S-box: L-L Cascade Chaotic Map and Line Map

Ye Tian[1,2(✉)] and Zhimao Lu[1,3]

[1] College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, People's Republic of China
hsdtianye@l26.com, lzm@dlut.edu.cn
[2] Key Laboratory of Photonic and Electronic Bandgap Materials, Ministry of Education, School of Physics and Electronic Engineering, Harbin Normal University, Harbin 150025, People's Republic of China
[3] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, People's Republic of China

Abstract. Being as an important nonlinear component of block ciphers, Substitution box (S-box) directly affect the security of the cryptographic systems. It is important and difficult to design cryptographically strong S-box that simultaneously meet with multiple cryptographic criteria such as bijection, non-linearity, strict avalanche criterion (SAC), bits independence criterion (BIC), differential probability (DP) and linear probability (LP). To address the issue, an S-box generation approach based on L-L cascade Chaotic Map and Line Map (LLCMLM) is proposed in this paper. L-L cascade chaotic map is used to generate an integer sequence ranging 0–255, and line map is applied to scramble the position of the integer sequence. A series of experiments have been conducted to compare multiple cryptographic criteria of LLCMLM with other algorithms. Simulation results indicate that LLCMLM meets well with the design criteria of the S-box.

Keywords: Substitution box (S-box) · Multiple cryptographic criteria · L-L cascade chaotic map · Line map

1 Introduction

With dynamic developments in the multimedia industry and internet, a large amount of worry has been brought up regarding the security of digital images transmitted over open or stored channels [1–3]. How to protect digital images from being unauthorized handled is becoming extremely crucial. As a branch of modern cryptography, digital images encryption is one of the most useful techniques for images security [4]. Block cipher algorithm is an important research direction in modern cryptography, which has the features of high speed, ease of standardization and software and hardware implementation, therefore it is an effective mean of digital images encryption. In block cipher algorithm, Substitution box (S-box) is the only one nonlinear component of cryptographic algorithm [5], providing the block cipher system with necessary confusing and

Y.-J. Zhang (Ed.): ICIG 2015, Part III, LNCS 9219, pp. 297–309, 2015.
DOI: 10.1007/978-3-319-21969-1_26

scrambling effect against attacks. And its cryptography security features directly determine the safety of the entire cipher performance [1]. Mathematically, a $n \times n$ size of S-box is a non-linear mapping $S : \{0, 1\}^n \rightarrow \{0, 1\}^n$, here $\{0, 1\}^n$ represents the vector spaces of n elements from GF(2), we set $n = 8$ in this paper.

S-box has the following main design criteria [6–8]: Nonlinearity, strict avalanche criterion (SAC), bits independence criterion (BIC), differential probability (DP) and linear probability (LP). The construction methods of S-box can be divided into two categories: one is based on the structure of mathematical functions including logarithmic functions, exponential functions, inverse map of finite fields and power function of finite fields. The other is a random selection method of construction, i.e., selecting better performance S-box from some randomly generated S-boxes [9]. There exist, however, two main disadvantages in these approaches, poor performance S-box and large amounts of computing resources consumption.

In recent years, most secure systems generate the S-box by chaotic scheme as it has some advantages such as ergodicity, pseudo-randomness and unpredictability. Literature [9] proposed a four-steps method of generating chaotic S-box based on discrete Logistic map. Literature [10] improved the work in [9] by means of bit extraction and Baker map. Furthermore, literature [11] proposed an S-box design approach based on iteration discrete chaotic. Literature [12] developed an S-box generating method using three-dimensional chaotic Baker map.

These algorithms have a common characteristic that they have strong S-boxes using the chaotic maps' random distribution property. However, the performance gap between the some of these chaotic S-boxes and classic ones still exists, for example, few chaos based S-boxes can achieve the high performance like the one used in advanced encryption standard (AES) [13].

To tackle this issue, researchers have attempted to design the S-boxes in the way of incorporating the advantages of the chaotic S-boxes and the genetic algorithms [13]. For example, literature [14] developed a new way of constructing S-box, that is combing chaotic maps and simulated annealing, thus resulting good performance. However, such schemes choose only one criterion, for example, the nonlinearity, for optimization in the process of designing the S-boxes [13].

Later, some literatures applied the chaotic system to the construction of S-boxes. Literature [15] used the continuous-time Lorenz system to design S-box. Literature [16] proposed to generate S-box by means of Rössler and Lorenz chaotic system. Moreover, Literature [17] presented an S-box design method based on Duffing chaotic system. For more S-box design approaches base on chaotic system, readers can refer to literatures [18–20].

Although we can obtain some S-boxes of good cryptography performance using the chaotic model, the non-linearity and differential uniformity of these S-boxes are still not ideal. And the generation of some superior performance S-boxes still has some difficulties. For example, output sequence constructed by the single chaotic system can not reach the theoretical random completely, due to the limited precision of computer, thus resulting the cyclical issues of the pseudo-random sequence [21].

Researchers have shown that multi-chaotic system and more complex chaotic systems can be applied to enhance security and produce pseudo-random sequences of excellent statistical properties. In this paper, we propose an S-box generation approach based on L-L cascade Chaotic Map and Line Map (LLCMLM). L-L cascade chaotic map is used to construct an integer sequence ranging 0–255, and line map is applied to scramble the position of the integer sequence. The experimental results show that LLCMLM meets well with the design criteria of S-box.

2 Cascade Chaotic Map and Line Map

2.1 Cascade Chaotic Map

We represent the cascade of two Logistic maps as L-L cascade [22]. Logistic map is,

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

where μ is the system parameter, $\mu \in [0, 4]$, x is the initial value, $x \in [0, 1]$. Because of its simple structure and complex behavior, it has been widely studied and applied. However, the chaotic map range of the Logistic system is small, that is, it is full map at the unit interval [0, 1] and can present strong chaotic characteristics only when $\mu = 4$. Figure 1(a), (b) depict the bifurcation diagram of the Logistic system and Lyapunov exponent. A smaller range chaotic map may have closer iteration values and may be easier to appear shorter cycle and kinetics degradation when performing quantization in a digital system.

In order to improve the dynamics of Logistic map, we process to cascade and observe its dynamics performance improvement. Logistic map cascade of two parameters μ_1 and μ_2 can be expressed as,

$$x_{n+1} = \mu_1[\mu_2 x_n(1 - x_n)]\{1 - [\mu_2 x_n(1 - x_n)]\} \tag{2}$$

where, μ_1, $\mu_2 \in [0, 4]$, x is the initial value [0, 1]. To extend the range of the full map and enhance chaotic characteristics, we set $\mu_1 = 4$, μ_2 be the bifurcation parameter. Figure 1(c), (d) show the bifurcation diagram of L-L cascade system and Lyapunov exponents.

The parameter range of L-L cascade system chaotic map expands larger than that of the Logistic chaotic map. And larger chaotic map parameter range provided a larger key space (with initial values and system parameters as the key), thus can enhancing the difficulty of deciphering and improving security. Comparing with non-full map, full map corresponds to the strength of strong chaos whose iteration value range is large. The latter iteration values may difficultly approximate to the previous iteration values, so we can extend the period of the chaotic sequence of numbers to improve the kinetics degradation of the chaotic sequence. Lyapunov exponents of the L-L cascade system is greater than that of the Logistic system in the chaotic region. The increase of Lyapunov exponent may enhance its initial sensitivity, thus improving its power.

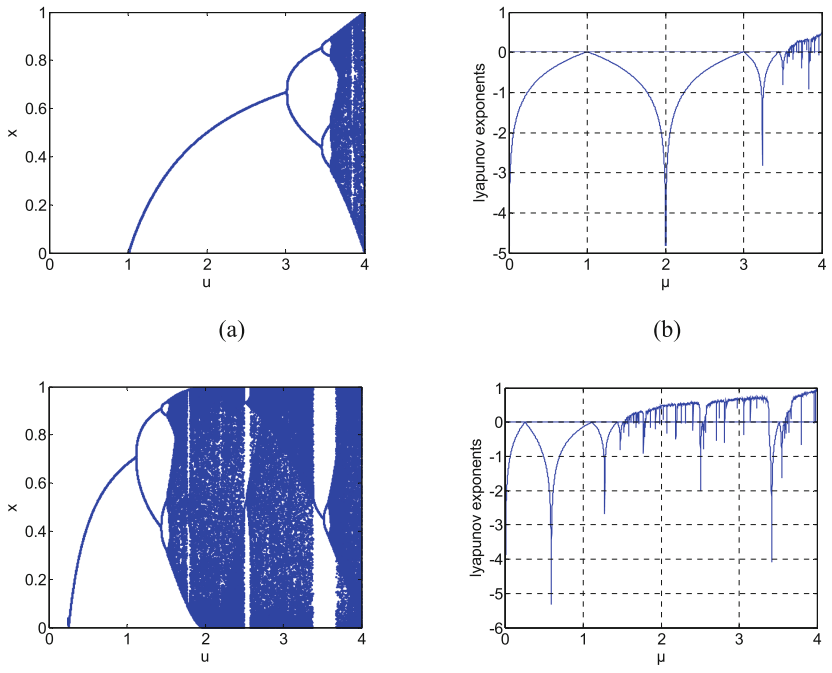


Fig. 1. The bifurcation diagrams of Logistic map and L-L cascade map and Lyapunov exponents (a) the bifurcation diagram of Logistic map, (b) the Lyapunov exponents of Logistic map, (c) the bifurcation diagram of L-L cascade map (d) the Lyapunov exponents of L-L cascade map ($\mu_1 = 4$)

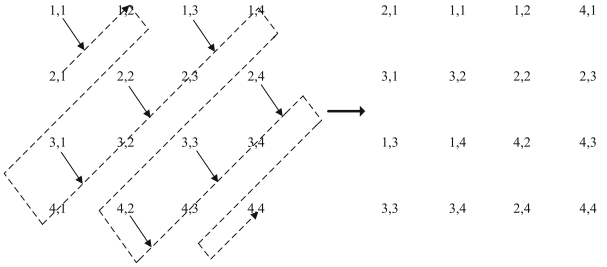
2.2 Line-Map

The main idea of Line-Map [23] is that we insert the line of pixels in the diagonal direction of the image pixel matrix into an adjacent row of pixels to be finally stretched into one-dimensional series, and then folded into the same size of the original image matrix. This can give the original adjacent pixels, not in the original position, high efficiency of scrambling. According to the direction of diagonal, we divide it into left and right line maps. The map transform patterns are shown in Fig. 2.

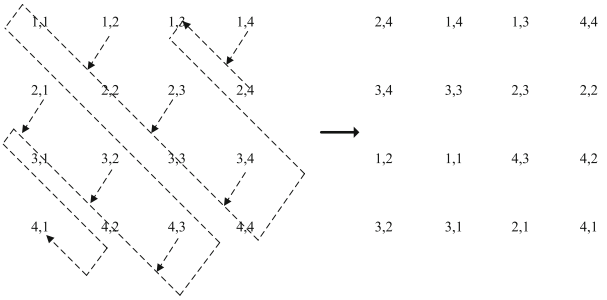
The Left Line Map. We assume that $A(i,j), \quad i,j = 0,1,\ldots,N-1$ is any point in the image. $L(i), \quad i,j = 0,1,\ldots,N^2-1$ is the dimensional vector after stretching $A(i,j)$.

$$L(\sum_{k=0}^{i-1}(4k-1)+j+1) = A(floor(\frac{4i-j+1}{2}), floor(\frac{j+1}{2})) \tag{3}$$

where $j = 1,2,\ldots,4i-1$, $i = 1,2,\ldots,floor(N/2)$.



(a) The left line map



(b)The right line map

Fig. 2. The process of line maps

$$L\Big(\sum_{k=1}^{floor(N/2)}(4k-1)+\sum_{k=floor(N/2)}^{i-1}(4N+1-4k)-4floor(\frac{N+1}{2})-1+j\Big) = A(floor(\frac{2N+2-j}{2}), 2i-N+floor(\frac{j}{2})) \tag{4}$$

where $j = 1, 2, \ldots, 4N+1-4i$, $i = floor(N/2)+1, floor(N/2)+2, \ldots, N$

The Right Line Map. We assume that $A(i,j), \quad i,j = 0, 1, \ldots, N-1$ is any point in the image. $L(i), \quad i,j = 0, 1, \ldots, N^2-1$ is the dimensional vector after stretching $A(i,j)$.

$$L\Big(\sum_{k=0}^{i-1}(4k-1)+j+1\Big) = A(floor(\frac{4i-j+1}{2}),\ M+1-floor(\frac{j+1}{2})) \tag{5}$$

where $j = 1, 2, \ldots, 4i-1$, $i = 1, 2, \ldots, floor(N/2)$.

$$L\Big(\sum_{k=1}^{floor(N/2)}(4k-1)+2N(i-1)+j\Big) = A(floor(\frac{2N+2-j}{2}),\ M-2i+2+\mathrm{mod}(N,2)-floor(\frac{j+2}{2})) \tag{6}$$

where $j = 1, 2, \ldots, 2N$, $i = 1, 2, \ldots, floor((M - 2floor(N/2))/2)$.

$$\begin{aligned} & L(\sum_{k=1}^{floor(N/2)} (4k-1) + 2N \cdot floor((M - 2floor(N/2))/2)) \\ & + \sum_{k=0}^{i-1} (2(M - M_1) + 5 - 4k) - 2(M - M_1) - 5 + j) \\ & = A(N - floor(\frac{j-1}{2}), M - M_1 - 2i + 3 + floor(\frac{j}{2})) \end{aligned} \tag{7}$$

where $j = 1, 2, \ldots, 2(M - M_1) + 5 - 4i$; $i = 1, 2, \ldots, 1 + floor((M - M_1)/2)$.

After stretching the image to a N^2 line $L(i)$, we also fold it into a picture,

$$B(i, j) = L(i \times N + j) \tag{8}$$

where $i = 0, 1, \ldots, N - 1$, $j = 0, 1, \ldots, N - 1$.

3 Algorithm Description

In summary, we can conclude the proposed algorithm as follows.

Step 1. The initial value x_0 is substituted into Eq. (1), iterate N_0 times to obtain x_1, and define a length of 256 integer array.
Step 2. With x_1 as the initial value, we begin to value from $N_0 + 1$, the real value of the resulting sequences is denoted by $x_i, i = 1, 2, \ldots$.
Step 3. Substitute x_i into Eq. (9) to obtain an integer Q_i in range [0, 255].

$$Q_i = \mathrm{mod}(floor(x_i \times 10^3, 256)) \tag{9}$$

Step 4. If Q_i has appeared in the array S, abandon Q_i, otherwise, deposit Q_i into S. When the array is filled in, the S-box is generated.
Step 5. The sequence of integers S is arranged in a 16 × 16 table to construct an initial prototype S-box.
Step 6. Use left line map to perform S-box m times and right line map n times, and fold the addressed S-box.

4 S-box Evaluation Criteria

In order to obtain the S-box of desired cryptography properties, many scholars designed many criteria to test S-box, among which Bijectivity, nonlinearity, Strict avalanche criterion, Bit independent criterion, Differential approximation probability, Linear approximation probability are widely accepted and adopted. In this paper, the evaluation of S-boxes will also use these criteria.

4.1 Bijectivity

Adamas C and Tavares S defined that f is bijective for a $n \times n$ S-box, if the sum of linear operation of Boolean functions of each component is 2^{n-1} [7],

$$\mathrm{wt}(\sum_{i=1}^{n} a_i f_i) = 2^{n-1} \tag{10}$$

where $a_i \in \{0, 1\}$, $(a_1, a_2, \ldots, a_n) \neq (0, 0, \ldots, 0)$, $wt()$ represents Hamming Weight.

The reversibility of S-box is usually required, especially in a displacement of the network S-box.

4.2 Nonlinearity

Definition 1. Let $f(x) : F_2^n \to F_2$ is an n Boolean function, the non-linearity of $f(x)$ can take the form,

$$N_f = \min_{l \in L_n} d_H(f, l) \tag{11}$$

where, L_n is a set of all linear and affine functions, $d_H(f, l)$ represents the Hamming distance between f and l.

The non-linearity represented by Walsh spectrum can take a different form,

$$N_f = 2^{-n}(1 - \max_{\omega \in GF(2^n)} \left| S_{<f>}(\omega) \right|) \tag{12}$$

The cyclic spectrum of $f(x)$ is,

$$S_{<f>}(\omega) = 2^{-n} \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x \cdot \omega} \tag{13}$$

where, $\omega \in GF(2^n), x \cdot \omega$ represents the dot product of x and w.

The larger the nonlinearity N_f of the function f, the stronger the ability of its resisting to the linear attacks, and vice versa.

4.3 Strict Avalanche Criterion

Webster A F and Tavares S E proposed strict avalanche criterion. Strict avalanche criterion describes this fact that when one bit in the input of Boolean function changes, the changing probability of every bit in its output should be 1/2. In practical application, a correlation matrix, the construction method of which can be found in literature [6], is always constructed to test SAC property of the Boolean function.

4.4 Bit Independent Criterion

Adams C and Tavares S proposed Bit independent criterion [7]. For the given Boolean function $f_j, f_k (j \neq k)$ is a two bits output of an S-box, if $f_j \oplus f_k$ is highly nonlinear and meets the SAC, it is possible to ensure that the correlation coefficient of each output bit pair is close to 0 when one input bit is inversed. Therefore, we can check the BIC of the S-box by verifying whether $f_j \oplus f_k (j \neq k)$ of any two output bits of the S-box meets the nonlinearity and SAC.

4.5 Differential Approximation Probability

The Differential probability DP_f is used to reflect the XOR distribution of the input and output of the Boolean function [9], i.e., maximum likelihood of outputting Δy, when the input is Δx,

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\neq \{x \in X | f(x) \oplus f(x \oplus \Delta x\} = \Delta y}{2^n} \right) \tag{14}$$

where, X represents the set of all possible inputs, 2^n is the number of elements in the set.

The smaller the DP_f, the stronger the ability of the S-box for fighting against differential cryptanalysis attacks, vice versa.

4.6 Linear Approximation Probability

Under the condition of randomly selecting two masks Γx and Γy, we use Γx to calculate the mask of all possible values of input x, and use Γy to calculate the mask of the output values $S(x)$ of the corresponding S-box. Mask the input and the output, and the maximum number of the same results is called the maximum linear approximation [24], which can be computed by the following equation,

$$LP = \max_{\Gamma x, \Gamma x \neq 0} \left| \frac{\neq \{x | x \cdot \Gamma x = S(x) \cdot \Gamma y\}}{2^n} - \frac{1}{2} \right| \tag{15}$$

where, Γx and Γy are the mask values of the input and output, respectively, $\boldsymbol{X}$ is a set of all possible input values of x, the elements of which is 2^n.

The smaller the LP, the stronger the ability of the S-box for fighting against linear cryptanalysis attacks, and vice versa.

5 S-box Performance Analysis

To validate the LLCMLM, we compare it with the algorithms in literatures [9–12, 14–20], respectively. And our experimental environment is Inter Core i3 CPU 540 3.07 GHz, memory 2.00 GHz. The program runs in Matlab2012b version. Set initial values of L-L cascaded chaotic map, $x_0 = 0.1, N_0 = 500$, parameters $\mu_1 = 4, \mu_2 = 2, m = 7, n = 1$, thus

resulting a 8 × 8 S-box, as shown in Table 1. Next, we test the S-box according to the above design criteria.

5.1 Bijectivity of the S-box of LLCMLM

According to the formula (13), we compute the bijectivity of the generated S-box. The computed value of S-box is just the desired value 128. This indicates that S-box of the LLCMLM meets the bijectivity.

5.2 Nonlinearity of the S-box of LLCMLM

Using (16) to calculate the non-linearity of the S-box of LLCMLM, the results are shown in Table 2. The minimum degree of a non-linear design of S-box 8 Boolean functions is 104 and a maximum of 108, with an average of 106.25. Comparing with the algorithms in literatures [9–12, 14–20], LLCMLM has a larger nonlinearity, shown in the nonlinearity column of Table 6. The results showed that the S-boxes are non-linear, and have the ability to resist linear cryptanalysis.

5.3 Strict Avalanche Criterion of the S-box of LLCMLM

The testing results are shown in Table 2, the maximum strict avalanche criterion of the generated S-box is 0.5625, the minimum is 0.3906, the average is close to the ideal value of 0.5. Comparing with the results of the literatures [9–12, 14–20], shown in the SAC column of Table 6, the S-box of LLCMLM can better meet the strict avalanche criterion.

Table 1. The S-box generated by LLCMLM

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

Table 2. The dependence matrix of the S-box of LLCMLM

0.5000	0.5000	0.4844	0.5156	0.5000	0.4375	0.5000	0.5156
0.5156	0.4219	0.5000	0.5000	0.4531	0.5469	0.5156	0.5625
0.5000	0.4844	0.4063	0.4531	0.4688	0.5313	0.5469	0.5625
0.5312	0.5000	0.5000	0.5000	0.5469	0.4375	0.5313	0.4688
0.5625	0.4688	0.5469	0.4375	0.5000	0.4844	0.4844	0.4844
0.5000	0.4531	0.3906	0.5469	0.4219	0.5313	0.4844	0.5000
0.5156	0.5156	0.4531	0.4375	0.4531	0.5156	0.4688	0.5156
0.5469	0.5469	0.5469	0.4688	0.5156	0.5000	0.4844	0.4531

Table 3. BIC-nonlinearity criterion for the S-box of LLCMLM

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

Table 4. BIC-SAC criterion for the S-box of LLCMLM

0	0.5020	0.5078	0.4844	0.5117	0.5156	0.5039	0.4941
0.5020	0	0.5215	0.4902	0.5156	0.5137	0.5215	0.4805
0.5078	0.5215	0	0.5059	0.4805	0.5176	0.5020	0.4727
0.4844	0.4902	0.5059	0	0.4824	0.5215	0.4902	0.4844
0.5117	0.5156	0.4805	0.4824	0	0.5156	0.4824	0.5215
0.5156	0.5137	0.5176	0.5215	0.5156	0	0.4941	0.5020
0.5039	0.5215	0.5020	0.4902	0.4824	0.4941	0	0.4844
0.49415	0.4805	0.4727	0.4844	0.5215	0.5020	0.4844	0

5.4 Bit Independent Criterion of the S-box of LLCMLM

The results of the testing are shown in Tables 3 and 4. The average value of non-linearity of the S-box of LLCMLM is 103.64, The average value of correlation matrix is 0.5007, which is close to the ideal value of 0.5. Comparing with the results of literatures [9–12, 14–20], shown in BIC column of Table 6, S-box has a better bit independent criterion.

5.5 Differential Approximation Probability of the S-box of LLCMLM

We use Eq. (17) to calculate differential approximation probability of the generated S-box, shown in Table 5. And comparing with the results of literatures [9–12, 14–20], shown in the DP column of Table 6, the results show that the maximum value of differential approximation probability of the S-box of LLCMLM is only 10, the minimum is 4, which means that the generated S-box has a good ability to resist differential cryptanalysis.

Table 5. Differential approximation probability of the S-box of LLCMLM

6	6	8	8	6	6	6	8	8	8	6	6	8	6	6	6
8	6	6	8	6	8	8	8	8	4	6	6	8	8	6	8
6	8	6	6	8	6	6	6	6	8	6	8	6	8	6	6
8	6	6	8	6	6	6	6	8	6	6	8	8	6	6	6
6	6	6	8	8	6	6	8	6	8	8	6	8	6	6	6
8	6	8	6	6	8	10	6	8	8	8	6	6	8	8	6
6	8	8	8	6	6	8	8	6	6	6	6	6	6	8	6
8	8	6	6	6	6	6	6	6	10	6	6	6	6	6	6
8	8	8	4	6	6	6	6	6	8	8	8	8	6	6	8
8	6	6	8	6	6	8	6	6	8	6	8	6	6	10	8
4	6	6	6	6	6	6	6	6	6	8	8	8	6	6	6
8	8	8	6	8	6	8	6	4	6	8	6	6	6	6	6
6	8	8	6	4	6	6	6	6	8	8	6	6	6	8	6
6	8	6	8	10	6	6	10	6	6	6	8	8	8	8	6
6	6	6	6	8	8	6	6	8	6	10	8	8	6	6	6
6	6	8	6	10	8	8	6	6	6	6	8	6	6	8	0

Table 6. Cryptanalysis comparison results of S-boxes

S-boxes	Nonlinearity			SAC			BIC-SAC	BIC	DP	LP
	Min	Max	Avg.	Min	Max	Avg.				
LLCMLM	104	108	106.25	0.3906	0.5625	0.4949	103.64	0.5007	0.03906	0.140625
Ref. [9]	100	108	103.250	0.3750	0.5938	0.5059	104.29	0.5031	0.04688	0.125000
Ref. [10]	103	109	104.875	0.3984	0.5703	0.4966	102.96	0.5044	0.03906	0.132813
Ref. [11]	101	108	103.875	0.3906	0.5781	0.5059	102.68	0.4958	0.03906	0.132813
Ref. [12]	100	106	103	0.4219	0.6094	0.5000	103.14	0.5024	0.05469	0.132813
Ref. [14]	102	106	104	0.3750	0.6094	0.4980	103.29	0.4971	0.03906	0.148438
Ref. [15]	96	106	103	0.3906	0.6250	0.5039	100.36	0.5010	0.03906	0.148438
Ref. [16]	98	108	103	0.4063	0.5938	0.5012	104.07	0.4989	0.04688	0.148438
Ref. [17]	100	106	104	0.3750	0.6250	0.4946	103.21	0.5019	0.03906	0.132813
Ref. [18]	103	109	105.125	0.4141	0.6094	0.5061	103.68	0.4983	0.03906	0.156250
Ref. [19]	102	108	105.250	0.4063	0.5781	0.5059	104.29	0.5029	0.04688	0.125000
Ref. [20]	100	108	104.5	0.4219	0.6094	0.4978	103.64	0.5010	0.04688	0.140625

5.6 Linear Approximation Probability of the S-box of LLCMLM

In this subsection, we use (18) to calculate Linear approximation probability of the generated S-box and compare LLCMLM with other algorithms proposed in literatures [9–12, 14–20]. The experimental results are shown in the right column of Table 6. For LLCMLM, it obtains a greater LP, 0.140625. And the remaining columns are the nonlinearity, SAC, BIC-SAC and BIC results of the comparison algorithms. Table 6 indicates that all of the chaotic based comparison algorithms can generate S-boxes with good performance, however, LLCMLM may obtain an S-box that has a better performance of resisting modern cryptanalysis attacks such as differential and linear cryptanalysis attacks.

6 Conclusion

An S-box generation approach based on L-L cascade Chaotic Map and Line Map (LLCMLM) is designed in this paper. LLCMLM uses L-L cascade chaotic map to generate an integer sequence ranging 0–255, and applies line map to scramble the position of the integer sequence. A series of experiments have been conducted to compare multiple cryptographic criteria of LLCMLM with other algorithms. The experimental results show that the S-box of the CSABC has some good cryptography features such as Bijectivity, Non-linearity, strict avalanche criterion (SAC), bit independent criterion (BIC), differential probability (DP) and linear probability (LP), and it can effectively resist to some attacks. Though LLCMLM can be used to find the S-box with good Cryptography performance, it is still hard to find some S-boxes with very good Cryptography performance. In the future, we will further clarify the relationship between chaos and cryptography, and research how to set chaos parameters to find the S-box with excellent performance.

References

1. Wang, X., Wang, Q.: A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. Nonlinear Dyn. **75**(3), 567–576 (2014)
2. Hussain, I., Shah, T., Gondal, M.A.: Application of S-box and chaoticmap for image encryption. Math. Comput. Model. **57**(9), 2576–2579 (2013)
3. Zhang, X., Mao, Y., Zhao, Z.: An efficient chaotic image encryption based on alternate circular S-boxes. Nonlinear Dyn. **78**(1), 359–369 (2014)
4. Hussain, I., Gondal, M.A.: An extended image encryption using chaotic coupled map and S-box transformation. Nonlinear Dyn. **76**(2), 1355–1363 (2014)
5. Liu, H., Kadir, A., Niu, Y.: Chaos-based color image block encryption scheme using S-box. AEU Int. J. Electron. Commun. **68**(7), 676–686 (2014)
6. Webster, A.F., Tavares, S.: On the design of S-boxes. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 523–534. Springer, Heidelberg (1986)
7. Adams, C.M., Tavares, S.: Good S-boxes are easy to find. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 612–615. Springer, Heidelberg (1990)

8. Dawson, M.H., Tavares, S.: An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 352–367. Springer, Heidelberg (1991)
9. Jakimoski, G., Kocarev, L.: Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans. Circ. Syst. I: Fundam. Theor. Appl. **48**(2), 163–169 (2001)
10. Tang, G., Liao, X., Chen, Y.: A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons Fractals **23**(2), 413–419 (2005)
11. Tang, G., Liao, X.: A method for designing dynamical S-boxes based on discretized chaotic map. Chaos, Solitons Fractals **23**(5), 1901–1909 (2005)
12. Chen, G., Chen, Y., Liao, X.: An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps. Chaos, Solitons Fractals **31**(3), 571–579 (2007)
13. Wang, Y., Wong, K.W., Li, C.B., Li, Y.: A novel method to design S-box based on chaotic map and genetic algorithm. Phys. Lett. A **376**(6), 827–833 (2012)
14. Chen, G.: A novel heuristic method for obtaining S-boxes. Chaos, Solitons Fractals **36**(4), 1028–1036 (2008)
15. Khan, M., Shah, T., Mahmood, H., Gondal, M.A., Hussain, I.: A novel technique for the construction of strong S-boxes based on chaotic lorenz systems. Nonlinear Dyn. **70**(3), 2303–2311 (2012)
16. Khan, M., Shah, T., Mahmood, H., Gondal, M.A.: An efficient method for the construction of block cipher with multi-chaotic systems. Nonlinear Dyn. **71**(3), 489–492 (2013)
17. Khan, M., Shah, T.: A construction of novel chaos base nonlinear component of block cipher. Nonlinear Dyn. **76**(1), 377–382 (2014)
18. Özkaynak, F., Yavuz, S.: Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dyn. **74**(3), 551–557 (2013)
19. Hussain, I., Shah, T., Gondal, M.A., Mahmood, H.: A novel method for designing nonlinear component for block cipher based on TD-ERCS chaotic sequence. Nonlinear Dyn. **73**(1–2), 633–637 (2013)
20. Khan, M., Shah, T.: An Efficient construction of substitution box with fractional chaotic system. SIViP 1–4 (2013)
21. Liu, X.C., Feng, D.G.: Construction of S-boxes with some cryptographic properties. J. Softw. **11**(10), 1299–1302 (2000)
22. Wang, G.Y., Yuan, F.: Cascade Chaos and Its Dynamic Characteristics. Acta Phys. Sin. **62** (2), 2–10 (2013). 020506
23. Feng, Y., Li, L., Huang, F.: A symmetric image encryption approach based on line maps. In: 1st International Symposium on Systems and Control in Aerospace and Astronautics, pp. 1362–1367. IEEE Press (2006)
24. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)