Article

Evolving Dynamic S-Boxes Using Fractional-Order Hopfield Neural Network Based Scheme

Musheer Ahmad 1, * and Eesa Al-Solami 2

1 Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
2 Department of Information Security, University of Jeddah, Jeddah 21493, Saudi Arabia; eaalsulami@uj.edu.sa
* Correspondence: mahmad9@jmi.ac.in or musheer.cse@gmail.com; Tel.: +91-112-698-0281

Received: 30 May 2020; Accepted: 27 June 2020; Published: 28 June 2020

Abstract: Static substitution-boxes in fixed structured block ciphers may make the system vulnerable to cryptanalysis. However, key-dependent dynamic substitution-boxes (S-boxes) assume to improve the security and robustness of the whole cryptosystem. This paper proposes to present the construction of key-dependent dynamic S-boxes having high nonlinearity. The proposed scheme involves the evolution of initially generated S-box for improved nonlinearity based on the fractional-order time-delayed Hopfield neural network. The cryptographic performance of the evolved S-box is assessed by using standard security parameters, including nonlinearity, strict avalanche criterion, bits independence criterion, differential uniformity, linear approximation probability, etc. The proposed scheme is able to evolve an S-box having mean nonlinearity of 111.25, strict avalanche criteria value of 0.5007, and differential uniformity of 10. The performance assessments demonstrate that the proposed scheme and S-box have excellent features, and are thus capable of offering high nonlinearity in the cryptosystem. The comparison analysis further confirms the improved security features of anticipated scheme and S-box, as compared to many existing chaos-based and other S-boxes.

Keywords: dynamic S-box; block cryptosystem; fractional Hopfield neural network; security

1. Introduction

With the recent advancements in the field of wired/wireless network communication and electronic sharing of confidential data, the need for information security within the organization has undergone major changes. There is heavy reliance on electronic transfer of confidential data in daily life. Examples include different wallets, ecommerce websites purchases use our debit card info, internet banking and emails, etc. Network security is required to protect data while in transit. Cryptography provides the secure exchange of information between two communicating parties [1]. In cryptography, the plain message is converted to cipher text prior to its being transferred over the communication network, so that the observers or the attackers cannot interpret the original information. Thus, in order to successfully encrypt the message, we need to form a secure cipher from the plain text. To form a secure cipher confusion and diffusion are two essential properties needed, as identified by Claude Shannon. In confusion, each bit of the cipher text depends upon several parts of the key hiding the relationship between the two, therefore making it hard to find the key even if someone has a long plain text. In diffusion, the output bits depend upon the input bits in a complex way: If we change a single bit in the plain text, then at least half of the bits in the output cipher text should vary, and, similarly, if we change one of the bits in the cipher text, then more than half of the bits in the input plain text should change. Therefore, this makes the relationship between the plain text and the cipher text complex [2–4].

Modern cryptographic applications extensively make use of block encryption algorithms. Strong block encryption algorithms can be designed with the help of substitution-boxes (S-boxes).
In cryptographic systems, the encryption process relies on the nonlinear mapping of plain data to the secure encrypted data. The nonlinear transformation of data is facilitated by the application of the substitution process embedded in the cipher [5,6]. S-box is the only nonlinear component for many block encryption algorithms like IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), and AES (Advanced Encryption Standard). S-boxes are responsible for creating confusion in data during the encryption process; due to this property of the S-box, it is the essential component of numerous block ciphers. For this reason, the cryptanalyst generally targets the S-box component of the block encryption algorithm; hence, the S-box construction methods have received significant importance and are an active area of research [7–10].

Basically, an $8 \times 8$ sized substitution-box indicates that the S-box is having 8 input bits, and 8 output bits can be viewed as a transformation $S: \{0, 1\}^8 \to \{0, 1\}^8$, i.e., it is a one-to-one mapping wherein each 8-bit input is uniquely mapped to a distinct 8-bit output. Therefore, the S-boxes can also be viewed as multi-input and multi-output Boolean functions. Thus, an $8 \times 8$ S-box inherently comprises of eight candidate Boolean functions. Each function takes 8-bit input and yields 1-bit as output; thereby, all eight Boolean functions collectively give output bits-streams of size 8-bit. The block ciphers make use of two types of S-boxes, namely the static and dynamic S-boxes [11]. The former remains unchanged during every operation of a block cipher, as it is independent to the cipher’s secret key. However, the dynamic S-boxes may be changed due to change in one or more secret key components. Thus, the dynamic S-boxes are highly key-dependent and make the ciphers stronger and more robust against different cryptanalysis, compared to the ciphers, which are based on static S-boxes. As a result, the secure dynamic S-boxes have a dominant part to decide the forte of block cryptosystems. The security features of S-boxes are of vast significance for the security of cryptosystems [12–14]. Henceforth, the progress of dynamic, potent, and robust S-boxes is of supreme impact for researchers aspiring to develop strong modern cryptosystems.

Dynamical systems have various applications in numerous disciplines, including cryptology, meteorology, physics, and engineering. They deal with analyses, design, and performance assessment of continuous or discrete nonlinear systems that are extremely subtle to initial conditions. The deterministic nonlinear systems which possess good sensitivity to initial conditions are said to exhibit chaotic behavior [15,16]. If this initial information is not available, the system appears pseudo-random to the observer. The designing of dynamical chaotic systems-based schemes for network security has been a growing area of research in recent years. In chaos-based cryptography, the objectives of a cryptographic system are to obscure information present in the plain text in order to secure the encrypted data. The integral part of creating the confusion is the inception of pseudo-randomness in data at the output. Many block ciphers have been proposed during the last few decades; S-boxes are one of the essential components of block cryptosystems. There are many other approaches, as well, to bring about uncertainty, but dynamical systems have developed to be one of the lucrative choices for creating confusion, generating mix-up, and bringing about nonlinear changes in the data. In recent times, various S-box construction methods have been proposed based on different forms of dynamical models like discrete, continuous, fractional-order, time-delayed, etc. Discrete systems have been used in most of the studies, to avoid the numerical deterioration that may occur in the case of continuous systems. Previously, quantization-based algorithms were used for the construction of S-boxes, using the integer-order continuous-time dynamical systems. More complex systems were used to increase the performance of the S-box component.

Over the past decade, the dynamical behavior of continuous chaotic systems, multi-scroll attractors, and hyperchaotic systems has been intensively studied for engineering and other applications [17]. It has been found out that integer-order nonlinear systems do not show sensitive dependence to initial conditions if the dimension of system is smaller than three [18]. However, in case of fractional-order nonlinear systems, a complicated dynamical behavior is observed even for the system whose dimension is smaller than three. The set of fractional-order dynamical systems is the superset of integer-order systems. Notably, more complicated dynamics and high sensitivity to initial conditions is
observed in fractional-order dynamical systems compared to integer-order systems [19]. Dynamics of fractional-order systems are found to be more complex because of their high nonlinearity and non-local character. As a result, the fractional-order systems have been employed in secure communication due to this soothing property. In addition, the incorporation of a time delay in fractional-order systems can further increase the complexity, unpredictability, pseudo-randomness, etc., and can contribute to make strong security primitives [20,21]. Time-delayed systems are applied in a large variety of cases, in many scientific fields, such as feedback loops, artificial neural network, control systems, and application of communications [22].

There exist many proposals for S-box construction where the dynamics of integer-order continuous systems (having dimension three or more) are applied. In Reference [23], it was shown that a good S-box can be obtained by using continuous chaotic 3D Lorenz system. In Reference [24], Khan et al. made use of two 3D continuous chaotic systems, namely the Lorenz and Rössler systems, to generate the candidate values of an 8 × 8 substitution-box. Meanwhile, Khan et al. gave a procedure wherein a 3D fractional Rössler chaotic system was applied to synthesis 8 × 8 S-boxes [25]. In Reference [26], the authors constructed an S-box, using a method based on the 3D four-wing autonomous chaotic system. In Reference [27], a continuous six-dimensional hyperchaotic system was explored to generate the initial S-boxes for an Artificial Bee Colony (ABC)-based optimization process which resulted in an optimized S-box. A new S-box design was proposed in Reference [28] which is honorable. The authors’ design was aided with rich dynamic features of a new scaled Zhongtang chaotic system. Islam et al. gave an S-box generation method which was based on a 4D hyperchaotic system in which two pseudo-random 8-bit sequences were obtained to yield an S-box on two-position swapping [29]. Solami et al. [30] designed a random heuristic search method to generate efficient bijective S-boxes by using 5D hyperchaotic system. Wang et al. [31] used a new three-dimensional continuous chaotic map with infinite equilibrium points to design an S-box, but its nonlinearity was also not good enough. Liu et al. [32] proposed employing spatiotemporal chaos to generate S-boxes. They used the non-adjacent coupled map lattices and Arnold’s cat map to extract the spatiotemporal chaotic behavior of the system. However, there exists only one proposal by Özkanak where the time-delayed models of 1D chaotic Ikeda, sine map, and Logistic are investigated to frame a simple scheme of yielding S-boxes [33], showing satisfactory performances. Similarly, there are only two research works which investigate the fractional-order systems for an S-box design. The first one was given by Özkanak in Reference [34], which investigated a simple approach of constructing S-boxes by using the 3D fractional Chen system. The second one was suggested by Khan et al. [35], who explored the features of a fractional-order 3D chaotic Rössler system to construct an 8 × 8 S-box. To date, no S-box method has been investigated based on the two-state continuous dynamical system which is of fractional-order and time-delayed as well. The two can also be marked as components of secret key to complicate the work of possible cryptanalysis. The orders of fractional derivatives and amount of time delay extend the possible key space of the security system. In this paper, a new S-box evolution scheme is proposed, using the dynamics of the fractional-order time-delayed two-state Hopfield neural network system. It has been shown that time delay plays a vital role in increasing the nonlinearity of the S-box.

The remaining portion of the paper is maintained as follows. The time-delay fractional Hopfield neural network is discussed in Section 2. Section 3 provides the proposed scheme of initial S-box generation and its evolution for high nonlinearity, using the selected Hopfield system. Section 4 is developed to report the security performance of the proposed S-box under some standard properties, followed by its analyses and comparison with contemporary S-box proposals on dynamical systems. Lastly, Section 5 concludes the research findings of this paper.

2. Fractional-Order Hopfield Neural Network

The two-state time-delayed fractional Hopfield neural network is defined as follows [19].

\[
D^\alpha x(t) = A_1 x(t) + B_1 f(x(t)) + C_1 f(y(t)) + D_1 f(x(t - \tau)) + E_1 f(y(t - \tau)) + I_1
\]
\[ D^\alpha y(t) = A_2 y(t) + B_2 f(x(t)) + C_2 f(y(t)) + D_2 f(x(t - \tau)) + E_2 f(y(t - \tau)) + I_2 \]

where \( x(t) \) and \( y(t) \) represent the states of the two neurons at time instance, \( t \); 0 < \( p \) and \( q < 1 \) are the derivative orders; \( \tau > 0 \) denotes the delay introduced in time; \( A, B, C, D, E, \) and \( I \) are the associated coefficients corresponding to each state; and \( f(x) \) is the piecewise-linear (PWL) function given as \( f(x) = 0.5 \times (|x + 1| - |x - 1|) \). We followed the procedure as per Grunwald–Letnikov (GL) definition, mentioned in Sections 2.3 and 2.9 in Reference [36], to solve the fractional-order derivative equations of the Hopfield system. The numerical solution of the above two-state time-delayed fractional Hopfield neural network is as follows:

\[
\begin{align*}
x(t_k) &= h^p(A_1 x(t_{k-1}) + B_1 f(x(t_{k-1}))) + C_1 f(y(t_{k-1})) + D_1 f(x(t_k - \tau) + E_1 f(y(t_k - \tau)) + I_1) - \sum_{j=0}^{k} c^{(p)}_j x(t_{k-j}) \\
y(t_k) &= h^p(A_2 y(t_{k-1}) + B_2 f(x(t_{k-1}))) + C_2 f(y(t_{k-1})) + D_2 f(x(t_k - \tau) + E_2 f(y(t_k - \tau)) + I_2) - \sum_{j=0}^{k} c^{(q)}_j y(t_{k-j})
\end{align*}
\]

where \( h \) is the time step, and
\[
\begin{align*}
c^{(p)}_j &= (1 - \frac{1+q}{p})^{j-1} c^{(p)}_0 = 1; \\
c^{(q)}_j &= (1 - \frac{1+q}{q})^{j-1} c^{(q)}_0 = 1;
\end{align*}
\]

Now the transmission delay in time terms are computed though the linear interpolation scheme, expression are as follows (assuming \( \tau > h \)).

\[
\begin{align*}
x(t_k - \tau) &= x(t_k - d) + \left( \frac{t_k - \tau - t_k - d}{t_k - d + 1 - t_k - d} \right) (x(t_k - d + 1)) - x(t_k - d) \\
y(t_k - \tau) &= y(t_k - d) + \left( \frac{t_k - \tau - t_k - d}{t_k - d + 1 - t_k - d} \right) (y(t_k - d + 1)) - y(t_k - d)
\end{align*}
\]

where \( d = \text{ceil}(\tau/h) \) when \( d \leq j \leq n + 1 \), and \( x(t_k - \tau) = x_0 \) for \( 0 \leq j < d \). After solving the system for pre-specified number of iterations, we get two sequences.

3. Proposed S-Box Construction Scheme

The two forms of the time delayed fractional Hopfield neural network with different derivative orders and time delays are identified as System (1) and System (2), given below. The coefficients for the two forms are set at \( A_1 = -0.25, A_2 = 0.2, B_1 = -0.05, B_2 = 0.02, C_1 = 0.01, C_2 = -0.01, D_1 = -0.01, D_2 = 0.02, E_1 = 0.02, E_2 = 0.01, I_1 = -0.1, \) and \( I_2 = 0.4 \).

**System (1):**

\[
\begin{align*}
D^\alpha x_1(t) &= -0.25x_1(t) - 0.05f(x_1(t)) + 0.01f(x_2(t)) - 0.01f(x_1(t - \tau_1)) + 0.02f(x_2(t - \tau_1)) - 0.1 \\
D^\alpha x_2(t) &= -0.2x_2(t) + 0.02f(x_1(t)) - 0.01f(x_2(t)) + 0.02f(x_1(t - \tau_1)) + 0.01f(x_2(t - \tau_1)) + 0.4 \\
\end{align*}
\]

(1)

**System (2)**

\[
\begin{align*}
D^\alpha y_1(t) &= -0.25y_1(t) - 0.05f(y_1(t)) + 0.01f(y_2(t)) - 0.01f(y_1(t - \tau_2)) + 0.02f(y_2(t - \tau_2)) - 0.1 \\
D^\alpha y_2(t) &= -0.2y_2(t) + 0.02f(y_1(t)) - 0.01f(y_2(t)) + 0.02f(y_1(t - \tau_2)) + 0.01f(y_2(t - \tau_2)) + 0.4 \\
\end{align*}
\]

(2)

where \( x_1(0) \neq y_1(0) \), and/or \( x_2(0) \neq y_2(0) \), and/or \( p_1 \neq p_2 \), and/or \( q_1 \neq q_2 \), and/or \( \tau_1 \neq \tau_2 \). The two systems are considered as to extend the possible key space of the proposed method. System (1) is utilized to generate the initial configuration of the S-box. However, System (2) is applied to improvise the nonlinearity strength of the initial S-box. The proposed scheme for the highly nonlinear S-box construction is as follows.

**Step I. Initialization of S-Box**

1. Take initial values of System (1) as \( x_1(0), x_2(0), p_1, q_1, \tau_1 \), and empty array \( S \);
2. Iterate System (1) to obtain $x_1$ and $x_2$;
3. Extract $w_1$, $w_2$ from current $x_1$ and $x_2$ as
   \[ w_j = \lfloor x_j \times 10^{15} \rfloor \mod (256) \quad \text{for } j = 1, 2; \]
4. Save first occurrence of $w_1$ and then $w_2$ in array $S$;
5. Repeat from Step 2 until all distinct 256 elements are recorded in array $S$.

**Step II.** Evolving S-Box Scheme

1. Take initial values of System (2) as $y_1(0), y_2(0), p_2, q_2, \tau_2, N, \text{itr}_{-}\text{max}, \text{step}_x, \text{step}_y, \text{prime}_1, \text{prime}_2$, and $\Delta \tau$;
2. Iterate System (2) for $\text{itr}_{-}\text{max}$ times, to get two arrays, $Y_1$ and $Y_2$;
3. Extract $U_1(i), U_2(i)$ from current $Y_1(i)$ and $Y_2(i)$ as
   \[ U_j(i) = \lfloor Y_j(i) \times 10^{5} \rfloor \mod (256) \quad \text{for } j = 1, 2, \text{and } i = 1, 2, \ldots, \text{itr}_{-}\text{max}; \]
4. Append arrays $U_1$ and $U_2$ to get a single array as
   \[ Q[1 \text{ to } \text{itr}_{-}\text{max}] = U_1; Q[\text{itr}_{-}\text{max} + 1 \text{ to } 2 \times \text{itr}_{-}\text{max}] = U_2; \]
5. Compute $\text{rating}_1 = \text{nonlinearity}(S)$;
6. For $k = 1$ to $2 \times \text{itr}_{-}\text{max}$
   \[ \text{step}_x = [\text{step}_x + (k \times \text{prime}_1) \mod (32)] \mod (16) \]
   \[ \text{step}_y = [\text{step}_y + (k \times \text{prime}_2) \mod (32)] \mod (16) \]
   \[ \text{spos} = 16 \times \text{step}_x + \text{step}_y \]
   \[ \text{val} = S(\text{spos}) \text{ XOR } Q(k) \]
   find index $m$ such that $S(m) = \text{val}$
   set $S_1 = S$
   $\text{Swap}(S_1(m), S_1(\text{spos}))$
   $\text{rating}_2 = \text{nonlinearity}(S_1)$
   if ($\text{rating}_2 >= \text{rating}_1$)
     $S = S_1$
     $\text{rating}_1 = \text{rating}_2$
   endif
   endfor
7. Increment delay as: $\tau_2 = \tau_2 + \Delta \tau$;
8. Repeat Step 2 to Step 7 for $N$ number of increments in $\tau_2$.

The proposed scheme is also illustrated through the flowchart shown in Figure 1.
4. Performance Results and Analyses

This section deals with the performance assessment, analyses, and the proposed S-box’s comparison with some state-of-the-art S-box schemes which are based on dynamical systems. Without loss of generality, the settings for simulation of proposed scheme are provided in Table 1. The S-box obtained with these settings, using the proposed scheme, is listed in Table 2. The secret key $K$ of proposed security scheme includes the components such as $K = (x_1(0), x_2(0), p_1, q_1, \tau_1, y_1(0), y_2(0), p_2, q_2, \tau_2, N, i_{tr\_max}, step_x, step_y, prime_1, prime_2, and \Delta \tau)$. All floating-point computations are performed as per the IEEE 754 standard. Thus, the possible key space is more than $2^{500}$. This enormously large key space is sufficient enough to withstand the brute-force cryptanalysis. The most popular and standard cryptographic properties of S-boxes are as follows: high nonlinearity, low differential uniformity, the strict avalanche criterion equals to 0.5, the satisfaction of bits independence criterion for high bits independence criterion (BIC) nonlinearity and BIC–strict avalanche criterion (SAC) close to 0.5, and low linear approximation probability. A majority of the existing S-boxes schemes have scrutinized their constructed S-boxes mainly against these security properties [37–41]. The following subsections analyzed the proposed S-boxes under the mentioned properties.

Figure 1. Flowchart of proposed substitution-box (S-box) construction scheme.
Table 1. Experimental settings for simulation.

| System (1) | System (2) |
|------------|------------|
| parameter  | value      | parameter | value      |
| $x_1(0)$   | 2.1        | $y_1(0)$  | 2.3        |
| $x_2(0)$   | 3.7        | $y_2(0)$  | 8.9        |
| $p_1$      | 0.12       | $p_2$     | 0.12       |
| $q_1$      | 0.3        | $q_2$     | 0.67       |
| $\tau_1$  | 0.1        | $\tau_2$  | 0.33       |
| $h$        | 0.005      | $\Delta\tau$ | 0.05 |
| $N$        | 200        | $itr_{\text{max}}$ | 2000 |
| $\text{step}_x$ | 57           | $\text{step}_y$ | 31            |
| $\text{prime}_1$     | 23           | $\text{prime}_2$ | 37            |

Table 2. Proposed 8 × 8 substitution-box.

| S-box entries |
|---------------|
| 127 180 219 232 97 108 195 39 |
| 191 163 134 21 200 66 23 202 |
| 98 161 14 205 42 12 102 68   |
| 4 26 70 137 41 199 171 142   |
| 168 133 30 103 190 253 250 92 |
| 105 83 76 187 69 238 235 246 |
| 135 252 173 179 176 220 99 244 |
| 194 177 87 82 84 37 170 204 |
| 57 215 70 79 75 186 91 131   |
| 224 251 96 40 164 207 213 62 |
| 206 19 159 67 88 63 222 60   |
| 38 221 72 100 129 209 228 157 |
| 0 106 192 166 90 65 153 125   |
| 0 106 192 166 90 65 153 125   |
| 178 121 141 185 226 197 56 43 |
| 229 188 47 216 255 59 234 124 |
| 24 237 242 36 236 1 211 74    |

4.1. Nonlinearity

The nonlinearity measure of a Boolean function, $f$, is computed by knowing the least distance of $f$ to the set of all affine functions [42]. Thus, the component Boolean functions of the S-box should have standing nonlinearities scores. The nonlinearity $NL(f)$ of any Boolean function $f$ is computed as follows:

$$NL(f) = 128 \left( 1 - 2^{-8} \max_{z \in \{0,1\}^8} |S_f(z)| \right)$$

where $S_f(z)$ is the Walsh–Hadamard transform of Boolean function, $f$. A Boolean function is deemed frail if it tends to have poor nonlinearity. The higher nonlinearity of balanced Boolean functions is considered one of the prominent measures responsible for providing better robustness to any type of linear attack [43]. We find that the nonlinearity scores of the proposed S-box are 110, 110, 112, 112, 112, 110, 112, and 112, which include the minimum $NL$ of 110 and an average score of 111.25. Thus, it is very evident that the proposed S-box possesses high nonlinearity performance. The reason being, the proposed scheme made to evolve the S-box based on the nonlinearity rating.

4.2. Strict Avalanche Criterion

The strict avalanche criterion was described by Tavares and Webster, and it gets its base on the completeness effect’s notion and the avalanche [44,45]. This criterion measures that by making a single
change in input bits, i.e., how many output bits get altered. The SAC is assumed to be satisfied when all the output bits are changed with a likelihood of 0.5, when only one input bit is flipped. Following the procedure given by Webster and Tavares, we get the SAC matrix shown in Table 3. The average of this matrix, which is 0.5007, indicates the SAC value. We can see that this score is close to ideal value of 0.5 with infinitesimal offset of only 0.0007. Thus, the proposed S-box has good avalanche when any of the single input bit is altered and decently satisfies the SAC criterion.

Table 3. Dependency matrix for strict avalanche criterion (SAC).

|       | 0.5312 | 0.4531 | 0.5 | 0.5625 | 0.5625 | 0.5 | 0.5312 | 0.4843 |
|-------|--------|--------|-----|--------|--------|-----|--------|--------|
| 0.5937| 0.4375 | 0.5156 | 0.5312| 0.4531 | 0.5   | 0.4843| 0.5468 |
| 0.4687| 0.4687 | 0.5468 | 0.5156| 0.5312 | 0.4843| 0.5  | 0.4687 |
| 0.4531| 0.4843 | 0.5   | 0.5312| 0.4531 | 0.5   | 0.4843| 0.5312 |
| 0.5312| 0.5312 | 0.4843| 0.5312| 0.4375 | 0.5   | 0.5468| 0.4843 |
| 0.5468| 0.4687 | 0.5   | 0.5312| 0.4375 | 0.4687| 0.5156| 0.4531 |
| 0.5156| 0.4062 | 0.5781| 0.5468| 0.4843 | 0.5   | 0.5  | 0.5    |
| 0.4843| 0.4843 | 0.5   | 0.4062| 0.5312 | 0.4843| 0.5781| 0.4687 |

4.3. Bits Independence Criterion

The input bits which remain unchanged are explored under the bits independence criterion. The revamping of the independent performance of pair-wise variables of avalanche vectors and unaltered input bits is the asset of this measure. Under this criterion, the avalanche component Boolean functions pairs should be independent to each. It is an effective criterion in symmetric cryptosystem, because by augmenting independence between bits, the recognition and prediction of patterns of the system is not possible [30,46]. Accordingly, the Boolean functions $f_i \oplus f_j \ (i \neq j)$ should behave well for nonlinearity and SAC properties both. The BIC performance of the proposed S-box for nonlinearity is shown in Table 4 and for SAC is provided in Table 5. The BIC-nonlinearity (NL) score is 102.57, and BIC–SAC is 0.5034, which indicates the acceptable performance of our S-box under BIC property.

Table 4. Bits independence criterion (BIC) results for nonlinearity.

|     | 0  | 104| 100| 104| 100| 98| 102| 98  |
|-----|----|----|----|----|----|---|----|-----|
| 0   | 104| 100| 104| 100| 98 | 102| 98 |    |
| 104 | 0  | 100| 104| 106| 108| 104| 104|    |
| 100 | 100| 0  | 104| 104| 108| 104| 98 |    |
| 104 | 104| 104| 0  | 104| 100| 104| 104|    |
| 100 | 106| 104| 104| 0  | 106| 102| 106|    |
| 98  | 108| 108| 100| 106| 0  | 96 | 102|    |
| 102 | 104| 104| 104| 102| 96 | 0  | 98 |    |
| 98  | 104| 98 | 104| 106| 102| 98 | 0  |    |

Table 5. BIC results for SAC.

|       | 0  | 0.5175| 0.5136| 0.5078| 0.5039| 0.5039| 0.5 | 0.5136 |
|-------|----|-------|-------|-------|-------|-------|----|-------|
| 0.5175| 0  | 0.5234| 0.5214| 0.5097| 0.4843| 0.5156| 0.4882| 0.5097 |
| 0.5136| 0.5234| 0   | 0.5214| 0.5097| 0.4843| 0.5156| 0.4882| 0.5097 |
| 0.5078| 0.5214| 0.5097| 0    | 0.4882| 0.4902| 0.4921| 0.4863| 0.5039 |
| 0.5039| 0.4843| 0.5039| 0.4882| 0    | 0.5195| 0.5117| 0.5214| 0.5039 |
| 0.5039| 0.5156| 0.4902| 0.4921| 0.5195| 0    | 0.5078| 0.5117| 0.5117 |
| 0   | 0.4882| 0.4863| 0.5117| 0.5078| 0    | 0    | 0.4726| 0    |
| 0.5136| 0.5097| 0.4726| 0.5039| 0.5214| 0.5117| 0.4726| 0    |     |

4.4. Differential Uniformity

The differential uniformity measures the resistivity of an S-Box against the differential cryptanalysis. The attack procedure of cryptanalysis was given by Biham and Shamir; it is related with developing imbalance on the input/output dissemination to assault block ciphers and S-boxes [47]. Confrontation
to this cryptanalysis can be consummate if the Exclusive-OR of each output has identical uniformity 
with the EX-OR value of each input. If an S-box is uniform in input/output distribution, then it is said 
to be resistant. It is preferred that the largest value of differential uniformity (DU) in EX-OR table 
should be as small as possible [48]. The differential uniformity is measured as follows:

$$\delta_S = \max_{\Delta x \neq 0, \Delta y} \left( \# \{ x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y \} \right)$$

where set X holds all probable input values, and the cardinality of its elements is 256 for 8x8 S-box. 
The largest value of EX-OR (differential distribution) table for an S-box should be as small enough 
to resist the differential cryptanalysis. The differential distribution matrix for the proposed S-box 
is obtained and is available as Table 6. The highest value of this matrix, i.e., 10, is the differential 
uniformity for our S-box, and such maximum values are only 7 out of the 256 values in the matrix, 
thus indicating the good differential uniformity and robustness of the proposed S-box.

### Table 6. Differential matrix for differential uniformity (DU).

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

4.5. Linear Approximation Probability

The method of linear approximation probability (LAP) is helpful in calculating the imbalance 
of an incident. The largest value of imbalance of an event is measured with the help of the analysis 
introduced by Matsui [49]. There must be no difference between output and input bits uniformity. 
Each of the input bits with its results in output bits is examined individually. If all the input elements 
are 256 for the 8 x 8 S-box, the class of all possible inputs is d, and the masks applied on the equality of 
output and input bits are respectively mx and my, then maximum linear approximation is the maximum 
number of the same results and calculated as follows:

$$LAP(S) = \max_{m_x, m_y \neq 0} \left| \left\{ x \in X | x.m_x = y.m_y \right\} \right| \frac{256}{256} - 0.5$$

A lower value of this measure indicates that S-box is more capable to resist the linear cryptanalysis. 
The LAP score of proposed S-box is 0.14025.

4.6. Comparison

A performance comparison analysis is significant in finding the actual standing of the proposed 
S-box. Almost all S-box methods were dynamical systems of the following types: (1) high dimensional 
continuous integer-order systems, (2) time delay system, (3) fractional-order 3D systems, and some
other recent S-boxes are opted for the comparison. The performance scores for different security properties of all selected S-boxes are displayed in Table 7.

Table 7. Performance comparison of 8 × 8 S-boxes.

| S-box        | Nonlinearity | SAC   | BIC–SAC | BIC-NL | DU | LAP |
|--------------|--------------|-------|---------|--------|----|-----|
|              | min          | max   | mean    |        |    |     |
| Proposed     | 110          | 112   | 111.25  | 0.5007 | 0.5034 | 102.57 | 10 | 0.1403 |
| Reference [23] | 100          | 106   | 103.2   | 0.5048 | 0.5009 | 103.7  | 10 | 0.1328 |
| Reference [24] | 98           | 108   | 103    | 0.5012 | 0.4988 | 104.07 | 12 | 0.1328 |
| Reference [25] | 100          | 108   | 104.5   | 0.4978 | 0.5009 | 103.6  | 12 | 0.1406 |
| Reference [26] | 104          | 108   | 105.80  | 0.4976 | 0.5032 | 104.5  | 10 | 0.1250 |
| Reference [27] | 106          | 110   | 108    | 0.5073 | 0.502  | 104    | 10 | 0.1523 |
| Reference [28] | 104          | 110   | 106    | 0.5039 | 0.5058 | 103.38 | 10 | 0.1406 |
| Reference [29] | 102          | 108   | 106    | 0.5002 | 0.5013 | 104.4  | 10 | 0.1484 |
| Reference [30] | 106          | 110   | 108.5  | 0.5017 | 0.5026 | 104    | 10 | 0.1328 |
| Reference [33] | 103          | 109   | 105.1  | 0.5061 | 0.4982 | 103.6  | 10 | 0.1563 |
| Reference [34] | 100          | 108   | 104.7  | 0.4982 | 0.4942 | 103.1  | 10 | 0.1406 |
| Reference [41] | 102          | 108   | 105.25 | 0.5037 | 0.4994 | 102.6  | 10 | 0.1328 |
| Reference [42] | 84           | 106   | 100    | 0.4812 | 0.4967 | 101.93 | 16 | 0.1796 |
| Reference [50] | 104          | 108   | 106.75 | 0.4076 | 0.5022 | 103.57 | 10 | 0.1328 |
| Reference [51] | 106          | 108   | 106.7  | 0.4941 | 0.4957 | 103.5  | 10 | 0.125  |
| Reference [52] | 106          | 110   | 107    | 0.5014 | 0.5016 | 104.2  | 10 | 0.1484 |
| Reference [53] | 106          | 108   | 107.5  | 0.4943 | 0.4982 | 104.36 | 10 | 0.125  |
| Reference [54] | 96           | 106   | 103.25 | 0.5151 | 0.4864 | 103.07 | 54 | 0.1562 |
| Reference [55] | 104          | 108   | 106.75 | 0.5031 | 0.5074 | 103.64 | 12 | 0.1484 |
| Reference [56] | 105          | 107   | 106    | 0.5066 | 0.5065 | 103    | 12 | 0.1445 |
| Reference [57] | 98           | 108   | 102.3  | 0.4836 | 0.4944 | 101.57 | 14 | 0.1679 |
| Reference [58] | 106          | 108   | 106.5  | 0.5009 | 0.5005 | 104.07 | 10 | 0.1328 |
| Reference [59] | 104          | 110   | 106.25 | 0.4990 | 0.5050 | 103.8  | 10 | 0.125  |
| Reference [60] | 106          | 108   | 106.5  | 0.5046 | 0.5023 | 104.14 | 10 | 0.1328 |
| Reference [61] | 94           | 108   | 103.5  | 0.5024 | 0.5009 | 103    | 10 | 0.1328 |
| Reference [62] | 96           | 108   | 102.25 | 0.5059 | 0.5050 | 103.5  | 12 | 0.125  |
| Reference [63] | 112          | 112   | 112    | 0.5058 | 0.502  | 112    | 4  | 0.0625 |
| Reference [64] | 112          | 112   | 112    | 0.5058 | 0.5046 | 112    | 4  | 0.0625 |

* Where, NL stands for nonlinearity.

The nonlinearity performance of the proposed S-box comes out to be outstanding, as all three statistics, namely the minimum (110), maximum (112), and average (111.25), are significantly higher than the S-boxes in Table 7. The same comparison is also shown graphically in Figure 2a. Thus, highly nonlinear S-boxes can be constructed by using the proposed novel scheme.

The proposed S-box was also found to show good SAC behavior, as our SAC value of 0.5007 is quite better than the scores of S-boxes constructed in References [23–28,30,33,34,41,42,50–60], as evident from Table 7 and Figure 2b. The proposed S-box satisfies the SAC criterion quite diligently as compared to other contemporary S-boxes.

The results of bits independence criterion show that the proposed S-box also exhibits acceptable BIC performance, as the BIC–SAC and BIC-nonlinearity scores are satisfactory, as shown in Figure 2c,d.

The differential uniformity of our S-box is only 10, which is less and better than S-boxes investigated in References [24,25,54–57], and it is comparable to other S-boxes in terms of robustness to differential cryptanalysis. The DU comparison is also shown graphically in Figure 2e.

A block cipher can withstand the linear cryptanalysis if the employed S-box is dynamic, highly nonlinear, and linear approximation probability is low. The LAP score of 0.14025 is obtained for the proposed S-box, which shows a satisfactory value. Moreover, this probability score is quite lower and
better than the LAP score of the S-boxes available in References [25,27–29,33,34,42,52,54–57]. The LAP comparison is also shown graphically in Figure 2f.

![Graphical comparison analyses of 8 × 8 S-boxes under (a) nonlinearity, (b) SAC, (c) BIC–SAC, (d) BIC-nonlinearity, (e) DU and (f) linear approximation probability (LAP).](image)

**Figure 2.** Graphical comparison analyses of 8 × 8 S-boxes under (a) nonlinearity, (b) SAC, (c) BIC–SAC, (d) BIC-nonlinearity, (e) DU and (f) linear approximation probability (LAP).

### 4.7. Time Analysis

The computation time is one of the essential features for any security application. In order to have an idea of time consumption of our proposed scheme, we calculated the time taken by the scheme to evolve an S-box. It was found that the scheme takes a very nominal amount of time, (on average) only 3.5459 s. This computational time is considerably nominal compared to many optimization-based evolution of S-boxes available in the literature, such as References [5,8,38,53].

### 4.8. S-Box Validation for Image Encryption Applications

In recent days, the strong S-boxes have been predominantly utilized for image encryption applications. It is prudent to validate the appropriateness of proposed S-box for such security application. Accordingly, we applied the S-box presented in this study, to encrypt the standard 8-bit encoded Baboon plain-image. The encryption involves the forward and reverse substitution using the proposed S-box. The results of encryption along with the distribution of pixels in the respective
images are shown in Figure 3. The obtained encrypted image shows high visual distortion and good encryption effect. To quantify the encryption performance exhibited by our S-box, we evaluated the statistical tests, such contrast, correlation, energy, and homogeneity, which are members of the Majority Logic Criteria (MLC) suite. The description and details of these tests are available in author’s previous studies [7,40,48]. The statistical scores of encryption performance under MLC analysis are listed in Table 8 and compared with encryption performances of S-boxes investigated in References [48,61]. The obtained results for MLC analysis validate the appropriateness of proposed S-box for image encryption applications.

![Figure 3](image-url)  
(a) (b)  
(c) (d)  
Figure 3. Results of image encryption using proposed S-box for Baboon image (a) plain-image, (b) histogram of plain-image, (c) encrypted image, and (d) histogram of encrypted image.

| Baboon Image      | Contrast | Correlation | Energy | Homogeneity |
|------------------|----------|-------------|--------|-------------|
| Plain-image      | 0.63265  | 0.7983      | 0.09438| 0.78209     |
| Encrypted image  | 10.4227  | 0.0064      | 0.01566| 0.39483     |
| Reference [48]   | 10.4291  | –0.0128     | 0.0157 | 0.3889      |
| Reference [61]   | 10.3986  | 0.0072      | 0.0158 | 0.4214      |

5. Conclusions

Highly nonlinear substitution-boxes provide good nonlinear transformation and confusion of input plaintext data to generate ciphertext data in block cryptosystems. Such S-boxes are also potent to offer great resistance to mitigate the linear and other types of attacks which may exploit the existence of linearity in the security system. Moreover, the key-dependent and dynamic S-boxes also tend to provide more strength to the cryptosystem. This paper has proposed a novel scheme of constructing dynamic and highly nonlinear S-boxes. Our scheme is based on the dynamics of two-state time-delayed fractional-order Hopfield neural network system. Firstly, the anticipated scheme generates an initial S-box which is made to evolve for high nonlinearity, using the heuristic. The proposed scheme and
constructed S-box possessed high cryptographic strength and large key space. It was found that the proposed scheme is able to evolve an S-box with nonlinearity of 111.25, strict avalanche criteria value of 0.5007, and differential uniformity of 10. The comparison analysis with some available dynamical-systems-based S-box methods and others validated the better performance of our S-box.

As future directions of the presented study, we can also check the effectiveness of proposed scheme in generating large-size \( n \times n \) S-boxes \((n > 8)\). The large-size S-boxes have better potential to offer resistance to several attacks than small-size S-boxes. The generation of large-size S-boxes is rarely investigated in the literature. Moreover, the evolution is initial S-box is based on only one criteria of nonlinearity. The evolution process can be executed to satisfy multiple S-box performance parameters.

Author Contributions: Conceptualization, M.A. and E.A.-S.; Writing-Original Draft Preparation, M.A. and E.A.-S. Both the authors contributed equally in all aspects. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References
1. Forouzan, B.A. Cryptography & Network Security; McGraw-Hill, Inc.: New York, NY, USA, 2007.
2. Faragallah, O.S. Efficient confusion–diffusion chaotic image cryptosystem using enhanced standard map. *Signal Image Video Process.* 2014, 9, 1917–1926. [CrossRef]
3. Ali, K.M.; Khan, M. A new construction of confusion component of block ciphers. *Multimed. Tools Appl.* 2019, 78, 32585–32604. [CrossRef]
4. Hayat, U.; Azam, N.A.; Asif, M. A method of generating \( 8 \times 8 \) substitution boxes based on elliptic curves. *Wired. Pers. Commun.* 2018, 101, 439–451. [CrossRef]
5. Alzaidi, A.A.; Ahmad, M.; Ahmed, H.S.; Al Solami, E. Sine-Cosine Optimization-Based Bijective Substitution-Boxes Construction Using Enhanced Dynamics of Chaotic Map. *Complexity* 2018, 2018, 1–16. [CrossRef]
6. Ahmad, M.; Chugh, H.; Goel, A.; Singla, P. A chaos based method for efficient cryptographic S-box design. In *International Symposium on Security in Computing and Communication*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 130–137.
7. Jamal, S.S.; Anees, A.; Ahmad, M.; Khan, M.F.; Hussain, I. Construction of Cryptographic S-Boxes Based on Mobius Transformation and Chaotic Tent-Sine System. *IEEE Access* 2019, 7, 173273–173285. [CrossRef]
8. Ahmad, M.; Mittal, N.; Garg, P.; Khan, M.M.; Mahtab, M. Efficient cryptographic substitution box design using travelling salesman problem and chaos. *Perspect. Sci.* 2016, 8, 465–468. [CrossRef]
9. Belazi, A.; Khan, M.; El-Latif, A.A.; Belgith, S. Efficient cryptosystem approaches: S-boxes and permutation substitution-based encryption. *Nonlinear Dyn.* 2016, 87, 337–361. [CrossRef]
10. Lambić, D. S-box design method based on improved one-dimensional discrete chaotic map. *J. Inf. Telecommun.* 2018, 2, 181–191. [CrossRef]
11. Ahmad, M.; Haleem, H.; Khan, P.M. A new chaotic substitution box design for block ciphers. In Proceedings of the 2014 International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 20–21 February 2014.
12. Ozkaynak, F. An Analysis and Generation Toolbox for Chaotic Substitution Boxes: A Case Study Based on Chaotic Labyrinth Rene Thomas System. *Iran. J. Sci. Technol. Trans. Electr. Eng.* 2019, 44, 89–98. [CrossRef]
13. Ahmad, M.; Malik, M. Design of chaotic neural network based method for cryptographic substitution box. In Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEETC), Chennai, India, 3–5 March 2016; pp. 864–868.
14. Razaq, A.; Ullah, A.; Waheed, A. A Novel Technique to Improve Nonlinearity of Substitution Box without Disturbing Its Mathematical Properties. *Wired. Pers. Commun.* 2019, 111, 1–15. [CrossRef]
15. Kotulski, Z.; Szczepański, J.; Górski, K.; Paszkiewicz, A.; Zugaj, A. Application of discrete chaotic dynamical systems in cryptography—Dec method. *Int. J. Bifurc. Chaos* 1999, 9, 1121–1135. [CrossRef]
16. Yu, W.; Cao, J. Cryptography based on delayed chaotic neural networks. *Phys. Lett. A* 2006, 356, 333–338. [CrossRef]
17. Garcia, M.; Ontañón-Garcia, L.; Campos, E.; Celikovsky, S.; Pimentel, L.J.O.G. Hyperchaotic encryption based on multi-scroll piecewise linear systems. *Appl. Math. Comput.* 2015, 270, 413–424.

18. Zhu, H.; Zhou, S.; Zhang, W. Chaos and synchronization of time-delayed fractional neuron network system. In *Proceedings of the 2008 the 9th International Conference for Young Computer Scientists*, Hunan, China, 18–21 November 2008; pp. 2937–2941.

19. Chen, L.; Chai, Y.; Wu, R.; Ma, T.; Zhai, H. Dynamic analysis of a class of fractional-order neural networks with delay. *Neurocomputing* 2013, 111, 190–194. [CrossRef]

20. Chen, L.; Qu, J.; Chai, Y.; Wu, R.; Qi, G. Synchronization of a Class of Fractional-Order Chaotic Neural Networks. *Entropy* 2013, 15, 3265–3276. [CrossRef]

21. Zhao, J.; Wang, S.; Chang, Y.; Li, X. A novel image encryption scheme based on an improper fractional-order chaotic system. *Nonlinear Dyn.* 2015, 80, 1721–1729. [CrossRef]

22. Banerjee, S. Synchronization of time-delayed systems with chaotic modulation and cryptography. *Chaos Solitons Fractals* 2009, 42, 745–750. [CrossRef]

23. Özkan, F.; Özer, A.B. A method for designing strong S-Boxes based on chaotic Lorenz system. *Phys. Lett. A* 2010, 374, 3733–3738. [CrossRef]

24. Khan, M.; Shah, T.; Mahmood, H.; Gondal, M.A. An efficient method for the construction of block cipher with multi-chaotic systems. *Nonlinear Dyn.* 2012, 71, 489–492. [CrossRef]

25. Khan, M.; Shah, T. An efficient construction of substitution box with fractional chaotic system. *Signal Image Video Process.* 2013, 9, 1335–1338. [CrossRef]

26. Liu, G.; Yang, W.; Liu, W.; Dai, Y. Designing S-boxes based on 3-D four-wing autonomous chaotic system. *Nonlinear Dyn.* 2015, 82, 1867–1877. [CrossRef]

27. Tian, Y.; Lu, Z. S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm. *J. Syst. Eng. Electron.* 2016, 27, 232–241.

28. Çavuşoğlu, Ü.; Zengin, A.; Pehlivan, I.; Kaçar, S. A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dyn.* 2016, 87, 1081–1094. [CrossRef]

29. Islam, F.U.; Liu, G. Designing S-Box Based on 4D-4Wing Hyperchaotic System. *3D Res.* 2017, 8, 9. [CrossRef]

30. Al Solami, E.; Ahmad, M.; Volos, C.; Doja, M.N.; Beg, M.M.S. A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-Boxes. *Entropy* 2018, 20, 525. [CrossRef]

31. Wang, X.; Akgül, A.; Cavusoglu, U.; Pham, V.-T.; Hoang, D.V.; Nguyen, X.Q. A Chaotic System with Infinite Equilibria and Its S-Box Constructing Application. *Appl. Sci.* 2018, 8, 2132. [CrossRef]

32. Liu, L.; Zhang, Y.; Wang, X. A Novel Method for Constructing the S-Box Based on Spatiotemporal Chaotic Dynamics. *Appl. Sci.* 2018, 8, 2650. [CrossRef]

33. Özkan, F.; Yavuz, S. Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dyn.* 2013, 74, 551–557. [CrossRef]

34. Ozkaynak, F.; Çelik, V.; Ozar, A.B. A new S-box construction method based on the fractional-order chaotic Chen system. *Signal Image Video Process.* 2016, 11, 659–664. [CrossRef]

35. Abd El-Latif, A.A.; Abd-El-Atty, B.; Venegas-Andraca, S.E. A novel image steganography technique based on quantum substitution boxes. *Opt. Laser Technol.* 2019, 116, 92–102. [CrossRef]

36. Petráš, I. Fractional-Order Nonlinear Systems: Modeling, Analysis and Simulation; Springer Science & Business Media: Berlin, Germany, 2011.

37. Azam, N.A.; Hayat, U.; Ullah, I. An Injective S-Box Design Scheme over an Ordered Isomorphic Elliptic Curve and Its Characterization. *Secur. Commun. Netw.* 2018, 2018, 1–9. [CrossRef]

38. Ahmad, M.; Doja, M.N.; Beg, M.M.S. ABC Optimization Based Construction of Strong Substitution-Boxes. *Wirel. Pers. Commun.* 2018, 101, 1715–1729. [CrossRef]

39. Yousaf, M.A.; Alolaiyan, H.; Ahmad, M.; Dilbar, M.; Razaq. A. Comparison of Pre and Post-Action of a Finite Abelian Group over Certain Nonlinear Schemes. *IEEE Access* 2020, 8, 39781–39792. [CrossRef]

40. Özkan, F. On the effect of chaotic system in performance characteristics of chaos based s-box designs. *Phys. A Stat. Mech. Appl.* 2020, 550, 124072. [CrossRef]

41. Khan, M.; Shah, T.; Batoool, S.I. Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Comput. Appl.* 2015, 27, 677–685. [CrossRef]

42. Khan, M.; Shah, T.; Batool, S.I. Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Comput. Appl.* 2015, 27, 677–685. [CrossRef]
43. Zhang, W.; Pasalic, E. Highly Nonlinear Balanced S-Boxes with Good Differential Properties. *IEEE Trans. Inf. Theory* **2014**, *60*, 7970–7979. [CrossRef]

44. Cusick, T.W.; Stanica, P. *Cryptographic Boolean Functions and Applications*; Elsevier: Amsterdam, The Netherlands, 2009.

45. Alzaidi, A.A.; Ahmad, M.; Doja, M.N.; Al Solami, E.; Beg, M.M.S. A New 1D Chaotic Map and $\beta$-Hill Climbing for Generating Substitution-Boxes. *IEEE Access* **2018**, *6*, 55405–55418. [CrossRef]

46. Adams, C.; Tavares, S. The structured design of cryptographically good s-boxes. *J. Cryptol.* **1990**, *3*, 27–41. [CrossRef]

47. Biham, E.; Shamir, A. Differential Cryptanalysis of DES-like Cryptosystems. In *Advances in Cryptology—EUROCRYPT ’93 Lecture Notes in Computer Science* 386–397; Springer: Berlin/Heidelberg, Germany, 1993.

48. Ye, T.; Zhimao, L. Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. *Nonlinear Dyn.* **2018**, *94*, 2115–2126. [CrossRef]

49. Matsui, M. Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology—EUROCRYPT ’93 Lecture Notes in Computer Science* 386–397; Springer: Berlin/Heidelberg, Germany, 1993.

50. Ye, T.; Zhimao, L. Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. *Nonlinear Dyn.* **2018**, *94*, 2115–2126. [CrossRef]

51. Ozkaynak, F. Construction of robust substitution boxes based on chaotic systems. *Neural Comput. Appl.* **2017**, *31*, 3317–3326. [CrossRef]

52. Ahmad, M.; Bhatia, D.; Hassan, Y. A Novel Ant Colony Optimization Based Scheme for Substitution Box Design. *Procedia Comput. Sci.* **2015**, *57*, 572–580. [CrossRef]

53. Ahmed, H.A.; Zolkipi, M.F.; Ahmad, M. A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. *Neural Comput. Appl.* **2018**, *31*, 7201–7210. [CrossRef]

54. Khan, M.; Asghar, Z. A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation. *Neural Comput. Appl.* **2016**, *29*, 993–999. [CrossRef]

55. Jamil, S.S.; Khan, M.U.; Shah, T. A Watermarking Technique with Chaotic Fractional S-Box Transformation. *Wirel. Pers. Commun.* **2016**, *90*, 2033–2049. [CrossRef]

56. Garcia, V.M.S.; Carapia, R.F.; Renteria-Marquez, C.; Luna-Benosco, B.; Aldape-Pérez, M. Substitution box generation using Chaos: An image encryption application. *Appl. Math. Comput.* **2018**, *332*, 123–135.

57. Lambić, D. A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. *Nonlinear Dyn.* **2020**, *1–13*. [CrossRef]

58. Lu, Q.; Zhu, C.; Wang, G. A Novel S-Box Design Algorithm Based on a New Compound Chaotic System. *Entropy* **2019**, *21*, 1004. [CrossRef]

59. Azam, N.A.; Hayat, U.; Ullah, I. Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field. *Front. Inf. Technol. Electron. Eng.* **2019**, *20*, 1378–1389. [CrossRef]

60. Khan, F.A.; Ahmad, J.; Khan, J.S.; Ahmad, J.; Khan, M.A.; Hwang, S.O. A new technique for designing $8 \times 8$ substitution box for image encryption applications. In Proceedings of the 2017 9th Computer Science and Electronic Engineering (CEEC), Colchester, UK, 27–29 September 2017.

61. Cassal-Quiroga, B.B.; Campos, E. Generation of Dynamical S-Boxes for Block Ciphers via Extended Logistic Map. *Math. Probl. Eng.* **2020**, *2020*, 1–12. [CrossRef]

62. Tran, M.T.; Bui, D.K.; Duong, A.D. Gray S-Box for Advanced Encryption Standard. In Proceedings of the 2008 International Conference on Computational Intelligence and Security, Suzhou, China, 13–17 December 2008.

63. Daemen, J.; Rijmen, V. The Rijndael block cipher: AES proposal. In Proceedings of the First Candidate Conference (AeS1), Ventura, CA, USA, 20–22 August 1998; pp. 343–348.