第 37 卷 第 15 期
Vol.37 No.15

计 算 机 工 程
Computer Engineering

2011 年 8 月
August 2011

• 安全技术 •

文章编号：1000—3428(2011)15—0092—03 文献标识码：A 中图分类号：TP309

基于网格状多涡卷蔡氏混沌系统的数字水印

刘竹松，陈平华

(广东工业大学计算机学院，广州 510006)

摘 要：基于网格状多涡卷蔡氏混沌系统和离散余弦变换(DCT)理论，提出一种改进的数字水印算法。采用网格状多涡卷蔡氏混沌系统生成的混沌序列作为密钥，增强算法的安全性；利用网格状多涡卷混沌系统复杂的混沌动力学行为，弥补低维混沌系统用于数字水印时密钥空间过小的缺陷。实验结果表明，该方案在抗几何攻击、抗裁剪和密钥空间抗穷举攻击方面具有较好的特性。

关键词：数字水印；混沌数字水印；网格状多涡卷；混沌吸引子；超混沌；密钥空间

Digital Watermark Based on Grid Multi-scroll Chua's Chaotic System

LIU Zhu-song, CHEN Ping-hua

(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China)

【Abstract】Based on the grid multi-scroll Chua's chaotic attractors and Discrete Cosine Transform(DCT) algorithm, a novel digital image watermark algorithm is proposed in this paper. It improves digital watermark algorithm using the grid multi-scroll Chua's chaotic sequences generated by chaotic systems as the key, which greatly enhanced the security of the algorithm. The complex dynamic behavior makes up the existence of defects in the key space is too small. Experiment results show that the scheme has excellent characteristics of resistance to geometric attacks, shear, and brute-force attacks against the key space and has good features.

【Key words】digital watermark; chaotic digital watermark; grid multi-scroll; chaotic attractors; hyper-chaos; key space

DOI: 10.3969/j.issn.1000-3428.2011.15.028

1 概述

混沌系统对初始条件和系统参数的极端敏感性及其生成的混沌序列的高度伪随机性使得混沌系统具备良好的密码学应用价值。近年来将混沌系统应用到数字水印领域的研究不断见于报道[1]，这些研究大部分采用低维混沌系统生成伪随机序列，并对生成的伪随机序列做一定变换后作为水印生成或隐藏的方法，这些低维混沌系统通常为 Logistic 映射，猫映射以及基于这 2 种映射的变型。这些混沌数字水印算法的共同点如下：(1)普遍认为低维混沌系统产生的伪随机序列比传统算法生成的伪随机序列数量大，足够组成各类数字水印算法的密钥空间。(2)对水印算法安全的评估偏重于混沌动力学行为的复杂性，忽略了密码学严格而系统的评价体系和设计原则。针对这些数字水印，文献[2]指出了密钥空间设计应该遵循的原则，文献[3]指出其设计的不足，并给出一种通用的攻击算法。

针对上述问题，本文提出一种基于网格状多涡卷蔡氏混沌系统的数字水印算法。网格状多涡卷蔡氏混沌系统丰富的系统参数和更为复杂的动力学行为特征弥补了低维混沌系统密钥空间的不足，改进算法的设计严格遵循密码学设计原则及评价体系，能有效防止类似文献[3]的攻击方法。同时本文验证了改进算法的鲁棒性和抗攻击能力。

2 网格状多涡卷蔡氏混沌系统

与水印系统中普遍采用的低维混沌系统相比，网格状多涡卷混沌系统具有更为复杂的混沌动力学行为，生成的混沌序列更具不可预测性，产生的密钥空间远大于低维混沌系统。基于分段线性函数、锯齿波、三角波、阶梯波、正弦函数等非线性函数可以产生多涡卷和网格状混沌吸引子[4]，但有关网格状多涡卷蔡氏混沌吸引子的文献报道却很少，主要原因是用于生成单方向多涡卷混沌吸引子的非线性函数，如多分段线性函数、正弦函数等不能推广到蔡氏电路中生成网格状多涡卷混沌吸引子。本文提出一个 4 阶蔡氏超混沌系统，并以该系统为基础产生数字水印算法中需要的混沌序列。该混沌系统在维数和运行时间上有很好的折衷，既能克服低维混沌系统应用到数字水印中的安全缺陷，又能避免高维混沌系统的运算复杂性。该混沌方程如下：

$$\begin{cases}\dfrac{\mathrm{d}x(t)}{\mathrm{d}t}=p\{g[y(t)-x(t)]-z(t)\}\\ \dfrac{\mathrm{d}y(t)}{\mathrm{d}t}=q\{-g[y(t)-x(t)]-w(t)\}\\ \dfrac{\mathrm{d}z(t)}{\mathrm{d}t}=r\{g[x(t)+z(t)\}\\ \dfrac{\mathrm{d}w(t)}{\mathrm{d}t}=sy(t)\end{cases} \tag{1}$$

其中，$p=2,q=20,r=1,s=1.5$；$g[y(t)-x(t)]$ 为分段非线性奇函数，其数学表达式如下：

$$g[y(t)-x(t)]=m_{N-1}[y(t)-x(t)]+0.5\sum_{i=1}^{N-1}(m_{i-1}-m_i)\cdot[|y(t)-x(t)+x_i|-|y(t)-x(t)-x_i|] \tag{2}$$

李氏指数谱为 $[u_1,u_2,u_3,u_4]=[0.24,0.06,0.00,-53.8]$，因此，式(1)是一个超混沌系统。当 N=4、参数如式(3)所示时，

基金项目：国家自然科学基金资助项目(60871025)；广东省自然科学基金资助项目(9151009001000021)

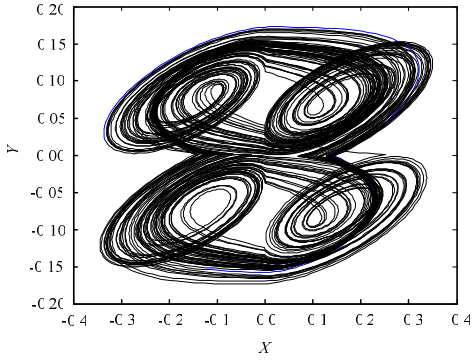
作者简介：刘竹松(1979－)，男，讲师、博士研究生，主研方向：混沌数字水印，混沌保密通信；陈平华，教授

收稿日期：2011-02-15 **E-mail：**liuzs@gdut.edu.cn

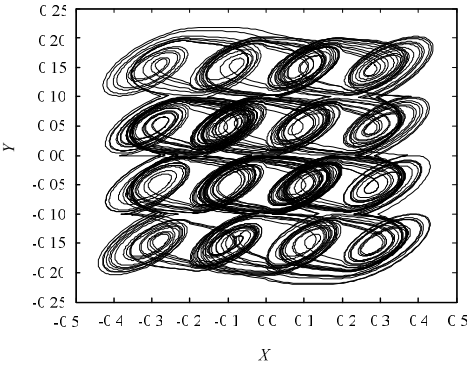
则该混沌系统可产生 4 涡卷混沌吸引子。

$$\begin{cases}[m_1,m_2,m_3,m_4]=[-0.8,2.8,-0.8,1.8]\\ [x_1,x_2,x_3]=[1.000,3.000,5.000]\end{cases} \tag{3}$$

对混沌方程式(1)采用 Matlab 2010 进行仿真，得到 2×2 及 4×4 网格状蔡氏吸引子的仿真结果，如图 1 所示。



(a)2×2 网格状蔡氏吸引子仿真结果



(b)4×4 网格状蔡氏吸引子仿真结果

图 1　2×2 与 4×4 网格蔡氏吸引子仿真结果

3　基于网格状多涡卷蔡氏混沌系统的数字水印

水印的实现过程包括以下 2 个步骤：

(1)利用网格状多涡卷蔡氏混沌系统产生随机序列，从部分涡卷中选取一组随机数字置乱外部图片，生成原始水印，同时，从其他涡卷中选取另外一组随机数字，用于确定水印的嵌入位置。

(2)将步骤(1)中生成的数字水印按照混沌系统确定的嵌入位置嵌入到宿主图像中。

算法具体步骤如下：

(1)导入 JPG 图，转换成 bmp 二值图像作为水印。

(2)置乱原始水印。

(3)采用网格状多涡卷蔡氏混沌系统生成的超混沌随机序列加密原始水印。

(4)对图像分层，并做 DCT 分块，将信息嵌入到分块中。嵌入的原理参见 3.2 节水印的嵌入与提取。

3.1　超混沌序列的产生

网格状多涡卷蔡氏混沌系统生成的超混沌随机序列的主要作用是用于置乱外部图片，生成原始水印及确定水印的位置。因此，实现水印算法的关键就在于超混沌序列的生成。超混沌序列的产生步骤如下：

(1)生成实数值序列，该序列为网格状多涡卷蔡氏混沌系统的轨迹点形成的 $n\times4$ 维矩阵，矩阵中的每一列元素对应方程中 x,y,z,w 的混沌轨迹值。该序列为 $X=\{x_{i,j}\},i=1,2,\cdots,n;\ j=1,2,\cdots,n$。

(2)阈值化处理：置乱外部图片，生成水印及确定水印的潜入位置时通常采用 0、1 组成的二进制随机序列，因此，需要定义一个阈值函数将实数随机序列转换成二进制随机序列。阈值函数 $\theta(x)=\begin{cases}0 & x\leqslant\alpha\\ 1 & x>\alpha\end{cases}$，其中，$\alpha$ 根据网格状多涡卷蔡氏混沌系统生成的实数取值范围而确定。

(3)生成超混沌序列：超混沌序列采用如下公式计算：

$$T(i,j)=[\boldsymbol{X}(i,2)*\boldsymbol{X}(j,1)^{\mathrm{T}}]*[\boldsymbol{X}(i,4)*\boldsymbol{X}(j,3)^{\mathrm{T}}],i,j=1,2,\cdots,N$$

其中，N 为矩阵的维数；X 为阈值化处理后的 $n\times4$ 维矩阵；$T(i,j)$ 为超混沌序列。

3.2　水印的嵌入与提取

传统的 DCT 算法直接采用 DCT 的定义进行变换，由于大量采用浮点运算，运算量大且精度差；传统 DCT 的变换编码方法以块为单位单独进行量化和编码，忽略了邻接块间的相关性，因而在高压缩比编码时由于粗糙量化使得相邻块的 DCT 系数取样落在不同的量化区间，导致原本很接近的像素重构后产生了较大的差异，形成明显的块边界[5]。本文在此基础上提出一种改进的 DCT 算法。

假设需要做 DCT 变换的灰度图像的大小为 256×256 像素，灰度在 0~255 之间变化。每 8×8 像素块作 DCT 变换，得到一个直流(DC)系数和 63 个交流(AC)系数。对于数据集分类，笔者分出 64 类，即：DC 1 类，AC(1)~AC(63)共 64 类，每类 1 024 个数据。AC(1)表示所有 8×8 块的 DCT 系数的第 1 个 AC 系数；AC(2)表示所有 8×8 块的 DCT 系数的第 2 个 AC 系数以此类推。嵌入方法采用量化 DC、AC 系统的方法进行[6]。量化的参考矩阵为 JPEG 标准量化矩阵。嵌入 1：类中取正数的个数大于取负数的个数；嵌入 0：类中取正数的个数小于取负数的个数。

水印嵌入算法如下：

(1)对图像做大小为 8×8 的 DCT 变换，由网格状多涡卷蔡氏混沌系统生成的随机序列生成的密钥 K 计算 DCT 系统的分类 $\chi(i),i=1,2,\cdots$。

(2)对 $\chi(i)$ 量化后取整数 $\lfloor\phi(\chi(i))\rfloor$，量化函数 ϕ 的量化步长为 JPEG 标准量化矩阵，取整后的尾数记为 $\Gamma(i)=\phi(\chi(i))-\lfloor\phi(x(i))\rfloor$。

(3)计算 $\lfloor\phi(\chi(i))\rfloor$ 取正数的数目 $\lambda(i)$，取负数的数目 $\delta(i)$。

(4)计算满足 $0<\lfloor\phi(\chi(i))\rfloor<\kappa$ 及 $-\kappa<\lfloor\phi(\chi(i))\rfloor<0$ 区间中的集合 f_- 和 f_+，其中，κ 称为水印的嵌入强度；$|f_-|$ 和 $|f_+|$ 分别表示前面 2 个集合的势。

(5)嵌入 1：若 $\lambda(i)>\delta(i)+\theta$，则不做处理；否则，如果 $|f_-|\geqslant\theta-(\lambda(i)-\delta(i))+1$，随机选择 f_- 集合中的 $\theta-(\lambda(i)-\delta(i))+1$ 项，并将 $\theta-(\lambda(i)-\delta(i))+1$ 项的数值都改为 0，θ 称为水印的鲁棒性强度。若 $0.5\times(\theta-(\lambda(i)-\delta(i))+1\leqslant|f_-|<\theta-(\lambda(i)-\delta(i))+1$，随机选择 f_- 集合中的 m 项，将其数值更改为相反数，其中，$m=0.5\times(\theta-(\lambda(i)-\delta(i))+1$。其他情况时，调整 θ 的值，返回执行第(4)步。嵌入 0：如果 $\lambda(i)>\delta(i)+\theta$，则不做任何处理。否则，如果 $|f_+|\geqslant\theta-(\lambda(i)-\delta(i))+1$，则随机选择 f_+ 集合中的 $\theta-(\lambda(i)-\delta(i))+1$ 项，将其数值更改为 0；若 $0.5\times(\theta-(\lambda(i)-\delta(i))+1\leqslant|f_+|<\theta-(\lambda(i)-\delta(i))+1$，则随机选择 f_+ 集合中的 n 项，将其数值更改为相反数；其中，$n=0.5\times(\theta-(\lambda(i)-\delta(i))+1$；其他情况时，调整 θ 的值，返回

执行第(4)步。

(6)将嵌入水印的$\lfloor\phi(\chi(i))\rfloor$系数加上尾数$\Gamma(i)$，然后乘上对应的量化步长，通过逆 DCT 变换，恢复成嵌入水印的图像。

水印提取算法如下：

(1)对图像做大小为 8×8 的 DCT 变换，得到 DCT 系数集合。

(2)按嵌入算法的思路，提取$\phi(\chi(1))$到$\phi(\chi(N))$，N为水印嵌入的容量长度。

(3)计算$\lfloor\phi(\chi(i))\rfloor$取正数的数目$\lambda(i)$，取负数的数目$\delta(i)$。

(4)判断：如果$\lambda(i)>\delta(i)$，则水印比特值为 1，否则为 0。

4 实验结果及分析

在实验中，采用 256×256 像素的 BMP Lena 彩色图像，如图 2(a)所示，然后转换成灰度图像，嵌入水印为 32×32 像素的“广东工大”PNG 图像，如图 2(b)所示。实验中取水印鲁棒性强度$\theta=5$，取水印嵌入强度$\kappa<3$。

(a)实验原图

(b)待嵌水印

图 2 实验原图及待嵌入水印

实验结果表明嵌入水印前后的 Lena 图像在视觉上不可区分，如图 3 所示。

(a)嵌入水印前图像

(b)嵌入水印后图像

图 3 嵌入水印前后图像对比

4.1 非几何攻击

为验证基于网格状多涡卷蔡氏混沌系统的数字水印在面对非几何攻击方面的特性，实验对网格混沌 DCT 算法、Logistic 混沌 DCT 水印算法、普通的 DCT 算法在面对典型的非几何攻击下的水印检测正确度列表分析，实验结果如表 1 所示。可以看到，网格状多涡卷蔡氏混沌数字水印在 5 种攻击类型下都优于其他 2 种数字水印。

表 1 典型非几何攻击下水印检测正确率 (%)

攻击类型	网格状混沌+DCT	Logistic 混沌+DCT	DCT
椒盐噪声(强度 0.1)	100	100.00	9.87
高斯白噪声(强度 0.05)	100	99.99	99.76
中值滤波(模块大小 3×3)	100	99.97	100.00
高斯模糊(模块大小 5×5)	100	100.00	99.50
锐化	100	98.60	100.00

4.2 几何攻击

几何攻击是目前对数字水印构成重大威胁的攻击手段之一[7]，大部分水印算法经过几何攻击后都无法幸免。在设计水印算法中，一个主要目标是能提高水印算法的抗攻击能力，如裁剪、平移、缩放、旋转等几何变换[8]。本文改进的 DCT 算法对典型的几何攻击如旋转、压缩具有较好的抵抗能力。表 2 为采用 ACDSee5.0 分别对含水印图像做压缩及旋转后，提取出的水印与原始水印相似比例对照表，其中相似比例为提取水印与原始水印比特数一一对应的比例。

表 2 旋转攻击和压缩攻击下提取水印与原水印的相似比例

旋转角度/(°)	相似比例/(%)				
	压缩比率为 100%	压缩比率为 80%	压缩比率为 50%	压缩比率为 30%	压缩比率为 10%
0	100	100	97	94	92
1	100	99	96	94	89
5	96	96	94	92	88
8	94	93	90	89	86
10	96	96	94	92	91
30	98	96	96	92	89
45	93	93	93	90	87
90	100	100	94	92	90

4.3 抗剪切攻击

为验证算法的抗剪切攻击能力，分别设计了从 4 个方向和中心位置不同程度的系列剪切攻击。对提取的水印通过检测正确率进行质量评估，水印检测正确率(*BCR*)的公式为：水印检测正确率=提取水印的正确比特数/嵌入水印的总比特数。实验结果如表 3 所示。

表 3 抗剪切攻击下的实验结果

剪切攻击类型	提取出的水印	*BCR*
剪切左上角 80×80 像素		0.981
剪切右上角 80×80 像素		0.992
剪切左下角 80×80 像素		0.996
剪切右下角 80×80 像素		0.998
剪切中心 80×80 像素		0.987
剪切中心 1/3		0.963
剪切右下角 1/3		0.979
剪切右下角 1/2		0.864

4.4 密钥空间分析

要获取计算 DCT 系统的分类$\chi(i),i=1,2,\cdots$的密钥K，进行穷尽攻击是不可能的。假设对一个 256 级的$m\times n$的灰度图像进行攻击，则行变换序列和列变换序列有$m!\times n!$种情况，若考虑引入的网格状多涡卷蔡氏混沌系统，其超混沌序列的取值可以是混沌轨迹x,y,z,w任一轨迹，假设普通 Logistic 混沌随机序列长度为L，则理论上有256^L个不同的值，网格状多涡卷蔡氏混沌仅从参数数量的简单叠加就有4×256^L个不

(下转第 109 页)