Novel Image Cryptosystem Based on New 2D Hyperchaotic Map and Dynamical Chaotic S-box

Xingyuan Wang (xywang@dlmu.edu.cn)
Dalian Maritime University
Shuang Zhou
chong qing shi fan da xue: Chongqing Normal University
Yuyu Qiu
chong qing shi fan da xue: Chongqing Normal University
Yingqian Zhang
xia men da xue: Xiamen University

Research Article

Keywords: S-box, Hyperchaotic system, Image encryption, Chaos

Posted Date: July 22nd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1837112/v1

Novel Image Cryptosystem Based on New 2D Hyperchaotic Map and Dynamical Chaotic S-box

Shuang Zhou[1)] Yuyu Qiu[1)] Xingyuan Wang[2)†] Yingqian Zhang3)

1)（School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331, China）

2)（School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China）

3)（School of Electrical Engineering and Artificial Intelligence, Xiamen University Malaysia, Sepang, 43900, Malaysia）

Abstract: Chaotic systems are widely used in image encryption due to their sensitivity to initial values. and many image encryption algorithms based on chaotic systems have been studied in the past few years. In order to obtain a simpler encryption algorithm, this work firstly proposes a new two-dimensional discrete hyperchaotic map, which has a large chaotic interval and Lyapunov exponent, and then uses the map to generate two chaotic sequences, and use these sequences to generate three S-boxes, and combine them in pairs, and finally twelve S-boxes are obtained. Then, the elements of the plaintext image are grouped, each group of pixels is summed, and then modular operations are used to specify specific S-boxes. Next, each set of elements is bitwise XOR with the corresponding S-box. Finally, the cipher image is obtained by scrambling using chaotic signal. Experiments show that compared with some other encryption algorithms, the proposed S-box based encryption method has higher security, and it resists to common attack.

Key Words: S-box; Hyperchaotic system; Image encryption; Chaos

1 Introduction

With the development of society, each of us is in the era of information explosion, and our privacy is becoming more and more transparent. Digital information is widely

† Corresponding author. E-mail: xywang@dlmu.edu.cn(X.Wang)

used around us, such as communication, image and so on. Compared with text information, image information is more intuitive and interactive. In image transmission, if image information is not processed, there may be a risk of privacy disclosure.

Since the emergence of "chaos" as a new scientific term in 1975, chaotic dynamics has been vigorously developed and studied [1-5]. Chaos is widely used in cryptography and related fields because of its nonlinearity, pseudo-randomness and sensitivity to initial values. To obtain better encryption effect, researchers began to improve the traditional continuous chaotic map and discrete chaotic map and apply them to encryption [6-15], Although the continuous chaotic map has high complexity, the efficiency of generating chaotic sequences is low. On the contrary, the discrete chaotic map has low complexity but high efficiency, so it is more suitable to apply the discrete chaotic map to encryption. Amine et al. used an improved one-dimensional discrete chaotic map for encryption [14]. To improve the problem that the existing chaotic map does not have complex dynamic performance, Gao et al. introduced a new two-dimensional hyperchaotic map in image encryption [15]. Of course, high-dimensional discrete chaotic systems are also widely studied due to their higher complexity and better unpredictability [16-19]. However, two-dimensional discrete chaotic systems are more used due to their simple form and strong anti-degeneration ability. At present, many discrete two-dimensional chaotic systems have been proposed [20-26]. Hua et al. proposed a two-dimensional (2D) modular chaotic system that can improve the chaotic complexity of any two-dimensional chaotic map [20]. He et al. presented a 2D spatiotemporal chaotic system which mixed linear–nonlinear and used it for image encryption [21]. Huang et al. designed a new 2D chaotic using two existing 1D chaotic maps map and use it for image encryption [22]. Hua et al. designed a two-dimensional chaotic system with continuous and wide chaotic range and designed a color image encryption algorithm based on this system [23]. Ahmad et al. proposed an improved 2D hyperchaotic system and used it for S-box generation [24]. Qi et al. proposed a 2D-TSCC chaotic system and used it for image protection [25]. Ma et al. proposed a two-dimensional chaotic system with a simple algebraic form and analyzed its chaotic

properties [26]. However, most of the existing two-dimensional chaotic maps still have the problem of narrow chaotic interval. To obtain a larger chaotic interval and ensure encryption efficiency, this paper presents a new two-dimensional hyper-chaotic map, which has a larger chaotic interval than most existing two-dimensional chaotic systems, and can be better used to design cryptographic algorithms.

To enhance the security of the encryption algorithm, this paper introduces S-box for XOR in the encryption process. S-box is usually the only nonlinear part of block cipher algorithm. Recently, there are more and more research on S-box [27-34]. At the same time, researchers found that the combination of chaotic system and S-box in image encryption can enhance the security of the algorithm [35-41]. To overcome the singularity of fixed S-boxes and make the encryption process more flexible, the concept of dynamic S-boxes is proposed. Wang et al. developed an image encryption scheme based on dynamic S-box [42]. Zhu et al. designed dynamic S-boxes by using the combination of chaotic mapping and adaptive function [43]. Devaraj et al. proposed an image encryption scheme based on improved standard mapping and dynamic S-boxes [44]. Liu et al. proposed an encryption algorithm based on hyperchaotic system and dynamic S-box [45]. However, these algorithms are often very complex, increasing the runtime of the algorithm. Therefore, this work constructs a simple and flexible encryption algorithm under the premise of security and efficiency. Different from most studies, this paper combines S-boxes to generate more S-boxes, which saves running time, and innovatively uses the S-box dynamically for the XOR step, making the algorithm more flexible and better resistant to noise attacks.

The main contributions of this paper are:

1). This paper presents a new two-dimensional discrete hyperchaotic system with a wider chaotic region, much larger Lyapunov exponents and more complex behavior.

2). We generate many new S-boxes using fixed S-box, which has higher security compared with a single S-box.

3). A novel image encryption algorithm combining the new chaotic system and dynamic S-box is proposed, which has higher security compared with the image

encryption methods based on fixed S-box.

This work is organized as follows: Sec.2 introduces the proposed two-dimensional hyperchaotic map and its dynamic characteristic; The constructed S-box is presented in Sec.3; Sec.4 describes the encryption algorithm; Simulation results and security analysis are showed in Sec.5; Sec.6 summarizes the full text and puts forward the direction of future work.

2 Dynamical system analysis

This section introduces the proposed two-dimensional hyperchaotic map and its chaotic characteristics.

2.1 Hénon map

The Hénon map is presented as follows [46]:

$$\begin{cases} x_{n+1} = y_n + 1 - a x_n^2, \\ y_{n+1} = b x_n. \end{cases} \tag{1}$$

where $x_n \in (-1.5, 1.5)$, when $a \in [1.07, 1.4], b = 0.3$, the map is chaotic.

2.2 The new hyperchaotic map

The proposed hyperchaotic map is:

$$\begin{cases} x_{n+1} = \sin(10^{17} r x_n + y_n), \\ y_{n+1} = \cos(10^{19} r \pi y_n). \end{cases} \tag{2}$$

where $r \in [100, 200]$ and $x_n \neq 0, y_n \neq 0$.

2.3 Phase diagram

Figure 1 gives a partial phase diagram for the parameter r from 100 to 200. From Fig.1, we can see that the attractor trajectory of the new two-dimensional hyperchaotic system is evenly distributed in the whole phase space when r ranges from 100 to 200. Therefore, the new system has good chaotic characteristics.

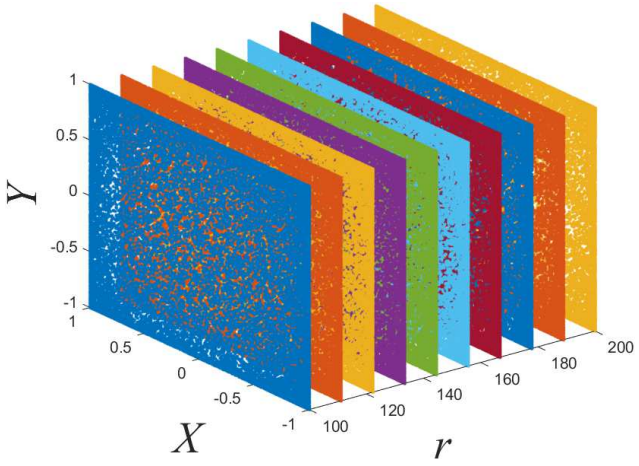
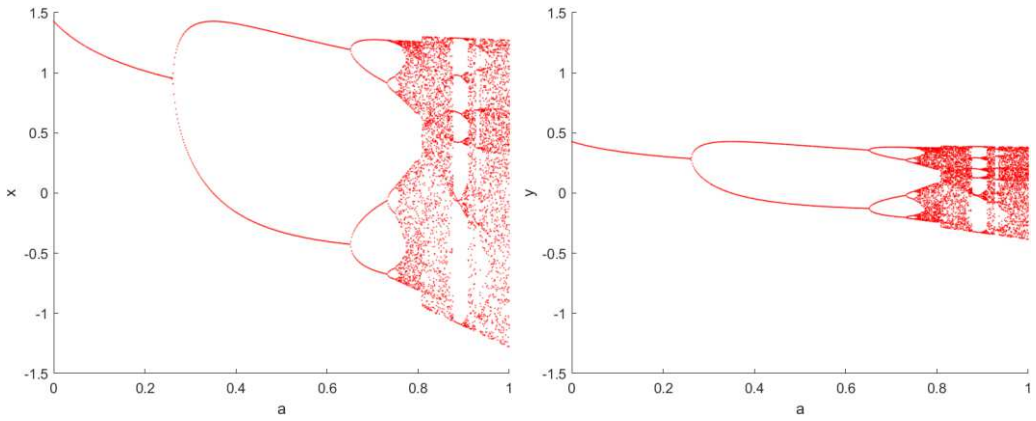


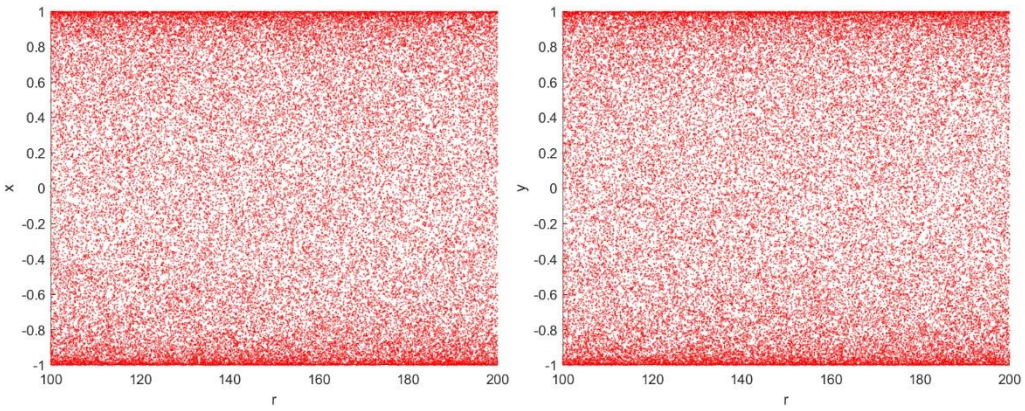
Fig. 1 Phase diagram of the new hyperchaotic mapping

2.4 Bifurcation diagram

The bifurcation phenomenon of chaotic map is one part of the symbols of chaos. By depicting the bifurcation diagram, we can intuitively observe the relevant information of chaos. The bifurcation diagram of Hénon map and the bifurcation diagram of new two-dimensional hyperchaotic map are shown in Fig. 2. From the Figs.2(a-d), we can infer that the new system has a larger chaotic interval than Hénon map.



(a) Bifurcation of x for Hénon map (b) Bifurcations of y for Hénon map



(c) Bifurcation of x for new map (d) Bifurcation of y for new map

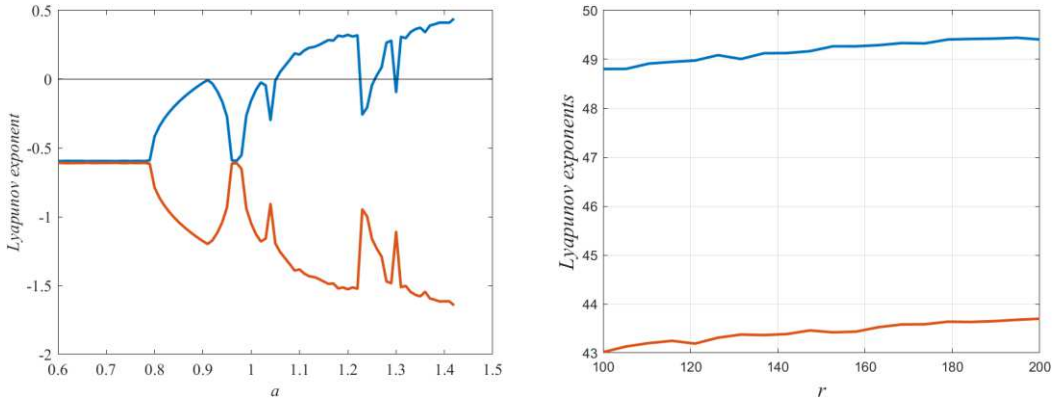
Fig.2 Bifurcation diagram

2.5 Largest Lyapunov Exponent

Lyapunov exponent describes the average change rate of orbit dispersion or convergence caused by the change of two slightly different initial values with time in the phase space generated by time series [47]. The two LEs of two-dimensional chaotic system at initial state x_0 is defined as

$$\lambda_i = \lim_{n\to\infty} \frac{1}{n} \ln \eta_i(\Psi_n), \quad i = 1, 2. \tag{3}$$

Where $\eta_i(\Psi_n)$ is the i-th eigenvalue of matrix Ψ_n, $\Psi_n = J(x_0)J(x_1)\cdots J(x_{n-1})$, and $J(x_j)$ is the Jacobin matrix of the chaotic system at observation time j. The map is chaotic when one Lyapunov exponent is greater than 0; If both Lyapunov exponents are greater than 0, the map is hyperchaotic [48]. The Lyapunov exponent of Hénon map and the new two-dimensional chaotic map are shown in Fig. 3. From Fig. 3, only one Lyapunov exponent of Hénon mapping is greater than 0, while the two Lyapunov exponents of the new two-dimensional chaotic system are greater than 0, indicating that the new two-dimensional chaotic system has better chaotic characteristics.



(a) Lyapunov exponent of Hénon map (b) Lyapunov exponent of new map

Fig. 3 Lyapunov exponent graph of chaotic map

2.6 NIST SP800-22 test

In this paper, SP800-22 standard is adopted to test the performance of the pseudo random sequence. which includes 15 major items. Each binary sequence test metric gives a test result of P-value, set a threshold $\alpha = 0.1$, If P-value is greater than α, the random reliability of the test sequence is $1-\alpha$, The sequence passed the random test of the index; on the contrary, it indicates that it has not passed the test [49].

As can be seen from the results in Table 1, the pseudo random sequences generated by new system passed these tests, which indicates that our pseudo-random sequence has a good pseudo-random performance.

Table 1 NIST SP800-22 test results

Test Item	**P-value**		**Results**
	x Sequences	y Sequences	
Approximate Entropy	0.576277	0.662228	Pass
Block Frequency	0.734371	0.814645	Pass
Cumulative Sums	0.759852	0.700063	Pass
FFT	0.854380	0.633482	Pass
Frequency	0.810330	0.953960	Pass
Linear Complexity	0.585907	0.875504	Pass
Longest Runs	0.790455	0.606152	Pass
Non-Overlapping Template	0.760042	0.791087	Pass
Overlapping Template	0.881497	0.802512	Pass
Random Excursions	0.724547	0.349166	Pass
Random Excursions Variant	0.911365	0.602256	Pass
Rank	0.862457	0.850852	Pass
Runs	0.438912	0.503020	Pass
Serial	0.885780	0.712745	Pass
Universal	0.774689	0.971905	Pass

3 S-box structure and performance analysis

S-box is the sole nonlinear structure of AES. S-box mainly plays a role of confusion and diffusion in the cryptography system. This work presents a new hyperchaotic system in Sec.2 used to generate chaotic sequences, which are used to scramble the number $0-255$ without repetition, and then the number is rearranged into a 16×16 matrix. The above steps are repeated to obtain three different S-boxes, which are compounded in pairs to obtain nine S-boxes. For space reasons, we chose one of the S-boxes (S_{10}) as the box for subsequent performance analysis. Table 2 shows the obtained S_{10} . Table 3 shows the S-box lookup table where $S_a(\bullet)$ represents S_a replacement of $\bullet$.

Table 2 The proposed S-box

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

Table 3 S-box lookup table

1	S_1	4	$S_1 \cdot S_1$	7	$S_2 \cdot S_1$	10	$S_3 \cdot S_1$
2	S_2	5	$S_1 \cdot S_2$	8	$S_2 \cdot S_2$	11	$S_3 \cdot S_2$
3	S_3	6	$S_1 \cdot S_3$	9	$S_2 \cdot S_3$	12	$S_3 \cdot S_3$

3.1 Bijectivity

Adamas and Tavares proposed the conclusion that f is bijective if the sum of the linear operations of the Boolean functions f_i of the components of the S-box of $n \times n$ is 2^{n-1} [50].

$$wt(\sum_{i=1}^{n} a_i f_i) = 2^{n-1}, \tag{4}$$

where $a_i \in \{0,1\}$ and $a_i (i = 1, 2 \cdots n)$ are not both 0 , $wt(\bullet)$ is the Hamming weight. According to the S-box construction method, the S-box constructed in this paper is bijective.

3.2 Nonlinearity

Nonlinearity is a measure of the ability of cryptographic function to resist linear attack. The ability of a function to resist linear attack is proportional to its nonlinearity [51]. The nonlinearity of the n-bit Boolean function $f(x)$ is defined as follows:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in F_2^n} \left| S_{(f)}(\omega) \right|, \tag{5}$$

where $S_{(f)}(\omega)$ is the Walsh cycle spectrum of $f(x)$. The results obtained by calculating the nonlinearity of S_{10} are shown in Table 4. It can be seen that the proposed S-box has high nonlinearity.

Table 4 Nonlinearity of the proposed S-box

Methods	1	2	3	4	5	6	7	8	Mean
The Proposed	106	108	104	104	104	106	106	104	105.25

3.3 Strict Avalanche Criterion (SAC)

Webster and Tavares presented a strict avalanche criterion combining completeness and avalanche effect. The strict avalanche criterion is when you change one input to a Boolean function, half of the output values will change, that is, the probable change of each output bit is 0.5. The independent matrix is used to obtain the SAC value of the S-box [52]. If an S-box satisfies SAC, each element of the independent matrix is close to 0.5. Table 5 shows the independent matrix of the newly constructed S-box. As we can see from Table 5, each element has a value close to 0.5.

Table 5 The independence matrix of the proposed S-box

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
00000001	0.53125	0.57812	0.54687	0.48437	0.56250	0.51562	0.53125	0.46875
00000010	0.46875	0.51562	0.51562	0.48437	0.46875	0.43750	0.53125	0.59375
00000100	0.43750	0.45312	0.54687	0.35937	0.48437	0.48437	0.48437	0.54687
00001000	0.48437	0.45312	0.48437	0.56250	0.48437	0.46875	0.56250	0.5
00010000	0.42187	0.56250	0.42187	0.54687	0.5	0.56250	0.48437	0.53125
00100000	0.46875	0.51562	0.53125	0.46875	0.53125	0.53125	0.51562	0.54687
01000000	0.54687	0.48437	0.51562	0.5	0.54687	0.5	0.46875	0.51562
10000000	0.51562	0.56250	0.5	0.48437	0.57812	0.56250	0.48437	0.51562

3.4 Output Bits Independence Criterion (BIC)

Adamas and Tavares designed a method to measure the independence between output bits [53]. There are two Boolean functions that output bits in the S-box: $f_j(x)$ and $f_k(x)$. If $f_j(x) \oplus f_k(x)$ is highly nonlinear and meets as strict an avalanche criterion as possible, the correlation coefficient of the output bit pairs may approach 0

when any input bit is inverted. Table 6 shows BIC-nonlinearity of the proposed S-box. Table 7 shows BIC-SAC of the proposed S-box.

Table 6 BIC-nonlinearity of the proposed S-box

0	106	110	104	100	102	106	102
106	0	104	106	106	106	100	104
110	104	0	108	98	104	96	102
104	106	108	0	100	100	96	102
100	106	98	100	0	106	102	102
102	106	104	100	106	0	104	102
106	100	96	96	102	104	0	98
102	104	102	102	102	102	98	0

Table 7 BIC-SAC of the proposed S-box

0	0.54148	0.51757	0.49804	0.50390	0.49023	0.53710	0.47851
0.52148	0	0.51757	0.50000	0.48632	0.50781	0.49309	0.50000
0.51757	0.51757	0	0.52148	0.53125	0.49804	0.52343	0.48242
0.49804	0.50000	0.52148	0	0.50585	0.50195	0.52148	0.49023
0.50390	0.48632	0.53125	0.50585	0	0.49023	0.50585	0.49023
0.49023	0.50781	0.49804	0.50195	0.49023	0	0.47565	0.48632
0.53710	0.49609	0.52343	0.52148	0.50585	0.47656	0	0.52539
0.47851	0.50000	0.48242	0.49414	0.49023	0.48632	0.52539	0

3.5 Difference approximation Probability (DP)

The difference approximation probability DP_f represents the XOR distribution of the input and output of the Boolean function [54]. Given an input difference Δx, the highest probability that the output is Δy. The smaller DP_f is, the more resistant it is to differential attacks. The maximum value of S-box DP proposed in this paper is 0.0390.

3.6 Linear approximation Probability (LP)

The probability of linear approximation is that when two masks Γx and Γy are

arbitrarily selected, perform mask Γx operation on all possible values of the input value x and mask Γy operation on the output value $S(x)$ of the corresponding S-box. the maximum number of the same result obtained after the operation of the input value and the output mask is the maximum linear approximation [55].

The smaller LP is, the more resistant it is to linear attacks. The maximum value of S-box LP constructed in this paper is 0.1328.

3.7 Comparison with other S-boxes

Table 8 shows the comparison between the indexes of the proposed S-box and other methods. It can be obtained from Table 8 that the S-box constructed is better and has strong encryption characteristics than some other methods, which is conducive to the subsequent research on encryption algorithms.

Table 8 Performance comparison of S-boxes

S-boxes	**Nonlinearity**	**SAC**	**BIC-SAC**	**BIC-NL**	**DP**	**LP**
Method	**Avg.**	**Avg.**	**Avg.**	**Avg.**	**Max.**	**Max.**
Ref. [36]	103.25	0.5151	0.4864	103.07	0.1718	0.1562
Ref. [37]	103	0.5039	0.5010	100.35	0.5	0.1484
Ref. [38]	104.75	0.5041	0.5050	104	0.0390	0.1406
Ref. [42]	104	0.5026	0.5033	103.214	—	0.1328
Ref. [44]	105.25	0.5037	0.4994	102.64	—	—
The Proposed	105.25	0.5070	0.5039	102.72	0.0390	0.1328

4. Dynamical chaotic S-boxes encryption algorithm

This section introduces the proposed encryption algorithm, as shown in Fig. 4. Then, we present the novel image cryptosystem, which is summarized as follows:

Step 1: Inputting the picture *P*, remember that the size of the picture is $M \times N$, and convert the picture into the sequence I of length $M \times N$;

Step 2: Using the hash function SHA-512 from sequence I to get y_0. Pick any real number $x_0 \in R$, $r \in [100, 200]$ to get chaotic sequences.

Step 3: Discarding the value of the first 1000 iterations and iterate the y sequence for $M \times N$ times to obtain the sequence y_1. Sorting it from smallest to largest to obtain Γ, and obtain the position sequence A according to the position of Γ in y_1;

Step 4: The structure of S-boxes

(1) Discarding the value of the first 1000 iterations and iterate the x sequence for 16×16 times to get the sequence x_1;

(2) Discarding the value of the previous 6000 iterations and iterate the y sequence for 16×16 times to get the sequence y_2;

(3) Discarding the value of the previous 6000 iterations and iterate the x sequence for 16×16 times to get the sequence x_2;

(4) Using sort function to get index set $k_1 = sort(x1), k_2 = sort(y2), k_3 = sort(x2)$, Mark $D = 0:255$, then we calculate

$$\begin{cases} S_1 = D(K_1), \\ S_2 = D(K_2), \\ S_3 = D(K_3). \end{cases}$$

to get three S-boxes;

Step 5: Compound the above S-boxes according to the method in Sec.3 to get twelve S-boxes;

Step 6: Calculating $\alpha = \dfrac{M \times N}{256}$ to get α, and further calculate

$$B(i) = \mathrm{mod}(sum(I(256\cdot(i-1)+1:256\cdot i)),12)+1,$$

where $i = 1,2\cdots\alpha$, Sequence B is obtained, that is, a different S-box is selected for each 256 elements of sequence I; As shown in Fig. 5;

Step 7: All the selected S-boxes are transformed into one-dimensional sequences of length 16×16, and the sequence S with length $M \times N$ is connected at one time. According to the S-box selected by I, calculate $P1 = bitxor(I, S)$ to get the sequence $P1$;

Step 8: Scrambling sequence $P1$ with A in Step 3 to get $P2$;

Step 9: Sequence $P2$ is transformed into the matrix of $M \times N$ to obtain the cipher image $C2$.

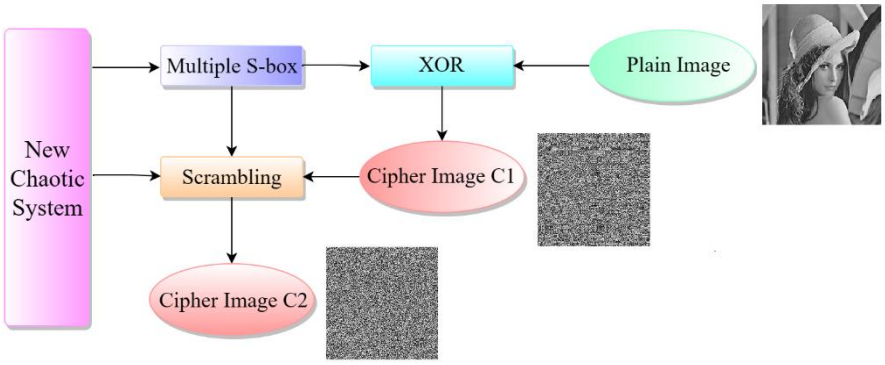


Fig. 4 Overall encryption process

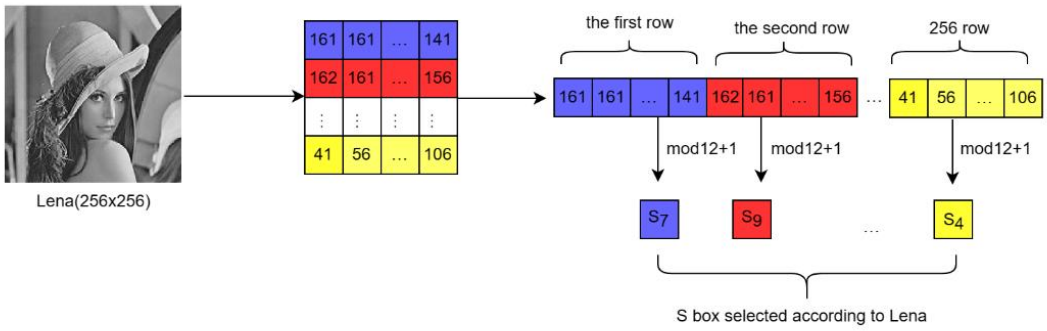


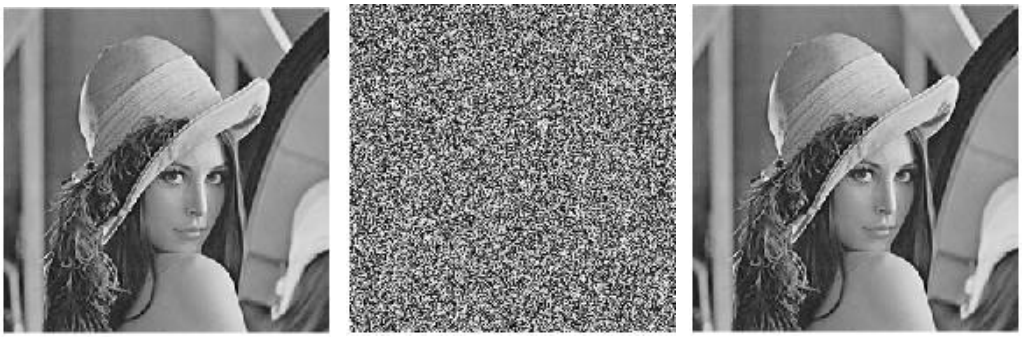
Fig. 5 Select S-box according to the picture

5 Simulation results and security analysis

In this section, the performance of gray image is analyzed, and the proposed encryption algorithm is compared with the results of recent research algorithms on image encryption.

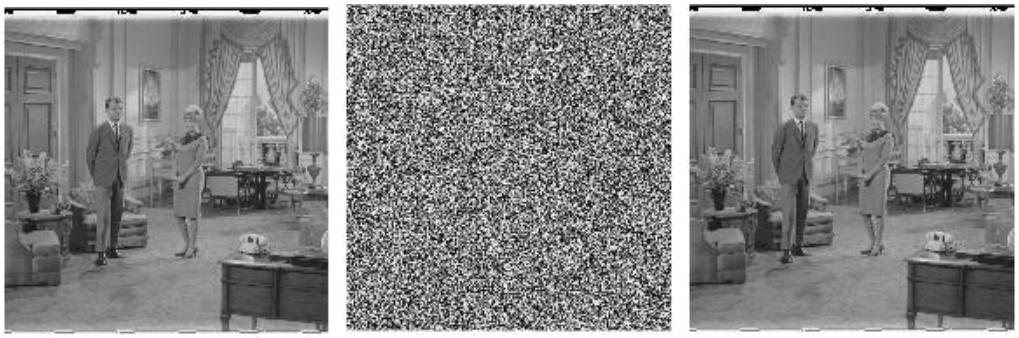
5.1 Gray image encryption simulation

The algorithm is used to encrypt images with different resolutions. Figs. 6-8 show the encryption and decryption results. It shows that the proposed algorithm can encrypt and decrypt the images effectively.



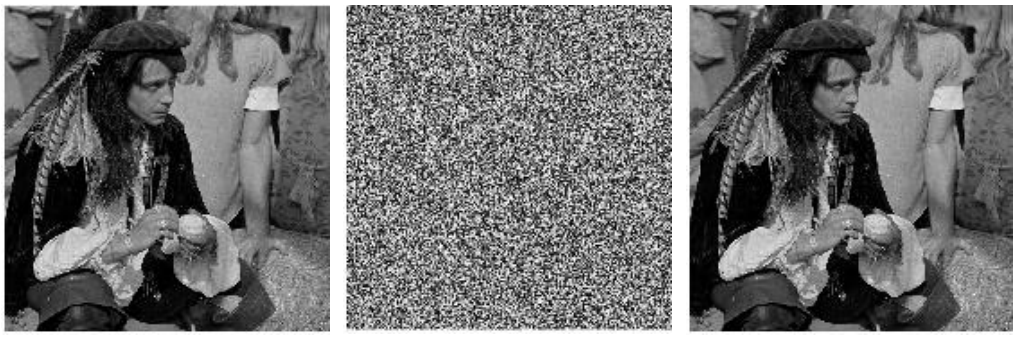
(a) Original image (b) Cipher image (c) Decrypted image

Fig. 6 Results of encryption and decryption by Lena (256×256)



(a) Original image (b) Cipher image (c) Decrypted image

Fig. 7 Results of encryption and decryption by Couple (512×512)



(a) Original image (b) Cipher image (c) Decrypted image

Fig. 8 Results of encryption and decryption by Male (1024×1024)

5.2 Key space

Our encryption key includes x_0, y_0, r and sequence B, where x_0 and y_0 are all real numbers, r is the real number of $[100, 200]$, the element in B is an integer from 1 to 12, and the length of B depends upon the size of the plaintext image. Since the computer precision is 10^{-14}, our key space should be greater than or equal to:

$$10^{14} \times 10^{14} \times 100^2 \times 12^{256} \approx 2^{1023} > 2^{100}, \quad (6)$$

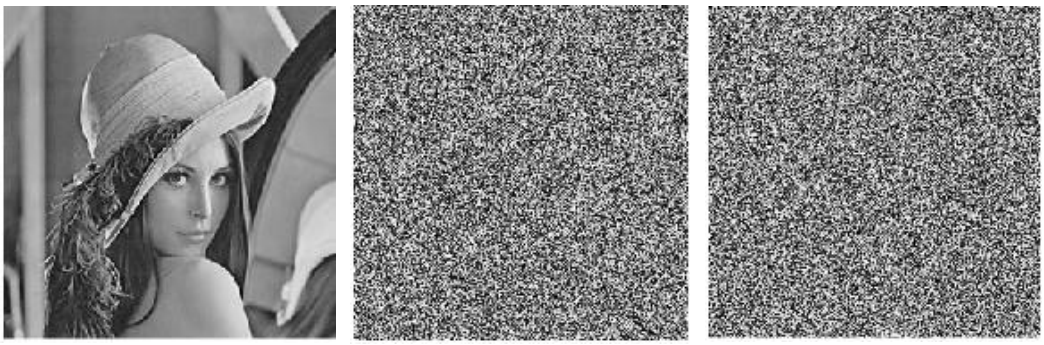
Obviously, the proposed encryption algorithm can defend against brute force attacks. Table 9 compares the key space of our algorithm with other algorithms. It's clear that our key space is large enough to against brute-force attack.

Table 9 Compares the key space with other algorithms

Cryptosystem	Our method	Ref.[37]	Ref.[38]	Ref.[39]
Key space	2^{1023}	10^{126}	2^{255}	2^{283}

5.3 Key sensitivity

A marvelous encryption algorithm must be key sensitive, that is, the plaintext image cannot be correctly solved after a small perturbation of the key. Figure 9 shows the decryption image after the perturbation of the key, which shows that the new encryption algorithm is sensitive to the key.



(a) Original image (b) Cipher image (c) Decrypted image

Fig. 9 Decryption result of disturbed key

5.4 Differential attack

Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used to analyze the influence of small changes in plaintext on the ciphertext [56]. The ideal value for NPCR is 99.61%, the closer you are to the ideal value, the more sensitive the ciphertext you are to the change of plaintext. The ideal value for UACI is 33.46%, the closer you are to the ideal value, the more resistant you are to differential attacks. Assuming that the two ciphertext images are C_1, C_2, corresponding to the plaintext images with only one pixel difference, then calculate

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%, \quad (7)$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\%, \quad (8)$$

where M, N are the number of rows and columns of the image. Table 10 shows that the NPCR value and UACI values are all close to stand value. As can be seen from this table, the algorithm presented can resist the selective plaintext attack and differential attack. Table 11 compares the NPCR and UACI obtained by this algorithm with other literatures. It indicated that our algorithm can effectively resist different attacks.

Table 10 NPCR and UACI for different images

Images	**NPCR**	**UACI**
Lena(256×256)	0.9961	0.3346
Clock(256×256)	0.9959	0.3345
Airport(256×256)	0.9963	0.3347
Pepper(256×256)	0.9960	0.3347
Tank(512×512)	0.9958	0.3345
APC(512×512)	0.9959	0.3343
Couple(512×512)	0.9959	0.3343
Male(1024×X1024)	0.9961	0.3342
Airplane(1024×1024)	0.9961	0.3348
Airport(1024×1024)	0.9961	0.3344

Table 11 Comparison with other algorithms for NPCR and UACI

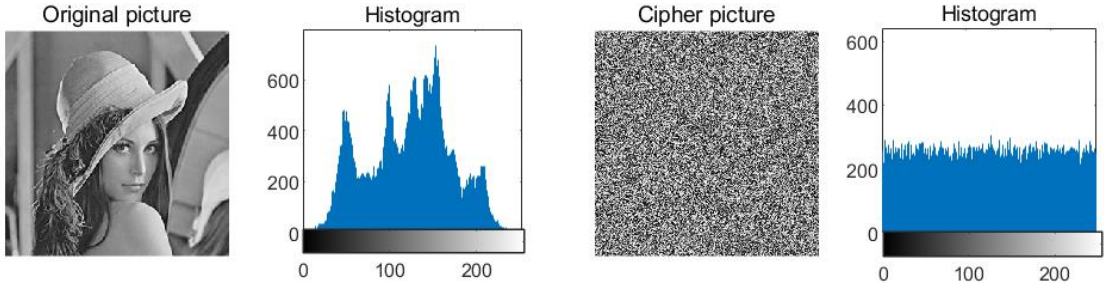
Lena(256×256)	Our method	Ref.[38]	Ref.[40]	Ref.[41]	Ref.[42]	AES[41]
NPCR	0.9961	0.9967	0.9961	0.9964	0.9959	0.0778
UACI	0.3336	0.3349	0.3340	0.3347	0.3345	0.0093

5.5 Histogram analysis

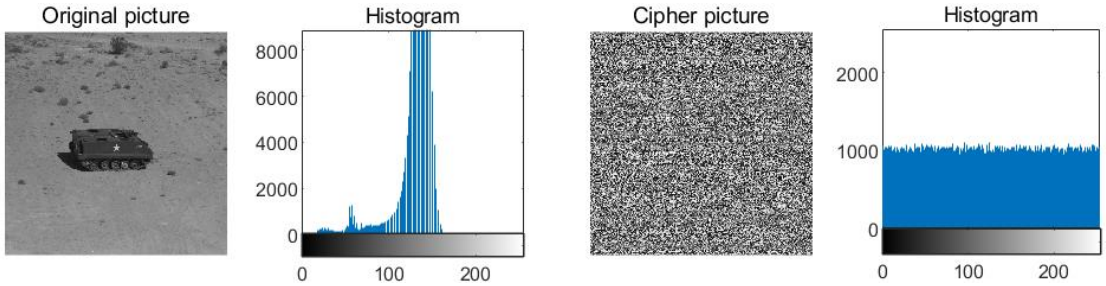
The histogram reflects the gray level statistics of all pixels in the image. The more evenly the histogram of the encrypted graph is distributed, the more difficult it is for an

attacker to obtain valid information from the encrypted image, that is, the more resistant it is to ciphertext only attack. The histogram of images with different resolutions and their encryption images are shown in Fig.10, which indicate that the distribution of our histogram of the encrypted images are uniform.

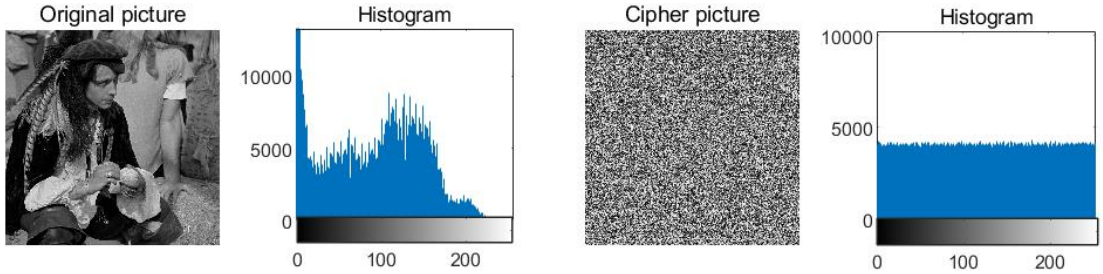
Fig. 11 shows that the spatial pixel value distribution of images with different resolutions and their encrypted images. It can be seen that all pixels of the encryption images are evenly distributed between 0 and 255.



(a) Encryption and decryption for histogram of Lena (256×256)

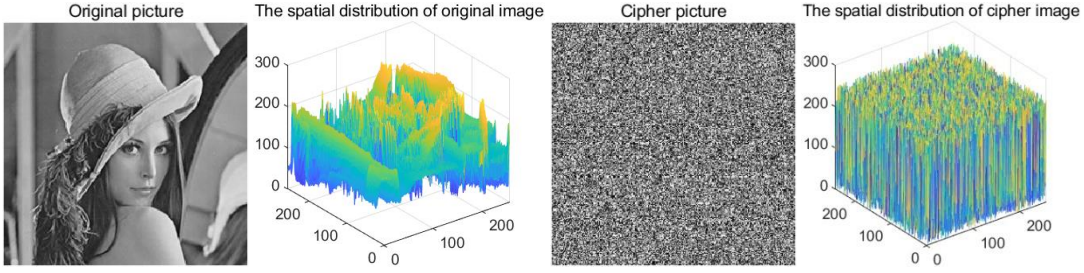


(b) Encryption and decryption for histogram of APC (512×512)

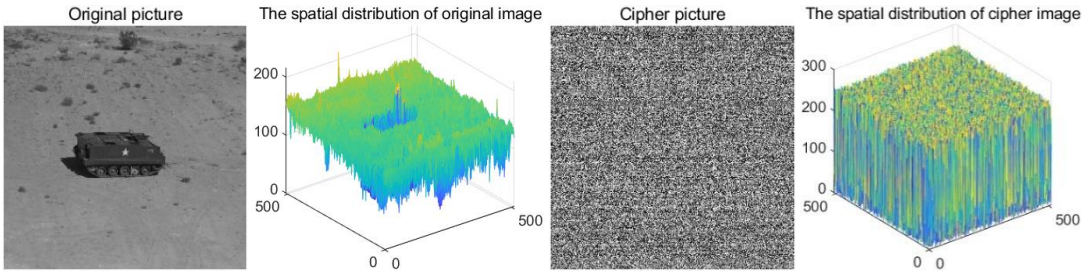


(c) Encryption and decryption for histogram of Male (1024×1024)

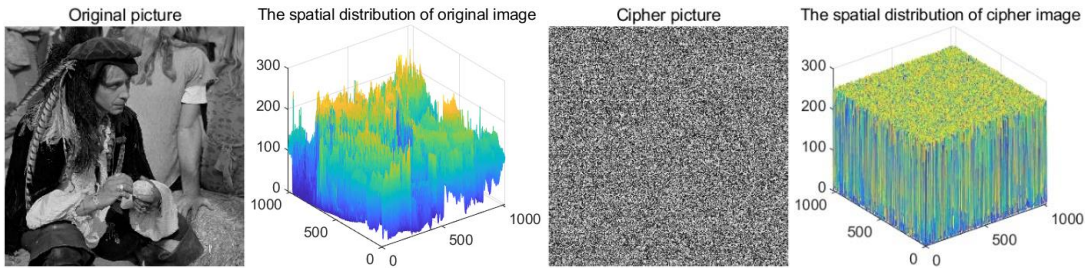
Fig. 10 Histogram of images with different resolutions and their encryption image



(a) Encryption and decryption for the spatial distribution of Lena(256×256)



(b) Encryption and decryption for the spatial distribution of APC(512×512)

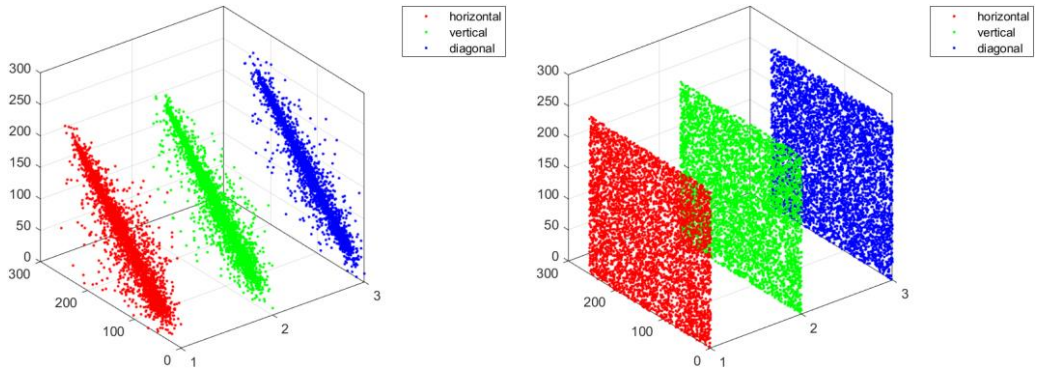


(c) Encryption and decryption for the spatial distribution of Male(1024×1024)

Fig. 11 Distribution of pixel values of images with different resolutions and their encryption images in space

5.6 Correlation Analysis of Adjacent Pixels

Encryption algorithms can resist statistical analysis attacks only when the correlation between adjacent pixels of ciphertext images should be as low as possible. The smaller the correlation coefficient of the image is, the weaker the correlation of the image is. In other words, the correlation coefficient should be close to 0, which means the safer the image is [57]. Fig. 12 shows the pixel correlation analysis of Lena. It can be obtained from Fig.12 that each direction of ordinary image has strong correlation, but each direction of encrypted image has a weak correlation. Table 12 shows the correlation coefficients of encrypted images with different resolutions. Table 13 shows the comparison of correlation coefficients of different methods. We can conclude that the weak correlation of each direction of the encryption images obtained by this algorithm are better than other algorithms.



(a) Correlation of original Lena graph (b) Correlation of Lena encryption graph

Fig. 12 Pixel correlation analysis of Lena

Table 12 Correlation coefficients of encrypted images with different resolutions

Images	Plain-image			Cipher-image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena(256×256)	0.9488	0.9250	0.8917	0.0004	0.0003	-0.0022
Clock(256×256)	0.9743	0.9601	0.9403	0.0008	-0.0004	0.0076
Airport(256×256)	0.9018	0.9433	0.8537	-0.0003	-0.0011	0.0004
Pepper(256×256)	0.9657	0.9525	0.9342	-0.0008	0.0028	0.0006
Tank(512×512)	0.9326	0.9485	0.9066	0.0005	0.0039	0.0006
APC(512×512)	0.9308	0.9535	0.9193	0.0009	0.0094	0.0007
Couple(512×512)	0.8950	0.9415	0.8285	0.0001	0.0003	0.0021
Male(1024×1024)	0.9816	0.9790	0.9669	-0.0074	0.0009	-0.0003
Airplane(1024×1024)	0.9494	0.9656	0.9448	0.0004	0.0094	0.0029
Airport(1024×1024)	0.9032	0.9118	0.8657	-0.0024	0.0041	0.0007

Table 13 Comparison of correlation coefficients of different methods

	Our method	Ref. [35]	Ref. [39]	Ref. [40]	Ref. [41]	AES [41]
Horizontal	0.0004	0.0141	0.0045	0.0013	0.0027	0.2724
Vertical	0.0003	0.0107	0.0018	-0.0015	0.0012	0.2681
Diagonal	-0.0022	0.0097	-0.0058	0.0098	0.0003	0.0765

5.7 Information entropy

Information entropy, which reflects the randomness of pixel gray value in the encrypted image, has a theoretical value of 8. If the information source is expressed as

s, the information entropy $H(s)$ is calculated as follows [58].

$$H(s)=\sum_{i=0}^{2^L} P(s_i)\log_2\frac{1}{P(s_i)}. \quad (9)$$

Table 14 shows the information entropy of the encrypted images obtained by using our encryption. It can be concluded from Table 14 that the information entropy of encrypted images with different resolutions are close to the theoretical value 8. Table 15 shows the information entropy comparison between the encryption algorithm in Sec.4 and other encryption algorithms. Certain generalizations can be derived from the data in Table 15, like the information entropy obtained by the encryption algorithm proposed in Sec.4 is closer to the theoretical value, and the gray value of the encrypted image pixel appears more random.

Table 14 Information entropy of encrypted images with different resolutions

Images	**Size**	**Information entropy**
Lena	256×256	7.9977
Clock	256×256	7.9976
Airport	256×256	7.9977
Pepper	256×256	7.9976
Tank	512×512	7.9994
APC	512×X512	7.9994
Couple	512×512	7.9994
Male	1024×1024	7.9998
Airplane	1024×1024	7.9998
Airport	1024×1024	7.9998

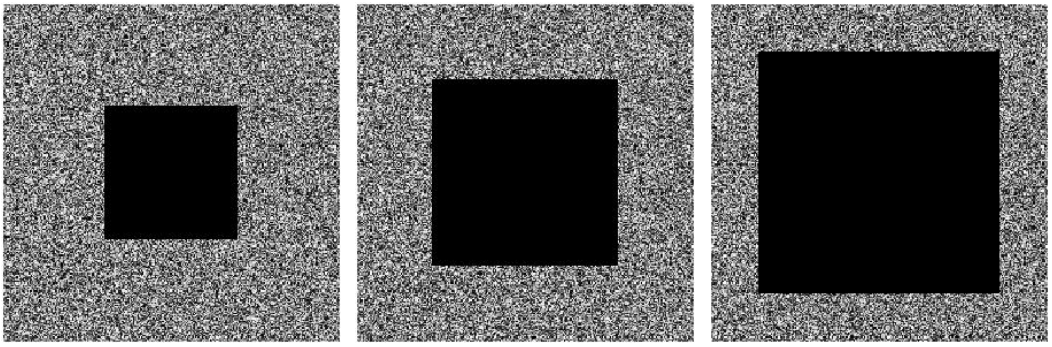
Table 15 Comparison of information entropy

Image	Size	Our method	Ref.[13]	Ref.[32]	Ref.[35]	Ref.[38]	Ref.[41]	AES[41]
Lena	256×256	7.9977	7.9971	7.9957	7.9972	7.9973	7.9974	7.8693

5.8 Robustness Analysis

A good encryption algorithm, even if the ciphertext image information is partially missing, should also be able to obtain part of the image information through decryption,

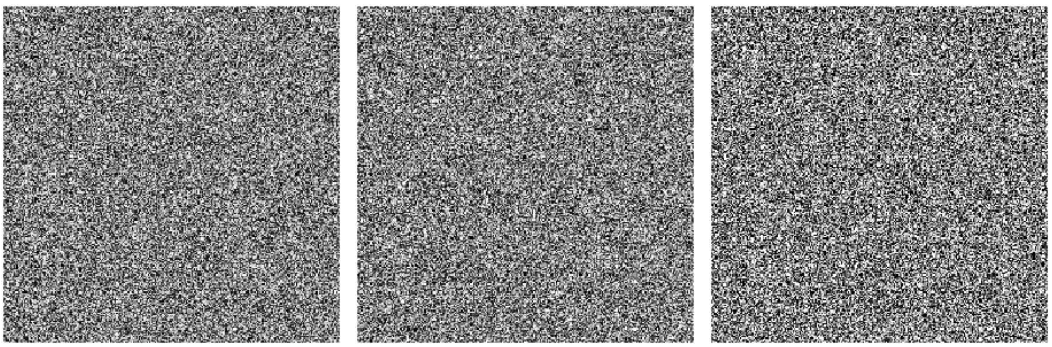
that is, it should have anti-shear ability and anti-noise ability. Fig. 13 shows the decryption situation in the absence of ciphertext. Through observation that the proposed encryption algorithm can effectively resist image clipping. Fig. 14 shows that the decryption results under Gaussian noise attack. From these figures, the decrypted image restores the important information of the original image, which can be inferred that the proposed algorithm has excellent robustness.



(a) 15% cut (b)30% cut (c) 50% cut

(d) Cut 15% decryption (e) Cut 30% decryption (f) Cut 50% decryption

Fig. 13 Decryption under different degrees of ciphertext loss



(a) 0.001 noise attack (b) 0.01 noise attack (c) 0.1 noise attack

(d) 0.001 decryption (e) 0.01 decryption (f) 0.1 decryption

Fig. 14 Decryption of encrypted graph under different noise attacks

6 Conclusions

This paper presents a new two-dimensional discrete hyperchaotic map, which has a wider chaotic region and two larger Lyapunov exponents compared with Hénon map. Next, we use it to generate many S-boxes. Then they are dynamically applied to image encryption. Simulation experiments prove that our encryption algorithm based on dynamic S-box is effective, and compared with some cryptosystems, it has better performance, and can resist some common attacks. Although the encryption algorithm has not been mathematically proven, we will investigate it in the future.

Data Availability Statements: The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Funding: This research is supported by the National Natural Science Foundation of China (No: 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (No: MMJJ20170203), Liaoning Province Science and Technology Innovation Leading Talents Program Project (No: XLYC1802013), Key R&D Projects of Liaoning Province (No: 2019020105-JH2/103), Jinan City'20 universities' Funding Projects Introducing Innovation Team Program (No: 2019GXRC031), the Science and Technology Research Program of Chongqing Municipal Education Commission (Nos: KJQN201900529 and KJQN202100506).

Conflict of Interest: The authors declare that they have no conflict of interest.

References

[1] Ma X, Mou J, Liu J, Ma C, Yang F, Zhao X. A novel simple chaotic circuit based on memristor-

memcapacitor. Nonlinear Dynamics, 2020, 100(3): 2859-2876.
[2] Márquez-Martínez L A, Cuesta-García J R, Pena Ramirez J. Boosting synchronization in chaotic systems: combining past and present interactions. Chaos, Solitons & Fractals, 2022, 155: 111691.
[3] Ma C, Mou J, Li P, Liu T. Dynamic analysis of a new two-dimensional map in three forms: integer-order, fractional-order and improper fractional-order. European Physical Journal-Special Topics, 2021, 203(7): 1945-1957.
[4] Feng D, An H, Zhu H, Zhao Y. The synchronization method for fractional-order hyperchaotic systems. Physics Letters A, 2019, 383(13): 1427-1434.
[5] Ma C, Mou J, Xiong L, Banerjee S, Liu T, Han L. Dynamical analysis of a new chaotic system: asymmetric multistability, offset boosting control and circuit realization. Nonlinear Dynamics, 2021, 103(3): 2867-2880.
[6] Wang X, Guan N. 2D Sine-Logistic-Tent-coupling map for image encryption. Journal of Ambient Intelligence and Humanized Computing, 2022.
[7] Gao X, Mou J, Xiong L, Sha Y, Yan H, Cao Y. A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. Nonlinear Dynamics, 2022, 108: 613-636.
[8] Wang X, Chen S, Zhang Y. A chaotic image encryption algorithm based on random dynamic mixing. Optics and Laser Technology, 2021, 138: 106837.
[9] Li X, Mou J, Banerjee S, Cao Y. An optical image encryption algorithm based on fractional-order laser hyperchaotic system. International Journal of Bifurcation and Chaos, 2022, 32(2): 2250035.
[10] Wang X, Yang J, Guan N. High-sensitivity image encryption algorithm with random cross diffusion based on dynamically random coupled map lattice model. Chaos, Solitons & Fractals, 2021, 143: 110582.
[11] Ge M, Ye R. A novel image encryption scheme based on 3D bit matrix and chaotic map with markov properties. Egyptian Informatics Journal, 2019, 20: 45-54.
[12] Wang X, Yang J. Spatiotemporal chaos in multiple coupled mapping lattices with multi-dynamic coupling coefficient and its application in color image encryption. Chaos, Solitons & Fractals, 2021, 147:110970.
[13] Maazouz M, Toubal A, Bengherbia B, Houhou O, Batel N. FPGA implementation of a chaos-based image encryption algorithm. Journal of King Saud University-Computer and Information Sciences, 2022. (In Press)
[14] Amine M M, Wang X, Zakariya T M. A sensitive dynamic mutual encryption system based on a new 1D chaotic map. Optics and Lasers in Engineering, 2021, 139: 106485.
[15] Gao X. Image encryption algorithm based on 2D hyperchaotic map. Optics and Laser Technology, 2021, 142: 107252.
[16] Wang F, Li X, Xia F, Xie Z. The novel control method of three dimensional discrete hyperchaotic Hénon map. Applied Mathematics and Computation, 2014, 247: 487-493.
[17] Hua Z, Zhang Y, Bao H, Huang H, Zhou Y. N-dimensional polynomial chaotic system with applications. IEEE Transactions on Circuits and Systems I, 2022, 69(2): 784-797.
[18] Wu A, Cang S, Zhang R, Wang Z, Chen Z. Hyperchaos in a conservative system with nonhyperbolic fixed points. Complexity, 2018, 2018: 9430637.
[19] Naim M, Pacha A, Serief C. A novel satellite image encryption algorithm based on

hyperchaotic systems and josephus problem. Advances in Space Research, 2021, 67(7): 2077-2103.

[20] Hua Z, Zhang Y, Zhou Y. Two-dimensional modular chaotification system for improving chaos complexity. IEEE Transactions on Signal Processing, 2020, 68: 1937-1949.

[21] He Y, Zhang Y, Wang Y. A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system. Neural Computing and Applications, 2020, 32(2): 247-260.

[22] Huang H, Yang S, Ye R. Efficient symmetric image encryption by using a novel 2D chaotic system. IET Image Processing, 2020, 14: 1157-1163.

[23] Hua Z, Zhu Z, Chen Y, Li Y. Color image encryption using orthogonal latin squares and a new 2D chaotic system. Nonlinear Dynamics, 2021, 104: 4505-4522.

[24] Ahmad M, Al-Solami E. Improved 2D discrete hyperchaos mapping with complex behaviour and algebraic structure for strong S-boxes generation. Complexity, 2020.

[25] Li Q, Wang X, Wang H, Ye X, Zhou S, Gao S, Shi Y. A secure image protection algorithm by steganography and encryption using the 2D-TSCC. Chinese Physics B, 2021, 30: 149-160.

[26] Ma C, Mou J, Li P, Liu T. Dynamic analysis of a new two-dimensional map in three forms: integer-order, fractional-order and improper fractional-order. The European Physical Journal Special Topics, 2021, 230: 1945-1957.

[27] Beg S, Ahmad N, Anjum A, Ahmad M, Khan A, Baig F, Khan A. S-box design based on optimize LFT parameter selection: a practical approach in recommendation system domain. Multimedia Tools and Applications, 2020, 79: 11667-11684.

[28] Wang Y, Zhang Z, Zhang L, Feng J, Gao J, Lei P. A genetic algorithm for constructing bijective substitution boxes with high nonlinearity. Information Sciences, 2020, 523: 152-166.

[29] Lambić D. A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. Nonlinear Dynamics, 2020, 100: 699-711.

[30] Hussain I. True-chaotic substitution box based on boolean functions. The European Physical Journal Plus, 2020, 135: 663.

[31] Liu H, Wang X. Cryptanalyze and design strong S-box using 2D chaotic map and apply to irreversible key expansion. Computer Science, 2021.

[32] Zahid A, Al-Solami E, Ahmad M. A novel modular approach based substitution-box design for image encryption. IEEE Access, 2020, 8: 150326-150340.

[33] Yan W, Ding Q. A novel S-box dynamic design based on nonlinear-transform of 1D Chaotic Maps. Electronics, 2020, 10: 1313.

[34] Si Y, Liu H, Constructing keyed strong S-box using an enhanced quadratic map. International Journal of Bifurcation and Chaos, 2021, 31: 2150146.

[35] Khan M, Shah T, Batool S I. Construction of S-box based on chaotic boolean functions and its application in image encryption. Neural Computing and Applications, 2016, 27: 677-685.

[36] Khan M, Asghar Z. A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and S8 permutation. Neural Computing and Applications, 2016, 29: 993-999.

[37] Wang X, Sun H, Gao H, An image encryption algorithm based on improved baker transformation and chaotic S-box. Chinese Physics B, 2021, 30: 060507.

[38] Idrees B, Zafar S, Rashid T, Gao W. Image encryption algorithm using S-box and dynamic Hénon bit level permutation. Multimedia Tools and Applications, 2020, 79: 6135-6162.

[39] Zhang Y, Hao J, Wang X. An efficient image encryption scheme based on S-boxes and

fractional-order differential logistic map. IEEE Access, 2020, 8: 54175-54188.
[40] Farah M A B, Guesmi R, Kachouri A, Samet M. A new design of cryptosystem based on S-box and chaotic permutation. Multimedia Tools and Applications, 2020, 79: 19129-19150.
[41] Arab A, Rostami M J, Ghavami B. An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 2019, 75: 6663-6682.
[42] Wang X, Yang J, A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system. Optik, 2020, 217: 164884.
[43] Zhu H, Tong X, Wang Z, Ma J. A novel method of dynamic S-box design based on combined chaotic map and fitness function. Multimedia Tools and Applications, 2020, 79: 12329-12347.
[44] Devaraj P, Kavitha C. An image encryption scheme using dynamic S-boxes. Nonlinear Dynamics, 2016, 86(2): 927-940.
[45] Liu Y, Tong X, Ma J. Image encryption algorithm based on hyper-chaotic system and dynamic S-box. Multimedia Tools and Applications, 2016, 75: 7739-7759.
[46] Hénon M. A two-dimensional mapping with a strange attractor. Communications in Mathematical Physics, 1976, 50(1): 69-77.
[47] Hua Z, Zhang Y, Zhou Y. Two-dimensional modular chaotification system for improving chaos complexity. IEEE Transactions on Signal Processing, 2020, 68: 1937-1949.
[48] Zhu H, Pu B, Zhu Z, Zhao Y, Song Y. Two-dimensional sine-tent hyperchaotic mapping and its application in image encryption. Small microcomputer system, 2019, 40(07): 1510-1518.
[49] Wei Y, Li Z, Li R. Design of pseudorandom number generator based on chaotic system. Application of electronic Technology, 2020, 46(10): 114-117, 122.
[50] Detombe J, Tavares S. Coustructing large crypographically strong S-boxes. Springer Berlin Heidelberg, 1993: 165-181.
[51] Adams C, Tavares S. The structured design of cryptographically good S-boxes. Journal of Cryptology, 1990, 3(1): 27-41.
[52] Webster A, Tavares S. On the design of S-boxes. Springer Berlin Heidelberg, 1986: 523-534.
[53] Adams C, Tavares S. Good S-boxes are easy to find, Springer New York, 1990: 612-615.
[54] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 1991, 4(1): 3-72.
[55] Matsui M. Linear cryptanalysis method for DES cipher. Springer Berlin Heidelberg, 1994: 386-397.
[56] Zhu C. A novel image encryption scheme based on improved hyperchaotic sequences. Optics Communications, 2012, 285(1): 29-37.
[57] Chen G, Mao Y, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 2004, 21(3): 749-761.
[58] Wang Y, Wong K W, Liao X, Chen G. A new chaos-based fast image encryption algorithm. Applied Soft Computing, 2011, 11(1): 514-522.