基于蔡氏电路混沌系统的图像加密方法

孙志娟， 陈 勇， 王颖学， 廖晓峰
(重庆大学 计算机学院，重庆 400044)

摘 要：鉴于低维混沌加密存在密钥空间相对较小的局限性，基于三维蔡氏电路混沌系统的图像空域置乱加密方法可避免该局限性。利用产生的混沌序列，经过预处理生成置乱索引矩阵用于图像加密。该方案密钥敏感性高，可实现多幅图像的并行加密，是一种具有较高的安全性，加密效率高，且易于实现的图像加密算法。

关键词：混沌系统；混沌序列；图像加密；蔡氏电路；置乱
中图法分类号：TP393.08 **文献标识码**：A **文章编号**：1000-7024 (2007) 14-3328-03

New image encryption algorithm based on Chua's circuit

SUN Zhi-juan, CHEN Yong, WANG Ying-xue, LIAO Xiao-feng
(College of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract: In view of the fact that the low dimension chaos encryption technology respectively has its limitation, a new image encryption algorithm based-on the Chua's circuit system is discussed. The real number value chaotic sequences is generated by using the key value and disperse them into scramble transformation matrix. This image encryption algorithm have high sensitive dependence on the initial condition. The algorithm provides good security, and have high encryption efficiency. Experimental results are satisfactory.

Key words: chaos system; chaos sequences; image encryption; Chua's circuit; scramble

0 引 言

近年来，随着通信技术的发展，网络系统、分布式多媒体系统中存在着大量的数字图像传输。由于通信传输和接收设备的充分发展，通过无线电和一般的通信网络非法获取数据已经变得越来越容易。因此，信息安全已经成为一个关键而迫切的问题，数字图像加密技术已经成为一项非常实用而又亟待快速发展的关键技术[1]。保护图像信息安全最经济有效的方法是采用密码技术。

混沌具有很好的加密性能，随着近年来混沌理论的广泛研究和逐渐成熟，越来越多的研究工作者着眼于混沌系统用于图像加密的研究工作，目前基于混沌序列图像加密技术的主要研究仍集中在一维和二维混沌系统。广泛应用的是基于logistic映射的图像加密方案[2-3]其具有形式简单、产生混沌时序时间短等优点，但其缺陷是密钥空间太小。对于低维混沌加密方案，已经有了一些攻击方法[4]可以将其破解；而高维混沌信号具有更好的伪随机性，基于高维混沌系统的加密算法可期望获得更好的保密性，因此，研究高维混沌加密算法已经成为新的研究热点。

本文提出了一类基于蔡氏电路混沌系统的图像加密方法。利用蔡氏电路混沌系统产生的伪随机混沌实值序列生成索引序列用于图像置乱。相关的安全性分析和仿真试验表明，该加密算法安全性高，速度快且易于实现。

1 Chua's Circuit 混沌系统

近年来，许多学者通过非线性电路对混沌行为进行了广泛地研究，其中最典型的是Leon.O.Chua提出的蔡氏电路，它是能产生混沌行为的最小最简单的三阶自治电路[5-7]。电路图如图1所示。

根据图1可以写出Chua's Circuit的三阶电路微分方程

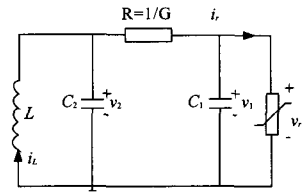


图1 蔡氏电路

收稿日期：2006-07-25 **E-mail**：aileen_szj@yahoo.com.cn
基金项目：国家自然科学基金项目 (60271019)；重庆自然科学基金项目 (20020611007)。
作者简介：孙志娟 (1981－)，女，甘肃通渭人，硕士研究生，研究方向为信息安全与图像加密； 陈勇 (1971－)，男，博士研究生，研究方向为编码理论、图像处理、混沌加密； 王颖学 (1982－)，男，硕士研究生，研究方向为信息安全与密码学； 廖晓峰 (1964－)，男，博士生导师，研究方向为信息安全、数据挖掘、人工神经网络与计算智能。

$$\begin{cases} C_1\dfrac{dv_1}{dt}=G(v_2-v_1)-f(v_1) \\ C_2=\dfrac{dv_2}{dt}=G(v_1-v_2)+i_L \\ L\dfrac{di_L}{dt}=-v_2 \end{cases} \tag{1}$$

方程组(1)可写为如下的微分方程形式

$$\begin{cases} \dfrac{dx}{d\tau}=\alpha(y-x-f(x)) \\ \dfrac{dy}{d\tau}=x-y+z \\ \dfrac{dz}{d\tau}=-\beta y \end{cases} \tag{2}$$

其中

$$f(x)=bx+(a-b)(|x+1|-|x-1|)/2 \tag{3}$$

分析微分方程 (3) 的平衡点和 Lyapunov 指数，当参数α=10,β=15.68, a=−1.276 8, b=−0.688 8 时，蔡氏电路处于混沌状态，出现双涡卷混沌吸引子。

2 加密算法

2.1 伪随机序列的产生

首先利用蔡氏电路产生加密所需的伪随机序列。采用四阶 Runge-Kutta 法 [8] 迭代，控制参数设为 (α,β, a, b)=(10,15.68, −1.27685,−0.688 85)积分步长 h=0.0005，就可得到三维的混沌实数值序列(x_i,y_i,z_i)，i=1,2,…,n，n 为数值积分算法的迭代次数。

对不同的控制参数产生的混沌序列(x_i,y_i,z_i)的统计分析表明：3 个分量 x_i, y_i, z_i 的值域分别为：$x_i\in(-4,4)$,$y_i\in(-1.8,1.8)$, $z_i\in(-20,20)$；对应的平均值分别为：avrx=−36.6, avry=−7.16, avrz=8.722 6。再将此类序列用于加密前尚需做如下的预处理操作：①去除各实数值的整数部分，统一值域；②在去整的基础上再将小数点后移数位，以增强序列的无规则性及整体分布的均匀性。经过预处理后的伪随机序列(x_i,y_i,z_i),i=1,2,…,n的值域为(10,−10)，平均值分别为：avrx=0.003 34,avry=−0.009 50, avrz=−0.001 52，趋于零。互相关特性近似为零，自相关特性是较理想的δ函数。

2.2 置乱索引矩阵的构建

利用上述的预处理后的序列，可构建一个如下的置乱索引矩阵I：

(1)矩阵I的定义：$I_{ij}\in\{1,2,3,\cdots\}$且$I_{ij}=I_{pk}$当且仅当$i=p,j=k$。

(2)矩阵I的生成：将混沌系统产生的实值序列的各维经过去整、小数点移位等预处理后得到伪随机序列(x_i,y_i,z_i)，由 3 组伪随机序列生成矩阵X, Y, Z，对这 3 个矩阵的每一行向量进行排序。将排序后的元素位置的变换记为置乱规则矩阵Ix, Iy, Iz，如X的第 i 行$\{x_{i1},x_{i2},x_{i3},\cdots,x_{ij}\}$按升序排序后为$\{x_{ij},x_{i3},x_{i2},\cdots,x_{i1}\}$则置乱矩阵$Ix$的第 i 行为{j,3,2,…,1}。置乱矩阵的大小由置乱块的大小决定。图像大小为 N*M 时，置乱块的大小为 K*L，则置乱矩阵的大小为(N/K)*(M/L)。如以像素为单位则置乱矩阵的大小为 256*256。

控制参数的敏感性测试如表 1 所示，去掉序列的初始阶段，置乱矩阵的位序变化率可以达到 100%。

结果表明，预处理后的序列具有很强的伪随机特性，用于图像置乱将会获得安全性极高的加密算法。考虑到(x_i,y_i,z_i)序列具有良好的各分量独立特性，利用 x_i,y_i,z_i 这 3 个序列可独立的构成 3 个单变量加密混沌序列，也可组合构成多重加密序列，可同时对多幅图像进行加密，加密算法有良好的可扩展性。

表 1 对参数和初始值微小变化的敏感性测试

参数变化	置乱矩阵变化率		
	Ix	*Iy*	*Iz*
$a\pm10^{-8}$	100%	100%	100%
$a\pm10^{-7}$	100%	100%	100%
$a\pm10^{-6}$	99.5%	99.9%	100%
$b\pm10^{-8}$	100%	100%	100%
$b\pm10^{-7}$	100%	100%	100%
$b\pm10^{-6}$	99.9%	99.1%	99.3%
$z_0\pm10^{-8}$	100%	100%	100%
$z_0\pm10^{-7}$	100%	100%	100%
$z_0\pm10^{-6}$	99.5%	99.9%	99.8%

2.3 加密解密算法

本文设计了一种利用置乱索引矩阵I对图像进行空间置乱的加密方法。加密和解密算法如下。加密密钥可根据需要选择系统参数和初始值(α,β,a,b,x,y,z)中的一个或几个。加密步骤：

(1)输入原始图像。如考虑到图像压缩效果，则可以对图像进行分块预处理，以块为单位对图像进行全局置乱变换。为符合 JPEG 图像压缩标准，将图像分为 8*8 的块。这样做不影响 DCT 系数的分布。也可以直接对像素进行全局置乱，不需要预处理；

(2)构造置乱索引矩阵。输入密钥，生成实值混沌序列(x_i, y_i,z_i),i=1,2,…,n，对 3 个分量进行预处理，按需要的长度截取实值混沌序列，为保证随机性，需去除序列的初始阶段。由混沌序列按规则构造索引矩阵Ix, Iy, Iz；

(3)图像置乱。按置乱索引矩阵的规则，重排置乱块的位置。为了获取更优的加密效果，对每幅待加密的图像选择Ix, Iy, Iz中的两个置乱索引矩阵构成二重加密，分别用于横向和纵向置乱。迭代 2 次即可达到理想的加密效果。如对 8*8 的分块进行置乱加密，迭代次数则应增加至 3~5 次。

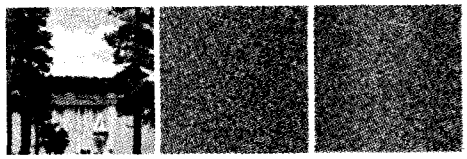
解密算法为加密算法的逆过程：①读入密图；②重现置乱索引矩阵。输入解密密钥，同加密步骤 2；③恢复原图像。是加密置乱过程的逆过程，根据置乱矩阵，将像素恢复到原位置。

3 安全分析和仿真测试

3.1 算法仿真

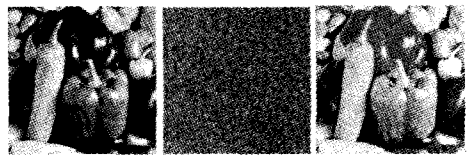
对上述算法进行了实验仿真，并对结果进行分析，验证算法的有效性和安全性。考虑到图像数据在网络传输过程中很难避免一些必要的数据处理或人为攻击，如压缩、噪声污染失真等。对这些常见的处理和攻击也进行了仿真测试。实验数据选择了具有不同纹理特征，大小为 256*256 的 lake, peppers, lena 这 3 幅标准图像作为仿真对象。设置参数(α,β,a,b,x,y,z)=(10,15.68,−1.276 85,−0.688 85,1.584 102 3,1.234 585 4,1.895 278 1)利用蔡氏电路产生三维混沌序列(x_i,y_i,z_i)，对各维进行预处理并产生置乱矩阵Ix, Iy, Iz选择p_2^3组合中的 3 种分别用于加密 3 幅标准图。图 2 为对 lake 图像进行的仿真结果，其中图 2(a)为 lake 原始图像，图 2(b)为加密后的图像，图 2(c)为密钥误差为10^{-7}时错误解密的图像。图 3 为对 peppers 图像进行仿真的结

果，其中图3(a)为peppers原图，图3(b)为加密后受到高斯噪声污染的图像，图3(c)为用正确密钥解密后的图像。图4为对lena图像进行仿真的结果，其中图4(a)为lena原图，图4(b)为对lena图像8*8的分块加密并进行有损压缩后的图像，压缩过程中保留了40%的DCT系数，图4(c)为正确密钥解密后的图像。



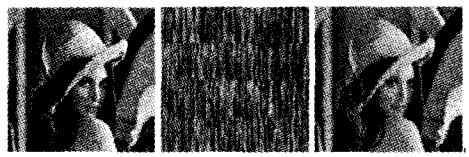
(a) lake　(b) 加密图像　(c) 密钥误差为 10^{-7} 时错误解密的图像

图2　对lake图像进行仿真的结果



(a) peppers　(b) 模糊加噪后的加密图像　(c) 正确密钥解密恢复的图像

图3　对peppers图像进行仿真的结果



(a) lena　(b) 分块加密并压缩的图像　(c) 正确密钥解密图像

图4　对lena图像进行仿真的结果

3.2　安全分析

通过对图2中加密前后的图像进行直方图、相邻像素相关分析以及差分攻击分析NPCR，UACI来验证算法的有效性。

3.2.1　直方图分析

图5为lake图像加密前后的直方图显示。可以看出加密后的直方图中灰度分布的更均匀。

3.2.2　相关性分析

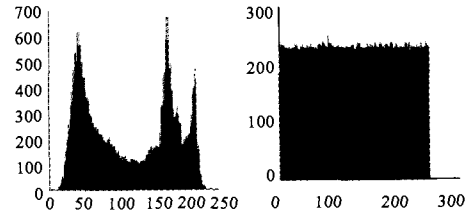
图6为加密前后水平相邻像素的相关性分析。对随机产生1 000对水平相邻的像素点，图6(a)为加密前的相关度。图6(b)为加密后同样位置的相邻像素的相关度。表2分别列出了加密前后相同位置的1 000对水平相邻、垂直相邻、对角相邻的像素相关系数。加密前相邻像素相关紧密，加密后，其相关系数明显降低。相关系数的计算公式

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

对图像加密前后的相关系数进行分析，可以看出，相邻像素间的相关系数大幅下降，可有效的抵抗基于统计分析的攻击。

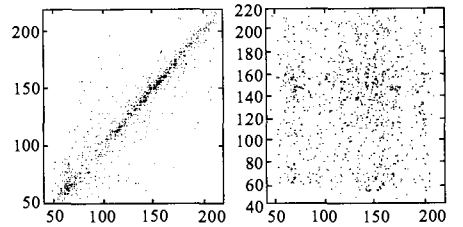
4　结束语

本文设计了一种基于蔡氏电路的混沌图像加密方法。利用混沌系统产生的实值混沌序列，经过预处理构造置乱索引矩阵。由于经过预处理的伪随机序列具有理想的自相关和互相关特性以及良好随机性，因此3个置乱索引矩阵可以分别



(a) 原图　(b) 加密图

图5　lake加密前后的直方图



(a) 原图相关系数 0.952 9　(b) 加密图相关系数-0.013 4

图6　水平相邻两点形成的相关系数

表2　原图和加密图的相关系数结果

项目	原图	加密图
水平方向	0.952 9	−0.013 4
垂直方向	0.955 3	0.015 1
对角方向	0.819 9	0.011 7

用于加密3幅图像，亦可组合用于加密多幅图像，从而提高了加密的效率，同时良好的随机性保证了加密的效果。该算法对图像进行全局空域置乱，仿真实验表明，图像置乱效果好，采用分块置乱时便于与图像压缩相结合，并且可抵抗噪声污染图像失真等。因此该算法具有可行性，可靠性，高效性以及抗攻击能力，是一种安全有效的数字图像空域加密方法。

参考文献：

[1] 李昌刚,韩正之,张浩然.图像加密技术综述[J].计算机研究与发展,2002,39(10):1317-1324.

[2] 孙鑫,易开祥,孙优贤.基于混沌系统的图像加密算法[J].计算机辅助设计与图形学学报,2002,14(2):136-139.

[3] 李雄军,彭建华,徐宁,等.基于二维超混沌序列的图像加密算法[J].中国图像图形学报,2003,8(10):1172-1177.

[4] Wang Shilhong,Kuang Jinyu,Li Jinghua,et al.Chaos-based communications in large community[J].Phys Rev,2002,66(6):1-4.

[5] Sobhy M,Shehata A.Chaotic algorithms for data encryption[C].IEEE International Conference on Acoustics, Speech, and Signal Processing.Salt Lake City,USA:IEEE,2001:997-1000.

[6] Borresen J,Lynch S.Further investigation of hysteresis in Chua's circuit[J].International Journal of Bifurcation and Chaos in Applied Sciences and Engineering,2002,12(1):129-134.

[7] Tang K-S, Man K-F, Zhong G-Q, et al. Modified Chua's circuit with x|x|[J].Control Theory and Applications,2003,20(2):223-227.

[8] 李庆扬.数值分析[M] 武汉:华中科技大学出版社,2002.