基于伪指纹特征密钥的二维码加密算法研究

滕 旭

(云南大学 旅游文化学院,云南 丽江 674164)

摘 要:二维条码用于证件管理在国外已经十分常见,但由于二维码的编解码技术已经非常成熟,很容易被不法分子伪造。提出了利用伪指纹特征密钥加密二维条码的技术方案,实现了“人证同一性”问题,对基于二维码的证件管理具有重要的现实意义。

关键词:伪指纹特征;密钥;二维码;加密

中图分类号:TP309.1 **文献标识码**:A **文章编号**:1672-7800(2013)008-0135-03

0 引言

二维码以其成本低廉、编码范围广、信息容量大、容错纠错能力强等优点,在社会生活的许多领域得到了广泛的应用。二维码用于证件管理可以实现证件信息的自动识读,便于网络化管理,并有一定的防伪功能,在国外已经有了成熟的应用。但在应用中发现二维码防伪功能十分有限,并且不能满足证件管理中的“人证同一性”问题,基于此,本文将指纹技术与二维码加密技术结合提出了一种应用方案,以期增强二维码在证件管理中的防伪功能[1]。

1 伪指纹特征密钥

1.1 随机数发生器概述

在密码学中为了防止密钥被破译,密钥必须没有任何规律,基于此种要求提出了利用随机数作为密钥的方法。目前对随机数发生器的研究很多,提出了很多方案,但迄今为止我们不能证明一个数字序列为完全随机,只是它的规律很难发现而已。目前用于密钥的随机数发生器主要有美国联邦信息处理标准的 ANSI X9.17 和 FIPS186 等多种。随机数发生器虽然对密钥被破译的问题提供了支持,但随机数是由谁产生的没有给出认证的问题,而这一点在证件管理中具有非常重要的意义。伪指纹特征随机发生器可以解决这种认证问题。

1.2 伪指纹特征随机发生器

伪指纹特征随机发生器的组成技术包括:指纹特征数据采集技术、伪指纹特征随机发生器技术、伪随机指纹特征密钥技术,如图 1 所示。

图 1 伪指纹特征随机发生器解决方案

(1)指纹特征数据采集器的作用是通过采集指纹数

询,点击照片;②弹出对话框,选择好保存照片的文件夹,如,“E:\PETS照片\”,单击“保存”,弹出确定对话框。此时要特别注意,必须单击“否”,导出所有已读入系统的以身份证号码命名的照片文件(JPG格式)。

将照片文件改名为以准考证号命名(用 Excel 和 DOS 命令)。①新建 Excel 表格,打开先前保存的“考生报名报考数据.xls”,将 zkzh、sfzh 两列数据复制到 A 列和 B 列,在 C1 单元格输入“=CONCATENATE(A1,".jpg")”(注:最外层双引号不要输入,下同)。在 D1 单元格输入“=CONCATENATE(B1,".jpg")”,在 E1 单元格输入“=CONCATENATE("rename"," ",d1," ",c1)”,复选 C1、D1、E1 拖动 E1 右下方的“十字形”句柄应用到所有行,保存。选中 E 列,点击复制,在 E 盘 PETS 照片文件夹目录下,创建一个“照片文件改名.BAT”文件,将复制的内容粘贴进去;②打开 E 盘 PETS 照片文件夹,双击“照片文件改名.BAT”,这样,原来以考生身份证命名的照片文件全部改名为以考生准考证号命名的照片文件。

打开全国英语等级考试管理系统和考试管理系统主程序,依次单击“参数设置数据装入”、“参数设置”、“设置相片存放目录”,将指定相片文件存放至目录。

参考文献:

[1] 廖亚辉.METS水平考试和PETS考试的比较和对接[J].中南林业科技大学学报:社会科学版,2010(12).

[2] 涂晶晶.从英语类图书入类看《中国图书馆分类法》(第四版)“H31”类目修订[J].科技情报开发与经济,2011(8).

(责任编辑:余 晓)

作者简介:滕旭(1977—),男,硕士,云南大学旅游文化学院助教,研究方向为信息处理与信息安全。

据，并经过指纹模式识别系统算法将它转化为指纹特征数据。

(2)伪指纹特征随机发生器的作用是通过伪指纹特征随机发生器，产生伪随机指纹特征。

(3)伪随机指纹特征密钥可使伪随机指纹特征数据生成相关的加/解密密钥，并且通过该密钥可以认证伪随机指纹特征数据的身份，即该密钥是谁的指纹[2]。

1.3 伪指纹特征密钥生成方法

伪指纹特征密钥的生成步骤如下：首先采集指纹进行处理得到初始指纹特征信息，接着对该指纹特征信息设定参数进行一系列的平移和旋转，形成伪随机指纹特征，最后编码成为伪随机指纹特征数据值。具体实现过程如下：

(1)如图 2 所示，图中的 P 点是某一个指纹特征点，T 为平移向量，P′是平移后的点。即：P′=P+T

$$P=\begin{bmatrix}x\\y\end{bmatrix}\ P'=\begin{bmatrix}x'\\y'\end{bmatrix}\quad T=\begin{bmatrix}t_x\\t_y\end{bmatrix}\begin{cases}x'=x+t_x\\y'=y+t_y\end{cases}$$

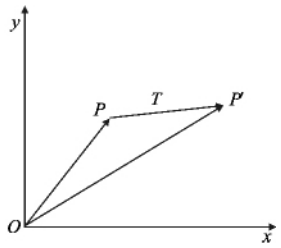

图 2 点的平移

(2)如图 3 所示，P 点是平移后的一点，P′是经过旋转后的一点，θ 是旋转的角度，R 是旋转矩阵。即 P′=R*P

$$R=\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}\quad\begin{cases}x'=x\cos\theta-y\sin\theta\\y'=x\sin\theta+y\cos\theta\end{cases}$$

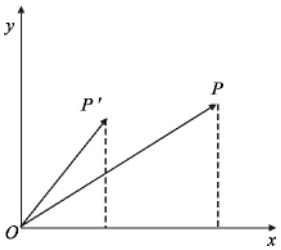

图 3 点的旋转

(3)如图 4 所示，P1 和 P0 经过平移旋转后的指纹特征点，P1′、P0′是 P1 和 P0 经过缩放后的点，其中 S 为缩放矩阵。为简化计算，SX 和 SY 一般取值相同。

$$\begin{cases}x'=S_x x\\y'=S_y y\end{cases}\quad P=S*P\quad S=\begin{bmatrix}S_x & 0\\0 & S_x\end{bmatrix}$$

(4)将得到的每个点的坐标拼接起来，产生一个伪指纹特征随机数。

通过上述处理，我们并没有改变指纹拓补结构，将变化前的指纹特征与变化后的指纹特征作指纹比对运算，结果是判定两指纹相同。由此伪指纹特征随机数不仅表示了一个人的身份特征，而且具有随机不确定性。若将其用作密钥，则既可表示该密码的人的身份，又难以破译。经过上述过程产生的随机数值序列一般都太大(有 256 个字节)，可以再利用哈希函数散列工具，将生成的伪指纹特征值散列成较小的随机数[3]。

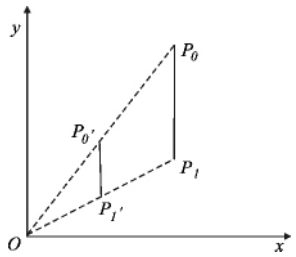

图 4 特征拓补结构缩放

生成伪指纹特征密钥的程序如图 5 所示。该程序取自《Visual C++指纹模式识别系统算法及实现》中源程序。可以用于产生伪指纹特征密钥对二维码进行加密解密。

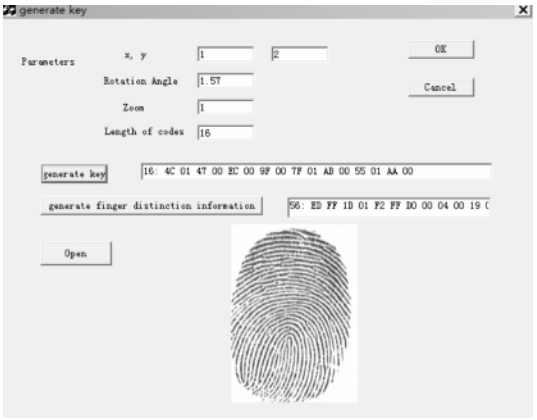

图 5 指纹密钥的生成程序

2 二维码加密方案研究

生成二维码及使用的正常流程如图 6 所示。

图 6 二维码正常使用流程

通过上面的流程，可以在不同的环节对二维条码加密和解密形成不同的解决方案，各种方案如下。

方案一：本方案是对信源先加密，再进行编码，对二维条码解码后得到的是信息密文，只有通过解密程序才能识读，如图 7 所示。

图 7 二维码加密方案一

方案二：本方案是对信源先编码，编码后对码字进行加密。为了避免码字加密对纠错的影响，我们只能在纠错码生成前对数据码字进行加密，如图 8 所示。

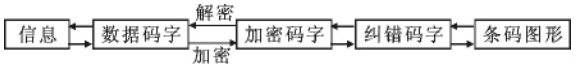

图 8 二维码加密方案二

除此之外还可在生成二维码图形时，对码图进行随机

加密,属高级加密,条码要通过高速解码芯片才能解密。对二维码进行加密时还可同时采用上面的方案形成更多混合方案。由于二维码识读器已经商业化,任何符合国家标准的二维码都可利用二维识读器直接解码得到信息,因此对一般用户来说,应该采用第一种加密方案。第二种方案对二维码设备开发商在扩充其设备功能时使用。本文选择第一种方案,利用伪指纹特征密钥将信息加密,改善二维码的防伪功能[4]。

3　伪指纹特征密钥加密证件信息的意义和流程

在证件管理中我们将证件信息存储在二维码中,将二维码打印在证件上实现证件信息的自动化读取,但没有证件的防伪功能。在对称密钥体制中,收发双方必须共享密钥,这就涉及到密钥的保存与传递问题,攻击者通常在密钥的保存传递环节中窃取密钥对密码体制进行攻击,伪指纹特征密钥可以有效防止这种攻击。我们用持证人的伪指纹特征密钥对证件信息加密后存储在二维码中,就可以使证件伪造者改动证件信息的同时不能相应改动二维码内存储的内容而被识破。在证件信息的读取过程中,只有持证人本人通过其指纹特征密钥才能解密证件信息,防止证件被冒名使用[5]。

伪指纹特征密钥加密解密流程如图 9 所示(其中 X 表示信息明文,Y 表示信息密文)。

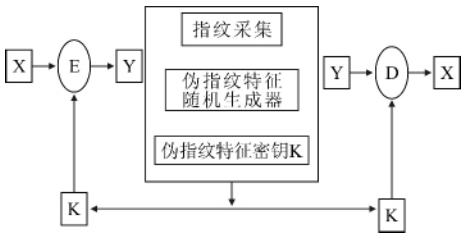

图 9　伪指纹特征密钥加密解密流程

4　结语

二维码技术用于证件管理,易于被复制和伪造,给应用带来了许多负面影响。本文对二维码加密技术做了大胆的尝试,利用伪指纹特征密钥将二维码进行加密,有效地解决了证件的防伪和认证问题。

参考文献:

[1] 刘洁,徐维维.二维条码证件管理与防伪技术综述[J].福建电脑,2009(7).

[2] 华龙.基于 CA 伪随机指纹特征密钥认证的 PKI 技术与实现[J].天津职业院校联合学报,2012(8).

[3] 李昊,傅曦.Visual C++指纹模式识别系统算法及实现[M].北京:人民邮电出版社,2008.

[4] 方媛,傅华明,张英姿.基于加密二维条码和指纹识别的证件防伪系统[J].计算机与数字工程,2009(1).

[5] 杨娱.基于指纹密钥的混合加密技术研究[D].兰州:兰州交通大学,2010.

(责任编辑:杜能钢)

Research of Encryption Algorithm of Two-Dimensional Code Based on Pseudo Fingerprint Feature

Abstract: In other countries, two-dimensional code has been common for document management, but because its encoding technology is mature, criminals can be forged. Using pseudo fingerprint key feature encryption of two-dimensional code technology program, achieves a" witness identity" issue, and has an important significance for document management base on two-dimensional code.

Key Words: Pseudo Fingerprint feature; Key; Two-Dimensional Code; Encryption