electronics

MDPI

Article

A Novel S-Box Dynamic Design Based on Nonlinear-Transform of 1D Chaotic Maps

Wenhao Yan and Qun Ding *

Electronic Engineering College, Heilongjiang University, Harbin 150080, China; 1202873@s.hlju.edu.cn
* Correspondence: qunding@aliyun.com

Abstract: In this paper, a method to enhance the dynamic characteristics of one-dimension (1D) chaotic maps is first presented. Linear combinations and nonlinear transform based on existing chaotic systems (LNECS) are introduced. Then, a numerical chaotic map (LCLS), based on Logistic map and Sine map, is given. Through the analysis of a bifurcation diagram, Lyapunov exponent (LE), and Sample entropy (SE), we can see that CLS has overcome the shortcomings of a low-dimensional chaotic system and can be used in the field of cryptology. In addition, the construction of eight functions is designed to obtain an S-box. Finally, five security criteria of the S-box are shown, which indicate the S-box based on the proposed in this paper has strong encryption characteristics. The research of this paper is helpful for the development of cryptography study such as dynamic construction methods based on chaotic systems.

Keywords: chaotic system; cryptography; S-box; sample entropy (SE)

check for updates

Citation: Yan, W.; Ding, Q. A Novel S-Box Dynamic Design Based on Nonlinear-Transform of 1D Chaotic Maps. *Electronics* **2021**, *10*, 1313. https://doi.org/10.3390/electronics10111313

Academic Editors: Gennady E. Veselov, Lilia Sabantina and Anton Pljonkin

Received: 6 May 2021
Accepted: 26 May 2021
Published: 30 May 2021

1. Introduction

Substitution box (S-box) is an important nonlinear module, used to substitute and permutate elements in block cipher, which ensures the security of the block cipher to a large extent. From the point of view of mathematics, an $n \times n$ S-box can be regarded as a nonlinear function $S : F_2^n \to F_2^n$, where F_2^n stands for the vector space of the n-tuple elemental form $GF(2)$, i.e., $\{0, 1\}^n$. A secure block cipher cryptosystem should possess confusion and diffusion to resist some known attacks, including linear analysis, differential analysis, the known plaintext attack, and so on. Chaos precisely has some characteristic sensitivity to initial values, intrinsic randomness, ergodicity, and nonlinearity properties, which can make it suitable to protect digital images. Some work such as information hiding, watermarking, and image encryption is done to protect the security of digital images [1–3].

In recent years, many S-boxes based on the continuous-time chaotic system have been proposed by scholars. The output value generated by a chaotic system can be converted through a series of processes into a number between 0 and $2^n - 1$. Then, we can put the numbers directly into an $n \times n$ table in order. The S-box construction based on the Lorenz system was proposed by Ozkaynak and Ozer [4]. In order to improve the cryptography characteristics, several S-boxes were constructed using chaotic systems with more complex dynamics behaviors. Ozkaynak et.al [5] proposed S-boxes based on time-delay chaotic systems. The S-box constructions based on fractional-order chaos were presented [6–8]. The S-box constructions based on hyperchaotic systems have been shown [9,10]. Besides, there are many other methods to generate S-boxes based on chaos theory. However, the above-mentioned continuous time chaotic system needs to be discretized in a simulation experiment because the computer does not support the continuous nature of a chaotic system. Thus, an increasing number of the S-box construction methods based on discrete-time have been proposed [11–16]. Iqtadar [17] proposed an S-box construction method based on a Logistic system, and dynamic S-box construction methods based on chaotic systems were proposed [18,19]. Then, an S-box construction method, based on the combined 2D Baker system and Chebyshev system, was proposed in [20]. A low-dimensional chaotic system is easier to be used in the actual secure communication due to its simple form, fast encryption speed, and easier implementation in hardware and software compared with a hyperchaotic system [21,22]. However, the low dimensional discrete-time chaotic map shares some common potential dangers: weak parameter space, short periodic behavior, blank window, and uneven output distribution, which limit its application in the construction methods of the S-box.

In this paper, nonlinear changes are proposed to enhance the chaotic properties of low-dimensional chaotic systems. In order to overcome the above weakness of the low dimensional discrete-time chaotic map, linear combinations of the output values of existing chaotic systems are proposed to enhance the chaotic characteristics in [23–27]. Because the linear combination cannot change the output value of the original system, only the linear combination of these values, the performance of the presented system is not very good. In order to furthermore enhance its chaotic characteristics, we use linear coupling first and then nonlinear transform based on existing chaotic systems (LNECS). A numerical chaotic map (CLS), based on a Logistic map and Sine map, is given. Through the analysis of the bifurcation diagram, LE and SE, we can see that CLS has overcome the shortcomings of the low-dimensional chaotic system and can be used in the field of cryptology. Another innovation in this article is the construction of eight functions designed to convert a decimal number into eight binary numbers. Turning an 8-bit binary number back into a decimal number is exactly between 0 and 255. Then, the 256 numbers can be converted to an S-box by line, whose security analysis shows that it can resist the well-known attacks and cryptanalysis. The main contributions and novelty of this paper are summarized as follows.

1. The linear coupling followed by the nonlinear transform based on existing chaotic systems (LNECS) was proposed. A numerical chaotic map (CLS) was generated to indicate the feasibility of the methods.
2. We present a novel S-box dynamic design based on CLS produced by LNECS.
3. The simulation and security analysis demonstrate that the S-box can resist well-known attacks and cryptanalysis. Some security criteria, such as nonlinearity and difference uniformity, are better than several other S-boxes based on dynamic design.

The rest of the paper is organized is as follows: a new 1D chaotic map (CLS) is proposed in Section 2, and a bifurcation diagram, LE and SE of CLS are presented. In Section 3, we introduce eight functions in order to transform the output values of CLS into binary numbers and then present the generation method of the S-box. Some basic security analysis of the proposed S-box is presented in Section 4. Finally, some conclusions are drawn in Section 5.

2. Enhanced 1D Discrete Chaotic Maps

This section presents a method for strengthening one-dimensional discrete chaotic systems and analyzes their chaotic properties. To demonstrate the effectiveness of this approach, a chaotic system is generated using an existing chaotic system.

2.1. New Chaotic Map

The method, i.e., strengthening one-dimensional discrete chaotic systems, is designed to solve the drawback of existing chaotic maps with respect to frail chaos and weak dynamic behaviors. In this paper, we propose to increase the characteristics of chaotic systems by nonlinear transforms, such as Sin function, Cos function, modular operation, and the product of linear terms. In this paper, the selected nonlinear function is the Cos function. Two basic one-dimensional chaotic systems are used as a seed map. The final output values are obtained through linear coupling and Cosine transform. The block diagram of constructing the LNECS is shown in Figure 1. Mathematically, LNECS can be defined as follows:

$$x_{k+1} = \cos(\pi(F(\alpha, x_k) + G(\beta, x_k) + \gamma)), \quad (1)$$

where $F(\alpha, x_k)$ and $G(\beta, x_k)$ are two existing chaotic maps, α and β are their system parameters, and γ is a control parameter. If the seed map chooses the Logistic and Sine maps, the new chaotic system, called LCLS, is represented as

$$x_{k+1} = \cos(\pi(4\alpha x_k(1 - x_k) + \beta \sin(\pi x_k) + \gamma)), \tag{2}$$

where system parameters α and β are set as r and $(1 - r)$, and control parameter γ is set as 0.5. The next subsection analyzes CLS from the bifurcation diagram, Lyapunov exponent, and the sample entropy, which indicates CLS exhibits complex chaotic characteristics.

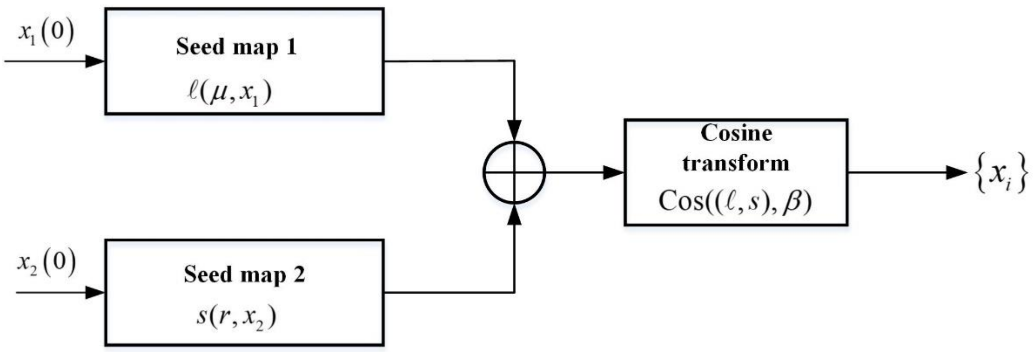
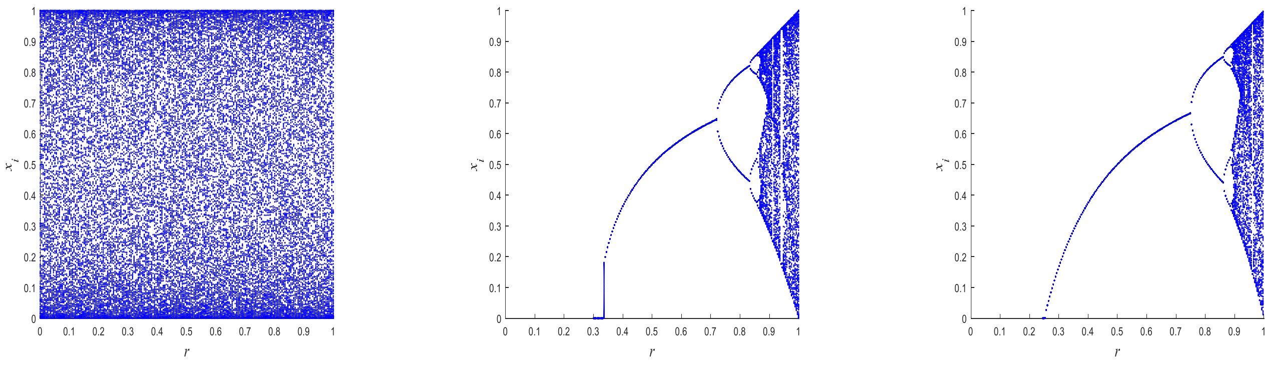


Figure 1. The block diagram of constructing the LCBCS.

2.2. *Bifurcation Diagram*

The bifurcation diagram of a dynamic system shows the points it traversed in phase space. It provides scholars with a visual method to study the properties of chaos. Figure 2 presents the bifurcation diagrams of the CLS, Logistic map, and Sine map. As Figure 2 shows, the Logistic map and Sine map both share fixed or periodic points in most parameter areas. Furthermore, their output values are not uniformly distributed in the phase space. However, the CLS has complex dynamic behaviors in all parameter ranges. Its output values fill the entire phase space, which indicates CLS has complicated dynamic behaviors and its output values are more random.



(**a**) (**b**) (**c**)

Figure 2. The bifurcation diagram of chaos. (**a**) LCLS, (**b**) Sine map, (**c**) Logistic map.

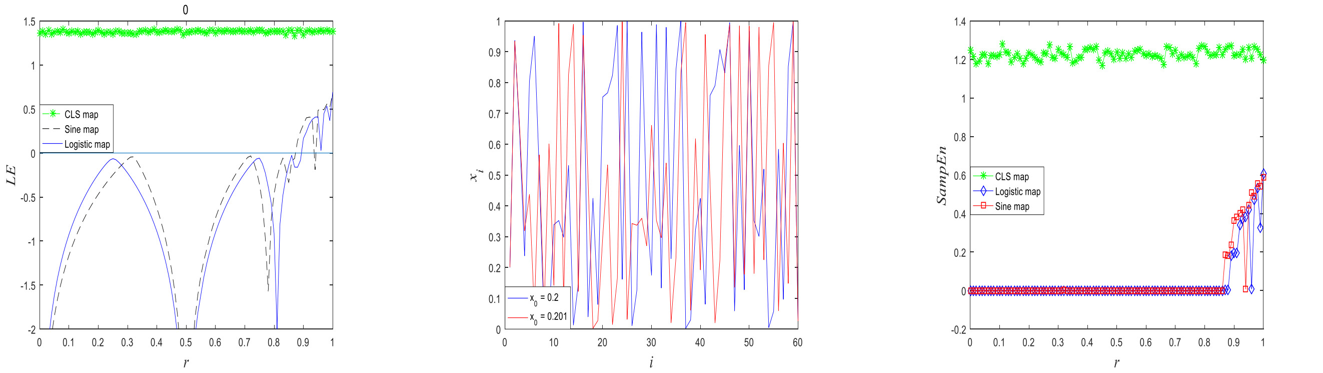
2.3. *Lyapunov Exponent*

In the theory of nonlinear dynamics, the Lyapunov exponent (LE) is an important characteristic to describe the infinitesimal deviation of orbit in phase space. Sensitive dependence on initial conditions is an important characteristic of chaos, that is, two orbits in phase space that are close to each other will separate exponentially as time goes on. LE can be presented using Definition 1.

Definition 1. *The LE of a 1D discrete-time system $x_{i+1} = F(x_i)$ is mathematically defined by as follows:*

$$\lambda = \lim_{n \to \infty} \left\{ \frac{1}{n} \ln \left| \frac{F^n(x+t) - F^n(x)}{t} \right| \right\}, \tag{3}$$

where t is a small positive number. The LE represents a measure of the mean convergence or mean divergence of similar orbitals in phase space. The larger the value of LE, the faster the phase space trajectory diverges. This means that the more sensitive it is to initial conditions, the more chaotic the system. As Figure 3a shows, the Logistic map and Sine map both have positive LEs for only a few parameters. However, CLS can obtain positive LEs in all parameter ranges, which indicates CLS is a chaotic map with more complex chaotic dynamic behaviors. As can be seen from Figure 3b, the difference in the initial value is 0.01, and the value of the function has changed considerably, indicating that the initial value of this system is very sensitive.



(**a**) (**b**) (**c**)

Figure 3. The LEs and SEs of chaotic maps. (**a**). The LEs of three chaotic maps; (**b**). CLS with different initial values; (**c**) The SEs of three chaotic maps.

2.4. Sample Entropy

At present, the approximate entropy (ApEn) algorithm [28] is widely used to measure the complexity of chaotic sequences. However, since the ApEn algorithm avoids errors by counting the number of templates that match its own data, if the threshold value is small, there will be a large number of template matches, resulting in the phenomenon that the effect of deviation is not obvious, so there is a margin for error. In 2000, a new quantization algorithm of time series complexity, called Sample Entropy (SE), was proposed [29], which is an improved algorithm of ApEn. The meaning of the parameters is consistent with that of ApEn. The algorithm uses the method of removing the comparison with its own template to enlarge the deviation value compared with the threshold value, which can estimate the probability of new data more accurately and reduce the error of ApEn; it is a more accurate algorithm to measure the complexity of time series. The SE of a time series $X = \{x_1,\ x_2,\ \cdots,\ x_n\}$ is defined by as follows:

$$SE(m, r, N) = -\log \frac{A}{B} \tag{4}$$

where m is a given dimension, $r = 0.1 \sim 0.25SD$, SD represents the standard deviation of a time series, and A and B are the number of vectors, which are $d[X_{m+1}(i),\ X_{m+1}(j)\ ] \ < \ r$ and $d[X_m(i),\ X_m(j)\ ] \ < \ r$, respectively. Figure 3c compares the SEs of chaotic maps. It can be observed that CLS has much larger SEs than the Logistic map and Sine map, which indicates CLS has more complex output sequences. In the next section, we will construct an S-box from the sequence generated by the chaotic system.

3. S-Box Dynamic Construction Method Based on CLS

A Boolean variable is a coordinate vector expressed in bits. If a and b represent two Boolean vectors, and the length of input and output of function $f(x): F_2^n \to F_2^m$ is set as n and m, respectively, then the function where $f(a) = b$ is called a Boolean function. An $n \times m$ S-box can be generally expressed as $S : \{0,1\}^n \to \{0,1\}^m$, which is composed of m Boolean functions of n variables, i.e., $S(x) = f_i(x_1,\ x_2, \cdots, x_n),\ i = 1, 2, \cdots,\ m$. For an 8×8 S-box, the eight functions based on CLS are defined as follows:

$$f_i(x) = \sum_{y=1}^{2^i-1} \left[(-1)^{y-1} \left(\varpi_{\frac{y}{2^i}}(x_i) \right) \right],\ i = 1,\ 2,\ \cdots,\ 8 \tag{5}$$

where

$$\varpi_{\frac{y}{2^i}}(x_i) = \begin{cases} 0,\ if\ x_i < \frac{y}{2^i}, \\ 1,\ if\ x_i \geq \frac{y}{2^i}. \end{cases} \tag{6}$$

The output of the eight functions represents eight binary bits for the decimal value of some element of the S-box. The value of x_i is taken from the output sequence of CLS. For the value of CLS at any time, the output values for eight functions will be calculated. Thus, the output values of eight functions are used to construct one element of the S-box. The detailed algorithm of constructing the S-box is described as Algorithm 1:

Algorithm 1 The construction method of the S-box

```
Input: The initial value $x(0)$ of CLS
Output: An S-box
1 Select parameter $r$ and the initial conditions $x(0)$ of CLS.
2 Iterate $k$ times, where $k \geq 900$, to obtain the value of CLS.
3 The value $x(k)$ is set as the input of eight function $f_i(x)$, and eight binary bits are converted to
  a decimal number between 0 and 255.
4 Define an empty sequence $S$ with 256
  elements. If two elements of $S$ are equal, discard the element with larger index.
5 Translate Sequence $S$ into an $8 \times 8$ table, i.e., an S-box is obtained.
```

The proposed algorithm for constructing the S-box is graphically illustrated in Figure 4. Further, an example of constructing the S-box is given. The process of the construction of the S-box is illustrated step by step in Table 1. The first column of the table k represents the given iteration number. Each iteration of the system produces one output value, and it is as fed as input for the eight functions. The outputs of the eight functions are shown in columns 2 through 9 of the table. The conversion of 8-bit binaries to decimal numbers is shown in the last column. Finally, the constructed S-box from the proposed one is shown in Table 2.

Table 1. The construction process of the S-box from the proposed one.

n	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	(0 255)
1	0	0	1	0	0	1	1	0	38
2	1	1	1	0	1	1	1	1	239
3	1	1	1	1	0	0	1	0	242
⋮	⋮	⋮	⋮		⋮	⋮	⋮	⋮	⋮
786	1	1	0	1	0	1	0	0	212

Table 2. The constructed S-box from the proposed one.

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

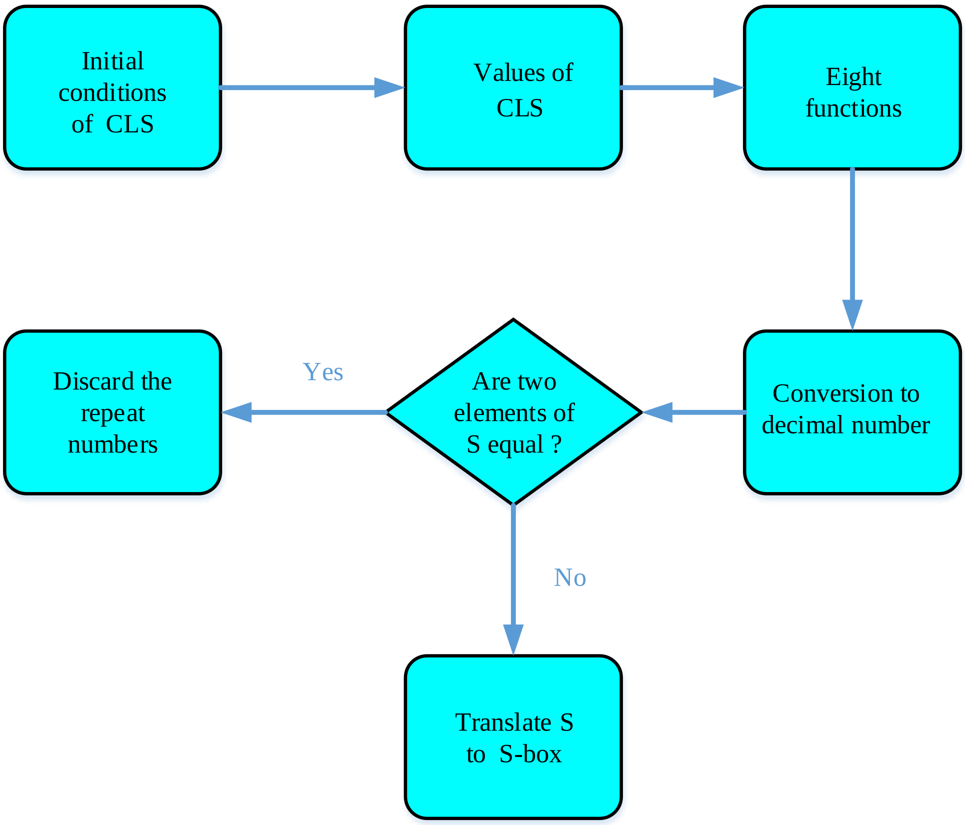

Initial conditions of CLS
Values of CLS
Eight functions
Conversion to decimal number
Are two elements of S equal ?
Yes
Discard the repeat numbers
No
Translate S to S-box

Figure 4. The proposed algorithm for constructing the S-box.

4. Security Analysis of the Proposed S-box

In order to test the superiority of the proposed S-box compared with other existing S-boxes, we test five basic criteria: the bijective property, nonlinearity, difference uniformity, strict avalanche criterion (SAC), and output bits independence criterion (BIC). These criteria are widely used to evaluate the performance of an S-box.

4.1. Bijective Property

In general, S-boxes are invertible mappings. Therefore, an S-box is bijective if it satisfies the following formula [30]:

$$wt(\sum_{i=1}^{n} a_i f_i(x)) = 2^{n-1}, \tag{7}$$

where $a_i = \{0, 1\}$, $(a_1, a_2, \cdots, a_n) \neq (0, 0, \cdots, 0)$, $f_i(x)$ is the Boolean function of the components of the S-box and $wt(\ )$ is the hamming weight. In this paper, there are 255 linear combinations of 8 Boolean functions of the S-box. By calculating the hamming weight of the XOR value of the vectors in each combination, it can be found that the results are all 128, so the S-box satisfies bijective property.

4.2. Nonlinearity

Nonlinearity is a measure of the ability of a cryptographic function to resist linear attacks [31,32]. The greater the nonlinearity of the function, the stronger the ability to resist linear and correlation attacks. For the convenience of calculation, we give the definition of nonlinearity based on the Walsh spectrum. The nonlinearity of the n-bits Boolean function $f(x)$ is defined by the following formula:

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\omega \in F_2^n} \left| S_{(f)}(\omega) \right|, \tag{8}$$

where $S_f(\omega)$ is the Walsh cyclic spectrum of $f(x)$. The Walsh cyclic spectrum of $f(x)$ is described by the following formula:

$$S_{(f)}(\omega) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus x \cdot \omega}, \tag{9}$$

where $x \cdot \omega$ denotes the dot product of the vector x with ω and $\omega \in F_2^n$. The nonlinearity of each Boolean function and the mean value of nonlinearity are computed, whose results are shown in Table 3, which shows the nonlinearity performance of other existing S-boxes. It is easy to see that the nonlinearity of the S-box proposed in this paper is better than that of other S-boxes.

Table 3. The nonlinearity performance of the S-boxes.

Methods	1	2	3	4	5	6	7	8	Mean
Method in [33]	101	104	107	107	106	101	106	106	104.50
Method in [34]	108	106	102	102	104	106	108	100	104.50
Method in [35]	108	104	106	106	102	98	104	108	104.00
Method in [36]	106	106	106	104	108	102	106	104	105.25
Method in [37]	100	103	104	104	105	105	106	109	104.50
The proposed	104	106	106	106	108	106	104	104	105.50

4.3. Difference Uniformity

Differential analysis is one of the effective attacks on cryptographic algorithms. In order to measure the ability of a cryptographic algorithm to resist differential analysis, the concept of differential evenness is introduced. Differential analysis attacks mainly through the imbalance of input/output XOR distribution. If an S-box has an equal probability output/input XOR distribution, it can effectively resist differential attacks. The smaller the maximum value of the S-box output and output differential distribution, the stronger the ability to resist differential analysis. The difference uniformity of some S-boxes can be described as follows:

$$\delta = \frac{1}{2^n} \max_{\alpha \in F_2^n,\ \alpha \neq 0} \max_{\beta \in F_2^n} |\{x \in F_2^n : S(x+\alpha) - S(x) = \beta\}|. \tag{10}$$

Differential probability for a given function can be defined by:

$$DP_f = \max_{\Delta x \neq 0, \Delta y} (\#\{x \in X | f(x) \oplus f(x + \Delta x) = \Delta y\}), \tag{11}$$

where X is the set of all possible input value. DP_f represents the maximum probability that the output difference is Δy when the input difference is Δx. The XOR distribution of the proposed S-box is shown in Table 4. The maximum DP value of the proposed S-box is 10, which indicates it can resist differential attacks.

Table 4. The output/input XOR distribution of the proposed S-box.

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
8	8	6	6	8	6	6	8	6	6	6	8	8	6	6	8
8	6	6	8	8	10	8	8	6	8	6	6	6	6	8	6
6	8	8	6	6	6	6	8	8	8	6	8	6	8	8	8
8	8	8	6	8	8	6	6	6	8	6	6	8	8	6	6
6	6	6	6	10	8	6	6	8	4	6	8	8	6	6	6
8	8	6	8	8	8	6	6	6	6	6	10	6	6	6	8
6	8	10	6	8	6	6	4	6	6	6	8	6	8	8	8
8	6	6	6	6	6	8	4	8	6	6	8	8	8	6	8
10	8	6	8	6	6	6	8	6	6	6	6	6	8	8	6
6	8	8	6	6	6	8	8	6	8	6	8	8	6	6	6
8	4	6	8	8	8	6	6	10	6	6	6	8	6	8	10
6	8	8	8	8	6	6	6	6	6	6	6	6	4	10	6
8	8	6	6	6	6	8	8	6	6	6	8	6	4	8	4
8	6	8	6	6	8	8	6	8	4	6	6	6	6	6	6
6	8	6	6	8	8	6	8	6	8	6	8	8	8	8	8
8	8	6	8	8	6	8	6	6	8	6	6	8	6	6	6

4.4. Strict Avalanche Criterion (SAC)

The strict avalanche criterion (SAC) combining completeness and the avalanche effect was introduced by Webster and Tavares [38]. SAC mainly analyzes changes in the behavior of ciphertext output bits. Suppose an S-box meets SAC, only half of one bit of the input change will cause the change in the output bits, namely, a change in the probability of each output bit by 0.5. The dependence matrix is used to obtain the SAC values of an S-box. If an S-box nearly satisfies SAC, each element of the dependence matrix is close to 0.5. The independence matrix of the proposed S-box is represented in Table 5. As Table 5 shows, these values are near to half of the better and optimum values.

Table 5. The independence matrix of the proposed S-box.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
00000001	0.51234	0.52694	0.46546	0.48694	0.50698	0.49873	0.52164	0.48961
00000010	0.55698	0.5	0.51269	0.50249	0.51364	0.49567	0.54983	0.51465
00000100	0.49825	0.47658	0.51693	0.53657	0.48238	0.46951	0.53267	0.52641
00001000	0.48956	0.47895	0.48976	0.5	0.52943	0.52462	0.51346	0.53941
00010000	0.52431	0.5	0.54132	0.48629	0.48762	0.51643	0.51649	0.53614
00100000	0.53841	0.49561	0.47561	0.50964	0.5	0.51274	0.53146	0.51236
01000000	0.5	0.47325	0.49167	0.48761	0.52498	0.54951	0.47351	0.49351
10000000	0.47891	0.46982	0.52149	0.48164	0.5	0.46924	0.53984	0.516984

4.5. Output Bits Independence Criterion (BIC)

The output bits independence criterion (BIC) was presented in the literature [39]. The Boolean function for any two outputs of an S-box $f_i(x)$ and $f_j(x)$ $(i \neq j,\ i \geq 1,\ j \leq n)$, if the S-box satisfies BIC- nonlinearity and $f_i(x) \oplus f_j(x)$, should satisfy the nonlinearity property; if the S-box satisfies BIC- SAC, $f_i(x) \oplus f_j(x)$ should satisfy SAC. The results obtained from the proposed S-box are represented in Tables 6 and 7. As shown in Table 5, the mean values of nonlinearity are greater than 101, and the average value of the dependence matrix for BIC is near 0.5. Therefore, the proposed S-box shares have a good BIC property.

Table 6. BIC-nonlinearity of the proposed S-box.

	106	102	100	106	104	102	100
104		108	104	102	100	104	104
102	104		106	104	102	106	102
104	102	104		104	102	108	106
106	106	106	104		102	106	104
102	100	106	106	102		104	106
100	104	104	104	104	100		104
106	104	102	104	100	100	102	

Table 7. BIC-SAC of the proposed S-box.

	0.50786	0.51052	0.52364	0.51068	0.49620	0.49562	0.52364
0.50264		0.51607	0.50651	0.49014	0.47587	0.50369	0.51564
0.47815	0.49654		0.49651	0.47982	0.52991	0.51201	0.51694
0.51496	0.48833	0.47694		0.51923	0.50540	0.51635	0.49561
0.50471	0.51374	0.52549	0.49563		0.50684	0.52469	0.48695
0.49512	0.48761	0.48304	0.51644	0.50764		0.49563	0.51984
0.50786	0.47640	0.52410	0.49741	0.51403	0.51916		0.49651
0.48466	0.49562	0.51463	0.48547	0.51492	0.48954	0.48691	

As can be seen from Table 8, the results of the security analysis demonstrate that the proposed one is better than the related work in terms of security and performance. In view of the above security indicators, we can conclude that the S-box based on the proposed method in this paper has strong encryption characteristics, which is helpful for the development of cryptography studies such as dynamic construction methods based on chaotic systems.

Table 8. The comparison results between the proposed and other existing methods.

S-box	Nonlinearity			SAC	DP	BIC-NL	BIC-SAC
	Min.	**Max.**	**Avg.**	**Avg.**			
Method in [33]	100	108	104.50	0.4978	12	103.64	0.5012
Method in [34]	101	107	104.50	0.4963	10	103.29	0.4938
Method in [35]	102	108	105.25	0.4956	10	1032.80	0.4996
Method in [36]	84	106	100.00	0.4812	16	101.93	0.4967
Method in [37]	96	106	103.20	0.5151	44	103.07	0.4864
The proposed	104	108	105.50	0.5065	10	103.57	0.5031

5. Conclusions

In this paper, we have presented the generation method S-box based on CLS. First, a Logistic map and Sine map are linearly combined to enhance chaotic behaviors. Furthermore, the chaotic characteristics of the system are further enhanced by the nonlinear variation of the linear combination of the values. Through the analysis of the Bifurcation diagram, LE and SE, we can see that CLS has overcome the shortcomings of the low-dimensional chaotic system and can be used in the field of cryptology. In addition, we conducted a series of security analysis after obtaining the S-box, whose results showed that it can resist well-known attacks and cryptanalysis. In later work, we will use FPGA to achieve this S-box and the optimized algorithm to obtain an S-box with better performance.

Author Contributions: W.Y. was in charge of methodology, software, validation and writing—original draft preparation. Project administration and supervision were done by Q.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China, under grant number 61471158.

Data Availability Statement: All results and data obtained can be found in open access publications.

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

References

1. Dragoi, A.V.; Colutc, D. On local prediction based reversible watermarking. *IEEE Trans. Image Process.* **2015**, *24*, 1244–1246. [CrossRef]
2. Lin, Y.T.; Wang, C.M.; Chen, W.S.; Lin, F.P.; Lin, W. A novel data hiding algorithm for high dynamical range images. *IEEE Trans. Multimed.* **2017**, *19*, 196–211. [CrossRef]
3. Zhou, Y.C.; Bao, L.; Chen, C.L.P. A new 1D chaotic map for image encryption. *Signal Process.* **2014**, *97*, 3039–3052. [CrossRef]
4. Ozkaynak., F.; Ozer, A.B. A method for designing strong S-Boxes based on chaotic systems. *Phys. Lett. A* **2010**, *374*, 3733–3738. [CrossRef]
5. Ozkaynak, F.; Yavuz, S. Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dyn.* **2013**, *74*, 551–557. [CrossRef]
6. Belazi, A.; Abd El-Latif, A.A.; Diaconu, A.; Rhouma, R.; Belghith, S. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Opt. Lasers Eng.* **2017**, *88*, 37–50. [CrossRef]
7. Li, C.; Lin, D.; Lü, J.; Hao, F. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. *IEEE Multimed.* **2018**, *25*, 46–56. [CrossRef]
8. Islam, F.U.; Liu, G. Designing S-Box Based on 4D-4 Wing Hyperchaotic System. *3D Res.* **2017**, *8*, 9. [CrossRef]
9. Liu, G.; Yang, W.; Liu, W.; Da, Y. Designing S-boxes based on 3-D four-wing autonomous chaotic system. *Nonlinear Dyn.* **2015**, *82*, 1867–1877. [CrossRef]
10. Dawson, M.H.; Tavares, S.E. An expanded set of design criteria for substitution boxes and their use in strengthening DES-like cryptosystems. In Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing Conference, Victoria, BC, Canada, 9–10 May 1991; Volume 1, pp. 191–195.
11. Biham, E.; Shamir, A. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptol.* **1991**, *4*, 3–72. [CrossRef]
12. Hussain, I.; Shah, T.; Gondal, M. Efficient method for designing chaotic S-boxes based on generalized Baker's map and TDERC chaotic sequence. *Nonlinear Dyn.* **2013**, *74*, 271–275. [CrossRef]
13. Khan, M.; Shah, T.; Batool, S. A new implementation of chaotic S-boxes in CAPTCHA. *Signal Image Video Process.* **2016**, *10*, 293–300. [CrossRef]
14. Hussain, I.; Shah, T.; Gondal, M. A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. *Nonlinear Dyn.* **2012**, *70*, 1791–1794. [CrossRef]
15. Alzaidi, A.A.; Ahmad, M.; Doja, M.N.; Al Solami, E.; Beg, M.M.S. A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes. *IEEE Access* **2018**, *6*, 55405–55418. [CrossRef]
16. Hussain, I. True-chaotic substitution box based on Boolean functions. *Eur. Phys. J. Plus* **2020**, *135*, 663. [CrossRef]
17. Malik, M.S.M.; Ali, A.; Khan, M.A.; Ehatisham-ul-Haq, M.; Mehmood, S.N.; Rehman, M.; Ahmad, W. Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. *IEEE Access* **2020**, *8*, 35682–35695. [CrossRef]
18. Wang, Y.; Wong, K.W.; Liao, X.; Xiang, T. A block cipher with dynamic S-boxes based on tent map. *Commun. Nonlinear Sci. Numer. Simul.* **2009**, *14*, 3089–3099. [CrossRef]
19. Chen, G. A novel heuristic method for obtaining S-boxes. *Chaos Solitons Fractals* **2008**, *36*, 1028–1036. [CrossRef]
20. Pljonkin, A.; Petrov, D.; Sabantina, L.; Dakhkilgova, K. Nonclassical Attack on a Quantum Key Distribution System. *Entropy* **2021**, *23*, 509. [CrossRef]
21. Pljonkin, A.; Rumyantsev, K.; Singh, P.K. Synchronization in Quantum Key Distribution Systems. *Cryptography* **2017**, *1*, 18. [CrossRef]
22. Yuan, H.; Luo, L.; Wang, Y. An S-box construction algorithm based on spatiotemporal chaos. In Proceedings of the 2010 International Conference on Communications and Mobile Computing, Shenzhen, China, 12–14 April 2010; Volume 1, pp. 61–65.
23. Pisarchik, A.N.; Flores-Carmona, N.J.; Carpio-Valadez, M. Encryption and decryption of images with chaotic map lattices. *Chaos Interdiscip. J. Nonlinear Sci.* **2006**, *16*, 033118. [CrossRef]

24. Wang, S.; Hu, G. Coupled map lattice based hash function with collision resistance in single-iteration computation. *Inf. Sci.* **2012**, *195*, 266–276. [CrossRef]
25. Lu, L.; Li, Y.; Sun, A. Parameter identification and chaos synchronization for uncertain coupled map lattices. *Nonlinear Dyn.* **2013**, *73*, 2111–2117. [CrossRef]
26. Liu, C.Y.; Ding, L.N.; Ding, Q. Research about the characteristic of chaotic systems based on multi-scale entropy. *Entropy* **2019**, *12*, 663. [CrossRef]
27. Pincus, S.M. Approximate entropy as a measure of system complexity. *Proc. Natl. Acad. Sci. USA* **1991**, *88*, 2297–2301. [CrossRef]
28. Richman, J.S.; Moorman, J.R. Physiological time-series analysis using approximate entropy and sample entropy. *Am. J. Physiol. Heart Circ. Physiol.* **2000**, *278*, 2039–2049. [CrossRef] [PubMed]
29. Zuras, D.; Cowlishaw, M.F.; Aiken, A.; Applegate, M.; Bailey, D.; Bass, S.; Bhandarkar, D.; Bhat, M.; Bindel, D.; Boldo, S.; et al. IEEE standard for floating-point arithmetic. In *IEEE Std754-2008*; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2008; pp. 1–70.
30. Jakimoski, G.; Kocarev, L. Chaos and cryptography: Block encryption ciphers based on chaotic maps. *IEEE Trans. Circuits Syst. I* **2001**, *48*, 163–169. [CrossRef]
31. Chen, G.; Chen, Y.; Liao, X. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. *Chaos Solitons Fractals* **2017**, *31*, 571–579. [CrossRef]
32. Alkhaldi, H.; Hussain, I.M.; Gondal, A. A novel design for the construction of safe S-boxes based on TDERC sequence. *Alex. Eng. J.* **2015**, *54*, 65–69. [CrossRef]
33. Khan, M.; Shah, T. An efficient construction of substitution box with fractional chaotic system. *Signal Image Video Process.* **2013**, *9*, 1335–1338. [CrossRef]
34. Ozkaynak, F.; Celik, V.; Ozer, 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. Belazi, A.; Khan, M.; El-Latif, A.A.A.; Belghith, S. Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption. *Nonlinear Dyn.* **2017**, *87*, 337–361. [CrossRef]
36. 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.* **2016**, *27*, 677–685. [CrossRef]
37. Khan, M.; Asghar, Z. A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S_8 permutation. *Neural Comput. Appl.* **2018**, *29*, 993–999. [CrossRef]
38. Webster, A.; Tavares, S. On the design of S-boxes. In *Advances in Cryptology: Proceedings of CRYPTO '85. Lecture Notes in Computer Science*; Springer: Berlin, Germany, 1986; pp. 523–534.
39. Cusick, T.; Stanica, P. *Cryptographic Boolean Functions and Applications*; Elsevier: Amsterdam, The Netherlands, 2009; pp. 25–32.