基于混沌映射的图像加密算法研究

赵 雨[1],杨 真[2],雍江萍[1],展爱云[3],张跃进[1]

(1. 华东交通大学信息工程学院,江西 南昌 330013; 2. 华东交通大学网络信息中心,江西 南昌 330013;
3. 华东交通大学电气与自动化工程学院,江西 南昌 330013)

摘要:由于传统的文本加密算法对图像加密的适用性不强,经典的 Logistic 映射存在系统参数范围受限、混沌序列分布不均等问题。通过一种基于循环移位结合改进型 Logistic 映射和 Tent 映射的图像加密算法。设置改进型 Logistic 映射和 Tent 映射的初始值和控制参数,并应用比特重拍技术提升过渡态中的混沌效果,达到提升图像加密算法的效果。明文图像进行处理时,先对其进行 Arnold 变换和异或的预加密处理,并对图像进行分块处理,然后利用 Tent 映射产生的序列进行排序索引与循环移位。在加密过程中明文图像经历了像素替换和像素扩散,使得明文像素的值和位置都发生了变化。实验结果表明,该算法具有良好的加密性能和安全性。

关键词:图像加密;混沌理论;改进型 Logistic 映射;Tent 映射
中图分类号:TP391.4 **文献标志码**:A

Research on Image Encryption Algorithm Based on Chaotic Map

Zhao Yu[1], Yang Zhen[2], Yong Jiangping[1], Zhan Aiyun[3], Zhang Yuejin[1]

(1. School of Information Engineering, East China Jiaotong University, Nanchang 330013, China; 2. Network & Information Center, East China Jiaotong University, Nanchang 330013, China; 3. School of Electrical and Automation Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: Traditional text encryption algorithm is not applicable to image encryption, so classical Logistic map has limited range of system parameters and unequal distribution of chaotic sequences. In this paper, an image encryption algorithm based on cyclic shift combined with improved Logistic and Tent map is proposed. The initial values and control parameters of improved Logistic and Tent map were set, and the bitt retake technology was applied to improve the chaos effect in the transition state, so as to improve the effect of image encryption algorithm. When the plaintext image was processed, Arnold transform and XOR pre-encryption were carried out first, and the image was partitioned. Then, the sequence generated by Tent map was used for sorting index and circular shift. In the process of encryption, the plaintext image underwent pixel replacement and pixel diffusion, so that the value and position of the plaintext pixel were changed. Experimental results show that this algorithm has good encryption performance and security.

Key words: image encryption; chaos theory; improved Logistic map; Tent map

收稿日期:2021-11-03
基金项目:国家自然科学基金项目(11862006);江西省自然科学基金项目(2018ACB21032);江西省教育厅科学技术研究项目(GJJ170381;GJJ209928)

信息安全问题,成为每个人以及每个国家的所关心的问题,重视程度也逐渐提高。在国家“互联网+”网络安全战略布局下,对多媒体数据进行加密处理,防止攻击者的盗取和篡改迫在眉睫[1-2]。

现代的加密技术是如今信息安全方面的主要研究方向之一,而混沌的出现将该这个方向的研究推向又一个新的领域。例如,谢涛[1]提出了 Logistic 映射再在密码学中的应用研究,并总结了 Logistic 映射的一些常见的安全缺陷,如映射轨道的短周期性,控制参数的低效率性,映射产生的相邻元素之间的相关性强等问题。为解决控制参数的低效率性,陈志刚等[3]针对 Logistic 序列存在的吸引子与空白区问题,提出一种基于初始值和分形控制参数之间关系的 Logistic 映射改进方法,解决了“稳定窗”与空白区的问题。武剖[4]提出了一种改进的 Logistic 映射,解决 Logistic 映射存在系统参数范围受到限制、混沌序列的分布不均匀等问题。单梁等[5]利用 Tent 映射来构成混沌序列,以此来构造良好的寻优策略,避免了传统优化算法易陷入局部最优点的缺陷,使之较快速地实现全局最优。混沌密码学领域的研究者基于一维混沌系统的安全性差问题,试图通过增加混沌系统的维度,但增加多个控制参数的同时也大大增加其复杂度,借此来改进一维系统的缺点。王文豪等[6]提出了基于二维的 Logistic 映射的图像加密,这样不仅集成了一维 Logistic 映射的优点,但随着多个控制参数的增加,使之行为更加复杂。

综上所述,为满足安全性与算法最优等要求,针对一维混沌系统不能满足要求的缺点,所以本文就提出一种基于二维的混沌映射的图像加密算法[7]。利用 Tent 映射和改进型 Logistic 映射两种混沌模型并结合比特重排技术来生成混沌序列,先利用 Arnold 变换对图像进行预加密,随后利用混沌序列对其进行异或、索引矩阵排序、左循环移位的位数等操作[8]。加密完成后,对图像仿真结果的分析与测试,其中密文图像直方图统计特性均匀平滑,与其他文献相比也具有一定优势,实现了图像的安全加密效果。

1 常用的混沌系统介绍

1.1 Logistic 映射

Logistic 映射[9]是应用最为广泛的一种混沌映射,其在研究时间离散的动力系统时具有较好的特性,且对于研究混沌以及分形控制等方向上是一个经典模型。其数学表达式如下

$$x_{n+1}=\mu x_n(1-x_n),x\in(0,1) \tag{1}$$

式中:$x\in(0,1)$ 为第 n 个混沌位置;μ 为控制参数,当 $\mu\in(3.569\ 94,4]$ 时,系统会不断迭代使之出现其该有的混沌特性,由此可得到 Logistic 映射的混沌序列[10]。当式(1)中取 x=0.72,$\mu\in[2.6,4]$ 时,如图 1 所示,可画出该混沌映射的分岔图。由此可见,μ 取值范围外的参数,系统都会不处于混沌的状态,只有当 $\mu\in(3.569\ 94,4]$ 时,其分岔图才表明其处在混沌状态。

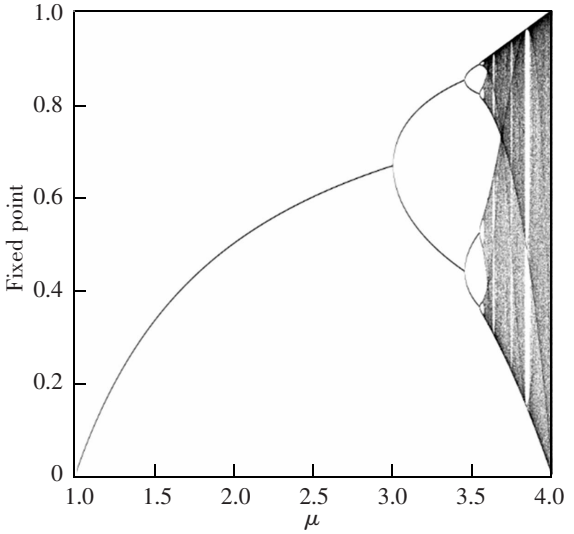


图 1 Logistic 映射分岔图

Fig.1 Logistic mapping bifurcation diagram

1.2 改进型 Logistic 映射

由它所迭代出来的混沌序列值出现吸引子与空白区问题,据图 1 可知,当 Logistic 映射进入到完全混沌状态时,要求 $3.569\ 94<\mu\leqslant 4$,显然其要产生生最佳的混沌效果的取值为 μ=4,那么 Logistic 方程就变成了 x_n+1=4x_n(1−x_n)。但由此产生了一个矛盾性的问题,其中控制参数 μ 就变成了一个常数,使得这样的一个混沌方程不满足参数设置要求,由此导致加密效果的安全性下降问题。常用的 Logistic 映射存在低效率性的问题,希望能用一个函数表达式来代替参数 μ,以解决以上混沌系统中为得到最佳控制参数 μ 而导致的常数化的问题,因此得到了改进的 Logistic 映射最好的混沌效果,并且通过不断迭代,虽然缺少参数 μ 减小了密钥的大小,但复杂度有所提高。改进型 Logistic 映射

方程如下

$$x_{n+1}=\left[3.569\ 945\ 973+(4-3.569\ 945\ 973)\sin\frac{\pi}{2}x_n\right]x_n(1-x_n) \quad (2)$$

式中：x_n 是映射变量，它的取值范围为：$0<x_n<1$。证明函数为

$$y=3.5699\ 459\ 73+(4-3.569\ 945\ 973)\sin\frac{\pi}{2}x \quad (3)$$

式中：自变量的取值范围为 $0<x<1$ 时，y 的值域范围为 $3.569\ 945\ 973<y<4$。对式(3)进行变换，可得

$$x_{n+1}=1-vx_n^2 \quad (4)$$

式中：x_n 为映射变量；v 为映射参量；x_n 和 v 的取值范围分别为：$-1<x_n<1$，$0<v\leqslant 2$。根据式(3)可知，当 $x\in(0,1)$ 时，函数 $y=\left|1-\frac{2}{2-x}x^2\right|$ 的值域为 $[0,1)$。改进型 Logistic 映射分岔图如图 2 所示。

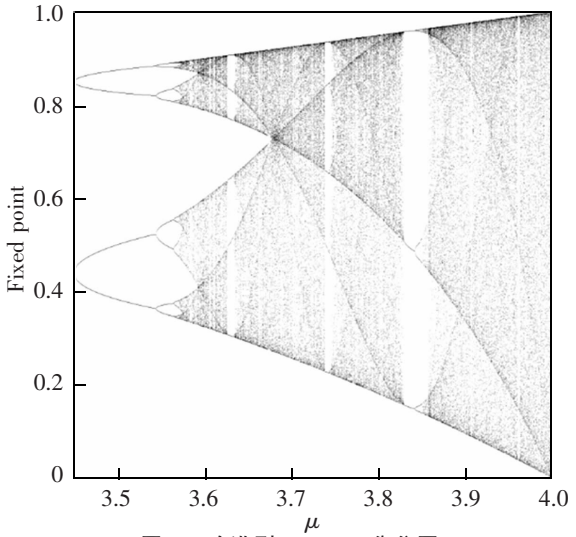


图 2 改进型 Logistic 分岔图

Fig.2 Improved Logistic bifurcation diagram

由图 2 中可知，改进型 Logistic 映射范围相较于传统的 Logistic 映射而言，其映射范围大大增加，可见用一个函数表达式替换控制参数可提升其混沌效果[11]。

1.3 Tent 映射

帐篷映射(Tent map)也是常用的一种分段的线性映射，它的方程形式决定了其函数图像近似于一个帐篷。Tent 映射算法简单，但却是序列复杂的离散映射，多应用于产生伪随机序列，其具有运算速度快、序列分布均匀的优势[12]。Tent 映射被广泛应用于混沌加密系统当中，也在产生混沌扩频码，构造混沌加密系统和实现混沌优选算法等方向等广泛使用[13]。Tent 映射的定义如下

$$x_{n+1}=f(x_n)=\begin{cases}x_n/\alpha, x_n\in[0,\alpha)\\(1-x_n)/(1-\alpha), x_n\in[\alpha,1]\end{cases} \quad (5)$$

如图 3 所示 Tent 映射分岔图，帐篷映射与 Logistic 映射是互为拓扑共轭映射的，所以在控制参数 α 的可取范围内，该系统处于混沌状态[14]。但是当 $\alpha=0.5$ 的时候，系统会呈现短周期状态，为避免使系统陷入这样不动点，应避免取该值。

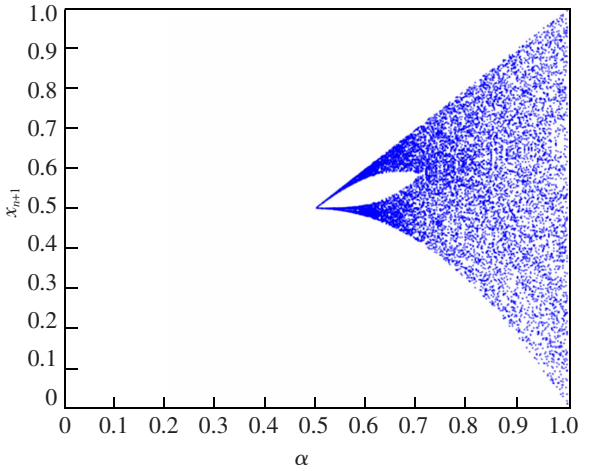


图 3 Tent 映射分岔图

Fig.3 Tent map bifurcation diagram

2 混沌图像加密算法技术

图像置乱效果的预加密可通过 Arnold 的变换与反变换来实现。再通过混沌序列比特重排技术，它用于解决在混沌过渡态中轨道的点差别小，序列值改变量不大的问题，从而使更新序列具有更好的敏感依赖性、伪随机性与遍历性等混沌特性[15]。

2.1 Arnold 变换与反变换

Arnold 变换，亦称猫脸变换[16]。Arnold 变换因为其直观简易的特性被应用于矩阵的置乱，每运行一次 Arnold 变换，就相当于对该图像矩阵进行了一次置乱。由于 Arnold 变换使用的矩阵维度很小，所以只使用一次变换得到的结果依旧能看出图像的部分纹理形状等特征，所以使用多次迭代是不可避免的，只有当以上特征不再能通过人眼观察到时，才算有意义的变换。Arnold 变换常用于图像预加密，方程定义如下

$$\begin{pmatrix}i'\\j'\end{pmatrix}=\begin{pmatrix}1&1\\1&2\end{pmatrix}\begin{pmatrix}i\\j\end{pmatrix}(\mathrm{mod}\ N) \quad (6)$$

式中：(i,j) 为变换前的位置；(i',j') 为变换后的位置

坐标。将式(6)进行推广得

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} 1 & b \\ a & ab+1 \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} (\mathrm{mod}\ N) \tag{7}$$

式中:a,b 为正整数;N 为图像矩阵的阶数;mod N 为取模返回余数。

运用 Arnold 变换时,如图 4 所示,首先对图像的水平方向进行割补变换,其次再对竖直方向的割补变换,最后的模运算就是将之前操作扩展的部分进行切割回填操作。

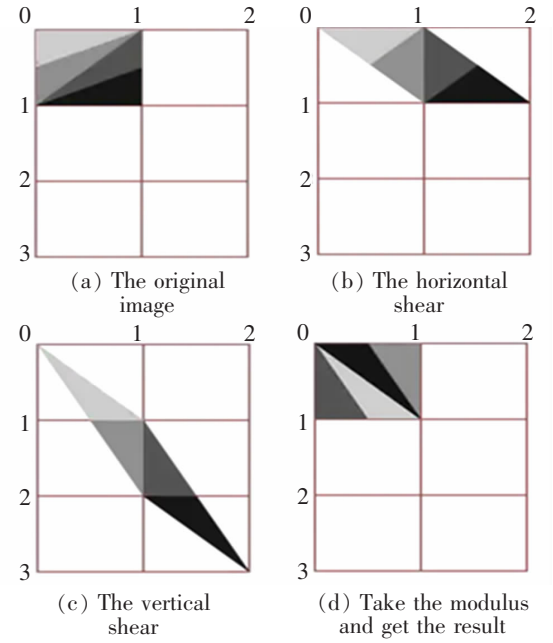


图 4 Arnold 变换示意图

Fig.4 Schematic diagram of Arnold transformation

Arnold 变换显然是有周期的,即在对图像进行反复 Arnold 变换后,在其周期范围内,不断地迭代变换会使得各个被置乱的像素位置一定会被置换回到原处。由此产生的问题在于如果利用该方法来恢复原图,就必然出现工作量庞大的后果,而且还必须计算其与图像有关的周期,这无疑不是合适的反置换算法。对此 Arnold 反变换发挥了作用,其公式如下

$$\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}^{n} \begin{pmatrix} i' \\ j' \end{pmatrix} (\mathrm{mod}\ N) \tag{8}$$

根据式(7)可以推出广义的 Arnold 变换

$$\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} ab+1 & -b \\ -a & 1 \end{pmatrix}^{n} \begin{pmatrix} i' \\ j' \end{pmatrix} (\mathrm{mod}\ N) \tag{9}$$

利用 Arnold 反变换的方法可使置乱图像恢复,不必花费时间先计算其周期,再去进行多次的 Arnold 变换。使用 Arnold 反变换后,可根据需求使其恢复到任意一次的置乱结果,并对其进行比较分析,工作效率大大提升。

2.2 混沌序列比特重排

当系统的初始值及其控制参数产生微小的改变时,处于混沌过渡态中,按此进行迭代产生的值显然具有高度的相似性,衍生轨道相近且具有一致的起伏特性,显然利用这样的值进行量化操作时,不可避免地出现大概率相同的值或相近的值,使序列值出现了一定的统计特性,而不具备良好的随机性。由此,设计出能够针对差异小的序列使之处理差异较大的值。下面介绍一种混沌序列比特重排技术,从而避免以上问题,使之具有更加出色的伪随机性,更符合使用要求。比特重排技术的过程具体步骤如下。

1) 由设置好的密钥产生的初值带入使用到的混沌方程中,迭代后得到一个混沌序列值 a。根据自己设计要求,将这个数 a 化为 L 位的二进制形式。例如,当一个序列值 a=0.63,把 0.63 写成 L 位的二进制形式,其中 L 可以取任意的正整数,这里假设 L=12,那么 0.63→0.1010 0001 0100。

2) 我们将小数部分二进制化,按照规则重新排序,将奇数位比特值倒序排在前半部分,将偶数位比特值倒序排在后半部分,得到一个新的数,示意图见图 5 所示。

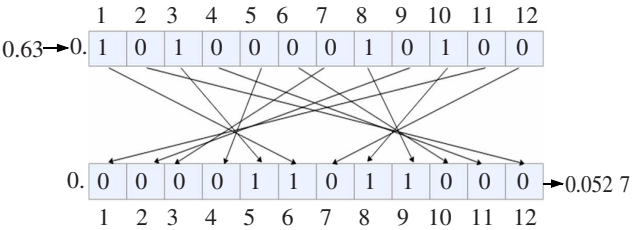


图 5 比特重排示意图

Fig.5 Bit rearrangement diagram

3) 最后将得到小数部的二进制数转化为常用的十进制数,以此值作为新的初始值代入公式,得到新的一个带排序得值。如此重复步骤,即可得到重排后混沌序列。

3 基于循环移位和多混沌映射的图像加密算法

本文提出一种基于循环移位和多混沌映射的图像加密算法。首先根据设好的密钥来控制 Tent 映

射和改进型 Logistic 映射的生成，使用比特重排技术生成新的重排混沌序列。并针对明文图像要先进行 Arnold 变换的预加密。为保证主要图像与序列的连续性，将其进行分块处理，并由重排 Tent 映射完成对该分块区域内的置乱操作，由 Logistic 映射完成循环移位的扩散操作。完成后，最后对图像仿真结果进行分析与测试。

3.1 图像加密算法参数设置

根据上文提出的改进型 Logistic 和 Tent 映射，若是直接设置各初始值和控制参数值显然不安全，采用下式生成这些值

$$x_{01}=\frac{1}{a_1}+t_1 \tag{10}$$

$$x_{02}=\frac{1}{a_2}+t_2 \tag{11}$$

$$\alpha=\frac{1}{a_2}+t_3 \tag{12}$$

式中：a_1,a_2,t_1,t_2,t_3 是算法的密钥；x_{01} 是改进型 Logistic 的初始值；x_{02} 和 α 是 Tent 映射的初始值和控制参数。具体密钥如表 1 所示，其中 r_1 和 r_2 为各自的迭代次数。

表 1 密钥参数设置

Tab.1 Key parameter setting

Parameters of the category	Parameter value
Generation parameters of improved Logistic chaos system	a_1=127，t_1=0.8，r_1=500
Tent chaos system generates parameters	a_2=117，t_2=0.001，t_3=0.001，r_2=500

3.2 图像加密过程

本文的图像加密算法如图 6 所示，由设置好的密钥输入各混沌系统，经重排得到混沌性能良好的序列。先对明文图像进行 Arnold 变换的预加密，为避免序列和图像的连续性，拟采用分块处理的模式。分块后使用重排后改进型 Logistic 序列完成对该部分的循环移位，使像素值发生改变完成扩散操作，用 Tent 序列完成像素位置点的置乱，以加快索引排序时间，使之更高效，最后对分块加密后的图像进行组合即可得到与明文大小相等的密文图像。加密步骤如图 6 所示。

1）通过运用改进型 Logistic 混沌系统生成混沌序列 $Q_1(i)$。由式(10)生成 Logistic 混沌映射的初值输入到 Logistic 映射方程式进行迭代，迭代 r_1+MN 次。舍弃前 r_1 项，由式(10)比特重排后得到 $Q_2(i)$。由式(13)得到的序列进行量化，转变成与明文图像大小一样的矩阵。

$$F=\mathrm{mod}(\mathrm{floor}(K\times 10^8),256) \tag{13}$$

式中：函数 floor(x)返回不大于 K 的最大整数。

2）由改进型 Tent 混沌系统生成混沌序列 $U_1(i)$。由式(11)、式(12)生成 Tent 混沌映射的初值带入到 Tent 映射方程式(5)进行迭代，迭代 r_2+MN 次。舍弃前 r_2 项，由式(11)比特重排后得到 $U_2(i)$。同(1)将得到的序列进行量化，转变成与明文图像大小相同的矩阵。

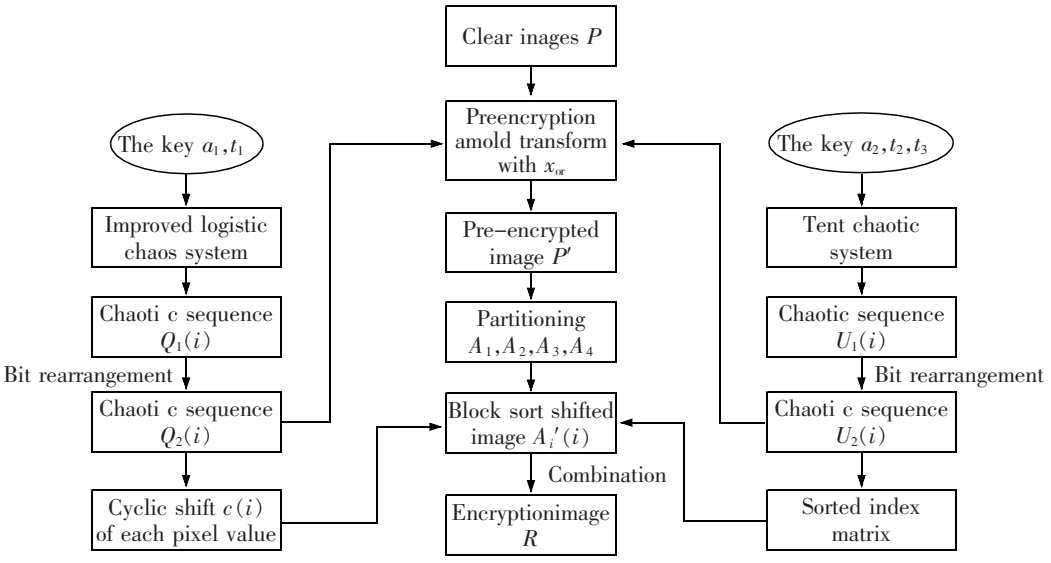


图 6 加密流程

Fig.6 The encryption process

3) 对图像 P 进行预加密。利用式(9)将明文进行 Arnold 变换,并利用式(14)与对应序列逐次进行异或。

$$\begin{cases} P'(1)=P\oplus Q_2(1)\oplus U_2(1), i=1 \\ P'(i)=P(i)\oplus P(i-1)\oplus Q_2(i)\oplus U_2(i), i\neq 1 \end{cases} \tag{14}$$

4) 生成索引矩阵。由式(15)将序列 $U_2(i)$ 转换成 M 行 N 列的二维矩阵 $\boldsymbol{B}$,由式(16)对二维矩阵 $\boldsymbol{B}$ 进行排序,得到索引矩阵 index $\boldsymbol{B}$

$$\boldsymbol{B}=\text{reshape}(U_2(i),[M,N]) \tag{15}$$

$$[\text{sort }\boldsymbol{B},\text{index }\boldsymbol{B}]=\text{Sort}(\boldsymbol{B}) \tag{16}$$

5) 分块进行置乱-扩散操作。将 P' 分成 A_1,A_2,A_3,A_4 于 4 块进行处理,以 A_1 为例。

① 对 A_1 进行像素替换。根据式(17),利用索引矩阵 index $\boldsymbol{B}$ 将像素进行索引排序,得到替换后图像 A_1',具体替换方式根据式进行处理。

$$R'(i,j)=R(\text{index }\boldsymbol{B}(i,j),j) \tag{17}$$

② 对图像 A_1'进行循环移位。通过式(18)求出对应位置的循环移位的位数得到 A_1'。再通过方程(19)将 A_1'循环移位得到 A_1''图像。

$$c(i)=\text{mod}(Q_2(i),7)+1 \tag{18}$$

$$R(i)=\text{circshift}(R(i),c(j)) \tag{19}$$

6) 将 A_1'',A_2'',A_3'',A_4''整合,得到密文 R。

3.3 图像解密过程

由于在设计加密算法之时就必须考虑到每一步流程的可逆性问题,所以在对密文解密时仅需进行逆向推导即可。解密算法的流程图如图 7 所示,通过设置好的密钥参数来得到序列。先分块进行逆向操作,通过 Tent 混沌映射和改进型的 Logistic 混沌映射完成反移位和反置乱排序索引,再对各分块进行组合,最后使用 Arnold 反变换和反异或的处理,即可求解得到解密图像。

1) 由图 5 中的加密过程中的式(1)、式(2)得到 Logistic 映射和 Tent 映射的混沌序列和。

2) 分块。将密文 C 分成 B_1,B_2,B_3,B_4 于 4 块进行处理,以 B_1 为例。

3) 由图 7 加密过程中式(4)得到索引矩阵,进行逆排序索引。

4) 反循环移位。由式(18)计算出像素循环移位的位数 $D(i)$,由式(20)对 D_1 进行右循环移位得到 D_1'。

$$D'(i)=\text{circshift}(-R(i),D(i)) \tag{20}$$

5) 由式(8)对密文图像 D′进行 Arnold 反变换,并进行序列异或操作求解图像矩阵,得到解密图像 R。

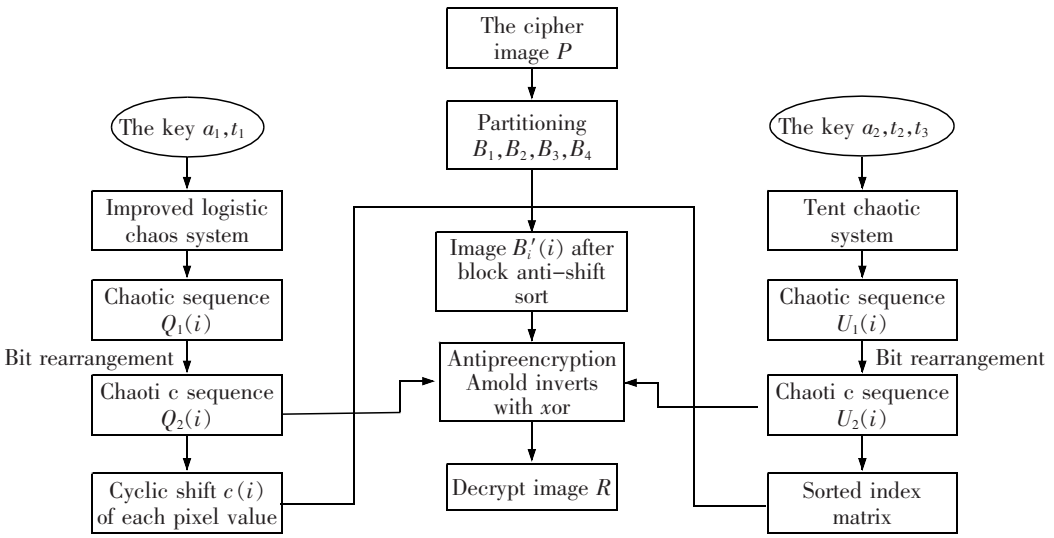


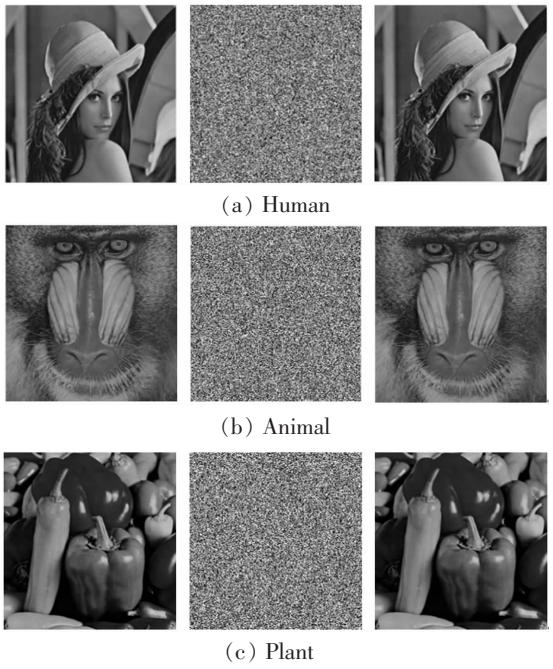
图 7 解密流程

Fig.7 Decryption process

4 实验结果与性能指标分析

4.1 实验结果

本文对 3 个大小为 256×256 的灰度图像进行加密,其名称分别是 Human,Animal,Plant。实验环境为 Windows10,MatlabR2014b。完成导入图像和添加密钥后,运行本文算法,得到加密图像和解密图像。



(a) Human

(b) Animal

(c) Plant

图 8 Human, Animal, Plant 图像加密、解密效果

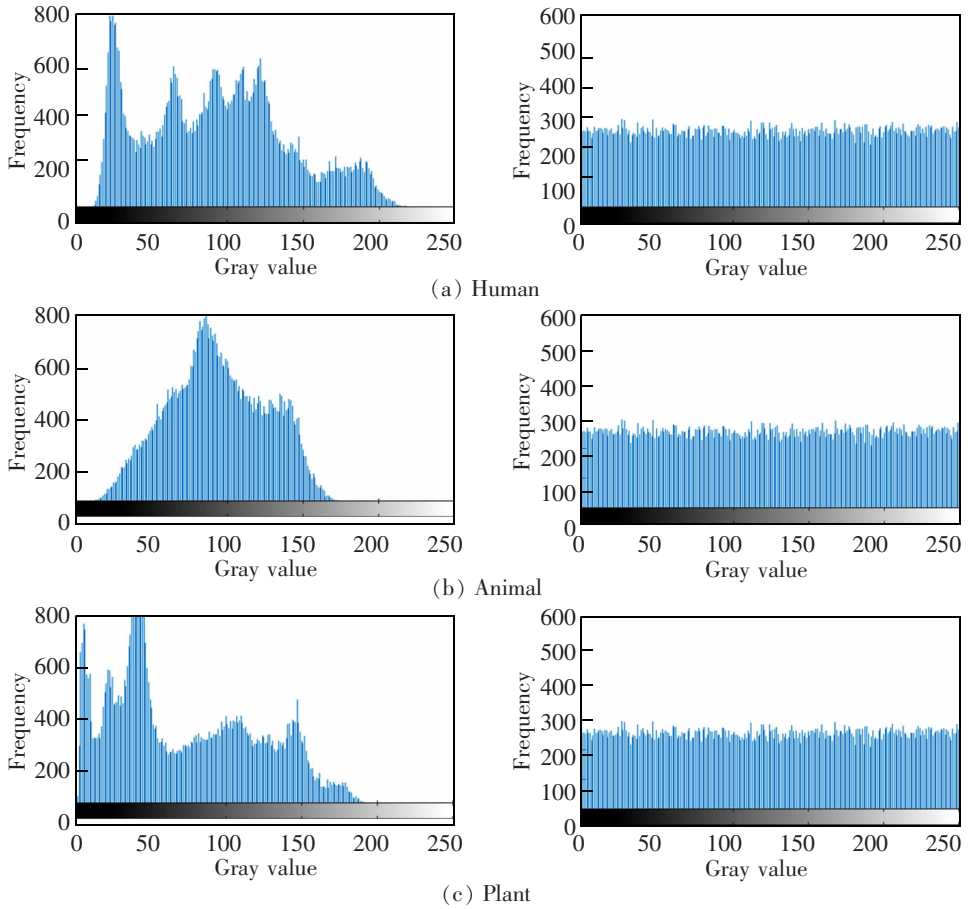
Fig.8 Human, Animal, Plant image encryption and decryption effect

图 8 分别是各自的明文和密文以及解密结果的显示结果。从直观看,人们是无法针对其中的密文得到任何信息的,因为以上的 3 幅加密效果图中都不存在任何的轮廓、纹理和形状等特征。而解密后可看到其与原图一致,没有任何像素点的损失。

4.2 性能指标分析

1) 密钥空间。如上所述,密钥空间必须大于 2^{100} 才符合加密算法的要求,本文算法密钥空间符合要求。由于当前 a_1,a_2,t_1,t_2,t_3,前期迭代次数 r_1,r_2,可得每一个数据的最小偏差为 10^{-15},由此可计算出算法的密钥空间大小为 $(10^{15})^7\approx 2^{348}$,由可知其对于穷举攻击的破解方法具有较强的抵抗效果。

2) 直方图分析。在图像的指标分析中,灰度直方图主要是针对图像的各个像素值频数进行统计,从而形成客观的图形数据。当该图像各个像素出现次数基本相同时就是趋于一条直线时,它不再会因为统计特性而被攻击。本次直方图分析同样是使用之前的 3 幅图像,进行明文和密文之间的对比效果(图 9)。



(a) Human

(b) Animal

(c) Plant

图 9 Human, Animal, Plant 明文直方图(左)、密文直方图(右)

Fig.9 Human, Animal, Plant plaintext histogram(left), ciphertext histogram(right)

如图 9 所示，明文的直方图分布是由高峰和低谷的,甚至会出现一部分灰度区间完全空白,显然这样的直方图具有很强的特征。由于每一幅图像的直方图是唯一的，该明文如果只进行位置的置乱操作显然不能改变直方图。但经过加密后得到的密文图像直方图是很均匀平滑的，其中显示的各个区间的像素值出现的概率基本上很相近，对直方图无法进行特征统计攻击,表明该算法具有良好的加密效果。

3）相邻像素相关性分析。由于图像蕴含一定信息,表明在其图像的一定区间内具有连续性和相似性,需要对加密前后的各个方向上的相关性进行计算分析,以此来判断本文加密算法的性能。前面已经对相关系数计算公式进行了说明,在测试加密图像时,会使用一个随机矩阵来确保选择的点的无序性,为使该样本数量较多,可以利用两个随机矩阵来选择对应的行与列，该方式选择了 8 000 对符合要求的像素点。在边界处选择的相邻点需要注意规则,遇到边界就向图像中心方向取点,而不是舍弃或循环至另一边。

对以上的测试图像进行相邻像素相关性分析，各个方向上的分布结果如图 10 所示，图中横坐标为(x,y)处的像素值,纵坐标为$(x+1,y)$处的像素值,相关系数值如表 2 所示。

由图 10 可知，我们随机选择的相邻像素点具有很大的相关性，这些像素点大致分布在倾角为45°的直线上,这表明当我们取一个点的像素值时,其周边都是与之大小很相近的像素值。而反观密文图像时，我们发现相邻点却散落分布在各个区域，

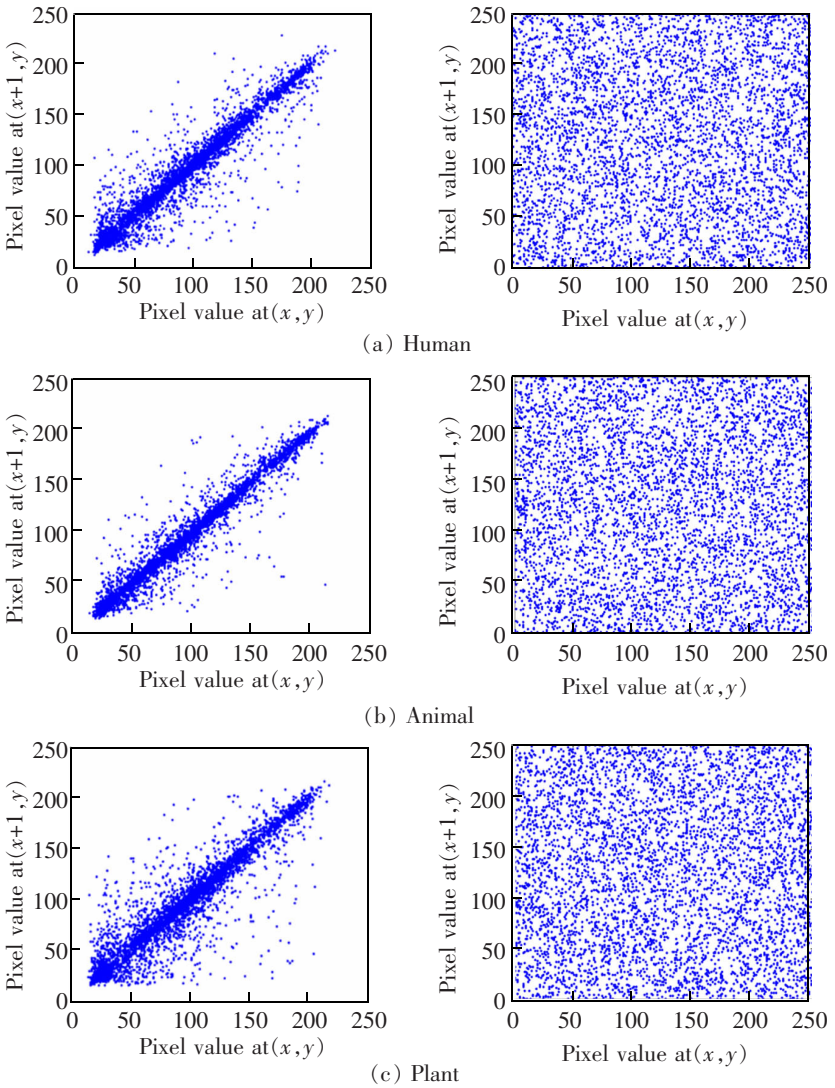


图 10　Human, Animal, Plant 水平、垂直及对角方向对比

Fig.10　Horizontal, vertical and diagonal contrast of Human, Animal, Plant

可以说相邻的像素点不存在任何联系,无法由该点像素值推测其附近的大小范围。具体相关性测试数据如表 2 所示。

表 2 明文和密文相邻像素相关系数

Tab.2 Correlation coefficient of adjacent pixels between plaintext and ciphertext

The test image	Plaintext, ciphertext	The horizontal direction	The vertical direction	Diagonal direction
Human (256×256)	Plaintext image	0.951 9	0.973 5	0.926 2
	Ciphertext image	0.003 1	−0.003 3	0.000 6
Animal (256×256)	Plaintext image	0.896 2	0.861 6	0.808 8
	Ciphertext image	−0.016 4	−0.000 5	−0.000 9
Plant (256×256)	Plaintext image	0.969 0	0.970 8	0.940 4
	Ciphertext image	0.003 1	−0.000 8	0.001 6

由表 2 可知,明文图像在这 3 个方向上的相关性系数都接近于 1, 尤其是 Human 和 Plant 图像都是在 0.92 以上,即其图像包含的内容越多所蕴含的信息就越多,相邻像素点的相关性就越高。反观加密后的图像数据,它们的值都已经大大减小,趋近于 0。由此可知,本文设计的图像加密算法可有效降低其各个相邻点的像素相关性,表明之前的置乱扩散等操作效果明显。同样使用 Human 图像和其它文献进行对比,如表 3 所示。

表 3 不同算法相邻像素相关系数对比

Tab.3 Comparison of correlation coefficients between adjacent pixels of different algorithms

Algorithm	Plaintext, ciphertext	The horizontal direction	The vertical direction	Diagonal direction
This paper	Plaintext	0.951 9	0.973 5	0.926 2
	Ciphertext	0.003 1	−0.003 3	0.000 2
Reference [17]	Ciphertext	0.003 7	0.002 5	0.002 9
Reference [18]	Ciphertext	0.004 9	0.004 1	−0.002 6
Reference [19]	Ciphertext	0.000 2	−0.003 2	0.002 1

由表 3 可知,对 Human 图像的加密效果优于文献[18],本算法在水平方向差于文献[17],但是垂直方向和对角方向优于文献[17]。与文献[19]相比,本算法水平、垂直方向上的相关系数差于该文献,对角方向上优于该文献。

4) 信息熵分析。图像的信息熵是人们常用来评估其图像信息各个取值及其占比的指标,其利用图像集合内各个数据及其权重计算的结果。当该图像的信息熵数值越大就表明其混乱程度越大。信息熵的理想值为 8, 实验对这 3 幅图像进行测试的结果如表 4 所示。

表 4 测试图像信息熵

Tab.4 Test image information entropy

The test image	Plaintext image	Ciphertext image
Human(256×256)	7.391 2	7.989 3
Animal(256×256)	6.996 5	7.989 5
Plant(256×256)	7.276 0	7.989 6

由表 4 可知,明文的信息熵在 7 左右,而通过加密后其信息熵大致都很接近 7.99,与理想值 8 很接近。表明在加密过程中的扩散等操作可使各个区间内的像素值都趋于平滑,使其分布特征不具备弱点。如表 5 所示,选择了一些数据与其他文献中的算法结果进行了对比。

表 5 不同算法的信息熵对比

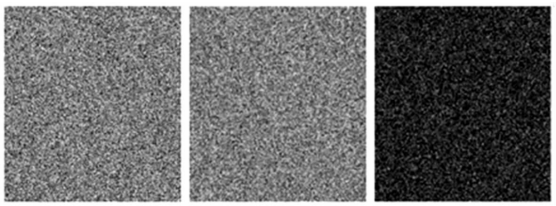
Tab.5 Information entropy comparison of different algorithms

Algorithm	The test image	Ciphertext image information entropy
This paper	Human(256×256)	7.989 3
Reference [21]	Human(256×256)	7.997 8
Reference [22]	Human(256×256)	7.980 1
Reference [23]	Human(256×256)	7.975 4
This paper	Plant(256×256)	7.989 6
Reference [22]	Plant(256×256)	7.989 4
Reference [23]	Plant(256×256)	7.989 9

由表 5 的对比结果可知, 在 Human 图对比中,本文的加密算法的信息熵优于文献[18],[19],但略低于文献[17];在 Plant 图对比中,本文算法的信息熵比其他文献的信息熵略差,但相差微小。这表明

本文的加密算法在针对不同图像时各有优劣,还存在一定不足。

5) 密钥敏感性分析。当利用密钥参数输入到设计的加密系统中时, 选择一个密钥来对其进行测试,如在该数值上进行微小变化,加上或减去 10~14 这样一个很小的值,再对明文图像进行加密,并对密钥变化前后密文图像分析, 并通过作差处理得到作差图像,如图 11 所示。



(a) The ciphertext image is not changed (b) The changed ciphertext image (b) The difference before and after changes

图 11 密钥敏感性

Fig.11 Key sensitivity

图 11(a)为不改变加密密钥的密文图像,图 11(b)为改变其中一个密钥的密钥参数,图 11(c)为图 11(a)和图 11(b)差值图。可以看到细微加密密钥的不同而导致的加密效果差别很大,由此可知,经过一系列处理后得到的混沌序列具有很强的敏感性。

6) 抗差分攻击分析。为了得到一张与原明文图像相差很小的图像矩阵, 可以对 Human 明文图像进行读取后, 将其中一个点的像素值减去 1,再用该矩阵通过相同的加密算法系统, 利用式(21)和式(22)对图像进行相关性分析,计算微小的明文改动对于整体加密效果的影响。从文献[16]可知,NPCR 的理想值为 99.609 6%,UACI 的理想值为 33.46%。其计算结果同其它文献中提出的算法相比较如表 6 所示。

表 6 使用 Human(256×256)测试与其它算法的对比

Tab.6 Comparison between the test by Human(256×256) with other algorithms

%

Algorithm	The average NPCR/%	The average UACI
This paper	99.55	33.38
Reference [17]	99.61	29.45
Reference [18]	99.61	29.45
Reference [19]	99.65	33.55

$$R_{x,y} = \frac{\mathrm{cov}(xy)}{\sqrt{D(x)D(y)}} \tag{21}$$

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

由表 6 对比,本文算法同其他文献相比较各有千秋, 平均 NPCR 虽然略微差于文献 [17], 平均 UACI 差于文献[19],但是相较于其他而言有微小优势,这表明一个良好的加密算法那能够抵抗差分攻击[25]。

5 结论

本文提出了一种基于循环移位和改进型 Logistic 映射和 Tent 映射的图像加密算法。

1) 使用 Arnold 变换技术和比特重排方法, 解决在混沌过渡态中轨道的点差别小,序列值改变量不大的问题。

2) 明文图像经历了像素的置乱和扩散处理,使其具有更好的随机性。

3) 根据前面的性能指标分析得出:密文图像直方图统计特性均匀平滑,密钥空间大,相邻像素间的相关系数大大降低而趋于 0,信息熵也接近于 8,抗差分数据分析接近理想值,与其他文献相比也具有一定优势,实现了图像的安全加密效果。

参考文献:

[1] 谢涛. Logistic 映射在密码学中的应用研究[D]. 湘潭:湘潭大学,2014.
XIE T. Application of logistic mapping in cryptography[D]. Xiangtan: Xiangtan University,2014.

[2] 周伟. 基于广义帐篷映射的图像加密算法[D]. 汕头:汕头大学,2011.
ZHOU W. Image encryption algorithm based on generalized tent mapping[J]. Shantou:Shantou University,2011.

[3] 陈志刚,梁涤青,邓小鸿,等. Logistic 混沌映射性能分析与改进[J]. 电子与信息学报,2016,38(6):1547-1551.
CHEN Z G,LIANG D Q,DENG X H,et al. Performance analysis and improvement of Logistic chaotic mapping[J]. Journal of Electronics and Information Technology, 2016,38(6):1547-1551.

[4] 武剀. 对经典 Logistic 映射图像的加密方案的改进及数字图像的双混沌加密技术探究[D]. 乌鲁木齐:新疆财经大学,2016.
WU K. The improvement of the encryption scheme of the classical Logistic mapping image and the research of the double chaotic encryption technology of digital image are

discussed[D]. Wulumuqi:Xinjiang University of Finance and Economics,2016.

[5] 单梁,强浩,李军,等. 基于 Tent 映射的混沌优化算法[J]. 控制与决策,2005(2):179-182.
SHAN L,QIANG H,LI J,et al. Chaotic optimization algorithm based on Tent map[J]. Control and Decision,2005(2):179-182.

[6] 王文豪,刘殷雷. 基于二维 Logistic 混沌序列的图像加密算法研究[J]. 长春理工大学学报(自然科学版),2010,33(4):111-113.
WANG W H,LIU Y L. Research on image encryption algorithm based on 2D logistic chaos sequences[J]. Journal of Changchun University of Science and Technology(Natural Science Edition),2010,33(4):111-113.

[7] 谭琳. 基于 DNA 序列和混沌的图像加密算法[J]. 信息工程,2014,11(20):90-92.
TAN L. Image encryption algorithm based on DNA sequence and chaos[J]. China CIO News,2014,11(20):90-92.

[8] 于竿. 基于混沌的图像加密算法研究[D]. 兰州:兰州大学,2014.
YU G. Research on image encryption algorithm based on chaos[D]. Lanzhou: Lanzhou University,2014.

[9] 乔建平. 基于二维 Logistic 混沌系统的图像加密算法分析[J]. 江苏科技信息,2021,38(28):34-36.
QIAO J P. Image encryption algorithm analysis based on two dimensional Logistic chaotic system[J]. Jiangsu Science & Technology Information,2021,38(28):34-36.

[10] 李春虎,罗光春,李春豹. 基于斜帐篷混沌映射和 Arnold 变换的图像加密方案[J]. 计算机应用研究,2018,35(11):3424-3427.
LI C H,LUO G H,LI C B. Image encryption scheme based on skew tent chaotic map and Arnold transformation [J]. Application Research of Computers,2018,35(11):3424-3427.

[11] LI P,LO K T. Survey on JPEG compatible joint image compression and encryption algorithms[J]. IET Signal Processing,14(8):475-488.

[12] RAZA S F,SATOUTE V. A novel bit permutation-based image encryption algorithm[J]. Nonlinear Dynamics,2019,95:859-873.

[13] WANG J,GENG Y,HAN L,et al. Quantum image encryption algorithm based on quantum key image[J]. International Journal of Theoretical Physics,2019,58:308-322.

[14] ZHANG L,ZHANG Z,YE H,et al. Multi-image holographic encryption based on phase recovery algorithm and ghost imaging[J]. Applied Physics B,126(8):136.

[15] ZHU C,SUN K. Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps[J]. IEEE Access,2018,6(1):18759-18770.

[16] 张艳鹏,侯冬梅,杨倩,等. 基于混沌同步技术的图像加密算法设计研究[J]. 现代电子技术,2021,44(19):39-42.
ZHANG Y P,HOU D M,YANG Q,et al. Research on image encryption algorithm design based on chaos synchronization technology[J]. Modern Electronics Technique,2021,44(19):39-42.

[17] 彭静静. 基于混沌系统的图像加密算法研究[D]. 开封:河南大学,2020.
PENG J J. Research on image encryption algorithm based on chaotic system[D]. Kaifeng:Henan University,2020.

[18] 陈军,张向利,张红梅. 基于 Lorenz 映射和 Logistic 映射的图像分块加密算法[J]. 桂林电子科技大学学报,2019,39(1):76-81.
CHEN J,ZHANG X L,ZHANG H M. An image block encryption algorithm based on Lorenz map and Logistic map [J]. Journal of Guilin University of Electronic Technology,2019,39(1):76-81.

[19] 吕群,薛伟. 结合混沌系统和动态 S 盒的图像加密算法[J]. 小型微型计算机系统,2018,39(3):607-613.
LYU Q,XUE W. Image encryption algorithm combining chaotic system and dynamic s-boxes[J]. Journal of Chinese Computer Systems,2018,39(3):607-613.

[20] 王宾. 混沌理论在图像加密中的研究与应用[D]. 大连:大连理工大学,2013.
WANG B. Research and application of chaos theory in image encryption[D]. Dalian:Dalian University of Technology,2013.

第一作者:赵雨(1997—),女,硕士研究生,研究方向为医学图像处理。E-mail:1604046196@qq.com。

通信作者:张跃进(1978—),男,教授,博士,硕士研究生导师,华中科技大学、加拿大麦克马斯特大学(McMaster University)访问学者。研究方向为计算机应用技术,图像处理技术,算法分析和机械生物技术。2017 年获华中科技大学生物医学工程博士学位。E-mail:zyjecjtu@foxmail.com。

(责任编辑:吴海燕 姜红贵)