DOI:10.16083/j.cnki.jeijp.2012.03.065

基于 QR 二维码的高校身份验证系统的研究

于　彤

(秦皇岛职业技术学院 信息工程系，河北 秦皇岛 066100)

摘要: QR 二维码是一种全新的信息存储、识别和传递的技术,拥有很多优点,并且在不同领域中应用广泛。本文首先阐述了 QR 二维码的基本知识,然后根据高校中对学生身份验证的需求,设计并实现了一个基于 QR 二维码的高校身份验证系统。

关键词: QR 二维码; 身份验证,RSA 算法

中图分类号: G647　　**文献标识码:** A　　**文章编号:** 1671—1580(2012)03—0111—03

1. 引言

在高校中,为了满足高校的各项管理,便出现了多种证件,如: 学生证、准考证、借书证等。但是在使用与验证时很不方便,而且比较容易伪造。随着各种信息化技术的进步,手机 3G 网络、WIFI 网络的普及,特别是一种新的信息处理方式——二维码的出现,便可以解决这一问题,实现一码多用,在多种场合可以作为电子身份证,便于携带与验证,并且相对于虹膜识别验证、指纹识别验证等技术,其实现成本低且更快捷高效。

2. QR 二维码

1994 年,日本 Denso 公司研制出了 QR Code (Quick Response Code,快速响应矩阵码) (其图形如图 1 所示),它是目前最具有代表性的二维码之一。它除具有信息容量大、可靠性高、可表示汉字及图像多种信息、保密防伪性强的特点之外,还具有如下主要特点:

(1) 高速识读

QR 码是通过 QR 码符号的位置探测图形来识读 QR 码符号中的信息。因此,信息识读过程所需时间很短。

(2) 全方位识读

QR 码具有全方位(360 度) 识读的特点,该特点有效地解决了因扫描倾斜而造成识别困难的问题。

(3) 能够有效地表示汉字

QR 码采用特定的数据压缩模式表示汉字,仅用 13 bit 表示一个汉字,而其他二维码则需用 16bit,因此,QR 码比其它的二维码表示汉字的效率提高了 20%。

(4) 高数据容量

QR 码最多可容纳数字字符 7089 个,字母数字字符 4296 个,汉字 1817 个。

(5) 强大的纠错能力

QR 码有 4 种纠错等级,分别为 L 级、M 级、Q 级和 H 级。可恢复的数据码字分别约为 7%、15%、25% 和 30%。该特性能够有效地去除噪声的干扰,达到准确识别的目的。

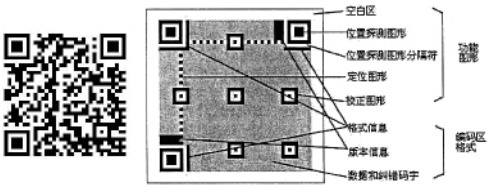

图 1 QR 码的图形　　图 2 QR 码的图形结构

2.1 QR 码的图形结构

每个 QR 码图形都是由若干个正方形模块组成的一个正方形阵列。这个正方形阵列包括功能图形区域和编码区区域两部分。功能图形区域是用于符号定位与特征识别的特定图形,不用于数据编码。编码区则是用来保存数据的区域。QR 码的图形结构如图 2 所示。

2.2 QR 码的编码和解码

收稿日期: 2012—01—16

作者简介: 于　彤(1981—),男,辽宁营口人,秦皇岛职业技术学院,助教,硕士,研究方向: 软件工程、数据库技术及其应用。

QR 码的编码包括数据编码和纠错编码两部分。其中，数据编码分为扩充解释 ECI 模式、数字模式、字母数字模式和 8 位字节模式等。纠错编码采用有限域 GF(28) 上的 RS(Reed－Solomon) 纠错编码算法。

QR 码的解码的基本流程如下:

(1) 识别格式。提取格式、版本信息，识别纠错等级和掩模图形。

(2) 去除掩模。用掩模图形对 QR 码阵列中的编码区域进行处理。

(3) 信息提取。从 QR 码阵列中，根据数据模板的排列方式，将 0、1 数据提取出来，得到相应的数据码字流和纠错码字流。

(4) RS 纠错。使用与纠错等级相对应的纠错码检测错误并纠正错误。

(5) 数据解码。按照使用的模式对纠错后的数据进行解码，并输出结果。

3. 系统的设计与实现

3.1 系统的功能需求

(1) QR 码作为学生证

学生证是学生在校期间的唯一身份凭证。一般的学生证上都会有学生的学号、姓名、系部、班级、照片等信息。但是在高度信息化、网络化、数字化的时代，使用电子证件是一种必然的趋势。

(2) QR 码作为准考证

使用 QR 码可以在生成二维码之前对学生的考试信息进行加密，在学生进入考场时通过专用的识别设备读取该二维码，核对相应的信息。

(3) QR 码作为考勤凭证

高校中的课程包括必修课和选修课，并且很多课程都是合班上课，采用传统的考勤方式很费时间且不一定能真实反映出学生的出勤情况，因此，可以采用 QR 码的方式来考核。要上课的学生在进入教学楼或实验楼时，可使用楼内的专用识别设备读取该二维码，下课时学生再次出示该二维码，系统会自动记录相应的信息，然后任课教师通过网络查询学生的出勤情况。

(4) QR 码作为借书证

在高校中，为了安全等多方面的考虑，一般进出图书馆都需要使用纸质的借书证(卡)，如果学生突然想去图书馆而又没带证件时，会很不方便。因此，使用便于携带的可以存储在手机中的 QR 码会为学生提供很大的方便。

(5) QR 码作为就餐卡

在高校的食堂中，各个窗口一般都不直接接受现金，而是采用刷卡的方式，这就要求学生要多带一种卡。如果使用可以存储在手机中的 QR 码，则会为学生带来方便，同样也省去了制作就餐卡的成本。

通过对系统进行需求分析得到的系统用例图如图 3 所示。

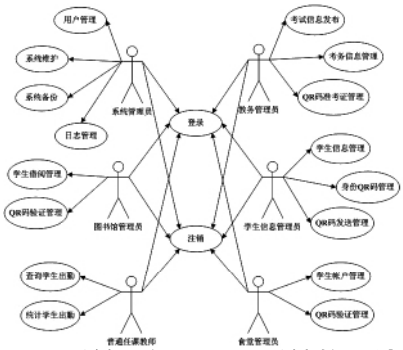

图 3 系统用例图 3.2 系统的设计

根据需求分析的结果，系统分为 QR 码管理模块，学生信息管理模块，考务管理模块，图书管理模块，食堂管理模块，系统管理模块。系统的总体结构图如图 4 所示。

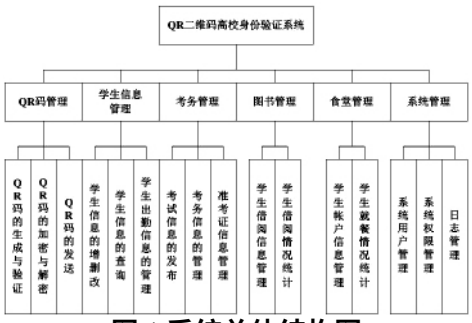

图 4 系统总体结构图

(1) QR 码管理模块

QR 码的生成与验证: 该模块的第一个功能是根据相关的信息和需要编码生成相应的 QR 码; 第二个功能是对从硬件设备采集到的 QR 码图形进行扫描，解码出相应的信息并验证。

QR 码的加密与解密: 目前已经有很多软件可以识别 QR 码图形并且也可以根据所给信息来生成 QR 码图形，所以，为了防止伪造事件的发生，必须在生成 QR 码图形之前对相关的数据进行加密。对扫描到系统中的 QR 码，要经过解密才能还原成原始信息来满足相关的验证。该模块的功能就是对数据进行加密和解密。

QR 码的发送: 系统根据需要生成 QR 码之后，可以采用三种方式(Email、手机彩信、打印成纸质)将生成的 QR 码发送到相应的学生手中。

(2) 学生信息管理模块

学生信息的增删改: 完成学生信息的添加、删除和修改。为了保证信息的准确性和权威性，可以从

学生处的学生学籍管理系统中导入学生的信息。

学生信息的查询: 完成学生信息的查询。

学生出勤信息的管理: 为了方便任课教师的教学管理,系统提供了自动统计学生出勤的功能。

(3) 考务管理模块

考试信息的发布: 负责在考试前发布与考试相关的信息。

考务信息的管理: 进行诸如考场安排、监考安排、时间安排等与考务相关的处理。

准考证信息管理: 根据考试的具体信息(考试名称、场次、考场、座位号等) 和学生的相关信息(学号、姓名、专业、班级、照片等) 组合成准考证。

(4) 图书管理模块

学生借阅信息管理: 完成学生借书、还书的信息的管理。学生的基本信息同样可以从学生处的学生学籍管理系统中导入。

学生借阅情况统计: 对学生借阅书籍的类型、种类、数量等数据进行统计,为分析学生的喜好等工作提供依据。

(5) 食堂管理模块

学生账户信息管理: 完成学生就餐情况的管理,包括充值和余额管理等。

学生就餐情况统计: 对学生就餐的食物类型、数量等数据进行统计,为分析学生的喜好,提高饭菜质量和服务水平等工作提供依据。

(6) 系统管理模块

系统用户管理: 完成用户账号的设定及密码的初始化工作。用户的基本信息可以从学校人事处的人事管理系统中导入。

系统用户权限管理: 进行系统用户权限的设定与分配,使各类管理员及用户都能在允许的权限之内完成自己的工作,互不干扰。

3.3 系统关键部分的实现

本系统的关键部分是 QR 码管理模块。

(1) QR 码生成的实现

系统中 QR 码的生成必须要有两种数据: 学生的照片和学号。由这两种数据能够唯一确定一名学生。

生成的步骤: 首先将包括学生照片和学号的数据与其它信息数据进行加密,然后使用 ZXing 类库提供的编码功能将加密后的数据编码成 QR 码图形,再把该图形保存在内存中或以图片的方式保存到系统指定的文件夹中。

(2) QR 码验证的实现

验证的步骤: 首先通过 CMOS(或 CCD) 摄像头、手持式扫描设备将 QR 码图形读取到系统中,然后使用 ZXing 类库提供的解码功能将 QR 码图形中的数据解析出来,再通过解密模块将数据还原成包括学生照片、学号和其它信息的数据,最后可以通过人工模式或自动识别模式对 QR 码持有者的身份进行比对验证。

(3) QR 码加密与解密的实现

为了保证生成 QR 码所需的数据的安全性和防伪性,需要对数据进行加密; 反之,在验证过程中需要对数据进行解密。本系统采用 RSA 算法进行数据加密与解密。RSA 算法的步骤:

a) RSA 算法的初始化。产生两个大素数 p、q(保密); 计算 $n = p * q$(公开),则 n 的欧拉函数 $\Phi(n) = (p-1) * (q-1)$(保密); 选取整数 e 作为公钥(公开),使其满足 $\gcd(e, \Phi(n)) = 1$,且 $1 < e < \Phi(n)$; 计算私钥 d(保密),使其满足 $e * d = 1 \pmod{(\Phi(n))}$。

b) RSA 加密、解密变换。首先将明文分块并数字化,每个数字化明文块的长度不大于 $[\log_2 n]$,然后对每个明文块 m 依次进行加密和解密变换。

加密变换: 使用公钥 e 对明文 m 加密,即 $c = m^e \pmod n$。

解密变换: 使用私钥 d 将密文 c 解密,获取明文 m,即 $m = c^d \pmod n$。

加密与解密模块首先根据 RSA 算法的步骤对相关数据进行加密和解密,然后将处理后的结果返回给生成模块或验证模块,以便继续完成任务。

4. 结语

本文研究了以 QR 二维码为核心的一种新型的高校身份验证系统,该系统所拥有的功能可以替代高校中很多现有的系统,达到除学生学籍管理系统和人事管理系统之外的多种系统的整合,节省了资源,并且能够减轻相关管理人员的工作量。

[参考文献]

[1] 曾子剑. 基于 QR 二维码编解码技术的研究与实现[D]. 成都: 电子科技大学,2010.

[2] 黄婷婷. QR 码识别方法研究[D]. 长沙: 中南大学,2008.

[3] 张军红. 基于二维码识读的集中式校园门禁系统[J]. 福建电脑,2011(12).

[4] 卢开澄. 计算机密码学[M]. 北京: 清华大学出版社,1998.

[5] 张颖,曹天人. 基于 RSA 算法的加密应用[J]. 科学咨询(科技管理),2011(9).

[6] William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition(影印版)[M]. 北京: 机械工业出版社,2006.