IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 16, 2021, accepted April 29, 2021, date of publication May 3, 2021, date of current version May 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3077194

A Novel Construction of Dynamic S-Box With High Nonlinearity Using Heuristic Evolution

AMJAD HUSSAIN ZAHID[1], ABDULLAH M. ILIYASU[2,3,4], (Senior Member, IEEE), MUSHEER AHMAD[5], MIAN MUHAMMAD UMAR SHABAN[1], MUHAMMAD JUNAID ARSHAD[6], HUSSAM S. ALHADAWI[7], AND AHMED A. ABD EL-LATIF[8]

[1]Department of Informatics and Systems, University of Management and Technology, Lahore 54700, Pakistan
[2]Department of Electrical Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[3]School of Computing, Tokyo Institute of Technology, Yokohama 226-8502, Japan
[4]School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China
[5]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[6]Department of Computer Science, University of Engineering and Technology, Lahore 54700, Pakistan
[7]Department of Computer Techniques Engineering, Dijlah University College, Baghdad 10011, Iraq
[8]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Menoufia 32511, Egypt

Corresponding authors: Abdullah M. Iliyasu (a.iliyasu@psau.edu.sa) and Musheer Ahmad (mahmad9@jmi.ac.in)

This study is sponsored by the Prince Sattam Bin Abdulaziz University, Saudi Arabia via the Deanship for Scientific Research funding for the Advanced Computational Intelligence and Intelligent Systems Engineering (ACIISE) Research Group Project Number 2020/01/12173.

ABSTRACT For decades, the security and privacy of data are among the major challenges faced by service providers dealing with public data. To cope with these challenges, most of the organizations rely on the adoption of cryptographic methods for protecting data against any illegitimate access and attacks. Modern day cryptographic ciphers utilize one or more substitution-boxes (S-boxes) that facilitate the realisation of strong security of plain data during encryption and legal decoding of it during decryption process. Security of ciphers is directly proportional to the cryptographic strength of S-boxes. This study proposes an efficient and simple method based on some modular operations for the construction of dynamic S- boxes with high nonlinearity using a heuristic evolution strategy. A large number of strong S-boxes can be easily constructed using slight variations in the parameters of the anticipated method. A specimen S-box is constructed and its critical performance analysis against standard security criteria including nonlinearity, strict avalanche criterion, bit independence criterion, differential uniformity, linear probability, and fixed points are reported as justification for the proposed technique's high cryptographic strength. Furthermore, the generated S-box is also applied to encrypt digital images to assess its cryptographic application performance. The performance and comparison study validates that the proposed S-box has better performance strength, which makes it a viable candidate for cryptographic applications in different areas of image security.

INDEX TERMS Security and privacy, substitution-box, block ciphers, encryption, image security, cyber physical systems.

I. INTRODUCTION

We are living in the technological era depending heavily on data and information that may include text, numbers, images, audio, video, etc. Most of this data is automatically generated and has to be stored or transferred over the public communication channels. Every so often, type of data being transmitted is sensitive and as a result, data security is much needed requirement. So, before its transmission over the public channels, steps are required to guard it by transforming it into a form that has no meaning for the intruders. There are many such ciphers available in the literature for securing the sensitive data. Ciphers used for the encryption of the plaintext and decryption of the ciphertext have two main types named as block ciphers and stream ciphers [1], [2]. A block cipher encodes/decodes data in a block-by-block manner. A block of data generally consists of one or more bytes. A stream cipher, on the other hand, performs these transformations using one bit or one byte in one go. In modern cryptography, a block cipher has emerged as the most effective method for the fortification of sensitive data [3]. Data Encryption Standard (DES), RC5, Advanced Encryption Standard (AES), etc. are some of the eminent block ciphers. Compared to stream ciphers, block ciphers are easily implementable and more commonly employed in real-life security applications [4]. One type of predominant block ciphers being utilized for the protection of data is recognized as the substitution-permutation block

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

ciphers. The significant operations used in these ciphers are permutation and substitution which help to transform data into a mystifying form. A permutation operation swaps the plaintext bits/bytes with other bits/bytes present in the same plaintext. Whereas, a substitution process replaces one block of data by another in nonlinear fashion. This replacement of data is performed with the help of substitution table or substitution-box (more often known as S-box) [5], [6]. An S-box is a vital constituent of contemporary block ciphers and assists greatly to produce a scrambled output data (ciphertext) for the given input data (plaintext). An S-box establishes a non-linear association between the input (plaintext) and the output (ciphertext) to produce more muddle for the attackers [7]. If a substitution box has the ability to produce more confusion for the invaders in the resultant ciphertext, the respective block cipher employing that S-box in its operations provides more security to the plaintext. Consequently, the protection that a block cipher provides to a given plaintext by employing one or more S-boxes is directly reliant on the strength of the respective S-boxes. Other constituents of a cipher work in a linear manner, while an S-box operates in a nonlinear fashion to increase the security of the plaintext [8], [9].

Modern-day ciphers employ two kinds of S-boxes known as static S-boxes and dynamic S-boxes. An S-box that has values placed in it at fixed locations and this arrangement of values always remains same is termed as static S-box. If an attacker obtains this S-box somehow, he/she will be very much able to attack the ciphertext to reach the original plaintext and security of the cipher employing that static S-box is compromised [10], [11]. Data Encryption Standard (DES) used such S-boxes and attackers broke it easily. Similarly, Advanced Encryption Standard (AES) have used static S-box in its working. To avoid this drawback of static S-boxes, designers of recent block ciphers mostly use dynamic S-boxes to exploit their strengths compared to the weaknesses inherent in the static S-boxes [12]. Such S-boxes are constructed with the aid of the cipher key and possess the capability to enhance the cryptographic forte of the respective cipher. As a result, researchers tried and have projected innovative techniques to construct S-boxes that are key-dependent and hence dynamic in nature.

One of the commonly used algebraic concepts to construct dynamic and strong S-boxes is linear fractional transformation (LFT). Authors in [13]–[16] used LFT concept as the base to design effective and robust S-boxes. The projected S-boxes demonstrated decent recitals with respect to the standard cryptographic criteria used to evaluate an S-box. Most of the S-boxes designed with LFT use Galois Field (GF) arithmetic that makes the process of S-box construction very inefficient. Researchers have proposed efficient methods other than LFT techniques to generate S-boxes such as authors in [17] proposed method that used the idea of cubic fractional transformation (CFT) to generate decent S-boxes. This transformation is simple, efficient, and capable of generating robust S-boxes. In [18] another simple technique has been projected to construct S-boxes using a cubic polynomial transformation. This method is very simple, effective, and efficient to create robust S-boxes. An innovative approach was proposed in [19] to construct robust S-boxes using linear transformation. This approach augments the strength of the resultant S-box using the permutation process. Authors using methods suggested in [20]–[25] used DNA computing to construct robust S-boxes and cryptographically strong ciphers. Analysis of these S-boxes and ciphers demonstrated their strength with respect to cryptographic criteria and against different attacks. Chaos is another equally significant area used in cryptography to construct robust S-box due to the features of randomness of chaos systems [26]. A number of researchers [27]–[34] used chaos theory to construct S-boxes possessing upright cryptographic forte. Authors in [35], [36] used hyperchaotic schemes to construct robust and sturdy S-boxes. The underlying schemes are capable to produce large number of S-boxes. Many researchers have employed other knowledge zones to construct S-boxes like cellular automata [37], graph theory [38], [39], elliptic curve [40], [41], optimization techniques [32], [42]–[45], etc.

Advanced Encryption Standard (AES) is one of the eminent symmetric block ciphers that utilize S-boxes in their working. Each value of original AES S-box is constructed by computing multiplicative inverse of values in the range [0 – 255] using Galois Field. Calculation of multiplicative inverse for each value using Galois Field is quite complicated and time consuming and consequently makes the S-box design process very complex for a reader and computationally less efficient. Researchers in [46]–[50] suggested numerous improvements to the security offered by AES while refining the original AES S-box. Today, researchers and academicians focus on the erection of dynamic S-boxes using cipher key. Methods for such constructions in the existing literature have complications as well as efficiency issues in the production of robust S-boxes. As a result, new and novel efficient techniques are needed to produce robust, key-dependent, and dynamic S-boxes while bearing simplicity in the generation process.

Original AES S-box is static in nature and bears the dangers associated with such S-boxes. This paper introduces a modest technique to produce dynamic key-dependent strong S-boxes. The proposed technique gets values of parameters A, B, C, and D from the key. One can choose any value for these parameters from a certain range as mentioned in the contribution part below. This choice of values by the user makes this technique dynamic and hence assists in enhancing the strength of the generated S-Box by creating confusion for attackers. The novel method utilizes a modular operation-based approach to get initial configuration of S-box of size 8×8. The various operations involved are affine transformation, modular multiplicative inversion, etc. Affine transformation employed here is much simpler and efficient than the linear fractional transformations applied in various S-box designs in the literature. The initial configuration of obtained S-box is further elevated and improved by using the novel

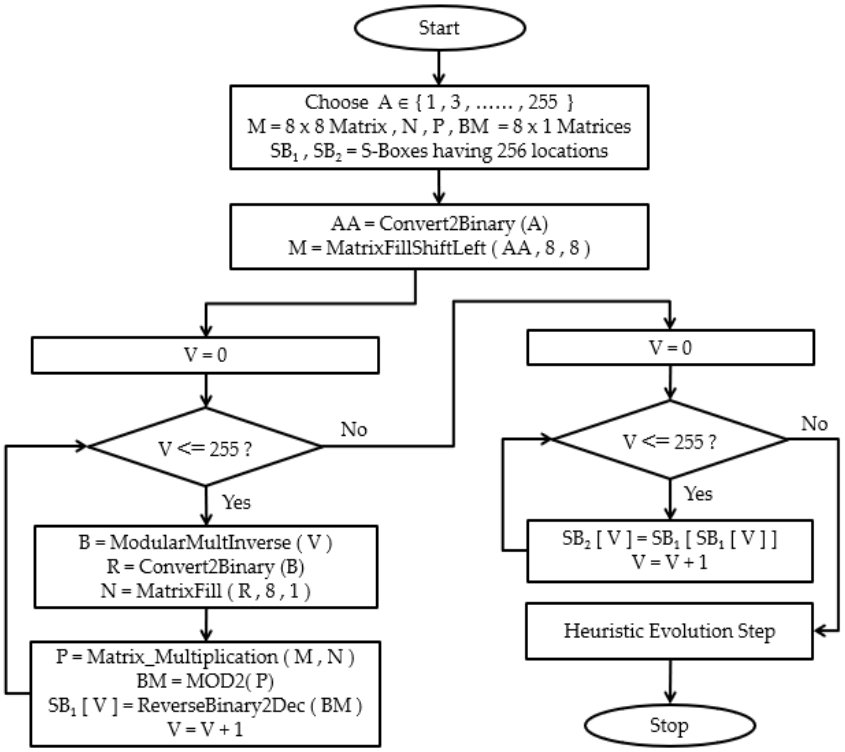

FIGURE 1. Flowchart of proposed S-box method.

heuristic evolution strategy which provides highly nonlinear S-box with excellent other cryptographic features.

Following are the main contributions reported in this paper:

- An innovative and simple approach is suggested to create initial S-boxes. A minor variation in the values of the parameters A, B, C, and D can yield very large number of S-boxes where A $\in$ {1, 3, ..., 255}, B $\in$ {1, 2, ..., 255}, and C, D $\in$ {0, 1, ..., $2^{16} - 1$}. So, a very large S-box space ($128 \times 255 \times 65536 \times 65536 = 140{,}187{,}732{,}541{,}440$) is there.
- A novel heuristic evolution strategy is proposed which improvises the S-box on the basis of nonlinearity criterion of the S-box. Dynamic nature of proposed method uses values from key and enhances the ciphertext sanctuary.
- Proposed S-box is critically analyzed using standard S-box evaluation criteria along with the S-boxes currently available in the literature. This performance analysis validates the noteworthy contribution of the projected S-box.
- The specimen S-box from proposed method is utilized for image security applications. The simulation and performance analyses show excellent encryption quality from the S-box based encryption.

The remaining parts of this paper have the following organization. In section II, methodology for the erection of S-boxes using a novel modular operations and heuristic evolution strategy is discussed in detail. In section III, performance and comparative analysis of a specimen S-box generated with the proposed technique is done with some existing contemporary S-boxes. The proposed S-box is applied and assessed for image security application in Section IV. Whereas, Section V concludes the research done in this paper.

II. PROPOSED CONSTRUCTION OF DYNAMIC S-BOX

Modern-day block ciphers employ S-boxes in their working to encrypt the data to produce more and more jumble in the resultant ciphertext. An S-box helps to produce a non-linear association among the input (plaintext) and output (ciphertext). As a result of application of this mapping, an invader's job to reach the original plaintext from the ciphertext becomes very difficult and annoying. Researchers have recurrently investigated such nonlinear transformations to generate robust S-boxes. An S-box generation process requires both simplicity and efficiency. A large number of existing S-box construction techniques are complex ones and less efficient.

As an example, AES S-box generation process is quite complicated as it calculates and utilizes multiplicative inverse with the help of Galois Field. The inversion process using Galois Field is quite intricate and inefficient. Many researchers like [46]–[50] have proposed different techniques for improving the efficiency of the original AES S-box construction process. S-box generation processes using these techniques still require simplicity and efficiency. Here, we present an innovative approach based on an affine transformation and a novel permutation process to generate a robust S-box. The comprehensive procedure of dynamic S-box creation is illustrated in the flowchart given in Figure 1.

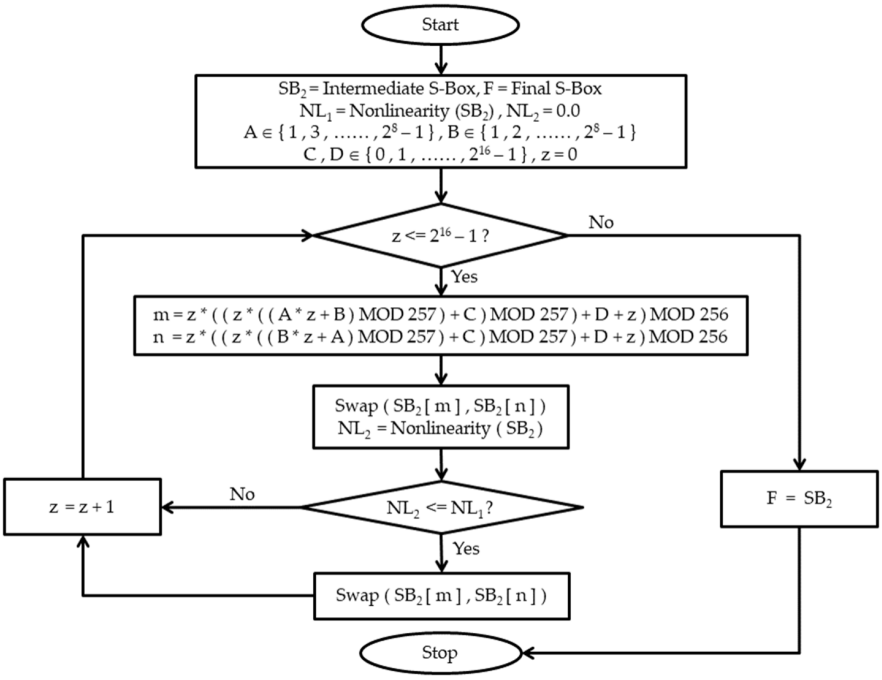

FIGURE 2. Heuristic Evolution Strategy.

Following section describes the major steps and functions of the proposed methodology in detail to have comprehensiveness of the complete S-box generation method.

Step-1 Generation of Binary Matrix: In this step, an 8×8 binary matrix is produced using the following functions.

string Convert2Binary (int A): This function changes the value of A into 8-bit binary string and returns the resultant string. Here, $A \in \{1, 3, \ldots, 255\}$.

matrix MatrixFillShiftLeft (*string AA, int r, int c*): This procedure fills an 8×8 matrix using $r = 8$ and $c = 8$. Each matrix cell is filled with 0 or 1. First row is filled with the string AA starting from left to right. Then, 1st row is left-shifted by 1 in circular fashion and the result is put in 2nd row. Then, 2nd row is left-shifted by 1 to left in circular fashion and the result is put in 3rd row and so on. For example, if the string AA is 10101100, the first row is filled as 1, 0, 1, 0, 1, 1, 0, 0. Shifting of the 1st row to the left in a circular fashion generates the 2nd row of the matrix as 0, 1, 0, 1, 1, 0, 0, 1. Resultant matrix, for this example, looks like as given in Table 1. The resultant matrix is named as M.

Step-2 Multiplicative Inverse Calculation: In this step, modular multiplicative inverse of a given value is computed and stored as an 8-bit value in 8×1 binary matrix. Procedure uses the following functions.

int ModularMultiplicativeInverse (int V): This procedure calculates the multiplicative inverse of a value V using MOD257. Mechanism of this calculation is described in [19].

matrix MatrixFill (string R, int r, int c): This procedure fills an 8×1 matrix using $r = 8$ and $c = 1$. Each matrix cell is filled with 0 or 1. Matrix is filled with the string R starting from 1st row to 8th row.

TABLE 1. Status of matrix after filling values.

1	0	1	0	1	1	0	0
0	1	0	1	1	0	0	1
1	0	1	1	0	0	1	0
0	1	1	0	0	1	0	1
1	1	0	0	1	0	1	0
1	0	0	1	0	1	0	1
0	0	1	0	1	0	1	1
0	1	0	1	0	1	1	0

Step-3 Matrix Multiplication: In this step, two matrices of sizes 8×8 and 8×1 are multiplied. Then modulo 2 operation is applied to generate an 8×1 binary matrix. Procedure uses the following functions.

matrix Matrix_Multiplication (matrix M, matrix N): This function multiplies two matrices $M_{8\times8}$ and $N_{8\times1}$ and returns matrix $P_{8\times1}$.

matrix MOD2 (matrix P): This function calculates the remainder of each value of matrix P using MOD 2 and returns matrix BM.

Step-4 Binary to Decimal Conversion: In this step, 8 bits of a byte are reversed, and the resultant binary value is converted into an equivalent decimal (integer) value. This step uses the following function.

int ReverseBinary2Dec (matrix P): This function reverses the binary value and then converts the reversed binary value to decimal. This decimal value is stored in the initial S-box S1.

Step-5 Permutation: In this step, values of initial S-box are permuted using the following function to generate an intermediate S-box.

TABLE 2. Proposed S-box.

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

int Initial_Permutation (matrix S1): This function permutes the values of initial S-box S1 and produces intermediate S-box S2. This permutation is done using the following operation.

SB2 [LOC] = SB1 [SB1 [LOC]]

Where, $0 \leq \text{LOC} \leq 255$.

Step-6 Heuristic Evolution: In this step, values of the intermediate S-box are once again permuted to produce final S-box using the following function.

matrix Final_Permutation (matrix S2): This function permutes the values of intermediate S-box S2 and produces final S-box S3. Final permutation process is shown in Figure 2. The resultant 8×8 S-box designed using the above technique is shown as a 16×16 look-up matrix in Table 2.

Heuristic evolution step has the significant contribution in the generation of strong and robust S-boxes in the proposed technique. Security of the data is of the utmost importance and concern of a user and can't be compromised. Considering modern day's CPU speed and availability of other sophisticated computational resources, heuristic evolution step produces good results.

III. PERFORMANCE EVALUATION OF S-BOX

An S-box must pass typical conditions known as standard criteria to be strong one and provide nonlinear association between input (plaintext) and output (ciphertext). This segment scrutinizes the forte of the produced S-box specified in Table 2 using following standard criteria which evaluates the cryptographic strength of S-boxes [30], [33], [51].

- Bijectiveness
- Nonlinearity
- Bit Independence Criterion
- Strict Avalanche Criterion

TABLE 3. Nonlinearity values of component boolean functions.

Bool Func	B1	B2	B3	B4	B5	B6	B7	B8
NL(B)	112	112	112	112	112	112	112	110

- Linear Probability
- Differential Uniformity
- Fixed Point

We choose recently investigated S-box methodologies for comparing the cryptographic features of our proposed S-box with these existing S-boxes. Also, the computational labor for the generation of proposed S-box is discussed at the end of this section.

A. BIJECTIVENESS

A mapping is a bijective (1-1) mapping if it has an inimitable output against a specific input. An S-box design should exhibit this property very well. In case of an 8×8 S-box, each input value in the range [0 – 255] should produce an inimitable output in the range [0 – 255]. Our projected S-box as shown in Table 2 validates this condition by having all possible diverse output values in the range [0 – 255]. In all coordinate Boolean Functions, number of 1's (128) is equal to the number of 0's as suggested by [9], [40].

B. NONLINEARITY

If a given S-box has a linear mapping between the output (ciphertext) and input (plaintext), an attacker can deduce the ciphertext in an easy manner. If an S-box structure has the capability to map an input to an output in a nonlinear fashion, respective S-box is believed to be stronger one. An S-box like

TABLE 4. Performance Comparison of S-boxes w.r.t. NL values.

S-box Method	Nonlinearity		
	Minimum	Maximum	Average
[19]	104	110	107.5
[52]	106	112	109.5
[53]	102	108	105.0
[54]	100	108	104.0
[55]	104	110	106.9
[56]	98	106	103.5
[57]	104	108	106.25
[58]	106	108	106.5
[59]	100	108	105.0
[60]	104	110	106.25
[61]	96	110	104.0
[62]	106	108	106.5
[63]	106	110	108
[64]	106	110	108.5
[65]	106	108	107.5
[66]	104	108	105
[67]	106	108	107
Proposed	**110**	**112**	**111.75**

TABLE 5. Dependency matrix of SAC values of proposed S-box.

0.5000	0.5156	0.5781	0.5000	0.5625	0.5313	0.5625	0.4688
0.4375	0.5156	0.5313	0.5781	0.5469	0.4844	0.4531	0.4844
0.4688	0.5313	0.5000	0.5000	0.4688	0.5000	0.5313	0.4688
0.4844	0.4688	0.4688	0.5000	0.5156	0.5000	0.4844	0.4688
0.5469	0.4375	0.5156	0.5000	0.5625	0.4844	0.4531	0.5469
0.5156	0.4219	0.5469	0.5469	0.5000	0.4688	0.5625	0.5313
0.5000	0.5469	0.5156	0.4531	0.4844	0.5469	0.5313	0.4375
0.5313	0.4844	0.4844	0.5156	0.4531	0.5000	0.4688	0.4844

this is helpful to defy linear cryptanalysis efforts by invaders. One can compute the value of nonlinearity of an 8-bit Boolean function B using Eq. (1) as given by [51]:

$$NL\,(B) = \left[2^{8-1} - 2^{-1}\,(WH_{max}(B))\right] \tag{1}$$

where, WH_{max} (B) = Walsh-Hadamard Transformation for an 8-bit Boolean function B. The Boolean functions that constitute our projected S-box and the corresponding non-linearity values are described in Table 3. It is evident that minimum, maximum, and average values of nonlinearity of our S-box are 110, 112, and 111.75 respectively. Comparison between values of nonlinearity of our S-box with recently projected S-box techniques is presented in Table 4.

It is apparent from the comparison that the nonlinearity value of our projected S-box outperforms nonlinearity results of other various current S-boxes.

TABLE 6. BIC-NL of Boolean functions Hx ⊕ hy (x ≠y).

-	102	108	104	102	104	104	106
102	-	100	104	104	104	102	104
108	100	-	102	104	108	102	104
104	104	102	-	106	104	104	100
102	104	104	106	-	104	102	108
104	104	108	104	104	-	104	96
104	102	102	104	102	104	-	108
106	104	104	100	108	96	108	-

TABLE 7. Performance comparison of BIC-NL and SAC values.

S-box Method	BIC-NL	SAC
[19]	103.5	0.498
[52]	106.9	0.507
[53]	102.9	0.503
[54]	102.6	0.497
[55]	106.1	0.509
[56]	103.5	0.496
[57]	103.6	0.501
[58]	104.1	0.501
[59]	103.0	0.500
[60]	103.9	0.503
[61]	103.0	0.493
[62]	103.6	0.499
[63]	102.9	0.499
[64]	103.9	0.500
[65]	103.1	0.509
[66]	103.5	0.506
[67]	102.3	0.493
Proposed	**103.7**	**0.502**

C. STRICT AVALANCHE CRITERION (SAC)

This characteristic of an S-box ensures that a single input bit change causes a modification of 50% of output bits [68]. Accordingly, an S-box that has SAC value approximately equal to 0.5 is considered as a strong one. Dependency matrix of SAC values of our S-box is given in Table 5.

TABLE 8. Differential uniformity values of proposed S-box.

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

Our S- box has SAC value as $0.502 \approx 0.5$. Consequently, our projected S-box satisfies the SAC obligation in a decent way. A comparison between SAC values of projected S-box and other S-boxes given in Table 7 illustrates that SAC score of our S-box has a graceful consistency with other S-boxes.

D. BIT INDEPENDENCE CRITERION (BIC)

This characteristic of an S-box ensures that change in any two output bits does not depend on each other whenever a single input bit is changes [68]. Table 6 illustrates the BIC nonlinearity (BIC-NL) values of component Boolean functions $H_x \oplus H_y$ ($x \neq y$) of our proposed S-box.

From Table 6, average value of BIC-NL comes out to be 103.7. This BIC-NL value indicates that the projected S-box gratifies the BIC requirement handsomely. BIC recital of different S-boxes is compared in Table 7.

E. LINEAR PROBABILITY (LP)

Designers of cryptosystems attempt to mix-up bits of plaintext in such a way that the invaders of ciphertext are unable to reach the original order of bits. A careful S-box design helps in creating this muddle by establishing nonlinear connotation among plaintext bits and ciphertext bits. The forte of this connotation of an S-box SB is evaluated by linear probability as given in Eq. (2) [69].

$$LP = \underset{\alpha_i, \beta_i \neq 0}{MAXIMUM} \mid 2^{-n}(\#\{i \in M \mid i.\alpha_i = SB(i) \cdot \beta_i\}) - 2^{-1} \mid \tag{2}$$

where,

α_i = input mask, β_i = output mas

M = {0, 1, 2, ..., 254, 255}.

If the connection between the input (plaintext) and output (ciphertext) is linear, the LP value for respective S-box is higher and linear cryptanalysis is easy for the attackers. The LP score of projected S-box is 0.125 and such a low value of LP is needed to resist linear cryptanalysis. Consequently, proposed S-box has adequate potential to counterattack such cryptanalytic efforts. A comparison of LP values of some current S-boxes and projected S-box is specified in Table 9. It is obvious that the projected S-box has good strength as compared to other current S-boxes in the literature.

F. DIFFERENTIAL UNIFORMITY (DU)

Attackers capture ciphertext and analyze it to reach the plaintext somehow by using variations in the ciphertext and modifications in the plaintext. Analysis of these differentials assists the attackers to identify the complete or partial plaintext or key [70]. S-box designers try to minimize the difference between these two variations. To calculate this difference, analysts evaluate the differential uniformity (DU) of a given S-box. To resist differential cryptanalysis, DU of an S-box should be low. Differential uniformity is assessed using Eq. (3) [71].

$$DU = \underset{\Delta g \neq 0, \Delta_f}{max} \left[\#\left\{g \in K \mid S(g) \oplus S\left(g \oplus \Delta_g\right) = \Delta_f\right\}\right] \tag{3}$$

where,

Δ_g = Input differential,

Δ_f = Output differential, and

K = {0, 1, 2, 3, 4, ..., 254, 255}.

An S-box that has small values of differentials possesses the capability to defy differential cryptanalytic efforts. DU values of projected S-box are listed in Table 8. Maximum DU score of projected S-box is 10, and consequently, value of differential probability (DP) evaluates to 0.039 that indicates that the projected S-box offers decent defiance to differential cryptanalysis. Table 9 illustrates a comparison of DP values of some current S-boxes and projected S-box.

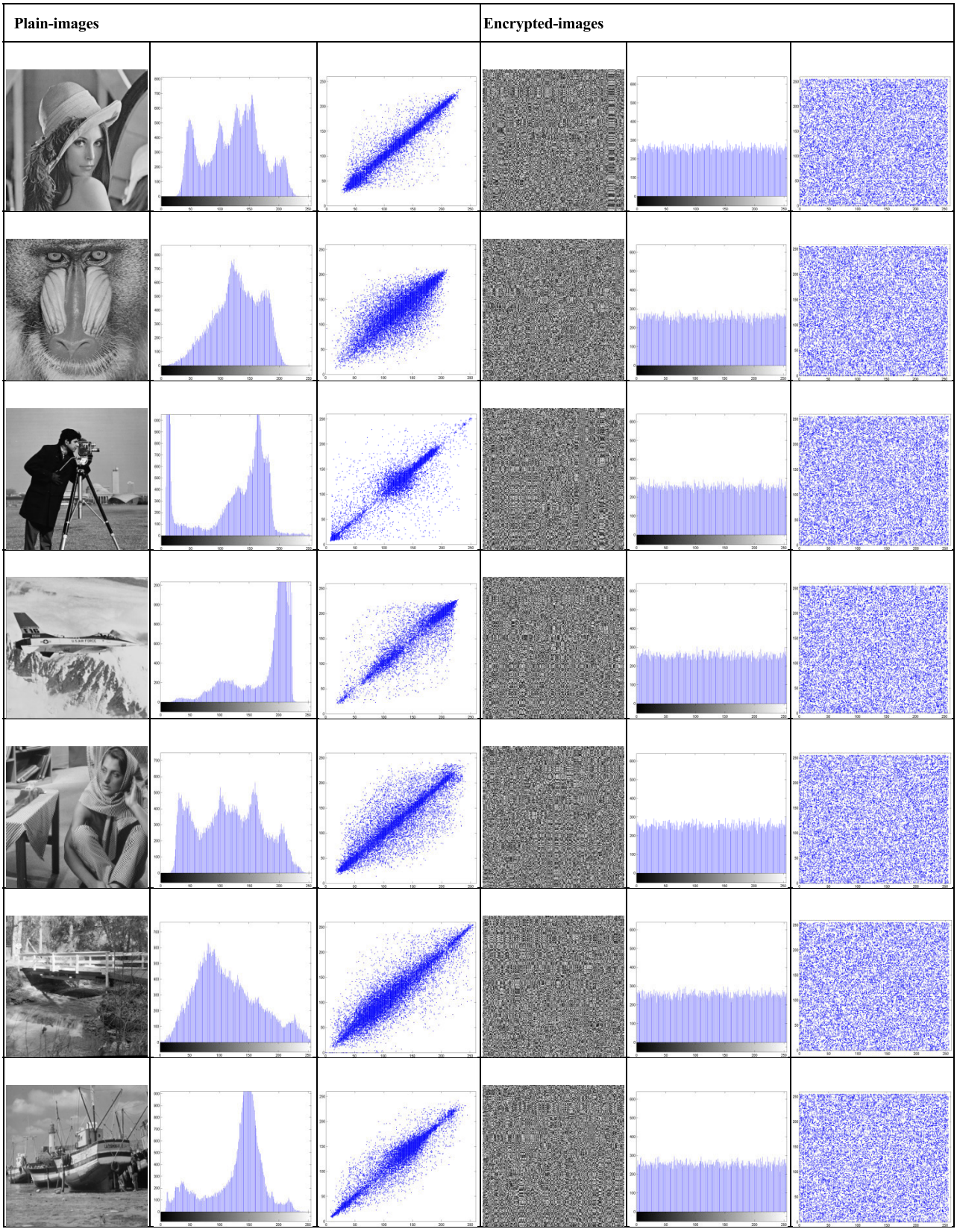

FIGURE 3. Visuals of plain and encrypted images for histogram and pixels correlation performance for S-box based image encryption; 1st column (a) shows plain-images; 2nd column (b) shows histograms of plain-images; 3rd column (c) shows vertically adjacent pixels correlation in plain-images; 4th column (d) shows encrypted-images using S-box based encryption; 5th column (e) shows histograms of encrypted-images; and 6th column (f) shows vertically adjacent pixels correlation in encrypted-images.

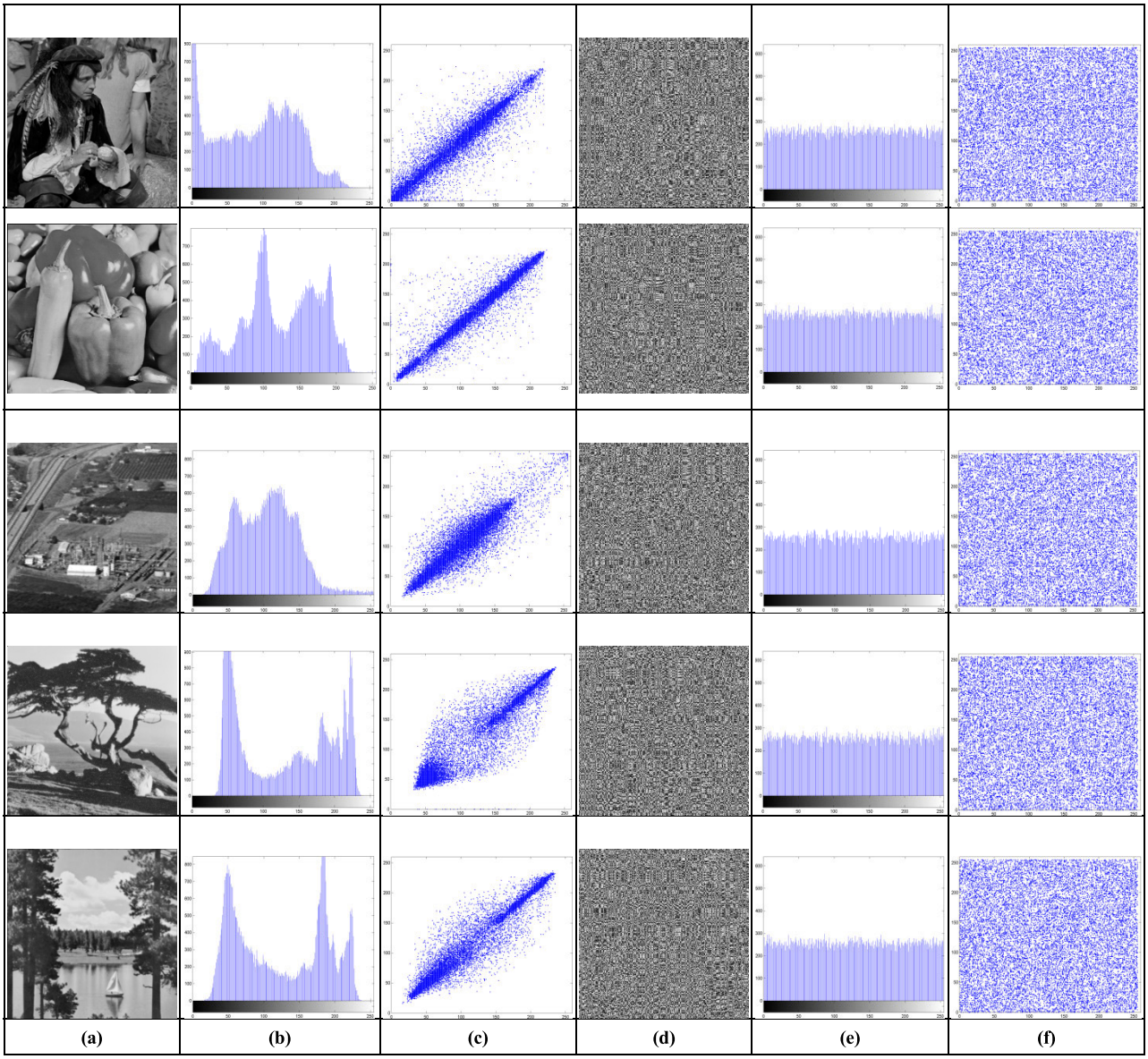

FIGURE 3. *(Continued)* **Visuals of plain and encrypted images for histogram and pixels correlation performance for S-box based image encryption; 1st column (a) shows plain-images; 2nd column (b) shows histograms of plain-images; 3rd column (c) shows vertically adjacent pixels correlation in plain-images; 4th column (d) shows encrypted-images using S-box based encryption; 5th column (e) shows histograms of encrypted-images; and 6th column (f) shows vertically adjacent pixels correlation in encrypted-images.**

G. FIXED POINTS

In cryptographic ciphers that utilize S-boxes in their working, the presence of one or more fixed points (e.g. $S(x) = x$) seems an exploitable feebleness which can assist the invaders to reach the plaintext data. Consequently, an S-box designer takes care of that any fixed point (FP) should not be there in the respective S-box [53]. Our projected S-box doesn't have any fixed point and meets fixed point analysis (FPA) criterion graciously. Moreover, a comparison using FPA with other current and relevant S-boxes is given in Table 9. This analysis reveals that several of these S-boxes have different number of fixed points making them a weaker choice for cryptosystem.

H. COMPUTATIONAL LABOR

To observe the efficiency of the proposed S-box method, its simulation is done on Windows 8 having 4GB RAM and Intel core i7 CPU which operates at 2.2 GHz using Visual C#. Along with it, AES S-box generation based on $GF(2^8)$ was simulated using Look-Up Table (LUT) approach and Extended Euclidean Algorithm (EEA). Efficiency of the proposed technique was observed in two phases that include initial S-box and final S-box which employs heuristic evolution strategy to enhance the cryptographic strength of the initial S-box. A comparison of computational time of these observations is given in Table 10.

TABLE 9. Performance Comparison of LP, DP, and fps of Different S-boxes.

S-box Method	LP	DP	FPs
[19]	0.1406	0.039	0
[52]	0.1328	0.031	0
[53]	0.1484	0.047	1
[54]	0.137	0.039	0
[55]	0.113	0.031	2
[56]	0.1328	0.055	0
[57]	0.139	0.039	0
[58]	0.1328	0.039	0
[59]	0.125	0.047	0
[60]	0.1328	0.039	1
[61]	0.125	0.031	1
[62]	0.125	0.039	0
[63]	0.141	0.047	1
[64]	0.109	0.039	1
[65]	0.1406	0.039	1
[66]	0.125	0.039	2
[67]	0.141	0.047	1
Proposed	**0.125**	**0.039**	**0**

TABLE 10. S-Box generation time (seconds) of AES method based on GF(2^8) and proposed method.

AES S-Box		Proposed method	
LUT	EEA	Initial S-Box	Final S-Box
0.160	0.413	0.002	307

It can be seen that initial S-box generation time is quite encouraging as compared to that of AES approaches. However, final S-box generation time for proposed technique is a bit on higher side. Heuristic approaches of evolving S-boxes have merits over the randomly generated S-boxes methods on the ground of cryptographic strengths. A random S-box generation method doesn't guarantee an S-box with good cryptographic features. However, with Heuristic evolution strategy, one can generate S-boxes with strong security features. Obviously, this evolution process takes more time compared to any static S-box method or random S-box generation method. The proposed method involves key-dependent robust S-box generation with the help of Heuristic evolution strategy. Heuristic evolution step used for final S-box has the significant contribution in the generation of strong and robust S-boxes in the proposed technique. As the protection of user's data is of the utmost importance and concern, this security aspect should not be compromised considering modern day's CPU speed.

TABLE 11. Chi-square performance for S-box based image encryption.

Image	Plain	Encrypted
Lena	39667.8	266.16
Baboon	55604.8	241.14
Cameraman	110973.3	234.84
Airplane	178403.2	246.66
Barbara	29671.09	296.71
Bridge	27572.10	249.41
Fishing Boat	100752.6	244.29
Man	37038.6	265.48
Peppers	36777.5	230.5
Plant	50326.4	304.16
Tree	66009.6	287.94
Sailboat	48876.7	248.21
Average	**65139.47**	**259.625**

IV. APPLICATION OF S-BOX FOR IMAGE SECURITY

The proposed S-box given in Table 2 is applied to encrypt digital images to gauge the suitability of S-box for image security applications. We apply the anticipated S-box to encrypt the pixels of pending digital plain-image by performing the double substitution operation on each pixel of the image. Firstly, the pixels are substituted nonlinearly using the proposed S-box in forward direction and same process is operated in the backward direction to obtain rich encryption effect in the encrypted content. In what follows, we presented and discussed different performance analyses to validate the excellent encryption quality of the proposed S-box.

A. PIXELS DISTRIBUTION ANALYSIS

A histogram represents the graphical view of image pixels' intensities distribution. Evenly distributed pixels indicate an equal probability of intensity in each interval. A plain image is expected to display pixel intensity distribution in a related manner. While, on the other hand, an encrypted image must have a uniform and flat histogram. Then only, a cipher-only attack is not possible for an attacker by analyzing the pixel distribution pattern only. The first column and fourth column of Figure 3 shows the considered benchmark plain-images, and their corresponding encrypted

TABLE 12. MLC performance scores of S-box based image encryption for benchmark images dataset.

Image	P / E	Entropy	Correlation	Contrast	Energy	Homogeneity
Lena	Plain	7.4439	0.9025	0.4483	0.1127	0.8622
	Encrypted	7.9971	0.0203	10.2846	0.0157	0.3856
Baboon	Plain	7.2649	0.7983	0.6326	0.0944	0.7821
	Encrypted	7.9973	0.0025	10.5517	0.0156	0.3888
Cameraman	Plain	7.0097	0.9227	0.5872	0.1805	0.8952
	Encrypted	7.9974	0.0278	10.8015	0.0157	0.3844
Airplane	Plain	6.7075	0.9172	0.3301	0.3618	0.9063
	Encrypted	7.9973	-0.0058	10.5735	0.0157	0.3886
Barbara	Plain	7.6309	0.8246	1.04568	0.0644	0.7696
	Encrypted	7.9967	-0.0138	10.6646	0.0156	0.3863
Bridge	Plain	7.6686	0.9077	0.5231	0.0793	0.8119
	Encrypted	7.9972	-0.0062	10.5261	0.0156	0.3877
Fishing Boat	Plain	7.1583	0.9048	0.3963	0.2023	0.8814
	Encrypted	7.9973	-0.0065	10.5591	0.0157	0.3882
Man	Plain	7.5360	0.9208	0.4743	0.1005	0.8505
	Encrypted	7.9971	0.0371	10.0766	0.0157	0.4016
Peppers	Plain	7.5327	0.9312	0.3849	0.1096	0.8881
	Encrypted	7.9975	-0.0045	10.5539	0.0156	0.3848
Plant	Plain	7.3424	0.9119	0.3198	0.1235	0.8654
	Encrypted	7.9966	0.0011	10.4948	0.0156	0.3878
Tree	Plain	7.3107	0.9573	0.3862	0.1298	0.8697
	Encrypted	7.9968	0.0170	10.4132	0.0157	0.3963
Sailboat	Plain	7.4493	0.9552	0.3543	0.1249	0.8769
	Encrypted	7.9973	0.0094	10.4244	0.0157	0.3921
Average	**Plain**	**7.3379**	**0.90452**	**0.49023**	**0.14031**	**0.85494**
	Encrypted	**7.9971**	**0.01266**	**10.49367**	**0.01566**	**0.38935**

images using S-box image encryption scheme. It is quite evident that the encrypted images have excellent visual encryption effect. The histograms of the two set of images (plain-images and encrypted images) are depicted in 2nd column and 5th column of Figure 3. The histograms of encrypted images are almost uniform and flat. Whereas, the histograms of plain-images have many peaks which are indicating uneven distribution of pixels. It is quite tedious to deduce the image information by seeing the histogram of an encrypted image as it exhibits a uniform pixel distribution throughout the plot.

There exists a quantitative measurement to analyze the pixel distribution in an image. The chi-square test used for pixel distribution analysis which is implemented using the following formula:

$$\chi^2 = \sum \frac{(P_i - E_i)^2}{E_i} \tag{4}$$

where, Pi represents the actual occurrence of pixel value i and the expected pixel frequency is denoted by Ei. For a uniformly distributed image, it is expected to have a chi-square test value less than the standard value 293.2478 at a significance level of 0.05 [40]. The calculated test value for strongly connected pixels (of plain-images), as well as randomly distributed pixels (in encrypted-images), are shown in Table 11. The average chi-square statistic score over all twelve encrypted images is 259.625 which quite close to the expected value and very far away from 65139.47 (the average over all plain-images).

The obtained result infers that the encrypted image pixels are uniformly distributed, which verifies that the proposed method can resist the statistical attack well.

B. MAJORITY LOGIC CRITERIA

The MLC stands for majority logic criterion [44], [72], [73] is a set of five different significant statistics such as: *entropy*, *correlation, contrast*, *energy*, and *homogeneity* which are mathematically expressed in Eq. (5)-(9). The examination of the encryption effect induced by substitution boxes during encryption scheme is the sole aim of MLC tool. The digital standard images are encrypted using proposed substitution-box to validate their practicable adoption for secure multimedia data applications. The plain-image is transformed during the progression of encryption and such alterations decide the proficiency of the proposed method. In correlation, the resemblance among the adjacent pixels in images is ascertained. Note that, the lesser correlation score diminishes the chances of deciphering original image. The value of contrast offers the calculation of damage of brightness in plain-images. A big score of contrast is always prerequisite for the benign encryption scheme. The randomness content in the encrypted image is assessed through the entropy analysis. The energy and homogeneity values depict the features of the encrypted image. The proposed substitution-box is employed to perform the encryption of some standard plain images and MLC tests are executed to know the performance scores.

$$Entropy : H(x) = \sum_{i} p(x_i) log_2 \left(\frac{1}{p(x_i)} \right) \tag{5}$$

$$Pixels\ Correlation : \gamma = \sum \frac{(i - \mu i)(j - \mu j)}{\sigma_i \sigma_j} \tag{6}$$

$$Energy : E = \sum p(i,j)^2 \tag{7}$$

$$Contrast : c = \sum |i - j|^2 p(i,j) \tag{8}$$

$$Homogeneity : h = \sum \frac{p(i,j)}{1 + |i - j|} \tag{9}$$

The obtained MLC results for plain-images and corresponding encrypted images are provided in Table 12. The simulation MLC results demonstrate an excellent encryption performance of S-box in encrypting the digital images for security applications.

C. MAD/MSE/PSNR/SSIM ANALYSIS

A mean absolute difference (MAD) and mean square error (MSE) tests are used to measure the encryption quality of an image cryptosystem. The tests are executed by calculating the pixel difference between plain image P and encrypted image E as follows:

$$MAD = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} |E(i,j) - P(i,j)| \tag{10}$$

$$MSE = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} (P(i,j) - E(i,j))^2 \tag{11}$$

TABLE 13. MAD, MSE, PSNR and SSIM scores for proposed S-box based image encryption.

Image	MAD	MSE	PSNR	SSIM
Lena	72.93	7757.1	28.23	0.001597
Baboon	70.26	7038.2	27.61	0.000105
Cameraman	79.56	9447.1	28.18	0.000158
Airplane	82.64	10224.5	27.18	0.000860
Barbara	75.82	8508.56	28.13	0.001811
Bridge	75.63	8435.41	28.50	-0.00152
Fishing Boat	72.49	7604.17	28.45	-0.00214
Man	82.18	10137.2	27.32	0.00166
Peppers	74.78	8251.72	28.51	0.00180
Plant	73.23	7812.18	28.67	-0.00171
Tree	82.02	10071.35	27.48	0.000715
Sailboat	80.23	9595.34	27.58	0.00228
Average	**76.814**	**8740.24**	**27.987**	**0.00136**

A PSNR value is the result of the ratio between the maximum pixel intensity and the MSE value of the given images having bit depth L. It is calculated as:

$$PSNR = 20 log_{10} \left(\frac{(2^L - 1)}{\sqrt{MSE}} \right) db \tag{12}$$

whereas, the structural similarity index measurement (SSIM) is computed to analyze the perceived change in structural information. The SSIM value can be calculated as:

$$SSIM = \frac{(2\mu_P \mu_E + \alpha)(2\sigma_{PE} + \beta)}{(\mu_P^2 + \mu_E^2 + \alpha)(\sigma_P^2 + \sigma_E^2 + \beta)} \tag{13}$$

where, μ_P and μ_E are the average pixel values and σ_P, and σ_E are the variance of corresponding images P and E. Also, σ_{PE} represents the covariance between P and E, and α and β are two predefined constants used for stability. All tests have their expected value range to exhibit a secure cryptosystem. To prove the validity of the proposed method, all tests are conducted using the mentioned twelve standard test images and statistical results are listed in Table 13. The average scores MAD = 76.814, MSE = 8740.24, PSNR = 27.987, and SSIM = 0.00136 indicate that the proposed S-box based image encryption attains high performance by having all four test values close to their standard theoretical value.

The statistics such as MSE, PSNR and SSIM of our encryption approach are compared in Table 14 with the image encryption scheme given in [74]. The comparison shows that

TABLE 14. MAD, MSE, PSNR and SSIM scores for proposed S-box based image encryption.

Method	Image	MSE	PSNR	SSIM
Proposed	Lena	7757.1	28.23	0.001597
	Baboon	7038.2	27.61	0.000105
	Barbara	8508.56	28.13	0.001811
	Peppers	8251.72	28.51	0.00180
Ref. [74]	Lena	5148.7	11.013	0.0112
	Baboon	4944.42	11.189	0.0116
	Barbara	7369.17	9.456	0.013
	Peppers	7217.26	9.547	0.0135

TABLE 15. Encryption time, throughput, and NCB performance of encryption methods.

Encryption Method	Time (sec)	Throughput (KBps)	Number of cycles per Byte (Hz/B)
Proposed	**0.3117**	**205.33**	**11234.9**
Ref. [75]	3.0658	20.875	95439.25
Ref. [76]	7.32	8.743	323819.65

our encryption scheme has pretty good statistics compared to scores obtained in Ref. [74].

D. EFFICIENCY ANALYSIS

The efficiency of the method is checked by computing its encryption time (ET), encryption throughput (ETP) and the number of cycles per byte (NCB) which are expressed as:

$$ETP = \frac{Image\ size\ \ (bytes)}{Encryption\ time\ (sec)} \tag{14}$$

$$NCB = \frac{CPU\ \ speed\ \ (Hz)}{Encryption\ throughput\ \ (bytes)} \tag{15}$$

Table 15 provides encryption time, encryption throughput, and number of cycles per byte scores for *Lena* test images of size 256×256. The simulation of proposed S-box encryption is done on Windows 8 having 4GB RAM and Intel core i7 CPU which operates at 2.2 GHz. The proposed S-box based encryption process takes around 0.3117 seconds to perform complete encryption. It can be seen from the obtained and listed results that the proposed method is sufficiently fast which makes it quite suitable to use in real-time secure image applications.

V. CONCLUSION

This paper proposed a novel and simple cryptographic dynamic substitution-box construction method using some modular operations. An effective heuristic evolution strategy has been put forward which has the potential to improvise the input S-box on the basis of nonlinearity feature. The proposed S-box method involves a number of input parameters of integer in nature. With the proposed simple method, a large number of highly nonlinear and robust S-boxes can candidly be created by slight variations in parameters. A specimen S-box is formed and its critical recital analysis against standard S-box criteria has been performed. The performance analysis of S-box and its application to image security validate that the projected S-box has strong features and it is true candidature for incorporation in modern block ciphers.

REFERENCES

[1] C. Paar, J. Pelzl, and B. Preneel, *Understanding Cryptography*, 1st ed. Berlin, Germany: Springer, 2010.

[2] A. Kadhim and S. Khalaf, "New approach for security chatting in real time," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 4, no. 3, pp. 30–36, 2015.

[3] 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.

[4] 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.

[5] A. Belazi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Selective image encryption scheme based on DWT, AES S-box and chaotic permutation," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, Art. no. 606610.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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)*, Langkawi Island, Malaysia, Sep. 2014, pp. 2–4.

[11] 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. (ICDIPC)*, Sierre, Switzerland, Oct. 2015, pp. 7–9.

[12] J. M. Hassan and F. A. Kadhim, "New S-box transformation based on chaotic system for image encryption," in *Proc. Int. Conf. Eng. Technol. Appl.*, Najaf, Iraq, Sep. 2020.

[13] S. Farwa, T. Shah, and L. Idrees, "A highly nonlinear S-box based on a fractional linear transformation," *SpringerPlus*, vol. 5, no. 1, Dec. 2016, Art. no. 1658.

[14] 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.

[15] A. Altaleb, M. S. Saeed, I. Hussain, and M. Aslam, "An algorithm for the construction of substitution box for block ciphers based on projective general linear group," *AIP Adv.*, vol. 7, no. 3, Mar. 2017, Art. no. 035116.

[16] M. Sarfraz, I. Hussain, and F. Ali, "Construction of S-box based on Mobius transformation and increasing its confusion creating ability through invertible function," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 2, pp. 187–199, 2016.
[17] 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.
[18] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019.
[19] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020.
[20] F. A. Kadhim, G. H. A. Majeed, and R. S. Ali, "Proposal new S-box depending on DNA computing and mathematical operations," in *Proc. Int. Conf. Multidisciplinary IT Commun. Sci. Appl.*, Baghdad, Iraq, May 2016, pp. 1–6.
[21] 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.
[22] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with DNA binary strands," *Biosystems*, vol. 57, no. 1, pp. 13–22, Jun. 2000.
[23] N. H. UbaidurRahman, C. Balamurugan, and R. Mariappan, "A novel DNA computing based encryption and decryption algorithm," *Procedia Comput. Sci.*, vol. 46, pp. 463–475, Jan. 2015.
[24] B. B. Raj, 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.
[25] H. Shaw, "A cryptographic system based upon the principles of gene expression," *Cryptography*, vol. 1, no. 3, p. 21, Nov. 2017.
[26] C.-M. Ou, "Design of block ciphers by simple chaotic functions," *IEEE Comput. Intell. Mag.*, vol. 3, no. 2, pp. 54–59, May 2008.
[27] S. Garg and D. Upadhyay, "S-box design approaches: Critical analysis and future directions," *Int. J. Adv. Res. Comput. Sci. Electron. Eng.*, vol. 2, no. 4, pp. 426–430, 2013.
[28] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 2, pp. 163–169, Feb. 2001.
[29] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3317–3326, Aug. 2019.
[30] 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.*, Delhi, India, Feb. 2014, pp. 255–258.
[31] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, Mar. 2017.
[32] A. A. A. EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019.
[33] 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.
[34] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons Fractals*, vol. 58, pp. 16–21, Jan. 2014.
[35] 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.
[36] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018.
[37] B. R. Gangadari and S. Rafi 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.
[38] 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.
[39] 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.
[40] 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.
[41] 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.
[42] 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.
[43] 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.
[44] 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.
[45] 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.
[46] 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-Tech.*, vol. 3, pp. 17–26, Jan. 2013.
[47] 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.
[48] 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.
[49] 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, 2013.
[50] M. S. M. Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-Haq, S. N. M. Shah, M. Rehman, and W. Ahmad, "Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices," *IEEE Access*, vol. 8, pp. 35682–35695, 2020.
[51] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Amsterdam, The Netherlands: Elsevier, 2009.
[52] 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.
[53] 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.
[54] Z. B. 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.
[55] 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.
[56] 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.
[57] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dyn.*, vol. 99, no. 4, pp. 3041–3064, Mar. 2020.
[58] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dyn.*, vol. 100, no. 1, pp. 699–711, Mar. 2020.
[59] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-box based on chaotic map and backtracking," *App. Math. Comp.*, vol. 376, pp. 1–11, Jul. 2020.
[60] 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.
[61] I. Hussain, T. Shah, M. A. Gondal, and W. A. Khan, "Construction of cryptographically strong 8×8 S-boxes," *World Appl. Sci. J.*, vol. 13, no. 11, pp. 2389–2395, 2011.
[62] 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(2^8))," *IEEE Access*, vol. 8, pp. 136736–136749, 2020.
[63] 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, Mar. 2020.

[64] H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, "A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7333–7350, Feb. 2021.
[65] Y. Tian and Z. Lu, "Chaotic S-box: Intertwining logistic map and bacterial foraging optimization," *Math. Problems Eng.*, vol. 2017, pp. 1–11, Nov. 2017.
[66] N. Siddiqui, A. Naseer, and M. Ehatisham-ul-Haq, "A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve," *Wireless Pers. Commun.*, vol. 116, no. 4, pp. 3015–3030, Feb. 2021.
[67] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, "Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box," *Symmetry*, vol. 13, no. 129, pp. 1–20, 2021.
[68] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Tech.*, Santa Barbara, CA, USA, Aug. 1986, pp. 523–534.
[69] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT'93*. Lofthus, Norway: Springer, 1994.
[70] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.
[71] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. A. EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci.*, vol. 515, pp. 191–217, Apr. 2020.
[72] N. Bibi, S. Farwa, N. Muhammad, A. Jahngir, and M. Usman, "Correction: A novel encryption scheme for high-contrast image data in the Fresnelet domain," *PLoS ONE*, vol. 13, no. 4, Apr. 2018, Art. no. e0196781.
[73] S. Farwa, N. Bibi, and N. Muhammad, "An efficient image encryption scheme using Fresnelet transform and elliptic curve based scrambling," *Multimedia Tools Appl.*, vol. 79, nos. 37–38, pp. 28225–28238, Oct. 2020.
[74] A. Kadhim, "New image encryption based on pixel mixing and generating chaos system," *Al-Qadisiyah J. Pure Sci.*, vol. 25, no. 4, pp. 1–14, 2020.
[75] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Jan. 2017.
[76] A. M. Ayoup, A. H. Hussein, and M. A. Attia, "Efficient selective image encryption," *Multimedia Tools Appl.*, vol. 75, no. 24, pp. 17171–17186, Dec. 2016.

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 a Program Advisor for B.S. (IT) Program and a member of many academic bodies. He has been an Active Member of Higher Education Commission (HEC) National Curriculum Revision Committee (NCRC), Pakistan. He has more than 23 years of qualitative experience in teaching. He possesses quality monitoring and maintaining capabilities along with the strong interpersonal, leadership, and team management skills. He has been an Active Member of Faculty Board of studies for Punjab University College of Information Technology (PUCIT) and Virtual University of Pakistan. He is vigorous in academic research. His research interests include information security, programming languages, algorithm design, enterprise architecture, technology management, IT infrastructure, and blockchain. He is serving as an efficient and effective reviewer in several reputed International research journals of high impact factor in the domain of information security.

ABDULLAH M. ILIYASU (Senior Member, IEEE) received the M.E., Ph.D., and Dr.Eng. degrees in computational intelligence and intelligent systems engineering from the Tokyo Institute of Technology (Tokyo Tech.), Tokyo, Japan. Concurrently, he is a Research Faculty with the School of Computing, Tokyo Tech, and also the Principal Investigator and the Team Leader of the Advanced Computational Intelligence and Intelligent Systems Engineering (ACIISE) Research Group, College of Engineering, Prince Sattam Bin Abdulaziz University (PSAU), Saudi Arabia. He is also a Professor with the School of Computer Science and Technology, Changchun University of Science and Technology, China. In addition to being among the pioneers of research in the emerging Quantum Image Processing (QIP) Subdiscipline, he has to his credit more than 120 publications traversing the areas of computational intelligence, quantum cybernetics, quantum image processing, quantum machine learning, cyber and information security, hybrid intelligent systems, the Internet of Things, 4IR, health informatics, and electronics systems reliability. He is the Managing Editor of the Fuji Technology Press, Japan. He is a member of editorial board of many journals, including *Journal of Advanced Computational Intelligence and Intelligent Informatics* (JACIII), *Quantum Reports* journal, *International Journal of Electrical and Computer Engineering* (IJECE), and the *Journal of Medical Imaging and Health Informatics* (JMIHI). He is also an Associate Editor in many other journals, including IEEE Access, *Telekomnika*, and *Information Sciences*.

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he has worked with the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia. He has published over 80 research papers in international reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. He has more than 1300 citations of his research works with an H-index of 22. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has served as a reviewer and the technical program committee member of many international conferences. He has also served as a referee of some renowned journals, such as *Signal Processing*, *Information Sciences*, *Journal of Information Security and Applications*, IEEE Access, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on Nanobioscience, *Wireless Personal Communications*, *Neural Computing and Applications*, *International Journal of Bifurcation and Chaos*, *Optik*, *Optics and Laser Technology*, *Neurocomputing*, *IET Information Security*, *IET Image Processing*, *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*, *Concurrency and Computation*, and *ETRI* journal.

MIAN MUHAMMAD UMAR SHABAN received the B.S. degree in computer science from Government College University (GCU), Faisalabad, Pakistan, and the M.S. degree in computer science from the University of Management and Technology (UMT), Lahore, Pakistan. His research interests include information security, ethical hacking, cryptanalysis, and blockchain.

MUHAMMAD JUNAID ARSHAD is currently working as an Associate Professor with the University of Engineering and Technology (UET), Lahore, Pakistan. He is also a HEC Approved Ph.D. Supervisor and very much active in research. He is working on three funded research proposals approved by HEC and UET, Lahore. He is an Advisor with Punjab Public Service Commission and Federal Public Service Commission. He has supervised more than 50 BS Research Projects, 60 M.Sc./M.Phil. theses, and currently supervising five Ph.D. scholars. He has more than 50 national and international publications to his credit. His research interests include protocols and algorithms for heterogeneous networks, data centre networks, multi-homed networks focusing on performance, computer architecture, mobile ad-hoc networks, simulation and modelling, information security, and cloud computing. He is a member of IEEE Computer Society and IEEE Communications Society Korea Information and Communications Society (KICS). He is serving as an editor/reviewer in many reputed International research journals.

HUSSAM S. ALHADAWI received the M.Sc. degree in information technology from Universiti Tun Abdul Razak (UNIRAZAK), in 2012, and the Ph.D. degree from Universiti Malaysia Pahang (UMP), Malaysia, in 2018. He is currently a Senior Lecturer and a Senior Researcher in the field of computer engineering with Dijlah University College. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, and optimization techniques. He has served as a reviewer and a technical program committee member of many international conferences. He also served as referee of some renowned journals, such as *Physica B* and IEEE Access.

AHMED A. ABD EL-LATIF received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2005 and 2010, respectively, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology (H.I.T), Harbin, China, in 2013. He is currently an Associate Professor of computer science with Menoufia University and School of Information Technology and Computer Science, Nile University, Egypt. He is authored or coauthored of more than 130 papers, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, and book chapters. His research interests include multimedia content encryption, secure wireless communication, the IoT, applied cryptanalysis, perceptual cryptography, secret media sharing, information hiding, biometrics, forensic analysis in digital images, and quantum information processing. He received many awards, such as the State Encouragement Award in Engineering Sciences 2016, the Arab Republic of Egypt, the Best Ph.D. Student Award from the Harbin Institute of Technology, China, in 2013, the Young Scientific Award from Menoufia University, in 2014. He is a fellow with the Academy of Scientific Research and Technology, Egypt. He has many collaborative scientific activities with international teams in different research projects. Furthermore, he has been reviewing papers for more than 115 International journals, including *IEEE Communications Magazine*, IEEE Internet of Things Journal, *Information Sciences*, IEEE Transactions on Network and Service Management, IEEE Transactions on Services Computing, *Scientific Reports Nature*, *Journal of Network and Computer Applications*, *Signal processing*, *Cryptologia*, *Journal of Network and Systems Management*, *Visual Communication and Image Representation*, *Neurocomputing*, and *Future Generation Computer Systems*. He is an Associate Editor of *Journal of Cyber Security and Mobility*.