An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map

YING-QIAN ZHANG[ID][1], **JUN-LING HAO**[1], **AND XING-YUAN WANG**[ID][2]

[1]School of Information Science and Technology, Tan Kah Kee College, Xiamen University, Zhangzhou Campus, Xiamen 363105, China
[2]Information Science and Technology College, Dalian Maritime University, Dalian 116023, China

Corresponding author: Jun-Ling Hao (junling@xujc.com)

ABSTRACT In this work, an efficient image encryption based on S-boxes and fractional-order logistic map is proposed. The features of the fractional-order chaotic system in dynamical behaviors are exhibited. By simulation and comparison with the traditional logistic map, it is proved that the fractional-order logistic map contains larger key space and more parameters. Therefore, the fractional-order logistic system has better efficiency and security against cryptanalyst attacks. The S-boxes construction algorithm is proposed. By comparing with the S-boxes of the former schemes, the proposed S-boxes have good performance under Bits Independence Criterion (BIC), the Strict Avalanche Criterion (SAC) and the nonlinearity. Finally, the image encryption scheme is proposed for the verification. In the encryption process, the proposed S-boxes are used for scrambling and confusion. The simulation and experimental results indicate that the fractional-order method is a preferred approach to integer-order chaotic system.

INDEX TERMS Chaos, fractional-order, logistic map, S-box, image encryption.

I. INTRODUCTION

Chaos is applied in many fields, such as meteorology, physics, computer science, cryptography and so on [1], [3]–[7], [59]–[61], [80]. In recent decades, chaos and image encryption have attracted wide attention [1], [2], [39], [42], [38], [46]–[79], [81]. Chaotic systems have high initial sensitivity and randomness, so they can be used to design cryptosystem [58]–[61], [79]. Chaotic sequence can produce confusion and diffusion in the S-box [3]–[22] and image encryptions [40], [41], [43]–[45], and [47]–[55]. Therefore, the image encryption based on S-box and chaotic system is feasible.

In recent years, fractional-order differential equations and their application have attracted wide attention [25]–[34]. In comparisons with the integer-order equations, the fractional-order nonlinear dynamic systems exhibit new

The associate editor coordinating the review of this manuscript and approving it for publication was Sun Junwei[ID].

dynamic behaviors in attractors, bifurcations and chaotic behaviors. Therefore, the motivation of the study is to exam the feasibility of applying the fractional-order chaotic systems in encryptions.

In this study, we mainly apply fractional-order differential logic map to design the encryption scheme. Jakimoski and Kocarev [24] proposed a four-step method to generate S-boxes by using employing chaotic maps. Farah *et al.* [13] proposed an S-box construction method based on two dimensional chaotic map and Chen *et al.* [9] ameliorated it by using a three dimensional map. Khan *et al.* [8] proposed a method for S-boxes generation based on multi-chaotic systems. Wang *et al.* [11] proposed a new method for designing S-box based on genetic algorithm and chaotic map. Hussain *et al.* [16] used a linear fractional transformation to construct a new S-box. Tang *et al.* [23] proposed a novel method to design S-boxes using chaotic maps. The aforesaid S-box construction methods are fast because the computational complexity of low-dimensional system is less than

that of high-dimensional systems; however, low-dimensional systems have limited and fixed parameter ranges due to the integer-order systems, which leads limited and fixed key space in encryptions. To overcome these problems, Hussain *et al.* [18] proposed an efficient LFT S-boxes construction method based on chaotic logistic map with the exponent as a parameter for good nonlinearity. Hussain's algorithm [18] achieves the larger parameter space. However, its fractional exponent is not continuous, which leads the uncertainty of employing the fractional exponent as a key.

To overcome the above-mentioned shortcomings, we propose an efficient algorithm for constructing S-boxes by using the fractional-order logistic map. In comparisons with the integer-order logistic map, the fractional-order logistic map contains good features: 1) larger key space; 2) unfixed range of parameters; 3) more parameters; 4) the low computational complexity as the one-dimensional logistic map. Furthermore, it breaks the limit of the range of the parameter $\mu \in (3.57, 4]$ and has better chaotic ergodicity. Meanwhile, the fractional-order is continuous and can be used as a key parameter. Additionally, the Lyapunov exponent curves indicate the parameter μ has a much larger range in the fractional-order logistic equation than in the traditional logistic map. Therefore, the proposed algorithm has better randomness and security against common attacks.

In this paper, we thoroughly analyze the dynamics of the fractional-order Logistic map. Then, we introduce the construction scheme of S-boxes and give an efficient image encryption scheme that exemplifies the feasibility of fractional-order logistic map. To the best of our knowledge, few literatures apply the fractional-order chaotic system and S-boxes to design the encryption Scheme. The simulation and experimental results indicate that the proposed encryption scheme have high security performance.

The rest of this paper is arranged as follows: Section II introduces the fractional-order differential equation and its discretization. Section III shows features of the fractional-order differential logistic map in dynamical behaviors. In Section IV, we present the chaotic S-box generation algorithm and related performance evaluation. In Section 5, the details of the image encryption scheme are proposed as well as the experimental results and performance analysis. In Section 6, the conclusions are drawn.

II. DISCRETE THE FRACTIONAL-ORDER DIFFERENTIAL LOGISTIC MAP

Consider the following fractional differential equations [34]:

$$D^\alpha x(t) = \mu x(t)(1 - x(t)), \quad t > 0, \tag{1}$$

where $D = \frac{d}{dt}$ with the initial condition $x(0) = x_0$. In the following section, we introduce the discretization process of Eq. (1) with piecewise constant arguments

$$D^\alpha x(t) = \mu x\left(\left[\frac{t}{r}\right]r\right)\left(1 - x\left(\left[\frac{t}{r}\right]r\right)\right), \tag{2}$$

where, the initial condition $x(0) = x_0$.

Set $t \in [nr, (n + 1)r)$ and n is a positive integer with $n = 0, 1, 2, 3 \ldots$, then $\frac{t}{r} \in [n, n + 1)$. And hence, Eq. (2) is converted [34] into

$$
\begin{aligned}
x_{n+1}(t) &= x_n(nr) + I^\alpha \mu x_n(nr)(1 - x_n(nr)) \\
&= x_n(nr) + \mu x_n(nr)(1 - x_n(nr)) \times \int_0^t \frac{(t - s)^{\alpha-1}}{\Gamma(\alpha)} ds \\
&= x_n(nr) + \mu x_n(nr)(1 - x_n(nr)) \frac{(t - nr)^\alpha}{\Gamma(\alpha + 1)}.
\end{aligned}
$$

Set $t \to (n + 1)r$, the above equation can be converted into

$$x_{n+1}((n + 1)r) = x_n(nr) + \mu x_n(nr)(1 - x_n(nr)) \frac{r^\alpha}{\Gamma(\alpha + 1)}.$$

Consequently, the following iteration equation is obtained:

$$x_{n+1} = x_n + \mu x_n(1 - x_n) \frac{r^\alpha}{\Gamma(\alpha + 1)}. \tag{3}$$

III. FEATURES OF THE FRACTIONAL-ORDER DIFFERENTIAL LOGISTIC MAP IN DYNAMICAL BEHAVIORS

A. BIFURCATION

The bifurcation diagram can directly reflect the dynamic behavior of the system in various parameter assignments. The fractional-order logistic system in Eq. (3) is analyzed, shown in Fig.1, with different values of the fractional-order parameter α.

In Fig. 1, the fractional-order logistic differential equation contains the same period-doubling bifurcations approach chaos as in the classical logistic map. However, the parameter μ in the fractional-order logistic differential map breaks the range of $\mu \in (3.57, 4)$ in the traditional logistic map. In addition, the value of the chaotic sequence x_n also breaks the range of $(0, 1)$. In this work, the fractional-order parameters α and μ are chosen as secret keys to construct S-boxes. The different orders of this chaotic map contribute various ranges of parameters. Therefore, the proposed scheme has a larger key space than the traditional logistic map does.

B. LYAPUNOV EXPONENTS

Lyapunov exponent is an important index to evaluate the dynamic behavior of chaotic systems. The maximum Lyapunov exponent is related to its predictability. Any system with chaotic behaviors has at least one positive Lyapunov exponent. We calculate the Lyapunov exponent curves of the fractional-order logistic map with different values of the parameter α and the traditional logistic map in Fig. 2.

In Fig.2, the fractional-order logistic map has a much larger interval of the Lyapunov exponent than the traditional logistic map does. Therefore, the fractional-order logistic map has a large range of parameters for dynamical behaviors.

C. THE CHAOTIC TRAJECTORY

The value of the chaotic sequence x_n, shown in Fig.3, breaks the range of $(0, 1)$. It has the better randomness than the
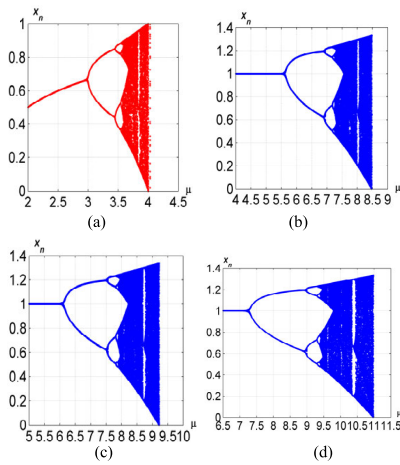
FIGURE 1. Bifurcation diagrams (a) The traditional logistic chaotic system (b) the fractional-order chaotic logistic system with $\alpha = 0.80, r = 0.25$ (c) the fractional-order chaotic logistic system with $\alpha = 0.85$, $r = 0.25$ (d) the fractional-order chaotic logistic system with $\alpha = 0.95, r = 0.25$.

FIGURE 2. Lyapunov exponent curves (a) The traditional logistic chaotic system (b) the fractional-order chaotic logistic system with $\alpha = 0.80, r = 0.25$ (c) the fractional-order chaotic logistic system with $\alpha = 0.85, r = 0.25$ (d) the fractional-order chaotic logistic system with $\alpha = 0.95, r = 0.25$.

traditional logistic system, which indicates the fractional-order logistic system has stronger energy and chaotic ergodicity. Therefore, the fractional-order logistic system is more suitable for constructing S-boxes.

IV. PROPOSED S-BOXES ALGORITHM AND ITS PERFORMANCE
A. CONSTRUCTION OF S-BOXES
The construction process of S-box is described as follows step by step:

Step 1: Set parameter μ, α, r and initial value x_0 for Eq. (3).

Step 2: Iterate Eq. (3) for n times to obtain the chaotic sequences $x_1, x_2, \ldots, x_n$.

FIGURE 3. Chaotic trajectories (a) The traditional logistic chaotic system (b) the fractional-order chaotic logistic system with $\alpha = 0.80, r = 0.25$ (c) the fractional-order chaotic logistic system with $\alpha = 0.85, r = 0.25$ (d) the fractional-order chaotic logistic system with $\alpha = 0.95, r = 0.25$.
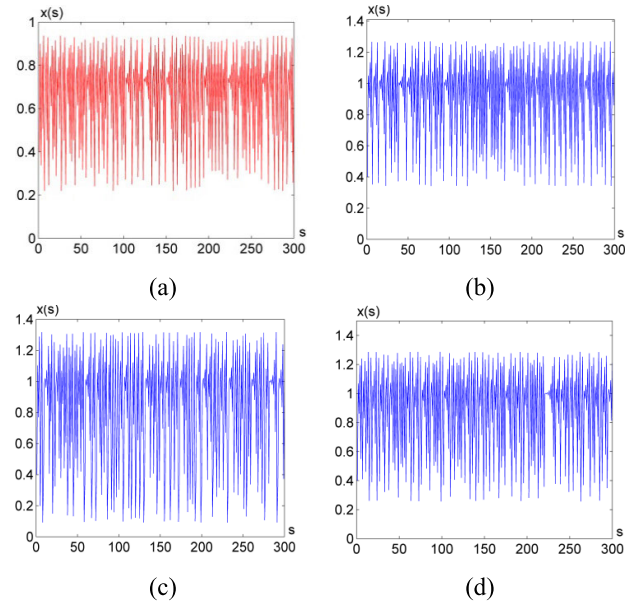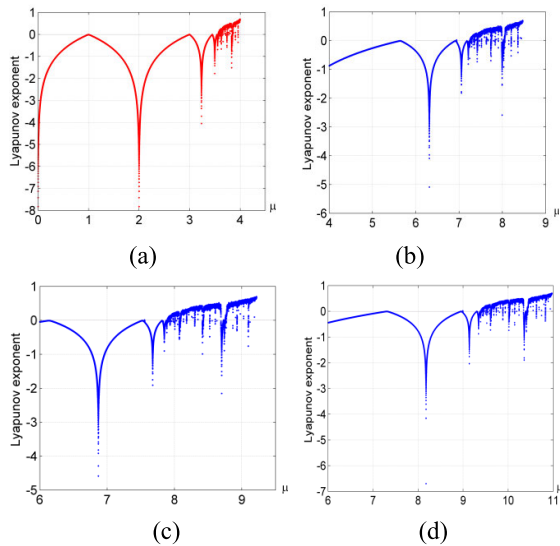
Step 3: Calculate the value $y_n = (floor(x_n \times 10^6))$ mod 256 for the S-box.

Step 4: Add y_n into the S-box if it does not exist in the S-box, otherwise the process returns to step 2 above to generate a new output value.

Step 5: Until all cell values of the S-box component are filled, the process continues.

Without loss of generality, we show two sample S-boxes designed by using the proposed algorithm and the first S-box is listed in Table 1. To evaluate the efficiency of the proposed scheme, we randomly choose different parameters to generate another S-box listed in Table 2.

B. PERFORMANCE ANALYSIS OF PROPOSED S-BOXES
Different standard performance analyses are accomplished to evaluate the strength of the proposed S-boxes. In this section, these assessments include strict avalanche criteria (SAC), bit independent criteria (BIC), nonlinearity, auto-correlation, correlation immunity, algebraic immunity, algebraic degree, fixed points, sum of squares, transparency order and NIST randomness test.

1) SAC
If half of the output bits of a Boolean function change when an input bit changes, the Boolean function is said to satisfy SAC. The ideal value for SAC is 0.5 [66]. And the SAC analyses of the proposed S-boxes are listed in Table 3.

2) BIC
In cryptographic systems, the bit independence is a very important property. As the independence between bits

TABLE 1. The S-box1 generated by proposed scheme with $\alpha = 0.95$, $\mu = 10$ $x_0 = 0.4$ and $r = 0.25$.

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

TABLE 2. The S-box2 generated by proposed scheme with $\alpha = 0.80$, $\mu = 8.3$, $x_0 = 0.4$ and $r = 0.25$.

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

increases, it becomes more difficult to attack the cryptosystem. Table 3 shows the results of BIC analysis of the proposed S-boxes.

3) NONLINEARITY

Nonlinearity is defined for Boolean functions. To resist linear cryptographic attacks, the nonlinearity of Boolean functions should be large enough. The nonlinearity test results of the proposed S-boxes are listed in Table 3 together with SAC and BIC.

As shown in Table 3, the proposed S-boxes have good performance under BIC, SAC and the nonlinearity in comparisons with Refs. [9], [24], [35]–[38]. The average SAC result of the proposed S-box2 is 0.5002, which is closer to the ideal value 0.5 than that of the obtained S-boxes in schemes [24], [35]–[38]. The fractional-order system has good ergodcity; therefore, the proposed S-box2 holds better SAC performance. Furthermore, the average values of the Nonlinearity of the proposed S-box1 and S-box2 are 105 and 104.5 respectively. The comparison in Table 3 shows that the

TABLE 3. Performance comparison for chaotic S-boxes.

S-box	SAC (min)	SAC (ave.)	SAC (max)	BIC	Nonlinearity (min)	Nonlinearity (ave.)	Nonlinearity (max)
Ref.9	0.4218	0.5000	0.6093	103.1	100	103	106
Ref.24	0.3671	0.5058	0.5975	104.2	98	103.2	108
Ref.35	0.4258	0.5007	0.5007	112	104	108	110
Ref.36	0.125	0.4812	0.4812	101.9	84	100	106
Ref.37	0.4218	0.5039	0.5039	104	98	104	104
Ref.38	0.125	0.4812	0.4812	101.9	84	100	106
Proposed S-box1	0.4063	0.5029	0.5781	102.9	102	**105**	108
Proposed S-box2	0.4219	0.5002	0.6094	103.4	96	104.25	108

TABLE 4. Fixed points test results.

S-box	Number of fixed points	
	direct	reverse
Proposed S-box1	1	3
Proposed S-box2	1	**0**

FIGURE 4. Autocorrelations (a) The proposed S-box1 (b) the proposed S-box2.

TABLE 5. Algebraic analysis of the proposed S-boxes.

S-box	Algebraic degree	Algebraic immunity	Transparency order
AES[36]	7	4	7.860
APA[36]	7	4	7.859
S8 AES[36]	7	4	7.857
Gray[36]	7	4	7.860
Xyi[36]	7	4	7.822
Prime[36]	7	4	7.756
Proposed S-box1	7	4	7.8093
Proposed S-box2	7	4	**7.7855**

proposed S-boxes have better performance than the S-boxes in Refs. [24], [35]–[38]. Additionally, the BIC results of the proposed S-box1 and S-box2 are 102.9 and 103.4 respectively. The results are also comparable or superior to those of S-boxes in literature. The proposed scheme by using the simple fractional-order logistic map has the equivalent performances as the schemes by two dimensional chaotic maps [35], three dimensional chaotic map [9].

4) FIXED POINTS
In cryptosystem, direct or reverse ($S(i) = i$ or $S(i) = 255 - i$) fixed points of S-boxes are usually undesirable, because they mean that the output is equivalent to the input. The test results of fixed points on the proposed S-boxes are presented on Table 4.

As shown in Table 4, there are very few fixed points for the proposed S-boxes. Therefore, it is impossible to attack the cryptosystem by analyzing the fixed points of the proposed S-boxes.

5) AUTOCORRELATION
Auto-correlation is a measure of the randomness of a chaotic sequence. In order to illustrate the randomness of the proposed S-boxes, the auto-correlation simulation experiments on the proposed S-boxes are carried out, and the results are shown in Fig. 4.

As shown in Fig. 4, the autocorrelation coefficients are close to 0. Therefore, the proposed S-boxes have the nature of randomness.
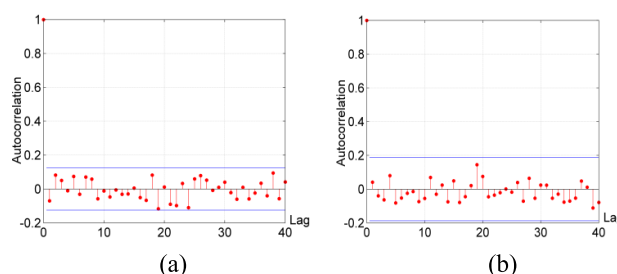
6) ALGEBRAIC IMMUNITY
It is important to measure the algebraic immunity of an S-box in cryptosystem. S-boxes with high algebraic immunity can effectively resist algebraic attacks for an encryption system. The algebraic immunity results of the proposed S-boxes are listed in Table 5.

7) ALGEBRAIC DEGREE
The S-boxes with high algebraic degree can effectively resist higher order differential attacks. Therefore, the algebraic degree of an S-box is desired to be as high as possible. The

TABLE 6. NIST 800-22 test on the proposed S-boxes.

Test name	P-value		Status	
	S-box1 (Proposed)	S-box2 (Proposed)	S-box1 (Proposed)	S-box2 (Proposed)
Approximate Entropy	0.046219	0.341143	SUCCESS	SUCCESS
Block Frequency	0.923351	0.962379	SUCCESS	SUCCESS
Cumulative Sums	0.999477	0.989269	SUCCESS	SUCCESS
FFT	0.871131	0.440973	SUCCESS	SUCCESS
Frequency	1.000000	1.000000	SUCCESS	SUCCESS
Linear Complexity	0.919679	0.919679	SUCCESS	SUCCESS
Longest Run	0.288436	0.546438	SUCCESS	SUCCESS
Non-Overlapping Template	0.856028	0.850132	SUCCESS	SUCCESS
Overlapping Template	0.107608	0.488416	SUCCESS	SUCCESS
Rank	0.741908	0.481248	SUCCESS	SUCCESS
Runs	0.929568	0.507387	SUCCESS	SUCCESS
Serial (P-value 1)	0.690775	0.084921	SUCCESS	SUCCESS
Serial (P-value 2)	0.568756	0.360630	SUCCESS	SUCCESS
Random Excursions	——	——	NOT APPLICABLE	NOT APPLICABLE
Random Excursions Variant	——	——	NOT APPLICABLE	NOT APPLICABLE
Universal	——	——	NOT APPLICABLE	NOT APPLICABLE

algebraic degree results of the proposed S-boxes are also listed in Table 5.

8) TRANSPARENCY ORDER
The transparency order (TO) of S-box can be used to illustrate the resistance against DPA attack. The lower the value of the TO is, the higher the resistance against DPA attack of an S-box would be. The TO value of m?mS-box can be calculated as follows [36]:

$$TO = \max_{\beta \in F_2^m} \left(|m - 2wt(\beta)| - \frac{1}{2^{2m} - 2^m} \right.$$

$$\left. \times \sum_{a \in F_2^m - \{0\}} \left| \sum_{v \in F_2^m, wt(v)=1} (-1)^{v \cdot \beta} W_{D_a S}(0, v) \right| \right)$$

where F_2^m is m dimensional vector space in binary finite field and $wt(\beta)$ is the Hamming weight of vector β. The transparency orders of the proposed S-boxes are also listed in Table 5.

As shown in Table 5, the algebraic degree values and the algebraic immunity values of the proposed S-boxes are 7 and 4, respectively, which are highly desirable. Therefore, the proposed S-boxes can reduce the possibilities of differential attacks and algebraic attacks. Additionally, the proposed S-boxes have lower TO values among the existing S-boxes, which further verifies the safety of the proposed S-boxes.

9) NIST TEST
NIST test is used to analyze the feature of randomness. We have performed NIST-800-22 test on the proposed S-boxes and the results are presented in Table 6. It can be seen that 12 tests have passed successfully. However, due to the insufficient sequence length, Random Excursions Test, Random Excursions Variant Test and Universal Statistical Test are not applicable.

V. PROPOSED IMAGE ENCRYPTION SCHEME
The proposed S-boxes are suitable for designing cryptosystem. This section exemplifies a specific application of the proposed S-boxes in image encryption.

A. GENERATION OF THE SECRET KEY
Our cryptosystem utilizes a 128-bit secret key K, which is generated by the hash algorithm MD2. For plaintext images, even if only one bit is changed, its hash value will change completely. By dividing the 128-bit secret key into 16-bit blocks (k_i), K can be expressed as follows:

$$K = k_1, k_2, \ldots, k_8.$$

The new initial values can be obtained by the following formula:

$$\alpha' = \alpha + (bin2dec\,(k_1 \oplus k_2)) \times 10^{-6}$$
$$\mu' = \mu + (bin2dec\,(k_3 \oplus k_4)) \times 10^{-6}$$
$$x_0' = x_0 + (bin2dec\,(k_5 \oplus k_6)) \times 10^{-6}$$
$$r' = r + (bin2dec\,(k_7 \oplus k_8)) \times 10^{-6}$$

where α, u, x_0 and r are the initial given values.

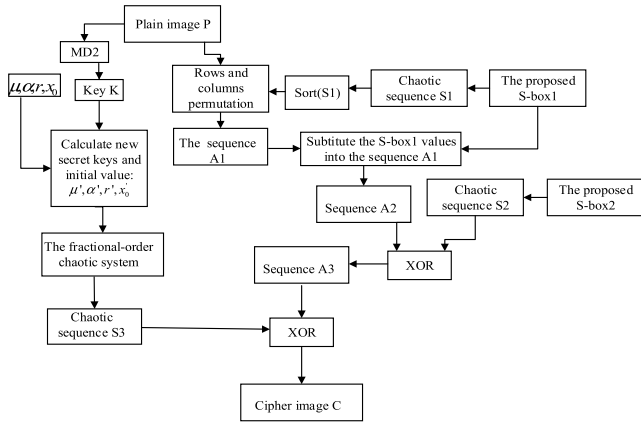**FIGURE 5.** Flowchart of encryption algorithm.

FIGURE 6. Flowchart of decryption algorithm.

B. IMAGE ENCRYPTION ALGORITHM

The proposed image encryption algorithm includes four parts. Firstly, the key sequence K and the new initial values are generated by the hash algorithm. Secondly, the rows and columns of the plain image are permuted by using the proposed S-box1 and the sort function. Thirdly, the pixel values of the plain image are replaced by the values in the proposed S-box1. Fourthly, the ciphered image is obtained by XOR operations and chaotic diffusions. The entire flowchart of the encryption algorithm is shown in Fig. 5.

Without loss of generality, assuming that the size of the original image is $M \times N$, the image encryption algorithm based on the proposed S-boxes consists of the following steps:

Condition: Suppose the plain-image P is of size $M \times N$ and A_1 is a matrix corresponding to the plain image P. Set S_1 is the chaotic sequence corresponding to the proposed S-box1 and S_2 is the chaotic sequence corresponding to the proposed S-box2.

Step 1: Generate the key sequence K and the initial values α', u', x_0' and r' of the fractional-order logistic system according to Sect. 5.1.

Step 2: Set $[S_1, NUM] = sort(S_1)$, $A_2 = A_1$, $i = 1$, $Row = M/256$ and $Col = N/256$.

Step 3: Permute the rows and columns of the plain image according to the following formula:

$$A_2(256 \times j + i, :) = A_1(NUM(i) + 256 \times j, :)$$
$$A_2(:, 256 \times j + i) = A_1(:, NUM(i) + 256 \times j)$$

where $i = 1, 2, \ldots, 256$ and $j = 0, 1, 2, \ldots, Row - 1$, $Col - 1$.

Step 4: Let $A_2 = reshape(A_2, M \times N, 1)$ and convert the elements of the matrix A_2 into 8-bits binary numbers and set $i = 1$. Choose four even digits and four odd digits of the ith 8-bit binary digits to form two four-bit binary digits, respectively. Then, these two decimal digits m and n are obtained by converting the two four-digit binary digits into decimal digits.
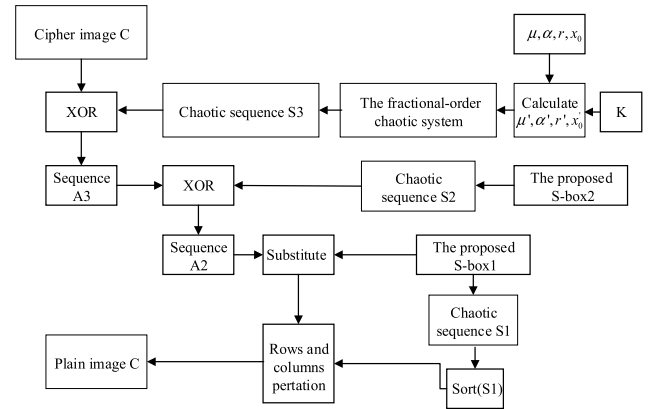
Step 5: Set $m = m + 1$, $n = n + 1$, and then, substitute the (m, n) element of the proposed S-box1 for $A_2(i)$ in A_2. Set $i = i + 1$, and return to step 4 until i reaches $M \times N$.

Step 6: Set $A_3 = A_2$. Encrypt the $(256 \times j + i)$th element in A_2 according to the following equation:

$$A_3(256 \times j + i) = A_2(256 \times j + i) \oplus S_2(i),$$

where $i = 1, 2, \ldots, 256$ and $j = 0, 1, 2, \ldots, (M \times N/256) - 1$.

Step 7: Generate the chaotic sequence S_3 whose length is 15000 by using the Fractional-order Logistic system with the initial values α', u', x_0' and r'.

Step 8: Set $N_1 = floor(M \times N/15000)$ and $A_4 = A_3$. Encrypt the first $15000 \times N_1$ elements in A_3 according to the following equation:

$$A_4(15000 \times j + i) = A_3(15000 \times j + i) \oplus S_3(i),$$

where $i = 1, 2, \ldots, 15000$ and $j = 0, 1, 2, \ldots, N_1 - 1$.

Step 9: Set $N_2 = \mod(M \times N, 15000)$. Encrypt the last N_2 elements in A_3 according to the following equation:

$$A_4(15000 \times N_1 + i) = A_3(15000 \times N_1 + i) \oplus S_3(i),$$

where $i = 1, 2, \ldots, N_2$.

Finally, the ciphered image is obtained.

In addition, this encryption scheme is also applicable to color images and binary images. A color image can be divided into three channels (red, green and blue) and encrypted separately by applying the proposed encryption scheme correspondingly. Then the final cipher image can be obtained by combining the red, green and blue cipher images.

C. DECRYPTION PROCEDURE

The decryption process is the reverse procedure to the encryption process. By using the secret keys, the receivers decrypt the cipher image according to the reverse operations of the encryption algorithm. The entire decryption algorithm is presented in Fig. 6.

TABLE 7. χ^2-test results for ciphered images.

Ciphered images	Lena	BARB
χ^2-test	238.4043	246.3359

D. SIMULATION EXPERIMENTS AND PERFORMANCE ANALYSIS

The performance analysis of the proposed encryption algorithm includes key space analysis, histograms, correlation coefficients and differential analysis. In the experiments, the test images are the 512×512 images with an 8-bit gray scale.

1) SECRET KEY SPACE

The total number of different keys used in the encryption process represents the size of the key space. For any encryption system, the key space must be large enough to resist violent attacks. During the construction of S-boxes, the secret keys include three decimal parameters μ, α, r and the initial value x_0 for Eq. (3). If the accuracy of the computer is 10^{16}, for the construction of an S-box, the total key space $H_1 \geq \left(10^{16}\right)^4 = 10^{64}$. In the proposed encryption algorithm, due to using two different S-boxes and the 128-bit secret key, the total key space $H_2 > 0.5 \times H_1 \times H_1 = 0.5 \times 10^{128} > 2^{383}$. To resist violent attacks, the size of the secret key space should not be less than 2^{100} [47]. Obviously, the proposed encryption algorithm has enough key space to resist all kinds of violent attacks.

2) HISTOGRAM ANALYSIS

The histogram represents the distribution characteristics of the pixel intensity of an image. To resist any statistical attacks, a secure encryption system must ensure that the encrypted image has a uniform histogram. The histograms of the plain image Lena, BARB and their cipher images are presented in Fig. 7. Obviously, the gray scale values of the cipher images are uniformly distributed in Fig. 7 (d, h). Therefore, there is a significant difference from the distribution of the plain image Lena and BARB in Fig. 7 (a, e). Additionally, as shown in Fig. 7 (i − k), the proposed encryption scheme is also effective for binary images.

In order to further verify the uniform distribution of ciphered image pixels, we have performed the χ^2-test on the ciphered images Lena and BARB. The value of the χ^2-test for a ciphered image is calculated according to the following formula:

$$\chi^2 = \sum_{0}^{255} \frac{(v_i - v_0)}{v_0} \qquad (4)$$

where $v_0 = \dfrac{M \times N}{256}$, $M \times N$ is the size of ciphered image and v_i is the observed frequency of a pixel value $i (i = 0, 1, 2, \ldots, 255.)$. The results of the test are listed in Table 7.
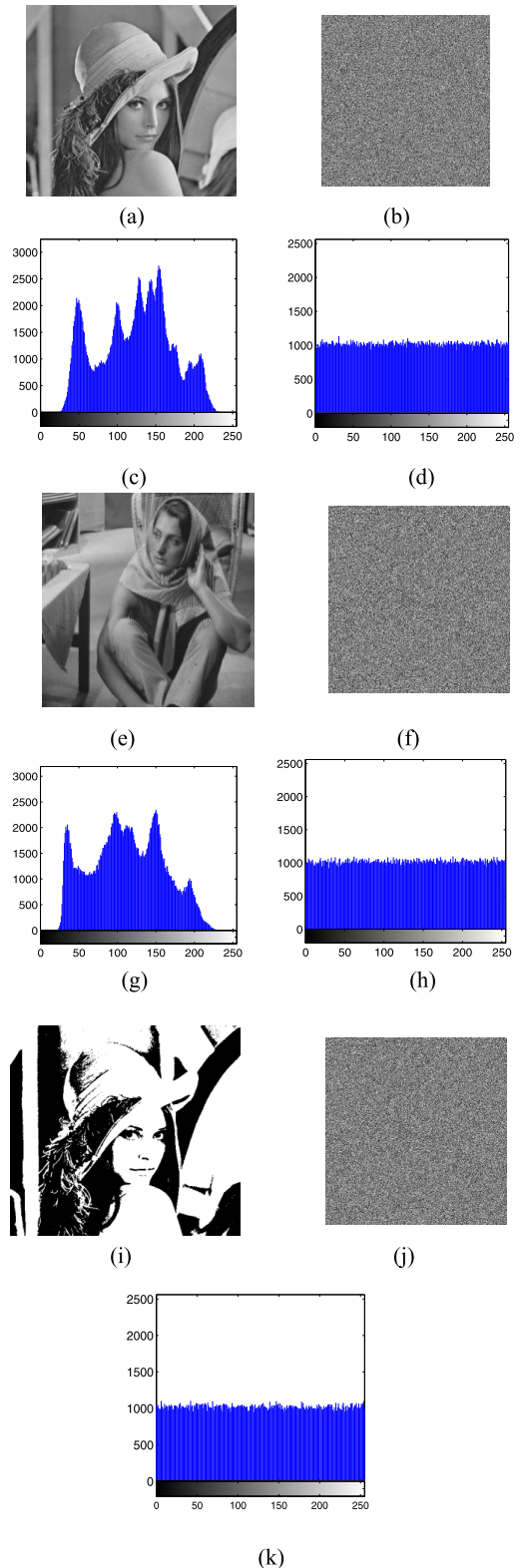

FIGURE 7. Histograms for the plain-image and ciphered image (a) Plain-image Lena (b) the ciphered image of Lena (c) the histogram of Lena (d) the histogram of ciphered image of Lena (e) plain-image BARB (f) the ciphered image of BARB (g) the histogram of BARB (h) the histogram of ciphered image of BARB (i) the binary image Lena (j) the ciphered image of binary image Lena (k) the histogram of ciphered image of binary image Lena.

TABLE 8. Correlation comparison of different encryption algorithms.

Test image	Direction	Plain-image	Ciphered image				
			Ref.[50]	Ref.[54]	Ref.[55]	Ref.[63]	Proposed
Lena	Horizontal	0.9718	-0.0045	-0.0071	0.0056	-0.0054	0.0045
	Vertical	0.9865	-1.62e-04	- 0.0045	0.0065	-0.0098	**0.0018**
	Diagonal	0.9620	0.0053	0.0229	0.0073	-0.0441	-0.0058
BARB	Horizontal	0.8534	——	——	——	——	**-0.0018**
	Vertical	0.9611	——	——	——	——	0.0091
	Diagonal	0.8353	——	——	——	——	-0.0129

TABLE 9. Comparison for Information entropy of different encryption algorithms.

Test image	Plain-image	Ciphered image				
		Ref.[51]	Ref.[52]	Ref.[53]	Ref.[63]	Proposed
Lena	7.4461	7.9968	7.9893	7.9972	7.9978	7.9992
BARB	7.4649	—	—	—	—	**7.9993**

As shown in Table 7, the χ^2-test values are lower than the critical value 293.25 [57], which indicates the proposed encryption scheme has passed the χ^2-test. Therefore, the pixel value distribution is uniform in the encrypted images.

3) CORRELATION ANALYSIS OF TWO ADJACENT PIXELS

In horizontal, vertical and diagonal directions of a plain image, there is a high correlation between adjacent pixels. To resist statistical attacks, the correlation between adjacent pixels of a ciphered image should be as low as possible. We perform the following steps to calculate the correlation between plain and ciphered images. First, randomly choose 3000 pairs of two adjacent pixels of an image. Then, calculate the correlation coefficient according to the following formula [64], [70]–[72], [76]- [77]:

$$r_{xy} = \text{cov}(x, y)/\sqrt{D(x)D(y)}, \tag{5}$$

where x and y are two adjacent pixels of an image with

$$E(x) = \frac{1}{3000} \sum_{i=1}^{3000} x_i, \tag{6}$$

$$D(x) = \frac{1}{3000} \sum_{i=1}^{3000} (x_i - E(x))^2, \tag{7}$$

$$\text{cov}(x, y) = \frac{1}{3000} \sum_{i=1}^{3000} (x_i - E(x))(y_i - E(y)). \tag{8}$$

By using the formulas (5)-(8) and the proposed encryption algorithm, the correlation coefficients of plain images Lena, BARB and their ciphered images are calculated and the results are presented in Table 8. Clearly, the correlation coefficients of the plain image approximate to 1, while those of the ciphered image approximate to 0 along all three directions. Therefore, the correlation between adjacent pixels of the ciphered images is extremely low, which means that the proposed encryption scheme has good confusion and diffusion properties.

4) INFORMATION ENTROPY ANALYSIS

Information entropy is the most important index to measure randomness. Calculate the information entropy according to the following formula [59], [60], [76], [78], [38]:

$$H(m) = -\sum_{i=0}^{2^n-1} p(m_i) \log_2(p(m_i)), \tag{9}$$

where m is the source of information, n is the bit number required for the symbol m_i, and $p(m_i)$ denotes the probability of symbol m_i. If all the pixels are uniformly distributed for an 8-bit gray image, the maximum entropy is 8, which means that the information is random. For a ciphered image, the information entropy should be close to 8. The closer to 8, the less possible the attacker will decrypt the cipher image.

By using Eq. (9), the information entropies of the plain images and the cipher images are calculated. The results are presented in Table 9. Obviously, the entropies of the ciphered images approximate to the ideal value 8, which means that the proposed scheme has the desired information entropy properties.

5) DIFFERENTIAL ATTACKS ANALYSES

To defend against a differential attack, a good encryption scheme needs to ensure that any minor modification of the plain image will lead to a significant difference in the ciphered images. The proposed encryption scheme can make

TABLE 10. NPCR and UACI of Lena and BARB with only one pixel change.

Pixel change (position)	NPCR			UACI		
	Lena	BARB	Mean	Lena	BARB	Mean
(1,1)	0.995621	0.995239	0.995430	0.334873	0.333325	0.334099
(256,256)	0.996212	0.994877	0.9955445	0.337386	0.330743	0.3340645
(180,320)	0.995731	0.994514	0.9951225	**0.334887**	0.333823	0.3343550

TABLE 11. NIST 800-22 test on the ciphered images.

Test name	P-value		Status	
	Lena	BARB	Lena	BARB
Approximate Entropy	0.454929	0.522945	SUCCESS	SUCCESS
Block Frequency	0.716477	0.423170	SUCCESS	SUCCESS
Cumulative Sums	0.082458	0.841699	SUCCESS	SUCCESS
FFT	0.769706	0.718900	SUCCESS	SUCCESS
Frequency	0.093078	0.759150	SUCCESS	SUCCESS
Linear Complexity	0.909126	0.851863	SUCCESS	SUCCESS
Longest Run	0.629803	0.109591	SUCCESS	SUCCESS
Non-Overlapping Template	0.554310	0.836963	SUCCESS	SUCCESS
Overlapping Template	0.421683	0.302966	SUCCESS	SUCCESS
Rank	0.220752	0.756578	SUCCESS	SUCCESS
Runs	0.339510	0.758050	SUCCESS	SUCCESS
Serial （P-value 1）	0.842798	0.806737	SUCCESS	SUCCESS
Serial （P-value 2）	0.440894	0.580714	SUCCESS	SUCCESS
Random Excursions	0.566901	0.150070	SUCCESS	SUCCESS
Random Excursions Variant	0.881787	0.309656	SUCCESS	SUCCESS
Universal	0.854741	0.410109	SUCCESS	SUCCESS

two ciphered images be different completely, even if their plain images have only one different pixel. Let c_1 and c_2 be the two ciphered images and calculate the measure value of the sensitivity to a minor change of the plain image according to Eq. (10) and Eq. (11) [63], [69], [76] and [38]:

$$NPCR = \frac{\sum\limits_{ij} D(i,j)}{M \times N} \times 100\%, \quad (10)$$

$$UACI = \frac{1}{M \times N \times 255} \sum\limits_{ij} [c_1(i,j) - c_2(i,j)] \times 100\% \quad (11)$$

where $D(i,j) = \begin{cases} 1, c_1(i,j) \neq c_2(i,j) \\ 0, \text{otherwise} \end{cases}$.

Without loss of generality, choose the Lena image and BARB image as the test images and calculate the values of NPCR and UACI. The results of NPCR and UACI are listed in Table 10. As observed, the proposed algorithm obtains the mean NPCR at over 99.5% and the mean UACI at over 33.4%. Therefore, the proposed encryption algorithm has

good NPCR and UACI scores, which means that there is strong robustness against differential attack.

6) CIPHERTEXT-ONLY ATTACK ANALYSES

Ciphertext-only attack refers to the exhaustive attack when only the encrypted text is known. Attacker tries a list of ciphertext to deduce the original secret key. As mentioned in the above sections, the proposed encryption scheme not only has fast encryption speed, but also has many keys and large key space. Additionally, the proposed cryptosystem applies a 128-bit secret key K generated by the hash algorithm MD2, which indicates the secret key is one-time pad. By Shannon's theory, ciphertext only attack cannot be carried out. So the proposed encryption scheme is secure.

7) NIST TEST

In order to test the pixels' randomness of the ciphered images, we have performed NIST-800-22 test on the ciphered images. The test results are presented in Table 11. It can be seen that all the tests have passed successfully.

TABLE 12. The results of MAE, MSE PSNR and SSIM for ciphered images.

Image	MAE	MSE	PSNR	SSIM
Lena	73.07	7771.88	8.7793	0.0095
BARB	73.56	7919.47	8.8269	0.0095

TABLE 13. The results of SSIM and NCC for decrypted images.

Image	Algorithm	SSIM	NCC
Lena	Ref.[56]	**1.0000**	0.9920
	Proposed	**1.0000**	**1.0000**
BARB	Ref.[56]	**1.0000**	0.9927
	Proposed	**1.0000**	**1.0000**

8) MAE, MSE, PSNR, SSIM AND NCC ANALYSES

Mean absolute error (MAE) and mean square error (MSE) can be used to evaluate the error of pixel values between two images. For a secure encryption system, the values of MSE and MAE between plaintext and ciphered images should be sufficiently large. Peak signal-to-noise ratio (PSNR) is a measure for the peak error between plain and ciphered images. Considering the huge difference between plain and ciphered images, the PSNR of plain and ciphered images should be low. Calculate the values of MAE, MSE and PSNR according to Eq. (12), Eq. (13) and Eq. (14) [69], [71]– [73], [77], and [38]:

$$MAE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|p_{ij} - c_{ij}|}{M \times N}, \quad (12)$$

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(p_{ij} - c_{ij})^2}{M \times N}, \quad (13)$$

$$PSNR = 20\log_{10}\left[\frac{I_{\max}}{\sqrt{MSE}}\right], \quad (14)$$

where p_{ij} and c_{ij} are the pixels of plain and ciphered images at the position (i, j), respectively, and $I_{\max}$ is the maximum pixel's estimation of image.

Both structural similarity index metric (SSIM) and normalized cross-correlation (NCC) can be used to measure the similarity two images. The difference is that SSIM focuses on the similarity of structure, contrast and luminance between images, while NCC focuses on the similarity of pixel values between images. Calculate the values of SSIM and NCC according to Eq. (15), and Eq. (16) [69], [71], [72]:

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}p_{ij} \times c_{ij}}{\sum_{i=1}^{M}\sum_{j=1}^{N}p_{ij}^2} \quad (15)$$

$$SSIM = \left(\frac{2\mu_p\mu_c + c_1}{\mu_p^2 + \mu_c^2 + c_1}\right)\left(\frac{2\sigma_{pc} + c_2}{\sigma_p^2 + \sigma_c^2 + c_2}\right) \quad (16)$$

where p_{ij} and c_{ij} are two images, μ_p, μ_c are their mean values, respectively, and σ_{pc} is the standard deviation.

Table 12 presents the results of MAE, MSE, PSNR and SSIM between the plain and ciphered images. Table 13 presents the results of SSIM and NCC between the ciphered and decrypted images. These show that the proposed encryption scheme achieves the desired effect.

9) CORRELATION BETWEEN PLAIN AND CIPHERED IMAGES AND CONTRAST, ENERGY ANALYSES

The correlation between plain and ciphered images is analyzed in this subsection. Calculate the correlation coefficient according to Eq. (17) [62]– [64], [72]:

$$Corr = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(p_{ij} - \bar{p})(c_{ij} - \bar{c})}{\sqrt{(\sum_{i=1}^{M}\sum_{j=1}^{N}(p_{ij} - \bar{p})^2)(\sum_{i=1}^{M}\sum_{j=1}^{N}(c_{ij} - \bar{c})^2}}, \quad (17)$$

where $\bar{p}, \bar{c}$ are the average of plain and ciphered images, respectively. The results of the correlation are listed in Table 14. Clearly, the correlation coefficients between the plain and ciphered images are close to 0, which means that the proposed encryption scheme has the desired correlation property.

The contrast analysis calculates the intensity difference between pixels and their neighboring pixels in the whole image [58]. The high contrast value reflects the superiority of Y. Q. Zhang *et al.*: An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map the image encryption scheme. The contrast value can be calculated by Eq. (18) [62], [63], [69] and [72]:

$$Contrast = \sum_{i=1}^{M}\sum_{j=1}^{N}|i - j|^2 p_{ij}, \quad (18)$$

where p_{ij} is given as the number of gray-level co-occurrence matrices (GLCM), M and N represent the number of rows and columns of GLCM, respectively. The contrast values of the proposed encryption scheme are listed in Table 14.

The energy analysis quantifies the information of ciphered image and reflects the disorder degree of ciphered image. The lower energy value of ciphered image indicates the higher encryption quality. The energy value is calculated by Eq. (19) [69], [72]:

$$Energy = \sum_{i,j} p_{ij}^2, \quad (19)$$

where p_{ij} is given as the number of GLCM. The energy values of the ciphered images given by the proposed encryption scheme are also listed in Table 14.

As shown in Table 14, the energy values are closer to 0 and the contrast values are much larger in the proposed

TABLE 14. The results of contrast, energy and correlation for ciphered images.

Image	Algorithm	Contrast	Energy	Correlation
Lena	Ref.[82]	4.9454	0.4263	—
	Ref.[83]	8.7587	0.2365	—
	Proposed	**10.4880**	**0.0156**	-0.0018
BARB	Ref.[82]	—	—	—
	Ref.[83]	—	—	—
	Proposed	10.4570	0.0156	-0.0007

scheme than in schemes [82], [83]. Therefore, the proposed encryption scheme has high security.

VI. CONCLUSION

In this paper, we not only propose an efficient construction scheme of S-boxes based on the fractional-order logistic system, but also present an image encryption scheme using the fractional-order Logistic system, S-boxes and Secure Hash Algorithm MD2. The simulation and experimental results of S-boxes indicate that the proposed S-boxes have better BIC property, SAC property and Nonlinearity property. Furthermore, the proposed construction scheme of S-boxes could find other S-boxes satisfying perfect cryptographic properties by changing the order of the fractional-order differential equation. Moreover, from the above discussion, not only the proposed S-boxes construction scheme but also the proposed image encryption algorithm is more efficient. Although the high dimensions chaotic systems may have large parameter space, the expense of more computational complexity. Therefore, the proposed algorithms based on the fractional-order logistic map have advantages in both better ability to withstand common cryptanalyst attacks and less execution time. In future practical research work, we will intend to apply the fractional-order chaotic logistic system to circuit board design.
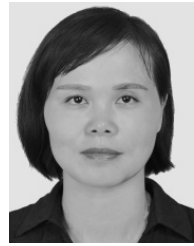
REFERENCES

[1] J. M. Amigó, L. Kocarev, and J. Szczepanski, "Theory and practice of chaotic cryptography," *Phys. Lett. A*, vol. 366, no. 3, pp. 211–216, Jun. 2007.

[2] J. Gleick and R. C. Hilborn, "Making a new science," *Phys. Today*, vol. 41, no. 2, p. 79, 1988.

[3] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a discrete chaotic cryptosystem using external key," *Phys. Lett. A*, vol. 319, nos. 3–4, pp. 334–339, Dec. 2003.

[4] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a chaotic secure communication system," *Phys. Lett. A*, vol. 306, no. 4, pp. 200–205, Jan. 2003.

[5] A. D. Pano-Azucena, J. de Jesus Rangel-Magdaleno, E. Tlelo-Cuautle, and A. de Jesus Quintas-Valles, "Arduino-based chaotic secure communication system using multi-directional multi-scroll chaotic oscillators," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2203–2217, Mar. 2017.

[6] M. R. K. Ariffin and M. S. M. Noorani, "Modified baptista type chaotic cryptosystem via matrix secret key," *Phys. Lett. A*, vol. 372, no. 33, pp. 5427–5430, Aug. 2008.

[7] M. S. Baptista, "Cryptography with chaos," *Phys. Lett. A*, vol. 240, pp. 50–54, Mar. 1998.

[8] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, and I. Hussain, "A novel technique for the construction of strong S-boxes based on chaotic lorenz systems," *Nonlinear Dyn.*, vol. 70, no. 3, pp. 2303–2311, Nov. 2012.

[9] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps," *Chaos, Solitons Fractals*, vol. 31, no. 3, pp. 571–579, Feb. 2007.

[10] Y. Wang, K.-W. Wong, X. Liao, and T. Xiang, "A block cipher with dynamic S-boxes based on tent map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 7, pp. 3089–3099, Jul. 2009.

[11] Y. Wang, K.-W. Wong, C. Li, and Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," *Phys. Lett. A*, vol. 376, nos. 6–7, pp. 827–833, Jan. 2012.

[12] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos," *Multimedia Tools Appl.*, vol. 74, no. 3, pp. 781–811, Feb. 2015.

[13] T. Farah, R. Rhouma, and S. Belghith, "A novel method for designing S-box based on chaotic map and teaching-learning-based optimization," *Nonlinear Dyn.*, vol. 88, no. 2, pp. 1059–1074, Apr. 2017.

[14] D. He, Y. Chen, and J. Chen, "Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol," *Nonlinear Dyn.*, vol. 69, no. 3, pp. 1149–1157, Aug. 2012.

[15] I. Hussain, T. Shah, and H. Mahmood, "A new algorithm to construct secure keys for AES," *Int. J. Contemp. Math. Sci.*, vol. 5, no. 26, pp. 1263–1270, 2010.

[16] I. Hussain, T. Shah, M. A. Gondal, M. Khan, and W. A. Khan, "Construction of new S-box using a linear fractional transformation," *World Appl. Sci. J.*, vol. 14, no. 12, pp. 1779–1785, 2013.

[17] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "Some analysis of S-box based on residue of prime numbers," *Proc. Pakistan Acad. Sci.*, vol. 48, no. 2, pp. 111–115, 2011.

[18] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "An efficient approach for the construction of LFT S-boxes using chaotic logistic map," *Nonlinear Dyn.*, vol. 71, nos. 1–2, pp. 133–140, Jan. 2013.

[19] X. Wang, X. Wang, J. Zhao, and Z. Zhang, "Chaotic encryption algorithm based on alternant of stream cipher and block cipher," *Nonlinear Dyn.*, vol. 63, no. 4, pp. 587–597, Mar. 2011.

[20] S. Li, X. Mou, and Y. Cai, "Improving security of a chaotic encryption approach," *Phys. Lett. A*, vol. 290, nos. 3–4, pp. 127–133, Nov. 2001.

[21] R. Hasimoto-Beltrán, "High-performance multimedia encryption system based on chaos," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 18, no. 2, Jun. 2008, Art. no. 023110.

[22] R. Rhouma and B. Safya, "On the security of a spatiotemporal chaotic cryptosystem," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 17, no. 3, Sep. 2007, Art. no. 033117.

[23] G. Tang, X. Liao, and Y. Chen, "A novel method for designing S-boxes based on chaotic maps," *Chaos, Solitons Fractals*, vol. 23, no. 2, pp. 413–419, Jan. 2005.

[24] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 2, pp. 163–169, Feb. 2001.

[25] F.-R. Lin and H. Qu, "A Runge–Kutta Gegenbauer spectral method for nonlinear fractional differential equations with Riesz fractional derivatives," *Int. J. Comput. Math.*, vol. 96, no. 2, pp. 417–435, Feb. 2019.

[26] M. El-Shahed and W. M. Shammakh, "Existence of positive solutions of the boundary value problem for nonlinear fractional differential equations," *Abstract Appl. Anal.*, vol. 25, no. 2, pp. 1363–1375, 2011.

[27] J. Ruan, K. Sun, J. Mou, S. He, and L. Zhang, "Fractional-order simplest memristor-based chaotic circuit with new derivative," *Eur. Phys. J. Plus*, vol. 133, no. 1, p. 3, Jan. 2018.

[28] R. Khalil, M. A. Horani, A. Yousef, and M. Sababheh, "A new definition of fractional derivative," *J. Comput. Appl. Math.*, vol. 264, no. 5, pp. 65–70, 2014.

[29] J. Singh, D. Kumar, and J. J. Nieto, "Analysis of an El Nino-Southern oscillation model with a new fractional derivative," *Chaos, Solitons Fractals*, vol. 99, pp. 109–115, Jun. 2017.

[30] D. Kumar, J. Singh, and D. Baleanu, "A hybrid computational approach for Klein–Gordon equations on cantor sets," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 511–517, Jan. 2017.

[31] V. E. Tarasov, "Lattice fractional calculus," *Appl. Math. Comput.*, vol. 257, pp. 12–33, Apr. 2015.

[32] H. M. Srivastava, D. Kumar, and J. Singh, "An efficient analytical technique for fractional model of vibration equation," *Appl. Math. Model.*, vol. 45, pp. 192–204, May 2017.

[33] C. Li, Z. Zhao, and Y. Chen, "Numerical approximation of nonlinear fractional differential equations with subdiffusion and superdiffusion," *Comput. Math. Appl.*, vol. 62, no. 3, pp. 855–875, Aug. 2011.

[34] Z. F. El Raheem and S. M. Salman, "On a discretization process of fractional-order logistic differential equation," *J. Egyptian Math. Soc.*, vol. 22, no. 3, pp. 407–412, Oct. 2014.

[35] X. Zhang, Z. Zhao, and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer," *Signal Process., Image Commun.*, vol. 29, no. 8, pp. 902–913, Sep. 2014.

[36] M. Khan, T. Shah, and S. I. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption," *Neural Comput. Appl.*, vol. 27, no. 3, pp. 677–685, Apr. 2016.

[37] M. Khan, T. Shah, and S. I. Batool, "A new implementation of chaotic S-boxes in CAPTCHA," *Signal, Image Video Process.*, vol. 10, no. 2, pp. 293–300, Feb. 2016.

[38] M. Khan, "A novel image encryption scheme based on multiple chaotic S-boxes," *Nonlinear Dyn.*, vol. 82, nos. 1–2, pp. 527–533, Oct. 2015.

[39] Y. Zhang, X. Wang, L. Liu, and J. Liu, "Fractional order spatiotemporal chaos with delay in spatial nonlinear coupling," *Int. J. Bifurcation Chaos*, vol. 28, no. 02, Feb. 2018, Art. no. 1850020.

[40] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Process.*, vol. 113, pp. 104–112, Aug. 2015.

[41] Y. He, Y.-Q. Zhang, and X.-Y. Wang, "A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system," *Neural Comput. Appl.*, vol. 32, no. 1, pp. 247–260, Jan. 2020.

[42] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.

[43] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," 2014, *arXiv:1410.7694*. [Online]. Available: http://arxiv.org/abs/1410.7694

[44] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultimediaMag.*, vol. 25, no. 4, pp. 46–56, Oct. 2018.

[45] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[46] H. Liu, A. Kadir, and J. Liu, "Keyed hash function using hyper chaotic system with time-varying parameters perturbation," *IEEE Access*, vol. 7, pp. 37211–37219, 2019.

[47] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 511–529, Jul. 2015.

[48] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.

[49] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image encryption using Josephus problem and filtering diffusion," *IEEE Access*, vol. 7, pp. 8660–8674, 2019.

[50] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[51] X. Wang and H.-L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.*, vol. 342, pp. 51–60, May 2015.

[52] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.

[53] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.

[54] X. Liu, Y. Cao, P. Lu, X. Lu, and Y. Li, "Optical image encryption technique based on compressed sensing and arnold transformation," *Optik*, vol. 124, no. 24, pp. 6590–6593, Dec. 2013.

[55] X. Wang and H.-L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dyn.*, vol. 83, nos. 1–2, pp. 333–346, Jan. 2016.

[56] B. Yang and X. Liao, "A new color image encryption scheme based on logistic map over the finite field ZN," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21803–21821, Aug. 2018.

[57] X.-Y. Wang, P. Li, Y.-Q. Zhang, L.-Y. Liu, H. Zhang, and X. Wang, "A novel color image encryption scheme using DNA permutation based on the lorenz system," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 6243–6265, Mar. 2018.

[58] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel image encryption based on lorenz equation, gingerbreadman chaotic map and S_8 permutation," *J. Intell. Fuzzy Syst.*, vol. 33, no. 6, pp. 3753–3765, Nov. 2017.

[59] J. Sun, Y. Wu, G. Cui, and Y. Wang, "Finite-time real combination synchronization of three complex-variable chaotic systems with unknown parameters via sliding mode control," *Nonlinear Dyn.*, vol. 88, no. 3, pp. 1677–1690, May 2017.

[60] J. Sun, Y. Wang, Y. Wang, and Y. Shen, "Finite-time synchronization between two complex-variable chaotic systems with unknown parameters via nonsingular terminal sliding mode control," *Nonlinear Dyn.*, vol. 85, no. 2, pp. 1105–1117, Jul. 2016.

[61] J. Sun, X. Zhao, J. Fang, and Y. Wang, "Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization," *Nonlinear Dyn.*, vol. 94, no. 4, pp. 2879–2887, Dec. 2018.

[62] J. S. Khan, J. Ahmad, S. F. Abbasi, A. Arshad, and S. K. Kayhan, "DNA sequence based medical image encryption scheme," in *Proc. 10th Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2018, pp. 24–29.

[63] J. S. Khan, J. Ahmad, and M. A. Khan, "TD-ERCS map-based confusion and diffusion of autocorrelated data," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 93–107, Jan. 2017.

[64] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019.

[65] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. A. Sheikh, "Visual meaningful encryption scheme using intertwining logistic map," *Intell. Comput.*, vol. 2, pp. 764–773, Nov. 2019.

[66] K. M. Ali and M. Khan, "Application based construction and optimization of substitution boxes over 2D mixed chaotic maps," *Int. J. Theor. Phys.*, vol. 58, no. 9, pp. 3091–3117, Sep. 2019.

[67] K. M. Ali and M. Khan, "A new construction of confusion component of block ciphers," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 32585–32604, Nov. 2019.

[68] M. Khan and N. Munir, "A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic," *Wireless Pers. Commun.*, vol. 109, no. 2, pp. 849–867, Nov. 2019.

[69] S. I. Batool and H. M. Waseem, "A novel image encryption scheme based on Arnold scrambling and Lucas series," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27611–27637, Oct. 2019.

[70] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 26203–26222, Sep. 2019.

[71] H. M. Waseem and M. Khan, "A new approach to digital content privacy using quantum spin and finite-state machine," *Appl. Phys. B, Lasers Opt.*, vol. 125, no. 2, p. 27, Feb. 2019.

[72] M. Khan and H. M. Waseem, "A novel digital contents privacy scheme based on Kramer's arbitrary spin," *Int. J. Theor. Phys.*, vol. 58, no. 8, pp. 2720–2743, Aug. 2019.

[73] A. Rafiq and M. Khan, "Construction of new S-boxes based on triangle groups and its applications in copyright protection," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 15527–15544, Jun. 2019.

[74] M. Khan and H. M. Waseem, "A novel image encryption scheme based on quantum dynamical spinning and rotations," *PLoS ONE*, vol. 13, no. 11, 2018, Art. no. e0206460.

[75] H. M. Waseem and M. Khan, "Information confidentiality using quantum spinning, rotation and finite state machine," *Int. J. Theor. Phys.*, vol. 57, no. 11, pp. 3584–3594, Nov. 2018.

[76] H. M. Waseem, M. Khan, and T. Shah, "Image privacy scheme using quantum spinning and rotation," *J. Electron. Imag.*, vol. 27, no. 6, p. 1, Dec. 2018.

[77] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, 2018.

[78] N. Munir and M. Khan, "A generalization of algebraic expression for nonlinear component of symmetric key algorithms of any characteristic p," in *Proc. Int. Conf. Appl. Eng. Math. (ICAEM)*, Sep. 2018, pp. 48–52.

[79] M. Khan, "An image encryption by using Fourier series," *J. Vibrat. Control*, vol. 21, pp. 3450–3455, 2015.

[80] J. Sun, G. Han, Z. Zeng, and Y. Wang, "Memristor-based neural network circuit of full-function pavlov associative memory with time delay and variable learning rate," *IEEE Trans. Cybern.*, to be published, doi: 10.1109/TCYB.2019.2951520.

[81] J. Sun, G. Han, and Y. Wang, "Dynamical analysis of memcapacitor chaotic system and its image encryption application," *Int. J. Control, Automat. Syst.*, to be published, doi: 10.1007/s12555-019-0015-7.

[82] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 9, pp. 3106–3118, Sep. 2014.

[83] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix lorenz systems S-boxes and their applications," *Chin. J. Phys.*, vol. 56, no. 4, pp. 1609–1621, Aug. 2018.

JUN-LING HAO received the B.S. degree in information and computing science from the Hunan University of Technology, in 2006, and the M.S. degree in basic mathematics from Jiangsu Normal University, in 2009. Her research interests focus on information security, chaos theory, and the existence of solutions to differential equations.

YING-QIAN ZHANG received the Ph.D. degree from the Dalian University of Technology, in 2015. He is currently a Professor with the Tan Kah Kee College, Xiamen University. He is interested in nonlinear systems, chaos theory, and information security.

XING-YUAN WANG was born in Liaoning, China, in 1964. He received the B.S. degree in application physics and the M.S. degree in optics from Tianjin University, Tianjin, China, in 1987 and 1992, respectively, and the Ph.D. degree in computer software and theory from Northeastern University, Shenyang, China, in 1999. From 1999 to 2001, he was a Postdoctoral Fellow with the Department of Automation, Northeastern University. He is currently a Professor with the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian, China. His research interests include biomedical information, computer graphics, image processing, complex networks, and chaos control and synchronization.

● ● ●