

基于双重混沌映射的数码防伪技术研究

魏 旭¹, 陆国平², 陈秋琼¹

(1 南通大学 电子信息学院, 江苏 南通 226019; 2 南通大学 电气工程学院, 江苏 南通 226019)

摘 要: 提出了一种基于双重混沌映射系统对商品的生产号进行数字加密的加密算法. 在加密的过程中用二维 logistic 映射和 Henon 映射联合对商品的生产号进行加密, 得到商品的防伪码, 并对双重混沌映射的性能进行了分析, 利用双重混沌系统的伪随机性、初值敏感性、遍历性等所特有的性质, 得出双重混沌映射具有良好的密码学特性, 提高了算法的复杂度, 增大了算法的密钥空间, 增加了破译的难度, 使商品在流通的过程中具有更强的防伪性能.

关键词: Logistic 映射; Henon 映射; 防伪; 破译; 密钥

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2012)08-0127-03

Research on Anti-counterfeiting Technology for Digital Based on Double Chaotic Map

WEI Xu¹, LU Guo-ping², CHEN Qiu-qiong¹

(1 School of Electronic and Information, Nantong University, Nantong 226019, China;

2 School of Electrical Engineering, Nantong University, Nantong 226019, China)

Abstract: The encryption algorithm of commodity production number for data encryption is proposed, which is based on double chaotic map system. In the encryption process, After we take the two-dimensional logistic map and Henon map together for the number of commodity production of scrambling encryption, we obtained the anti-counterfeit of commodity. Meanwhile, the performances under the double chaotic map are analyzed. Utilize the pseudo-randomness and initial value sensitivity and ergodicity characteristic of the double chaos map, The results show that double chaotic map have the good properties of cryptographic. which makes constructing algorithm more complex, key space of algorithm will be bigger and it's harder to break into this cryptosystem, As a result, the goods process of commodity circulation have a stronger function of anti-counterfeiting.

Key words: Logistic map; Henon map; anti-counterfeiting; decipher; key

1 引言

目前数码防伪技术由于防伪性能好、成本低廉、易于识别等优势得到了企业的青睐, 逐渐成为了当前社会防伪领域的主要技术. 尽管数码防伪的应用研究取得了较大的成果, 但算法的研究工作目前仍然存在一些困难, 使其在应用方面一直停滞不前. 从上个世纪的 80 年代末期混沌理论进入密码学领域以来, 混沌的加密算法得到了越来越多的重视, 而

且也已成为密码学研究的重要前沿.

把混沌系统用于加密最早是由英国数学家 Matthews 提出的^[1-2]. 混沌是一种非线性动态系统, 混沌具有不可预测性、不可分解性. 但是又有一定的规律性, 混沌对初始参数有高度敏感性, 初始值有微小的变化就会让一个混沌系统产生完全不同的混沌序列值. 但由于混沌系统具有一定的规律性, 在计算机上计算又存在精度问题, 鉴此本文提出用双重混沌映射进行加密, 其更好地弥补了单个混沌映射存

在周期性、短精度、密钥少等缺陷.

2 混沌系统

(1) Logistic 混沌映射

Logistic 映射是一种经典的混沌映射,其最初是用于预测人口的算法,其数学的表达式为

$$x_{n+1} = ux_n(1 - x_n) \quad (1)$$

式中, $x \in [0, 1]$, $u \in [0, 4]$ 称之为 Logistic 的参数. 研究表明, 随着参数 u 值的变化, Logistic 映射所产生的序列由倍周期分岔逐渐的转化为混沌. 通过实验可知: 当 $u \in (0, 3)$ 时, 函数经过多次迭代而慢慢的趋近于同一个值; 当 $u \in [3, 3.6)$ 时, 函数经过多次迭代后在若干个值之间振动, 且出现周期性; 当 $u \in [3.6, 4)$ 时, 周期现象消失, 表现出混沌现象; 且当 $u = 4$ 时, 该映射处于满射混沌状态^[3].

目前所使用的大多数的混沌序列发生器所采用的混沌的映射都是一维的, 虽然一维的混沌映射具有速度快等优点, 但是一维的混沌映射相对简单, 其密钥的空间相对较小, 可以通过重构的方法破译; 在本文中, 用两个一维的 Logistic 映射组合构成一个二维的混沌映射, 此映射较一维的映射有复杂度高、敏感性强、密钥空间大等优点. 其映射的表达式为

$$\begin{cases} x_{n+1} = u_1 x_n (1 - x_n) \\ y_{n+1} = u_2 y_n (1 - y_n) \end{cases} \quad (2)$$

式中, u_1, u_2 为混沌映射的参数, 和一维 Logistic 映射一样, 当 $u_1 = u_2 = 4$ 时, 研究表明该映射的混沌性能最好.

(2) Henon 映射

Henon 映射是由天文学家 Henon 提出的, Henon 映射的表达式为

$$\begin{cases} x_{k+1} = 1 + y_k - ax_k^2 \\ y_{k+1} = bx_k \end{cases} \quad (3)$$

式中 a, b 均为参数. Henon 映射的雅可比矩阵行列式为

$$|J| = \begin{vmatrix} -2ax & b \\ 1 & 0 \end{vmatrix} = -b \quad (4)$$

当 $|b| < 1$ 时, 说明面积是收缩耗散的^[4], 即每迭代一次, 使平面 (x, y) 上的面积收缩为原来的 $|b|$ 倍. 在 Henon 映射中, 含有两个参数为 a 和 b , 因此可以令一个参数为常数而取另一个参数为变量进行迭代, 这样就可以得到类似于 Logistic 映射的分岔, 也是经历了一系列的倍周期的分岔而达到混沌的.

文献[5]给出了一种二值序列的生成方法, 将 Henon 映射生成的序列 $\{x_1, x_2, \dots, x_n | x_i \in (0, 1), i$

$= 0, 1, \dots, n\}$, 将此序列进行二值转化得到序列 $\{y_1, y_2, \dots, y_n | y_i \in (0, 1), i = 0, 1, \dots, n\}$, 其转化方法为

$$y_i = \begin{cases} 0, & x_i \leq 0.5 \\ 1, & x_i > 0.5 \end{cases} \quad i \in 1, 2, \dots, n \quad (5)$$

那么得到的序列 $y_i \in \{0, 1\}, i = 1, 2, \dots, n$. 文献[6]对文献[5]进行了改进, 定义得到的二值序列 $\{y_1, y_2, \dots, y_n\}$ 为

$$y_i = \begin{cases} 0, & x_i \leq u \\ 1, & x_i > u \end{cases} \quad i \in 1, 2, \dots, n \quad (6)$$

式中, u 为序列 $\{x_1, x_2, \dots, x_n\}$ 的均值, 即: $u = \frac{1}{n} \sum_{i=1}^n x_i$

a_i . 在本文中可以对方法进行改进, 生成二进制序列, 从而完成对序列的加密.

3 加密算法的实现

算法实现的流程如图 1 所示.

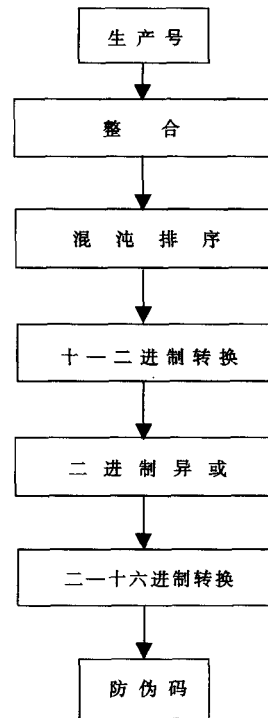


图 1 双重混沌算法流程图

由文献[7]可以知道, 一维的 Logistic 映射, 当 $u \in [3, 3.6)$ 时出现周期性; 当 $u \in [3.6, 4)$ 时, 周期现象消失, 表现出混沌效果, 但是该混沌也具有一定的问题, 比如: 存在明显的“稳定窗”, 即迭代的点聚集于某个区间, 而其他区间内则没有点. 由于单一混沌形式简单, 而且可以控制的参数比较小, 容易受到混沌重构攻击. 如果被截获一段连续的明文和密文,

就容易重构出混沌的原型. 二维的 Logistic 映射增加了控制的参数, 同时又使混沌的行为高度的复杂^[8]. 所以在本文的混沌系统中采取的是两个初值不同的 Logistic 映射组成的二维 Logistic 映射对产品的生产号进行置乱.

在商品的生产过程中, 我们可以给每一个商品一个 12 位的生产号, 将 12 位的生产号进行整合, 得到 8 位的身份码, 其整合的原则为将生产号的前六位整合成为一个两位数, 并将这个两位数作为身份码的前两位, 身份码的后六位则依次为生产号的后六位, 这样便可以得到一个 8 位的身份码.

用二维的 Logistic 映射对产品的身份码进行置乱可以得到产品的置乱码, 其二维的混沌序列为

$$\begin{cases} x_{n+1} = 4x_n(1-x_n) \\ y_{n+1} = 4y_n(1-y_n) \end{cases} \quad (7)$$

将置乱码的每一位都转化为四位的二进制数, 那样就可以得到置乱的二进制数组.

用 Henon 映射进行迭代 32 次. 在本文中, 可以对文献[6]的介绍的方法进行改进, 在用序列的均值作为中间值, 有的时候因为序列值的变化比较大, 在某个值的区间内出现值的堆积, 而序列值的波动有非常的大, 这样产生的二值序列平衡性很差, 所以, 本文中采用对中间值进行赋值, 这样在加密的过程中, 所取的中间值也可以作为密钥的一部分. 将迭代所产生的序列值与所取的中间值进行比较, 大于中间值的则赋值为“1”, 小于中间值的则赋值为“0”:

$$f(x) = \begin{cases} 1, & x > u \\ 0, & \text{其他} \end{cases} \quad (8)$$

式中, u 为所取的中间值, 其值可以根据需要而不断变化, 增加了系统算法的复杂度. 将得到的二进制组与置乱码的二进制组按位进行异或, 这样就可以得到一个新的二进制组, 然后按四位的二进制数转化为一位的十六进制数进行转化, 则可以得到 8 位的十六进制数, 即为防伪码.

4 仿真结果

在本算法中, 我们取二维 Logistic 映射的参数 $u=4$, 且两个初值为 0.521 1, 0.545 6; Henon 映射的初值为 0.6 和 0.2, 表 1 所示为加密结果, 表 2 所示为 Henon 映射的初值为 0.61 和 0.21 的加密结果. 通过表 1 和表 2 中对相同的生产号进行加密, 由

于初值的不同, 所得到的防伪码截然不同, 这符合密码学的特点.

表 1 加密结果 1 (Henon 初值为 0.6、0.2)

生产号	身份码	防伪码	解密后的生产号
110324010001	38010001	f5fa961d	110324010001
210527091024	53091024	fdabb016	210527091024
170905173001	31173001	e3f99614	170905173001
351101122591	47122591	e6f80142	351101122591
461015079999	71079999	f3730284	461015079999

表 2 加密结果 2 (Henon 初值为 0.61、0.21)

生产号	身份码	防伪码	解密后的生产号
110324010001	38010001	f5ba9e35	110324010001
210527091024	53091024	fdabb83e	210527091024
170905173001	31173001	e3b99e3c	170905173001
351101122591	47122591	e6b8096a	351101122591
461015079999	71079999	f3330aac	461015079999

5 敏感性测试

在本文中, 对 Henon 映射进行序列二值化时取 $u=0.4$, 那么可以对 Henon 映射进行频数测试, 从而可知 Henon 映射产生的二值序列所具有的平衡

针对序列的随机性的问题, 2001 年美国国家标准局 NIST 发布的白皮书中, 给出了测试序列的随机性和伪随机性的 16 项测试方法和认证标准, 目前这些已经成为多数国家安全部门检测密钥随机性的权威评测标准^[9]. 文献[9]给出了给出了一种测试序列的随机性的测试方法. 测试结果证明, 本算法产生的序列是随机的, 可用于作随机密钥, 对数字进行加密.

6 结束语

本文将双重混沌映射的产生的混沌序列用于数码防伪技术中, 以一种新的思路和方法来生成商品的防伪码. 利用双重混沌序列具有更强伪随机性、初值敏感性等独有的一些性质, 满足数码防伪过程中对密钥敏感性的要求. 把混沌序列应用到数码防伪技术中, 实现了一个快速可靠、安全方便的数码防伪

(下转第 133 页)

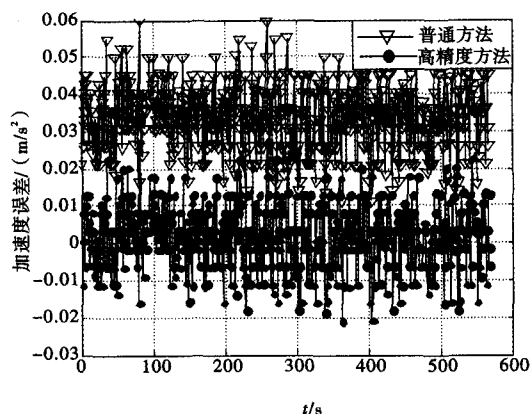


图1 两种方法加速度计输出误差对比

精确标定方法标定以后,得到的加速度与实际加速度值更接近,并且抖动范围也比较小,充分证明了本文标定方法的有效性。再对比表中两种方法的系数可以知道,本次标定,高精度标定方法主要是对粗略标定的零偏进行修正,两种方法的其它系数项基本相同。

5 结束语

本文分析了现有标定方法的优缺点,并针对已有标定方法的不足给出了一种无需转台的高精度标定方法。该方法应用两种加速度计模型先进行粗略标定,以粗标定结果作为精确标定的初始值进行迭代,最终求解出加速度计系数的精确值。

(上接第129页)

系统。在今后的研究中,可通过多测试不同的混沌系统的随机性、安全性等等,致力于研究和开发更具有安全实用的数码防伪系统。

参考文献:

- [1] 徐大雄. 列入中华人民共和国国家标准的10项防伪技术[J]. 激光杂志, 1999, 10(4): 1-5.
- [2] 盛苏英, 吴新华. 一种新的图像加密算法研究与应用[J]. 微电子学与计算机, 2011, 28(2): 124-128.
- [3] 孙炯, 赵东风, 丁洪伟. 扩展 Logistic 混沌序列性能分析[J]. 云南大学学报: 自然科学版, 2007(2), 136-139.
- [4] 赵芮. 基于二维 logistic 与 chebyshev 映射的 AES 的混沌加密算法[D]. 山西: 太原理工大学, 2008.
- [5] Zhang Han, Wang Xiu Feng. A new image encryption algorithm based on chaos system[C]// Proceedings of the International Conference on Robotics, Intelligent Systems and Signal Processing. China, ChangSha;

参考文献:

- [1] 陈北欧, 孙文胜. 捷联组合(设备无定向)六位置测试标定[J]. 导弹与航天运载技术, 2001(3): 23-27.
- [2] 刘百奇, 房建成. 一种改进的 IMU 无定向动静混合高精度标定方法 [J]. 仪器仪表学报, 2008(6): 1250-1254.
- [3] Syed Z F, Aggarwal P, Goodall C, et al A new multi-position calibration method for MEMS inertial navigation systems[J]. Measurement Science And Technology, 2007, 18(7): 1987-1907.
- [4] 张红宇, 叶新生. 一种改进的 IMU 加表标定模型及快速标定方法 [J]. 理论与实践, 2009(3): 11-13.
- [5] 吕晶晶, 姚金杰. 基于最小二乘和牛顿迭代法的空中目标定位 [J]. 微电子学与计算机, 2011(9), 108-110.
- [6] 何坤鹏, 吴俊伟. 光纤捷联惯性测量组件在无安装基准时标定方法 [J]. 北京理工大学学报, 2009(3): 219-223.
- [7] John J Hall, Robert L Williams. Inertial measurement unit calibration platform [J] Journal of Robotic Systems, 2000, 17(11): 623-632.
- [8] 温银萍, 温廷敦. 介观压阻型硅锗加速度计研究 [J]. 微电子学与计算机, 2009(3): 22-25.

作者简介:

陈剑 男, (1986-), 硕士研究生. 研究方向为组合导航算法.

IEEE, 2003: 778-782.

- [6] 张雪峰, 范九伦. 改进的混沌序列产生方法[J]. 计算机工程与设计, 2007, 28(3): 600-601.
- [7] 李长庚, 周家令, 孙克辉, 等. 四种数字混沌扩频序列的平衡性分析[J]. 计算机应用, 2008, 28(1): 68-70.
- [8] 刘成斌. 混沌加密算法的研究与实现[D]. 北京: 邮电大学, 2009.
- [9] 张颖. 基于数字混沌的密钥系统设计与应用研究[D]. 大连: 大连海事大学, 2010.

作者简介:

魏旭 男, (1988-), 硕士研究生. 研究方向为混沌加密技术与保密通信.

陆国平 男, (1965-), 教授, 博士生导师. 研究方向为非线性信号处理、智能控制、鲁棒控制研究.

陈秋琼 女, (1987-), 硕士研究生. 研究方向为混沌图像加密技术.