IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 July 2022, accepted 14 August 2022, date of publication 26 September 2022, date of current version 1 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3209202

RESEARCH ARTICLE

Multi-Objective Evolution of Strong S-Boxes Using Non-Dominated Sorting Genetic Algorithm-II and Chaos for Secure Telemedicine

MUSHEER AHMAD[1], REEM ALKANHEL[2], (Member, IEEE), WALID EL-SHAFAI[3,4], ABEER D. ALGARNI[2], FATHI E. ABD EL-SAMIE[3], AND NAGLAA F. SOLIMAN[2]

[1]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[3]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[4]Security Engineering Laboratory, Department of Computer Science, Prince Sultan University, Riyadh 11586, Saudi Arabia

Corresponding authors: Musheer Ahmad (musheer.cse@gmail.com) and Reem Alkanhel (rialkanhal@pnu.edu.sa)

This work was supported by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Research Funding Program under Grant FRP-1443-11.

ABSTRACT There exist several performance criteria for cryptographically-strong substitution boxes (S-boxes), which are often conflicting with each other. Constructing S-boxes that satisfy multiple criteria with optimal tradeoffs is one of the challenging tasks for cryptographers. In practice, the existing S-box design algorithms are used to optimize performance according to a single performance criterion, mainly the nonlinearity, which usually results in weak scores for other equally-significant criteria. To overcome this problem, a multi-objective optimization-based method is presented in this paper. In this method, 8×8 S-boxes are constructed satisfying multiple criteria of balancedness, high nonlinearity, low differential uniformity, and low auto-correlation. Multiple objectives are fulfilled by applying the chaos-assisted non-dominated sorting genetic algorithm-II to introduce the S-boxes. The performance assessment of the proposed method and the comparative analysis with available optimization tools and other state-of-the-art algorithms demonstrate its proficiency in generating significantly-better S-box solutions with good Pareto-optimal security features. Eventually, the S-boxes with minimum nonlinearity (NL) of 110, differential uniformity (DU) as low as 8, and auto-correlation function (ACF) as low as 80 are obtained after the optimization. Furthermore, the obtained Pareto-optimal S-box is utilized to put forward a medical image encryption algorithm for secure telemedicine services. The suggested encryption algorithm uses an S-box to perform the required permutation and diffusion of images. The encryption performance assessment and comparison analyses validate its effectiveness for securing medical imagery data in telemedicine networks.

INDEX TERMS Multi-objective evolution, substitution box, NSGA-II, chaotic map, telemedicine.

I. INTRODUCTION

The field of information technology has gone through fast progression throughout the long term and has wound up consolidated into different fields that incorporate businesses, broadcasting, defence, medical care, medication, and so on. Data is stored on an advanced gadget, and data sharing is accomplished by broadcasting in a communication network. The problem of getting safe data communication provokes multiplying interest of cryptographic designs, which is more capable of thwarting illegal and unauthorized consumption of private and personal data [1]. To handle the prominent security issues, the present-day block ciphers have been undertaking a significant role for the past couple of years. To have high resistance against attacks is very important for a cipher. During 1949, Claude E. Shannon put forward two properties for codes to hinder diffusion and cryptanalysis confusion. Diffusion conceals the connection between the plaintext and

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

ciphertext. The connection between the cipher and the key is convoluted by confusion [2], [3]. These features have changed the foundations of the design of present-day block ciphers. The building block that helps in creating confusion in block ciphers is the S-box [4], [5]. Block cipher security intensely relies upon the power and cryptographic quality of the adopted S-boxes. These S-boxes are chief parts of the block security systems at substitution phases, which are intended to complete the nonlinear change and thus induce confusion. Weak S-boxes used in DES are responsible for making it frail under related cryptanalysis. On the other hand, strong cryptographic S-boxes provide resistance to relieve such attacks [6], [7]. Hence, the focal idea of S-boxes is that the security of cryptosystems has effectuated generous exploration in the design of stronger S-boxes. Consequently, the S-box generation techniques have acquired critical significance and are a prominent field of research in security [8].

An S-box of size $n \times n$ is a numerical 1 to 1 mapping S from bitstrings of $\{0, 1\}^n$ to $\{0, 1\}^n$. It is likewise viewing a multi-input and multi-output Boolean function as $S(x) = [f_{n-1}(x), f_{n-2}(x), \ldots, f_1(x), f_0(x)]$, $f_i(0 \leq i \leq n-1)$ is an n-variable capacity characterized as f_i: $\{0, 1\}^n \rightarrow \{0, 1\}$ [9]. An S-box with input and output bits of length n is also referred to as a bijective S-box. The quantity of pre-images of every output appears only once and must lie in the interval of $\{0, 1, 2, \ldots, 2^n - 1\}$. S-boxes are fundamental parts of cryptosystems innately utilized in block ciphers. Their security significantly depends on the intensity mapping of S-boxes, nonlinearly changing plaintext into ciphertext. Finally, the symmetric cryptosystem power intensely relies upon the employed cryptographic strength of S-boxes, which weighs on their design method. Hence, for a good symmetric cryptosystem, designing strong S-boxes is truly fundamental [10]. The strategies dependent on algebraic methods are examined as they show solid properties like resilience to differential/linear cryptanalyses and nonlinearity whose value is high [11]. Ongoing mathematical cryptanalysis has uncovered that they are prune to algebraic attacks [12]. Accordingly, rather than focusing on algorithms based on algebraic methodologies, the researchers are investigating alternative S-box design methods to develop stronger S-boxes. Various optional methodologies have been explored in the recent years to produce S-boxes depending on various optimization techniques and chaotic systems [13], [14], [15], [16], [17], [18].

The literature work shows that a considerable number of S-box studies have been presented, depending on chaotic systems and transformative methods that can be utilized for producing better S-boxes. G. Chen used the concepts of chaotic swapping and the simulated annealing heuristic to pursue robust S-boxes, which fulfill the significant performance criteria in [19]. Wherein, the Baker map, which is chaotic in nature, is utilized to investigate the searchable topic for conceivable S-boxes. An efficient S-box has been generated based on the chaotic Chebyshev map. The use of genetic algorithms for S-box optimization was introduced by Wang *et al.* [20] and Guesmi *et al.* [21]. The initial population and control parameters for the genetic algorithms are spawned using a 1-D logistic map and a chaotic tent map [20]. In [21], 3D chaotic Lorenz system was used with the logistic map for mutation and crossover during the genetic algorithm operation. Optimization of insect colony was applied to create an optimized arrangement of 8×8 S-boxes [22]. For the generation of the initial S-box that is changed to a moving salesman problem via edge matrix, it is reiterated by a balanced chaotic tent map via the logistic map to show good resistance to attacks. Investigations of 6D hyper-chaotic and artificial optimization of bee colony algorithm were introduced for building sturdy 8×8 S-boxes [23]. Another strategy, including chaos and optimization based on teaching-learning for the S-boxes, was proposed by Farah *et al.* [24] to acquire keys for building S-boxs. In [25], Hussam *et al.* explored the firefly algorithm (FA) for enhancing an S-box produced from a discrete chaotic map. In [26], Zhang *et al.* innovatively utilized the operators known as I-Ching operators extracted from Chinese I-Ching literature to build optimized S-boxes. In most of the optimization-based S-box studies available in the literature, only a single performance parameter (usually the nonlinearity measure) has been adopted for optimal S-box design.

Image broadcasting and communication on uncertain channels is an indispensable task that should be considered because of the reformist extension of the Internet and communication networks. Interlopers might essentially recover the transmitted, broadcasted digital images because of the deficiency of protection on the Internet and telecommunication systems [27]. Accordingly, ensuring the security of the transmitted images has turned into a fundamental concern. The need to secure medical information, particularly clinical images, is expanding step by step [28]. The dependability, the wellbeing of capacity, and correspondence of digital images are significant worries in a few. The expert classification depends on electronic medical images. Thusly, because of the fast enhancement in the medical sector and telemedicine administrations, the transfer of electronic medical images distantly among a few hospitals is required. In applied telemedicine, the therapy, diagnosis, and treatment rely upon the clinical images of the person to be treated, which are imparted between different areas with modern communication networks [29], [30]. Because of the impact of noise and interlopers, erratic issues might influence the nature of the communicated images. Digital medical images should have a zero-tolerance, as they address trusted and private information [31], [32], [33]. An effective encryption scheme is needed in order to offer an adequate security of the sensitive data shared or exchanged over insecure channels in telemedicine networks. Here, a simple yet efficient encryption method based on generating strong S-boxes is advocated to secure the clinical imagery data exchanged between specialists and patients during tele-consultation for the correct case diagnosis as a secure telemedicine service.

In this paper, we introduce an approach that can satisfy multiple performance criteria instead of only one. Three crucial performance parameters of strong S-boxes have been optimized using the multi-objective optimization NSGA-II method. In addition, an image encryption scheme is suggested for securing clinical imagery data of patients in telemedicine networks. The significant contributions made in the paper are as follows:

1. A novel method for multi-parameter optimization for generating secure 8×8 S-boxes using NSGA-II is presented.
2. Three crucial performance parameters, namely nonlinearity (NL), differential uniformity (DU), and auto-correlation function (ACF), are considered for multi-objective optimization to obtain Pareto-optimal S-boxes.
3. A discrete chaotic map is utilized to generate initial populations and values of other variables of the proposed method.
4. The performance of the proposed method is analyzed and a comparison of the generated S-boxes with existing related S-boxs is also presented.
5. The designed S-boxes are applied to secure the digital medical imagery data used in the telemedicine environment to validate its suitability for the encryption of healthcare radiological and other imagery data.
6. The performance of medical image encryption is assessed against statistical analysis, confirming the good encryption quality.

The remaining parts of the paper are offered as follows. The details of the NSGA-II are provided in Section II. Performance parameters chosen for multi-objective optimization of S-boxes are described in Section III. Section IV introduces the proposed method for getting Pareto-optimal S-boxes using NSGA-II. The performance of the proposed method is discussed, and the cryptographic strength of the proposed S-boxes is discussed in Section V. The application of the proposed S-box for the security of medical images in healthcare networks is presented in Section VI. Section VII gives the conclusion of the research work in this paper.

II. NON-DOMINATED SORTING GENETIC ALGORITHM-II

Non-dominated sorting genetic algorithm II is a multi-objective optimization algorithm, which was developed by Deb *et al.* [34]. It is one of the efficient algorithms to solve multi-objective problems (MOP), where there exist conflicting performance criteria. As a designer, it is not facetious to neglect one parameter over the other, while pursuing an efficient solution to a given problem under investigation. The NSGA-II holds several merits over the standard genetic algorithm (GA) in terms of steering towards optimal solutions. It has better diversity and time complexity. The basic norm of its operation begins with the generation of the initial population, like other meta-heuristic algorithms. The fitness values of each individual in the initially-spawned populations are determined as per the chosen performance parameters. The initial population is sorted through the non-dominated sorting approach, decomposed into various fronts. The dominance is decided by the fitness value of the individuals. Non-dominated individuals of the population reside on the very first front. The individuals of the former front are dominated by the individuals of the later fronts during any iteration and so on. In NSGA-II, the diversity is maintained through the crowding distance feature. Under this condition, the distance of individuals from their neighbors is computed. It has been argued that the mean crowding distance should be higher for diversity and significance of desired results [35]. This process is followed by the tournament selection operation, which aims to choose the parents on the basis of lower fitness values and higher crowding distances. Unlike the standard GA, the offsprings are formed through crossover and mutation operations. This causes the formation of new populations of offspring. Now, the non-dominated sorting is again executed to obtain the best individuals for the population size restriction. The motivation behind using NSGA-II is that it has fast and efficient convergence; can tackle problems that begin in non-feasible regions; can handle the non-penalty constraint effectively, and employs non-dominated sorting concepts to determine the optimal fronts along with crowding distance operation [36]. The basic flow of the NSGA-II is illustrated in Figure 1.

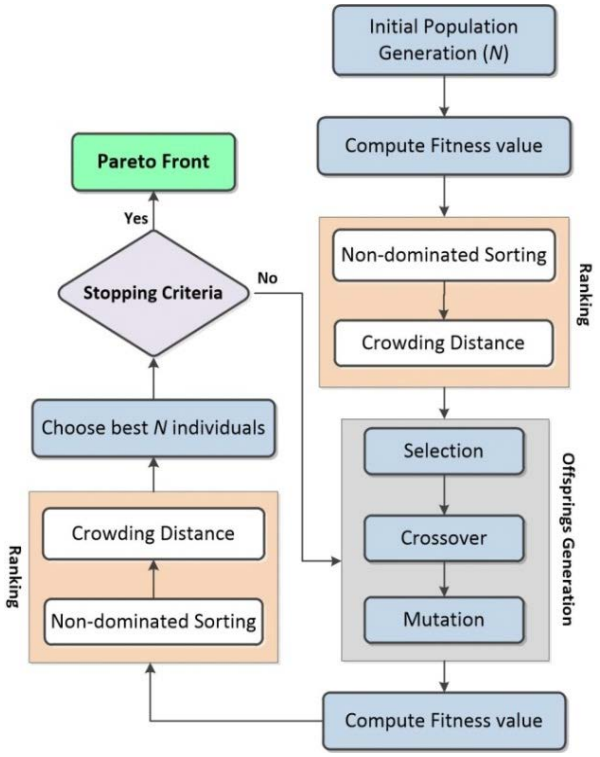


FIGURE 1. Workflow of the NSGA-II algorithm.

III. S-BOX PERFORMANCE PARAMETERS

The main target of using S-boxes in cryptosystems is to transform the input data into ciphertext data in a highly nonlinear

fashion. That is, a nonlinear change is induced in the input secret data. The degree of the nonlinear transformation corresponds to the high nonlinearity score of the S-box, which in turn is also responsible for providing robustness against linear attacks or cryptanalysis. The NL of the S-box is deemed as the most crucial feature of the S-box for the designers. Therefore, it has been mainly deliberated as the deciding parameter, while designing S-boxes in almost all S-box studies investigated so far except a few [37]. Besides the NL, the DU is equally significant in resisting the potential cryptanalysis as stated by Biham *et al.* [38]. An S-box should have a low score of DU to leak no information or clue to the attackers. Moreover, the global Avalanche criteria (GAC) are examined as the decisive cryptographic quality metrics, which lead to effective diffusion [39]. The GAC characteristic of S-boxes is measured through the ACF. It is also known as the absolute indicator of the S-box. With this reasoning and motivation, the three vital performance parameters i.e., NL, DU, and ACF, have been adopted as optimization objectives using multi-objective meta-heuristic NSGA-II to generate optimal S-boxs. Specifically, these three parameters are discussed in what follows.

A. NONLINEARITY

The nonlinearity of a Boolean function f is calculated if we have the smallest distance of f known to the set of all relative affine functions [37]. Along these lines, the S-box constituent function f ought to have nonlinearity η_f defined as:

$$\eta_f = \frac{1}{2}(2^n - WH_{\max}(f)) \tag{1}$$

Here, the Walsh-Hadamard transform of the function f is $WH_{\max}(f)$ [40]. Any n-variable function is considered fragile on the off chance that it will generally have weak nonlinearity. The adjusted Boolean function maximization of nonlinearity is viewed as one of the desirable characteristics liable for giving power against any sort of attacks related to linearity [41].

B. DIFFERENTIAL UNIFORMITY

Differential uniformity is estimated to discover the S-box ability to resist the expected differential cryptanalysis. It is a picked plaintext attack outlined by Biham and Shamir to attack block ciphers, who are DES-like [38]. Differential uniformity (DU) addresses the maximum likelihood of creating an output differential $\Delta y = y_i \oplus y_j$, when the input differential is $\Delta x = x_i \oplus x_j$. In this strategy, the XOR distribution among inputs and outputs of S is analyzed. Numerically, it is evaluated as:

$$DU_S = \max_{\Delta x \neq 0, \Delta y} (\#\{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}) \tag{2}$$

Its value ought to be as low as conceivable to resist the Biham and Shamir potential differential cryptanalysis.

C. AUTO-CORRELATION FUNCTION

Let $\alpha(t)$ and $\beta(t)$ be Boolean functions, and the cross-correlation of these two functions, denoted by $\hat{c}_{\alpha\beta}(s)$, be demarcated as [42]:

$$\hat{c}_{\alpha\beta}(s) = \sum_t \frac{1}{2^n}\left((-1)^{\alpha(t)\oplus\beta(t\oplus s)}\right) \tag{3}$$

In the case of binary Boolean functions α, the auto-correlation is expressed as $\hat{c}_{\alpha\alpha}(s)$, that is, the squares of values of the spectrum of α are the values of the spectrum of the ACF [42]. The ACF for $GF(2^m) \rightarrow GF(2^n)$ is designated as $\hat{r}_\alpha(s)$. The mathematical formulation to compute the ACF is accounted as:

$$\hat{r}_\alpha(s) = \sum_t \frac{1}{2^n}\left((-1)^{\alpha(t)\oplus\alpha(t\oplus s)}\right) \tag{4}$$

The lower value of ACF is desirable for a strong S-box that satisfies GAC and effective diffusion [39].

IV. PROPOSED S-BOX GENERATION METHOD

Construction of cryptographic strong and robust S-boxes has been one of the challenging tasks for researchers, scholars, and security experts. Conventionally, the NL has been adopted for strong S-box design in almost all S-box studies investigated so far. In the literature, several optimization-based S-box studies are available. They generate S-boxes with optimal NL only. In contrary, other equally-significant parameters have to be considered to enhance the security of S-boxes for usage in block ciphers. One feature of the S-box cannot be overlooked compared to the other features. In addition, some trade-offs must be made for obtaining a suitable and strong configuration of the S-box. The decision of the optimal trade-off among features of S-boxes cannot be made, manually. To overcome these limitations and shortcomings of the existing methods, a novel S-box design method is suggested in this paper, which heuristically achieves a good trade-off among the adopted performance parameters to obtain the optimal S-boxes. The generation of optimal S-boxes that satisfy multiple performance parameters using an improved version of the NSGA-II is discussed as follows.

A. DISCRETE CHAOTIC MAP

In [35], random numbers with uniform distribution have been suggested for use in the NSGA-II. Recent research focused on the use of deterministic chaotic sequences from chaotic maps to augment the efficiency of the NSGA-II [43], [44]. Therefore, in order to proceed with such findings and to generate optimal S-boxes under the control of keys, we incorporated a simple but rich-in-dynamics chaotic map defined in Eqn. (4). The chaotic map is incorporated during the initial S-box population generation, tournament selection, crossover, and mutation operations.

$$\psi_{i+1} = chaotic - map(\psi_i, \varepsilon) = (\varepsilon \times \psi_i) \bmod (1) \tag{5}$$

where ε is the map bifurcation parameter, ψ_i is a chaotic variable that lies in [0, 1]. This map converges to zero, when ε is an even integer. However, the analysis shows that this map has chaotic performance only when ε is floating-point and greater than unity. It has a positive Lyapunov exponent,

which is a measure of the degree of chaos and the sensitivity to initial conditions, when $\varepsilon > 1$ [35].

B. ALGORITHM

The proposed algorithm for the design of optimal S-boxes satisfying multiple performance criteria simultaneously using multi-objective NSGA-II optimization is presented in this section. The multi-objective optimization of performance parameters is treated as a minimization problem. Hence, the suggested optimization process works by minimizing the negative of NL, minimizing the DU, and minimizing the ACF in addition to bijectivity criterion.

1) INITIAL POPULATION GENERATION

The NSGA-II is a population-based multi-objective optimization algorithm. Therefore, the proposed method requires spawning of a set of bijective 8×8 S-boxes as initial population to begin the processing. As mentioned earlier, the usage of deterministic chaos for effective NSGA-II is adopted and the initial N S-boxes are generated using the chaotic map defined in Eq. (4). The process of initial population generation is dynamic, deterministic and key-dependent, which makes it suitable for key-controlled cryptographic applications. The process of generating S-boxes of initial population is given in Algorithm 1.

Algorithm 1 *gen_sbox*(ψ, ε)

for $k \leftarrow 1$ to 256
  $\psi_{new} \leftarrow$ chotic_map(ψ_{old}, ε)
  $A[k] \leftarrow \psi_{new}$
end
$B \leftarrow$ sort(A, '*ascend*')
for $k \leftarrow 1$ to 256
  $x \leftarrow B[k]$
  for $l \leftarrow 1$ to 256 do:
    if ($x == A[l]$) then:
      $sbox[k] \leftarrow l - 1$
      break
    end
  end
end
return $sbox$, ψ_{new}

2) FITNESS CALCULATION

As discussed earlier in section III, the three crucial performance parameters of S-boxes, namely the NL, DU, and ACF have been chosen as the parameters to be optimized for strong S-box generation at Pareto-fronts. These three parameters of S-boxs are responsible for providing strong resistance to pertinent cryptanalysis (like linear and differential attacks), and strong diffusion. During optimization, the maximization of NL, minimization of DU, and ACF is desired for strong S-box generation.

3) NON-DOMINATED SORTING

The non-dominated sorting is applied to the generated population of S-boxes so as to decide the dominance of solutions at each iteration. The dominance is definite by the fitness values of the individual S-boxes. It is worth mentioning that the dominance of solution vector U over solution vector V in multi-objective problems is decided iff $fit_i(U) \leq fit_i(V)$ or $fit_i(U) < fit_i(V)$, where fit_i is the i-th fitness value or objective of solution vectors. Non-dominated S-boxes of population reside into the first front. The S-boxes of former front are dominated by the S-boxes of the later fronts during any iteration and so on.

4) CROWDING DISTANCE

The NSGA-II maintains the diversity through the crowding distance operation. Here, the distance of individuals from their neighbors is calculated. A higher value of crowding distance is preferred for diversity and significance of the obtained results. This module computes the required crowding distances of individual S-boxes, which will help to make rational selection of S-boxes.

5) TOURNAMENT SELECTION

This operation selects the pool of parents having better leading factors based on fitness values or higher crowding distances. The two randomly-generated indices using chaotic map help to choose the individual S-boxes from the population. The S-box as a parent comes ahead in the pool if it has a better leading factor. If leading factors are the same then selection is based on the higher crowding distance compared to other individual S-boxs.

6) CROSSOVER

Crossover operation is applied to generate the new offspring S-boxes. In order to bring a diversity of solutions, the crossover is done on randomly-chosen parents from the pool maintained, earlier. The random generation of parent indices is again made with the help of a chaotic map. The number of crossover operations to generate offsprings depends on the crossover probability p.

7) MUTATION

Mutation operation supports to avoid trapping of solutions in local optima. It helps to have diversity and makes the optimization process faster to achieve global optima. In the proposed method, the mutation in an individual S-box of the pool is performed by swapping its two elements. The choice of an individual S-box and its two elements is made randomly with the help of a chaotic map. The mutation operation is made $N \times q$ times, where q is the mutation probability. The mutation probability is kept low as compared to the crossover probability.

8) ADJUSTMENT

Bijective nature is one of the main features of the proposed S-box generation method. It entails that the elements of an 8×8

Algorithm 2 S-Box Generation Using NSGA-II With Multiple Parameter Optimization

begin

Initialization:

1. N = number of initial population
2. max_itr = number of iterations
3. ψ = initial value of chaotic map
4. ε = parameter of chaotic map

   Generate intial population of S-boxes:
5. $\psi = chaotic\_map(\psi, \varepsilon, 100)$
6. population = $zeros(2N, 256)$
7. for $i = 1: N$
8. [sbox, ψ] = $gen\_sbox(\psi, \varepsilon)$
9. population[i] = sbox
10. end for

    Calculate fitness:
11. for $i = 1: N$
12. $P_{NL} = (-1)^{*}nonlinearity$(population[$i$])
13. $P_{DU} = differentialuniformity$(population[$i$])
14. $P_{ACF} = autocorrelation$(population[$i$])
15. end for

    Non domination soting and crowding distance:
16. fronts = $non\_dominated\_sort(P)$
17. $crowding\_distance$(fronts)
18. while ($max\_itr > 0$) do
19. pool = $tournament(P)$
20. Perform *crossover* of parents from population, whose indices are obtained from pool array to get offsprings.
21. Perform *mutation* on generated offsprings from $2N$ population, whose indices are also given in pool array.

    Calculate fitness:
22. for $i = 1: 2N$
23. $P_{NL} = (-1)^{*}nonlinearity$(population[$i$])
24. $P_{DU} = differentialuniformity$(population[$i$])
25. $P_{ACF} = autocorrelation$(population[$i$])
26. end for

    Non domination soting and crowding distance:
27. fronts = $non\_dominated\_sort(P)$
28. $crowding\_distance$(fronts)

    Preserve best N candidates:
29. Preserve the best N candidates from the $2N$ population size
30. $max\_itr = max\_itr - 1$
31. end while

    Output the best S-boxes:
32. Display the S-boxes from the first front

end

S-box should be all distinct and lie in the interval of $[0, 2^8 - 1]$. However, the crossover operations on parent S-boxes may lead to the generation of offsprings with disturbed bijectivity. Thus, an adjustment process on all offsprings is required to guarantee the bijective nature of the child S-boxes. Hence, after crossover and mutation operations, adjustments have to be done on the offsprings to restore the bijectivity of offspring S-boxes.

The proposed method for generating S-boxes using the multi-objective NSGA-II satisfying multiple performance parameters is given in Algorithm 2.

V. EXPERIMENTAL RESULTS AND ANALYSIS

We performed a set of experiments and simulations to assess the performance of the proposed S-box generation method for triple-objective optimization in addition to bijectivity. The implementation has been done on Windows 8.1 Pro with Intel *i*5-4590 CPU @ 3.3GHz, 4GB RAM, and 500GB storage using Python programming. The default experimental settings are as follows:

- $\psi = 0.1234$
- $\varepsilon = 137.0$
- $N = 250$

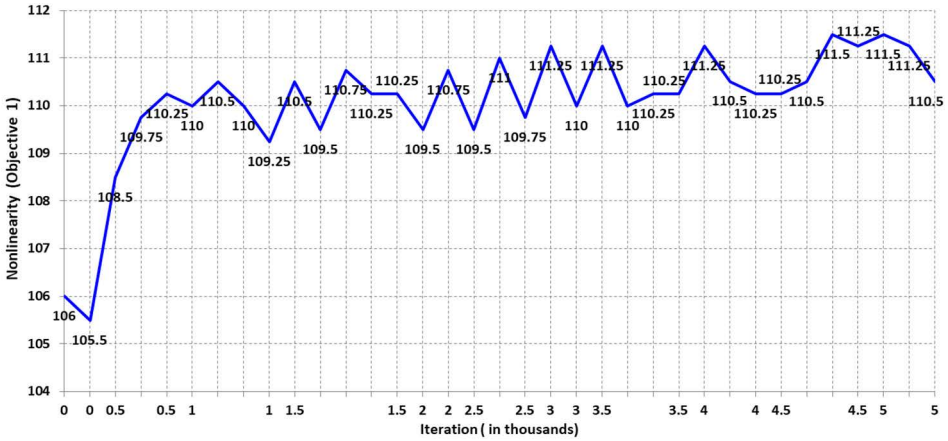


FIGURE 2. Nonlinearity (NL) scores of multi-objective optimized S-boxes from first front.

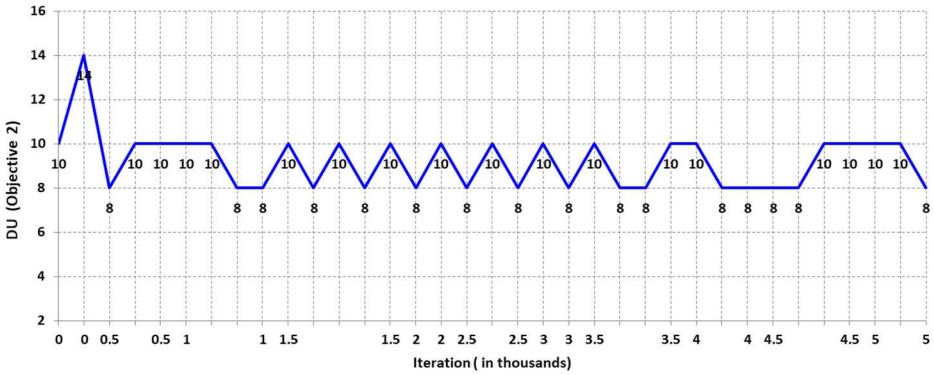


FIGURE 3. Differential uniformities (DU) of multi-objective optimized S-boxes from first front.

- $max\_itr = 5000$
- crossover probability $(p) = 0.7$
- mutation probability $(q) = 1 - p$

In what follows, we present the results and analysis of the proposed method for generating S-boxes, and its security compared with existing optimization-based S-box generation methods.

A. ANALYSIS OF S-BOXES FROM FIRST FRONTS

Sufficient iterations of the multi-objective S-box optimization phase have been applied. The proposed method begins with the generation of initial population. Two S-boxes are found at the first front after initial population generation with fitness features of $(-\text{NL}, \text{DU}, \text{ACF}) = (-106, 10, 96)$, and $(-105.5, 14, 88)$. Then, the multi-objective optimization phase is started and improvements in fitness values of S-boxes are noticed as iterations progress. The fitness values of three chosen objectives of optimized S-boxes available at first fronts are analyzed after every interval of 500 iterations. The fitness values of NL (*objective*-1), DU (*objective*-2), and ACF (*objective*-3) of optimized S-boxes of first fronts only are presented in Figures 2, 3 and 4, respectively. Consequently, we obtained the finally-optimized S-boxes after completion of 5000 iterations. The proposed multi-objective evolution method strives sensibly to find good Pareto-optimal combination of three adopted objectives. The fitness values of objectives get better as a whole as the iterations progress with time. As can be seen from the figures, there are three optimized S-boxes (named as F_1, F_2, and F_3) found at the first front after 5000 iterations. One such final S-box from the final first front is given in Table 1. This S-box is chosen as the best one among the final three. The NL scores of all eight coordinate Boolean functions of the three 8×8 S-boxes are shown in Table 2. It is evident that these S-boxes have admirable NL performance as the minimum and maximum values are 110 and 112 for each of these S-boxes. Table 3 presents the optimized fitness values of all three final S-boxes for the proposed method.

The statistics show that as low as 8 and 80 DU and ACF scores, respectively, have been achieved through the proposed method unlike many optimization-based and chaos-based S-boxes generation methods available in the literature, which are merely better in NL.

B. QUALITY INDICATOR OF SOLUTION SETS

The multi-objective optimization method works on more than one objective function, simultaneously. It is evident that such objectives are often conflicting with each other, and hence

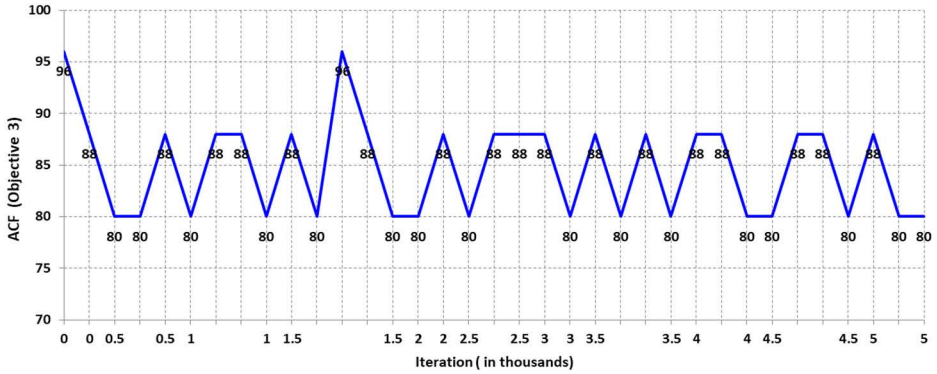


FIGURE 4. Auto-correlation functions (ACF) of multi-objective optimized S-boxes from first front.

TABLE 1. Proposed optimized S-box F_3 (NL, DU, ACF) = (110.5, 8, 80).

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

TABLE 2. Nonlinearities of proposed multi-objective optimized S-boxes from first front.

S-box	η_1	η_2	η_3	η_4	η_5	η_6	η_7	η_8
F_1	112	112	112	110	110	112	112	112
F_2	112	112	112	112	110	112	110	110
F_3	110	112	110	112	110	110	110	110

TABLE 3. Fitness values of three objectives (NL, DU, ACF) of proposed optimized S-boxes from first front.

Proposed S-box	Nonlinearity	DU	ACF
F_1	111.5	10	88
F_2	111.25	10	80
F_3	110.5	8	80

it is difficult to have the best value of all the objectives under consideration. Instead of an optimal solution, there exists multiple Pareto-optimal solution sets. All generated Pareto-optimal solutions are not significant. Therefore, there is a need to evaluate the quality of the Pareto-optimal sets, while comparing the behavior of different optimizers or approaches. Focusing on the convergence aspect of solution sets, there is a quality indicator known as generational distance (GD), which evaluates the quality of the obtained Pareto-optimal sets. It measures the Euclidean distance of solutions of set X with respect to the closest point on the Pareto front. Mathematically, for a solution set $X = [x_1, x_2, \ldots, x_n]$, the GD is computed as:

$$GD(X) = \frac{1}{n}\left(\sum_{k=1}^{n}(g(x_k, PF))^2\right)^{0.5} \quad (6)$$

where $g(x_k, PF)$ stands for the L^2-norm Euclidean distance of x_k to the Pareto front PF. In practice, a reference set which

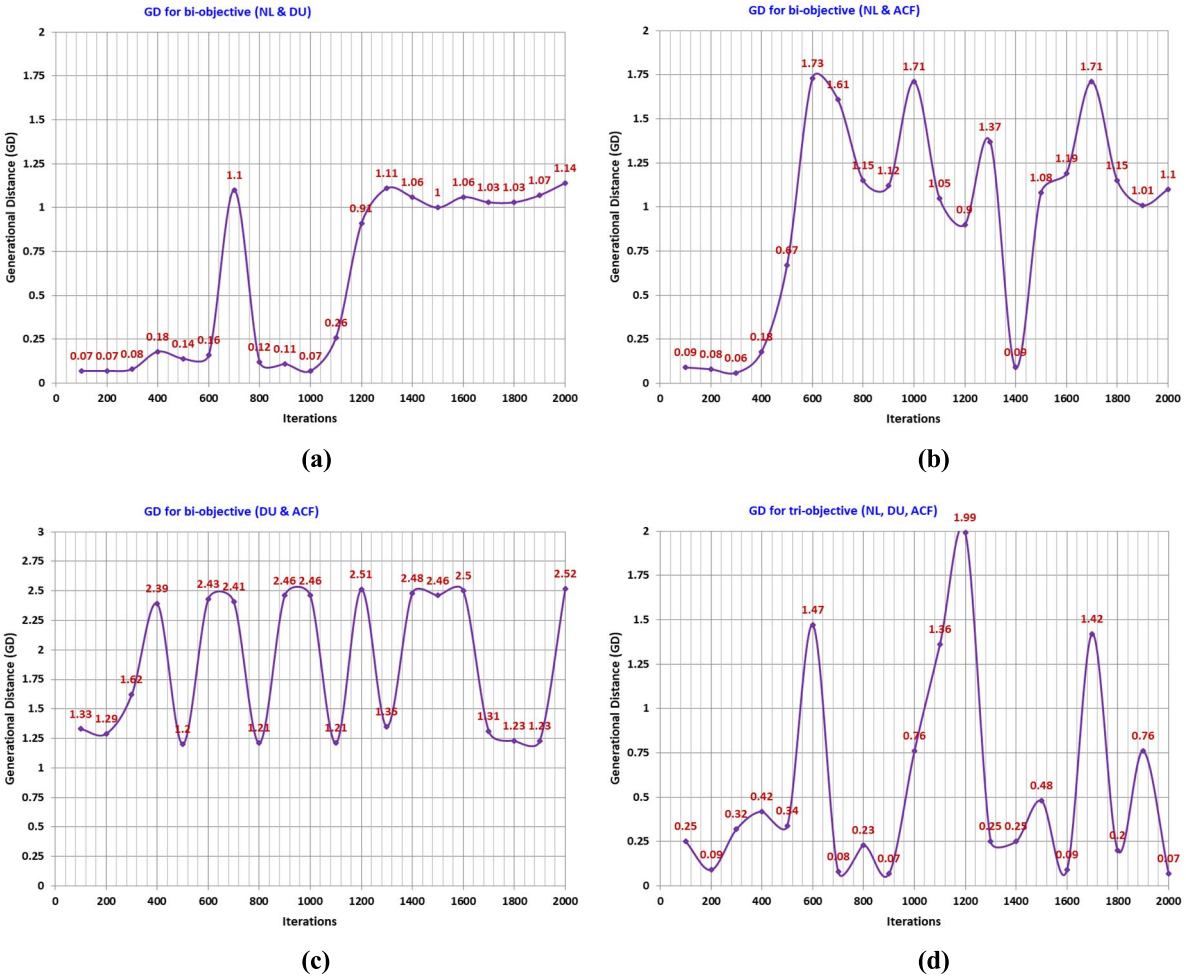


FIGURE 5. GD behaviour for solution sets for (a) bi-objective (NL, DU), (b) bi-objective (NL, ACF), (c) bi-objective (DU, ACF), and (d) tri-objective (NL, DU, ACF).

well represents the PF is utilized. It is worth mentioning that a minimum *GD* score is desired as it indicates that the solution set tends to show a better progress towards the *PF* i.e. the solution set has better convergence towards *PF*. To perform the GD analysis of the solution sets generated by the proposed method and to justify the selection of tri-objective optimization instead of bi-objective cases, we evaluated the GD for the three possible cases of bi-objective optimization. The GD evaluation and analysis is carried out for (1) *NL* and *DU*, (2) *NL* and *ACF*, (3) *DU* and *ACF*, and (4) *NL*, *DU* and *ACF*. The obtained GDs and their behavior for the mentioned four scenarios are graphically shown in Figure 5. The analysis reveals that the tri-objective problem shows a lower score of 0.07 compared to other 3 cases of bi-objective problems.

C. OTHER CRYPTOGRAPHIC FEATURES OF GENERATED S-BOXES

In practice, there are few other security parameters to gauge the quality, power, and robustness of S-boxes. This section is focused on the analysis of S-boxes based on strict Avalanche criteria (SAC), bit independence criteria (BIC), and linear approximation probability (LAP).

1) STRICT AVALANCHE CRITERIA (SAC)

The SAC for S-boxes [45] was suggested by Webster and Tavares. For S-boxes, to fulfill SAC, the reversal of a single bit of the vector, which gives the input must prompt fifty percent of change in the vector, which gives the output. A value close to 0.5 is constantly seen as respectable. The computation of the dependency matrix is performed by the methodology mentioned in [46]. The values of the matrix reveal that every entry is close to 0.5. The mean of dependency matrices provides the SAC of three S-boxes F_1, F_2, and F_3 as 0.4995, 0.5032, and 0.4929, respectively. The SAC values close to 0.5 signify that the proposed S-boxes gracefully fulfill the the SAC.

2) BIT INDEPENDENCE CRITERIA (BIC)

One of the similarly critical criteria for strong S-boxes is the BIC. A strategy to check BIC was recommended by Adams and Tavares in [45] and [46]. Suppose that the Boolean

function components of an 8×8 S-box are $f_1, f_2, \ldots, f_8$. If the S-box meets BIC, the Boolean function XOR(f_j, f_k) (where, $j \neq k$ and $1 \leq j, k \leq 8$) ought to be exceptionally nonlinear [51], [52]. Thusly, BIC is confirmed by computing NL of each of such 56 XOR(f_j,f_k) functions for any 8×8 bijective S-box. The potential scores of NL of functions for our three S-boxes are figured and displayed in Table 4. The scores of BIC for S-boxes F_1, F_2, and F_3 are found as 103.93, 103.93, and 104.21, respectively. The obtained scores reveal good satisfaction of BIC.

TABLE 4. Other cryptographic features of the proposed optimized S-boxes.

Proposed S-box	SAC	BIC	LAP
F_1	0.4995	103.93	0.14062
F_2	0.5032	103.64	0.14062
F_3	0.4929	104.21	0.14062

3) LINEAR APPROXIMATION PROBABILITY (LAP)

The strategy for linear approximation probability is useful in computing the imbalance of an event. Matsui in [47] presented the largest value of imbalance of an event measured with the assistance of examination. There should be no distinction of bit uniformity among the output and the input. Each of the input bits along with the corresponding output bits is analyzed independently. On the off-chance that each of the input components is 2^n, d is the class of all potential inputs and the masks applied on the correspondence of output and input bits are individually m_a and m_b. At that point, the most extreme linear guess is the greatest number of similar outcomes, and it is mathematically determined as follows:

$$LAP(S) = \max_{m_a, m_b \neq 0} \left| \frac{\#\{a \in S | \, a.m_a = b.m_b\}}{2^n} - 0.5 \right| \quad (7)$$

The fact that the S-box is more competent to battle against linear cryptanalysis is attributed to the low value of likelihood. The LAP scores of the three designed S-boxes come out as being the same with a value of 0.140625. This score is low, and it allows resistance of linear cryptanalysis.

D. PERFROMANCE COMPARISON WITH OTHER OPTIMIZATION-BASED S-BOXES

In order to assess the proposed Pareto-optimized S-boxes, the designed S-boxes have been compared with other existing S-boxes, which are based on meta-heuristics. The literature reveals that a number of meta-heuristics have been investigated to obtain the optimized 8×8 S-boxes. Both Tiki-Taka algorithm (TTO) [48], Bacteria foraging optimization (BFO) [49], fireworks algorithm [50], Jaya optimization [51], Cuckoo search (CS) [52], human behaviour based optimization (HBBO) [53], genetic algorithms (GA) [20], sine-cosine optimization (SCO) [54], firefly algorithm [24], teaching-learning based optimization (TLBO) [25], I-Chings optimization (ICO) [26], ant colony optimization (ACO) [22], artificial bee colony optimization (ABC) [23], and particle swarm optimization (PSO) [55] have been considered. The Pareto-optimal S-boxes from the first front for the proposed method are compared. The comparative analysis on standard performance parameters is presented in Table 5. Besides, optimized fitness objectives i.e. NL, DU, ACF, and other security metrics are also compared. It is evident from the comparison study that Pareto-optimal S-boxes obtained with the proposed multi-objective optimization method have reached high NL scores compared to other optimization-based S-boxes. On the basis of resistance to differential cryptanalysis, the S-box F_3 has a low score of DU of 8, thereby showing a better robustness against DC attack compared to all other S-box studies. Moreover, the generated S-boxes F_1, F_2, and F_3 also have good ACF scores, as desired for good diffusion, compared to all other existing optimization-based S-boxes. We picked S-box F_3 as the best candidate which is generated from the given experimental settings among all three of the first front as it shows a trade-off among the three objective parameters. In addition, it is important to consider the performance of the S-box generation using the GA and chaos as investigated by Wang *et al.* [20]. Wherein, the authors utilized the 1D logistic and PWLCM map to generate the initial population, and their experimental results showed that $N = 5000$ populations were initially generated. This value of N is too large compared to $N = 250$ in the proposed method. Moreover, the authors worked only on the NL during the optimization phase of the GA and achieved a minimum NL of 108, which is quite less compared to our minimum NL of 110. Unfortunately, the other equally-significant security metrics like DU $= 10$ and ACF $= 96$ were poor, which shows low diffusion for the generated S-box by Wang [20] compared to the proposed S-box. We were able to achieve a DU as low as 8 and an ACF as low as 80 with the proposed multi-objective NSGA-II and chaos method. The comparative analysis based on NL, DU, and ACF with various S-box optimization methods is also graphically depicted in Figure 6. It is clear that the proposed S-box generation method through the multi-objective optimization is able to yield S-boxes with high cryptographic robustness and security strength.

VI. SECURE TELEMEDICINE APPLICATIONS

Telemedicine services such as telediagnosis and teleconsultation demand data interchange over unsecure public open networks. Protection of the integrity and confidentiality of medical images has been a problem in the governance of medical services [56], [57]. Confidentiality means that unauthorized coalitions should not be granted to access medical images during transmission. Integrity means that sensitive images should not be altered any how during communication. In general, a medical image consists of two parts, an image header and an image body. The nominative data header of the delicate patient data needs to be facilely safeguarded by all

TABLE 5. Performance comparison with other competitive optimization-based 8 × 8 S-boxes.

S-box	*min*(*NL*)	*max*(*NL*)	*mean*(*NL*)	DU	ACF	SAC	BIC	LAP
Tiki-Taka algorithm [48]	106	110	109.25	10	112	0.5017	104.07	0.1171
BFO [49]	106	110	107.5	10	96	0.5093	103.07	0.1406
Fireworks algorithm [50]	98	108	105.75	10	96	0.4991	102.57	0.14062
Jaya [51]	104	108	106.25	10	104	0.5009	103.64	0.1328
Cuckoo Search [52]	108	110	109.25	12	88	0.5075	102.93	0.1406
HBBO [53]	102	110	106.5	12	96	0.4943	103.35	0.14844
GA [20]	108	108	108	10	96	0.5068	103.36	0.1406
SCO [54]	108	110	109.5	10	96	0.4985	104.07	0.1328
Firefly algorithm [24]	106	108	107.5	10	96	0.4943	104.35	0.125
TLBO [25]	104	110	106.5	10	96	0.4995	104.57	0.1172
ICO [26]	108	110	108.75	10	96	0.4946	102.78	0.1328
ACO [22]	106	110	107	10	96	0.5015	104.21	0.1484
ABC [23]	106	110	108	10	96	0.5073	104	0.1523
PSO [55]	104	111	106.5	10	112	0.5036	102.86	0.14062
F1 (This work)	110	112	111.5	10	88	0.4995	103.93	0.14062
F2 (This work)	110	112	111.25	10	80	0.5032	103.64	0.14062
F3 (This work)	110	112	110.5	8	80	0.4929	104.21	0.14062

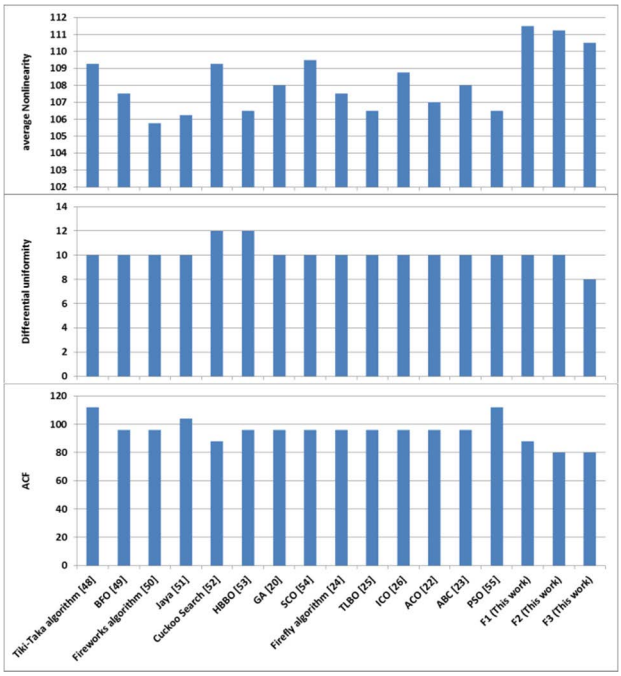


FIGURE 6. Comparison of N, DU, and ACF of different 8 × 8 S-boxes.

protection means, while the issue of major concern for the medical images is image integrity. A medical image is distributed among opus of clinicians in telediagnosis, and every one of them has all the data related to patient's medical case [58]. Revealing the secret clinical data about a momentous medical ailment of patients to each of the clinicians is a challenging protection concern. Authorizations for guarantying health data protection have been allotted by the civil regimen alike as Health Insurance Portability and Responsibility Act (HIPAA), where medical institutes are favored to take felicitous moves to guarantee that patient's data is only handed to people who possess a legal access. Telemedicine image protection is all about to preserve privacy of the patient critical information in the image and to console data truthfulness that prevents others from illegal alterations in the medical images in telemedicine networks [59], [60]. This section is dedicated to put forward an image encryption scheme based on our Pareto-optimal S-box for realization of strong and fast medical image protection in telemedicine environments. Our proposed encryption scheme employs the S-box based on shuffling and substitution in a novel and simple manner. The operations performed under the suggested encryption scheme include the following.

Step 1. Generate S-Box *SB* using the proposed method discussed in Section IV.
Step 2. Take as input a pending plain-image *P*.
Step 3. Evaluate 512-bit hash code *H* of the plain-image *P* using the SHA-512 hash function.
Step 4. Convert the hash code *H* into 64 bytes i.e. as a block *K* consisting of 64 bytes.

Step 5. Convert the input image to a 2D vector of size $256 \times L$. The image has 256 rows and L columns.
Step 6. Perform shuffling of rows through the generated S-box SB by moving row at index ω to row at index $SB(\omega)$, where $\omega = 1, 2, \ldots, 256$.
Step 7. Decompose the image into W blocks of 64 bytes.
Step 8. Perform substitution of blocks in forward direction (from first block to last one) using S-Box SB and hash code K as:

$$PB(x) = bitxor(PA(x), K, SB(y))$$
$$K = PB(x); \quad x = 1, 2, \ldots, W.$$

where x is the block number in the shuffled image PA, y is the quarter of the S-Box SB, and it takes values as $y = (x) mod(4)$.
Step 9. Convert the intermediate image to a 2D vector of size $L \times 256$. The image has L rows and 256 columns.
Step 10. Perform shuffling of columns by moving the column at index ω to the column at index $SB(\omega)$ to get image PC, where $\omega = 1, 2, \ldots, 256$.
Step 11. Decompose the image into blocks of 64 bytes.
Step 12. Perform substitution of blocks in backward direction (from last block to first) using S-Box SB and updated code K as:

$$C(x) = bitxor(PC(x), K, SB(y))$$
$$K = C(x); \quad x = W, W-1, \ldots, 2, 1.$$

Step 13. Display C as the encrypted image.

The suggested encryption scheme based on Pareto-optimal S-box generated using the proposed method is also described through a flowchart shown in Figure 7. The decryption algorithm is applied in a reverse manner to get the decrypted image with correct key values.

An encryption scheme makes drastic modifications in the content of the encrypted image body. The magnitude of distortions that take place in the image determines the quality of encryption offered by the anticipated scheme. It needs to be quantified statistically and compared with the state-of-the-art methods [61], [62]. We applied the proposed encryption scheme to encrypt some medical images and Lena image, which are shown in Figure 8a. Several performance metrics have been evaluated in order to assess statistically the encryption strength of the proposed encryption scheme. The standard set of performance metrics that have been chosen for assessment of our scheme includes histogram analysis through Chi-square test, visual security analysis, adjacent pixel correlation analysis, information entropy analysis, differential attack (plain-image sensitivity) analysis, and speed analysis. The obtained performance results are also compared to those of some recent S-box based image encryption schemes.

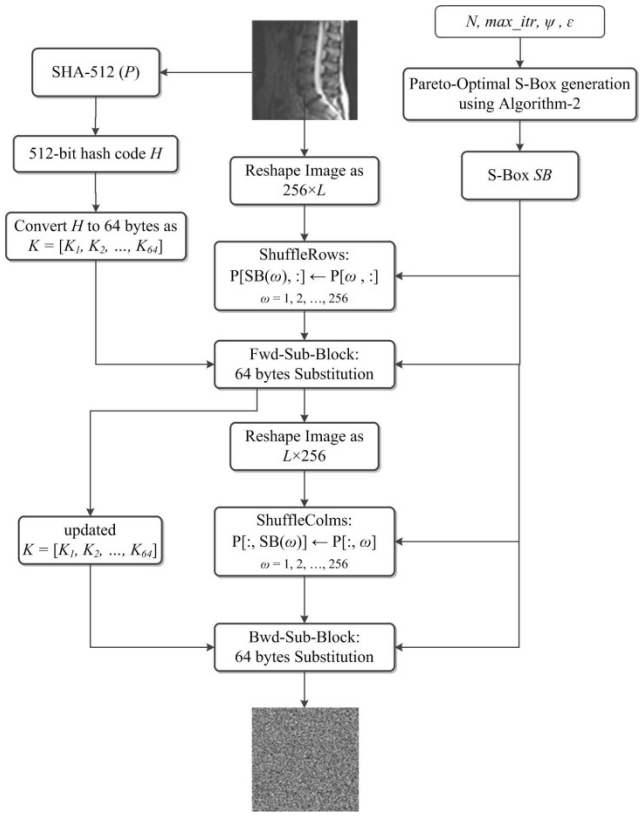
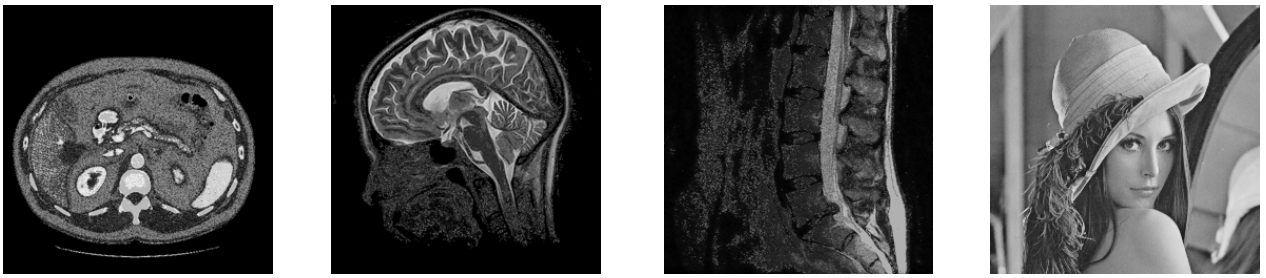


FIGURE 7. Proposed medical image encryption scheme using Pareto-optimal S-box based on NSGA-II.

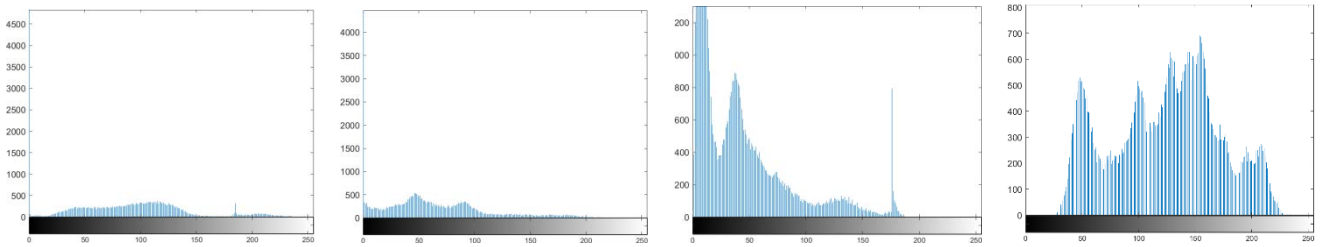
A. HISTOGRAM ANALYSIS

Statistical attacks exploit some information leakage, which is evident through the distribution of the encrypted content. To mitigate such attacks, the distribution of encrypted data should be as uniform as possible. Likewise, a strong image encryption algorithm should be able to bring randomness into the encrypted information. One way to visualize the scattering of image information is its histogram. A histogram is used to depict the frequency of image pixels per their intensity levels. Hence, the histograms of encrypted images should have uniform frequencies of all their pixel levels. Intuitively, the histogram should be as flat and uniform as possible to showcase the effectiveness of the encryption algorithm in making the statistical attack complicated to the assailants [63]. The histograms of encrypted images shown in Figure 9b demonstrate the uniform distribution of pixels. Hence, the encrypted images seem not to leak information of the plain images. The histograms of encrypted images are fairly flat and uniform similar to perfectly-random or noise-like images. The measure of chi-square χ^2 is computed to quantify and verify the uniform distribution of image pixels in the encrypted images. Mathematically, the chi-square is accounted as:

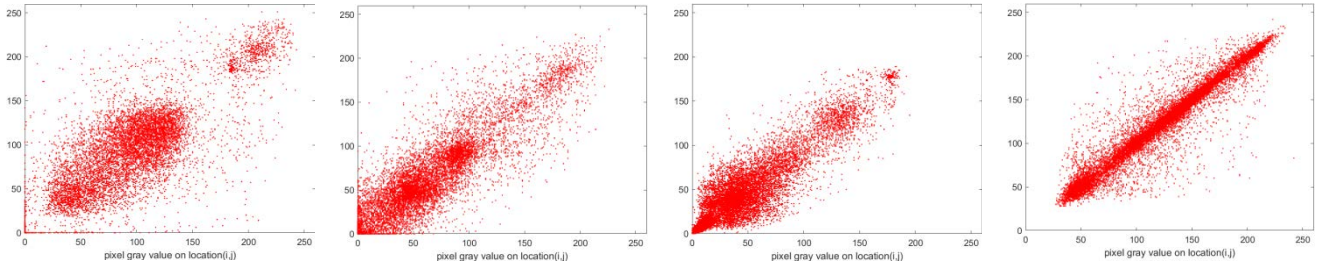
$$\chi^2 = \frac{1}{p_0} \sum_{i=0}^{255} (p_i - p_0) \tag{8}$$



(**a**) Plain images (a1. Med16, a2. Med17, a3. Med18, and a4. Lena images)



(**b**) Corresponding histograms of plain images



(**c**) Correlation of adjacent pixels in plain images

FIGURE 8. **Plain images, their histograms and pixels correlation plots.**

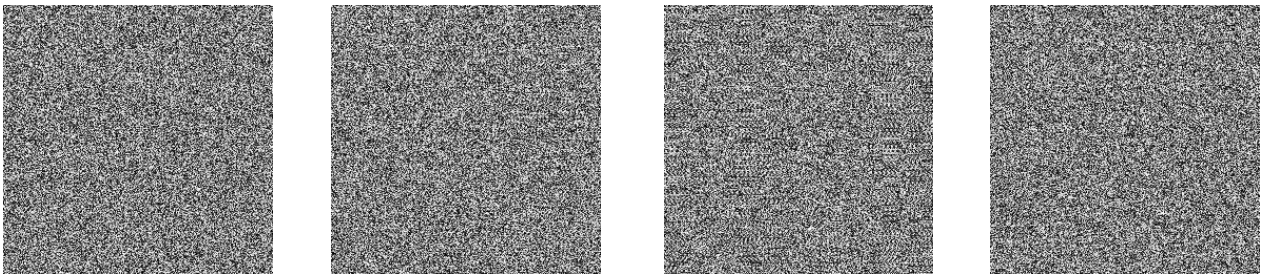
where $p_0 = numPixels/256$, $numPixels$ is the total number of pixels in the image, and p_i is frequency of the gray intensity i. A score of less than 293.2478 at a significance level of 0.05 denotes the expected value of χ^2 measure [64]. We compute the χ^2 scores for both the pending plain-images and the encrypted images as well. The results obtained are displayed in Table 6. It is quite evident that the χ^2 scores for plain-images are extremely high, thereby showing the high imbalance among the pixel gray level frequencies. On the other hand, the encrypted images have χ^2 scores, which are close to the expected value, and hence the proposed encryption scheme passes the χ^2 test, and it can be said that the proposed encryption scheme does not leak information for statistical analysis of the attackers.

TABLE 6. **Chi-square scores for the proposed encryption scheme.**

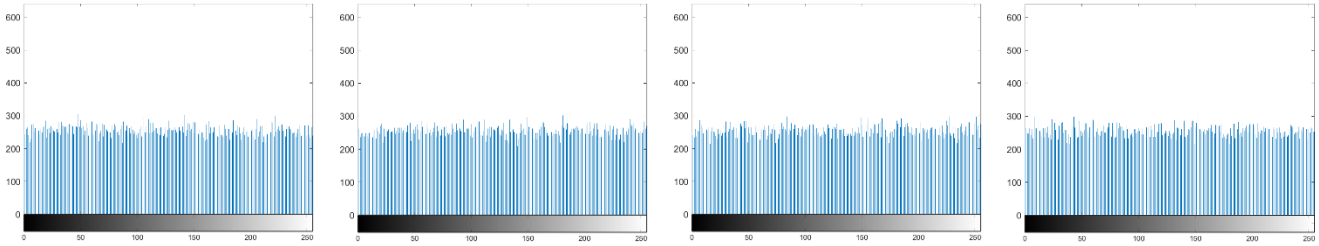
Image	Plain-image	Encrypted image
Med16	3684812.6	258.68
Med17	3136522.9	254.33
Med18	206534.7	259.47
Lena	39666.87	258.55

B. VISUAL SECURITY ANALYSIS

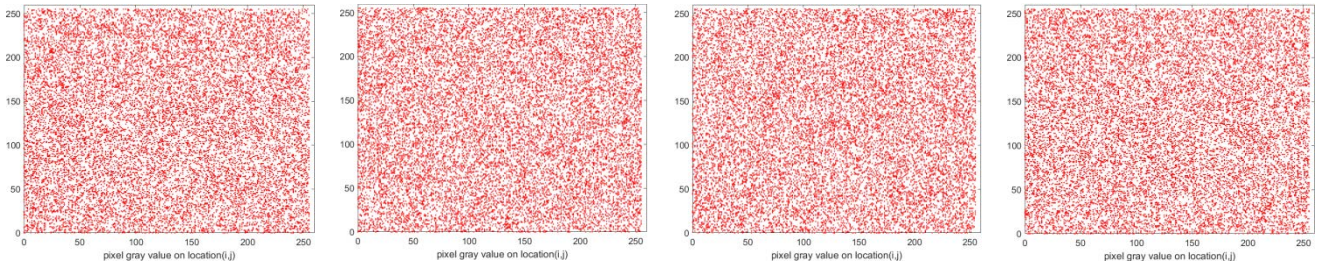
The basic requirement of any encryption scheme is to provide the visual protection of the plain-text data to hide the real content or information against any unwanted acquisition. The encrypted images obtained from the proposed encryption scheme are displayed in Figure 9a. One can easily observe that the encrypted images are highly distorted and indistinguishable compared to their respective plain-images. Unauthorized observers cannot get idea of the real content through visual description [64]. To quantify the degree of visual content security, we calculated the mean square errors (MSE), peak signal-to-noise ratio (PSNR), and structure similarity index measure (SSIM) for the pair of plain and encrypted images. The results obtained are depicted in Table 7. The high MSE scores, small PSNR and extremely low SSIM indicate that the plain images and encrypted images are highly different and dissimilar. Hence, the proposed encryption scheme is competent enough to secure the real information visually.



(a) Encrypted images (a1. Med16, a2. Med17, a3. Med18, and a4. Lena images)



(b) Corresponding histograms of encrypted images



(c) Correlation of adjacent pixels in encrypted images

FIGURE 9. Encrypted-images their histograms and pixels correlation plots.

TABLE 7. Results of MSE, PSNR and SSIM for the proposed encryption scheme.

Test	Med16	Med17	Med18	Lena
MSE	14643.63	15582.96	14732.06	7753.95
PSNR	6.474	6.204	6.448	9.236
SSIM	0.001709	0.002309	0.000467	0.000041

TABLE 8. CCF performance for the proposed encryption scheme.

Image	Plain-image	Encrypted
Med16	0.92114	-0.00203
Med17	0.93195	-0.00052
Med18	0.93262	-0.00088
Lena	0.95696	0.00091

C. CORRELATION ANALYSIS

The measurement of similarity of pixel groups is done through correlation coefficient. There exists a solid correlation between adjoining pixels in plain images. The correlation among pixels can be decreased through the encryption schemes [65]. Uncorrelated pixel patches are better over an insecure channel. The coefficients of correlation between two pixel patches are estimated as:

$$\gamma = \sum \frac{(i-\mu_i)(j-\mu_j)}{\sigma_i \sigma_j} \tag{9}$$

Here, i and j determine the patches to be compared. The μ and σ represent the mean and standard deviation, respectively. The correlation coefficients for plain and encrypted images are shown in Table 8.

D. ENTROPY ANALYSIS

The progressive idea of data entropy was instituted by Claude E. Shannon in 1948. Entropy is the measure of arbitrariness of data, which is innate in potential outcomes of variables [66]. It is measured in bits, relating to base 2. It is

numerically given as:

$$H(x) = \sum_i p(x_i)\, log_2 \left(\frac{1}{p(x_i)}\right) \tag{10}$$

Here, $p(x_i)$ is the probability of a symbol of message source x. The distribution of pixels is more uniform with higher entropy values. In this event, the entropy of the scrambled image is close to 8, revealing good randomness of encrypted images. The entropies for plain and encrypted images are shown in Table 9.

TABLE 9. Information entropy scores for proposed encryption scheme.

Image	Plain-image	Encrypted
Med16	4.9317	7.9971
Med17	5.1331	7.9972
Med18	6.5872	7.9972
Lena	7.4439	7.9972

E. DIFFERENTIAL ATTACK ANALYSIS

The fundamental objective of assailant is to acquire fractional or complete information on privileged information, which is securely encrypted on the sender side for a veritable client at the collector side. The ordinary act of aggressors is to roll out certain patterns in the images, obtain the encoded images, and dissect the sets to accomplish the objective. To rule out this methodology of attackers is to make the encryption procedure exceptionally plain-image subordinate. So, a noise-like image can be collected at the receiver side [67]. Any encryption scheme that has this feature is considered ready to relieve such assaults for ill-conceived admittance of restricted information [68]. The proposed encryption scheme has the ability of beating the cryptanalytic attempts of assailants. There exist metrics to evaluate differential analysis to be specific: number of pixels change rate (NPCR) and unified average changing intensity (UACI). The NPCR gives the pace of altered pixels which are adjusted in the encrypted content when slim modification is made in the plain information. On the other hand, UACI measures the difference between plain and encrypted images caused due to minute changes. The calculation methodology includes two images, which have dissimilarity of one pixel in particular. Let their corresponding encrypted images be C_1 and C_2. The numerical estimation of NPCR and UACI follows the formulas given below.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100 \tag{11}$$

$$D(i,j) = \begin{cases} 1 & if\ C_1(i,j) \neq C_2(i,j) \\ 0 & if\ C_1(i,j) = C_2(i,j) \end{cases} \tag{12}$$

$$UACI = \frac{1}{M \times N}\left[\sum \frac{|C_1(i,j) - C_2(i,j)|}{2^8 - 1}\right] \times 100 \tag{13}$$

The scores of NPCR/UACI acquired for the suggested S-box based encryption scheme are introduced in Table 10. As can be seen, the acquired value of NPCR is over 99.6% and UACI is also above 33.4%. The anticipated analysis justifies the robustness, consistent and acceptable performance of the proposed encryption scheme, which makes the differential attacks ineffective.

TABLE 10. Plain image sensitivity analysis results for the proposed image encryption scheme.

Test	Med16	Med17	Med18	Lena
NPCR	99.41	99.38	99.39	99.41
UACI	33.8	33.79	33.78	33.72

F. COMPARISON ANALYSIS

Of late, there is a trend to utilize S-boxes for efficient image cryptosystem designs. The underlying challenges include strong encryption quality, simple structure, short encryption time, etc. The performance of the proposed Pareto-optimal S-box based medical image encryption scheme is compared with recent S-box based encryption schemes to validate its optimal and competitive performance. All the performance metrics like chi-square χ^2, MSE, PSNR, SSIM, correlation coefficients, information entropy, NPCR, and UACI discussed and quantified in previous sections are compared for the encryption schemes investigated in [69], [70], [71], [72], and [73] in Table 11. The comparison analysis indicates that the proposed encryption scheme achieves near optimal values of all the performance metrics. The χ^2 results show the uniform distribution of pixels in encrypted content. Our scheme offers excellent visual distortion and indistinguishability proven by low PSNR and SSIM scores. The encrypted images have high randomness in the content due to high entropy scores. The adjacent pixels in encrypted images are highly uncorrelated with each other, which destroys the chances of guessing any sensitive information secured by the proposed encryption scheme. Near optimal scores of NPCR and UACI indicate that our scheme has high resistance to differential attacks due to the high plain text sensitivity feature. The comparison made in Table 11 demonstrates the competitive and consistent standing of the suggested scheme, which makes it suitable to secure medical imagery in telemedicine networks.

G. SPEED ANALYSIS

For real-time security applications, the encryption time is a significant metric. As a shorter encryption time of an algorithm along with statistically sound encryption performance is always preferred and desired. The proposed S-box based encryption scheme meant for secure telemedicine services is implemented using MATLAB tool, which runs on Windows 7 having 8GB RAM and Intel core *i*5-4590 CPU operating at 3.3GHz. Table 12 presents the time (in milliseconds) taken

TABLE 11. Comparison of encryption performance of the proposed scheme with other S-box based encryption schemes.

Encryption Scheme	Chi-Sq	MSE	PSNR	SSIM	CCF	Entropy	NPCR	UACI
Proposed	258.55	7753.95	9.24	0.000041	0.00091	7.9972	99.41	33.72
Ref. [69]	238.40	7771.88	8.78	0.0095	0.0018	7.9992	99.56	33.48
Ref. [70]	234.16	7835.4	9.19	-	-0.0014	7.9974	99.61	33.65
Ref. [71]	265.8	7795.5	9.21	-	0.0028	7.9970	99.61	33.47
Ref. [72]	234.13	7952.7	9.18	-	-0.0079	7.9975	99.66	33.71
Ref. [73]	-	40.26	9.12	-	0.0324	7.9046	98.91	32.78

TABLE 12. Time analysis of the S-box based encryption schemes.

Scheme	Time(*ms*)	Throughput(*kbps*)
Proposed	325.16	1574.6
Ref. [74]	3065.8	167
Ref. [70]	2398.7	213.5
Ref. [57]	1120.4	456.98
Ref.[72]	24567	228
Ref. [75]	631	811.4
Ref. [73]	801	639.2
Ref.[76]	382	1340.3

by our Pareto-optimal S-box based encryption scheme. A comparison of encryption speeds of different competing S-box based encryption schemes is also introduced in the same Table. It is found that an encryption time of 325.16 ms and a throughput of 1574.6 *kbps* are better compared to those of many recent similar encryption schemes. Hence, the presented encryption scheme is quite faster and better compared to competitive schemes and this justifies its suitability for real-time security applications.

VII. CONCLUSION

This paper provided a novel multi-objective evolution method for creating cryptographically-strong S-boxes. Existing methods strived to construct S-boxes by focusing on achieving high values of nonlinearity. Unfortunately, an S-box with good nonlinearity score may be susceptible to differential and correlation based cryptanalysis. This paper presented a method to yield S-boxes that can satisfy multiple performance parameters instead of only nonlinearity. The performance parameters such as bijectivity, nonlinearity, differential uniformity, and auto-correlation function have been optimized, simultaneously. The proposed method involves the non-dominated sorting algorithm-II, which is assisted with the chaotic map to obtain Pareto-optimal S-boxes. The performance assessment and comparison analyses showed that the proposed method is sufficiently better than many of the competitive optimization-based S-box construction methods available in the literature. Moreover, the Pareto-optimal S-box obtained from the proposed method has been applied in the area of telemedicine services to protect the medical imagery for secure tele-diagonosis and protection of sensitive patient data. Specifically, a new image encryption scheme is suggested, which is based on the Pareto-optimal S-box. The strength, robustness, and speed of the proposed encryption scheme have been compared with those of similar S-box based encryption schemes to justify its consistency, suitability and competence for the security of imagery data in telemedicine environment.

ACKNOWLEDGMENT

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University, through the Research Funding Program, Grant No. (FRP-1443-11).

REFERENCES

[1] M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, and H. Alhakami, "LAKE-IoD: Lightweight authenticated key exchange protocol for the internet of drone environment," *IEEE Access*, vol. 8, pp. 155645–155659, 2020.
[2] L. R. Knudsen and M. J. B. Robshaw, *The Block Cipher Companion*. Berlin, Germany: Springer, 2011.
[3] W. Feng, Y.-G. He, H.-M. Li, and C.-L. Li, "A plain-image-related chaotic image encryption algorithm based on DNA sequence operation and discrete logarithm," *IEEE Access*, vol. 7, pp. 181589–181609, 2019.
[4] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol. 130, pp. 1438–1444, Feb. 2017.
[5] 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.
[6] M. Ahmad, H. Chugh, A. Goel, and P. Singla, "A chaos based method for efficient cryptographic S-box design," in *Proc. Int. Symp. Secur. Comput. Commun.*, 2013, pp. 130–137.
[7] M. Ahmad, H. Haleem, and P. M. Khan, "A new chaotic substitution box design for block ciphers," in *Proc. Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Feb. 2014, pp. 255–258.
[8] 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.
[9] 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.
[10] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based S-box designs," *Phys. A, Stat. Mech. Appl.*, vol. 550, Jul. 2020, Art. no. 124072.

[11] 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.

[12] A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shuaib, W. Aslam, and M. Alawida, "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," *IEEE Access*, vol. 8, pp. 75473–75490, 2020.

[13] M. A. Khan, A. Ali, V. Jeoti, and S. Manzoor, "A chaos-based substitution box (S-box) design with improved differential approximation probability (DP)," *Iranian J. Sci. Technol., Trans. Electr. Eng.*, vol. 42, no. 2, pp. 219–238, 2018.

[14] 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.

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

[16] 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.

[17] 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.

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

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

[20] 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.

[21] R. Guesmi, M. A. B. 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.

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

[23] 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.

[24] 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.

[25] 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.

[26] 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. 3349–3358, Dec. 2018.

[27] H. Li, T. Li, W. Feng, J. Zhang, J. Zhang, L. Gan, and C. Li, "A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion," *J. Inf. Secur. Appl.*, vol. 61, Sep. 2021, Art. no. 102844.

[28] D. A. Trujillo-Toledo, O. R. López-Bonilla, E. E. García-Guerrero, E. Tlelo-Cuautle, D. López-Mancilla, O. Guillén-Fernández, and E. Inzunza-González, "Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps," *Chaos, Solitons Fractals*, vol. 153, Dec. 2021, Art. no. 111506.

[29] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou, G. Muhammad, M. S. Hossain, and A. M. Abbas, "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 160433–160449, 2020.

[30] W. El-Shafai and E. E.-D. Hemdan, "Robust and efficient multi-level security framework for color medical images in telehealthcare services," *J. Ambient Intell. Humanized Comput.*, pp. 1–16, Sep. 2021, doi: 10.1007/s12652-021-03494-1.

[31] E. E. García-Guerrero, E. Inzunza-González, O. R. López-Bonilla, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via ZigBee channels," *Chaos, Solitons Fractals*, vol. 133, Apr. 2020, Art. no. 109646.

[32] D. Jiang, L. Liu, L. Zhu, X. Wang, X. Rong, and H. Chai, "Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform," *Signal Process.*, vol. 188, Nov. 2021, Art. no. 108220.

[33] 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 Manag.*, vol. 17, no. 1, pp. 118–131, Mar. 2020.

[34] K. Deb, S. Agrawal, A. Pratap, and T. Meyarivan, "A fast elitist non-dominated sorting genetic algorithm for multi-objective optimization: NSGA-II," in *Proc. Int. Conf. Parallel Problem Solving Nature*. Berlin, Germany: Springer, 2000, pp. 849–858.

[35] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II," *IEEE Trans. Evol. Comput.*, vol. 6, no. 2, pp. 182–197, Jan. 2002.

[36] Y. Yusoff, M. S. Ngadiman, and A. M. Zain, "Overview of NSGA-II for optimizing machining process parameters," *Proc. Eng.*, vol. 15, pp. 3978–3983, Feb. 2011.

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

[38] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, pp. 3–72, Jan. 1991.

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

[40] U. Hayat, N. A. Azam, H. R. Gallegos-Ruiz, S. Naz, and L. Batool, "A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings," *Arabian J. for Sci. Eng.*, vol. 46, no. 9, pp. 8887–8899, Sep. 2021.

[41] M. M. Dimitrov, "On the design of chaos-based S-boxes," *IEEE Access*, vol. 8, pp. 117173–117181, 2020.

[42] 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.

[43] T. Peng, C. Zhang, J. Zhou, X. Xia, and X. Xue, "Multi-objective optimization for flood interval prediction based on orthogonal chaotic NSGA-II and kernel extreme learning machine," *Water Resour. Manag.*, vol. 33, no. 14, pp. 4731–4748, Nov. 2019.

[44] I. Pan and S. Das, "Chaotic multi-objective optimization based design of fractional order $PI^{\lambda}D^{\mu}$ controller in AVR system," *Int. J. Electr. Power Energy Syst.*, vol. 43, no. 1, pp. 393–407, Dec. 2012.

[45] 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.

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

[47] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 1994, pp. 386–397.

[48] 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.

[49] Y. Tian and Z. Lu, "Chaotic S-box: Intertwining logistic map and bacterial foraging optimization," *Math. Problems Eng.*, vol. 2017, pp. 1–11, Nov. 2017.

[50] 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.

[51] M. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dyn.*, vol. 99, pp. 3041–3064, Dec. 2019.

[52] H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, "A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7333–7350, Feb. 2021.

[53] 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.

[54] 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.
[55] 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.
[56] S. Koppu and V. M. Viswanatham, "Medical image security enhancement using two dimensional chaotic mapping optimized by self-adaptive grey wolf algorithm," *Evol. Intell.*, vol. 11, nos. 1–2, pp. 53–71, Oct. 2018.
[57] M. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A new design of cryptosystem based on S-box and chaotic permutation," *Multimedia Tools Appl.*, vol. 79, pp. 19129–19150, Mar. 2020.
[58] L. D. Singh and K. M. Singh, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017.
[59] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, "Medical image encryption algorithm based on Latin square and memristive chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 35419–35453, Dec. 2019.
[60] M. Ahmad and T. Ahmad, "A framework to protect patient digital medical imagery for secure telediagnosis," *Proc. Eng.*, vol. 38, pp. 1055–1066, Jan. 2012.
[61] W. Feng and J. Zhang, "Cryptanalzing a novel hyper-chaotic image encryption scheme based on pixel-level filtering and DNA-level diffusion," *IEEE Access*, vol. 8, pp. 209471–209482, 2020.
[62] A. Flores-Vergara, E. E. García-Guerrero, E. Inzunza-González, O. R. López-Bonilla, E. Rodríguez-Orozco, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic," *Nonlinear Dyn.*, vol. 96, no. 1, pp. 497–516, Apr. 2019.
[63] M. Ahmad, M. N. Doja, and M. M. S. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 33, no. 1, pp. 77–85, Jan. 2021.
[64] N. A. Azam, U. Hayat, and M. Ayub, "A substitution box generator, its analysis, and applications in image encryption," *Signal Process.*, vol. 187, Oct. 2021, Art. no. 108144.
[65] J. Tamang, J. D. D. Nkapkop, M. F. Ijaz, P. K. Prasad, N. Tsafack, A. Saha, J. Kengne, and Y. Son, "Dynamical properties of ion-acoustic waves in space plasma and its application to image encryption," *IEEE Access*, vol. 9, pp. 18762–18782, 2021.
[66] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020.
[67] M. Ahmad, M. Z. Alam, S. Ansari, D. Lambić, and H. D. AlSharari, "Cryptanalysis of an image encryption algorithm based on PWLCM and inertial delayed neural network," *J. Intell. Fuzzy Syst.*, vol. 34, no. 3, pp. 1323–1332, 2018.
[68] L. Liu, D. Jiang, X. Wang, X. Rong, and R. Zhang, "2D logistic-adjusted-chebyshev map for visual color image encryption," *J. Inf. Secur. Appl.*, vol. 60, Aug. 2021, Art. no. 102854.
[69] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020.
[70] M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi, and A. R. Alharbi, "Construction of S-boxes using different maps over elliptic curves for image encryption," *IEEE Access*, vol. 9, pp. 157106–157123, 2021.
[71] K. A. K. Patro and B. Acharya, "A novel multi-dimensional multiple image encryption technique," *Multimedia Tools Appl.*, vol. 79, nos. 19–20, pp. 12959–12994, May 2020.
[72] I. Khalid, S. S. Jamal, T. Shah, D. Shah, and M. M. Hazzazi, "A novel scheme of image encryption based on elliptic curves isomorphism and substitution boxes," *IEEE Access*, vol. 9, pp. 77798–77810, 2021.
[73] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, "A new image encryption scheme based on dynamic S-boxes and chaotic maps," *3D Res.*, vol. 7, no. 1, pp. 1–8, Mar. 2016.
[74] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, 2016.
[75] T. S. Ali and R. Ali, "A novel medical image signcryption scheme using TLTS and Henon chaotic map," *IEEE Access*, vol. 8, pp. 71974–71992, 2020.
[76] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he has worked with the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia. He has published over 100 research papers in internationally reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. 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. Recently, he has been listed among World's Top 2% Scientists in a study conducted by Elsevier and Stanford University in 2021 and 2022 as well and the report were published by Elsevier. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has served as a reviewer and a technical program committee member of many international conferences. He has also served as a Referee of some renowned journals, such as *Information Sciences*, *Signal Processing*, *Expert Systems With Applications*, *Journal of Information Security and Applications*, IEEE JOURNAL OF SELECTED AREAS IN COMMUNICATIONS, IEEE TRANSACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS: SYSTEMS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON RELIABILITY, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON NANOBIOSCIENCE, IEEE ACCESS, *Wireless Personal Communications*, *Neural Computing and Applications*, *International Journal of Bifurcation and Chaos*, *Chaos, Solitons & Fractals*, *Physica A*, *Signal Processing: Image Communication*, *Neurocomputing*, *IET Information Security*, *IET Image Processing*, *Security and Communication Networks*, *Optik*, *Optics & Laser Technology*, *Complexity*, *Computers in Biology and Medicine*, *Journal of Computational and Applied Mathematics*, and *Concurrency and Computation*.

REEM ALKANHEL (Member, IEEE) received the B.S. degree in computer science from King Saud University, Riyadh, Saudi Arabia, in 1996, the M.S. degree in information technology (computer networks and information security) from the Queensland University of Technology, Brisbane, Australia, in 2007, and the Ph.D. degree in information technology (networks and communication systems) from Plymouth University, Plymouth, U.K., in 2019. She has been with Princess Nourah Bint Abdulrahman University, Riyadh, since 1997. She is currently a Teacher Assistant at the College of Computer and Information Sciences. Her current research interests include communication systems, networking, the IoT, information security, and quality of service.

WALID EL-SHAFAI was born in Alexandria, Egypt. He received the B.Sc. degree (Hons.) in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from the Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from the Faculty of Electronic Engineering, Menoufia University, in 2019. Since January 2021, he has been joining as a Postdoctoral Research Fellow at the Security Engineering Laboratory (SEL), Prince Sultan University (PSU), Riyadh, Saudi Arabia. He is currently working as a Lecturer and an Assistant Professor with the Electronics and Communication Engineering (ECE) Department, FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC, H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software defined networks, the Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, cybersecurity applications, malware and ransomware detection and analysis, deep learning in signal processing, and communication systems applications. He has several publications in the above research areas in several reputable international and local journals and conferences. Also, he serves as a reviewer for several international journals.

ABEER D. ALGARNI received the B.Sc. degree (Hons.) in computer science from King Saud University, Riyadh, Saudi Arabia, in 2007, and the M.Sc. and Ph.D. degrees from the School of Engineering and Computer Sciences, Durham University, U.K., in 2010 and 2015, respectively. She has been working as an Assistant Professor at the College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, since 2008. Her current research interests include networking and communication systems, digital image processing, digital communications, and cyber security.

FATHI E. ABD EL-SAMIE received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. Since 2005, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. His current research interests include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications. He was a recipient of the Most Cited Paper Award from the *Digital Signal Processing* journal, in 2008.

NAGLAA F. SOLIMAN received the B.Sc., M.Sc., and Ph.D. degrees from the Faculty of Engineering, Zagazig University, Egypt, in 1999, 2004, and 2011, respectively. She has been working at the Faculty of Computer Science, PNU, Saudi Arabia, since 2015. She has been a Teaching Staff Member with the Department of Electronics and Communications Engineering, Faculty of Engineering, Zagazig University. Her current research interests include digital image processing, information security, multimedia communications, medical image processing, optical signal processing, big data, and cloud computing.