计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190800003

基于循环移位和多混沌映射的图像加密算法

田军锋[1,2]　彭静静[1]　左宪禹[1,2,3]　葛　强[1,2,3]　范明虎[1,2]
1 河南大学计算机与信息工程学院　河南 开封 475004
2 河南省大数据分析与处理重点实验室　河南 开封 475004
3 河南大学数据与知识工程研究所　河南 开封 475004
(tjf328@126.com)

摘　要　利用单一混沌系统实现的加密算法结构简单且容易被攻击,采用多个混沌系统加密是提高加密系统安全性的有效措施。文中提出一种基于循环移位和多混沌映射的图像加密算法,循环移位操作可以有效地改变图像的像素值。首先,利用分段线性混沌映射(Piecewise Linear Chaotic Map,PWLCM)和 Logistic 映射产生不同的混沌序列,并根据不同混沌序列生成索引矩阵和循环移位数。然后,根据索引矩阵对明文图像进行置换操作,根据循环移位数对置换图像依次做左循环移位操作。最后,通过 Logistic 混沌序列和 PWLCM 混沌序列对循环移位后的图像进行置乱和扩散操作,最终得到加密图像。对图像直方图、信息熵、差分攻击、相关性进行的测试和分析结果表明,所提加密算法具有高安全性和抵御各种攻击的能力,可以应用于图像加密系统中。

关键词:图像加密;混沌加密;多混沌映射;索引矩阵;循环移位
中图法分类号　TP391

Image Encryption Algorithm Based on Cyclic Shift and Multiple Chaotic Maps

TIAN Jun-feng[1,2],PENG Jing-jing[1],ZUO Xian-yu[1,2,3],GE Qiang[1,2,3] and FAN Ming-hu[1,2]
1 College of Computer and Information Engineering,Henan University,Kaifeng,Henan 475004,China
2 Key Laboratory of Big Data Analysis and Processing of Henan Province,Henan University,Kaifeng,Henan 475004,China
3 Institute of Data and Knowledge Engineering,Henan University,Kaifeng,Henan 475004,China

Abstract　The encryption algorithm implemented by a single chaotic system has a simple structure and is easy to be attacked, using multiple chaotic systems to encrypt is an effective measure to improve the security of the encryption system. A new image encryption algorithm based on cyclic shift and multiple chaotic maps was proposed, and cyclic shift operation can change the values of the pixels efficiently. First, using piece-wise linear chaotic map (PWLCM) and Logistic map to generate different chaotic sequences, generating index matrix and cyclic shift number according to the different chaotic sequences. Then, the plaintext image is replaced on the basis of index matrix. The left cyclic shift operation is performed on the replacement image in turn according to the cyclic shift number. Finally, the image after cyclic shift is scrambled and diffused by Logistic chaotic sequence and PWLCM chaotic sequence. Ultimately, an encrypted image is obtained. Tests and analyses of image histogram, information entropy, differential attack and correlation were carried out. Theoretical analysis and simulation results show that this algorithm has high security, a desirable ability to resist different kinds of attacks and can be used to implement an image encryption system.

Keywords　Image encryption, Chaotic encryption, Multiple chaotic maps, Index matrix, Cyclic shift

1　引言

数字图像是一种被广泛采用的数据格式,因具有快捷方便、信息量大等特点,其在各个领域都具有广泛的应用;同时对数字图像的安全保护变得越来越重要。混沌是一种复杂的非线性、非平衡的动力学过程,混沌映射具有对初始值极端敏感、遍历性、非周期性和类随机性等特点[1],逐渐被应用到图像加密中。

Matthews[2]首先提出用一维混沌映射来加密图像;在此基础上,许多新的基于混沌系统的图像加密算法被提出[3-15]。

到稿日期:2019-08-01　返修日期:2019-10-20　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家重点研发计划课题(2017YFD0301105);国家自然科学基金(U1604145,U1704122);河南省重点研发与推广专项(182102210242,182102110065,192102210096)
This work was supported by the National Key Research and Development Program of China (2017YFD0301105), National Natural Science Foundation of China (U1604145, U1704122) and Special Research and Development and Promotion Project of Henan Province (182102210242, 182102110065, 192102210096).
通信作者:范明虎(fmh139@163.com)

Logistic 映射和分段线性混沌映射是两种常见的产生混沌序列的函数。许多学者提出了基于 Logistic 映射的混沌加密算法[4-5,10]和基于 PWLCM 映射的混沌加密算法[6-15]。Liu 等[5]提出了一种可变参数的 Logistic 映射，该混沌映射可以弥补传统一维 Logistic 映射的缺陷，有效抵抗相空间攻击。Nasir 等[6]提出的嵌套 PWLCM 映射的位级置换算法提高了加密系统的安全性，但是需要多次生成 PWLCM 混沌序列，增加了系统的复杂性和计算成本。由于混沌映射定义在实数域，动力学特性才出现混沌特性，而计算机系统处理的是离散量，因此需要对混沌映射进行离散化，导致产生的混沌序列可能产生短周期窗口、严重不平衡的分布函数和较低的线性复杂度。该类混沌加密算法虽然具有结构简单、产生的混沌序列短等优点，但是密钥空间低，很容易受到外部因素破坏。因此，使用单一混沌系统实现的加密算法是不够安全的，目前已经有很多攻击方法破解了这类混沌加密方案[8-9]。为了提高混沌系统的复杂性，Wang 等[10]提出混合哈希函数和循环移位的混沌系统加密算法，让明文图像和哈希函数相关，这使得攻击者在不知密钥的情况下不可能通过异或操作获取密钥的哈希值。同时，该算法根据 Logistic 映射生成每一个位置像素循环移位数来对图像进行扩散操作，从而提高加密系统的安全性。Hua 等[12]于 2015 年提出一种正弦映射和 Logistic 映射相结合的二维混沌序列产生模型，该模型利用正弦映射和参数 β 来调整 Logistic 映射的输出，从而增强二维混沌序列的非线性和随机性，在一定程度上提高了加密系统的安全性。Hua 等[12]后来又提出基于余弦变换的混沌系统，利用两个混沌映射作为余弦变换的种子，生成的混沌序列具有复杂动力学行为。高维混沌系统比低维混沌系统具有更复杂的动力学行为以及更好的随机性，在一定程度上提高了加密的安全性。Zhu 等[13]构造了一个新的四维离散混沌映射，该混沌序列具有更复杂的动力学行为，其产生的伪随机数范围更大，在一定程度上提高了混沌系统的安全性。采用多维混沌系统[3,13-15]虽然具有复杂混沌行为，混沌序列很难被预测，但是由于复杂性和实现成本太高而很难应用于实际系统中。

为了得到高安全性的图像加密方案，本文提出了一种新的基于循环移位和多混沌映射的图像加密算法。首先，利用 PWLCM 映射和 Logistic 映射产生不同的混沌序列，并根据混沌序列生成索引矩阵以及与明文相关的循环移位数。然后，根据索引矩阵对明文图像进行置换操作，根据循环移位数对置换图像依次做左循环移位操作。最后，Logistic 混沌序列和 PWLCM 混沌序列对循环移位后的图像进行置乱和扩散操作，最终得到加密图像。数值模拟实验验证了该算法的有效性和鲁棒性，其能够抵抗常见的密码学攻击，编码具有更高的安全性。

2 多混沌映射

2.1 Logistic 映射

Logistic 映射[5]是研究动力系统、混沌、分形等复杂系统行为的一个经典模型，其由于原理简单、计算方便而被广泛应用于图像加密领域。经典的 Logistic 函数如式(1)所示：

$$x_{n+1}=f(x_n)=\mu x_n(1-x_n) \tag{1}$$

当参数 $\mu\in(3.5699456,4)$，初值 $x_n\in(0,1)$ 时，系统是混沌的。但是在参数 μ 的整个区间，该混沌系统存在周期窗口，为了避免出现周期窗口，本文设置 μ 的取值范围为 $\mu\in(3.90,4]$。

2.2 分段线性混沌映射

PWLCM 映射[6]是由多个线段构成的混沌映射，如式(2)所示：

$$x_{n+1}=g(x_n,\eta)=\begin{cases}\dfrac{x_n}{\eta}, & 0<x_n<\eta\\ \dfrac{x_n-\eta}{0.5-\eta}, & \eta\leqslant x_n<0.5\\ g(1-x_n,\eta), & 0.5\leqslant x_n<1\end{cases} \tag{2}$$

其中，η 为控制参数，且 $\eta\in(0,0.5)$，$x_n\in(0,1)$。给控制参数 η 和 x_0 赋初值，经过循环迭代可以得到区间(0,1)上的随机序列，该随机序列具有很好的统计特性[7]。

由于一维分段线性映射生成的序列具有良好的统计特性，本文将用产生的混沌序列来加密图像。

3 加密算法

3.1 混沌系统控制参数和初始值

假设待处理的明文图像 R 的大小为 $M\times N$，$R(i,j)$ 表示 i 行 j 列位置对应的灰度值，满足 $1\leqslant i\leqslant M$，$1\leqslant j\leqslant N$。根据式(3)－式(6)生成 Logistic 映射和 PWLCM 映射控制参数初始值。

$$x_{01}=\frac{1}{a_1}+t_1 \tag{3}$$

$$\mu=\frac{1}{a_1}+t_2+3.90 \tag{4}$$

$$x_0=\frac{1}{a_2}+t_3 \tag{5}$$

$$\eta=\frac{1}{a_2}+t_4 \tag{6}$$

其中，a_1 和 a_2 是 2 个控制参数；(x_{01},μ) 是一个 Logistic 映射初始值；(x_0,η) 是一个 PWLCM 映射初始值；t_1，t_2，t_3 和 t_4 是控制参数，用来控制 Logistic 映射和 PWLCM 映射的初始值，可以作为加密密钥。

3.2 加密过程

加密过程的具体步骤如下。

(1)像素替换。当前大部分的像素替换规则是行行替换或列列替换，或是某种特定规则替换，这些替换方法容易受到攻击。为了解决以上问题，本文提出了一种利用混沌序列产生的索引矩阵对图像像素值进行替换操作的方法，因为混沌序列对初始值敏感，所以根据混沌序列替换使加密系统变得更加复杂，从而提高了加密的安全性。

替换规则：根据式(5)和式(6)生成 PWLCM 映射 x_0 和 η 的初值；然后根据式(2)迭代 r_1+MN 次生成混沌序列，为了消除暂态效应，舍掉前 r_1 项；接着根据后 MN 项生成混沌序列，记为 $U(i)$，$i=1,2,\cdots,MN$。根据式(7)将 $U(i)$ 转换成 M 行 N 列的二维矩阵 $\boldsymbol{B}$，再根据式(8)对二维矩阵 $\boldsymbol{B}$ 进行排序，得到索引矩阵 ***indexB***。根据索引矩阵 ***indexB*** 将明文图像像素按照式(9)进行替换，得到替换后的图像 R'。最后，根据式(10)将混沌序列转换成整数序列 $Z(i)$，再利用 $Z(i)$ 对图像进行加密。

$$\boldsymbol{B}=reshape(U,[M,N]) \tag{7}$$

$$[sortB,\boldsymbol{indexB}]=Sort(\boldsymbol{B}) \tag{8}$$

$$R'(i,j)=R(\boldsymbol{indexB}(i,j),j) \tag{9}$$

$$Z(i)=\mathrm{mod}(floor(U(i)\times 10^{14}),256) \tag{10}$$

为了更好地说明通过索引矩阵进行替换的过程，这里举一个例子。假设索引矩阵 $\boldsymbol{I}$ 的大小为 4×4，如图 1(a)所示，$\boldsymbol{I}$ 的值是对混沌序列进行按列排序生成的下标。索引矩阵 $\boldsymbol{I}$ 中的值表示行，列使用默认列。$\boldsymbol{I}$ 中第一行 4 个值为(4，3，1，2)，则它对应的二维坐标为(4，1)，(3，2)，(1，3)和(2，4)，即明文图像坐标(4，1)的灰度值替换到坐标(1，1)处，明文图像坐标(3，2)的灰度值替换到坐标(1，2)处，明文图像坐标(1，3)的灰度值替换到坐标(1，3)处，明文图像坐标(2，4)的灰度值替换到坐标(1，4)处；其余行依次进行变换。图 1(b)为原像素替换后的位置分布。

4	3	1	2
2	4	4	3
1	2	2	1
3	1	3	4

(a)索引矩阵 $\boldsymbol{I}$

(4,1)	(3,2)	(1,3)	(2,4)
(2,1)	(4,2)	(4,3)	(3,4)
(1,1)	(2,2)	(2,3)	(1,4)
(3,1)	(1,2)	(3,3)	(4,4)

(b)T 置换后像素位置分布

图 1 利用索引矩阵替换例子

Fig. 1 Example of determining substitution order by index matrix

(2)循环移位。将 R' 按行优先存储转换成一维矩阵，第一步替换操作仅能够改变像素的位置，不能改变像素值。先根据式(3)和式(4)生成一维 Logistic 映射 x_{01} 和 η 的初值；然后根据式(1)迭代 r_2+MN 次生成混沌序列，为了消除暂态效应，舍掉前 r_2 项；接着根据后 MN 项生成混沌序列，记为 $U1(i)$，$i=1,2,\cdots,MN$。根据式(11)将混沌序列转换成整数序列 $M(i)$，再利用 $M(i)$ 对图像进行加密。根据式(12)求出每一个位置像素值需要循环移位的位数。最后根据式(13)将 R' 循环移位，得到 R'' 图像。

$$M(i)=\mathrm{mod}(floor(U1(i)\times 10^{14}),256) \tag{11}$$

$$c(i)=\mathrm{mod}(M(i),7)+1 \tag{12}$$

$$R''(i)=circshift(R'(i),c(i)) \tag{13}$$

其中，$i=1,2,\cdots,MN$，cirshift 表示左循环移位运算，mod 表示取模运算。

(3)扩散加密。利用第一步生成的序列 $Z(i)$ 和第二步生成的序列 $M(i)$ 对循环移位后的图像 R'' 进行加密处理。根据式(14)得到密文 C。

$$\begin{cases} C(1)=R''(1)\oplus R''(MN)\oplus Z(1)\oplus M(1), & i=1 \\ C(i)=R''(i)\oplus C(i-1)\oplus Z(i)\oplus M(i), & i\neq 1 \end{cases} \tag{14}$$

3.3 解密过程

解密过程的具体步骤如下：

(1)将加密密钥代入混沌序列，根据加密过程(1)到第(3)生成混沌序列 Z，M 和索引矩阵 $\boldsymbol{I}$；

(2)根据式(15)求解 E；

$$\begin{cases} E(i)=C(i)\oplus C(i-1)\oplus Z(i)\oplus M(i), & i\neq 1 \\ E(1)=C(1)\oplus R''(MN)\oplus Z(1)\oplus M(1), & i=1 \end{cases} \tag{15}$$

(3)根据混沌序列 M 和式(14)计算 $c(i)$，根据 $c(i)$ 右循环移位 E 得到 E'；

(4)根据索引矩阵 $\boldsymbol{I}$，对 E' 反向求解，得到明文 P。

4 实验结果

选择 4 个尺寸为 256×256 像素的标准灰度图像 Lena，Baboon，Peppers 和 Elaine 进行实验验证。实验环境为：内存 4 GB，处理器 i5-3230M，CPU2.6 GHz，操作系统 Windows 7，仿真软件为 MatlabR2014a。

密钥设置如下：$a_1=130$，$a_2=117$，$t_1=0.1$，$t_2=0.02$，$t_3=0.001$，$t_4=0.001$，混沌运算迭代参数 $r_1=1\,000$，$r_2=1\,000$。经过加密后的实验结果如图 2 所示，第一列为不同的明文图像，第二列为明文图像对应的密文图像，第三列为根据加密密钥对密文图像解密后的图像。从图 2 中第二列完全看不出原始明文图像信息，说明本文算法达到了很好的加密效果；从图 2 第三列可以看出，使用正确的加密密钥，密文图像可以完全恢复。

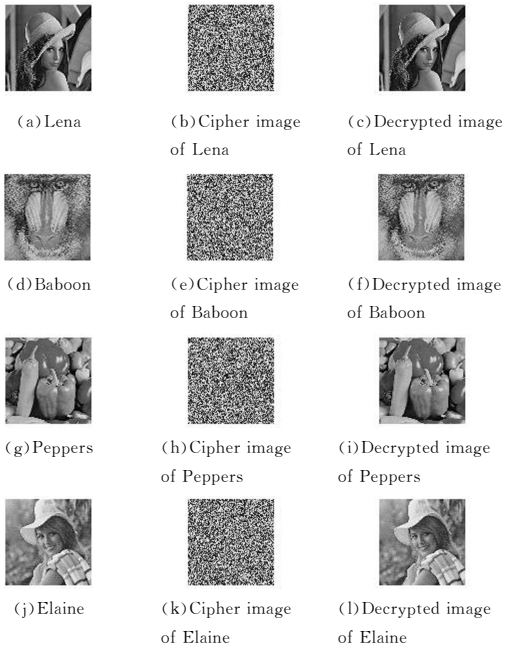

图 2 实验结果

Fig. 2 Encryption experiment results

5 安全性分析

本节对明文和密文进行统计分析，包括直方图分析和相邻像素相关性分析。

5.1 图像直方图分析

直方图是数字图像的一个基本属性，它反映了图像的灰度级与图像出现频率之间关系的统计特性。一种好的加密方法可以使加密图像像素较为均匀地分布。为了验证本文算法的有效性，选择尺寸为 256×256 像素的标准 Lena，Baboon，Peppers 和 Elaine 图像进行测试，测试结果如图 3 所示。每一行的 4 列分别为明文图像、密文图像、明文图像直方图和密文图像直方图，其中，直方图横坐标代表 256 个灰度等级，纵坐标代表图像所有像素中每个灰度等级出现的次数。从图 3 可以看出，4 幅测试图像的直方图分别与对应的明文图像的直方图相比，密文图像的直方图更为均匀，这使得攻击者难以通过统计特性获得原始图像的特征，从而提高了密文的安全性。

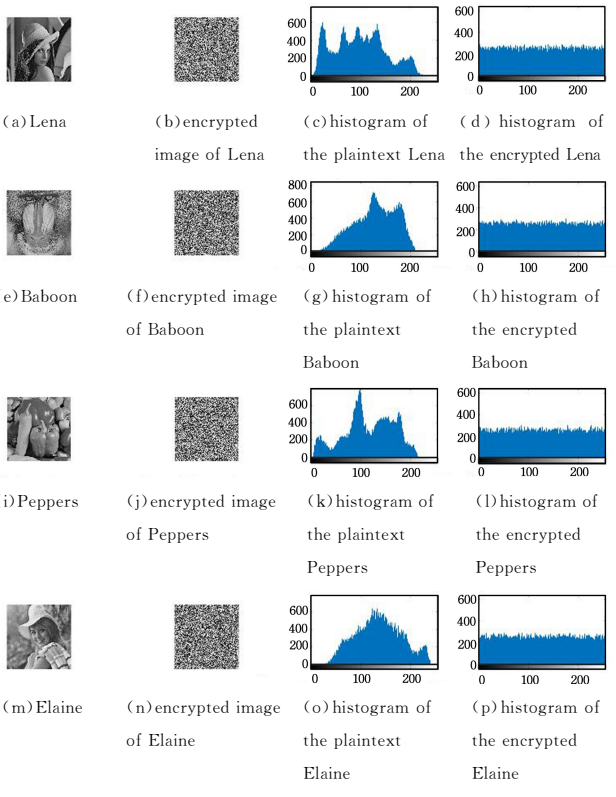

图 3 不同图像的实验结果

Fig. 3 Encryption experiment results of different images

5.2 信息熵分析

信息熵是反映信息随机性的重要度量指标。图像灰度值分布得越均匀，信息熵就越大。设 m 代表一种信息源，则 m 的信息熵 $H(m)$ 可用式(16)进行计算：

$$H(m)=-\sum_{i=0}^{2^n-1}p(m_i)\log_2 p(m_i) \tag{16}$$

其中，2^n 表示信息源 m 的总状态个数，$p(m_i)$ 代表符号 m_i 出现的概率。对于完全理想的随机图像，其信息熵为 8。图像的信息熵越接近于 8，说明图像灰度值分布越均匀，它抵抗统计攻击的能力就越强。对几幅标准图像进行测试，并将所提算法与其他算法进行比较，测试结果如表 1 所列。

表 1 测试图像的信息熵

Table 1 Information entropy of the test images

序号	测试图像	原始明文	密文图像
1	Lena(512×512)	7.4455	7.99944
2	Lena(256×256)	7.5683	7.9978
3	Peppers(256×256)	7.5256	7.9974
4	Baboon(256×256)	7.3385	7.9976
5	Elaine(256×256)	7.5046	7.9978
6(文献[7])	Lena(256×256)	7.5683	7.9974
7(文献[7])	Peppers(256×256)	7.5276	7.9973
8(文献[10])	Lena(256×256)	7.5683	7.9975
9(文献[10])	Peppers(256×256)	7.5256	7.9973

由表 1 可知，利用本文算法对 Lena(256×256)图像加密，得到的密文图像信息熵为 7.9978，更接近理想值 8，密文内容不容易泄漏，安全性高。

5.3 差分分析

根据密码学原理，好的加密算法应该对明文充分敏感，敏感性越强，抵抗差分攻击的能力也就越强。差分分析虽然对数据量的要求比较高，但却是一种行之有效的攻击方法。像素数变化率(Number of Pixels Change Rate，NPCR)和归一化平均变化强度(Unified Average Changing Intensity，UACI)是衡量图像加密算法抵抗差分攻击的重要指标。它们分别表示随机地改变原始图像的某个像素值以后，加密图像像素值发生改变的数目所占的比例以及变化程度。如果图像的某个像素值的改变可以很大程度地改变加密图像，则说明该算法具有较强的抵抗差分攻击的能力。对于 8 位灰度图像，*NPCR* 和 *UACI* 的理想值分别为 99.6096%和 33.46%。*NPCR* 和 *UACI* 的定义如式(17)和(18)所示。

$$NPCR=\sum_{i=1}^{i=M}\sum_{j=1}^{j=N}D(i,j)/(M\times N)\times 100\% \tag{17}$$

$$UACI=\frac{1}{M\times N}\sum_{i=1}^{i=M}\sum_{j=1}^{j=N}\frac{|C(i,j)-C'(i,j)|}{255}\times 100\% \tag{18}$$

其中，C 和 C' 分别表示两幅加密图像，并且它们对应的明文图像只在一个位置像素值不同；$D(i,j)$ 表示 $C(i,j)$ 和 $C'(i,j)$ 对应的像素值是否相同，如果相同，$D(i,j)=0$，否则 $D(i,j)=1$。

将明文图像 Lena(256×256)中第一个像素值增加 1，通过式(17)和式(18)计算得 *NPCR* 和 *UACI* 值分别为 99.61%和 33.45%。表 2 比较了本文算法与文献[3]和文献[15]算法得到的 Lena 密文图像的平均 *NPCR* 和 *UACI*。由表 2 可知，原始图像的稍微变化会引起密文图像的明显变化，这表明本文算法可以有效抵抗明文攻击。

表 2 不同图像加密方法的平均 *NPCR* 与 *UACI*

Table 2 Average NPCR and *UACI* of various image encryption schemes

(单位：%)

敏感性指标	本文	文献[3]	文献[15]
平均 *NPCR*	99.61	99.61	99.68
平均 *UACI*	33.45	33.453	33.47

5.4 算法效率分析

采用文献[3]的测试环境，分别用本文算法、文献[3]中的算法和文献[14]中的算法对同一幅大小为 256×256 像素、图像类型为 pgm 格式的图像 Lena 进行加密时间测试。结果得出，文献[14]中的算法的加密操作需要 10.54 s，文献[3]中的算法的加密操作需要 7.2 s，而本文的加密算法需要 3.2009 s，因此本文的加密算法具有较好的加密效率。

5.5 相关性分析

图像像素的扩散程度采用相邻像素的相关性来表示，而相邻像素之间的相关性是验证图像加密方案优劣的一个重要指标。相关系数的计算公式参见文献[3]：

$$R_{x,y}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{19}$$

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{20}$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{21}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{22}$$

在明文图像和密文图像的水平方向、垂直方向和对角方向，各随机选取 5000 对相邻的像素点进行测试。明文和密文图像中相邻像素灰度值在水平、垂直和对角线方向的相关性关系如图 4 所示。由图 4 可知，明文图像有很强的相关性；密文图像相邻点之间几乎没有任何关系。

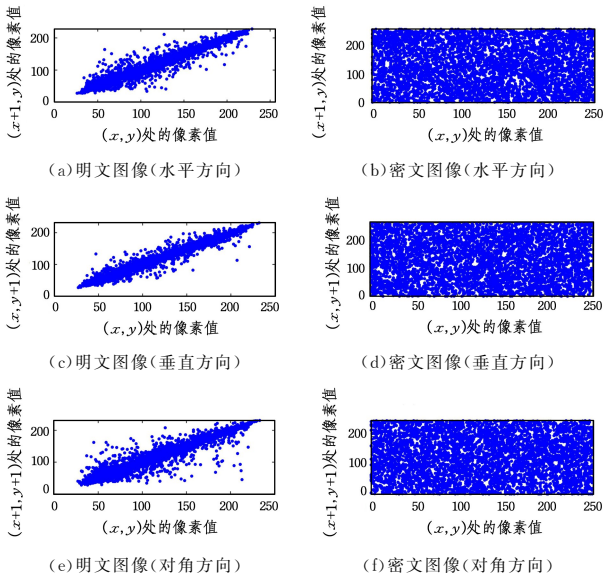

图 4 Lena 图像相邻像素相关性分布图

Fig. 4 Correlation of adjacent pixels of Lena

选择尺寸为 256×256 像素的标准图像 Lena，Peppers，Baboon，Elaine，分别计算明文和密文图像中相邻像素在水平、垂直和对角线方向之间的相关系数，结果如表 3 所列。由表 3 可知，明文图像相邻像素的相关系数接近于 1，而密文图像相邻像素的相关系数接近于 0，表明本文算法破坏了原始图像中相邻像素的相关性，密文图像的像素分布具有良好的随机性，增大了图像被非法恢复的难度，从而提高了算法的安全性。

表 3 明文和密文相邻像素的相关系数

Table 3 Correlation coefficients of the plain image and ciphered image

测试图像	明文、密文	水平方向	垂直方向	对角方向
Lena (256×256)	明文图像	0.9410	0.9725	0.9186
	密文图像	0.0037	0.0025	0.0029
Peppers (256×256)	明文图像	0.9459	0.9234	0.8508
	密文图像	−0.0026	−0.0095	0.0080
Baboon (256×256)	明文图像	0.7452	0.6474	0.6413
	密文图像	0.0014	0.0041	0.0035
Elaine (256×256)	明文图像	0.9528	0.9493	0.9267
	密文图像	−0.0009	−0.0002	−0.0083
Lena (256×256)[7]	明文图像	0.9713	0.9400	0.9267
	密文图像	−0.0230	0.0019	−0.0083
Lena (256×256)[10]	明文图像	0.9757	0.9594	0.9415
	密文图像	−0.0037	−0.0029	0.0047

结束语 本文提出了一种新的基于循环移位和多混沌映射的图像加密算法。首先，利用 PWLCM 映射和 Logistic 映射产生不同的混沌序列，并根据混沌序列生成索引矩阵以及与明文相关的循环移位数。然后，根据索引矩阵对明文图像进行置换操作，根据循环移位数对置换图像依次做左循环移位操作。最后，通过 Logistic 混沌序列和 PWLCM 混沌序列对循环移位后的图像进行置乱和扩散操作，最终得到加密图像。数值模拟实验验证了该算法的有效性和鲁棒性，其能够抵抗常见的密码学攻击，编码具有更高的安全性，可用于保密通信中。但是，本文算法的验证实验仅针对灰度图像进行了有效测试，未来可以继续对彩色图像、遥感图像等不同图像的加密算法进行进一步的研究，同时对算法的并行化展开研究。

参 考 文 献

[1] LIAN S, SUN J, WANG Z. A block cipher based on a suitable use of the chaotic standard map[J]. Chaos Soliton Fract, 2005, 26(1): 117-129.

[2] MATTHEWS R. On the derivation of chaotic encryption algorithm[J]. Cryptologia, 1989, 13(1): 29-42.

[3] CHAI X L, GAN Z H. New Bit-level Self-adaptive Color Image Encryption Algorithm Based on Hyperchaotic System[J]. Computer Science, 2016, 43(4): 134-139.

[4] CAI J, CHEN X, XIANG X D. Substitution permutation network structured image encryption algorithm based on chaotic map[J]. Computer Science, 2014, 41(9): 158-164.

[5] LIU L F, MIAO S X. A new image encryption algorithm based on logistic chaotic map with varying parameter[J]. Springer Plus, 2016, 5(1): 1-12.

[6] NASIR Q, ABDLRUDHA H H. High security nested PWLCM chaotic map bit-level permutation based image encryption[J]. International Journal of Communications, Network and System Sciences, 2012, 5(9): 548-556.

[7] XU L, LI Z, LI J, et al. A novel bit-level image encryption algorithm based on chaotic maps[J]. Optics and Lasers in Engineering, 2016, 78: 17-25.

[8] LI C, LI S, KWOK-TUNG L. Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps[J]. Commun. Nonlinear Sci. Numer. Simul., 2011, 16: 837-843.

[9] LI C. Cracking a hierarchical chaotic image encryption algorithm based on permutation[J]. Signal Process, 2016, 118: 203-210.

[10] WANG X Y, ZHU X Q, WU X J, et al. Image encryption algorithm based on multiple mixed hash functions and cyclic shift [J]. Optics and Lasers in Engineering, 2018, 107: 370-379.

[11] HUA Z Y, ZHOU Y C, PUN C M, et al. 2D sine Logistic modulation map for image encryption[J]. Information Sciences, 2015, 297(10): 80-94.

[12] HUA Z Y, ZHOU Y C, HUANG H J. Cosine-transform-based chaotic system for image encryption[J]. Information Sciences, 2019, 480: 403-419.

[13] ZHU S Q, LI J Q, GE G Y. New image encryption algorithm Based on new four-dimensional discrete-time chaotic map[J]. Computer Science, 2017, 44(1): 188-193.

[14] XU B, SUN Y W, LI Y, et al. Improved Encryption Algorithm Based on High-dimension Chaotic System[J]. Journal of Jilin University(Information Science Edition), 2012, 30(1): 12-17.

[15] CHENG D S, TAN X, XU Z L, et al. Dimensional Hyper-chaotic System and Bit Decomposition[J]. Journal of University of Electronic Science and Technology of China, 2018, 47(6): 906-912.

TIAN Jun-feng, born in 1980, Ph.D, lecturer. His main research interests include digital image processing and image encryption.

FAN Ming-hu, born in 1974, Ph.D, lecturer. His main research interests include remote sensing image and information space processing.