doi 10.3969/j.issn.1671-1122.2012.10.011

安全实用的二维码研究与实现

高彦受，许春根

（南京理工大学理学院，江苏南京 210094）

摘 要：二维码是将大量信息以图片的形式承载，达到快捷方便的目的，目前广泛运用于电子商务、票务系统等。然而，二维码也面临着信息泄露和信息涂改等安全威胁，文章对二维码所面临的主要问题进行了研究，以 QR 码为例，为防止信息泄露，在进行 QR 码生成时对数据进行了加密处理，主要是 RC4 加密，最后设计并实现了 QR 码的生成，该设计方案不仅不会泄露个人信息，而且生成效率很高，在实际中具有应用价值。

关键词：二维码；QR；加密；RC4；编码

中图分类号：TP393.08 文献标识码：A 文章编号：1671-1122（2012）10-0047-03

Research and Implementation of a Secure Two-dimensional Code

GAO Yan-shou, XU Chun-gen

(*School of Science,Nanjing University of Science and Technology, Nanjing Jiangsu* 210094,*China*)

Abstract: Two-dimensional code is carried large amounts of information in the form of pictures, to achieve the purpose of fast and convenient. So far, It is widely used in e-commerce and ticketing systems. However, two-dimensional codes is also faced with security threats such as information disclosure and information altered. Our article research the main problem faced by the two-dimensional code. For example, when we generated the QR code, we encrypt the source data to prevent information leakage. The encryption method is RC4. Finally, designed and implemented a QR code. This design will not disclose personal information and generate high efficiency. The important is application value in practice.

Key words: two-dimensional code; QR; encrypt; RC4; encode

0 引言

二维条码技术[1]是在一维条码无法满足实际应用需求的前提下产生的，其主要思想方法是把一维码自上而下地堆叠在一起。最具代表性的有 Code49[2]、Code16K[3] 等。1990 年美国 Symbol Technologies，Inc.的王寅军在缝合算法的理论基础上开发了一种新型的行排列二维码，命名为 PDF417[4] 条码。几乎同时，矩阵码也发展起来。矩阵码是一种原理和方法与行排列二维码完全不同的条码系统。Date Matrix[5] 是最早的二维条码，早期的 Date Matrix 码是从 ECC-000 到 ECC-140，它是把卷尺算法用于纠错的二维条码。1995 年 5 月，Jason Le 对 Date Matrix 码进行了改进，他把 Read-Solomon 纠错算法用于 Date Matrix 码，称为 ECC-200。1995 年 10 月国际自动识别制造商协会接受 Date Matrix 码为国际标准，Date Matrix 码成为公开的二维条码。QR code[6,7] 是由日本 Denso 公司于 1994 年 9 月研制的一种矩阵码，它是最早对中文汉字进行编码的条码。

在我国，二维条码起步比较晚，2003 年初，上海龙贝信息科技有限公司开发了一种龙贝码，打破了只有美国，日本等少数国家的垄断。2005 年末，中国物品编码中心承担国家“十五”重大科技专项“二维条码新码制开发与关键技术标准研究”取得突破性成果。手机二维码业务在国内是由中国移动通信集团于 2006 年 8 月正式推出的，采取的是 QR 码与 Date Matrix 码并行码制。中国联通公司于 2006 年 5 月推出国内第一款条码手机 ET980；中国移动公司于 2006 年 8 月推出手机二维码应用条码识别业务，并且与多家手机二维码解决方案提供商进行了合作。这都极大的促进了手机二维码业务的发展。自此，手机二维码不断出现在各大媒体网站中，成为电信领域关注的焦点。

1 二维码编码理论

1.1 二维码的分类

1.1.1 二维条码的分类

1）行排式二维条码[8]：具有代表性的矩阵式二维条码有 Code16K、Code49、PDF417 等。

收稿时间：2012-07-05

基金项目：江苏省自然科学基金重大项目[BK2011023]

作者简介：高彦受（1988-），男，山东，硕士，主要研究方向：信息安全与密码学；许春根（1969-），男，安徽，教授，博士，主要研究方向：编码与密码学。

2）矩阵式二维条码[9]：Code One、Maxi Code、QR code、Data Matrix 等。

1.1.2 二维条码的主要编码方式

1）PDF417 层叠式条码。PDF417 层叠式条码是由于组成条码的每一符号字符都是由 4 个条和 4 个空共 17 个模块构成，所以称为 PDF417 码。它是一种多层、可变长度、具有高容量和错误纠正能力的连续型二维条码。PDF417 码技术特点：（1）信息容量大；（2）编码范围广；（3）保密、防伪性能好；（4）译码可靠性高；（5）修正错误能力强；（6）容易制作且成本低；（7）条码符号的形状可变。

2）Data Matrix 矩阵编码。Data Matrix 最大特点就是“小”，Data Matrix 采用 Read-Solomon 交织交插编码，编码时加入了纠错码，使 Data Matrix 的纠错性能比较强。Data Matrix 符号的数据区由规则排列的方形深浅模块构成。数据区的四周是探测图形，探测图形外则是空白区。探测图形为一个模块宽度，是数据区的边界，其中两条邻边为暗实线，形成了一个 L 型边界，用于限定物理尺寸、定位和符号失真。另两条邻边由交替的深色模块和浅色模块组成，主要用于限定符号的单元结构，也能帮助确定物理尺寸及失真。

3）QR 快速响应矩阵码。QR code 码除具有一维条码及其它二维条码所具有的信息容量大、可靠性高、可表示汉字及图像多种文字信息、保密防伪性强等优点外，还具有如下主要特点：（1）超高速识读；（2）全方位识读；（3）能够有效地表示中国汉字、日本汉字。

1.1.3 三种码制的结构图

图 1、2、3 为 PDF417、DM 和 QR 的结构图。

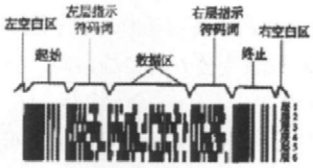

图1 PDF417结构图

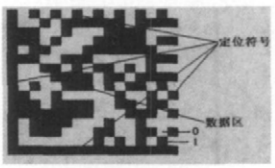

图2 DM结构图

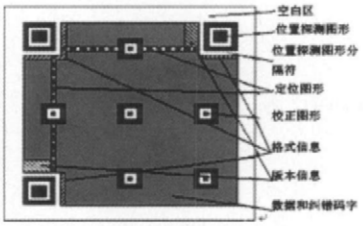

图3 QR结构图

表1 三种码制的比较表

码制名称	PDF417 码（美国，行排列式）	Date Matrix 码（美国，矩阵式）	QR code 码（日本，矩阵式）
识读速度及汉字表示	3 个 / 秒 16bit	2-3 个 / 秒 16bit	30 个 / 秒 13bit
识读方向和方法	±10° 条空宽度尺寸判别	360° 深浅模块判别	360° 深浅模块判别
数字、字母、字节、汉字的最大容量	2700/1800 /1100/550	3116/2335 /1558/778	7000/4200 /2900/1800
最大纠错能力	50%	35%	30%
最大识读精度	6mll	6mll	6mll
识读方式	激光式 /CCD	CCD	CCD
适用范围	EDI/ 高品质运输 / 产品行销 / 设备管理 / 物品安全管制表	小零件标识 / 电路板的零组件	工业自动化生产管理 / 表示中日文字

1.1.4 三种码制的比较

下表 1 是三种码制的具体对比表。

1.2 二维码的安全

随着网络应用的不断扩大，人们对网络安全保护提出了更高要求。二维条码防伪加密技术[10]是在二维条码的基础上运用密码学的原理，把密钥的私钥或公钥体制与二维条码的编码技术结合起来，从而克服了二维条码所载信息在网上和其他物理空间传输时容易被破译和复制的缺点。二维条码的加密和解密方案主要分为以下三种方案。

方案一：对源信息先加密再编码，具体过程如图 4。

图4 先加密后编码方案

方案二：对源信息先编码后加密，如图 5。

图5 先编码后加密方案

方案三：双重加密，具体如图 6。

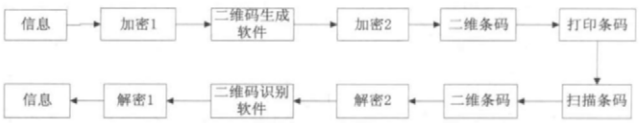

图6 双重加密方案

1.3 二维码的编码理论

1.3.1 二维码的编码流程

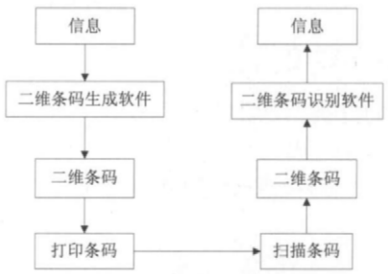

图7 条码的生成和识别过程

二维码的生成和识别基本流程如图 7 所示，二维码的生

成技术包括信息编码、纠错编码、符号表示、符号印制等4个主要技术过程。

1）信息编码。二维条码的信息编码分为两个阶段：（1）二维条码的预编码过程（原始的数据的信息化处理过程）；（2）数字信息（数字、汉字、图像等信息）按照一定的规则映射到二维条码的基本信息单元—码字的过程（二维条码编码的核心内容）。

2）纠错编码。在完成了二维条码的编码后，为了提高条码的可读性，在二维码的生成过程中引入了纠错。它是通过在原有信息的基础上增加信息冗余，并通过一定的纠错码生成算法生成纠错码字，从而保证在出现脱墨、污损时也可以利用纠错码字通过特定的纠错译码算法正确的还原原始数据信息。在众多码制中涉及到最常用的是算法 Read-Solomon 算法[11]。

3）符号表示。符号表示是指在数据信息流转换为码字流之后，将码字流用相应的二维条码符号进行表示的过程。符号表示技术主要研究的条码符号设计、码字排布等。二维条码由此可分为行排列二维条码和矩阵式二维条码。

4）符号印制。在二维条码符号的印制过程中，对诸如反射率、对比度以及模块大小与分辨率等均由严格要求。

1.3.2 RS纠错

二维条码识读解码得到的数据码字中可能含有错误信息，必须进行纠错译码以恢复编码时的原始信息。二维条码中广泛采用 RS 纠错。

RS 译码分为三步：第一步由接收到的码组计算伴随式；第二步由伴随式计算出错误图样；最后，由错误图样和接收码组计算出可能发送的码字。

设发送的码多项式为 $F(X)$ 接收码多项式为 $G(X)$ 存储器系统错误模式多项式为 $W(X)$ 则：$G(X)=F(X)+W(X)$。

设码的纠错能力为 a，存储器产生的实际错误个数为 $e \leqslant a$ 故而在 $W(X)$ 中只有，W 不为 0，假定这 W 项为 $Y_1X_{l1},Y_2X_{l2},...,Y_eX_{le}$，其他项为 0，则有：$W(X)=Y_1X_{l1}+Y_2X_{l2}+...+Y_eX_{le}$。

式中 $X_{l1},X_{l2},...,X_{le}$ 称为错误位置数，而 $l1,l2,...,le$ 为错误位置，$Y_1,Y_2,...,Y_e$ 为相应位置上的错误值。

译码的任务便是从接受码多项式 $G(X)$ 求出错误位置数 $X_{l1},X_{l2},...,X_{le}$，和相应的错误值 $Y_1,Y_2,...,Y_e$，再从 $G(X)$ 中减去 $W(X)$，则得码字 $F(X)$ 的估值 $\bar{F}(X)$，从而完成译码。

2 具体实现

选取 QR 码制并对上述方案一实现，主要过程如下：

本设计运用的加密算法是 RC4[12]，是运用 cryptAPI 来实现的，具体函数是 BOOL WINAPI CryptEncrypt（HCRYPTKEY hKey、HCRYPTHASH hHash、BOOL Final、DWORD dwFlags、BYTE *pbData、DWORD *pcbData、DWORD cbBuffer），参看 MSDN。

对输入的数据进行 QR 编码时由函数 BOOL EncodeData（int nLevel、int nVersion、BOOL bAutoExtent、int nMasking、LPCSTR lpsSource、int ncSource）实现。

如图 8 所示，首先在用户订单信息栏中输入相应信息，提交订单并显示结果，然后产生随机密钥并处理数据，最后就生成了二维码。图 9 中是对生成的二维码进行解码，解码出来的数据时经过加密的数据，不会显示个人信息，所以是安全的。

图8 编码

图9 解码

3 结束语

本文设计并实现了对于订单下的 QR 码的生成，充分考虑到在实际中的应用，特别进行了加密处理，这样不仅生成效率高，而且提高了安全性，使得用户和商家可以放心的使用二维码。本文只设计了二维码生成软件，相应的二维码识别软件有待开发。此外，本软件中的部分功能还未实现，如发送密钥和二维码，对二维码信息进行签名等可做进一步的研究和实现。（责编 张岩）

参考文献：

[1]The Pavlidis, Jerome, and Ynjiun P.Wang. Information Encoding with Two-Dimen-sional Bar codes[J].IEEE Computer Magazine 1992,6.25(6):18-28.

[2] 张玲，胡东红，孔华锋等．二维条码图结构特性分析 [J]. 湖南大学学报，2004，26（03）：226-231.

[3] ANSI 1998. 美国国家标准协会 统一符号规范 16k 编码 [S].

[4]Sriram T,Rao V K. Application of Barcode Technology in Automated Storage&Retri-eval Systems[J]. IECON Proceedings,1996,1:5-10.
[5]International Organization for Standardization ISO.IEC 16022 Information Technology International Symbology Specification:Data Matrix 2000[S].
[6]Bill McCracken, Mark Worthington.2D codes provide larger data capacity for Automation identification applications[J]. I&CS.1994.12.
[7] 张成海，郭卫华等 . QR Code 二维码 [M]. 北京 ：中国标准出版社 .2000.07.
[8]Vangils W.J. Two-dimensional dot codes for product identification[J]. IEEE Transactions on Information Theory. 1987 33(5):620-631.
[9] 刘宁钟 . 高维条码识别技术和编码理论的研究 [D]. 江苏 ：南京理工大学，2003.
[10] 张茹，刘明业 . 二维条码在信息安全领域的应用研究 [J]. 计算机工程与科学，2004，26（02）：108-109.
[11]J.Piatek.AutomativeIndustryReeommendZ-DStandards[J].AutomatieI.D.News, 1994, (08): 54-56.
[12] 胡亮，迟令，袁巍等 . RC4 算法的密码分析与改进 [J]. 吉林大学学报 ，2012，50（03）：511-516.

资 讯

北京市“全警廉政监督信息网”系统启动仪式在京举行

2012 年 9 月 3 日上午，在北京市公安局举行了“ 全警廉政监督信息网 ” 系统启动仪式，北京市委常委、市公安局局长傅政华亲自开启了该系统，标志着“ 全警廉政监督信息网 ” 系统的正式运行。

该系统是首次由北京市公安局科技信息化部独立自主研发的全局性应用系统，在北京市公安局科技信息化部党委的高度重视下，专门成立了由北京市公安局科技信息化部党委书记、主任贾胜文任组长，副主任董红路任副组长的系统研发组，经过两个多月努力奋战，圆满完成了系统研发，并且实现了系统软件 100% 自行设计、100% 自行编码、100% 自行培训、100% 自行维护。

傅政华局长在北京市公安局党委委员、市局副局长董小兵、党委委员、纪委书记马燕军和北京市公安局科技信息化部党委书记、主任贾胜文等领导陪同下，亲切接见并慰问了系统研发组的全体民警。傅政华局长对此次工作给予了充分肯定，指出“ 开展应用系统自主研发，是新的历史时期首都公安应用系统建设模式的一次实践创新，是首都公安信息化建设的一项重要举措。此次‘ 全警廉政监督信息网 ’ 系统建设是我局首次全部由民警自主研发的应用系统，这不仅证明了首都公安科信民警较强的业务素质和工作技能，体现了首都公安科信民警敢于创新、敢于碰硬、敢于担当的时代精神，更重要的是研究探索出了一条首都公安机关自主研发应用系统的科技建设新路，为全面推进首都公安创新型警务建设做出了重要贡献 !” 北京市公安局科技信息化部领导也表示将以此为工作契机，打造一支懂业务懂技术的公安科技信息化复合型人才队伍，充分发挥专业特长，为推动公安科技信息化工作的创新发展和首都公安科技信息化工作创新发展再立新功。（记者 于春兰）