Optik xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps

Bin Wang[a,*], Yingjie Xie[b], Changjun Zhou[a], Shihua Zhou[a], Xuedong Zheng[a]

[a] Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education, Dalian 116622, China
[b] Applied Technology College of Dalian Ocean University, Dalian 116300, China

ARTICLE INFO

Article history:
Received 4 November 2015
Accepted 6 January 2016
Available online xxx

Keywords:
Image encryption
Chaotic map
Permutation and diffusion operation

ABSTRACT

In recent years, there has been a growing interest in image encryption based on chaotic maps. In this paper, we evaluate the permutation and diffusion operations used in image encryption based on chaotic maps. Firstly, we research the permutation operation and diffusion operation, respectively. We use common analytical criterion to measure the effect of encryption operation. Then we employ the same method to evaluate the combinational operation, which is widely used in chaotic image encryption. Finally, we reverse the order of combinational operation and reevaluate the effect of encryption operation. By the evaluating results, researchers can choose the best operation to encrypt image, and improve the effect and security of algorithm based on chaotic maps.

1. Introduction

Due to the development of information technology, the security of image is becoming more and more important for image transmission. The digital image possesses some inherent features such as bulk data capacity and high correlation among adjacent pixels, so encryption algorithms are different from the traditional methods, such as DES, AES and so on. Chaotic maps have good potential character, such as ergodicity, sensitivity to initial conditions and control parameters. So many chaos-based image encryption algorithms have been proposed [1–10]. In Ref. [1], the authors generalized two-dimensional chaotic cat map to 3D for designing a real-time secure symmetric encryption scheme, used 3D cat map to permute the position of image pixels in the permutation stage and employed logistic chaotic system to diffuse the permuted image in the diffusion stage. A fast image encryption algorithm combined with permutation and diffusion was proposed in Ref. [2]. First, the image was partitioned into blocks of pixels. Then, spatiotemporal chaos was employed to shuffle the blocks, and at the same time, to change the pixel values. Meanwhile, an efficient method for generating pseudorandom numbers from spatiotemporal chaos was suggested, which further increased the encryption speed. In Ref. [3], the authors firstly analyzed the parameter sensitivity of standard map, and compared the secret key space of standard map with that of cat map and baker map. Then an improved standard map was used to realize position permutation, and the diffusion function consisted of logistic map that was used to realize the diffusion of image. In Ref. [4], it was a typical map—the baker map—that was further extended to be 3D and then used to speed up image encryption while permuting the position of plain-image. The logistic map was also used to diffuse the permuted image. In Ref. [5], the authors introduced a certain diffusion effect in the permutation stage by simple sequential add-and-shift operations. Although that led to a longer processing time in a single round, the overall encryption time was reduced as fewer rounds were required. A novel image encryption algorithm based on a 3D chaotic map that could defeat the aforementioned attack among other existing attacks was proposed in Ref. [6]. The design of proposed algorithm was simple and efficient, and based on three phases which provided necessary properties for a secure image encryption algorithm including permutation and diffusion properties. In Ref. [7], the paper proposed a novel chaos-based image encryption algorithm to encrypt color images by using a Coupled Two-dimensional Piecewise Nonlinear Chaotic Map, called CTPNCM, and a masking process. Distinct characteristics of the algorithm were high security, high sensitivity, and high speed that can be applied in encryption of color images.

In Ref. [1], the authors proposed a general cryptographic chaos-based architecture for image encryption, namely permutation–diffusion architecture, as shown in Fig. 1. This architecture includes two important operations, permutation operation and diffusion operation. The former permutes the plain-image, instead of changing the value of pixel. The latter changes the value of pixel,

* Corresponding author. Tel.: +86 041187402106.
E-mail address: wangbinpaper@gmail.com (B. Wang).

http://dx.doi.org/10.1016/j.ijleo.2016.01.015
0030-4026/

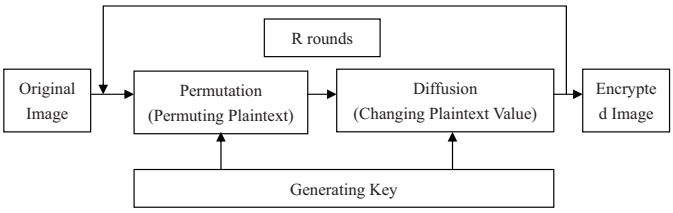


Fig. 1. Flowchart of permutation–diffusion type of chaos-based image cryptosystems.

instead of altering the position of pixel. In order to improve encryption effect of algorithms, the whole permutation–diffusion round will be repeated.

There are a large number of chaotic maps used in permutation–diffusion architecture, for example Logistic map, Tent map, Standard chaotic map, Cat chaotic map, generalized Baker chaotic map, Chen's chaotic system, Lorentz chaotic system and so on [1–6,11–15]. Although these chaotic maps can be used in the image encryption, some chaotic maps could cause a loophole, such as Cat map, Tent map and so on [16–18]. At the same time, using complex chaotic systems can make the rise of runtime of chaos-based image encryption, like Chen's chaotic system, Lorentz chaotic system. To design fast image encryption architecture, the complex chaotic map is not advised to be used. So in this paper, we use the Logistic map to encrypt image, and evaluate the permutation and diffusion operator. It can be denoted as Eq. (1):

$$x_{i+1} = \mu x_i(1 - x_i) \tag{1}$$

Here, μ is the control parameter for chaotic map, x_i and x_{i+1} are the ith and the $i+1$th state of chaotic map, respectively. A number of works related to logistic map have been published, including parameter sensitivity, initial value sensitivity, statistical properties and degradation phenomenon [19,20].

In order to test the effect of permutation and diffusion operation, we design different experiments to evaluate them. Firstly, we employ common analytical criterion to measure the permutation operation and diffusion operation, respectively. Then we test the effect of combinational operation, namely permutation–diffusion architecture. Finally, we evaluate the reverse combinational operation, namely diffusion–permutation architecture, using the common analytical criterion. In above experiments, the whole permutation round, diffusion round or combinational round will be not repeated to elaborate the encrypted effect of encrypted algorithm and used operation.

The paper is organized as follows. In the next section, the process of image encryption and decryption is described in detail. In Section 3, the performance analyses and simulation is described in detail. Finally, conclusions are drawn in Section 4.

2. The process of image encryption and decryption

In this part, the process of image encryption is described in detail. The process is divided into three different types, namely permutation type, diffusion type and combinational type. These types have same initial key which is randomly generated and related to plain-image by XOR operation. Owning to the characteristic of logistic map, it is chosen as chaotic map in image encryption. Different parameters and initial values for the Eq. (1) are denoted as μ_1, μ_2, $x_1(0)$ and $x_2(0)$, respectively,

where $\mu_1, \mu_2 \in [3.9, 4]$ and $x_1(0), x_2(0) \in (0, 1)$. Ikey is denoted as the initial key.

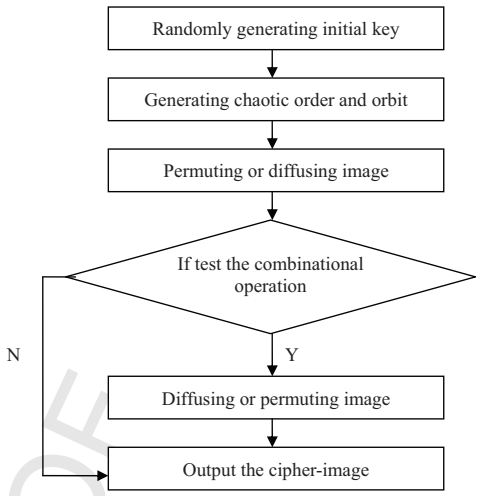


Fig. 2. The flowchart of image encryption.

2.1. Encryption algorithm

The details of encryption are described as follows, and illustrated in Fig. 2:

Step 1. Randomly generating the initial key and making the Ikey related to the plain image by XOR operation;
Step 2. Using Ikey as the parameter and value of logistic maps, and iterating logistic maps for100 times to get rid of the transient effect;
Step 3. Sorting the chaotic orbit obtained from previous step ascendingly, and permuting the diffused or plain-image by this order;

$$\mathrm{Mim}(i) = \mathrm{permute}(P(i) \quad \text{or} \quad D(i), \quad \mathrm{Order}(i)), \quad i = 1, 2, \ldots, M * N \tag{2}$$

Step 4. Generating cipher key by permuted image and Ilkey with XOR operation;
Step 5. Diffusing the permuted or plain-image by the logistic chaotic orbit from Step 3;

$$C(i) = (\mathrm{Mim}(i) \quad \text{or} \quad P(i)) \oplus \mathrm{Orbit}(i), \quad i = 1, 2, \ldots, M * N \tag{3}$$

Step 6. Outputting the cipher-image.

Where $P(i)$ is the original image pixel value, $\mathrm{Mim}(i)$ is the pixel value which is permuted by the order or diffused by the orbit, $\mathrm{Order}(i)$ is the ordered position of $P(i)$, $\mathrm{Orbit}(i)$ is the logistic chaotic orbit from step 5, $D(i)$ is the pixel value which is diffused by the orbit and $C(i)$ is the cipher-image. M and N are the width and height of the plain-image.

2.2. Decryption algorithm

The decryption process is similar to that of encryption procedure in the reversed order. It can be briefly stated as follows:

Step 1. Iterating the logistic maps for 100 times to get rid of the transient effect;
Step 2. Concurrently generating the chaotic orbit as encryption process;
Step 3. Obtaining $\mathrm{Orbit}(i)$ and $\mathrm{Order}(i)$;
Step 4. Recovering the $\mathrm{Mim}(i)$ by Eq. (4);

$$\mathrm{Mim}(i) = C(i) \oplus \mathrm{Orbit}(i), \quad i = 1, 2, \ldots, M * N \tag{4}$$

Please cite this article in press as: B. Wang, et al., Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps, Optik - Int. J. Light Electron Opt. (2015), http://dx.doi.org/10.1016/j.ijleo.2016.01.015

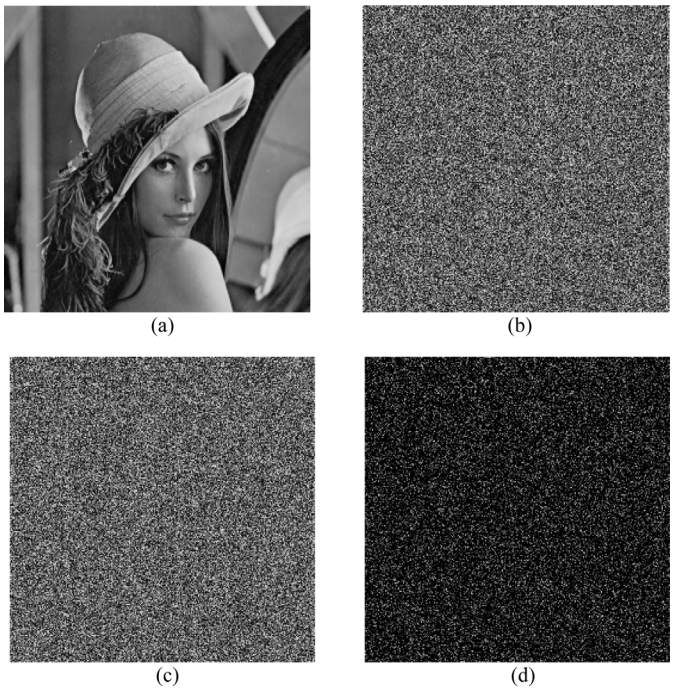


Fig. 3. Evaluating the permutation operation. (a) Plain-image of Lena; (b) encrypted image by key: 987654321012345; (c) encrypted image by key: 987654321012346; (d) difference image.

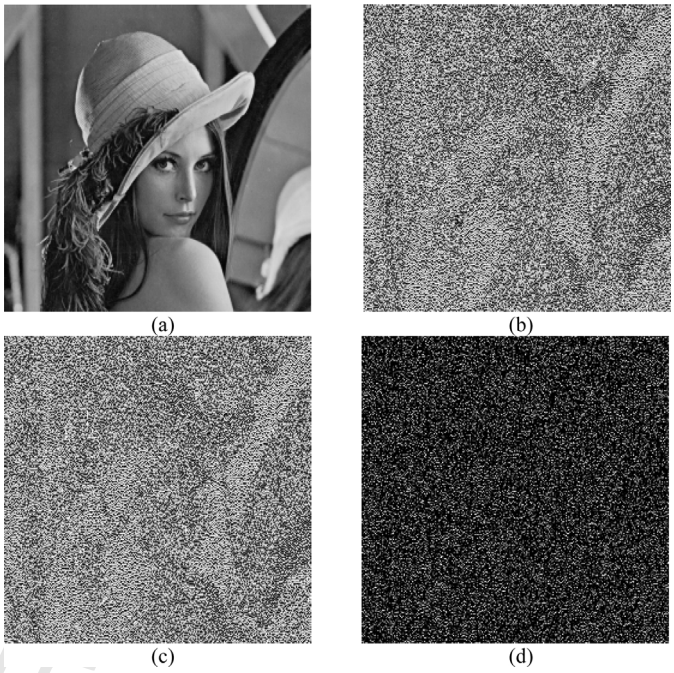


Fig. 4. Evaluating the diffusion operation. (a) Plain-image of Lena; (b) encrypted image by key: 987654321012345; (c) encrypted image by key: 987654321012346; (d) difference image.

Step 5. Recovering the $P(i)$ by Eq. (5);

$$P(\mathrm{Order}(i)) = \mathrm{Mim}(i), \quad i = 1, 2, \ldots, M * N \tag{5}$$

Step 6. Outputting the plain-image.

3. The performance analyses and simulation

3.1. The space of key

In a good image cryptosystem, the space of key should be large enough to make brute-force attack infeasible. In this paper, the Ikey consists of 16 elements, namely Ikey = $\{x_i\}$, $i = 1, 2, \ldots, 16$, $x_i \in [0, 255]$. So the key space of the proposed architecture is equal to $2^{128} \approx 3.4 \times 10^{38}$, which is sufficiently large to meet the need for practical application. All the experiments have same the space of key.

3.2. Key sensitivity

In this part, the test of key sensitivity will be performed as follows:

Step 1. Calculating the Imkey of the standard test 256×256 image Lena;
Step 2. Encrypting the test image by Ikey 987654321012345;
Step 3. Slightly changing the generated Ikey 987654321012346, and encrypting the same plain-image;
Step 4. Comparing the cipher-image encrypted by different keys.

In Fig. 3, the image encrypted by the key 987654321012345 has 99.43 percent different from the image encrypted by the key 987654321012346 in terms of pixel values, although there is only one bit difference in the two keys. In Fig. 4, it has 99.36 percent difference. In Fig. 5, it has 99.58 percent difference. In Fig. 6, it has 99.42 percent difference. From the above values, we can find that the diffusion–permutation operation is the worst method for key sensitivity. The permutation diffusion operation is the best method.

3.3. Statistical analysis

As Shannon said: 'It is possible to solve many kinds of ciphers by statistical analysis' [21]. Therefore, diffusion and confusion operations should be adopted to resist the attack in any cryptosystem. In

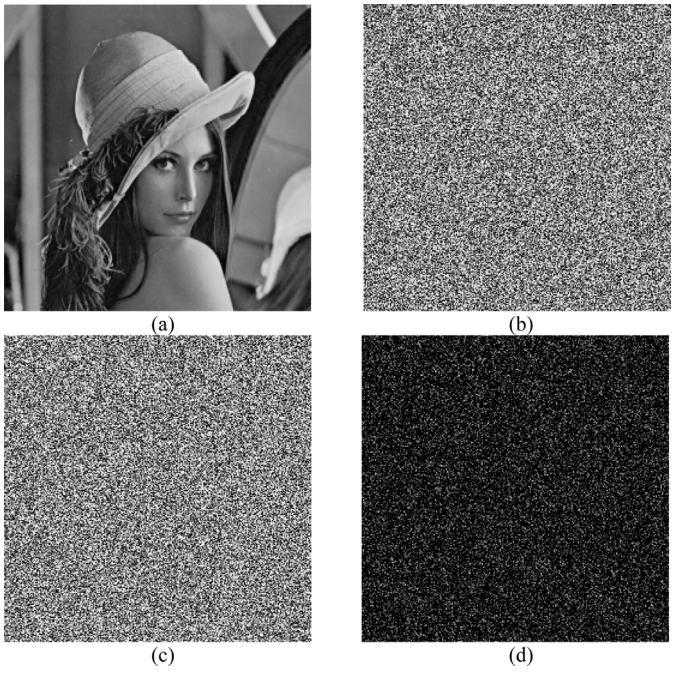


Fig. 5. Evaluating the permutation–diffusion operation. (a) Plain-image of Lena; (b) encrypted image by key: 987654321012345; (c) encrypted image by key: 987654321012346; (d) difference image.

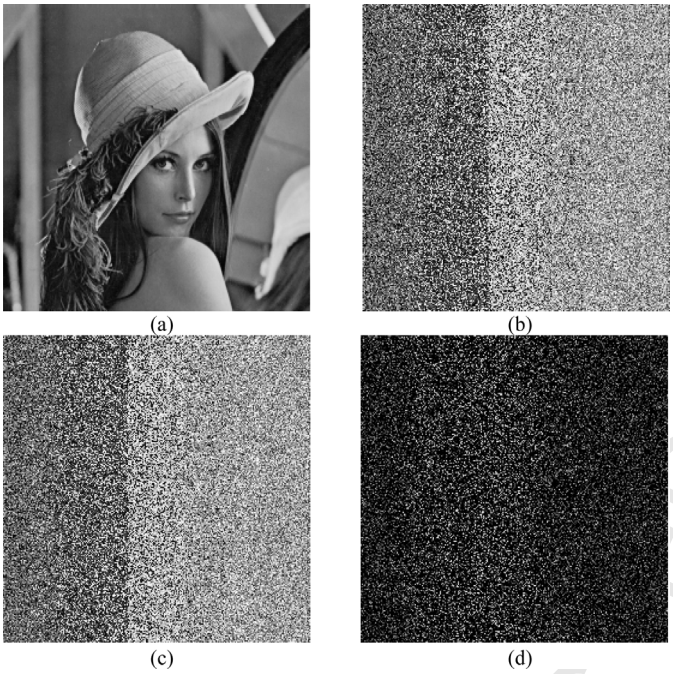
Please cite this article in press as: B. Wang, et al., Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps, Optik - Int. J. Light Electron Opt. (2015), http://dx.doi.org/10.1016/j.ijleo.2016.01.015

Table 1
The correlation coefficient of adjacent pixels.

	Permutation operation	Diffusion operation	Permutation–diffusion	Diffusion–permutation
Horizontal	**0.0668** (0.9680)	−**0.0807** (0.9721)	−**0.0087** (0.9683)	**0.1512** (0.9705)
Vertical	**0.0405** (0.9509)	**0.0076** (0.9462)	−**0.0279** (0.9464)	**0.0814** (0.9272)
Diagonal	**0.0195** (0.9246)	**0.0143** (0.8922)	**0.0246** (0.9021)	**0.1043** (0.9291)

Table 2
Q5 The value of NPCR and UACI.

	Permutation operation	Diffusion operation	Permutation–diffusion	Diffusion–permutation
NPCR	99.37	99.38	99.61	99.45
UACI	23.48	31.92	32.55	29.28



Q4 **Fig. 6.** Evaluating the diffusion–permutation operation. (a) Plain-image of Lena; (b) encrypted image by key: 987654321012345; (c) encrypted image by key: 987654321012346; (d) difference image.

this paper, the standard Lena test image of size 256 × 256 is selected to test the property of resisting statistical analysis.

To calculate the correlation of two adjacent pixels, we randomly select 1000 pairs of two adjacent pixels including vertically adjacent pixels, horizontally adjacent pixels and diagonally adjacent pixels. Then we calculate the correlation coefficient of each pair by using the following two formulas [1]:

$$cov(x, y) = E\{(x - E(x))(y - E(y))\} \tag{6}$$

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{7}$$

where x and y are gray-scale values of two adjacent pixels in the image. In numerical computation, the following discrete formulas are employed:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{9}$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N} \{(x_i - E(x))(y_i - E(y))\} \tag{10}$$

Table 1 shows the results of horizontal, vertical and diagonal directions.

In Table 1, the bold face is the correlation coefficient after encrypting image. The values in the brackets are the correlation coefficient before encrypting image. From the Table 1, we can find that the diffusion-permutation operation is the worst method for statistical analysis. The diffusion operation is the best method.

3.4. Differential attack

To test the property of resisting differential attack of this paper, two common quantitative criteria are employed: number of pixels change rate (NPCR) and unified average changing intensity (UACI). The NPCR and UACI are defined as follows [22,23]:

$$\text{NPCR} = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\% \tag{11}$$

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i, j - C_2(i, j))|}{255}\right] \times 100\% \tag{12}$$

where C_1 and C_2 are the two cipher-images whose corresponding plain-image have one pixel difference, the gray-scale values of the pixels at point (i, j) of C_1 and C_2 are denoted as $C_1(i, j)$ and $C_2(i, j)$, respectively; W and H are the width and height of the cipher-image; $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$, namely, if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 0$ otherwise, $D(i, j) = 1$.

From the Table 2, we can find that the permutation–diffusion operation is the best method for statistical analysis.

4. Conclusions

In this paper, we evaluate the permutation operation, diffusion operation, permutation–diffusion operation and diffusion–permutation operation based on chaotic image encryption. Firstly, we research the permutation operation and diffusion operation, respectively. We use common analytical criterion to measure the effect of encryption operation. Then we employ the same method to evaluate the combinational operation, which is widely used in chaotic image encryption. Finally, we reverse the order of combinational operation and reevaluate the effect of encryption operation. By the evaluating results, researchers can choose the best operation to encrypt image, and improve the effect and security of algorithm based on chaotic maps.

Please cite this article in press as: B. Wang, et al., Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps, Optik - Int. J. Light Electron Opt. (2015), http://dx.doi.org/10.1016/j.ijleo.2016.01.015

Acknowledgments

We would like to thank the anonymous reviewers for helpful comments. This work is supported by the National High Technology Research and Development Program ('863'Program) of China (No. 2009AA01Z416), the National Natural Science Foundation of China (Nos. 31170797, 30870573), Program for Changjiang Scholars and Innovative Research Team in University (No. IRT1109), the Program for Liaoning Innovative Re-search Team in University (No. LT2011018), the Program for Liaoning Excellent Talents in University (No. LR201003), the Program for Liaoning Science and Technology Research in University (No. LS2010179) and the open fund of Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education, Dalian University (No. ADIC2010012).

References

[1] G. Chen, et al., A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solitons Fractals 21 (3) (2004) 749–761.
[2] Y. Wang, et al., A new chaos-based fast image encryption algorithm, Appl. Soft Comput. 11 (1) (2011) 514–522.
[3] S. Lian, et al., A block cipher based on a suitable use of the chaotic standard map, Chaos Solitons Fractals 26 (1) (2005) 117–129.
[4] Y. Mao, et al., A novel fast image encryption scheme based on 3D chaotic Baker maps, Int. J. Bifurc. Chaos 14 (10) (2004) 3613–3624.
[5] K.W. Wong, et al., A fast image encryption scheme based on chaotic standard map, Phys. Lett. A 372 (15) (2008) 2645–2652.
[6] A. Kanso, M. Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, Commun. Nonlinear Sci. Numer. Simul. 17 (7) (2012) 2943–2959, http://dx.doi.org/10.1016/j.cnsns.2011.11.030.
[7] S.M. Seyedzadeh, S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Signal Process. 92 (5) (2012) 1202–1215, http://dx.doi.org/10.1016/j.sigpro.2011.11.004.
[8] N. Pareek, et al., Image encryption using chaotic logistic map, Image Vis. Comput. 24 (9) (2006) 926–934.
[9] K. Gupta, S. Silakari, Novel approach for fast compressed hybrid color image cryptosystem, Adv. Eng. Softw. 49 (2012) 29–42.
[10] L. Teng, X. Wang, A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive, Opt. Commun. 285 (20) (2012) 4048–4054, http://dx.doi.org/10.1016/j.optcom.2012.06.004.
[11] Y. Wang, et al., A chaos-based image encryption algorithm with variable control parameters, Chaos Solitons Fractals 41 (4) (2009) 1773–1783.
[12] Z. Zhu, et al., A chaos-based symmetric image encryption scheme using a bit-level permutation, Inf. Sci. 181 (6) (2011) 1171–1186.
[13] D. Xiao, et al., Analysis and improvement of a chaos-based image encryption algorithm, Chaos Solitons Fractals 40 (5) (2009) 2191–2199.
[14] X.Y. Wang, et al., A chaotic image encryption algorithm based on perceptron model, Nonlinear Dyn. 62 (3) (2010) 615–621, http://dx.doi.org/10.1007/s11071-010-9749-8.
[15] M.J. Wang, X.Y. Wang, A chaotic secure communication method based on parameter identification, Int. J. Mod. Phys. B 24 (28) (2010) 5515–5525, http://dx.doi.org/10.1142/s0217979210056967.
[16] K. Wang, On the security of 3D Cat map based symmetric image encryption scheme, Phys. Lett. A 343 (6) (2005) 432–439.
[17] S. Lian, et al., Security analysis of a chaos-based image encryption algorithm, Physica A: Stat. Mech. Appl. 351 (2-4) (2005) 645–661.
[18] N. Masuda, et al., Chaotic block ciphers: from theory to practical algorithms, IEEE Trans. Circ. Syst. I: Regul. Pap. 53 (6) (2006) 1341–1352.
[19] S. Li, et al., On the dynamical degradation of digital piecewise linear chaotic maps, Int. J. Bifurc. Chaos Appl. Sci. Eng. 15 (10) (2005) p3119.
[20] S. Li, et al., Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding, Cryptogr. Coding (2001) 205–221.
[21] C.E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28 (4) (1949) 656–715.
[22] H. Kwok, W.K.S. Tang, A fast image encryption system based on chaotic maps with finite precision representation, Chaos Solitons Fractals 32 (4) (2007) 1518–1529.
[23] J. Peng, et al., A digital image encryption algorithm based on hyper-chaotic cellular neural network, Fundam. Inform. 90 (3) (2009) 269–282.

Please cite this article in press as: B. Wang, et al., Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps, Optik - Int. J. Light Electron Opt. (2015), http://dx.doi.org/10.1016/j.ijleo.2016.01.015