IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 29, 2020, accepted August 10, 2020, date of publication August 13, 2020, date of current version August 26, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3016401

A Novel Modular Approach Based Substitution-Box Design for Image Encryption

AMJAD HUSSAIN ZAHID[1], EESA AL-SOLAMI[2], AND MUSHEER AHMAD[3]

[1]Department of Informatics and Systems, University of Management and Technology, Lahore 54700, Pakistan
[2]Department of Information Security, University of Jeddah, Jeddah 21493, Saudi Arabia
[3]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India

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

ABSTRACT In modern-day block ciphers, the role of substitution-boxes is to transform the plaintext data nonlinearly to generate ciphertext data with sufficient confusion. It has been well-confirmed that the robustness and security of such block ciphers heavily based on the cryptographic strength of the underlying substitution-boxes. Reason being, they are the only components that are held responsible to bring required nonlinearity and complexity into the security system which can frustrate the attackers. Accordingly, a number of different concepts have been explored to construct strong S-boxes. To move forward with the same aim, a novel simple modular approach, the very first time, is investigated to construct nonlinear S-box in this paper. The proposed new modular approach consists of three operations such as new transformation, modular inverses, and permutation. A number of highly nonlinear S-boxes can be easily constructed with slight changes in the novel transformation parameters. An example S-box is presented whose critical performance assessment against some benchmarking criterions such as high nonlinearity, absence of fixed points, fulfillment of SAC and BIC properties, low differential uniformity and linear approximation probability and comparison with recent S-boxes demonstrate its upright cryptographic potentiality. In addition, an image encryption algorithm is also proposed wherein the generated S-box is applied to perform the pixels shuffling and substitution for strong statistical and differential encryption performance.

INDEX TERMS Substitution-box, modular approach, linear transformation, image encryption, block cipher.

I. INTRODUCTION

Data and information communication has become very important ingredient of today's technological life and considered as significant assets of an individual or organization. If the confidentiality of information is compromised, then the information can be used for harmful purposes. Current innovations in information technology and their prolific applications in our life have caused in a gigantic growth in the size of the data being transmitted online. The private information being very sensitive assets require protection from attackers. Therefore, prior to its transmission, data demand its protection and needs methods for its transformation into a meaningless form for the invaders. Cryptographic algorithms are the mathematical methods and techniques that assist in the protection of data [1]. Stream ciphers transform the data in a bit-by-bit or byte-by-byte manner. Whereas, the block ciphers transform data in chunks which comprise large number of bits or bytes at a time. In modern symmetric encryption, block ciphers are considered as one of the most effective tools for data protection [2]. Data Encryption Standard (DES), Blowfish, Advanced Encryption Standard (AES), RC5, etc. are examples of contemporary block ciphers. Precise implementations of block ciphers are easy and are more general in nature than the stream ciphers [3]. One category of prevalent block ciphers is known as the SP network-based block ciphers. These block ciphers use two major operations of substitution and permutation for the transformation of data into a perplexing form. A substitution operation substitutes a byte/block with another byte/block using a substitution table known as a substitution box or S-box [4], [5]. On the other hand, a permutation process shuffles the input bits or bytes in some linear fashion.

A substitution-box is a pivotal constituent of modern-day block ciphers that helps in the generation of a muddled ciphertext for the specified plaintext. Through the incorporation of S-box, a nonlinear mapping among the input and output data is established to create confusion [6]. The more confusion

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

an S-box can create in the output data, the more secure a block cipher is. As a result, the provision of security by a block cipher employing one or more S-boxes directly depends on how much stronger S-boxes are. Block ciphers consist of many components in addition to one or more S-boxes. Contrary to other components, an S-box is the alone nonlinear component of block ciphers that supports the enhancement of data protection [7], [8].

Generally, a block cipher uses either a static S-box or one or more dynamic S-boxes. A static S-box is fixed for every incoming data and secret key which is used repeatedly in the block cipher. A block cipher based on a static S-box employs that S-box in all its rounds. A static S-box allows an attacker to inspect its characteristics, discover its fragilities, and eventually find the chance of getting plaintext from the respective ciphertext [9], [10]. As an example, static S-boxes employed in Data Encryption Standard (DES) were an easy target for the attackers. Consequently, to overcome the weaknesses due to static S-boxes, many cryptographers have explored innovative techniques to design dynamic S-boxes. Dynamic S-boxes are generated using cipher key and provide a way to augment the cryptographic power of a block cipher. Construction and usage of the key-dependent and dynamic S-boxes in a cipher enhance its cryptographic power. Blowfish cipher employs such dynamic S-boxes in its working [11].

The researchers, scholars, and academicians have explored and investigated various concepts to generate cryptographic strong S-boxes. They evaluated the strength using some typical criteria, such as nonlinearity, absence of fixed points, bit independence criterion (BIC), linear and differential probabilities, strict avalanche criterion (SAC), etc., that must an S-box satisfy to fight against various type of attacks. If an S-box possesses more of these characteristics, it provides more security to the block cipher. In particular, the nonlinearity has been considered as one of the significant measures to evaluate the strength of a given S-box. Any substitution box exhibiting a larger value of nonlinearity ensures more fight against the linear cryptanalytic attacks [12]. In particular, Du *et al.* [12] and Patil *et al.* [13] projected and investigated dynamic S-boxes based on Feistel structure. The subsequent S-boxes exhibited decent robustness against the attacks. In [14]–[16], different techniques to yield a huge number of dynamic and key-dependent S-boxes have been investigated and evaluated the quality of each resultant S-box. Performance results disclosed that the resultant S-boxes show considerate security strength. The authors in [17]–[21] suggested various enhancements to the sanctuary offered by AES while improving the AES S-box. Moreover, many investigators [22]–[29] have projected novel S-boxes based on chaos and demonstrated that the chaos-based S-boxes are adequately resilient to different attacks. Others have used the knowledge areas to design S-boxes like linear fractional transformation [30]–[32], DNA computing [5], [33], [34], elliptic curve [35], [36], graph theory [37], [38], optimization techniques [39]–[43], cellular automata [44], etc.

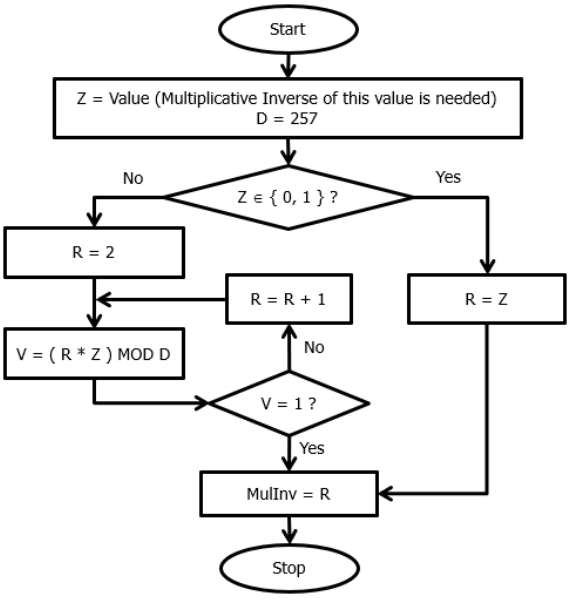

FIGURE 1. Multiplicative inverse computation process.

Dynamic and key-dependent S-box construction techniques available in the literature are either complicated or consume considerable time to produce a strong S-box. Hence, there is a need for a method that is quite simple, efficient, and capable of generating dynamic strong S-boxes. In this paper, a simple scheme that assists in generating dynamic S-boxes is proposed. The novel scheme employs the idea of new transformation, multiplicative inverses, and permutation operations for generating the final S-box. The core contributions of this paper are as follows:

- A novel and simple modular approach is explored to construct nonlinear S-boxes. A large number of robust S-boxes can be created straightforwardly with minute variations in the new transformation parameters.
- A novel and dynamic permutation operation is applied to the values of S-box to create more confusion. The dynamic nature of this operation depends upon the order of the values in the S-box and hence adds forte to the security of the ciphertext.
- Performance comparison analysis is carried out which validates the remarkable recital effort of the S-box with respect to several current S-boxes.
- A new image encryption algorithm using generated S-box based pixels permutation and substitution is also proposed which demonstrates its capability and landscape for securing sensitive data.

The portion which is left to discuss is organized as follows. Section II provides description of the proposed modular-based approach for the generation of S-boxes. Security analysis of an example S-box is discussed and compared in section III. A new image encryption method based on generated S-box and encryption performance assessment and comparison is done in Section IV. The conclusions of the research study are made in Section V.

II. PROPOSED MODULAR APPROACH FOR S-BOX DESIGN

The modern symmetric ciphers designed these days often use S-boxes that create more confusion for the invaders. S-boxes help in the provision of data security by creating jumbled ciphertext. An S-box design establishes a nonlinear relation between the input and output data in such a way that an attacker is unable to deduce input data from the output data. Research investigators have broadly explored such nonlinear mappings to produce strong S-boxes. The process of construction of an S-box should be simple and efficient. The construction process of most of the S-boxes presented in the literature is very time consuming and complicated. As an example, S-boxes generated with the help of linear fractional transformation (LFT) depend heavily on the use of the Galois field. LFT also known as the Mobius transformation is one of the many mappings that have been comprehensively applied for the creation of S-boxes [30]–[32]. However, the procedure of S-box construction using LFT is computationally inefficient and complicated too. Here, we outspread the awareness of LFT and construct a novel transformation to produce an S-box with good cryptographic features through a simple modular approach. The overall process of dynamic S-box construction involves three simple steps in sequence:

1. $L(z)$: novel transformation of $z \in N$
2. $MI(L(z))$: Multiplicative inverse of value $L(z)$
3. Action of permutation process

Each of these steps involved in the creation of final S-box candidate are described in what follows.

A. NOVEL TRANSFORMATION

The novel transformation employed in the production of an S-box having size $n \times n$ is a function expressed mathematically as:

$$L(z) = [A * z + B] \, MOD \left(2^n + 1\right) \quad z \in N \tag{1}$$

where, $N = \{0, 1, 2, \ldots, 2^n - 1\}$, $O = \{1, 3, 5, \ldots, 2^n - 1\}$, $A \in O$, and $B \in N$.

B. MULTIPLICATIVE INVERSES

The S-box design method which uses linear fractional transformation (LFT) as the core of the S-box construction process needs to find the multiplicative inverse for each byte of the input data. Finding the multiplicative inverse of a value using Galois field is considerably complicated process as indicated in [45], [46]. Our technique of finding the multiplicative inverse using modular operator is very simple, straight forward, and above all efficient as compared to the multiplicative inverse calculation process used in Galois field domain.

This steps aims to compute the multiplicative inverse of each value produced in Step A using the following function given in Eq. (2). The detail of determining the inverse for any value $z \in \{0, 1, \ldots\ldots, 255\}$ is presented through Algotihm and flowchart shown in Figure 1.

$$MI(L(z)) = [L(z)] \, MOD \left(2^n + 1\right) \quad z \in N \tag{2}$$

where, $N = \{0, 1, 2, \ldots, 2^n - 1\}$. It may be noted that $MI(0) = 0$ and $MI(1) = 1$. Also, $MI(256)$ is not used in this process as described in Figure 1. Steps A and B of the proposed approach as described above generate an initial S-box which is also demonstrated in Figure 2.

C. PERMUTATION PROCESS

Initial S-box values are permuted using permutation process described by the flowchart shown in Figure 3. Permutation process is dynamic and dependent on the order of values of initial S-box. For an 8×8 S-box constructed through the proposed approach, total number of permutations is equal to $2^{16}! = 20{,}922{,}789{,}888{,}000$ which is quite a large number. It makes the job of invader complex and near to impossible. The permutation step generates the final S-box.

To demonstrate the process of S-box generation through Eq. (1)-(2) and Figures 2 and 3, let us consider an explicit

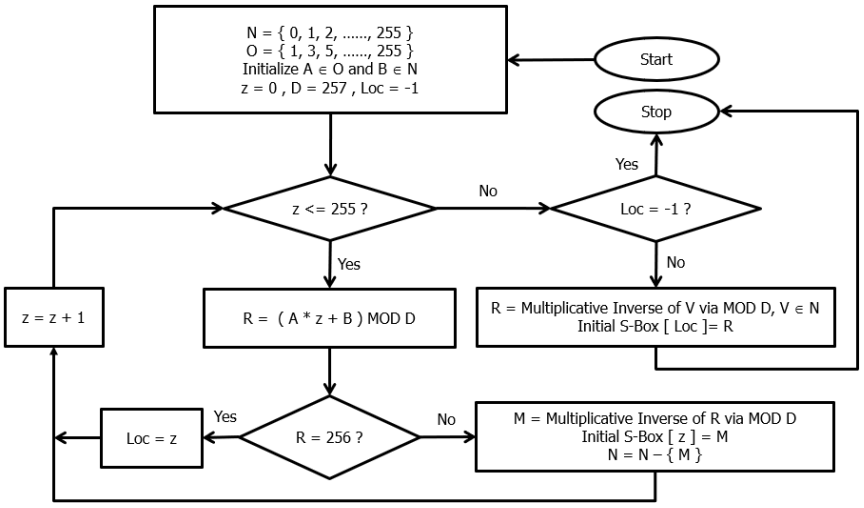

FIGURE 2. Initial S-box construction process.

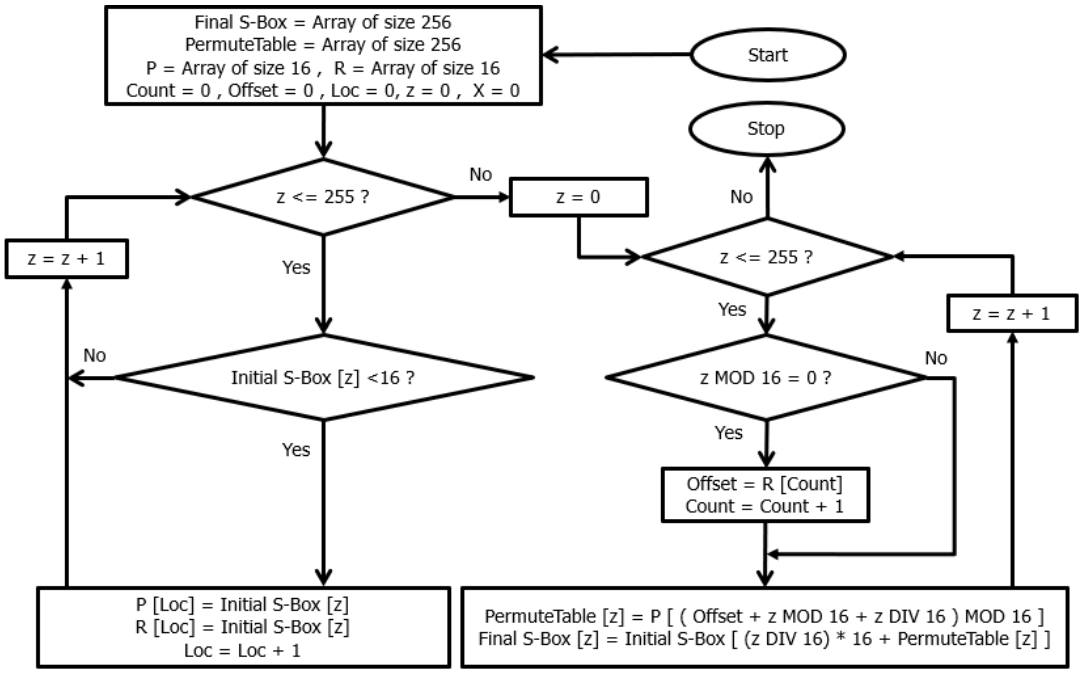

FIGURE 3. Proposed final S-box construction through permutation process.

Algorithm Multiplicative Inverse Calculation

Take input arguments as:
  Z // Multiplicative inverse of this value is needed
    // Z ∈ {0, 1, ... , 255}
  D // *This is the divisor and helps in finding the*
    // *multiplicative inverse of Z*
$D = 257$ // for 8 × 8 S-box
if Z ∈ {0, 1}
  return Z
else
  $R = 1$ // Auxiliary variable
  do
    $R = R + 1$
    $V = (R * Z)\ mod\ D$
  while (V != 1)
  return R
endif

type of transformation as given in (3) and (4). We have, $N = \{0, 1, 2, \ldots, 2^n - 1\} = \{0, 1, 2, \ldots, 2^8 - 1\}$ and $O = \{1, 3, 5, \ldots, 2^n - 1\} = \{1, 3, 5, \ldots, 2^8 - 1\}$ for $n = 8$. A specimen S-box of size 8 × 8 is spawned using novel linear transformation for specified values of $A = 161$ and $B = 138$, where $L: N \rightarrow N$, is as follows:

$$L(z) = \begin{Bmatrix} [161 * z + 138]\, MOD\, (257) & z \in N - \{229\} \\ 234 & z = 229 \end{Bmatrix} \quad (3)$$

$$MI(L(z)) = [L(z)]\, MOD(257) \quad z \in N \quad (4)$$

For the sake of demonstration and computation purposes, we have chosen $A = 161$ and $B = 138$. Function, $L(z)$, given in Eq. (3) creates values of $N - \{234\}$ when $z \in N - \{229\}$. When $z = 229$, $L(z)$ produces value $256 \notin N$. For preserving the bijectiveness of function $L(z)$, we express $L(z)$ for $z = 229$ explicitly in Eq. (3). The design has the flexibility of using any value for both parameters of novel transformation $L(z)$ that is A and B. The specific transformation given in (3) and (4) spawn the values of our initial 8 × 8 S-box, which are shown as a 16 × 16 matrix in Table 1. Using permutation process shown in Figure 3, the permutation table is generated which is operated to permute the values of initial S-box in a row by row fashion. Table 2 presents the permutation table generated for initial S-box given in Table 1. Through the permutation given in Table 2, the final S-box shown in Table 3 is obtained.

III. SECURITY ANALYSIS OF PROPOSED S-BOX

This section critically inspects the strength of generated S-box given in Table 3 against standard criteria that is used to quantify the cryptographic features of an S-box. An S-box is expected to satisfy the following criterions for good cryptographic strength [22]–[43], [48].

- Bijectiveness.
- High nonlinearity.
- Absence of any fixed points.
- Strict avalanche criterion.
- Output bits independence criterion.
- Low differential uniformity
- Low linear approximation probability.

TABLE 1. Initial S-box before permutation process.

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

TABLE 2. Permutation table.

8	2	9	13	7	12	11	4	1	5	14	10	0	6	3	15
10	0	6	3	15	8	2	9	13	7	12	11	4	1	5	14
2	9	13	7	12	11	4	1	5	14	10	0	6	3	15	8
2	9	13	7	12	11	4	1	5	14	10	0	6	3	15	8
10	0	6	3	15	8	2	9	13	7	12	11	4	1	5	14
5	14	10	0	6	3	15	8	2	9	13	7	12	11	4	1
3	15	8	2	9	13	7	12	11	4	1	5	14	10	0	6
1	5	14	10	0	6	3	15	8	2	9	13	7	12	11	4
12	11	4	1	5	14	10	0	6	3	15	8	2	9	13	7
0	6	3	15	8	2	9	13	7	12	11	4	1	5	14	10
13	7	12	11	4	1	5	14	10	0	6	3	15	8	2	9
2	9	13	7	12	11	4	1	5	14	10	0	6	3	15	8
3	15	8	2	9	13	7	12	11	4	1	5	14	10	0	6
1	5	14	10	0	6	3	15	8	2	9	13	7	12	11	4
13	7	12	11	4	1	5	14	10	0	6	3	15	8	2	9
10	0	6	3	15	8	2	9	13	7	12	11	4	1	5	14

We opted recently published S-box studies to make the performance comparison of our S-box.

A. BIJECTIVENESS

Bijectiveness property of an 8 × 8 S-box demands that each specific 8-bit input should map to only one unique 8-bit output. Means, there should exist a one-to-one mapping in the generated S-box structure. This results in all 256 distinct output values in the S-box table in the range [0, 255]. The proposed S-box in Table 3 fulfills this criterion as the S-box has all possible distinct output values $\{0, \ldots, 255\}$. Also, each coordinate Boolean function has equal number of 0's and 1's which is 128 [8], [11].

B. NONLINEARITY (NL)

An S-box provides a mapping between input and output bits. If generated S-box maps input and output in a linear fashion, the cryptographic strength of that S-box is very less. An S-box deemed strong if it is able to transform the inputs to outputs in highly nonlinear way. Such an S-box facilitates in protecting the plaintext data against linear cryptanalytic attacks. The nonlinearity of an n-bit Boolean function h is calculated as [48].

$$NL\,(h) = 128 - \frac{1}{2}(T_{max}\,(h)) \tag{5}$$

where, $T_{max}(h)$ represents Walsh-Hadamard Transform for a given n-bit Boolean function h. The coordinate Boolean

TABLE 3. Final S-box after permutation operation.

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

TABLE 4. Nonlinearities of proposed S-box.

Boolean Function	BF_1	BF_2	BF_3	BF_4	BF_5	BF_6	BF_7	BF_8
Nonlinearity(BF)	106	108	104	110	106	110	108	108

functions of our S-box and their respective nonlinearities are presented in Table 4. The nonlinearity test results indicates the minimum NL = 104, maximum NL = 110, and average NL = 107.5 is achieved. The nonlinearity strength of our proposed S-box is also compared in Table 5 with recent S-boxes studies investigated in [49]–[62]. The comparison table makes evident the better nonlinearity performance of our S-box over many recent S-boxes.

C. FIXED POINTS (FPs)

In cryptosystems involving the S-boxes, the existence of any fixed points (i.e. $S(k) = k - 1$) may be a weakness that can be exploited by the attacker to gain the knowledge of secret data. Accordingly, care has been taken by the AES block cipher designer to eliminate the fixed points by employing the concept of additive constant in AES S-box. Therefore, it is to be taken care that the S-boxes shouldn't have any fixed points [49]. We checked this test for our proposed S-box and found that there is not a single fixed point and this analysis is further compared with some other recent S-boxes in Table 5. The comparison states that there exist a number of recent S-box studies where the respective S-boxes are not free from existence of fixed points.

TABLE 5. Nonlinearity performance comparison of proposed S-box with other recent S-boxes.

S-box	Min-NL	Max-NL	Average-NL	FPs
Proposed	104	110	107.5	0
Ref. [49]	102	108	105	1
Ref. [50]	98	106	103.5	0
Ref. [51]	100	110	105.5	3
Ref. [52]	106	108	106.5	0
Ref. [53]	104	110	106.25	1
Ref. [54]	96	104	100.5	2
Ref. [55]	106	108	106.5	0
Ref. [56]	106	112	109.5	0
Ref. [57]	104	110	106.87	2
Ref. [58]	104	108	106.5	1
Ref. [59]	98	106	102.5	1
Ref. [60]	102	108	105.25	2
Ref. [61]	104	110	106	1
Ref. [62]	106	108	107.25	1

D. STRICT AVALANCHE CRITERION (SAC)

Webster *et al.* presented this criterion as the vital characteristic of any strong S-box [63]. This criterion requires that if an input has a single bit flip, it should flip $n/2$ bits out

of n output bits. Consequently, a SAC score ≈ 0.5 is considered acceptable. The dependency matrix for SAC criteria is evaluated which is shown in Table 6. The SAC value of our S-box comes out as 0.498 which is fairly close to 0.5. Hence, it can deduce that the S-box presented in Table 3 gratifies the SAC requirement very well. The SAC performance is consistent with the recent S-boxes as evident from the SAC comparison made in Table 8.

TABLE 6. SAC dependency matrix for proposed S-box.

0.5625	0.4843	0.4531	0.5468	0.5156	0.5625	0.5000	0.5000
0.4531	0.5625	0.4843	0.5468	0.5937	0.5000	0.5468	0.5156
0.5156	0.5468	0.5468	0.4843	0.5156	0.5000	0.4687	0.5312
0.5312	0.4687	0.4375	0.4843	0.5000	0.4531	0.4062	0.4843
0.5156	0.5312	0.4843	0.5156	0.4375	0.4687	0.5000	0.4375
0.4687	0.5000	0.5000	0.5625	0.4375	0.4687	0.5312	0.5000
0.4843	0.5468	0.4687	0.4375	0.5312	0.5000	0.4843	0.5312
0.5156	0.4531	0.3906	0.5312	0.4375	0.5625	0.4843	0.4531

E. BIT INDEPENDENCE CRITERION (BIC)

This criterion was presented by Webster *et al.* as an important property for any strong S-box. This criterion requires that any coordinate Boolean function must be mutually independent and possesses the features of high nonlinearity [64]. The BIC table for the nonlinearity of each of the Boolean functions $h_i \oplus h_j$ $(i \neq j)$ is listed in Table 7. The BIC performance with respect to nonlinearity is averaged at 103.5. This value is an indication that our S-box satisfies the bit independence criterion quite well. The comparison of BIC performance is made in Table 8.

TABLE 7. BIC table for nonlinearity of Boolean functions $h_i \oplus h_j$ $(i \neq j)$ w.r.t. proposed S-box.

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

F. DIFFERENTIAL UNIFORMITY (DU)

Differential cryptanalysis is a valuable instrument that is used to obtain the input differential from the output differential. An attempt is made to obtain modifications in the input data and variations in the respective output data. Combining both variations help the attackers to know the whole or parts of the plaintext data or cipher key [65]. Efforts are made to have the difference of these two values to be very minimal. For this purpose, the differential uniformity of an S-box is usually assessed. To resist a differential cryptanalytic attempt, a less score of differential uniformity (DU) is preferred. To calculate differential uniformity, equation (6) is used [66].

$$DU = \max_{\Delta m \neq 0, \Delta n} (\#\{m \in \mathrm{G} | S(m) \oplus S(m \oplus \Delta m) = \Delta n\}) \quad (6)$$

where, $G = \{0, 1, \ldots, 2^n - 1\}$. The differential distribution table (DDT) for proposed S-box shown in Table 9 is obtained. The differential uniformity of our S-box is evaluated to 10 only. This small value of DU shows that our S-box can defy the differential cryptanalytic efforts very well. The proposed S-box score is also compared with DU of recent S-boxes in Table 10 which shows better robustness to differential cryptanalysis than S-box studies in [50], [51], [61], [62] and comparable to [52]–[55], [58]–[60].

TABLE 8. SAC and BIC performance comparison.

S-box	SAC	BIC-NL
Proposed	0.4980	103.5
Ref. [49]	0.5029	102.9
Ref. [50]	0.4958	103.5
Ref. [51]	0.5	103.78
Ref. [52]	0.5009	104.07
Ref. [53]	0.5032	103.9
Ref. [54]	0.4973	102.78
Ref. [55]	0.4990	103.57
Ref. [56]	0.5068	106.86
Ref. [57]	0.509	106.1
Ref. [58]	0.4990	103.21
Ref. [59]	0.5037	103.92
Ref. [60]	0.5037	102.6
Ref. [61]	0.4978	103.92
Ref. [62]	0.5034	105.29

G. LINEAR APPROXIMATION PROBABILITY (LAP)

Block cipher designers try to muddle bits of input data as much as possible. A strong S-box assist in accomplishing this task as it provides a nonlinear mapping between plaintext and ciphertext. Linear cryptanalysis is an effort by attackers to expose the feeble relationship between plaintext and ciphertext. The strength of this mapping is measured by linear approximation probability (LAP) given in Eq. (7) [67].

$$LAP = \max_{m_x, m_y \neq 0} \frac{1}{2} \left| \frac{\#\{x \in G | x \cdot m_x = S(x) \cdot m_y\}}{2^{n-1}} - 1 \right| \quad (7)$$

where, $G = \{0, 1, \ldots, 2^n - 1\}$. The lower value of LAP for an S-box is the target to defy linear cryptanalytic effort.

TABLE 9. Differential distribution table for proposed S-box.

8	8	8	6	6	6	8	10	6	8	6	6	6	6	10	6
10	8	6	6	6	8	6	6	6	6	10	6	6	6	6	6
6	6	6	8	6	6	6	8	6	8	6	8	6	8	8	6
6	6	10	6	6	8	6	6	6	6	6	6	6	6	6	8
8	6	10	6	6	6	6	8	8	8	6	6	6	6	6	8
6	6	6	8	8	8	6	8	6	8	6	6	8	6	6	6
8	6	8	6	8	6	6	6	10	8	8	6	6	6	6	6
6	6	8	8	6	8	8	8	8	6	8	8	6	4	8	6
6	8	8	6	6	6	8	6	8	10	6	6	8	6	8	6
6	8	6	8	6	6	8	8	6	6	8	10	8	6	6	6
6	6	6	6	10	8	6	6	8	6	8	6	8	6	6	8
6	6	6	6	6	8	6	6	6	8	8	6	6	6	6	6
6	6	8	6	6	6	6	6	6	8	8	6	6	8	6	6
8	6	6	8	8	6	6	6	8	6	6	6	6	8	10	10
6	6	8	8	8	6	10	6	6	6	6	6	6	8	8	8
6	8	4	6	8	8	8	8	8	6	8	6	8	6	8	0

The LAP score of our S-box given in Table 3 is 0.140625 which is quite low. So, our S-box has sufficient potentiality to defy linear cryptanalysis. The LAP scores of some recent S-boxes are compared in Table 10 to demonstrate that our S-box has improved robustness against many recent S-boxes as well.

The performance assessment and the recital judgement make it clear that our S-box meets the required security standards and henceforth owns healthier cryptographic strength against different attacks compared to many recent S-boxes.

IV. IMAGE ENCRYPTION METHOD USING GENERATED S-BOX

In this section, we present our proposed method for encrypting the multimedia gray-scale images using the proposed S-box given in Table 3. We employed our S-box to execute the permutation-substitution operations purely based on the S-box. The following image encryption method exemplifies one specific use of proposed S-box. The steps of proposed encryption method are as follows:

1. Generate the S-box using the proposed modular approach discussed.
2. Read the input plain-image PP, S-box S and $C(0)$
3. Find row and column of PP as M and N, respectively.
4. Scale the permutation sequence of S to the size of M, take it as $S1$. Similarly, scale the permutation sequence of S to the size of N, take it as $S2$.
5. Perform the permutation of pixels of image PP using the sequences S1 and S2 as follows:
   for $k = 1$ to M
   $PS(S1(k),:) = PP(k,:)$
   end
   $PP = PS$
   for $k = 1$ to N
   $PS(:, S2(k)) = PP(:, k)$
   end
6. Reshape permuted image PS to 1-D array.
7. Repeat the following operations for all pixels of permuted image PS starting from first pixel to last pixel ($t = 1 \sim \mathrm{M} \times \mathrm{N}$).
   $i = \{\mathrm{C0}\} mod(16)$
   $j = floor(\mathrm{C0}/16)$
   $K_1 = S(i, j)$
   $m = \{i \times \mathrm{C0} + K_1\} mod(16)$
   $n = \{j \times K_1\} mod(16)$
   $K_2 = S(m, n)$;
   $\mathrm{C}(t) = \{PS(t) + K_2\} mod(256) \oplus \{K_1 \oplus \mathrm{C0}\}$
   $q = \{K_1 + K_2\} mod(251)$
   $C(t) = circshift(C(\mathrm{t}), mod(q,8))$
   $\mathrm{C0} = \mathrm{C}(t)$
   where, t is the pixel number.
8. Reshape encrypted image C to 2-D form.

The suggested image encryption method is also described through the flowchart shown in Figure 4. The decryption method is very similar to the above mentioned steps of encryption but should be followed in reverse order.

In the next subsections, we evaluate the encryption performance of our proposed algorithm and S-box as well for gray-scale images, but the same algorithm can also be extended for color images as well by decomposing the different color channels which can be encrypted by following the steps mentioned. We performed simulation and analyses on the benchmark images (such as *Lena*, *Baboon, Cameraman, Peppers, Tree, Barbara*) shown in Figure 5 which are taken from USC-SIPI image dataset selectively so that we can make a fair comparison of encryption strength with recent S-box based image encryption methods. MATLAB is used for experimentation and simulation on Intel core i7 CPU @ 2.2GHz with 4GB RAM and Windows 8. The encrypted images obtained using our encryption procedure are depicted in Figure 6. It is quite clear from the encrypted images that

TABLE 10. Differential and linear cryptanalysis performance score and comparison of S-boxes.

S-box	Proposed	[49]	[50]	[51]	[52]	[53]	[54]	[55]	[56]	[57]	[58]	[59]	[60]	[61]	[62]
DU	10	12	14	12	10	10	10	10	8	8	10	10	10	12	12
LAP	0.14063	0.1484	0.1328	0.125	0.1328	0.1328	0.15625	0.125	0.1328	0.113	0.14063	0.125	0.1328	0.1563	0.1328

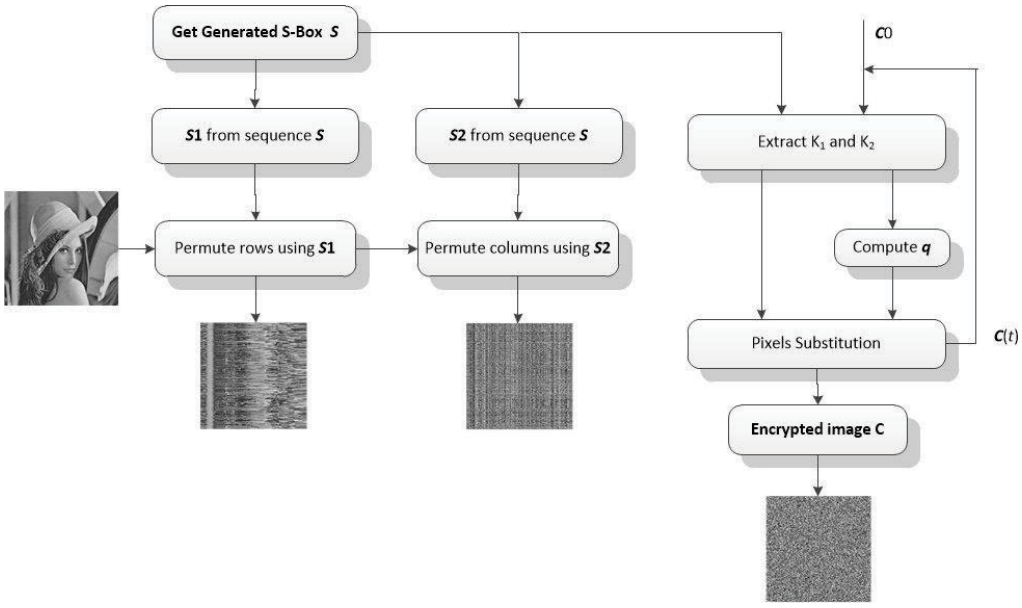

FIGURE 4. Schematic diagram for image encryption method based on generated S-box.

FIGURE 5. Test plain-images (a) Lena, (b) Baboon, (c) Cameraman, (d) Tree.

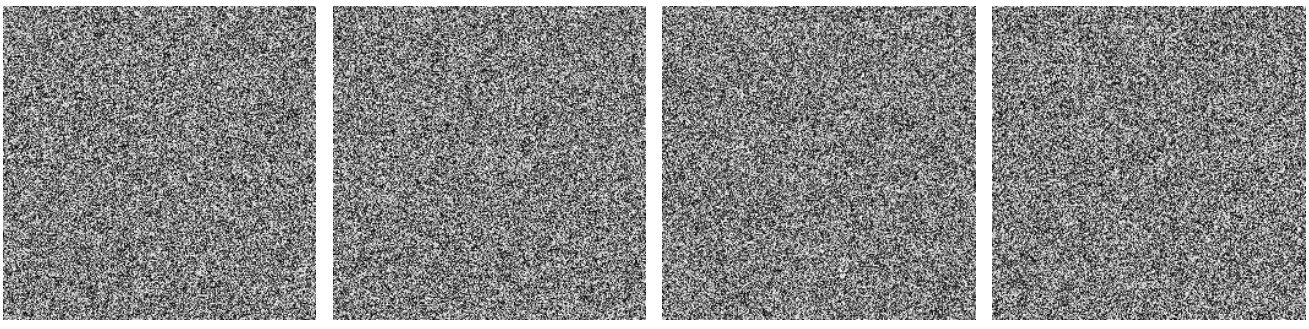

FIGURE 6. Encrypted-images using proposed encryption method (a) Lena, (b) Baboon, (c) Cameraman, (d) Tree.

the visual distortion is pretty good as they are highly indistinguishable and distorted. It is very difficult for the attacker to guess or know any pattern or partial information of respective plain-images.

A. HISTOGRAM ANALYSIS

Histogram of an image is a graphical description of its pixels distribution. For a strong cryptographic sense, it is always desired that the distribution of elements in an encrypted

content should have uniform distribution i.e. each of the element is equally likely probable. The histograms of plain-images and encrypted-images are shown in Figure 7. The histogram enables us to study distribution of pixels in both plain-image and encrypted-images [68]. Also, the comparison of their histograms makes evident the huge difference between the characteristics of such a pair of images. It is clear from the Figure 7 that the histograms of encrypted images are considerably different than their respective plain-images. Moreover, the encrypted images have uniform and fairly flat type of histograms. The variances of histograms are computed to show the difference between the pairs of histograms statistically. The variance of histogram of an 8-bit encoded gray-scale image is expressed as follows [53]:

$$V = \frac{1}{256 \times 256} \sum_{n=0}^{255} \sum_{m=0}^{255} \frac{1}{2} (g_m - g_n)^2 \quad (8)$$

where, g_m denotes the number of image pixels having gray value of m. The obtained scores of variances for plain-images and encrypted images are listed in Table 11 and the same are compared with corresponding results of encrypted images analyzed in [53], [69]–[71]. Our results demonstrate the consistent performance of the proposed encryption method. Hence, our encryption method can resist the histogram-based statistical attacks.

TABLE 11. Variance V of different images for histogram analysis.

Image	Lena	Baboon	Cameraman	Tree
Plain-image	39666.8	55604.8	110973.3	66009.7
Proposed	391.078	485.15	642.234	458.05
Ref. [69]	609.73	405.94	1074.2	496.18
Ref. [53]	262.5	267.81	201.79	270.59
Ref. [70]	280.12	272.92	339.59	310.66
Ref. [71]	284.58	268.21	223.36	257.69

B. DIFFERENCE, ERROR, SIMILARITY ANALYSIS

It is advisable to quantify the perceptual comparison of encrypted images with respect to their plain-images. For this, the statistical measures used to assess the difference (via mean absolute difference), errors (via mean square error), peak signal to noise ratio, and similarity index (via structural similarity index) [49]. Mathematically, they are calculated as per the following governing formulas expressed through Eq. (9) to (12), respectively.

$$MAD = \frac{1}{M \times N} \sum_{n=1}^{N} \sum_{m=1}^{M} |P(m,n) - C(m,n)| \quad (9)$$

$$MSE = \frac{1}{M \times N} \sum_{n=1}^{N} \sum_{m=1}^{M} (P(m,n) - C(m,n))^2 \quad (10)$$

$$PSNR = 20log_{10}\left[\frac{255}{\sqrt{MSE}}\right] \quad (11)$$

$$SSIM = \left(\frac{2\mu_P\mu_C + c_1}{\mu_P^2 + \mu_C^2 + c_1}\right)\left(\frac{2\sigma_{PC} + c_2}{\sigma_P^2 + \sigma_C^2 + c_2}\right) \quad (12)$$

where, μ_P and μ_C represents the mean value of plain-image P and encrypted image C, σ^2 denotes the variance and σ_{PC} denotes the covariance of images P and C. The c1 and c2 are constants which are set as $c_1 = (K_1 \times L)^2$, and $c_2 = (K_2 \times L)^2$, where $K_1 = 0.01$, $K_2 = 0.03$ and $L = 2^8 = 256$ for 8-bit coded images.

The scores of these statistical measures for the pair of plain-images and encrypted images available in Figure 5 and Figure 6 are listed in Table 12. The obtained values demonstrate that the encrypted contents are considerably different from their plain-images statistically in addition to visual inspections. Our results are also compared with recently investigated encryption algorithm outcomes in Table 13 and it is observed that both are consistent in performance on the ground of these statistical measures.

TABLE 12. MAD, MSE, PSNR, and SSIM results for proposed encryption method.

Image	MAD	MSE	PSNR	SSIM
Lena	72.79	7756.65	9.234	0.00915
Baboon	69.96	7022.94	9.665	0.0067
Cameraman	78.37	9230.99	8.478	0.00847
Tree	82.12	10083.22	8.095	0.00881

TABLE 13. Comparison on Lena encrypted images.

Image	MAD	MSE	PSNR	SSIM
Lena	72.79	7756.65	9.234	0.00915
Ref. [49]	73.07	7771.88	8.779	0.00950

C. MAJORITY LOGIC CRITERIA ANALYSIS

Majority logic criteria (MLC) suite is the exploration of different set of analyses which enables us to determine the suitability of substitution-boxes for image encryption applications. This set of tools also provides to assess the encryption effect and compare the encrypted content with the plain-images [38], [55], [56]. The complete suite of MLC analysis includes different component measures such as entropy, correlation, contrast, energy, and homogeneity. An S-box based encrypted image deemed strong if encrypted images tend to show high entropy close to 8, low correlation close to 0, high contrast, low energy, and low homogeneity. These individual components of MLC suite are mathematically defined as follows:

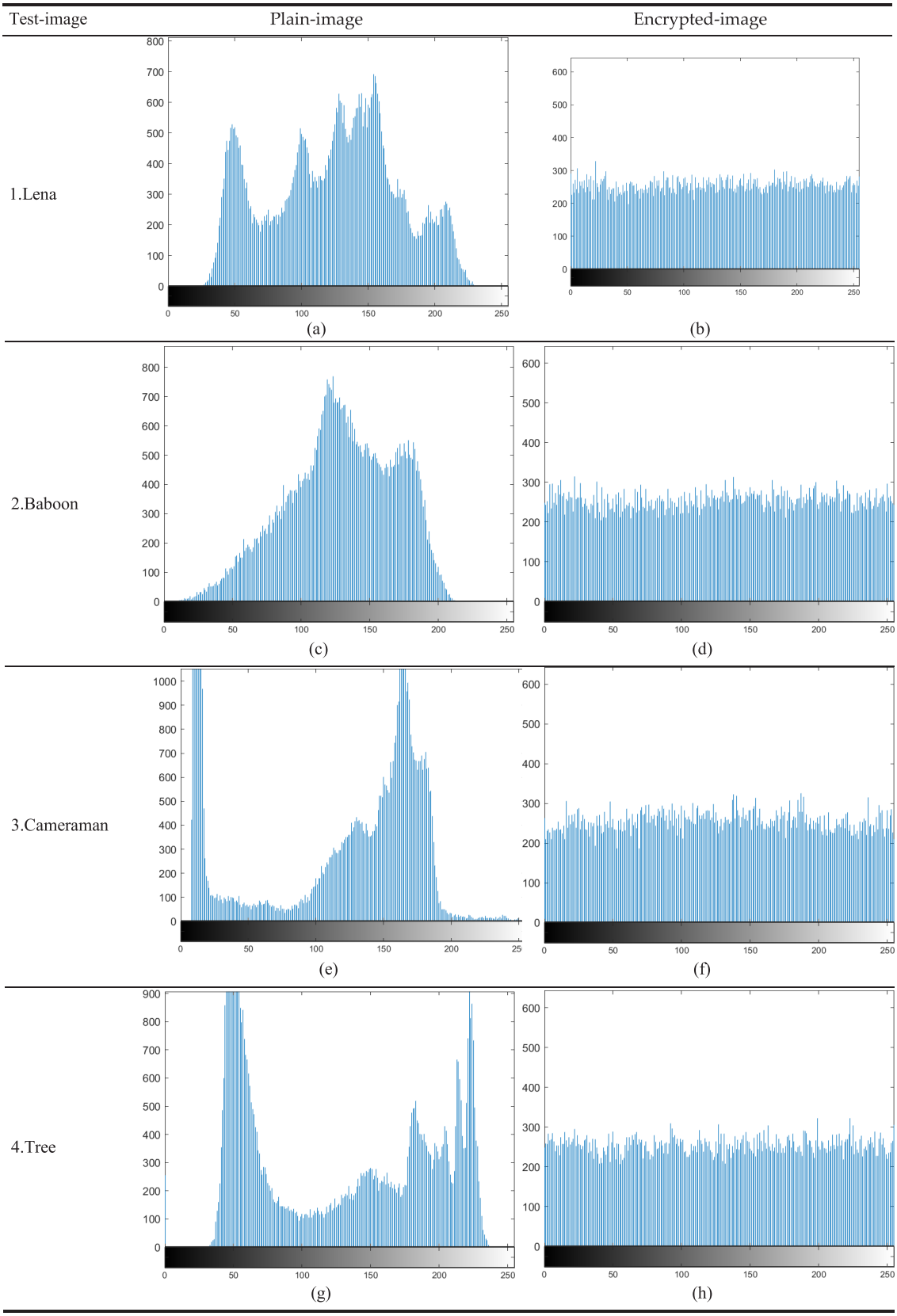

FIGURE 7. Histograms of test images: plain-images (first column) and encrypted-images (second column).

Information entropy is used to measure the randomness content in data. If the data is having uniformly distributed elements then the entropy of data will be high [72], [73]. The entropy is expressed as:

$$Entropy = \sum_{i} p(s_i) log_2 \left(\frac{1}{p(s_i)} \right) \tag{13}$$

where, $p(s_i)$ is the probability of pixel's gray-value s_i $(i = 0 \sim 255)$ of an image source.

The meaningful imagery data have high correlation within neighboring pixels. A strong image cryptosystem should have efficacy to diminish the existence of any such correlation within the encrypted content [74]. The correlation coefficient is defined as:

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

where, i represents the position of row and j indicates its column value of image under examination. The parameters μ *and* σ are the variance and standard deviation, respectively.

The contrast is related to the intensity difference among the neighboring pixels of an image. A good encryption method tends to bring high contrast in the encrypted image [75]. It is computed as:

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

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

The energy of an image measures the rate of change in color or brightness of the pixels in an image. Accordingly, an encrypted image is expected to have low energy [76]. The energy is evaluated as:

$$Energy = \sum \eta(i, j)^2 \tag{16}$$

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

Homogeneity of region is related to the changes in intensities that appear in that region of images [77], [78]. The homogeneity is calculated as:

$$Homogeneity = \sum \frac{p(i, j)}{1 + |i - j|} \tag{17}$$

We applied this suite of statistical analysis to evaluate the stability and suitability of our generated S-box based image encryption method performance. The MLC analysis is performed on the four test images and results obtained for plain-images and encrypted-images from our method are shown in Table 14. We make the comparison of our S-box encryption results with some recently investigated S-boxes based image encryption algorithms. Table 15 reports the comparison of MLC results on standard Lena image. Whereas, the comparison of the MLC results for Baboon image is made in Table 16. It is quite clear that our S-box based image encryption method is fairly better than many other S-box based image encryption algorithm performances.

TABLE 14. MLC results of entropy, correlation, contrast, energy, homogeneity from proposed encryption method.

Image	Entropy	Correlation	Contrast	Energy	Homogeneity
Plain-image					
Lena	7.4439	0.90249	0.4483	0.11275	0.8622
Baboon	7.2649	0.7983	0.6327	0.09438	0.7821
Cameraman	7.0097	0.92272	0.58716	0.18053	0.8952
Tree	7.3103	0.95727	0.38615	0.12989	0.8697
Encrypted-image					
Lena	7.9957	0.00080	10.4818	0.01565	0.38996
Baboon	7.9929	-0.00267	10.5155	0.01566	0.3889
Cameraman	7.9929	-0.00441	10.2265	0.01568	0.39168
Tree	7.9949	-0.00439	10.5963	0.01565	0.3873

TABLE 15. MLC results comparison on Lena image.

Lena	Entropy	Correlation	Contrast	Energy	Homo geneity	MAD
Proposed	7.9957	0.0008	10.4818	0.01565	0.3899	72.79
Ref. [57]	7.9353	0.0487	9.9764	0.0161	0.4131	38.45
Ref. [49]	7.992	-0.0018	10.4880	0.0156	-	73.07
Ref. [73]	7.9633	0.0019	8.5969	0.0174	0.4070	38.56
Ref. [74]	7.9924	-0.0002	8.7587	0.2365	0.9953	-
Ref. [75]	7.9801	-0.0293	8.6603	0.0674	0.9102	-
Ref. [76]	7.9621	0.0067	8.7032	0.0172	0.4056	-

TABLE 16. MLC results comparison on Baboon image.

Lena	Entropy	Correlation	Contrast	Energy	Homo geneity	MAD
Proposed	7.9929	-0.00267	10.5155	0.01566	0.3889	69.96
Ref. [55]	7.3583	0.0075	10.5005	0.0163	0.4005	71.22
Ref. [77]	7.3583	0.0176	9.8992	0.0165	0.4094	71.84
Ref. [32]	7.3583	0.0267	9.4156	0.0163	0.4088	66.88
Ref. [78]	7.3583	0.0343	9.8414	0.0161	0.4084	67.04
Ref. [79]	7.9829	0.0023	8.5483	0.0174	0.4115	73.26

D. ENCRYPTION TIME ANALYSIS

The encryption time is amongst the imperative factors for its practicability and suitability for wireless sensor network-based systems, Internet of Things and other lightweight security applications. An image cryptosystem should con-

TABLE 17. Encryption time analysis and comparison with recent algorithms (time in secs).

Encryption Method	Proposed	Ref. [80]	Ref. [53]	Ref. [70]	Ref. [71]	Ref. [69]	Ref. [62]	Ref. [76]	Ref. [81]
256×256	0.3732	8.181	0.382	1.245	1.212	0.959	0.4071	2.275	1.1204
512×512	1.3605	32.727	1.489	4.826	4.749	3.253	1.5619	-	-

sume negligible time to encrypt or decrypt the images. The proposed image encryption algorithm performs M re-arrangements of rows, N re-arrangements of columns during the pixels permutation phase. Whereas, the algorithm needs to perform $6L$ *mod*(.), L *floor*(.), $2L$ *bitxor*(.), and L *circshift*(.) operations during the substitution-phase, here $L = M \times N$. To perform the encryption time analysis, we computed the time taken by our S-box based image encryption method. We found that it takes only 0.3732 secs to encrypt an 8-bit encoded gray-scale image of size 256×256, and 1.3605 secs to encrypt 512×512 sized images. This provides a throughput of more than 1370 kbps. The encryption time comparison analysis made in Table 17 indicates that our encryption method is considerably faster in generating the encrypted images. The encryption time is shorter than many recent encryption algorithms investigated in [53], [62], [69]–[71], [76], [80], [81].

V. CONCLUSION

In this paper, we have proposed a simple and efficient technique for S-box construction using the idea of novel transformation, modular inverse and permutation. An example S-box was evaluated and analyzed to verify its cryptographic forte using standard criteria. Then, its performance was analyzed by comparing it with other recently projected S-boxes. The investigation outcomes are in synchronization with the required benchmarks to validate our technique and the performance of the proposed S-box hums decent when it was equated with other S-boxes. An image encryption method is also suggested based on the generated S-box. Image encryption method involves pixels permutation and substitution using our S-box. The different statistical performance measures indicate the suitability of proposed S-box for image encryption applications.

REFERENCES

[1] C. Paar, J. Pelzl, and B. Preneel, *Understanding Cryptography*, 1st ed. Berlin, Germany: Springer, 2010.
[2] M. Ahmad, E. Al Solami, X.-Y. Wang, M. Doja, M. Beg, and A. Alzaidi, "Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos," *Symmetry*, vol. 10, no. 7, p. 266, Jul. 2018.
[3] M. M. Lauridsen, C. Rechberger, and L. R. Knudsen, "Design and analysis of symmetric primitive," Tech. Univ. Denmark, Kgs. Lyngby, Denmark, Tech. Rep. 382, 2016.
[4] A. Belazi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Selective image encryption scheme based on DWT, AES S-box and chaotic permutation," *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, p. 606610.
[5] F. A. Kadhim, G. H. A. Majeed, and R. S. Ali, "Proposal new S-box depending on DNA computing and mathematical operations," in *Proc. Al-Sadeq Int. Conf. Multidisciplinary IT Commun. Sci. Appl. (AIC-MITCSA)*, May 2016, pp. 1–6.
[6] M. Ahmad, H. Chugh, A. Goel, and P. Singla, "A chaos based method for efficient cryptographic S-box design," in *Proc. Int. Symp. Secur. Comput. Commun.* Berlin, Germany: Springer, 2013, pp. 130–137.
[7] E. Tanyildizi and F. Ozkaynak, "A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838, 2019.
[8] M. Ahmad, E. Al-Solami, A. M. Alghamdi, and M. A. Yousaf, "Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures," *IEEE Access*, vol. 8, pp. 110397–110411, 2020.
[9] K. Mohamed, M. N. M. Pauzi, F. H. H. M. Ali, S. Ariffin, and N. H. N. Zulkipli, "Study of S-box properties in block cipher," in *Proc. Int. Conf. Comput., Commun., Control Technol. (I4CT)*, Kedah, Malaysia, Sep. 2014, pp. 2–4.
[10] A. Alabaichi and A. I. Salih, "Enhance security of advance encryption standard algorithm based on key-dependent S-box," in *Proc. 5th Int. Conf. Digit. Inf. Process. Commun.*, Sierre, Switzerland, Oct. 2015, pp. 7–9.
[11] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyper-chaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018.
[12] Z. Du, Q. Xu, J. Zhang, and M. Li, "Design and analysis of dynamic S-box based on Feistel," in *Proc. Int. Conf. Adv. Inf. Technol., Electron. Automat. Control*, Chongqing, China, Dec. 2015, pp. 19–20.
[13] J. Patil, G. Bansod, and K. S. Kant, "LiCi: A new ultra-lightweight block cipher," in *Proc. Int. Conf. Emerg. Trends Innov. (ICT)*, Pune, India, Feb. 2017, pp. 40–45.
[14] K. Kazlauskas, R. Smaliukas, and G. Vaicekauskas, "A novel method to design S-boxes based on key-dependent permutation schemes and its quality analysis," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 4, pp. 93–99, 2016.
[15] 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.*, St. Petersburg, Russia, Oct. 2012, pp. 474–478.
[16] K. Kazlauskas, G. Vaicekauskas, and R. Smaliukas, "An algorithm for key-dependent S-box generation in block cipher system," *Informatica*, vol. 26, no. 1, pp. 51–65, 2015.
[17] S. Sahmoud, W. Elmasry, and S. Abudalfa, "Enhancement the security of AES against modern attacks by using variable key block cipher," *Int. Arab J. e-Technol.*, vol. 3, no. 1, pp. 17–26, 2013.
[18] J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, "An improved AES S-box and its performance analysis," *Int. J. Innov. Comput., Inf. Control*, vol. 7, no. 5, pp. 2291–2302, 2011.
[19] P. Agarwal, A. Singh, and A. Kilicman, "Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant," *Adv. Mech. Eng.*, vol. 10, no. 7, pp. 1–18, 2018.
[20] E. M. Mahmoud, A. A. E. Hafez, T. A. Elgarf, and A. Zekry, "Dynamic AES-128 with key-dependent S-box," *Int. J. Eng. Res. Appl.*, vol. 3, no. 1, pp. 1662–1670, Jan. 2013.
[21] M. S. M. Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-Haq, S. N. M. Shah, M. Rehman, and W. Ahmad, "Generation of highly non-linear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices," *IEEE Access*, vol. 8, pp. 35682–35695, 2020.
[22] M. Ahmad, H. Haleem, and P. M. Khan, "A new chaotic substitution box design for block ciphers," in *Proc. Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Feb. 2014, pp. 255–258.
[23] 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.
[24] Q. Lai, A. Akgul, C. Li, G. Xu, and Ü. Çavuşoğlu, "A new chaotic system with multiple attractors: Dynamic analysis, circuit realization and S-box design," *Entropy*, vol. 20, no. 1, p. 12, 2018.

[25] J. Peng, S. Jin, L. Lei, and R. Jia, "A novel method for designing dynamical key-dependent S-boxes based on hyperchaotic system," *Int. J. Adv. Comput. Technol.*, vol. 4, no. 18, pp. 282–289, Oct. 2012.

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

[27] M. Ahmad and E. Al-Solami, "Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme," *Entropy*, vol. 22, no. 7, p. 717, Jun. 2020.

[28] D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," *J. Inf. Telecommun.*, vol. 2, no. 2, pp. 181–191, Apr. 2018.

[29] Q. Lu, C. Zhu, and G. Wang, "A novel S-box design algorithm based on a new compound chaotic system," *Entropy*, vol. 21, no. 1004, pp. 1–15, 2019.

[30] L. C. N. 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] A. Qureshi and T. Shah, "S-box on subgroup of galois field based on linear fractional transformation," *Electron. Lett.*, vol. 53, no. 9, pp. 604–606, Apr. 2017.

[32] S. S. Jamal, Attaullah, T. Shah, A. H. AlKhaldi, and M. N. Tufail, "Construction of new substitution boxes using linear fractional transformation and enhanced chaos," *Chin. J. Phys.*, vol. 60, pp. 564–572, Aug. 2019, doi: 10.1016/j.cjph.2019.05.038.

[33] 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, pp. 1–9, Aug. 2015.

[34] A. H. S. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "Generating a new S-box inspired by biological DNA," *Int. J. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 32–42, 2015, doi: 10.12783/ijcsa.2015.0401.04.

[35] U. Hayat, N. A. Azam, and M. Asif, "A method of generating 8×8 substitution boxes based on elliptic curves," *Wireless Pers. Commun.*, vol. 101, no. 1, pp. 439–451, Jul. 2018.

[36] N. A. Azam, U. Hayat, and I. Ullah, "An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Dec. 2018.

[37] B. N. Tran, T. D. Nguyen, and T. D. Tran, "A new S-box structure based on graph isomorphism," in *Proc. Int. Conf. Comput. Intell. Secur.*, Beijing, China, Dec. 2009, pp. 463–467.

[38] 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.

[39] A. A. Alzaidi, M. Ahmad, H. S. Ahmed, and E. A. Solami, "Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map," *Complexity*, vol. 2018, pp. 1–16, Dec. 2018.

[40] Y. Wang, K.-W. Wong, C. Li, and Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," *Phys. Lett. A*, vol. 376, nos. 6–7, pp. 827–833, Jan. 2012.

[41] 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.

[42] 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.

[43] 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.

[44] B. R. Gangadari and S. R. Ahamed, "Design of cryptographically secure AES like S-box using second-order reversible cellular automata for wireless body area network applications," *Healthcare Technol. Lett.*, vol. 3, no. 3, pp. 177–183, Sep. 2016.

[45] K. Kobayashi, N. Takagi, and K. Takagi, "An algorithm for inversion in GF(2^m) suitable for implementation using a polynomial multiply instruction on GF(2)," in *Proc. 18th IEEE Symp. Comput. Arithmetic (ARITH)*, Jun. 2007, pp. 105–112.

[46] M. Saeed and M. S. Mian, "Methods of finding multiplicative inverses in GF(28)," *Comput. Commun.*, vol. 31, no. 17, pp. 4117–4123, Nov. 2008.

[47] 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.

[48] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Amsterdam, The Netherlands: Elsevier, 2009.

[49] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020.

[50] A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Sci. Rep.*, vol. 10, no. 1, p. 116, Dec. 2020.

[51] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik Int. J. Light Electron Opt.*, vol. 58568, pp. 1–11, 2016.

[52] 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, Jan. 2020, Art. no. 699711.

[53] 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.

[54] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, Mar. 2020, Art. no. 118131.

[55] W. Gao, B. Idrees, S. Zafar, and T. Rashid, "Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(28))," *IEEE Access*, vol. 8, pp. 136736–136749, 2020, doi: 10.1109/ACCESS.2020.3010615.

[56] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," *IEEE Access*, vol. 8, pp. 116132–116147, 2020.

[57] S. Hussain, S. S. Jamal, T. Shah, and I. Hussain, "A power associative loop structure for the construction of non-linear components of block cipher," *IEEE Access*, vol. 8, pp. 123492–123506, 2020.

[58] J. Wang, B. Pan, C. Tang, and Q. Ding, "Construction method and performance analysis of chaotic S-box based on fireworks algorithm," *Int. J. Bifurcation Chaos*, vol. 29, no. 12, Nov. 2019, Art. no. 1950158.

[59] A. A. A. El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, p. 92102, Aug. 2019.

[60] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based S-box designs," *Phys. A, Stat. Mech. Appl.*, vol. 550, Jul. 2020, Art. no. 124072.

[61] A. K. Farhan, R. S. Ali, H. Natiq, and N. M. G. Al-Saidi, "A new S-box generation algorithm based on multistability behavior of a plasma perturbation model," *IEEE Access*, vol. 7, pp. 124914–124924, 2019.

[62] A. Ullah, S. S. Jamal, and T. Shah, "A novel scheme for image encryption using substitution box and chaotic system," *Nonlinear Dyn.*, vol. 91, no. 1, pp. 359–370, Jan. 2018.

[63] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, Santa Barbara, CA, USA, Aug. 1986, pp. 523–534.

[64] C. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," *J. Cryptol.*, vol. 3, no. 1, pp. 27–41, Jan. 1990.

[65] E. Biham and A. Shamir, "Differential cryptanalysis of Des.like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.

[66] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. A. El-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci.*, vol. 515, p. 191217, Apr. 2020.

[67] M. Matsui, "Linear cryptanalysis method for DES cipher," *Advances in Cryptology*. Trondheim, Norway: Springer, 1994, pp. 386–397.

[68] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran, A. K. Bashir, O.-Y. Song, and W. Mazurczyk, "Providing end-to-end security using quantum walks in IoT networks," *IEEE Access*, vol. 8, p. 9268792696, 2020.

[69] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons Fractals*, vol. 95, Feb. 2017, Art. no. 92101.

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

[71] X.-P. Zhang, R. Guo, H.-W. Chen, Z.-M. Zhao, and J.-Y. Wang, "Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes," *Chin. Phys. B*, vol. 27, no. 8, Aug. 2018, Art. no. 080701.

[72] A. Kadhim and R. M. Mohamed, "Visual cryptography for image depend on RSA & AlGamal algorithms," in *Proc. Al-Sadeq Int. Conf. Multidisciplinary IT Commun. Sci. Appl. (AIC-MITCSA)*, May 2016, pp. 1–6.
[73] Y. Naseer, T. Shah, S. Hussain, and A. Ali, "Steps towards redesigning cryptosystems by a non-associative algebra of IP-loops," *Wireless Pers. Commun.*, vol. 108, May 2019, Art. no. 13791392.
[74] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix lorenz systems S-boxes and their applications," *Chin. J. Phys.*, vol. 56, no. 4, pp. 1609–1621, Aug. 2018.
[75] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1839–1850, Dec. 2015.
[76] Y. Naseer, T. Shah, Attaullah, and A. Javeed, "Advance image encryption technique utilizing compression, dynamical system and S-boxes," *Math. Comput. Simul.*, vol. 178, pp. 207–217, 2020.
[77] 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, doi: 10.1007/s11277-017-5054-x.
[78] 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, 2020, doi: 10.1007/s11042-019-08282-w.
[79] A. Ullah, A. Javeed, and T. Shah, "A scheme based on algebraic and chaotic structures for the construction of substitution box," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 32467–32484, Nov. 2019.
[80] 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.
[81] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A new design of cryptosystem based on S-box and chaotic permutation," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19129–19150, Jul. 2020.

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

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

MUSHEER AHMAD received the Ph.D. degree from the Department of Computer Engineering, Jamia Millia Islamia, in the area of Chaos-based cryptography. the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively. He has worked with the Department of Computer Engineering, Aligarh Muslim University, from 2007 to 2010. He has been working as an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, since 2011. He has published over 80 research articles in international reputed refereed journals and conference proceedings of IEEE/Springer/Elsevier. He has more than 1000 citations of his research works with an h-index of 18. His areas of research interests include, but not limited to, multimedia security, Chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has served as a referee of some renowned journals such as: Signal Processing, Information Sciences, Journal of Information Security and Applications, the IEEE Access, the IEEE Journal on Selected Areas in Communications, the IEEE Transactions on Neural Networks & Learning Systems, Wireless Personal Communications, Neural Computing and Applications, International Journal of Bifurcation and Chaos, Optik, Optics and Laser Technology, Neurocomputing, IET Information Security, Security and Communication Networks, Complexity, Computers in Biology and Medicine, Chaos, Solitons & Fractals, Physica A: Statistical Mechanics and its Applications, Signal Processing: Image Communication, Journal of the Chinese Institute of Engineers, Computational and Applied Mathematics, and ETRI Journal.