

Article

A Novel Virtual Optical Image Encryption Scheme Created by Combining Chaotic S-Box with Double Random Phase Encoding

Peiran Tian * and Runzhou Su *

Department of Physics, College of Science, Northeast Forestry University, Harbin 150040, China

* Correspondence: 19tpr@nefu.edu.cn (P.T.); surunzhou@nefu.edu.cn (R.S.); Tel.: +86-451-8219-0652 (R.S.)

Abstract: The double random phase encoding (DRPE) system plays a significant role in encrypted systems. However, it is a linear system that leads to security holes in encrypted systems. To tackle this issue, this paper proposes a novel optical image encryption scheme that combines a chaotic S-box, DRPE, and an improved Arnold transformation (IAT). In particular, the encryption scheme designs a chaotic S-box to substitute an image. The chaotic S-box has the characteristics of high nonlinearity and low differential uniformity and is then introduced to enhance the security of the DRPE system. Chaotic S-boxes are resistant to algebraic attacks. An IAT is used to scramble an image encoded by the DRPE system. Meanwhile, three chaotic sequences are obtained by a nonlinear chaotic map in the proposed encryption scheme. One of them is used for XOR operation, and the other two chaotic sequences are explored to generate two random masks in the DRPE system. Simulation results and performance analysis show that the proposed encryption scheme is efficient and secure.

Keywords: chaotic map; substitution box; virtual optical image encryption; DRPE



Citation: Tian, P.; Su, R. A Novel Virtual Optical Image Encryption Scheme Created by Combining Chaotic S-Box with Double Random Phase Encoding. *Sensors* **2022**, *22*, 5325. <https://doi.org/10.3390/s22145325>

Academic Editor:
Malgorzata Kujawinska

Received: 12 June 2022

Accepted: 14 July 2022

Published: 16 July 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the rapid development of computers and the Internet, information security has received extensive attention from academia and industry, in which the security protection of image data is a significant and current research topic. To guarantee the security of images, researchers have developed many techniques including image encryption [1–3], watermarking [4,5], and data hiding [6,7], wherein image encryption is the most direct and effective method. Owing to the characteristics of high speed, and multi-dimensional and parallel processing of optical systems, the researcher took a keen interest in the study of optical image encryption [8,9]. For example, the double random phase encoding (DRPE) architecture based on a 4f optical system was first proposed by Refregier and Javidi [10].

DRPE can encrypt images into stationary white noise. To achieve better encryption performance, many image encryption schemes combining DRPE with other encryption methods such as fractional Fourier transform [11,12], Fresnel transform [13,14], and gyrator transform [15,16] were proposed.

Although DRPE is an effective scheme, it is a linear encryption process; as a result, DRPE-based image encryption algorithms are vulnerable to some specific attacks. To tackle this issue, many scholars have recently studied nonlinear optical image encryption. For instance, Qin et al. proposed a secure nonlinear cryptosystem based on phase truncation in the Fourier transform domain, which overcame the linear weakness of DRPE systems [17], but it was cracked by the authors of [18]. Chen et al. proposed a method to enhance the security of DRPE using phase preservation and compression and applied a nonlinear correlation algorithm to authenticate the decrypted image to improve the security of the DRPE system [19]. Wang et al. proposed an encryption-efficient asymmetric optical image encryption algorithm based on improved amplitude and phase recovery [20]. By introducing nonlinear terms, Dou et al. developed a novel DRPE system [21]; it was, however, cracked by the authors of [22]. In addition, Faragallah et al. introduced an efficient compression

encryption scheme based on research results of the SPIHT/JPEG compression of DRPE-encrypted images based on optical discrete cosine transform (DCT), where the compression was involved to reduce the bandwidth requirement in the communications [23].

Since chaotic systems have inherent properties of ergodicity, pseudo-randomness, and sensitivity to initial conditions and control parameters, many chaos-based cryptosystems were proposed in the past decade [24–28]. For example, Li et al. proposed to utilize the Arnold transform to scramble the pixels in the local area of the complex function composed of two original images, and then conducted the gyrator transform operation to encrypt the scrambled image [24]. Sui et al. developed a double-image encryption algorithm with discrete fractional random transformation and logistic mapping. In the proposed algorithm, the logistic mapping was applied to the diffusion process such that the correlation between adjacent bit planes could be reduced [25]. Lang et al. designed an asymmetric optical color image encryption algorithm using compressed sensing and quantum logistic mapping. In this algorithm, compressed sensing was explored to reduce data transmission, and quantum chaotic mapping was utilized to generate random phase masks [26]. Huang et al. designed a nonlinear multi-image encryption algorithm with a chaotic system and two-dimensional (2-D) linear regular transformation. This algorithm could encrypt images in the space domain and frequency domain and compress multiple images into a small amount of data [27]. Additionally, Abd El Atty et al. developed a novel optical encryption method using the quantum walk and a DRPE system, where the quantum walk was applied for generating the two random masks used in the DRPE system and the permutation and diffusion of an original image as well [28]. From the above research results, it can be seen that the application of chaotic systems in cryptography is in the ascendant.

In encryption systems, an S-box is a crucial module that plays a significant role in confusion and diffusion in block cipher systems such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES). An $n \times n$ S-box is a nonlinear map $S: \{0, 1\}^n \rightarrow \{0, 1\}^n$, with $\{0, 1\}^n$ representing the vector spaces of n elements from $GF(2)$ [29,30]. Traditional cryptography utilizes an algebraic method to construct an S-box to achieve a high degree of nonlinearity. However, the constructed S-box has weak differential performance and is vulnerable to algebraic attacks [31,32]. To tackle this issue, the researcher constructed many chaotic S-boxes [33–55]. In 2001, Jakimoski et al. first constructed an S-box based on discrete chaotic systems [33]. Since then, various chaotic S-box construction methods were proposed based on discrete-time chaotic systems [34–36,43,45,50,53–55], continuous-time chaotic systems [37–42,44], hyper chaotic systems [46,47], and joint optimization and chaotic systems [48,49,51,52]. The computational complexity of optimally generating S-boxes is highest, followed by high-dimensional continuous-time chaotic systems, and low-dimensional discrete chaotic systems is the lowest. Therefore, the generation of S-boxes for low-dimensional discrete chaotic systems has received extensive attention.

Recently, some image encryption algorithms using chaotic S-Boxes have been proposed [56–63]. For example, Zhang et al. developed an efficient chaotic image encryption scheme using alternate circular S-boxes with the chaotic S-boxes being produced by the Chen chaotic system [56]. Belazi et al. introduced a novel image encryption scheme based on a substitution-permutation structure and a chaotic S-box constructed by the logistic-sine map [57]. Lu et al. proposed an image encryption algorithm using a chaotic S-box generated by the discrete compound chaotic map [58]. The performance analysis showed that the proposed encryption algorithm exhibited outstanding diffusion and confusion properties. Idrees et al. proposed a cryptosystem using a substitution-permutation network, where the S-box was constructed by the chaotic sine map [59]. Wang et al. developed a novel image encryption scheme employing a spatiotemporal chaos-based dynamic S-box and random blocks [60]. This S-box was constructed using one-dimensional (1-D) and 2-D chaos mapping and DNA sequencing [61]. Simulation results showed that the proposed algorithm had the ability to resist many kinds of attacks. Ali et al. utilized the generated S-box by PWLCM, the tent logistic system, to design a novel image encryption scheme [62]. In addition, Deb et al. proposed a new algorithm with key-dependent bijective S-Boxes un-

der a 2-D Henon-map [63]. The performance analysis showed that this algorithm achieved good confusion and diffusion capabilities. Therefore, encrypting images based on chaotic S-boxes can produce good encryption effects.

S-boxes were introduced in some algorithms to enhance DRPE [64–66]. Hussain et al. proposed to utilize an information-hiding technique to design an optical image encryption algorithm [64]. In the designed algorithm, the DRPE and S-box transformation were applied. They also designed an optical image encryption system based on a fractional Hartley transform and an S-box using linear fractional transform and chaotic maps [65]. Girija et al. proposed to encrypt images with DRPE and a random S-Box [66]. However, the research on the combination of DRPE and the Chaotic S-box to achieve a high degree of nonlinearity has been under-studied.

The main contributions of this work are summarized as follows:

- (1) Exploring a chaotic map and conducting the transformation of stretch and fold to construct an efficient and secure S-box. The cryptographic performance of the constructed S-box is testified.
- (2) A secure image encryption scheme is developed by integrating the chaotic S-box, DRPE, and IAT. In this scheme, the plaintext information is involved in the control parameters of IAT. All the gray pixel values are substituted by the S-box. We XOR the substituted image with a nonlinear chaotic sequence. Next, the two random-phase masks are generated by a nonlinear chaotic map. The XOR result is encoded by DRPE, and the obtained result is further confused by IAT.
- (3) Simulation and security analysis are conducted to verify the effectiveness of the proposed encryption scheme. Simulation results and performance analysis show that the proposed scheme is efficient and secure.

The remainder of the present paper is organized as follows. Some relevant fundamental knowledge is briefly introduced in Section 2. Section 3 presents the S-box obtained in our paper. The proposed cryptosystem approach for grayscale images is described in Section 4. Section 5 shows results and security analyses. Finally, we summarize this work in Section 6.

2. Fundamental Knowledge

2.1. Overview of Optical DRPE Cryptosystem

The following encryption processes are performed on the original image: (1) modulate the original image with the first random phase mask placed in front of the input plane; (2) modulate the obtained result with the second random phase mask placed in front of the output plane to obtain an encrypted image [9]. After that, the encrypted image becomes stationary white noise of complex amplitude.

Figure 1 depicts the principle of the optical DRPE cryptosystem. The process of encryption and decryption is given by Equations (1) and (2):

$$G(x, y) = FT^{-1}\{FT\{F(x, y) \cdot \exp[i2\pi m(x, y)] \cdot \exp[i2\pi n(u, v)]\}\} \quad (1)$$

$$F(x, y) = FT^{-1}\{FT\{G(x, y) \cdot \exp[-i2\pi n(u, v)] \cdot \exp[-i2\pi m(x, y)]\}\} \quad (2)$$

where $F(x, y)$ and $G(x, y)$ denote plain and cipher images, respectively; $FT\{\cdot\}$ indicates the FT , and $FT^{-1}\{\cdot\}$ represents the IFT. Two random phase masks $m(x, y)$ and $n(u, v)$ with $\exp[i2\pi m(x, y)]$ and $\exp[i2\pi n(u, v)]$ are uniformly distributed between 0 and 1.

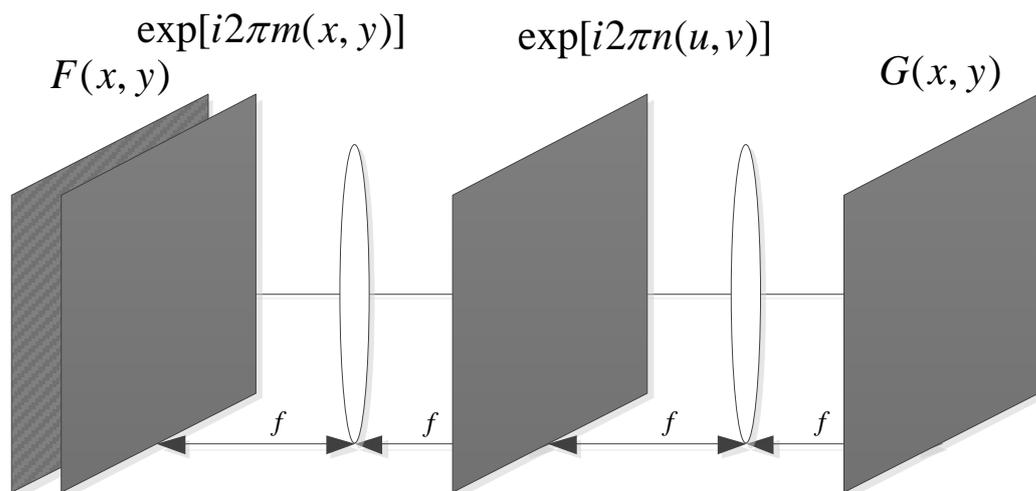


Figure 1. The architecture of the optical DRPE cryptosystem.

2.2. Nonlinear Chaotic Map

The formulas of a nonlinear chaotic map are given by Equation (3) [67]:

$$\begin{aligned}
 x_{n+1} &= [\mu \times k_1 \times (1 - x_n)^2 \times y_n + z_n] \bmod 1 \\
 y_{n+1} &= [\mu \times k_2 \times x_{n+1} + (1 + (y_n)^2) \times z_n] \bmod 1 \\
 z_{n+1} &= [\mu \times k_3 \times \sin(x_{n+1}) \times z_n + y_{n+1}] \bmod 1
 \end{aligned}
 \tag{3}$$

where μ, k_i are system parameters of the nonlinear chaotic map and when $0 < \mu \leq 3.999$, $|k_1| > 29.5$, $|k_2| > 31.3$, $|k_3| > 25.1$. With $k_1 = 32.5, k_2 = 34.3, k_3 = 28.1$, and $\mu \in (0, 3.999]$, this system exhibits chaotic bifurcation diagrams and Lyapunov exponents as shown in Figure 2a–d, respectively. When $k_1 = 32.5, k_2 = 34.3, k_3 = 28.1$, and $\mu = 3.999$, the chaotic attractor of this system is shown in Figure 2e.

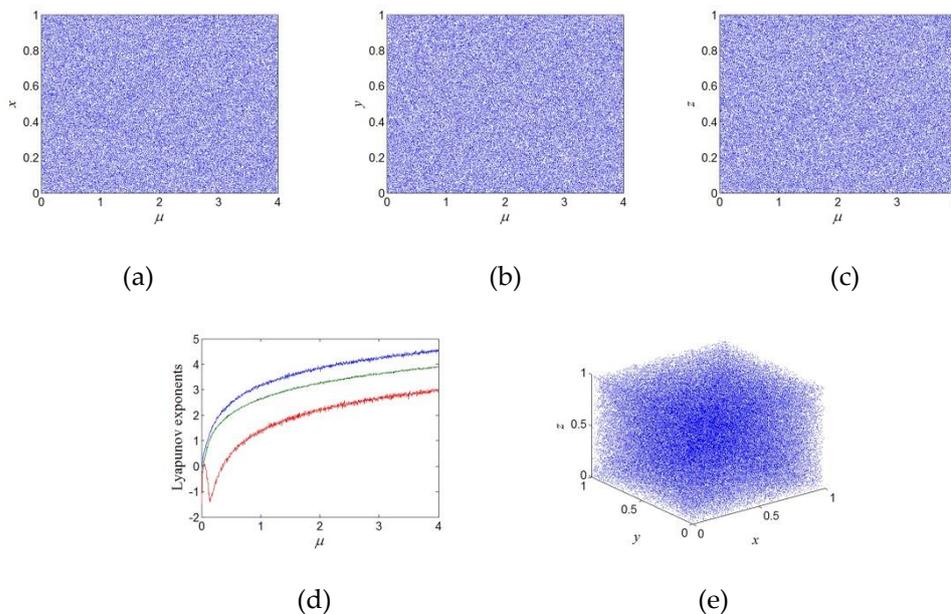


Figure 2. Chaotic bifurcation diagram, Lyapunov exponents, and attractor diagram: (a) the chaotic bifurcation diagram of the chaotic map x ; (b) the chaotic bifurcation diagram of the chaotic map y ; (c) the chaotic bifurcation diagram of the chaotic map z ; (d) Lyapunov exponents; (e) the chaotic attractor in the x - y - z plane.

2.3. Improved Arnold Transformation

In the 1960s, Vladimir Arnold discovered the Arnold map (AM), which has no attractor and is used to scramble images [68].

AT can be described as the following Equation (4):

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N \quad (4)$$

where the four parameters $a, b, c,$ and d are all positive integers in AT, and $\gcd(ad - bc, N) = 1$.

The Equation (4) can be further transformed as follows:

$$\begin{aligned} x_{n+1} &= (ax_n + by_n) \bmod N \\ y_{n+1} &= (cx_n + dy_n) \bmod N \end{aligned} \quad (5)$$

To improve the performance of AT, we should use Equation (6) rather than Equation (5) [69].

$$\begin{aligned} x_{n+1} &= (x_n + hy_n) \bmod N \\ y_{n+1} &= (gx_n + (hg + 1)y_n + e(x_{n+1}^r + k)) \bmod N \end{aligned} \quad (6)$$

where $r \in \{2, 3, 4, 5, 6, 7\}$ and $k \in \{1, 2, \dots, 255\}$.

The nonlinear term makes the improved AT change the deficiency of quasi-affine transform and enhances the ability and security of AT against differential attacks.

2.4. Transform of Stretch and Fold

a. The stretch transform of nonadjacent rows and columns

The procedure of stretch transform of nonadjacent rows and columns [70] is as follows: insert the pixels of a row or column of the image pixel matrix into other adjacent rows or columns of pixels, stretch the obtained pixels into 1-D series, and then fold them to the same size as the original image matrix. This will guarantee efficient scrambling of the original adjacent pixels (not at the original positions). Figures 3 and 4a,b illustrate the detailed process.

1,1	1,2	1,3	1,4	1,5	1,6
2,1	2,2	2,3	2,4	2,5	2,6
3,1	3,2	3,3	3,4	3,5	3,6
4,1	4,2	4,3	4,4	4,5	4,6
5,1	5,2	5,3	5,4	5,5	5,6
6,1	6,2	6,3	6,4	6,5	6,6

Figure 3. A 6×6 image matrix.

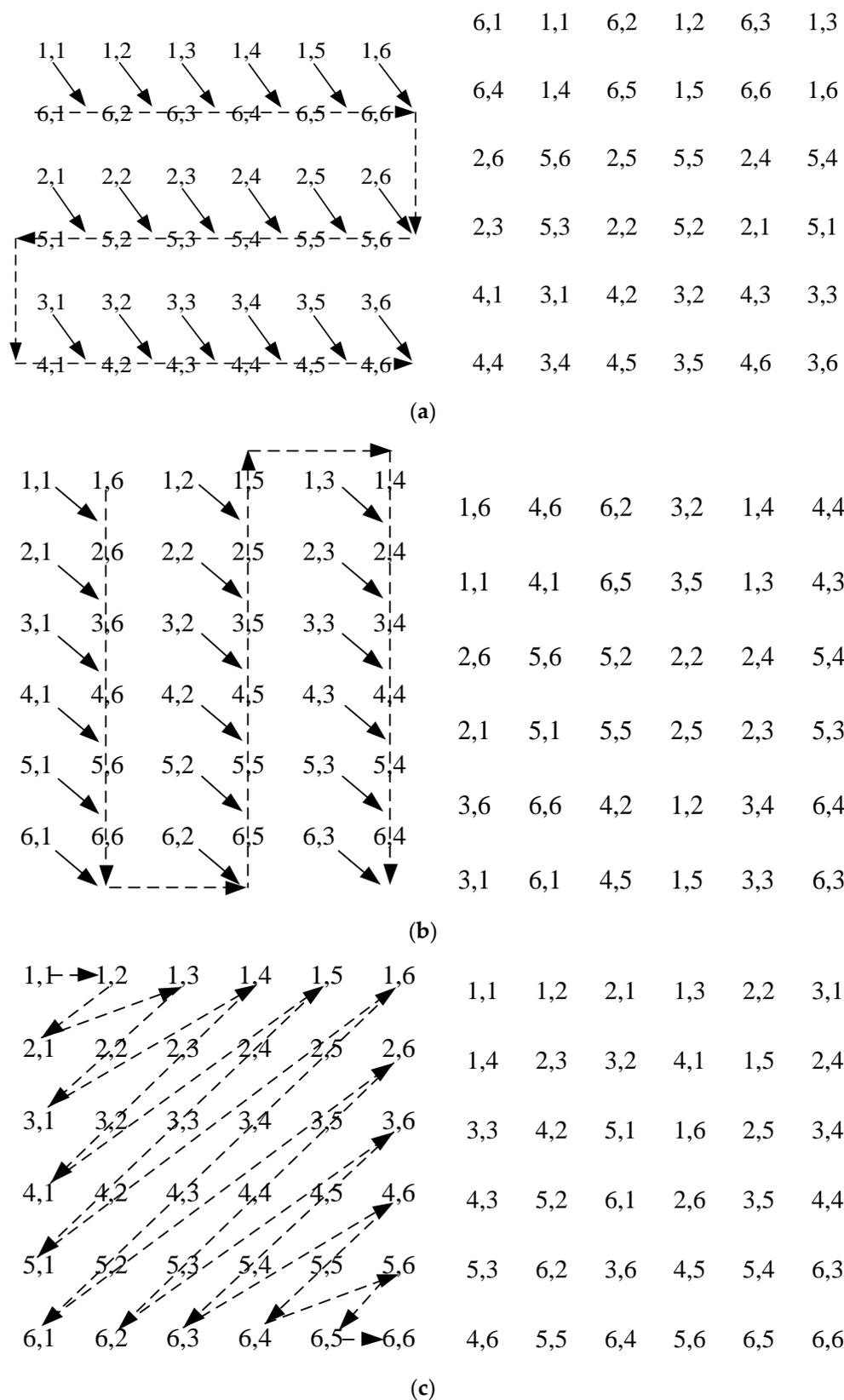


Figure 4. Process of the transform. (a) The stretch transform of nonadjacent rows; (b) The stretch transform of nonadjacent columns; (c) the fold transform of a snake line.

b. The fold transform of a snake line

The process of fold transform of a snake line can be described as the following: arrange the pixels in the image matrix in an order of a snake line, put the obtained pixels into 1-D series, and then fold them to the same size as the original image matrix [70]. Figures 3 and 4c show the detailed process.

3. S-Box Construction and Evaluation Criteria

3.1. The Proposed S-Box Generation Scheme

Step 1: We iterate the chaotic system Equation (3) with initial values x'_0, y'_0, z'_0 . For the N_0 th iteration, x'_1, y'_1, z'_1 can be obtained. Then, S is defined as an array of 256 integers.

Step 2: We take x'_1, y'_1, z'_1 as initial values to avoid the transient effect; then to obtain three chaotic sequences from the $N_0 + 1$ -th value, $(x'_i, i = 1, 2, \dots), (y'_i, i = 1, 2, \dots), (z'_i, i = 1, 2, \dots)$.

Step 3: An integer sequence t_i ranging from $[0,2]$ is calculated by using Equation (7):

$$t_i = \text{floor}(x'_i \times 10^3) \bmod 2 + 1 \tag{7}$$

Step 4: Substitute y'_i and z'_i into Equations (8) and (9) to obtain an integer sequence Y_i and Z_i ranging from $[0,255]$, respectively.

$$Y_i = \text{floor}(y'_i \times 10^3) \bmod 2^8 \tag{8}$$

$$Z_i = \text{floor}(z'_i \times 10^3) \bmod 2^8 \tag{9}$$

Step 5: The array S can be calculated by the following Equation (10). The number stored in S is not repeated. When array S is filled, the S-box is obtained.

$$S(i) = \begin{cases} Y_i, & t_i = 1 \\ Z_i, & t_i = 2 \end{cases} \tag{10}$$

Step 6: The integer sequence S is arranged into a 16×16 table to obtain an initial prototype S-box.

Step 7: Perform the stretch and fold transform on the initial prototype S-box (see Figure 4a–c, and turn upside down, perform the stretch and fold transform for M_0 times on the transformed S-box to obtain the proposed S-box (see Table 1).

Table 1. The obtained S-box.

No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	132	211	219	33	46	9	224	202	155	187	34	154	13	28	102	221
2	117	228	166	250	63	159	177	100	182	58	85	170	60	52	238	64
3	142	6	78	247	248	4	108	18	68	107	194	45	209	50	87	119
4	158	54	37	109	150	114	65	181	234	14	243	123	76	21	72	217
5	3	24	227	113	0	19	208	17	111	70	171	110	156	2	145	152
6	5	192	231	89	193	240	244	20	215	149	173	229	180	40	255	49
7	201	143	179	169	147	32	137	47	15	239	176	253	80	252	204	225
8	44	165	73	105	56	160	133	134	191	55	206	1	183	12	203	36
9	35	7	74	184	212	129	8	23	26	127	122	162	172	242	118	214
10	223	120	16	125	207	199	148	226	144	95	51	71	103	41	77	178
11	88	222	174	164	146	130	188	126	216	81	200	249	29	140	157	10
12	189	91	22	98	198	205	61	161	190	151	94	245	233	163	195	136
13	25	31	97	79	39	82	135	218	141	11	196	168	186	175	101	121
14	69	27	30	115	53	42	210	246	220	232	96	116	90	43	83	237
15	48	139	241	213	92	106	59	124	153	86	197	138	112	93	67	254
16	75	38	84	57	104	251	236	131	66	235	167	230	99	185	128	62

3.2. Performance Analysis of the Designed S-Box

We compare our obtained S-box with many S-boxes generated in [33–55]. Initialization parameters are configured as the following: $x_0 = 0.36$, $y_0 = 0.25$, $z_0 = 0.78$, $k_1 = 32.5$, $k_2 = 34.3$, $k_3 = 28.1$, $\mu = 3.999$, $N_0 = 1000$, and $M_0 = 757$. The obtained S-box is described in Table 1, and Table 2 lists the comparison results.

Table 2. Cryptanalysis comparison results of S-boxes.

S-Boxes	Nonlinearity			SAC			BIC-Nonlinearity	BIC-SAC	DP	LP
	Min	Max	Avg.	Min	Max	Avg.				
Proposed	104	110	107	0.4219	0.5781	0.4954	102.93	0.5034	0.04688	0.148438
Ref. [33]	100	108	103.25	0.3750	0.5938	0.5059	104.29	0.5031	0.04688	0.125000
Ref. [34]	104	108	105	0.4063	0.5781	0.4971	103	0.5044	0.03906	0.132813
Ref. [35]	101	108	103.88	0.3906	0.5781	0.5059	102.68	0.4958	0.03906	0.132813
Ref. [36]	100	106	103	0.4219	0.6094	0.5000	103.14	0.5024	0.05469	0.132813
Ref. [37]	100	106	103.25	0.4219	0.5938	0.5049	103.71	0.5010	0.03906	0.132813
Ref. [38]	96	106	103	0.3906	0.6250	0.5039	100.36	0.5010	0.03906	0.148438
Ref. [39]	102	108	104.75	0.3906	0.5938	0.5056	104.07	0.5022	0.04688	0.125000
Ref. [40]	98	108	104.25	0.2813	0.6094	0.4954	102.86	0.5048	0.04688	0.140625
Ref. [41]	100	106	104	0.3750	0.6250	0.4946	103.21	0.5019	0.03906	0.132813
Ref. [42]	100	106	103	0.3906	0.5938	0.5020	102.93	0.4999	0.03906	0.140625
Ref. [43]	84	106	100	0.1250	0.6250	0.4812	101.93	0.4967	0.06250	0.179688
Ref. [44]	104	110	106.25	0.4219	0.5938	0.5039	103.36	0.5059	0.03906	0.140625
Ref. [45]	100	110	105.50	0.4063	0.6094	0.5010	103.79	0.5036	0.04688	0.132813
Ref. [46]	101	107	104.5	0.4219	0.5781	0.4963	103.29	0.4938	0.03906	0.140625
Ref. [47]	104	108	106.75	0.4063	0.6250	0.4976	103.57	0.5022	0.03906	0.132813
Ref. [48]	104	108	106.25	0.3594	0.6094	0.5002	103.64	0.4993	0.03906	0.132813
Ref. [49]	112	112	112	0.4531	0.5625	0.5051	112	0.5044	0.01560	0.062500
Ref. [50]	102	108	105.25	0.4688	0.5938	0.5352	103.21	0.5085	0.05469	0.140625
Ref. [51]	106	110	108.5	0.4063	0.5781	0.4995	103.86	0.5016	0.03906	0.132813
Ref. [52]	110	112	112.5	0.4063	0.5938	0.4985	103.79	0.5014	0.03906	0.132813
Ref. [53]	104	110	107	0.4219	0.5938	0.4993	103.29	0.5051	0.03906	0.132813
Ref. [54]	102	108	105.5	0.4219	0.5781	0.5061	103	0.5009	0.03906	0.140625
Ref. [55]	102	110	106.5	0.4063	0.5938	0.5010	103.43	0.4980	0.0391	0.132813

We select five criteria including nonlinearity [71], strict avalanche criterion (SAC) [72], bits independence criterion (BIC) [73], differential approximation probability (DP) [74], and linear approximation probability (LP) [75] to verify the cryptographic characteristics of our S-box.

The minimum, maximum, and average nonlinearities of the obtained S-box are 104, 110, and 107, respectively, as shown in Table 2. Thus, the obtained S-box is resistant to differential linear attacks.

The dependency matrix of the obtained S-box is shown in Table 2. Specifically, the achieved maximum, minimum, and average values of the obtained S-box are 0.5781, 0.4219, and 0.4954, respectively. The following observations can be obtained from Table 2: (1) the S-boxes designed in refs. [34,36,38,40,44–48,51–53,55] outperform the obtained S-box; (2) however, the average value of the obtained S-box is closer to the ideal value, 0.5, than those designed in refs. [33,35,37,39–41,43,49,50,54]. Therefore, the designed S-box meets the SAC criterion.

The BIC test results of the obtained S-box are depicted in Table 2. In the table, the average BIC-nonlinearity and the average BIC-SAC value of the obtained S-box are 102.93 and 0.5034, respectively. The following conclusion can be obtained from this table: (1) the average BIC-nonlinearity value of the obtained S-box is lower than those designed in refs. [33,34,36,37,39,41,44–55]; (2) the average BIC-nonlinearity value of the obtained S-box is greater than those constructed in refs. [35,38,40,43]; (3) the average BIC-SAC value of

the obtained S-box is better than those proposed in refs. [34,35,40,44–46,49,50,53], which is closer to the ideal value of 0.5. Therefore, the obtained S-box can meet the BIC characteristic.

The DP test results of all comparison S-boxes are depicted in Table 2. From this table, we can draw the following observations: (1) those constructed S-boxes in refs. [34,35,37,38, 41,42,44,46–49,51–55] can obtain larger DP values than the obtained S-box; (2) yet, the DP value of those of the other comparison S-boxes is not better than the obtained S-box. Thus, the obtained S-box can resist a differential cryptanalysis attack effectively.

Additionally, the maximum LP value of the obtained S-box is 0.148438 in Table 2. From these results, we can make the following observations: (1) the LP value of the generated S-boxes in refs. [33–37,39–42,44–55] are better than the obtained S-box; (2) the LP value of the obtained S-box is not worse than those of the other comparison S-boxes. Therefore, the obtained S-box can also resist the linear cryptanalysis attack effectively.

4. Proposed Encryption and Decryption Framework

Encryption Scheme

The encryption scheme is presented in Figure 5. We suppose the grey plaintext image P is of size $M \times N$, and the pixel value ranges from 0 to 255. The detailed description is presented as below.

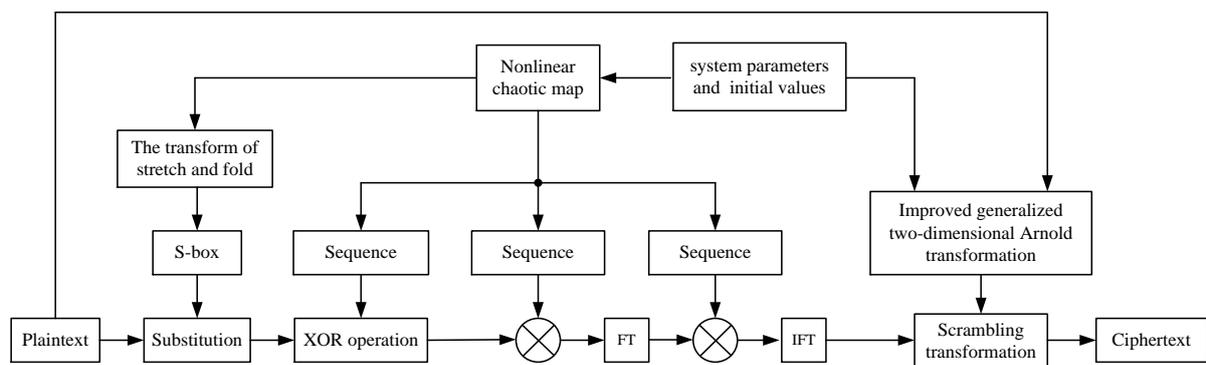


Figure 5. The architecture of the developed encryption scheme.

Step 1: Substituting the initial values x_0, y_0, z_0 into Equation (3), we can obtain x_1, y_1, z_1 after N_0 iterations.

Step 2: Consider x_1, y_1, z_1 as initial values; then to obtain three chaotic sequences from the $N_0 + 1$ -th value, $(x_i, i = 1, 2, \dots, M \times N)$, $(y_i, i = 1, 2, \dots, M \times N)$, $(z_i, i = 1, 2, \dots, M \times N)$.

Step 3: Substitute x_i, y_i and z_i into Equations (11)–(13) to obtain an integer sequence xx_i, yy_i and zz_i ranging from $[0,255]$, respectively.

$$xx_i = \text{floor}(x_i \times 10^3) \bmod 2^8 \quad i = 1, 2, \dots, M \times N \quad (11)$$

$$yy_i = \text{floor}(y_i \times 10^3) \bmod 2^8 \quad i = 1, 2, \dots, M \times N \quad (12)$$

$$zz_i = \text{floor}(z_i \times 10^3) \bmod 2^8 \quad i = 1, 2, \dots, M \times N \quad (13)$$

Step 4: For the plain image P , use a binary value $w = b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$ to represent a pixel of it. Denote $i = b_7 b_6 b_5 b_4$ by a binary representation of a row index value, and convert it to a decimal value s . Denote $j = b_3 b_2 b_1 b_0$ by a binary representation of a column index value, and convert into a decimal value t . Replace the elements of the $s + 1$ th row of the S-box and that of the $t + 1$ th column to obtain the plain image P' .

Step 5: Arrange the pixels of P' into a 1-D sequence $B = \{b_1, b_2, \dots, b_{M \times N}\}$ in left-to-right and top-to-bottom order.

Step 6: Calculate c_i by Equation (14):

$$c_i = b_i \oplus zz_i \quad (14)$$

where \oplus is the XOR operation, and c_i is the output pixel data.

Step 7: $m(x, y)$ is formed by the matrix $\{xx_i'(i, j) | i = 1, 2, \dots, M; j = 1, 2, \dots, N\}$ after rearranging the sequence $xx_i \{i = 1, 2, \dots, M \times N\}$. Similarly, $n(x, y)$ is produced by the matrix $\{yy_i'(i, j) | i = 1, 2, \dots, M; j = 1, 2, \dots, N\}$ after rearranging the sequence $yy_i \{i = 1, 2, \dots, M \times N\}$.

Step 8: Perform FT and IFT according to Equation (1), and then to obtain an image D .

Step 9: The average value of the plaintext P is calculated by Equation (15):

$$mean = \frac{\sum_{x \in [1, M], y \in [1, N]} P(x, y)}{M \times N} \quad (15)$$

Step 10: The parameter k is calculated by Equation (16):

$$k = \text{mod} \left(\left\lfloor mean \times 10^5 + x_0 \times 10^8 + y_0 \times 10^8 + z_0 \times 10^8 \right\rfloor, 256 \right) \quad (16)$$

Step 11: Substitute k into Equation (6); that is IAT. Then scramble the complex-valued image D ; finally, encrypted image E can be obtained. It is noteworthy that the encrypted image E is a complex-valued distribution.

In our paper, the proposed scheme is symmetric. The decryption process will not be repeated here.

5. Simulation and Security Analysis

5.1. Simulation Results

The test images include "Lena", "Boat", "Cameraman", "Peppers", "House", "Lake", "Moon surface", and "Plane", and the size of eight gray images is 256×256 (from USC-SIPI Image Database [76]). The keys are as follows: $x_0 = 0.16$, $y_0 = 0.36$, $z_0 = 0.56$, $k_1 = 32.5$, $k_2 = 34.3$, $k_3 = 28.1$, $\mu = 3.999$, $N_0 = 1000$, $h = 2$, $g = 1$, $e = 1$, $r = 3$. All experiments are conducted in MATLAB R2012b. The operating system is Microsoft Windows 7. The hardware environment is a 2.9 GHz CPU and 16 GB memory. The simulation results of the proposed scheme on the above four gray images are shown in Figure 6.

5.2. Security Analysis

5.2.1. Key Space Analysis

In the proposed scheme, the initial values x_0 , y_0 , z_0 and the parameters k_1 , k_2 , k_3 , μ of a chaotic system are used as the secret keys. If the precision is set to 10^{-14} , the key space of this scheme is $10^{14} \times 7 = 10^{112} \approx 2^{372} \gg 2^{100}$ [77], which can resist brute-force attacks effectively.

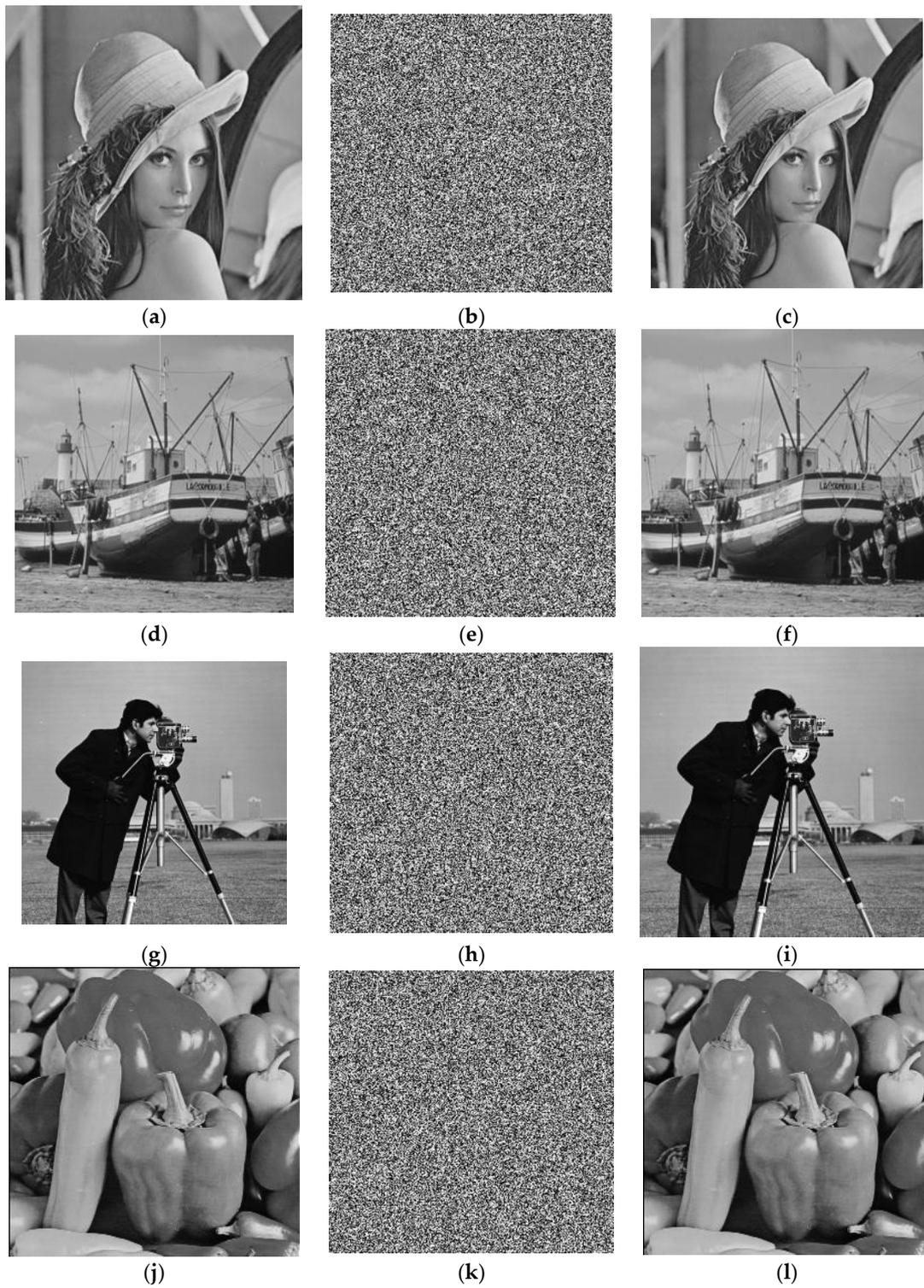


Figure 6. Cont.

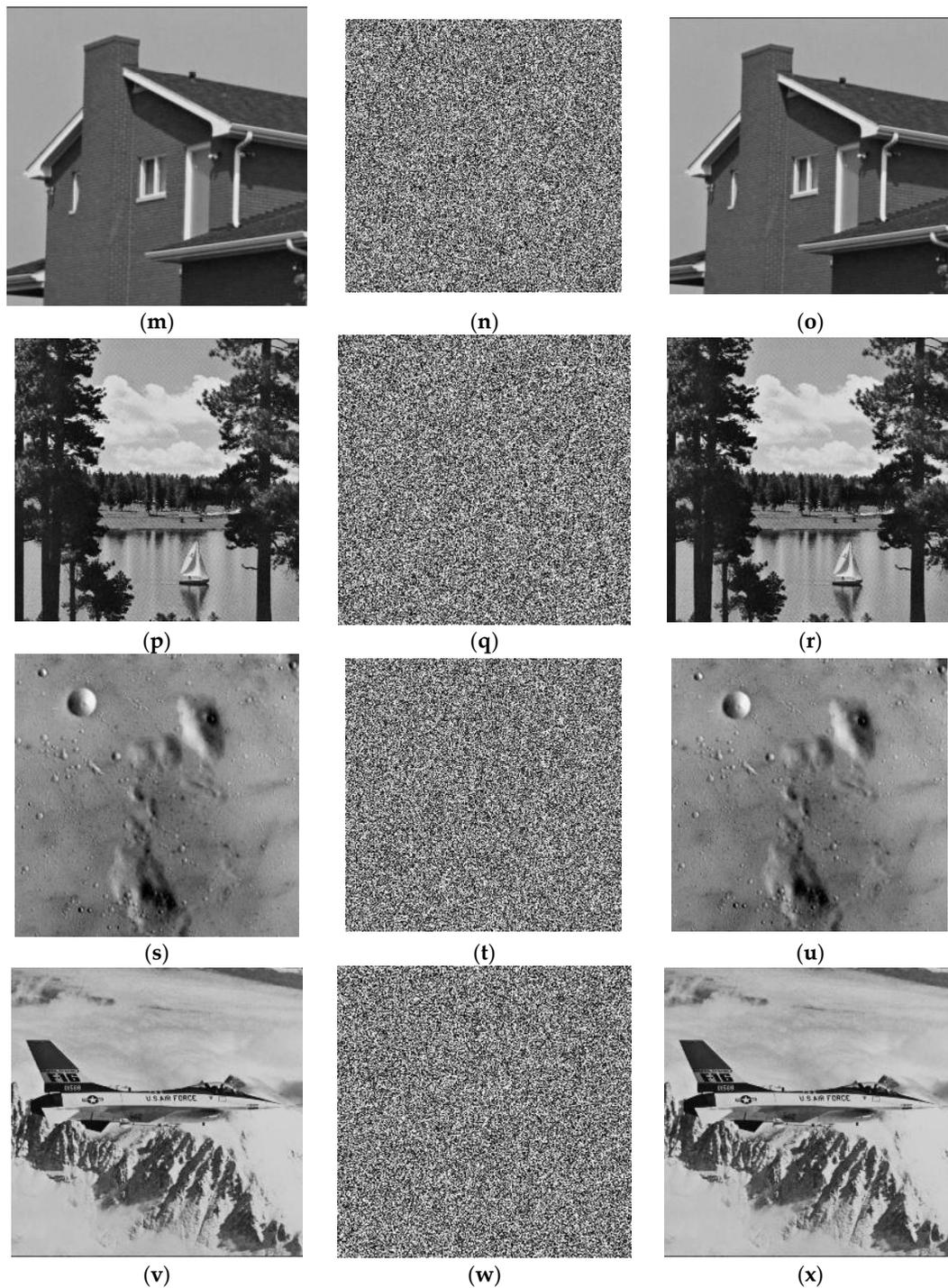


Figure 6. Simulation results of four gray images. (a) plaintext image of Lena; (b) the amplitude of encrypted image of Lena; (c) decrypted image of Lena; (d) plaintext image of Boat; (e) the amplitude of encrypted image of Boat; (f) decrypted image of Boat; (g) plaintext image of Cameraman; (h) the amplitude of encrypted image of Cameraman; (i) decrypted image of Cameraman; (j) plaintext image of Pepper; (k) the amplitude of encrypted image of Pepper; (l) decrypted image of Pepper; (m) plaintext image of House; (n) the amplitude of encrypted image of House; (o) decrypted image of House; (p) plaintext image of Lake; (q) the amplitude of encrypted image of Lake; (r) decrypted image of Lake; (s) plaintext image of Moon surface; (t) the amplitude of encrypted image of Moon surface; (u) decrypted image of Moon surface; (v) plaintext image of Plane; (w) the amplitude of encrypted image of Plane; (x) decrypted image of Plane.

5.2.2. Key Sensitivity Analysis

The key is sensitive if a slight change in the key with other keys remaining unchanged will result in a completely different decryption result. Figure 7 shows sensitivity analysis results of security keys. Figure 7a–c show the decrypted images corresponding to the encrypted image Figure 6b with the keys $x_0 = 0.16 + 10^{-14}$, $k_1 = 32.5 + 10^{-14}$, $\mu = 3.999 + 10^{-14}$, respectively. Therefore, the proposed algorithm scheme exhibits high key sensitivity.

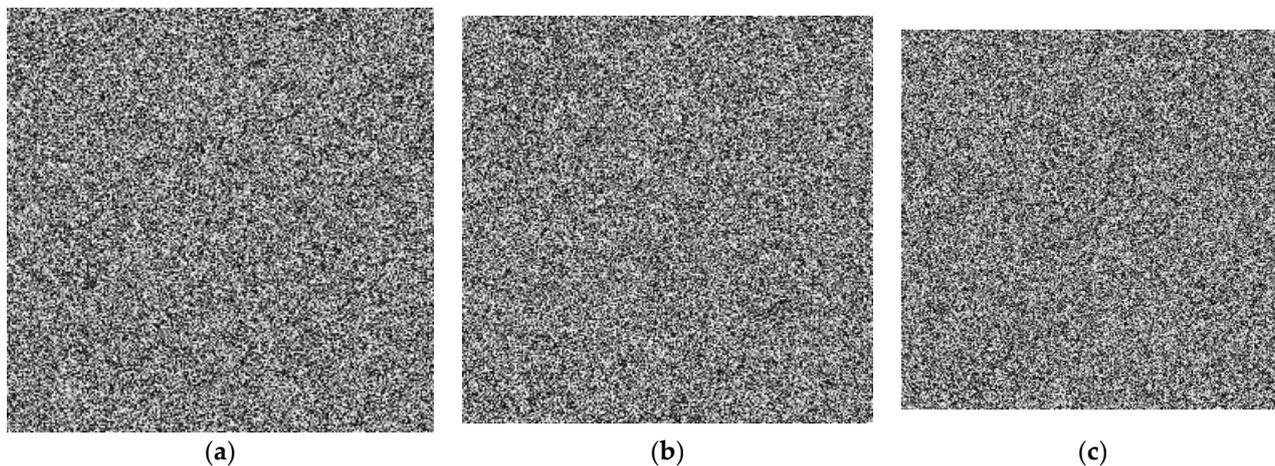


Figure 7. Decrypted image using incorrect keys (a) $x_0 = 0.16 + 10^{-14}$; (b) $k_1 = 32.5 + 10^{-14}$; (c) $\mu = 3.999 + 10^{-14}$.

5.2.3. Histogram Analysis

The histogram of an excellent encryption image should be uniformly distributed [56]. The histograms of the plaintext images are shown in Figure 8a,c,e,g,i,k,m and o, respectively. The histograms of the corresponding encrypted images are shown in Figure 8b,d,f,h,j,l,n and p, respectively.

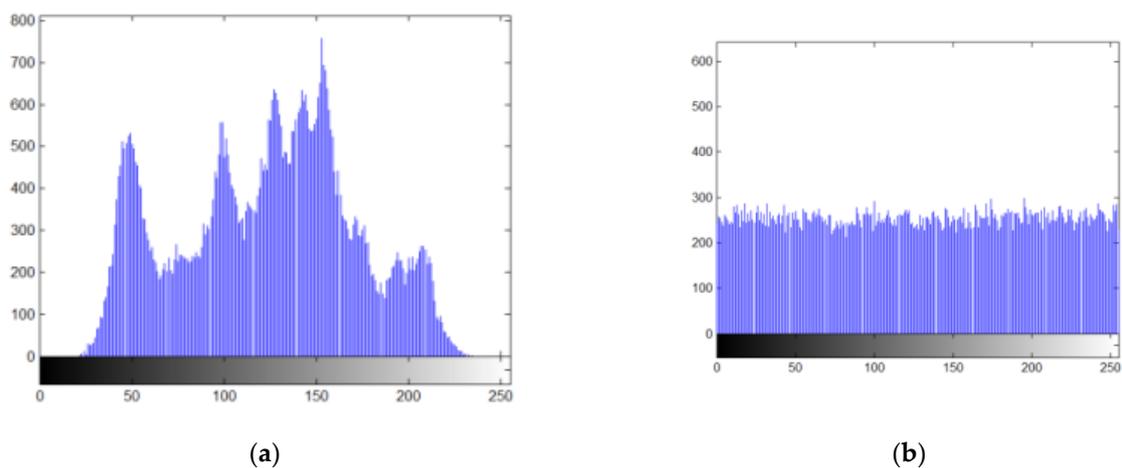
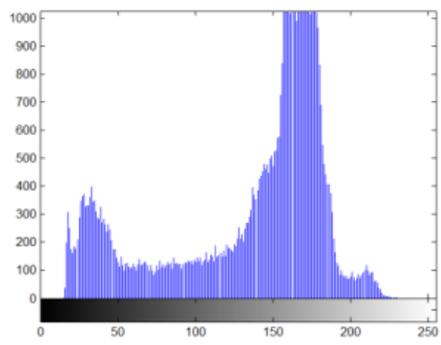
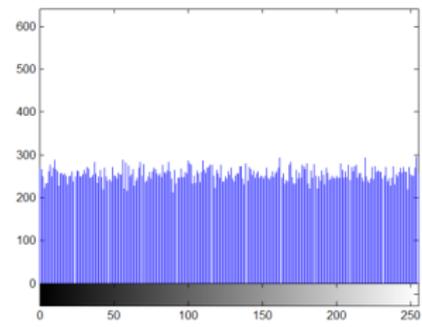


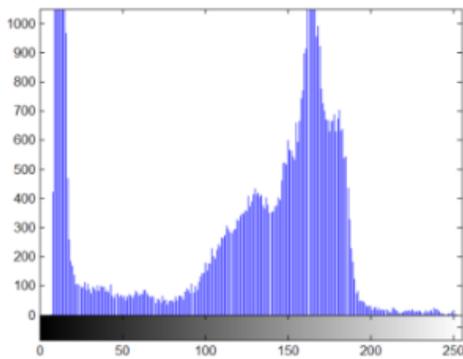
Figure 8. Cont.



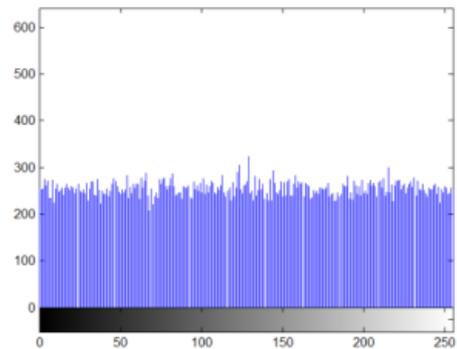
(c)



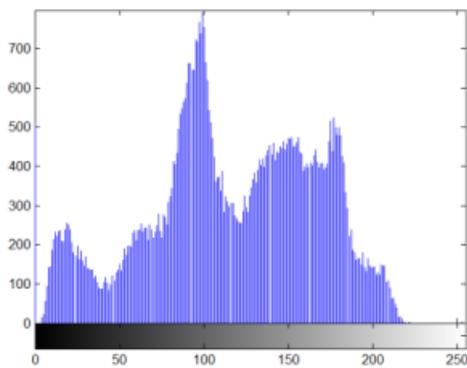
(d)



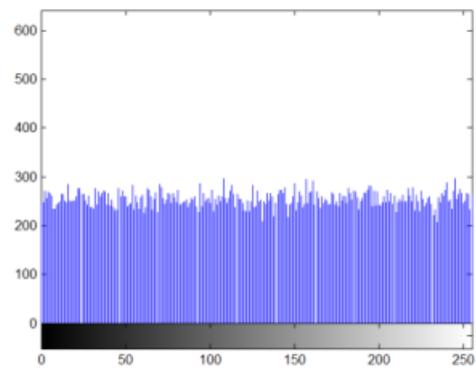
(e)



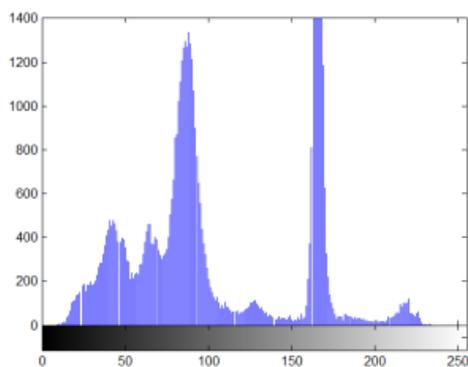
(f)



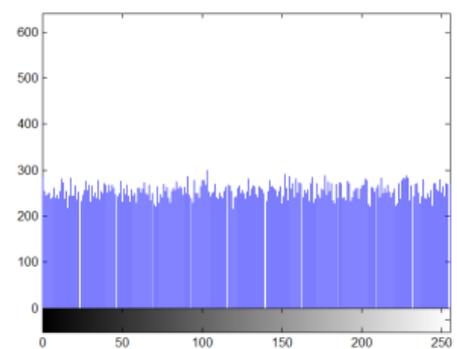
(g)



(h)



(i)



(j)

Figure 8. Cont.

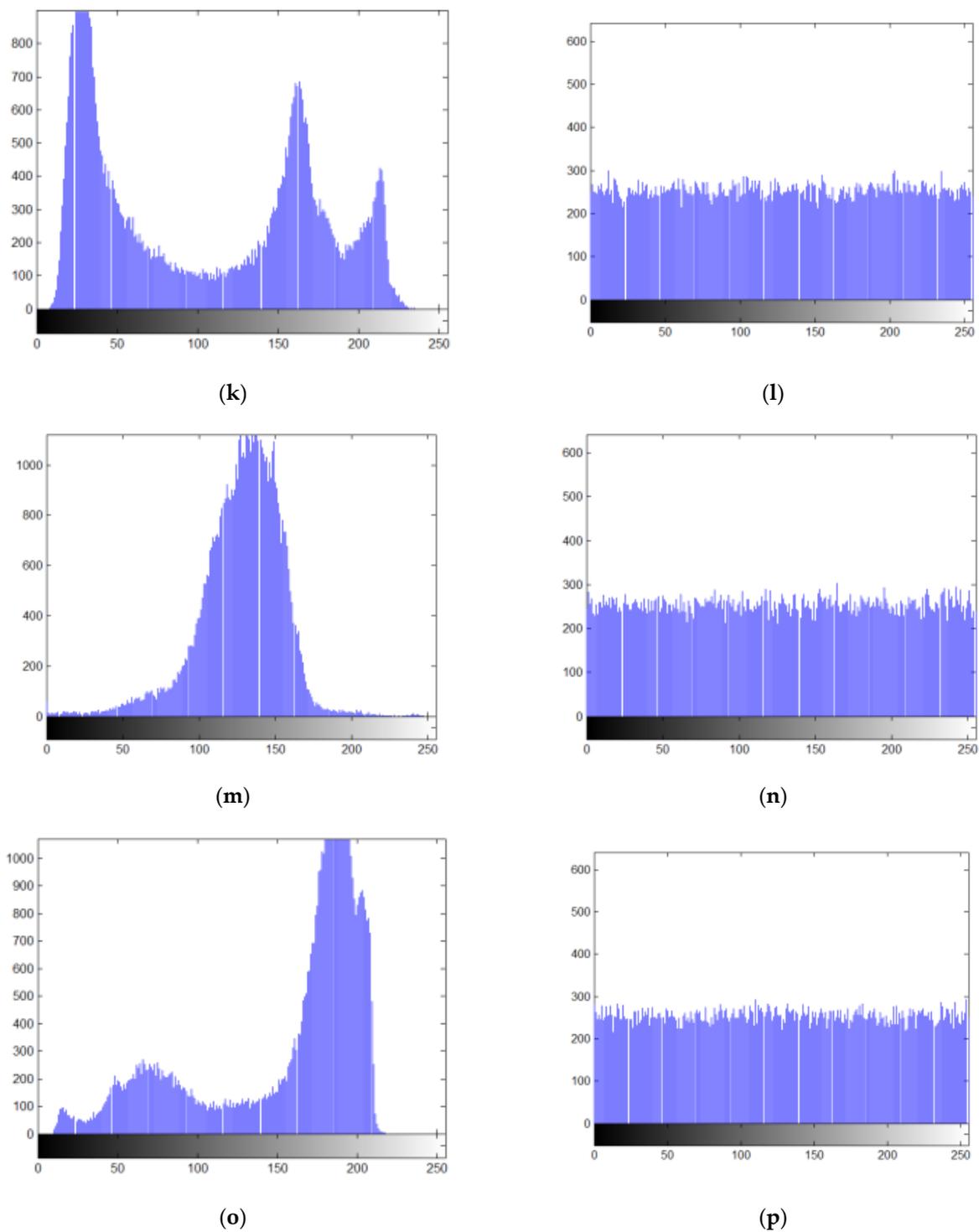


Figure 8. Histograms of the magnitude of the plaintext and encrypted images. (a) Lena; (b) ciphered Lena; (c) Boat; (d) ciphered Boat; (e) Cameraman; (f) ciphered Cameraman; (g) Peppers; (h) ciphered Peppers; (i) House; (j) ciphered House; (k) Lake; (l) ciphered Lake; (m) Moon surface; (n) ciphered Moon surface; (o) Plane; (p) ciphered Plane.

We can observe that the image information distribution of ciphertext encrypted with different plaintext is uniform. Therefore, the scheme proposed can resist statistical attacks.

5.2.4. Chi-Square Test Analysis

To analyze the distribution of the encrypted image histogram intuitively, we perform a Chi-square test. The more uniform the encrypted image pixels are, the lower the Chi-square value is.

The encrypted Chi-square test can be calculated by Equation (17) [56]:

$$\chi^2 = \sum_{i=0}^{255} \frac{(q_i - q)^2}{q}, \quad q = \frac{M \times N}{256} \quad (17)$$

where q_i is the number of pixels i , and $M \times N$ the size of a cipher image.

The Chi-square test results of the encrypted images are given in Table 3. At the 5% significance level, the Chi-square value $\chi_{0.05}^2 = 293.2478$. Table 3 shows that the test results of cipher images are not greater than 293.2478. Thus, the proposed scheme has the ability of resisting statistical attacks.

Table 3. Chi-square test results of encrypted images.

Cipher Image	Chi-Square Value	Result
Lena	246.4219	Pass
Boat	242.7656	Pass
Cameraman	244.4688	Pass
Peppers	248.6797	Pass
House	262.9219	Pass
Lake	240.4375	Pass
Moon surface	287.6328	Pass
Plane	240.6016	Pass

5.2.5. Mean Squared Error and Peak Signal-To-Noise Ratio Analysis

The mean square error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are explored to assess the difference between two images [78].

The MSE and PSNR can be computed by Equations (18) and (19), respectively:

$$\text{MSE} = \frac{\sum_{i,j} (C(i,j) - D(i,j))^2}{M \times N} \quad (18)$$

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{\text{MSE}} \right) \quad (19)$$

where $M \times N$ is the size of an image, and $C(\cdot)$ and $D(\cdot)$ are the corresponding pixel values of two comparison images. The smaller the PSNR between the original image and the encrypted one, the better the encryption effect. If the PSNR value equals infinity, then the two images are the same. The test results in Table 4 show that the proposed scheme can achieve a good encryption effect.

Table 4. Test results of the encryption and decryption performances by different metrics.

Test Image	MSE (Original vs. Encrypted)	PSNR (Original vs. Encrypted)	MSE (Original vs. Decrypted)	PSNR (Original vs. Decrypted)
Lena	7802.8866	9.2083	0	∞
Boat	8263.2444	8.9593	0	∞
Cameraman	9439.7874	8.3812	0	∞
Peppers	8193.0659	8.9963	0	∞
House	8454.3259	8.8600	0	∞
Lake	10,728.4255	7.8254	0	∞
Moon surface	6217.3002	10.1948	0	∞
Plane	8987.5783	8.5944	0	∞

" ∞ " denotes "infinity" in the related study.

5.2.6. Correlation Analysis

To resist statistical analysis attacks, the encryption scheme should reduce the correlation of adjacent pixels of the encrypted image.

We calculate the correlation coefficients of the plain image and the cipher image according to Equations (20)–(23) [57]:

$$\gamma_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (20)$$

$$\text{cov}(x, y) = E((x_i - E(x))(y_i - E(y))) \quad (21)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (22)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (23)$$

In this paper, we randomly chose 3000 pairs of adjacent pixels from a plaintext image "Lena" and its corresponding ciphertext image, and calculated their correlation coefficients in horizontal, vertical, and diagonal directions. The adjacent pixel correlation distributions of Lena's plaintext image in each direction are shown in Figure 9a–c, respectively. The adjacent pixel correlation distributions of the magnitude of Lena's encrypted image in each direction are shown in Figure 9d–f, respectively. The correlation coefficients of Lena in each direction are shown in Table 5. The comparison results also reflect that our scheme indicates a negligible correlation. Thus, our scheme can resist statistical attacks effectively.

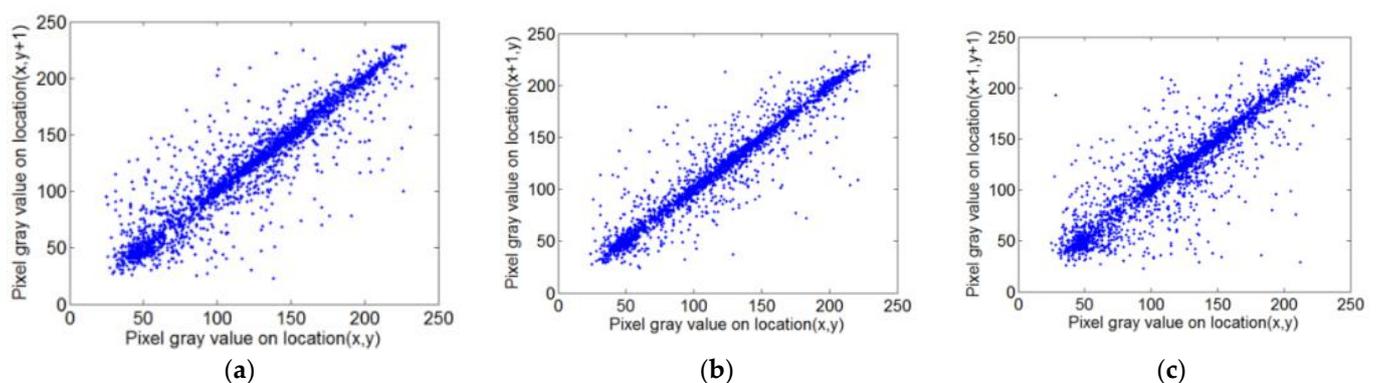


Figure 9. Cont.

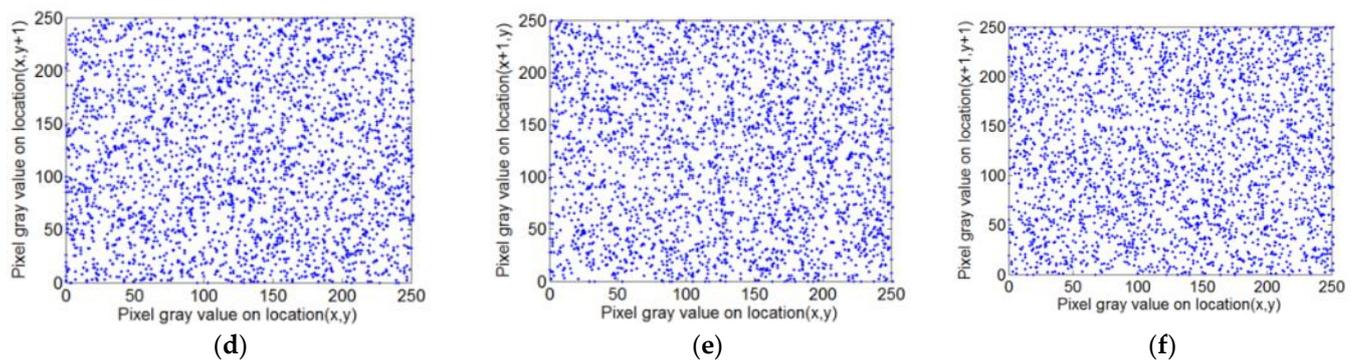


Figure 9. Correlation coefficients of Lena. (a) Horizontal correlation of plain image; (b) vertical correlation of plain image; (c) diagonal correlation of plain image; (d) horizontal correlation of the magnitude of ciphered image; (e) vertical correlation of the magnitude of ciphered image; (f) diagonal correlation of the magnitude of ciphered image.

Table 5. Correlation coefficients of Lena.

Test Image	Horizontal	Vertical	Diagonal
Plaintext image Lena	0.9051	0.9652	0.9293
Encrypted image Lena	−0.0053	−0.0012	0.0050
Ref. [56]	0.0032	−0.0003	0.0012
Ref. [58]	−0.0056	0.0006	0.0018
Ref. [59]	−0.0009	−0.0030	0.0062

5.2.7. Differential Attack Analysis

The number of pixels change rate (NPCR) and unified average changing intensity (UACI) can be utilized to analyze the differential attack performance of an encryption algorithm scheme. NPCR is often utilized to measure the absolute number of value-changed pixels in differential attacks, and UACI is often utilized to measure the averaged difference between two paired ciphertext images. They are computed by Equations (24) and (25), respectively [58]:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j) \times 100\%}{M \times N} \quad (24)$$

$$\text{UACI} = \frac{\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%}{M \times N} \quad (25)$$

where $C_1(i,j)$, $C_2(i,j)$ denote two different encrypted images. $M \times N$ represents the size of an image. If $C_1(i,j) \neq C_2(i,j)$, then $D(i,j) = 1$, otherwise, $D(i,j) = 0$.

The ideal value of NPCR is 99.6093%, and the ideal value of UACI is 33.4635% [61]. The NPCR and UACI values of ciphertexts of different images obtained by our scheme are shown in Table 6. The simulation results show that the NPCR and UACI values of the proposed scheme are close to the ideal values. Therefore, our scheme can resist differential attacks effectively.

Table 6. The NPCR and UACI values of encrypted images.

Test Image	NPCR (%)	UACI (%)
Lena	99.6216	33.6642
Boat	99.6017	33.3610
Cameraman	99.5987	33.3694
Peppers	99.6033	33.5057
House	99.5865	33.3840
Lake	99.5987	33.4928
Moon surface	99.5880	33.3971
Plane	99.5941	33.4519

5.2.8. Robustness Analysis

We utilize data loss attacks and noise attacks to evaluate our scheme robustness.

a. Data loss attack

To evaluate the performance of our scheme in resisting data loss attacks [60], the encryption images with 1/16, 1/8, 1/4, and 1/2 data loss are shown in Figure 10a,c,e and g, and the corresponding decryption images are shown in Figure 10b,d,f and h, respectively. The simulation results show that our proposed scheme can resist loss attacks effectively in both Table 7 and Figure 10.

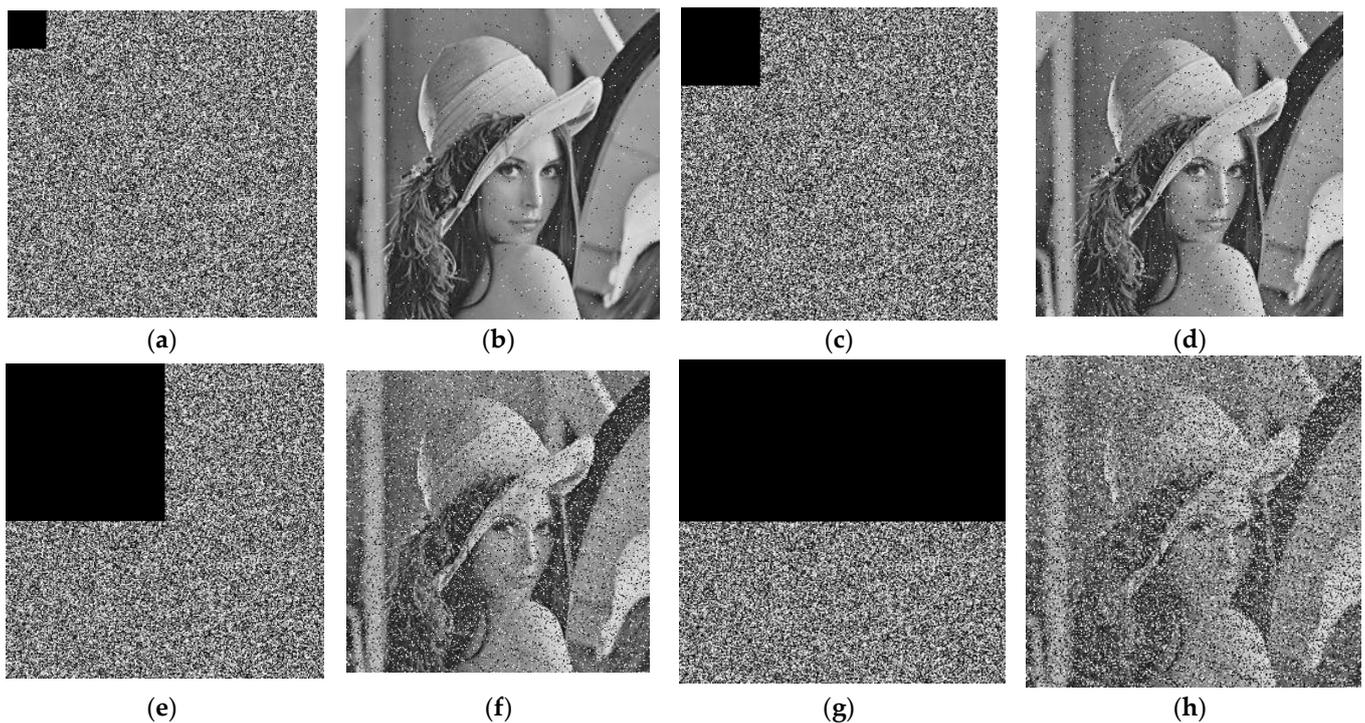


Figure 10. Data loss attack test. (a) 1/16 cropped; (b) corresponding decrypted image of (a); (c) 1/8 cropped; (d) corresponding decrypted image of (c); (e) 1/4 cropped; (f) corresponding decrypted image of (e); (g) 1/2 cropped; and (h) corresponding decrypted image of (g).

Table 7. PSNR and MES testing results subject to data loss attacks.

Data Loss	1/16	1/8	1/4	1/2
PSNR	9.0229	8.7816	7.6823	6.3940
MSE	8143.1129	8608.3023	11,087.8870	14,917.0311

b. Noise attack

To evaluate the scheme performance, we added salt-and-pepper noise with different intensities and Gauss noise with diverse variances to a cipher image and then decrypted the noise-added cipher images [62]. The Gauss noise variances were 0.2, 0.3, 0.4 and 0.5, and the salt-and-pepper noise intensities were 0.001, 0.01, 0.05, and 0.1. In Table 6, the noise intensity and the values of the corresponding PSNR and MES are shown. Obviously, the proposed scheme can resist noise attacks effectively, as shown in both Table 8 and Figure 11.

Table 8. PSNR and MES testing results under noise attacks.

Noise Type	Salt-and-Pepper Noise				Gaussian White Noise			
Noise intensity	0.001	0.01	0.05	0.1	0.2	0.3	0.4	0.5
PSNR	9.2002	9.1446	8.4837	9.2083	9.1789	9.0572	8.8713	8.6525
MSE	7817.4412	7918.1615	9219.6355	7802.8866	7855.7743	8079.0790	8432.4675	8868.1909



Figure 11. Noise attack test. (a–d) with salt-and-pepper noise densities of 0.001, 0.01, 0.05, 0.1, respectively; (e–h) with Gaussian white noise variance values of 0.2, 0.3, 0.4, 0.5 respectively.

5.2.9. Entropy Analysis

The information entropy is used to reflect the randomness of the result of the encrypted image. The information source is denoted by t , and the entropy value is calculated by Equation (26) [63]:

$$H(t) = \sum_{i=0}^{255} p(t_i) \log_2 \frac{1}{p(t_i)} \quad (26)$$

where $p(t_i)$ is the probability of the occurrence of pixel gray value t_i .

The closer it is to 8, the more disordered the information. Table 9 lists the entropy values of ciphertexts of different images encrypted by our scheme. The entropy values of the encrypted Lena image by the proposed scheme in refs. [56,58,59] is depicted in

Table 10. The entropy value of our scheme is closer to 8, as shown in Tables 9 and 10, which demonstrates that the scheme proposed is effective.

Table 9. Entropy values of different images.

Test Image	Plaintext Image	Encrypted Image
Lena	7.4551	7.997286
Boat	7.1011	7.997322
Cameraman	7.0097	7.997325
Peppers	7.5251	7.997258
House	6.5637	7.997106
Lake	7.3767	7.997353
Moon surface	6.7093	7.996827
Plane	6.9860	7.997342

Table 10. Entropy values of the Lena image encrypted by different comparison schemes.

Encryption Schemes	Entropy Values
Proposed	7.9973
Ref. [56]	7.9994
Ref. [58]	7.9971
Ref. [59]	7.9973

5.2.10. Speed Analysis

The simulation was conducted in MATLAB R2012b on a computer with the operating system Windows 7 and 16-GB RAM, Intel(R) Core(TM) i5-9400 CPU @ 2.90 GHz. The average running time of this encryption/decryption scheme for encrypting/decrypting the Lena image was 3.081 s.

6. Conclusions

In our paper, a novel virtual optical image encryption scheme combining a chaotic S-box, DRPE, and IAT was proposed. In the proposed scheme, a new chaotic S-box was constructed. We XORed the substituted image with a nonlinear chaotic sequence. The XOR result was encoded by DRPE, and the encoded result was further scrambled by IAT. Simulation results show that our scheme can resist statistical attacks, brute-force attacks, and differential attacks.

Author Contributions: R.S. conceived and designed the experiments; P.T. performed the experiments; R.S. analyzed the data; P.T. and R.S. wrote the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Fundamental Research Funds for the Central Universities of Northeast Forestry University (2572021DJ02).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are available within the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Amin, M.; Abd El-Latif, A.A. Efficient modified RC5 based on chaos adapted to image encryption. *J. Electron. Imaging* **2010**, *19*, 013012. [\[CrossRef\]](#)
2. Li, L.; Abd-El-Atty, B.; Abd El-Latif, A.A.; Ghoneim, A. Quantum color image encryption based on multiple discrete chaotic systems. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3–6 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 555–559.

3. Abd-El-Latif, A.A.; Abd-El-Atty, B.; Venegas-Andraca, S.E.; Mazurczyk, W. Providing end-to-end security using quantum walks in IoT networks. *IEEE Access* **2020**, *8*, 92687–92696. [[CrossRef](#)]
4. Wang, C.P.; Wang, X.Y.; Xia, Z.Q.; Zhang, C. Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm. *Inf. Sci.* **2019**, *470*, 109–120. [[CrossRef](#)]
5. Zear, A.; Singh, A.K.; Kumar, P. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimed. Tools Appl.* **2018**, *77*, 4863–4882. [[CrossRef](#)]
6. Abd-El-Atty, B.; Iliyasu, A.M.; Alaskar, H.; El-Latif, A.; Ahmed, A. A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. *Sensors* **2020**, *20*, 3108. [[CrossRef](#)]
7. Luo, Y.J.; Qin, J.H.; Xiang, X.Y.; Tan, Y.; Liu, Q.; Xiang, L.Y. Coverless real-time image information hiding based on image block matching and dense convolutional network. *J. Real-Time Image Proc.* **2020**, *17*, 125–135. [[CrossRef](#)]
8. Matoba, O.; Nomura, T.; Perez-Cabre, E.; Millan, M.; Javidi, B. Optical techniques for information security. *P. IEEE* **2009**, *97*, 1128–1148. [[CrossRef](#)]
9. Liu, S.; Guo, C.; Sheridan, J.T. A review of optical image encryption techniques. *Opt. Laser Technol.* **2014**, *57*, 327–342. [[CrossRef](#)]
10. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [[CrossRef](#)]
11. Zhong, Z.; Chang, J.; Shan, M.G.; Hao, B.G. Fractional Fourier-domain random encoding and pixel scrambling technique for double image encryption. *Opt. Commun.* **2012**, *285*, 18–23. [[CrossRef](#)]
12. Liu, Z.J.; Li, S.; Liu, W.; Wang, Y.H.; Liu, S.T. Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. *Opt. Lasers Eng.* **2013**, *51*, 8–14. [[CrossRef](#)]
13. Situ, G.H.; Zhang, J.J. Double random-phase encoding in the Fresnel domain. *Opt. Lett.* **2004**, *29*, 1584–1586. [[CrossRef](#)] [[PubMed](#)]
14. Chen, W.; Chen, X.D.; Sheppard, C.J.R. Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain. *Opt. Express* **2012**, *20*, 3853–3865. [[CrossRef](#)] [[PubMed](#)]
15. Liu, Z.J.; Chen, H.; Liu, T.; Li, P.F.; Dai, J.M.; Sun, X.G.; Liu, S.T. Double-image encryption based on the affine transform and the gyrator transform. *J. Opt.* **2010**, *12*, 035407. [[CrossRef](#)]
16. Wang, Q.; Guo, Q.; Lei, L. Double image encryption based on phase-amplitude mixed encoding and multistage phase encoding in gyrator transform domains. *Opt. Laser Technol.* **2013**, *48*, 267–279. [[CrossRef](#)]
17. Qin, W.; Peng, X. Asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Lett.* **2010**, *35*, 118–120. [[CrossRef](#)]
18. Wang, X.; Zhao, D. A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Commun.* **2012**, *285*, 1078–1081. [[CrossRef](#)]
19. Chen, W.; Chen, X. Double random phase encoding using phase reservation and compression. *J. Opt.* **2014**, *16*, 025402. [[CrossRef](#)]
20. Wang, Y.; Quan, C.; Tay, C.J. Asymmetric optical image encryption based on an improved amplitude–phase retrieval algorithm. *Opt. Laser Eng.* **2016**, *78*, 8–16. [[CrossRef](#)]
21. Dou, S.; Shen, X.; Lin, C. Security-enhanced optical nonlinear cryptosystem based on double random phase encoding. *Opt. Laser Technol.* **2020**, *123*, 105897. [[CrossRef](#)]
22. Singh, P.; Kumar, R.; Yadav, A.K.; Singh, K. Security analysis and modified attack algorithms for a nonlinear optical cryptosystem based on DRPE. *Opt. Laser Eng.* **2021**, *139*, 106501. [[CrossRef](#)]
23. Faragallah, O.S.; Naeem, E.A.; El-sayed, H.S.; El-Samie, A.; Fathi, E. Efficient compression processing of optically DCT-based DRPE encrypted images. *Opt. Quant. Electron.* **2022**, *54*, 273. [[CrossRef](#)]
24. Li, H.J.; Wang, Y.R.; Yan, H.T.; Li, L.B.; Li, Q.Z.; Zhao, X.Y. Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform. *Opt. Laser Eng.* **2013**, *51*, 1327–1331. [[CrossRef](#)]
25. Sui, L.S.; Lu, H.W.; Wang, Z.M.; Sun, Q.D. Double-image encryption using discrete fractional random transform and logistic maps. *Opt. Laser Eng.* **2014**, *56*, 1–12. [[CrossRef](#)]
26. Lang, J.; Fu, X.X.; Guo, P. Optical color image asymmetric compressed encryption in fractional Fourier transform domain. *Opto-Electron. Eng.* **2018**, *45*, 170732. (In Chinese)
27. Huang, Z.J.; Cheng, S.; Gong, L.H.; Zhou, N.R. Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. *Opt. Laser Eng.* **2020**, *124*, 105821. [[CrossRef](#)]
28. Abd-El-Atty, B.; Iliyasu, A.M.; Alanezi, A.; Abd El-latif, A.A. Optical image encryption based on quantum walks. *Opt. Laser Eng.* **2021**, *138*, 106403. [[CrossRef](#)]
29. Lambi'c, D. A novel method of S-box design based on chaotic map and composition method. *Chaos Solitons Fractals* **2014**, *58*, 16–21. [[CrossRef](#)]
30. Ahmad, M.; Al-Solami, E.; Alghamdi, A.M.; Yousaf, M.A. Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures. *IEEE Access* **2020**, *8*, 110397–110411. [[CrossRef](#)]
31. Özkaynak, F.; Yavuz, S. Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dyn.* **2013**, *74*, 551–557. [[CrossRef](#)]
32. Ahmad, M.; Haleem, H.; Khan, P.M. A new chaotic substitution box design for block ciphers. In Proceedings of the 2014 International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 20–21 February 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 255–258.
33. Jakimoski, G.; Kocarev, L. Chaos and cryptography: Block encryption ciphers based on chaotic maps. *IEEE Trans. Circuits Syst.* **2001**, *48*, 163–169. [[CrossRef](#)]

34. Tang, G.P.; Liao, X.F.; Chen, Y. A novel method for designing S-boxes based on chaotic maps. *Chaos Solitons Fractals* **2005**, *23*, 413–419. [[CrossRef](#)]
35. Tang, G.P.; Liao, X.F. A method for designing dynamical S-boxes based on discretized chaotic map. *Chaos Solitons Fractals* **2005**, *23*, 1901–1909. [[CrossRef](#)]
36. Chen, G.; Chen, Y.; Liao, X.F. An extended method for obtaining S-boxes based on three-dimensional chaotic Bakermaps. *Chaos Solitons Fractals* **2007**, *31*, 571–579. [[CrossRef](#)]
37. Özkaynak, F.; Özer, A.B. A method for designing strong S-Boxes based on chaotic Lorenz system. *Phys. Lett. A* **2010**, *374*, 3733–3738. [[CrossRef](#)]
38. Khan, M.; Shah, T.; Mahmood, H.; Gondal, M.A.; Hussain, I. A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dyn.* **2012**, *70*, 2303–2311. [[CrossRef](#)]
39. Hussain, I.; Shah, T.; Gondal, M.A. A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. *Nonlinear Dyn.* **2012**, *70*, 1791–1794. [[CrossRef](#)]
40. Khan, M.; Shah, T.; Gondal, M.A. An efficient technique for the construction of substitution box with chaotic partial differential equation. *Nonlinear Dyn.* **2013**, *73*, 1795–1801. [[CrossRef](#)]
41. Khan, M.; Shah, T. A construction of novel chaos base nonlinear component of block cipher. *Nonlinear Dyn.* **2014**, *76*, 377–382. [[CrossRef](#)]
42. Anees, A.; Ahmed, Z. A technique for designing substitution box based on Van der Pol Oscillator. *Wirel. Pers. Commun.* **2015**, *82*, 1497–1503. [[CrossRef](#)]
43. Khan, M.; Shah, T.; Batool, S.I. Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Comput. Appl.* **2016**, *27*, 677–685. [[CrossRef](#)]
44. Çavuşoğlu, Ü.; Zengin, A.; Pehlivan, I.; Kaçar, S. A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dyn.* **2017**, *87*, 1081–1094. [[CrossRef](#)]
45. Belazi, A.; El-Latif, A.A. A simple yet efficient S-box method based on chaotic sine map. *Optik-Int. J. Light Electron Opt.* **2017**, *130*, 1438–1444. [[CrossRef](#)]
46. Özkaynak, F.; Çelik, V.; Özer, A.B. A new S-box construction method based on the fractional-order chaotic Chen system. *Signal Image Video P.* **2017**, *11*, 659–664. [[CrossRef](#)]
47. Tian, Y.; Lu, Z. Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. *Nonlinear Dyn.* **2018**, *94*, 2115–2126.
48. Ben Farah, M.A.; Farah, A.; Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dyn.* **2020**, *99*, 3041–3064. [[CrossRef](#)]
49. Yousaf, M.A.; Alolaiyan, H.; Ahmad, M.; Dilbar, M.; Razaq, A. Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes. *IEEE Access* **2020**, *8*, 39781–39792. [[CrossRef](#)]
50. Hua, Z.Y.; Li, J.; Chen, Y.Y.; Yi, S. Design and application of an S-box using complete Latin square. *Nonlinear Dyn.* **2021**, *104*, 807–825. [[CrossRef](#)]
51. Alhadawi, H.S.; Majid, M.A.; Lambić, D.; Ahmad, M. A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. *Multimed. Tools Appl.* **2021**, *80*, 7333–7350. [[CrossRef](#)]
52. Liu, X.; Tong, X.; Wang, Z.; Zhang, M. Efficient high nonlinearity S-box generating algorithm based on third-order nonlinear digital filter. *Chaos Solitons Fractals* **2021**, *150*, 111109. [[CrossRef](#)]
53. Zhou, P.; Du, J.; Zhou, K.; Wei, S. 2D mixed pseudo-random coupling PS map lattice and its application in S-box generation. *Nonlinear Dyn.* **2021**, *103*, 1151–1166. [[CrossRef](#)]
54. Tong, X.; Liu, X.; Liu, J.; Zhang, M.; Wang, Z. A Novel Lightweight Block Encryption Algorithm Based on Combined Chaotic S-Box. *Int. J. Bifurc. Chaos* **2021**, *31*, 2150152. [[CrossRef](#)]
55. Hematpour, N.; Ahadpour, S.; Sourkhani, I.G.; Sani, R.H. A new steganographic algorithm based on coupled chaotic maps and a new chaotic S-box. *Multimed. Tools Appl.* **2022**, *14*, 895. [[CrossRef](#)]
56. Zhang, X.; Mao, Y.; Zhao, Z. An efficient chaotic image encryption based on alternate circular S-boxes. *Nonlinear Dyn.* **2014**, *78*, 359–369. [[CrossRef](#)]
57. Belazi, A.; Khan, M.; El-Latif, A.A.A.; Belghith, S. Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. *Nonlinear Dyn.* **2017**, *87*, 337–361. [[CrossRef](#)]
58. Lu, Q.; Zhu, C.; Deng, X. An efficient image encryption scheme based on the LSS chaotic map and single S-box. *IEEE Access* **2020**, *8*, 25664–25678. [[CrossRef](#)]
59. Idrees, B.; Zafar, S.; Rashid, T.; Gao, W. Image encryption algorithm using S-box and dynamic Hénon bit level permutation. *Multimed. Tools Appl.* **2020**, *79*, 6135–6162. [[CrossRef](#)]
60. Wang, X.; Yang, J. A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system. *Optik-Int. J. Light Electron Opt.* **2020**, *217*, 164884. [[CrossRef](#)]
61. Masood, F.; Masood, J.; Zhang, L.; Jamal, S.S.; Boulila, W.; Rehman, S.U.; Khan, F.A.; Ahmad, J. A new color image encryption technique using DNA computing and Chaos-based substitution box. *Soft Comput.* **2021**, 1–17. [[CrossRef](#)]
62. Ali, T.S.; Ali, R. A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box. *Multimed. Tools Appl.* **2022**, *81*, 20585–20609. [[CrossRef](#)]

63. Deb, S.; Behera, P.K. Design of key-dependent bijective S-Boxes for color image cryptosystem. *Optik-Int. J. Light Electron Opt.* **2022**, *253*, 168548. [[CrossRef](#)]
64. Hussain, I.; Azam, N.A.; Shah, T. Stego optical encryption based on chaotic S-box transformation. *Opt. Laser Technol.* **2014**, *61*, 50–56. [[CrossRef](#)]
65. Hussain, I. Optical image encryption based on S-box transformation and fractional Hartley transform. *J. Vib. Control* **2016**, *22*, 1143–1146. [[CrossRef](#)]
66. Girija, R.; Singh, H. Enhancing security of double random phase encoding based on random S-Box. *3D Res.* **2018**, *9*, 1–20. [[CrossRef](#)]
67. Shatheesh, S.I.; Devaraj, P.; Bhuvaneshwaran, R.S. An efficient quasigroup based image encryption using modified nonlinear chaotic maps. *Sens. Imaging* **2014**, *15*, 1–21.
68. Zhu, H.G.; Zhao, C.; Zhang, X.D.; Yang, L.P. An image encryption scheme using generalized Arnold map and affine cipher. *Optik-Int. J. Light Electron. Opt.* **2014**, *125*, 6672–6677. [[CrossRef](#)]
69. Wu, C.M. An improved discrete Arnold transform and its application in image scrambling and encryption. *Acta Phys. Sin.* **2014**, *63*, 090504.
70. Li, J.; Feng, Y.; Yang, X.Q.; Huang, F. Invertible map set based image encryption algorithm. *J. Optoelectron. Laser* **2009**, *20*, 78–83. (In Chinese)
71. Adams, C.; Tavares, S. The structured design of cryptographically good S-boxes. *J. Cryptol.* **1990**, *3*, 27–41. [[CrossRef](#)]
72. Webster, A.F.; Tavares, S.E. On the design of S-boxes. In Proceedings of the Advances in Cryptology CRYPTO 85, Lecture Notes in Computer Science, The University of California, Santa Barbara, CA, USA, 18–22 August 1985; Springer: Berlin/Heidelberg, Germany, 1985; Volume 218, pp. 523–534.
73. Adams, C.; Tavares, S.E. Good S-boxes are easy to find. In Proceedings of the Advances in Cryptology CRYPTO 89, The University of California, Santa Barbara, CA, USA, 20–24 August 1989; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1989; Volume 435, pp. 612–615.
74. Biham, E.; Shamir, A. Differential cryptanalysis of DES-like cryptosystems. In Proceedings of the Advances in Cryptology CRYPTO 90, The University of California, Santa Barbara, CA, USA, 11–15 August 1990; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1990; Volume 537, pp. 2–21.
75. Matsui, M. Linear cryptanalysis method for DES cipher. In Proceedings of the Advances in Cryptology EUROCRYPT 93, Lofthus, Norway, 23–27 May 1993; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1993; Volume 765, pp. 386–397.
76. Usc-Sipi Image Database for Research in Image Processing, Image Analysis, and Machine Vision. Available online: <http://sipi.usc.edu/database/> (accessed on 6 June 2017).
77. Alvarez, G.; Li, S.J. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurcation Chaos Appl. Sci. Eng.* **2006**, *16*, 2129–2151. [[CrossRef](#)]
78. Wang, X.; Chen, X. An image encryption algorithm based on dynamic row scrambling and Zigzag transformation. *Chaos, Solitons & Fractals* **2021**, *147*, 110962.