publication April 22, 2020, date of current version May 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989676

A Novel Method for Generation of Strong Substitution-Boxes Based on Coset Graphs and Symmetric Groups

ABDUL RAZAQ[1], HANAN ALOLAIYAN[2], MUSHEER AHMAD[3], MUHAMMAD AWAIS YOUSAF[4], UMER SHUAIB[5], WAQAR ASLAM[6], (Member, IEEE), AND MOATSUM ALAWIDA[7]

[1]Department of Mathematics, Division of Science and Technology, University of Education, Lahore 54770, Pakistan
[2]Department of Mathematics, King Saud University, Riyadh 11451, Saudi Arabia
[3]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[4]Department of Mathematics, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
[5]Department of Mathematics, Government College University Faisalabad, Faisalabad 38000, Pakistan
[6]Department of Computer Science and Information Technology, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
[7]School of Computer Sciences, Universiti Sains Malaysia, Minden 11800, Malaysia

Corresponding author: Musheer Ahmad (musheer.cse@gmail.com)

This work was supported by the Research Center of the Center for Female Scientific and Medical Colleges, Deanship of Scientific Research, King Saud University.

ABSTRACT The success of AES encryption standard created challenges for the cryptographers to construct strong substitution-boxes using different underlying approaches. It is because they are solely responsible to decide the robustness of cryptosystem against linear and differential cryptanalyses. With an aim to fulfill the mentioned requirement of robustness, a novel group theoretic and graphical method is proposed to construct S-box with optimal features. Firstly, a strong S-box is generated with the help of orbits of coset graphs and the action of proposed powerful permutation of symmetric group S_{256}. In addition, a specific group is designed the action of whose pairs of permutations has the ability to generate as many as 462422016 strong S-boxes. Few of such proposed S-boxes are reported and assessed against standard performance parameters to validate the effectiveness of proposed findings. The features of proposed S-boxes are compared with most of the recent S-boxes to validate the superior performance. Moreover, they are also applied for image encryption to demonstrate their suitability for multimedia security applications.

INDEX TERMS Substitution-boxes, coset graphs, modular symmetric group, block ciphers.

I. INTRODUCTION

Recent developments in technology and their productive use in daily life have led to a significant increase in the amount of information being imparted. The security of information transmitted over the Internet is the main concern of the public. The sensitivity of the data requires the development of techniques and protective measures. Before transmitting, a user's data must be converted to a format that makes no sense to an unauthorized user [1]. Cryptography has been regarded as a developed scientific discipline over the past several decades. It is used to send data covertly at the recipient end while constructing reverse key or algorithm to retrieve the information at the transmitter end. Different mathematical and computational techniques are used to change important information into illegible and irrational forms.

In practice, cryptosystems are categorized into two main branches, symmetric and asymmetric cryptosystems. The symmetric cryptosystems are further partitioned into stream ciphers and block ciphers. In block encryption techniques, the plaintext data is scattered on blocks of the same size as the key and enciphering is performed over the entire block. Usually, a number of transformation operations on plaintext data bytes such as permutation, substitution, adding key and mixing are used in modern block ciphers [2]–[8]. Symmetric block ciphers are among the most broadly utilized systems because they are easy to implement and provide essential cryptographic strength [9], [10]. The block ciphers make

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

use of substitution and permutation operations. The input information (plaintext) is converted into an absurd output data (ciphertext) by utilizing a symmetric key and diverse number of rounds are applied for better encryption effects and quality. Where, each round performs substitution and permutation processes on the input block of binary data. A substitution process replaces an input block with another output block using substitution box (S-box) [11]. Advanced Encryption Standard (AES), as an example, is most commonly used symmetric block cipher. The S-boxes are the key components in block ciphers to create uncertainty and nonlinearity. Because of the efficient utilization of the 8×8 substitution box for the AES block cipher, development of robust and strong S-boxes, particularly of the size 8×8 attracted the attention of cryptographers worldwide. The improvement on information security standard is the primary objective of the cryptographers. The design of strong S-boxes has become a vital area of research for cryptographers.

In the recent past, various approaches and methods for the construction of S-boxes have been introduced. In [12], the authors introduced I-Ching operators and used them to construct an S-box. The designed S-Box was evaluated through various tests. The outcomes indicate that it has very good cryptographic properties. A technique to generate key dependent substitution box is presented in [13]. The authors claimed to expand the security level of the AES block encryption. In [14] a new S-box is designed with the help of quantum map. The suggested S-box is found to be strong enough to meet the requirements of secure encryption process. Zahid *et al.* [15] proposed an S-box formation method based on cubic fractional transformation. They used static values of transformation to generate the S-box. In [16], an efficient method for designing S-boxes is proposed by using Intertwining logistic map and bacterial foraging optimization. Zhu *et al.* proposed a novel chaotic system and constructed a secure double chaotic S-Box [17]. Further, they utilized newly generated S-box in image encryption applications. An efficient method for the generation of strong S-boxes with the help of innovative compound chaotic system is proposed in [18]. Lu *et al.* [19] utilized a newly generated strong chaotic S-Box to propose an efficient image encryption algorithm. Another recent secure S-box based on Cubic-Logistic function is generated in [20]. Lambić [21] constructed a novel discrete-space chaotic map by means of multiplication of integers and utilized it to generate an efficient S-box. In [22] an S-box with decent properties is proposed based on symmetric group and novel chaotic system. Yousaf *et al.* [23] used the action of finite Abelian group to construct an S-box with almost optimal features. An effective approach based on optimize linear fractional transformation is presented in [24]. Jamal *et al.* in [25] presented a novel technique based on the LFT and improved chaotic Tent-Sine system (TSS) to construct an S-box. Shuai *et al.* used cayley graph for the Symmetric group to generate a high quality S-box [26]. Machowski and Niemiec used key-dependent substitution boxes to design symmetric block cipher [27]. They also proposed a method to construct a large number of S-boxes with reasonable cryptographic features to counter various attacks. Iqtadar *et al.* claimed [28] that if we convert the entries of an S-box into 8 bits and interchange the position each bit by using a permutation from symmetric group S_8, the resulting new S-box has the same algebraic features. Since the order of S_8 is $8! = 40320$, so they were able to design 40320 S-boxes. The validity of the approach was analyzed by creating some copies of Liu J S-box.

The procedures and techniques of the S-boxes construction, presented in the literature are either feasible for the static S-boxes or complex and monotonous. Static S-boxes have their own deficiencies that can affect the safety of the cipher. The static S-boxes may help attacker in the cryptanalysis of the captured ciphertext. Also, the algorithms that form dynamic and key-dependent S-boxes are confusing and less productive. This requires a simple and effective methodology to develop dynamic and enormous collection of S-boxes. In this paper, we presented a novel method of strong S-boxes generation which has the following main highlights.

1. A novel graphical S-box construction procedure based on the orbits of coset graphs of symmetric group S_4 is proposed.
2. A powerful permutation of symmetric group S_{256} is suggested after rigorous experimental study which is incredibly productive to improve the features of obtained S-box.
3. We designed a specific group using three permutations of S_{16} which is credible enough to generate as many as 462422016 copies of S-boxes with great ease.
4. We reported few of such proposed S-boxes and compared their features with many recent and state of the art S-boxes.
5. All the proposed copies of S-boxes have strength and features quite similar to AES S-box.
6. We also applied the proposed S-boxes for image encryption to validate its suitability and usage for multimedia encryption.

The rest of article has the following structure. Some mathematical concepts of coset graphs and symmetric groups are described in section 2. The proposed method of S-boxes generation is explained and discussed in section 3. The performance assessment of proposed method and S-boxes is done section 4. We also presented the image encryption application of proposed S-boxes in section 5. At last, the contributions made in this paper are concluded in section 6.

II. MATHEMATICAL PRELIMINARIES

In this section, we briefly present some basic concepts of the coset graphs and symmetric groups to be used in the generation of the S-boxes.

A. COSET GRAPHS FOR MODULAR GROUP

The modular group $PSL(2, Z)$ is an infinite group generated by two mappings u and v such that $(x)u = \frac{-1}{x}$ and $(x)v = \frac{x-1}{x}$. The finite presentation of $PSL(2, Z)$ is $S_4 = \langle u, v : u^2 = v^3 = 1 \rangle$ [29]. It is the most significant infinite discrete group, through several associations with geometry,

topology and number theory. There is a rich history of studying the actions of $PSL(2, Z)$, especially on finite sets, that goes back to before the turn of the 20th century. In 1978, Graham Higman gave the concept of coset graphs for the modular group. Since, the generators u and v of $PSL(2, Z)$ have order 2 and 3, respectively. Therefore, these graphs consist of triangles and lines connecting the vertices of the triangles. The vertices of triangles are permuted anti-clockwise by v. If a triangle T has the vertices a, b, and c, it means that $(a)v = b$, $(b)v = c$, and $(c)v = a$. If the line representing u joins two vertices d and e (which may be of same triangle), then $(d)u = e$. The readers are referred to [30], [31] for more on coset graphs.

Consider a set $Z_n = \{0, 1, 2, \ldots, n-1\}$ under multiplication modulo n. It is a known fact that if n is a prime number p, then Z_n forms a field. The modular group acts on $Z_p \cup \{\infty\}$ and a finite coset graph emerges. Since $(0)u = \infty$, therefore, we adjoin $_\infty$ with Z_p to make the action possible. For instance, consider the action of the modular group on $Z_{17} \cup \{\infty\} = \{0, 1, 2, 3, \ldots, 16, \infty\}$.

The permutation representations of u and v, calculated by $(x)u = \frac{-1}{x}$ and $(x)v = \frac{x-1}{x}$., are given as:

u : $(0, \infty)(1, 16)(2, 8)(3, 11)(4)(5, 10)(6, 14)$
$(7, 12)(9, 15)(13)$

v : $(0, \infty, 1)(3, 12, 8)(2, 916)(15, 10, 6)(11, 4, 5)(13, 14, 7)$

The permutation of v contains six cycles, therefore, the coset graph of $Z_{17} \cup \{\infty\}$ consists of six triangles. The cycle $(0, \infty, 1)$ in the permutation of v represents a triangle of coset graph with vertices 0, ∞, and 1. In this way, 6 six triangles can be drawn. The permutations of u are utilized to join the vertices of this triangle. For example, by the cycle (2, 8) in u, we mean a line joining 2 and 8. In Figure 1, the coset graph evolves by using above permutation representations of v and u is shown.

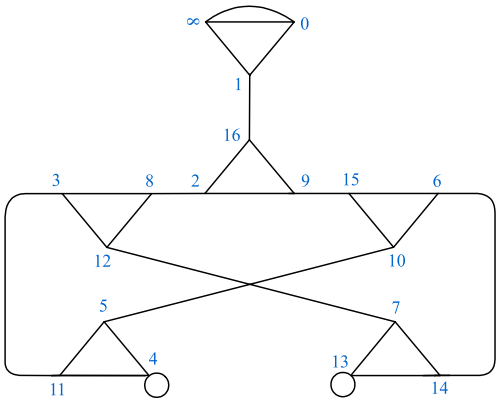


FIGURE 1. The coset graph for the action of modular group on $Z_{17} \cup \{\infty\}$.

The coset graph in Figure 1 arises from natural action $PSL(2,Z)$ on $Z_p \cup \{\infty\}$. These coset graphs always represent the group $\langle u, v : u^2 = v^3 = (uv)^p = 1\rangle$. It can be seen that each vertex of the graph in Figure 1 is fixed by $(vu)^{17}$. Therefore, it is the graphical representation of $\langle u, v : u^2 = v^3 = (uv)^{17} = 1\rangle$. In case of natural action, we obtain only one coset graph for each p. In [32], Mushtaq proved that a coset graphs for each element $\theta \in Z_p$ can be drawn. He gave the procedure of drawing coset graphs known as parametrization method. Thus, p number of coset graphs can be composed for each field Z_p. In the coset graphs, we can easily obtain the order of uv of own choice. Hence, we can make the coset graphs for different triangle groups. The Mushtaq's technique is briefed as follows (see [32] for complete proof and details). First, set $u = \frac{ax+kc}{cx-a}$ and $v = \frac{dx+kf}{fx-d-1}$. For each element $\theta \in Z_p$, the values of a, c, d, k and f can be computed by solving the following equations.

$$\theta = \frac{r^2}{\Delta} \tag{1}$$

$$r^2 + ks^2 = 3 \tag{2}$$

$$d^2 + f^2 + kd + 1 = 0 \tag{3}$$

$$r = a(2d + 1) + 2kcf \tag{4}$$

$$s = 2af - c(2d + 1) \tag{5}$$

The Table 1 provides the existing relation between the order of uv and the element $\theta \in Z_p$. The values of θ for higher order of uv can be obtained by using parametrization method [32].

TABLE 1. Relation between order of uv and values of θ.

Equation satisfied by θ	Order of uv
$\theta = 4$	1
$\theta = 0$	2
$\theta = 1$	3
$\theta = 2$	4
$\theta^2 - 3\theta + 1 = 0$	5
$\theta = 3$	6
$\theta^3 - 5\theta^2 + 6\theta - 1 = 0$	7
$\theta^2 - 4\theta + 2 = 0$	8
$\theta^3 - 6\theta^2 + 9\theta - 1 = 0$	9
$\theta^2 - 5\theta + 5 = 0$	10

B. SYMMETRIC GROUP AND ITS RELATION WITH S-BOX

A collection of all bijective maps from a set Ω, of k elements, to itself forms a group and is called symmetric group. It is denoted by S_k. The bijective maps in S_k are written in the form of cycles. For example, consider a bijective map from a set of 6 elements to itself such that 1, 2, 3, 4, 5 and 6 are mapped on 3, 4, 1, 6, 2 and 5 respectively. In cyclic form, it is written as (1, 3) (2, 4, 6, 5). An 8×8 substitution box has 256 unique elements arranged in a matrix of order 16.

By reshuffling the rows or columns in this matrix, a new S-box can be generated. Mathematically, this can be achieved using single permutation from S_{16}. Similarly, the positions of all 256 elements of 8×8 S-box can also be re-arranged through a certain permutation of S_{256}, so that a new S-box gets generated.

III. PROPOSED GENERATION OF STRONG S-BOXES

The proposed method of S-boxes generation explores the concepts of coset graphs, and symmetric groups. The procedure of their usage to achieve the task is described in this section.

A. COSET GRAPH BASED S-BOX FORMATION

The coset graph for the symmetric group $\langle u, v : u^2 = v^3 = (uv)^4 = 1\rangle$ emerges as a result of the action of $PSL(2, Z)$ on $Z_{257} \cup \{\infty\}$. An 8×8 substitution-box has 256 entries and 257 is the nearest prime number to 256, therefore, the field Z_{257} is opted. First, solve the equations (1) to (5) to find the values of a, c, d, k and f. Since in S_4 the order of uv is 4, therefore, we have $\theta = 2$ (see Table 1). Now we solve equations 1 to 5 to find the values of a, c, d, k and f. For equation (1), $\theta = \frac{r^2}{\Delta}$, assume $\Delta = 1$ to obtain $r = 60$. As $r^2 + ks^2 = 3$, and we take $k = 1$, then $s = 1$ is obtained. By putting $d = 0$ in equation (3), $f = 16$ is gotten. By substituting $r = 60, d = 0$, $k = 1$, $s = 1$ and $f = 16$ in equation (4) and (5), we find $a = 55$ and $c = 217$. Thus, we have $u(x) = \frac{55x+217}{217x-55}$ and $v(x) = \frac{16}{16x-1}$. Next, we apply these maps on each element of $Z_{257} \cup \{\infty\}$ to compute their permutation representations. Clearly, for any $x \in Z_{257}$, the values of $u(x)$ and $v(x)$ are in the form of fraction, since $257 \equiv 0$ in Z_{257}, so we keep adding 257 in numerator until the denominator completely divides it. Finally, we have integral values from Z_{257}. For instance

$$u(0) = \frac{55(0)+217}{217(0)-55} = \frac{257+217}{257-55} = \frac{237}{101} = \frac{237+257\times 164}{101} = 211$$

$$u(1) = \frac{55(1)+217}{217(1)-55} = \frac{272}{327} = \frac{136}{81} = \frac{136+257\times 25}{81} = 81$$

$$u(2) = \frac{55(2)+217}{217(2)-55} = \frac{379}{162} = \frac{35}{61} = \frac{35+257\times 2}{61} = 9$$

This way, the computations of $u(x)$ and $v(x)$ for all $x \in Z_{257}$ are performed and write them in the form of permutations as follows:

u : (211, 0)(81, 1)(9, 2)(3, 36)(4, 41)(5, 246)(6, 60)(7, 45)
(136, 8)(10, 13)(11, 165)(12, 203)(14, 120)(15, 40)
(16, 241)(17, 32)(18, 148)(19, 240)(122, 20)(105, 21)
(22, 253)(91, 23)(138, 24)(25, 179)(26, 102)(27, 121)
(37, 28)(29, 114)(30, 225)(31, 219)(33, 223)(34, 65)
(35, 193)(117, 38)(39, 200)(42, 172)(43, 129)(44, 44)
(215, 46)(47, 89)(48, 67)(234, 49)(140, 50)(252, 51)
(52, 166)(53, 235)(54, 182)(55, 242)(56, 226)(57, 128)
(58, 115)(87, 59)(61, 147)(62, 133)(63, 86)(64, 94)
(218, 66)(68, 170)(69, 163)(70, 176)(71, 83)(116, 72)
(73, 152)(118, 74)(132, 75)(76, 161)(77, 79)(78, 199)
(80, 230)(82, 231)(84, 209)(85, 169)(88, 164)(243, 90)
(92, 256)(93, 208)(95, ∞)(96, 126)(239, 97)(98, 191)
(99, 167)(100, 204)(143, 101)(103, 131)(104, 127)
(106, 238)(107, 119)(108, 216)(109, 189)(110, 217)
(113, 111)(112, 248)(123, 142)(124, 229)(125, 156)
(130, 184)(134, 221)(135, 205)(137, 212)(139, 195)
(141, 213)(144, 232)(145, 183)(146, 146)(186, 149)
(175, 150)(151, 247)(153, 162)(154, 187)(155, 254)
(157, 224)(158, 173)(159, 228)(160, 222)(168, 194)
(171, 207)(174, 206)(177, 180)(178, 244)(181, 188)
(185, 201)(190, 236)(192, 196)(197, 249)(198, 250)
(202, 237)(210, 245)(214, 227)(220, 233)(251, 255).

v :: (0, 241, ∞)(121, 242, 1)(256, 120, 240)(113, 2, 100)
(239, 128, 141)(230, 70, 3)(171, 11, 238)(4, 90, 177)
(151, 237, 64)(87, 5, 49)(236, 154, 192)(222, 27, 6)
(214, 19, 235)(190, 131, 7)(110, 51, 234)(8, 75, 209)
(166, 233, 32)(9, 72, 184)(169, 232, 57)(10, 89, 164)
(152, 231, 77)(134, 12, 101)(229, 107, 140)(195,162,13)
(79, 46, 228)(14, 60, 186)(181, 227, 55)(199, 104, 15)
(137, 42, 226)(225, 16, 249)(148, 105, 17)(136, 93, 224)
(189, 84, 18)(157, 52, 223)(74, 20, 50)(221, 167, 191)
(132, 33, 21)(208, 109, 220)(22, 115, 206)(126, 219, 35)
(145, 174, 23)(67, 96, 218)(59, 24, 45)(217, 182, 196)
(163, 56, 25)(185, 78, 216)(153, 73, 26)(168, 88, 215)
(111, 85, 28)(156, 130, 213)(179, 29, 40)(212, 62, 201)
(95, 44, 30)(197, 146, 211)(175, 183, 31)(58, 66, 210)
(173, 34, 36)(207, 68, 205)(116, 37, 97)(204, 125, 144)
(119, 99, 38)(142, 122, 203)(129, 39,243)(202,112,255)
(147, 41, 248)(200, 94, 250)(43, 61, 247)(180, 198,251)
(47, 102, 159)(139, 194, 82)(150, 48, 253)(193, 91, 245)
(149, 81, 53)(160, 92, 188)(103, 54, 246)(187, 138, 252)
(86, 63, 244)(178, 155, 254)(165, 71, 65)(170, 76, 176)
(127, 133, 69)(108, 114, 172)(135,80,83)(161,106,158)
(124, 123, 98)(118, 117, 143).

Since each vertex of the coset graph evolved from above permutation representation is fixed by u^2, v^3 and $(uv)^4$. Therefore, it is the graphical representation of the symmetric group $S_4 = \langle u, v : u^2 = v^3 = (uv)^4 = 1\rangle$. It has 12 orbits (fragments) comprising 10 copies of γ_j (each is having the same structure as shown in Figure 2), one copy of λ (Figure 3) and δ (Figure 4) each.

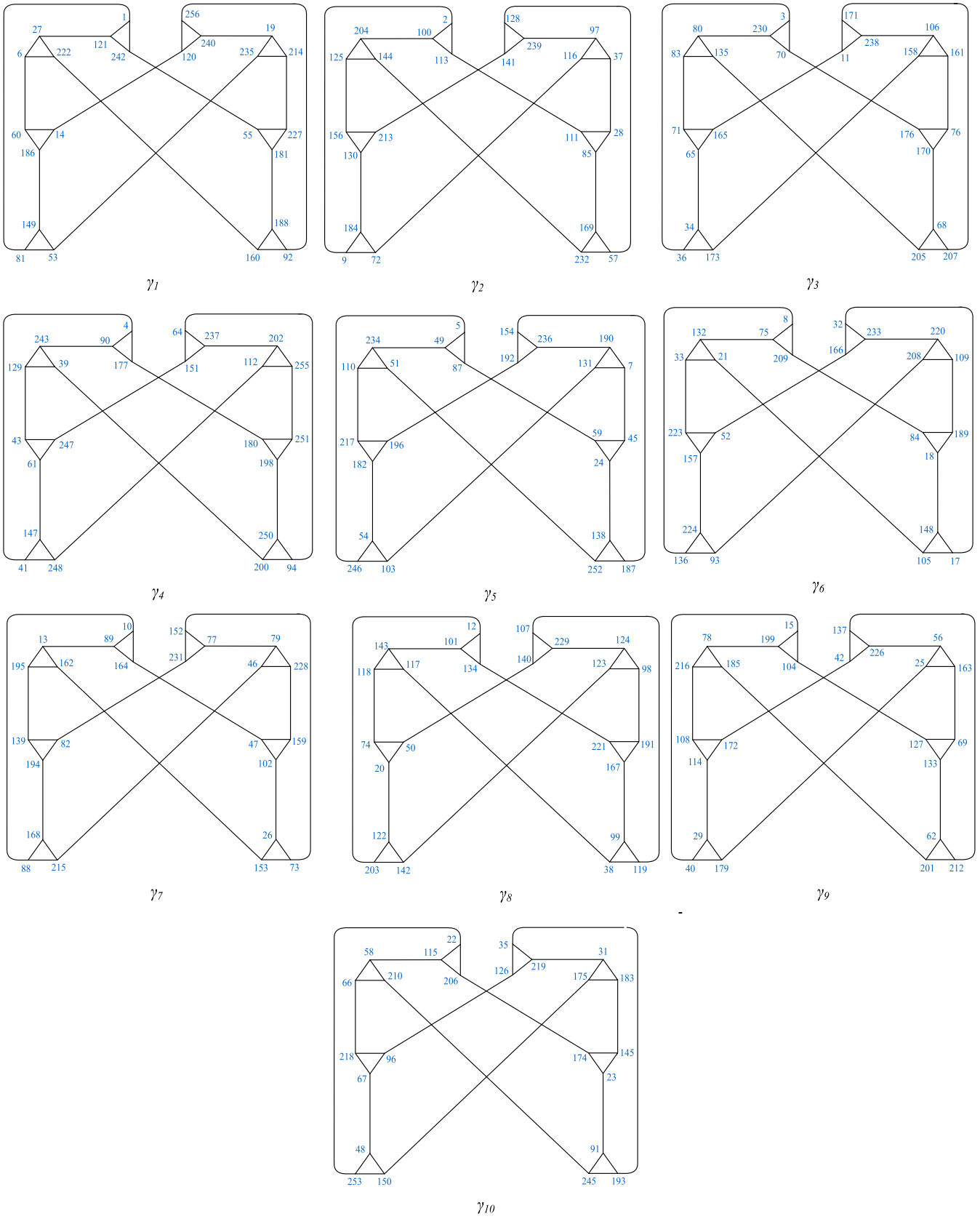


FIGURE 2. Ten orbits γ_i ($i = 1, 2, \ldots, 10$) of the coset graph for symmetric group S_4.

TABLE 2. Square matrix of order 16 obtained after step A.

00	197	225	95	16	44	30	146	211	241	249	01	53	214	55	06
186	81	121	14	240	235	149	19	188	227	27	242	181	160	60	222
92	120	02	72	37	111	09	100	125	130	28	97	128	169	57	141
156	144	85	232	204	113	116	184	213	239	03	173	161	176	11	71
135	207	34	165	238	158	36	230	83	65	68	76	106	171	70	170
205	80	04	248	255	180	39	94	151	43	41	90	129	61	64	250
251	202	112	147	247	237	177	198	200	243	05	103	07	59	24	252
234	87	45	190	154	138	49	110	182	246	51	187	192	217	54	196
236	131	08	93	109	84	17	166	223	21	18	105	132	209	32	148
189	220	33	157	136	75	52	233	208	224	10	195	194	88	13	89
102	153	26	159	79	152	46	168	82	77	47	164	215	228	73	231
139	162	12	142	98	221	20	203	101	118	38	143	134	167	50	229
123	122	74	117	119	140	99	191	124	107	15	179	163	127	25	29
172	226	40	199	216	114	42	108	185	212	56	137	62	69	78	104
133	201	22	150	183	174	23	245	58	206	31	35	91	145	48	96
219	175	66	67	253	115	126	218	210	193	63	86	244	155	178	254

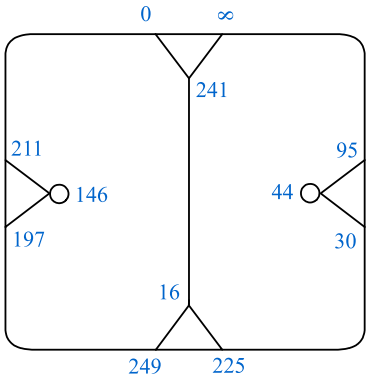


FIGURE 3. The orbit λ of the coset graph for symmetric group S_4.

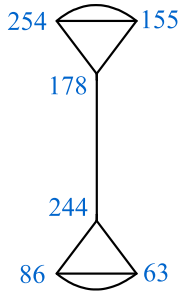


FIGURE 4. The orbit δ of the coset graph for symmetric group S_4.

B. PROPOSED S-BOX METHOD

The trivial sequence of 0, 1, 2,…, 255 is destroyed by using the vertices of the coset graphs for S_4. Therefore, our first objective is to present the vertices of coset graph in a 16×16 matrix. The vertices 256 and ∞ are ignored as they only utilized to make the action of $PSL(2, Z)$ possible. The proposed method of generation of 462422016 strong 8×8 S-boxes contains three major steps.

Step A.

The coset graph of S_4 has 12 orbits as shown in Figure 2, 3, and 4.

1. Locate the orbit γ_1 containing the least element 0 of $Z_{257} - \{256\}$.

a. Apply $(uv)^4$ on 0 so that we travel through a closed path

$$0 \dashrightarrow^{uv} 197 \dashrightarrow^{uv} 225 \dashrightarrow^{uv} 95 \dashrightarrow^{uv} 0.$$

Now, choose the vertices 0, 197, 225, and 95, which are at a distance of uv from each other, and declare them as 1st four elements of the 1st row of 16×16 matrix.

b. From the remaining vertices of γ_1, find the least element (vertex) and repeat step **1(a)**. This process

TABLE 3. The permutation $\sigma \in S_{256}$.

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

continues until all the vertices of the selected orbit are exhausted.

2. Now, pick the next orbit that has the smallest element of $Z_{257} - \{256\} - \gamma_1$ and repeat step **1**. Step **1** is considered completed once all the vertices of coset graph are terminated.

After step **2**, we are able to form a 16×16 matrix having unique entries from $\{0, 1, 2, \ldots, 255\}$. This matrix is considered as the initial 8×8 S-box (shown in Table 2) and it is found to have sufficient cryptographic performance. It has an average nonlinearity of 100.5. The next procedural step **B** is framed to improvise on the cryptographic strength of obtained S-box by using the action of symmetric group S_{256}.

Step B.

After exhaustive research and analysis, we came through to find that a certain permutations of S_{256} are incredibly productive to improve the quality of an 8×8 S-box. Theoretically, there are having 256! distinct permutations in S_{256}. In this step, we applied around 10 million random permutations of the symmetric group S_{256} on 16×16 S-box matrix obtained after step **A** (Table 2) and found a permutation σ (shown in Table 3) the most powerful to enhance the performance of the S-box. The permutation σ reshuffles all 256 elements of Table 2 and yields a strong S-box (shown in Table 4) as consequence of the action.

Step C.

In this step, we construct a large number of S-boxes having the same algebraic properties as that of the S-box from step **B**. Proceed as follows to operate this step **C**. Consider the following three permutations of S_{16}.

$$a = (1, 7, 14, 4, 2, 8, 13, 3)(5, 12, 9, 16, 6, 11, 10, 15)$$
$$b = (1, 3, 5, 7)(2, 4, 6, 8)(9, 11, 13, 15)(10, 12, 14, 16)$$
$$c = (1, 5, 11)(2, 6, 12,)(7, 13, 9)(8, 14, 10)$$

It is verified that if we reshuffle the rows or columns of the generated S-box (Table 4) by using these three permutations, then resulting new S-boxes found to have the same properties. Let us denote the group generated by a, b, and c as G. Then each element of the group G is a product a, b, and c. Through GAP (*Groups, Algorithms, Programming - a System for Computational Discrete Algebra*, see https://www.gap-system.org/index.html), it is found that there are 21504 distinct possible products of a, b, and c, which indicates that the order of proposed group G is 21504. Now, the finite presentation of this particular proposed group G is as follows:

$$\begin{aligned} a, b, c : a^8 &= b^4 = c^3 = (bc^{-1})^2 = (a^2b^2)^2 \\ &= a^2(ca^{-1})^2ca = (a^{-1}b^{-1})^4 \\ &= (ab^{-1}a^{-1}b^{-1})^2 = (aba^{-1}b^{-1})^2 \end{aligned}$$

TABLE 4. Proposed generated S-box I.

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

$$\begin{aligned} &= (acab^{-1})^2 = acab(c^{-1}a^{-1})^2c^{-1}b \\ &= a^2b^{-1}a^{-1}c^{-1}a^{-1}b^{-1}a^{-1}c^{-1}a \\ &= a^6c^{-1}ba^{-1}baca^2b^{-1}c = 1 \end{aligned} \tag{6}$$

A GAP structural description of the formulated G is shown in Figure 5. For instance, if we reshuffle the rows of an S-box S_1 by using the generators of G (say using a) so that a new S-box S_2 emerges. Then S_1 and S_2 are found to have the same algebraic and cryptographic strength. We can also construct another S-box S_3 by the action of another generator b on rows of S_2. Note that, element of G which generates S_3 is ab Hence, proceeding this way, 21504 distinct different S-boxes of the same properties can be created by applying all permutations of G on rows of the S-box S_1. Next, corresponding to each S-box S_i (where $i = 1, 2, 3, \ldots, 21504$) obtained by reshuffling the rows of S_1, we can further create 21504 more S-boxes by reshuffling the columns of each S_i using permutations from the proposed group G. Ultimately, we can generate a total of $21504^2 = 462422016$ strong 8×8 S-boxes of the same algebraic and cryptographic strength using group G in this step $\boldsymbol{C}$.

In this paper, we present four such S-boxes through the action of a specified pair of permutations of proposed group G to reshuffle the rows and columns of S-box in Table 4 which in turn generates three more S-boxes shown in Table 5 to 7.

Consider the following pairs of permutations of formulated G to generate three more S-boxes.

$$\begin{aligned} \varpi_1 &= bc \\ &= (1, 3, 11, 9)(2, 4, 12, 10)(5, 13, 15, 7)(6, 14, 16, 8) \\ \varpi_2 &= ac^2b^3 \\ &= (1, 15, 7, 6, 3, 9, 14, 2, 16, 8, 5, 4, 10, 13)(11, 12) \end{aligned}$$

The rows and columns of the proposed generated S-box I are reshuffled using the permutations ϖ_1 and ϖ_2, respectively to get the proposed S-box II (shown in Table 5). Next, we use following permutations ϖ_3 and ϖ_4 on the same S-box I to evolve proposed S-box III (see Table 6).

$$\begin{aligned} \varpi_3 &= cab^2 = (1, 16, 2, 15)(3, 5, 14, 11)(4, 6, 13, 12) \\ \varpi_4 &= ac = (1, 13, 3, 5, 2, 14, 4)(7, 10, 15, 11, 8, 9, 16, 12) \end{aligned}$$

We have generated the proposed S-box IV (shown in Table 7) by applying the following pair (ϖ_5 and ϖ_6) of permutations of G on rows and columns of S-box I, respectively.

$$\begin{aligned} \varpi_5 &= ab = (5, 14, 6, 13)(7, 16, 8, 15)(9, 10)(11, 12) \\ \varpi_6 &= ab^2 \\ &= (1, 3, 5, 16, 2, 4, 6, 15)(7, 10, 11, 14, 8, 9, 12, 13) \end{aligned}$$

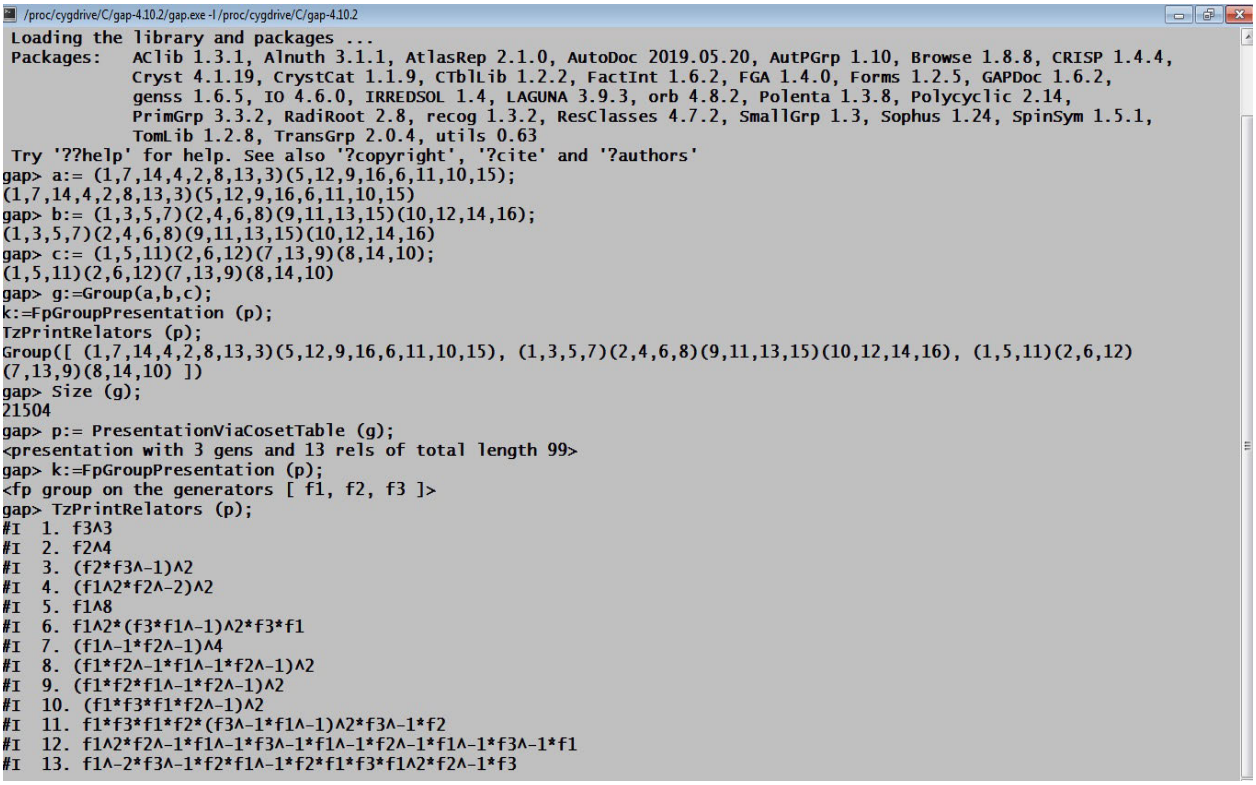


FIGURE 5. A screenshot of GAP system for the structural description of proposed group *G* and its order.

IV. PERFORMANCE ANALYSIS AND COMPARISON

In this section, we analyze the performance of our proposed algebraic method for the generation of a large number of strong 8 × 8 S-boxes. All the generated S-boxes are bijective. The conducts of S-boxes are assessed against the well-established set of test criterions such as nonlinearity, strict avalanche criterion, output bits independence criterion, differential uniformity, linear approximation probability, and auto-correlation function for absolute indicator. The encryption process involves substitution by suggested S-boxes in two rounds. In the first round, the substitution is carried out in forward direction (from first to the last pixel) followed by substitution in backward direction (from last to the first pixel). We have used our S-boxes to encrypt plain images. Two standard gray images of *Pepper* and Baboon both having size 256 × 256 are used to perform MLC test. We have used MATLAB tool to execute all the computational experiments. A high satisfaction of any S-box for the mentioned test criterions entails its high credibility to mitigate the linear, differential and other types of attacks. The results obtained from various tests show the incredibly high cryptographic strength and capability of proposed generated S-boxes to resist different algebraic attacks is similar to that of AES S-box.

A. NONLINEARITY

Nonlinearity test, introduced by Pieprzyk and Finkelstein in 1988 [33], is the most important parameter to determine the efficiency of substitution boxes. An S-box is considered weak, if the mapping between the plaintext and the ciphertext is linear. In such scenarios, it is easier for the attacker to initiate a linear attack on the ciphertext to obtain the plaintext. This linear attack can be neutralized by designing an S-box with extremely nonlinear mapping between the plaintext and the ciphertext. The Mathematical formula to compute the nonlinearity of an n-bit Boolean function B is

$$nl(B) = \frac{2^n - max\,|WS_B(u)|}{2}$$
$$WS_B = \sum (-1)^{B(v)\oplus u.v} \tag{7}$$

where, WS_B is Walsh spectrum of function B and u, v belongs to $\{0, 1\}^n$. The optimal value of nonlinearity for an n-variable Boolean function is $2^{n-1} - 2^{\frac{n}{2}-1}$. But, such functions are bent functions and not balanced. The optimal score of nonlinearity exhibit by AES S-box (112) is still considered as the best value for the case of 8×8 S-boxes. The reason being, so far no 8 × 8 S-box has been reported which has more nonlinearity than AES S-box. The nonlinearity scores of eight balanced component Boolean functions for each proposed S-boxes are listed in Table 8. Whereas, the nonlinearities of initial S-box matrix (in Table 2) are 104, 100, 102, 106, 100, 102, 102, 88, which gives an average of 100.5.

B. STRICT AVALANCHE CRITERION

In [34] Webster and Tavares introduced this criterion. The SAC is said to be satisfied, if all output bits of a function change with a 0.5 probability by complementing a single

TABLE 5. Proposed generated S-box II.

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

input bit. Generally, the value of SAC of an S-box is calculated by using dependence matrix. The S-box is considered to meet this criterion, if the average value of the matrix is near to the optimal value of $1/2$. In [34] the process of calculating the average value of dependence matrix is given. The SAC values for our four proposed S-boxes are 0.5017, 0.4995, 0.5019, and 0.4973, respectively. A comparison of the SAC values between generated S-boxes and different recently developed S-boxes is given in Table 9.

C. BITS INDEPENDENT CRITERION

Suppose h_i denote a Boolean mapping and h_j is a two bits output of a substitution box. If $h_i \oplus h_j$ fulfills the requirements of SAC and has high value of nonlinearity, then by inverting a single input the value of correlation coefficient of each output bit pair is near to zero. In this way the BIC reading of an S-box can be calculated by verifying whether $h_i \oplus h_j$ $(i \neq j)$ of any two output bits of the S-box satisfies the nonlinearity and SAC. This analysis is very important to know the confusion strength of any nonlinear algorithm. The requirement of this analysis is that all values should be approximately equal to 0.5 which has been experimentally verified for our S-boxes. The BIC for nonlinearity are found to have all 112 values for all four proposed S-boxes showing the same BIC strength as that of AES S-box.

D. DIFFERENTIAL UNIFORMITY

Differential uniformity is computed by examining the function from the input bits to the output bits. The insurance of differential uniformity is the main focus of this test. The input differential $\Delta\varphi$ must be related with an output differential $\Delta\psi$ in a unique way. The formula to calculate differential uniformity is given as

$$DU = \max_{\Delta\varphi \neq, \Delta\psi} \left[\#\{\varphi \in I | S(\varphi) \oplus S(\varphi + \Delta\varphi) = \Delta\psi\}\right] \tag{8}$$

The differential uniformity of all four proposed generated S-boxes (in Table 4 to 7) is same and it is just 4 with a differential approximation probability of 0. 015625 only, which verify its high resistance capability to mitigate the differential cryptanalysis like the AES.

E. LINEAR APPROXIMATION PROBABILITY

Like differential probability, the linear approximation probability (denoted by *LAP*) is also concerned with the highest value of the respective LAT Table. In this test, an imbalance of an event is examined, and its highest value is noted. The parity of the input bits selected by the mask χ_x is exactly the same as the parity of the output bits selected by the mask χ_y. This analysis was introduced by Matsui [35]. The mathematical formula to calculate linear approximation probability of a

TABLE 6. Proposed generated S-box III.

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

given S-box is given below.

$$LAP = \max_{\chi_x, \chi_y \neq 0} \left| \frac{\#\{d/d \cdot \chi_x = S(d) \cdot \chi_y\}}{2^n} - \frac{1}{2} \right| \tag{9}$$

where, d represents the collection of all possible inputs and 2^n is the total number of elements. The LAP readings of our proposed S-boxes are 0.0625 and this is again the equal to AES S-box value.

F. AUTO-CORRELATION FUNCTION

This test was introduced by L. D. Burnett in [36]. The auto-correlation function of a Boolean function f is computed as:

$$r_f(d) = \sum\nolimits_{\forall x, d \in [0,1]^n} (-1)^{f(x)} (-1)^{f(x \oplus d)} \tag{10}$$

where for all Boolean functions $r(0) = 2^n$ and for all other possible inputs $2^{-n} \leq r(d) \leq 2^n$. The highest value of ACF, known as absolute indicator of Boolean function f, is used to determine the cryptographic quality to achieve good diffusion characteristics [37]. It is denoted as:

$$\left|ACF_f\right| = max\left(\left|r_f(d)\right|\right) \quad for\ d \neq 0 \tag{11}$$

We can extend this cryptographic metric ACF of Boolean function to S-boxes Ψ: $\{0, 1\}^n \rightarrow \{0, 1\}^n$ by considering all 2^n -1 non-zero linear combinations F of its n component functions. This can be achieved by using the following equation [38].

$$|ACF_\Psi| = max\left(\left|r_{F_i}(w)\right|\right), \quad where\ w, i = 1, 2, \cdots, 2^n - 1$$

The ACF of S-box should be as small as possible for cryptographic strength. The maximum ACF for both the AES S-box and generated S-boxes is 32 only. The score is confirming the great cryptographic quality and strength of the proposed S-boxes and the anticipated method.

The quantified performance values of all four S-boxes from proposed method of generation are compared with some selectively picked most recent state-of-the-art S-boxes. Wherein, the concepts such as chaos, meta-heuristics, optimizations, algebraic techniques, etc., are applied to achieve best possible generated S-boxes. We maintained the Table 9 which compares the cryptographic features of these S-boxes. Firstly, the comparative study show that all proposed S-boxes have performance strength same as that of the famous AES S-box over all quality metrics and parameters. Secondly, the proposed S-boxes have optimal performance values for nonlinearities, strict avalanche criterion, bits independence criterion, differential uniformities, linear approximation probabilities, and auto-correlation functions to validate the effectiveness and credibility of not only the proposed S-boxes but also the proposed method of generation.

TABLE 7. Proposed generated S-box IV.

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

TABLE 8. Nonlinearity scores of all four proposed generated 8 × 8 S-boxes.

Proposed S-box	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
S-box I	112	112	112	112	112	112	112	112
S-box II	112	112	112	112	112	112	112	112
S-box III	112	112	112	112	112	112	112	112
S-box IV	112	112	112	112	112	112	112	112

Thirdly, the proposed S-boxes have better parameter values compared to almost all available 8 × 8 S-boxes and they are more capable to offer resistance to differential and linear cryptanalyses. The comparative analysis unarguably portrays the reasonably good security performance of our all four S-boxes and proposed method.

V. APPLICATION IN DIGITAL IMAGE SECURITY

The encryption process distorts the image; these types of alterations determine the reliability of the scheme. So it is important to examine the statistical features through majority logic criterion (MLC). The MLC is a comprehensive exploration set of metrics which includes the entropy, contrast, correlation, energy, and homogeneity tests, as suggested in [60]. The statistical stability of the generated S-boxes is examined by this set of analyses.

A. ENTROPY

The value of randomness of encrypted image is measured by entropy analysis. The entropy is mathematically formulated as.

$$Entropy = -\sum p(x_i) log_2 p(x_i) \tag{12}$$

where, $p(x)$ is the probability of symbol x. A greater value of entropy shows that the distribution of pixels gray values is more uniform. There would be a chance of predictability if the entropy of encrypted image is significantly less than 8, and it may threaten security of image.

B. CONTRAST

The difference in the brightness of an object relates to contrast. Contrast analysis enables the user to visualize objects to identify the underlying information. Therefore, the contrast and brightness of the images are properly adjusted during image processing for better visual effects and viewing. In encryption process, due to the nonlinear mapping of the S-box the contrast is directly proportional to the randomness

TABLE 9. Performance comparison of different 8 × 8 S-boxes.

S-box	Nonlinearity			SAC	BIC-NL	BIC-SAC	DU	LAP	ACF
	min	max	mean						
Proposed S-box I	112	112	112	0.5017	112	0.5030	4	0.0625	32
Proposed S-box II	112	112	112	0.4995	112	0.5020	4	0.0625	32
Proposed S-box III	112	112	112	0.5019	112	0.5013	4	0.0625	32
Proposed S-box IV	112	112	112	0.4973	112	0.5012	4	0.0625	32
Ref. [19]	104	110	106.25	0.503	100	0.507	10	0.133	96
Ref. [25]	112	112	112	0.504	112	0.504	4	0.0625	32
AES [39]	112	112	112	0.5058	112	0.5046	4	0.0625	32
Ref. [3]	106	110	108.5	05017	100	0.5026	10	0.1328	96
Ref. [12]	108	110	108.75	0.4946	94	0.5054	10	0.1328	104
Ref. [40]	110	112	110.25	0.50	104	0.5052	10	0.125	96
Ref. [41]	84	106	100	0.4812	96	0.4967	16	0.1796	104
Ref. [42]	108	110	109	0.5026	102	0.5026	10	0.1406	104
Ref. [43]	106	110	107.5	0.4971	196	0.5034	10	0.125	96
Ref. [44]	106	110	107	0.5015	98	0.5016	10	0.1484	96
Ref. [45]	106	110	108	0.5073	100	0.5020	10	0.1523	96
Ref. [46]	106	110	107.5	0.5036	90	0.5040	10	0.1484	104
Ref. [47]	104	110	106.5	0.4995	98	0.4983	10	0.1172	96
Ref. [48]	106	108	107.5	0.4943	98	0.4982	10	0.125	96
Ref. [49]	100	106	105.5	0.4946	96	0.4988	10	0.1328	96
Ref. [50]	108	112	109.25	0.5012	104	0.5056	8	0.0937	72
Ref. [51]	106	108	106.75	0.5034	100	0.4951	10	0,1328	104
Ref. [52]	106	108	106.75	0.4939	102	0.5040	16	0.125	168
Ref. [53]	106	108	107.25	0.5034	98	0.4980	12	0.1328	104
Ref. [54]	106	108	106.75	0.4941	98	0.4957	10	0.125	96
Ref. [55]	104	108	106.75	0.4076	98	0.5022	10	0.1328	96
Ref. [56]	102	108	106	0.5066	96	0.5065	12	0.1445	96
Ref. [57]	106	110	107.75	0.4976	100	0.5023	10	0.125	96
Ref. [58]	108	110	109.5	0.4985	98	0.5052	10	0.1328	96
Ref. [59]	112	112	112	0.5009	112	0.5015	4	0.0625	32

TABLE 10. Comparison of encryption MLC results for different S-boxes.

S-boxes	Entropy	Contrast	Correlation	Energy	Homogeneity
Pepper Image					
Plain-image	7.5909	0.3131	0.9441	0.1161	0.8982
S-box I	7.9545	10.5377	-0.0061	0.0157	0.3894
S-box II	7.9529	10.3818	-0.0049	0.0158	0.3913
S-box III	7.9545	10.2847	0.0026	0.0157	0.3927
S-box IV	7.9568	10.5365	-0.0004	0.0157	0.3900
Prime [61]	7.7059	8.1003	0.0090	0.0158	0.4960
Xyi [62]	7.7619	8.1945	0.0517	0.0158	0.4940
Skipjack [63]	7.7561	7.7058	0.1205	0.0239	0.4708
Belazi [64]	7.9233	8.1423	−0.0112	0.0286	0.4648
AES [39]	7.9211	7.5509	0.0554	0.0202	0.4662
Baboon Image					
Plain-image	7.1278	0.8566	0.6849	0.0895	0.7488
S-box I	7.9817	10.4391	-0.0128	0.0157	0.3889
S-box II	7.9551	10.4279	0.0015	0.0157	0.3896
S-box III	7.9540	10.3797	-0.0046	0.0157	0.3902
S-box IV	7.9567	10.4983	-0.0008	0.0157	0.3893
Prime [60]	6.9311	7.6236	0.0855	0.0202	0.4640
Xyi [61]	7.2531	8.3108	0.0417	0.0196	0.4533
Skipjack [62]	7.2531	7.7058	0.1025	0.0193	0.4689
Belazi [63]	7.9252	8.0391	0.0119 0	.02219	0.4428
AES [39]	7.9325	7.2240	0.0815	0.0211	0.4701

of image [47]. Mathematically, it is computed as:

$$Contrast = \sum |i-j|^2 p(i,j) \tag{13}$$

where, $p(i, j)$ represents the position of pixels in gray level co-occurrence matrix (GLCM).

C. CORRELATION

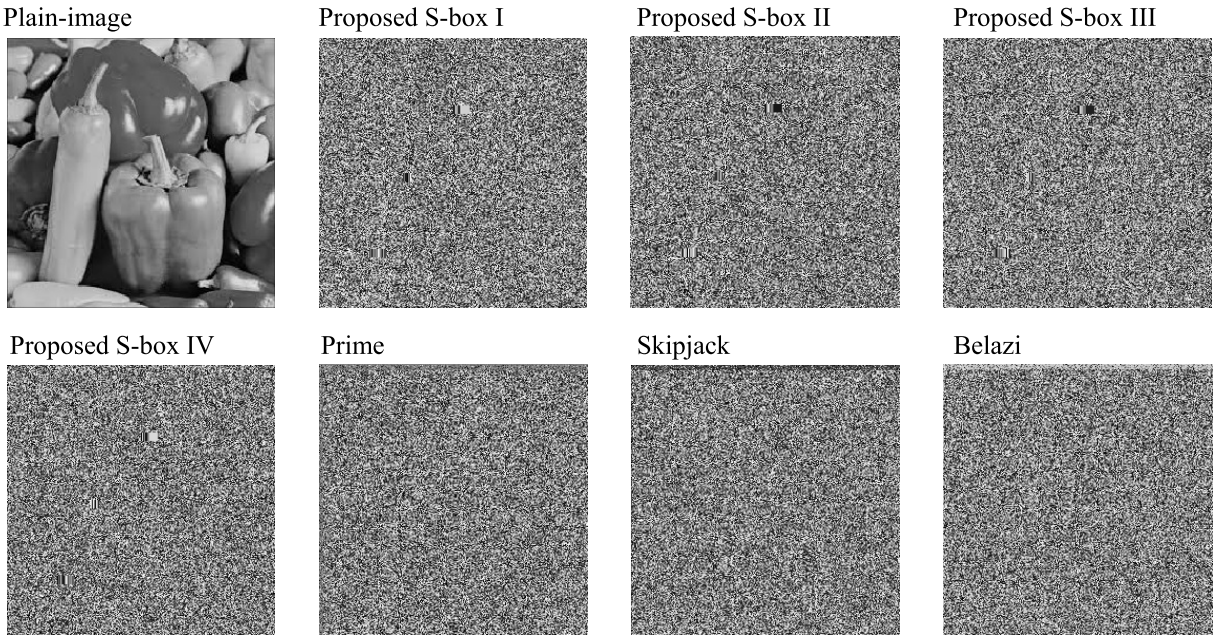
Resemblance of pixels to their neighbors is measured through correlation. In the plain-images, there exists a strong correlation among neighboring pixels. The correlation between pixel values can be soften by encryption schemes. Therefore, in insecure channel the encrypted image with negligible correlated values is considered more robust. Correlation has following formulation:

$$Correlation = \sum \frac{(i-\mu i)\,(j-\mu j)}{\sigma_i \sigma_j} \tag{14}$$

where, $p(i, j)$ indicates the pixel value and i represent the position of row and j indicates its column value of digital images. The parameters μ *and* σ are the variance and standard deviation, respectively.

D. ENERGY

The sum of squared members of gray level co-occurrence is calculated in energy analysis. In gray level co-occurrence matrix, high valued pixels are found in some places of plain-images; therefore, the energy value is high. Whereas,



(2) *BABOON*

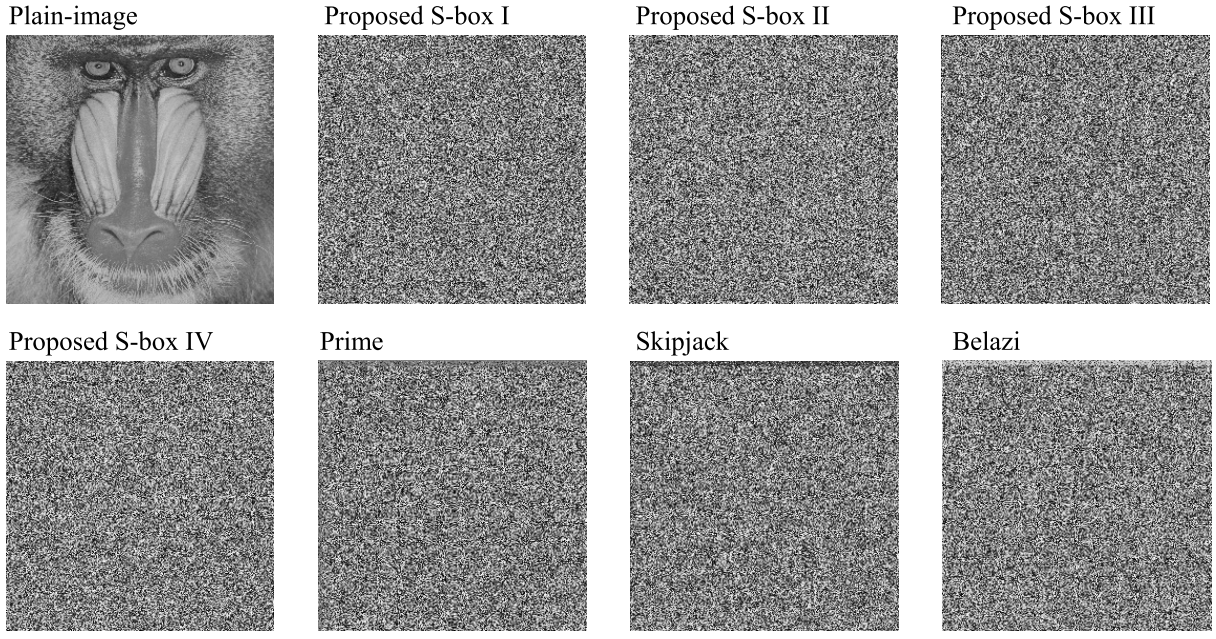


FIGURE 6. Plain-images and the encrypted images with two rounds of encryption using different S-boxes for (a) *Pepper* and (b) *Baboon*.

compared to the plain-image energy, the energy of encrypted image is smaller because in encrypted image the values are distributed. Energy analysis involves the computation of its associated value which is defined as follows:

$$Energy = \sum p(i,j)^2 \tag{15}$$

where, $p(i, j)$ is the number of GLCM matrices.

E. HOMOGENEITY

Homogeneity deals with the intimacy of distribution of elements in gray level co-occurrence matrix (GLCM) to its diagonal. Mainly, its value is dependent on the components presents on the diagonal of the gray level co-occurrence matrix. The small value of homogeneity in encryption reveals the strength of the encryption algorithm. Homogeneity is calculated as:

$$Homogeneity = \sum \frac{p(i,j)}{1+|i-j|} \tag{16}$$

To demonstrate that the proposed S-boxes can be used for encryption and multimedia security, we have used two standards plain-images *Pepper* and *Baboon* for MLC encryption performance analysis. The results of these analyses in

comparison with the other well-known S-boxes are depicted in Table 10. Figure 6 shows the result of image encryption with proposed S-boxes and few others also. Majority logic criterion analysis results indicate that the proposed S-boxes are suitable for encryption applications and is adequate enough to a become part of algorithms meant for multimedia based safe communication between two legitimate parties.

VI. CONCLUSION

Generation of cryptographically robust and algebraically strong S-box is promising area of research these days. The available proposals either deals with construction of single S-box, which may or may not have the optimal features compared to AES S-box or deals construction of a small set of S-boxes with sufficient computation overheads. But, these two issues have been tackled in this paper quite comfortably. The proposed method explored the orbits of coset graphs to obtain the initial S-box matrix quite innovatively. The quality of the S-box is augmented up to the optimum level by the action of a powerful permutation of S_{256}. We presented a novel method which is not only able to yield an S-box with features quite close to AES S-box but also provide a simple and powerful procedure of generating as much as 462422016 strong S-boxes. The features of proposed S-boxes are compared against a number of existing recent S-boxes. It is found that our S-boxes have excellent performance strength compared to almost all over all parameters. The proposed S-boxes are also used to encrypt some standard plain-images to evaluate their encryption performance; the results show that they are sufficiently suitable for use in secure multimedia applications.

REFERENCES

[1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, Jun. 1998.
[2] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 12, pp. 1498–1509, Dec. 2001.
[3] 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, 2018.
[4] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 2, pp. 163–169, 2001.
[5] 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.
[6] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, Mar. 2001.
[7] X. Li, L. Wang, Y. Yan, and P. Liu, "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems," *Optik*, vol. 127, no. 5, pp. 2558–2565, Mar. 2016.
[8] M. Ahmad and T. Ahmad, "Securing multimedia colour imagery using multiple high dimensional chaos-based hybrid keys," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 12, no. 1, p. 113, 2014.
[9] C. Paar, J. Pelzl, and B. Preneel, *Understanding Cryptography*, 1st ed. Berlin, Germany: Springer, 2010.
[10] A. Shamir, "Stream ciphers: Dead or alive?" in *Proc. 10th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Jeju Island, South Korea, Dec. 2004, p. 78.
[11] K. M. Ali and M. Khan, "Application based construction and optimization of substitution boxes over 2D mixed chaotic maps," *Int. J. Theor. Phys.*, vol. 58, no. 9, pp. 3091–3117, Sep. 2019.
[12] 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.
[13] K. Kazlauskas and J. Kazlauskas, "Key-dependent S-box generation in AES block cipher system," *Informatica*, vol. 20, no. 1, pp. 23–34, 2009.
[14] F. Firdousi, S. I. Batool, and M. Amin, "A novel construction scheme for nonlinear component based on quantum map," *Int. J. Theor. Phys.*, vol. 58, no. 11, pp. 3871–3898, Nov. 2019.
[15] 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, May 2019.
[16] Y. Tian and Z. Lu, "Chaotic S-box: Intertwining logistic map and bacterial foraging optimization," *Math. Problems Eng.*, vol. 2017, pp. 1–11, 2017.
[17] S. Zhu, Z. Wang, and C. Zhu, "A secure and fast image encryption scheme based on double chaotic S-boxes," *Entropy*, vol. 21, no. 8, p. 790, 2019.
[18] Lu, Zhu, and Wang, "A novel S-box design algorithm based on a new compound chaotic system," *Entropy*, vol. 21, no. 10, p. 1004, 2019.
[19] 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.
[20] 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.
[21] 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, doi: 10.1007/s11071-020-05503-y.
[22] A. Javeed, T. Shah, and A. Ullah, "Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group," *Wireless Pers. Commun.*, Jan. 2020.
[23] 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.
[24] S. Beg, N. Ahmad, A. Anjum, M. Ahmad, A. Khan, F. Baig, and A. Khan, "S-box design based on optimize LFT parameter selection: A practical approach in recommendation system domain," *Multimedia Tools Appl.*, pp. 1–18, Jan. 2020.
[25] 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.
[26] L. Shuai, L. Wang, L. Miao, and X. Zhou, "S-boxes construction based on the Cayley graph of the symmetric group for UASNs," *IEEE Access*, vol. 7, pp. 38826–38832, 2019.
[27] M. Niemiec and L. Machowski, "A new symmetric block cipher based on key-dependent S-boxes," in *Proc. IV Int. Congr. Ultra Modern Telecommun. Control Syst.*, Oct. 2012, pp. 474–478.
[28] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "Construction of S8 Liu J S-boxes and their applications," *Comput. Math. Appl.*, vol. 64, no. 8, pp. 2450–2458, Oct. 2012.
[29] G. Higman and Q. Mushtaq, "Coset diagrams and relations for PSL (2, Z)," *Arab Gulf J. Sci. Res.*, vol. 1, no. 1, pp. 159–164, 1983.
[30] P. J. Cameron, "Encyclopaedia of design theory," in *Cayley Graphs and Coset Diagrams*. 2013, pp. 1–9.
[31] R. C. Lyndon and E. Paul, *Combinatorial Group Theory*, vol. 89. Springer, 2015.
[32] Q. Mustaq, "Parametrization of all homomorphisms from PGL(2, Z) into PGL(2, q)," *Commun. Algebra*, vol. 20, no. 4, pp. 1023–1040, 1992.
[33] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *IEE Proc. E Comput. Digit. Techn.*, vol. 135, no. 6, pp. 325–335, 1988.
[34] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology—CRYPTO*. 1986, pp. 523–534.
[35] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1993, pp. 386–397.
[36] L. D. Burnett, "Heuristic optimization of Boolean functions and substitution boxes for cryptography," Ph.D. dissertation, Dept. Inf. Technol., Inf. Secur. Inst., Queensland Univ. Technol., Brisbane, QLD, Australia, 2005.
[37] S. Kavut, "Results on rotation-symmetric S-boxes," *Inf. Sci.*, vol. 201, pp. 93–113, Oct. 2012.
[38] X.-M. Zhang and Y. Zheng, "GAC—The criterion for global avalanche characteristics of cryptographic functions," in *J.UCS The Journal of Universal Computer Science*. Berlin, Germany: Springer, 1996, pp. 320–337.
[39] J. Daemen and V. Rijmen, *The Design of Rijndael-AES:The Advanced Encryption Standard*. Berlin, Germany: Springer, 2002.

[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, 2018.

[41] M. Khan, T. Shah, and S. I. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption," *Neural Comput. Appl.*, vol. 27, no. 3, pp. 677–685, Apr. 2016.

[42] W. Yong and L. Peng, "An improved method to obtaining S-box based on chaos and genetic algorithm," *HKIE Trans.*, vol. 19, no. 4, pp. 53–58, Jan. 2012.

[43] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel design of chaos based S-boxes using genetic algorithm techniques," in *Proc. IEEE/ACS 11th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2014, pp. 678–684.

[44] 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, 2015.

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

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

[47] 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.

[48] 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.

[49] M. Khan, T. Shah, H. Mahmood, and M. A. Gondal, "An efficient method for the construction of block cipher with multi-chaotic systems," *Nonlinear Dyn.*, vol. 71, no. 3, pp. 489–492, Feb. 2013.

[50] 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.

[51] 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.

[52] A. Ullah, S. S. Jamal, and T. Shah, "A novel construction of substitution box using a combination of chaotic maps with improved chaotic range," *Nonlinear Dyn.*, vol. 88, no. 4, pp. 2757–2769, Jun. 2017.

[53] Attaullah, S. S. Jamal, and T. Shah, "A novel algebraic technique for the construction of strong substitution box," *Wireless Pers. Commun.*, vol. 99, no. 1, pp. 213–226, Mar. 2018.

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

[55] 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.

[56] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, "Substitution box generation using chaos: An image encryption application," *Appl. Math. Comput.*, vol. 332, pp. 123–135, Sep. 2018.

[57] 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.

[58] 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.

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

[60] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "Generalized majority logic criterion to analyze the statistical strength of S-boxes," *Zeitschrift für Naturforschung A*, vol. 67, no. 5, pp. 282–288, May 2012.

[61] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, and U. Y. Bhatti, "Some analysis of S-box based on residue of prime number," *Proc. Pakistan Acad. Sci.*, vol. 48, no. 2, pp. 111–115, 2011.

[62] X. Yi, S. Xin Cheng, X. Hu You, and K. Yan Lam, "A method for obtaining cryptographically strong 8×8 S-boxes," in *Proc. IEEE Global Telecommun. Conf. Rec. (GLOBECOM)*, vol. 2, Nov. 1997, pp. 689–693.

[63] J. Kim and R. C.-W. Phan, "Advanced differential-style cryptanalysis of the NSA's skipjack block cipher," *Cryptologia*, vol. 33, no. 3, pp. 246–270, Jul. 2009.

[64] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Jan. 2017.

ABDUL RAZAQ received the Ph.D. degree from the Department of Mathematics, Quaid-i-Azam University, Islamabad, in 2015. He is currently an Assistant Professor with the University of Education at Jauharabad, Lahore. His main research interests include algebra and analysis and cryptography.

HANAN ALOLAIYAN received the Ph.D. degree in mathematics from King Saud University, Saudi Arabia. She is currently an Assistant Professor with the Department of Mathematics, King Saud University. She has published several research articles in reputable journals. Her research interests include algebra and analysis and cryptography.

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. He has been as Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, since 2011. He has published over 70 research articles in international reputed refereed journals and conference proceedings. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, and optimization techniques.

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 an Assistant Professor with The Islamia University of Bahawalpur. His main research interests include the theory of group graphs, chemical graph theory, algebraic cryptography, homomorphic public-key cryptosystems over groups, and algorithms development over Galois fields.

UMER SHUAIB was born in Faisalabad, in June 1980. He received the Ph.D. degree in group theory from Quaid-i-Azam University, Islamabad, Pakistan, in 2016. He is currently an Assistant Professor in mathematics with Government College University, Faisalabad, Pakistan. His research interests include group theory and its generalization, fuzzy logic, and cryptography.

WAQAR ASLAM (Member, IEEE) received the M.Sc. degree in computer science from Quaid-i-Azam University, Islamabad, Pakistan, and the Ph.D. degree in computer science from the Eindhoven University of Technology, The Netherlands. He is currently an Assistant Professor in computer science and information technology with The Islamia University of Bahawalpur, Pakistan. His research interests include performance modeling and QoS of wireless/computer networks, performance modeling of (distributed) software architectures, radio resource allocation, the Internet of Things, fog computing, effort/time/cost estimation of software development in (distributed) agile setups, social network data analysis, and DNA/chaos-based information security. He received the Overseas Scholarship for the Ph.D. degree from HEC, Pakistan.

MOATSUM ALAWIDA received the B.Sc. degree from Mutah University, Jordan, in 2005, and the M.Sc. degree in information systems from The University of Jordan, in 2010. He is currently pursuing the Ph.D. degree with the School of Computer Sciences, Universiti Sains Malaysia. His research interests include chaotic systems, chaos-based applications, and cryptography.