

An image encryption algorithm based on improved baker transformation and chaotic S-box

Xing-Yuan Wang(王兴元) , Huai-Huai Sun(孙怀怀) , and Hao Gao(高浩)
Citation: Chin. Phys. B, 2021, 30 (**6**): 060507. DOI: 10.1088/1674-1056/abdea3
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Fractal sorting vector-based least significant bit chaotic permutation for image encryption

Yong-Jin Xian(咸永锦), Xing-Yuan Wang(王兴元), Ying-Qian Zhang(张盈谦), Xiao-Yu Wang(王晓雨), and Xiao-Hui Du(杜晓慧)
Chin. Phys. B, 2021, 30 (**6**): 060508. DOI: 10.1088/1674-1056/abda35

A multi-directional controllable multi-scroll conservative chaos generator: Modelling, analysis, and FPGA implementation

En-Zeng Dong(董恩增), Rong-Hao Li(李荣昊), and Sheng-Zhi Du(杜升之)
Chin. Phys. B, 2021, 30 (**2**): 020505. DOI: 10.1088/1674-1056/abc239

Memristor-based hyper-chaotic circuit for image encryption

Jiao-Jiao Chen(陈娇娇), Deng-Wei Yan(闫登卫), Shu-Kai Duan(段书凯), and Li-Dan Wang(王丽丹)
Chin. Phys. B, 2020, 29 (**11**): 110504. DOI: 10.1088/1674-1056/abbbfe

New chaotical image encryption algorithm based on Fisher-Yatess scrambling and DNA coding

Xing-Yuan Wang(王兴元), Jun-Jian Zhang(张钧荐), Fu-Chen Zhang(张付臣), Guang-Hui Cao(曹光辉)
Chin. Phys. B, 2019, 28 (**4**): 040504. DOI: 10.1088/1674-1056/28/4/040504

Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem

Zeyu Liu(刘泽宇), Tiecheng Xia(夏铁成), Jinbo Wang(王金波)
Chin. Phys. B, 2018, 27 (**3**): 030502. DOI: 10.1088/1674-1056/27/3/030502

An image encryption algorithm based on improved baker transformation and chaotic S-box*

Xing-Yuan Wang(王兴元)†, Huai-Huai Sun(孙怀怀)‡, and Hao Gao(高浩)

School of Information Science and Technology, Dalian Maritime University, Dalian 116026, *China*

(Received 8 December 2020; revised manuscript received 15 January 2021; accepted manuscript online 22 January 2021)

The algorithm is an image encryption algorithm based on the improved baker transformation and chaotic substitution box (S-box). It mainly uses the initial values and parameters of a one-dimensional logistic chaotic system as an encryption key. Specifically, in the image scrambling stage, the algorithm primarily uses an improved baker transform method to process the image. In the image diffusion stage, the algorithm first uses the chaotic S-box method to process the encryption key. Secondly, an exclusive OR (XOR) operation is performed on the image and the encryption key to initially diffuse the image. Finally, the image is again diffused using the method of ortho XOR. Simulation analysis shows that the algorithm can achieve good encryption effect, simple and easy implementation, and good security. In the digital image communication transmission, it has good practical value.

Keywords: image encryption, improved baker transformation, chaotic S-box, chaotic sequence

PACS: 05.45.Gg, 05.45.Ac, 07.05.Pj **DOI:** 10.1088/1674-1056/abdea3

1. Introduction

With the continuous development of computer network technology, the confidentiality of network information has attracted more and more attention. Because digital images have the advantages of long-term preservation, multiple replication, and easy transmission, they have gradually become the main way for people to obtain information on the network. However, there are also hidden dangers. Mainly because the image involves a lot of information, it is easy to be stolen in the transmission of the network, thereby bringing great trouble to people. Due to the rapid development of the network, it is possible for one to collect the digital image information in the network.[1] Therefore, it is extremely important to transmit digital image information over the network to ensure its security. Nowadays, many image protection schemes have been proposed, such as encryption, watermarking, steganography, and other methods.[2–4] For image encryption, designing a safe and effective encryption algorithm has become an inevitable option. Since the classical encryption algorithm does not take into account the inherent characteristics of large data capacity and high redundancy of images, these algorithms are not suitable for image encryption. Chaos is not only a new form of existence in nonlinear dynamic systems, but also closely related to fractals in nonlinear science. It can be said that chaos is the fractal of time, and fractal is the chaos of space.[5–7] In the chaotic image encryption algorithm used cleverly are the initial conditional sensitivity, pseudo-randomness, ergodicity, and reproducibility of the motion law of the chaotic system. These properties can meet the requirements for the security sensitivity characteristics of encryption algorithms. Based on this, many researchers home and abroad have proposed many efficient and secure chaotic image encryption algorithms. Chaos-based image encryption algorithms have become a research hotspot.

In general, chaotic-based image encryption algorithms mainly include two steps: scrambling of image pixel positions and diffusion of image pixel values. At present, common image scrambling methods cover scrambling methods based on Arnold transform, magic square transform, and baker transform. The baker transformation method is a transformation technique that stretches and folds continuous planar regions.[8] Applying the traditional baker transformation method to the image scrambling, if the number of transformations is unreasonable, it will get a bad scrambling effect. In addition, when the continuous plane area processed by the conventional baker transformation method is too large, there is a disadvantage that the transformation randomness is poor and the transformation time is long. Therefore, this article proposes an improved method of applying the baker transformation to the image scrambling stage. The encrypted image is divided into 16 small blocks on average, and the image is scrambled by using a conventional baker transform method for each block,

*Project supported by the National Natural Science Foundation of China (Grant No. 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund, China (Grant No. MMJJ20170203), the Liaoning Provincial Science and Technology Innovation Leading Talents Program Project, China (Grant No. XLYC1802013), the Key Research and Development Projects of Liaoning Province, China (Grant No. 2019020105-JH2/103), the Jinan City '20 universities' Funding Projects Introducing Innovation Team Program, China (Grant No. 2019GXRC031), and the "Double First-rate" Construction Project ("Innovation Project"), China (Grant No. SSCXXM013).

†Corresponding author. E-mail: xywang@dlmu.edu.cn

‡Corresponding author. E-mail: 2471054392@qq.com

© 2021 Chinese Physical Society and IOP Publishing Ltd

and the number of transformations is controlled by the chaotic sequence, so that the scrambling effect is more random. In addition, the S-box is a module that plays a central role in a block cipher system, and mainly plays a role of confusion and proliferation. The security strength of the S-box determines the security of the encryption algorithm. Traditional cryptography uses algebraic methods to construct the S-box. Although a high degree of nonlinearity can be obtained, the differential performance is relatively weak due to the simplistic structure and cannot resist algebraic attacks.[9,10] The application of chaotic systems to the design of nonlinear S-box is more effective. Based on this, this paper cites the chaotic S-box designed in Ref. [11] to process the encryption key of the algorithm. Therefore, the main contribution of this paper lies in proposing a new chaotic image encryption algorithm. In the algorithm,the improved baker transformation and chaotic S-box are utilized. Experimental results prove that the algorithm proposed in this article is more efficient and safer.

The rest of this article is organized as follows. In Section 2 presented is the initial preparation, describing the theoretical knowledge and chaotic systems used in the algorithm. In Section 3 given is an algorithm description that describes the encryption process of the algorithm and comes with an encryption flowchart. In Section 4 the results of the simulation experiment are provided. Several digital images are selected and the simulation results are presented. In Section 5 analyzed is the security of the algorithm from various attack methods. In Section 6,some conclusions are drawn from the present study and the direction of future work is also suggested.

2. Initial preparation work

2.1. Improved baker transformation

In fact, the baker transformation can produce stretch-like and folding effects in the state space, just like a baker rubbing a piece of dough. Imagine that adding a blue food colorant to the dough, which is repeatedly stretched and folded by the baker, the blue color is evenly mixed in the dough. The stretching and folding mechanisms cause adjacent points to eventually separate in an exponential manner, creating a sensitive dependence on the initial state. Therefore, the baker transformation has chaotic dynamic characteristics, and thus very much suits an image scrambling method.[12]

In this paper, a baker discrete transformation method for data dot matrix scrambling of digital images is designed and described as follows:

$$p(x,y)=\begin{cases}(2x,2y-1), & 1\le x\le M/2, 1\le y\le N/2,\\ (2x-M,2y), & M/2<x\le M,\ 1\le y\le N/2,\\ (2x-1,2N-2y+2), & 1\le x\le M/2,\ N/2<y\le N,\\ (2x-M-1,2N-2y+1), & M/2<x\le M,\ N/2<y\le N,\end{cases} \tag{1}$$

where the plain image $A_{M\times N}$ pixel value is represented by $p(x,y)$. An example of a traditional baker transformation is shown in Fig. 1.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

→

24	6	23	5	22	4
1	19	2	20	3	21
30	12	29	11	28	10
7	25	8	26	9	27
36	18	35	17	34	16
13	31	14	32	15	33

Fig. 1. Traditional baker transformation process of 6×6 matrix.

It can be seen that there are certain limitations to applying the traditional baker transformation to the image scrambling. On the one hand, when the number of transformations is too small, the visual scrambling effect is not good. In Ref. [12], it was proved experimentally that the original image is unrecognizable when the number of transformations exceeds 4 times; on the other hand, the continuous plane area of processing is very large, and there will be disadvantages such as long time-consuming and poor randomness of scrambling. Therefore, in this paper the traditional baker transformation is improved to some extent. On the one hand, the original image is divided into multiple blocks, and each small image is separately transformed into a traditional baker, and finally each small image after being scrambled is spliced into a scrambled image. In addition, the number of times the Baker transforms is controlled by the chaotic sequence, so that the number of times of each small image transformation is different, so the scrambling randomness is better.

2.2. S-box description

In general, the S-box is also known as the replacement box. It is a nonlinear transformation tool. There are three main methods of constructing the S-box. They are stochastic construction methods, mathematical construction methods, and a combination of the two methods.[13,14] In actual use, it can be considered that the S-box is a Boolean map, and the S-box of size $M\times N$ has the form $F_2^M\to F_2^N$, that is, the data of the number of bits M are input to the S-box, and the data of the N bits are output. The M-bit data change nonlinearly and can become seemingly random N-bit data.[15]

Table 1. 16×16 matrix representation of S-box.

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

In addition, applying the chaotic system to the design and generation process of the S-box will achieve more desirable results. Khan *et al.*[11] proposed a robust S-box construction technique based on the chaotic Lorenz system. This S-box can effectively eliminate the need of using a separate key in the scrambling diffusion structure, and the generated S-box has an ideal nonlinear performance. Simulation experiment analysis shows that the S-box has a good encryption performance. The chaotic S-box discussed in Ref. [11] is cited in this paper, and its compositions are shown in Table 1.

2.3. Chaotic system

The one-dimensional logistic mapping is a typical nonlinear iterative equation. The equation is as follows:

$$x_{k+1} = ux_k(1-x_k). \tag{2}$$

where the logistic mapping system is in a chaotic state when $3.5699 < u \leq 4$, x_k refers to the iterative state value, defined between consecutive real fields from 0 to 1, and x_0 is the iteration initial value. For a given initial value x_0, the sequence generated under the action of Eq. (2) is aperiodic, non-convergent and sensitive to initial conditions. Because the logistic mapping is a simple nonlinear one-dimensional discrete iterative mapping, it is easy to implement in hardware. So it has become one of the most widely used chaotic maps in digital chaotic systems.[16–18]

3. Algorithm description

The encryption algorithm proposed in this paper has the same encryption steps as most of previous algorithms, that is, image processing, scrambling and diffusion of images. Because the security and effectiveness of the proposed algorithm should be strengthened, different encryption keys are used in different image encryption stages. Aiming at the encryption algorithm proposed in this paper, the specific implementation process is presented as follows.

3.1. Image processing

The image encryption algorithm proposed in this paper and most of previous algorithms have the same requirements for image sizes, that is, the original encrypted image is in the form of a square matrix. In other words, for a pair of grayscale digital images of size $M \times N$, $M = N$ is required. If $M \neq N$, the method of zeroing the original image is taken, so that the number of rows and the number of columns of the original image are equal.

3.2. Scrambling process

Step 1 Enter the keys a_0 and u_1, and substitute the two into the formula of the logistic chaotic map. The 1000 iterations eliminate the transient effects. After 16 consecutive iterations, the obtained chaotic sequence is recorded as $a_i (i = 1, 2, \ldots, 16)$. The substitution of a chaotic sequence a_i of length 16 into Eq. (3) yields a one-dimensional sequence $a'_i (i = 1, 2, \ldots, 16)$.

$$a'_i = \text{floor}(a_i \times 10) + 20. \tag{3}$$

Step 2 The original image P is divided into 16 sub-images according to the rank and column average. The sub-image obtained after the division is recorded as p_i $(i = 1, 2, \ldots, 16)$. The baker transformation is performed separately for each small image, and the number of baker transformations is controlled by the one-dimensional sequence a'_i. The 16 small images obtained by the baker transformation are sequentially spliced into a large decrypt image, which is recorded as P_1.

Step 3 Similarly, the keys b_0 and u_2 are substituted into the formula of the logistic map. The 1000 iterations eliminate the transient effects. After continuing to implement $M \times N$ iterations, the obtained chaotic sequence is recorded as b_i $(i = 1, 2, \ldots, M \times N)$. And the substitution of b_i into Eq. (4)

yields

$$b_i' = \text{sort}(b_i), \tag{4}$$

where sort$(\cdot)$ represents the sorting function. Using the sorting function, the corresponding subscript of each value in the sequence b' in the sequence b is stored as the sequence D. A scrambled arrangement in which D is a sequence of integers from 1 to $M \times N$ can be obtained. The image P_1, from the first pixel point to establish P_{1i} to P_{Di} mapping. The positions are exchanged from the first element to the last element one by one. After that, image P_1 is converted into image P_2 with a size of $M \times N$.

At this point, the scrambling process for the encrypted image is completed.

3.3. Diffusion process

Step 1 First, enter the keys x_0 and u_3, and substitute the two keys into the logistic chaotic mapping formula. The 1000 iterations eliminate the transient effects. Then $M \times N$ consecutive iterations are implemented. The chaotic sequence x_i $(i = 1,2,\ldots,M \times N)$ is obtained and substituted into the following formula:

$$x_i' = \text{floor}(x_i \times W) \bmod W, \tag{5}$$

where $W = \max(M,N)$. Thus, a one-dimensional sequence x_i' is obtained, and the sequence length is $M \times N$.

Step 2 Let $\text{key}_0 = \text{floor}(P_{\text{mean}}) + R$, where key_0 refers to an initial key in the encryption process, P_{mean} represents an average pixel value of the image P, and R is a given integer. The initial key key_0 converted from a decimal number to an 8-bit binary number is still denoted as key_0.

Step 3 Take the 3rd to 6th digits of the 8-bit binary number key_0 and record it as key_{01}. Convert these 4-bit binary numbers into decimal numbers. Then take the first 2 bits and the last 2 bits of the 8-bit binary number key_0 and record it as key_{02}. Convert these 4-bit binary numbers into decimal numbers. Enter the chaotic S-box for nonlinear transformation. The specific operation is indicated by the following formula:

$$\begin{aligned} \text{key} = \text{Sbox}((&\text{bin2dec}(\text{key}_{01}) + 1), \\ &(\text{bin2dec}(\text{key}_{02}) + 1)). \end{aligned} \tag{6}$$

Here, the bin2decc$(.)$ function converts binary numbers into decimal numbers. The key is the value obtained by processing the initial key key_0 into the chaotic S-box. It is a decimal number.

Step 4 Use the left shift operator. For the decimal number key, the respective loops are shifted leftward by 2 bits and 5 bits. The specific operation is as shown in the following formula:

$$\text{key}' = \text{key} \oplus (\text{key} \ll 5) \oplus (\text{key} \ll 2). \tag{7}$$

Step 5 Expand the two-dimensional image matrix P_2 with a size of $M \times N$ into a one-dimensional vector A_i $(i = 1,2,\ldots,M \times N)$. Then use the following formula to operate:

$$\begin{cases} A_i' = A_i \oplus x_i' \oplus \text{key}', \\ \text{key}_0 = A_i'. \end{cases} \tag{8}$$

The obtained one-dimensional vector A_i' $(i = 1,2,\ldots,M \times N)$ is converted into an image $M \times N$ and referred to as P_3.

Step 6 Enter the keys y_0 and u_4, and substitute the two keys into the logistic chaotic mapping formula. The 1000 iterations eliminate the transient effects. Implement the selected $M \times N$ iterations again. The chaotic sequence y_i (where $i = 1,2,\ldots,M \times N$) is obtained. The chaotic sequence y_i is substituted into the following formula to obtain the processed one-dimensional sequence y_i':

$$y_i' = \text{floor}(y_i \times 10^{14}) \bmod W. \tag{9}$$

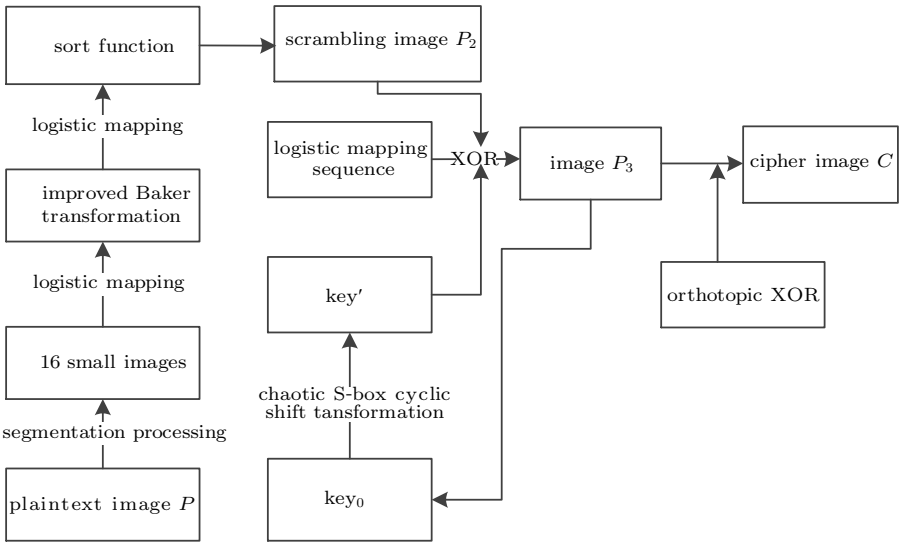


Fig. 2. Flowchart of encryption process.

Step 7 Convert a one-dimensional sequence y'_i into a two-dimensional array B with a size of $M \times N$. The adjacent-side XOR operation is performed with the encrypted image P_3 obtained from the first step of diffusion. The specific description is as follows:

$$C = \begin{cases} C_1 = E_1 \oplus B_1, & i = 1, \\ C_i = E_i \oplus E_{i-1} \oplus B_i, & i \neq 1, \end{cases} \tag{10}$$

where E_i refers to the i-th element of image P_3.

In summary, the diffusion process for the encrypted image P_2 ends. And the diffused image is denoted as C.

Thus, the cipher image C is obtained. The encryption flow chart of the algorithm is shown in Fig. 2.

4. Results of simulation experiment

The simulation experiments in this paper are performed with the software Matlab R2017a. The computer configuration used is a 2.80-GHz CPU, 8 GB of memory and Microsoft Windows 10 operating system. In order to verify the effectiveness of the above algorithm, in this paper, Lena, Girl, and House gray digital images with a size of 256×256 are selected as the plain images in the simulation experiment.

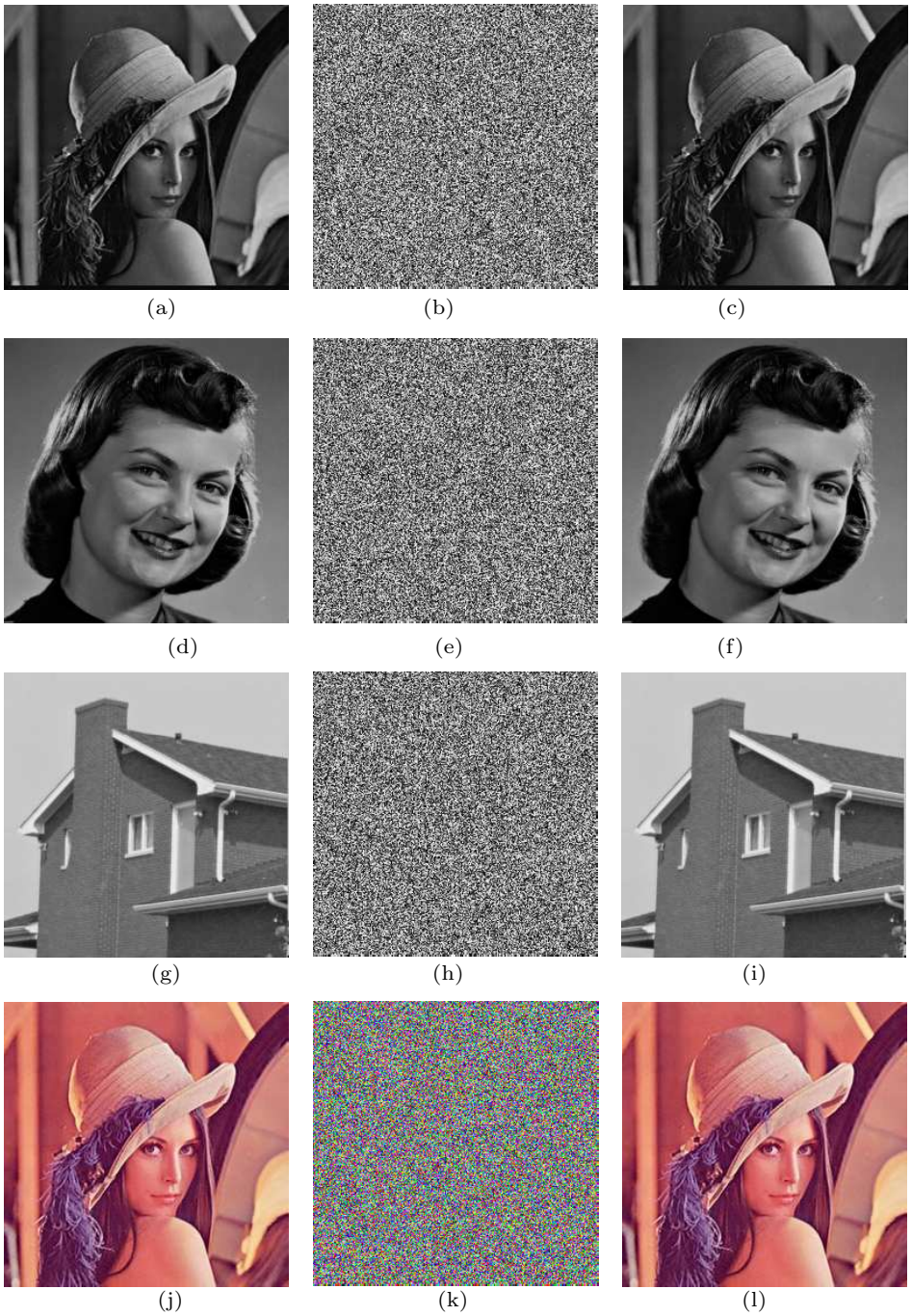


Fig. 3. Four image encryption/decryption experiment results: (a) Lena, (b) cipher image, (c) decoding image, (d) Girl, (e) cipher image, (f) decoding image, (g) House, (h) cipher image, (i) decoding image, (j) Lena2, (k) cipher image, (l) decoding image.

The encryption and decryption results of Lena, Girl, and House grayscale images are shown in Fig. 3. In addition, the chaotic image encryption algorithm is also suitable for the encryption of color images. We only need to decompose the color image into three grayscale images, and then use the algorithm to encrypt the three grayscale images, and finally combine them into a color cipher map. Experiments are performed using a Lena color image, and the results are still shown in Fig. 3.

5. Security analysis

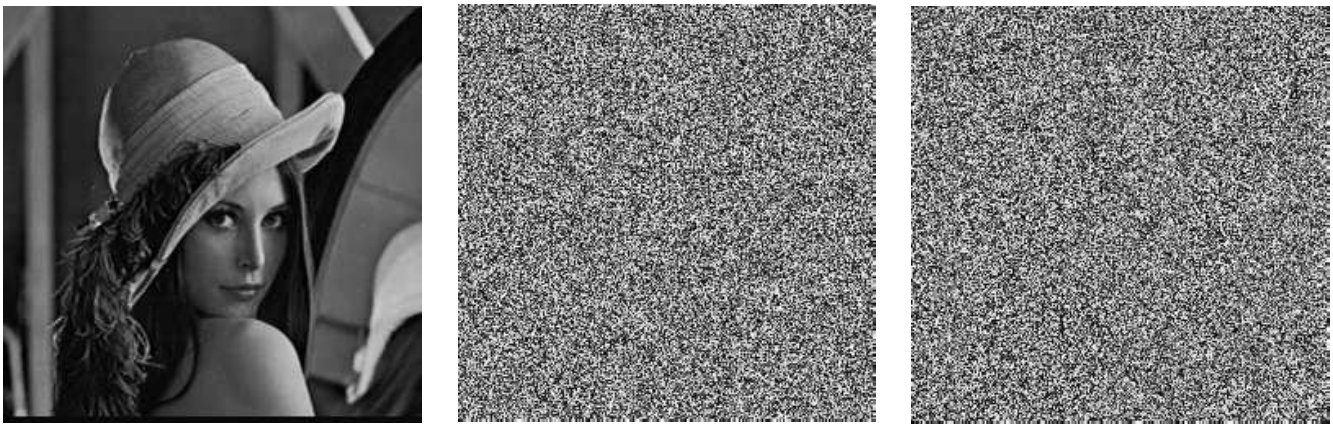
5.1. Exhaustive attack analysis

5.1.1. Key space analysis

The key is the core of the entire cryptosystem. Usually, the more the parameters and the larger the key space, the higher the difficulty in deciphering is and the more secure the encryption system. The key space analysis in the algorithm is mainly to prevent possible exhaustive attacks.[19,20] The key of this paper is as follows: the chaotic initial value and control parameters of the logistic chaotic mapping formula in the scrambling and diffusion stage of the plain image; and key_0, specifically, a_0, b_0, x_0, y_0, u_1, u_2, u_3, u_4, and key_0. If the computing precision of the computer is 10^{-14}, the key space of the algorithm proposed in this paper is 10^{126}. In Refs. [21,22] proposed was the algorithms with key spaces of 10^{89} and 10^{98} respectively. Therefore, the algorithm proposed in this paper has a larger key space value, and this value meets the security requirements of the key space.

5.1.2. Key sensitivity analysis

In order to test the sensitivity of the key, the initial values x_0 and y_0 of the chaotic system are increased by 10^{-14} respectively, with the other keys unchanged. The image is decrypted using the correct key and a slightly altered key. The experimental object is a Lena grayscale image. Figure 4 shows the test results. Figure 4(a) shows that using the correct key for decryption, the original image can be correctly decrypted. Figure 4(b) shows the use of the key $x_0 = x_0 + 10^{-14}$ for decryption. Figure 4(c) shows the use of the key $y_0 = y_0 + 10^{-14}$ for decryption. It can be clearly observed that the two images obtained by being decrypted with the wrong key have no information containing the original image at all. Therefore, the algorithm is very sensitive to encryption keys and has high confidentiality.



(a) (b) (c)

Fig. 4. Key sensitivity test: (a) decrypt with the correct key, (b) decrypt with wrong key, (c) decrypt with wrong key.

5.2. Statistical attack analysis

5.2.1. Histogram analysis

The histogram statistics of the encryption system is mainly the area that reflects the distribution of image pixel values. After the image is encrypted, the image is not recognized after encryption, and its statistical characteristics will also change accordingly. Generally, the histogram distribution of the plain image is concentrated. After processing by the encryption algorithm, the more uniform the pixel value distribution of the cipher image, the more ideal it is. That is, the more uniform the histogram looks, the better the image is.[23–25] Figure 5 shows the histograms of the plain and cipher images of Lena, Girl, and House, respectively. The experimental results show that the pixel values of the plain image are unevenly distributed, and the pixel values of the cipher image obtained by the algorithm are evenly distributed in the whole pixel space, and the pixel gray value appears in a range of [0, 255]. The probabilities are almost equal, and it can be analyzed that it is difficult for an illegal attacker to use the statistical properties of image pixel values to recover the original image.

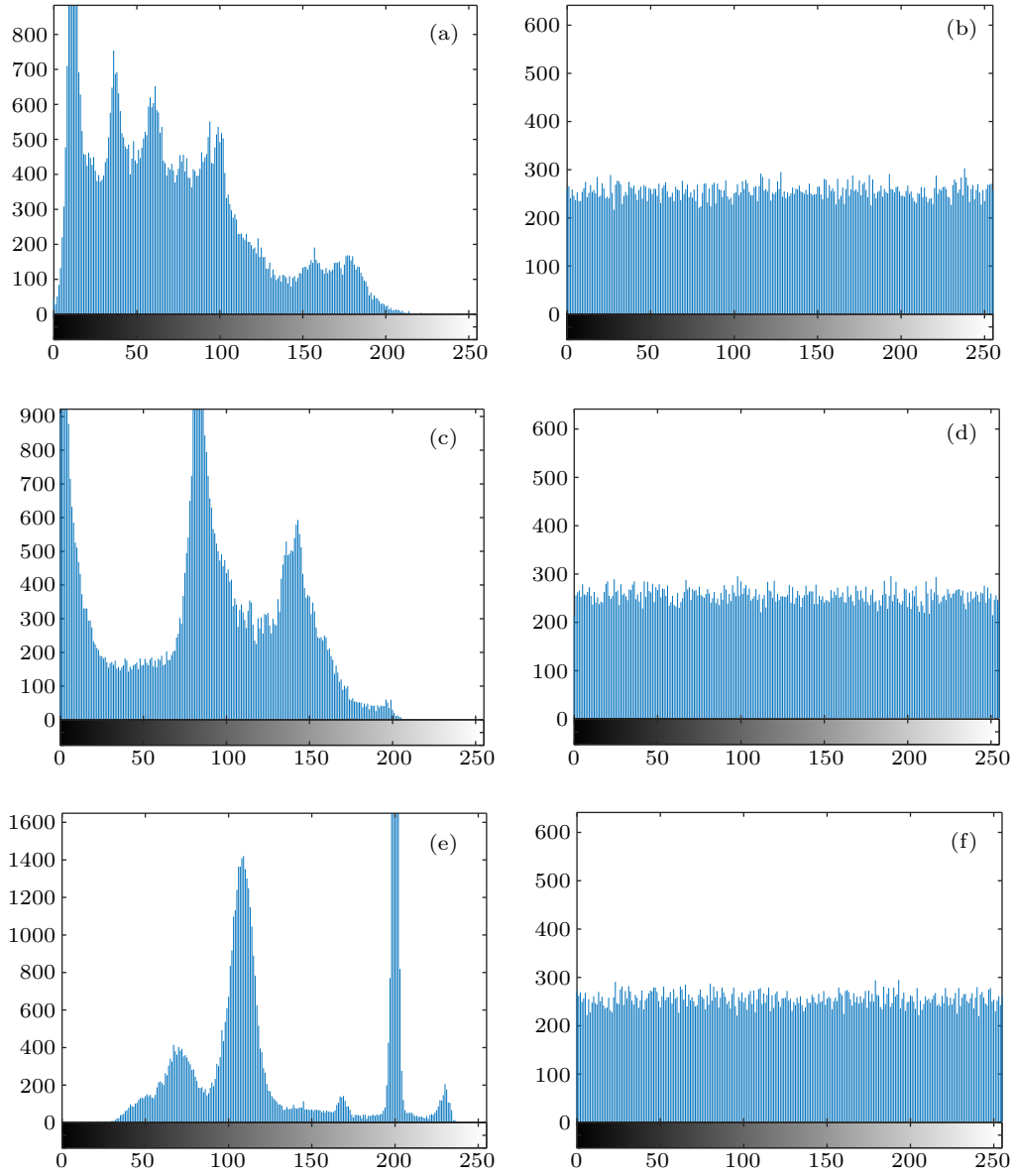


Fig. 5. Histogram of plain and cipher images: (a) Lena plain histogram, (b) Lena cipher histogram, (c) Girl plain histogram, (d) Girl cipher histogram, (e) House plain histogram, (f) House cipher histogram.

5.2.2. Adjacent pixel correlation analysis

The high correlation of adjacent pixels of an image is an essential feature of digital images. In order to resist the statistical attacks, the correlation of adjacent pixels must be reduced, and the smaller the correlation coefficient, the better the encryption performance is.[26,27] In order to analyze the correlation of adjacent pixels, taking the Girl gray image for example, 10^4 pixel points are randomly selected for correlation analysis. Their correlation coefficients are calculated according to Eqs. (11) and (12).[28] Table 2 shows the correlation coefficients of the three grayscale images in three directions before and after encryption. Figures 6(a), 6(c), and 6(e) show the distribution of adjacent pixel correlations of the plain image of Girl in three directions. Figures 6(b), 6(d), and 6(f) show the adjacent pixel correlation distributions of the cipher image of Girl in three directions.

Table 2. Correlation of adjacent pixels.

Direction	Plain image			Cipher image		
	Lena	Girl	House	Lena	Girl	House
Horizontal	0.9721	0.9599	0.9874	−0.0005	0.0053	0.0018
Vertical	0.9775	0.9561	0.9831	−0.0057	−0.0086	−0.0166
Diagonal	0.9675	0.9330	0.9699	0.0032	−0.0012	−0.0022

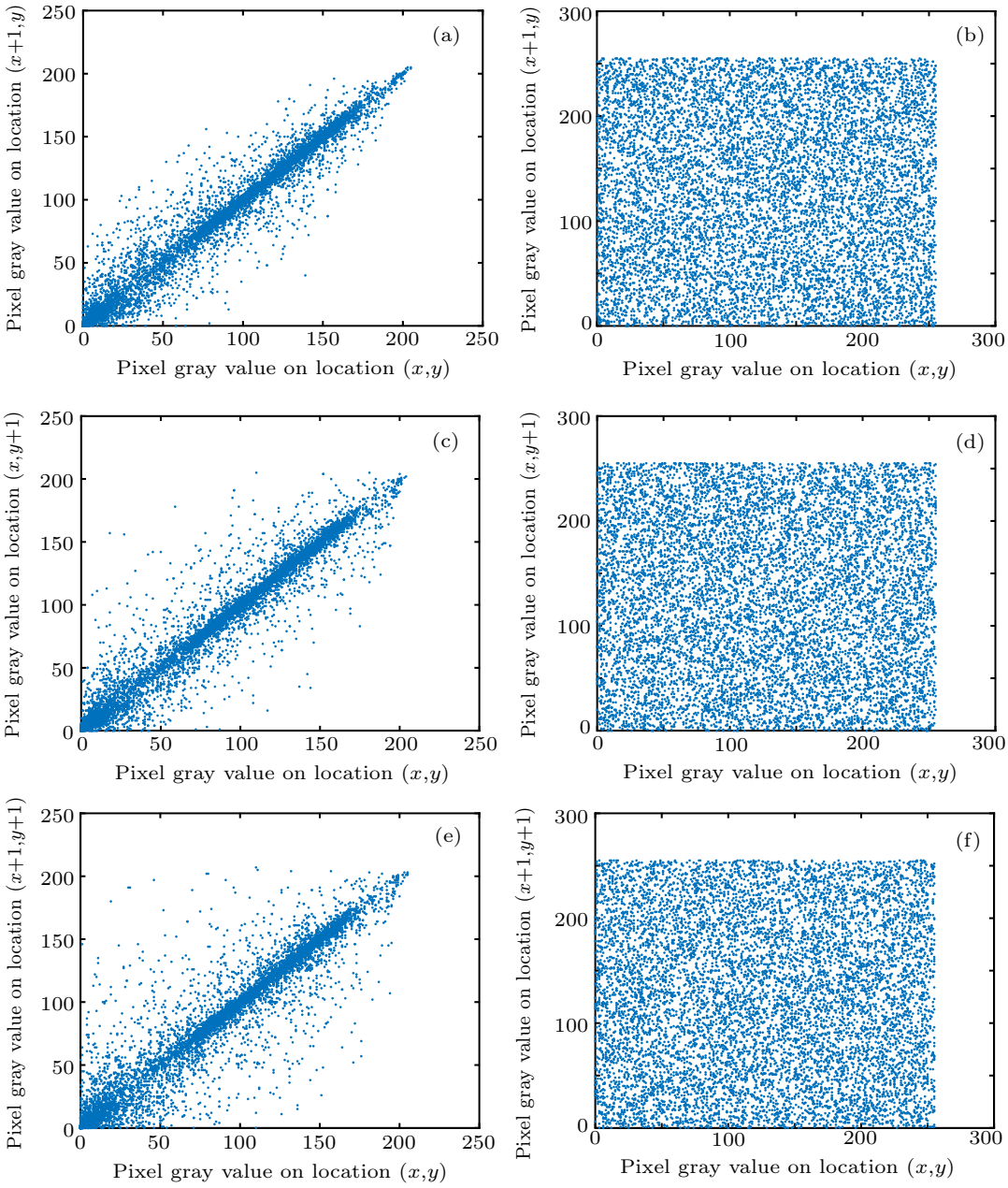


Fig. 6. Adjacent pixel correlation between pre-encrypted and encrypted images: (a) horizontal correlation of Girl image, (b) horizontal correlation of cipher, (c) vertical correlation of Girl image, (d) vertical correlation of cipher, (e) diagonal correlation of Girl image, (f) diagonal correlation of cipher.

Table 3. Comparisons among correlation coefficients of images.

Image	Lena	Ref. [21]	Ref. [22]	Ref. [29]	Ref. [30]
Horizontal	−0.0005	0.0214	0.0114	−0.0074	0.0008
Vertical	−0.0057	0.0465	−0.0011	0.0069	0.0016
Diagonal	0.0032	−0.0090	−0.0032	−0.0191	0.0115

In addition, in Table 3 the gray-scale image Lena is taken for example, and the experimental results of its adjacent pixel correlation with other algorithms are compared. All experimental results prove that the cipher image correlation is greatly reduced after encryption by the algorithm, which can better resist statistical attacks based on correlation analysis.

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}}, \tag{11}$$

where

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x)(y_i - E(y)),$$
$$D(x) = \frac{1}{N}\sum_{i+1}^{N}(x_i - E(x))^2, \quad E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i. \tag{12}$$

5.2.3. Information entropy

In this subsection the information entropy analysis in security analysis is conducted. It is a measure of the order of information. The closer to a uniform distribution the probability distribution of image pixel values, the larger the information entropy is and the smaller the information entropy. In particular, When there is a probability that the pixel values are equal, the image information is the largest.[31,32] The image

information entropy is given by Eq. (13). In Table 4 listed are the information entropy of the plain and cipher maps of the three grayscale images. The experimental results show that the information entropy of each plain image is significantly different from the theoretical value, and all pixel values of the cipher image appear with almost equal probability. In Table 5 the gray-scale image Lena is taken for example to compare the results of the information entropy experiment with those from other algorithms. This proves that the algorithm proposed in this paper is effective.

$$H(s) = \sum_{i=0}^{2^L-1} p(s_i) \log_2 \frac{1}{p(s_i)}. \tag{13}$$

Table 4. Information entropy of plain images and cipher images.

Images	Lena (256×256)	Girl (256×256)	House (256×256)
Plain images	7.3218	7.2575	6.3323
Cipher images	7.9975	7.9973	7.9975

Table 5. Comparison among results of information entropy.

Image	Lena (256×256)	Ref. [21]	Ref. [22]	Ref. [29]	Ref. [30]
Plain image	7.3218	–	–	–	–
Cipher image	7.9975	7.9993	7.9969	7.9963	7.9970

5.3. Cropping attack analysis

Cropping attack is also a common attack method for an attack to image encryption, launched exerted by an illegal attacker.[33] Therefore, in order to test the resistance of the image encryption algorithm to the cropping attack, proposed in this paper, the cipher graph of the experimental object House in four degrees is cut, then the correct encryption key is input to execute the decryption program, and the decrypted image is observed. Figure 7 shows the experimental results. It can be seen that even if the cipher image is cropped by 1/2 degrees, the plain image can still be recognized after being correctly decrypted. Therefore, the chaotic image encryption algorithm proposed in this paper possesses a certain resistance to cropping attacks.

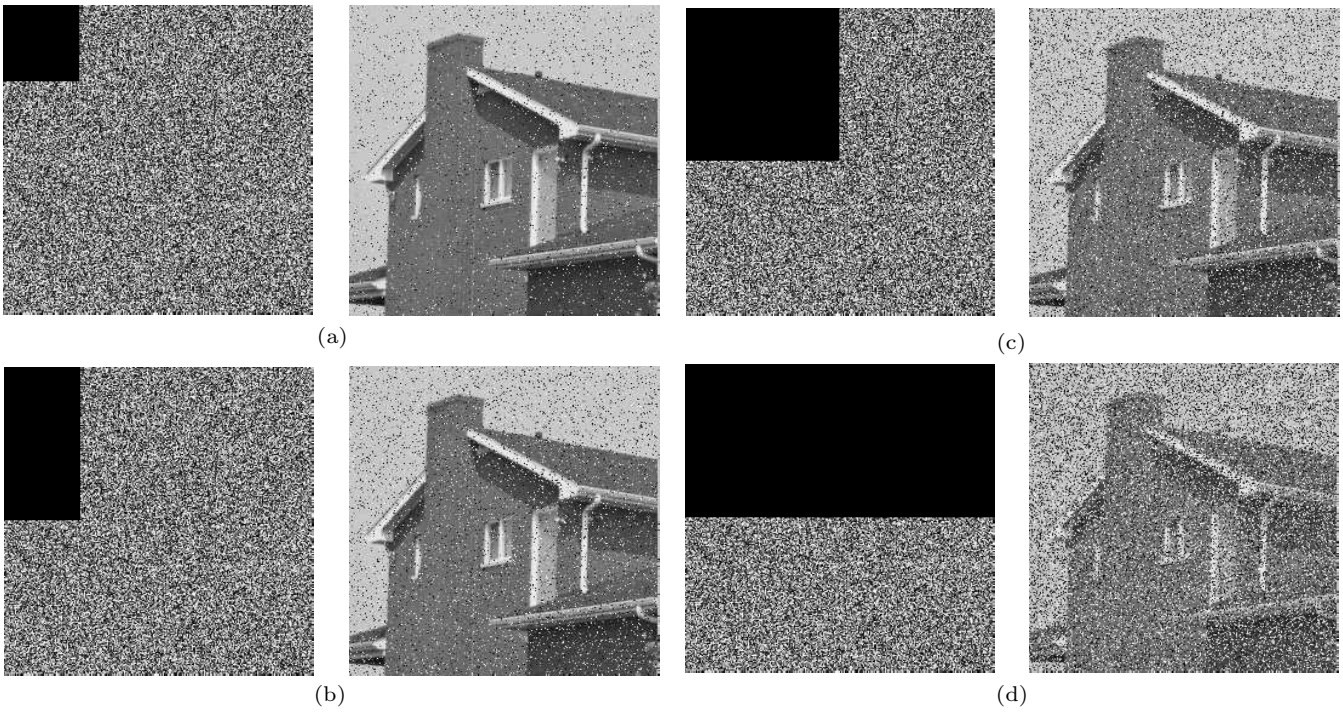


Fig. 7. Recovery after tailoing attacke at different degrees: (a) 1/16-degree cropping and decrypting image, (b) 1/8-degree cropping and decrypting image, (c) 1/4-degree cropping and decrypting image, (d) 1/2-degree cropping and decrypting image.

5.4. Noise attack analysis

In a real-time transmission channel, there is often noise that affects the plain image. Noise attacks are also a way to verify the robustness of cryptosystems.[34–36] In order to evaluate the ability of the encryption algorithm to resist noise in this paper, different salt and pepper noise are added to the House cipher image, and the correct key is used for decryption. The experimental results are shown in Fig. 8. The experimental results show that the encryption algorithm of this paper has better resistance to noise attacks.

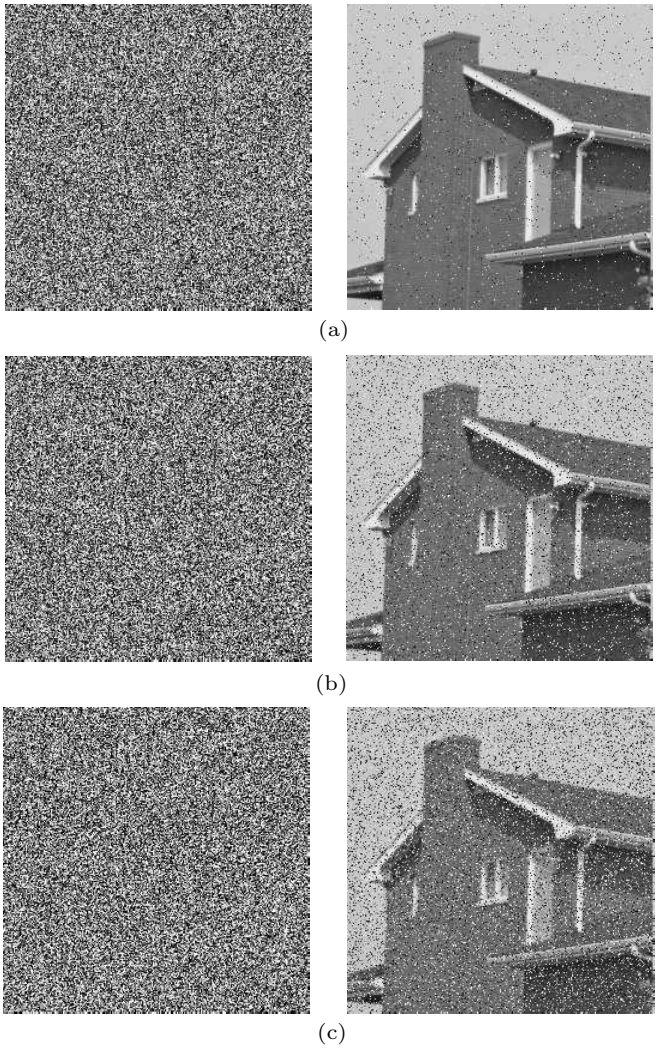


Fig. 8. Cipher image adds different degrees of noise and corresponding decryption maps: (a) cipher and decrypted image with noise intensity of 0.01, (b) cipher and decrypted image with noise intensity of 0.05, (c) cipher and decrypted image with noise intensity of 0.1.

6. Conclusions

In this work, a new image encryption algorithm is proposed. It is based on an improved baker transform and chaos S-box. In the image scrambling phase, the plain image is manipulated primarily using an improved baker transform method. On the other hand, in the image diffusion stage, the chaotic S-box is referenced and the initial key is processed. It also performs XOR operations on image, key, and chaotic sequences. The experimental results and security analysis prove that the digital image encryption algorithm proposed in this paper is effective in resisting multiple attacks; in other words, the image encryption algorithm proposed in this paper is highly secure and excellent encrypted randomness. In addition, in the future direction of work, we can not only starting from the existing encryption methods, improve or propose new encryption methods for chaotic image encryption, but also starting from the chaotic system, improve or propose a more efficient chaotic system, which can be applied to the image encryption algorithms.

References

[1] Tan J T, Luo Y R, Zhou Z and Hai W H 2016 *Chin. Phys. Lett.* **33** 070302
[2] Wang C P, Wang X Y, Xia Z Q, Ma B and Shi Y Q 2020 *IEEE T. Circ. Syst. Vid.* **30** 4440
[3] Wang X Y and Sun H H 2020 *Opt. Laser Technol.* **122** 105854
[4] Wang C P, Wang X Y, Xia Z Q and Zhang C 2019 *Inf. Sci.* **470** 109
[5] Wang Y P, Liu S T and Li H 2020 *Nonlinear Dyn.* **102** 579
[6] Liu S T and Wang P 2018 *Fractal Control Theory* (Singapore: Springer) p. 3
[7] Liu S T, Zhang Y P and Liu C A 2020 *Fractal Control and Its Applications* (Singapore: Springer) p. 235
[8] Wang M L 2007 *Journal of Mianyang Normal University* **26** 126
[9] Tian Y and Lu Z M 2017 *AIP Adv.* **7** 085008
[10] Farah T, Rhouma R and Belghith S 2017 *Nonlinear Dyn.* **88** 1059
[11] Khan M, Shah T, Mahmood H, Gondal M A and Hussain I 2012 *Nonlinear Dyn.* **70** 2303
[12] Zhao X F 2003 *Journal of Northwest Normal University (Natural Science)* **39** 26
[13] Wang Y, Wong K W, Li C B and Li Y 2012 *Phys. Lett. A* **376** 827
[14] Liu H J, Kadir A, Sun X B and Li Y L 2018 *Multimed. Tools Appl.* **77** 1391
[15] Zhang X P, Guo R, Chen H W, Zhao Z M and Wang J Y 2018 *Chin. Phys. B* **27** 080701
[16] Hai Q, Liu S T and Hu C Q 2019 *Asian J. Control* **21** 649
[17] Yan D W, Wang L D and Duan S K 2018 *Acta Phys. Sin.* **67** 110502 (in Chinese)
[18] Zhang F F and Liu S T 2015 *Asian J. Control* **17** 297
[19] Wang X Y, Zhang J J, Zhang F C and Cao G H 2019 *Chin. Phys. B* **28** 040504
[20] Zhang L P, Liu Y, Wei Z C, Jiang H B and Bi Q S 2020 *Chin. Phys. B* **29** 060501
[21] Zhen P, Zhao G, Min L Q and Jin X 2016 *Multimed. Tools Appl.* **75** 6303
[22] Chai X L, Gan Z H, Yuan K, Chen Y R and Liu X X 2019 *Neural Comput. Appl.* **31** 219
[23] Xian Y J and Wang X Y 2021 *Inf. Sci.* **547** 1154
[24] Wang X Y and Gao S 2020 *Inf. Sci.* **507** 16
[25] Wang X Y, Feng L and Zhao H Y 2019 *Inf. Sci.* **486** 340
[26] Wang X G, Li M, Yu N N, Xi S X, Wang X L and Lang L Y 2019 *Acta Phys. Sin.* **68** 240503 (in Chinese)
[27] Chen T H and Wu C S 2010 *Inf. Sci.* **180** 1690
[28] Xi S X, Yu N N, Wang X L, Zhu Q F, Dong Z, Wang W, Liu X H and Wang H P 2019 *Acta Phys. Sin.* **68** 110502 (in Chinese)
[29] Guo Y, Shao L P and Yang L 2015 *Appl. Res. Comput.* **32** 1131
[30] Ye R S 2011 *Opt. Commun.* **284** 5290
[31] Zhang X C, Wang L F, Zhou Z and Niu Y 2019 *IEEE Access* **7** 74734
[32] Wang X Y, Wang Y, Wang S W, Zhang Y Q and Wu X J 2018 *Chin. Phys. B* **27** 110502
[33] Liu L F and Miao S X 2016 *Multimed. Tools Appl.* **76** 16511
[34] Wang X Y and Gao S 2020 *Inf. Sci.* **539** 195
[35] Li Q, Wang X Y, Wang X Y, Ma B, Wang C P and Shi Y Q 2021 *Inf. Sci.* **553** 19
[36] Shi H and Wang L D 2019 *Acta Phys. Sin.* **68** 200501 (in Chinese)