

混沌数码防伪技术研究与应用

盛苏英, 陈 轶

(南通大学 电气工程学院, 江苏 南通 226019)

摘 要: 基于混沌密码技术, 提出并完善了一种混沌密码数码防伪技术, 以解决数码防伪技术长期面临的技术难题. 研究一种混沌加密算法以生成商品防伪码和验证码, 并提出一种支持多种查询方式多次查询验证的“双向验证”算法, 形成并优化了“双标双码、双向验证”防伪工作机制; 同时构建了一套既可现场识别又可通过电话、短信、网络(Internet、WAP)查询验证的全方位数码防伪系统, 实现了防伪查询智能鉴别, 以此证明所提数码防伪技术的有效性和可靠性.

关键词: 混沌密码; 数码防伪; 双标双码; 双向验证; 防伪码; 验证码; 查询验证

中图分类号: TP309.7; TP391

文献标识码: A

文章编号: 1000-7180(2012)08-0169-06

Research and Application of Chaotic Digital Anti-counterfeiting Technology

SHENG Su-ying, CHEN Yi

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

Abstract: A novel chaotic digital anti-counterfeiting technology is proposed and improved based on chaotic cryptography, ordering to resolve the long-term technical problems. A new chaotic encryption algorithm is studied to generate commodity security codes and verification codes, and a new type of checking algorithm of “two-way authentication” is proposed which can provide many ways to search and multiple query verification, so as to form and optimize an anti-counterfeiting mechanism of “two codes, two-way authentication”. Then a comprehensive digital anti-counterfeiting system is constructed to realize intelligent identification, which provides not only site identification but also checking by phone, short message and network (Internet or WAP). It is proved that the proposed technology is effective and reliable.

Key words: chaotic cryptography; digital anti-counterfeiting; double-label with double-code; two-way authentication; security codes; verification codes; query validation

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, 其不仅极大损害了生产厂商和广大消费者的切身利益、扰乱了市场秩序, 而且对品牌建设和维护社会稳定带来了极其恶劣的影响^[1]. 数码防伪技术的应用可一定程度上防止和减少商品假冒伪劣现象的发生.

数码防伪在短短十几年的时间中得到了迅速发展, 现已成为防伪行业中应用最为广泛的防伪技术之一. 综观其发展过程, 先后出现了基于随机条码、加密有序流水号, 以及综合数码三种防伪模型^[2-3]; 同时出现了电话、短信、Web 网络等多种查询方式的数码防伪系统^[4-5]. 尽管数码防伪技术的研究已取得较大成绩, 但现有数码防伪普遍缺乏密码学理论技术支撑, 生成防伪码的安全性不够理想^[6], 同时

收稿日期: 2012-01-12; **修回日期:** 2012-03-09

基金项目: 国家自然科学基金项目(61004027, 61174065); 江苏省自然科学基金项目(BK2010275); 南通市应用研究计划项目(K2010017); 江苏省高校自然科学研究项目(10KJB120002); 江苏省高等学校大学生实践创新训练计划项目

在应用时依然存在一些防伪漏洞,这些防伪技术漏洞,一直困扰着整个防伪行业,也一直是防伪公司不敢提及、刻意回避的尴尬,极大影响了防伪技术的权威性与可信度,很大程度上制约了防伪行业的健康发展。

针对现有防伪码生成机制难以满足实际应用中的安全性要求,综合考虑现有数码防伪技术存在的安全漏洞,本文引入混沌密码技术,提出并完善了混沌数码防伪技术——采用混沌密码加密算法生成在消费后能自动分离的“双标双码”即防伪码和验证码标签,支持用户通过多种查询方式多次查询,商品真伪查询时采用快速的“双向验证”算法,从而解决了数码防伪技术长期面临的技术难题。同时构建了一套既能现场认定又可通过电话、短信、网络(Internet、WAP)查询验证的全方位数码防伪系统,方便有效地实现商品真伪的鉴别,以验证所提混沌数码防伪技术的有效性和可靠性。

2 混沌数码防伪技术

2.1 数码防伪工作机制的提出与完善

现有文献资料表明,目前数码防伪技术基本上都是基于伪随机序列(PN Pseudo-noise Sequence)或有序流水号经过 DES(Data Encryption Standard)对称加密后进行的研究^[7-8],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,普遍缺乏密码学理论技术支持。而将防伪码变成随机码,即将有序变为无序的过程,本身就是一个“混沌化”的过程。由于混沌系统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和伪随机性的特性,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^[9-11]。因此笔者设想将混沌密码技术引入数码防伪领域,结合混沌密码加密算法,生成具有混沌特性的防伪码,满足数码防伪技术“不可伪造性和唯一性”的性能要求。

进一步研究发现,现有的数码防伪技术在应用时依然存在一些漏洞,如:(1)单枚合法身份标签批量复制造假的防伪漏洞;(2)未破损、未查询包装物回收利用造假的防伪漏洞;(3)商品生产企业掌管物流资源的职工,以及渠道经销商利用合法的身份和渠道,挂羊头卖狗肉式造假的防伪漏洞;(4)提供服务的数码防伪系统可能被攻击、篡改或假冒的防伪漏洞。同时文献^[6]初步提出了“双标双码、双向验证”的数码防伪机制概念,但其所提混沌密码加密算法在商品身份码编码、算法速度与安全性方面均存

在一定问题,其所提的双向验证算法无法满足消费者多种查询方式、多次查询、快速查询反馈的普适性需求。在此情况下,笔者引入商品身份码的概念,结合商品物流管理理念,采用一个商品拥有消费后能自动分离的防伪码和验证码两个标签,消费者和防伪查询系统可进行多次、多种交互验证的工作方式,从而提出了数码防伪工作机制——“双标双码,双向验证”工作机制(具体见图1),以解决困扰防伪行业多年的防伪技术漏洞。

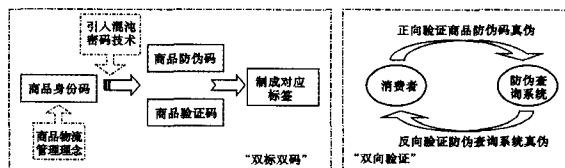


图1 数码防伪工作机制图

对于数码防伪系统而言,数据存储量以及数据存储安全是系统可靠运行的前提,现有数码防伪技术普遍将商品的防伪码信息、查询验证信息全部直接存在数据库中,造成数据库存储容量的不断增大,同时面临诸多安全隐患。防伪码生成算法的安全性和实时性(即生成速度)是一对矛盾,提高算法的安全性必然会影响其实时性,而一味地要求算法的实时性也必然会使其实时性大打折扣。针对上述情况,笔者对提出的数码防伪工作机制进行了适当的补充与完善:商品的防伪码等敏感信息不存入数据库,同时商品查询验证信息的数据库存储当且仅当在消费者进行有效查询后才执行,以此节约数据库资源、保证敏感数据的安全;该技术支持消费者通过电话、短信、网络(WAP、WEB)或现场识别仪等多种查询验证方式多次重复查询,方便实用;对所提混沌密码加密算法进行修改和优化,以期在其安全性和实时性之间找到一个平衡点,满足混沌数码防伪技术的安全性和生产实时性的双重需求。

本文在混沌密码技术的基础上,提出并完善了数码防伪工作机制——“双标双码、双向验证”,使其具有更大的实用价值和应用推广价值。

2.2 “双标双码”

本文引入混沌密码技术,采用混沌密码加密算法产生22位防伪码和8位验证码,制成消费后能实现自动分离的防伪码标签和验证码标签,形成了“双标双码”防伪技术。为了保证每个厂家生产的每件商品都有唯一的商品身份码,本文按一定规则定义14位的商品身份码;为了兼顾防伪码、验证码生成算法的安全性和快速性,本文调整混沌加密算法,采用较

为简单的 Tent 与 Logistic 混沌映射,生成 22 位防伪码和 8 位的商品验证码。

2.2.1 防伪码、验证码生成算法

(1)混沌密码加密算法——防伪码、验证码的生成

步骤 1. 给每个商品设定唯一的 14 位身份码(其中前 4 位代表厂家代码和商品代码,第 5 至第 10 位代表商品生产日期,最后 4 位代表该商品在某流水线上的生产序号),再形成 8 位的商品身份整合码。

步骤 2. 首先利用混沌 tent 帐篷映射(见式(1)),产生混沌序列 $\{z_i\}$,从中取 8 个元素,得到随机数组并按升序排列,按对应排序规律由商品身份整合码得身份置乱码;再利用 Logistic 混沌映射(见式(2))产生混沌序列 $\{x_i\}$,从中取 8 个元素并扩大 1 000 倍,然后将其和身份置乱码对应元素相加后对 10 求余,得到身份防伪号;最后组合生成 22 位的商品防伪码(前 14 位为商品身份码,后 8 位为身份防伪号)。

步骤 3. 将 8 位商品身份整合码和防伪号进行异或运算,得到商品验证临时号,然后将各位大于 9 的数值变换为 0~9 的数值,形成商品验证号;再对其每一位减 9 后进行求绝对值运算,从而得到 8 位商品验证码(具体过程见图 2)。

其中:Tent 帐篷映射方程为

$$z_{i+1} = f(z_i) = \begin{cases} \frac{z_i}{p} & \text{if } 0 \leq z_i \leq p \\ \frac{1-z_i}{1-p} & \text{if } p < z_i \leq 1 \end{cases} \quad (1)$$

Logistic 映射方程为

$$x_{k+1} = \mu x_k (1 - x_k) \quad (2)$$

系统取 $P=0.56$, $\mu=0.395$,混沌密钥即初值 z_0 和 x_0 均由商品身份码按一定规则组合提供,且满足 $z_0 \in [0,1]$ 和 $x_0 \in [0,1]$,使帐篷映射和 Logistic 映射均工作于混沌状态。

(2)算法性能测试

本文对算法的运算速度、生成防伪码的唯一性等分别进行了如下测试:

笔者采集 10 000 组商品身份码进行混沌密码加密运算,生成防伪码和验证码平均每组耗时约为 3.69 ms,可见该算法的运算速率较高。

防伪码和验证码的生成由混沌系统参数、混沌密钥、加密算法共同决定,如造假者即使知晓该防伪码、验证码的生成算法机制,而不知道混沌密钥产生

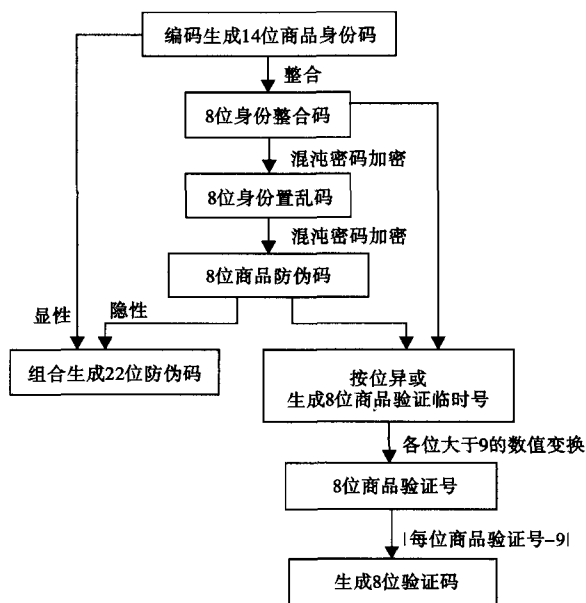


图2 防伪码、验证码生成算法流程图

方式,只要混沌密钥发生细微的变化,生成的防伪码、验证码与真实的防伪码、验证码“差之千里”,实验结果显示混沌密钥敏感度达到 $10^{-10} \times 10^{-11}$,从而保证了商品防伪码唯一性的性能需求。

(3)算法封装

本文将混沌密码加密算法封装成函数,可方便地嵌入数码防伪系统中,使用非常简单。其中 $\text{char} * \text{fangwyzm}(\text{char} * \text{shenfm})$ 表示生成防伪码、验证码的函数,其中参数 shenfm 表示输入的商品身份码,函数返回商品防伪码和验证码。

2.2.2 “双标双码”的制作与数据存储

商品防伪码印刷或喷涂在粘贴于商品或商品包装的标签上,其中商品身份码是以数字和条形码两种形式显性印刷,而将商品防伪号涂敷覆盖;商品验证码是隐性印刷或喷涂在商品开口即可脱落的封条、拉线或隐藏于包装盒内的卡片等标签上,使得商品在消费后其防伪码和验证码标签即可实现自动分离。

在商品防伪码标签上显性设置商品身份码,可在不破坏防伪码标签的情况下利用条形码扫描装置批量扫描商品身份码,便于开展大规模防窜货普查,以满足生产厂家和总经销商对物流跟踪和防窜货监管的需要。

算法生成的商品防伪码和验证码均不存储在数码防伪中心数据库中;同时混沌加密密钥分别由商品身份码按一定规则生成,也不需存储在数据库中,这样不仅节约系统资源,而且保证了数据的存储安

全.

2.3 “双向验证”

本文提出的混沌数码防伪技术支持消费者通过多种查询方式多次查询,查询时采用混沌密码解密算法验证所输入防伪码的真伪,同时将结果返回给消费者——如解密不通过,则提示消费者该防伪码为假,如解密通过,则生成验证号和重复查询密码一起反馈给消费者,以便消费者根据返回验证号可同时辨别商品和防伪系统的真伪,从而实现“双向验证”防伪技术.

2.3.1 防伪码查询、双向验证算法

(1)混沌密码解密算法——防伪码查询,双向验证

步骤 1,首先根据查询输入的商品防伪码,由商品身份码判断该商品是否已被查询,如已查过,则再次判断输入的重复查询密码是否正确,如不正确,则返回信息“该商品已于××年××月××日××时

××分查询,谨防假货!”,否则进入下一步.此步骤可满足消费者多次查询的需要.

步骤 2,首先将商品防伪码分解为商品身份码和商品防伪号;然后进行防伪码生成算法(即混沌密码加密算法的步骤 2)的逆运算,由商品防伪号生成商品身份整合码;最后对比由商品防伪号生成的和商品身份码所整合而成的商品身份整合码是否一致,如查询不一致,则返回信息“该商品为假货,请谨慎购买!”,如查询一致,则进入下一步,同时将此次查询的相关信息记录入数据库.

步骤 3,根据查询输入的防伪码,进行验证码生成算法(即混沌密码加密算法的步骤 3)的运算,将生成的验证号和重复查询密码返回给消费者,消费者可根据验证提示,快速心算商品上的验证码和返回的验证号每一位相加是否为 9,从而校验商品的真伪.防伪码查询、双向验证算法流程图见图 3.

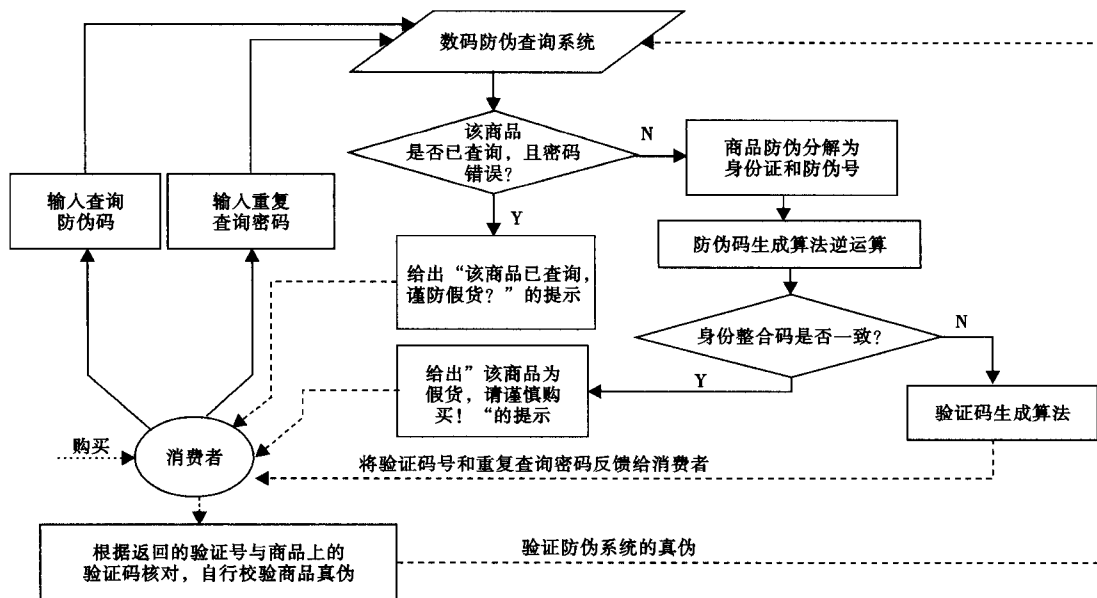


图3 防伪码查询、双向验证算法流程图

(2)算法性能测试

本文对算法的运算速度、防伪识别性能分别进行了如下测试:

笔者采集 10 000 组商品防伪码(防伪码正确率占 50%)进行混沌密码解密运算,返回“输入防伪码为假”提示或验证号平均耗时约为 3.75 ms,可见该算法的运算速率较高.

防伪识别性能是指在防伪码极其相似的情况下,系统正确识别防伪码真假的能力.笔者以商品身份码 43211105091234 为例,假设攻击者产生的防伪

码与正确防伪码仅存在某位差别,实验结果显示,只有在极个别的情况下,系统不能正确识别错误的防伪码,但由此生成的验证号与正确验证号截然不同,因此混沌密码解密时采用的“双向验证”机制保障了算法的防伪识别性能.

(3)算法封装

本文将混沌密码解密算法封装成函数,可方便地嵌入数码防伪系统中,使用非常简单.其中 $\text{char} * \text{fangwxc}(\text{char} * \text{fangwm})$ 表示对防伪码进行查询验证的函数,其中参数 fangwm 表示输入的防伪

码,函数根据解密通过与否返回验证号或者“输入防伪码为假”的字符串。

2.3.2 查询存储与数据返回

商品查询验证信息的数据库存储只有在消费者进行有效查询后方可进行,即当商品防伪码查询验证正确时,才会自动记录该商品的查询次数、此次查询时间以及其它相关查询信息。

返回给消费者的验证信息,是验证码生成算法所生成的验证号,而不是验证码,否则造假者极易回收二次利用造假,即使是商品的外包装已破损或防伪码与验证码已分离,造假者仍可利用查询返回的验证码造假,这样可以提高造假难度和造假成本;同

时为了兼顾消费者多次重复查询的需求,数码防伪查询系统随机生成重复查询密码,返回给消费者。

3 混沌数码防伪系统

3.1 系统概述

本文利用混沌数码防伪技术,构建了一套能进行现场认定又可通过电话、短信、网络(Internet、WAP)查询验证的全方位数码防伪系统,实现了混沌数码防伪的“双标双码”生成以及基于电话、短信、网络或现场识别仪的“双向验证”查询,具有很强的保密性和较高的查询便捷性、实时性,可进行多用户并发多次查询,系统框图见图 4。

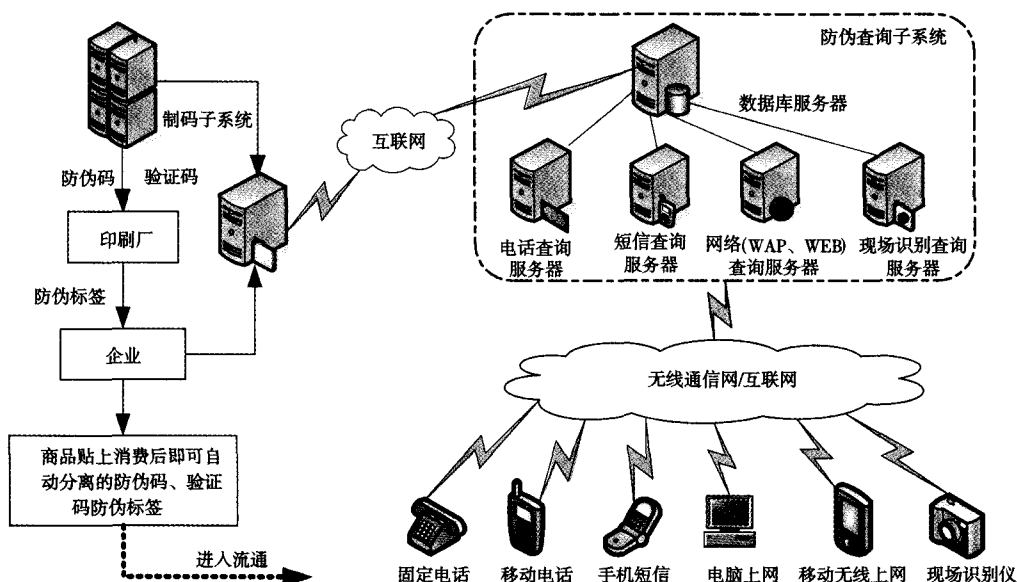


图 4 数码防伪系统框图

3.2 系统设计

系统基于混沌数码防伪技术,结合混沌数码防伪工作机制,采用 C# 编程语言,嵌入混沌密码加解密算法(即防伪码、验证码生成算法,以及防伪码查询、双向验证算法),构建了一套全方位数码防伪系统,其中包括一个基于 C/S 架构的制码子系统和一个基于 B/S 架构的防伪查询子系统。

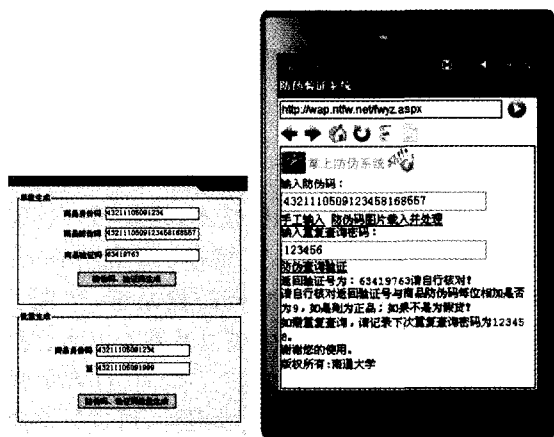
“制码子系统”界面可单组或批量生成防伪码和验证码,当单组生成时,输入“商品身份码”,点击“防伪码、验证码生成”按钮即可自动生成一组相应防伪码和验证码;当批量生成时,输入“商品身份码”的范围,点击“防伪码、验证码批量生成”按钮即可自动生成一批防伪码和验证码(系统界面见图 5)。该系统提供数据接口给印刷厂,用于防伪标签的制作。

消费者购买商品获得防伪码后,可通过现场识别仪进行商品现场真伪鉴别,也可根据防伪标签提

供的电话、短信号、网址,通过电话、短信、网络等多种查询方式查询。其中 WAP 网络查询系统界面见图 5,消费者可点击“手工输入”按钮后,直接在防伪码文本框中输入防伪码,也可点击“防伪码图片载入并处理”按钮后,防伪码文本框中直接显示防伪码图片处理后的防伪码信息;然后点击“防伪查询验证”按钮,系统自动调用混沌密码解密函数进行运算,在“提示信息”框中给出相应的验证信息。传统的数码防伪系统普遍采用消费者手工输入一长串防伪码的方式,操作费时且极易引起输入误差。该系统设计的防伪码输入方式兼顾手工输入和防伪码照片调用两种模式,消费者可将防伪码标签拍摄成照片进行存储,上网查询时可直接调用该照片,省却了手工输入的繁琐,同时提高了输入正确率。

3.3 系统测试

笔者对系统的防伪性能、抗攻击能力、防伪漏洞



(a) 制码子系统界面 (b) WAP 查询系统界面

图 5 数码防伪系统(WAP 查询)界面图

查堵等方面进行了测试,结果表明系统具有如下优点:

(1)利用混沌密码加密算法生成的防伪码和验证码,具有防伪安全度高、防伪效果好、不易破译和生产实时性等特点。

(2)采用“双标双码”,消费后其防伪码和验证码标签能实现自动分离,可堵住未破损、未查询包装物回收利用造假的防伪漏洞;采用“双向验证”,可堵住提供服务的数码防伪系统可能被假冒的防伪漏洞。

(3)在防伪标签上显性印刷商品身份码(条形码和数字),可在不破坏防伪码标签的情况下利用条形码扫描装置批量扫描商品身份码,便于开展大规模防伪普查,提高对销售商品的跟踪能力。

(4)生成的防伪码和验证码均不存储在防伪中心数据库中,查询时只依赖混沌密码解密算法进行辨别,便于数据的安全管理,可抵挡一定的木马攻击;而且商品的查询验证信息也不全部记录在数据库中,当且仅当在消费者进行有效查询后才自动记录该商品的查询信息,可有效节省数据库资源。

(5)支持消费者通过多种查询方式对某件商品多次查询,操作便捷,方便现场实时识别商品真伪,同时克服了现有数码防伪系统“一次查询、一次有效”的窘境。

由此可见,本文构建的数码系统防伪系统安全可行,而且操作简单,方便实用,适合推广。

4 结束语

本文引入混沌密码技术,研究提出并完善了混

沌数码防伪技术——以全新的思路和方法生成商品防伪码和验证码,研究提出了一种新型的防伪查询“双向验证”算法,形成了“双标双码、双向验证”防伪工作机制;同时应用所提混沌数码防伪技术,设计并实现了一套既可进行现场识别又可通过电话、短信、网络(Internet、WAP)查询验证的全方位数码防伪系统,方便有效地实现商品真假的鉴别。在今后的研究工作中,我们将结合多种最新技术(如二维码、RFID、Android 智能手机等),致力于研究更具实用价值的数码防伪技术并将其应用推广。

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] 张元梅, 朱桂云, 王同心. 数码信息防伪的方法 [P]. 中国专利: 101500018, 2009-08-05.
- [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] 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.
- [5] 杨艳华, 张志鹏, 马叶助. 基于 Internet 的数码防伪系统 [J]. 包装工程, 2003, 24(6): 19-21.
- [6] 盛苏英, 吴新华. 基于混沌的数码防伪系统研究与实现 [J]. 微电子学与计算机, 2011, 28(5): 63-66.
- [7] 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.
- [8] 姚建松, 杨胜利. 三级关联数码组合防伪方案在香烟防伪中的应用 [J]. 包装工程, 2007, 28(8): 85-86.
- [9] Kanso A. Cipher system based on controlled exact chaotic maps [J]. International Journal of Bifurcation and Chaos (Int. JBC), 2010, 20(12): 4039-4053.
- [10] Wang X Y, Wang X J. A new chaotic encryption algorithm based on the ergodicity of chaos [J]. International Journal of Modern Physics, 2011, 25(15): 2047-2053.
- [11] Reza M S, Mehdi D. Chaotic behavior and dynamics of maps used in a method of scrambling signals [J]. International Journal of Bifurcation and Chaos (Int. JBC), 2010, 20(12): 4097-4101.

作者简介:

盛苏英 女, (1979—), 硕士, 讲师. 研究方向为混沌密码技术、混沌保密通信。