IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 September 2022, accepted 22 October 2022, date of publication 28 October 2022, date of current version 9 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3218062

RESEARCH ARTICLE

A Strong Hybrid S-Box Scheme Based on Chaos, 2D Cellular Automata and Algebraic Structure

AMIRUL HAQUE[1], TABARAK ALI ABDULHUSSEIN[2], MUSHEER AHMAD[1], MAYADAH WAHEED FALAH[3], AND AHMED A. ABD EL-LATIF[4,5], (Senior Member, IEEE)

[1]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[2]Department of Accounting, College of Administrative and Financial Sciences, Imam Ja'afar Al-Sadiq University, Baghdad 10001, Iraq
[3]Building and Construction Engineering Technology Department, Al-Mustaqbal University College, Hillah 51001, Iraq
[4]EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[5]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Kom, Menoufia 32511, Egypt

Corresponding author: Ahmed A. Abd El-Latif (aabdellatif@psu.edu.sa)

This work was supported by the EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia.

ABSTRACT Substitution-boxes are the main deciding components in symmetric-key cryptosystems for resisting many cryptanalytic attacks. It has been a challenging task for the designers to construct strong S-box which satisfies multiple cryptographic properties simultaneously. A number of S-box studies have been investigated in literature; but, the generated S-box found to exhibit one single property with good score. This paper proposes a novel creation of S-boxes which possess excellent scores of multiple cryptographic properties instead of only one property. The suggested hybrid S-box method explores the science of two-dimensional cellular automata theory, discrete chaotic maps, and algebraic group structure. The proposed anticipated 8×8 S-box holds excellent security performance features such as: minimum nonlinearity as high as 110, no fixed points, satisfaction of strict avalanche and bits independence criterions, differential uniformity as low as 6, linear approximation probability as low as 0.0703, and auto-correlation function (absolute indicator) of 40. The performance comparison indicates the proposed S-box has superior features, greater inherent security and robustness strength than many available state of the art S-box methods.

INDEX TERMS Substitution-box, 2D cellular automata, discrete chaotic maps, symmetric cryptography, algebraic group.

I. INTRODUCTION

Due to the rapid progress in online communication and data transferring, the importance of security mechanisms is increasing manifold. It is of utmost importance to secure the important data in transit, across networks. The cryptography algorithms are employed for the same purpose, as they provide the required security over the insecure channels of network [1]. Symmetric cryptosystems have been the most critical of cryptography to realize security mechanisms for last many decades. It was only in 1949 that Shannon introduces the notion of modern cryptography. There are various block cryptosystems namely Data Encryption Standard, BLOWFISH, and Advanced Encryption Standard, etc. and these rely on the two important concepts of *Confusion* and *Diffusion* introduced by Shannon [2]. Making the association between the ciphertext and the key as convoluted and difficult as possible is referred to be confusing, and the goal is to prevent anyone from understanding the key by simply getting the ciphertext. Diffusion is the procedure of decreasing the influence of a single plaintext piece on several encoded text in order to mask the plaintext's statistical redundancy. To create an encrypted text, a block cipher iteratively operates the process to retrieve multiple effects of confusion and diffusion properties. The most famous block ciphers in the field to employ this method are Data Encryption Standard (DES), BLOWFISH, Advanced Encryption Standard (AES), GOST, etc. The most potent attacks against these block encryption algorithms are linear and differential cryptanalyses [3]. The primary goal of a differential attack is to extract patterns from

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

encoded data, and to do this, the assailant uses a certain set of inputs to track changes in output. Goal of a linear assault is to identify a linear relationship between plain text, cipher text, and the accompanying keys. The confusion component is entirely accountable for furnishing resistance to these two attacks as well as for creating a randomized association between the ciphertext and the key [4]. Substitution-box (S-box), the block cipher's confusion mechanism, converts k input bits into m output bits. The dynamic components of block ciphers that cause confusion by making nonlinear transformations of inputs into outputs are the S-boxes. A cryptosystem must have S-box(es) that can produces great nonlinearity effect and robustness to related attacks [4], [5].

The success of the AES block cipher and its substitution box has been greatly aided by the development and enhancement of ideas devoted to the creation of S-boxes [6]. They involve methods of algebraic tactics, optimization, the chaotic function as well as structures, and other techniques, and they are stable. The creation of efficient S-boxes with varying sizes is a challenging subject. One of the primary motives for this issue is the size of the enormously large search space. In order to establish a reliable frame of an S-box that can yield useful S-boxes, meta-heuristic optimization approaches have been developed in recent past [7]. S-boxes are the main building blocks of symmetric block ciphers to implement substitution process. For encryption methods to achieve the notion of complete security, S-boxes, are essential. An S-box usually receives m input bits, and transform inputs into n output bits, is said to known as an $m \times n$ S-box is the transformation function of bits $S(x) : B^m \rightarrow B^n$, where $B = [0, 1]^m$. It transforms nonlinearly each m-bits binary input values 2^m to the n-bits binary output values 2^n. It can be actualized as a look-up table with 2^m words of n-bits each, where m may or may not be equal to n. The case when $m = n$ leads to a bijective S-box and it acts as a one-to-one mapping from set of input streams to set of output streams. The bijective S-boxes correspond to a permutation sequence of $[0, 1, 2, .., 2^n - 1]$. Consequently, they have a theoretical state space of $(2^n)!$ which is more than 10^{506} for 8×8 S-boxes [8].

Literature reveals that chaotic systems have been extensively explored to generate the S-boxes. With an aim to create safe S-boxes that can withstand linear, differential, and algebraic attacks, the schemes based on chaotic maps have been demonstrated. Using a Lorenz chaotic system, Ozkaynak and Ozer [9] produced secure S-boxes. Using chaotic maps and a genetic algorithm, Wang et al. [10] suggested an S-box scheme. A chaotic map iterative S-box generator was proposed by Yin et al. [11]. S-boxes were produced by Lambi'c [12] using an enhanced 1-dimensional discrete chaotic map. S-boxes were produced by Ozkaynak et al. [13] using a fractional-order chaotic Chen system. Dynamic S-boxes were designed by Cassal-Quiroga and Campos-Canton [14] using an enhanced logistic map. Tanyildizi and Ozkaynak [15] created S-boxes with respectable algebraic and differential features using an optimized one-dimensional chaotic map. El-Latif et al. [16] created a cryptographically robust S-box using quantum walks and chaos induction. But, the sole use of chaotic systems for their generation involves some demerits. The chaos based S-box designs have the shortcomings such as: (1) they are computationally intensive making the key-dependent S-box generation a time-consuming process, and (2) most of them involved continuous-time systems which suffers from precision errors when digitized and a slight change in value drastically affect the future dynamics of such systems, and (3) they are also have complex hardware implementations. Hence, the researchers have been investigating different methods and alternatives to strengthen the S-boxes features, the techniques explored are: algebraic theory such as group and rings [17], cellular automata [18], cubic fractional transformation [19], and elliptic curve [20]. An S-box is deliberate in [21] with the help of LFT (linear fractional transformation) and a Gaussian distribution. For generating the S-box, the Box-Muller transform, polarisation decision, and central limit algorithm are applied. The authors of [8] presented a technique for producing nonlinear $n \times n$ S-boxes (for $n < 8$). Basha et al. explored the DNA computing and Bent function concepts to yield S-boxes for image encryption application in [22]. Farhan et al. applied the features of RNA computing approach to generate multi-S-boxes in [23]. However, the majority of S-box designs do not produce findings that are statistically significant.

A number of significant attempts have been made by few researchers to apply different forms of elliptic curves to generate the S-box with less computational overheads. To this end, Azam et al. in [24], constructed efficient S-boxes based on the class of Mordell elliptic curves (MEC) over prime fields. Ibrahim and Abbas in [25] presented an elegant construction method for strong S-box design with the help of key-permuted finite elliptic curves which is suited for real-time applications. In [26], authors made use of ordered Mordell elliptic curve to generate the efficient S-boxes with less time and space complexities for quicker generation operation. Hayat and Azam in [27], suggested an S-box construction approach for use in image encryption application. Their scheme applied exhaustive approach to generate points of finite elliptic curve which are utilized to obtain a randomized S-box. In [28], an image encryption scheme is suggested using quasi-resonant triads which are utilized for PRNG design to compute MEC meant for S-box construction. The constructed PRNG and S-box are applied to perform the diffusion and confusion during encryption process. Subsequently, the development of a substitution box possessing excellent cryptographic characteristic is the most important part of any cryptographic system. The cryptographers have been investigating different concepts in order to achieve following performance objectives while designing 8×8 S-boxes. This paper put forward a novel S-box creation scheme which is hybrid in the sense that it explores the features of 2-D cellular automata, chaos theory, and algebraic theory. The initial S-box is obtained with the help of discrete chaotic maps and working of cellular automata. The performance augmentation is carried out by applying the action

of experimentally designed a specific algebraic group whose action results into strong S-box. The constructed S-box has excellent security and robustness features as evident by the performance comparison analysis.

In what follows, we prepared the different sections as follows: Section II provides some insight of cellular automata concepts that are relevant to the proposed S-box generation work. The proposed scheme of S-box design procedure using 2-D cellular automata, two discrete chaotic maps, and algebraic group structure is pronounced in Section III. The security assessment and comparison analysis of the projected S-box is done in Section IV. The work is concluded in Section V.

II. CELLULAR AUTOMATA

The mathematical model of Cellular Automata (CA) was probed by John von Neumann and his collaborator Stanisław Ulam [29]. It is a simple system wherein the states, space, and the time instances are discrete. The structure of the CA is regular, it has feature of parallelism, and cells interact locally to imitate random-like phenomenon. The structure of the cellular automata is investigated as the distinct mesh section of cells where value can be either 0 (off) or 1(on) for every cell. Cellular automata also can be seen as grid or network of cells or as arrays of cells where each cell stores single information bit. Every cell of automata adjusted autonomously by advancing the distinct time stamp. The use of the progress function to each cell in the network prompts the accompanying 'age' for the framework. In spite of the fact that these functions rely on their state of input, but each cell accompany the similar guideline or *Rule* in terms of cellular automata to determine the transition to next state. An underlying situation ($t = 0$) is chosen by allotting a situation for every cell. Another age is made (propelling t by 1), as indicated by some settled *Rule* (for the most part, a function) that decides the new situation or state of every cell as far as the present condition of the cell and the conditions of the cells in its neighborhood. Regularly, the administering *Rule* for refreshing the situation of cells is similar for every cell and not changing after some time and is connected to the entire lattice.

Formally, CA can be defined as four tuples: CA = (D, S, N, F),

where,

D = dimension of the cellular automata

S = set of all the possible states

N = neighborhood vector or number of neighbors

F = transition function which is local rule by nature

Let n denote the cells counting in cellular automata of any dimension. Then the CA state can be mathematically shown as X_t. Where, $X_t = \{S_0(t), S_1(t), \ldots\ldots\ldots\ldots\ldots, S_{n-1}(t)\}$. Here $S_i(t)$ denotes the state of i^{th} cell at t^{th} instant of time. In similar manner at time $(t+1)^{th}$ instant state of the automata can be denoted as $X_{t+1} = \{S_0(t+1), S_1(t+1), \ldots\ldots\ldots\ldots\ldots, S_{n-1}(t+1)\}$, where $S_i(t+1) = F[S_{i-1}(t), S_i(t), S_{i+1)}(t)]$, the numbers of neighbors depends on the neighbor radius. Here only one neighbor before the i^{th} cell and one neighbor after i^{th} cell has been considered, and this is called neighbor with radius 1. The state of the automata:

$$X_t = \{S_0(t), S_1(t), \ldots\ldots\ldots\ldots\ldots, S_{n-1}(t)\}$$
$$X_{t+1} = \{S_0(t+1), S_1(t+1), \ldots\ldots\ldots\ldots\ldots, S_{n-1}(t+1)\}$$
$$S_i(t+1) = F[S_{i-1}(t), S_i(t), S_{i+1)}(t)]$$

where,

X_t = automata state at time instant t

X_{t+1} = automata state at time instant $(t+1)$

$S_i(t) = i^{th}$ cell state at time stamp t

$S_i(t+1) = i^{th}$ cell state at time instant $(t+1)$

One-dimensional CA is the elementary case of the cellular automata. It can be simply represented as one-dimensional array of cells. Assume an automata of length N, and the radius $r = 1$. Then, the neighborhood of any i^{th} cell can be defined as $n_i = 2r + 1$ cells, counting the i^{th} cell itself. Considering a limited size CA and with closely wrapped boundary, then a circular grid is formed. For a 1-D CA of length N and $r = 1$, the following statistics hold:

- Neighborhood Cell $n = 3$
- Length of the rule $L = 8$ $(=2^n)$
- Total number of rules $= 256$ $(=2^L)$

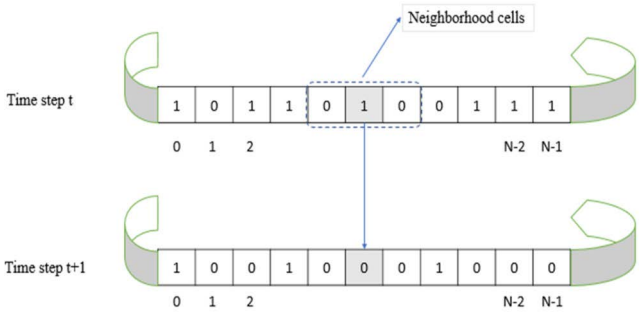

FIGURE 1. 1-D CA cell updating according to rule-194.

If cell state value is represented as a state table (see Table 1), then decimal value to the binary number is termed as *Rule* of the CA. Three bits binary number can have 8 possible arrangements and each arrangement can have either 0 or 1 possible value at next step. This will provide the rule for updating the cell of automata.

TABLE 1. Generation of rule for 1-D CA.

Neighborhood State	000	001	010	011	100	101	110	111	Rule↓
Next State	1	1	0	0	0	0	1	0	194
Next State	0	1	0	1	1	0	1	0	90

A two-dimensional CA is represented as a 2D lattice of cells. Each cell may depict finite states which are updated in discrete time instances as per the specified CA rule. In 2D CA, the next state automata cells value relies upon every

one of its neighbor's cells value around it in 2-D lattice. The significance of the 2D CA is evident from its usage in vast applications which include pattern testing, encryption methods design, image processing, bioinformatics, compression, intrusion detection systems, etc., [30]. The two-dimensional CA that includes an entire framework of cells with the information bit of every cell being refreshed by a rule that relies upon its neighbors in each of the four heading as shown in Figure 2. Von-Neumann technique is one of the generally utilized neighborhood definition techniques. Figure 2 represents the Von-Neumann neighbors of a green color cell, here considered cell is of color green and its neighbors are in shown in grey shade. Von Neumann defined the neighborhood [31] in horizontal and vertical direction only. Number of neighborhood cells may depend on neighborhoods radius r, but only that cell will be taken which present either in vertical or in horizontal direction to the updating cell. Neighborhood radius r can be any integer, $r = 1, 2$, and so on. Figure 3 demonstrates an example of 2-D CA of size $N \times N$. The cell filled with green color has value 1 at time stamp t. This cell value will be updating according to some rule (say 2361501363) and neighbors (shown in shades of blue). Similarly, all cell value will update and gives new state of CA at time stamp $t+1$. The values of cell will be like 11**0**10 which updated like 11**1**10 according to Rule 2361501363 as shown in Figure 4. For rule generation please refer to section III.C.

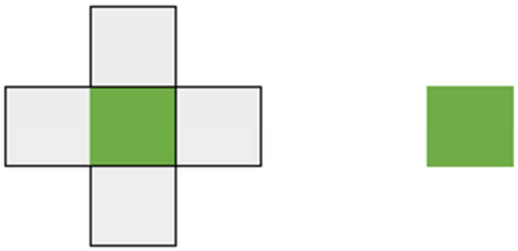

FIGURE 2. Basic cell representation for radius r = 1.

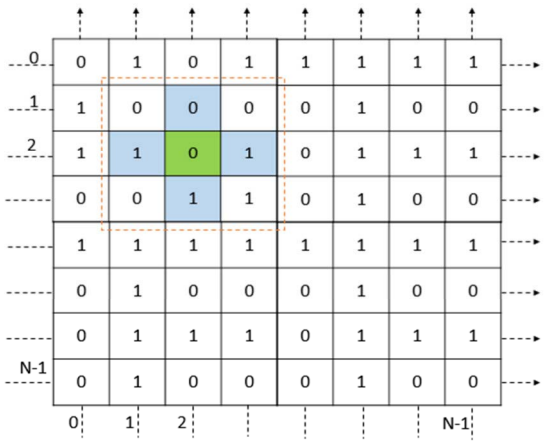

FIGURE 3. Demonstrative cellular automata of size N×N at time stamp t.

III. PROPOSED S-BOX SCHEME

The proposed scheme utilized 2-D cellular automata, discrete chaos, and algebraic group structure to design the S-box for excellent cryptographic properties. To start with good randomness throughout the automata, the two-dimensional CA is initialized with the help of PWLCM chaotic map. This randomly initialized 2-D CA cells will be updated later using rules of automata for specified count of iteration.

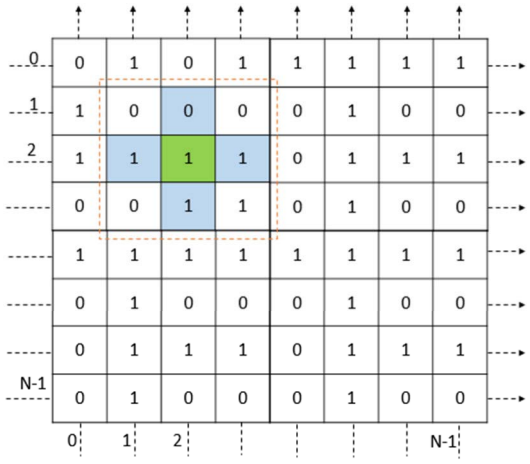

FIGURE 4. Demonstrative cellular automata of size N×N at time stamp t+1.

A. INITIALIZATION

The CA initialization is the first step to have a table, so that it could be changed later. Here, a simple system is used to define random function to get the initial value for lesser complexity and time efficient as well. Initialization would affect the result of the final S-box because all initials value will be replaced by the calculated value of defined sliding window value. In the suggested method, an 8×8 S-box is initialized using the system based function with random values. As a matter of the fact, the beginning value has vital impact on the optimization process. Keeping in mind the end goal to get automata with initial random values, it is important to begin with initial automata. To get pseudo random number with good randomness, there are many chaotic maps which can be used to do so. To initialize the two-dimensional automata PWLCM chaotic map is used. The PWLCM map is defined as follows.

$$x_{new} = \begin{cases} \frac{x}{p}, & if\ 0 < x < p \\ \frac{1-x}{1-p}, & else \end{cases}$$

where, $p = 0.49876$; $x = 0.12345$ be the initial setting for the map. The PWLCM shows chaotic behavior when parameters value lies inside the range (0, 0.5) and its beginning constraint selected inside the range (0, 1). We are initializing the 2-D automata using PWLCM dependent procedure. All entries e of automata will be in binary form i.e. either 0 or 1 using the following predefined condition.

$$e = \begin{cases} 0 & if\ x_{new} < 0.5 \\ 1 & if\ x_{new} \geq 0.5 \end{cases}$$

where, x if the chaotic variable generated from PWLCM map after iteration. The size of the two-dimensional automata S will be of $a \times a$,

Let

$$A = a \times a$$
$$a = 2^n + 3$$

where, a is size of row and column of the automata, and n is size of S-box i.e. $n \times n$.

B. DEFINING NEIGHBORHOOD CELLS USING VON NEUMANN TECHNIQUE

The Von-Neumann method is used to define the neighbors (see Figure 5) of any cell of our two-dimensional cellular automata. To define the rule number for updating the cell at next state at time instant $t + 1$, there should be some sequence, order and indices for each cell. The cell indices are defined in i and j, where i denotes the row number and j denotes the column number of cell located at (i, j). Below Figure 5 describes the over layout of the all neighbors of the cell (i, j) along with indices of neighbors of cell at (i, j).

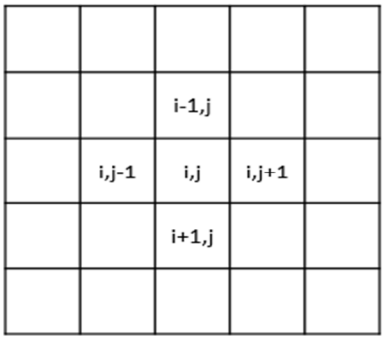

FIGURE 5. Neighbors of cell (i, j) as per Von-Neumann technique.

C. RULES GENERATION AND CELL UPDATING

Rule generation in CA is the most crucial part of cellular automata theory. Different rules can produce different output for the same initial value of cellular automata. The CA rules are responsible for increased power and beauty of cellular automata working. It is evident that there are at most 256 rules for 1-D CA. However, in 2D CA the cell (i, j) updates its value at time stamp $t + 1$, depending on the value of its previous state, its neighbor's previous state values, and the rule. These updates can be also seen as Boolean function dependent. A Boolean function is a mapping as $f : \{0, 1\}^n \rightarrow \{0, 1\}$. The cell state updates can be represented through the following local rule:

$$S^{t+1}_{[i,j]} = f(S^t_{[i,j-1]}, S^t_{[i+1,j]}, S^t_{[i,j]}, S^t_{[i,j+1]}, S^t_{[i-1,j]}) = 0 \text{ or } 1(\text{according to rule})$$

where, t: time stamp, $S^{t+1}_{[i,j]}$: state of cells $[i, j]$ value at time $t + 1$, $S^t_{[i,j]}$: state of cell $[i, j]$ value at time t. The local rule involves 5 variables, each one has 2 states thereby resulting $2^{2^5} = 2^{32} = 4294967296$ rules for 2-D CA with defined neighbors for radius $r = 1$. For $r = 1$, there are 5 cells including updating cell to decide the cell's next state value. Cell's value at time instant $t + 1$ will be decided by all five cells value at time instant t. There are 5! ways to arrange all the five cells. Arrangement used in proposed method is shown below in Figure 6.

Binary: 10001100110000011010011010110011

Rule number (decimal equivalent): 2361501363

If we put all five cells value at time instant t and correspondingly updating the cell (i, j) value at next time instant at $t + 1$ for each then 32 arrangements are possible per truth table. The decimal value of all 32 arrangements at time instant $t + 1$ provides the rule number. The representation shown in Figure 7 demonstrates such rule number calculation and generation.

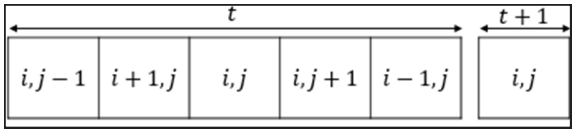

FIGURE 6. Bits (cell) arrangement.

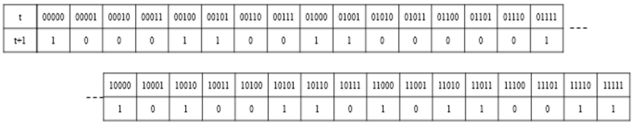

FIGURE 7. Rule generation example.

D. WINDOW SELECTION

The window selection operation enables the algorithm to decide the element of the anticipated S-box. Therefore, it is considered as one of the most main aspects of the proposed scheme. Through window selection operation, the value of S-box cell is calculated from two-dimensional automata binary cell values. Sliding window technique is used to fill the next cell value of S-box. To obtain the value in range (0, 256), we need 8-bits, hence a 2×4 window has been implemented to fulfill the 8-bits requirement.

Window initialized at position (0, 0) of automata to calculate the value of S-box cell and the value is appended to S-box table. To get next value, the window is shifted two positions in the right direction, and the calculated value is searched in S-box, if value is already present in S-box table then value is rejected else it is appended, and the window is further shifted. Suppose window has reached at right bottom corner of automata then update function is called to refresh the automata and remaining values are calculated in same fashion. In this way, it computes all required 256 unique values of 8×8 S-box table by sliding or shifting its position from left to right and top to down as per requirements.

The diagram shown in Figure 8 demonstrates the working of sliding window method used in the proposed scheme.

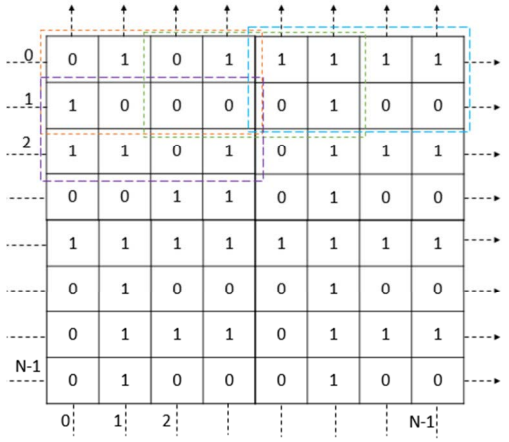

FIGURE 8. Sliding window operation.

E. S-BOX VALUE GENERATION FROM WINDOW

This section describes how decimal values are being calculated from 2 × 4 window. Rows of current window are taken in linear order i.e. row with index 1 is appended after the row with index 0, and then decimal equivalent number of 8-bits binary number is computed. Figure 9 demonstrates this diagrammatically, taking first window of Figure 8 as an example.

The suggested S-box scheme has several parts. In the first part, an empty S-box is generated. In second part, a 2-D cellular automaton is generated using PWLCM map. The automata iterated further to have excellent randomness by predefined number of times. In third part, a sliding window method is used to calculate the S-box values from 2-D automata, this calculated value is compared with pre-existing value of automata, if matched then window slides to calculate new unmatched value. If calculated value not matched, then value is appended in S-box. The working of proposed method is described below as:

1. Initializing the 8 × 8 S-box with random values using. These random values will be substituted by other calculated values of the S-box using 2-D cellular automata.
2. A chaotic map is used to initialize the 2-D CA table.
3. Function is defined to generate the desired output bit of the defined rule. This function produces the desired bit to update the next state of the cell.
4. Function is defined to update the initial automata to desired number of time. It is the function which iterates predefined number of time to update the 2-D CA.
5. Another function is called to update the initial S-box value, with calculated value from the automata using sliding window protocol.
6. After completion of all the above process we get our desired substitution box with excellent non-linearity and other cryptographic characteristic of substitution box.

Table 2 presented below provides generated substitution box of size 8 × 8 having nonlinearity 107.0 is produced from proposed algorithm. Further analysis of this substitution box is done in next section.

F. PROPOSED GROUP STRUCTURE AND ACTION

The usefulness of algebraic theory for the design of S-boxes has been evolved after the success of the AES S-box [32]. There have been proposals for the S-boxes which are based on algebraic structures. Unfortunately, the S-boxes which are purely algebraic technique based are found to be prune to algebraic attacks. Therefore, there is need to mix the concepts of chaos, CA, and algebraic technique which can complicate the works of attackers to make algebraic attacks infeasible. Moreover, there is very limited work which has focused on the improvisation of an S-box with the help of the action of effective algebraic structure. This requires efforts to construct the strong algebraic structure whose action results in the improvisation of S-boxes security strength. On this line, we have designed a hybrid method to construct final S-box with excellent security performance. The proposed method involves the design and action of an algebraic permutation group which has the efficacy of augmenting the cryptographic features of the S-box. Here, a suitable algebraic structure is designed, after rigorous experiments and experiments, whose action on the S-box yielded by 2-D CA enhances the security strength of the S-box. In what follows, the description of the obtained algebraic group and its action are presented.

We designed an algebraic permutation group "$G = C_{93240} \times C_{180} \times C_{30} \times C_{30}$" of order 15104880000 having following eight generators.

$a :=$ (1, 71, 57, 245, 98, 111, 137, 196, 33, 253, 60, 66,
48, 199, 141, 13, 22, 155, 158, 133, 54, 135, 246,
134, 122, 96, 221, 99, 232, 8, 41, 244, 142, 85, 125,
106, 12, 6, 231, 208, 36, 140, 239, 188, 162, 251,
117, 82, 88, 149, 58, 21, 212, 38, 40, 157, 105, 230,
69, 129, 90, 184, 187, 20, 53, 216, 2, 195, 138, 160,
250, 223, 121, 123, 26, 18, 80, 101, 93, 161, 43, 183,
124, 81, 132, 103, 64, 242, 46, 116, 118, 240, 91,
225, 27, 186, 30, 79, 42, 3, 62, 177, 190,
156, 32, 165, 229, 74, 9, 35, 175);

$b :=$ (4, 97, 148, 7, 172, 102, 176, 108, 159,
201, 203, 67, 34, 51, 61, 39, 219,
220, 145, 59, 210, 218, 247, 254, 164, 11, 49,
171, 112, 213, 174, 44, 16, 94,
28, 24, 197, 180, 84, 241, 214, 152, 104,
206, 228, 128, 234, 95, 68, 113, 115,
222, 63, 147, 109, 193, 211, 107, 23, 236, 14, 29, 50);

$c :=$ (5, 179, 55, 10, 47, 233, 52, 151, 154, 92,
237, 182, 77, 150, 72,

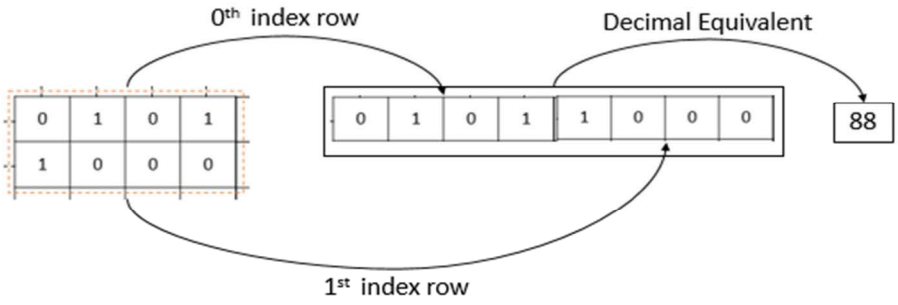

FIGURE 9. Value computation from current sliding window.

TABLE 2. Generated S-box using chaos assisted 2D cellular automata based procedure.

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

185, 110, 143, 255, 167, 119, 136, 100, 45,
19, 166, 153, 114, 144, 83);

$d := (15, 25, 170, 168, 249);$

$e := (17, 37, 65, 178, 163, 238, 86, 70, 181,$
$202, 56, 194, 248, 200, 76, 205, 209, 192, 217, 204);$

$f := (31, 73, 131, 224, 78, 75, 235, 191, 127);$

$g := (87, 89, 215, 256, 139, 173, 146, 126);$

$h := (120, 243, 227, 189, 130, 169, 226, 252, 198, 207);$

This permutation group is applied to update the S-box shown in Table 2. The action of the suggested permutation group on the elements of the S-box generated another S-box which is found to possess strong security features compared to the seed S-box. The complete process of the proposed scheme is shown in Figure 10. The S-box retrieved after the action of proposed algebraic group is displayed in Table 3.

IV. PERFORMANCE ANALYSES

The recital accountability of the anticipated method and S-box is conducted in this section. The known standard security parameters are adopted to assess the features of the S-boxes. The results outcomes are also compared with many prevailing S-boxes methods investigated recently in the literature.

A. NONLINEARITY

Block ciphers typically employ an S-box to offer a non-linear transition from confidential information to encrypted information. The most crucial component of all the security

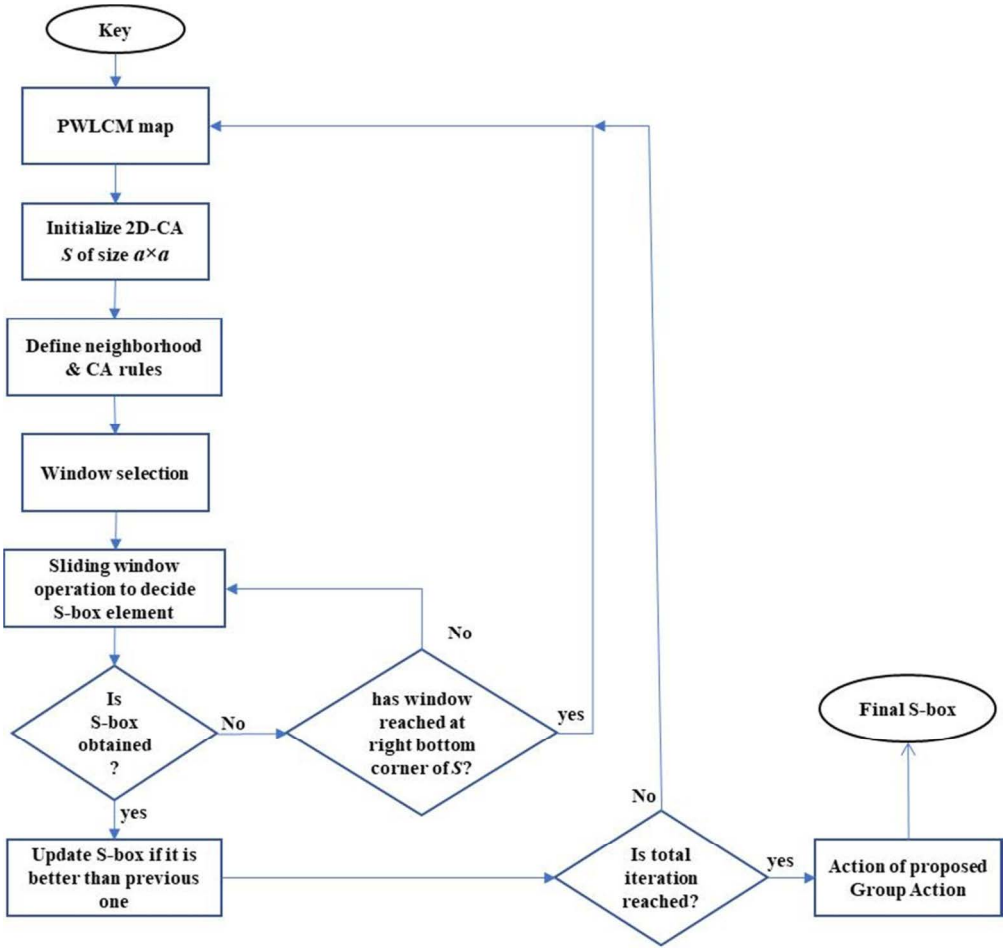

FIGURE 10. Diagram of the proposed scheme for S-box design.

TABLE 3. Proposed improvised 8 × 8 S-box after the action of suggested permutation group *G*.

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

measures is the nonlinearity provided by the cipher [33]. In order to lessen the impact of linear cryptanalysis, block ciphers have robust immunity and nonlinearity. In reality, for an 8-bit Boolean function, Walsh spectrum utilized to

estimate the nonlinearity of f as shown in [34].

$$nonlinearity(f) = 2^7 - \frac{1}{2}\left(\max_{z\in\{0,1\}^8} \left|S_f(z)\right|\right)$$

where,

$$S_f(z) = \sum_{x\in\{0,1\}^8} (-1)^{f(x)\oplus x.z}$$

It is to note that x.z denotes the bitwise dot product. The NLs (nonlinearities) for the suggested S-box are found to be 110, 112, 110, 110, 112, 110, 112 and 110. It shows an excellent nonlinearity performance statistics of the anticipated S-box that the least, maximum, and mean values are 110, 112, and 110.75, respectively, which are considerably high scores. However, the S-box prior to group action has an average score of 107.0 with the minimum value of 102 only, as listed in Table 4. All nonlinearities of final S-box are evidently fairly high and greater than or equivalent to 110. This demonstrates the pronounced capability of the suggested S-box to provide high nonlinear transformation to defend against related attacks [35].

TABLE 4. Nonlinearities of S-box prior and post group action.

Group action	nl_1	nl_2	nl_3	nl_4	nl_5	nl_6	nl_7	nl_8	Min	Max	Mean
Before	106	106	104	108	110	102	110	110	102	110	107
After	110	112	110	110	112	110	112	110	110	112	110.75

B. DIFFERENTIAL UNIFORMITY

To determine the ability of an S-box to withstand prospective differential cryptanalysis, the metric of differential uniformity is taken into account. It is a specific plaintext attack designed by Biham and Shamir to attack block ciphers similar to DES [36], [37]. Whenever an input differential is $\Delta a = \text{XOR}(a_i, a_j)$, the differential uniformity (DU) reflects the highest probability of producing an output differential $\Delta b = \text{XOR}(b_i, b_j)$. This process establishes the XOR (differential) distribution between the S-box's inputs and outputs. In mathematics, it is expressed as:

$$DU_F = \max_{\Delta a\neq 0, \Delta b} (\#\{a \in X | F(a) \oplus F(a \oplus \Delta a) = \Delta b\})$$

To withstand the differential attack of Biham and Shamir, the S-box must have a DU value as low as feasible. It is determined as the biggest value of the differential distribution table. In Table 5, the potential I/O XOR differential scattering for the anticipated S-box is presented. The Table reveals that the largest count in the entire differential scattering is 6 which occur in the distribution only 4 times. However, Du of the S-box prior to group action was 10.

TABLE 5. Differential distribution of proposed S-box.

4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	6	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	6	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	6
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	6	4	4	4	4	4	4	4	4	4	4	4	0

TABLE 6. Dependency matrix for SAC.

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

C. STRICT AVALANCHE CRITERIA

The strict avalanche standard as imperative for strong S-boxes was acquired by Webster and Tavares [38]. To fulfill SAC criteria in S-boxes, the reversing of one bit of vector which gives input must prompt fifty percent of change in the vector which gives out. Because half avalanche is important to lessen any sort of correlation between I/O mix and neglects to spill the sensitive data. A SAC value nearer to 0.5 is constantly seen as respectable. To confirm SAC, Webster and Tavares gave a procedure for computing the dependency matrix as mentioned in [38]. The dependency matrix for the projected S-box displayed in Table 6 is obtained. The dependency matrix reveals that every entry of the table is quite close to 0.5. This matrix has an average score of 0.5012 which signifies the proposed S-box fulfills the strict avalanche criterion well as it is very near to ideal score of 0.5. Hence, the S-box satisfactorily has good avalanche effect.

D. BITS INDEPENDENCE CRITERIA

One of the equally critical criterions for strong S-boxes is bits independence criterion. A strategy to test BIC was recommended by Adams and Tavares [39]. Supposing, the Boolean function's component of a 8×8 S-box are $f_0, f_1, \ldots, f_7$. It is said that the S-box meets BIC, the Boolean functions $XOR(B_j, B_k)$ $(j \neq k$ and $0 \leq j, k \leq 7)$ ought to be exceptionally

TABLE 7. BIC-NL results for proposed S-box.

0	110	110	112	112	110	110	112
110	0	112	110	112	110	110	110
110	112	0	112	110	112	112	112
112	110	112	0	112	112	112	112
112	112	110	112	0	110	112	112
110	110	112	112	110	0	112	112
110	110	112	112	112	112	0	112
112	110	112	112	112	112	112	0

nonlinear and fulfills avalanche criterion nicely. Thus, BIC is confirmed by computing SAC and nonlinearity of each of the 56 combination Boolean functions $XOR(B_j, B_k)$ for an 8×8 S-box. The potential values of NLs of all 56 possibilities of $XOR(B_j, B_k)$ functions for anticipated S-box are evaluated which are displayed in Table 7. The average score of BIC as for nonlinearities are found as 111.28 which appear to be excellent and better compared to the S-box score before the group action which was 103.57 only. Hence, the BIC score for proposed S-box verifies the fantastic performance as far as fulfillment of bits independent criterion is concern.

E. AUTO-CORRELATION FUNCTION

Assuming that $A(t)$ and $B(t)$ are the Boolean mappings. Their correlation is symbolized as $\hat{C}_{AB}(x)$ and mathematically expressed as [40]:

$$\hat{C}_{AB}(x) = \sum_{t} \frac{1}{2^n} \left((-1)^{A(t)\oplus B(t\oplus x)}\right)$$

However, $\hat{C}_{AA}(x)$ represents the auto-correlation function (ACF) for mapping $A(t)$. $\hat{C}_{AA}(x)$ is the squares of elements of spectrum of $A(t)$ responsible for the elements of the spectrum of ACF. The ACF for $A : GF(2^n) \rightarrow GF(2^n)$ is denoted by $\hat{\hat{R}}_A(x)$ which has the following algebraic formulation.

$$ACF = \hat{R}_A(x) = \sum_{t} \frac{1}{2^n} \left((-1)^{A(t)\oplus A(t\oplus x)}\right)$$

For an S-box exhibiting better diffusion effect, the lower score of ACF is appropriate [40]. The proposed S-box after group action found to have an ACF score of 40 only which is sufficiently better than the ACF of the S-box before the group action where it was 104.

F. LINEAR APPROXIMATION PROBABILITY

The strategy for linear approximation probability (LAP) is useful in computing the unevenness of an event. Matsui in [41] presented the largest probability showing the unevenness of an event accounted with the assistance of the examination. There should be no distinction of bits uniformity among output and input. Every one of the input bits along its outcomes in output bits is analyzed independently. On the off chance that every one of the input components are 2^8, D is the set of all potential inputs and the masks functional on the correspondence of output and input bits are individually w_x and w_y, then, at that point, most extreme linear guess is the greatest number of similar outcomes which is determined as shown in Eqn (4).

$$LAP(S) = \max_{w_x, w_y \neq 0} \left| \frac{\#\left\{x \in S | x.w_x = y.w_y\right\}}{2^8} - 2^{-1} \right|$$

The fact that that S-box is more competent to resist against linear cryptanalysis attack is because of the lower value of LAP. Following the definition of LAP, the proposed S-box found to have an LAP score of 0.0703 only this is considerably improved score after the group action as prior to group action LAP was 0.1406. Hence, LAP analysis shows that final S-box has superior capability to repel linear cryptanalysis than S-box we had before group action.

The performance features other than nonlinearity of S-boxes we have prior and post group action are provided in Table 8 to make evident the effectiveness of proposed permutation group action and excellent security forte of the final S-box.

TABLE 8. Other features of S-box prior and post group action.

Group Action	SAC	BIC-NL	DU	LAP	ACF
Before	0.4941	103.57	10	0.1406	104
After	0.5012	111.28	6	0.0703	40

G. COMPARISON ANALYSIS

Researchers have been investigating different methods to spawn cryptographically tough S-boxes for the last two decades. Eventually, a number of proposals came up to fulfill the research goal based on chaotic systems, algebraic approaches, number-theoretic concepts, meta-heuristics, and other random design strategies. Hence, it is rational to assess the performance of any new S-box against the security features of existing S-boxes studies [16], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60]. Therefore, the features of suggested S-box are compared with some of the state of the art and recently investigated S-box methods. The comparison analysis is based on the Table 9 maintained for this purpose. Table 9 consists of some well-known and recently investigated S-box studies whose design concepts are based on chaos, elliptic curve, algebraic method, meta-heuristics, and their combinations.

In almost all S-box studies, it has been found that nonlinearity has been deliberated as the main focused performance parameter while scheming S-boxes [61]. Due to which the generated S-box have high nonlinearity but other performance parameters don't have good enough scores which might make the S-box susceptible to attacks other than linear attacks. Hence, it necessary to generate S-box which should have good score on all other parameters as well in addition

TABLE 9. Comparison of cryptographic features of S-boxes.

S-box	Min(NL)	Max(NL)	Mean(NL)	DU	SAC	BIC-NL	LAP	ACF
Proposed	110	112	110.75	6	0.5012	111.28	0.0703	40
Chaos-based methods								
Lambic *et al.* [34]	106	108	106.5	10	0.501	104.1	0.1328	96
Çavuşoğlu [43]	104	110	107	12	0.5004	102.85	0.1328	96
Garcia *et al.* [44]	105	107	106	12	0.5066	103	0.1445	96
Zhou *et al.* [49]	104	110	107	10	0.4993	103.28	0.1328	104
Jamal *et al.* [51]	98	108	102.25	14	0.4836	101.57	0.1679	108
Artuğer *et al.* [52]	108	112	110	10	0.4995	103.14	0.1328	104
Meta-heuristics based methods								
Zhang *et al.* [45]	108	110	108.75	10	0.4946	102.28	0.1328	96
Zamli *et al.* [47]	108	112	109.75	10	0.5068	104.35	0.1250	96
Alhadawi *et al.* [48]	106	110	108.5	10	0.4995	103.85	0.1250	96
Wang *et al.* [50]	110	112	110.25	10	0.4953	104.07	0.1250	96
Tian *et al.* [53]	106	110	108	10	0.5073	104	0.1523	96
Farah *et al.* [54]	104	110	106.5	10	0.4995	104.57	0.1172	96
Ahmed *et al.* [55]	106	108	107.5	10	0.4943	104.35	0.125	96
Zamli *et al.* [56]	106	110	109.25	10	0.5017	104.07	0.1171	112
Wang *et al.* [57]	98	108	105.75	10	0.4991	102.57	0.14062	96
Soto *et al.* [58]	102	110	106.5	12	0.4943	103.35	0.14844	96
Alzaidi *et al.* [59]	108	110	109.5	10	0.4985	104.07	0.1328	96
Hematpour *et al.* [60]	104	111	106.5	10	0.5036	102.86	0.14062	112
Other methods								
Latif *et al.* [16]	96	104	100.5	10	0.4973	102.78	0.15625	96
Azam *et al.* [24]	106	108	106.5	10	0.5046	104.14	0.1328	96
Ibrahim *et al.* [25]	106	110	106.5	10	0.5009	103.92	0.1250	96
Ullah *et al.* [26]	112	112	112	4	0.4997	112	0.063	32
Latif *et al.* [42]	96	106	102.5	10	0.5037	103.9	0.1250	96
Yousaf *et al.* [46]	100	108	106.5	12	0.5064	103.71	0.1406	108

to nonlinearity to make it tough and robust. The comparison study made in Table 9 reveals that the anticipated S-box has superb nonlinearity feature compared to almost all S-boxes of the Table. As the proposed S-box has minimum nonlinearity of 110 with an awesome average of 110.75, thereby enabling the S-box to offer high nonlinear transformation of plaintext to ciphertext during substitution phase in block cryptosystems. In addition to high nonlinearity feature, the XOR distribution analysis of our S-box shows a decent value of differential uniformity which is 6 in our proposed case. This DU score is the lowest among all the scores presented in the Table 9. Hence, it can be clearly stated that the suggested S-box offers quite better robustness and resistance to differential cryptanalysis than the other recently investigated S-boxes. The SAC of the proposed S-box is found as 0.5012 which is comparable to all other SAC values of the Table, thereby

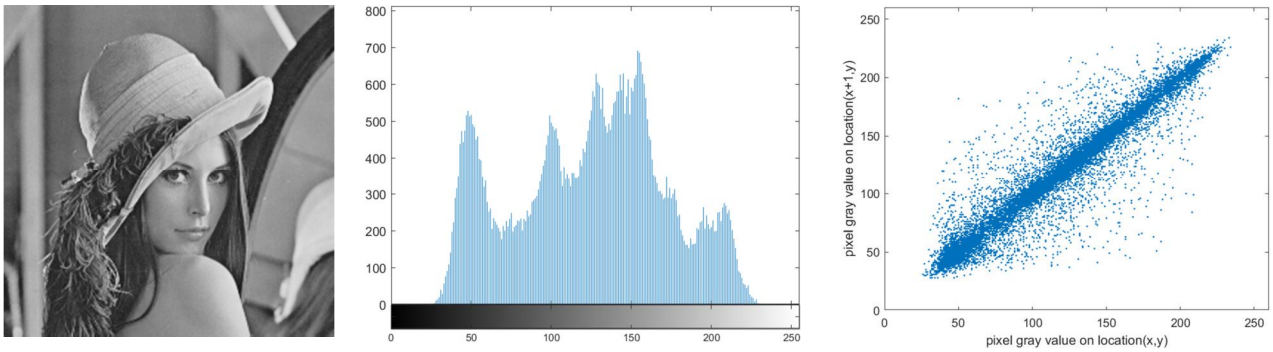

FIGURE 11. Plain-image with its histogram and neighbouring pixels correlation plot.

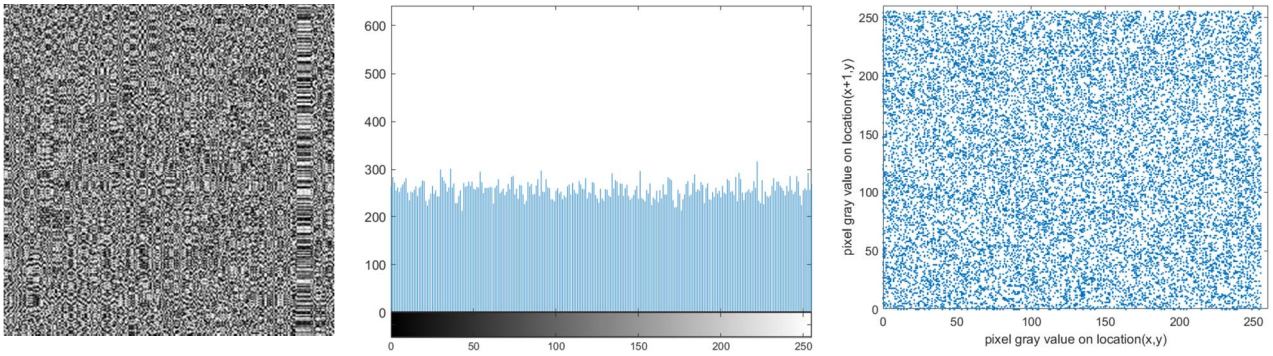

FIGURE 12. Encrypted image obtained using proposed S-box with its histogram and neighbouring pixels correlation plot.

indicating that S-box suitably satisfies the SAC criteria. The bits independence analysis showed that the BIC-NL value for the projected S-box is 111.28 which is pretty higher and better among the many existing S-boxes. To withstand the Mitsui's linear cryptanalysis effort, it is mandatory for the S-box to exhibit lower linear approximation probability. Our S-box has LAP of 0.0703 which is lowest compared to of all other S-boxes LAP scores. Hence, the projected S-box also has improved ability to mitigate linear attacks. The auto-correlation function or the absolute indicator is also another equally crucial performance parameter to gauge the security and diffusion ability of the S-box. The projected S-box found to have an excellent ACF score of 40 which is best among all other S-boxes of the comparison Table 9.

H. S-BOX APPLICATION

It is prudent to assess the security performance of generated S-box on cryptographic application. Here, the generated S-box is applied to assess its suitability and feasibility for encryption applications on benchmark *Lena* plain-image of size 256×256. This plain-image is shown in Figure 11 along with its histogram and adjacent pixels correlation plot. Obviously, the plain-image is having non-uniform distribution of its pixels and the adjacent pixels are highly correlated to each as evident from their respective plots. The encryption method based on S-box suggested in Ref. [62] is applied to encrypt the image using proposed S-box. The encrypted image obtained using proposed S-box is shown in Figure 12. The same figure also presents the histogram and correlation among adjacent pixels of the encrypted image. It is clear from the encrypted image that it has excellent visual distortion as the image is noise-like and it is difficult to visually recognize the plain-image. Moreover, the histogram shows that the pixels distribution in the encrypted image are fairly uniform as the histogram is quite flat, and the adjacent pixels are not correlated to each unlike plain-image.

TABLE 10. MLC scores for encryption performance.

MLC Parameters	Plain	Encrypted	Ref. [63]
Contrast	0.44825	10.1568	9.9764
Energy	0.11275	0.01572	0.0161
Homogeneity	0.8622	0.4033	0.4131
Correlation	0.9025	0.0386	0.0487
Entropy	7.4439	7.9967	7.9353
Chi-square	39666.8	296.75	NA

We have also evaluated the majority logic criteria (MLC) parameters to quantify the encryption performance statistically. Readers are advised to refer to the Ref. [62] for MLC description. The results of MLC analysis are provided in Table 10. The obtained MLC results are also compared with similar kind of S-box based encryption scheme to fairly assess the level of performance. We can see that the obtained MLC parameters scores are pretty better than scores obtained for plain-image and encryption scheme investigated in [63]. Thus, the analysis confirms the acceptable performance of our S-box for image encryption applications. Apart from image encryption applications, several other applications of S-box have been also investigated such as watermarking, steganography, hash functions, and pseudo-random number generations, etc.

V. CONCLUSION

A cryptographically strong S-box must have excellent cores of almost all performance parameters. Existing methods main focused on improvising only one parameter which is nonlinearity in most of the investigations which neglects the improvisation of other and equally significant parameters. This paper reported a hybrid method which is based on the features of chaos, 2-D cellular automata, and algebraic approach as well. Initially, an S-box is produced with the help of chaos and 2-D cellular automata. The security features of obtained S-box are augmented with the help of a suggested permutation group action. The proposed method aims to generate a cryptographic strong S-box which possesses near perfect scores of most of the performance parameters. The minimum NL of 110, DU of 6, BIC-NL of 111.28, LAP of 0.0703, and ACF of 40 are the features of the proposed S-box. The comparison analysis revealed that proposed S-box exhibits considerably better security strength and robustness as compared to many recent and other S-boxes, thereby confirming the suitable conduct of proposed method for strong S-box candidates design for usage in secure block cipher implementations.

ACKNOWLEDGMENT

This work was supported by the EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia.

REFERENCES

[1] L. R. Knudsen and M. J. B. Robshaw, *The Block Cipher Companion*. Berlin, Germany: Springer-Verlag, 2011.
[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[3] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York, NY, USA: Wiley, 1996.
[4] A. M. Youssef and S. E. Tavares, "Resistance of balanced s-boxes to linear and differential cryptanalysis," *Inf. Process. Lett.*, vol. 56, no. 5, pp. 249–252, Dec. 1995.
[5] 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.
[6] M. T. Tran, D. K. Bui, and A. D. Duong, "Gray S-box for advanced encryption standard," in *Proc. Int. Conf. Comput. Intell. Secur.*, Dec. 2008, pp. 253–258.
[7] A. Alhudhaif, M. Ahmad, A. Alkhayyat, N. Tsafack, A. K. Farhan, and R. Ahmed, "Block cipher nonlinear confusion components based on new 5-D hyperchaotic system," *IEEE Access*, vol. 9, pp. 87686–87696, 2021.
[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] F. Özkaynak and A. B. Özer, "A method for designing strong S-boxes based on chaotic Lorenz system," *Phys. Lett. A*, vol. 374, no. 36, pp. 3733–3738, 2010.
[10] Y. Wang, K.-W. Wong, C. Li, and L. Yang, "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, 2012.
[11] R. Yin, J. Yuan, J. Wang, X. Shan, and X. Wang, "Designing key-dependent chaotic S-box with larger key space," *Chaos, Solitons Fractals*, vol. 42, no. 4, pp. 2582–2589, Nov. 2009.
[12] D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," *J. Inf. Telecommun.*, vol. 2, no. 2, pp. 181–191, 2018.
[13] F. Özkaynak, V. Çelik, and A. B. Özer, "A new S-box construction method based on the fractional-order chaotic Chen system," *Signal, Image Video Process.*, vol. 11, no. 4, pp. 659–664, 2016.
[14] B. B. Cassal-Quiroga and E. Campos-Cantón, "Generation of dynamical S-boxes for block ciphers via extended logistic map," *Math. Problems Eng.*, vol. 2020, p. 12, Mar. 2020.
[15] 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.
[16] 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, pp. 118–131, Mar. 2020.
[17] A. Razaq, Iqra, M. Ahmad, M. A. Yousaf, and S. Masood, "A novel finite rings based algebraic scheme of evolving secure S-boxes for images encryption," *Multimedia Tools Appl.*, vol. 80, no. 13, pp. 20191–20215, May 2021.
[18] 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, 2016.
[19] A. H. Zahid, M. J. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, May 2019.
[20] 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.
[21] M. F. Khan, A. Ahmed, and K. Saleem, "A novel cryptographic substitution box design using Gaussian distribution," *IEEE Access*, vol. 7, pp. 15999–16007, 2019.
[22] H. A. M. A. Basha, A. S. S. Mohra, T. O. M. Diab, and W. I. E. Sobky, "Efficient image encryption based on new substitution box using DNA coding and bent function," *IEEE Access*, vol. 10, pp. 66409–66429, 2022.
[23] A. K. Farhan, R. S. Ali, H. R. Yassein, N. M. G. Al-Saidi, and G. H. Abdul-Majeed, "A new approach to generate multi S-boxes based on RNA computing," *Int. J. Innov. Comput. Inf. Control*, vol. 16, pp. 331–348, Oct. 2020.
[24] N. A. Azam, U. Hayat, and I. Ullah, "Efficient construction of a substitution box based on a mordell elliptic curve over a finite field," *Frontiers Inf. Technol. Electron. Eng.*, vol. 20, no. 10, pp. 1378–1389, Oct. 2019.
[25] S. Ibrahim and A. M. Abbas, "Efficient key-dependent dynamic S-boxes based on permutated elliptic curves," *Inf. Sci.*, vol. 558, pp. 246–264, May 2021.
[26] I. Ullah, N. A. Azam, and U. Hayat, "Efficient and secure substitution box and random number generators over mordell elliptic curves," *J. Inf. Secur. Appl.*, vol. 56, Feb. 2021, Art. no. 102619.
[27] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Process.*, vol. 155, no. 3, pp. 391–402, Feb. 2019.

[28] I. Ullah, U. Hayat, and M. D. Bustamante, "Image encryption using elliptic curves and Rossby/Drift wave triads," *Entropy*, vol. 22, no. 4, p. 454, Apr. 2020.
[29] S. Wolfram, *A New Kind of Science*. Champaign, IL, USA: Wolfram Media, 2002, p. 1197.
[30] S. Roy, M. Shrivastava, C. V. Pandey, S. K. Nayak, and U. Rawat, "IEVCA: An efficient image encryption technique for IoT applications using 2-D von-neumann cellular automata," *Multimedia Tools Appl.*, vol. 80, nos. 21–23, pp. 31529–31567, Sep. 2021.
[31] D. Mukhopadhyay, "Design and analysis of cellular automata based cryptographic algorithms," Ph.D. dissertation, Dept. Comput. Sci. Eng., IIT, Kharagpur, West Bengal, 2007.
[32] M. S. Fadhil, A. K. Farhan, M. N. Fadhil, and N. M. G. Al-Saidi, "A new lightweight AES using a combination of chaotic systems," in *Proc. 1st. Inf. Technol. Enhance e-learning Appl. (IT-ELA*, Jul. 2020, pp. 82–88.
[33] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Amsterdam, The Netherlands: Elsevier, 2009.
[34] 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, 2020.
[35] K. Nyberg, "Perfect nonlinear S-boxes," in *Proc. Workshop Theory Appl. Cryptographic Techn.* Berlin, Germany: Springer, 1991, pp. 378–386.
[36] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, pp. 3–72, Jan. 1991.
[37] J. M. Hassan and F. A. Kadhim, "New S-box transformation based on chaotic system for image encryption," in *Proc. 3rd Int. Conf. Eng. Technol. Appl. (IICETA)*, Sep. 2020, pp. 214–219.
[38] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology*. Berlin, Germany: Springer, 1986, pp. 523–534.
[39] C. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," *J. Cryptol.*, vol. 3, no. 1, pp. 27–41, Jan. 1990.
[40] X.-M. Zhang, Y, Zheng, and H. Imai, "Relating differential distribution tables to other properties of substitution boxes," *Des. Codes Cryptography*, vol. 19, no. 1, pp. 45–63, 2000.
[41] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology*. Berlin, Germany: Springer, 1994, pp. 386–397.
[42] 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.
[43] Ü. Çavuşoğlu, "S-box-based video stenography application of variable-order fractional Hopfield neural network (VFHNN)," *Eur. Phys. J. Special Topics*, vol. 231, no. 10, pp. 2017–2035, Aug. 2022.
[44] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, "Substitution box generation using Chaos: An image encryption application," *Appl. Math. Comput.*, vol. 332, pp. 123–135, Sep. 2018.
[45] T. Zhang, C. L. P. Chen, L. Chen, X. Xu, and B. Hu, "Design of highly nonlinear substitution boxes based on I-Ching operators," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 1–10, Jul. 2018.
[46] 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.
[47] K. Z. Zamli, "Optimizing S-box generation based on the adaptive agent heroes and cowards algorithm," *Expert Syst. Appl.*, vol. 182, Nov. 2021, Art. no. 115305.
[48] 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, 2020.
[49] P. Zhou, J. Du, K. Zhou, and S. Wei, "2D mixed pseudo-random coupling PS map lattice and its application in S-box generation," *Nonlinear Dyn.*, vol. 103, no. 1, pp. 1151–1166, Jan. 2021.
[50] Y. Wang, Z. Zhang, L. Y. Zhang, J. Feng, J. Gao, and P. Lei, "A genetic algorithm for constructing bijective substitution boxes with high nonlinearity," *Inf. Sci.*, vol. 523, pp. 152–166, Jan. 2020.
[51] S. Jamal, M. Khan, and T. Shah, "A watermarking technique with chaotic fractional S-box transformation," *Wireless Pers. Commun.*, vol. 90, no. 4, pp. 2033–2049, 2016.
[52] F. Artuğer and F. Özkaynak, "An effective method to improve nonlinearity value of substitution boxes based on random selection," *Inf. Sci.*, vol. 576, pp. 577–588, Oct. 2021.
[53] Y. Tian and Z. Lu, "S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm," *J. Syst. Eng. Electron.*, vol. 27, no. 1, pp. 232–241, Feb. 2016.
[54] 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, 2017.
[55] 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, 2019.
[56] K. Z. Zamli, A. Kader, F. Din, and H. S. Alhadawi, "Selective chaotic maps tiki-taka algorithm for the S-box generation and optimization," *Neural Comput. Appl.*, vol. 33, no. 23, pp. 16641–16658, Dec. 2021.
[57] 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.
[58] R. Soto, B. Crawford, F. G. Molina, and R. Olivares, "Human behaviour based optimization supported with self-organizing maps for solving the S-box design problem," *IEEE Access*, vol. 9, pp. 84605–84618, 2021.
[59] 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.
[60] N. Hematpour and S. Ahadpour, "Execution examination of chaotic S-box dependent on improved PSO algorithm," *Neural Comput. Appl.*, vol. 33, no. 10, pp. 5111–5133, May 2021.
[61] F. Artuğer and F. Özkaynak, "SBOX-CGA: Substitution box generator based on chaos and genetic algorithm," *Neural Comput. Appl.*, vol. 34, no. 22, pp. 20203–20211, Nov. 2022, doi: 10.1007/s00521-022-07589-4.
[62] 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.
[63] 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.

AMIRUL HAQUE received the B.Tech. degree from the Maulana Azad National Institute of Technology, Bhopal, India, in 2015, and the M.Tech. degree from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India, in 2018, where he is currently pursuing the Ph.D. degree with the Department of Computer Engineering, in the area of GPU based intrusion detection and prevention. His research interests include cyber security, machine learning, and GPU computing.

TABARAK ALI ABDULHUSSEIN was born in Iraq, in 1990. She received the B.Sc. degree in software engineering from Madenat Alelem University, Iraq, in 2013, and the M.Sc. degree in computer science from the University of Baghdad, Iraq, in 2021. She is currently a Lecturer at the Department of Accounting, College of Administrative and Financial Science, Imam Ja'afar Al-Sadiq University, Iraq. Her current research interests include medical image processing, neural networks, machine learning, the IoT, wireless sensor networks, network mobility management, fog computing, and information security.

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 at the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor at the Department of Computer Engineering, Jamia Millia Islamia. He has published over 100 research papers in internationally reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has more than 2300 citations of his research works with an H-index of 30, i-10 index of 65, and cumulative impact factor of more than 200. He has been listed two times among World's Top 2% researchers in studies conducted by Elsevier and Stanford University, in 2021 and 2022. He has served as a reviewer and a technical program committee member of many international conferences. He has also served as a Referee for some renowned journals, such as *Information Sciences*, *Signal Processing*, *Journal of Information Security and Applications*, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE TRANSACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON NANOBIOSCIENCE, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, IEEE TRANSACTIONS ON BIG DATA, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE IOTJ, IEEE MULTIMEDIA, IEEE ACCESS, *Expert Systems with Applications*, *Wireless Personal Communications*, *Neural Computing and Applications*, *International Journal of Bifurcation and Chaos*, *Chaos Solitons and Fractals*, *Physica A*, *Signal Processing: Image Communication*, *Neurocomputing*, *IET Information Security*, *IET Image Processing*, *Security and Communication Networks*, *Optik*, *Optics and Laser Technology*, *Complexity*, *Computers in Biology and Medicine*, *Journal of Computational and Applied Mathematics*, and *Concurrency and Computation*.

MAYADAH WAHEED FALAH received the bachelor's degree in civil engineering and the M.Sc. degree in civil engineering (structural engineering) from the Department of Civil Engineering, Engineering College, University of Babylon, Babil, Iraq, in 2009 and 2013, respectively. She is currently pursuing the Ph.D. degree. She is a lecturer and a researcher in the field of civil engineering. In 2013, she joined the Department of Building and Construction Technologies Engineering, Al-Mustaqbal University College, as an Academic Staff Member. She has a lot of research published in the field of civil engineering.

AHMED A. ABD EL-LATIF (Senior Member, IEEE) received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science all 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, Harbin, China, in 2013. He is a Research Professor at the EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia. He is the author and the coauthor of more than 200 papers, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, 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 is a member of ACM. He is also a fellow of the Academy of Scientific Research and Technology, Egypt. He received many awards, such as the State Encouragement Award in Engineering Sciences 2016, Arab Republic of Egypt; the Best Ph.D. Student Award from the Harbin Institute of Technology, China 2013; and the Young Scientific Award, Menoufia University, Egypt, in 2014. He is the editor/a guest editor of several reputed SCI journals. Currently, he had many books, more than ten books, in several publishers for process in Springer, IET, CRC press, IGI-Global, Wiley, and IEEE.