mathematics

MDPI

Article

A Novel Dynamic S-Box Generation Scheme Based on Quantum Random Walks Controlled by a Hyper-Chaotic Map

Lijun Zhang [1], Caochuan Ma [2,3], Yuxiang Zhao [1] and Wenbo Zhao [1,*]

[1] School of Electronic Information and Electrical Engineering, Tianshui Normal University, Tianshui 741000, China; zhanglj_81@tsnu.edu.cn (L.Z.); zhaoyx@tsnu.edu.cn (Y.Z.)
[2] School of Mathematics and Statistics, Tianshui Normal University, Tianshui 741000, China; ccma@tsnu.edu.cn
[3] College of Mathematics and Physics, Wenzhou University, Wenzhou 325035, China
* Correspondence: zhaowenbo211211@163.com

Abstract: For many years, chaotic maps have been widely used in the design of various algorithms in cryptographic systems. In this paper, a new model (compound chaotic system) of quantum random walks controlled by a hyper-chaotic map is constructed and a novel scheme for constructing a dynamic S-Box based on the new model is proposed. Through aperiodic evaluation and statistical complexity measurement, it is shown that the compound chaotic system has features such as complex structure and stronger randomness than classical chaotic systems. Based on the chaotic sequence generated by the composite system, we design a dynamic S-Box generation mechanism. The mechanism can quickly generate high-security S-Boxes. Then, an example of randomly generating S-Boxes is given alongside an analytical evaluation of S-Box standard performance criteria such as bijection, boomerang uniformity, bit independence, nonlinearity, linear approximate probability, strict avalanche effect, differential uniformity, the and generalized majority logic criterion. The evaluation results confirm that the performance of the S-Box is excellent. Thus, the proposed dynamic S-Box construction technique can be used to generate cryptographically strong substitution-boxes in practical information security systems.

Keywords: compound chaotic system; quantum random walk; S-Box generation mechanism; standard performance criteria; information security

MSC: 94A60; 39A33; 68M25

Citation: Zhang, L.; Ma, C.; Zhao, Y.; Zhao, W. A Novel Dynamic S-Box Generation Scheme Based on Quantum Random Walks Controlled by a Hyper-Chaotic Map. *Mathematics* **2024**, *12*, 84. https://doi.org/10.3390/math12010084

Academic Editors: José Balthazar, Angelo Marcelo Tusset, Átila Madureira Bueno and Diego Colón

Received: 29 November 2023
Revised: 18 December 2023
Accepted: 21 December 2023
Published: 26 December 2023

1. Introduction

In recent years, with the rapid development of network communication technology, network security has become an increasingly important research field. Accordingly, information security technology, which is used for data transmission security, has attracted widespread attention. Scholars have proposed various secure communication mechanisms, including a large number of data encryption algorithms. The user data is converted to cipher text by encryption technology before data transmission. This means that the input data block (plaintext) is converted into insignificant output block (ciphertext) and the ciphertext is useless to an attacker. In symmetric cryptographic systems, block encryption algorithms are widely used as they are easy to implement and provide the required cipher strength [1]. In block cipher systems, as the only nonlinear component, the substitution box (abbreviated as S-Box) is an important nonlinear component in many block cipher systems such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). In these block cipher systems, that use of an S-Box provides a complex relationship between plaintext and ciphertext and plays a scrambling effect (chaotic effect). The security of the S-Box determines the security strength of the whole block cipher system. Thus, it is meaningful to study how to quickly generate high security S-Boxes and this has attracted more and more attention. Usually, a designer must evaluate the strength

of respective S-Boxes in block cipher system. For S-Box security, there are some typical evaluation criteria, such as bijection, bit independence, nonlinearity, linear approximate probability, and strict avalanche effect. Some new attack technologies against S-Boxes have emerged with the development of new theories and technologies, such as the boomerang attack [2,3]. The authors of [4] summarize the many security attributes (including some new tests) of S-Boxes. A strong S-Box can resist cryptanalysis-based attacks if it can pass standard benchmarks tests. Thus, determining how to build a strong S-Box has received intensive attention.

However, the S-Box that is used in block cipher systems such as AES is a fixed component. That is, a block cipher has a static S-Box and employs the unchanged S-Box in each round. A static S-Box allows a third party to check the characteristics of the S-Box, which will lead to the attacker discovering its defects and eventually having the opportunity to cryptanalyze the ciphertext generated by the block cipher [5]. If high-quality S-Boxes (based on a user key) can be dynamically generated and applied, the encryption strength of the cryptosystem would be more able to resist various cryptanalytical attacks. A dynamically generated S-Box mechanism can be used to improve classic block cipher algorithms and design new block cipher algorithms. In recent years, researchers have explored elements of the concept of dynamic S-Box design, such as S-Box generation efficiency and randomness. In an actual cryptographic system, the S-Box is not only required to be safe but also the time and space efficiency of the algorithm for generating the S-Box must be high. Researchers have sought alternative S-Box design approaches. There are some approaches that are frequently applied to the construction of S-Boxes, such as the analytical approach [6], algebraic techniques [7], triangle groups [8], and chaotic maps [9–11]. Since chaos-based cryptography is considered highly secure, robust, and computationally powerful, and is complex enough to make cryptanalysis harder, chaos-based design emerges as the best method from the above approaches [11].

Chaotic dynamical systems have special nonlinear dynamic characteristics such as the sensitivity to initial conditions, unpredictability of long-term behavior, intrinsic randomness, and the ergodic nature of the processes. These characteristics of chaotic systems are equivalent to diffusion and confusion in traditional cryptographic systems [12]. Chaos cryptography is an important application field of chaos theory. For cryptosystems, there have many chaos-based algorithms proposed in recent years such as chaos-based image encryption, which was utilized in studies such as "Color image encryption using orthogonal Latin squares and a new 2D chaotic system" [13]; "Exploiting semi-tensor product compressed sensing and hybrid cloud for secure medical image transmission" [14]; and "A parallel image encryption algorithm using intrabitplane scrambling" [15]. For the development of modern cryptographic systems, chaotic maps have emerged as an alternative chaotic typology, and as part of this work, researchers have used chaos in the design of S-Boxes. An S-Box is essentially a random placement of $n \times n$ numbers from 0 to $n \times n - 1$. Chaotic systems with complex dynamic behaviors are able to generate high-quality pseudo random numbers. These pseudo random numbers can be used to design S-Box generation schemes. In the past few years, chaotic systems have been widely used in the design of S-Boxes due to the useful properties of chaotic maps, and analysis shows that an S-Box based on chaos has strong resistance to different attacks and higher space–time efficiency [16]. Scholars such as Ye and Zhimao [10], Masood et al. [11], Zheng and Zeng [17], Bin Faheem et al. [18], Zhu et al. [19], Lu et al. [20] have proposed many S-Box-based cryptographic systems that include effective S-Boxes that possess favorable characteristics such as bit independence, nonlinearity, etc.

However, problems such as unpredictability and short cycle may occur when implementing chaotic systems in digital devices (digital chaos) [21,22]. This will result in successful attacks on a cryptographic systems based on the original digital chaotic maps. Many cryptographic systems have serious security problems due to improper selection and application of chaotic maps [23]. Several researchers are working to rid chaotic maps of their weak points and further improve their chaotic behavior and randomness. Modified

chaotic maps can be used to enhance the security characteristics of various encryption schemes. It is necessary to combat the degradation of chaotic dynamic performance and further optimize chaos. Lu et al. [20], proposed 8×8 S-Boxes based on a improved compound chaotic map (tent-logistic system) that has a large key space, better chaotic behavior, and chaos at a large scale. In another study [24], a novel method of constructing S-Boxes is proposed that can generate strong S-Boxes through the use of TSS maps and algebraic Mobius transformations.

Inspired by the above discussion, we aim to search for a compound chaotic map with complex dynamic behavior and develop a new S-Box generation algorithm that can improve the linear probability (LP) and other characteristics of S-Boxes and enhance the robustness of cryptographic systems to linear analysis attacks, differential cryptanalysis attacks and boomerang attacks. The innovations of this work include the following:

1. A new compound chaotic system based on a two-dimensional hyper-chaotic map and quantum random walks is proposed, which has a larger key space and better chaotic performance and is more suitable for practical applications;
2. A simple and efficient dynamic S-Box generation algorithm is proposed;
3. A comprehensive and detailed security analysis of the generated S-Box is made to evaluate it against cryptographic landscapes. The analytical results demonstrate that the S-Box can well meet multiple cryptographic criteria.

The rest of this paper is organized as follows. Section 2 proposes a new compound chaotic system based on a two-dimensional hyper-chaotic map and quantum random walks. Section 3 describes an efficient dynamic S-Box generation algorithm based on the compound chaotic system. In Section 4, we show safety analyses of the proposed S-Box generated by the algorithm and make a comparison with some recent S-Boxes from the literature.

2. A Compound Chaotic System Based on a Two-Dimensional Hyper-Chaotic Map and Quantum Random Walks

In this section, we select a known two-dimensional hyper-chaotic map whose output is used as the control source of quantum random walks on the ring graph. Thus, a compound chaotic system with a complex structure that is sensitive to initial conditions and can generate uniform sequences is obtained.

2.1. Two-Dimensional Hyper-Chaotic Map Controlling Quantum Random Walks

A hyper-chaotic system has at least two expanding directions due to a minimum of two positive LEs [25]. The expression of a two-dimensional hyper-chaotic map is as follows [26] (p. 49):

$$\begin{aligned} u_{n+1} &= k_{11} + k_{12}u_n + k_{13}u_n^2 + k_{14}v_n + k_{15}v_n^2 + k_{16}u_nv_n, \\ v_{n+1} &= k_{21} + k_{22}u_n + k_{23}u_n^2 + k_{24}v_n + k_{25}v_n^2 + k_{26}u_nv_n. \end{aligned} \tag{1}$$

We simplify Expression (1) to make most of the parameter coefficients zero, i.e., $k_{11} = k_{12} = k_{13} = k_{16} = k_{21} = k_{23} = k_{25} = k_{26} = 0$. Finally, we obtain a simple two-dimensional hyper-chaotic map:

$$\begin{aligned} u_{n+1} &= k_{14}v_n + k_{15}v_n^2, \\ v_{n+1} &= k_{22}u_n + k_{24}v_n, \end{aligned} \tag{2}$$

where $k_{14} = 1.55$, $k_{15} = -1.55$, $k_{24} = 0.1$ and k_{22} is the control parameter. A fixed point of System (2) is $O = (0, 0)$, and the norm can be defined as follows:

$$\|(u, v)\| = \sqrt{u^2 + v^2}.$$

Let $h = (h_1, h_2)$, where

$$h_1(u, v) = -1.55v^2 + 1.55v, h_2(u, v) = k_{22}u + 0.1v.$$

h is continuously differentiable on R^2, and the Jacobian matrix is

$$Dh(u,v) = \begin{pmatrix} 0 & -3.1v + 1.55 \\ k_{22} & 0.1 \end{pmatrix}.$$

For the fixed point $O = (0,0)^T$, as $k_{22} < -1.003558730$ and $k_{22} > 1.003558730$, Map (2) may be chaotic if the absolute value of the eigenvalues of the matrix $Dh(O)$ is greater than 1. The randomness of the hyper-chaotic Map (2) will be investigated by trajectory diagram, Lyapunov exponent, and bifurcation diagrams with control parameters .

2.1.1. Trajectory Diagram

For a sequence generated by a dynamical system, in different stage from the initial state, values can be presented by using the trajectory diagram. If values occupy the entire phase space and occupy this space by choosing the correct initial conditions for a dynamical system, it can be concluded that the system appears chaotic if the correct initial conditions are chosen. The trajectory of Map (2) with the initial $(u_0, v_0) = (0.1, 0.1)$ is shown in Figure 1. In Figure 1, the effect of different k_{22} control parameter values is assessed according to the values generated by the hyper-chaotic map. As shown in Figure 1, the occupancy of the phase space in the trajectory increases as k_{22} grows increasingly negative.

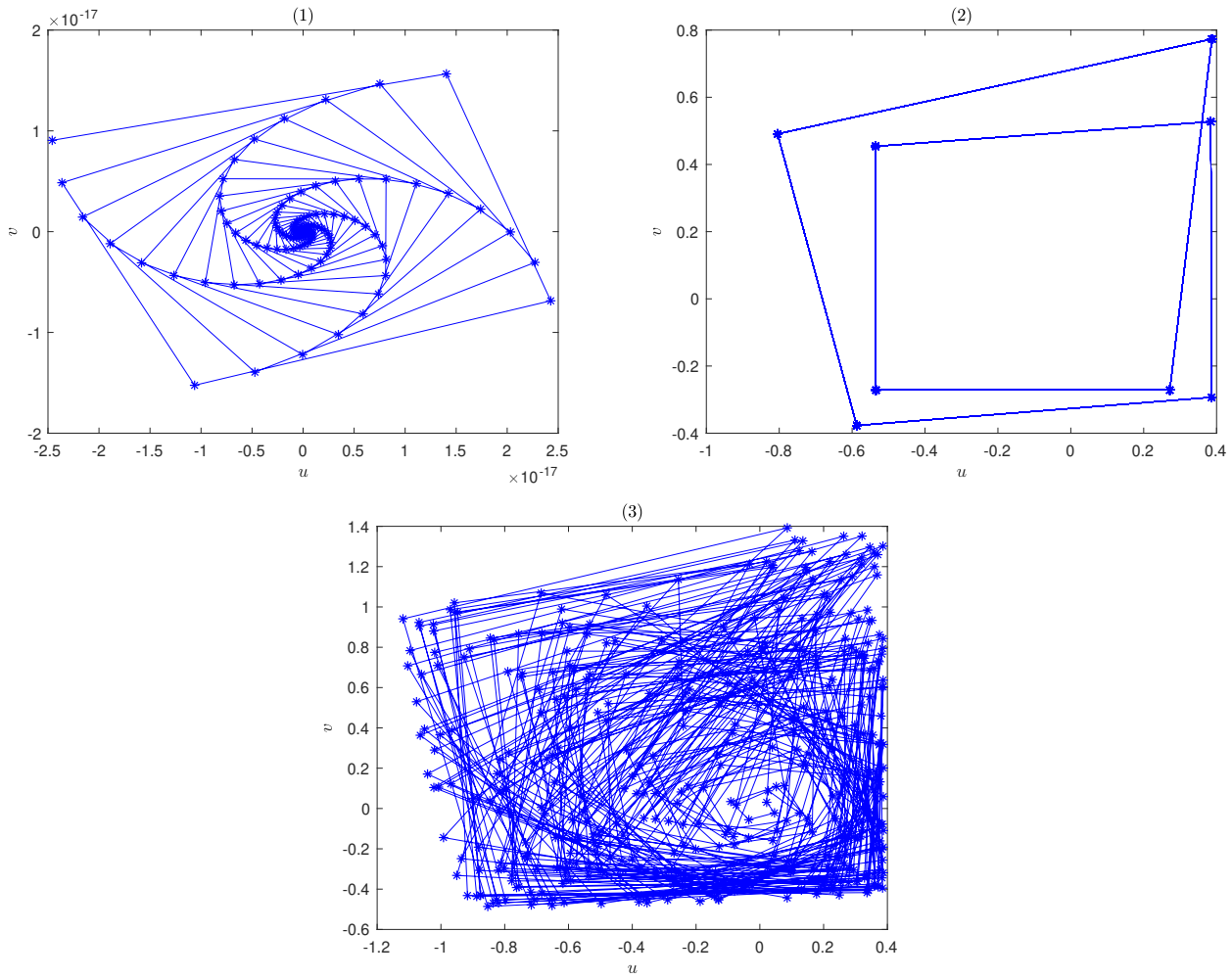

Figure 1. Trajectory diagram of map (2) with different values of the k_{22} control parameter ($k_{22} = 0.1$ in subfigure (1), $k_{22} = -0.9$ in subfigure (2), and $k_{22} = -1.16$ in subfigure (3)).

2.1.2. Lyapunov Exponents

The Lyapunov exponents (LEs) are one of the most important criteria for checking the randomness of a map and it sensitivity to the initial conditions. If the motion is chaotic, the Lyapunov exponent will be positive. Let $K_{area} = [-1.165, -1.105] - [-1.137, -1.135] - [-1.121, -1.117] - [-1.091, -1.088]$. Figure 2(1–3) show the Lyapunov exponents of the hyper-chaotic map, in which sub-figures (2) is refined using the subdivision method by selecting sub intervals. From Figure 2(1,2), it can be seen that the Lyapunov exponent is positive as $k_{22} \in K_{area}$.

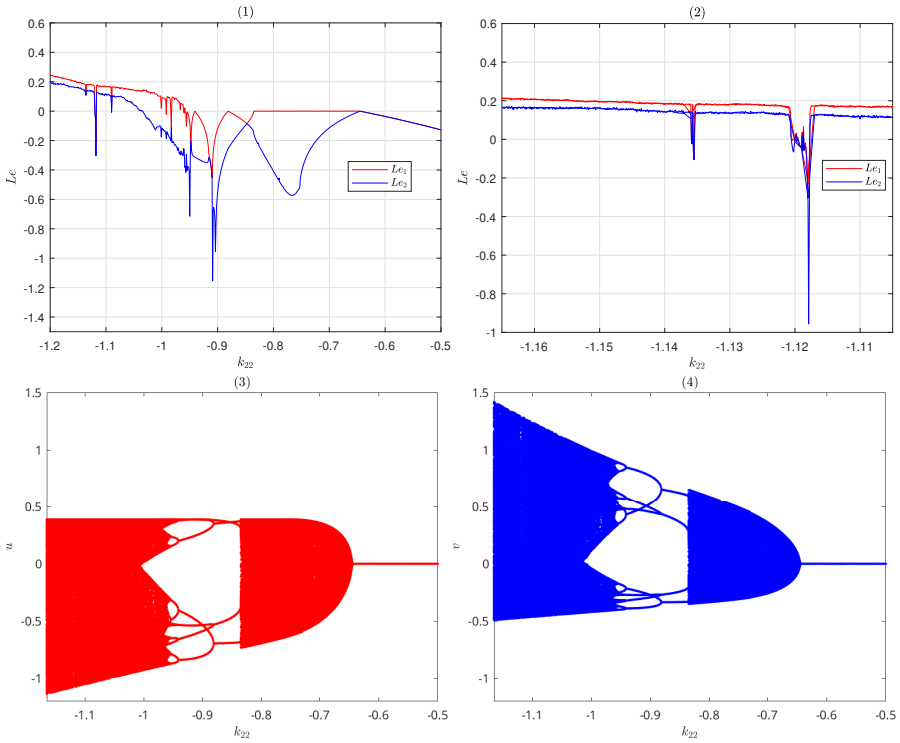

Figure 2. Lyapunov exponent and Bifurcation diagram of Sys (2) with different values of the k_{22} control parameter (Lyapunov exponents are shown in subfigure (1,2) and Bifurcation diagrams are shown in subfigure (3,4)).

2.1.3. Bifurcation Diagram

As a visual tool, a bifurcation diagram displays the process of period-doubling through the change of nonlinear dynamical system parameters. A chaotic system can achieve the best chaotic state by adjustment of the control parameters. That is, filling the phase space can be considered as the optimal value of the control parameters. Bifurcation diagrams of the system with changing k_{22} parameter are shown in Figure 2(3,4). It can be seen from Figure 2(3,4) that the filling space of the variable becomes greatest as $k_{22} \in K_{area}$.

2.2. A Scheme for a Sequence Generated by Quantum Random Walks on a Cycle Graph

G is a n-cycle graph and the degree of every node is 2. The quantum random walks on the cycle graph G contains two sub systems: Walker and Coin. Walker can be denoted as a position in an n-dimensional Hilbert space H_p and the basis state is $\{|i\rangle, i \in \{0, 1, 2, \cdots, n\}\}$ that span H_p. Any position of Walker can be represented as $\sum_i k_i|i\rangle$, and $\sum_i |k_i|^2 = 1$. Coin is a sub quantum system in two-dimensional dimensional Hilbert space H_c, and the canonical basis state is $\{|0\rangle, |1\rangle\}$. The state of Coin can be expressed as $a|0\rangle + b|1\rangle$, where $|a^2| + |b^2| = 1$. The joint state of Walker and Coin resides in $H_t = H_p \otimes H_c$, where p and c correspond to Walker and Coin, respectively.

The coin operator $\hat{C}$ has been extensively employed [27]:

$$\hat{C} = \cos\theta|0\rangle\langle 0| + \sin\theta|0\rangle\langle 1| + \sin\theta|1\rangle\langle 0| - \cos\theta|1\rangle\langle 1|.$$

The Walker shift operator has the following form:

$$\hat{S} = \sum_i (|i + forward(mod\ n)\rangle\langle i| \otimes |0\rangle\langle 0| + |i - back(mod\ n)\rangle\langle i| \otimes |1\rangle\langle 1|),$$

where $forward$ means that Walker takes steps to the right when the accompanying coin state is $|0\rangle$, and *back* means steps to left when the coin state is $|1\rangle$. Each operator on the total Hilbert space can be expressed as

$$\hat{U} = \hat{S}(\hat{C} \otimes I). \tag{3}$$

The initial state of the total system is $|\varphi(0)\rangle$, after t steps, the state is

$$|\varphi(t)\rangle = \hat{U}^t|\varphi(0)\rangle = \left(\hat{S}(\hat{C} \otimes I)\right)^t|\varphi(0)\rangle. \tag{4}$$

The probability of Walker at position $|v\rangle$ after t steps is

$$P_t(v|\varphi(0)) = |\langle(v,1)|\varphi(t)\rangle|^2 + |\langle(v,0)|\varphi(t)\rangle|^2, \tag{5}$$

and the resulting probability distribution is as follows:

$$\mathbf{P}_t = [P_t(v_1|\varphi(0)),\ P_t(v_2|\varphi(0)), \cdots P_t(v_n|\varphi(0))]. \tag{6}$$

The limiting distribution of Walker at position $|v\rangle$ is

$$\lim_{T\to\infty} \bar{P}_T(v|\varphi(0)) = \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} P_t(v|\varphi(0)). \tag{7}$$

According to Theorem 3.6 and Theorem 4.1 in the study [28], Equation (7) is close to a uniform distribution as n is odd. It can be seen from Equation (5) that there is a nonlinear map between initial state $|\varphi(0)\rangle = (i_0, c_0)$ and the resulting probability distribution $\mathbf{P}_t$ that is highly sensitive to the initial conditions [29]. According to Equations (4) and (5), a uniformly distributed sequence can be generated. Following this, the steps of a sequence generation scheme using quantum random walks on a ring graph are as shown in Algorithm 1.

Algorithm 1 Random number generation algorithm based on ring graph

Input: $(\theta,\ forward,\ back,\ n,\ i_0,\ c_0, r)$
Output: $AllOutputSeq$
(1) Init: $|\varphi(0)\rangle = (i_0,\ c_0)$,
$\hat{C} = \sin\theta|0\rangle\langle 1| - \cos\theta|1\rangle\langle 1| + \cos\theta|0\rangle\langle 0| + \sin\theta|1\rangle\langle 0|$
$\hat{S} = \sum_i (|i + forward(mod\ n)\rangle\langle i| \otimes |0\rangle\langle 0| + |i - back(mod\ n)\rangle\langle i| \otimes |1\rangle\langle 1|)$
$\Phi = |\varphi(n)\rangle = \hat{U}^n|\varphi(0)\rangle = \left(\hat{S}(\hat{C} \otimes I)\right)^n|\varphi(0)\rangle$,
$T_{max} = n$, $AllOutputSeq = \varnothing$;
(2) $for\ T = 1 : T_{max}$
$\Phi = \hat{U}^r\Phi = \left(\hat{S}(\hat{C} \otimes I)\right)^r\Phi$,
$for\ j = 1 : n$
$p_j = |\langle(j,0)|\Phi\rangle|^2 + |\langle(j,1)|\Phi\rangle|^2$
$endfor$
$OutputSeq = [p_1, p_2, \cdots, p_n]$,
$AllOutputSeq += OutputSeq$,
$end\ for$.
(3) $return\ AllOutputSeq$

2.3. A New Compound Chaotic System Based on Quantum Random Walks Controlled by a Hyper-Chaotic Map

In this section, a new compound chaotic system will be constructed by using quantum random walks and a two-dimensional hyper-chaotic map. Let $Q(\cdot)$ be Algorithm 1, which is essentially a pseudo random number generator. However, $Q(\cdot)$ can only generate $n \times n$ random numbers at a time. To generate new random numbers, there are two options. One is to continue to perform step (2) of Algorithm 1, and the other is to modify the relevant parameters except n, c_0, and i_0 before executing step (2) of Algorithm 1. Obviously, the second method is more flexible. If a two-dimensional system is used to adjust the corresponding parameters, the key space can be enlarged on the basis of increasing the complexity. Thus, the output (u, v) of hyper-chaotic map (2) is used to construct the parameter θ of $Q(\cdot)$. Let the normalization function be:

$$norm(x) = \frac{x - x_{min}}{x_{max} - x_{min}},$$

and the parameters $(\theta, forward)$ are constructed as follows:

$$\begin{aligned} \theta &= (1 - norm(v)) \times norm(u) + norm(v) \times \theta, \\ forward &= back = mod(floor(Z \times (norm(v) + norm(v))), \end{aligned} \tag{8}$$

where $floor(x)$ is the integral function and Z is an integer, which is generally larger to improve the randomness. The new compound chaotic system is based on quantum random walks controlled by a hyper-chaotic map. As the control parameter $k_{22} \in [-1.165,\ -1.105]$, the non-periodicity and statistical complexity of the compound chaotic system will be evaluated.

2.3.1. Degree of Non-Periodicity

The Scale index, which is based on the continuous wavelet transform (CWT), is presented by Benítez et al. [30], and we will use the tool to study non-periodicity in sequences generated by the proposed compound chaotic system. For chaotic sequences, wavelets are more suitable for studying non-periodicity due to their non-stationary nature [31]. We can assume that sequence f is a continuous function and $f \in L^2(\mathbb{R})$, which is defined over a finite time interval $I = [a,\ b]$. In Benítez et al. [30], the CWT of f at scale s and time u is defined as

$$Wf(u,s) := \langle f, \psi_{u,s} \rangle = \int_{-\infty}^{+\infty} f(t)\psi^*_{u,s}(t)\mathrm{d}t,$$

and from there it is possible to obtain the frequency component of f corresponding to time location u and scale s. The f scalogram, which is the energy of the CWT of f at scale s, is defined as

$$\mathcal{S}(s) = \|Wf(u,s)\| = \left(\int_{-\infty}^{+\infty} |Wf(u,s)|^2 du \right)^{\frac{1}{2}}.$$

Let $J(s) = [c(s),\ d(s)] \subseteq I$ and it is the maximal subinterval in I. The inner scalogram of f at a scale s can be defined by

$$\mathcal{S}^{inner}(s) = \|Wf(u,s)\|_{J(s)} = \left(\int_{c(s)}^{d(s)} |Wf(u,s)|^2 du \right)^{\frac{1}{2}},$$

where I must be big enough and $b - a \gg sl$ [32]. In order to compare the values of the inner scalogram at different scales, the inner scalogram should be normalized:

$$\overline{\mathcal{S}}^{inner}(s) = \frac{\mathcal{S}^{inner}(s)}{(d(s) - c(s))^{\frac{1}{2}}}.$$

In the scale interval $[s_0,\ s_1] \subseteq I$, the Scale index of f is given by

$$i_{scale} = \frac{\mathcal{S}^{inner}(s_{min})}{\mathcal{S}^{inner}(s_{max})},$$

where $s_{max} \in [s_0,\ s_1]$ is the maximal scale such that $\mathcal{S}^{inner}(s_{max}) \geq \mathcal{S}^{inner}(s)$ for all $s \in [s_0,\ s_1]$, and $s_{min} \in [s_{max},\ 2s_1]$ is the smallest scale such that $\mathcal{S}^{inner}(s_{min}) \leq \mathcal{S}^{inner}(s)$ for all $s \in [s_{max},\ 2s_1]$ [32]. For highly non-periodic sequences, the Scale index will be close to 1; while, it will close to 0 for periodic sequences [30].

We set $s_0 = 1$ and $s_1 = 20$, and choose a Haar wavelet as the mother wavelet function for calculating the Scale index. Figure 3 shows the Scale index of the compound chaotic system, the logistic map, and the Henon map. From a comparison of Figure 3a–c, we can obtain that the Scale index of the compound system is higher than those of the other two chaotic maps. Thus, we can conclude that the sequence generated by the compound system is more non-periodic.

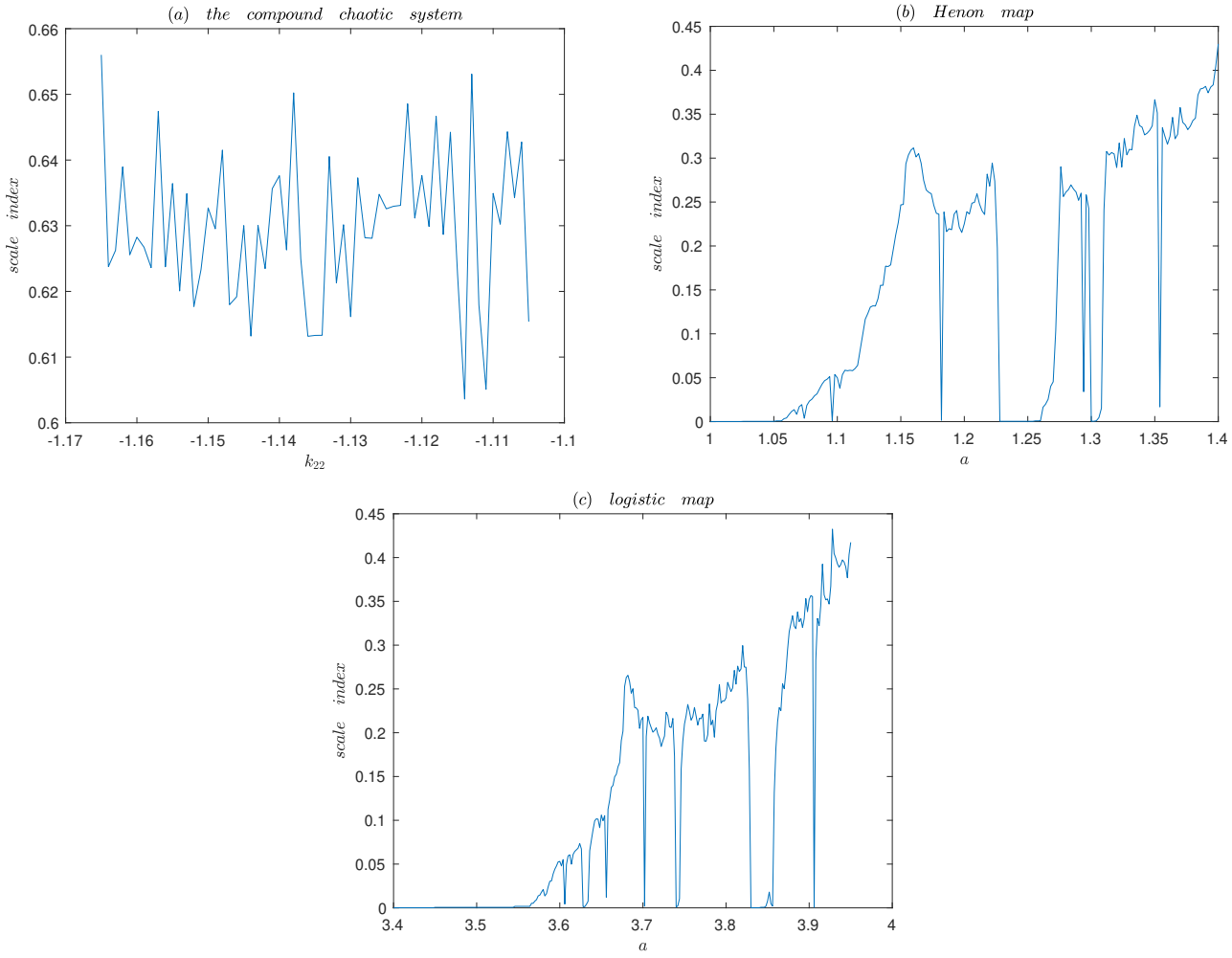

Figure 3. The Scale index of the Henon map, the logistic map, and the compound chaotic system.

2.3.2. Statistical Complexity Measures

The authors of [33], proposed statistical complexity measures (SCMs), which are used to quantify the degree of physical structure in a sequence. We use the the method of Larrondo et al. [34] to calculate the SCMs. The intensive SCM ($C_j[P]$) can be thought

of as a quantity that represents the probability distribution P that is associated with a sequence [35]. $C_j[P]$, introduced by Larrondo et al. [34], is defined as:

$$C_j[P] = H_S[P]Q_j \cdot [P, P_e], \tag{9}$$

where Q_J is "disequilibrium" and $H_S[P]$ is the entropic measure (normalized entropy). $H_S[P]$ can be calculated by

$$H_S[P] = H[P]/H_{max}, \tag{10}$$

where H is the Shannon entropy. The entropy of a byte sequence is given by the following:

$$H = \sum_{i=1}^{N} p(a_i) log_2 p^{-1}(a_i), \tag{11}$$

where $p(a_i)$ is the probability that a_i occur in the sequence. For a byte sequence, the ideal value of entropy (H_{max}) is 8. Q_J is an intensive quantity [35] and Q_J is given by

$$Q_j[P, P_e] = Q_0 \cdot \{H[(P + P_e)/2] - H[P]/2 - H[P_e]/2\},$$

where Q_0 is a normalization coefficient, which can be calculated by

$$Q_0 = -2\left\{\left(\frac{N+1}{N}\right)\ln(N+1) - 2\ln(2N) + \ln N\right\}^{-1}.$$

If a PRNG can generate high-quality pseudo-random numbers, it can be expected that "no attractor" will be reconstructed. It is reasonable to obtain a homogeneity cloud of points with a strong performance that "fill" up a d-dimension space [34]. Consequently, the associated permutation probability distribution will be $P \simeq P_e$, so $H_S[P] \simeq 1$ and $C_J[P] \simeq 0$ and for periodic sequences will have $H_S[P] \simeq 0$ and $C_J[P] \simeq 0$ [34]. H_S and C_J as functions of the number of 8 bits are shown in Figure 4 based on the above calculation method. From Figure 4, it can be see that C_j and H_s tend to 0 and 1, respectively, when the number of words of the analyzed sequence increases. Thus, the randomness of the PRNG based on the proposed compound chaotic system is successfully verified by statistical complexity and the normalized Shannon entropy.

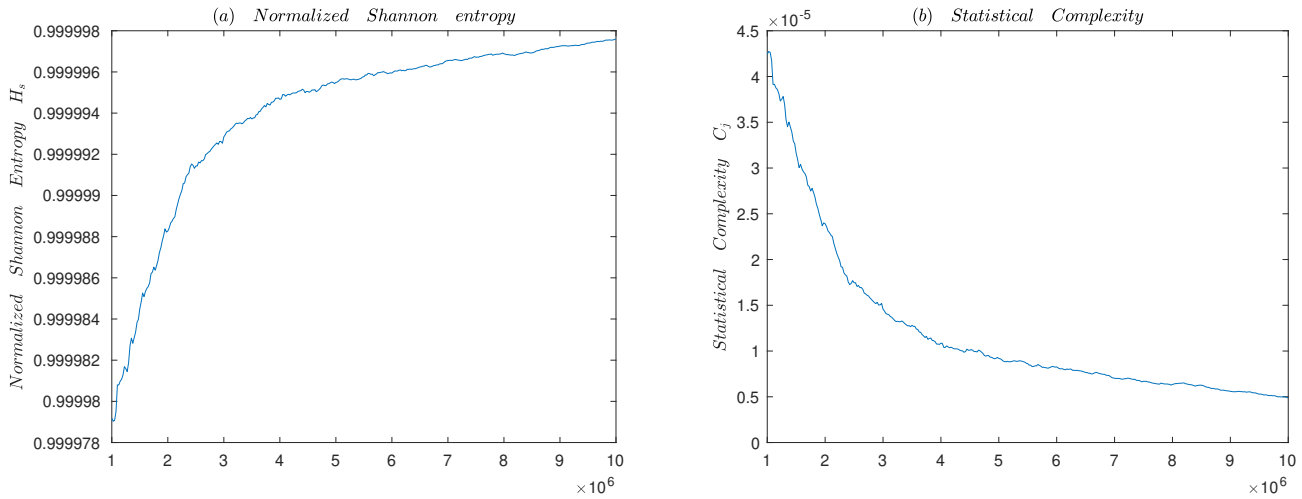

Figure 4. H_s and C_j for the proposed PRNG.

3. Dynamic S-Box Generation Algorithm Based on the Compound Chaotic System

3.1. Introduction of the S-Box

In a symmetric block cipher system, the S-Box plays an important role as the only nonlinear component. An S-Box is essentially a nonlinear permutation function, which can be understood as an encrypted black box. Furthermore, it confuses the relationship

between the ciphertext and plaintext. An S-Box can be abstracted as a vector Boolean function of n-bit input and m-bit output:

$$Sbox: \begin{array}{c} \mathbb{F}_2^n \to \mathbb{F}_2^m \\ \{0,1\}^n \to \{0,1\}^m \end{array}.$$

For most S-Boxes in cryptography, commonly the case of $n = m$ is used and an $n \times n$ S-Box is shown in Figure 5. We focused on the design algorithm for 8×8 S-Boxes, which are the most commonly used type in cryptography. An 8×8 S-Box is a set of integers $S_{set} = \{0, 1, 2, \cdots, 2^8 - 1\}$, which is unique for a matrix Sb: $Sb = \{ Sb(i,j) \,|i = 1, 2, \ldots, 16;\ j = 1, 2, \ldots, 16\}$. The matrix Sb can be obtained:

$$\begin{cases} i = floor(x/16),\ j = x \bmod 16 + 1, \\ y = Sbox(x) = Sb(i,j), \end{cases} \tag{12}$$

if the vector Boolean function corresponding to an 8×8 S-Box is $y = Sbox_{8\times8}(x)$, where both x and y are elements in S_{set}. Conversely, it is known that an 8×8 S-Box corresponds to $Sbox_{8\times8}^{-1}(y)$:

$$\begin{cases} y = Sb(i,j), \\ x = Sbox_{8\times8}^{-1}(y) = 16(i-1) + j - 1. \end{cases} \tag{13}$$

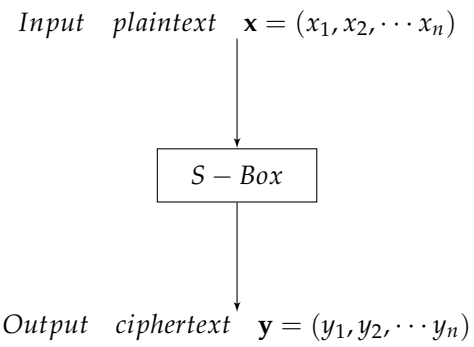

Figure 5. The function and basic principle of an $n \times n$ S-Box.

3.2. Pseudo-Random Number Generator (PRNG) Based on the Proposed Compound Chaotic System

In this section, a PRNG is designed based on the proposed compound chaotic system, followed by a NIST Statistical Test of the PRNG. The fixed-point algorithm [35] expressed by P-bit precision is adopted, and the specific steps of generating random number are as follows:

1. Initialization $(u_0, v_0, k_{22}, \theta,\ faward,\ back,\ n,\ i_0,\ c_0, r)$;
2. $Q_{Hy}^{1000}(u_0, v_0)$;
3. Let $Y_k = \sqrt{3}p_{3(k-1)} + \sqrt{5}\left(p_{3(k-1)+1}p_{3(k-1)+2}\right)$. Furthermore, the following formula is used to generate and output the random number z_k:

$$z_n = \bmod\left(floor\left(\sqrt{2}\left(2^P - 1\right) \cdot 10^5 \cdot Y_k\right), 2^P\right),$$

where $floor(\cdot)$ is an integral function.

NIST Statistical Test

We will use NIST SP800-22 [36] to estimate the randomness of sequences generated by the PRNG based on the compound system. In the NIST suite, there are 17 test items and every test item concentrates on one type of non-randomness that can exist in a sequence. There are two performance indicators, pass rate and p-value, to determine the random

performance of the sequence. In our tests, the following settings were used: the number of sequences to be tested was 100, the sequence length was 10^6 bits, and the significance level was $\alpha = 0.01$, which implies that if the sequence passed the test, it can be referred to as being random with a probability of 99%. For each statistical test item except for the random excursion test, the minimum pass rate is around 96 for sample capacity = 100 bit sequences. The results of NIST SP800–22 test for the PRNG are given in Table 1. The results of the sequence generated by proposed PRNG are all "Pass". Hence, the sequence generated by the PRNG be considered to have high randomness, and the PRNG can be used in information security systems.

Table 1. Results of the NIST SP800–22 for the PRNG.

Test Name	*p*-Value	Pass Rate	Result
Frequency	0.816537	99/100	Pass
Block Frequency (m = 128)	0.249284	98/100	Pass
Cumulative Sums (Forward)	0.289667	99/100	Pass
Cumulative Sums (Reverse)	0.319084	99/100	Pass
Runs	0.935716	98/100	Pass
Longest Run of Ones	0.419021	99/100	Pass
Rank	0.955835	100/100	Pass
FFT	0.202268	99/100	Pass
Non-Overlapping Templates (m = 9, B = 000000001)	0.964295	100/100	Pass
Overlapping Templates (m = 9)	0.595549	100/100	Pass
Universal	0.494392	99/100	Pass
Approximate Entropy (m = 10)	0.191687	98/100	Pass
Random-Excursions (data1)	0.848588	63/63	Pass
Random-Excursions Variant Serial (data7)	0.788728	63/63	Pass
Serial Test 1 (m = 16)	0.383827	99/100	Pass
Serial Test 2 (m = 16)	0.319084	100/100	Pass
Linear complexity (M = 500)	0.595549	100/100	Pass

3.3. Dynamic S-Box Generation Algorithm Based on the Proposed PRNG

Generally, complex designs can generate S-Boxes with high cryptographic strength, but the time cost is very large while the efficiency is low. Here, we propose a simple and effective method of constructing strong 8×8 S-Boxes based on the proposed PRNG. The new method takes advantage of the excellent chaotic characteristics of the compound system.

For generating S-Boxes, the steps of algorithm based on the proposed PRNG are shown in Algorithm 2.

By the proposed method, the length of sequences generated by the PRNG is used to construct an S-Box that corresponds to a 16×16 matrix. The proposed new S-Boxes are generated by the above algorithm and the parameters are set as $\{u_0 = 0.1, v_0 = 0.1, k_{22} = -1.1, n = 15,\ r = 5,\ i_0 = 2,\ c_0 = 1,\ \theta = \frac{\pi}{r}, forward = back = 1\}$. The matrix Sb corresponding to the first generated S-Box is shown in Table 2.

Table 2. The *Matrix* representing the proposed S-Box.

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

Algorithm 2 The algorithm for generating S-Boxes

Input: $(N, r, i_0, c_0, \theta, farward, u_0, v_0, k_{22})$ and m (number of S-Boxes required)
Output: $AllSboxes$
(1) $AllSboxes = \{\}$;
(2)
%%
Initialize the state of an S-Box:
%%
$Sbox[i] = i,\ i = 0, 1, \cdots 2^8 - 1$;
(3) for $0 \le i < 2^8$
Obtain a number j from the proposed PRNG;
swap values of $Sbox\left[2^8 - 1 - i\right]$ and $Sbox[j]$;
end for;
(4) $status = 1$;
%%
Check whether the S-Box meets the criteria of high diffusion and low differential uniformity [37].
%%
for $0 \le i < 2^8$
if $\left|Sbox[i] - Sbox\left[\mathrm{mod}\left(i + 1, 2^8\right)\right]\right| \le 2 \parallel \delta(Sbox) > 10$
%%
The operator $\delta()$ is used to obtain the differential uniformity value of an S-Box.
%%
$status = 0$;
break;
end if
end for;
If $status == 1$
$AllSboxes+ = Sbox$;
else
jump to (2);
(5) if $count(AllSboxes) < m$
jump to (2);

4. Performance Tests of the Constructed S-Box

An S-Box is the only nonlinear component in a block encryption system (providing nonlinear mapping between plaintext and ciphertext), so it is very important to evaluate the robustness of encrypted data attacks by analyzing the nonlinear characteristics of the S-Box. We will evaluate the encryption strength of the proposed S-Box given in Table 2. We will use S-Box performance evaluation criteria such as strict avalanche criterion (SAC), bijection, nonlinearity, BIC, and Linear approximation probability (LAP).

4.1. Basic Cryptographic Evaluation Criteria

4.1.1. Bijection

For a function or S-Box $Y = S(X) : \ X \in \mathbb{F}_2^n \rightarrow Y \in \mathbb{F}_2^n$, it is bijective if it is a one-to-one map. From Table 2, it can be seen that a clearly different value of Y corresponds to only one X. Conversely, one can obtain a distinct value X by Equation (13) and Table 2. Hence, the obtained S-Box of Table 2 has bijective properties.

4.1.2. Algebraic Degree

The algebraic degree of the S-Box can provide an upper limit for the algebraic degree of the whole cryptographic system [4].

Definition 1. *For a Boolean function $Y = S(X)$, the algebraic normal form of Y is as the follows [4]:*

$$\mathrm{ANF}_S = \bigoplus_{u \in \mathbb{F}_2^n} \alpha_u \prod_{i=0}^{n-1} x_i^{u_i},$$

where $\alpha_u \in \mathbb{F}_2$. The Algebraic degree of $S(X)$

$$\mathrm{Deg}(S) \triangleq \max\{\mathrm{wt}(u) \mid u \in \mathbb{F}_2^n \text{ and } \alpha_u \neq 0 \in \mathbb{F}_2^n \text{ in } \mathrm{ANF}_S\}.$$

For an 8×8 S-Box, $S(X)$ is usually represented by a collection of 8 Boolean functions of 8 variables called the coordinates of S. Thus, $S(X)$ can be represented as

$$\mathrm{S}(X) = \mathrm{S}_1(X)\mathrm{S}_2(X) \ldots \mathrm{S}_8(X),$$

where $\mathrm{S}_i(X) \in \{0, 1\}$. In practical calculation, $\mathrm{Deg}(S)$ is given by estimate the maximum among all degrees of the coordinate functions:

$$\mathrm{Degree}(S) = \max\{degree(S_i) | S(X) = (S_1(X), S_2(X), \cdots S_n(X))\}. \quad (14)$$

The degree of the coordinate functions of the listed S-Box is presented in Table 3 according to Equation (14). We can see that degree of every coordinate function is 7, the largest possible value.

Table 3. Degree of coordinate functions of the proposed S-Box.

$Sbox_i$	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
degree	7	7	7	7	7	7	7	7

4.1.3. Algebraic Complexity (Univariate Degree)

For a cryptosystem, the algebraic complexity of the S-Box can be used to evaluate the ability of the system to cope with interpolation attacks [4]. If the univariate degree of the S-Box is too low, it can lead to successful interpolation attacks [38].

It is clear from Bao et al. [4], [p. 17] that if $\mathbb{F}_{2^n}[X]/(f(X)) \cong \mathbb{F}_{2^n}$, $S(X)$ can be uniquely represented as a univariate polynomial in $\mathbb{F}_{2^n}[X]/(f(X))$ from:

$$S(X) = \sum_{i=0}^{2^n-1} A_i X^i.$$

$A_0 = S(0)$, $A_{2^n-1} = \sum_{x \in \mathbb{F}_{2^n}} S(x)$, and the other coefficien A_i can be calculated by discrete Fourier transform of the values of S, that is:

$$A_i = \sum_{k=0}^{2^n-2} S\left(\alpha^k\right)\alpha^{-ki},\ 0 \le i \le 2^n - 2, \tag{15}$$

is a primitive element in $\mathbb{F}_{2^n}[X]/(f(X))$. The Algebraic Complexity AC of $S(X)$ is the number of non-zero coefficients in the linear polynomial representation of $S(X)$.

For an 8×8 S-Box, $f(X) = X^8 + X^4 + X^3 + X^2 + 1$ is an irreducible polynomial and β is taken as a root of $f(X)$ in $\mathbb{F}_{2^8}$. β is a primitive element and we identify $\mathbb{F}_2^8$ with $\mathbb{F}_{2^8} = \left\{0, 1, \beta, \beta^2, \cdots, \beta^{254}\right\}$ using the basis $\left\{1, \beta, \beta^2, \cdots, \beta^7\right\}$. Because $\mathbb{F}_{2^8}[X]/(f(X)) \cong \mathbb{F}_{2^8}(\beta) \cong \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \cdots \oplus \mathbb{F}_2$, we can obtain that the corresponding codes for $0, 1, X^1, \cdots, X^{254}$ shown in Table 4. Then, coefficient A_i of X^i in the univariate expression corresponding to the S-Box can be calculated by Equation (15), as shown in Table 5. From Table 5, We can see that the AC is 255, the largest possible value.

Table 4. Code of $X^t = X^{(m-1)\times 16+n}$.

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

Table 5. The coefficients $A_i = A_{(m-1)\times 16+n-1}$ (coefficient of univariate polynomial representation).

m/*n*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	145	33	253	168	50	241	221	168	150	208	54	179	157	196	216	21
2	44	151	203	161	238	133	253	107	223	199	184	244	229	154	44	176
3	129	69	236	230	239	250	186	45	158	139	78	198	29	56	99	31
4	36	206	82	115	33	35	1	194	139	133	45	47	163	233	203	184
5	169	112	221	31	45	205	101	169	141	190	234	148	172	100	129	157
6	201	14	91	123	222	143	49	209	221	39	156	206	76	19	7	99
7	37	69	33	126	22	103	140	233	73	72	186	3	168	9	175	49
8	49	174	30	81	115	124	232	221	123	23	75	207	18	139	22	11

Table 5. *Cont.*

m/*n*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
9	254	82	194	182	201	173	168	226	90	104	205	190	62	15	40	20
10	193	114	89	84	219	1	98	146	52	106	139	194	69	199	39	170
11	176	185	66	62	245	220	99	94	43	44	43	11	246	199	83	110
12	63	238	98	188	167	30	180	214	95	249	101	5	148	154	219	76
13	115	5	215	170	233	45	112	37	119	253	88	89	223	32	52	243
14	107	171	144	56	148	61	150	130	117	255	55	22	29	143	248	210
15	63	251	113	209	158	134	61	59	164	114	130	147	184	249	143	194
16	106	98	219	204	166	88	116	200	170	54	212	225	23	64	186	0

4.1.4. Nonlinearity

For an S-Box $S(X)$, in order to effectively resist linear cryptanalysis attacks, the relationship between outputs and inputs should be highly nonlinear. We will use the nonlinearity of every Boolean function S_i to estimate the S-Box's nonlinear strength. Based on the Walsh transform of the Boolean function S_i, the evaluation criteria for nonlinearity is defined. The Walsh transform of a Boolean function S_i is defined as [39]:

$$WS_{S_i}(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{w \cdot x \oplus S_i(X)},$$

where the $\cdot$ operator denotes the scalar product. For a Boolean function S_i, the nonlinearity calculation is based on the following equation [40]:

$$N_{S_i} = 2^{n-1} - 2^{-1} \max_{w \in F_2^n} WS_{S_i}(w).$$

The nonlinearity values of all constituent 8-bit Boolean functions of the proposed S-Box are provided in Table 6. From Table 6, we can see that the average nonlinearity was 106.5, the maximum nonlinearity was 112, and the minimum nonlinearity was 104.

Table 6. Nonlinearities of coordinate functions of the proposed S-Box.

$S-Box/S_i$	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	*Average*
Nonlinearity	104	106	106	104	110	106	112	104	106.5

4.1.5. Strict Avalanche Criterion (SAC)

An imperative cryptographic feature for an S-Box is the Strict Avalanche Criterion (SAC), which was first introduced in Webster and Tavares [41]. If an S-Box satisfies the SAC, as a single bit is changed in the input, half the output bits should be modified. For an S-Box, the SAC property requires that all the values in the dependency matrix are close to the ideal value of 0.5. The SAC values provided by the dependency matrix of the proposed S-Box are listed in Table 7. From Table 7, it can be seen that the average value is equal to 0.5. Thus, the proposed S-Box has good SAC performance.

Table 7. *SAC_Dep* matrix of the proposed S-Box.

0.5746	0.5517	0.5188	0.4753	0.4772	0.5379	0.4979	0.5276
0.4719	0.4821	0.5756	0.4837	0.5895	0.5004	0.4463	0.4622
0.5407	0.4823	0.5816	0.5187	0.4307	0.4070	0.4942	0.4878
0.5474	0.4812	0.5162	0.4815	0.5114	0.5339	0.4757	0.4535
0.5065	0.4680	0.5365	0.5185	0.5197	0.4902	0.5321	0.4392
0.5367	0.5240	0.4952	0.5165	0.5976	0.5691	0.5347	0.5091
0.5654	0.5288	0.5458	0.5255	0.4708	0.4594	0.4648	0.5513
0.5229	0.5791	0.5664	0.5164	0.4262	0.6032	0.3924	0.4726

4.1.6. Bit Independence Criterion (BIC)

Based on the reverse of plaintext, a set of avalanche vectors can be generated, and all avalanche variables should be paired and independent. The degree of independence ρ can be measured by calculating the phase relation of two avalanche vectors A and B:

$$\rho\{A,B\} = \frac{cov\{A,B\}}{\sigma\{A\}\sigma\{B\}},$$

where $\sigma^2\{A\} = E\{A^2\} - (E\{A\})^2$ and $cov\{A,B\} = E\{AB\} - E\{A\}E\{B\}$. If ρ is 0, the two variables are independent of each other. Furthermore, the two variables are the "same" if ρ is 1, while if it is equal to -1, the two variables are complementary.

A method of actually measuring BIC was proposed by C.Adams and S.Tavares in [41,42]: for the coordinate Boolean functions S_j and $S_k(j \neq k)$ of a given S-Box, if $S_i \oplus S_k$ is highly nonlinear or $S_i \oplus S_k$ satisfies SAC as much as possible and the correlation coefficient of every output bit pair approaches 0 if only one input bit is inverted. By verifying whether $S_i \oplus S_k$ between any two output bits of the S-Box strictly satisfies the avalanche effect, or by calculating the nonlinearity of $S_i \oplus S_k$, whether the S-Box satisfies BIC can be tested. For 8 Boolean functions of the proposed S-Box, the nonlinearity and SAC values, respectively, are listed in Tables 8 and 9. We can see from Tables 8 and 9 that the SAC values and average nonlinearity for BIC are 0.50698 and 105.6, respectively. Thus, there is an extremely weak linear association among the output bits, and, thus, the obtained S-Box had good BIC performance.

Table 8. Bit independence criterion for SAC.

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
S_1	-	0.46875	0.54688	0.54688	0.51562	0.54688	0.56250	0.51562
S_2	0.54688	-	0.48438	0.48438	0.46875	0.53125	0.53125	0.57812
S_3	0.51562	0.57812	-	0.51562	0.54688	0.48438	0.54688	0.56250
S_4	0.46875	0.48438	0.51562	-	0.51562	0.51562	0.53125	0.51562
S_5	0.48438	0.59375	0.42188	0.50000	-	0.59375	0.46875	0.42188
S_6	0.53125	0.50000	0.40625	0.53125	0.48438	-	0.45312	0.59375
S_7	0.50000	0.43750	0.50000	0.46875	0.53125	0.53125	-	0.39062
S_8	0.51562	0.46875	0.48438	0.45312	0.43750	0.51562	0.54688	-

Table 9. Bit independence criterion for nonlinearity.

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
S_1	-	108	108	108	106	104	112	106
S_2	108	-	108	106	106	102	108	108
S_3	108	108	-	102	102	108	100	104
S_4	108	106	102	-	108	102	106	106
S_5	106	106	102	108	-	106	102	104
S_6	104	102	108	102	106	-	106	106
S_7	112	108	100	106	102	106	-	106
S_8	106	108	104	106	104	106	106	-

4.1.7. Differential Probability

The XOR distribution of the input and output of an S-Box can be obtained from the differential probability [43] of the S-Box. By analyzing the differential probability, it is possible to obtain the original plaintext. Differential probability is computed by:

$$DP_S = \mathrm{Max}_{\Delta X \neq 0, \Delta Y}\left(\frac{\#\{X \in N \mid \Delta Y = S(X \oplus \Delta X) \oplus S(X)\}}{2^n}\right),$$

where ΔY is the output difference and ΔX is the input difference. The lower the value of the differential probability, the stronger the ability of the S-Box to resist differential cryptanalysis. The maximum DP value of the S-Box generated by this algorithm is only 0.0390625.

4.1.8. Maximal Degree of the Product of k Coordinates

For a cryptosystem, the degrees of the product of any k coordinates of the S-Box can provide the degree of the superior upper bound. For an S-Box $S(X)$, to obtain the definition of maximal algebraic degree of the product of any k coordinates, we go through generalized definitions of an S-Box.

Definition 2. *For an S-Box, the Walsh transform [39] of the corresponding $S(X)$ is defined as the following:*

$$\mathcal{W}_S(\alpha, \beta) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\beta \cdot S(x) \oplus \alpha \cdot x}, \quad \alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^n.$$

In matrix $\mathcal{W}_S$, the value of point (α, β) represent the Walsh coefficient at (α, β). The maximal algebraic degree of the product of any k coordinates of $S(X)$ is given by Bao et al. [4]:

$$d_k(S) = \max_{K \subseteq \{1,\ldots,8\}, |K| \leq k} \deg\left(\prod_{i \in K} S_{e_i}\right),$$

where S_{e_i} is called the ith coordinate of the S-Box and

$$S_{e_i}(x) = \frac{1}{2} - \frac{1}{2^{n+1}} \sum_{a \in \mathbb{F}_2^n} \mathcal{W}_S\left(a, 2^i\right)(-1)^{a \cdot x}.$$

The values of $d_k(S)$ are closely related to resistance against higher-order differential attacks [4]. This means that the higher their values, the stronger the S-Box's ability to resist high-order differential attacks . The $d_k(S)$ values of the proposed S-Box are shown in Table 10. We can see that all $d_k(S)$ values are 7, the largest possible value.

Table 10. Maximal degree of the product of k coordinates of the proposed S-Box.

k	1	2	3	4	5	6	7
d_k	7	7	7	7	7	7	7

4.1.9. Differential Uniformity

The differential uniformity of an S-Box is defined as [4]:

$$\delta_S = \max_{a \neq 0, b} \delta(a, b) = \max_{a \neq 0, b} \#\left\{X \in \mathbb{F}_2^8 : S(X \oplus a) \oplus S(X) = b\right\}, \tag{16}$$

where $a,\ b \in F_2^8$. Low differential uniformity is advantageous for a good S-Box. The smaller δ_S is, the better the S-Box approximates to being perfectly nonlinear [44]. δ_S of the proposed S-Box is 10 according to Equation (16).

4.1.10. Linear Approximation Probability

The linear approximation probability (LAP) is mainly concerned with linear attacks on block encryption technology, and it is used to measure the ability of a cryptographic system to resist linear cryptanalysis. The linear approximation probability of an S-Box is the maximum unbalance value, which is presented as [43]:

$$\mathrm{LAP} = \max_{\alpha, \beta} \left| \frac{\#\{X \in \mathbb{GF}(2^n) \mid X \cdot \alpha = S(X) \cdot \beta\}}{2^n} - \frac{1}{2} \right|, \tag{17}$$

where α and β are the input and output mask values, and $\cdot$ is the dot product operation on $\mathbb{F}^2$. The maximum value of LAP of the proposed S-Box is only 0.1328125.

4.2. Security Analysis

4.2.1. Resistance to Algebraic Attacks

A cryptosystem can be regarded as an algebraic system and the fundamental principles of algebraic attacks can be traced back to Shannon's work [45], in which he said that the entire cryptosystem can be mathematically modeled and expressed as a multivariate algebraic equation. The resistance of cryptographic systems to algebraic attacks can be evaluated by calculating the nonlinearity, algebraic complexity, and algebraic degree.

It is clear from Tables 5 and 3 that AC and $\mathrm{Deg}(S)$ need to be high for the cryptosystem to resist algebraic attacks efficiently.

4.2.2. Resistance to Differential Attack

A differential attack is an analysis of the distribution of output differences caused by an input with a fixed difference [4]. The security of an 8×8 S-Box against differential attack is quantified by computing its differential probability $DP(S)$, maximal algebraic degree of the product of any k coordinates $d_k(S)$, and differential uniformity δ_S. The $DP(S)$ and δ_S of the proposed S-Box are small, while the $d_k(S)$ values are the largest possible. Thus, the S-Box has good resistance to differential attacks.

4.2.3. Resistance to Linear Attack

The linear attack was proposed by Mitsuru Matsui [46]. A linear attack exploits the fact that a cryptosystem $C = E_K(P)$ can form a Boolean function that behaves as non-random (imbalanced) on the set of P [46]. In a linear attack, the cyber attacker searches for the most biased linear relation between the input and output bits of the S-Box. Security against linear attack is quantified by computing LAP, nonlinearity, and AC. If LAP is small while the nonlinearity and AC are high, an S-Box can be highly resistant to linear attack. It can be clearly seen from the above nonlinearity of the proposed S-Box (in Table 6), AC value of 255, and LAP value of 0.1328125 that the NL and AC of the proposed S-Box and are sufficiently high, while the LAP is low. Thus, the S-Box has good resistance to linear attack.

4.2.4. Resistance to Boomerang Attack

A differential-style attack called the boomerang attack was first described by Wagner [3]. The boomerang attack is considered an extension of classical differential attacks. In a classic boomerang attack, cryptosystem E is regarded as a combination of two sub-cryptosystems E_0 and E_1 such that $E = E_1 \circ E_0$. There are two different inputs, α and γ; α is exported to β by E_0 with probability p and γ is propagated to δ by E_1 with probability q. In the original study [3], the boomerang attack is based on the expectation probability:

$$\Pr\left[E^{-1}(E(x) \oplus b) \oplus E^{-1}(E(x \oplus a) \oplus b) = a\right] = p^2 q^2.$$

Since Wagner put forward this kind of attack, many improved boomerang attacks have been proposed [2]. In particular, the cryptosystem E is decomposed into three modules: $E = E_1 \circ E_m \circ E_0$, and the E_m corresponds to a simple change (usually an S-Box). The probability of generating a right quartet in each S-Box in the middle S-Box layer is given by the following equation [47]:

$$\frac{\#\left\{x \in \{0,1\}^n \mid S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_o) = \Delta_i\right\}}{2^n},$$

where (∇_o, Δ_i) is a given differential pair. Cid et al. focused on the effect of S-Box construction on boomerang attacks, and constructed a pre-calculated table to evaluate this probability. This table is called the boomerang connectivity table (BCT), which is defined as follows.

For an S-Box, the boomerang connectivity table (BCT) of the corresponding $S(X)$ is defined by the following equation [47]:

$$\beta_S(a,b) \triangleq \#\left\{x \in \mathbb{F}_2^n \mid S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\right\}. \quad (18)$$

The highest value in the BCT except for point $(0,0)$ is defined as boomerang uniformity [4]:

$$\mathcal{BU}(S) = \max(\beta_S(a,b)). \quad (19)$$

For an S-Box, the smaller the $\mathcal{BU}(S)$, the stronger the resistance to boomerang attack. The $\mathcal{BU}(S)$ value of the proposed S-Box is 20 according to Equations (18) and (19), which indicates that the proposed S-Box has strong resistance to boomerang attack.

4.3. Performance Comparison with Different S-Boxes

In this section, linear approximation probability (LAP), strict avalanche criterion (SAC), nonlinearity (NL), differential approximation probability (DP), and algebraic complexity (AC) are selected as the key cryptanalysis attributes of S-Boxes, and the cryptographic performance of the S-Box proposed in this paper is compared with some recently proposed S-Boxes. The key cryptanalysis results of the different S-Boxes are shown in Table 11. From the table, we can make the following observation: the S-Box generated by the proposed algorithm has good nonlinearity and DP value, and the nonlinear values of SAC, BIC-SAC, and BIC are close to the ideal values. Thus, the proposed algorithm to generated an S-Box can meet the needs of data encryption.

Table 11. Performance comparison of different S-Boxes.

S-Box Method	Nonlinearity			SAC	BIC-NL	LAP	DP	AC
	Min	Max	Average					
Ref. [1]	102	108	104.5	0.498	104.6	0.125	0.048	254
Ref. [16]	104	108	106.8	0.507	103.9	0.140	0.054	254
Ref. [20]	104	110	106	0.499	103.8	0.125	0.039	255
Ref. [48]	104	110	106.5	0.495	103.8	0.141	0.039	255
Ref. [49]	98	110	102	0.493	104.6	0.140	0.046	255
Proposed S-Box	104	112	106.5	0.506	105.6	0.132	0.039	255

5. Conclusions and Discussion

In a summary, we proposed a novel compound chaotic system based on quantum random walks controlled by a hyper-chaotic map. We have evaluated the new system by using some test tools such as Scale index and statistical complexity measures. The results show that the new system has complex dynamic behavior. We have proposed a new PRNG, which passes all the standard statistical tests in NIST SP800-22. Next, we built a new chaotic S-Box generation algorithm based on the PRNG. We have evaluated the performance of the S-Box so-generated by using various cryptographic criteria such as the bit independence criterion (BIC), bijection, strict avalanche criterion (SAC), nonlinearity, differential probability (DP), and linear probability (LP). Test results demonstrated that the S-Box can well meet multiple cryptographic criteria and the new chaotic S-Box generation algorithm is effective.

The results lead us to the following conclusions. By controlling or perturbing the parameters of two types of chaos based on the outputs of one chaotic map, a compound chaotic system can be constructed. Based on the compound chaotic system, designers can easily propose efficient S-Box generation mechanisms that can produce secure S-Boxes. Our proposed compound chaotic system has more complex dynamic behavior. Therefore, based on this dynamical system, it is easy to design modules for cryptosystems such as image encryption algorithms.

In future work, we will take advantage of the proposed compound chaotic system in applications such as image encryption schemes and video authentication.

Author Contributions: Conceptualization, L.Z. and W.Z.; formal analysis and investigation, L.Z. and W.Z.; discussion and suggestion, C.M. and Y.Z.; writing—original draft preparation, C.M. and W.Z.; writing—review and editing, C.M., W.Z. and L.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (No. 12161077); the Natural Science Foundation of Gansu Province (Nos. 23JRRE0737, 22JR11RE189, 22CX8GA075); and the Innovation Fund Project of Tianshui Teachers College (Nos. CXJ2021-04, CXJ2021-01, PTJ2022-01) and Tianshui Natural Science Foundation (No. 2020-FZJHK-9757).

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to the reason that data could have been generated by the algorithm provided in this paper.

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

Abbreviations

The following abbreviations are used in this manuscript:

LAP	Linear approximation probability
SAC	Strict avalanche criterion
CWT	Continuous wavelet transform
DP	Differential approximation probability
SCM	Statistical complexity measure

References

1. 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]
2. Boura, C.; Canteaut, A. On the Boomerang Uniformity of Cryptographic Sboxes. *IACR Trans. Symmetric Cryptol.* **2018**, *2018*, 290–310. [CrossRef]
3. Wagner, D. The Boomerang Attack. In *Fast Software Encryption*; Knudsen, L., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; pp. 156–170.
4. Bao, Z.; Guo, J.; Ling, S.; Sasaki, Y. PEIGEN—A Platform for Evaluation, Implementation, and Generation of S-Boxes. *IACR Trans. Symmetric Cryptol.* **2019**, *2019*, 330–394. [CrossRef]
5. Katiyar, S.; Jeyanthi, N. Pure Dynamic S-Box Construction. *Int. J. Comput.* **2016**, *1*, 42–46.
6. Adams, C.; Tavares, S. Good S-Boxes Are Easy To Find. In *Advances in Cryptology—CRYPTO' 89 Proceedings*; Brassard, G., Ed.; Springer: New York, NY, USA, 1990; pp. 612–615.
7. Hussain, I.; Anees, A.; Al-Maadeed, T.A.; Mustafa, M.T. Construction of S-Box Based on Chaotic Map and Algebraic Structures. *Symmetry* **2019**, *11*, 351. [CrossRef]
8. Rafiq, A.; Khan, M. Construction of new S-Boxes based on triangle groups and its applications in copyright protection. *Multimed. Tools Appl.* **2019**, *78*, 15527–15544. [CrossRef]
9. Artuğer, F.; Özkaynak, F. SBOX-CGA: Substitution box generator based on chaos and genetic algorithm. *Neural Comput. Appl.* **2022**, *34*, 20203–20211. [CrossRef]
10. 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]
11. Masood, F.; Boulila, W.; Alsaeedi, A.; Khan, J.S.; Ahmad, J.; Khan, M.A.; Rehman, S.U. A novel image encryption scheme based on Arnold cat map, Newton–Leipnik system and Logistic Gaussian map. *Multimed. Tools Appl.* **2022**, *81*, 30931–30959. [CrossRef]
12. Sambas, A.; Vaidyanathan, S.; Tlelo-Cuautle, E.; Abd-El-Atty, B.; El-Latif, A.A.A.; Guillén-Fernández, O.; Sukono; Hidayat, Y.; Gundara, G. A 3-D Multi-Stable System with a Peanut-Shaped Equilibrium Curve: Circuit Design, FPGA Realization, and an Application to Image Encryption. *IEEE Access* **2020**, *8*, 137116–137132. [CrossRef]
13. Hua, Z.; Zhu, Z.; Chen, Y.; Li, Y. Color image encryption using orthogonal Latin squares and a new 2D chaotic system. *Nonlinear Dyn.* **2021**, *104*, 4505–4522. [CrossRef]
14. Chai, X.; Fu, J.; Gan, Z.; Lu, Y.; Zhang, Y.; Han, D. Exploiting Semi-Tensor Product Compressed Sensing and Hybrid Cloud for Secure Medical Image Transmission. *IEEE Internet Things J.* **2023**, *10*, 7380–7392. [CrossRef]
15. Song, W.; Fu, C.; Zheng, Y.; Tie, M.; Liu, J.; Chen, J. A parallel image encryption algorithm using intra bitplane scrambling. *Math. Comput. Simul.* **2023**, *204*, 71–88. [CrossRef]

16. Zahid, A.H.; Arshad, M.J. An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping. *Symmetry* **2019**, *11*, 437. [CrossRef]
17. Zheng, J.; Zeng, Q. An image encryption algorithm using a dynamic S-Box and chaotic maps. *Appl. Intell.* **2022**, *52*, 15703–15717. [CrossRef]
18. Bin Faheem, Z.; Ali, A.; Khan, M.A.; Ul-Haq, M.E.; Ahmad, W. Highly dispersive substitution box (S-Box) design using chaos. *ETRI J.* **2020**, *42*, 619–632. [CrossRef]
19. Zhu, H.; Tong, X.; Wang, Z.; Ma, J. A novel method of dynamic S-Box design based on combined chaotic map and fitness function. *Multimed. Tools Appl.* **2020**, *79*, 12329–12347. [CrossRef]
20. Lu, Q.; Zhu, C.; Wang, G. A Novel S-Box Design Algorithm Based on a New Compound Chaotic System. *Entropy* **2019**, *21*, 1004. [CrossRef]
21. Zhao, W.; Chang, Z.; Ma, C.; Shen, Z. A Pseudorandom Number Generator Based on the Chaotic Map and Quantum Random Walks. *Entropy* **2023**, *25*, 166. [CrossRef]
22. Sambas, A.; Vaidyanathan, S.; Zhang, S.; Abd El-Latif, A.A.; Mohamed, M.A.; Abd-El-Atty, B. Multistability Analysis and MultiSim Simulation of a 12-Term Double-Scroll Hyperchaos System with Three Nonlinear Terms, Bursting Oscillations and Its Cryptographic Applications. In *Cybersecurity: A New Approach Using Chaotic Systems*; Springer International Publishing: Cham, Switzerland, 2022; pp. 221–235. [CrossRef]
23. Ahmad, M.; Alam, M.Z.; Ansari, S.; Lambić, D.; AlSharari, H.D. Cryptanalysis of an image encryption algorithm based on PWLCM and inertial delayed neural network. *J. Intell. Fuzzy Syst.* **2018**, *34*, 1323–1332. [CrossRef]
24. 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]
25. Singh, J.P.; Roy, B. The nature of Lyapunov exponents is (+, +, −, −). Is it a hyperchaotic system? *Chaos Solitons Fractals* **2016**, *92*, 73–85. [CrossRef]
26. Guo, F.; Xu, L. *Applications of Chaos Theory to Cryptography*, 1st ed.; Beijing Institute of Technology Press: Beijing, China, 2015.
27. Venegas-Andraca, S.E. Quantum walks: A comprehensive review. *Quantum Inf. Process.* **2012**, *11*, 1015–1106. [CrossRef]
28. Aharonov, D.; Ambainis, A.; Kempe, J.; Vazirani, U. Quantum Walks on Graphs. In Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, Hersonissos, Greece, 6–8 July 2001; Association for Computing Machinery: New York, NY, USA, 2001; STOC '01, pp. 50–59. [CrossRef]
29. Yang, Y.G.; Zhao, Q.Q. Novel pseudo-random number generator based on quantum random walks. *Sci. Rep.* **2016**, *6*, 20362. [CrossRef] [PubMed]
30. Benítez, R.; Bolós, V.J.; Ramírez, M.E. A wavelet-based tool for studying non-periodicity. *Comput. Math. Appl.* **2010**, *60*, 634–641. [CrossRef]
31. Chandre, C.; Wiggins, S.; Uzer, T. Time–frequency analysis of chaotic systems. *Phys. D Nonlinear Phenom.* **2003**, *181*, 171–196. [CrossRef]
32. Bolós, V.J.; Benítez, R.; Ferrer, R. A New Wavelet Tool to Quantify Non-Periodicity of Non-Stationary Economic Time Series. *Mathematics* **2020**, *8*, 844. [CrossRef]
33. Martin, M.; Plastino, A.; Rosso, O. Statistical complexity and disequilibrium. *Phys. Lett. A* **2003**, *311*, 126–132. [CrossRef]
34. Larrondo, H.A.; González, C.M.; Martín, M.T.; Plastino, A.; Rosso, O.A. Intensive statistical complexity measure of pseudorandom number generators. *Phys. A Stat. Mech. Its Appl.* **2005**, *356*, 133–138. [CrossRef]
35. Akhshani, A.; Akhavan, A.; Mobaraki, A.; Lim, S.C.; Hassan, Z. Pseudo random number generator based on quantum chaotic map. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 101–111. [CrossRef]
36. Bassham, L.E.; Rukhin, A.L.; Soto, J.; Nechvatal, J.R.; Smid, M.E.; Barker, E.B.; Leigh, S.D.; Levenson, M.; Vangel, M.; Banks, D.L.; et al. SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Technical Report; NIST: Gaithersburg, MD, USA, 2010.
37. Biham, E.; Shamir, A. Differential Cryptanalysis of Feal and N-Hash. In *Advances in Cryptology—EUROCRYPT '91*; Davies, D.W., Ed.; Springer: Berlin/Heidelberg, Germany, 1991; pp. 1–16.
38. Jakobsen, T. Attacks on block ciphers of low algebraic degree. *J. Cryptol.* **2001**, *14*, 197–210. [CrossRef]
39. Carlet, C. Vectorial Boolean Functions for Cryptography. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*; Encyclopedia of Mathematics and its Applications; Cambridge University Press: Cambridge, UK, 2010; pp. 398–470. [CrossRef]
40. Canteaut, A.; Carlet, C.; Charpin, P.; Fontaine, C. Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. In *Advances in Cryptology—EUROCRYPT 2000*; Preneel, B., Ed.; Springer: Berlin/Heidelberg, Germany, 2000; pp. 507–522.
41. Webster, A.F.; Tavares, S.E. On the Design of S-Boxes. In *Advances in Cryptology — CRYPTO '85 Proceedings*; Williams, H.C., Ed.; Springer: Berlin/Heidelberg, Germany, 1986; pp. 523–534.
42. Adams, C.; Tavares, S. The structured design of cryptographically good s-boxes. *J. Cryptol.* **1990**, *3*, 27–41. [CrossRef]
43. Hussain, I.; Shah, T.; Mahmood, H.; Gondal, M.A. Construction of S8 Liu J S-Boxes and their applications. *Comput. Math. Appl.* **2012**, *64*, 2450–2458. [CrossRef]
44. Nyberg, K.; Knudsen, L.R. Provable Security Against Differential Cryptanalysis. In *Advances in Cryptology—CRYPTO' 92*; Brickell, E.F., Ed.; Springer: Berlin/Heidelberg, Germany, 1993; pp. 566–574.

45. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
46. Matsui, M. Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology—EUROCRYPT '93*; Helleseth, T., Ed.; Springer: Berlin/Heidelberg, Germany, 1994; pp. 386–397.
47. Cid, C.; Huang, T.; Peyrin, T.; Sasaki, Y.; Song, L. Boomerang Connectivity Table: A New Cryptanalysis Tool. In *Advances in Cryptology—EUROCRYPT 2018*; Nielsen, J.B., Rijmen, V., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 683–714.
48. Wang, X.; Ünal, Ç.; Kaçar, S.; Akgul, A.; Pham, V.T.; Jafari, S.; Alsaadi, F.E.; Nguyen, X.Q. S-Box Based Image Encryption Application Using a Chaotic System without Equilibrium. *Appl. Sci.* **2019**, *9*, 781. [CrossRef]
49. Ali, T.S.; Ali, R. A novel color image encryption scheme based on a new dynamic compound chaotic map and S-Box. *Multimed. Tools Appl.* **2022**, *81*, 20585–20609. [CrossRef]