文章编号：1005-8451（2012）11-0037-05

QR码信息加密的研究与实现

刘彦伟，王根英，刘　云
（北京交通大学　通信与信息系统北京市重点实验室，北京　100044）

摘　要：针对QR码存在的安全性不足的缺点，本文通过研究QR码编解码规则和加密算法，提出利用PBE算法对QR码中信息进行加密。编码时在QR码中加入加密标志位，输入口令并用PBE算法对信息加密。解码时采用开发的专用识别软件输入正确口令即可解密出明文信息。实验表明，本方法可大幅提高QR码的安全性，具有很强的实用性。

关键词：QR码；PBE算法；编解码规则；加密标志位
中图分类号：U293：TP391　**文献标识码：**A

Research and implementation of QR Code information encryption

LIU Yan-wei, WANG Gen-ying, LIU Yun
(Key Laboratory of Communication & Information Systems, Beijing Jiaotong University, Beijing Municipal Commission of Education, Beijing　100044, China)

Abstract: Though research on the encode/decode rules of QR Code and encryption algorithm, the paper put forward a method that PBE algorithm was used to encrypt information of QR Code. When encoding a barcode, Encryption Mark Bit was put into QR Code; then the information was encrypted by using PBE algorithm with a password. The barcode could be decoded by using the private decoder and inputting the right password, the plain information could be get soon. Experiments showed that this method could improve the security of QR Code remarkable and also had strong practicability.

Key words: QR Code; PBE algorithm; encode/decode rules; encryption mark bit

二维码在横向和纵向两个方位同时表达信息，较一维条码具有信息容量大、可靠性高、支持多种纠错级别且不依赖于数据库和网络等优点，具有广泛应用前景。QR码是矩阵式二维码的一种，除具有以上特点外，还有快速、全方位识别的特性，具有广泛的应用前景，现在已应用于印刷、交通和移动通信等社会生活的许多领域。

对于QR码泄露个人信息的问题国内外已有不少专家学者做了研究，并提出一些算法。文献[1]采用DES加密算法先对原始信息进行加密，将加密后的密文作为编码输入信息来生成二维码。解码时先解出密文，再进行解密得出明文信息。文献[2]提出在电子票务应用中采用Rijnael算法先对明文信息进行加密，并将加密后密文用Base64转换为易于记忆的信息，最后以此生成二维码。解码时反之。文献[3]利用混沌序列的非线性、随机性、不可预测性、对初始条件值非常敏感等特性，采用Logistic混沌对原始QR码二值图像进行加密和解密。但是这种对二维码图像加密的方法会降低二维码的纠错能力。

本文根据QR码的编解码规则和PBE（Password Based Encryption，基于口令加密）算法的特点，研究了一种安全、实用的QR码内容信息加密方法。

1　相关工作

1.1　QR码编码及解码

QR码（Quick Response Code，快速响应码）是一种矩阵式二维码，所谓矩阵式二维码是在一个矩形空间通过黑、白像素在矩阵中的不同分布进行编码。每个QR码符号由名义上的正方形模块构成，组成一个正方形阵列，它由编码区域和包括寻象图形、分隔符、定位图形和校正图形在内的功能图形组成[4]。功能图形不能用于数据编码。图1为QR码版本2符号的结构图。

QR码的编码步骤共分为7步，具体是：（1）

收稿日期：2012-03-27
作者简介：刘彦伟，在读硕士研究生；王根英，副教授。

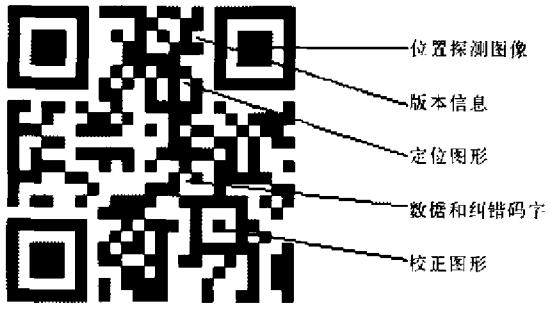


图1 QR码版本2符号结构图

数据分析：对输入数据进行分析，选择合适的模式；(2) 数据编码：按照选择的模式将数据转换为位流；(3) 纠错编码：按需要将码字序列分块，以便按块生成相应的错误纠正纠错码字，并将其加入到相应的数据码字序列的后面；(4) 构造最终信息：在每一块中置入数据和纠错码字，必要时加剩余位；(5) 在矩阵中布置模块：将寻象图形、分隔符、定位图形、校正图形与码字模块一起放入矩阵；(6) 掩模：依次将掩模图形用于符号的编码区域。评价结果并选择最优结果；(7) 格式和版本信息：生成格式和版本信息，形成符号。图2是QR码的编码流程图。

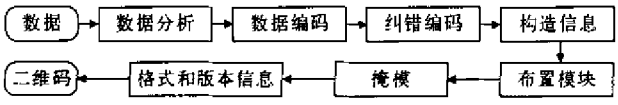


图2 QR码的编码流程图

QR码的解码是编码的逆过程，首先是定位图像符号，识读格式信息、版本信息，消除编码区掩模。其次，根据模块排列规则，恢复数据、纠错，划分数据码字。最后，按照使用的模式译码得出数据字符并输出结果。

由于二维码的编解码算法公开，且未实现对其携带的信息加密。使得一些未授权的人员或单位，可以在手机或电脑上使用公开二维码解码软件随意读取二维码信息[5]，造成信息泄露。如此低的安全级别，对二维码的广泛应用确实造成了不少威胁。

1.2 PBE算法

PBE (Password Based Encryption，基于口令加密)算法是一种基于口令的加密算法，其特点是使用口令代替了密钥，而口令由用户自己掌管，采用随机数杂凑多重加密等方法保证数据的安全性。PBE算法在加密过程中并不是直接使用口令来加密，而是加密的密钥由口令生成，这个功能由PBE算法中的KDF函数完成。KDF函数的实现过程为：将用户输入的口令首先通过“盐”(salt)的扰乱产生准密钥，再将准密钥经过散列函数多次迭代后生成最终加密密钥，可描述为：

T_1=Hash(Password,Salt),

T_2=Hash(T1),

…

T_C=Hash(T_C-1),

Key=T_C<0，dkLen-1>.

其中Password为口令；Salt为随机字节数“盐”；T_i (i=1,2,…,c)是第i次迭代产生的散列值，Hash是单向散列函数，c是迭代数；Key是最终生成密钥，取T_C的前dkLen位，dkLen是具体所采用对称加密算法的密钥要求长度。

密钥生成后，PBE算法采用对称加密算法对数据进行加密，可以选择DES、3DES、RC5等对称加密算法。在加密之前，需要对加密信息进行定长分组形成固定长度的消息组，对于小于固定长度的消息组采用PKCS#5填充方法进行填充。PKCS#5填充采用填充字节数作为填充值，从而可以方便识别原始数据和填充数据[6]。具体过程为：对于明文消息M，计算出其数组长度||M||，则填充数组PS满足如下规则：

PS=01 if ||M|| mod 8=7;

PS=02,02 if ||M|| mod 8=6;

…

PS=08,08,08,08,08,08,08,08 if ||M|| mod 8=0;

计算出填充数组PS后，将PS加入最后一个消息组，并被加密。在解密时，明文消息组的最后一个组就包含填充数据PS，可根据填充内容迅速过滤掉填充数据。

对称加密算法则可以将填充后的消息组用生成的密钥直接加密，生成密文。由此可见，PBE算法是杂凑算法和对称加密算法的综合应用，即首先采用杂凑算法生成密钥，再用对称加密算法进行加密。PBE算法加密流程如图3。

2 QR码信息的PBE加密

2.1 加密流程

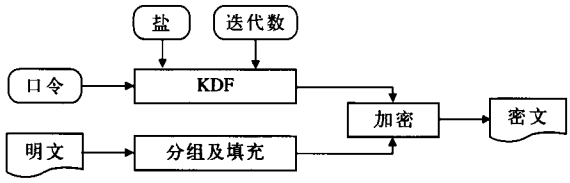


图3　PBE算法加密流程

为保证QR码加密的高效与便捷，本文将PBE算法内嵌于QR码编解码步骤中。为避免加密算法影响QR码图像的排列规则和生成1:1:3:1:1图形，而降低QR码的识别和纠错能力，本文将加密操作置于QR编码步骤第2步“数据编码”步骤后，对编码位流进行加密，之后再将密文进行“纠错编码”及后续处理。解码时反之。QR码信息的PBE加密算法流程为：

（1）输入明文信息，加密口令；

（2）将明文信息按QR码编码进行数据分析和数据编码操作，形成明文位流；

（3）根据模式，在编码信息流中插入加密标志位；

（4）将明文位流转换为字节流，并进行分组和填充，形成适于加密的消息组；

（5）将加密口令和随机字节数“盐”杂凑、迭代生成加密密钥；

（6）根据设定的对称加密算法，用密钥对消息组进行加密，生成密文消息组；

（7）将密文消息组按序插入编码信息流中；

（8）对编码信息流进行“纠错编码”及后续处理，生成加密QR码。

2.2　QR码加密的实现

QR码的PBE加解密实现采用Java语言编写，是在开源项目和基础函数库的基础上进行的二次开发。开源项目用于初步实现QR码的编码和解码，在此基础上再编写函数进行加密和解密操作。

（1）QR编码函数

```
public void Encode(String info, String password, String path){
    …
    BitMatrix bitMatrix;
        bitMatrix = new MultiFormatWriter().encode(info,password,
                        BarcodeFormat.QR_CODE, 200, 200); //形成QR码二值矩阵
    File file = new File(path);
    MatrixToImageWriter.writeToFile(bitMatrix, "png", file);
        …
    }
```

（2）密码标志位

在上述加密流程步骤（2）中，向编码信息流中插入加密标志位。在QR码中加入加密标志位，可以使解码软件快速识别出加密QR码，对其进行解密。本文使用QR码的保留字作为加密标志位。通过QR码编解码规则计算出部分保留字如表1。

表1　QR码保留字列表（部分）

模式	保留字	bit长度
数字	1 000～1 023	10
	100～127	7
	10～15	4
字母数字	2 025～2 047	11
	45～63	9
8位字节	255	8
汉字	-23 904，-24 065等	16

说明：1.表中保留字的数值为十进制表示；
2.“汉字”模式中的保留字与编码制式有关，表中的保留字为GB2312码中的未编码码字。“-23904”对应“A2A0”，“-24065”对应“A1FF”。

插入密码标志位的函数：

```
public BitArray InsertEncryMark(BitArray bits){
        bits.appendBits(MARK,MARKLENGTH); // 插入加密标志位
        return bits;
    }
```

（3）位流字节转换

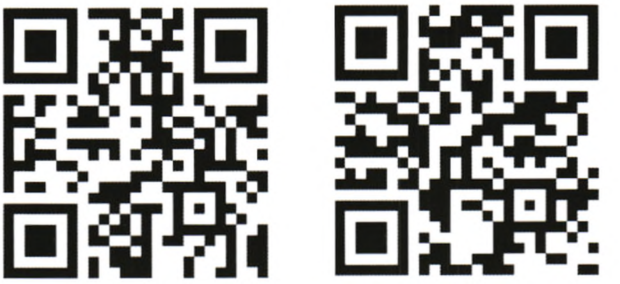
QR码编码在“数据编码”步骤后，将明文信息已经转换为二进制位流，但是PBE加密函数信息输入要求为字节数组格式，所以必须加以转换。位流字节转换函数为：

```
public static byte[] BitArray2Byte(BitArray bit, int count){
    …
      for(int v=tempBit.bits.length-1,z=0;v>=0; v--,z++){
            int tempNum=tempBit.bits[v];
            tempBytes[0+z*4]=(byte)((tempNum >> 24) & 0xFF);
            tempBytes[1+z*4]=(byte)((tempNum >> 16) & 0xFF);
```

```
            tempBytes[2+z*4]=(byte)((tempNum
>> 8) & 0xFF);
            tempBytes[3+z*4]=(byte)((tempNum)
& 0xFF);
        }
    ...
    }
```

(4) PBE加密函数

```
    public byte[] PBEEncryptio(byte[] con-
tentByte, String password)throws
Exception {
        byte[] salt=PBECoder.
initSalt();        //初始化“盐”
        Key key=toKey(password,
salt);        //生成密钥
        PBEParameterSpec para-
mSpec=new PBEParameterSpec
(salt,ITERATION_COUNT);
        Cipher cipher=Cipher.
getInstance(ALGORITHM);
            cipher.init(Cipher.
ENCRYPT_MODE, key, param-Spec);  //初始化
        byte[] encryData= cipher.doFinal(data);
//加密
        return encryData;
    }
```



(a) 未加密QR码　　(b) 加密QR码

图5　实验QR码

表2　QR码加密解密测试数据

模式	信息内容	是否加密	口令(密码)	识别结果		
				QR码加解密软件		普通识别软件
				解码内容	时间(ms)	解码内容
数字	0123456789	是	qrcode	0123456789	490	1000
		否	无	0123456789	240	0123456789
字母数字	BJTU2012	是	abc12345	BJTU2012	480	(无法识别)
		否	无	BJTU2012	240	BJTU2012
8位字节	123@bjtu.*?	是	Beijing	123@bjtu.*?	550	\[illegible\]蠍鑛;
		否	无	123@bjtu.*?	270	123@bjtu.*?
汉字	北京交通大学	是	001001	北京交通大学	490	H蕐墤irNy硬硖:
		否	无	北京交通大学	250	北京交通大学

注：测试中的普通软件采用的是Quick Mark二维码识别软件。

3　实验及分析

为测试本文提出方法的有效性，使用短文本信息在QR码的数字、字母数字、8位字节、汉字4种模式下均做了实验，利用作者开发的QR码加解密软件和普通识别软件进行解码对比，并测定了QR码加解密软件的识别时间。测试中PBE算法的实现为PBEWithMD5AndDES，CBC模式，迭代数为1 000。测试计算机配置为：Intel Core i3 2.27 GHz，2.00 GB内存。测试数据如下，图5为汉字模式下“北京交通大学”信息的QR码图像，其中图(a)未加密，可以使用普通二维码识别软件进行识读，而图(b)为加密QR码，必须采用专用识别软件才能正确识读。表2为详细测试数据。

通过以上数据发现：(1) QR码加解密软件可以正确识读所有加密和非加密QR码，而普通二维码识别软件只能正确识别非加密QR码，对加密QR码的正确识别率为0%。所以采用PBE加密的QR码具有很高的安全性，可以抵御二维码软件的未授权识读。(2) 加密口令简单、灵活，且由用户掌握。(3) 在QR码加密解密软件识读加密QR码时，可以发现其识别时间要大于识别未加密QR码。经过计算，QR码在加密后的识别时间平均延长了252 ms左右。在实际应用中0.252 s的时延几乎可以忽略。(4) 对比图5中(a)、(b)两图发现非常相似，说明PBE算法加密并没有改变QR码的图像排列规则，所以不会对QR码的纠错造成影响。

4　结束语

本文研究了QR码编解码规则和对称加密算法。针对QR码存在的安全性缺陷，提出用PBE算法对QR码进行加密。在QR码编码时，输入口令对信息加密后生成QR码，解码时输入正确口令进行解密。通过实验证明，本方法可以将普通二维码识别软件对加密QR码的正确识别率降至0%，必

须采用专用识别软件输入正确口令才能正确识别加密QR码，显著提高了QR码的安全性，具有很强的实用性，可广泛应用于客票等票务领域。同时利用加密口令由用户掌握的特点，还可以扩展QR码的应用范围。

参考文献：

[1] DroidLa. Encrypted QR codes: Share secret messages[EB/OL]. http://qrdroid.com/encrypted-qr-codes-share-secret-messages.html，2011-7-13.

[2] D.C-Lagoa, E.C-Montenegro, F.J.G-Castao, F.G-Castieira. Secure eTickets Based on QR-Codes with User-Encrypted Content[C]. Consumer Electronics (ICCE), 2010 Digest of Technical Papers International Conference. 2010: 257-258.

[3] 张定会，郭静波，江　平，等. QR码二值图像混沌加密与解密[J]. 移动通信，2011，35（3）：131-134.

[4] GB/T 18284—2000，快速响应矩阵码[S]. 北京：国家质量技术监督局，2000.

[5] M. Jian, Y.Yang. Application of Mobile 2D Barcode in China [C]. Wireless Communications, Networking and MobileComputing, 2008. WiCOM '08. 4th International Conference.2008: 1-4.

[6] RSA Laboratories. PKCS #5:Password-Based Cryptography Standard[S]. Version 2.1, October 5, 2006.

责任编辑　徐侃春

（上接P36）

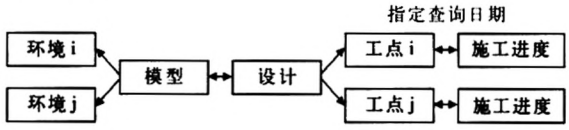
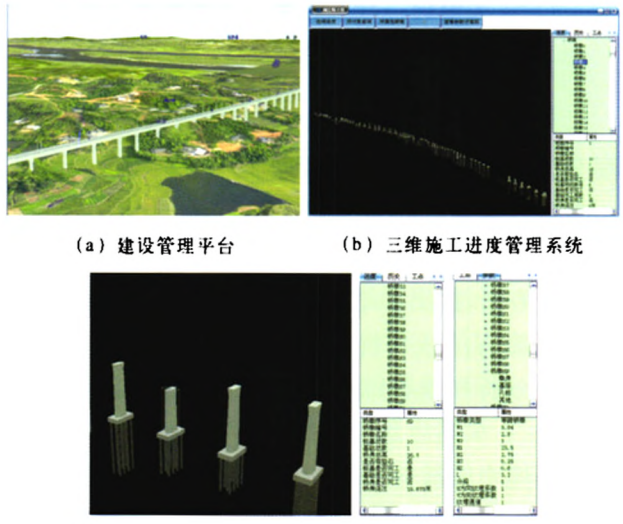


图5　数据关系示意图

生成模型导入铁路三维建设管理平台中，通过环境参数与桥梁模型的映射，获取施工进度管理系统的输入参数并调用本系统，在三维环境下查看选中桥梁的设计资料、工点信息与施工进度。以湘江特大桥为例，图6（a）为湘江特大桥在铁路三维建设管理平台中的环境，图6（b）为本系统所显示的湘江特大桥当前施工进度。如图6（c），在进度管理系统中选择某桥墩墩身，右侧选项卡内即可查看该桥墩的施工信息与设计信息。



（a）建设管理平台　　（b）三维施工进度管理系统

（c）交互查询

图6　应用实例

4　结束语

高速铁路桥梁三维施工进度管理系统已初步应用于长昆线施工管理，形象、直观地表现了该线路内桥梁的施工过程，使项目管理者可在虚拟环境中浏览桥梁工程建设情况，提高施工管理效率。开发过程中所涉及的数据库管理、参数化建模、形象进度表达、交互信息查询技术可应用于路基、隧道等其他工程的施工进度管理。

参考文献：

[1] 金　丹，朱培民，罗中杰，等. 桥梁施工进度的三维可视化管理[J].计算机应用与软件，2008，25（5）：187-190.

[2] 付　强，谢谟文. 基于快鸟卫星影像的高速公路施工三维可视化管理平台应用[J]. 公路，2011（5）：48-51.

[3] 史湘石，陆大为. 公路建设三维形象进度系统的开发和应用[J]. 公路与汽运，2011（6）：157-171.

[4] 黄利芒. 计算机图形技术在高速公路建设管理中的应用[J]. 公路与汽运，2011（6）：161-165.

[5] 曾　臻，朱　伟，赵建平. 施工进度动态形象显示[J]. 建筑施工，2005，27（11）：56-57.

[6] 王志刚，戴光华. OpenGL在工程实体形象进度中的应用[J]. 计算机工程与应用，2003（17）：133-135.

[7] 潘晓波. 形象进度图法编制桥梁工程施工进度计划[J]. 建筑科学，2010（11）：114-118.

责任编辑　杨利明