

基于混沌的数码防伪系统研究与实现

盛苏英^{1,2}, 吴新华³

(1 南通大学 杏林学院, 江苏 南通 226007; 2 南通大学 电气工程学院, 江苏 南通 226019;

3 南通纺织职业技术学院 现教中心, 江苏 南通 226007)

摘 要: 设计并实现了一套基于混沌的数码防伪系统. 基于混沌密码技术, 分别提出一种生成防伪码和验证码的混沌密码加密算法, 并采用“双标双码、双向验证”防伪工作机制, 构建了一个能进行电话查询的混沌数码防伪系统, 实现了防伪查询智能鉴别, 系统测试表明该系统防伪效果好且方便实用, 适合推广.

关键词: 混沌; 数码防伪; 双向验证

中图分类号: TP309.7; TP391

文献标识码: A

文章编号: 1000-7180(2011)05-0063-04

Study and Implementation of a Digital Anti-counterfeiting System Based on Chaos

SHENG Su-ying^{1,2}, WU Xin-hua³

(1 Xinglin College, Nantong University, Nantong 226007, China;

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

3 Modern Education Technology Center, Nantong Textile Vocational Technology College, Nantong 226007, China)

Abstract: A chaotic digital anti-counterfeiting system is designed and implemented. At first, a new chaotic encryption algorithm to generate anti-counterfeiting code and identifying code is proposed on the basic of chaotic cryptography. Then an anti-counterfeiting mechanism of "two codes, two-way authentication" is adopted. And a digital anti-counterfeiting system inquired by telephone is constructed to realize intelligent identification. At last, the results of system testing show that the system is effective, convenient and practical to popularize.

Key words: chaos; digital anti-counterfeiting; two-way authentication

1 引言

当今社会, 商品伪造已日益成为全球经济领域面临的严重问题, 小到一粒药片, 大到飞机、汽车零部件, 几乎所有品牌产品都被造假行为所困扰^[1]. “造假”已成为世界各国仅次于贩毒的第二大社会公害, “防伪”也已成为全世界范围内的重大课题.

数码防伪自 1996 年诞生以来, 经过各界人士的不懈努力, 现已成为防伪行业中应用最为广泛的防伪技术之一. 根据防伪码生成方式的不同, 数码防伪技术主要经历了随机条码、加密有序流水号, 以及综

合防伪模型三个阶段^[2-3]; 数码防伪查询方式多种多样, 消费者可通过上网、拨打免费电话或发送手机短信方式查询商品的真伪^[4-5]. 尽管数码防伪技术的应用研究已取得了较大的成绩, 但防伪码生成的研究工作仍然存在许多困难, 使其在应用领域一直停滞不前. 究其原因, 主要是因为现有的数码防伪技术, 基本上都是建立在伪随机序列, 或者有序流水号经过对称加密的基础上产生的防伪码, 与数码防伪技术“不可伪造性和唯一性”的性能要求有一定的差距, 缺乏密码学的理论技术支撑.

混沌信号具有隐蔽性、不可预测性和易于产生、

收稿日期: 2010-07-14; **修回日期:** 2010-09-28

基金项目: 国家自然科学基金项目(60474076); 江苏省自然科学基金项目(BK2010275); 南通市应用研究计划项目(K2010017); 南通大学杏林学院科研基金项目(2010K110)

复制等特点,混沌系统作为一种天然的密码系统,已被引入到密码学领域.自 1980 年代末期混沌理论进入密码学应用领域以来,混沌密码技术、混沌加密算法得到了越来越多的重视,现已成为密码学研究的重要前沿^[6-8].文中引入混沌密码技术,以全新的思路和方法生成防伪码和验证码,研究提出“双标双码、双向验证”防伪工作机制,从而实现一个基于混沌的电话查询数码防伪系统.

2 系统概述

系统利用 BCB 编程语言,结合混沌密码、网络通信和语音合成技术,实现了混沌数码防伪生成与查询,具有很强的保密性和较高的实时性,可进行多用户并发查询,系统框图见图 1.

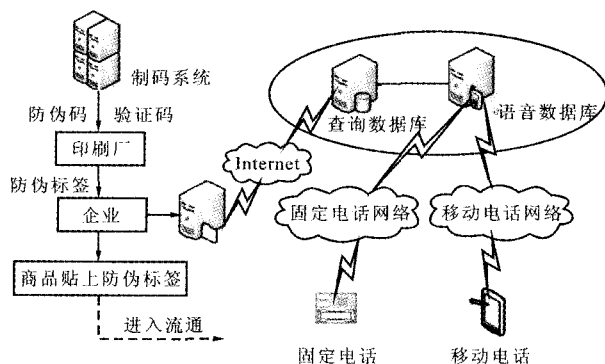


图 1 系统整体框图

首先,“制码系统”利用混沌密码加密算法生成商品的防伪码和验证码,并交给印刷厂制成防伪标签,企业在每个商品上粘贴防伪标签,然后将商品流入市场.消费者购买商品后,可以方便地通过固定电话或移动电话输入防伪码,查询服务器会自动调用混沌解密函数校验防伪码的真伪,并将结果返回给消费者,实现“双向验证”.

3 系统设计与实现

3.1 混沌系统

系统采用的 Logistic 混沌映射形式如下:

$$x_{k+1} = \mu x_k (1 - x_k) \quad (1)$$

混沌动力系统的研究指出:当 $3.569\ 945\ 6\cdots < \mu \leq 4, x_k \in (0, 1)$ 时, Logistic 映射工作于混沌状态;而且 Logistic 映射对参数 μ 具有极度敏感性.

系统采用的 Cubic-Henon 复合混沌映射形式如下:

$$\begin{cases} x[k+1] = -3x[k] + 4x^3[k] \\ y[k+1] = 1 + 0.3z[k] - 1.4y^2[k] \\ z[k+1] = y[k] \end{cases} \quad (2)$$

式中, $x[k]$ 是 Cubic 混沌映射的状态; $y[k], z[k]$ 是 Henon 混沌映射的状态.

系统采用了一种新的混沌系统,其形式为

$$x_{n+1} = (1 - \beta^{-4}) * \operatorname{ctg}\left(\frac{\alpha}{1 + \beta}\right) * (1 + \beta)^{\beta} * \operatorname{tg}(\alpha x_n) * (1 - x_n)^{\beta}$$

式中, $x_n \in (0, 1)$, 控制参数为 $\alpha \in (0, 1.4], \beta \in [5, 43]$ 或 $\alpha \in [1.4, 1.5], \beta \in (9, 38]$ 或 $\alpha \in (1.5, 1.57], \beta \in (3, 15]$ 时, 该迭代函数均能产生混沌现象.

3.2 混沌加解密算法

混沌加密算法用于产生 20 位的防伪码和验证码, 具体见图 2.

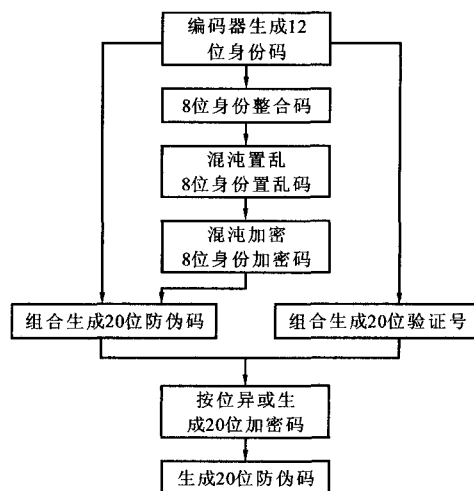


图 2 防伪码和验证码生成原理图

(1) 混沌加密——20 位防伪码的生成

步骤 1: 首先给每个商品设定唯一的 12 位身份码(其中前 6 位代表了商品生产的日期, 第 7、8 位代表生产该商品的生产流水线号, 最后 4 位代表该商品在某流水线上的生产序号), 再形成 8 位的身份整合码.

步骤 2: 利用 Cubic-Henon 复合混沌映射, 产生 3 个数组 $x[n], y[n], z[n]$, 分别从中随机取 8 个元素对应相加, 得到随机数组并按升序排列, 按对应排序规律由身份整合码得身份置乱码.

步骤 3: 利用 Logistic 混沌映射产生数组 $x_1[n]$, 进行技术处理, 使数组 x_1 中各元素都是属于 $[0, 9]$ 之间的整数. 取身份整合码和数组 $x_1[n]$ 中 8 个元素按位异或并对 10 取整, 得到身份加密码.

步骤 4: 组合生成 20 位的商品防伪码(前 12 位为商品身份码, 后 8 位为身份加密码).

(2) 混沌加密——20 位验证码的生成

步骤1:组合生成商品验证号(前8位为身份置乱码组成,后12位为商品身份码)。

步骤2:将商品验证号和防伪码中各元素按位异或,得到一个20位的加密码数组,各元素均为属于 $[0,9]$ 的整数。

步骤3:利用新混沌映射函数将加密码数组置乱,置乱后得到商品验证码。

(3) 防伪解密

防伪码的解密过程就是防伪码生成的逆过程,这里就不赘述了。

3.3 “双标双码、双向验证”防伪机制

系统利用混沌密码加密算法,分别生成商品的防伪码和验证码,将两个码分别打印在标签上,形成“双标双码”。防伪查询时,消费者输入商品防伪码,系统自动调用混沌解密快速算法:如果解密不通过,则系统提示消费者该防伪码为假;如果解密通过,则生成验证码反馈给消费者,让消费者自我识别,从而实现“双向验证”防伪查询机制,这样可以提高查询速率,有效防止假冒者伪造一个数码防伪系统来欺骗消费者,具体见图3。

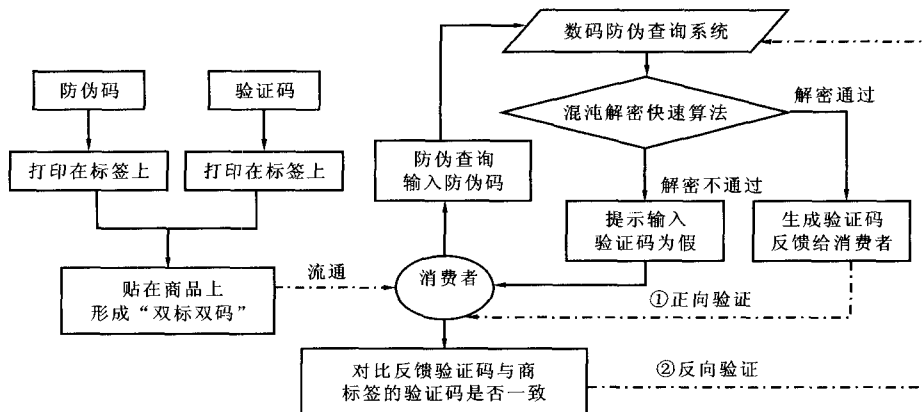


图3 “双标双码、双向验证”工作原理图

3.4 系统界面设计

本系统分为两个子系统:防伪码、验证码生成系统(即制码系统)和电话查询系统。

“制码系统”界面中输入“商品身份码”,点击“防伪码、验证码生成”按钮即可自动生成相应防伪码和验证码(系统界面见图4),然后将防伪码和验证码做成防伪标签(标签表面喷有涂层)贴于商品表面。

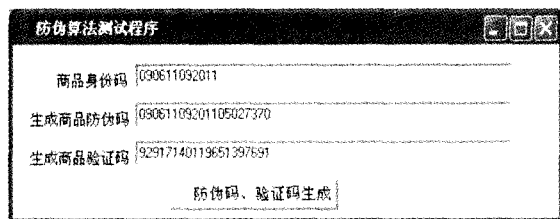


图4 制码系统界面

消费者购买商品获得防伪码后,电话查询系统提供商品真伪辨别服务,其界面如图5所示。

若无查询电话打入时,“流程状态”栏显示“空闲”。

若消费者打入电话进行防伪查询时,“流程状态”栏显示“接受外线来电”,系统工作流程如下:

(1)连接成功摘机后,“流程状态”栏显示“致欢

迎词”,同时播放欢迎词;

(2)致欢迎词完毕后,“流程状态”栏显示“请输入防伪码”,同时进行语音提示,“输入商品防伪码”栏会实时显示消费者输入的防伪码;

(3)待消费者输入防伪码结束,“流程状态”栏显示“确认防伪码的输入”,并进行语音提示确认;

(4)待消费者确认后,系统进行商品真伪判别,若消费者输入的防伪码经查询有误,在“商品真伪”栏将显示“假货”字样,若消费者输入的防伪码经查询正确,“商品验证码”栏可以显示反馈给消费者的验证码。

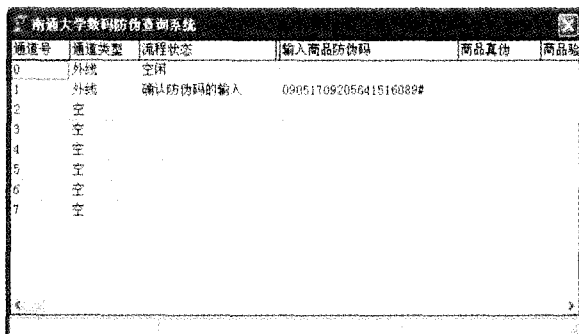


图5 电话查询系统界面

4 系统测试

文中对“制码系统”和电话防伪查询系统分别作如下测试:

(1)“制码系统”运算速度快,密钥敏感性高,真伪鉴别能力强,生成的防伪码具有唯一性,适合运用于防伪系统中。

(2)分析数码防伪电话查询系统可能遭到的几种攻击途径。攻击途径说明:①入侵者模仿用户;②入侵者在应用服务器上放置木马攻击程序;③入侵者使用木马程序窃取数据库服务器上的防伪信息(防伪码、验证码)。

对于途径①,即入侵者伪造防伪码,其安全性可由制码系统所生成防伪码的不可伪造性保证;对于途径②,可以通过加强应用服务器的管理和规范来避免,同时将混沌加密、解密程序封装成 DLL 文件,使整个加解密算法运算过程“不可见”,从而抵挡一定的木马攻击;对于途径③,系统使用的数据库,只存储了查询商品身份码、查询电话、查询时间等信息,而没有存储商品的防伪码、验证码、混沌密钥等关键信息,即使数据库被木马攻击,也不会造成很大的影响。

从上面的分析来看,文中构建的“制码系统”和数码防伪电话查询系统是安全可行的,而且操作简单,方便实用,适合推广。

5 结束语

文中将混沌密码技术引入数码防伪领域,以全新的思路和方法生成防伪码和商品验证码;同时研究提出了一种新型的“双向验证”快速算法,形成“双标双码、双向验证”防伪机制,独创性地提出了混沌数码防伪技术,实现了一个可靠、安全、高速和人性

化的数码防伪系统。在今后的工作中,可结合多种最新技术,致力于研究和开发更具实用价值和推广价值的混沌数码防伪系统。

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] 王向华, 刘秀功, 谢涛. 一种新型的数码防伪系统[J]. 计算机工程, 2006, 32(3): 171—174.
- [3] 赵卓, 陈立杰. 密码技术在数字防伪系统中的应用[J]. 计算机工程与设计, 2005, 26(10): 2860—2862.
- [4] 刘怀. 电话数字防伪系统的设计与实现[J]. 控制工程, 2003, 5(10): 410—413.
- [5] Wang Y. Design of an anti-counterfeiting system based on SMS[C]// IEEE International Conference on Granular Computing (GRC'09). Nanchang: IEEE, 2009: 572—575.
- [6] Kwok H S, Tang W K, Man K F. Online secure chatting system using discrete chaotic map[J]. International Journal of Bifurcation and Chaos (Int JBC), 2004, 14(1): 285—292.
- [7] Zheng Y F, Chen G R, Zhu C Y. A system inversion approach to chaos-based secure speech communication [J]. International Journal of Bifurcation and Chaos (Int JBC), 2005, 15(8): 2569—2566.
- [8] Liu Y, Mao Y, Tang W K, et al. Cryptanalysis of chaotic communication schemes by dynamical minimization algorithm [J]. International Journal of Bifurcation and Chaos (Int. JBC), 2009, 19(7): 2429—2437.

作者简介:

盛苏英 女, (1979—), 硕士, 讲师. 研究方向为混沌保密通信。

吴新华 男, (1980—), 硕士. 研究方向为混沌加密。