

基于矩阵理论的动态防伪包装研究

赵亮

(郑州大学, 郑州 450001)

摘要: 主要阐述了可变图形在防伪包装设计中的应用。即采用计算机辅助生成技术,将若干独立的图形,经过矩阵加密排列运算,生成不重复的海量图形组合,能够通过无版印刷制作出防伪标签,并可通过短信及网站查询。对打击假冒伪劣产品,保护企业、国家和消费者的利益,具有重要的意义。

关键词: 可变图形; 防伪; 矩阵

中图分类号: TB482; TB488 **文献标识码:** A **文章编号:** 1001-3563(2011)09-0047-04

Research of Dynamic Anti-counterfeit Packaging Based on the Matrix Theory

ZHAO Liang

(Zhengzhou University, Zhengzhou 450001, China)

Abstract: The application of changeable picture in anti-counterfeit packaging design was introduced. This method created a large number of different picture-combinations from several individual pictures by using computer-assisted generation technology and the operations of matrix encrypt permutation. Anti-counterfeit labels were produced by plateless printing and the labels can also be checked by mobile phone message and website.

Key words: changeable pictures; anti-counterfeit; matrix

愈演愈烈的假冒伪劣现象对企业、国家和社会造成了极大的危害。在这一背景下,信用体系不完善已成为制约我国经济持续快速健康发展的主要瓶颈。假冒伪劣是当前我国市场信用体系建设中较为突出的问题,也是影响比较恶劣的问题^[1]。基于这一形势,为了保护企业、国家和消费者的利益,防伪技术尤其是防伪印刷得到了广泛的应用。

目前随着科学技术的不断发展,催生了一大批高科技的防伪手段,诸如激光防伪、荧光防伪、磁性防伪、变温防伪及特种制版等各种平面标识防伪技术,但这些防伪方法在应用过程中要受到许多限制,有的需要学习专业的鉴别知识才能鉴别(如激光防伪),有的需要专门的仪器工具进行鉴别(如荧光防伪),导致了绝大多数消费者在购买商品时因为受现场鉴别条件的限制,难以对商品的真伪进行有效地鉴别^[2]。另外,上述2种防伪技术都很难提供市场信息反馈、物流管理等服务,因此,对于可变数据印刷的防伪技术开始被越来越多的人所关注。

传统印刷方式虽然速度快,但一次只能印刷若干数量、内容固定的印刷品,不能满足目前商品个性化包装发展的需求。而可变数据印刷,采用固定基础图形与海量数字组合变换技术,即按照一定的算法,每次从基础图形中选定若干个不重复的图形,经组合后生成一个组合图形,在高速计算机的运算下,将组合后的图形编码、排版,这样每个页面、每个组合图形都不相同,使得从第一张到最后一张印刷品都具有不同的图像,每张印刷品都可以针对其特定的发放对象而设计并印刷。如果造假者想仿制,也只能仿制其中的一个标签,成本极高,关键是不知道全部的基础图形和算法,所以从理论上可以认为这种技术是无法批量仿制的。在以上过程中,基础图形和算法都可以随商品的不同而改变,但要做到这一点,就必须使用计算机生成大量的接口文件,提供给大型数码印刷机进行印刷,这个接口文件的特点是:采用程序编程自动生成,以避免手工操作;文件数量多、容量大,比如制作100万个标签所生成的接口文件可达300GB^[3]。

收稿日期: 2011-03-05

基金项目: 河南省重点科技攻关项目(102102210074)

作者简介: 赵亮(1961—),男,河南人,郑州大学副教授,主要研究方向为电子商务及企业信息化。

目前国内外还无法解决海量图形组合、变换处理、生成、无版印刷等技术难题,使得该理念尚未应用到企业实际中。从防伪的角度出发,为避免编码在短时间内被破解,综合考虑目前常用的几种算法,笔者决定采用基于矩阵变换理论的算法,这种算法打破了字符间的对应关系,极大地增加了破译密码的工作量,保障了数据的安全。

1 系统结构

该系统具备的功能主要包括:制码系统、网站查询系统和短信平台查询系统,见图 1。其中制码系统将生

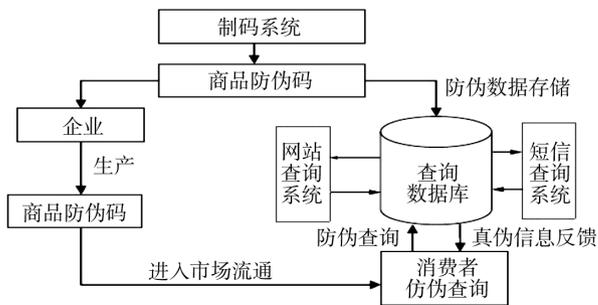


图 1 系统结构

Fig. 1 System structure drawing

成的海量数据存放在数据库中,同时将数据通过 VC 程序转化为 PDF 文件提供给企业进行批量生产;网站查询系统兼具文件生成与防伪查询功能,方便客户验证商品真伪以及了解和使用本系统;短信查询系统则是通过向短信平台发送验证码得到商品真伪的验证。

2 系统实现

2.1 防伪码加解密技术^[4]

基于矩阵理论的动态防伪系统的核心在于制码系统,而制码系统的核心又在于对验证码的加解密。这里主要使用基于逆矩阵的加密算法:采用密钥对验证码进行加密处理,得到加密信息,是验证码加密的基本方法,由于破解者不知加密所用的具体密钥及加密算法,因而在一定时期内无法知道信息内容,信息的接收方则可通过解密算法迅速译出密文验证真伪。所采用的密钥一般是一个矩阵,所要加密的数据为 k 个数,每一个位均为十进制数,将这 k 个十进制数转变为 $m \times n$ 的矩阵,与密钥相乘后得到的数据展开

后即为生成的验证码。作为查询码一般都是 10 位以上的十进制数字,如太短则不能适应大批量的生产需要,太长则查询输入不便。对于企业生产的产品,年产量按照 10 亿计算,需要用 $0 \sim 999999999$ 来描述,可用有序数列 $A_1 A_2 A_3 A_4 A_5 A_6 A_7 A_8 A_9$ 来表示,其中的任何一位在 $0 \sim 9$ 之间,转成矩阵的形式为:

$$\begin{bmatrix} A_1 & A_2 & A_3 \\ A_4 & A_5 & A_6 \\ A_7 & A_8 & A_9 \end{bmatrix}$$

将上面的矩阵与密钥矩阵 K 相乘,可得到加密后的矩阵 M :

$$\begin{bmatrix} A_1 & A_2 & A_3 \\ A_4 & A_5 & A_6 \\ A_7 & A_8 & A_9 \end{bmatrix} \cdot \begin{bmatrix} K_1 & K_2 & K_3 \\ K_4 & K_5 & K_6 \\ K_7 & K_8 & K_9 \end{bmatrix} = \begin{bmatrix} M_1 & M_2 & M_3 \\ M_4 & M_5 & M_6 \\ M_7 & M_8 & M_9 \end{bmatrix}$$

通过上面的运算,得到加密后的矩阵 M ,由于 M_i 可能是一个 2 位数, $M_i < 10$,可在前面补 0,再将矩阵 M 展开后得到 18 位的查询码。用户输入查询码,系统对查询码进行求逆运算,即:

$$\begin{bmatrix} M_1 & M_2 & M_3 \\ M_4 & M_5 & M_6 \\ M_7 & M_8 & M_9 \end{bmatrix} \cdot \begin{bmatrix} K_1 & K_2 & K_3 \\ K_4 & K_5 & K_6 \\ K_7 & K_8 & K_9 \end{bmatrix}^{-1} = \begin{bmatrix} A_1 & A_2 & A_3 \\ A_4 & A_5 & A_6 \\ A_7 & A_8 & A_9 \end{bmatrix}$$

再对 $A_1 A_2 A_3 A_4 A_5 A_6 A_7 A_8 A_9$ 进行验证,将结果反馈给查询者。

采用以上方法进行验证码的加解密时,恢复明文的关键是矩阵的求逆。为了增加破解难度,可将密钥矩阵按某种方式进行循环变换,即 $K_1 K_2 K_3 K_4 K_5 K_6 K_7 K_8 K_9$ 的排列顺序是根据查询码而变化的,那么随着 k 和密钥矩阵位数的增加,在一段时期内明文数据是相当困难的,另外也可以对有序数列 $A_1 A_2 A_3 A_4 A_5 A_6 A_7 A_8 A_9$ 适当顺序组合及变换,以增加破解难度,所以此办法对于验证码的保密具有很好的可靠性。

2.2 防伪码的生成与验证以及需要解决的问题

1) 研究平台:采用 VC 软件设计。

首先,VC 软件界面简洁,占用资源少,操作方便,

大多数大型软件都是用 C 或 C++ 编的,所以可利用源代码多;其次,VC 的开发工具特别多,从控件公司到硬件开发商,其产品很少不提供 VC 接口的,例如 Photoshop,就有 VC 的编程接口;最后,其运行速度比 VB, JAVA 等要快很多,适合组织大工程。

2) 研究组合图形的输出接口,特别是文字与图形的大小、位置、层次等关系。

3) 在加密算法研究方面,采用矩阵变换理论。

综合考虑目前常用的几种算法,决定采用类似于希尔密码的基于矩阵变换理论的算法,代替密码与移位密码的一个致命弱点是明文字符和密文字符有相同的使用频率,破译者可从统计出来的字符频率中找到规律,进而找出破译的突破口。要克服这一缺陷,提高保密程度,就必须改变字符间的一一对应。利用线性代数中的矩阵运算,打破了字符间的对应关系,极大地增加了破译密码的工作量,保障了数据的安全。

4) 成果以 PDF 形式实现。

PDF 是跨平台的通用格式,经过压缩它的数据量很小,但仍能提供图像要素,每一个页面都独立包含自身的全部图文信息,可极大提高计算机处理文件的速度和 RIP 的速度。PDF 具有完全独立性,无需启动原程序,也无需专门的软件就能使用,并且对任何特定打印机都适用。目前,PDF 已广泛用在印前处理中,大多数印前系统提供商都提出了基于 PDF 的工作流程解决方案。此外,PDF 还适合任何显示分辨率,放大观看不会明显失真,其限定文本的读、写和修改权限的特点,可以一定程度上保护知识产权。

5) 关于 PDFlib。

PDFlib 是一个帮助生成符合 Adobe 的可移植文档格式(PDF)文件的中间件。PDFlib 充当用户自己程序的后端。当应用程序员负责抽取要处理的数据时,PDFlib 承担生成 PDF 输出(图解数据)的任务。PDFlib 让人无需再关注 PDF 的内部细节问题,并提供了各种方法来帮助设置输出的格式。PDFlib 方法具有下面几个优点:PDFlib 可被直接集成到生成数据的应用程序中;PDFlib 是生成 PDF 的最快方法,完全适用于 Web;PDFlib 的多线程安全及其可靠的内存和错误处理,可支持实现高性能的服务器应用程序;PDFlib 可用于多种操作系统和开发环境。

采用计算机辅助生成技术,主要是在 VC6.0 平台上加载 PDFlib 库文件,就能够按照 Adobe 的可移植文档格式生成 PDF 文件。在 Visual C 6.0 下编制

一定的 PDF 文档程序,再结合数据库,将若干独立的图形,经过矩阵加密排列运算,生成不重复的海量图形组合,实现对商品包装特别是标签的大批量定制,使得每件商品的包装均不相同,能够有效地提高商品的防伪性能,用户可以通过短信系统或网站系统进行商品真伪的验证查询。

2.3 系统的实现过程

2.3.1 设计基础图形

对于 N 个基础图形,从中抽取采用 6 个不同的图形组合进行变换,可以有 $V=N(N-1)(N-2)(N-3)(N-4)(N-5)$ 个不同的组合,如果 $N=50$,则 $V=114$ 亿,完全满足一般企业 5 年的生产量。如果更换基础图形或者从中抽取 8 个不同的图形,则理论上可以生成几乎无限的图形组合。由于是每件商品一个标签,数据量很大,因此每个基础图形的容量就受到限制,一般要求大小为 100×100 ,并且不超过 20 kB 的 PNG 格式图片。

2.3.2 建立图形与原始数据的对应关系

将基础图形进行编码,生成 01, 02, 03, ... N 的编号,根据不重复的原则,遍历基础图形的排列组合,与自然数排列的顺序一一对应,形成对应关系,保存在数据库中,见表 1。

表 1 数据对应关系

Tab. 1 The corresponding relationship of data

自然数序列	图形组合
123157012	010203040506
123157013	010203040507
123157014	010203040508
...	...

2.3.3 生成查询码与解析过程

按照前面介绍的方法,将自然数序列 123157012 变换为矩阵:

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 5 & 7 \\ 0 & 1 & 2 \end{bmatrix}$$

该矩阵与矩阵 $\begin{bmatrix} 1 & 1 & 2 \\ -1 & 2 & 0 \\ 1 & 1 & 3 \end{bmatrix}$ 相乘后得到矩阵:

$$\begin{bmatrix} 2 & 8 & 11 \\ 3 & 18 & 23 \\ 1 & 4 & 6 \end{bmatrix}。$$

将此矩阵中的数据提取出来,不足 2 位的前面补 0,顺序排列为 020811031823010406,即为生成的查询码。当用户进行查询时,系统将该查询码转换为矩阵

$$\begin{bmatrix} 2 & 8 & 11 \\ 3 & 18 & 23 \\ 1 & 4 & 6 \end{bmatrix}, \text{ 并与作为密钥的逆矩阵相乘,即:}$$

$$\begin{bmatrix} 2 & 8 & 11 \\ 3 & 18 & 23 \\ 1 & 4 & 6 \end{bmatrix} \begin{bmatrix} 2 & -1/3 & -4/3 \\ 1 & 1/3 & -2/3 \\ -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 5 & 7 \\ 0 & 1 & 2 \end{bmatrix}$$

将解析后的数据排列成 123157012 的形式,通过数据检索,即可判断商品的真伪。

3 结语

随着电子化、信息化社会的不断发展,动态防伪包装技术已经脱颖而出,代表了新时期商品防伪的发

(上接第 14 页)

受力稳定性。石头纸蜂窝纸板具有高耐破性更主要取决于它的主要材料——石头纸。石头纸是在石头的主要成分碳酸钙中加入高分子化合物(如聚乙烯等),通过挤出工艺加工,再经“纸状化”处理得到的。这种工艺使石头纸不仅在外观上与普通纸张相似,同时还兼具塑料和纸张的功能特征。其蜂窝纸板耐破性能与其抗张强度呈正相关性。抗张强度高的石头纸原纸必定使得石头纸蜂窝纸板的耐破性能高。在施加外力作用的情况下,石头纸蜂窝纸板可以沿其高分子链的分子取向方向延伸,分子间作用力将比原来大大增加,更耐撕裂,故在受相同的作用力的情况下,石头纸蜂窝纸板比传统类似纸板更能抵抗破坏而保持力学平衡。

3 结论

研究表明,石头纸蜂窝纸板的平压强度优于传统普通纸板,边压强度低于纤维纸板国家标准,耐戳穿强度符合纤维纸板国家标准,耐破坏性能突出。试验时石头纸蜂窝纸板受制作过程误差的影响,各样品的力学性能与结构参数也不尽相同,为此进行不同结构参数的力学性能试验,寻求合理的结构参数,探讨性能与结构参数之间的关系及刚度、强度预测,是石头纸蜂窝纸板需要解决的问题。

展趋势之一。通过讲解可变图形在防伪包装设计中的应用,即采用计算机辅助生成技术,将若干经过矩阵加密排列运算的独立图形生成不重复的海量图形组合,阐述了新的防伪技术对打击假冒伪劣产品、保护企业、国家和消费者的利益的重要意义。

参考文献:

- [1] 甘光伟. 数码防伪技术[M]. 北京: 中国标准出版社, 2002.
- [2] 李清扬. 防伪原理及防伪技术的发展趋势[J]. 安防科技, 2003(4): 19-20.
- [3] 翟震, 曹国华. 基于 VC6.0 环境下的 PDF 文件生成技术[J]. 包装工程, 2010, 31(17): 111-113.
- [4] 焦留旺. 密码技术及密钥管理[J]. 焦作大学学报, 2001(9): 30-33.

参考文献:

- [1] 钱俊. 石头纸的特性及其应用分析[J]. 印刷技术, 2010(8): 38-39.
- [2] 覃炳达. “石头纸”相关专利技术概述[J]. 造纸信息, 2010(4): 9.
- [3] 伟洪. 新型环保石头纸[J]. 造纸化学品, 2010(3): 36.
- [4] 都学飞, 张伟. 瓦楞/蜂窝复合结构纸板强度性能的试验研究[J]. 包装工程, 2008, 29(8): 42.
- [5] 张改梅. 蜂窝纸板及纸板箱性能的研究[C]. 西安: 西安理工大学, 2001.
- [6] 崔立华, 朱婷婷, 黄俊彦. 蜂窝纸板生产工艺技术[M]. 北京: 印刷工业出版社, 2009.
- [7] 曹国荣, 邓江玉. 瓦楞纸板戳穿强度检测项目的分析和研究[J]. 农业机械学报, 2000, 31(6): 111-113.
- [8] THOMSEN O T, BANKS W M. An Improved Model for the Prediction of Intra-cell Buckling in CFRP Sandwich Panels under in Plane Compressive Loading[J]. Composite Structures, 2004, 65: 259-2681.
- [9] CHUNG J, WAAS A M. Compressive Response of Circular Cell Polycarbonate Honeycombs under in Plane Biaxial Static and Dynamic Stresses-experiments[J]. Int J Impact Eng, 2002, 27: 729-54.
- [10] CHUNG J, WAAS A M. Compressive Response of Circular Cell Polycarbonate Honeycombs under in Plane Biaxial Static and Dynamic Loading—Part II: Simulations, Int J Impact Eng, 2002, 27: 1015-1047.