基于Logistic与标准映射的数字图像加密算法

胡春强 邓绍江 秦明甫 黄桂林
(重庆大学计算机学院 重庆 400030)

摘 要 基于Logistic和标准映射,提出了新的数字图像加密算法。首先利用离散混沌系统初值敏感性、参数敏感性和具有白噪声统计特性的特点,结合Logistic映射和标准映射设计了置乱变换系统,这种置乱是依赖于密钥的。接着通过一种替代变换使置乱后图像的像素灰度值改变并产生互相依赖,即将每一像素值扩散到其它像素中去。这样,加密算法便具有置乱、替代、扩散等加密系统的基本要素。实验仿真和分析表明,该算法密钥空间大,易于实现,有较好的加密效果和统计特性。

关键词 Logistic映射,标准映射,图像加密,图像置乱变换
中图法分类号 TP309 **文献标识码** A

Image Encryption Algorithm Based on Logistic and Standard Map

HU Chun-qiang DENG Shao-jiang QIN Ming-fu HUANG Gui-lin
(College of Computer, Chongqing University, Chongqing 400030, China)

Abstract Based on Logistics and Standard Map, a new image encryption algorithm was proposed. By using the properties of chaotic map such as sensitive to initial values, sensitive to parameters and the statistic specialty of white noise, the confusion system was designed through discrete chaotic map and standard map. This confusion is dependent on the secret keys generated by a different chaotic system. Then changed the pixel values of encrypted image through the substitution system and made pixels associated with each other. At the same time, every pixel value was diffused to others. The system contains confusion, substitution and diffusion, which are necessary factors for a good cryptosystem. The experimental simulation and analysis illuminate that the algorithm has such advantages: larger key space, easily realized and perfect statistical characteristics.

Keywords Logistic map, Standard map, Image encryption, Image scrambling transform

随着网络技术的发展和信息交换的日益频繁,信息安全问题也越来越突出。当涉及到国家安全、重大商业利益或者个人隐私问题的数字图像需要在网络上传输时,图像数据的安全与保密就显得尤为重要。对图像进行加密是保证图像信息安全的重要手段之一,但是由于数字图像具有数据量大、数据相关度高等特点,用传统的加密方式效率比较低。近年来兴起的混沌加密技术为图像加密提供了一种新的有效途径,混沌加密的研究也成为密码研究领域的一个热点[1-6]。

混沌是一种貌似无规则的运动,是在确定性非线性系统中不需附加任何随机因素也可出现的一种内在随机性,因此其伪随机行为能准确再生。混沌系统具有下面几个重要特性:对初始条件和系统参数的极端敏感性、拓扑传递性、周期点的稠密性(系统具有很强的确定性和规律性)[7]。这些特性与密码学要求的扩散、混合和随机特性相吻合。如果把系统的参数或初值作为密钥,混沌系统就成为一个具有优良密码特性的密码系统[8]。

本文提出了一种新的基于混沌序列的图像加密方法,即在Logistic映射和标准映射的基础上,构造一种具有强非线性耦合结构的置乱变换(类似于传统加密方式中的Feistel结构)来实现图像像素位置的置乱变换。然后对置乱后像素的灰度值进行替代变换,并将每一个像素值扩散到密图其他像素中,以改变图像的统计特性,达到更好的加密效果。

1 算法原理

1.1 Logistic混沌映射

Logistic映射是一种可产生混沌的非线性系统[9-12],其模型为

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

式中,$0<\mu\leqslant 4$,$0<x<1$,$n\in N$,μ为分岔参数,x_n在区间[0,1]上遍历。研究表明,当$3.569945\cdots<\mu\leqslant 4$时,映射处于混沌状态。

1.2 标准映射

人们对于弹跳球模型的研究由来已久,标准映射是弹跳

到稿日期:2010-01-08 返修日期:2010-03-18 本文受国家自然科学基金(No. 60873201, 60973114),重庆市自然科学基金(No. 2009BA2024,2008B2193),重庆大学"输配电装备及系统安全与新技术"国家重点实验室自主课题(2007DA10512709207)资助。

胡春强(1982-),男,博士生,主要研究方向为信息安全、混沌密码学、图像处理,E-mail:hcq0394@cqu.edu.cn;邓绍江(1971-),男,教授,硕士生导师,主要研究方向为信息安全、混沌理论;秦明甫(1982-),男,硕士,主要研究方向为信息安全、图像处理;黄桂林(1982-),男,硕士生,主要研究方向为计算技术、信息安全。

球模型在高弹跳情形下的二维映射。标准映射形式上为显函数，却具有极其丰富的动力学性质，是研究混沌现象的基本模型，其理论意义重大，已在理论物理、力学等各个领域得到了深入研究。

在混沌动力学中有一种标准映射，其定义如下[2]

$$S(x,y)=(S_1,S_2)=((x+y)\bmod 2\pi,(y-k\sin(x+y))\bmod 2\pi) \tag{2}$$

式中，参数 k 为正常数。式(2)可推广为

$$\begin{cases}S_1(x,y)=(x+F(y))\bmod 2\pi\\ S_2(x,y)=(y+G(S_1))\bmod 2\pi\end{cases} \tag{3}$$

易知式(3)的逆为

$$\begin{cases}x=(S_1-F(y))\bmod 2\pi\\ y=(S_2-G(S_1))\bmod 2\pi\end{cases} \tag{4}$$

2 算法设计

2.1 置乱变换

为了设计置乱变换系统，需要先将式(3)和式(4)离散化。

$$\begin{cases}S_1(i,j)=(i+\phi(j))\bmod N\\ S_2(i,j)=(j+\varphi(S_1))\bmod N\end{cases} \tag{5}$$

及

$$\begin{cases}i=(S_1-\phi(j))\bmod N\\ j=(S_2-\varphi(S_1))\bmod N\end{cases} \tag{6}$$

由此可设计置乱变换为

$$\begin{cases}i'=(i+\phi(j))\bmod N\\ j'=(j+\varphi(i'))\bmod N\end{cases} \tag{7}$$

易知式(7)的逆为

$$\begin{cases}i=(i'-\phi(j))\bmod N\\ j=(j'-\varphi(i'))\bmod N\end{cases} \tag{8}$$

其中，i,j,i',j',N 均为整数。函数 $\phi(\cdot)$ 和 $\varphi(\cdot)$ 应选择为对其各自的自变量充分敏感的函数，而混沌系统刚好满足这一特性，因此选取函数 $\phi(\cdot)$ 和 $\varphi(\cdot)$ 为

$$\begin{aligned}&\phi(j)=(j+\mathrm{round}(j\cdot c_n))\bmod N\\ &\phi(i')=(i'+\mathrm{round}(i'\cdot c_n'))\bmod N\\ &n=1,2,\cdots,N\times N\end{aligned} \tag{9}$$

式中，round 函数表示按四舍五入方式求整数，c_n，c_n' 为密钥序列，由 Logistic 映射迭代式(1)产生，且在 Logistic 映射控制参数为 μ_1、初值为 $c(0)$ 时产生 c_n；在控制参数为 μ_2、初值为 $c'(0)$ 时产生 c_n'。为了取得更好的随机性，取迭代 m 次(可设 $m>10000$)以后的迭代值。

应用式(8)可以对大小为 $N\times N$ 的数字图像进行像素置乱变换。在上述系统中，i,j 为图像像素的当前位置坐标，i'，j' 为置乱后该像素的位置坐标。

由此可得置乱变换系统的密钥为

$$\begin{aligned}&Key1=(\mu_1,c(0),m)\\ &Key2=(\mu_2,c'(0),m)\end{aligned} \tag{10}$$

2.2 灰度值变换

置乱和替代是加密技术中的两个基本方法[13]。除了上述置乱操作，下面将引入对像素值的替代变换。设 $I(i,j)$ 是位置为 (i,j) 的像素的灰度值，$I'(i,j)$ 为 $I(i,j)$ 经过替代变换后的值，$I'(i',j')$ 为替代变换循环中上一个处理过的像素灰度值。这里我们设置一个替代变换放大倍数 G_n，利用 Logistic 映射式(1)，取控制参数为 μ_3、初值为 $g(0)$，同样取迭代 m 次之后的混沌序列产生 g_n，则

$$G_n=\mathrm{round}(10000\times g_n),n=1,2,\cdots,N\times N \tag{11}$$

取灰度值替代变换为

$$I'(i,j)=I(i,j)+G_n\cdot I'(i',j')\bmod 256 \tag{12}$$

易知替代变换的逆过程为

$$I(i,j)=I'(i,j)-G_n\cdot I'(i',j')\bmod 256 \tag{13}$$

则替代变换系统的密钥为

$$Key3=(\mu_3,g(0),m) \tag{14}$$

通过上面的操作，可以将加密图像中每一个像素值都联系在一起，也就是扩散到密图所有像素中。改变任何一个像素的像素值，都会影响到所有像素，从而提高了替代变换系统的安全强度。

整个加密系统的密钥为

$$K=(Key1,Key2,Key3)=(\mu_1,\mu_1,\mu_1,c(0),c'(0),g(0),m) \tag{15}$$

2.3 加解密算法

假设要加密的数字图像其大小为 $N\times N$，灰度级为 256，加密算法如下：

(1)读入原始图像和密钥 K；

(2)将给定密钥 $Key1=(\mu_1,c(0),m)$ 和 $Key2=(\mu_2,c'(0),m)$ 分别带入 Logistic 映射式(1)，分别取迭代 m 次以后的值产生混沌序列 c_n 和 c_n'；

(3)将 c_n 和 c_n' 带入式(9)，构造函数 $\phi(\cdot)$ 和 $\varphi(\cdot)$；

(4)选取原图中任意一点，应用式(7)对原始图像像素进行置乱变换，直至图像中所有像素完成置乱变换；

(5)将给定密钥 $Key3=(\mu_3,g(0),m)$ 带入 Logistic 映射式(1)，取迭代 m 次以后的值产生混沌序列 g_n，并将 g_n 带入式(11)得到 G_n；

(6)对置乱过后的图像，应用式(12)按照电视扫描线方式从第一个像素开始对图像进行像素值替代变换；

(7)重复步骤(6) $N\times N$ 次，直至置乱后图像的所有像素值被替代；

(8)完成一轮加密操作后，可根据需要进行多轮加密。

解密算法与加密算法刚好相反，要先对密图进行替代变换，应用式(13)采用逆电视扫描线的方式从最后一个像素开始对密图像素进行替代变换，直至第一个像素也替代变换完毕。然后对此时的图像进行逆置乱变换，即运用式(8)对此时图像进行逆置乱变换，直至图像中所有像素均完成逆置乱变换。

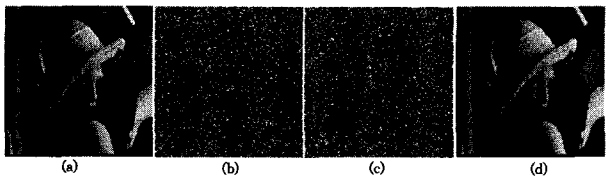
3 算法分析及仿真实验

本文算法先根据标准映射设计了像素的置乱变换，又通过替代变换使各像素值改变并相互依赖。所采用的加密解密算法都具有迭代结构，因而适合计算机快速计算；对于图像矩阵，也不需要进行预处理，提高了效率。同时，应用混沌系统产生了算法中各部分所需要的密钥流，使其简单快速又具有非线性，还具有对初始值敏感的特性。

为了不被穷举攻击解密图像，图像加密方案应该具有尽可能大的密钥空间。本文算法中由于密钥参数有 7 个，并且是在实数范围内取值，因此算法有足够大的密钥空间，使得穷举攻击不可能。

3.1 加密密钥敏感性测试

仿真环境为 Matlab 7.0，原始图像为 256×256 的 Lena 灰度图像。用密钥 $K1=(3.86,3.67,3.72,0.86,0.76,0.59,10000)$ 进行加密，加密一轮，分别使用 $K1$ 及与 $K1$ 略有不同的 $K2=(3.86,3.67,3.72,0.86,0.76,0.5900001,10000)$ 进行解密。实验结果如图 1 所示。



(a)Lena 原图像；(b)经过一轮加密的图像；
(c)密钥略有不同时解密图像；(d)密钥正确时解密图像

图 1 密钥敏感性测试

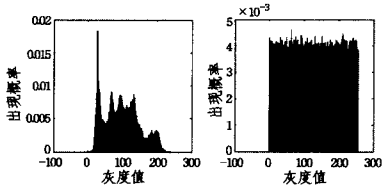
通过实验结果可以看出，当解密密钥与加密密钥有一点微小的差别时，都完全不能正确解密出原始图像，所以本算法对密钥有极强的敏感性。而且可以看出，在加密只进行一轮的情况下，已经达到了相当好的效果。也可以根据需要进行多轮加密。

3.2 统计分析

抗统计分析攻击能力的好坏是评判图像加密算法优劣的重要标准[14]。

1) 统计直方图

图 2 为加密前后图像的直方图。可以看出，加密前后的图像直方图有很大的区别，加密后像素值分布非常均匀，非常好地掩盖了原始图像的分布规律，增加了破译难度。



(a)原图像直方图 (b)加密图像直方图

图 2 加密前后统计直方图

2) 相邻像素的相关性

相邻像素的相关性可以反映出图像像素的扩散程度[15]。原始图像中相邻 2 个像素的相关性通常非常大，加密后图像相邻像素的相关性应该接近为 0。在图 1(a)和图 1(b)中随机选取 1500 对像素对，测试其水平方向、垂直方向和对角方向的像素相关性。并应用式(16) 计算相关系数(见表 1)。

$$R_{AB}=\frac{\sum_m\sum_n(A_{mn}-\bar{A})(B_{mn}-\bar{B})}{\sqrt{[\sum_m\sum_n(A_{mn}-\bar{A})^2][\sum_m\sum_n(B_{mn}-\bar{B})^2]}} \tag{16}$$

式中，A 为原始图像，B 为加密图像，$\bar{A}$ 和 $\bar{B}$ 是均值。

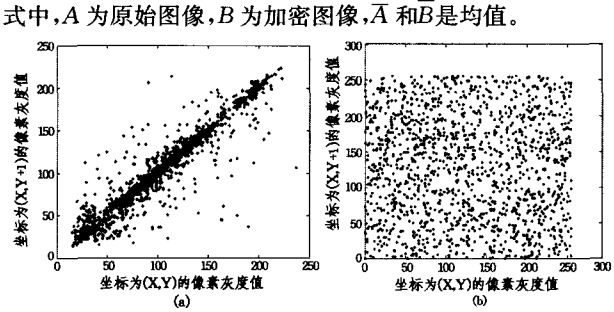


图 3 原图和加密图水平方向相邻像素的相关性

表 1 原图和加密图相邻像素的相关系数

相关系数	原图	密图
水平方向	0.94573	0.0028
垂直方向	0.96723	0.0029
对角线方向	0.92952	0.0046

通过图 3(a)和图 3(b)的对比，明显可见加密后图像相邻像素间的相关性呈随机的对应关系。从表 1 也可以看出，加密图像的相邻像素相关系数接近于零，其相邻像素已基本不相关。

结束语 本文提出了一种新的基于 Logistic 映射和标准映射相结合的图像加密算法。仿真实验结果表明，该算法可以很好地达到对图像加解密的效果。对算法的安全性分析可见，算法密钥空间大，有极强的密钥敏感度和较好的统计特性，能较好地抵御各种破解攻击。算法设计符合模块化准则，具有迭代结构，适合计算机快速计算，可有效地提高算法的执行效率。

参 考 文 献

[1] Alvare G, Montoya F, Romera M. Key stream cryptanalysis of a chaotic cryptographic method [J]. Computer Physics Communications, 2004, 156(2): 205-207

[2] 李昌刚，韩正之，张浩然. 一种基于随机密钥及类标准映射的图像加密算法[J]. 计算机学报，2003，26(4)：465-410

[3] 洪联系，李传目，卢明玺. 扩散映射置乱与超混沌系统组合图像加密算法[J]. 计算机应用，2007，27(8)：1891-1894

[4] Zhang Lin-hua, Liao Xiao-feng, Wang Xue-bing. An image encryption approach based on chaotic maps [J]. Chaos Solitons and Fractals, 2005, 24: 759-765

[5] 邓绍江，濮忠良，张岱固. 基于小波压缩和混沌置乱的图像处理算法[J]. 重庆大学学报，2008，31(8)：918-920

[6] Gao Hao-jiang, Zhang Yi-sheng, Liang Shu-yun. A new chaotic algorithm for image encryption [J]. Chaos Solitons and Fractals, 2006, 29(2)

[7] 朱从旭，陈志刚，欧阳文卫. 一种基于广义 Chen's 混沌系统的图像加密新算法[J]. 中南大学学报：自然科学版，2006，37(6)：1142-1148

[8] Zbigniew K, Janusz S. Application of discrete chaotic dynamical systems in cryptography-DCC method [J]. International Journal of Bifurcation and Chaos, 2000, 10(8): 1867-1874

[9] 邓绍江，张岱固，濮忠良. 一种基于混沌的图像置乱算法[J]. 计算机科学，2008，35(8)：238-240

[10] 郝柏林. 从抛物线谈起——混沌动力学引论[M]. 上海：上海科技教育出版社，1995：64-85

[11] Kelber K. General design rules for chaos-based encryption systems 2005 [J]. International Symposium on Nonlinear Theory and Its Applications, 2005(1): 456-468

[12] Frey D. Chaotic digital encoding an approach to secure communication [J]. IEEE Transaction on CAS, 1993, CAS 40(10): 660-666

[13] 刘向东，焉德军，朱志良，等. 基于排序变换的混沌图像置乱算法[J]. 中国图像图形学报，2005，10(5)：656-660

[14] 张琼，沈民奋，翟懿奎. 基于三维混沌猫映射的数字图像加密算法[J]. 数据采集与处理，2007，22(3)：292-298

[15] 郑凡，田小建，范文华，等. 基于 Henon 映射的数字图像加密[J]. 北京邮电大学学报，2008，31(1)：66-70