Hindawi
Security and Communication Networks
Volume 2020, Article ID 7913061, 12 pages
https://doi.org/10.1155/2020/7913061

Research Article

Design and Analysis of a Novel Chaos-Based Image Encryption Algorithm via Switch Control Mechanism

Shenyong Xiao, ZhiJun Yu, and YaShuang Deng

The School of Information and Safety Engineering, Zhongnan University of Economics and Law, Wuhan 430073, China

Correspondence should be addressed to YaShuang Deng; dys0377@163.com

Received 18 December 2019; Accepted 13 February 2020; Published 16 March 2020

Guest Editor: Farrukh Aslam Khan

Chaos has been widely used in image encryption due to its rich properties. However, it remains an irreconcilable contradiction for security and implementation efficiency for image encryption schemes. In this paper, a novel chaos-based image encryption scheme has been proposed, where the Lorenz chaotic system is applied to generate pseudorandom sequences with good randomness, and a random switch control mechanism is introduced to ensure the security of the encryption scheme. Experimental results demonstrate the effectiveness and superiority of the algorithm.

1. Introduction

Mass data transmission on various communication networks has led to a security risk in multimedia data. Digital images have become an important expression in the network of information transmission due to its intuitive and vivid attribute; meanwhile, a great deal of researches on image processing has emerged [1–4]. The increasingly rampant network crime makes the digital image security particularly important. In the past few decades, many encryption algorithms such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and Advanced Encryption Standard (AES) have been put forward. However, those methods are more suitable for text encryption rather than image encryption owing to the special properties of images including large amount of data, high redundancy, and strong correlation between pixels. Chaotic system has features such as sensitivity to initial conditions and control parameters, dense periodic points, and topological transitivity, which make it especially suitable for image encryption. A chaotic image encryption algorithm was firstly proposed in 1989 [5]. Ever since then, a variety of chaos-based image encryption algorithms have been put forward [6–16].

Early chaotic image encryption schemes were mostly based on simple low-dimensional chaotic systems, such as Logistic chaotic map [17], tent chaotic map [18], cat chaotic map [11], Baker chaotic map [19], and so on [20]. Specific can elaborate as: El Assad and Farajallah [11] proposed an image encryption system based on 2D cat map, where a diffusion layer along with a bit-permutation layer was contained. Li et al. [18] proposed a novel image encryption scheme based on the tent map, which had been proved to perform well. Zhang and Wang [21] proposed a new multiple-image encryption algorithm based on the mixed image element and piecewise linear chaotic map, which is a quite fast way to encrypt, and the like. However, some existing schemes have been revealed to be security risk owing to the simple structure of the applied chaotic maps [22]. Then, researchers tried to design image encryption schemes by using various deformation or combinations of these well-known chaotic maps and other mathematical manipulation [23–26], such as the composition of logistic and tent map [27], the Logistic-Sine-coupling map [28], and baker map and logistic map [29]. These solutions have enhanced the security of algorithms and were effective to some certain extent. With the further study of chaotic systems, more and more image encryption schemes based on higher-dimensional chaotic systems, especially for hyperchaos and spatiotemporal chaos, emerge gradually [13, 30–32]. Actually, most of these schemes have a high level of security, as opposed to a high implementation cost. Moreover, some new technologies have been

introduced to the design and security analysis of image encryption schemes such as neural network [33], DNA coding [34], genetic recombination [31], compressed sensing [35], and machine leaning [36]. In general, there exists an irreconcilable contradiction between the security and implementation complexity of cryptographic algorithms.

Switch control technology has been addressed in many fields such as biological and medical systems [37], electric power systems [38], and others. It is worth mentioning that switch control can be used to realize the chaotification of given dynamical systems or make an original simple system become complex, etc. Motivated by the above discussion, in this paper, we introduce the switch control mechanism into the chaos-based image encryption scheme, where the required pseudorandom numbers for encryption are still generated by chaos, and substitutions of rows or columns of image in the permutation of plain images are determined by the designed random switch control mechanism. Moreover, the confusion of the permuted image is completed to ensure the security of the whole image encryption. Finally, experimental results are carried out to show the effect of the scheme. Given that the process of image encryption can hide any information about the original image as much as possible, the whole process can be regarded as the process of decreasing entropy. Then, performance comparisons with some existing image schemes are carried out by using information entropy along with other indicators to show the superiority of the proposed image encryption algorithm.

The rest of this paper is organized as follows. Some preliminaries are given in Section 2. In Section 3, we present a novel image encryption scheme via switch control mechanism. In Section 4, some numerical examples are given to illustrate the validity and superiority of image encryption algorithm. Section 5 concludes this paper.

2. Pseudorandom Number Generator Based on Lorenz Chaotic System

For a given plain image, the whole encryption requires a series of random numbers to produce secret image. Therein, this paper exploits the effectiveness of the Lorenz chaotic system to generate pseudorandom numbers. The Lorenz system is formally defined as

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = cx - y - xz, \\ \dot{z} = xy - bz, \end{cases} \tag{1}$$

where a, b, and c are system parameters. It is well known that the system has a strange chaotic attractor over the parameters $a = 10$, $b = 8/3$, and $c = 28$, as depicted in Figure 1.

Motivated by the idea in [39] that proper stretch transformation along with modular operation can make the chaotic system generate pseudorandom numbers with good randomness, two new pseudorandom number generators are designed as

$$S1_i = \mathrm{mod}\left(\mathrm{round}\left(\left(x_i + y_i\right) * 10^{12}, 2\right)\right); \quad i = 1, 2, \ldots, \tag{2}$$

$$S2_i = \mathrm{mod}\left(\mathrm{round}\left(z_i * 10^{12}\right), 256\right); \quad i = 1, 2, \ldots, \tag{3}$$

where $\{x_i\}$, $\{y_i\}$, and $\{z_i\}$ are sample sequences of the Lorenz chaotic system over the sampling interval $T = 0.1$. Actually, the chaotic signal can be completely described by its samples for this sampling interval [39].

The standard NIST SP800-22 test is applied to evaluate the performance of two pseudorandom number generators, and the test results are summarized in Table 1. As shown in the table, two pseudorandom number generators have passed all the tests, which indicate that both of them have good randomness, thus can be used in the next image encryption process.

3. Proposed Image Encryption Scheme

This section presents the proposed image encryption in detail. The encryption scheme consists of two main parts: image confusion and image diffusion. The confusion process generates scrambled images from a series of plain images by relocating image pixels, where it is determined by a switch control rule. The diffusion increases the security of permutated images by using mixed operation on relocated pixel values of images.

3.1. Image Encryption Process. Let I be an image with the size of $M \times N$, which can be turned into the vector form as follows:

$$I = \{I_1, I_2, \ldots, I_{MN}\}, \tag{4}$$

where I_i denotes the image pixel at i-th position, for $i = 1, 2, \ldots, M \cdot N$.

3.1.1. Image Confusion via Switch Control Mechanism. To perform the image confusion, the proposed method exploits the Lorenz chaotic system to generate two chaotic sequences denoted as follows:

$$\begin{aligned} R &= \{R_1, R_2, \ldots, R_M\}, \\ L &= \{L_1, L_2, \ldots, L_N\}. \end{aligned} \tag{5}$$

The proposed method then sort two these chaotic sequences R and L to yield the following sets:

$$\begin{aligned} SR &= \{SR_1, SR_2, \ldots, SR_M\}, \\ SL &= \{SL_1, SL_2, \ldots, SL_N\}. \end{aligned} \tag{6}$$

Finally, marking the positions of each point in the sequences SR and SL in the original sequences R and L, we can get two random permutations denoted as follows:

$$\begin{aligned} TR &= \{TR_1, TR_2, \ldots, TR_M\}, \\ TL &= \{TL_1, TL_2, \ldots, TL_N\}. \end{aligned} \tag{7}$$

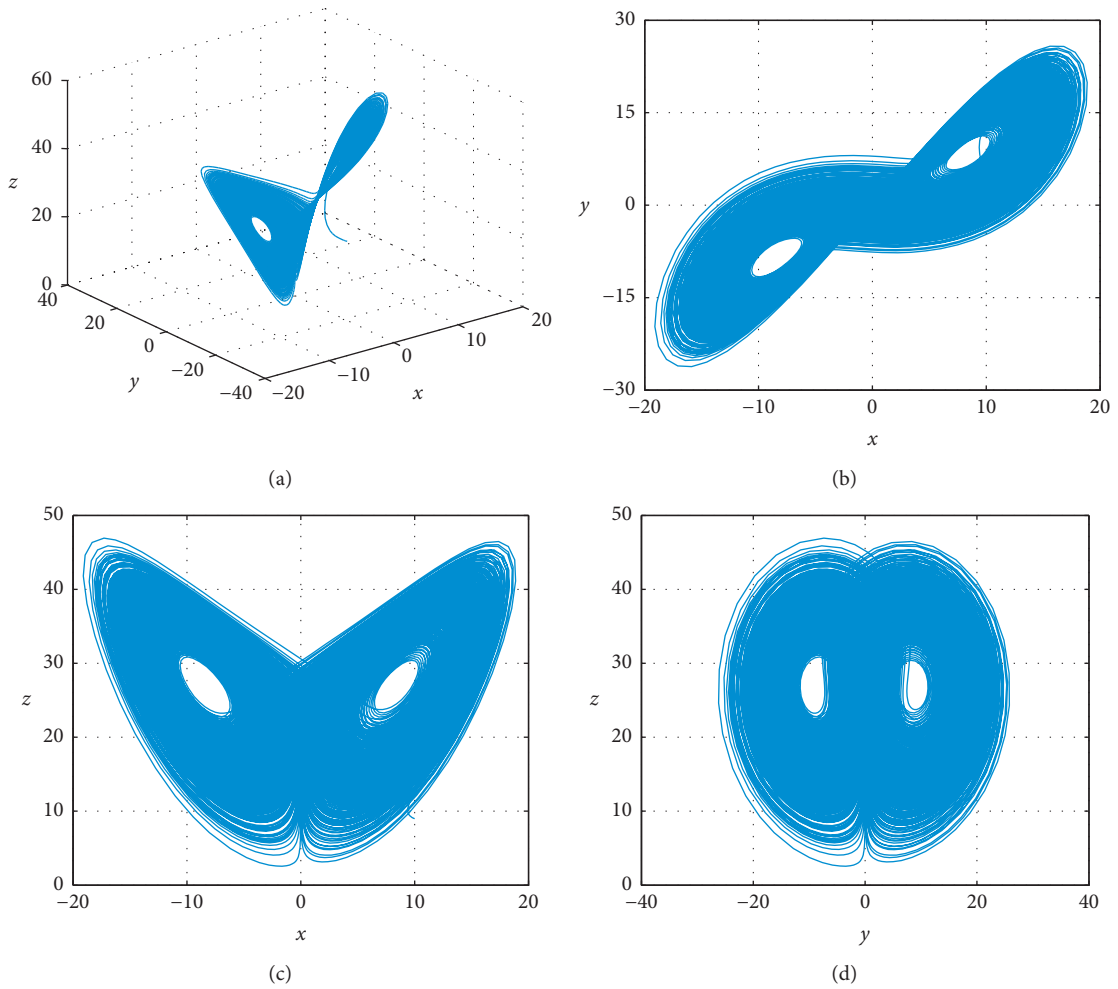

Figure 1: Lorenz chaotic attractor. (a) All directions. (b) x-y direction. (c) x-z direction. (d) y-z direction.

Table 1: NIST SP800-22 test results of two generators.

Test name	S1		S2	
	p value	Results	p value	Results
Frequency	0.115026	SUCCESS	0.852445	SUCCESS
Block frequency	0.479345	SUCCESS	0.335341	SUCCESS
Cumulative sums	0.133011	SUCCESS	0.739284	SUCCESS
Runs	0.628042	SUCCESS	0.648365	SUCCESS
Longest runs of ones	0.746332	SUCCESS	0.269936	SUCCESS
Rank	0.955981	SUCCESS	0.057146	SUCCESS
FFT	0.713570	SUCCESS	0.818546	SUCCESS
Overlapping template matching	0.360195	SUCCESS	0.434233	SUCCESS
Universal statistical	0.689639	SUCCESS	0.693656	SUCCESS
Random excursions	0.364557	SUCCESS	0.504450	SUCCESS
Random excursions variant	0.490487	SUCCESS	0.490322	SUCCESS
Serial	0.880692	SUCCESS	0.157533	SUCCESS
Nonperiodic template	0.541996	SUCCESS	0.474985	SUCCESS
Linear complexity	0.519593	SUCCESS	0.736412	SUCCESS
Apen	0.909288	SUCCESS	0.401933	SUCCESS

To increase the randomness of rearrangement of image pixels, a switch control mechanism is injected into the image confusion step, which can be used to determine whether a row or column transformation will be performed on plain images. The switch control mechanism can be designed as follows:

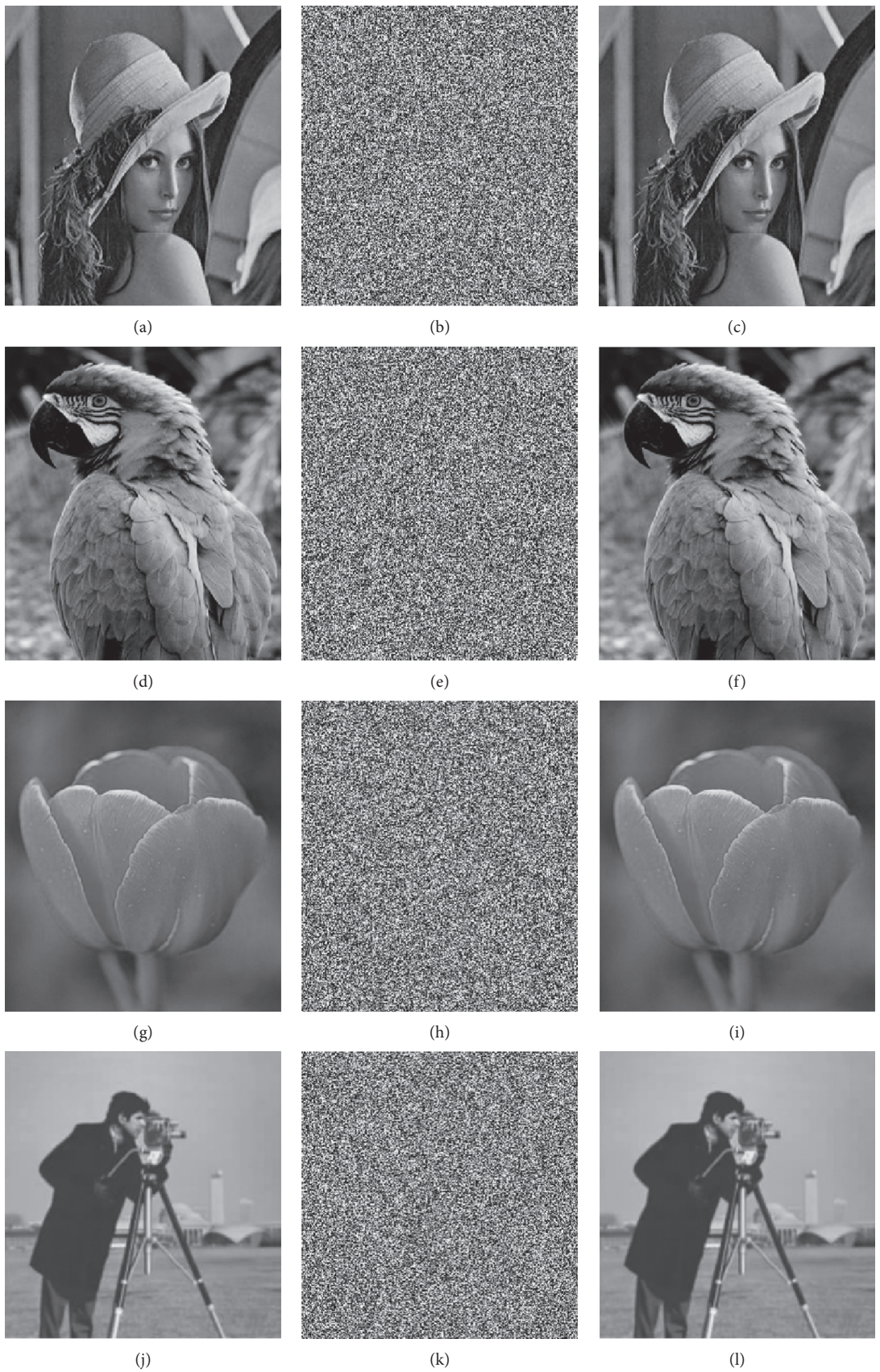

Figure 2: Encryption and decryption of images. (a) Plaintext of Lena. (b) Encryption of Lena. (c) Decrypion of Lena. (d) Plaintext of bird. (e) Encryption of bird. (f) Decryption of bird. (g) Plaintext of flower. (h) Encryption of flower. (i) Decryption of flower. (j) Plaintext of photographer. (k) Encryption of photographer. (l) Decryption of photographer.

$$\overline{I} = \begin{cases} f_1(I), & if\ S1_i = 0, \\ f_2(I), & if\ S1_i = 1, \end{cases} \tag{8}$$

where I is the plain image, $\overline{I}$ is the scrambled image, and $S1$ is the pseudorandom number generator expressed by equation (2), whose randomness determines that the proposed switch control law is also random. $f1$ and $f2$ represent row and column transformation described as follows.

Row transformation (f_1): rearrange the positions of the rows in I according to the order of TR, e.g., move the TR_1 row to the first row, the TR_2 row to the second row, . . ., the TR_M row to the M th row.

Column transformation (f_2): rearrange the positions of the columns in I according to the order of TL, e.g., move the TL_1 column to the first column, the TL_2 column to the second column, . . ., the TL_N column to the Nth column.

Based on the above switch control rule, the confusion process can be described as follows:

Step 1: select the first K points from $S1$ and let $\theta = S1_i$ $i = 1, 2, \ldots, K$, where K represents the maximum value of M and N.

Step 2: relocate the pixels of image I according to the switch control rule represented by equation (8) along with the pseudorandom sequence $S1$. That is, if $\theta = 0$, a row transformation will be performed on the plain image; otherwise, column transformation works.

Step 3: a new matrix $\overline{I}$ can be got after MN times transformations. If the pixel in the image has not been permutated completely, discard the first MN points in $S1$, and repeat Step 1-Step 2 until the results perform well.

3.1.2. Image Diffusion Process. To further increase the security level of the proposed image encryption, the scrambled image $I1'$ can be made more confusing via the pseudorandom numbers $S2$ designed previously, where the whole image can be processed as a sequence with length of MN.

The image diffusion can simply perform by utilizing the following computation:

$$C_i = \left(\mathrm{mod}\left(C_{i-1} + \overline{I}_i + \overline{I}_{i-1}\right), 256\right) \oplus S2, \tag{9}$$

where C_i is the current ciphered value, C_{i-1} is the previous ciphered value, $\overline{I}_i$ is the current scrambled image value, and $\overline{I}_{i-1}$ is the previous scrambled image value, and $S2$ has been calculated by equation (3). Set the initial value $C_0 = 0$.

3.2. The Decryption Process. The inverse process of image diffusion aims to recover back the diffused image into its original value, which can be viewed as the reverse of the encryption part. The same keys as used in the encryption process are introduced into the Lorenz chaotic system to obtain three output sequences $\{x_i\}$, $\{y_i\}$, and $\{z_i\}$, $i = 1, 2, \ldots, N$. Then, the same method employed above to calculate $S1$ and $S2$ was used.

The formula of the decryption is given as

$$\overline{I}_i = \mathrm{mod}\left(C_i \oplus S2 - C_{i-1} - \overline{I}_{i-1}, 256\right), \tag{10}$$

where C_i is the current ciphered value, C_{i-1} is the previous ciphered value, $\overline{I}_i$ is the current scrambled image value, and $\overline{I}_{i-1}$ is the previous scrambled image value, and $S2$ has been calculated by equation (3) . Without loss of generality, set initial value $\overline{I}_0 = 0$.

The confusion of decryption: extract K points from $S1$ to get θ. If $\theta = 0$, the corresponding part will be performed by row transformation; else, the column transformation works. And it is determined by the random permutation TR and TL how the image transforms. It is worth noting that the round of permutation part used here should be the same as the one designed in the encryption process. In this way, the plain image I can be recovered.

4. Experimental Results and Performance Analysis

Series of images are chosen here to verify the performance of the proposed image encryption algorithm, where all image sizes are normalized to 256×256 for convenience. Setting the parameters and initial values of the Lorenz chaotic system as $a = 10$, $b = 8/3$, $c = 28$, $x_0 = 10$, $y_0 = 5$, and $z_0 = 9$, we carry out the encryption scheme.

We first invest the performance of the proposed encryption algorithm for different images. It can be shown from Figure 2 that the algorithm destroys the obvious pattern of the plain image and makes the ciphered image display a space filling with a noise-like pattern. The shuffling process of pixels of the image hides the information of the original plain image and makes the ciphered image seem random to the intruder. Thus, the encryption scheme is effective.

Then, we analyze the security of the proposed encryption scheme. Generally, a good encryption scheme not only can hide any information of the plain image but also can resist some attacks. Some commonly used test indicators have been applied to analyse the security of the proposed image encryption scheme, which include key space and key sensitivity analysis, histogram analysis, NPCR (number of pixel change rate) and UACI (unified average changing intensity) analysis, entropy analysis, and correlation analysis.

4.1. Key Space and Sensitivity Analysis. The size of key space is an important indicator to measure the ability of resistance to exhaustion attack. In general, the smaller the key space, the more vulnerable the scheme is to attack. From the cryptographic point of view, the size of key space should be no smaller than 2^{128} to make brute force attack ineffective. Given that the secret keys include the initial value x_0, y_0, and z_0 and system parameters a, b, and c, the size of the key space can reach 10^{6L} with computing precision 10^L. In the case, the key space is far more than $10^{84}(\approx 2^{128})$ if the precision $L \geq 14$. Therefore, the key space is large enough to resist the exhaustion attack.

A good image encryption scheme should also be sensitive to tiny changes of keys, which means any tiny changes of the keys can induce huge changes of the encrypted images.

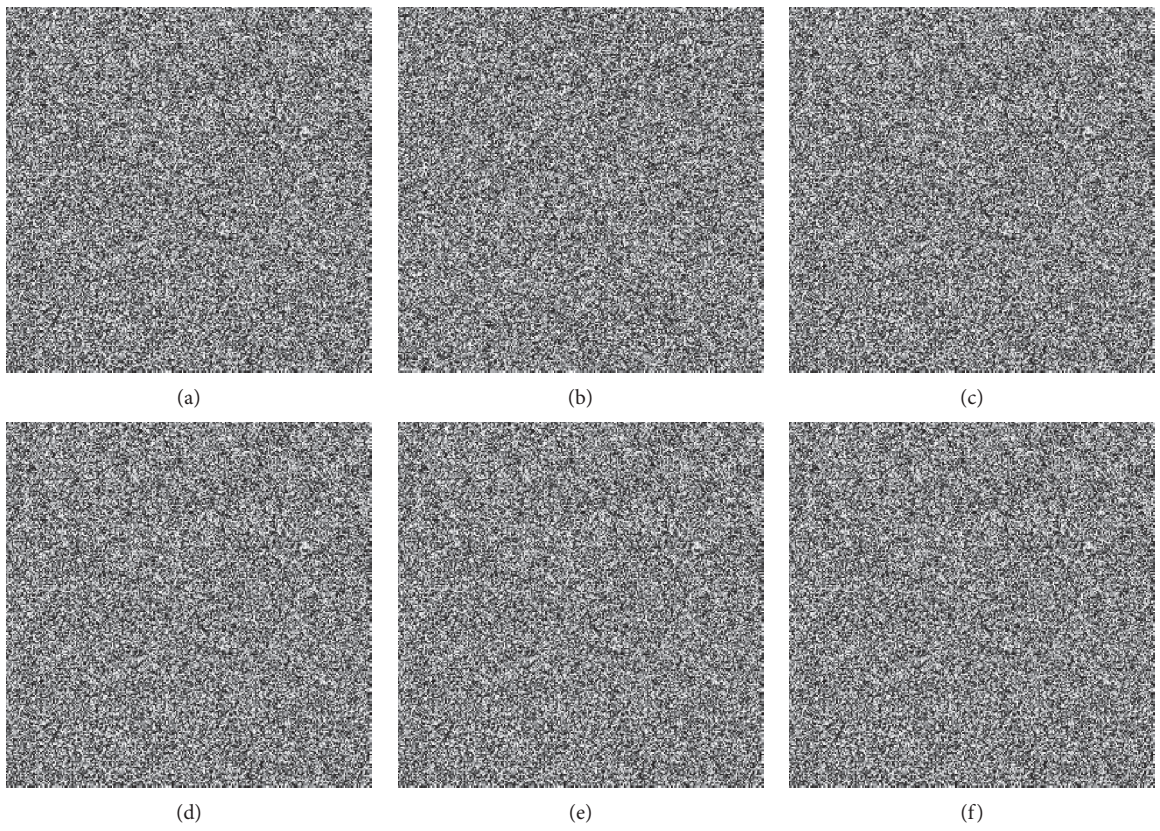

Figure 3: Key Sensitivity Analysis. (a) Change a restoring diagram. (b) Change b restoring diagram. (c) Change c restoring diagram. (d) Change x_0 restoring diagram. (e) Change y_0 restoring diagram. (f) Change z_0 restoring diagram.

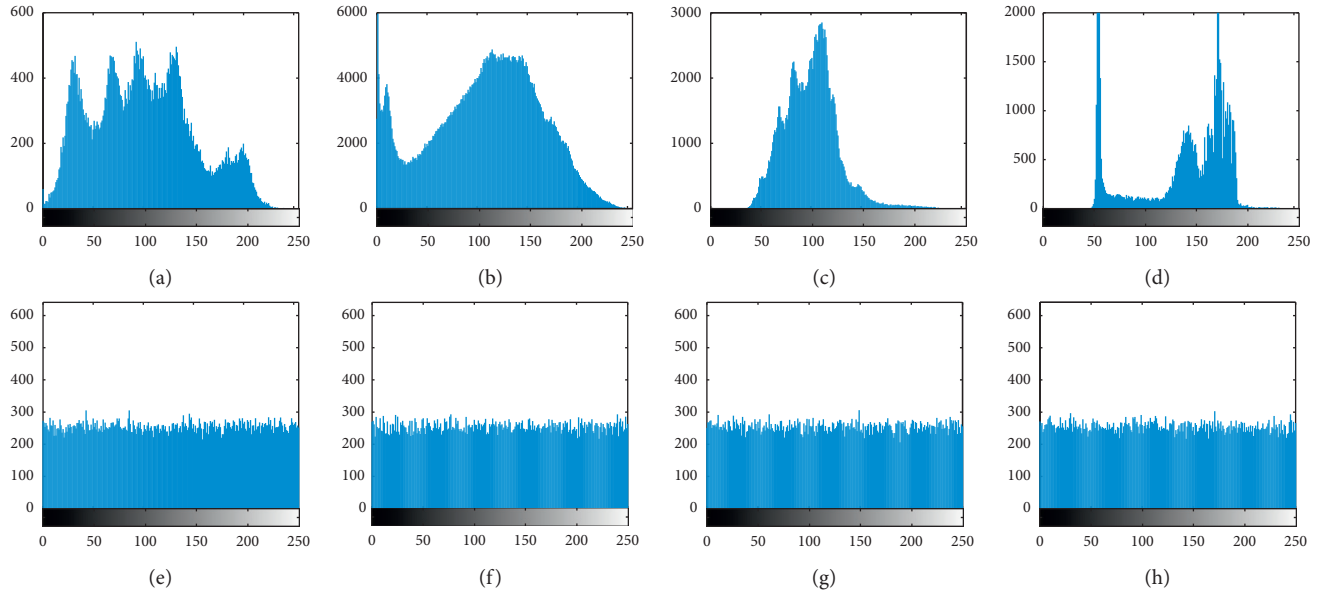

Figure 4: Histograms of plain and ciphered images. (a–d) Histograms of Lena, bird, flower, and photographer. (e–h) Histograms of ciphered Lena, bird, flower, and photographer.

In this way, the attacker cannot decode the original image by using the keys similar to the real ones.

Without loss of generality, we choose randomly system parameters and initial values to carry out the process of encryption and decryption and observe the influence of tiny changes on the decryption. For each secret key, suppose that the last one bit is changed in it and other keys are unchanged and then investigate if the original images can be restored

Table 2: NPCR and UACI of different positions.

Position	(1, 1)	(64, 64)	(128, 128)	(1, 256)	(256, 1)	(256, 256)
NPCR (%)	99.6063	99.6048	99.6201	99.5880	99.6048	99.5926
UACI (%)	33.4621	33.2419	33.4538	33.3603	33.3034	33.3788

Table 3: NPCR and UACI of proposed algorithm.

Image	Lena	Bird	Flower	Photographer
NPCR (%)	99.6063	99.6002	99.5834	99.6086
UACI (%)	33.4621	33.4665	33.4696	33.4434

Table 4: Comparison of NPCR and UACI with other methods.

Scheme	Proposed	Ref. [26]	Ref. [34]	Ref. [12]	Ref. [16]
NPCR (%)	99.6063	99.62000	99.6173	99.6552	99.6094
UACI (%)	33.4621	33.46000	29.5664	33.4846	28.6181

Table 5: Correlation coefficients of images.

Image	Plain image			Ciphered image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9728	0.9281	0.9050	−0.0011	0.0014	0.0005
Bird	0.9687	0.9596	0.9298	0.0004	−0.0020	0.0028
Flower	0.9694	0.9528	0.9301	0.0026	−0.0041	−0.0023
Photographer	0.9626	0.9231	0.9496	0.0029	−0.0024	−0.0008

using the changed key. Setting the parameters $a = 10$, $b = 8/3$, $c = 28$, $x_0 = 10$, $y_0 = 5$, and $z_0 = 9$, the decrypted images using the same settings can be shown in Figure 2 in front. Meanwhile, the decrypted image with the keys a, b, c, x_0, y_0, and z_0 changed to 0.00000000001 is shown in Figure 3. To be exact, the key a is changed to 10.00000000001. Similar conclusions can be got for other keys. As shown in Figure 3, the encrypted image cannot be cracked by using a similar key ($x_0 = 10.00000000000001$). Hence, the algorithm is sensitive to tiny changes of keys.

4.2. Histogram Analysis. The histogram of an image is an important statistical property which can reflect the relation between gray level and its corresponding frequency. For a good image encryption algorithm, its encrypted image should have a histogram with uniform distribution to hide the statistical characteristic. The images before and after encryption are shown in Figure 4. It can be seen from Figures 4(a)–4(d) that the frequency distributions of given images are not uniform for different gray levels, which makes attackers often easily get information from them. It can be found from Figures 4(e)–4(h) that the frequency distribution becomes quite uniform after encryption, which indicates that the statistical characteristic has been hidden and will not leak any information of the plain images, thus enhance the security of the images.

4.3. NPCR and UACI Analysis. NPCR and UACI are two measures to examine the performance of an image encryption algorithm to resist differential attack. Actually, NPCR depicts the number of pixels change rate while one pixels of plain image changed, while UACI stands for the average intensity of difference between the plain image and the ciphered image. Two these indicators can be defined as follows:

$$\begin{aligned} \mathrm{NPCR} &= \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \\ \mathrm{UACI} &= \frac{1}{W \times H} \sum_{i,j} \frac{\left| C_1(i,j) - C_2(i,j) \right|}{255} \times 100\%, \end{aligned} \tag{11}$$

where W and H are the width and height of C_1 or C_2. C_1 or C_2 is the encrypted image before and after one pixel of the plain image is changed. $D(i, j)$ can be defined as follows: if $C_1 \neq C_2$, $D(i, j) = 1$; else, $D(i, j) = 0$.

And the expectation of the NPCR and UACI with 8 bits representation can be described as [40]

$$\begin{aligned} \mathrm{NPCR}_E &= \left(1 - 2^{-n}\right) \times 100\% \\ \mathrm{UACI}_E &= \frac{1}{2^{2n}} \frac{\sum_{i=1}^{2^n - 1} i(i+1)}{2^n - 1} \times 100\%, \end{aligned} \tag{12}$$

where n denotes the digit. It can be calculated that NPCR_E and UACI_E are close to 99.6094070 and 33.4635070 for 8 bits digits.

We invest the NPCR and UACI results of the encrypted Lena images for different positions and different images separately, and the results are shown in Tables 2 and 3, respectively. As shown in two these tables, the values of NPCR are close to the ideal value, which means the encryption scheme is very sensitive to small changes in the plain image. With respect to UACI, the values for different

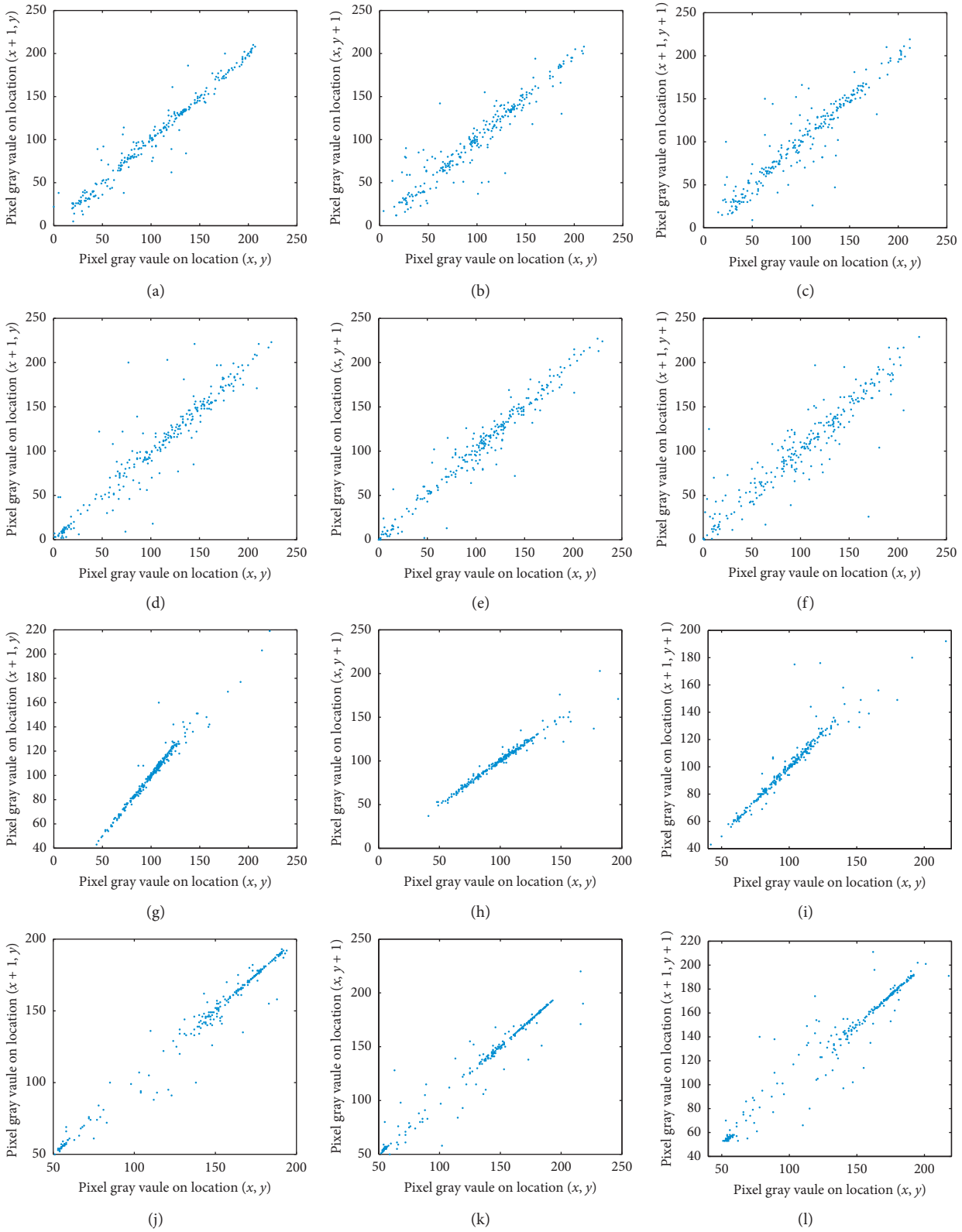

Figure 5: Correlations of plain images in horizontal, vertical, and diagonal adjacent pixels. (a–c) Lena. (d–f) Bird. (g–i) Flower. (j–l) Photographer.

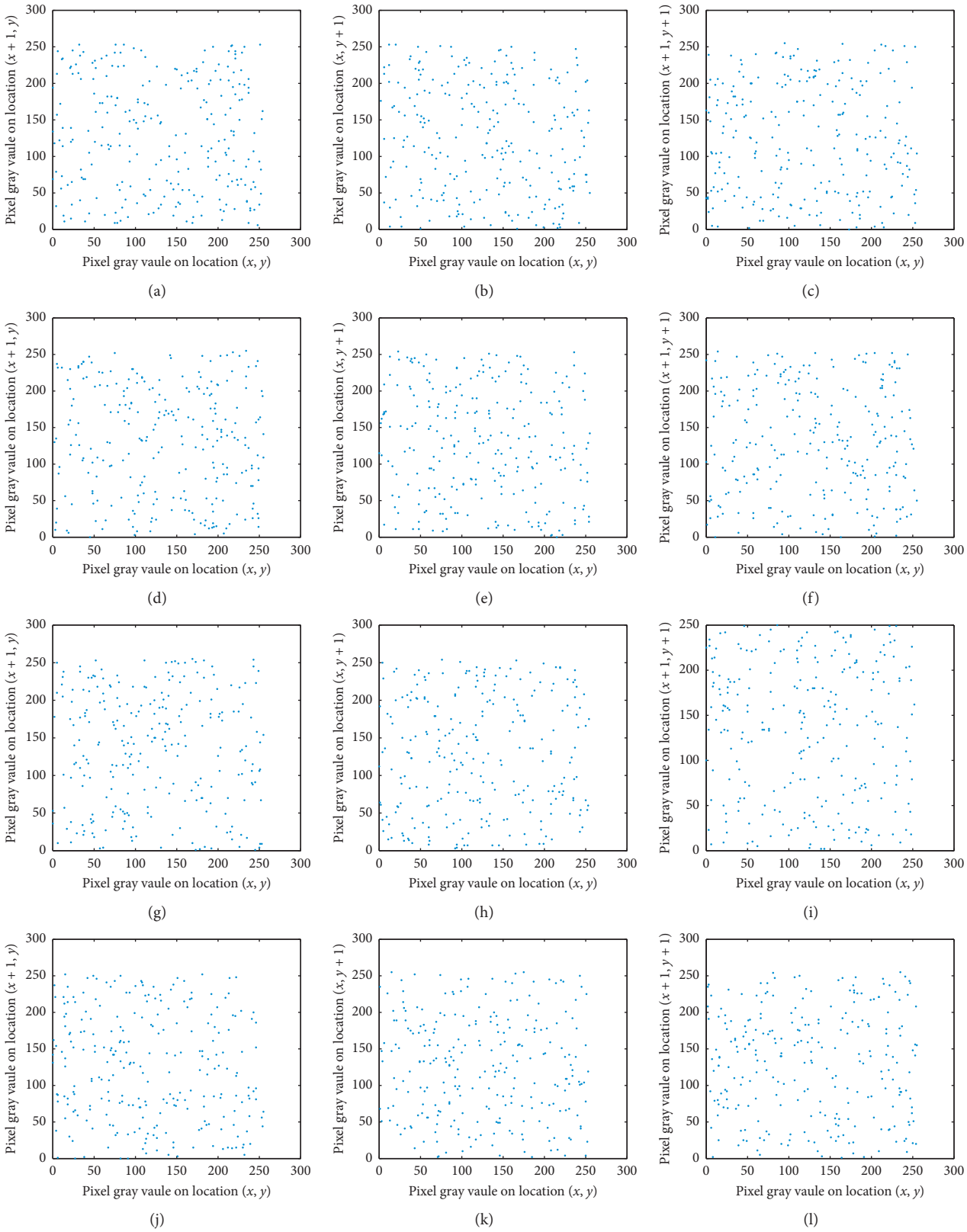

Figure 6: Correlations of ciphered images in horizontal, vertical, and diagonal adjacent pixels. (a–c) Lena. (d–f) Bird. (g–i) Flower. (j–l) Photographer.

Table 6: Comparison of correlation coefficients with other methods.

Scheme	Lena	Proposed	Ref. [26]	Ref. [34]	Ref. [12]	Ref. [16]
Horizontal	0.9728	−0.0011	−0.0285	0.0027	−0.0038	−0.0245
Vertical	0.9281	0.0014	0.0014	0.0005	−0.0026	−0.0226
Diagonal	0.9050	0.0005	0.0013	−0.0045	0.0017	−0.0193

Table 7: Information entropy of images.

Image	Lena	Bird	Flower	Photographer
Plain	7.5545	7.6515	6.6792	6.5786
Ciphered	7.9974	7.9973	7.9970	7.9971

Table 8: Approximate entropy of images.

Image	Lena	Bird	Flower	Photographer
Plain	0.6434	0.7828	0.4613	0.2723
Ciphered	2.1733	2.1785	2.1815	2.1734

Table 9: Comparison of information entropy with other methods.

Scheme	Plain image	Encrypted image	Ref. [26]	Ref. [34]	Ref. [12]	Ref. [16]
Entropy	7.5545	7.9997	7.9993	7.9972	7.9874	7.9975

images are also close to the ideal value, which indicates that the rate of influence due to one pixel change is very large. In this way, the algorithm has strong ability to resist differential attacks.

To further show the superiority of the algorithm, comparisons with other existing schemes have been made here, as depicted in Table 4. It is clear from the analysis result that the algorithm has higher ability to resist differential attack.

4.4. Correlation Analysis. The correlation between image pixels is an important indicator to measure whether the ciphered image can resist the chosen-plaintext attack. The correlation between adjacent pixels can be characterized by correlation coefficients, which can be defined as follows:

$$r_{x,y} = \frac{\mathrm{Cov}(x, y)}{\sqrt{D(x) * D(y)}}, \tag{13}$$

where x and y are the grayscale values of two adjacent pixels in the given image. $D(x)$ and $D(y)$ are the variance of x and y, respectively. $\mathrm{Cov}(x, y)$ shows the covariance of x and y.

To measure the correlation of adjacent pixels, we first select 2000 pairs of adjacent pixels (in vertical, horizontal, and diagonal directions) randomly from plain images and ciphered images, respectively, and calculate their correlation coefficients. The mean value of the correlation coefficients for different images is shown in Table 5. Obviously, the correlation between two adjacent pixels can be greatly reduced after encryption. Figures 5 and 6 also depict the correlations of plain and ciphered images in horizontal, vertical and diagonal adjacent pixels, respectively. In addition, correlation performance comparison with other existing image encryption algorithms is made, as shown in Table 6. It can be observed that the correlation between two adjacent pixels of plain images has been eliminated to a large extent and then enhances the ability to resist the chosen-plaintext attack. All these results indicate the proposed image encryption algorithm is effective and has higher security.

4.5. Entropy Analysis. For a given image, it is ideal that the character information of the image can be hidden entirely after being encrypted, and thus the intruder cannot carry an effective attack on it. To measure the complexity or uncertainty of given images, two entropy indicators are introduced here: information entropy and approximate entropy (ApEn) [41]. The former mainly measures the uncertainty of an information source, while the latter depicts the probability of new patterns appearing in the information source. Normally, the more complicated the sequence, the higher the entropy, and the less likely it is to leak information.

The information entropy $H(x)$ of an information source x can be calculated as

$$H(x) = -\sum p(x)\log_2 p(x), \tag{14}$$

where $p(x)$ represents the probability of source x. Normally, the greater the uncertainty of source x, the higher the entropy. A source with uniform distribution has the greatest uncertainty, and the information entropy is at its maximum. That is, the more information entropy closes to 8, the more uncertainty there is, and less information the system may leak. As shown in Table 7, the information entropy of images is enhanced to be in close proximity to the maximum value 8 under the current digit after encryption. That is, the probability of information leakage is very small, which means the encryption scheme is effective.

Generally, the more evenly distributed, the less likely new patterns are to emerge and the greater the ApEn value is. As shown in Table 8, the ApEn values of the ciphered images are enhanced to be more than 2.5 times than the ones of the original images and even be close to the mean value (about 2.1773nat) of the random images with uniform distribution, which further ensure the validity of the proposed scheme.

Furthermore, we compare the entropy performance of the proposed algorithm with other existing chaos-based image encryption schemes. As shown in Table 9, the information entropy of the proposed scheme is not only larger than that of other schemes but also closer to the maximum value of 8. In this way, the proposed scheme has higher security.

5. Conclusion

Given that there exists a contradiction between the security and implementation for most existing chaotic image encryption schemes, a novel chaos-based encryption scheme via switch control technology has been proposed. In this scheme, the three-dimensional Lorenz chaotic system is introduced to generate pseudorandom sequences with good randomness, and a switch control law is designed to realize the random permutation of the given images. The simulation results show that the proposed algorithm has a good performance, and the comparisons of entropy and other indicators also show its superiority.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work described in this paper was supported by the National Natural Science Foundation of China (no. 61702554) and the National Crypto Development Fund of China (no. MMJJ20170109). Thanks are due to the National Natural Science Foundation of China and the State Encryption Administration of China.

References

[1] T. Liu, H. Liu, Z. Chen, and A. M. Lesgold, "Fast blind instrument function estimation method for industrial infrared spectrometers," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 12, pp. 5268–5277, 2018.

[2] T. Liu, H. Liu, Y. Li, Z. Zhang, and S. Liu, "Efficient blind signal reconstruction with wavelet transforms regularization for educational robot infrared vision sensing," *IEEE/ASME Transactions on Mechatronics*, vol. 24, no. 1, pp. 384–394, 2018.

[3] T. Liu, Y. Fu Li, H. Liu, Z. Zhang, and S. L. Risir, "Rapid infrared spectral imaging restoration model for industrial material detection in intelligent video systems," *IEEE Transactions on Industrial Informatics*, 2019.

[4] T. Liu, H. Liu, Y.-F. Li, Z. Chen, Z. Zhang, and S. Liu, "Flexible ftir spectral imaging enhancement for industrial robot infrared vision sensing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 544–554, 2020.

[5] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[6] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[7] L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 759–765, 2005.

[8] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[9] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1d chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

[10] C. Song and Y. Qiao, "A novel image encryption algorithm based on dna encoding and spatiotemporal chaos," *Entropy*, vol. 17, no. 10, p. 6954, 2015.

[11] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing: Image Communication*, vol. 41, pp. 144–157, 2016.

[12] C. Pak and L. Huang, "A new color image encryption using combination of the 1d chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[13] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map," *Signal Processing*, vol. 143, pp. 122–133, 2018.

[14] S. S. Moafimadani, Y. Chen, and C. Tang, "A new algorithm for medical color images encryption using chaotic systems," *Entropy*, vol. 21, no. 6, p. 577, 2019.

[15] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.

[16] Y. Zhang and Y. Tang, "A plaintext-related image encryption algorithm based on chaos," *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 6647–6669, 2018.

[17] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 4653–4661, 2012.

[18] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[19] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3d chaotic baker maps," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

[20] H. M. Ghadirli, N. Ali, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing*, vol. 164, pp. 163–185, 2019.

[21] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and chaos," *Computers & Electrical Engineering*, vol. 92, pp. 6–16, 2017.

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

[23] C. Zhu, G. Wang, and K. Sun, "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1d chaotic maps," *Entropy*, vol. 20, no. 11, p. 843, 2018.

[24] Y. Xiong, C. Quan, and C. J. Tay, "Multiple image encryption scheme based on pixel exchange operation and vector decomposition," *Optics and Lasers in Engineering*, vol. 101, pp. 113–121, 2018.

[25] D. C. Mishra, R. K. Sharma, S. Suman, and A. Prasad, "Multi-layer security of color image based on chaotic system combined with RP2DFRFT and Arnold transform," *Journal of Information Security and Applications*, vol. 37, pp. 65–90, 2017.

[26] X. Chai, "An image encryption algorithm based on bit level brownian motion and new chaotic systems," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 1159–1175, 2017.

[27] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic-tent map," *Entropy*, vol. 21, no. 7, p. 656, 2019.

[28] Z. Hua, F. Jin, B. Xu, and H. Huang, "2d logistic-sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[29] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 22023–22043, 2019.

[30] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Information Sciences*, vol. 273, no. 8, pp. 329–351, 2014.

[31] X. Wang and H. Li Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 83, no. 1-2, pp. 333–346, 2016.

[32] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dynamics*, vol. 89, no. 1, pp. 61–79, 2017.

[33] A. Kassem, H. Al Haj Hassan, Y. Harkouss, and R. Assaf, "Efficient neural chaotic generator for image encryption," *Digital Signal Processing*, vol. 25, no. 2, pp. 266–274, 2014.

[34] A. Kulsoom, D. Xiao, S. A. Aqeel-ur-Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and dna complementary rules," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 1–23, 2016.

[35] Y. Xie, J. Yu, S. Guo, Q. Ding, and E. Wang, "Image encryption scheme with compressed sensing based on new three-dimensional chaotic system," *Entropy*, vol. 21, no. 9, p. 819, 2019.

[36] X. Li, Y. Jiang, M. Chen, and F. Li, "Research on iris image encryption based on deep learning," *EURASIP Journal on Image and Video Processing*, vol. 2018, no. 1, p. 126, 2018.

[37] J. Schuijers, J. P. Junker, M. Mokry et al., "Ascl2 acts as an R-spondin/wnt-responsive switch to control stemness in intestinal crypts," *Cell Stem Cell*, vol. 16, no. 2, pp. 158–170, 2015.

[38] N. Lu, P. Zhang, Q. Zhang et al., "Electric-field control of tri-state phase transformation with a selective dual-ion switch," *Nature*, vol. 546, no. 7656, pp. 124–128, 2017.

[39] H. Hu, L. Liu, and N. Ding, "Pseudorandom sequence generator based on the chen chaotic system," *Computer Physics Communications*, vol. 184, no. 3, pp. 765–768, 2013.

[40] Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, and J. Liu, "A chaotic map-control-based and the plain image-related cryptosystem," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2293–2310, 2016.

[41] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proceedings of the National Academy of Sciences*, vol. 88, no. 6, pp. 2297–2301, 1991.