IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 16, 2018, accepted September 15, 2018, date of publication October 2, 2018, date of current version October 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2871557

A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes

AMER AWAD ALZAIDI[1], MUSHEER AHMAD[2], M. N. DOJA[2], EESA AL SOLAMI[3], AND M. M. SUFYAN BEG[4], (Senior Member, IEEE)

[1]Department of Information System, University of Jeddah, Jeddah 6111, Saudi Arabia
[2]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[3]Department of Information Technology, University of Jeddah, Jeddah 6111, Saudi Arabia
[4]Department of Computer Engineering, Aligarh Muslim University, Aligarh 202002, India

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

ABSTRACT One-dimensional (1-D) chaotic maps have been considered as prominent pseudo-random source for the design of different cryptographic primitives. They have the advantages of simplicity, easy to implement, and low computation. This paper proposes a new 1-D discrete-chaotic map which holds better dynamical behavior, lyapunov exponent, bifurcation, and larger chaotic range compared with the chaotic logistic map. We propose a method to construct cryptographically efficient substitution-boxes (S-boxes) using an improved chaotic map and β-hill climbing search technique. S-boxes are used in block ciphers as nonlinear components to bring strong confusion and security. Constructing optimal S-boxes has been a prominent topic of interest for security experts. To begin, the anticipated method generates initial S-box using the improved chaotic map. Then, β-hill climbing search is applied to obtain notable configuration of S-box that optimally satisfies the fitness function. The simulation results are compared with some recent S-boxes approaches to demonstrate that the proposed approach is more proficient in generating strong nonlinear component of block encryption systems.

INDEX TERMS β-hill climbing, block ciphers, improved chaotic map, substitution-box.

I. INTRODUCTION

The field of Information Technology has undergone rapid advancement over the years and has found itself incorporated into various fields that include trade and commerce, defense, education, broadcasting, healthcare and medicine, etc. Information is stored on a digital device and sharing of information is achieved by transmission over a communication network. The issue of realizing secure exchange of information creates proliferating demand for more proficient cryptographic algorithms to forestall illegal interception, manipulation and unauthorized usage of secret information. To tackle the eminent security demands, the modern block ciphers have been playing crucial role for past many years [1]. It is imperative for any cipher to have impregnable resistance against cryptographic attacks. In 1949, Claude E. Shannon, in his masterpiece work "*Communication theory of secrecy systems*", suggested two deciding properties for ciphers to impede cryptanalysis- confusion and diffusion [2]. Diffusion hides the relationship between the cipher and plaintext. The structure of the plaintext is distributed in the ciphertext such that it cannot be discerned from the ciphertext. Confusion complicates the relationship between the ciphertext and the key [3]. These properties have become the cornerstone of design of modern block ciphers. In modern block ciphers, either based on Substitution-Permutation network or Feistel network, the component responsible for confusion is the substitution-box (S-box) [1]. The security of block ciphers heavily depends on the cryptographic strengths of S-boxes employed. S-boxes are prime components for these networks at substitution layers and meant to carry out nonlinear transformation which in turn brings confusion. A weak S-box in ciphers such as DES makes it breakable under differential and linear cryptanalysis [4], [5], where as a cryptographically better S-box offers immunity to mitigate these attacks [6]. Therefore, the crucial nature of S-boxes in the security of modern block cryptosystems has effectuated substantial research in the design of cryptographically stronger S-boxes. A good S-box should optimally satisfy pertinent performance criterias such as nonlinearity, strict avalanche, bits independence, differential uniformity, linear approximation probability, etc [7].

Mathematically, any $m \times n$ substitution-box acts as a nonlinear mapping S: $\{0, 1\}^m \rightarrow \{0, 1\}^n$ and generated an n-bit output string to an input string of size m-bit. An S-box S is a multi-output Boolean function which consists of n Boolean functions each in m-variable as S: $f_n(x)f_{n-1}(x)\ldots\ldots f_1(x)$, where each $f_i(x)(1 \leq i \leq n)$ is function from $\{0, 1\}^m$ to $\{0, 1\}$ [8], [9].

Chaos is aperiodic long-termed behavior found in some nonlinear dynamical systems that exhibits sensitive dependence on initial conditions. Chaos theory has diverse applications in fields of engineering, mathematics, cryptology, physics, biology, chemistry, etc [10]. A chaotic system having well dynamical behaviour possess deterministic and noise-like nature, extreme sensitiveness to initial conditions, long periodicity, and ergodicity. These features of chaos have close analogy with properties of cryptography [11]. Therefore, the chaotic maps have been considerably investigated and explored to develop security methods for image, audio, video encryptions, information hiding, authentication, hash functions, S-boxes, pseudo-random sequences, etc, [12]. Compared to high-dimensional chaotic systems which are complex in nature, multi-parameters, difficult in hardware/software realization, the 1D chaotic maps have merits of simplicity, easy to implement in both hardware and software, processing speed [13]. But, they suffer with limited chaotic range and behaviour, non-uniform distribution of its trajectory in phase space, low lyapunov exponent [14]. This motivates the designers to model one-dimensional chaotic maps which have better dynamical features and behaviour for better security performance in the area chaos-based cryptography [13]–[16].

In literature, a substantial number of proposals have been investigated based on chaotic systems and evolutionary techniques using chaos with sole aim of generating strong S-boxes. Guo Chen employed the idea of chaotic multi-swapping and simulated annealing optimization to search cryptographically strong 8 × 8 S-boxes which satisfy the major performance criterias in [17], where 2D chaotic baker map is used to explore the search space of possible S-boxes and chaotic Chebyshev map is utilized to generate initial S-box for optimization through simulated annealing. Thereafter, Wang *et al.* [18], Wang and Peng [19], and Guesmi *et al.* [20] used genetic algorithm for optimization of initial S-box. Yong and Peng [19] used chaotic logistic map and chaotic tent map to generate initial populations and control parameters of genetic algorithm, the adjustment phase of same approach is updated to synthesis better S-boxes. Where as, Guesmi *et al.* adopted logistic map for initial S-box generation and 3D chaotic Lorenz system for crossover and mutation points during genetic algorithm operation. In [21], Ahmad *et al.* applied ant colony optimization to yield optimized configuration of an 8 × 8 S-box. A modulated chaotic tent map through logistic map is iterated to generate initial S-box which is transformed to a traveling salesman problem through edge matrix. Their optimized S-box claimed to possess good cryptographic features and resistant to attacks as compared to some S-boxes. Tian and Lu [22] explored artificial bee colony optimization algorithm and 6D hyper-chaotic map to construct strong 8×8 S-box, wherein hyperchaotic map was meant to generate initial population of S-boxes needed during optimization phase. Tian and Lu [23] followed bacteria foraging optimization algorithm but with intertwining logistic map with similar methodology for S-box optimization. In both of Tian *et al.* S-box studies, the nonlinearity and differential uniformity was collectively taken as fitness function. In [24], the traveling salesman problem is explored to obtain a good configuration of S-box, where the weights of edges, of sub-graphs extracted from initial S-box, are assigned by chaotic skew tent map. Farah *et al.* [25] suggested a new method involving chaos and teaching-learning based optimization for S-box design. Through TLBO, the authors obtained optimized keys that resulted into optimized S-box with excellent performance particularly the linear approximation probability. In [26], Ahmed *et al.* applied the firefly algorithm for optimizing an initial S-box generated from a discrete-space chaotic map. Recently, Zhang *et al.* [27] employed I-Ching operators (ICOs) innovatively that were evolved from Chinese I-Ching philosophy for constructing optimized S-boxes.

Referring to some recent S-box proposals based on only chaos, Liu *et al.* [28] constructed an S-box using method based on the 3D four-wing autonomous chaotic system and the recommended S-box has good performance. Khan and Asghar came up with a unique method of designing S-boxes by using S_8 symmetry group and Gingerbreadman chaotic map. The S_8 permutations and chaotic map combinations proved to be useful for encryption of images [29]. A new S-box design was proposed in [30] which is honourable as their design method is aided with rich dynamic features of scaled Zhongtang chaotic system. Lambic suggested an efficient approach by applying composition operations on some existing standard S-boxes to construct a strong S-box in [31]. The investigation showed that the generated S-box has good cryptographic properties. Another method for bijective 8 × 8 S-box design using discrete chaotic map was investigated by Lambić [32]. Attaullah *et al.* investigated the improved chaotic system and linear fractional transformation in [33] and group actions of projective general linear group on units of finite local ring in [34] for designing some strong S-boxes. Özkaynak [35] did some analysis with two types of chaotic systems namely discrete chaotic system and continuous chaotic system to yield corresponding S-boxes which were found to possess good performance. Recently, Tian and Zhimao developed an O-shaped path scrambling algorithm to yield strong S-box in [36], where the preliminary S-box is constructed through a six-dimensional fractional Lorenz-Duffing chaotic system.

Motivated to explore concepts for further performance improvisation, we proposed an improved 1D chaotic map that has excellent dynamical behaviour as compared to logistic map in terms of lyapunov exponent, uniform distribution, bifurcation, entropy and chaotic range. The same chaotic map is then utilized to facilitate the β-hill climbing technique to generate notable configuration of an 8 × 8 S-box that optimizes the given fitness function. The proposed S-box generation method is found competent to yield strong S-boxes as it possesses excellent cryptographic strength when compared with recent proposals of chaos-based S-boxes and optimization-based S-boxes.

Rest of the paper is prepared as follows: The model and analysis of proposed 1D chaotic map is presented in Section II. A brief discussion of recent β-hill climbing technique is given in Section III. The proposed method for generating optimized S-box using improved chaotic map and β-hill climbing is provided in Section IV. The results of proposed S-box method and performance assessment is done in Section V, a comparative study with recent S-box methods is also exercised in the same section. Lastly, the conclusions of work are made in Section VI.

II. IMPROVED 1D CHAOTIC MAP AND ITS DYNAMICAL BEHAVIOUR

Logistic map is one of the widely used and famous one-dimensional discrete-chaotic maps given by May [37], whose state evolves according to the equation (1).

$$x_{n+1} = \mu x_n\,(1 - x_n) \tag{1}$$

Where, $0 < \mu \leq 4$ is control parameter and x_n is the state variable of logistic map whose trajectory is decided by the initial condition x_0. The chaotic outputs x_n of map (1) are bounded within [0, 1] for all $n \geq 0$. To illustrate the dynamical behaviour, the lyapunov exponent diagram and bifurcation diagram are shown in Fig. 1(a) and 1(b). It is evident from the diagrams that the logistic map shows chaotic phenomenon when μ lies to the interval of [3.57, 4]. It shows no chaotic performance when $\mu < 3.57$ as its lyapunov exponent is zero. The phase diagram of logistic map is provided in Fig. 1(c) to show that its attractor has parabola-like shape and don't spread over entire range. Despite of its wide usage, the logistic map has certain limitations such as:

- It has limited chaotic range as seen in Fig. 1(a) and 1(b).
- It has low largest lyapunov exponent as 0.693495 only.
- It has non-uniform distribution in interval [0, 1] as seen in Fig. 1(b).
- It has some non-chaotic windows for $3.83 < \mu < 3.86$ i.e. even when μ lies in [3.57, 4].
- Chaotic attractor in phase space follows a parabola-like trajectory.

In order to overcome the above limitations of logistic map, a new 1D discrete-chaotic map is proposed which is defined by the equation (2).

$$\left.\begin{aligned} F(x_n, a, b) &= ax_n(1 - x_n) + b(1 + x_n)\tan(x_n)\\ x_{n+1} &= F(x_n, a, b) \times alpha - floor\;(F(x_n, a, b)\times alpha)\end{aligned}\right\} \tag{2}$$

Where, a and b are its control parameter, x_n is state variable which is bounded in [0, 1]. In fact, the control parameters don't have any limited range. Here, *alpha* is constant which is incorporated to augment the chaotic phenomenon of the map in (2), it can be any non-negative integer greater than 1. Incorporation of one more control parameter is desirable for cryptographic applications as it extends the key space.

For simulation analysis of dynamical behaviour of proposed chaotic map, the values are initialed without loss of generality as $x_0 = 0.123456789$, $a \in (0, 10]$, $b \in (0, 10]$, $alpha = 12345$.

In literature, a simple 1D discrete-chaotic known as Renyi map is available which has excellent dynamical behaviors and whose states evolve according to equation (3) [38].

$$x_{n+1} = (cx_n) \bmod (1) \tag{3}$$

Where, c is its control parameter and x_n is state variable which is bounded in [0, 1]. The Renyi map exhibits chaotic phenomenon when $c > 1$. Its lyapunov exponent is $\log(c)$ which shows that the chaotic phenomenon gets more upright as control parameter c increases. The lyapunov exponent spectrum, bifurcation and phase diagrams for $c = 10$ are depicted in Fig. 2. We can see that the Renyi map in (3) has excellent dynamics. The largest lyapunov exponent is 2.3026 for $c \in (0, 10]$ in Fig. 2, it bifurcates indiscriminately over whole region for $c > 1$, and its corresponding attractor is uniformly distributed over [0, 1]. Unlike Logistic map, the Renyi map found to have uniform probability distribution [38]. The 1D chaotic Renyi map is presented here to

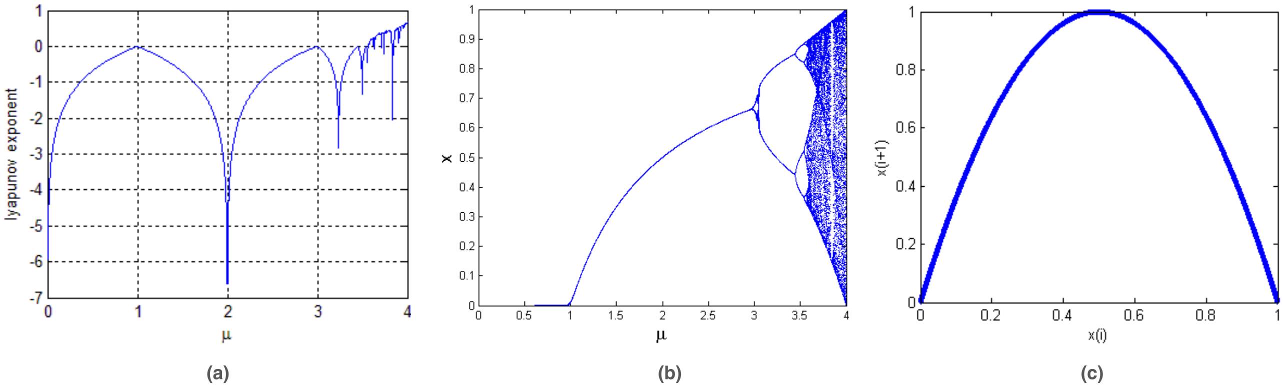

FIGURE 1. Dynamical behaviour of chaotic Logistic map (a) lyapunov exponent, (b) bifurcation plot, and (c) phase diagram representing its attractor.

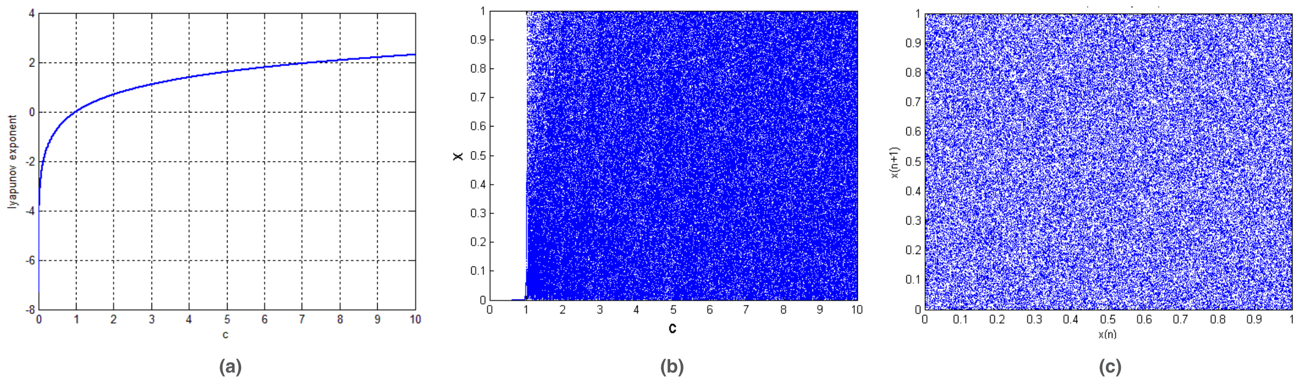

FIGURE 2. Dynamical behaviour of chaotic Renyi map (a) lyapunov exponent, (b) bifurcation plot, and (c) phase diagram.

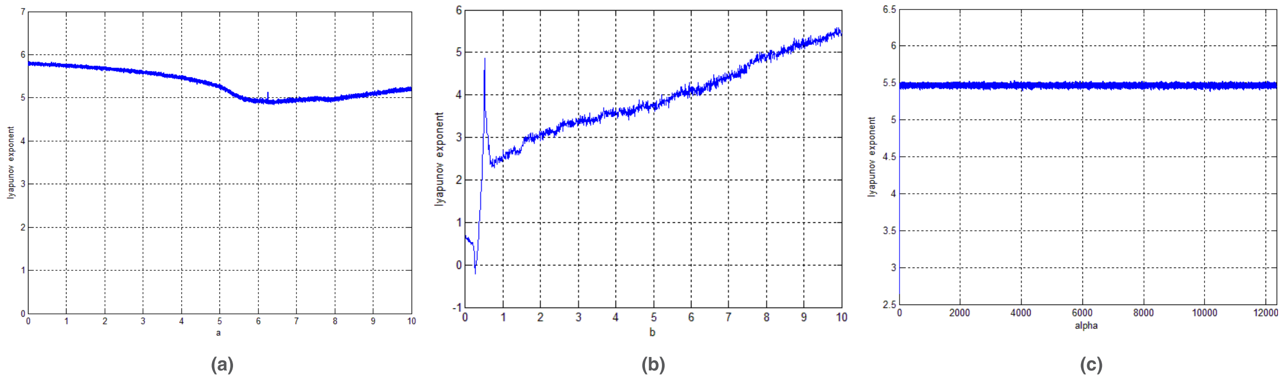

FIGURE 3. Lyapunov exponent diagram of improved chaotic map versus parameter (a) *a*, (b) *b*, and (c) *alpha*.

make comparative analysis of dynamics of chaotic map in (2) so as to justify the performance of our map.

A. LYAPUNOV EXPONENT

Lyapunov exponent is statistical measure to characterize the chaotic performance of a dynamic behaviour. A 1D dynamical map is said to have high sensitivity to initial conditions and parameters provided that it has presence of positive lyapunov exponent. Lyapunov exponent (LE) of dynamical map refers to pace of separation of infinitesimal close trajectories. Presence of positive exponent indicates the existence of chaotic behaviour in the map. Larger the value of LE, the better chaotic performance of map is [39] and [40]. We calculated the lyapunov exponent for different parameters of proposed map (2). Interestingly, it has been shown that for a, $b \in [1, 10]$, and $alpha \in (0, 12345]$, the new map shows positive exponents for wider range of all three parameters. Keeping $b = 10$ and $alpha = 12345$, the lyapunov diagram for different values of a is shown in Fig. 3(a). When $a = 4$ and $alpha = 12345$, the diagram of lyapunov exponents verses $b \in (0, 10]$ is shown in Fig. 3(b). It is noted that the parameter $b \geq 1$ is recommended to ensure chaotic behaviour by map (2). The lyapunov exponents verses $alpha \in (0, 12345]$ is shown in Fig. 3(c) for $a = 4$ and $b = 10$. The three lyapunov diagrams show excellent chaotic phenomenon exhibited by proposed map. The LE diagrams affirm that proposed map has chaotic phenomenon for wider range of parameters. The respective largest LEs are 5.8399, 5.5133 and 5.5286 in Fig. 3, which are considerably higher than maximum LE of 0.6931495 of logistic map for $\mu \in (0, 4]$ and 2.3026 of Renyi map for $c \in (0, 10]$. Moreover, it is also found that the LE becomes more and more larger with increase in parameter b like Renyi map. When $a = 4$, $alpha = 12345$ and $b = 10^8$, the largest LE obtained is 42.0616. This is considerably higher than largest LE of 26.5754 of Renyi map for $c = 10^8$.

B. BIFURCATION

Bifurcation plot represents the manner in which output values are approached asymptotically, whether they are fixed points, periodic orbits, or chaotic attractors, of a dynamical system when bifurcation control parameter is changed [41]. The bifurcation behaviour of new chaotic map is obtained for different parameters conditions and shown in Fig. 4. In comparison to chaotic Logistic map, the output values x_n of proposed chaotic map are not limited to any specific region, rather they are more uniformly distributed over entire range of [0, 1] and for wider values of all three control parameters. The proposed chaotic map has excellent bifurcation behaviour

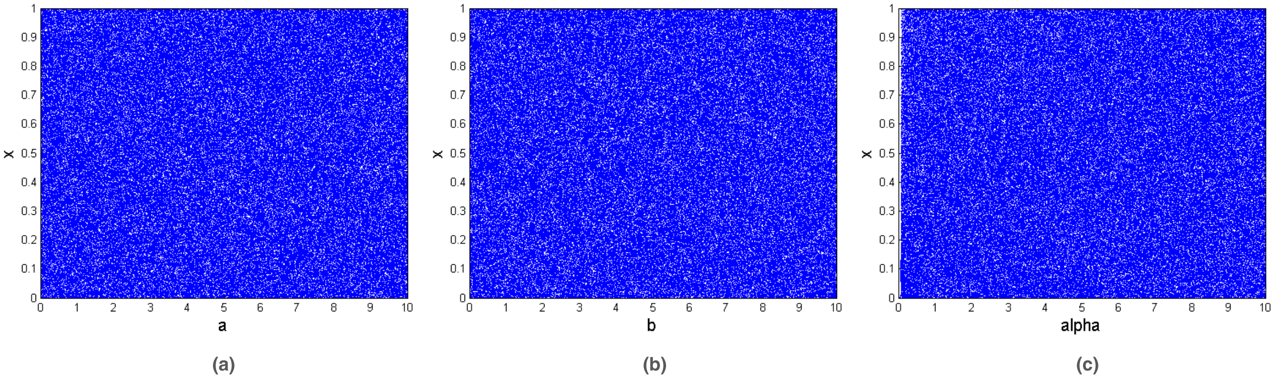

FIGURE 4. Bifurcation plot of improved chaotic map versus parameter (a) *a*, (b) *b*, and (c) alpha.

and ergodicity for all three control parameters similar to Renyi map.

C. PHASE DIAGRAM

The phase diagram of proposed chaotic map is shown in Fig. 5. It can be seen that its attractor randomly covers the entire range like a fractal and doesn't has a specific shape. This indicates that the phase space of proposed chaotic map is more complex and random unlike original logistic map's phase space in Fig. 1(c) and similar to the attractor of Renyi map shown in Fig. 3(c).

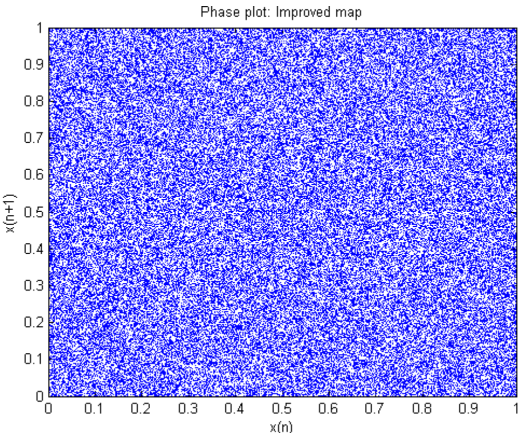

FIGURE 5. Phase diagram representing attractor of improved chaotic map.

D. APPROXIMATION ENTROPY

Approximation entropy (ApEn) is one of the most famous entropy statistics to determine the system complexity which was suggested by Steve Pincus [42], [43]. ApEn is a complexity measure to quantify the amount of irregularity and unpredictability within a given time-series. The approximation entropy for sequence of floating-point values from chaotic logistic map (for $\mu = 4$), chaotic Renyi map (for $c = 10$) and proposed chaotic map (for $a = 4$, $b = 10$, $alpha = 12345$) for different lengths of sequences are shown in Fig. 6. It is clear from Fig. 6 that the ApEn of sequences from proposed chaotic map (average is 1.328179) is considerably higher than entropy of sequences from logistic map (average is 0.606598), and slightly better than the value for chaotic Renyi map. It shows that proposed chaotic map has better complexity and unpredictability than chaotic logistic map and it is similar to Renyi map.

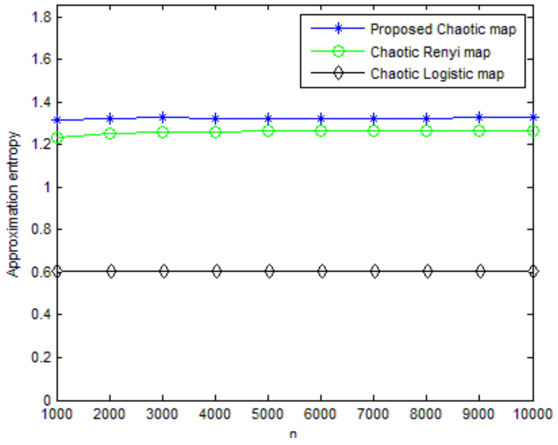

FIGURE 6. Approximation entropy (ApEn) for three discrete-chaotic maps.

E. HISTOGRAM

The distribution of trajectory points of proposed chaotic map (2) is analyzed and compared with that of Renyi map (3) in this subsection. The complete range [0, 1] of chaotic variable is divided into equal-sized 10000 bins. The map is iterated to collect N number of trajectory points starting from initial condition x_0 and keeping other parameters fixed as $a = 4$, $b = 10$, $c = 10$, $alpha = 12345$. The normalized histogram of sampled trajectory points for proposed map are plotted and shown in Fig. 7(a), the same plot is also obtained for Renyi map and shown in Fig. 7(b). We can see that the two histograms are quite similar, flat and uniform. It has been also observed that same shaped histograms are obtained for both maps when tested for different initial conditions i.e. the histograms are invariant of starting point of trajectory x_0. Moreover, the probability of each 10000 bin is also computed

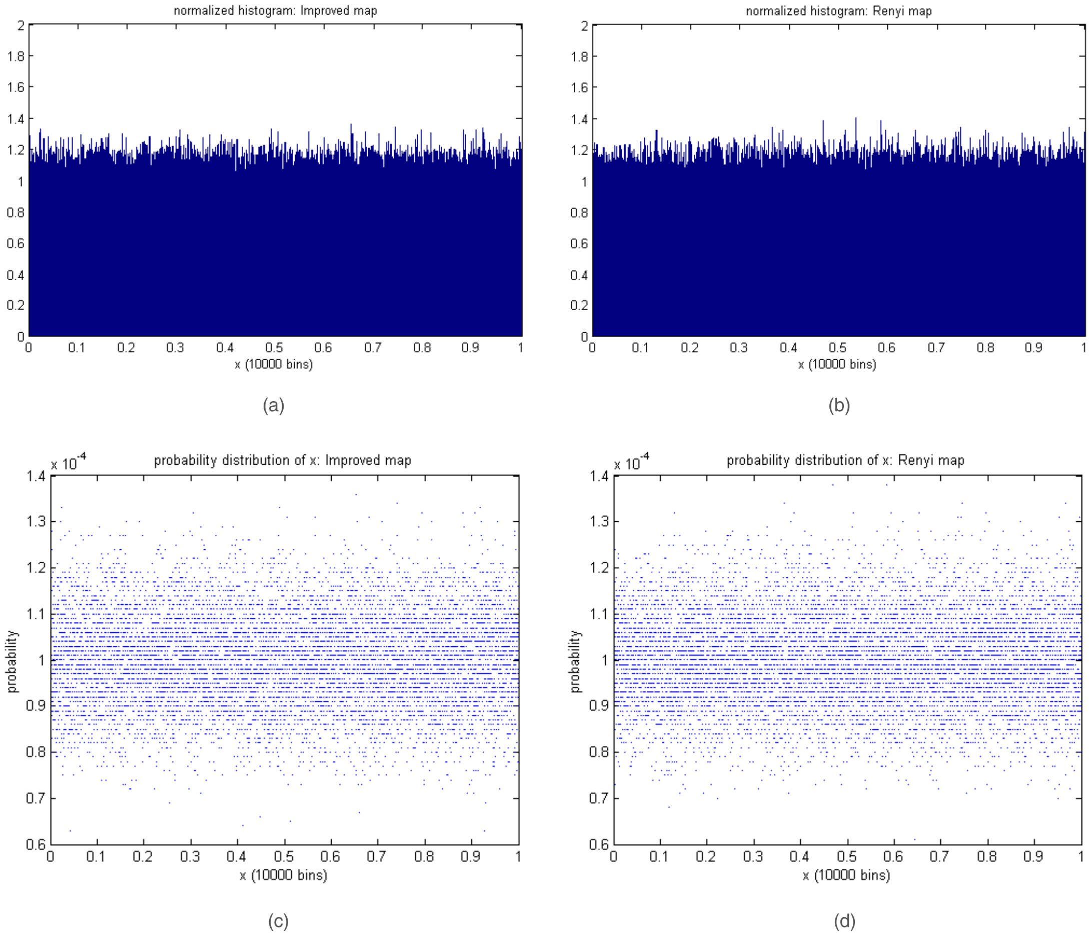

FIGURE 7. Trajectory points distribution as: (a)-(b) normalized histograms, and (c)-(d) probability distributions for chaotic Renyi and proposed map.

and shown in Fig. 7(c) and 7(d) for two maps, respectively. We can see from probability plots in Fig. 7(c) and 7(d) that most of trajectory points have probability equal to 0.0001. Hence, it is clear that the proposed chaotic map has invariance property and almost uniform-probability distribution similar to chaotic Renyi map.

F. RANDOMNESS

In chaos-based cryptographic applications, it is somewhat significant to assess the quality of randomness of chaotic map in generating the random numbers. The standard NIST SP800-22 test suite consisting of 15 statistical tests is performed. Each individual test in NIST suite computes a p-value which is compared with chosen significance level $\alpha = 0.01$. A test which has a p-value $> \alpha$ indicates that the sequence under specified test is random with a confidence of 99%, otherwise it is non-random [44]. If all p-values of NIST randomness suite are found greater than α, then sequence is said to possess satisfactory randomness. Three sequences are generated using proposed chaotic map which are converted to three binary sequences, each of size 1000000. The NIST randomness results of three sequences are evaluated and minimum of p-values for three sequences corresponding to 15 different test indicators are provided in Table 1 [45]. According to p-values in Table 1, we can infer that the sequence has passed all tests of NIST suite as each p-value is fairly higher than 0.01, which confirms the satisfaction of NIST SP800-22 randomness requirement from proposed chaotic map. Hence, the proposed chaotic map exhibits adequate randomness and suitable for use in cryptographic applications.

G. β-HILL CLIMBING SEARCH

Recently, a new local-search based meta-heuristic technique termed as β-hill climbing is proposed for global optimization by Al-Betar in [46]. It is an extension of hill climbing local search, which has the feature of exploration as well with exploitation of conventional hill climbing to overcome its problem of getting stuck in local optima [47]. The exploration in search methods is recommended to explore the regions that are not yet examined, if needed. The β-hill climbing incorporates stochastic operators to improve the overall efficiency over the base version and other variants as demonstrated in [46] and [48]. The new search technique begins with generation of initial random solution $X \in [LB_\mathrm{i}, UB_\mathrm{i}]$ (where LB_i and UB_i denote the lower and upper bounds

TABLE 1. Nist SP800-22 randomness results for proposed chaotic map.

NIST Test Name	Min p-value	Results
Frequency	0.292800	Passed
Block Frequency	0.871944	Passed
Runs Test	0.701640	Passed
Longest Runs Test	0.865930	Passed
Rank Test	0.541847	Passed
DFT Spectral	0.273595	Passed
Non-Overlapping Template Matching	0.035829	Passed
Overlapping Template Matching	0.607439	Passed
Maurer's Universal	0.361805	Passed
Linear Complexity	0.870490	Passed
Serial Test	0.519472	Passed
Approximate Entropy	0.136288	Passed
Cumulative Sums	0.257515	Passed
Random Excursions	0.182735	Passed
Random Excursions Variant	0.185612	Passed

for the decision variable $X(i)$) which is evaluated using computation of fitness values. In search loop for optimization of solution, β-hill climbing utilizes two operators namely neighboring operator i.e. N-operator and exploration operator i.e. β-operator. N-operator navigates to the neighboring solution X_1 from the current solution X, where $N \in [0, 1]$. This operator is considered as source for exploitation in search process as it generates neighboring solution from current solution. Through β-operator, the variables of new solution (after N-operator) $X_2(i)$, where $i \in [1, 2, \ldots, Size]$, are changed randomly based on the probability β according to following rule:

$$X_2(i) = \begin{cases} X_r & rnd \leq \beta \\ X(i) & else \end{cases}$$

This β-operator is the actual source of exploration and the exploration effect is controlled by the probability parameter $\beta \in [0, 1]$. Lastly, the S-operator is a greedy selection operator aimed to choose the solution X or X_2 depending whose fitness is better [49]. The pseudo-code of β-hill climbing is presented as:

Algorithm 1 β-Hill Climbing Pseudo-Code

```
$X\ (i) = LB(i) + (UB(i) - LB(i)) \times U(0, 1)$
Evaluate fitness of $X$
$itr = 0$
while ($itr \leq Max\_itr$)
    $X_1 = X$
    $X_1(i) = X_1(i) + U(0, 1) \times N$    // $N$-operator
    for $i = 1$ to $Size$
        if ($rnd_i \leq \beta$) // $\beta$-operator
            $X_2(i) = LB(i) + (UB(i) - LB(i)) \times U(0, 1)$
        end if
    end for
    Evaluate fitness of $X_2$
    if ($fitness(X2)$ is better than$fitness(X)$)
        $X = X_2$    // $S$-operator
    end if
    $itr = itr + 1$
end while
```

III. PROPOSED SUBSTITUTION-BOX METHOD

The proposed substitution-box method based on new 1D chaotic map and β-hill climbing search is presented in this section. Firstly, the new chaotic map is iterated starting from given x_0 for T times and the obtained chaotic values are discarded, except the last, to die out the transient effect. Then, initial solution X is generated with $U\ (0, 1)$, where $U(0, 1)$ are random chaotic values in [0, 1] from new chaotic map. Then, an initial 8×8 S-box candidate S is generated from X using *Generate*() routine. This routine prepare an S-box using input vector, wherein *sort*() function performs sorting of input array in increasing order. The appropriateness of current solution X_2 or S^* is determined by computing the S-box performance parameters such as nonlinearity, differential uniformity and BIC-nonlinearity. These parameters are opted as they are the mainly responsible metrics to resist the differential and linear cryptanalysis [5], [6]. The fitness of two competing solutions is decided as per the condition given in Eqn.(3). The parameters such as nonlinearity, differential uniformity and bits independence are discussed in next section.

$$F(S^*, S) = Fitness(S^*, S) = \begin{cases} true & if\ (nl(S^*) \geq nl(S) \& du(S^*) \leq du(S)\ \&\ bicnn(S^*) \geq bicnn(S)) \\ false & otherwise \end{cases} \tag{4}$$

Where, $nl(S^*)$ denotes the average nonlinearity of S^*, $du(S^*)$ denotes the differential uniformity of S^*, and $bicnn(S^*)$ denotes the minimum of bic-nonlinearity of S^*.

IV. PERFORMANCE RESULTS AND ANALYSIS

The proposed 8×8 S-box obtained for initial values set as $x_0 = 0.123456789$, $a = 4$, $b = 10$, $alpha = 12345$, $Size = 2^8$, $T = 500$, $\beta = 0.5$, $N = 0.00123$, $X^{min} = 0.01$, $X^{max} = 0.99$, $Max\_itr = 500000$ is shown in Table 2. The secret key consists of x_0, a, b, $alpha$, T, and β. All floating-point operations are performed as per IEEE-754 floating point standard of double floating point arithmetic. The performance of proposed S-box method

Algorithm 2 Proposed Substitution-Box Generation Method

```
Parameter initialization
  Set $x_0$, $a$, $b$, $alpha$, $Size$, $T$, $\beta$, $N$, $X^{\min}$, $X^{\max}$, $Max\_itr$
Initial solution generation
  $x_{\text{old}} = x_0$
  for $i = 1$ to $T$
    $x_{new} = newChaoticMap(x_{old}, a, b)$
    $x_{old} = x_{new}$
  end for
  for $i = 1$ to $Size$
    $U(0, 1) = newChaoticMap(x_{old}, a, b)$
    $X(i) = X^{\min} + (X^{\max} - X^{\min}) \times U(0, 1)$
    $x_{old} = U(0, 1)$
  end for
  $S = Generate(X)$
Optimized solution (s-box) search
  $counter = 0$
  while($counter \leq Max\_itr$)
    $X_1 = X$
    $k \in [1, Size]$
    $X_1(k) = X_1(k) + U(0, 1) \times N$
    $X_2 = X_1$
    for $i = 1$ to $Size$
      $rnd_i = newChaoticMap(x_{old}, a, b)$
      $x_{old} = rnd_i$
    if ($rnd_i \leq \beta$)
      $U(0, 1) = newChaoticMap(x_{old}, a, b)$
      $X_2(\text{i}) = X^{\min} + (X^{\max} - X^{\min}) \times U(0, 1)$
      $x_{old} = U(0, 1)$
    end if
  end for
  $S^* = Generate(X_2)$
  $F(S^*, S) = Fitness(S^*, S)$
  if ($F(S^*, S) == true$)
    $X = X_2$
    $S = S^*$
  end if
  increment $counter$
end while
```

is analyzed through standard criteria such as bijectivity, nonlinearity, strict avalanche criteria, bits independent criterion, differential uniformity, linear approximation probability, autocorrelation, transparency order, algebraic immunity, algebraic degree and discussed in this section. It is also compared with some recent optimization and chaos based 8 × 8 S-boxes to claim that the proposed S-box has better security strength than many of the existing S-boxes.

A. BIJECTIVITY

An 8 × 8 S-box is said to be bijective if its all 8 Boolean functions are 0/1 balanced, resulting that all 256 output values of S-box are distinct and bounded in [0, 2^8 -1]. A Boolean function f_i (i = 1, 2, …, 8) is 0/1 balanced if it satisfies [18], [24]

Algorithm 3 $S = Generate(X)$

```
$Y = Sort(X)$
for $k_1 = 1$ to $Size$
  $q = Y(k_1)$
  for $k_2 = 1$ to $Size$
    if ($q == X(k_2)$)
    $S(k_1) = k_2$- 1
    $break$
  end if
 end for
end for
```

$$hwt\left(\sum_{i=1}^{8} a_i f_i\right) = 2^8 - 1 \tag{5}$$

Where, $a_{\text{i}} \in \{0, 1\}$, $(a_1, a_2, \ldots, a_8) \neq (0, 0, \ldots, 0)$, and $hwt(.)$ is the hamming weight. Every Boolean function f_i basically needs to be 0/1 balanced so as not to leak any information to attacker [50]. It has been verified that the proposed S-box satisfies the property of bijectivity as all eight Boolean functions are balanced.

B. NONLINEARITY

The main purpose of an S box in block ciphers is to offer the nonlinear change from the secret information to the encoded information. The nonlinearity offered by the cipher is the most essential part of the entire security system [50]. The nonlinearity is connected to strong confusion and immunity of block ciphers to mitigate linear cryptanalysis. In practice, the nonlinearity for an 8-bit Boolean function f is computed using Walsh spectrum as [32], [50].

$$nonlinearity(f) = 2^7 - \frac{1}{2}\left(\max_{z\in\{0,1\}^8} \left|S_f(z)\right|\right) \tag{6}$$

Where $S_f(z)$ is the Walsh spectrum of Boolean function f, computed as:

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

Where, $x.\ z$ is the bitwise dot product and $z \in \{0, 1\}^8$. The eight nonlinearity scores for proposed S-box are 110, 112, 110, 110, 110, 110, 110, 110 having excellent minimum, maximum and average statistics as 110, 112, and 110.25, respectively. We can see that all nonlinearities are quite high and larger than or equal to 110. This means that the proposed S-box has excellent capability to offer high nonlinear transformation to resist related attacks.

C. STRICT AVALANCHE CRITERIA

Webster and Tavares brought in the strict avalanche criteria as requisite for good S-boxes [51]. For S-boxes, to satisfy SAC, the flipping of any single bit of input vector should leads to half change in output vector. Since, an avalanche

TABLE 2. Proposed 8 × 8 substitution-box.

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

of 50% is significant to diminish any correlation among I/O combination and fails to leak information. Any value closer to 0.5 is always viewed as honorable. In order to verify the SAC property, we determined the matrix by procedure given in [38] and provided in Table 3. It can be seen that all entries of this matrix are close to the 0.5. The average value of matrix, represents the SAC, comes out as 0.5 which is same as ideal value and shows that the proposed S-box satisfies the strict avalanche criterion excellently.

TABLE 3. SAC matrix.

0.546	0.421	0.453	0.5	0.484	0.546	0.531	0.484
0.468	0.484	0.515	0.468	0.5	0.437	0.5	0.5
0.515	0.531	0.468	0.5	0.515	0.515	0.5	0.453
0.484	0.531	0.468	0.515	0.531	0.468	0.5	0.546
0.468	0.5	0.437	0.609	0.546	0.531	0.468	0.468
0.453	0.453	0.562	0.468	0.5	0.531	0.5	0.531
0.546	0.484	0.484	0.562	0.484	0.468	0.531	0.515
0.5	0.5	0.453	0.484	0.515	0.546	0.468	0.531

D. BITS INDEPENDENCE CRITERIA

Bits independence is another equally crucial design criterion for strong S-boxes. Adams and Tavares suggested a method to test BIC in [38]. Assume $f_1, f_2, \ldots., f_8$ be the component Boolean functions of an 8 × 8 S-box. It was pointed out that if the S-box met BIC, the Boolean function $f_j \oplus f_k$ (where, $j \neq k$ and $1 \leq j, k \leq 8$) should be highly nonlinear and satisfies the avalanche criterion well [51], [52]. Therefore, BIC can be verified by calculating nonlinearity and SAC of all 56 functions $f_\mathrm{j} \oplus f_\mathrm{k}$ for any 8 × 8 bijective S-box. The possible scores of nonlinearities and SAC of functions $f_\mathrm{j} \oplus f_\mathrm{k}$ for proposed S-box are computed and shown in Table 4 and 5. The average scores of BIC with respect to nonlinearities and SAC are found as 105.21 and 0.5, respectively. The obtained scores justify the excellent performance of proposed S-box for bits independent criterion.

TABLE 4. Bits independence criterion with respect to nonlinearity.

f	1	2	3	4	5	6	7	8
1	-	106	108	104	106	104	106	104
2	106	-	104	106	106	104	106	104
3	108	104	-	106	106	108	104	104
4	104	106	106	-	106	104	104	106
5	106	106	106	106	-	106	106	106
6	104	104	108	104	106	-	104	104
7	106	106	104	104	106	104	-	104
8	104	104	104	106	106	104	104	-

E. DIFFERENTIAL UNIFORMITY

The measure of differential uniformity is accounted to find S-box capability to resist potential differential cryptanalysis. It is a chosen plaintext attack framed by Biham and Shamir to assault DES-like block ciphers [5], [53]. Differential uniformity (DU) represents maximum likelihood of generating an output differential $\Delta y = y_i \oplus y_j$ when input differential is $\Delta x = x_i \oplus x_j$. In this method, the XOR distribution between inputs and outputs of S-box is determined. Mathematically, it is quantified as

$$DU_S = \max_{\Delta x \neq 0, \Delta y} (\# \{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}) \qquad (7)$$

TABLE 5. Bits independence criterion with respect to SAC.

f	1	2	3	4	5	6	7	8
1	-	0.506	0.480	0.506	0.476	0.509	0.523	0.519
2	0.505	-	0.519	0.517	0.5	0.506	0.48	0.515
3	0.480	0.519	-	0.515	0.523	0.509	0.494	0.529
4	0.506	0.517	0.515	-	0.498	0.519	0.494	0.498
5	0.476	0.5	0.523	0.498	-	0.494	0.496	0.498
6	0.509	0.506	0.509	0.519	0.494	-	0.523	0.486
7	0.523	0.480	0.494	0.494	0.496	0.523	-	0.505
8	0.519	0.515	0.529	0.498	0.498	0.486	0.506	-

Its value should be as low as possible to resist the Biham and Shamir cryptanalysis. The possible I/O XOR differential distribution for proposed S-box is evaluated and listed in Table 6. The Table shows that the DU of our S-box is 10 and whose count in the whole differential distribution is only 3.

TABLE 6. I/O XOR differential distribution matrix.

6	8	8	6	6	6	8	6	8	6	6	8	6	6	6	6
8	6	6	8	6	6	6	6	8	8	6	8	6	8	4	8
6	6	8	6	8	6	8	6	6	8	8	6	8	6	6	8
8	6	6	6	6	6	6	6	6	6	6	6	8	8	8	6
6	8	6	6	6	6	6	6	8	6	6	6	6	6	8	6
6	8	8	4	10	4	6	6	8	6	6	6	8	6	6	8
6	6	6	6	6	8	6	6	8	6	4	8	8	6	8	4
6	6	8	6	6	6	8	6	6	6	6	6	6	8	8	6
8	6	6	6	6	4	6	8	6	8	8	8	8	6	6	8
6	6	6	6	6	6	6	6	6	6	6	6	8	8	6	6
6	6	8	6	6	8	6	6	6	8	6	8	8	6	6	6
6	8	6	8	8	6	6	10	6	8	8	8	8	6	8	8
6	8	8	6	8	8	6	6	6	8	6	8	6	6	8	8
6	8	6	6	6	4	6	6	6	6	6	6	6	6	6	10
8	8	6	6	6	8	6	8	8	8	8	6	8	8	6	6
6	8	8	4	6	8	6	6	6	6	6	6	8	8	6	-

F. LINEAR APPROXIMATION PROBABILITY

A known-plaintext attack was regulated by Matsui to break popular DES block cipher in 1993 which is famously referred as linear cryptanalysis [6]. This analysis approximates relationship between inputs, outputs and key. The magnitude of linear approximation probability (LP) should be aimed to keep as low as possible to resist this attack [6]. According to Matsui, LP is highest value of event that parity of incoming bit selected by mask ω_x is same as parity of output bits chosen by mask ω_y. It is expressed mathematically as:

$$LP = \max_{\omega_a,\omega_b \neq 0} \left| \frac{\#\{a \in A \,|\, a.\omega_a = S(a).\omega_b\}}{2^8} - \frac{1}{2} \right| \qquad (8)$$

Where, A is set of all possible inputs a whose cardinality is 2^8 for an 8×8 S-box. Any S-box having lower LP score tends to have better resistance to linear cryptanalysis. The maximum value of LP for proposed S-box comes out only 0.1250, which is fairly low to claim that it can resist the Matsui's linear cryptanalysis for S-boxes.

G. AUTO-CORRELATION FUNCTION

The auto-correlation function (ACF) of a Boolean function f is computed as [54]:

$$r_f(d) = \sum_{\forall x,d \in \{0,1\}^n} (-1)^{f(x)}(-1)^{f(x \oplus d)} \qquad (9)$$

Where, $r(0) = 2^n$ for every Boolean function, and for other possible inputs $r(d) \in [2^{-n}, 2^n]$. The maximum score of ACF known as absolute indicator of Boolean function f is used to ascertain the cryptographic quality to have good diffusion property [55]. It is denoted as:

$$|ACF_f| = \max\left(\left|r_f(d)\right|\right) \quad for\ d \neq 0$$

This cryptographic metric ACF of Boolean function f is extended to S-box S: $\{0, 1\}^n \rightarrow \{0, 1\}^n$ by considering all $2^n - 1$ non-zero linear combinations F of its n component functions. using the following equation [56].

$$|ACF_S| = \max\left(\left|r_{F_i}(w)\right|\right) \; w = 1, \ldots, 2^n \quad i = 1, \ldots, 2^n - 1 \qquad (10)$$

The ACF of S-box should be as small as possible for cryptographic strength. The maximum ACF for proposed S-box comes out as 96. It is also computed for all S-boxes listed in Table 7 and scores are provided in same comparison Table.

H. TRANSPARENCY ORDER

Prouff introduced the metric of transparency order which is used to quantify the resistance of S-box to differential power analysis (DPA) attacks [57]. It has been pointed out that some cryptographically strong Boolean functions or S-boxes found to have low robustness to DPA attacks like AES inverse mappings [58]. According to Prouff, the transparency order τ_S of an S-box S can be computed as per the following formulation [57], [58], (11) as shown at the top of the next page

Where, $HW(\beta)$ denotes the hamming weight of β, and $W_{\alpha,S}(u, v)$ is calculated as

$$W_{\alpha,S}(u, v) = \sum (-1)^{v.\{S(x) \oplus S(x \oplus \alpha)\} \oplus u.x}$$

If an S-box has smaller transparency order, then it tends to show more resistance towards DPA attacks. The transparency orders (TOs) of proposed S-box founds as 7.824. The TO of other S-boxes under comparison are also determined and listed in Table 7

I. ALGEBRAIC IMMUNITY

Algebraic immunity (AI) denotes the resistance of an S-box against algebraic attacks and inversely the effectiveness of the XSL attack. The procedure of computing the algebraic immunity $AI(f)$ of Boolean function f is explained in [59]. The algebraic immunity of an $n \times n$ S-box S is defined in

$$\tau_S = \max_{\beta\in F_2^n}\left(|n-2HW(\beta)| - \frac{1}{2^{2n}-2^n}\sum_{\alpha\in F_2^{n*}}\left|\sum_{\substack{v\in F_2^n\\ HW(v)=1}}^{m}(-1)^{v.\beta}W_{\alpha,S}(0,v)\right|\right) \tag{11}$$

terms of the algebraic immunity AI of n component Boolean functions as [53]:

$$AI(S) = \min_{c\in F_2^n}(AI(c_1f_1 \oplus c_2f_2 \oplus \ldots\ldots \oplus c_nf_n)) \tag{12}$$

Where, $c = (c_1, c_2, \ldots, c_\mathrm{n})$ be non-zero elements in S-box, and $c_1f_1 + c_2f_2 + \ldots + c_\mathrm{n}f_\mathrm{n}$ is a linear combination of component Boolean functions. A high score of algebraic immunity is desirable to complicate algebraic attacks on S-boxes. The algebraic immunity of all S-boxes provided in Table 7 is found same which is equal to 4.

J. ALGEBRAIC DEGREE

The notion of algebraic degree of Boolean functions is extended to S-boxes to determine their strength of resistance to higher-order differential cryptanalysis [1], [60]. Algebraic degree of an n-variable Boolean function f is defined as degree of polynomial representing the algebraic normal form (ANF) of Boolean function f. That is, it is the number of variables in largest monomial in its ANF. An $n \times n$ S-box consists of n Boolean functions in n-variables. Algebraic degree of S-box S is the minimum degree of all component Boolean functions f_i [50]. Mathematically,

$$\deg(S) = \min(\deg(f_1), \deg(f_2), \ldots, \deg(f_n)) \tag{13}$$

The algebraic degree of n-1 correspond to upper bound for an $n \times n$ S-box. In [61], a preferable score of deg $(S) \geq 4$ was suggested to withstand higher-order differential attack. It has been found that all S-boxes listed in comparison Table 7 have an algebraic degree equal to upper bound i.e. 7.

TABLE 7. Performance Comparison of Chaotic and Optimization Based 8 × 8 substitution-boxes.

S-box S	Nonlinearity			SAC	BIC-NL (min)	BIC-SAC	DU	LP	|ACF|	TO
	min	max	average							
Proposed	110	112	110.25	0.5	104	0.5052	10	0.125	96	7.824
Wang [18]	108	108	108	0.5068	96	0.5017	10	0.1406	96	7.830
Wang [19]	108	110	109	0.5026	102	0.5026	10	0.1406	104	7.828
Guesmi [20]	106	110	107.5	0.4971	96	0.5034	10	0.125	96	7.823
Ahmad [21]	106	110	107	0.5015	98	0.5016	10	0.1484	96	7.821
Ye [22]	106	110	108	0.5073	100	0.502	10	0.1523	96	7.815
Ahmad [24]	106	110	107.5	0.5036	90	0.504	10	0.1484	104	7.807
Farah [25]	104	110	106.5	0.4995	98	0.4983	10	0.1172	96	7.810
Hussam [26]	106	108	107.5	0.4943	98	0.4982	10	0.125	96	7.815
Zhang [27]	108	110	108.75	0.4946	94	0.5054	10	0.1328	104	7.817
Lambic [31]	108	112	109.25	0.5012	104	0.5056	8	0.0937	72	7.834
Lambic [32]	106	108	106.75	0.5034	100	0.4951	10	0.1328	104	7.798
Ataullah [33]	106	108	106.75	0.4939	102	0.504	16	0.125	168	7.825
Attaullah [34]	106	108	107.25	0.5034	98	0.498	12	0.1328	104	7.833
Özkaynak [35]	106	108	106.75	0.4941	98	0.4957	10	0.125	96	7.809
Ye [36]	104	108	106.75	0.4076	98	0.5022	10	0.1328	96	7.827
Solami [39]	106	110	108.5	0.5017	100	0.5026	10	0.1328	96	7.826
Garcia [62]	105	107	106	0.5066	96	0.5065	12	0.1445	96	7.810
AES [63]	112	112	112	0.5058	112	0.504	4	0.0625	32	7.860
Gray [64]	112	112	112	0.5058	112	0.502	4	0.0625	32	7.860
APA [65]	112	112	112	0.4987	112	0.4993	4	0.0625	32	7.859

K. COMPARISON

Based on the discussed security criterias, the performance of proposed S-box, in Table 1, is compared with recent state-of the art optimization based S-boxes, chaos-based S-boxes and number-theoretic inverse-power mapping based AES, Gary, APA S-boxes in Table 7. On comparing with these S-boxes, we find that:

- The average of nonlinearity score for proposed S-box is 110.25 which is largest compared to S-boxes Table 7. The other statistics like minimum (110) and maximum (112) of nonlinearities are also higher than most of the S-boxes except AES, Gray, APA S-boxes which has optimal nonlinearity of 112. Means, the proposed S-box method is capable to generate S-boxes with high nonlinearity for better nonlinear transformation of input plaintext bits to cipher bits.
- As discussed that the ideal value of SAC is 0.5. It is evident from the comparison Table 7 that our SAC of 0.5 is exactly equal to ideal value of 0.5 and comparable to SAC of other S-boxes including AES, Gray, APA S-boxes. Hence, like other chaos-based S-boxes, the proposed S-box also yields close to ideal result to satisfy the SAC criteria well.
- The minimum of BIC result for nonlinearity is 104 which considerably higher than other chaos-and-optimization based S-boxes in Table 7. The average is 105.214. The BIC result for SAC is 0.5052. As desired, our BIC-nonlinearity is much higher than other S-boxes and BIC-SAC is closest to the ideal SAC value. The BIC-nonlinearity performance of our S-box is the most optimal and better among all S-boxes except AES, Gray, APA S-boxes.
- The differential uniformity of our S-box comes out as 10 which is comparable to S-boxes in [18]–[22], [24]–[27], [32], and [34]–[36]. But, it is significantly better than that of S-boxes proposed constructed in [33], [34], and [62]. Where as, the Lambic S-box in [31], AES, Gray, and APA S-boxes have uniformities of 8, 4, 4, and 4, respectively.
- According to linear cryptanalysis of Matsui, the linear approximation probability should be kept as low as possible which has a value of 0.125 for our S-box. We can see that proposed S-box offers better resistant to Matsui attack as compared to most of the S-boxes in Table 7 except in [25], [31], and [63]–[65].
- A lower value of maximum absolute autocorrelation function of S-boxes is desirable for cryptographic strength. The maximum absolute ACF for our S-box is 96 which is fairly better than ACF of S-boxes in [19], [24], [27], and [32]–[34], comparable to [18], [20]–[22], [25], [26], [35], [36], [39], [62]. Compared to these recent S-boxes, the proposed S-box is able to provide better autocorrelation property and diffusion. The ACF score for our S-box is higher than that of Lambic S-box [31], AES, Gray, APA S-boxes.
- It is known that AES, Gray, and APA S-boxes holds some optimal S-box performance scores for nonlinearity, BIC, maximum ACF, LP, and therefore considered as cryptographically most strong S-boxes. But, they are found to have high transparency order. These three S-boxes have TO of 7.86 and are higher compared to all S-boxes of Table 7. Hence, they offer lowest resistance towards DPA attacks. The proposed S-box has transparency order of 7.824 which is lower i.e. better than S-boxes in [18], [19], [31], [33], [34], [36], [39], and [63]–[65], and higher than other S-boxes.

V. CONCLUSION

This paper reports a novel method to search optimal configuration of substitution-box using improved discrete-chaotic map and β-hill climbing technique. To inhibit the limitations of chaotic logistic map for designing security applications like S-boxes, we proposed a new improved 1D chaotic map. The new chaotic map found to possess better dynamic, lyapunov exponent, bifurcation and larger chaotic range compared to logistic map. The features of new chaotic map make it more suitable for generating efficient S-boxes with guided search using β-hill climbing which have the balance of exploration and exploitation characteristics. The S-box generated with proposed method is tested and analyzed to assess security strength under some well-accepted and standard parameters specific to S-boxes. The obtained performance parameters show that the generated S-box has good cryptographic strength and found better as compared to recent S-boxes available in literature. Hence, the proposed method is competent to yield efficient S-boxes needed for the design of strong block cryptosystems.

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. 29, pp. 656–715, Oct. 1949.

[3] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York, NY, USA: Wiley, 1996.

[4] S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 1994, pp. 17–25.

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

[6] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 1994, pp. 386–397.

[7] 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, 1995.

[8] 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.

[9] M. Ahmad, M. N. Doja, and M. M. S. Beg, "ABC optimization based construction of strong substitution-boxes," *Wireless Pers. Commun.*, vol. 101, no. 3, pp. 1715–1729, Aug. 2018.

[10] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. Boston, MA, USA: Perseus Books, 1994.

[11] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, 3rd Quart., 2001.

[12] L. Kocarev and S. Lian, *Chaos-Based Cryptography*, vol. 354. Berlin, Germany: Springer-Verlag, 2011.

[13] M. A. Chenaghlu, S. Jamali, and N. N. Khasmakhi, "A novel keyed parallel hashing scheme based on a new chaotic system," *Chaos, Solitons Fractals*, vol. 87, pp. 216–225, Jun. 2016.

[14] Z. Hua, B. Zhou, and Y. Zhou, "Sine-transform-based chaotic system with FPGA implementation," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2557–2566, Mar. 2018.

[15] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new Beta chaotic maps," *Opt. Lasers Eng.*, vol. 96, pp. 39–49, Sep. 2017.

[16] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.

[17] G. Chen, "A novel heuristic method for obtaining S-boxes," *Chaos, Solitons Fractals*, vol. 36, no. 4, pp. 1028–1036, 2008.

[18] 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, 2012.

[19] W. Yong and L. Peng, "An improved method to obtaining S-box based on chaos and genetic algorithm," *HKIE Trans.*, vol. 19, no. 4, pp. 53–58, 2012.

[20] R. Guesmi, M. A. Ben Farah, A. Kachouri, and M. Samet, "A novel design of chaos based S-boxes using genetic algorithm techniques," in *Proc. IEEE/ACS 11th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2014, pp. 678–684.

[21] M. Ahmad, D. Bhatia, and Y. Hassan, "A novel ant colony optimization based scheme for substitution box design," *Procedia Comput. Sci.*, vol. 57, pp. 572–580, 2015.

[22] 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, 2016.

[23] Y. Tian and Z. Lu, "Chaotic S-box: Intertwining logistic map and bacterial foraging optimization," *Math. Problems Eng.*, vol. 2017, Nov. 2017, Art. no. 6969312.

[24] M. Ahmad, N. Mittal, P. Garg, and M. M. Khan, "Efficient cryptographic substitution box design using travelling salesman problem and chaos," *Perspect. Sci.*, vol. 8, pp. 465–468, Sep. 2016.

[25] 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.

[26] 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.*, pp. 1–18, May 2018.

[27] 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.*, to be published, doi: 10.1109/TCYB.2018.2846186.

[28] G. Liu, W. Yang, W. Liu, and Y. Dai, "Designing S-boxes based on 3-D four-wing autonomous chaotic system," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1867–1877, 2015.

[29] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S_8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Jan. 2016.

[30] Ü. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar, "A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear Dyn.*, vol. 87, no. 2, pp. 1081–1094, 2017.

[31] 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.

[32] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn*, vol. 87, no. 4, pp. 2407–2413, 2017.

[33] A. Ullah, S. S. Jamal, and T. Shah, "A novel construction of substitution box using a combination of chaotic maps with improved chaotic range," *Nonlinear Dyn.*, vol. 88, no. 4, pp. 2757–2769, 2017.

[34] A. Ullah, S. S. Jamal, and T. Shah, "A novel algebraic technique for the construction of strong substitution box," *Wireless Pers. Commun.*, vol. 99, no. 1, pp. 213–226, 2017.

[35] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," *Neural Comput. Appl.*, pp. 1–10, Nov. 2018, doi: 10.1007/s00521-017-3287-y.

[36] T. Ye and L. Zhimao, "Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling," *Nonlinear Dyn.*, pp. 1–12, Jul. 2018.

[37] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459–467, Jun. 1976.

[38] M. Ibnkahla, *Signal Processing for Mobile Communications Handbook*. Boca Raton, FL, USA: CRC Press, 2005, ch. 27.

[39] E. A. Solami, M. Ahmad, C. Volos, M. N. Doja, and M. M. S. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Dec. 2018.

[40] G.-C. Wu and D. Baleanu, "Chaos synchronization of the discrete fractional logistic map," *Signal Process.*, vol. 102, pp. 96–99, Sep. 2014.

[41] A. A. Elsadany, A. M. Yousef, and A. Elsonbaty, "Further analytical bifurcation analysis and applications of coupled logistic maps," *Appl. Math. Comput.*, vol. 338, pp. 314–336, Dec. 2018.

[42] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proc. Nat. Acad. Sci. USA*, vol. 88, no. 6, pp. 2297–2301, 1991.

[43] S. Pincus, "Approximate entropy (ApEn) as a complexity measure," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 5, no. 1, pp. 110–117, 1995.

[44] L. E. Bassham, III, *et al.*, "SP 800-22 Rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-22, 2010.

[45] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[46] M. A. Al-Betar, "β-hill climbing: An exploratory local search," *Neural Comput. Appl.*, vol. 28, no. S1, pp. 153–168, 2016.

[47] S. S. Skiena, *The Algorithm Design Manual*. London, U.K.: Springer, 2008.

[48] Z. A. A. Alyasseri, A. T. Khader, M. A. Al-Betar, and M. A. Awadallah, "Hybridizing β-hill climbing with wavelet transform for denoising ECG signals," *Inf. Sci.*, vol. 429, pp. 229–246, Mar. 2018.

[49] E. Alsukni, O. S. Arabeyyat, M. A. Awadallah, L. Alsamarraie, I. Abu-Doush, and M. A. Al-Betar, "Multiple-reservoir scheduling using β-hill climbing algorithm," *J. Intell. Syst.*, pp. 1–12, 2017, doi: 10.1515/jisys-2017-0159.

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

[51] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 1986, pp. 523–534.

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

[53] C. A. Wood, "Large substitution boxes with efficient combinational implementations," M.S. thesis, Rochester Inst. Technol., Rochester, NY, USA, 2013.

[54] L. D. Burnett, "Heuristic optimization of Boolean functions and substitution boxes for cryptography," Ph.D. dissertation, Fac. Inf. Technol., Inf. Secur. Inst., Queensland Univ. Technol., Brisbane, QLD, Australia, 2005.

[55] S. Kavut, "Results on rotation-symmetric S-boxes," *Inf. Sci.*, vol. 201, pp. 93–113, Oct. 2012.

[56] X.-M. Zhang and Y. Zheng, "GAC—The criterion for global avalanche characteristics of cryptographic functions," *J. Univ. Comput. Sci.*, pp. 320–337, 1996.

[57] E. Prouff, "DPA attacks and S-boxes," in *Fast Software Encryption* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2005, pp. 424–441.

[58] B. Mazumdar, D. Mukhopadhyay, and I. Sengupta, "Constrained search for a class of good bijective S-boxes with improved DPA resistivity," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2154–2163, Dec. 2013.

[59] F. Didier and J.-P. Tillich, "Computing the algebraic immunity efficiently," in *Fast Software Encryption* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2006, pp. 359–374.

[60] L. R. Knudsen, "Truncated and higher order differentials," in *Fast Software Encryption* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 1995, pp. 196–211.

[61] G. Piret, T. Roche, and C. Carlet, "PICARO—A block cipher allowing efficient higher-order side-channel resistance," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2012, pp. 311–328.

[62] V. 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.

[63] J. Daemen and V. Rijmen, *The Design of RIJNDAEL: AES—The Advanced Encryption Standard*. Berlin, Germany: Springer-Verlag, 2002.

[64] M. T. Tran, D. K. Bui, and A. D. Duong, "Gray S-box for advanced encryption standard," in *Proc. Int. Conf. Comput. Intell. Secur.*, 2008, pp. 253–258.

[65] L. Cui and Y. Cao, "A new S-box structure named affine-power-affine," *Int. J. Innov. Comput., Inf. Control*, vol. 3, no. 3, pp. 751–759, 2007.

AMER AWAD ALZAIDI received the bachelor's degree in computer science from Taif University, Saudi Arabia, the master's degree in computer science from the University of Bradford, U.K., and the Ph.D. degree in artificial intelligence from the Department of Computer Science, University of York, U.K. He is currently the Founder of the Computation and Islamic Finance Special Interest Group, University of York. He is also the Dean at the University of Jeddah, Saudi Arabia. He has a number of research articles of international repute to his credit. His area of research interest includes, but not limited to, artificial intelligence, re-engineering, secure banking and finance, 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. He is currently with the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India, as an Assistant Professor. He has published about 60 research articles in refereed journals and conference proceedings of international repute. His areas of research interest include multimedia security, chaos-based cryptography, and cryptanalysis and image processing.

M. N. DOJA received the B.Sc. (Engg.) degree from the Birla Institute of Technology, India, the M.Tech degree from IIT Delhi, and the Ph.D. degree from Jamia Millia Islamia (JMI), New Delhi. He is currently the Founder Head and a Professor of the Department of Computer Engineering, JMI. He has published various books and has over 100 publications in the journals and conferences of national and international esteem. His research areas include computer networks, mobile wireless networks, network security, artificial intelligence, and soft computing. He is a peer reviewer of various international journals and conferences.

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

M. M. SUFYAN BEG received the B.Tech. degree from Aligarh Muslim University, India, in 1992, the M.Tech. degree from IIT Kanpur, India, in 1994, and the Ph.D. degree from IIT Delhi, India, in 2002. He also visited the University of California at Berkeley as a BT Fellow. He is currently a Professor with the Department of Computer Engineering, Aligarh Muslim University, India. He has published 16 book chapters and over 120 papers on a wide range of topics in Web mining and soft computing. His current research interests are in the areas of parallel and distributed processing, soft computing, question answering systems, natural language processing, and Web mining and searching.