

基于加密 QR 二维码的商品包装防伪技术

解 龙¹, 杜艳平¹, 程明智¹, 杨义先², 李 璟³

(1. 北京印刷学院, 北京 102600; 2. 北京邮电大学, 北京 100086;
3. 中国电信集团卫星通信有限公司, 北京 100191)

摘要: 为了改善大众商品包装的防伪效果, 采用了基于唯一商品编码生成加密 QR 二维码的商品包装防伪技术。基于非对称加密密钥生成算法产生公私钥密钥对, 利用私钥对唯一商品编码及商品名称等信息进行加密处理, 针对加密后的密文信息形成 QR 二维码。公钥被植入到 QR 二维码识读软件中, 作为解密密钥用来还原二维码信息。在应用中, QR 二维码以“一品一码”的方式粘贴或采用数字印刷方式喷印到对应商品的包装盒上, 智能手机终端通过运行加密 QR 二维码识读软件, 实现对加密 QR 二维码识读的功能。

关键词: 包装防伪; QR 二维码; 商品编码; 非对称加密
中图分类号: TS853+.5; TS851+.6; TS896 **文献标志码:** A
文章编号: 1004-8626(2013)04-0016-05

Packaging of Goods Anti-counterfeiting Technology Research Based on Encrypted QR Code

XIE Long¹, DU Yanping¹, CHENG Mingzhi¹,
YANG Yixian², LI Jing³

(1. Beijing Institute of Graphic Communication, Beijing 102600, China; 2. Beijing University of Posts and Telecommunications, Beijing 100086, China; 3. China Telecom Satellite Communications Limited, Beijing 100191, China)

Abstract: In order to improve the effect of the public anti-counterfeit packaging of goods, encrypted QR two-dimensional code is used in the packaging of goods anti-counterfeiting technology based on a unique commodity code. It generates public key and private key based on asymmetric encryption key generation algorithm, encrypted the information of the commodity, such as the unique commodity code, commodity name and other information, with the private key and then generate QR two-dimensional code. The public key is implanted into the QR two-dimensional code reading software, and as the decryption key, it is used to restore the QR two-dimensional code. In the

application, QR two-dimensional code paste or spray based on digital printing way to the correspondence product packaging as “one product one code”, smart mobile terminals by running the encrypted QR two-dimensional code reading software, enables commodity QR two-dimensional code encryption read.

Key words: anti-counterfeit packaging of goods; QR two-dimensional code; commodity code; asymmetric encryption

商品包装防伪一直是生产厂商生产商品考虑的主要问题, 如何对商品进行防伪也是学术界研究的重点。二维码用某种特定的几何图形按一定规律在平面(二维方向)分布的图形上记录数据符号信息, 能够以隐含方式存放被防伪对象的信息进行防伪; 二维码的制作成本较低, 不会增加可变数据印刷的额外成本, 研究利用其在可变数据印刷领域实现防伪有一定的意义^[1-2]。

针对商品生产及包装的特殊性, 本文结合现有的防伪技术, 利用二维码容纳信息多、并可快速识别的特点^[3] 结合加密技术, 形成了一种可用于商品防伪, 并且能大量生产的防伪技术。在不增加生产成本的前提下, 使用本方案能提高防伪效果, 且不影响商品的美观。

1 包装防伪应用现状

目前, 防伪包装应用有多种方式, 但从防伪成本低、仿造成本高和真伪检测方便等方面看, 各自都有不足。基于特殊材料的防伪油墨、激光全息类防伪、热敏材料防伪一般防伪成本较高, 而且存在环境污染的问题, 并且这类防伪技术的防伪策略不易公开, 因为一旦公开, 则为仿造者提供了仿造思路, 然而, 在大众商品防伪包装中, 防伪策略必须公开, 而且必须易于用户进行真伪检测, 这就存在一对矛盾。这类防伪包装方式从防伪成本角度来说也不适用^[4]。微缩文字印刷、开锁、安全线等基于版纹的防伪技术的防伪方式主要存在两个问题: 第

收稿日期: 2013-05-06

基金项目: 北京市教委面上项目 (KM201210015006, KM201210015007); 北京市自然科学基金资助项目 (4122026); 北京市自然科学基金重点项目 (KZ201210015015); 北京市本科生物科研项目 (08150113026)

一,版纹都是以模版方式批量制作,防伪信息无法与包装商品个性化关联,仿造成本较低^[5];第二,微缩文字印刷还存在检测不方便的缺点。基于信息化技术的防伪技术有电话电码防伪、短信防伪或者通过条形码、RFID 与后台计算机系统相结合,这类防伪方式的优点是能够做到与包装产品的一一对应,个性化防伪^[6],缺点是检测不方便,即每次真伪检测时需要通过短信或者网络访问等方式与后台系统进行交互^[7]。各种防伪技术综合使用的综合防伪方式(如人民币的防伪)提升了仿造难度,防伪效果虽好,但防伪成本大大提高。

2 包装防伪技术方案

本文论述了一种基于非对称加密技术和二维码防伪技术进行包装防伪应用的方案^[8]。本方案的信息非对称加密处理的对象是商品编码。将商品编码加密处理后,印刷成相应的 QR 二维码图标并粘贴在对应产品的包装盒上,随商品一起流通;当商品消费者购买商品后,可以利用终端设备(如安装有专用二维码识读软件智能手机)对 QR 二维码图标进行识读,从而检测出包装商品的真伪。

本技术可应用于大众商品的包装防伪,比如白酒、香烟、化妆品等。

2.1 系统部署及软件模块说明

本方案在实际应用时,需要商品生产厂家创建一个 Web 系统,供智能手机用户下载专用二维码识读软件,还需要开发一个后台软件系统,添置一套喷墨印刷设备。

在商品出厂前,后台软件系统根据每件商品的商品编码信息批量生成 QR 二维码图标,然后发送给喷墨印刷设备,由喷墨印刷设备在每个包装盒上喷印相应的二维码图标以及对应的商品编码。

智能手机登录 Web 系统下载与自己手机操作系统对应的专用二维码识读软件^[9]。在商品流通过程中,消费者利用安装有专用二维码识读软件的智能手机摄像头获取包装盒上的二维码图标。专用二维码识读软件能够准确识读出该二维码图标所包含的商品编码信息,这样,消费者就可以人工比对识读出来的商品编码信息与喷印在包装盒上的商品编码信息,如果一致,则表示商品为真品;否则,说明该商品为仿制品。本方案在实际应用时的系统部署如图 1 所示。

系统中的喷墨印刷设备可以是通用的任何喷墨印刷设备;消费者所使用的智能手机可以是具有

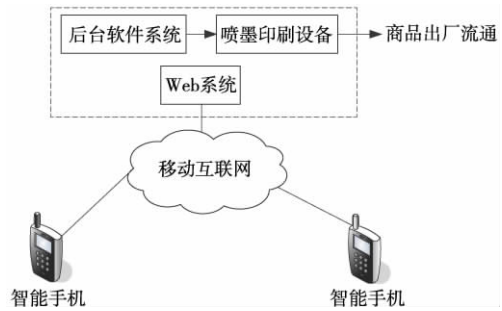


图 1 商品 QR 包装防伪系统总体架构图

摄像头功能的 Android 操作系统的手机。

后台软件系统主要部署个性化信息安全处理软件,该软件的核心模块包括信息录入模块、密钥对生成模块、信息加密模块、二维码生成模块以及喷墨印刷信息接口模块。各个模块结构及其相互间的关系如图 2 所示。

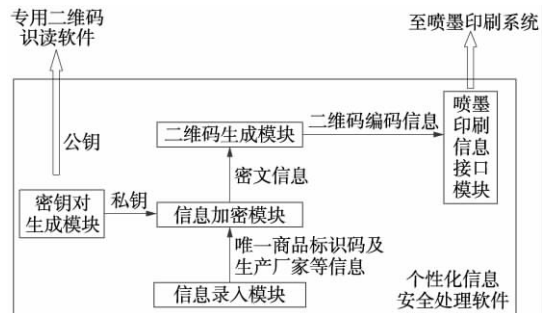


图 2 个性化信息安全处理软件模块结构图

信息录入模块: 商品出厂前,厂商会分配唯一商品编码给每件商品。信息录入模块接收这些唯一商品编码和其他信息(比如生产厂家信息、生产日期、产品型号)的批量导入,作为 QR 二维码生成的信息源。

密钥对生成模块: 根据各个唯一商品编码,密钥对生成模块按照随机方式批量生成与该唯一商品编码对应的公钥密码对,作为可变信息安全处理软件中信息编码加密模块的加密密钥,并且作为专用二维码识读软件中二维码信息解密模块的解密密钥。

信息编码加密模块: 针对信息录入模块接收到的可变信息,包括唯一商品编码、生产厂家信息、生产日期、产品型号等,利用密钥对生成模块生成的对应密钥,进行加密处理,输出密文信息。

二维码生成模块: 依据信息编码加密模块生成的密文信息,采用目前通用的二维码生成算法生成对应的二维码信息。

喷墨印刷信息接口模块: 本模块将二维码生成

模块所产生的二维码信息发送到喷墨印刷系统,本模块为可选模块,如果不用这个模块,则可以采用二维码信息文件手工导入的方式录入信息。

Web系统用于向智能手机用户提供专用二维码识读软件下载功能,专用二维码识读软件包括通用二维码图像识读模块和二维码信息解密模块。各个模块结构及其相互之间的关系如图3所示。

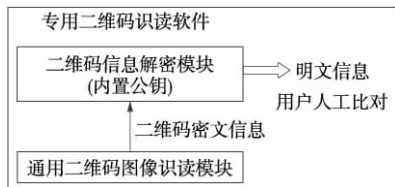


图3 专用二维码识读软件模块结构图

通用二维码图像识读模块:是通用模块,目前市面上已有相应的二维码图像识读软件,主要面向QR条形码、PDF417等不同的二维码码制所对应的图形进行识读。

二维码信息解密模块:由于采用本方案时,通用二维码图像识读模块所识读出来的信息还是密文信息,但是可以在密文信息的第一行得到专用二维码识读软件的下载网址,联网之后,便可到该网址下载专用二维码识读软件。本模块设计的目的主要是对通用二维码图像识读模块所识读出来的密文信息进行解密处理,而解密密钥的获取是本方案的创新点。

由于在印刷二维码时还会以明文方式在包装盒上喷印唯一商品编码,二维码信息解密模块在获得二维码明文信息后,就可以解析出二维码中包含的唯一商品编码的内容,用户通过人工方式比较解析出来的唯一商品编码与喷印的唯一商品编码是

否一致,以判断商品的真伪。

2.2 业务流程说明

本课题在包装防伪过程中的应用流程如图4所示。

实际应用过程中,涉及的业务流程包括专用二维码识读软件下载、个性化信息安全处理、二维码印刷、商品出厂流通以及真伪检测等5个环节。其中,专用二维码识读软件下载环节与其他几个环节没有先后次序关系;商品出厂流通环节是一个线下环节。具体描述如下:

1) 专用二维码识读软件下载。在Web系统上部署已经开发好的专用二维码识读软件,智能手机用户可通过公司网址获取下载网址,随时登录Web网站,选择并下载与所使用手机操作系统匹配的专用二维码识读软件。

2) 可变信息安全处理环节。在产品包装出厂前,针对每一件不同的产品,依据生产厂家、生产日期、产品批次等可选信息以及必须录入的唯一商品编码,由后台可变信息安全处理软件按照一定的编码、压缩、加密算法处理后,生成与该件商品对应的二维码编码信息。

这些二维码编码信息是密文方式,而且是可以作为喷墨印刷设备进行二维码喷印的数据源。由于是密文信息,所以喷印出来的二维码图像利用通用的二维码识读软件识读时,识读出来的是密文信息。

3) 二维码印刷环节。在得到每一件产品的二维码编码信息后,这些产品的二维码编码信息将经过喷墨信息接口模块或者手动复制的方式,成批地发送至喷墨印刷系统,由喷墨印刷设备在包装盒上进行二维码印刷。同时,将可变信息安全处理环节

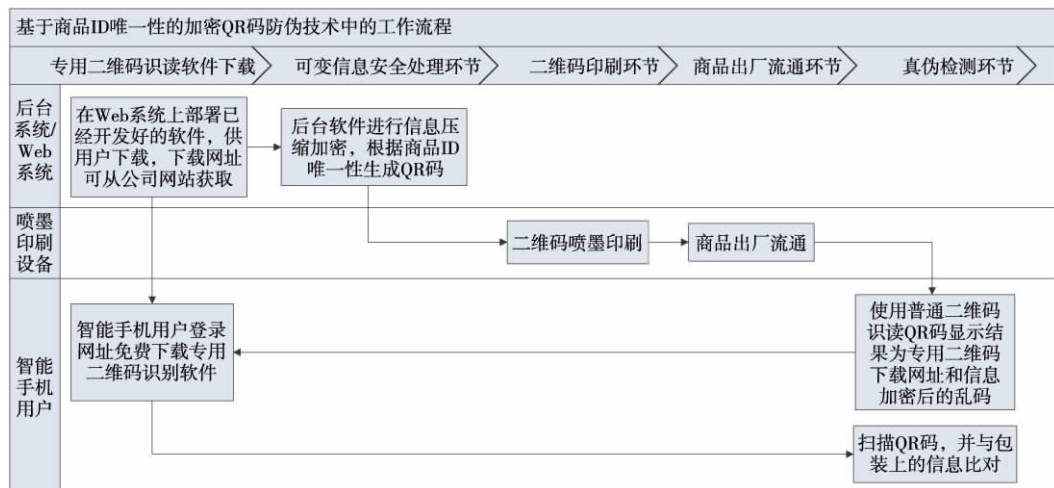


图4 商品QR包装防伪系统工作流程

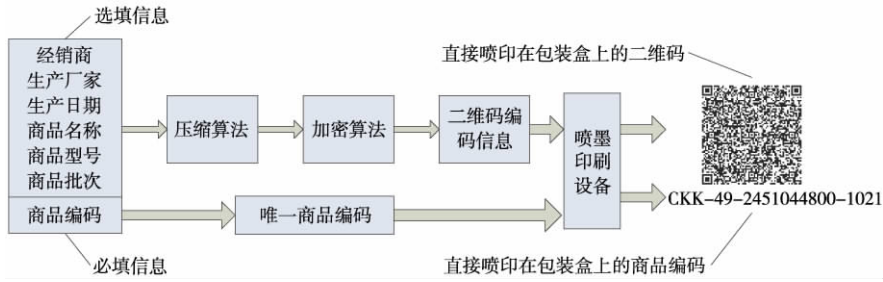


图 5 二维码图形生成的具体流程

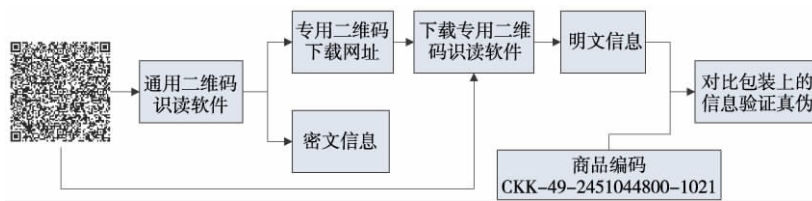


图 6 真伪检测流程

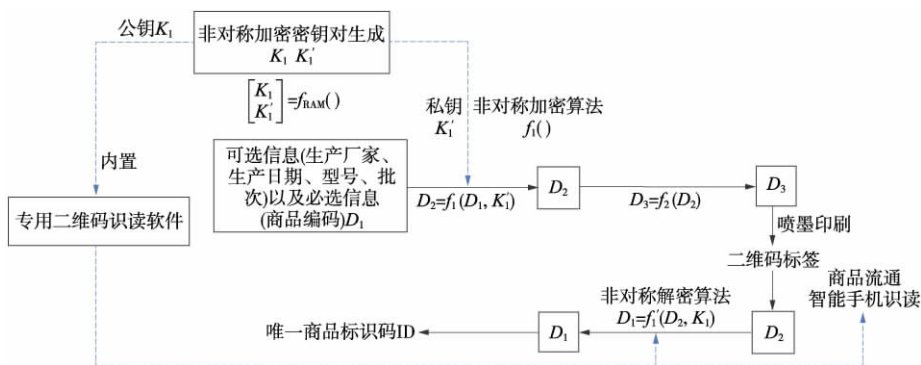


图 7 技术实现方法及原理

输入信息中的唯一商品编码也发送至喷墨印刷设备,由喷墨印刷设备以数字方式喷印在包装盒上,从而完成出厂流通。

从可变信息安全处理到二维码印刷环节的二维码图标生成的具体流程如图 5 所示。

4) 商品出厂流通环节。商品出厂流通环节为现有流通方式,属于线下操作环节,与本方案没有直接关联。

5) 真伪检测环节。智能手机用户在下载并安装了专用二维码识读软件后,可以随时识读所有包装盒上由本方案制作出来的二维码图标,并解析出相应的密文信息,用户可以看到其中唯一的商品编码。用户将识读出来的唯一商品编码与喷印在包装盒上的唯一商品编码进行对比,以判别真伪。具体实现流程图如图 6 所示。

3 算法原理

本方案在包装出厂环节,可以进行批量二维码

图标形成作业,这里以一件产品出厂时的二维码图标喷印以及真伪检测为例,对本方案的技术实现方法及原理进行描述,如图 7 所示。

个性化信息安全处理软件的密钥对生成模块根据公钥密钥体制对公、私密钥对的要求,随机生成密钥对 K_1 (公钥) 和 K_1' (私钥),数学表达式为 $\begin{bmatrix} K_1 \\ K_1' \end{bmatrix} = f_{RAM}()$,其中,密钥对随机生成算法 $f_{RAM}()$ 可以是通用的算法。

密钥对生成后,公钥 K_1 被植入专用二维码识读软件中,当手机用户下载该软件并对本方案生成的二维码进行识读时,公钥 K_1 将作为二维码编码信息的解密密钥进行解密处理;私钥 K_1' 作为个性化信息安全处理软件中信息加密模块的加密密钥。

D_1 为生产厂家信息、产品名称型号信息、生产厂家信息、生产日期信息等可选信息,以及与该产品对应的唯一商品编码这项必选信息。

信息加密模块从密钥对生成模块获得密钥对中的私钥 K_1' (基于公钥密钥体制,这里可任选 K_1 或者 K_1' 作为私钥),利用通用的非对称加密算法,比如 RSA 算法,对数据 D_1 进行加密处理,得到密文信息 D_2 ,数学表达式为: $D_2 = f_1(D_1, K_1')$ 。

密文信息 D_2 信息交给二维码生成模块,由二维码生成模块根据通用的二维码生成算法得到二维码编码信息 D_3 ,数学表达式为 $D_3 = f_2(D_2)$ 。

得到二维码编码信息后,就可以将该信息 D_3 以数据文件的方式发送给喷墨印刷设备,由喷墨印刷设备根据 D_3 在对应的包装盒上喷印出相应二维码标签,亦即二维码图标。

同时,唯一商品编码 ID 以数字喷印方式,被喷印在包装盒上,这时,该商品就可以进入市场进行流通。智能手机用户可以随时登录中心平台的 Web 系统,下载与本手机操作系统匹配的专用二维码识读软件。智能手机用户需要检测商品真伪时,只需要用手机摄像头拍摄喷印的二维码,由于本方案中二维码标签是由二维码编码信息 D_3 基于通用的二维码喷印方式印刷出来的,所以,智能手机用户拍摄商品二维码后,专用二维码识读软件中的通用二维码图像识读模块能够准确地识读出二维码标签喷印前对应的 D_2 数据,这时识读出来的 D_2 信息仍然是密文信息。

专用二维码识读软件获取数据 D_2 后,二维码信息解密模块利用已经内置的解密密钥 K_1 、与非对称加密算法 $f_1()$ 对应的非对称解密算法 $f_1'()$ 及数学表达式 $D_1 = f_1'(D_2, K_1)$ 进行解密。

由于 D_1 已经是明文信息,且其中包含唯一商品编码,因而二维码信息解密模块可以提取出唯一商品编码。

另外,由于唯一商品编码已经以数字方式喷印在包装盒上,手机用户可以通过人工比对的方式,实现商品的真伪判定:从专用二维码识读软件识读出来的唯一商品编码如果与包装盒上喷印的唯一

商品编码一致,则为真品;否则,可以判定其为仿制品。

4 结 论

本文通过介绍加密二维码的生成与识读,为防伪包装提供了一种新思路,通过生成加密的 QR 二维码来实现防伪。这种防伪二维码可进行批量生产,并能够以“一品一码”的方式实现与实际商品的一一对应,一个商品唯一编码对应一个防伪二维码。在经过信息录入处理后,生成防伪二维码。使用普通的二维码识读软件,识读出来的信息为专用的二维码软件下载网址和乱码,只有使用专用的二维码识读软件才能准确识读出商品信息。其中加密密钥的获取采用的是非对称加密密钥算法。通过对软件的操作,实现二维码的批量生成,是一项可以用于大众商品防伪包装的技术。

参考文献:

- [1] BALASU BRAMANIAN R. Optimization of the Spectral Neugebauer Model for Printer Characterization [J]. J Electron Imaging, 1999, 8(2): 156-166.
- [2] 肖菲菲,刘真. 二维码防伪技术在可变数据印刷中的应用 [J]. 包装工程, 2011, 32(21): 102-105.
- [3] 中国物品编码中心. QR Code 二维码 [S]. 北京: 中国标准出版社, 2001.
- [4] 安粒. 一种基于喷墨打印技术的变色材料的研究 [D]. 北京: 北京印刷学院, 2009: 5-14.
- [5] 阳郁. 版纹防伪技术在包装防伪中的应用 [J]. 中国包装工业, 2004(3): 41-42.
- [6] 张圳. 基于 RFID 的防伪关键技术研究 [D]. 成都: 电子科技大学, 2010: 15-80.
- [7] 李秀芝. 基于 RFID 标签的商品防伪技术研究 [D]. 洛阳: 河南科技大学, 2009: 25-28.
- [8] 廖东方. 二维码电子标签的安全技术研究 [D]. 北京: 北京邮电大学, 2008.
- [9] 王明振. QR 码在 Android 手机平台的解码算法研究 [D]. 郑州: 郑州大学, 2011.

(责任编辑: 邱林华)

2016 年全球包装工业年增长将达 8200 亿美元

史密瑟斯·皮拉(Smithers Pira)市场研究所的调查显示,全球包装的销售额自2010年开始每年将增长6700亿美元,预计到2016年,年增长将达8200亿美元。美国以1370亿美元的销售额成为全球最大的包装市场,中国以800亿美元紧随其后。

(来源: <http://www.keyin.cn/news/gngj/201308/08-1068835.shtml>)