Received June 4, 2021, accepted June 14, 2021, date of publication June 17, 2021, date of current version June 24, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3090163

Block Cipher Nonlinear Confusion Components Based on New 5-D Hyperchaotic System

ADI ALHUDHAIF[1], MUSHEER AHMAD[2], AHMED ALKHAYYAT[3], NESTOR TSAFACK[4], ALAA KADHIM FARHAN[5], AND RAFEEQ AHMED[6]

[1]Department of Computer Science, College of Computer Engineering and Sciences in Al-kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[2]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[3]Department of Computer Technical Engineering, College of Technical Engineering, Islamic University, Najaf 192122, Iraq
[4]Research Unit of Laboratory of Automation and Applied Computer (LAIA), Electrical Engineering Department of IUT-FV, University of Dschang, Bandjoun, Cameroon
[5]Department of Computer Sciences, University of Technology, Baghdad 10066, Iraq
[6]Department of Computer Science and Engineering, Kamla Nehru Institute of Technology, Sultanpur 228118, India

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

ABSTRACT The security strengths of block ciphers greatly rely on the confusion components which have the tendency to transform the data nonlinearly into the perplexed form. This paper proposes to put forward a novel scheme of generating cryptographically strong nonlinear confusion components of block ciphers, usually termed as substitution-boxes (S-boxes). The anticipated S-box design scheme is based on a novel five-dimensional (5-D) chaotic system analyzed in this paper. The proposed 5-D dynamical system consists of hyperchaotic phenomenon, KY dimension, conservativity, unstable equilibrium point, and complex phase attractors which are suited for cryptographic applications. The S-box based on hyperchaotic system is made to evolve in order to generate an optimized S-box for high nonlinearity score to make it robust against many linear attacks. The performance analysis of proposed S-box demonstrates that it has bijectivity, high nonlinearity; satisfied strict avalanche criterion and bits independent criterion; low differential and linear probabilities. Moreover, performance appraisal of proposed S-box justifies its better strength and features over many recently investigated S-boxes.

INDEX TERMS Block ciphers, hyperchaotic system, substitution-box, security.

I. INTRODUCTION

The security and protection of sensitive data has been an issue of concern since decades as the open nature of internet makes it vulnerable towards attacks. Researchers have been suggesting various techniques and measures to protect the crucial data since years. One of the major techniques is encryption. The encryption algorithms are further divided into two categories, depending on how data is being processed, called block ciphers and stream ciphers. In block cryptosystems, the whole process is applied on a chunk of data at one time with an invariable makeover [1], [2]. Modern block ciphers consist of rounds of permutation and substitution processes, thereby, strongly exhibiting Shannon's confusion and diffusion properties. The two extensively deliberated architectures, used to build the block ciphers, are the famous Fiestal network and other one is the Substitution-Permutation (S-P) network [3]. The substitution boxes are an important part of such networks which help in nonlinear transformation of data, thereby helping in building the algorithms with required confusion and diffusion, making the algorithm robust against various types of attacks. The process of substitution and permutation are two mainstays of block ciphers and are completely mathematical procedures [4]. A substitution-box (S-box) operates on blocks of bits as input and converts these bits nonlinearly thereby producing a different block of output bits. On the other hand, permutation shuffles the input pattern, which is a linear transformation. A permutation-box on the other hand takes the output of the first round of S-box and feeds it to next round after permuting it. The combination of two creates the cipher tough and cryptic. And it's highly commended to have cryptographically strong S-boxes depicting confusion and diffusion strongly.

An $n \times m$ S-box receives n-bits of input and produces m bits of output. The output produced is a nonlinear transformation of input bits. In Galois Field theory, it can be represented as

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

$GF(2^n) \rightarrow GF(2^m)$, thereby transforming input data (of n bits) to output cipher data (of m bits) [5]. If $n = m$, the mapping would be one to one, which means there is a one to one mapping of input bits to the output bits. S-boxes depicting this one to one mapping are popularly known as Bijective S-boxes and are very important from the design perspective of S-P network based block ciphers. It's due to this property only, that $n \times n$ S-box can be treated as rearrangement of a series of numbers comprising values in the range of 0 to 2^{n-1} (inclusive).They can also be treated as Boolean functions with more than one input and output. An 8×8 S-box, thus, comprises 8 Boolean functions, every one taking total number of eight input bits and producing one bit of output, which means we will be getting 8 bits of output in totality. The strength of S-boxes can be evaluated via same metrics as that used to assess performance of Boolean functions. The S-boxes play a precise central part in determining the proficiency of block cryptosystems. The characteristic features of S-boxes are very significant in dispositioning secure cryptosystems [6]. This is why researchers are trying to build state-of-art S-boxes for deploying robust ciphers. Lately also, S-boxes have found their application in areas like Image encryption, watermarking, steganography, etc. [7].

The chaotic dynamic systems exhibit various features that are totally employable in the field of cryptography. The various features that can be counted on are: sensitive dependence on starting settings including its initial conditions and parameters, speedy acquisition of random-like feature of generated real-valued numbers, great entropy and complexity, etc [8]. These individualities make such systems highly fitting for building of robust encryption algorithms. Over the last decade, they have been used in construction of digital data security, design of S-boxes, hash functions, watermarking, steganography algorithms etc., [7], [9]. But, the fitness of these procedures strongly depends on the usage of profuse dynamics of these maps. Moreover, it is not always true that all chaotic maps exhibit the properties to fit in the field of cryptography. It has been found by researchers that most of the 1-D chaotic maps inherently have various limitations that make them unfit to develop a robust security system [10], [11].

Literature reports a number of S-box generation studies using chaotic systems [12], [13]. In [14], it has been proven that a decent S-box can be received by employing 3D chaotic Lorenz system. Authors in [15] designed S-box with the help of a technique relied on 3-D continuous-time chaotic system. In [16], Tian *et al.* explored a continuous-time 6-D hyperchaotic system to get the preliminary S-box matrix for an Artificial Bee Colony dependent optimization technique which led to an optimized S-box. The researchers in [17] suggested an S-box method using enhanced dynamics of scaled versioned Zhongtang chaotic system to yield S-box of good features. In [18], authors investigated an S-box construction approach which was dependent on a 4-D hyperchaotic system based swapping scheme. In [19], authors presented a systematic heuristic to get good balanced S-boxes with the aid of the usage of 5-D hyperchaotic system. Whereas, Wang *et al.* in [20] adopted 3-D chaotic system consisting of countless equilibrium points to propound an S-box, but it suffers with low nonlinearity feature. Authors in [21] investigated spatiotemporal chaos to get S-boxes. Wherein, the non-adjoining coupled map lattices and Arnold's cat map are applied to explore the chaotic phenomenon for S-box development. Notably, the literature reported the usage of time-delayed versions of some 1-D chaotic maps for to frame the acceptable configuration of S-boxes [22]. In the same way, there exists an S-box study which works on the dynamics of fractional-order chaotic structures for S-box construction investigated by Özkaynak in [23].

Existing S-boxes generation based on (discrete or continuous) chaotic methods does not lead to good nonlinearity and other performance parameters. In order to generate S-boxes with high nonlinearity scores, simple S-box generation should be followed with some novel method responsible for performance improvement. Motivated with this fact, the nonlinearity of initially generated S-box is augmented with the help of Arnold transform. This transformation makes major alteration in the given S-box and generates a new S-box within the possible search space. The main contributions of the work include the following.

1. The security of cryptographic primitives depends upon the dynamics of the chaotic systems. Therefore, a novel high-dimensional hyperchaotic system is proposed in this paper which found to have rich dynamics.
2. The novel system found to have hyperchaotic phenomenon, conservativity, good bifurcation, complex phase attractors and single unstable equilibrium point.
3. The new 5-D hyperchaotic system is explored to generate an initial 8×8 S-box. The S-box is enforced to optimize its performance by making Arnold transformation based search in the possible search space. This search enables to obtain an S-box with high nonlinearity feature.
4. The performance of proposed S-box is computed through some well-known performance parameters such as nonlinearity, bijectivity, strict avalanche criterion, bits independence criterion, differential probability and linear approximation probabilities. The obtained results show excellent security performance of the proposed S-box.
5. The generated S-box is also compared with many existing S-box methods to justify the improved performance of anticipated method.

The remaining portion of the paper is arranged as follows. The description of novel continuous-time 5-D hyperchaotic system and its dynamical behaviors are presented in Section 2. The proposed 8×8 S-box construction method which is primarily based on the dynamics of new 5-D hyperchaotic system is discoursed and delivered in Section 3. Section 4 is prepared to assess and analyze the security performance of generated S-box along with its strength comparison with some good S-box methods. Finally, the conclusion of the work presented in the paper is made in Section 5.

II. ESTABLISHMENT OF NOVEL 5-D HYPERCHAOTIC SYSTEM

The novel five-dimensional autonomous dynamical system is proposed whose dynamics is governed by the mathematical differential equations given in Eq. (1).

$$\begin{cases} \dot{x} = ay + du \\ \dot{y} = -ax + cz + b(x^2+1)w \\ \dot{z} = -cy + cw \\ \dot{w} = -b(x^2+1)y - cz \\ \dot{u} = -dx \end{cases} \tag{1}$$

where, x, y, z, w, u are the state variables of system (3), a, b, c, d are positive parameters of the novel system. It has been found after rigorous numerical analysis that the proposed 5-D system expressed in Eq. (3) exhibits hyperchaotic phenomenon for system parameters and initial conditions setting as: $a = b = c = d = 6$; $x_0 = y_0 = 0$, $z_0 = 0.5$, $w_0 = 1$, $u_0 = 0$. But these parameters and initial values can be tuned to achieve more dynamical behavior. In what follows, the characteristics and multifarious dynamics of our new 5-D system are investigated, such as the conservative property, equilibrium points, phase attractors, bifurcation diagrams, Lyapunov spectrum, and Kaplan-Yorke dimension.

III. LYAPUNOV EXPONENT AND DIMENSION

In nonlinear dynamical theory, Lyapunov exponent is a computable quantity for divergence rate of close trajectories. High dimensional dynamical system may have different trajectories of its starting separation vector. Each trajectory has its own divergence rate and hence multiple Lyapunov exponents exit for high dimensional systems. It is a measure to assess the chaotic and/or hyperchaotic characteristics of nonlinear dynamic systems. For a 5-D dynamical system computations yield five Lyapunov exponents. In this work the parameters and initial states are fixed as $a = b = c = d = 6$; $x_0 = y_0 = 0$, $z_0 = 0.5$, $w_0 = 1$, $u_0 = 0$. From the Lyapunov computation results, it is observed that the Lyapunov exponents are symmetric around the horizontal axis. This can be used to further support the conservative dynamics of the system. Literature designates that when $LE_{1,2} > 0$, $LE_3 \approx 0$, $LE_{4,5} < 0$ then the system is hyperchaotic in the selected range of parameter. For the specified settings of parameters values and initial states, the five Lyapunov exponents are obtained as: $\boldsymbol{LE_1} = 0.063$, $\boldsymbol{LE_2} = 0.005$, $\boldsymbol{LE_3} = 0.000$, $\boldsymbol{LE_4} = -0.005$, $\boldsymbol{LE_5} = -0.063$. The obtained values of Lyapunov exponents are indicating that the system exhibits hyperchaotic behavior as it has two positive, one zero and two negative Lyapunov exponents. Moreover, the parameter a is selected as the tunable parameter in the range $2 \leq a \leq 6$ and the Lyapunov exponents spectrum shown in Figure 1 is observed.

The fractal dimension is another measure which can demonstrate typical feature of chaotic systems. The Kaplan-Yorke dimension calculated through Lyapunov exponents of system is the widely used fractal dimension. The Kaplan-Yorke dimension D_{KY} defined in Eq. (2) is obtained [24].

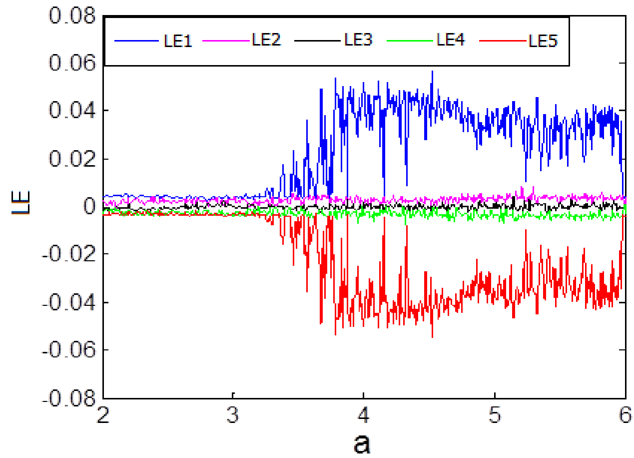

FIGURE 1. Lyapunov exponents diagram for $2 \leq a \leq 6$.

$$D_{KY} = k + \frac{1}{|\lambda_{k+1}|} \sum_{i=1}^{k} LE_i \tag{2}$$

$$\sum_{i=1}^{k} LE_i \geq 0 \tag{3}$$

where, k is the largest integer satisfying Eq. (3) ($k = n = 5$ in this case). For the proposed system (1), it can be easily observed that $LE_1 + LE_2 + LE_3 + LE_4 + LE_5 = 0$ as the dynamical system is conservative. Consequently, $D_{KY} = 5$ and the attractors are typical of hyperchaos nature.

A. CONSERVATIVITY

In order analyze the conservative property of the proposed system with respect to its divergence. Let us consider the vector notation given in Eq. (4) of the new system.

$$h = \begin{cases} h_1 = \dot{x} = ay + du \\ h_2 = \dot{y} = -ax + cz + b(x^2+1)w \\ h_3 = \dot{z} = -cy + cw \\ h_4 = \dot{w} = -b(x^2+1)y - cz \\ h_5 = \dot{u} = -dx \end{cases} \tag{4}$$

The divergence [25] of the vector field h on R^5 is given by Eq. (5) as follows:

$$\nabla \cdot h = \frac{\partial h_1}{\partial x} + \frac{\partial h_2}{\partial y} + \frac{\partial h_3}{\partial z} + \frac{\partial h_4}{\partial w} + \frac{\partial h_5}{\partial u} \tag{5}$$

This divergence measures identify the speed at which volumes altered under the flow Φ_t of field h. Let D to denote a region in space R^5 with a clear periphery and let $D(t) = \Phi_t(t)$, the image of D under Φ_t at the time t of the flow of h. Let $V(t)$ to represent the volume of $D(t)$. By theorem from Liouville, we have:

$$\frac{dV}{dt} = \int_{D(t)} (\nabla \cdot h)\, dxdydzdwdu \tag{6}$$

$$\nabla \cdot h = \frac{\partial h_1}{\partial x} + \frac{\partial h_2}{\partial y} + \frac{\partial h_3}{\partial z} + \frac{\partial h_4}{\partial u} + \frac{\partial h_5}{\partial w} = 0 \quad (7)$$

Now, substituting Eq. (7) in Eq. (6) and solving, we get

$$V(t) = V(0) \quad (8)$$

This shows that the volume $V(t)$ in the state space is conservative and thus the system belongs to the class of conservative 5-D hyperchaotic systems.

B. EQUILIBRIUM POINTS

The equilibrium point is obtained when each equation of the system (1) is zero, i.e.

$$\begin{cases} \dot{x} = ay + du = 0 \\ \dot{y} = -ax + cz + b(x^2+1)w = 0 \\ \dot{z} = -cy + cw = 0 \\ \dot{w} = -b(x^2+1)y - cz = 0 \\ \dot{u} = -dx = 0 \end{cases} \quad (9)$$

By solving Eq.(9) we found that the equilibrium points of system (1) follow a continuous curve defined by:

$$E_k \{ (x_0, y_0, z_0, w_0, u_0) \in R^5 \,|x_0 = 0, y_0 = k, z_0 = 0, w_0 = k, u_0 = -ak/d \}$$

The Jacobian matrix $\boldsymbol{J}$ of system (1) around the equilibrium curve is expressed in Eq. (10) and (11) below.

$$J = \begin{bmatrix} \frac{\partial h_1}{\partial x} & \frac{\partial h_1}{\partial y} & \frac{\partial h_1}{\partial z} & \frac{\partial h_1}{\partial u} & \frac{\partial h_1}{\partial w} \\ \frac{\partial h_2}{\partial x} & \frac{\partial h_2}{\partial y} & \frac{\partial h_2}{\partial z} & \frac{\partial h_2}{\partial u} & \frac{\partial h_2}{\partial w} \\ \frac{\partial h_3}{\partial x} & \frac{\partial h_3}{\partial y} & \frac{\partial h_3}{\partial z} & \frac{\partial h_3}{\partial u} & \frac{\partial h_3}{\partial w} \\ \frac{\partial h_4}{\partial x} & \frac{\partial h_4}{\partial y} & \frac{\partial h_4}{\partial z} & \frac{\partial h_4}{\partial u} & \frac{\partial h_4}{\partial w} \\ \frac{\partial h_5}{\partial x} & \frac{\partial h_5}{\partial y} & \frac{\partial h_5}{\partial z} & \frac{\partial h_5}{\partial u} & \frac{\partial h_5}{\partial w} \end{bmatrix} \quad (10)$$

$$J = \begin{bmatrix} 0 & a & 0 & 0 & d \\ -a & 0 & c & b & 0 \\ 0 & -c & 0 & c & 0 \\ 0 & -b & -c & 0 & 0 \\ -d & 0 & 0 & 0 & 0 \end{bmatrix} \quad (11)$$

The characteristic equation is obtained as:

$$\lambda^5 + (a^2+b^2+d^2+2c^2)\lambda^3 + (a^2c^2+b^2d^2+2c^2d^2)\lambda = 0 \quad (12)$$

The solution of the above characteristic equation is computed for the case $a = b = c = d = 6$ and the result given as $\lambda_1 = 0; \lambda_{2,3} = \pm 12i; \lambda_{4,5} = \pm 6i$. From this result it is observed that one Eigen value is equal to zero (λ_1=0), two pairs of eigenvalues are purely imaginary numbers ($\lambda_{2,3} = \pm 12i; \lambda_{4,5} = \pm 6i$). This observation indicates that the equilibrium is not asymptotically stable.

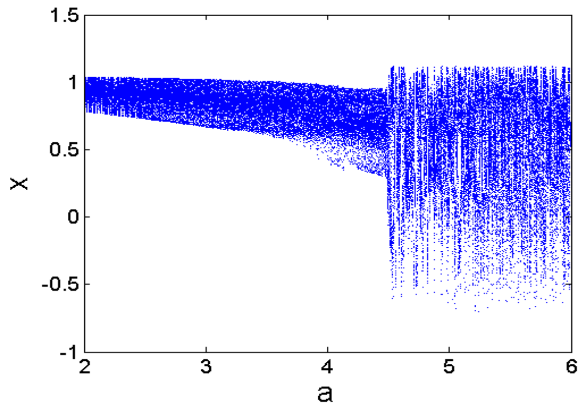

FIGURE 2. Bifurcation diagram of system (1) for b = c = d = 6; x0 = y0 = 0, z0 = 0.5, w0 = 1, u0 = 0.

C. BIFURCATION AND PHASE PORTRAITS

The bifurcation diagram is usually exploited to reveal the complete dynamic behavior of a dynamical system. It is obtained by solving the system equation and storing the local maximum of a variable with respect to the variation of the selected control parameter. For mentioned settings of parameters and initial states and a is selected as the tunable parameter, the bifurcation behavior shown in Figure 2 is observed. The bifurcation diagram indicates that the system displays no limit cycle in the selected range of parameters. Complex attractors of hyperchaotic systems in the phase space are considered as one of the indicator of rich dynamics and good performance of the system. For our hyperchaos system (1), the projections of strange asymmetric attractors onto different spaces and plans are displayed in Figure 3 for $a = b = c = d = 6$; $x_0 = y_0 = 0$, $z_0 = \pm 0.5$, $w_0 = \pm 1$, $u_0 = 0$. The complicated phase plots make it clear that the new system possess very fascinating, multifaceted and disordered dynamical behavior within the phase spaces.

IV. PROPOSED S-BOX GENERATION USING NEW 5-D HYPERCHAOTIC SYSTEM

The new S-box generation scheme based on the rich dynamics of our 5-D hyperchaotic system is discoursed in Section 2 is presented. Earlier, many high dimensional chaotic systems have been applied to construct the 8 × 8 S-boxes. But, our proposed scheme comes out better and efficient compared to prevailing S-box studies in terms of cryptographic recital of S-box. The proposed scheme majorly consists of two parts; each part is assisted by the new hyperchaotic system and under key-controlled. First part is devoted to the formation of initial S-box which is based on the chaotic sequences generated from the hyperchaotic system after applying numerical analysis method for its solution. Second part is to evolve the initial S-box for optimized nonlinearity criteria of the S-box. The nonlinearity improvisation is done with the help of key-dependent shuffling of S-box to yield another S-box. The new S-box is discarded if it is not better than the previous S-box over nonlinearity score; else it is retained for the next iteration to operate.

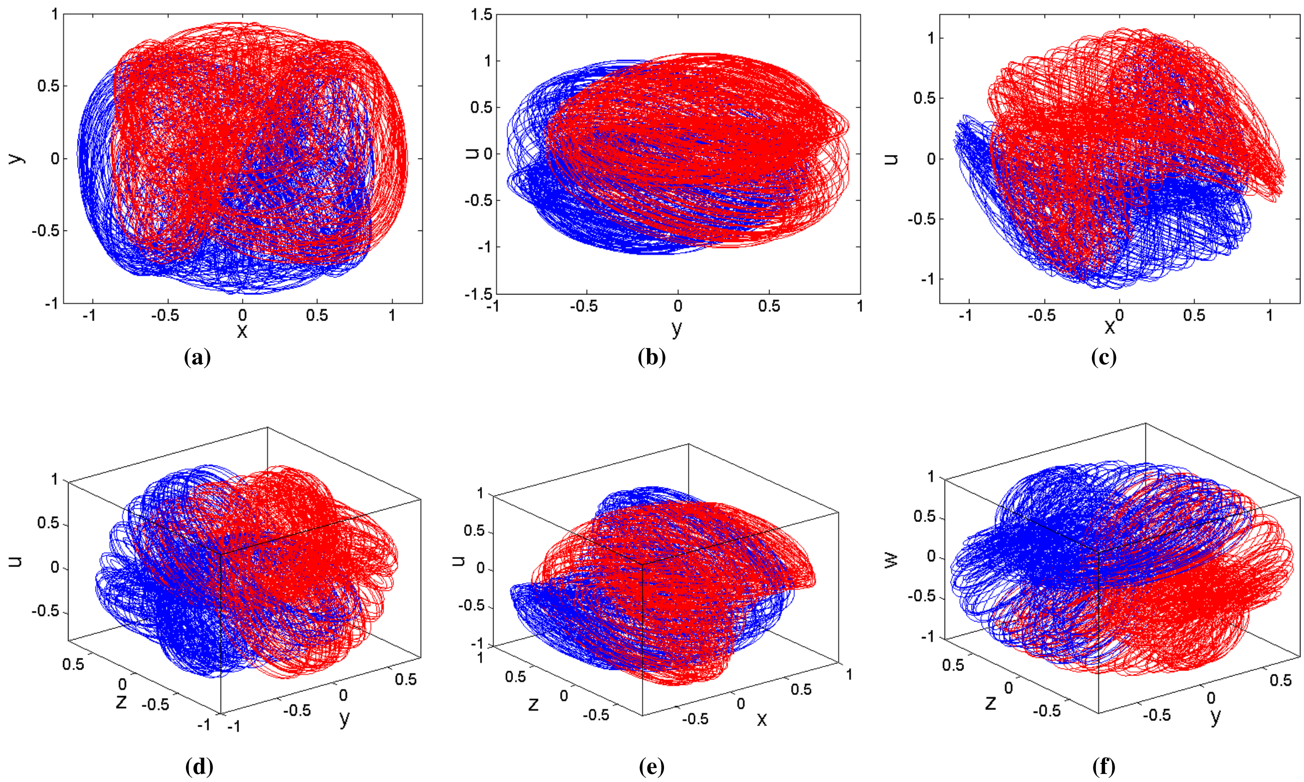

FIGURE 3. Projections of attractors of new 5-D hyperchaotic system onto different spaces (a) x-y, (b) y-u, (c) x-u, (d) y-z-u, (e) x-z-u, (f) y-z-w.

The key-dependent shuffling, to get new S-box configuration, is applied using parametric Arnold transform. Arnold transform is a simple discrete ergodic stretch and fold mapping found by Vladimir Arnold in 1968 [26]. The 2D Arnold transform has the following form.

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = A \begin{pmatrix} i \\ j \end{pmatrix} mod(N) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} mod(N) \tag{13}$$

The classical transform (13) computes the new position (i', j') corresponding to the old position (i, j) within the bounded region of $N \times N$. This mapping has consists of many exclusive features such as (1) it is one-to-one area preserving map and performs transform $N \times N \rightarrow N \times N$, (2) the determinant of transformation matrix A i.e. $\det(A) = 1$, (3) it is reversible mapping, and (4) sufficient number of rounds r cause the randomized permutation of the 2D data matrix. The classical Arnold transform is generalized by introducing two parameters into the transformation matrix A to make its behavior controllable and key dependent. The parametric Arnold transform is defined as.

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} mod(N) \tag{14}$$

The parametric transform inherits all the features of classical one. This parametric form of Arnold transform is extensively utilized in many security applications [27]–[32]. This discrete transform have been utilized in the proposed work to make possible search within search space of 8×8 S-box. Therefore, the parameters of this transform are altered in each iterations to make it more random and effective in disturbing the positions of S-box elements with an aim to get considerably new S-box. The proposed S-box generation scheme based on hyperchaotic system is as follows.

1. Take initial values of all state variables and system parameters of system (1) and let $S = [\,]$.
2. Iterate system (1) for m times and reject the values of state variables except the last one.
3. Further iterate system (1) once to get next state of hyperchaotic variables x, y, z, u, w.
4. Let $\Theta(1)= x$, $\Theta(2)= y$, $\Theta(3)= z$, $\Theta(4)= u$, $\Theta(5)=w$ and preprocess them as:
   $\Omega(i) = \Theta(i) \times 10^5 - floor(\Theta(i) \times 10^5)$, where $i = 1 \sim 5$
5. Extract possible legal candidate elements of 8×8 S-box S as:
   $\Omega(i) = floor(\Omega(i) \times 10^{10})$
   $K(i) = [\Omega(i)]mod(256)$
   $K(6) = [sum(K(1) \text{ to } K(5))]mod(256)$
6. Compute select lines s_1 and s_2 as:
   $s_1 = [\Omega(1)+\Omega(2)+\Omega(3)]mod(3)$
   $s_2 = [\Omega(4) + \Omega(5)]mod(3)$
7. Find R_1 and R_2 as
   If $(s_1 == 0)$ set $R_1 = K(1)$
   else if $(s_1 == 1)$ set $R_1 = K(2)$
   else set $R_1 = K(3)$

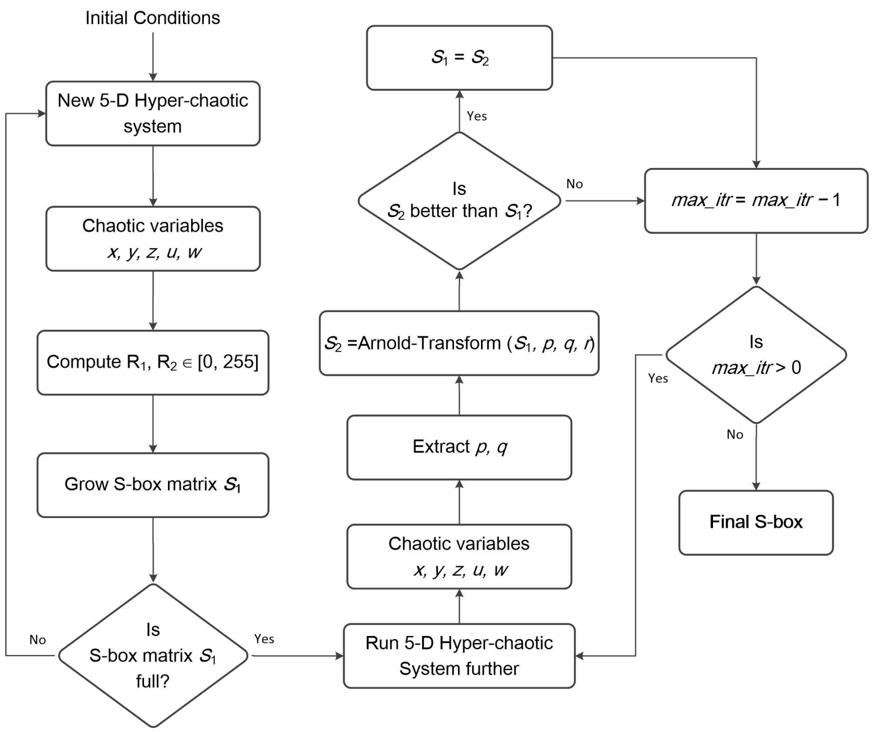

FIGURE 4. Schematic diagram of S-box generation using proposed method.

If ($s_2 == 0$) set $R_2 = K(4)$
else if ($s_2 == 1$) set $R_2 = K(5)$
else set $R_2 = K(6)$

8. Populate S-box array S as:
   If (R_1 is not in S) insert R_1 in array S
   If (R_2 is not in S) insert R_2 in array S
9. If ($length(S) < 256$) go back to Step 3.
10. Reshape as $S = reshape(S, 16, 16)$ and let $nl_1 = nonlinearity(S)$,
11. Set $S_1 = S_2 = S$
12. Further iterate system (1) once to get next state of hyperchaotic variables x, y, z, u, w.
13. Let $\Theta(1)= x$, $\Theta(2)= y$, $\Theta(3)= z$, $\Theta(4)= u$, $\Theta(5)=w$ and preprocess them as:
    $\Omega(i) = \Theta(i) \times 10^5 - floor(\Theta(i) \times 10^5)$, where $i = 1 \sim 5$
14. Extract parameters of Arnold Cat transform:
    $\Omega(i) = floor(\Omega(i) \times 10^{10})$
    $p = 11 + [\Omega(1) + \Omega(2) + \Omega(3)]mod(53)$
    $q = 19 + [\Omega(4)+ \Omega(5)]mod(37)$
15. Do the following permutation for r number of rounds
    for $i_1 = 1$ to 16
        for $j_1 = 1$ to 16
            $i_2 = 1 + [i_1 + q \times j_1]mod(16)$
            $j_2 = 1 + [p \times i_1 + (1+p \times q) \times j_1]mod(16)$
            $S_2(i_2, j_2) = S_1(i_1, j_1)$
        end
    end
    $S_1 = S_2$
16. Evaluate $nl_2 = nonlinearity(S_2)$
17. If ($nl_2 >= nl_1$) set $nl_1 = nl_2$ and $S = S_2$
18. Repeat from Step 11 for *max_itr* times
19. Announce S as the evolved 8×8 S-box

The proposed S-box generation method is also shown in the block diagram given in Figure 4.

V. PERFORMANCE RESULTS AND ANALYSES

The security recital of generated S-box is assessed and examined in this section. The S-box shown in Table 1 is our anticipated 8×8 S-box. The set of standard security metrics engaged to appraise the cryptographic forte of our S-box includes bijectivity, nonlinearity, bits independence criterion, strict avalanche criterion, differential probability, and linear probability. An S-box is deemed more secure, robust and better if it has higher NL and BIC-NL scores, SAC value close to 0.5, and lower differential/linear probabilities. In what follows, these performance parameters are further analyzed.

A. BIJECTIVITY

Bijectivity criterion demands that a unique n-bit input of an n × n S-box should produce a unique output of n-bits. Similarly, for any n-bit output of an n × n S-box, there should be a distinct n-bit input. Proposed n × n S-box for n = 8 portrayed in Table 1 validates this criterion very well as unique inputs harvests unique outputs. Typical bijectivity value of an 8×8 S-box is $2^{8-1} = 128$ [7]. Our projected S-box as shown in Table 1 holds this condition by having all

TABLE 1. Proposed S-box (confusion component).

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

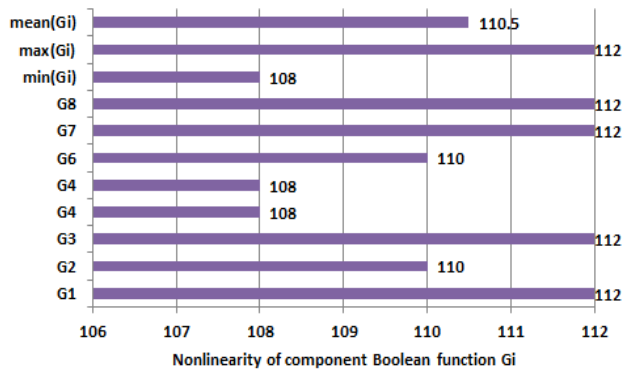

FIGURE 5. Nonlinearities of component Boolean functions G_i ($1 \le i \le 8$) of proposed S-box.

possible diverse output values in the permissible range. In all coordinate Boolean Functions, number of ones is equal to the number of zeros.

B. NONLINEARITY (NL)

An S-box is less immune and weak if it has a linear mapping between the output and input. If an S-box structure has the capability to map an input to an output in a nonlinear fashion, respective S-box is believed to be stronger one. Such nonlinear components i.e. S-boxes are capable to defy linear cryptanalysis efforts by attackers. One can compute the value of nonlinearity (NL) of an 8-bit Boolean function G using Eq. (16) given below [33], [34]:

$$NonLin(G) = 128 \times \left(1 - 2^{-8}\left(WH_{max}(G)\right)\right) \tag{15}$$

where, $WH_{\max}(G)$ is the Walsh-Hadamard transformation for an 8-bit Boolean function G. The 8 component Boolean functions that make up our proposed S-box are having the

TABLE 2. Nonlinearities of component Boolean functions of proposed S-box.

Boolean Function	G_1	G_2	G_3	G_4	G_5	G_6	G_7	G_8
$NonLin(G)$	112	110	112	108	108	110	112	112

nonlinearity values shown in Table 2 and graphically depicted in Figure 5. The proposed S-box has largest nonlinearity value of 112 and minimum value of 108 with a decent mean score of 110.5. This certainly demonstrate that the proposed confusion component (S-box) has excellent nonlinearity performance and highly capable to resist any linear attacks.

C. STRICT AVALANCHE CRITERION (SAC)

This performance representative of an S-box guarantees that one bit change at input side causes an alteration of 50% of output bits [35]. Consequently, an S-box that has strict avalanche criterion (SAC) value near to 0.5 is deliberated as a strong one. Dependency matrix of SAC values of our S-box is specified in Table 3. The mean of this table indicates the SAC of proposed S-box which comes out as 0.5065 with a slight deviation from ideal value of 0.5. Thus, our S-box satisfies the SAC criterion quite well.

D. BITS INDEPENDENCE CRITERION (BIC)

This distinctive feature of S-boxes ensure that variation in any two output bits does not depend on each other whenever a single input bit is changes [36]. As per this criterion, the Boolean functions $G_{xy} = bitxor(G_x, G_y)$ $(x \neq y)$ should be able to depict good nonlinearity performance. Means,, there should exist pairwise independence of all possible set of avalanche vectors obtained by single bit flipping of input. We followed the standard procedure for computing BIC-nonlinearity (BIC-NL) scores for our proposed S-box.

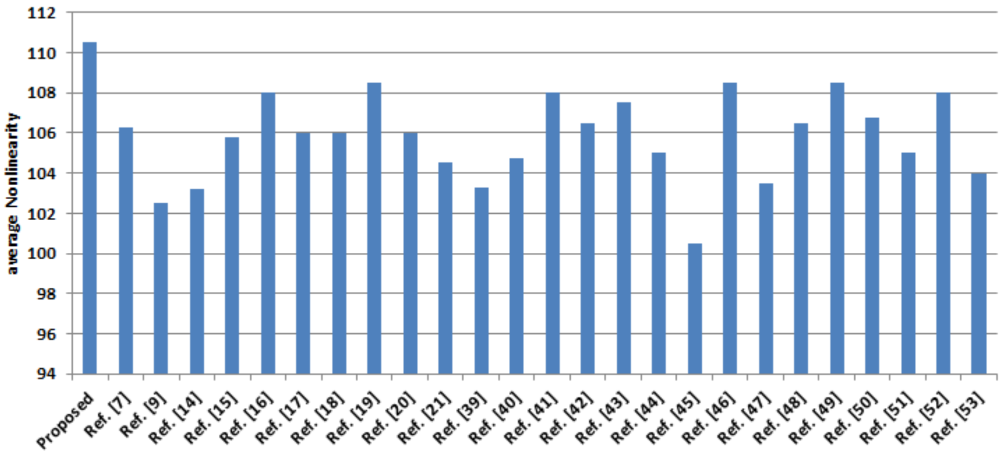

FIGURE 6. Comparison of nonlinearities of 8 × 8 S-boxes.

TABLE 3. SAC table for proposed S-box.

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

TABLE 4. BIC-nonlinearity scores for proposed S-box.

	G_1	G_2	G_3	G_4	G_5	G_6	G_7	G_8
G_1	-	108	110	104	104	110	108	108
G_2	108	-	110	108	106	110	108	108
G_3	110	110	-	102	102	108	108	110
G_4	104	108	102	-	100	104	106	104
G_5	104	106	102	100	-	98	106	104
G_6	110	110	108	104	98	-	110	108
G_7	108	108	108	106	106	110	-	108
G_8	108	108	110	104	104	108	108	-

Table 4 is prepared to provide the BIC-NL values of 56 possible Boolean functions G_{xy} for our S-box; it has an average score of 106.43 which is fairly better than many available S-boxes.

E. DIFFERENTIAL PROBABILITY (DP)

Assailants apprehension ciphertext and examine the existing I/O mapping via some differentials to catch any existing evidence for plaintext. Investigation of these differentials supports the assailants to recognize the comprehensive or partial plaintext or key [37]. S-box designers strive to keep dissimilarity between these two variations as low as achievable. To calculate this difference, analysts evaluate the differential probability (DP) of an S-box under examination. To counterattack differential cryptanalysis, DP of an S-box should be short. Differential probability is gauged using standard formula shown in Eq. (16).

$$DP = \frac{\underset{\Delta_u \neq 0, \Delta_v}{MAX} \ [\#\{u \in K | S(u) \oplus S(u \oplus \Delta_u) = \Delta_v\}]}{256} \tag{16}$$

where, Δ_u is the input differential, Δ_v is the output differential, and $K = \{0, 1, 2, \ldots, 255\}$. An S-box that has small values of differentials possesses the capability to defy differential cryptanalytic efforts. Maximum differential probability of suggested S-box evaluates to 0.03906 only which designates that the proposed S-box deals appreciable insolence to differential cryptanalysis. Table 5 demonstrates appraisal of DP values of some existing S-boxes with proposed S-box.

F. LINEAR APPROXIMATION PROBABILITY (LAP)

The main objective behind the design of a good cipher is to generate a nonlinear association between its input and output. This nonlinear association helps in creating a ciphertext that bears more meaninglessness for its invaders. An S-bx generated in a thought-provoking way assists in achieving such a nonlinear mapping conveniently. Attackers attempt to exploit the weaker mapping between input and output by linear cryptanalysis. linear approximation probability (LAP) helps in measuring the forte of this association using Eq. (17) [38].

$$LAP = \max_{\alpha_i, \beta_i \neq 0} \left| 2^{-8} \left(\#\{i \in K \,|\, i.\alpha_i = S(i).\beta_i\}\right) - 0.5 \right| \tag{17}$$

where, α_i is the input mask and β_i is the output mask. If the linking between the plaintext and ciphertext holds linear structure, the LAP value for the S-box is greater and linear cryptanalysis is calm for the assailants. The LAP score of suggested S-box is only 0.1172 which is sufficiently small LAP desired to fight linear cryptanalysis. Thus, proposed S-box holds ample latent to defense such cryptanalytic labors. A comparison of LAP values of some existing S-boxes and

TABLE 5. Differential distribution table for proposed S-box.

.01563	.01563	.02344	.01563	.02344	.01563	.02344	.02344	.01563	.02344	.02344	.03906	.02344	.02344	.01563	.01563
.02344	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.01563	.02344	.02344	.02344	.01563	.02344	.02344	.01563
.02344	.02344	.01563	.02344	.02344	.02344	.01563	.02344	.02344	.02344	.01563	.01563	.01563	.02344	.02344	.02344
.02344	.02344	.02344	.02344	.02344	.01563	.03125	.02344	.01563	.02344	.03125	.02344	.02344	.01563	.01563	.01563
.02344	.02344	.02344	.03125	.02344	.03125	.02344	.01563	.02344	.02344	.02344	.02344	.02344	.02344	.01563	.01563
.02344	.02344	.02344	.02344	.02344	.01563	.02344	.02344	.02344	.01563	.02344	.02344	.02344	.01563	.02344	.02344
.02344	.02344	.02344	.01563	.02344	.02344	.02344	.02344	.02344	.01563	.01563	.02344	.02344	.02344	.01563	.02344
.01563	.02344	.01563	.02344	.02344	.02344	.01563	.02344	.02344	.01563	.02344	.02344	.02344	.02344	.01563	.02344
.02344	.02344	.01563	.01563	.02344	.02344	.01563	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.02344
.01563	.02344	.03125	.01563	.02344	.01563	.02344	.03125	.02344	.02344	.02344	.02344	.02344	.01563	.02344	.02344
.01563	.01563	.02344	.01563	.01563	.03125	.01563	.01563	.02344	.02344	.02344	.02344	.02344	.02344	.01563	.01563
.02344	.02344	.01563	.01563	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.01563	.01563	.02344	.02344
.02344	.02344	.02344	.02344	.01563	.01563	.02344	.02344	.01563	.02344	.01563	.02344	.01563	.02344	.02344	.01563
.02344	.02344	.01563	.01563	.02344	.02344	.02344	.01563	.02344	.02344	.02344	.01563	.02344	.02344	.01563	.02344
.01563	.02344	.01563	.01563	.02344	.02344	.02344	.02344	.02344	.02344	.01563	.02344	.02344	.01563	.01563	.01563
.01563	.02344	.01563	.02344	.01563	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.01563	0

TABLE 6. Performance comparison of 8 × 8 S-boxes.

S-box	Nonlinearity			SAC	BIC-NL	DP	LAP
	min	max	mean				
Proposed S-box	108	112	110.5	0.5065	106.43	0.03906	0.1172
Ref. [7]	104	108	106.25	0.5009	103.64	0.03906	0.1328
Ref. [9]	96	106	102.5	0.5037	103.9	0.03906	0.1250
Ref. [14]	100	106	103.2	0.5048	103.7	0.03906	0.1250
Ref. [15]	104	108	105.8	0.4976	104.5	0.03906	0.1250
Ref. [16]	106	110	108	0.5073	104	0.03906	0.1523
Ref. [17]	104	110	106	0.5039	103.38	0.03906	0.1406
Ref. [18]	102	108	106	0.5002	104.4	0.03906	0.1484
Ref. [19]	106	110	108.5	0.5017	104	0.03906	0.1328
Ref. [20]	104	110	106	0.5197	104.21	0.03906	0.1328
Ref. [21]	102	108	104.5	0.4980	104.64	0.0496	0.1250
Ref. [39]	96	106	103.25	0.5151	103.07	0.21094	0.1562
Ref. [40]	100	106	104.75	0.4980	102.71	0.03906	0.1328
Ref. [41]	106	110	108	0.4993	101.93	0.04687	0.1496
Ref. [42]	106	108	106.5	0.4990	103.57	0.03906	0.1250
Ref. [43]	104	110	107.5	0.4980	103.5	0.03906	0.14063
Ref. [44]	102	108	105	0.5029	102.9	0.04687	0.1484
Ref. [45]	96	104	100.5	0.4973	102.78	0.03906	0.15625
Ref. [46]	106	110	108.5	0.4995	103.85	0.03906	0.1094
Ref. [47]	98	106	103.5	04958	103.5	0.05468	0.1328
Ref. [48]	106	108	106.5	0.5009	104.07	0.03906	0.1328
Ref. [49]	108	110	108.5	0.4910	103.78	0.03906	0.0791
Ref. [50]	104	108	106.75	0.4976	103.75	0.03906	0.1328
Ref. [51]	104	108	105	0.5060	103.5	0.03906	0.1250
Ref. [52]	104	110	108	0.5007	104.21	0.03906	0.1250
Ref. [53]	100	108	104	0.5160	103.5	0.03906	0.1328

suggested S-box is listed in Table 6. It is noticeable that the suggested S-box has respectable strength as compared to other S-boxes in the Table.

The security performance of suggested S-box is compared with some S-boxes in Table 6. The comparative study is based on the well accepted parameters of S-box like nonlinearity, SAC, BIC-NL, differential probability, and linear approximation probability. It is quite clear from the comparison of average nonlinearity depicted in Figure 6 that the proposed S-box has optimized and excellent performance on the nonlinearity aspect of S-box performance. Hence, the proposed S-box has the adequate power and robustness to withstand the linear attacks. It is also evident that the performance of our S-box on other parameters is also pretty satisfactory and consistent with other S-box studies.

VI. CONCLUSION

This first phase of the paper presents a new five-dimensional hyperchaotic system which exhibits rich phenomenon. The dynamical analysis of novel 5-D system showed that it has good bifurcation behavior, hyperchaotic nature, KY dimension of 5, conservativity, unstability at equilibrium point, complex attractors in phase portraits. The high-dimensional hyperchaotic systems considered as better candidate for cryptographic applications. Based on the fact, a cryptographically strong S-box construction method is proposed using the dynamics of new 5-D hyperchaotic system in second phase of the paper. The generated S-box found to have excellent cryptographic security features to diminish the differential and linear assaults. The strong recital of anticipated S-box makes it qualifiable as a successful nonlinear component candidate for use in block ciphers. Any lightweight block cipher based on proposed S-box will make it robust and powerful to meet the requirements of nodes of wireless sensor networks. The future work of the presented study is to design a lightweight block cipher using the proposed S-boxes and other important primitives for wireless sensor networks security.

REFERENCES

[1] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA, CRC Press, 2005.
[2] L. R. Knudsen and M. Robshaw, *The Block Cipher Companion*. Berlin, Germany: Springer-Verlag, 2011.
[3] M. Ahmad, H. Chugh, A. Goel, and P. Singla, "A chaos based method for efficient cryptographic S-box design," in *Proc. Int. Symp. Secur. Comput. Commun.*, Berlin, Germany: Springer, Aug. 2013, pp. 130–137.
[4] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7201–7210, Nov. 2019.
[5] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. A. Solami, and M. M. S. Beg, "A new 1D chaotic map and β-hill climbing for generating substitution-boxes," *IEEE Access*, vol. 6, pp. 55405–55418, 2018.
[6] U. Hayat, N. A. Azam, and M. Asif, "A method of generating 8×8 substitution boxes based on elliptic curves," *Wireless Pers. Commun.*, vol. 101, no. 1, pp. 439–451, Jul. 2018.
[7] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dyn.*, vol. 99, no. 4, pp. 3041–3064, Dec. 2019.
[8] M. García-Martínez, L. J. Ontañón-García, E. Campos-Cantón, and S. Čelikovský, "Hyperchaotic encryption based on multi-scroll piecewise linear systems," *Appl. Math. Comput.*, vol. 270, pp. 413–424, Nov. 2015.
[9] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019.
[10] M. García-Martínez and E. Campos-Cantón, "Pseudo-random bit generator based on multi-modal maps," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 2119–2131, Dec. 2015.
[11] M. García-Martínez and E. Campos-Cantón, "Pseudo-random bit generator based on lag time series," *Int. J. Modern Phys. C*, vol. 25, no. 04, Apr. 2014, Art. no. 1350105.
[12] B. B. Cassal-Quiroga and E. Campos-Cantón, "Generation of dynamical S-boxes for block ciphers via extended logistic map," *Math. Problems Eng.*, vol. 2020, pp. 1–12, Mar. 2020.
[13] 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.
[14] F. Özkaynak and A. B. Özer, "A method for designing strong S-boxes based on chaotic lorenz system," *Phys. Lett. A*, vol. 374, no. 36, pp. 3733–3738, Aug. 2010.
[15] 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, Dec. 2015.
[16] 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.
[17] 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, Jan. 2017.
[18] F. U. Islam and G. Liu, "Designing S-box based on 4D-4Wing hyperchaotic system," *3D Res.*, vol. 8, no. 1, p. 9, Mar. 2017.
[19] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018.
[20] X. Wang, A. Akgul, U. Cavusoglu, V.-T. Pham, D. Vo Hoang, and X. Nguyen, "A chaotic system with infinite equilibria and its S-box constructing application," *Appl. Sci.*, vol. 8, no. 11, p. 2132, Nov. 2018.
[21] L. Liu, Y. Zhang, and X. Wang, "A novel method for constructing the S-box based on spatiotemporal chaotic dynamics," *Appl. Sci.*, vol. 8, no. 12, p. 2650, Dec. 2018.
[22] F. Özkaynak and S. Yavuz, "Designing chaotic S-boxes based on time-delay chaotic system," *Nonlinear Dyn.*, vol. 74, no. 3, pp. 551–557, Nov. 2013.
[23] F. Özkaynak, V. Çelik, and A. B. Özer, "A new S-box construction method based on the fractional-order chaotic chen system," *Signal, Image Video Process.*, vol. 11, no. 4, pp. 659–664, May 2017.
[24] F. Djimasra, J. D. D. Nkapkop, N. Tsafack, J. Kengne, J. Y. Effa, A. Boukabou, and L. Bitjoka, "Robust cryptosystem using a new hyperchaotic oscillator with stricking dynamic properties," *Multimedia Tools Appl.*, to be published, doi: 10.1007/s11042-021-10734-1.
[25] S. Vaidyanathan, V.-T. Pham, and C. K. Volos, "A 5-D hyperchaotic Rikitake dynamo system with hidden attractors," *Eur. Phys. J. Special Topics*, vol. 224, no. 8, pp. 1575–1592, Jul. 2015.
[26] V. I. Arnold and A. Avez, *Mathematical Methods of Classical Mechanics*. New York, NY, USA: W. A. Benjamin, 1968.
[27] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 7, pp. 2943–2959, Jul. 2012.
[28] E. Avaroğlu, "Pseudorandom number generator based on Arnold cat map and statistical analysis," *TURKISH J. Electr. Eng. Comput. Sci.*, vol. 25, pp. 633–643, 2017.
[29] R. J. Mstafa, Y. M. Younis, H. I. Hussein, and M. Atto, "A new video steganography scheme based on Shi-Tomasi corner detector," *IEEE Access*, vol. 8, pp. 161825–161837, 2020.
[30] F. Musanna and S. Kumar, "A novel fractional order chaos-based image encryption using Fisher Yates algorithm and 3-D cat map," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 14867–14895, Jun. 2019.
[31] S. H. Soleymani, A. H. Taherinia, and A. H. Mohajerzadeh, "WACA: A new blind robust watermarking method based on Arnold cat map and amplified pseudo-noise strings with weak correlation," *Multimedia Tools Appl.*, vol. 78, no. 14, pp. 19163–19179, Jul. 2019.
[32] O. B. Chanu and A. Neelima, "A (k, n) multi-secret image sharing scheme based on Chinese remainder theorem and Arnold cat map," *J. Electron. Imag.*, vol. 30, no. 2, Mar. 2021, Art. no. 023004.
[33] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Amsterdam, The Netherlands: Elsevier, 2009.

[34] 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.
[35] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, Santa Barbara, CA, USA, Aug. 1986, pp. 523–534.
[36] C. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," *J. Cryptol.*, vol. 3, no. 1, pp. 27–41, Jan. 1990.
[37] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.
[38] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT'93*. Lofthus, Norway: Springer, 1994.
[39] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and s8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.
[40] N. Sanam, A. Ali, T. Shah, and G. Farooq, "Non-associative algebra redesigning block cipher with color image encryption," *Comput., Mater. Continua*, vol. 67, no. 1, pp. 1–21, 2021.
[41] A. Razaq, Iqra, M. Ahmad, M. A. Yousaf, and S. Masood, "A novel finite rings based algebraic scheme of evolving secure S-boxes for images encryption," *Multimedia Tools Appl.*, vol. 80, no. 13, pp. 20191–20215, May 2021.
[42] W. Gao, B. Idrees, S. Zafar, and T. Rashid, "Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(2^8))," *IEEE Access*, vol. 8, pp. 136736–136749, 2020.
[43] 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.
[44] 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.
[45] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 118–131, Mar. 2020.
[46] 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.
[47] A. A. Abd 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, pp. 1–16, Dec. 2020.
[48] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dyn.*, vol. 100, no. 1, pp. 699–711, Mar. 2020.
[49] H. S. Alhadawi, D. Lambić, M. F. Zolkipli, and M. Ahmad, "Globalized firefly algorithm and chaos for designing substitution box," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102671.
[50] Z. Jiang and Q. Ding, "Construction of an S-box based on chaotic and bent functions," *Symmetry*, vol. 13, no. 4, p. 671, Apr. 2021.
[51] N. Siddiqui, A. Naseer, and M. Ehatisham-ul-Haq, "A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve," *Wireless Pers. Commun.*, vol. 116, no. 4, pp. 3015–3030, Feb. 2021.
[52] J. Wang, Y. Zhu, C. Zhou, and Z. Qi, "Construction method and performance analysis of chaotic S-box based on a memorable simulated annealing algorithm," *Symmetry*, vol. 12, no. 12, p. 2115, Dec. 2020.
[53] Z. B. Faheem, A. Ali, M. A. Khan, M. E. Ul-Haq, and W. Ahmad, "Highly dispersive substitution box (S-box) design using chaos," *ETRI J.*, vol. 42, no. 4, pp. 619–632, Aug. 2020.