Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 427349, 13 pages
http://dx.doi.org/10.1155/2014/427349

Research Article

An Efficient Diffusion Scheme for Chaos-Based Digital Image Encryption

Jun-xin Chen,[1] Zhi-liang Zhu,[2] Li-bo Zhang,[2] Chong Fu,[1] and Hai Yu[2]

[1] *School of Information Science and Engineering, Northeastern University, Shenyang 110004, China*
[2] *Software College, Northeastern University, Shenyang 110004, China*

Correspondence should be addressed to Zhi-liang Zhu; zhuzhiliang.sc@gmail.com

Received 14 November 2013; Revised 17 February 2014; Accepted 26 February 2014; Published 31 March 2014

Academic Editor: Jui-Sheng Lin

In recent years, amounts of permutation-diffusion architecture-based image cryptosystems have been proposed. However, the key stream elements in the diffusion procedure are merely depending on the secret key that is usually fixed during the whole encryption process. Cryptosystems of this type suffer from unsatisfactory encryption speed and are considered insecure upon known/chosen plaintext attacks. In this paper, an efficient diffusion scheme is proposed. This scheme consists of two diffusion procedures, with a supplementary diffusion procedure padded after the normal diffusion. In the supplementary diffusion module, the control parameter of the selected chaotic map is altered by the resultant image produced after the normal diffusion operation. As a result, a slight difference in the plain image can be transferred to the chaotic iteration and bring about distinct key streams, and hence totally different cipher images will be produced. Therefore, the scheme can remarkably accelerate the diffusion effect of the cryptosystem and will effectively resist known/chosen plaintext attacks. Theoretical analyses and experimental results prove the high security performance and satisfactory operation efficiency of the proposed scheme.

1. Introduction

With the rapid development of communication technologies, the utilization of visual content in addition to textual information becomes much more prevalent than the past. Cryptographic approaches are therefore critical for secure digital image storage and distribution over public networks. However, traditional data encryption algorithms such as Triple-DES, IDEA, AES, and other symmetric cryptographic algorithms are found poorly suited for digital images characterized with some intrinsic features such as high pixel correlation and redundancy [1].

The fundamental characteristics of chaotic systems, such as ergodicity and sensitivity to initial condition and control parameters, have attracted researchers' attention since such features can be considered analogous to the desired cryptographic properties. In 1998, Fridrich proposed the first general architecture for chaos-based image cryptosystems. This architecture is composed of two stages: permutation and diffusion [2]. In the first stage, pixels are shuffled by a two-dimensional area-preserving chaotic map to erase the high correlation between adjacent pixels. Then, pixel values are modified sequentially using a certain discretized one-dimensional chaotic map in the diffusion procedure. Fridrich's architecture has become the most popular structure and has been adopted in amounts of chaos-based image cryptosystems subsequently proposed [3–22]. In [3, 4], the 2D chaotic cat map and baker map are generalized to 3D for designing a real-time secure symmetric encryption scheme. The two approaches employ the 3D map to shuffle the positions of image pixels and use another chaotic map to confuse the relationship between the cipher image and plain image. In [5], Xiang et al. proposed a selective gray-level image encryption scheme, in which only 50% of the whole image data is encrypted, and therefore the encryption time is reduced. In [6], Wang et al. proposed a chaos-based image encryption algorithm with variable control parameters with the purpose to resist known/chosen plaintext attacks. In [7], Patidar et al. proposed an image cipher using two rounds of confusion and two rounds of diffusion. In the diffusion

phase, the vertical and horizontal diffusions are performed using standard map and logistic map, respectively. In [8], Fu et al. proposed an improved diffusion strategy named bidirectional diffusion to accelerate the spreading process and reduce the required diffusion rounds. An improved permutation-diffusion type image cipher was proposed in [9]. By the comprehensive utilization of the orbit-perturbing chaotic map, pixel swapping-based confusion approach, and the reverse direction diffusion innovation, a satisfactory security performance can be achieved with low computational complexity. In order to achieve larger key space and overcome the weak security in one-dimensional chaotic system, hyperchaotic systems were employed for image encryption in [10–12], and multichaotic systems or coupled nonlinear chaotic map was used in [13–17]. DNA encoding and balanced two-dimensional cellular automata are employed for image encryption to achieve enhanced security level and fast encryption speed in [18, 19], respectively. In [20–22], researchers developed the permutation procedure from the pixel level to bit level so as to achieve certain diffusion effects in the permutation stage.

As pointed out by many previous works, the diffusion procedure is the highest cost of the whole cryptosystem. This is because a considerable amount of computation load is devoted to the chaotic map iteration and quantization operation that is required for the key stream generation. Therefore, the critical issue of an efficient image cryptosystem is to reduce the required diffusion rounds. Moreover, Wang et al. pointed out that the same key stream may be used to encrypt different plain images if the secret key remains unchanged [6]. Opponents may crack the key stream [23] by known plaintext or chosen plaintext attacks, that is, by encrypting some special plain images (plain image with identical pixel values) and then comparing them with the corresponding ciphered images [24]. Therefore, to further enhance the security, the key stream elements extracted from the same secret key should better be distinct and related to the plain image. In this regard, Wang et al. proposed a chaos-based image encryption algorithm with variable control parameters, in which the key stream elements used for diffusion are related to the current processing plain pixels. Accordingly, different plain images result in distinct key streams, and hence the cryptosystem can effectively resist known/chosen plaintext attacks. However, approximately 50% more than required chaotic iterations have to be implemented to produce sufficient key stream elements in Wang's algorithm, and that downgrades the efficiency of the cryptosystem.

In order to accelerate the diffusion effect of permutation-diffusion type image cryptosystems and further enhance the security performance, we propose a more efficient diffusion scheme. The novel scheme consists of two relevant diffusion procedures in one overall encryption round. A supplementary diffusion module is padded after the normal diffusion procedure, in which the control parameter of the chaotic map will be altered by the resultant image generated after the normal diffusion operation. This scheme can make full use of the chaotic system's sensitivity to control parameters, as the slight difference in the image can be transferred to the chaotic iteration and then brings about distinct key streams even though the same secret keys are applied. Therefore, totally different cipher images will be produced and hence the spreading effect of the cryptosystem will be remarkably accelerated. Besides, as the key stream elements produced in the supplementary diffusion stage not only depend on the secret key but also the plain image, different key streams will be produced when ciphering different plain images. Accordingly, opponents cannot obtain any clues about the secret key by launching chosen/known plaintext attacks, and the cryptosystem can resist known/chosen plaintext attacks effectively. Experimental results demonstrate that the proposed diffusion scheme has a high level of security and satisfactory encryption speed for practical secure image applications.

The remaining of this paper is organized as follows. In the next section, the architecture of permutation-diffusion type image cryptosystems is described. Then, the proposed diffusion strategy for image encryption is given in detail in Section 3. Simulation results and the effectiveness and efficiency of the proposed scheme are reported in Section 4, while the security analyses are addressed in Section 5. Finally, conclusions will be drawn in the last section.

2. Architecture of Permutation-Diffusion Type Image Cryptosystems

The architecture of permutation-diffusion type chaos-based image cryptosystems [6] is shown in Figure 1. There are two stages in this type of cryptosystems, namely, the permutation stage and diffusion stage.

In the permutation stage, image pixels are generally shuffled by a two-dimensional area-preserving chaotic map, without any modification to their values. Traditionally, three types of chaotic maps, Arnold cat map, baker map, and standard map, are applied and their discretized versions are given by, respectively [2],

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod N, \tag{1}$$

$$x_{i+1} = \frac{N}{n_j}\left(x_i - N_j\right) + y_i \bmod \frac{N}{n_j},$$

$$y_{i+1} = \frac{k_j}{N}\left(y_i - y_i \bmod \frac{N}{n_j}\right) + N_j,$$

$$\text{with} \quad n_0 + n_1 + \cdots + n_t = N,$$

$$N_j = n_0 + n_1 + \cdots + n_j, \tag{2}$$

$$0 \le y_i \le N,$$

$$N_j \le x_i \le N_j + n_{j+1},$$

$$0 \le j \le t-1,$$

$$n_0 = 0,$$

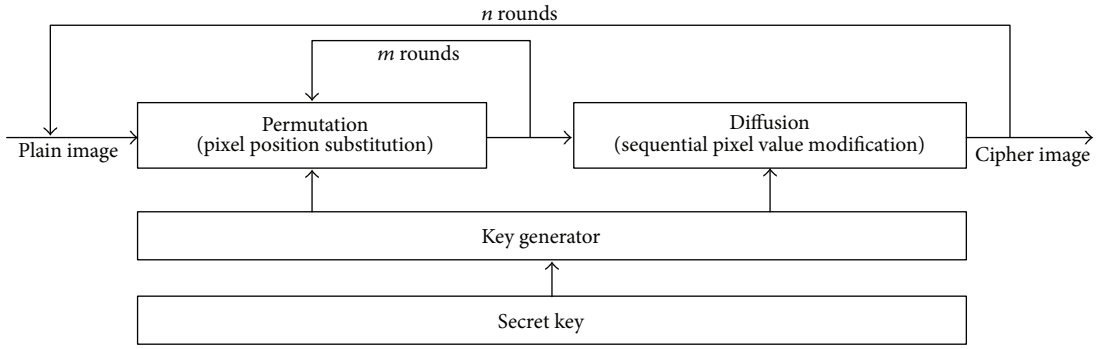
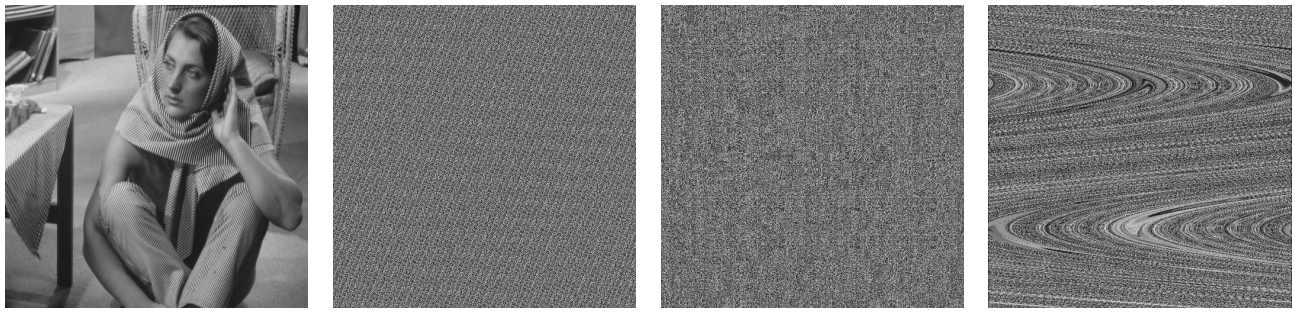


Figure 1: Architecture of permutation-diffusion type image cryptosystems.



(a) (b) (c) (d)

Figure 2: Confused images using different permutation approaches: (a) plain image, (b) confused image with 3-round cat map, (c) confused image with 3-round baker map, and (d) confused image with 3-round standard map.

$$x_{i+1} = (x_i + y_i) \bmod N,$$
$$y_{i+1} = \left(y_i + K \sin \frac{x_{i+1} N}{2\pi}\right) \bmod N, \tag{3}$$

where N is the width or height of the square image, (x_i, y_i) and (x_{i+1}, y_{i+1}) are the original and the permuted pixel position, and (p, q), n_j $(j = 1, 2, \ldots, t-1)$, and K are control parameters of the three maps, respectively. All pixels are scanned sequentially from left to right and top to bottom.

Figure 2 shows the confused images using 3-round cat map, baker map, and standard map, respectively. The test image is the standard 256 gray scale Barb image with size of 512×512.

In the diffusion stage, pixel values are modified sequentially by mixing with the key stream elements that are generated by a one-dimensional chaotic map. Generally, the modification to one particular pixel depends not only on the corresponding key stream element but also on the accumulated effect of all the previous pixel values [25], as described by

$$c(n) = k(n) \oplus p(n) \oplus c(n-1), \tag{4}$$

where $p(n)$, $k(n)$, $c(n)$, and $c(n-1)$ represent the current plain pixel, key stream element, output cipher-pixel and the previous cipher-pixel, respectively. Such diffusion algorithm can spread a slight difference in the plain image to large scale pixels in the ciphered image and thus differential attack may be practically useless. Additionally, to cipher the first pixel, $c(-1)$ has to be set as a seed. In general, $k(n)$, the key stream element, can be obtained from the current state of the chaotic map iteration [8] according to

$$k(n) = \bmod \left[\text{floor}\left(\left(\frac{x(n)+1}{2}\right) \times 10^{14}\right), \text{Grey}\right], \tag{5}$$

where $\bmod[a, b]$ means a modulo b and the outcome is the remainder of the Euclidean division of a by b, $\text{floor}(x)$ returns the value nearest integers less than or equal to x, and Grey is the gray level of the plain image.

In the present paper, chaotic logistic map [25] is employed as the key stream generators, and the mathematical formula is defined as

$$x(n+1) = \mu \times x(n) \times (1 - x(n)), \tag{6}$$

where μ and x_n are the control parameter and state value, respectively. If one chooses $\mu \in [3.57, 4]$, the system is chaotic. The initial value x_0 and control parameter μ can be combined as the secret key. Note that there exist some periodic (nonchaotic) windows in chaotic region of logistic map. To address this problem, values correspond to positive Lyapunov exponents should be selected for parameter μ, so as to keep the effectiveness of the cryptosystem.

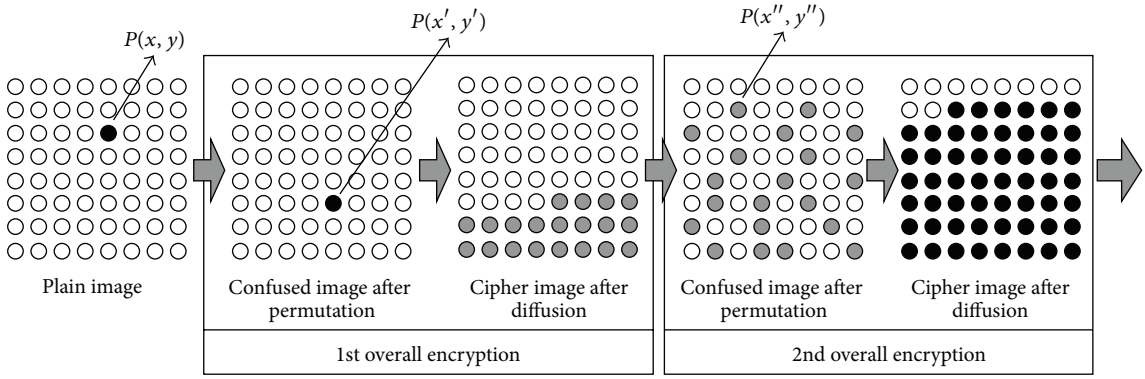


Figure 3: Diffusion process of traditional image cryptosystems.

3. An Efficient Diffusion Scheme for Image Encryption

As pointed out by many previous works, an efficient image cipher should spread a minor change in the plain image to the whole cipher image in order to resist differential attack. Opponents usually make a slight change (e.g., change one pixel) of the plain image and then obtain some clues of the keys by comparing the difference of cipher images. Therefore, if the change in the plain image can spread out to larger scale pixels in the cipher image, the attacker will be unable to find out any valuable clues about the keys. Two performance indices, NPCR (number of pixels change rate) and UACI (unified average changing intensity), are utilized to measure the influence of one pixel change in plain image on the entire cipher image. Suppose that $P_1(i, j)$ and $P_2(i, j)$ are the (i, j)th pixel of two images P_1 and P_2, respectively; NPCR is defined as

$$\mathrm{NPCR} = \frac{\sum_i \sum_j D(i, j)}{W \times H} \times 100\%, \tag{7}$$

where W and H are the width and length of P_1 and P_2 and $D(i, j)$ is

$$D(i, j) = \begin{cases} 0, & \text{if } P_1(i, j) = P_2(i, j), \\ 1, & \text{if } P_1(i, j) \neq P_2(i, j). \end{cases} \tag{8}$$

Assume that L is the gray level of the two images; the index UACI is defined as

$$\mathrm{UACI} = \frac{1}{W \times H} \left[\sum_i \sum_j \frac{|P_1(i, j) - P_2(i, j)|}{L - 1} \right] \times 100\%. \tag{9}$$

From the above two mathematical formulas, we can draw the conclusion that NPCR is used to measure the spreading scale, whereas UACI is the measurement of the spreading degree. For a 256 gray-level image, the expected NPCR and UACI values are 99.61% and 33.46%, respectively [8]. The diffusion performance can be regarded as an essential factor for the efficiency and security of an image cryptosystem.

3.1. Diffusion Effect Analysis of Traditional Image Cryptosystems. In this section, the diffusion effect of the traditional permutation-diffusion type image cryptosystems is analyzed theoretically and experimentally. In the present paper, the plain image and the encrypted image with the size of $N \times N$ are viewed as two-dimensional matrices, and the coordinates of the pixels are between $(0, 0)$ and $(N - 1, N - 1)$ from the upper-left corner to the lower-right corner.

Traditional diffusion algorithm, as described by (4), which makes the modification to one particular pixel, depends on not only the corresponding key stream element but also on the previous cipher-pixel value. As a result, a tiny change in one pixel can spread out to all the subsequent pixels, as illustrated by Figure 3.

Without loss of generality, we assume that the differential pixel is at (x, y). After the permutation in the first encryption round, the pixel is shuffled to (x', y'). Through the first round diffusion operation, the difference will spread out to all pixels subsequent to (x', y'). Next in the second encryption round, the different pixels produced in the first round are scattered to a wider scale after the permutation procedure, and the difference ratio is greatly broadened to (x'', y'') after the second round encryption. With several overall rounds encryption, the tiny difference can be spread out to the whole cipher image. In general, 3-4 overall rounds are required to achieve a satisfactory security performance.

We can now infer from the above analysis that two features of the spreading process may exist in the first encryption round.

(1) *Spreading scale*. The difference will spread out to all pixels subsequent to (x', y') certainly. This is because for each pixel value's masking operation subsequent to the (x', y'), $p(n)$ and $k(n)$ keeps the same, whereas $c(n - 1)$ is different, and hence the outcome of (4) will be different. Therefore, a satisfactory NPCR can be obtained in the first encryption round.

(2) *Spreading degree*. As the new pixel value is obtained by exclusive-OR (XOR) operation, the modification to one bit cannot influence the outcome in other bits according to the mathematical calculations. Therefore, the difference will be fixed on the corresponding

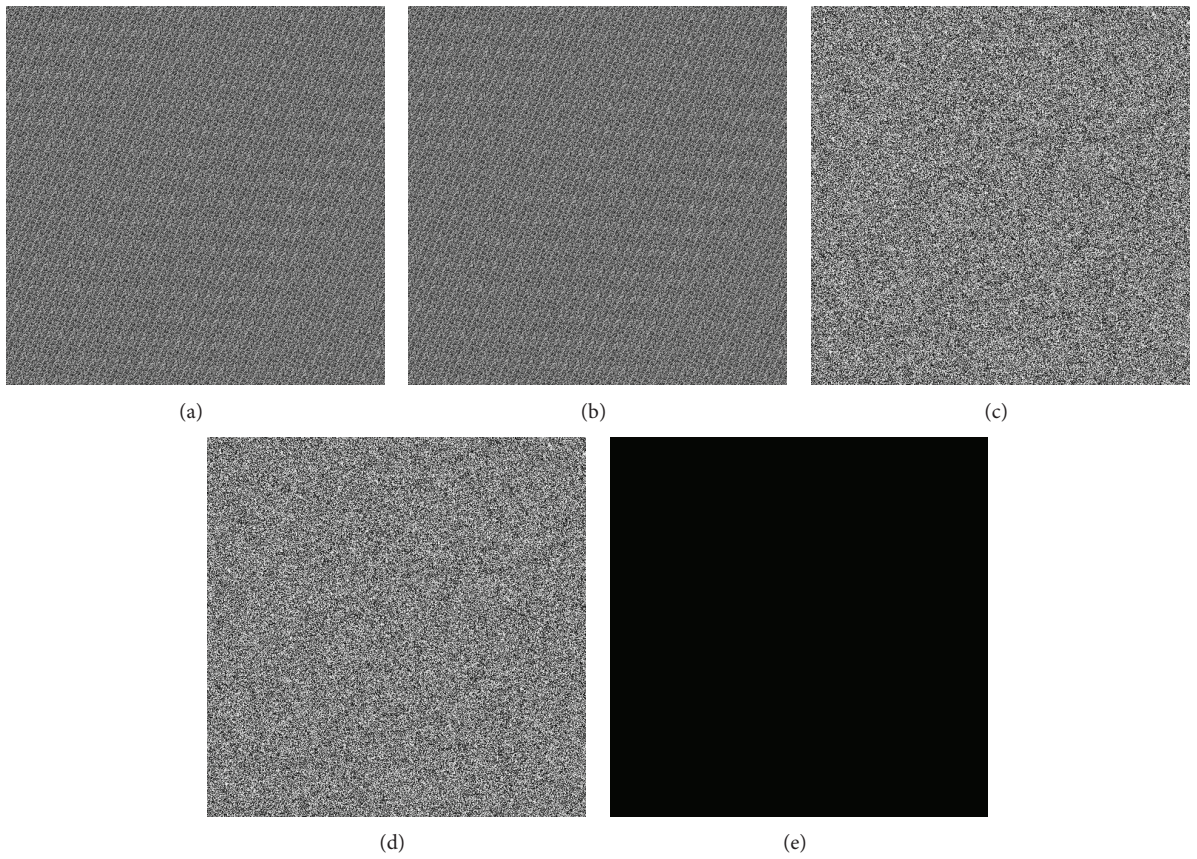


Figure 4: Simulation results of the diffusion effect (i): (a) confused image of Barb using 3-round cat map, (b) modified version of (a), (c) output image of (a) after diffusion, (d) output image of (b) after diffusion, and (e) differential image of (c) and (d).

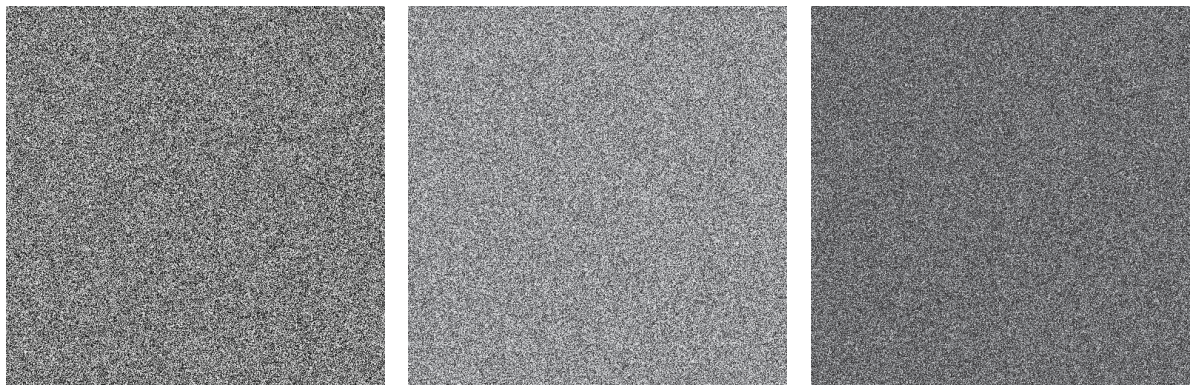
differential bit coordinate. For example, if the difference locates at the last bit of the pixel, the difference between the resultant pixel values will be either 1 or −1. Accordingly, UACI in the first encryption round will be much more disappointed than expected.

Simulations have been performed to testify the theses mentioned above. In order to better represent the spreading effect of the diffusion procedure, two relevant shuffled images are directly applied as the inputs of the diffusion module. The first one is the confused image of Barb using 3-round cat map, whereas the other one is the modified version obtained by changing the last bit of the first pixel from 0 to 1. Chaotic logistic map with coefficients ($x_0 = 0.3, \mu = 3.999$) is used as key stream generator. The input images, output images, and their differential image are shown in Figure 4.

Based on precise numerical calculations using Matlab R2010a, the differential ratio of the corresponding pixels between Figures 4(c) and 4(d) is 100%, which means that all the pixels at the same position have different grey values. On the other hand, the pixel values of the differential image are either 1 or −1 according to our mathematical analysis, with the proportion of 1 and −1 being 49.94% and 50.06%, respectively. The NPCR and UACI between the two output images are 100% and 0.39%, respectively. This result proves the two above-mentioned features convincingly.

According to (4) and previous analyses, as there is only one differential variable in the formula and hence the spreading degree keeps on a lightweight degree, in this regard, another experiment has been carried out to investigate the diffusion performance when the key stream elements are changed simultaneously. Figures 4(a) and 4(b) are also used as the input images, while the key stream used for ciphering Figure 4(a) is extracted from a logistic map with coefficients ($x_0 = 0.3, \mu = 3.999$). On the other hand, the key stream applied for Figure 4(b)'s encryption is produced by the logistic map with coefficients ($x_0 = 0.3, \mu = 3.9990000000001$). The two output images and their differential image are depicted in Figure 5.

Based on numerical calculations using Matlab, the NPCR and UACI are 99.61% and 33.41%, respectively. Both of the two performance indices are very close to the expected values. Therefore, two output images can be viewed as two random ones and there are no statistical correlations between them. The slight difference in the plain images has spread out to the whole image. Opponents cannot obtain any clues by comparing such two output images, and hence the cryptosystem can resist known/chosen plaintext attacks effectively. Therefore, it is of great significance to investigate how to



(a) (b) (c)

Figure 5: Simulation results of the diffusion effect (ii): (a) output image of Figure 4(a), (b) output image of Figure 4(b), and (c) differential image of (a) and (b).

make the difference in the input image transferred to the chaotic iteration so as to produce distinct key stream elements and hence obtain satisfactory diffusion performance at an early age.

3.2. Continuous Diffusion with a Control Parameter Perturbing Mechanism. In this section, we propose a novel diffusion scheme named continuous diffusion that can accelerate the spreading effect remarkably. The proposed diffusion scheme can collaborate with any chaotic maps that are used as key stream generator for diffusion, and logistic map is employed as an example for illustrating the proposed scheme clearly.

Different from the traditional diffusion strategies, the proposed diffusion scheme consists of two relevant diffusion procedures with the normal diffusion module being unchanged and a supplementary diffusion procedure padded next. In the normal diffusion stage, plain pixel values are modified sequentially by the logistic map with the chosen parameters (x_0, μ). So, the difference will spread out to all the pixels from (x', y') to the last pixel, the same as the spreading process in the traditional diffusion procedure. Then, in the supplementary diffusion stage, the control parameter μ of the logistic map is altered by $C_1(N-1, N-1)$, the last pixel of the resultant image produced by the first diffusion stage. Through this mechanism, the slight spreading effect produced in the normal diffusion procedure will be introduced to the chaotic map, and hence result in totally different key streams due to its high sensitivity to the control parameter. Therefore, the difference will spread out to the whole cipher image and bring about totally different cipher images, and hence a satisfactory diffusion effect is obtained, as shown in Figure 6.

In our scheme, the control parameter μ of the logistic map is altered according to

$$\mu' = \mu \pm L \times \Delta, \tag{10}$$

where L is the grey value of $C_1(N-1, N-1)$ and Δ is the basic perturbation unit. Δ should be set properly to make sure that at least one outcome of (10) falls within the chaotic region, and the usage of "±" is for the same purpose. We prefer that the orbit value is increasing progressively for logistic map. That means that μ' is preferred producing according to

$$\mu' = \mu + L \times \Delta, \tag{11}$$

whereas if the calculated $\mu' > 4$, the orbit perturbing formula will change to

$$\mu' = \mu - L \times \Delta. \tag{12}$$

Note that, for deciphering smoothly, key stream element used for ciphering the last pixel in the supplementary diffusion stage has to be generated by the given parameter "μ" rather than the perturbed control parameter. Therefore, totally, $N \times N + 1$ key stream elements have to be generated by the given parameter "μ," with the previous $N \times N$ elements being required in the first diffusion stage and the last one used for ciphering the last pixel in the supplementary diffusion procedure.

The detailed process of above proposed that diffusion scheme is described as follows.

Step 1. Iterate (6) for N_0 times continuously to avoid the harmful effect of transitional procedure, where N_0 is a constant.

Step 2. The logistic map is iterated for $N \times N + 1$ times continuously. With each of the iteration, we can get one key stream element from the current state value according to (5).

Step 3. Calculate the cipher-pixel value sequentially according to (4). One may set an initial value $c(-1)$ as a seed.

Step 4. Alter the control parameter "μ" of the logistic map referring to (10).

Step 5. Iterate the logistic map for $N \times N - 1$ times continuously with the modified control parameter produced in Step 4, and get the corresponding key stream elements according to (5).

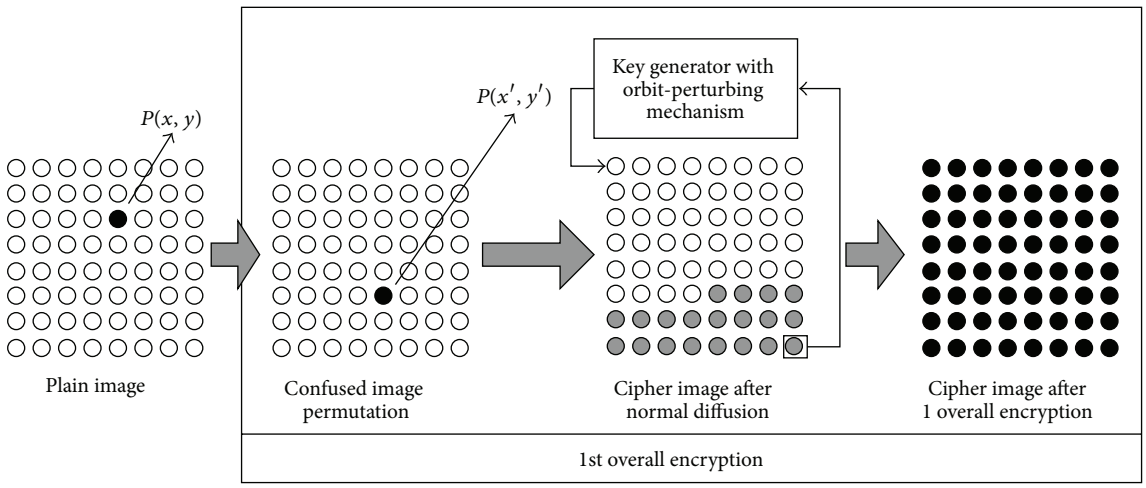


Figure 6: The proposed image diffusion scheme.

Table 1: Testing results when using cat map.

Test	1 round		2 rounds		3 rounds		4 rounds	
Items	Proposed	Wang's	Proposed	Wang's	Proposed	Wang's	Proposed	Wang's
NPCR	**99.61%**	50.51%	99.62%	**99.61%**	99.62%	99.60%	99.60%	99.61%
UACI	**33.41%**	16.86%	33.51%	**33.47%**	33.46%	33.45%	33.51%	33.48%
Times (ms)	**7.8**	6.7	15.6	**13.4**	23.4	20.1	26.8	31.2

Step 6. Except the last one, modify the pixel values sequentially by (4), using the key stream elements produced in Step 5.

Step 7. Encrypt the last pixel in supplementary diffusion stage using the last key stream element produced in Step 2.

Note that when other chaotic maps are applied for key stream generation, the control parameter perturbing operation could be implemented referring to that of the logistic map described above. Besides, any 2D or higher dimensional discretized chaotic maps can be employed for image permutation and collaborated with the proposed diffusion scheme.

4. Simulation Results

In this section, simulation results are given out to demonstrate the efficiency and the effectiveness of the proposed diffusion scheme in comparison with Wang's algorithm in [6]. A number of tests have been carried out with different permutation strategies and numbers of encryption rounds, using the standard 256 gray scale Barb image with size of 512×512. NPCR and UACI are computed to measure the influence of a plain pixel change on the entire cipher image. The consumption time is measured by running the standard C program in our computing platform, a personal computer with an Intel(R) Core(TM) i5 CPU (2.27 GHZ), 2 GB memory, and 320 GB hard-disk capacity. Chaotic logistic map with coefficients ($x_0 = 0.3, \mu = 3.999$) is employed for key stream elements generation in the diffusion stage. The basic perturbation unit Δ used for simulation is taken as 10^{-15}, which is the computational precision of the 64-bit double-precision number according to the IEEE floating-point standard [26]. Tables 1, 2, and 3 list the simulation results of cryptosystems with the cat map, baker map, and standard map adopted for image permutation, respectively. The permutation round is $m = 3$.

As demonstrated in the tables, to achieve a satisfactory security level such as NPCR > 99.60% and UACI > 33.4%, only one overall round is required when using the proposed diffusion scheme no matter what technique is applied for permutation. However, such satisfactory security performance will be produced after the second encryption round when using Wang's algorithm. Compared with Wang's scheme, at least 40% of the encryption time can be saved even though a little more time is needed in one overall round due to the computation in the supplementary diffusion procedure. The significant acceleration in encryption speed is due to the reduction of the encryption rounds, and thus the encryption efficiency is more satisfactory. Besides, as the key stream elements produced in our diffusion stage are decided not only by the secret key but also by the plain image, different plain images can result in distinct key stream elements, and this advantage ensures the robustness against known/chosen plaintext attacks of the proposed scheme.

5. Security Analysis

In this section, image cryptosystems based on the proposed diffusion scheme and various permutation strategies are analyzed versus different security performances.

Table 2: Testing results when using baker map.

Test	1 round		2 rounds		3 rounds		4 rounds	
Items	Proposed	Wang's	Proposed	Wang's	Proposed	Wang's	Proposed	Wang's
NPCR	**99.60%**	51.02%	99.61%	**99.61%**	99.62%	99.60%	99.61%	99.62%
UACI	**33.44%**	16.91%	33.47%	**33.49%**	33.51%	33.46%	33.48%	33.49%
Times (ms)	**68.8**	67.2	137.6	**134.4**	206.4	201.6	275.2	268.8

Table 3: Testing results when using standard map.

Test	1 round		2 rounds		3 rounds		4 rounds	
Items	Proposed	Wang's	Proposed	Wang's	Proposed	Wang's	Proposed	Wang's
NPCR	**99.59%**	49.87%	99.61%	**99.61%**	99.60%	99.61%	99.63%	99.60%
UACI	**33.43%**	16.75%	33.48%	**33.46%**	33.48%	33.48%	33.52%	33.46%
Times (ms)	**103.4**	101.8	206.8	**203.6**	310.2	305.4	413.6	407.2

5.1. Key Space Analysis. The key space is the total number of different keys that can be used in a cryptosystem, and the key space should be sufficiently large to make brute-force attack infeasible. For permutation-diffusion type image cryptosystems, the secret key consists of two parts: permutation key key_p and diffusion key key_d. According to the IEEE floating-point standard [26], the computational precision of the 64-bit double-precision number is about 10^{-15}. For logistic map, x_0 can be any number among those 10^{15} possible values and μ can be any one of $(4 - 3.57) \times 10^{15}$ possible values, so the total key space of the diffusion module is

$$\text{key}_d = 10^{15} \times 0.43 \times 10^{15} = 0.43 \times 10^{30} \approx 2^{98}. \quad (13)$$

Throughout the previous works, the key space of the cat map with permutation round $m = 3$, baker map and standard map are approximately 2^{54}, 2^{418}, and 2^{63}, respectively. Therefore, the total key spaces of the image cryptosystems based on corresponding chaotic maps are 2^{152}, 2^{516}, and 2^{161}, respectively, and hence are sufficiently large to make brute force infeasible.

5.2. Key Sensitivity Test. The key sensitivity of a cryptosystem can be observed in the following two aspects: (i) completely different cipher images should be produced when using slightly different keys to encrypt the same plain image and (ii) the cipher image cannot be correctly decrypted even though there is slight difference between the encryption and decryption keys.

The following key sensitivity tests have been performed to evaluate the key sensitivity in the first case.

(1) The plain image Barb is firstly encrypted with the chosen coefficients ($x_0 = 0.3, \mu = 3.999$) for logistic map and certain permutation map, and *cipher-barb* image is produced.

(2) The initial value x_0 is changed from 0.3 to $0.3 + 10^{-14}$ while μ is kept unchanged, and then performs the encryption again, and the resultant image is represented as *cipher-barb2*.

Table 4: Key sensitivity test (i).

Permutation approaches	Difference between *cipher-barb* and *cipher-barb2*	Difference between *cipher-barb* and *cipher-barb3*
Cat map	99.59%	99.60%
Baker map	99.59%	99.61%
Standard map	99.62%	99.61%

(3) The control parameter μ is changed from 3.999 to $3.999 + 10^{-14}$, while x_0 remain 0.3, then encrypt the plain image again, and get the image *cipher-barb3*.

(4) Compute the difference between the original cipher image obtained in step (1) and the cipher images produced in steps (2) and (3).

(5) Repeat the above steps using different permutation strategies.

The testing results when using cat map, baker map, and standard map are listed in Table 4. The corresponding cipher images using cat map for permutation and the differential images are depicted in Figure 7. The results obviously show that the cipher images exhibit no similarity between one another and there is no significant correlation that could be observed from the differential images.

In addition, decryption operations using different keys with slight changes also have been performed in order to evaluate the key sensitivity in the second case.

(1) Barb is firstly encrypted with the chosen coefficients ($x_0 = 0.3, \mu = 3.999$) for logistic map and certain permutation chaotic map, and *cipher-barb* is obtained.

(2) Decrypt the *cipher-barb* with x_0 being changed to $0.3 + 10^{-14}$ while μ remained unchanged, and the decrypted image is represented as *decipher-barb2*.

(3) Decrypt the *cipher-barb* with the control parameter μ varied to $3.999 + 10^{-14}$, while x_0 remain at 0.3, and then get the *decipher-barb3*.

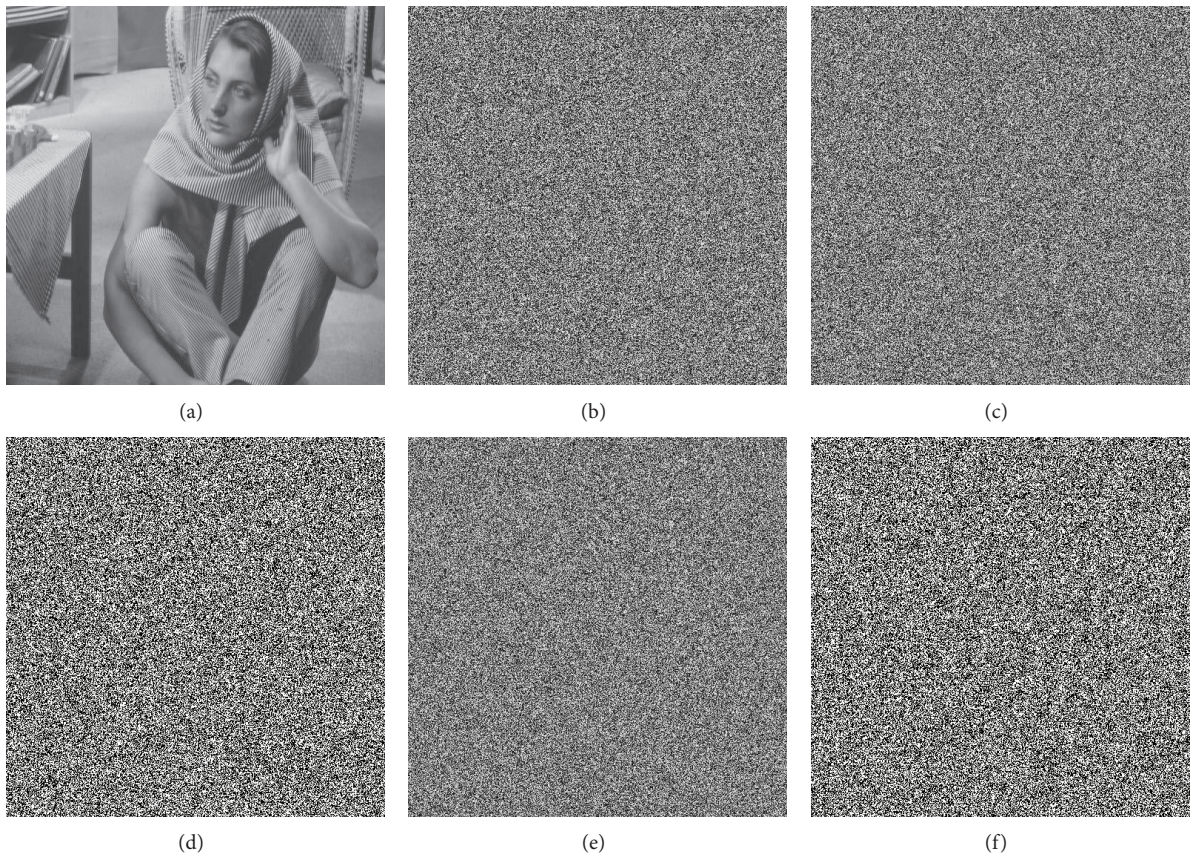


Figure 7: Key sensitivity test (i) using cat map for permutation: (a) plain image, (b) cipher image ($x_0 = 0.3, \mu = 3.999$), (c) cipher image ($x_0 = 0.30000000000001, \mu = 3.999$), (d) differential image between (b) and (c), (e) cipher image ($x_0 = 0.3, \mu = 3.99900000000001$), and (f) differential image between (b) and (e).

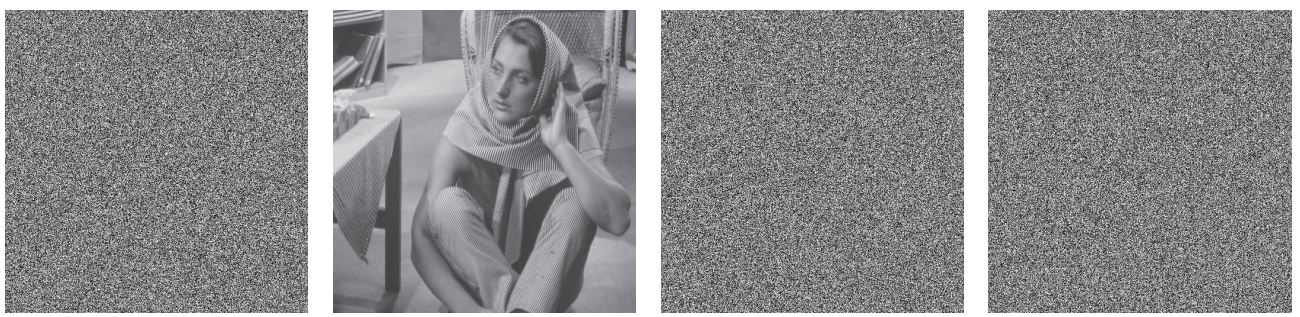


Figure 8: Key sensitivity test (ii) using cat map for permutation: (a) cipher image ($x_0 = 0.3, \mu = 3.999$), (b) plain image, (c) decipher image ($x_0 = 0.30000000000001, \mu = 3.999$), and (d) decipher image ($x_0 = 0.3, \mu = 3.99900000000001$).

(4) Compute the difference between the plain image Barb and the decipher images produced in steps (2) and (3).

(5) Repeat the above steps using different permutation techniques.

The simulation results when using cat map, baker map, and standard map are listed in Table 5. The corresponding decipher images using cat map for permutation are illustrated by Figure 8. The results obviously show that the cipher images exhibit no similarity between one another and there is no significant correlation that could be observed from the differential images.

The above two tests prove that the proposed image diffusion scheme is highly sensitive to the secret key. Even an almost perfect guess of the key does not reveal any valuable information about the cryptosystem and hence differential attack would become inefficient and practically useless.

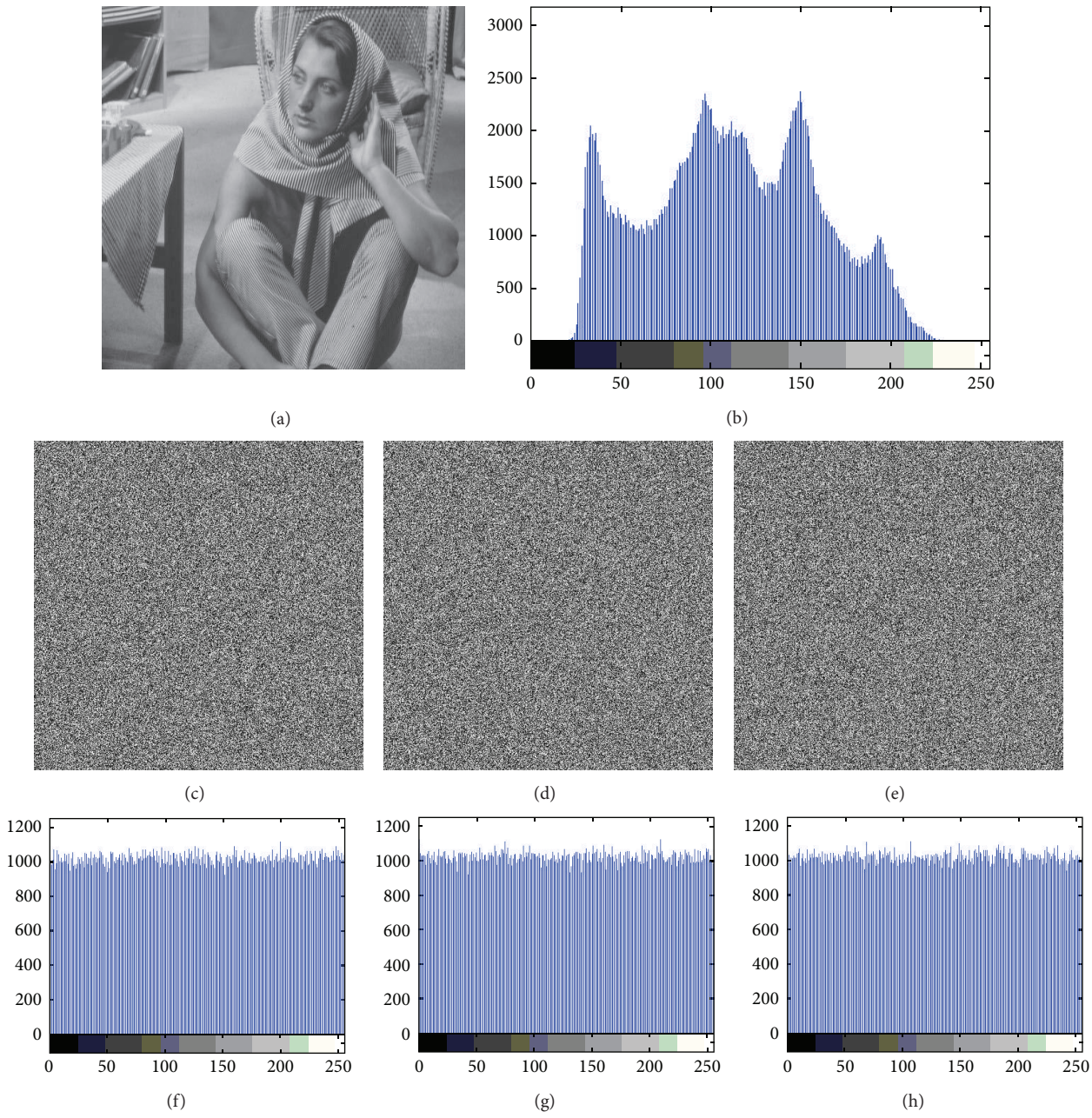


Figure 9: Histograms analysis: (a) plain image, (b) histogram of plain image, (c) cipher image using cat map, (d) cipher image using baker map, (e) cipher image using standard map, (f) histogram of (c), (g) histogram of (d), and (h) histogram of (e).

5.3. Statistical Analysis

5.3.1. Histogram Analysis. Histogram of an image demonstrates the distribution of the pixel values by plotting the number of pixels at each gray scale level. The histogram of an effectively ciphered image should be uniform and significantly different from that of the plain image so as to prevent the attacker from obtaining any useful statistical information. The histograms of the plain image and its cipher images produced by the image cryptosystems based on the proposed diffusion scheme and different permutation strategies are depicted in Figure 9. It is obvious that the histograms of the encrypted images are uniformly distributed and quite different from those of the plain image, which implies that the redundancy of the plain image is successfully hidden after the encryption and consequently does not provide any clue to apply statistical attacks.

5.3.2. Correlation of Adjacent Pixels. For an ordinary image with meaningful visual content, each pixel is highly correlated with its adjacent pixels in horizontal, vertical, and diagonal

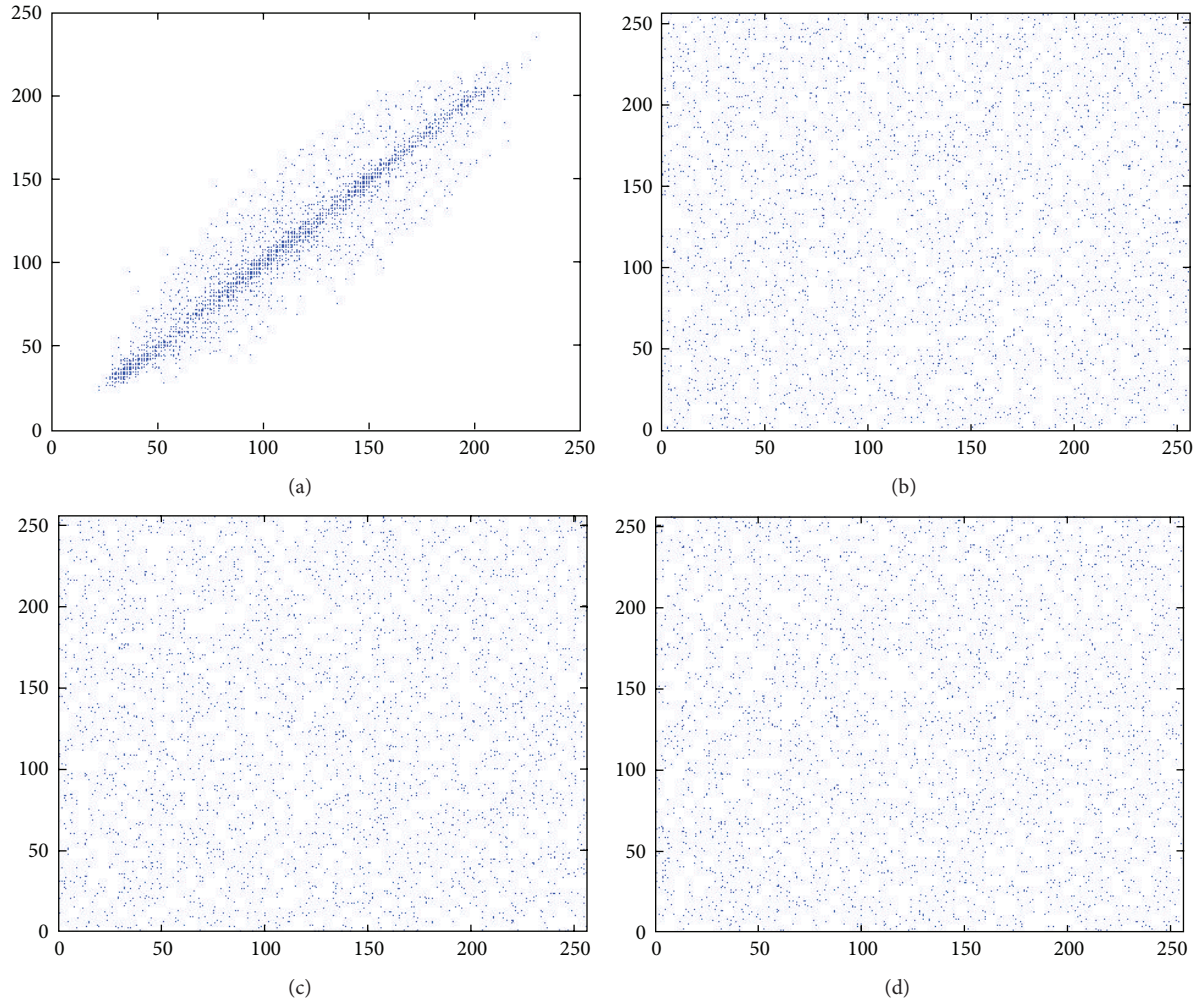


Figure 10: Correlation of two horizontally adjacent pixels: (a) correlation of the plain image, (b) correlation of the cipher image using cat map, (c) correlation of the cipher image using baker map, and (d) correlation of the cipher image using standard map.

direction. An effective cryptosystem should produce a cipher image with sufficiently low correlation between the adjacent pixels. To test this, 3000 pairs of adjacent pixels of the plain image and the cipher image are randomly selected from the horizontal, vertical, and diagonal direction, respectively. The correlation coefficient r_{xy} of each pair is calculated according to the following three formulas:

$$r_{xy} = \frac{E\left(x - E\left(x\right)\right)\left(y - E\left(y\right)\right)}{\sqrt{D\left(x\right)}\sqrt{D\left(y\right)}},$$

$$E\left(x\right) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{14}$$

$$D\left(x\right) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E\left(x\right)\right)^2,$$

Table 5: Key sensitivity test (ii).

Permutation approaches	Difference between Barb and *decipher -barb2*	Difference between Barb and *decipher-barb3*
Cat map	99.62%	99.59%
Baker map	99.60%	99.63%
Standard map	99.61%	99.59%

where x_i and y_i are gray-level values of the ith pair of the selected adjacent pixels and N represents the total number of the samples. The correlation coefficients of adjacent pixels in Barb image and its cipher images are listed in Table 6. The correlation distributions of two horizontally adjacent pixels in the plain image and the cipher images using various permutation chaotic maps are shown in Figure 10. Both the calculated correlation coefficients and the figures can substantiate that the strong correlation among the neighboring pixels of a plain

Table 6: Correlation coefficients of two adjacent pixels in the plain and cipher images.

	Correlation of plain image	Correlation of cipher images		
		Cat map	Baker map	Standard map
Horizontal	0.9565	0.0023	−0.0056	0.0015
Vertical	0.8617	−0.0057	−0.0023	−0.0018
Diagonal	0.8396	−0.0013	0.0036	0.0023

Table 7: Entropies of plain images and cipher images.

	Entropies of plain images	Entropies of cipher images		
		Cat map	Baker map	Standard map
Lena	7.445568	7.999370	7.999424	7.999413
Baboon	7.357949	7.999356	7.999189	7.999342
Barb	7.466426	7.999305	7.999335	7.999355
Bridge	5.705560	7.999287	7.999297	7.999305
Peppers	7.571478	7.999351	7.999378	7.999371

image can be decorrelated by using the proposed encryption scheme effectively.

5.3.3. Information Entropy. Entropy is a significant property that reflects the randomness and the unpredictability of an information source; it was firstly proposed by Shannon in 1949 [27]. The entropy $H(s)$ of a message source s is defined as

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i), \tag{15}$$

where s is the source, N is the number of bits to represent the symbol s_i, and $P(s_i)$ is the probability of the symbol s_i. For a truly random source consisting of 2^N symbols, the entropy is N. Therefore, for a secure cryptosystem, the entropy of the cipher image having 256 gray levels should ideally be 8. Otherwise, the information source is not sufficiency random and there exists a certain degree of predictability for breaking the cryptosystem.

Five 256 gray scale test images with size 512 × 512 are encrypted for 1 round and the information entropies are then calculated, as listed in Table 7. It is obvious that the entropies of the cipher images are very close to the theoretical value of 8, which means that information leakage in the encryption procedure is negligible and the proposed algorithm is secure against entropy analysis.

6. Conclusions

In the present paper, an efficient diffusion scheme is proposed to address the efficiency and security flaws of the traditional permutation-diffusion type image cryptosystems. Our diffusion scheme consists of two relevant diffusion procedures in one overall round encryption. The first one is the same as the normal diffusion module, whereas, in the supplementary diffusion procedure, the control parameter of the selected chaotic map is altered by the resultant image generated after the first diffusion operation. This scheme makes full use of the sensitivity property of the chaotic systems, and a slight difference in the image can be transferred to the chaotic map iteration and then brings about totally different key stream elements. Through this mechanism, the spreading effect of the cryptosystem can be significantly accelerated in the supplementary diffusion procedure and the cryptosystem can resist chosen/known plaintext attacks effectively. Experimental results have proved the higher efficiency and the security level of the proposed scheme. These improvements can motivate the practical applications of permutation-diffusion architecture chaos-based image cryptosystems.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. 61271350, 61374178, and 61202085), the Fundamental Research Funds for the Central Universities (no. N120504005), the Liaoning Provincial Natural Science Foundation of China (no. 201202076), the Specialized Research Fund for the Doctoral Program of Higher Education (no. 20120042120010), and the Ph.D. Start-up Foundation of Liaoning Province, China (Nos. 20111001, 20121001, and 20121002).

References

[1] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images and videos," in *Multimedia Security Handbook*, chapter 4, pp. 133–167, CRC Press, 2005.

[2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.

[3] G. R. Chen, Y. B. 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.

[4] Y. B. Mao, G. R. Chen, and S. G. Lian, "A novel fast image encryption scheme based on 3D chaotic Baker maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 14, no. 10, pp. 3613–3624, 2004.

[5] T. Xiang, K. W. Wong, and X. F. Liao, "Selective image encryption using a spatiotemporal chaotic system," *Chaos*, vol. 17, no. 2, Article ID 023115, 2007.

[6] Y. Wang, K. W. Wong, X. F. Liao, T. Xiang, and G. R. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1773–1783, 2009.

[7] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.

[8] C. Fu, J. J. Chen, H. Zou, W. H. Meng, Y. F. Zhan, and Y. W. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Optics Express*, vol. 20, no. 3, pp. 2363–2378, 2012.

[9] J. X. Chen, Z. L. Zhu, C. Fu, and H. Yu, "An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism," *Optics Express*, vol. 21, no. 23, pp. 27873–27890, 2013.

[10] F. Y. Sun, S. T. Liu, and Z. W. Lü, "Image encryption using high-dimension chaotic system," *Chinese Physics*, vol. 16, no. 12, pp. 3616–3623, 2007.

[11] Y. S. Zhang, D. Xiao, Y. L. Shu, and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations," *Signal Processing: Image Communication*, vol. 28, no. 3, pp. 292–300, 2013.

[12] T. G. Gao and Z. Q. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.

[13] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Optics Communications*, vol. 282, no. 11, pp. 2123–2127, 2009.

[14] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[15] A. N. Pisarchik and M. Zanin, "Image encryption with chaotically coupled chaotic maps," *Physica D: Nonlinear Phenomena*, vol. 237, no. 20, pp. 2638–2648, 2008.

[16] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," *Chaos, Solitons & Fractals*, vol. 42, no. 3, pp. 1745–1754, 2009.

[17] Y. Cao, "A new hybrid chaotic map and its application on image encryption and hiding," *Mathematical Problems in Engineering*, vol. 2013, Article ID 728375, 13 pages, 2013.

[18] Q. Zhang, X. Xue, and X. P. Wei, "A novel image encryption algorithm based on DNA subsequence operation," *The Scientific World Journal*, vol. 2012, Article ID 286741, 10 pages, 2012.

[19] X. Y. Zhang, C. Wang, S. Zhong, and Q. Yao, "Image encryption scheme based on balanced two-dimensional cellular automata," *Mathematical Problems in Engineering*, vol. 2013, Article ID 562768, 10 pages, 2013.

[20] Z. L. Zhu, W. Zhang, K. W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

[21] C. Fu, B. B. Lin, Y. S. Miao, X. Liu, and J. J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, no. 23, pp. 5415–5423, 2011.

[22] X. Y. Wang and D. P. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[23] D. Xiao, X. F. Liao, and P. C. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[24] J. Wei, X. Liao, K. W. Wong, and T. Zhou, "Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 12, no. 5, pp. 814–822, 2007.

[25] C. Fu, W. H. Meng, X. F. Zhan et al., "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in Biology and Medicine*, vol. 43, no. 8, pp. 1000–1010, 2013.

[26] IEEE Computer Society, "IEEE standard for binary floating-point arithmetic," ANSI/IEEE Std 754-1985, 1985.

[27] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.