# 一种新的混沌加密算法及其应用

高昊江, 张宜生, 梁书云, 李德群

(华中科技大学 模具技术国家重点实验室, 湖北 武汉, 430074)
E-mail: hustphd@126.com

摘 要: 混沌加密技术广泛应用于网络通信、图像加密等信息安全领域. 本文研究出一种新的混沌加密算法, 它克服了现有 Logistic 映射的缺陷, 利用正切函数和幂函数设计混沌迭代函数, 利用混沌序列作为密钥进行加密运算. 该算法具有很好的发散性、实时性和安全性. 本文给出了其在烟草物流防伪系统中的具体应用.

关 键 词: 混沌加密; 算法; 物流管理; 商品防伪
中图分类号: TP393 文献标识码: A 文 章 编 号: 1000-1220(2006)04-0655-03

# New Chaotic Encryption Algorithm and the Application

GAO Hao-jiang, ZHANG Yi-sheng, LIANG Shu-yun, LI De-qun
(*State Key Lab of Plastic Forming Simulation and Die & Mould Technology, Huazhong University of Science & Technology, Wuhan* 430074, *China*)

**Abstract**: The technologies of chaotic encryption are widely used in information security fields, such as network communication and image encryption. This paper presents a new chaotic encryption algorithm, which overcomes the limitation of Logistic map, uses tangent function and power function for chaotic function design, and uses chaotic numbers as encryption keys. The new algorithm is perfectly emanative, real-time and security. An example of logistics management and anti-counterfeiting system is given.

**Key words**: chaotic encryption; algorithm; logistics management; anti-counterfeiting

## 1 引 言

确定性系统产生的类似随机的现象就是混沌; 混沌系统是一种复杂的非线性动态系统, 具有对初始条件和混沌参数非常敏感以及生成的混沌序列具有非周期性、类随机性和非重复性的特性. 这些特性与密码学的很多要求相吻合, 如密码学对密钥的敏感性、对明文的敏感性以及密文的随机性和发散性. 那么结合运用两者的混沌加密系统更是发扬了上述各种特性, 具有对输入控制参数的极端敏感性、行为无规律性、结果貌似无穷性和非重复性.

本文研究出一种新的混沌加密算法, 它主要应用于数码物流防伪信息系统. 数码防伪技术是在传统防伪技术逐渐失去保护能力的情况下, 依托飞速发展的信息技术、网络技术及计算机技术, 产生并发展起来的一种新兴技术. 数码物流防伪信息系统给每件商品分配一个唯一的编码, 该编码可通过查询系统进行验证, 包括网络查询、电话查询、短信查询等多种方式. 这些编码都是密码, 相近的产品被分配的编码却差别很大, 看上去毫无规律, 谁也不能据此推断出其他编码的构成, 因此也就无法伪造. 若选择复制现有的编码, 那么受"编码非重复性"限制, 很容易被看出是伪造产品, 无法实现大批量伪造. 利用编码的唯一性还可进行商品物流跟踪. 下面将分别阐述混沌加密算法的混沌迭代函数的设计及加密算法设计.

## 2 混沌迭代函数设计

### 2.1 现有 Logistic 映射分析

Logistic 映射用一维非线性迭代函数来表征混沌行为, 通过微小地改变调节参数的值来产生完全不同的伪随机序列; 其函数可表示为 $x_{n+1}=\lambda x_n(1-x_n)$, 其中 $\lambda$ 为调节参数, $\lambda\in(0,4)$, $x_n\in(0,1)$, $n=0,1,2,\cdots$. 取 $x_0=0.3$, 那么通过实验分析可得到如下结论: 当 $\lambda\in(0,3)$ 时, 函数经过多次迭代而趋近于同一个值, 如图 1(a)所示; 当 $\lambda\in[3,3.6)$ 时, 函数经过多次迭代后在几个值间振动, 出现周期性, 如图 1(b)所示, 作者通过上万次的迭代实验发现此结果, 比文献[1]中的结论(3, 3.8)要准确; 当 $\lambda\in[3.6, 4)$ 时, 周期现象消失, 表现出混沌效果. 该混沌迭代函数的问题是: 存在明显的"稳定窗"[1], 即点聚集于某个区间, 而其他区间内则是空白, 例如当 $\lambda=3.7$ 时, 函数的取值仅局限于(0.25, 0.93)这个区间; 当 $\lambda<3$ 时, 迭代会趋于某一个固定值; 控制参数的有效取值范围太小, 仅为 0.4 左右; 所以, 此迭代函数不能满足技术发展的要求.

### 2.2 一种新的混沌迭代函数

根据原混沌系统存在的问题, 文献[2]提出了改进系统, 在混沌迭代函数中加入了幂函数 $(1-x)^{\beta}$. 本文则考虑加入正

收稿日期: 2005-01-04 作者简介: 高昊江, 男, 1981 年生, 博士研究生, 研究方向为信息安全、协同制造信息系统; 张宜生, 男, 1951 年生, 教授, 博士生导师, 研究方向为协同制造、计算机辅助设计和图形学、网络数据库软件的应用; 梁书云, 女, 1961 年生, 高级工程师, 研究方向为计算机辅助设计应用; 李德群, 男, 1945 年生, 教授, 博士生导师, 研究方向为计算机模拟理论和算法.

切函数和幂函数, 形成新的混沌生成算法, 这样做是因为随着 x 的增大, 幂函数会快速衰减, 为了使衰减周期变长, 那么设法提高 x 增大带来的函数值增大效果, 一个很好的选择就是正切函数. 新算法的公式表示为:

$$f(x,\lambda,\alpha,\beta)=\lambda\cdot tg(\alpha x)\cdot(1-x)^{\beta} \quad (1)$$

讨论 $\lambda,\alpha,\beta$ 满足的条件: 首先, $\lambda,\alpha,\beta$ 必须为正数; 其次引入 $\alpha$ 的目的是为了能调整正切函数原象的取值空间, 比如由 $(0,1)$ 放大到 $(0,\pi/2)$; 然后考虑函数在固定点处的斜率的模大于等于 1 的要求[1,3], 并让 $f(1/(1+\beta))>1/(1+\beta)$, 可初步得出

$$\lambda=\mu\cdot ctg\left(\frac{\alpha}{1+\beta}\right)\cdot\left(1+\frac{1}{\beta}\right)^{\beta},\ \mu>0 \quad (2)$$

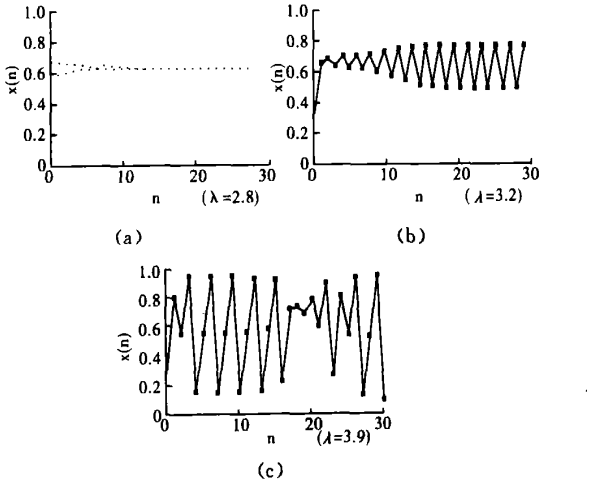


**图 1 Logistic 映射迭代特性**

最后利用实验—理论法, 得出 $\mu=1-\beta^{-4}$, 即新的混沌函数表示为:

$$f(x)=(1-\beta^{-4})\cdot ctg\left(\frac{\alpha}{1+\beta}\right)\cdot\left(1+\frac{1}{\beta}\right)^{\beta}\cdot tg(\alpha x)\cdot(1-x)^{\beta} \quad (3)$$

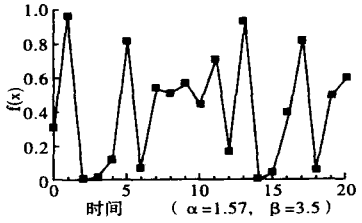


图 2 新算法的迭代特性

其中 $x\in(0,1)$, 控制参数 $\alpha\in(0,1.4]$, $\beta\in[5,43]$ 或 $\alpha\in(1.4,1.5]$, $\beta\in[9,38]$ 或 $\alpha\in(1.5,1.57]$, $\beta\in[3,15]$; 可见控制参数的取值区间较大. 在 $(0,1.4]$ 内随机选取 100 个 $\alpha$ 值, 对每一个 $\alpha$, 从 $\beta=5$ 开始, 每次增大 0.01, 直到 $\beta=43$, 经过约 39 万组(每组 100 万个)实验数据证明该迭代函数均能产生混沌现象, 满足非重复性、随机性、发散性要求. 随机选取其他 $\alpha,\beta$ 值做类似的迭代实验, 结果表明都能产生良好混沌效果. 取 $x_0=0.3$, $\alpha=1.57$, $\beta=3.5$ 时函数的迭代情况如图 2 所示.

### 2.3 实验分析

新的混沌迭代函数能够较好的产生混沌效果, 下面就算法的发散性做一下实验比较. 实验方法: 迭代次数选为 4000 次; 如图 3 所示, 视窗宽度方向坐标表示迭代时间, 高度方向坐标表示函数值; 视窗宽度选为200次迭代时到达的宽度, 从

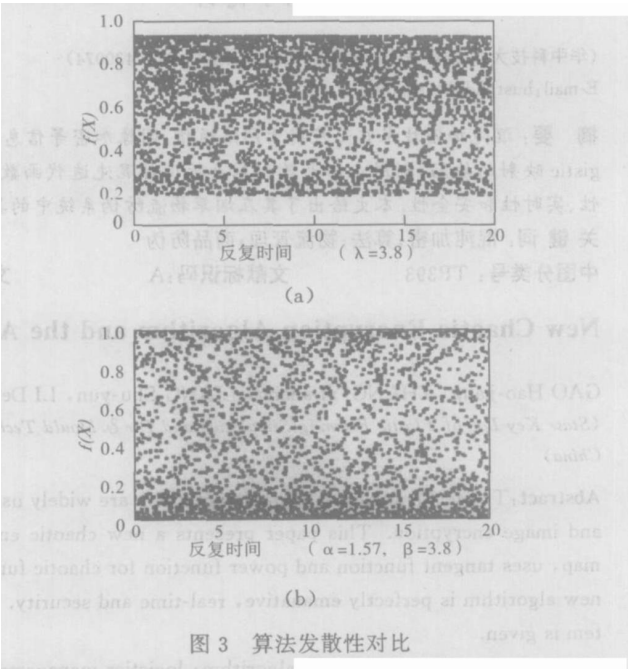


图 3 算法发散性对比

第 201 次迭代起返回坐标原点, 如此反复. 实验结果: 如图 3(a)为 Logistic 迭代函数在 $x_0=0.5$, $\lambda=3.8$ 的条件下函数值充填象空间的情形, 图 3(b)则为新算法在 $x_0=0.5$, $\beta=3.8$, $\alpha=1.57$ 时的充填情况; 可见前者存在明显的"稳定窗", 有盲区, 而本文的算法则基本能充满整个象空间, 具有较好的发散性, 因此具有更高的安全性.

## 3 基于混沌的加密算法设计

从美观角度考虑及受限于商品尺寸限制, 防伪数码的长度一般在 20 位左右. 加密算法设计的着眼点是利用混沌序列作为密钥. 加密前的信息可视为明文信息, 它由原始明文信息(6 位)、校验码(4 位)、混沌序列(10 位)组成; 其中校验码由原始明文信息和混沌序列运算得出, 混沌序列还起到保证密文满足非重复性要求的作用. 加密过程为: 从原始明文信息和校验码的信息集合 P 中, 取出一个字节 byte1, 再从混沌序列 Q 中取出一个字节 byte2, 两者做异或运算, 用新生成的一字节码 byte3 替换 byte1, 接着对第 2 个字节做类似运算, 直到存储 P 的 5 个有效字节全部运算完毕为止; 至此, 信息 P 已被混沌序列初步加密, 形成中间结果 M = P ⊕ Q, 然后利用 5 字节密钥 K 用类似的异或算法对 M 进行最后加密, 形成密文. 解密过程是加密过程的逆运算, 其过程大致为: 将密文 C 和密钥 K 进行异或运算, 求得 M, 从 M 中分离出 P 和 Q, 将两者做异或运算, 即求得原始明文信息和校验码.

## 4 安全性分析

该算法具有抗穷举攻击能力. 密码分析遇到的问题有 2 个: 一是获得密钥 K, 二是获得初值 $x_0$ 和控制参数 $\alpha$、$\beta$, 只有这样才能伪造数码. 因为 K 是 5 字节密钥, 那么可能的组合为 $2^{40}$. 再考虑 $x_0$、$\alpha$ 和 $\beta$, 其中 $x_0$ 取 10 位有效数字, 参考文献[4]的研究, 假设一台计算机浮点数的有效值位数为 16 位, 那么就有 10+ 15+ 15= 40 位数是不固定的, 其可能的组合为 $10^{40}$. 而现有的 56bitDES 加密算法具有的密钥组合为 $2^{56}$. 易证 $10^{40}* 2^{40}> 2^{56}$. 可见该算法具有较好的抗穷举破译的安全性.

该算法具有抗选择明文攻击能力. 通过将 $X_n$ 与 $X_{n+1}$ 之间的关系复杂化, 以避免攻击者解出 $\alpha$ 和 $\beta$ 如果在 $X_n$ 与 $X_{n+1}$ 之间隔几个数, 那么表示 $X_{n+1}$ 与 $X_n$ 之间的关系的方程就会循环套用自身, 从而变得异常复杂, 也就难以求解 $\alpha$ 和 $\beta$

## 5　物流防伪信息系统实例

本文给出一个烟草物流防伪信息系统实例, 该系统的功能是实现小包卷烟、条包卷烟的防伪功能及部分物流管理功能; 其系统结构如图 4 所示, 由数码生成模块、电子喷印设备(喷码机)、物流管理模块、查询识别统计模块组成; 喷码机自带有光电传感器以感应生产线上运动的商品.

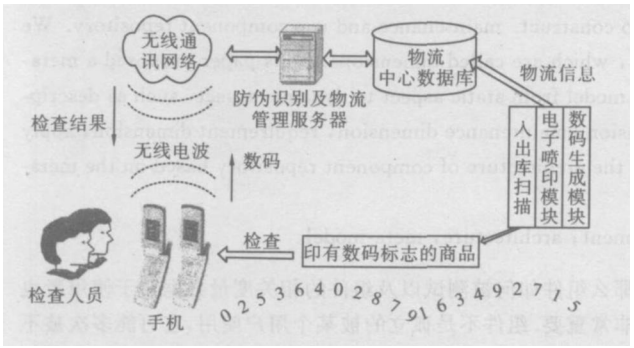


图 4　烟草物流防伪信息系统逻辑结构

系统的处理流程为: 首先, 数码生成模块利用混沌加密算法生成虚拟随机数码, 并存放在缓存中, 当有产品到来时, 利用 RS232 通信将随机数码送给喷码机喷印, 并在喷印完一件卷烟时出具一个条形码. 其中每个商品上的随机数码都与其对应件的条形码相绑定, 日后若要搜索商品的销售地, 就只需搜索其对应件的销售地. 这些数据被打包传送到物流中心数据库. 算法能够满足实时性要求, 并且相对激光刻印等方法来讲, 采用电子喷印技术能够保证生产速度; 在烟厂的实地实验数据表明, 其喷印速度可达 400 包/ 分钟以上. 喷印后的产品进入物流管理模块: 对 "件烟条形码 "进行出库扫描, 销售地信息通过网络记录到物流中心数据库; 收货方也可进行入库扫描以核对运输过程中有无遗漏真品、掺入赝品. 当商品流通到市场上后, 消费者可通过随机数码的非重复性、喷印样式的特殊性进行直观识别, 还可利用手机或者互联网进行验证. 进行数码验证时, 如果系统发现所查数码不存在或者解密后对应的明文信息不对或者校验码错误, 那么查询服务系统就会给出 "假冒产品 "的提示; 对于合法数码, 系统会回复其对应产品的生产信息及销售地信息, 如 "真品 XXX 牌香烟, 2004 年 10 月 15 号生产, XX 县销售 "; 同一数码被第 2 次查询时会给出 "谨防假冒, 第一次查询者是 XXX "的提示; 多次查询则被回馈 "怀疑是赝品 ", 并给出第一次查询者的信息. 查询服务模块力求做到查询的便捷, 同时能实现对稽查工作人员日、月、周工作量的考评以及产品物流和销售情况的模糊统计.

其混沌加密算法的控制参数分为两类: 一类是生产信息参数, 包括生产日期、商品品牌、生产线机组号等; 另一类则是控制参数 $\alpha$ 和 $\beta$, 不同的生产单位选用不同的控制参数. 对于每条生产信息, 混沌迭代次数(商品数) 在 30 万以内, 经计算机模拟等实验分析, 满足非重复性、非相关性要求.

物流防伪系统与传统的防伪技术相比有如下优势:

(1) 克服了防伪标志千篇一律的缺陷, 做到了标志的 "非重复性 ", 增大了复制难度;

(2) 识别方便, 可直观判断还可通过短信、电话等手段进行验证;

(3) 一般只要系统的密钥不丢失, 制假者想实现批量性假冒商品的行为而不被发现是很难的;

(4) 由于数码和商品一一对应, 还可实现部分物流跟踪功能.

## 6　结　论

本文为物品编码提供了一种混沌加密算法, 克服了 Logistic 映射存在的明显 "周期性窗口 "[5]缺陷, 具有更好的发散性; 以混沌序列作为加密密钥, 抗攻击能力强, 具有高安全性; 实地生产表明能够满足系统实时性要求. 此混沌加密算法还可应用于网络通信安全、图像加密等领域.

**References:**

[1] Yuan chun, Zhong Yu-zhuo, He yu-wen. Chaos based encryption algorithm for compressed video[J]. Chinese Journal of Computers, 2004, 27(2): 257-263.

[2] Robert Matthews. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989, XIII(1): 29-41.

[3] Wheeler D D, Matthews R A J. Super computer investigations of a chaotic encryption algorithm[J]. Cryptologia, 1991, 15(2): 140-152.

[4] Sun Ke-hui, Zhang Tai-shan. Design and implement of a data encryption algorithm based on chaotic sequenc[J]. Mini-Micro Systems, 2004, 25(7): 1368-1371.

[5] Wang Dong-sheng, Cao Lei. Chaos, fractals, applications[M]. Hefei: University of Science & Technology of China Press, 1995.

附中文参考文献:

[1] 袁　春, 钟玉琢, 贺玉文. 基于混沌的视频流选择加密算法[J]. 计算机学报, 2004, 27(2): 257-263.

[4] 孙克辉, 张泰山. 基于混沌序列的数据加密算法设计与实现[J]. 小型微型计算机系统, 2004, 25(7): 1368-1371.

[5] 王东生, 曹　磊. 混沌、分形及其应用[M]. 合肥: 中国科学技术大学出版社, 1995.