IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 7 November 2023, accepted 26 November 2023, date of publication 28 November 2023,
date of current version 8 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3337443

RESEARCH ARTICLE

A Robust S Box Design Using Cyclic Groups and Image Encryption

RASHAD ALI[1], MUHAMMAD KAMRAN JAMIL[1], AMAL S. ALALI[2], JAVED ALI[1], AND GULRAIZ AFZAL[1]

[1]Department of Mathematics, Riphah International University, Lahore 54000, Pakistan
[2]Department of Mathematical Sciences, College of Science, Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia

Corresponding author: Muhammad Kamran Jamil (m.kamran.sms@gmail.com)

This work was supported by Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia, under Project PNURSP2023R231.

ABSTRACT Modern cryptographic systems use substitution boxes (S-boxes) throughout the encryption process to enhance the security of the plaintext. The integrity of the communication process is ensured by these S-boxes, which are vital in converting the ciphertext back into the original plaintext during the decryption phase. The cryptographic strength of a certain S-box has a substantial impact on the overall security of a given cipher. As a result, many researchers have used innovative construction techniques to create robust S-boxes. The method used in this paper is a novel combination of a specific map on the direct product of cyclic groups of order 16×16 and an inversion map of a Galois field with order 256. This strategy aims to produce dynamic S-boxes. The proposed method can produce a large number of strong S-boxes by making little changes to the map's parameters. Four S-boxes were created and their performance was analyzed using industry standards such as bijectivity, the strict avalanche criterion (SAC), nonlinearity (NL), the bit independence criterion (BIC), linear probability (LAP), and differential probability (DAP). The performance of the recommended S-boxes was compared to that of state-of-the-art S-boxes to show their efficacy. The proposed S-box also exhibits considerable potential as a candidate for modern cryptosystems aiming at securing multimedia information, as shown by a suggested method for protecting the privacy of digital images using it. The effectiveness of the encryption method was then assessed using several tests including contrast, correlation, homogeneity, entropy, energy, Number of Pixel change rate (NPCR), and Unified Average changing intensity (UACI). We observed the efficacy of the suggested method for image encryption by comparing our results with different methods.

INDEX TERMS AES, CBC, direct product of cyclic groups, galois field, NPCR, UACI.

I. INTRODUCTION

A major difficulty for cryptographers is to ensure data security in light of the quick development of communication technologies. To ensure the security of transmitted data, a variety of useful encryption methods and approaches have been created in fascinating literary publications. Block encryption methods are widely used in modern cryptographic systems because of their significance in such circumstances. Block encryption techniques depend heavily on the S-box. Numerous cryptographic methods, including the Advanced Encryption Standard (AES), the International Data Encryption Algorithm (IDEA), and the Data Encryption Standard (DES) use the S-box. The S-box's security has an impact on the overall security of the complete cryptosystem. To ensure the security of cryptographic systems, the S-box is thus confirmed to play a significant role as a non-linear component. After the DES was released in 1977 by a well-known computer manufacturing company, intensive research resulted in major improvements to the cryptographic method. A group of college students eventually managed to breach the security of DES. After that, it became clear that a more effective and secure encryption technique needed to be devised. The AES designed by Daemen and Rijmen in 2002 is the most extensively used encryption system nowadays, [1]. The S-box plays an indispensable part in

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

determining the reliability of encryption. It is analogous to undermining the encryption's security to use a poor S-box during the encryption procedure. Therefore, before utilizing an S-box in a cryptosystem, it is imperative to assess its robustness. The nonlinearity, linear approximation probability, bit independence criteria, severe avalanche criterion, and differential approximation probability are some of the strength assessment techniques used in the evaluation of S-boxes.

A. LITERATURE REVIEW

There are a lot of methods available in the literature for building strong S-boxes. The S-box of AES was generated using an affine map and inversion map of $GF(2^8)$. The resulting S-box has very sound cryptographic properties and it is still used as a standard to compare newly generated S-boxes using other techniques as developed by researchers. One of the strong S-boxes is the APA S-box which was created using the composition of affine, inversion, and affine maps on a Galois field of order 256. The authors in [49] used an affine map and inversion map to construct strong S-boxes using 3 finite fields of order 256. The utilized approach is simple and very efficient for the generation of strong S-boxes, but we can generate a limited number of S-boxes using this approach. Razaq et al. introduced the term of coset graphs and used symmetric groups to construct robust S-boxes of good cryptographic properties [41]. The authors further used S-boxes to encrypt digital images and compared their results with some available S-boxes. The proposed technique can be used to generate 462422016 S-boxes. Hussain et al. used the chaos theory and algebraic theory to design sturdy S-boxes in [67]. The authors used the chaotic logistic map and Mobius transformation to design an S-box. They applied a suitable random permutation of degree 256 to enhance the cryptographic strength of the designed S-box. Mahboob et al. [40] proposed a new approach for assembling S-boxes using a specific quantic fraction transformation. They used the fractional function over a finite field of order 257 to generate s-boxes. They used a specific permutation of S_{256} to amplify the strength of generated S-boxes. The authors used these substitution boxes for the image encryption scheme and the contrast in the encrypted image was noticeable with a sound score of entropy. Razaq et al. [63] used the coset graph of the action of the modular group on a finite field to generate cryptographically robust S-boxes. The authors also used some specific permutations to enhance the strength of initial S-boxes.

The main objective of this work is to enhance the security of the S-box by introducing supplementary measures. There are a lot of techniques available in literature using symmetric groups and cyclic groups to construct S-boxes. The usage of ring and field theory is really common in cryptography for creating S-boxes. As per our information, there is not a single S-box developed using direct product of groups. The methods and strategies discussed in the literature can be categorized as either being appropriate for producing static S-boxes or being overly difficult and time-consuming. Static S-boxes have inherent flaws and restrictions. By crypt-analyzing the intercepted ciphertext with the help of these S-boxes, attackers may be able to determine the original plaintext. The methods described in the literature for developing dynamic and key-dependent S-boxes are especially complicated and inefficient. Thus, there is a dire need for a simple and efficient approach that can generate a large number of S-boxes in a very short time. In this study, we have presented an efficient approach to generate a large number of S-boxes using the composition of a specific map on the direct product of cyclic groups and inversion of a finite field of order 256. The S-box created in this way has a high level of security and closely resembles the ideal values specified by the conventional S-box. The security strength of the proposed S-box is thoroughly tested and compared with other S-boxes, confirming its high level of security.

B. MOTIVATION

The following are the main goals for this study to improve the strength of S-boxes over algebraic structures and their applicability in different cryptosystems:

1) There are a few S-boxes in literature based on cyclic groups with nonlinearity less than 112.
2) There is no usage of the direct product of cyclic groups in cryptography for designing S-boxes as per our knowledge.
3) There is a lot of usage of permutations of S_{256} in existing schemes as compared to the inversion of the Galois field.
4) Usage of S-boxes for image encryption to maximize entropy to 8.

C. CONTRIBUTION

In summary, the important contributions of the proposed study are:

1) We introduced the concept of Direct Product of Cyclic groups to generate S-boxes.
2) A new class of bijective functions on the direct product of cyclic groups is introduced which can be used for the study of the automorphism group of the direct product of cyclic groups.
3) We designed 4 S-boxes with each having nonlinearity 112 and we can get 983040 S-boxes of almost optimal features by this algorithm.
4) Time consumption for generating an S-box by the proposed algorithm is merely 0.01 sec.

D. STRUCTURE OF THE ARTICLE

The remaining six sections make up the study. In Section II, we deal with a direct product of cyclic groups and we present some irreducible polynomials of degree 8. The tables of multiplicative inverses of the elements of the Galois field of order 256 were constructed by utilizing the irreducible

polynomials. We presented the proposed algorithm for the construction of the S-box in section III. The created S-box was examined using the tests of NL, SAC, BIC, LAP, and DU in section IV. The application of the created S-box for picture encryption using AES is covered in Section V and the comparison of the outcomes was explored using majority logic criteria (MLC) and Differential analysis. Section VI concluded and discussed possible plans.

II. DIRECT PRODUCT OF GROUPS AND GALOIS FIELD

Let $G_1, G_2, G_3, \ldots, G_n$ be finite groups then the external direct product of $G_1, G_2, G_3, \ldots, G_n$ is denoted by $G_1 \times G_2 \times G_3 \times \ldots \times G_n$ and is defined as $G_1 \times G_2 \times G_3 \times \ldots \times G_n = \{(g_1, g_2, g_3, \ldots, g_n) \mid g_i \in G_i ; \forall i = 1, 2, 3, \ldots, n\}$ where the operation is component wise. Consider two copies of $\mathbb{Z}_{16}$ then $\mathbb{Z}_{16} \times \mathbb{Z}_{16} = \{(x, y) \mid x, y \in \mathbb{Z}_{16}\}$ is a group of order 256.

Recall that for any irreducible polynomial $r(v)$ of degree 8 the ring $\frac{\mathbb{Z}_2[v]}{< r(v) >} = \{a_7 t^7 + a_6 t^6 + \ldots a_1 t + a_0 \mid a_0, a_1, \ldots, a_7 \in \mathbb{Z}_2\}$ is a finite field of order 256 denoted by $GF(2^8)$, where t is particular root of $r(v)$. Consider the four polynomials $m_1(t) = t^8 + t^6 + t^5 + t + 1, m_2(t) = t^8 + t^4 + t^3 + t + 1, m_3(t) = t^8 + t^7 + t^6 + t^5 + t^4 + t + 1$ and $m_4(t) = t^8 + t^4 + t^3 + t^2 + 1$, then four finite fields of order 256 are produced. The Tables 1, 2, 3, 4 represent the multiplicative inverses of the elements of $GF(2^8)$ with respect to irreducible polynomials m_1, m_2, m_3 and m_4.

The algorithm for multiplicative inverse is described as

1) $m = 8; p = 2, irrpolydecimal = 283$
2) $GF = gf(0 : (p^m - 1), m, irrpolydecimal)$
3) $GFinv = gf(zeros(1, p^m), m, irrpolydecimal)$
4) for $i = 2 : p^m GFinv(i) = inv(GF(i))$ end
5) $GFint = double(GF.x)$
6) $GFinvint = double(GFinv.x)$

III. CONSTRUCTION OF S-BOXES

In this section, we will formulate the proposed algorithm for the construction of new S-boxes. Define a map $T : \mathbb{Z}_{16} \times \mathbb{Z}_{16} \to \mathbb{Z}_{16} \times \mathbb{Z}_{16}$ by $T(x, y) = (ay + c(\mod 16), bx + d(\mod 16))$ for all $(x, y) \in \mathbb{Z}_{16} \times \mathbb{Z}_{16}$, where $a, b \in U(16)$ and $c, d \in \mathbb{Z}_{16}$. The map T is an Automorphism of $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ if and only if $c = 0 = d$ but it does not produce robust S-boxes as compared to non-zero values of c and d. So, we used non-zero values of c and d to design S-boxes. For non-zero c and d the map T is just a bijection and not a homomorphism.

We choose $a = 15, b = 15, c = 7, d = 11$ for calculations, then the map $T(x, y) = (15y + 7(\mod 16), 15x + 11(\mod 16))$ is used to generate 256 ordered pairs. We will use the composition of outputs of T and inversion map of Galois field of order 256. Before applying inversion map we convert x, y in binary and concatenate bits to form 8 bits. Convert this 8 bit to a decimal and finally we get the result in $\{0, 1, 2, \ldots 255\}$. Let f_i be the inversion map of Galois field of order 256 corresponding to irreducible polynomial m_i

$$f_i(t) = \begin{cases} 0, & \text{if } t = 0 \\ t^{-1}, & \text{if } t \neq 0 \end{cases}$$

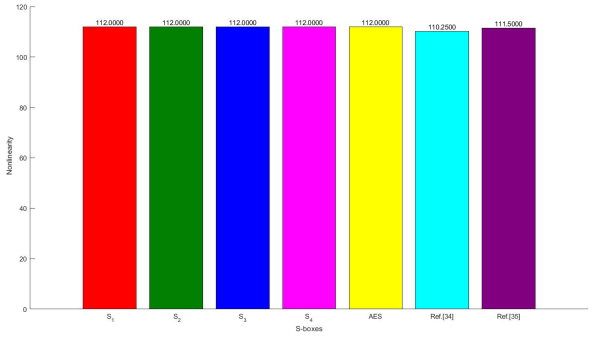

FIGURE 1. Nonlinearity Comparison of generated S-boxes with some 8 × 8 S-boxes.

where $i = 1, 2, 3, 4$. Now, we will formulate all 4 S-boxes according to the following map

$$S_i(u) = (T \circ f_i)(u), \quad u \in \{0, 1, 2, 3, 255\}$$

The algorithm for generating S-boxes is described as

1) Convert each entry of set {0, 1, 2, 3, , , 255} into binary and separate each of the 4 bits a part. Form decimal values from these two binary values and get an ordered pair (x, y), where $0 \leq x \leq 15, 0 \leq x \leq 15$.
2) Apply the map T on these ordered pairs and reverse the process described in 1st step.
3) Compose the result of step 2 with inverse map of Galois field to obtain final S-box.

Both compositions $(T \circ f)$ and $(f \circ T)$ can be used to generate robust S-boxes of optimal features. In this article, we are only interested in $(T \circ f)$.

IV. ANALYSIS OF PROPOSED S-BOXES

In this section, we evaluate the capability of the provided algebraic method to generate reliable 8 × 8 S-boxes. All generated S-boxes are balanced and bijective. The effectiveness of S-boxes is assessed by accepted testing standards, such as nonlinearity, strict avalanche criterion, output bit independence, differential uniformity, and linear approximation probability. The efficiency of the evaluations was then assessed by contrasting the results with those of widely employed S-boxes.

A. NONLINEARITY (NL)

The degree to which an S-box deviates from a linear relationship between its input and output bits in terms of magnitude is referred to as its nonlinearity. In simple terms, it should not be possible to predict the output bits of an S-box accurately by using a basic linear combination of its input bits. When considering 8 × 8 S-boxes, the AES S-box (112) is still thought to be the best option for generating the highest level of nonlinearity.

B. STRICT AVALANCHE CRITERIA (SAC)

The degree to which a small change in the input bits of an S-box causes appreciable changes in the output bits is determined by a feature known as the strict avalanche

TABLE 1. Multiplicative inverses of $GF(2^8)$ w.r.t m_1.

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

TABLE 2. Multiplicative inverses of $GF(2^8)$ w.r.t m_2.

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

TABLE 3. Multiplicative inverses of $GF(2^8)$ w.r.t m_3.

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

requirements for an S-box. It demands that no matter how many input bits are left, on average, for any single-bit input difference, exactly half of the output bits must change. This characteristic guarantees a high degree of dispersion and makes it challenging to infer the input from the output even when a little change in the input to the S-box results in a complete transformation in the output. The strict avalanche criteria is a crucial component for symmetric encryption algorithms to provide robust cryptographic features.

C. BIT INDEPENDENCE CRITERIA (BIC)

A set of requirements called the "bit independence criteria for an S-box" is used to assess the reliability and security of an S-box. It assesses the degree of statistical independence between the input and output bits of an S-box. By assessing the correlation between input and output bits for various input differentials (the difference between input pairs), the bit independence criteria evaluate the behavior of an S-box. The output bits of a good S-box should be statistically uncorrelated with the input bits, demonstrating a high degree of bit independence.

D. LINEAR APPROXIMATION PROBABILITY (LAP)

The linearity of an S-box can be evaluated using a metric called linear approximation probability. It measures the probability of a linear relationship between the input and output of

TABLE 4. Multiplicative inverses of $GF(2^8)$ w.r.t m_4.

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

TABLE 5. Working for S-box S_1.

Input	Elements of $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$	Images under T	Binary values	Concatenation of bits	Decimal	Inverse of input	Entry of S-box
0	$(0, 0)$	$(7, 11)$	$(0111, 1011)$	01111011	123	0	123
1	$(0, 1)$	$(6, 11)$	$(0110, 1011)$	01101011	107	1	107
2	$(0, 2)$	$(5, 11)$	$(0101, 1011)$	01011011	91	177	96
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
254	$(15, 14)$	$(9, 12)$	$(1001, 1100)$	10011100	156	68	55
255	$(15, 15)$	$(8, 12)$	$(1000, 1100)$	10001100	140	125	164

TABLE 6. S-box S_1.

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

TABLE 7. S-box S_2.

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

an S-box. Calculating the likelihood of a linear approximation involves comparing the number of input-output pairs that meet a given linear equation to the total number of possible input-output pairs. For the S-box to have strong cryptographic qualities, there should be a lower linear approximation probability, which denotes a higher amount of nonlinearity.

TABLE 8. S_3.

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

TABLE 9. S_4.

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

TABLE 10. Comparison of SAC of generated S-boxes with some 8 × 8 S-boxes.

S-box	S_1	S_2	S_3	S_4	AES	Ref. [35]	Ref. [36]
SAC	0.5051	0.5034	0.5091	0.4900	0.5040	0.5070	0.5060

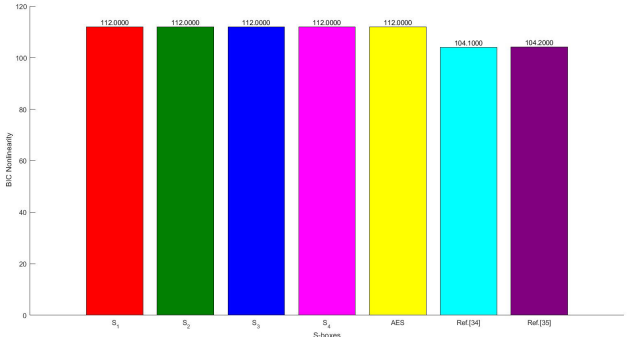

FIGURE 2. BIC-Nonlinearity Comparison of generated S-boxes with some 8 × 8 S-boxes.

TABLE 11. Comparison of BIC-SAC of generated S-boxes with some 8 × 8 S-boxes.

S-box	S_1	S_2	S_3	S_4	AES	Ref. [35]	Ref. [36]
BIC-SAC	0.5066	0.5066	0.5080	0.5017	0.5046	0.5025	0.5029

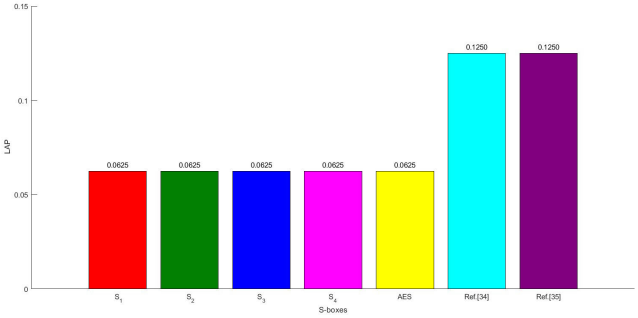

FIGURE 3. Comparison of Probability of Linear Approximation of generated S-boxes with some 8 × 8 S-boxes.

E. DIFFERENTIAL APPROXIMATION PROBABILITY (DAP)

The possibility of a particular input difference resulting in a particular output difference is quantified by the differential approximation probability of an S-box. Typically, differential cryptanalysis or other cryptanalysis methods are used to calculate the differential approximation probability. It entails examining the input-output differences for various inputs to analyze the behavior of the S-box. A lower probability suggests more resistance to differential attacks because it becomes less likely that an attacker will make use of an S-box's differential properties.

F. FIXED POINTS

One of the design goals of an S-box is to ensure that it does not have fixed points, which means that no input value maps to itself under the S-box transformation. A point $x \in \{0, 1, 2, , , 255\}$ is called a fixed point of an S-box if $S(x) = x$. An S-box is considered good if it has no fixed points.

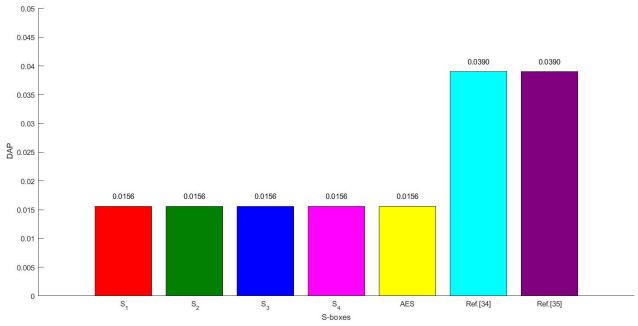

FIGURE 4. Comparison of Probability of Differential Approximation of generated S-boxes with some 8 × 8 S-boxes.

TABLE 12. Fixed point analysis of S-boxes.

S-boxes	S-box S_1	S-box S_2	S-box S_3	S-box S_4	AES	[42]	[41]
No. of fixed points	0	1	2	0	0	2	1

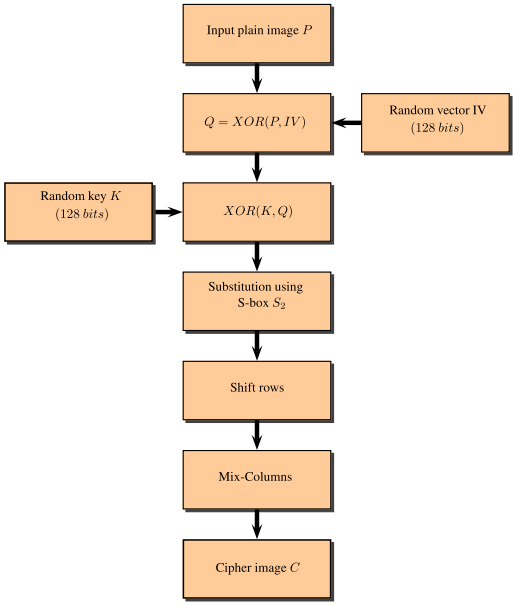

FIGURE 5. Flowchart of Image Encryption Scheme.

V. IMAGE ENCRYPTION SCHEME

To determine the applicability of the S-box for image security applications, the suggested S-box presented in Table 7 is employed to encrypt digital photographs. We used different criteria to measure the strength of the image encryption scheme and generated an S-box. We employed Barbara, Baboon, Cameraman, and Pepper of size 512 × 512 as test images. The key space of the algorithm is 2^{256}, which is a quite large number and shows the strength of the scheme. The flowchart of the proposed scheme is depicted in Figure 5.

A. HISTOGRAM ANALYSIS

The distribution of pixel intensities in an image can be examined using the histogram analysis approach. A consistent and balanced distribution of the elements in the encrypted data is ideal for a strong cryptographic technique.

B. ENTROPY

Entropy is a measure used to express the degree of disorder or randomness in an image's pixel values. When the entropy value of scrambled illustrations is close to 8, it indicates that the pixel values are distributed as uniformly as possible throughout the image. As a result, it becomes challenging to anticipate the original image based on the altered or scrambled version.

$$\text{Entropy} = -\sum_{j} p(v_j) log_2 p(v_j).$$

C. CONTRAST

The difference in brightness and color between the image's light and dark portions is referred to as contrast. Any visual patterns, structures, or statistical dependencies found in the original image should be disrupted by a powerful encryption system when it comes to protecting images. Our scheme can successfully mask the original content and make it difficult for attackers to decipher important information by achieving a high level of contrast in the encrypted image. It would be challenging to extract details, characteristics, or patterns in a high-contrast encrypted image.

$$\text{Contrast} = \sum_{i}\sum_{j}(i-j)^2 p(i,j).$$

D. CORRELATION

The statistical link between various elements of an image, especially between the pixel values, is referred to as correlation. High degrees of correlation between adjacent pixels in the encrypted image is a desirable quality in image encryption. This gives the image a more random appearance and aids in hindering the recovery of useful information from local visual patterns. The original image may be recovered or security flaws in the encryption method may be exposed if there is a low correlation between neighboring pixels, which suggests that they are different or independent. Low cross-correlation and high auto-correlation qualities are the goals of the correlation analysis used in picture encryption. By reducing statistical correlations between pixels and making it more difficult for an attacker to exploit patterns or retrieve the original image, the encryption approach improves security in this way.

$$r_{uv} = \frac{\sum_{i=1}^{m}(u_i - \bar{u})(v_i - \bar{v})}{\sqrt{\sum_{i=1}^{m}(u_i - \bar{u})^2}\sqrt{\sum_{i=1}^{m}(v_i - \bar{v})^2}}.$$

E. ENERGY

Energy is a measure that describes the total contrast or complexity of the texture in an image. It is computed by summing up the squared values of all the elements in the Gray-Level Co-occurrence Matrix (GLCM). An image with a high energy value has fine features and clear edges, which creates a striking contrast and texture. On the other hand, if an

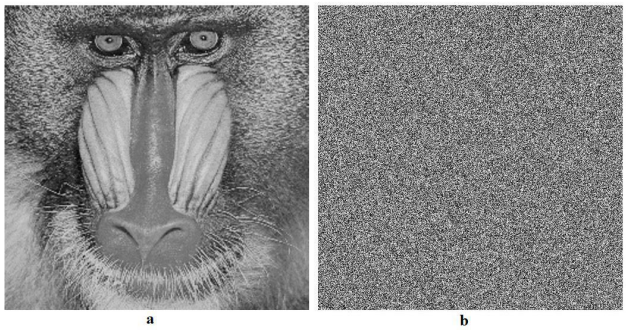

FIGURE 6. Plain and Cipher image of Baboon.

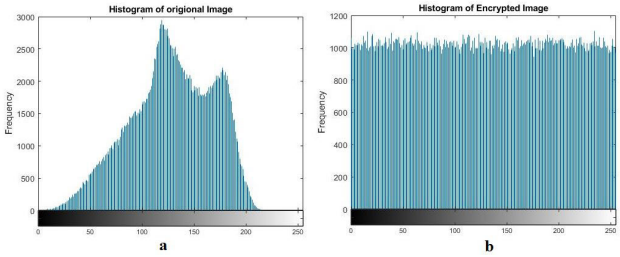

FIGURE 7. Histogram of Plain and Cipher image of Baboon.

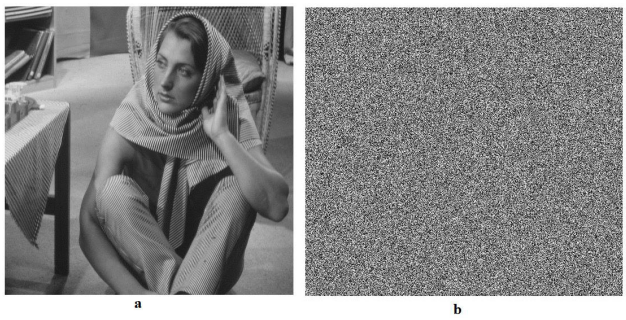

FIGURE 8. Plain and Cipher image of Barbara.

image has a low energy value, it tends to exhibit a uniform and less textured appearance.

$$Energy = \sum_{u=1}^{N}\sum_{v=1}^{N} GLCM(u,v)^2.$$

F. HOMOGENEITY

In an image encryption scheme, homogeneity refers to the level of uniformity or similarity within an encrypted image. Homogeneity is a texture attribute that quantifies the level of similarity between adjacent pixels' gray or color tones, measuring how uniform or consistent they are.

$$Homogeneity = \frac{1}{1 + \sum_{u=1}^{M}\sum_{v=1}^{M}\frac{(u-v)^2}{M^2}},$$

G. NUMBER OF PIXEL CHANGE RATE (NPCR)

This metric quantifies the dissimilarity between two images by measuring the percentage of pixels that are different. The NPCR (Number of Pixel Change Rate) metric evaluates how a single pixel alteration affects the entirety of an

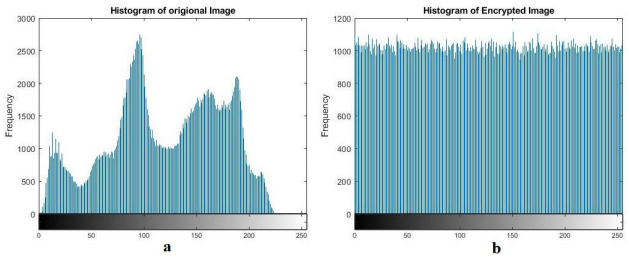

FIGURE 9. Histogram of Plain and Cipher image of Barbara.

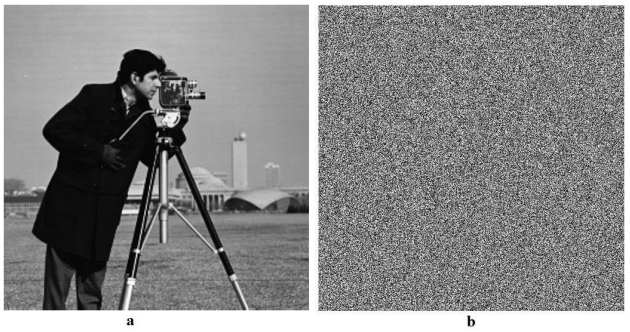

FIGURE 10. Plain and Cipher image of Cameraman.

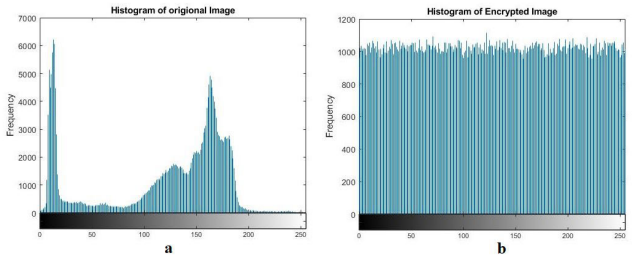

FIGURE 11. Histogram of Plain and Cipher image of Cameraman.

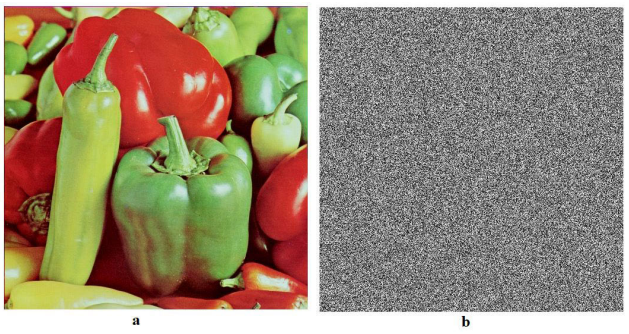

FIGURE 12. Plain and Cipher image of Pepper.

image encrypted using the suggested approach. It measures the frequency of pixel changes in the encrypted image corresponding to each pixel change in the original image. Consider two encrypted images C and D with dimensions M and N, corresponding to two plain images who has one pixel change. We can measure NPCR by

$$NPCR = \frac{\sum_{i,j} E(i,j)}{M \times N}$$

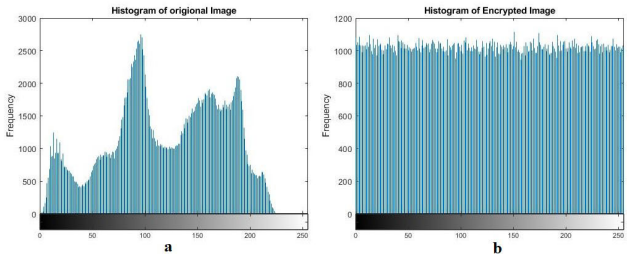

FIGURE 13. Histogram of Plain and Cipher image of Pepper.

TABLE 13. Results of majority logic criterion for Plain and Cipher images of Barbara, Baboon, cameraman and Pepper.

	S-box	Entropy	Contrast	Correlation	Energy	Homogeneity
Barbara	Host image	7.552179	0.60717	0.87616	0.088185	0.83093
	S-box S_2	7.999645	10.5730	-0.004432	0.015627	0.38832
	Ref. [44]	7.9967	10.6646	-0.0138	0.0156	0.3863
	Ref. [53]	7.9967	-	-0.0061	-	-
	Ref. [52]	7.9983	-	-	-	-
Baboon	Host image	7.292549	0.34764	0.89358	0.11627	0.84504
	S-box S_2	7.999436	10.6137	-0.007901	0.01563	0.38739
	AES	7.73018	7.322085	0.087904	0.0244776	0.483523
	Skipjack	7.673853	6.805101	0.195849	0.026131	0.495087
	Residue Prime	7.65955	6.368367	0.099634	0.026099	0.49848
	Xyi	7.2531	8.3108	0.417	0.0196	0.4533
Cameraman	Host image	7.047955	0.18618	0.97505	0.19736	0.93719
	S-box S_2	7.999417	10.5535	-0.004453	0.015628	0.38825
	AES	7.9122	9.2322	0.081311	0.017216	0.4337
	Skipjack	7.7561	7.7058	0.1205	0.0239	0.4708
	Residue Prime	7.7059	8.1003	0.0090	0.0158	0.4940
	Xyi	7.7619	8.1945	0.0517	0.0158	0.4960
Pepper	Host image	7.593654	0.25607	0.95596	0.11068	0.89893
	S-box S_2	7.999457	10.6004	-0.005549	0.015628	0.38789
	Ref. [40]	7.9972	11.2629	-0.0039	0.0159	0.3855
	Ref. [41]	7.9973	12.0124	-0.0024	0.0124	0.3251
	Ref. [44]	7.9975	10.5539	-0.0045	0.0156	0.3848
	Ref. [49]	7.999253	-	0.02254	-	-
	Ref. [50]	7.9977	-	-	-	-
	Average	7.999489	10.5852	-0.005583	0.015628	0.3879

TABLE 14. NPCR and UACI results.

S-box	NPCR	UACI
Barbara		
Proposed	99.6220	33.450
Ref. [53]	99.6002	33.8184
Ref. [64]	99.6090	33.4907
Baboon		
Proposed	99.5980	33.354
Ref. [53]	99.6048	33.5547
Ref. [63]	99.6368	33.5321
Cameraman		
Proposed	99.6020	33.465
Ref. [61]	99.6150	33.4212
Ref. [62]	99.6152	33.4953
Pepper		
Proposed	99.6020	33.453
Ref. [54]	99.6300	33.410
Ref. [55]	99.6223	33.497
Average	99.6060	33.4248

where

$$E(i,j) = \begin{cases} 0, & \text{if } C(i,j) = D(i,j) \\ 1, & \text{if } C(i,j) \neq D(i,j). \end{cases}$$

Score of our proposed scheme is 99.6060, which is quite exceptional with very sound score of entropy.

H. UNIFIED AVERAGE CHANGING INTENSITY (UACI)

When a single pixel in the original image is changed, UACI evaluates the average intensity difference in the encrypted image compared to the original image. We can measure UACI by the formula

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|C(i,j) - D(i,j)|}{255}$$

whereas C, D, M, N are defined in NPCR. The UACI for our proposed scheme is 33.4248 which shows quality of encryption scheme.

VI. CONCLUSION AND FUTURE STUDY

We have demonstrated the utilization of the direct product of cyclic groups and the Galois field in this manuscript to obtain a superior S-box for encrypting images. We used a specific map and then by composing with inversion map of the Galois field of order 256, we obtained four new S-boxes. The proposed scheme can generate 983040 robust S-boxes of almost optimal features. The proposed approach guarantees good differential and linear probability, as well as the success of the SAC, nonlinearity, and BIC. We can observe the strength of generated S-boxes from comparison tables and bar charts, so our S-boxes can be used to secure plaintext. We employed one S-box to encrypt digital images using CBC mode of AES with a key space of 2^{256}. Tables 13 and 14 show that our proposed S-box and encryption scheme are better as compared to other image encryption schemes. In the future, we aim to construct S-boxes by a combination of some other groups and different algebraic structures.

ACKNOWLEDGMENT

The authors extend their appreciation to Princess Nourah Bint Abdulrahman University for funding this research under Researchers Supporting Project number (PNURSP2023R231), Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] J. Daeman and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Cham, Switzerland: Springer, Nov. 2002.
[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[3] Z. Gan, X. Chai, K. Yuan, and Y. Lu, "A novel image encryption algorithm based on LFT based S-boxes and chaos," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8759–8783, Apr. 2018.
[4] 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.
[5] I. Hussain, T. Shah, M. A. Gondal, M. Khan, and W. A. Khan, "Construction of new S-box using a linear fractional transformation," *World Appl. Sci.* , vol. 14, no. 2, pp. 1779–1785, 2011.
[6] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, Nov. 2018.
[7] 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, pp. 1–9, Oct. 2018.
[8] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "An efficient approach for the construction of LFT S-boxes using chaotic logistic map," *Nonlinear Dyn.*, vol. 71, nos. 1–2, pp. 133–140, Jan. 2013.
[9] N. Siddiqui, U. Afsar, T. Shah, and A. Qureshi, "A novel construction of S16 AES S-box," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 8, pp. 810–818, Aug. 2016.

[10] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," *Neural Comput. Appl.*, vol. 22, no. 6, pp. 1085–1093, May 2013.
[11] 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, pp. 1–16, Jan. 2017.
[12] S. Mahmood, S. Farwa, M. Rafiq, S. M. J. Riaz, T. Shah, and S. S. Jamal, "To study the effect of the generating polynomial on the quality of nonlinear components in block ciphers," *Secur. Commun. Netw.*, vol. 2018, pp. 1–8, Nov. 2018.
[13] 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.
[14] Y. Naseer, T. Shah, D. Shah, and S. Hussain, "A novel algorithm of constructing highly nonlinear S-p-boxes," *Cryptography*, vol. 3, no. 1, p. 6, Jan. 2019.
[15] 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.
[16] 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.
[17] Z. Bin Faheem, A. Ali, M. A. Khan, M. E. Ul-Haq, and W. Ahmad, "Highly dispersive substitution box (S-box) design using chaos," *ETRI J.*, vol. 42, no. 4, pp. 619–632, Aug. 2020.
[18] 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.
[19] Y. Tian and Z. Lu, "Chaotic S-box: Intertwining logistic map and bacterial foraging optimization," *Math. Problems Eng.*, vol. 2017, pp. 1–11, Jan. 2017.
[20] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.
[21] I. Vergili and M. D. Yücel, "Avalanch and bit independence properties for the ensembles of randomly chosen n×n S-boxes," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 9, pp. 137–145, Sep. 2001.
[22] J. Seberry, X.-M. Zhang, and Y. Zheng, "Systematic generation of cryptographically robust S-boxes," in *Proc. 1st ACM Conf. Comput. Commun. Secur.*, 1993, pp. 171–182.
[23] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT'93* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 1994, pp. 386–397.
[24] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *IEE Proc. E-Comput. Digital Techn.*, vol. 135, no. 6, p. 325, 1988.
[25] A. F. Webster and S. E. Tavares, "On the design of S-boxes, advances in cryptology," in *Proc. CRYPTO*. Berlin, Germany: Springer, 1986.
[26] 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.
[27] 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.
[28] 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.
[29] D. Lambic, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons Fractals*, vol. 58, pp. 16–21, Jan. 2014.
[30] L. C. Nizam Chew and E. S. Ismail, "S-box construction based on linear fractional transformation and permutation function," *Symmetry*, vol. 12, no. 5, p. 826, May 2020.
[31] B. Arshad and N. Siddiqui, "Construction of highly nonlinear substitution boxes (S-boxes) based on connected regular graphs," *Int. J. Comput. Sci. Inf. Secur.*, vol. 18, no. 4, pp. 105–122, 2020.
[32] N. Siddiqui, F. Yousaf, F. Murtaza, M. Ehatisham-ul-Haq, M. U. Ashraf, A. M. Alghamdi, and A. S. Alfakeeh, "A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field," *PLoS ONE*, vol. 15, no. 11, Nov. 2020, Art. no. e0241890.
[33] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019.
[34] 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.
[35] A. H. Zahid, L. Tawalbeh, M. Ahmad, A. Alkhayyat, M. T. Hassan, A. Manzoor, and A. K. Farhan, "Efficient dynamic S-box generation using linear trigonometric transformation for security applications," *IEEE Access*, vol. 9, pp. 98460–98475, 2021.
[36] F. A. Kadhim, G. H. A. Majeed, and R. S. Ali, "Proposal new s-box depending on DNA computing and mathematical operations," in *Proc. Al-Sadeq Int. Conf. Multidisciplinary IT Commun. Sci. Appl. (AIC-MITCSA)*, Baghdad, Iraq, May 2016, pp. 1–6.
[37] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "A new DNA-based S-box," *Int. J. Eng. Technol.*, vol. 15, no. 4, pp. 1–9, 2015.
[38] J. Frank and T. Mahalakshmi, "Secure data transfer through DNA cryptography using symmetric algorithm," *Int. J. Comput. Appl.*, vol. 133, no. 2, pp. 19–23, Jan. 2016.
[39] M. Asif, S. Mairaj, Z. Saeed, M. U. Ashraf, K. Jambi, and R. M. Zulqarnain, "A novel image encryption technique based on Mobius transformation," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–14, Dec. 2021.
[40] A. Mahboob, M. Asif, M. Nadeem, A. Saleem, S. M. Eldin, and I. Siddique, "A cryptographic scheme for construction of substitution boxes using quantic fractional transformation," *IEEE Access*, vol. 10, pp. 132908–132916, 2022.
[41] 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.
[42] J. Masseyand and X. Lai, "International data encryption algorithm," Signal Inf. Process. Lab, Eidgenossische Technique Hoehschule (ETH) Zurich, Zurich, Switzerland, Tech. Rep., 9752, 2023.
[43] A. H. Zahid, A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad, H. S. Alhadawi, and A. A. A. El-Latif, "A novel construction of dynamic S-box with high nonlinearity using heuristic evolution," *IEEE Access*, vol. 9, pp. 67797–67812, 2021.
[44] G. Hanchinamani and L. Kulkarni, "An efficient image encryption scheme based on quintuple encryption using Gumowski–Mira and tent maps," *Int. J. Contents*, vol. 11, no. 4, pp. 56–69, Dec. 2015.
[45] A. F. Shimal, B. H. Helal, and A. T. Hashim, "Extended of TEA: A 256 bits block cipher algorithm for image encryption," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 5, p. 3996, Oct. 2021.
[46] G. Ye, H. Wu, K. Jiao, and D. Mei, "Asymmetric image encryption scheme based on the quantum logistic map and cyclic modulo diffusion," *Math. Biosciences Eng.*, vol. 18, no. 5, pp. 5427–5448, 2021.
[47] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "A novel image encryption scheme using the composite discrete chaotic system," *Entropy*, vol. 18, no. 8, p. 276, Aug. 2016.
[48] P. S. Sneha, S. Sankar, and A. S. Kumar, "A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 3, pp. 1289–1308, Mar. 2020.
[49] A. Bejo and T. B. Adji, "The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box," *Nonlinear Dyn.*, vol. 93, no. 4, pp. 2105–2118, Sep. 2018.
[50] P. Wang, B. Cai, S. Xu, and B. Chen, "Reversible data hiding scheme based on adjusting pixel modulation and block-wise compression for encrypted images," *IEEE Access*, vol. 8, pp. 28902–28914, 2020.
[51] B. Idrees, S. Zafar, T. Rashid, and W. Gao, "Image encryption algorithm using S-box and dynamic Hénon bit level permutation," *Multimedia Tools Appl.*, vol. 79, nos. 9–10, pp. 6135–6162, Mar. 2020.
[52] 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.
[53] Z. Li, C. Peng, W. Tan, and L. Li, "A novel chaos-based color image encryption scheme using bit-level permutation," *Symmetry*, vol. 12, no. 9, p. 1497, Sep. 2020.
[54] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.
[55] O. M. AbuZaid, N. A. El-Fishawy, E. M. Nigm, and O. S. Faragallah, "A proposed encryption scheme based on Henon chaotic system (PESH) for image security," *Int. J. Comput. Appl.*, vol. 61, no. 5, pp. 29–39, Jan. 2013.
[56] X. Gao, M. Miao, and X. Chen, "Multi-image encryption algorithm for 2D and 3D images based on chaotic system," *Frontiers Phys.*, vol. 10, p. 498, Jun. 2022.

[57] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, "Image encryption with double spiral scans and chaotic maps," *Secur. Commun. Netw.*, vol. 2019, pp. 1–15, Jan. 2019.
[58] Z. Cheng, W. Wang, Y. Dai, and L. Li, "2D Sin-Cos-Henon map for color image encryption with high security," *J. Appl. Math.*, vol. 2022, pp. 1–11, Aug. 2022.
[59] Y. Hu, C. Zhu, and Z. Wang, "An improved piecewise linear chaotic map based image encryption algorithm," *Sci. World J.*, vol. 2014, pp. 1–7, Jan. 2014.
[60] A. Gupta, R. Thawait, K. A. K. Patro, and B. Acharya, "A novel image encryption based on bit-shuffled improved tent map," *Int. J. Control Theory Appl.*, vol. 9, no. 34, pp. 1–16, 2016.
[61] A. Al-Khedhairi, A. Elsonbaty, A. A. Elsadany, and E. A. A. Hagras, "Hybrid cryptosystem based on pseudo chaos of novel fractional order map and elliptic curves," *IEEE Access*, vol. 8, pp. 57733–57748, 2020.
[62] J. Deng, M. Zhou, C. Wang, S. Wang, and C. Xu, "Image segmentation encryption algorithm with chaotic sequence generation participated by cipher and multi-feedback loops," *Multimedia Tools Appl.*, vol. 80, pp. 13821–13840, Jan. 2021.
[63] A. Razaq, S. Akhter, A. Yousaf, U. Shuaib, and M. Ahmad, "A group theoretic construction of highly nonlinear substitution box and its applications in image encryption," *Multimedia Tools Appl.*, vol. 81, no. 3, pp. 4163–4184, Jan. 2022.
[64] X. Wang and J. Yang, "A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system," *Optik*, vol. 217, Sep. 2020, Art. no. 164884.
[65] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Arch. Comput. Methods Eng.*, vol. 27, no. 1, pp. 15–43, Jan. 2020.
[66] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "A novel pixel-split image encryption scheme based on 2D Salomon map," *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 118845.
[67] I. Hussain, A. Anees, T. Al-Maadeed, and M. Mustafa, "Construction of S-box based on chaotic map and algebraic structures," *Symmetry*, vol. 11, no. 3, p. 351, Mar. 2019.
[68] S. Kaliswaran and M. M. Parvees, "Image encryption using generalized feedback shift register, S-box and elliptic curve cryptosystem (GFSR-EC-SB)," *Image*, vol. 17, no. 1, pp. 1–18, 2023.
[69] H. Nazir, I. S. Bajwa, S. Abdullah, R. Kazmi, and M. Samiullah, "A color image encryption scheme combining hyperchaos and genetic codes," *IEEE Access*, vol. 10, pp. 14480–14495, 2022.
[70] L. Wang, Y. Cao, H. Jahanshahi, Z. Wang, and J. Mou, "Color image encryption algorithm based on double layer Josephus scramble and laser chaotic system," *Optik*, vol. 275, Mar. 2023, Art. no. 170590.

RASHAD ALI received the Graduate degree from the Government Graduate College of Science, Lahore, Pakistan, in 2017. He is currently pursuing the M.Phil. degree in mathematics with Riphah International University, Raiwind Campus, Lahore, Pakistan. He immerses himself fully in the enigmatic realms of cryptography. He joined HED, Punjab, in 2018, as a Lecturer in mathematics, currently posted with the Government Associate College, Haveli Lakha, Okara, Punjab, Pakistan.

MUHAMMAD KAMRAN JAMIL received the B.S. degree in mathematics from the University of Punjab, in 2009, the M.Phil. degree in mathematics (chemical graph theory) from the Abdus Salam School of Mathematical Sciences (ASSMS), Government College University Lahore, in 2013, under the supervision of Prof. Ioan Tomescu, and the Ph.D. degree from ASSMS, in 2016. He is currently the Head and an Associate Professor with the Department of Mathematics, Riphah International University, Lahore. He was a postdoctoral researcher position with United Arab Emirates University, United Arab Emirates. During the Ph.D. degree, he received the Premature-Ph.D. Quality Research Award. His research interests include topological indices of graphs, extremal graph theory, graph labeling, coloring in graphs, and distances in graphs. His major contribution to research is in chemical graph theory. In this area, he has published more than 100 research articles in international reputed journals. His research articles are cited more than 1000 times in scientific papers with H-index 21. He is a Reviewer to various international prestigious journals, including the *Mathematical Reviews* under American Mathematical Society and IEEE. He delivered various scientific lectures at international and national forums.

AMAL S. ALALI is working at the Department of Mathematical Sciences, College of Science, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. She has published many articles in well reputed journals. Her research interests include algebra, coding theory, cryptography, number theory, semi group theory, graph theory, and fuzzy logic.

JAVED ALI received the Master of Science degree in mathematics from the esteemed college. He is currently pursuing the M.Phil. degree in mathematics with RICAS, Raiwind Campus, Lahore, Pakistan. He holds the position of an Assistant Professor with the prestigious Government Graduate College of Science, Lahore. He is also teaching with the esteemed college. He has focused his dedication on the algebraic cryptography, specializing in the intricate field as he pursued higher education.

GULRAIZ AFZAL received the B.S. degree (Hons.) in mathematics from the Government Graduate College of Science, Lahore, Pakistan. He is currently pursuing the M.Phil. degree in mathematics with RIU, Raiwind Campus, Lahore. He is also working under SED Punjab, Pakistan. He is also working in the domain of cryptography where intricate algorithms and cryptographic protocols interwine forming an enigmatic and safeguarded world of secure communication.