基于 QR 二维码的多级融合加密算法的设计与实现*

于英政　许宏丽
（北京交通大学计算机与信息技术学院　北京　100044）

摘　要　随着二维码的广泛应用，二维码加密技术受到越来越多的关注。快速响应（Quick Response，QR）二维码是一种被广泛使用的二维码，其实现过程的不同阶段有不同的特点。论文提出一种基于 QR 二维码的多级融合加密算法概念，通过对不同阶段采取 DES 加密和固定密钥的 RC4 加密大大提高 QR 二维码的加密强度，同时不明显增加二维码的长度和处理时间。实验数据表明了论文所提算法的有效性。

关键词　快速响应二维码；多级融合加密算法；DES；RC4
中图分类号　TP309.7　　**DOI**：10.3969/j.issn1672-9722.2014.12.031

Design and Development of Multilevel Fusion Encryption Algorithm Based on QR Two-dimensional Code

YU Yingzheng　XU Hongli
(School of Computer and Information Technology, Beijing Jiao Tong University, Beijing　100044)

Abstract　With the wide application of two-dimensional code, two-dimensional code encryption technology has attracted more and more attention. QR(Quick Response) two-dimensional code is a widely used two-dimensional code. The different stages of the implementation procedure have different characteristics. This paper presents a multilevel fusion encryption algorithm based on QR code, greatly improved the encryption intensity of QR code by using DES and fixed keys RC4 encryption in different stages. This algorithm does not significantly increase the length and the processing time of QR code. The experimental data show the validity of the algorithm.

Key Words　QR code, multi-level fusion encryption algorithm, DES, RC4
Class Number　TP309.7

1　引言

1.1　产生背景

二维码是近年来最为流行的信息传递方式之一，而快速响应（Quick Response，QR）二维码是其中应用最广，也颇具代表性的一员。QR 二维码在设计之初主要解决的是携带信息量和纠错问题。国家技术监督局发布的《快速响应矩阵码》标准[1]中并没有对加密部分的描述。随着应用的深入，QR 二维码的身影出现在了支付、传递密钥、记录个人敏感信息等涉及到加密的领域，火车票、支付宝等都出现了加密二维码的影子。QR 二维码加密越来越需要重视。

加密二维码技术是指在各种二维码技术的基础之上，运用密码学的原理，把加密技术与二维码的编码技术相结合，以实现二维码中信息的加密传递。目前应用于二维码的加密算法分为对信息加密和对生成的图像加密。已有的算法对信息的加密并没有与二维码的生成过程紧密结合，只是加密与二维码生成的简单组合。因此，如何不影响二维码的使用，又能够增强其加密性能，成为保证二维码广泛使用的保证。

1.2　研究现状

加密二维码属于刚起步阶段，还没有得到大量的关注。2007 年，中国物品编码中心编著的《二维

* 收稿日期：2014 年 6 月 12 日，修回日期：2014 年 7 月 30 日
作者简介：于英政，男，硕士研究生，研究方向：图像处理，二维码工程。许宏丽，女，博士，教授，研究方向：图像处理，信息检索。

条码的技术与应用》[2]中提出了几种对二维码加密的方案，但没有给出实现。2012 年，刘云龙等在 android 手机上实现了 DES 加密的 QR 二维码[3]，任勇金研究了 Rijndae 算法和异或运算的 QR 二维码加密[4]。2013 年，高彦受研究了 RC4 加密的 QR 二维码[5]，周庆等研究了基于 Ising 模型的 QR 二维码加密算法[6]，单利安对 QR 二维码水印加密解密算法进行了研究[7]。主要研究方向是对初始信息加密，缺少对二维码生成过程中的信息加密。

2　加密 QR 二维码算法设计

2.1　二维码的加密位置

QR 二维码编/解码信息的流程如图 1 所示。

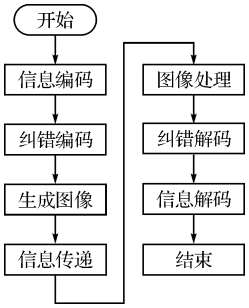

图 1　QR 二维码信息传递流程图

在图 1 中信息传递之前的几个阶段之中及之间均可以用来加密，信息传递之后的几个阶段之中及之间用来解密，因此，一般的加密方案都是在以下阶段加密的基础上进行的。

1）在信息编码之前进行加密，在信息解码之后解密。这样整个二维码的处理过程都是对已经加密的信息进行的，事实上即传输了加密信息。

2）在信息编码和纠错编码之间进行加密，在纠错解码和信息解码之间解密。这种加密方式加密的是二进制代码，可以选择比较简单的加密算法。

3）在纠错编码的过程中融入加密编码，纠错解码中进行解密。这需要研究二维码所采用的纠错编码（Reed-Solomon 编码），实现纠错编码和加密编码的混合。

4）在纠错编码后生成图像前进行加密，在图像处理完成之后进行解密。纠错编码完成后，可进行改动的空间比较小，加密后的长度需要固定或接近，并且尽量不能影响纠错编码的纠错性能。

5）在生成图像时对图像数据进行加密，在图像处理的过程中进行解密。这需要了解二维码图像生成的特点，不能因加密而损坏了二维码图像本身的结构。

加密方案的选择一般会根据要求的不同，在上述五个阶段中挑取一个或几个进行，在各种加密方案中选取一种或几种来进行。在编码越深处加密，需要考虑的方面也越多，对加密算法的要求就越高。

2.2　加密方案的选择

按有无密钥，加密算法可以分为无密钥加密与有密钥加密。有密钥加密中的固定密钥加密通常也可视为无密钥加密。由于加密算法通常是可知的，无密钥加密主要是防止普通人窥探信息，但往往容易被别有用心的人得到并解密。如火车票上二维码用的加密算法就是无密钥加密或固定密钥加密。

有密钥加密变换分为单密钥加密和双密钥加密两种，单密钥加密使用同一个密钥加密和解密，可以分为流密码和分组密码两种。双密钥加密又称公钥加密，使用一个密钥加密，另一个密钥解密。

在上述五个阶段中，一阶段对加密算法的要求少，可以采取比较成熟的分组密码加密算法。二、三两个阶段容易对二维码的编码造成破坏。四阶段要求加密算法不影响编码的长度，并且加密可能会对二维码的纠错能力造成影响。故这几个阶段应使用不影响加密前后信息长度的流密码。五阶段加密需要与图像处理相结合。

2.3　基于 QR 二维码的多级融合加密算法

基于 QR 二维码的多级融合加密（Multilevel Fusion Encryption）算法是指在二维码编码、解码流程中的各不同阶段进行加密，在不同阶段的加密考虑各阶段不同的要求，将加密与信息编码过程融合在一起。与仅作一次信息加密的算法相比，多级融合加密使得二维码加密无法用通常的设备读出，从而使已知密文无效。

QR 二维码生成过程可表示为

$$C=GI(ECC(IE(I)))$$

其中 C 表示二维码，I 表示信息，IE 表示信息编码，ECC 表示纠错编码，GI 表示图像生成编码。多级融合加密的密码生成阶段可表示为（只表示了二级）

$$C=GI(SC(ECC(IE(BC(I+s_1))))+s_2)$$

其中 BC 为分组密码加密，SC 为流密码加密，s_1 为可变密钥，s_2 为固定密钥。

QR 二维码的多级融合加密算法流程如下：

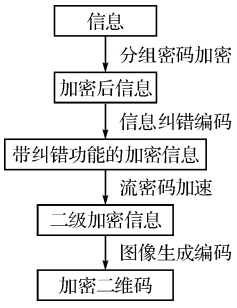

图 2　QR 二维码的多级融合加密

分组密码加密阶段需要密钥，对信息第一次加密。使用比较简单的加密方案已知可以攻破，而使用过于复杂的方案则时间复杂性陡增。利用二维码的流程在之前使用一次或几次流密码加密，流密码的密钥固定在程序中，并利用网络按时更新密钥，这使得常

见的方法难以攻破加密系统。

加密的过程是可逆的。由于经过纠错编码后信息带有纠错功能,所以之后的流密码加密可能对纠错功能造成一定影响。

3 加密 QR 二维码算法实现

QR 二维码测试系统使用 Matlab R2012a 实现。界面如图 3 所示。

图 3 QR 二维码测试系统

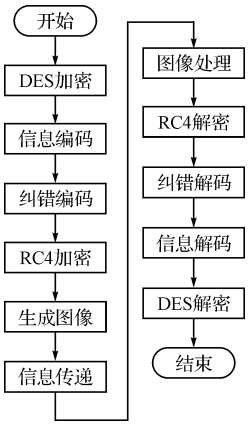

图 4 加密系统流程图

系统采用分别在第一和第四阶段加密。在一阶段信息编码之前加密,对加密算法的要求比较宽泛,可以使用适于信息编码的比较完善的加密算法,这里使用 DES 分组密码。在四阶段加密要求加密后的长度需要固定或接近且尽量不能影响纠错编码的纠错性能,因此选择固定密钥的流密码算法。这里使用了 RC4 算法[8],这样加密后的信息与加密前等长。DES 密码可以任意设置,RC4 使用简单的密钥,使用伪随机子密码生成算法()可以自动扩展密码。

加密系统流程如图 4 所示。

经过测试,加密后的 QR 二维码可以并且只能被解密系统识别。经过对 20 个加密后二维码进行简单的遮挡、加噪测试,认为加密对 QR 二维码的纠错功能不造成影响。测试使用的部分图形如图 5 所示。

图 5 测试使用的部分图形

分别对无加密,只有 DES 一级加密和二级融合加密的 QR 二维码各 10 个进行测试,取其平均值,测试结果如表 1 所示。

表 1 加密测试实验数据表

	无加密	一级加密	二级加密
码长/位(bit)	807	1079	1079
编码时间/秒(s)	3.51	4.58	4.61
解码时间/秒(s)	3.75	4.70	4.81

4 结语

QR 二维码实现过程中有多个阶段可加入加密措施,不同阶段对加密算法有不同要求。多级融合加密算法可以充分利用二维码的复杂流程,让破解更难进行,保证了加密二维码的安全性。

参 考 文 献

[1] CN-GB. 快速响应矩阵码[S]. 2000.
CN-GB. Quick Response Matrix Code[S]. 2000.

[2] 中国物品编码中心. 二维条码技术与应用[M]. 2007,7.
GS1 China. Two Dimensional Bar Code Technology and Application[M]. 2007,7.

[3] 刘云龙,吕韬,曾晋,等. 基于 android 手机的加密 QR 二维码识别系统[J]. 软件,2012,33(4):34-36.
LIU Yunlong, LV Tao, ZENG Jin, *et al*. Encrypted QR Code Recognition System Based on Android Mobile Phone[J]. 2012,33(4):34-36.

[4] 任勇金. 基于 Rijndae 和异或运算的 QR 二维码双重加密研究[J]. 华章,2012(29):338.
REN Yongjin. Research on QR Code Double Encryption Based on Rijndae and XOR Operation[J]. Magnificent Writing,2012(29):338.

[5] 高彦受. QR 二维码的安全实现与设计分析[D]. 南京理工大学,2013.
GAO Shouyan. Design and implementation of QR two-dimensional code[D]. Nanjing University of Science & Technology,2013.

[6] 周庆,黄党志. 基于 Ising 模型的 QR 码加密算法[J]. 计算机应用,2013,33(10):2861-2864.
ZHOU Qing, HUANG Dangzhi. Encryption algorithm for QR code based on using model[J]. Journal of Computer Applications,2013,33(10):2861-2864.

[7] 单利安. QR 二维码水印加密及解密算法研究[J]. 无线互联科技,2013(10):122-123.
SHAN Li'an. Research on QR two-dimensional code watermark encryption and decryption algorithm[J]. Wireless Internet technology,2013(10):122-123.

[8] 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(理学版),2012,50(3):511-516.
HU Liang, CHI Ling, YUAN Wei, et al. Cryptanalysis and Improvements of RC4 Algorithm[J]. Journal of Jilin University (Science Edition), 2012, 50(3): 511-516.

(下转第 2395 页)

摄像机内参数可以将 3D 坐标转化为 2D 图像坐标[2,9]。内参数由变量 intrinsic_matrix 和 distortion_coeffs 构成。

外参数说明物体(棋盘)相对于摄像机的位置，由旋转和平移表征。旋转通过 cvRodrigues2()来实现，平移通过 translation_vectors 来实现。标定结果如表 1 所示。

表 1　单目摄像机的标定结果

内参数矩阵	$\begin{pmatrix} 253.433 & 0 & 127.927 \\ 0 & 159.466 & 125.102 \\ 0 & 0 & 1 \end{pmatrix}$
畸变系数	(0.120589　−1.95258　−0.028296　0.00834556)
第一幅图像的旋转向量	(1.79827　2.31843　−0.215067)
第一幅图像的平移向量	(−7.35069　−32.6347　121.299)

5) 计算像机系统的外参数[10]。需要注意的是，在采取图像时两部像机必须都是同时采集，在计算外参数的时候也必须选取同一时刻对应的图像来完成。在 OpenCV 中用 cvStereoClibrate()来实现。结果如表 2 所示。

表 2　双目摄像机标定结果

矢量名	结果
旋转矢量	om=(−0.15781　−0.01623　0.01054)
平移矢量	T=(159.08160　−17.03331　24.85399)

6　结语

本文在双目立体视觉的基础上，介绍了摄像机标定的原理、畸变的矫正、双目摄像机标定的原理和基于 OpenCV 的双目摄像机标定实验，最终获得了左、右两个摄像机的内外参数，以及两个摄像机之间的关系参数，最终完成了双目摄像机的标定，从而为三维立体重建等技术的研究奠定了基础。

参 考 文 献

[1] 于仕琪，宋瑞祯. 学习 OpenCV[M]. 北京：清华大学出版社，2009：406-432.
YU Shiqi, SONG Ruizhen. Study OpenCV[M]. Beijing: Tsinghua University press, 2009: 406-432.

[2] 陈胜勇，刘盛. 基于 OpenCV 的计算机视觉技术实现[M]. 北京：科学出版社，2008：364-383.
CHEN Shengyong, LIU Sheng. Computer vision technology OpenCV implementation based on[M]. Beijing: Science Press, 2008: 364-383.

[3] 赵鹏. 机器视觉理论及应用[M]. 北京：电子工业出版社，2011：20-23，64-68.
ZHAO Peng. The theory of machine vision and application[M]. Beijing: Publishing House of electronics industry, 2011: 20-23, 64-68.

[4] 蓝福明. 双目立体视觉的摄像机标定与特征点匹配技术研究[D]. 广州：广东工业大学，2013.
LAN Fuming. The camera calibration of binocular stereo vision and feature point matching[D]. Guangzhou: Guangdong University of Technology, 2013.

[5] 罗桂斌. 双目立体视觉深度感知与三维重建若干问题研究[D]. 长沙：中南大学，2012.
LUO Guibin. The binocular stereo vision depth perception and 3D reconstruction based on some problems of [D]. Changsha: Central South University, 2012.

[6] 熊凡. 双目立体视觉系统标定及重构方法研究[D]. 长沙：湖南工程大学，2012.
XIONG Fan. study of binocular stereo vision system calibration and reconstructionmethods[D]. Changsha: Hunan University of engineering, 2012.

[7] 赵小松. 摄像机标定技术的研究[J]. 机械工程学报，2002，38(3)：149-151.
ZHAO Xiaosong. Study on camera calibration technology[J]. Journal of mechanical engineering, 2002, 38(3): 149-151.

[8] 李斌，史忠科. 基于计算机视觉的行人检测技术的发展[J]. 计算机工程与设计，2005，26(10)：2565-2568.
LI Bin, Shi zhongke. [J]. computer engineering and design development of pedestrian detection based on computer vision, 2005, 26(10): 2565-2568.

[9] Zhang Z. A flexible new technique for camera calibration[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2000, 22(11): 1330-1334.

[10] Gibson S, Cook J, Howard T, et al. Accurate camera calibration for off-line, video-based augmented reality [C]//Proceedings of the IEEE and ACM International Symposium on Mixed and Augmented Reality, 2002: 37-46.

(上接第 2364 页)

[9] 李琴，曾凡平. RC4 密码的改进方法及其性能分析[J]. 计算机工程，2008，34(18)：181-183.
LI Qin, ZENG Fanping. Improved RC4 Cipher Method and Its Performance Analysis[J]. Computer Engineering, 2008, 34(18): 181-183.

[10] 宋维平. 流密码与 RC4 算法[J]. 吉林师范大学学报(自然科学版)，2005，26(2)：71-72.
SONG Weiping. The Stream Cipher of Symmetrical Ciphers[J]. Jilin Normal University Journal(Natural Science Edition), 2005, 26(2): 71-72.