J Inf Process Syst, Vol.21, No.2, pp.216~226, April 2025
https://doi.org/10.3745/JIPS.03.0204
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Constructing S-Box Using Fractional-Order Nonlinear Coupled Map and Elementary Cellular Automata

Liyan Liu[1], Cheng Zhang[1,*], and Yingqian Zhang[2,3]

Abstract

A novel substitution box (S-box) construction method is proposed by using a fractional-order nonlinear coupled map lattices chaotic system combined with an elementary cellular automaton. An original S-box is produced by utilizing chaos sequences from the fractional-order nonlinear coupled map lattices spatiotemporal chaotic system. The S-box elements are then rearranged by applying different state values of various cells in the elementary cellular automaton. These chaotic sequences with independent properties are subsequently used to perturb the S-box's elements. Comparative results with previous schemes indicate that the constructed S-box demonstrates enhanced security performance and could be effectively utilized in the development of block encryption algorithms.

Keywords

Elementary Cellular Automaton, Fractional-Order Nonlinear Coupled Map Lattices, S-Box

1. Introduction

Substitution boxes (S-boxes) are of vital importance in many block cipher algorithms, including the data encryption standard, international data encryption algorithm, and advanced encryption standard. As the sole nonlinear component in these algorithms, S-boxes provide confusion and diffusion, which are essential for enhancing security.

A variety of design methods for S-boxes have emerged in recent years [1-18]. One notable approach is to construct S-boxes by employing spatiotemporal chaotic systems, which have garnered extensive attention, due to their superior dynamic behaviors compared to traditional chaotic systems. These behaviors include longer cycles, higher positive Lyapunov exponents, and enhanced randomness. For instance, Yuan et al. [1] designed an algorithm to generate S-boxes based on spatiotemporal chaos. Similarly, Peng et al. [2] dynamically designed S-boxes utilizing a spatiotemporal chaotic system. Liu et al. [4] designed S-boxes using nonlinear coupled map lattices (NCML) and coupled map lattices (CML) [5]. In [6], the dynamic S-box values were initialized using the logistic dynamic coupled map lattice spatio-temporal chaos system. However, these spatiotemporal chaos systems are fundamentally rooted in classical integer-order logistic maps. In recent years, fractional-order spatiotemporal chaotic systems [19,20] have gained popularity, due to their unique characteristics, such as a broader state amplitude range for ergodicity and a wider parameter range, leading to an expanded key space for encryptions. This

Manuscript received November 21, 2024; first revision December 23, 2024; accepted December 24, 2024.
*Corresponding Author: Cheng Zhang (zhangc@dlut.edu.cn)
[1] City Institute, Dalian University of Technology, Dalian, China (liuliyan81@sina.com, zhangc@dlut.edu.cn)
[2] School of Electrical Engineering and Artificial Intelligence, Xiamen University Malaysia, Sepang, Malaysia (zhangyqxmu@xmu.edu.cn)
[3] School of Information Science & Technology, Xiamen University Tan Kah Kee College, Zhangzhou, China

study introduces the fractional-order nonlinear coupled map lattices (FONCML) spatiotemporal chaotic system [19] as a novel approach to designing S-boxes. To enhance the robustness of our S-box design, we combine the FONCML spatiotemporal chaotic system with another dynamic system instead of relying on it alone. Cellular automata [21], recognized as intelligent algorithms, have attracted widespread interest [22,23]. The elementary cellular automaton (ECA) [24], a simple one-dimensional cellular automaton demonstrates excellent dynamic performance due to its discrete nature in both time and space, with calculations occurring in the binary domain. This characteristic mitigates issues of dynamic degradation when utilized in cryptographic systems. In addition, the properties of pseudo-randomness and long periodicity of the generated sequence can be ensured if suitable iteration rules are chosen. Due to the unpredictable nature of input and iteration rules, mathematical analysis becomes exceedingly challenging, which can augment the complexity of S-box construction. For example, Zhao et al. [12] designed S-boxes using Lorenz and skew tent systems in conjunction with ECA, achieving good security. However, their method relied on low-dimensional chaos system.

Building upon this analysis we explore an innovative approach to constructing S-boxes by employing both the FONCML spatiotemporal chaos system and ECA. The key results of our research are as below.

- The FONCML spatiotemporal chaotic system is utilized to construct S-boxes due to its high dimensional characteristics, broad state amplitude for ergodicity and wide parameter range. These attributes enhance encryption performance and security of S-boxes.
- The using of ECA complicates the mathematical analysis of the constructed S-boxes.
- The S-box constructed in this study exhibits greater nonlinearity compared to those designed using only spatiotemporal chaos systems [4,5].
- The combination of the FONCML spatiotemporal system and ECA ensures that the reliance on the FONCML spatiotemporal system alone reduced, thereby improving the security performance of the S-boxes.
- Compared to previous studies, our S-box demonstrates superior performance. The S-box construction method using both the FONCML spatiotemporal system and ECA is highly recommended.

The layout of the remaining sections of this paper is as described below. Section 2 outlines the FONCML system and ECA. An innovative S-box construction method is introduced in Section 3. A performance analysis of the constructed S-box is provided in Section 4. Section 5 concludes the study.

2. Preliminaries

2.1 FONCML Spatiotemporal System

The FONCML spatiotemporal system [19] is described as

$$x_{tt+1}(l) = (1-\varepsilon)\big(x_{tt}(l) + \beta\mu x_{tt}(l)(1-x_{tt}(l))\big) + \varepsilon/2\begin{Bmatrix}\big(x_{tt}(g) + \beta\mu x_{tt}(g)(1-x_{tt}(g))\big)\\ +\big(x_{tt}(s) + \beta\mu x_{tt}(s)(1-x_{tt}(s))\big)\end{Bmatrix}. \quad (1)$$

The system consists of N lattices. In (1), tt represents time, ε denotes the coupling coefficient ($0 \le \varepsilon \le 1$), $\beta = r^{\alpha}/\Gamma(1+\alpha)$, α represents a fraction, $\Gamma(\cdot)$ is the Eulerian gamma-function and r is a fraction used for segmentation. The variables l, g, and s correspond to lattices ($1 \le l, g, s \le N$) and meet the following Arnold cat map:

$$\begin{bmatrix} g \\ s \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} l \\ l \end{bmatrix} (\mathrm{mod} N), \quad (2)$$

which a and b represent the parameters.

The FONCML system exhibits exceptional chaotic properties when parameters are set to appropriate values. Compared to the integer-order spatiotemporal chaotic systems previously mentioned, the FONCML spatiotemporal chaotic system has a higher percentage of lattices that exhibit chaotic behavior and a larger parameter range conducive to chaos. In addition, its bifurcation diagrams do not feature periodic windows. These novel characteristics make the FONCML spatiotemporal chaotic system particularly suitable for cryptography [19].

2.2 ECA

ECA is made of a linear arrangement of cells, with two possible states represented as {0,1}. Each cell has a half-diameter of 1, with the neighboring cells as its left and right neighbors. In ECA, for a cell, the states of its neighbors and its current state determine its next state, as expressed by

$$A_{t+1}(c) = f_{ir}\big(A_t(c-1), A_t(c), A_t(c+1)\big), \tag{3}$$

where t represents time, c ($c \in [1, M]$) is the index of a cell, $A_t(c)$ is the state of cell c at time t, ir represents an iteration rule of ECA and f denotes a Boolean function.

ECA's boundary conditions are periodic, as expressed in the following equation.

$$\begin{cases} c+1 = 1, c = M \\ c-1 = M, c = 1 \end{cases}. \tag{4}$$

Fig. 1 illustrates the iterative process when ECA employs a cyclic boundary condition.

$A_t(M)$	$A_t(1)$	$A_t(2)$	$\cdots$	$A_t(c-1)$	$A_t(c+1)$	$\cdots$	$A_t(M)$	$A_t(1)$

Fig. 1. Iterative process.

According to (3), f is a Boolean function defined over a binary field, where the input consists of three state values and the output includes one state value. This means that the input comprises three binary numbers, whereas the output contains one. The possibility of $2^3 = 8$ inputs and two outputs yields $2^8 = 256$ distinct ECA rules. The iteration rules of ECA can be categorized into five types based on the nature of their results: invalid, periodic, fixed point, global chaos and local chaos rules [25,26]. Among these, the iteration results under global chaos rules exhibit long period and chaotic characteristics. The study in [26] identifies 34 types of global chaos rules, as depicted in Fig. 2.

1	2	3	4	5	6	7	8	9
8	22	30	45	60	75	86	89	90
10	11	12	13	14	15	16	17	18
101	102	105	106	110	120	122	124	126
19	20	21	22	23	24	25	26	27
129	135	137	146	149	150	151	153	161
28	29	30	31	32	33	34		
165	169	182	183	193	195	225		

Fig. 2. Global chaos rules.

Table 1 lists all output values corresponding to any input values of the function f_{169}. Because the Boolean function f of ECA has multiple inputs that yield the same output, it is classified as a nonlinear and irreversible function. However, it can generate correct results if iteration rules and the initial value of the ECA are determined. When the input and iteration rules are unknown, mathematical analysis

becomes quite challenging. This characteristic is relevant to S-box construction, as it complicates mathematical analysis.

Table 1. Function f_{169}

Iteration results	Binary number							
$A_t(c-1)$	1	1	1	1	0	0	0	0
$A_t(c)$	1	1	0	0	1	1	0	0
$A_t(c+1)$	1	0	1	0	1	0	1	0
$A_{t+1}(c)$	1	0	1	0	1	0	0	1

3. S-Box Construction Method

This section describes our development of an innovative S-box construction method utilizing the FONCML system and ECA. To construct the S-box, we first set the parameters of $N = 100$, $\varepsilon = 0.8$, $\mu = 10$, $r = 0.25$, $\alpha = 0.95$, $M = 200$. The specific steps are as below:

Step 1. Compute (1) and obtain a matrix $x_{tt}(j)(tt \in [1,2000], j \in [1, N])$.

Step 2. Construct a new sequence y as follows:

$$y(i) = \mathrm{mod}(floor(x_{200+i}(66) \times 10^{14}), 512), (i \in [1,256]). \tag{5}$$

Step 3. Obtain an index sequence $z(1 \times 256)$ of the sequence $y(1 \times 256)$ whose elements are sorted in ascending order.

Step 4. Convert each value in the sequence $x_{tt}(66)$ into an 8-bit unsigned integer.

Step 5. Convert these unsigned integers into binary numbers and obtain a binary sequence u.

Step 6. Extract M bits from the 660th in the sequence u and use them as values from $A_1(1)$ to $A_1(M)$.

Step 7. Compute (3) and obtain a matrix $A_t(i)(t \in [1,10000], i \in [1, M])$.

Step 8. Extract 60 to 67 columns from the matrix $A_t(i)$ and convert the binary number of each row into a decimal number; then, add 1to achieve a new sequence $v(10000 \times 1)$.

Step 9. Swap the values in sequence z using (6).

$$z(i) \leftrightarrow z\big(v(200+i)\big), (i \in [1,256]). \tag{6}$$

Step 10. Reconvert $z(1 \times 256)$ into a matrix $S(16 \times 16)$.

Step 11. Compute u and w using (7) and (8), respectively.

$$u = \mathrm{Mod}(\lfloor (FONCML(\mathrm{Mod}(S((g-1) \times 16 + l, 100) + 1{,}600 + (g-1) \times 16 + l) \times 10^{14}) \rfloor, 16) + 1, \tag{7}$$

$$w = \mathrm{Mod}(\lfloor (FONCML(m, n) \times 10^{14}) \rfloor, 16) + 1, \tag{8}$$

where $g, l \in [1,16]$, m and n meet the following Arnold cat map.

$$\begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} g \\ l \end{bmatrix} (\mathrm{mod} N). \tag{9}$$

Step 12. Swap the values in matrix S using (10).

$$S(u, w) \leftrightarrow S(g, l). \tag{10}$$

The final result, S, is the constructed S-box.

4. Performance Analysis

The following six criteria are commonly used to evaluate S-boxes [4,5]. The constructed S-box using the proposed method is showcased in Table 2.

Table 2. Obtained S-box

230	223	89	72	27	200	99	28	171	169	203	91	240	232	215	114
207	177	229	145	20	74	111	216	151	124	63	75	32	77	175	110
127	113	93	23	246	79	253	224	82	199	15	78	21	248	170	122
178	54	33	135	19	35	14	42	80	119	38	237	65	58	43	115
244	183	150	139	9	143	76	12	6	140	123	31	100	105	17	172
57	221	71	103	161	61	156	92	157	40	37	222	11	13	142	152
195	16	197	56	166	120	44	208	242	204	256	249	206	102	10	168
69	49	5	2	59	87	220	238	132	159	191	133	164	160	188	217
3	192	34	243	245	213	117	198	189	88	193	22	233	252	154	190
210	162	66	109	180	155	7	26	70	98	62	128	50	146	186	112
118	247	236	107	225	108	48	29	138	136	24	121	241	211	167	149
96	41	126	25	184	187	90	251	81	94	227	30	163	125	51	83
4	97	254	84	64	174	228	8	173	231	18	147	239	53	95	55
106	137	205	250	181	235	47	226	1	129	234	39	45	60	36	194
131	209	67	144	86	158	182	185	141	218	46	176	148	68	85	214
73	116	134	219	104	153	202	165	196	130	212	52	101	179	201	255

4.1 Property of the Bijective

If an S-box satisfies the formula $hw(\sum_{i=1}^{n} a_i f_i) = 2^{n-1}$, in which $hw(\cdot)$ expresses the Hamming weight, $a_i \in \{0,1\}$ and f_i is a Boolean function, then the S-box is bijective. Based on the proposed method, the constructed S-box demonstrates bijective performance.

4.2 Nonlinearity

Nonlinearity is a critical criterion for assessing the security of a cryptosystem, as the nonlinear structure significantly influences its overall safety. The formula for determining nonlinearity N_f is expressed as

$$N_f = 2^{n-1}\left(1 - 2^{-n} \max_{\omega \in GF(2^n)} \left|S_{(f)}(\omega)\right|\right), \tag{11}$$

in which the definition of the $S_{(f)}(\omega)$ of $f(x)$ is

$$S_{(f)}(\omega) = \sum_{\omega \in GF(2^n)} (-1)^{f(x) \oplus x \cdot \omega}, \tag{12}$$

where $x \cdot \omega$ is the dot product of x and ω.

Table 3 lists the results of the nonlinearity analysis. For the constructed S-box, the smallest nonlinearity value was 102, the largest nonlinearity value was 108, and the mean was 105.75, indicating commendable nonlinearity. The constructed S-box showed nonlinearity comparable to other S-boxes [12,14-18] and outperformed those that were constructed using spatiotemporal chaotic system alone [4,5].

Table 3. Nonlinearity analysis results

S-boxes	Nonlinearity		
	Max	Min	Average
Proposed method	108	102	105.75
Liu et al. [4]	108	102	104.50
Liu and Lei [5]	108	102	104.25
Javeed et al. [7]	110	106	107.50
Jiang and Ding [9]	108	104	106.75
Zhao et al. [12]	108	104	106.00
Zhang et al. [14]	112	104	106.50
Hua et al. [15]	108	102	105.25
Liu et al. [16]	108	100	105.00
Aslam et al. [17]	108	104	106.00
Zhou et al. [18]	108	104	105.25

4.3 Strict Avalanche Criterion

When an input bit has its value complemented, each output bit has a 50% chance of being changed, indicating compliance with the strict avalanche criterion (SAC). An independent matrix is often employed to represent the SAC. In fact, a well-constructed S-box possesses a dependence matrix with elements close to 0.5.

The formula for estimating the dependence matrix offsets is given as

$$S(f) = 1/n \sum_{1\le i\le n} \sum_{1\le j\le n} \left|1/2 - P_{i,j}(f)\right|, \tag{13}$$

where $P_{i,j}(f) = 2^{-n} \sum_{x\in B^n} f_j(x) \oplus f_j(x \oplus e_i), e_i = \left[\delta_{i,1}\delta_{i,2} \cdots \delta_{i,n}\right]^T$, $[\cdot]^T$ indicates a matrix transpose, and $\delta_{i,j} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$.

Table 4. Dependence matrix

0.5000	0.4688	0.5313	0.4375	0.4531	0.5000	0.5000	0.4688
0.4375	0.5469	0.3906	0.4219	0.5000	0.5625	0.4063	0.5156
0.5313	0.4531	0.5313	0.5156	0.5313	0.5469	0.5313	0.4531
0.5000	0.5313	0.5000	0.5156	0.4844	0.5313	0.4844	0.5156
0.3906	0.5000	0.5156	0.5000	0.5156	0.5156	0.6094	0.5469
0.5938	0.4688	0.5469	0.4844	0.5156	0.5313	0.4531	0.4375
0.4688	0.5313	0.5313	0.3750	0.5000	0.4844	0.4375	0.6094
0.5469	0.5156	0.4844	0.5469	0.5156	0.3750	0.5000	0.4531

Table 4 outlines the dependence matrix of the constructed S-box. All values fall between 0.6094 and 0.3750, and an average of 0.4968 is near the desired value of 0.5, indicating that the S-box is compliant with the SAC. Comparisons of various S-boxes about SAC are outlined in Table 5, showing that the constructed S-box displays superior SAC characteristics.

Table 5. SAC comparison results

S-boxes	SAC average
Proposed method	0.4968
Liu et al. [4]	0.4980
Liu and Lei [5]	0.5083
Javeed et al. [7]	0.4997
Jiang and Ding [9]	0.4975
Zhao et al. [12]	0.5014
Zhang et al. [14]	0.5060
Hua et al. [15]	0.5351
Liu et al. [16]	0.5002
Aslam et al. [17]	0.4983
Zhou et al. [18]	0.5070

4.4 Output Bits Independence Criterion

The output bits independence criterion (BIC) asserts that any pair of output bits should be mutually independent when an input bit is complemented. When the value of $f_m \oplus f_n$ fulfills the SAC and is highly nonlinear, the S-box possesses the BIC property, where f_m, $f_n (m \neq n)$ are Boolean functions and represent two distinct output bits of the S-box.

For the constructed S-box, its BIC-nonlinearity values are listed in Table 6, its BIC-SAC values are listed in Table 7, and its mean values for BIC-nonlinearity and BIC-SAC were 103.57 and 0.5001, respectively. The comparisons of various S-boxes for BIC are summarize in Table 8, showing that the constructed S-box are consistent with other S-boxes [4,5,7,9,12,15,16]. Thus, the constructed S-box demonstrates a strong BIC property.

Table 6. BIC-nonlinearity results

-	98	100	104	108	104	104	104
98	-	104	100	102	106	104	100
100	104	-	102	102	104	108	106
104	100	102	-	104	104	104	100
108	102	102	104	-	106	100	106
104	106	104	104	106	-	108	104
104	104	108	104	100	108	-	104
104	100	106	100	106	104	104	-

Table 7. BIC-SAC results

-	0.4805	0.5117	0.4883	0.5176	0.4941	0.4922	0.5137
0.4805	-	0.5039	0.5117	0.4980	0.5020	0.5195	0.5117
0.5117	0.5039	-	0.5254	0.5020	0.4941	0.5078	0.5039
0.4883	0.5117	0.5254	-	0.4844	0.4941	0.4863	0.5176
0.5176	0.4980	0.5020	0.4844	-	0.4922	0.4941	0.4785
0.4941	0.5020	0.4941	0.4941	0.4922	-	0.4902	0.4785
0.4922	0.5195	0.5078	0.4863	0.4941	0.4902	-	0.5078
0.5137	0.5117	0.5039	0.5176	0.4785	0.4785	0.5078	-

Table 8. BIC comparison results

S-boxes	BIC-SAC	BIC-nonlinearity
Proposed method	0.5001	103.57
Liu et al. [4]	0.5079	104.64
Liu and Lei [5]	0.5008	103.07
Javeed et al. [7]	0.5048	104.64
Jiang and Ding [9]	0.5022	103.57
Zhao et al. [12]	0.5001	103.79
Zhang et al. [14]	-	105.60
Hua et al. [15]	0.5000	103.21
Liu et al. [16]	0.5038	103.00
Aslam et al. [17]	0.5002	106.00
Zhou et al. [18]	0.5039	102.72

4.5 Equiprobable Input/Output XOR Distribution

The ability of an S-box to resist differential attacks can be analyzed by examining the imbalances in its input/output XOR distribution table. This analysis typically utilizes the differential approximation probability (DP) and the differential approach table to assess the input/output XOR distribution. DP is defined as

$$DP_h = \max_{\Delta x \neq 0, \Delta y} (\#\{x \in X \mid h(x) \oplus h(x \oplus \Delta x) = \Delta y\}/2^n), \tag{14}$$

where the set X includes every possible input, and 2^n indicates the quantity of elements in the set X. A well-constructed S-box will have a DP_h value that is small as possible.

For the constructed S-box, its differential approach table is delineated in Table 9. The maximum DP value observed to be 12, indicating that the S-box has a high level of resistance towards differential attacks. Comparisons of maximum DP values for various DP_h are provided in Table 10. The constructed S-box shows a maximum DP_h value consistent with most other S-boxes, confirming its robust DP feature.

Table 9. Differential approach table

6	8	8	6	6	6	6	6	6	6	6	8	6	6	8	6
4	6	6	6	8	8	10	6	6	6	6	6	8	8	6	6
8	6	6	6	6	8	8	8	6	6	6	8	6	6	6	6
6	6	8	8	8	6	4	8	6	8	8	8	6	6	8	6
8	6	12	6	6	8	6	6	6	6	6	6	8	6	8	6
6	6	8	6	6	8	6	6	8	6	6	8	8	6	6	6
6	8	6	6	6	6	6	8	8	6	6	6	6	8	6	6
6	6	8	6	6	8	6	6	6	8	6	6	6	6	8	8
6	6	6	12	8	8	8	10	10	6	6	6	6	6	8	6
6	6	6	6	6	8	8	6	6	6	6	8	8	6	6	8
8	8	6	6	10	8	6	6	6	6	6	6	8	8	6	8
6	6	10	6	8	6	6	6	6	6	6	6	6	6	6	4
8	8	6	8	8	6	6	6	6	8	6	6	8	6	6	8
6	6	6	6	6	6	6	6	10	8	8	6	8	8	8	6
6	6	6	6	6	6	6	8	6	8	6	8	6	6	6	4
6	8	6	6	6	8	6	6	10	6	6	4	6	6	6	0

Table 10. DP comparison results

S-boxes	MaxDP
Proposed method	0.0469
Liu et al. [4]	0.0469
Liu and Lei [5]	0.0469
Zhao et al. [12]	0.0391
Aslam et al. [17]	0.0380
Zhou et al. [18]	0.0390

4.6 Linear Approximation Probability

An event's largest imbalance value is determined by the linear approximation probability (LP) defined as

$$LP = \max_{\alpha_1,\alpha_2 \neq 0} (\#\{x \in X \mid x \cdot \alpha_1 = h(x) \cdot \alpha_2\}/2^n - 1/2), \quad (15)$$

where α_1 represents the input mask, and α_2 is the output mask. Here, the input bits parity selected by α_1 matches the output bits parity selected by α_2.

Table 11 lists the comparative results for the maximum LP of different S-boxes. For maximum LP, the constructed S-box is comparable to other S-boxes. Accordingly, it demonstrates strong LP performance.

Table 11. Maximum LP comparison results

S-boxes	MaxLP
Proposed method	0.1328
Liu et al. [4]	0.1250
Liu and Lei [5]	0.1406
Javeed et al. [7]	0.1406
Jiang and Ding [9]	0.1328
Zhang et al. [14]	0.1320
Aslam et al. [17]	0.1328
Zhou et al. [18]	0.1328

5. Conclusion

An innovative S-box construction method is developed by utilizing the FONCML spatiotemporal chaotic system and ECA in this study. The FONCML system is characterized by broad range of state amplitude for ergodicity and wide parameter range, which contribute to the development of S-boxes with strong encryption capabilities and high security. In addition, ECA adds complexity, making mathematical analysis of S-boxes challenging. The integration of the FONCML system and ECA enhances the overall complexity of the S-box. During the construction phase of the S-box, chaos sequences created by the FONCML system are utilized to establish its initial value. Different state values for various cells in the ECA are then employed to rearrange the elements of the S-box. A perturbing operation is finally executed utilizing independent chaotic sequences. Performance analysis indicates that this S-box construction method is effective. The resulting S-box demonstrates greater nonlinearity than those produced solely with spatiotemporal chaotic system. Compared to previous S-boxes, the obtained S-box using the proposed method exhibits superior safety properties. Consequently, the constructed S-box is suitable for block encryption algorithms. Furthermore, this S-box construction method could benefit the design of other cryptographic algorithms that utilize nonlinear transformation at their core. Although this construction method has yet to be mathematically proven, further research will continue in the future.

Conflict of Interest

The authors declare that they have no competing interests.

Funding

None.

References

[1] H. Yuan, L. Luo, and Y. Wang, "An S-box construction algorithm based on spatiotemporal chaos," in *Proceedings of 2010 International Conference on Communications and Mobile Computing*, Shenzhen, China, 2010, pp. 61-65. https://doi.org/10.1109/CMC.2010.48

[2] J. Peng, S. Jin, L. Lei, and X. Liao, "Construction and analysis of dynamic S-boxes based on spatiotemporal chaos," in *Proceedings of 2012 IEEE 11th International Conference on Cognitive Informatics and Cognitive Computing*, Kyoto, Japan, 2012, pp. 274-278. https://doi.org/10.1109/ICCI-CC.2012.6311160

[3] D. Lambic, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dynamics*, vol. 87, pp. 2407-2413, 2017. https://doi.org/10.1007/s11071-016-3199-x

[4] L. Liu, Y. Zhang, and X. Wang, "A novel method for constructing the S-box based on spatiotemporal chaotic dynamics," *Applied Sciences*, vol. 8, no. 12, article no. 2650, 2018. https://doi.org/10.3390/app8122650

[5] L. Liu and Z. Lei, "An approach for constructing the S-box using the CML system," *Journal of Physics: Conference Series*, vol. 1303, no. 1, article no. 012090, 2019. https://doi.org/10.1088/1742-6596/1303/1/012090

[6] X. Wang and J. Yang, "A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system," *Optik*, vol. 217, article no. 164884, 2020. https://doi.org/10.1016/j.ijleo.2020.164884

[7] A. Javeed, T. Shah, and Attaullah, "Design of an S-box using Rabinovich-Fabrikant system of differential equations perceiving third order nonlinearity," *Multimedia Tools and Applications*, vol. 79, pp. 6649-6660, 2020. https://doi.org/10.1007/s11042-019-08393-4

[8] Y. Si, H. Liu, and Y. Chen, "Constructing keyed strong S-Box using an enhanced quadratic map," *International Journal of Bifurcation and Chaos*, vol. 31, no. 10, article no. 2150146, 2021. https://doi.org/10.1142/S0218127421501467

[9] Z. Jiang and Q. Ding, "Construction of an S-box based on chaotic and bent functions," *Symmetry*, vol. 13, no. 4, article no. 671, 2021. https://doi.org/10.3390/sym13040671

[10] S. Deb and P. K. Behera, "Design of key-dependent bijective S-Boxes for color image cryptosystem," *Optik*, vol. 253, article no. 168548, 2022. https://doi.org/10.1016/j.ijleo.2021.168548

[11] F. Artuger and F. Ozkaynak, "SBOX-CGA: substitution box generator based on chaos and genetic algorithm," *Neural Computing and Applications*, vol. 34, no. 22, pp. 20203-20211, 2022. https://doi.org/10.1007/s00521-022-07589-4

[12] G. Zhao, S. Gao, Y. Ma, and Y. Dong, "Design of dynamic S-box based on anti-degradation chaotic system and elementary cellular automata," *Computer Science*, vol. 50, no. 11, pp. 333-339, 2023. https://doi.org/10.11896/jsjkx.220900026

[13] S. Yang, X. Tong, Z. Wang, and M. Zhang, "S-box generation algorithm based on hyperchaotic system and its application in image encryption," *Multimedia Tools and Applications*, vol. 82, no. 17, pp. 25559-25583, 2023. https://doi.org/10.1007/s11042-023-14394-1

[14] L. Zhang, C. Ma, Y. Zhao, and W. Zhao, "A novel dynamic S-box generation scheme based on quantum random walks controlled by a hyper-chaotic map," *Mathematics*, vol. 12, no. 1, article no. 84, 2023. https://doi.org/10.3390/math12010084

[15] Z. Hua, J. Li, Y. Chen, and S. Yi, "Design and application of an S-box using complete Latin square," *Nonlinear Dynamics*, vol. 104, no. 1, pp. 807-825, 2021. https://doi.org/10.1007/s11071-021-06308-3

[16] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-box based on chaotic map and backtracking," *Applied Mathematics and Computation*, vol. 376, article no. 125153, 2020. https://doi.org/10.1016/j.amc.2020.125153

[17] M. Aslam, S. Beg, A. Anjum, Z. Qadir, S. Khan, S. U. R. Malik, and M. P. Mahmud, "A strong construction of S-box using Mandelbrot set an image encryption scheme," *PeerJ Computer Science*, vol. 8, article no. e892, 2022. https://doi.org/10.7717/peerj-cs.892

[18] S. Zhou, Y. Qiu, X. Wang, and Y. Zhang, "Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box," *Nonlinear Dynamics*, vol. 111, no. 10, pp. 9571-9589, 2023. https://doi.org/10.1007/s11071-023-08312-1

[19] Y. Q. Zhang, X. Y. Wang, L. Y. Liu, Y. He, and J. Liu, "Spatiotemporal chaos of fractional order logistic equation in nonlinear coupled lattices," *Communications in Nonlinear Science and Numerical Simulation*, vol. 52, pp. 52-61, 2017. https://doi.org/10.1016/j.cnsns.2017.04.021

[20] Y. Zhang, X. Wang, L. Liu, and J. Liu, "Fractional order spatiotemporal chaos with delay in spatial nonlinear coupling," *International Journal of Bifurcation and Chaos*, vol.28, no. 2, article no. 1850020, 2018. https://doi.org/10.1142/S0218127418500207

[21] P. JoshI, D. Mukhopadhyay, and D. RoyChowdhury, "Design and analysis of a robust and efficient block cipher using cellular automata," in *Proceedings of the 20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06)*, Vienna, Austria, 2006, pp. 67-71. https://doi.org/10.1109/AINA.2006.138

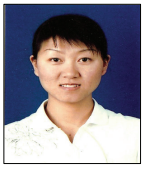
[22] P. K. Naskar, S. Bhattacharyya, D. Nandy, and A. Chaudhuri, "A robust image encryption scheme using chaotic tent map and cellular automata," *Nonlinear Dynamics*, vol. 100, pp. 2877-2898, 2020. https://doi.org/10.1007/s11071-020-05625-3

[23] J. V. Neumann, *Theory of Self-Reproducing Automata*. Champaign, IL: University of Illinois Press, 1966.

[24] C. G. Langton, "Self-reproduction in cellular automata," *Physica D: Nonlinear Phenomena*, vol. 10, no. 1-2, pp. 135-144, 1984. https://doi.org/10.1016/0167-2789(84)90256-2

[25] S. Wolfram, "Cellular automata as models of complexity," *Nature*, vol. 311, no. 5985, pp. 419-424, 1984. https://doi.org/10.1038/311419a0

[26] W. Li and N. Packard, "The structure of the elementary cellular automata rule space," *Complex Systems*, vol. 4, no. 3, pp. 281-297, 1990.



Liyan Liu **https://orcid.org/0000-0002-0279-5076**

She received a master's degree from Lanzhou Jiaotong University and is currently a professor at the City Institute, Dalian University of Technology. Her research interests include image processing using chaos theory and algorithm analysis.

Cheng Zhang **https://orcid.org/0000-0001-8439-4892**

He graduated from Dalian University of Technology and is currently a professor at the City Institute, Dalian University of Technology. He has published over 20 papers in the fields of digital image processing and virtual reality.

Yingqian Zhang **https://orcid.org/0000-0001-9568-0392**

He received his Ph.D. in computer application from Dalian University of Technology in 2014 and is currently a professor at the School of Electrical Engineering and Artificial Intelligence at Xiamen University Malaysia and the School of Information Science and Technology at Xiamen University Tan Kah Kee College. His research interests include nonlinear dynamics, cryptography, and image processing.