Hindawi
Security and Communication Networks
Volume 2018, Article ID 4987021, 9 pages
https://doi.org/10.1155/2018/4987021

Research Article

A Novel Technique for the Construction of Safe Substitution Boxes Based on Cyclic and Symmetric Groups

Abdul Razaq[1], **Hanan A. Al-Olayan**[2], **Atta Ullah**[3], **Arshad Riaz**[1] and **Adil Waheed**[4]

[1]*Department of Mathematics, University of Education Lahore, Jauharabad Campus, Pakistan*
[2]*Department of Mathematics, King Saud University, Saudi Arabia*
[3]*Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan*
[4]*Department of Information Technology, University of Education Lahore, Jauharabad Campus, Pakistan*

Correspondence should be addressed to Abdul Razaq; makenqau@gmail.com

Received 4 June 2018; Accepted 19 September 2018; Published 4 October 2018

Academic Editor: Stelvio Cimato

In the literature, different algebraic techniques have been applied on Galois field $GF(2^8)$ to construct substitution boxes. In this paper, instead of Galois field $GF(2^8)$, we use a cyclic group C_{255} in the formation of proposed substitution box. The construction proposed S-box involves three simple steps. In the first step, we introduce a special type of transformation T of order 255 to generate C_{255}. Next, we adjoin 0 to C_{255} and write the elements of $C_{255} \cup \{0\}$ in 16×16 matrix to destroy the initial sequence $0, 1, 2, \ldots, 255$. In the 2^{nd} step, the randomness in the data is increased by applying certain permutations of the symmetric group S_{16} on rows and columns of the matrix. In the last step we consider the symmetric group S_{256}, and positions of the elements of the matrix obtained in step 2 are changed by its certain permutations to construct the suggested S-box. The strength of our S-box to work against cryptanalysis is checked through various tests. The results are then compared with the famous S-boxes. The comparison shows that the ability of our S-box to create confusion is better than most of the famous S-boxes.

1. Introduction

The foundation of modern cryptography was laid by Shannon [1]. Cryptography is the science of converting the secret information into dummy data so that it could reach the destination safely without leakage of the information. The modern cryptography is divided into several branches. However, symmetric key cryptography and public key cryptography are the two main areas of study. In symmetric key cryptography, the same key is used at both ends to encrypt and decrypt data/information, but in public key cryptography two different keys, public and private keys, are used. It is well-known that, in symmetric key cryptography the substitution box is a standout and basic ingredient, which performs substitution. In block ciphers, it is widely used to make the relationship between the ciphertext and the key unclear and vague. Due to these important applications of substitution box many algorithms have been developed to construct safer and more reliable S-boxes. Substitution boxes are used for the strong design of block encryption algorithms. S-box is the only nonlinear component for most of the block encryption algorithms such as international data encryption algorithm (IDEA), advanced encryption standard (AES), and data encryption standard (DES) [2]. Substitution boxes yield a DES-like cryptosystem with the perplexity property depicted by Shannon. In [3], it is shown that for weaker S-boxes, DES can be easily broken. It means that the security of DES-like cryptosystems is merely determined by the quality of the S-boxes used. Thus, in order to develop secure cryptosystems, the formation of safe S-boxes is a main focus of the researcher. To examine the strength of S-boxes, nonlinearity test, bit independent criterion, strict avalanche criterion, linear approximation probability analysis, differential uniformity test, and majority logic criterion are used. In the literature, there are many S-box construction methods such as inversion mapping, power polynomial, heuristic methods, and pseudorandom methods [4]. Incursions on the S-box component of data encryption standard (DES) damage

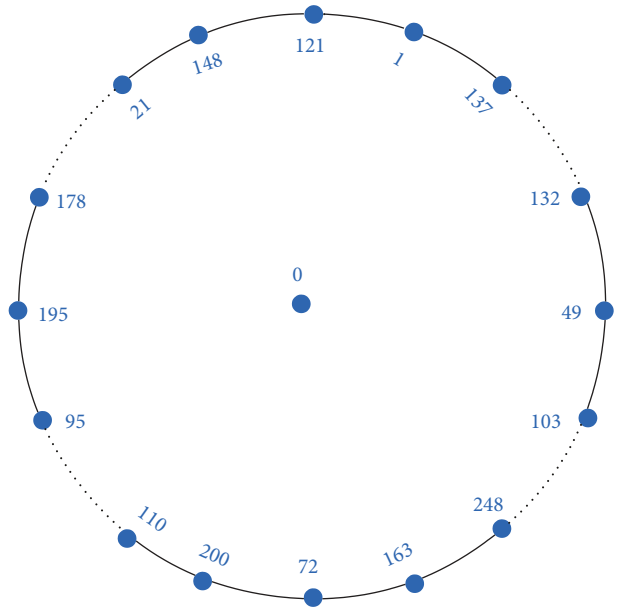

Figure 1: Cayley graph of $C_{255} \cup \{0\}$.

the design process of advanced encryption standard (AES) [3, 5]. Therefore, the substitution box component of AES is designed to ensure the security of the data/information in the presence of differential and linear cryptanalysis attacks [6].

Recently, since proposed algebraic attacks have been succeeded in some loops of AES, researchers have focused on alternative construction methods for substitution box [21]. Therefore, substitution box construction techniques based on group theory have been applied for alternative substitution box designs.

2. Algebraic Structure of Proposed Substitution Box

Let us denote a set of positive integers less than 256 by Υ; that is, $\Upsilon = \{1, 2, 3, \ldots, 255\}$. Consider a transformation $T : \Upsilon \longrightarrow \Upsilon$ defined by

$$T(z) = \begin{cases} \left(\dfrac{z}{16z+1}\right) \pmod{257} & if\ z \in \Upsilon - \{16, 136\} \\ \left(\dfrac{z}{32z+1}\right) \pmod{257} & if\ z = 16, 136. \end{cases} \quad (1)$$

It can be easily verified that T has order 255; that is, for any $z \in \Upsilon$, $T^{255}(z) = z$. Thus for all $z \in \Upsilon$, $T(z)$ generates a cyclic group $C_{255}=\{T(z), T^2(z), T^3(z), \ldots, T^{254}(z), z\}$. In this paper, we have taken $z = 1$.

Step I. First we simply present the elements of

$$C_{255} \cup \{0\} = \left\{T(1), T^2(1), T^3(1), \ldots, T^{254}(1), 1, 0\right\} \quad (2)$$

in 16×16 matrix (see Table 2). Cayley graph of $C_{255} \cup \{0\}$ is shown in Figure 1. In this way, the initial sequence $0, 1, 2, \ldots, 255$ is destroyed. If this matrix is conceded as S-box, its nonlinearity is 103.75, which is acceptable. Now we move to step II to create more randomness.

Step II. Since we have presented our data in 16×16 matrix, that is, a matrix with 16 rows and 16 columns, the randomness can be increased by interchanging the positions of the rows and columns. Algebraically, it is achieved by applying permutations of the symmetric group S_{16} on the matrix. Since order of S_{16} is 16!, therefore corresponding to one matrix (S-box) formed after applying one permutation on rows, 16! number of new S-boxes can be created by applying all the permutations on columns. Thus by this technique, we can construct $(16!)^2$ different S-boxes. We choose two particular types of permutations of the symmetric group S_{16} such that one of them is applied on the rows and the other on columns. This action increases the diffusion capability of the cipher. The permutations are as follows.

$$\begin{gathered} (1)\,(2,7,11)\,(3,6,10,13,5,8)\,(4,9,12)\,(14)\,(15)\,(16) : \text{applied on rows} \\ (1,5,10,13,15,3,7,12)\,(2,6,9,14)\,(4,8,11,16) : \text{applied on columns} \end{gathered} \quad (3)$$

Table 1: The permutation of S_{256} used in step 3.

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

The resulting S-box (see Table 3) has nonlinearity of 106.25. In step III, we further enhance its working capability.

Step III. Recently, we have noticed that certain permutations of the symmetric group S_{256} are amazingly constructive. In this step, we apply a permutations of S_{256} (see Table 1) on the data/matrix obtained after step II to construct a very strong S-box (see Table 4).

3. Security Analysis

In this section, a point by point exploration of the suggested S-box is presented. Furthermore, we have made a comparison with the famous S-boxes, such as AES S-box, Xyi S-box, Skipjack S-box, S8 AES S-box, Residue Prime S-box, APA S-box, and Gray S-box. The illustration of various analysis applied on these substitution boxes is given. It is seen that our S-box meets all the standards near the ideal status.

3.1. Nonlinearity. The key objective of the substitution box is to provide assistance in giving nonlinear change from unique data to the encoded information. The measure of nonlinearity presented by the cipher considered as the most important part in the entire process of encryption. It is defined as

$$N_f = 2^{r-1}\left(1 - 2^{-r}\max\left|W_{(f)}(z)\right|\right). \tag{4}$$

Here

$$W_{(f)}(z) = \sum_{z\epsilon F_2^r} (-1)^{f(x)\otimes+.z} \tag{5}$$

is the Walsh Spectrum. The average values of the nonlinearity of newly constructed S-box is 112. A comparison between the nonlinearity of the suggested S-box and multiple renowned substitution boxes is given in Table 5.

3.2. Bit Independence Criterion. Webster and Tavares firstly demonstrated bit independence criterion [22]. A function $h : \{0,1\}^n \longrightarrow \{0,1\}^n$ fulfils the BIC requirements if $\forall i, j, k \in \{1, 2, 3, \ldots, n\}$, the output bits j and k, where $j \neq k$, change independently by inverting the input bit i. In cryptographic systems, the BIC is a very important characteristic because by increasing independence between bits, it is very hard to decipher and predict the scheme of the system. The outcomes of nonlinearity of BIC are presented in Table 6. In order to find the independence properties a comparison of the bits, created by the eight basic functions, with each other is established. The relationship between the outcomes of change in ith input bit and the change in jth and kth output bits is identified. In the first phase the ith bit is varied from 1 to n by keeping jth and kth bits fixed. Next, the values of j and k are altered from 1 to n. Furthermore, the minimum and average values of BIC along with square deviation of the proposed S-boxes are presented in Table 7. The average and minimum values of BIC of the proposed S-box are 112. The square deviation of the newly created substitution box is 0. All these results are better than most of the well-known S-boxes and similar to AES, S_8 AES, and Gray S-boxes.

3.3. Strict Avalanche Criterion Analytically. Tavares and Webster introduced strict avalanche criterion [22]. In this criterion, the output bits are examined after changing a single input bit. In ideal condition, by changing a single input bit, half of the output bits change their shape. In [23] an effective technique is presented to check whether a complete substitution box satisfies the SAC or not. The results of SAC of the suggested S-box (see Table 8) are nearly equal to 1/2, which shows its strength.

3.4. Linear Approximation Probability. In this analysis, the imbalance of an event is examined. It is useful in finding the maximum value of an imbalance of the output in an

Table 2: 16 × 16 matrix evolved after 1st step.

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

Table 3: 16 × 16 matrix obtained after 2nd step.

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

event. Let us denote the input and output masks by T_x and T_y, respectively. Then mathematically, linear approximation probability is defined as follows.

$$LP = \max_{T_x, T_y \neq 0} \left| \frac{\#\left\{x \in I / x \bullet T_x = S(x) \bullet T_y\right\}}{2^n} - \frac{1}{2} \right| \quad (6)$$

In above expression I denotes the set of all possible values in domain and 2^n is the number of elements of the S-box.

The maximum LP value is 0.0625, which is matching with the best known S-boxes such as Gray, APA, and AES. In Table 9, a comparison of the results of this analysis, between our S-box and some famous S-boxes, is given.

3.5. Differential Uniformity. Differential uniformity is another important method of block cipher cryptanalysis. It was introduced by Biham and Shamir to break block ciphers [3]. It exploits certain events of I/O differences and represents the maximum likelihood of generating an output differential $\Delta k = K_i \oplus K_j$ when the input differential is $\Delta h = H_i \oplus H_j$. In this analysis, the XOR distribution between the inputs and outputs of substitution box is computed. Mathematically, it is defined as

$$DU = \left[\# \left\{ \frac{h \varepsilon H}{S(h)} \bigoplus S\left(h \bigoplus \Delta h\right) = \Delta k \right\} \right] \quad (7)$$

where # denotes cardinality and H is set of all inputs h [3, 24, 25]. By using the approach introduced in [3], an input/output

Table 4: Proposed S-box evolved after 3rd step.

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

Table 5: The nonlinearity test outcomes of different substitution boxes.

S boxes	0	1	2	3	4	5	6	7	Ave
Suggested S-box	112	112	112	112	112	112	112	112	112
Coset Diagram S-box [7]	108	106	108	108	108	104	106	106	106.75
Gray [8]	112	112	112	112	112	112	112	112	112
Arun [9]	108	106	104	98	102	102	98	74	99
Prime [10]	94	100	104	104	102	100	98	94	99.5
S_8 AES [11]	112	112	112	112	112	112	112	112	112
Xyi [12]	106	104	106	106	104	106	104	106	105
AES [6]	112	112	112	112	112	112	112	112	112
Skipjack [13]	104	108	108	108	108	104	104	106	106.75
Alkhaldi [14]	108	104	106	106	102	98	104	108	104
Chen [15]	100	102	103	104	106	106	106	108	104.3
Tang [16]	100	103	104	104	105	105	106	109	104.5
Khan [17]	102	108	106	102	106	106	106	98	104.25
Belazi [18]	106	106	106	104	108	102	106	104	105.25

XOR distribution matrix of size 16 × 16 is calculated for suggested S-box and is provided in Table 10. As a general S-box design guideline, the maximum differential uniformity has to be kept as low as possible to withstand differential attacks. The highest value of differential uniformity for suggested S-box is 4, which is compared with some well-known S-boxes in Table 11 to show the strength of suggested S-box.

4. Majority Logic Criterion

In majority logic criterion, statistical analyses are performed to examine the statistical strength of the S-box in image encryption application [26]. The encryption process creates a distortion in the image, these kinds of distortions determine the strength of the algorithm. Therefore, it is necessary to investigate the statistical properties through various analyses. These analyses are correlation, entropy, contrast, homogeneity, and energy. The suggested S-boxes can further be used for encryption and multimedia security. We have used two JPEG images, Pepper and Baboon, for MLC analysis. The results of these analyses in comparison with the other well-known S-boxes are depicted in Table 12. Figure 2 shows the result of image encryption with proposed S-box. The histograms of the original image and the encrypted images of Baboon and Pepper are shown in Figure 3. These results indicate that the proposed S-box is suitable for encryption applications and is adequate enough to become part of the algorithms designed for the secure transmission of information/data.

5. Conclusion

In this study, we introduce a group theoretic technique to form strong S-boxes. The cyclic group C_{255} instead of a Galois

Table 6: BIC nonlinearity for the suggested S-box.

Rows/Columns	0	1	2	3	4	5	6	7
0	-	112	112	112	112	112	112	112
1	112	-	112	112	112	112	112	112
2	112	112	-	112	112	112	112	112
3	112	112	112	-	112	112	112	112
4	112	112	112	112	-	112	112	112
5	112	112	112	112	112	-	112	112
6	112	112	112	112	112	112	-	112
7	112	112	112	112	112	112	112	-

Table 7: BIC results of different S-boxes.

S-boxes	Minimum value	Average	Square deviation
Suggested S-box	112	112	0
Gray	112	112	0
Arun	92	103	3.5225
Prime	94	101.71	3.53
S_8 AES	112	112	0
Xyi	98	103.78	2.743
AES	112	112	0
Skipjack	102	104.14	1.767

Table 8: Values of SAC for the suggested S-box.

Rows/Columns	0	1	2	3	4	5	6	7
0	0.4844	0.4688	0.4844	0.5469	0.4688	0.5625	0.5469	0.5313
1	0.4531	0.5313	0.5156	0.5469	0.4688	0.4688	0.4844	0.5469
2	0.5000	0.4688	0.4609	0.4688	0.5156	0.4531	0.5469	0.5625
3	0.5313	0.5234	0.5313	0.5156	0.4531	0.4688	0.5234	0.4375
4	0.5625	0.4844	0.4688	0.5156	0.5469	0.5469	0.5625	0.4844
5	0.5000	0.4844	0.5156	0.5625	0.4844	0.5469	0.4844	0.5156
6	0.4844	0.5156	0.5000	0.4844	0.4844	0.4844	0.4688	0.5625
7	0.5469	0.5625	0.4531	0.4688	0.5156	0.4844	0.5313	0.4844

Table 9: Linear approximation probability analyses of different S-boxes.

S-boxes	Suggested S-box	AES	Skipjack	Prime	Gray	Arun	S_8 AES	Xyi
Max value	144	144	156	162	144	164	144	168
Max LP	0.062	0.062	0.109	0.132	0.062	0.2109	0.062	0.156

field is used to destroy the initial sequence $0, 1, 2, \ldots, 255$. The construction of S-box involves three simple steps:

(i) First present the elements of $C_{255} \cup \{0\} = \{T(1), T^2(1), T^3(1), \ldots, T^{254}(1), 1, 0\}$ in 16×16 matrix.

(ii) Next, apply two permutations of S_{16} on rows and column of the matrix. It will significantly improve the performance of the S-box.

(iii) In the last step, a permutation of S_{256} is applied on the matrix (obtained in step (ii)) to form proposed S-box.

The results acquired from different analyses show that the performance of our S-box against various algebraic attacks is much better than most of well-known S-boxes and similar to AES, S_8 AES, and Gray S-boxes. Therefore, our S-box meets all the requirements and is considered as a strong S-box for the secure communication.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Table 10: Differential uniformity of proposed S-box.

4	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	- - - - -

Table 11: Maximum differential uniformity of various S-boxes.

S-boxes	Suggested S-box	AES	Gray	Skipjack	Chen	Khan	S_8 AES	Tang	Xyi
Max DU	4	4	4	12	12	16	4	10	12

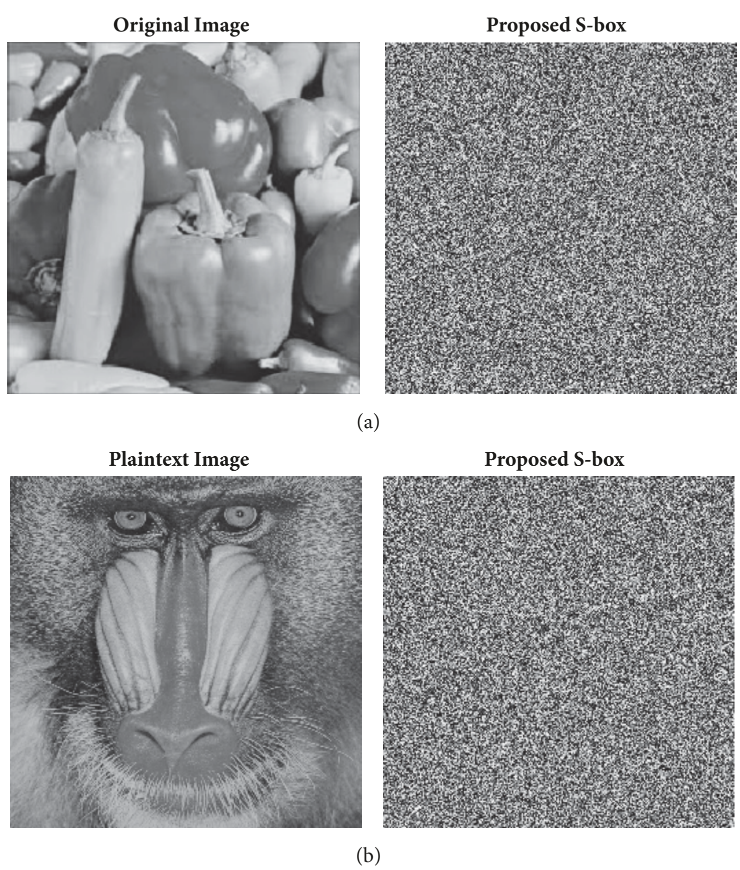

Figure 2: Original image and the encrypted images using two rounds of encryption: (a) Pepper and (b) Baboon.

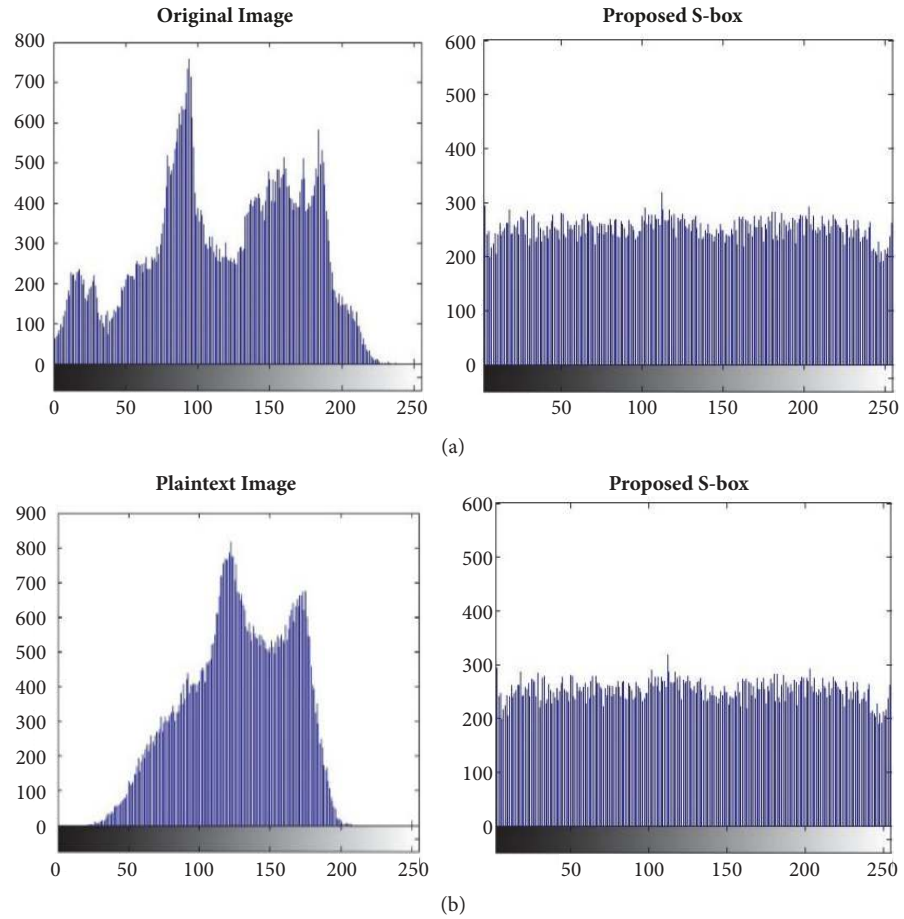

Figure 3: Histogram of the original image and the encrypted images: (a) Pepper and (b) Baboon.

Table 12: Comparison of Majority logic criterion for S-box over various S-boxes.

S-boxes	Correlation	Entropy	Contrast	Homogeneity	Energy
Pepper Image					
Plain Text	0.9383	7.5909	0.2760	0.9024	0.1288
Suggested S-box	**-0.0134**	**7.9842**	**8.6969**	**0.4045**	**0.0174**
Atta [19]	**−0.0043**	**7.9823**	**8.6727**	**0.4076**	**0.0173**
Skipjack	**0.1205**	**7.7561**	**7.7058**	**0.4708**	**0.0239**
Khan [20]	0.0103	7.9562	8.3129	0.4219	0.0180
Belazi	−0.0112	7.9233	8.1423	0.4648	0.0286
Baboon Image					
Plain Text	0.6782	7.1273	0.7179	0.7669	0.1025
Suggested S-box	**-0.0060**	**7.9820**	**8.6488**	**0.4062**	**0.0174**
AES	0.0554	7.2531	7.5509	0.4662	0.0202
Prime	0.0855	6.9311	7.6236	0.4640	0.0202
Xyi	0.0417	7.2531	8.3108	0.4533	0.0196
Skipjack	0.1025	7.2531	7.7058	0.4689	0.0193
Khan [14]	−0.0512	7.9612	8.1213	0.4011	0.0210
Belazi	0.0119 0	7.9252	8.0391	0.4428	.02219

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research project was supported by a grant from the Research Center of the Center for Female Scientific and Medical Colleges, Deanship of Scientific Research, King Saud University.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] L. R. Knudsen and M. J. B. Robshaw, *The Block Cipher Companion*, Springer, Berlin, 2011.

[3] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[4] T. W. Cusick and P. Stanica, *Cryptographic Boolean functions and applications*, Academic Press, San Diego, CA, USA, 2009.

[5] T. Helleseth, "Linear cryptanalysis method for des cipher," in *Advances in Cryptology—EUROCRYPT*, vol. 765 of *Lecture Notes in Computer Science*, pp. 386–397, Springer, Berlin, Germany, 1993.

[6] J. Daemen and V. Rijmen, *The design of Rijndael-AES: the advanced encryption standard*, Springer, Berlin, 2002.

[7] 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," *Security and Communication Networks*, vol. 2017, 2017.

[8] M. T. Tran, D. K. Bui, and A. D. Doung, "Gray S-box for advanced encryption standard," in *Proceedings of the International Conference on Computer Intel Security*, vol. 1, pp. 253–258, 2008.

[9] A. Gautam, G. S. Gaba, R. Miglani, and R. Pasricha, "Application of Chaotic Functions for Construction of Strong Substitution Boxes," *Indian Journal of Science and Technology*, vol. 8, no. 28, pp. 1–5, 2015.

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

[11] I. Hussain, T. Shah, and H. Mahmood, "A new algorithm to construct secure keys for AES," *International Journal of Contemporary Mathematical Sciences*, vol. 5, no. 25-28, pp. 1263–1270, 2010.

[12] X. Y. Shi, Hu. Xiao, X. C. You, and K. Y. Lam, "A method for obtaining cryptographically strong 8*8 S-boxes," in *Proceedings of the International Conference on Advanced Information Networking and Applications*, vol. 2, pp. 14–20, 2002.

[13] *Skipjack and Kea: Algorithm Specifications Version*, 1998, http://csrc.nist.gov/CryptoToolkit/.

[14] A. H. Alkhaldi, I. Hussain, and M. A. Gondal, "A novel design for the construction of safe S-boxes based on TDERC sequence," *Alexandria Engineering Journal*, vol. 54, pp. 65–69, 2015.

[15] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps," *Chaos, Solitons & Fractals*, vol. 31, no. 3, pp. 571–579, 2007.

[16] G. Tang, X. Liao, and Y. Chen, "A novel method for designing S-boxes based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 23, no. 2, pp. 413–419, 2005.

[17] M. Khan, T. Shah, and M. A. Gondal, "An efficient technique for the construction of substitution box with chaotic partial differential equation," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1795–1801, 2013.

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

[19] 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 Dynamics*, vol. 88, no. 4, pp. 2757–2769, 2017.

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

[21] G. V. Bard, *Algebraic Cryptanalysis*, Springer, Berlin, 2009.

[22] A. Webster and S. Tavares, "On the design of S-boxes," in *Advancesin Cryptology: Proc. of Crypto'85 Lecture Notes in Computer Science*, pp. 523–534, 1986.

[23] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *IEE Proceedings Part E Computers and Digital Techniques*, vol. 135, no. 6, pp. 325–335, 1988.

[24] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Computing and Applications*, pp. 1–10.

[25] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-Boxes," *Entropy*, vol. 20, no. 7, p. 525, 2018.

[26] 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, 2012.