大连理工大学本科毕业设计（论文）

二维码的信息隐藏技术

Information Hiding Techniques in QR Code

学 院（系）：电子信息与电气工程学部

专　　业：电子信息工程

学 生 姓 名：王晨曦

学　　号：201181371

指 导 教 师：王波

评 阅 教 师：李建华

完 成 日 期：2015 年 6 月 13 日

大连理工大学

Dalian University of Technology

摘　要

21 世纪以来，随着计算机网络与通信技术的快速发展，信息安全问题日益引起人们的广泛关注，而在信息安全领域存在一个非常重要的分支----信息隐藏技术；信息隐藏技术主要包括隐写术与数字水印两大应用较为广泛的分支，其基本特征包括安全性、不可见性、嵌入容量和鲁棒性等。本文主要研究并利用当前非常流行的 QR 二维码技术作为信息隐藏的载体来实现秘密信息的隐藏与传递，属于上述两大分支中的隐写术，并且综合考虑 QR 二维码的技术原理，重点关注其嵌入容量与安全性的问题。

本文设计了一个利用 QR 二维码作为信息隐藏的载体来进行秘密信息的嵌入与提取的系统。其中，针对 QR 二维码的编码原理，选用压缩编码方法中的零阶自适应算术编码方法并进行一定程度上的改进使其更适合本系统，首先对秘密信息进行一定程度的压缩，从而提高嵌入容量。通信双方可以按照事先约定的密钥来完成秘密信息的嵌入与提取，并且密钥的选择非常方便。同时针对安全性的问题，设计并实现了第二种方案，以损失一定的嵌入容量为代价，并以嵌入秘密信息后所引起的 QR 二维码的失真最小为最优策略指标，在一定程度上可以减少 QR 二维码的失真，从而提高安全性。整个系统使用 MATLAB GUI 编程实现，在不影响 QR 二维码原始信息正常扫描的情况下，按照既定的标准实现了秘密信息的隐藏与传递。

关键词：信息隐藏；QR 二维码；隐写术；嵌入容量；安全性

Information Hiding Techniques in QR Code

Abstract

Since the 21st century, with the rapid development of computer network and communication technology, information security has gradually attracted many people's eyes. And in the field of information security, there exists a very important branch----information hiding technology. Information hiding technology mainly includes two widely used branches of steganography and digital watermarking technology and its basic features include security, invisibility, embedding capacity and robustness etc. The main study in this paper is to use the QR code technology which is with high popularity currently as the information hiding cover to hide and transfer secret information, belonging to steganography of the two branches. Considering the theory of QR code technology, this paper may concentrate more on the embedding capacity and security problems.

In this paper, a system of the embedding and extraction of the hidden information is designed, which is based on the QR code image as the information hiding cover. According to the theory of QR code, a selection of compression coding method of Zero-Arithenco method which is improved to make it more suitable for the system is made, so as to improve the embedding capacity. The two parties can complete the embedding and extraction of the secret information according to the agreed key, and the key is quite convenient. Also according to the security problem, this paper has designed a second scheme. At a cost of certain embedding capacity, the second scheme can reduce the distortion of the cover to some extent, so as to improve security. The whole system is completed by MATLAB GUI programming, and the secret information can be extracted in terms of no affecting of the normal scanning of the original information in QR code.

Key Words： information hiding; QR code; steganography; embedding capacity; security

目　　录

1 绪论

二维码技术是一种综合商品管理与流通、编码、差错控制、图像、印刷、光学扫描与识别等多种技术的条码技术，它的前身便是传统的一维条码。同时在人类步入信息时代的今天，信息安全、信息隐藏等概念已然并不陌生，尤其是自美国发生“911 事件”以来，各国加大信息隐藏等技术的研究力度，并逐步发展成为一门新兴学科[1]。鉴于目前 QR 二维码技术的流行和普遍应用，本文主要研究并利用 QR 二维码作为信息隐藏的载体来实现秘密信息的隐藏与传递，属于信息隐藏领域中的隐写术范畴，并且综合考虑 QR 二维码技术的编解码原理，重点关注其嵌入容量与安全性的问题。

1.1 研究背景与意义

1.1.1 信息隐藏概述

21 世纪的人类社会开始步入信息时代，然而随着计算机网络与通信技术的快速发展，信息安全问题逐渐成为当前研究的热点问题，例如与人们的现实生活密切相关的个人隐私的保护、数字作品的版权保护等问题。其中在信息安全领域存在一个非常重要的分支----信息隐藏技术，鉴于传统的基于密码学的加密技术更加着重于保护秘密信息本身，很容易暴露秘密信息的存在性和消息的重要性，同时对于某些特殊职业如情报工作者等难以发挥其作用，各种新型的信息隐藏技术不断被研究和开发应用，逐渐发展成为一门新兴学科。信息隐藏技术根据不同的标准具有不同的分类情况，如图 1. 1 所示，其中根据使用方式的不同主要分为隐写术和数字水印两大应用较为广泛的分支，其中隐写术主要应用于秘密通信方面，而数字水印技术主要应用于数字多媒体的版权保护等方面，基本特征包括隐蔽性、安全性、鲁棒性和嵌入容量等[2]。

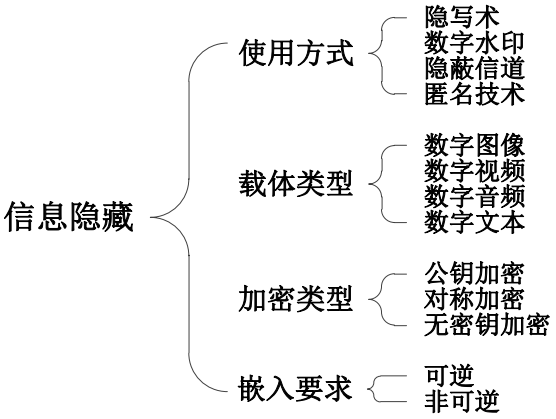

图 1.1 信息隐藏的分类

1.1.2 隐写术

有关隐写术的应用古已有之，非常经典的例如：中国诗体中的“藏头诗”，《水浒传》中，“及时雨”宋江和“智多星”吴用就曾使用这种手段拉拢卢俊义上山；而在古罗马时期，有人把奴隶的头发剃光，然后将情报刺在头皮上，待头发再生之后，便可以达到秘密隐藏与传递消息的目的。近年来，随着计算机网络与通信技术的快速发展，很多信息的表示和传递越来越多的依赖于数字多媒体，如数字图像、数字音频和数字视频等形式，而数字多媒体大多存在一定的冗余，这时采用隐写技术便可以将秘密信息嵌入到上述数字多媒体当中同时又不损坏他们的质量，这样第三方便察觉不到秘密信息的存在，从而使得各种密码和密钥、数字签名、间谍情报等秘密信息都可以在开放的环境（如因特网、无线通信）下进行安全的传输[3]。

隐写术与传统的加密技术是实现秘密通信的两种重要技术，而其中最根本的区别在于：传统的加密技术以密码学为根基，通过将明文信息转换为密文信息，使得即使消息被第三方所非法获取，也无法获取消息的实质内容，从而保证了信息的安全性，其中最经典的应用实例莫过于二战时期的情报工作；但加密技术的缺点异常明显，第一，第三方很容易发现消息的存在，并采取一定的措施对其进行篡改和拦截，致使传输失败，第二，随着计算机技术的超高速发展，普通的加密技术非常容易被攻破，而研究绝对安全的加密算法是相当困难的。当前形势下，隐写术巧妙的避开了加密技术的缺点，通过隐藏秘密信息的存在性，达到秘密通信的目的，具有非常广阔的发展前景。

隐写术同样存在众多分支，在数字图像方面，当前研究的主要内容在于以彩色图像与灰度图像为载体来进行信息的隐写等方面，鉴于 QR 二维码技术的流行，本文主要研究利用 QR 二维码图像作为信息隐藏载体的隐写术。

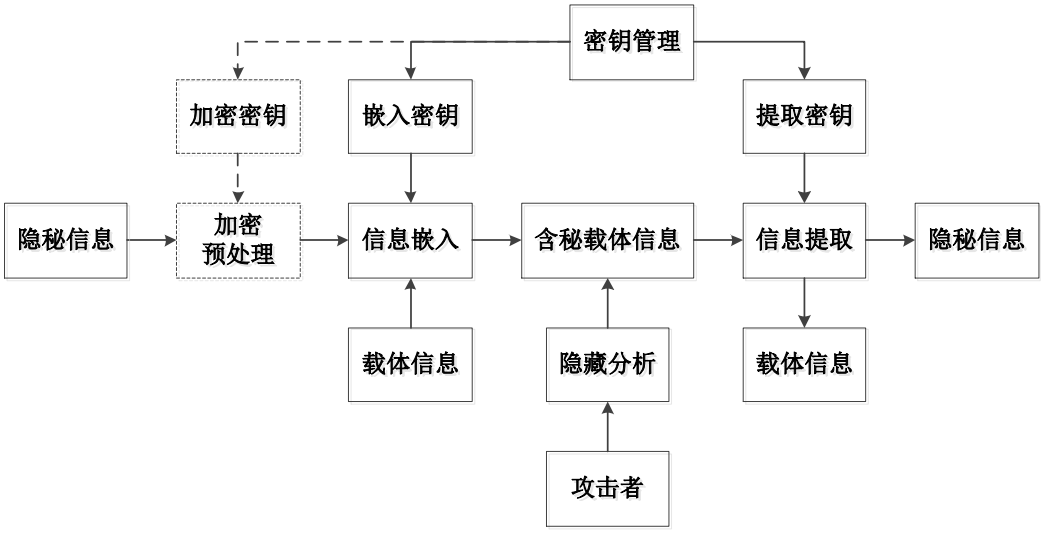

图 1.2　隐写术实现基本流程图

1.1.3 QR 二维码技术

QR 二维码好像是突然流行开来，遍布生活的每个角落，如活动和广告宣传、微信二维码名片、火车票等都可以见到它的身影，而利用智能手机扫码来获取信息的行为已然十分普遍，QR 二维码究竟具备什么样的特性致使它的发展如雨后春笋般迅速？

事实上人们在商场进行购物的过程中都会发现商品上印有一种条码，进行结账时售货员会使用专用的扫描设备对其进行扫描然后得到商品的价格、来源等信息，而这种条码便是一维码，甚至有的人会根据所购买的商品上是否印有条码来判断商品的真伪，虽然这种做法是错误的，因为条码不具备任何的防伪功能。一维条码的广泛应用为商品的流通和管理带来了极大的方便，然而一维条码存在一些固有的缺点，如可以存储的信息量有限、仅支持字母和数字编码、对数据库和网络的依赖性强等，因此人们对于条码技术的研究也在不断跟进。鉴于传统的一维条码仅仅在水平方向上存储信息而在垂直方向上不存储任何信息，对空间的利用存在浪费，二维码技术逐渐发展成熟；二维码由于在水平方向上可以携带信息，极大的增加了编码容量，而在此基础上，支持的字符集也更加丰富如中文字符等，同时引入差错控制编码方法，使得二维码在遭受一定的污损、破坏之后仍可正确解码，而这些都是传统的一维条码所无法做到的。二维码还存在一个令传统的条码技术设计思想脱胎换骨的根本特点，就是如果一维条码仅仅是对物品进行简单的代号标识，那么二维码就是对商品细节的描述，并且甚至可以脱离商品而独立存在如用于简单的通信和身份认证。表 1.1 中列出了一维码与二维码的优缺点比较情况，可以更为直观的看到二维码技术的优势所在。

表 1.1　一维码与二维码的优缺点比较

	信息密度与容量	错误校验与纠错	垂直方向是否携带信息	用途	对后台数据库与网络的依赖	识读设备
一维码	密度低 容量小	可校验 无纠错	不携带	商品标识	后台支撑	专用条码扫描器
二维码	密度高 容量大	可校验 可纠错	携带	商品描述	独立应用	智能手机等

近年来，各国的信息技术和商业自动化管理产业得到了迅速发展，而在信息技术产业和商业自动化管理需求的带动下，作为信息数据自动采集的重要手段之一的二维条码技术得到了快速推广与应用，尤其是智能手机的普及，为二维码的平民化、日常化提供了可靠而方便的平台。因此，针对二维码技术的研究已经成为各国国民信息化发展的必然趋势[4]。

图 1.3　各种商标上常见的条形码

图 1.4　PDF417 型二维码

图 1.5　QR 二维码

二维码主要分为行排式和矩阵式两种，其中比较典型且应用最为广泛的主要有如图 1.4 所示的 PDF417 型二维码就是一种行排式二维码，它看起来就是一维条码在垂直方向上简单的压缩堆积，因此又叫堆叠式二维码，如图 1.5 所示的 QR 二维码为矩阵式二维码，它的编码方式已经不再局限于传统的一维条码的设计思想，而是利用图像像素来存储编码信息，QR 来自英文“Quick Response”，它拥有二维码技术的所有优势，同时不再使用原来线性扫描的工作方式而是使用经红外光增强的摄像头，扫码软件会自动识别视场内的 QR 二维码，且无需对准，无论以何种角度，资料均可被正确读取，同时也正是基于这点才使得智能手机成为 QR 码应用普及的重要平台，二者可谓相辅相成。鉴于 QR 码不论是相对于一维条码还是普通的二维码都具有相当的优势且应用最为广泛，本文主要研究 QR 二维码[5]。

1.2 国内外研究现状

迄今为止，数字图像的隐写技术虽然仍未发展完善，但人们已经研究并提出了多种成功的隐写算法，同时对隐写分析的研究也在不断发展，并且取得了显著成效。按照嵌入域的划分，隐写算法基本可以分为空间域和变换域两类，空间域上最经典的嵌入算法就是 LSB 算法，其他的还有位平面复杂度分割隐写、PVD 隐写和 Patchwork 等主要算法，并综合利用置乱、隐蔽信道和奇偶校验等技术；变换域上主要是采用离散余弦变换和小波变换等变换方法首先对图像进行变换处理，然后在变换后的频域系数上进行秘密信息的嵌入。另一方面，上述许多算法已经被成功开发成为隐写软件工具，为数字图像的隐写带来了极大的应用方便，表 1.2 中列出了几种典型的隐写工具[6]。

表 1.2　典型的隐写工具

序号	工具	作者	主要方法	图像格式
01	EzStego	Romana Machado	LSB 方法	GIF
02	DCT-Steg	Stefan Katzenbeisser	DCT 系数修改	JPEG
03	BMP Secrets		空域替换法	JPEG、GIF、BMP
04	Hide and Seek 95 v1.1	Colin Moroney	空域 LSB 方法	BMP
05	F5 V F0.9	Andreas Wachado	修改量化后的 DCT 系数	JPEG、GIF、BMP
06	OutGuess	Niels Provos	修改量化后的 DCT 系数	JPEG、PNM
07	Jsteg Shell	John Korejwa	修改量化后的 DCT 系数	输出 JPEG
08	Jsteg Jpeg	Derek Upham	修改量化后的 DCT 系数	输出 JPEG
09	JPHSWin	Allan Latharn	修改量化后的 DCT 系数	JPEG
10	JP Hide and Seek	Allan Latharn	修改量化后的 DCT 系数	JPEG

在 QR 二维码的应用方面，当前的主要研究内容是 QR 二维码技术与数字水印技术

相结合，从而达到数字作品的版权保护、商品追踪与制作防伪标签等目的，主要从下几个角度进行研究：一是，把水印信息当作编码信息生成相应的 QR 二维码，然后直接进行传输；二是，直接把 QR 二维码图像当作数字水印嵌入数字图像之中，同时利用 QR 二维码图像的高纠错特性，提高数字水印的鲁棒性，主要用于数字作品的版权保护等方面；三是，把 QR 二维码图像当作载体图像嵌入不可见的数字水印，主要用于商品流通方面防伪标签的制作[7]。

1.3 本文的主要工作

本文主要从以下几个方面开展研究工作：

一、简单了解信息隐藏和 QR 二维码技术的相关研究背景；

二、根据国家标准文献 GB/T 18284-2000 中制定的 QR 二维码国家标准，对 QR 二维码的定义、约定、符号描述、数据编码与符号表示、结构链接、符号印制、符号质量、译码过程等相关内容进行较为充分的了解；

三、重点研究 QR 二维码的纠错原理，确定纠错容量，为系统设计提供参考；

四、重点研究 QR 二维码符号的字符布置，研究其中的规律；

五、研究压缩编码方法中的零阶自适应算术编码，并且在一定程度上作出必要的改进以适应本系统；

六、设计实现具体的基于 QR 二维码的信息隐藏技术方案，并使用 MATLAB GUI 编程实现，然后对信息隐藏的方案进行简单评价，主要包括嵌入容量、安全性等内容。

从 QR 二维码的编解码原理可以看到，只要稍微修改一下字符布置规律，就会产生一种新型的 QR 二维码标准，而相应的只要修改部分编解码程序即可；同时，由于 QR 二维码本身不具有观赏性，有很多应用正在或者已经开发了美化 QR 二维码的功能，比如加入颜色、形状变化等，这更加使得 QR 二维码的形式五花八门，没有统一的标准，这对本文的研究是非常不利的。基于上述原因，本文最终选择按照我国在 2000 年发布、2001 年开始实施的快速响应矩阵码（即 QR 二维码）的国家标准 GB/T 18284—2000 中所讲述的编解码原理与规则来进行本文的研究，这样做的好处是，尽管 QR 二维码的形式可以有很多种，但其最基本的原理是相通的，因此，选择研究其中的一种标准所得出的结论基本适合其他的形式，只要到时按照需要稍加改动即可，避免了不必要的麻烦。同时由于工作量与时间的限制，对 QR 二维码的 40 种版本一一进行研究并实现是不太现实的，这是一个大工程。

本文通过综合以下多方面的考虑，仅完成了对 QR 二维码的前 5 个版本的研究与实现：首先前 5 个版本的工作量是合适的；其次，鉴于目前微信平台的流行，微信二维码

名片、微信扫一扫等应用已十分普遍，而微信二维码采用的规格正是 QR 二维码的第 5 个版本，因此对于第 5 个版本的研究就显得特别有意义，同时，普通的带有网址链接的 QR 二维码比如 App 应用商店的手机应用链接，其版本一般为第 2、3 和 4 个版本，也就是说对于这三个版本的应用也是非常广泛的，而对于第 1 个版本，由于其结构最为简单，比较适合用在研究的初期阶段，比如对方案、算法等进行可行性的测试，优化程序结构等；第三，本文的主要目的是找到合适的方案、算法以实现信息隐藏的目的，而并非一项工程问题。最后的研究成果表明，这种取舍是必要的。

本文设计了一个利用 QR 二维码图像作为信息隐藏的载体来进行秘密信息的嵌入与提取的系统，基于不同的考虑一共设计并实现了两种方案，最后在不影响 QR 二维码原始信息正常扫描的前提下，按照既定的标准实现了秘密信息的隐藏与传递。整个系统使用 MATLAB GUI 编程实现，并着重于研究算法的普适性与可扩展性，而如果要完成全部的工程，只需要按照相同的方法完成各版本函数的编写然后直接添加即可，无需修改任何主函数或调用部分；通过这次课题研究，本人对于 MATLAB GUI 编程有了更多的心得体会，并且在系统的程序设计上制作了一些小花样，但是由于毕竟对课题本身的研究没有什么实质性的帮助与提升，因此这里与后文均不再提及。

1.4 本文的组织安排

本文总共分为四章，具体的组织安排情况如下：

第一章：绪论，主要介绍了信息隐藏技术、隐写术的研究背景和 QR 二维码技术的发展现状，然后简单介绍本文的主要工作；

第二章：QR 二维码的编解码原理，主要介绍了 QR 码符号的基本组成结构和相关概念、QR 码的纠错原理以及 QR 码符号的字符布置规则；

第三章：基于 QR 二维码的信息隐藏的方案设计，主要介绍了基于第二章所述基本原理的具体方案的设计与实现，在对秘密信息进行压缩编码的基础上，一共设计并实现了两种方案，第一种方案重点关注信息隐藏系统的嵌入容量问题，而第二种方案以损失部分嵌入容量为代价，重点考虑系统的安全性问题；

第四章：数据分析与方案评价，通过设计一系列的实验，确定算法的嵌入容量并对两种方案进行安全性的分析对比；

本文最后是研究过程中所引用的参考文献和致谢。

2 QR 二维码的编解码原理

QR 二维码的编解码综合了编码、差错控制、图像、印刷、光学扫描与识别等多种技术，而本文主要研究的是如何利用 QR 二维码来进行信息隐藏，因此无需关注 QR 二维码编解码的所有细节，本章首先会在 2.1 节中对 QR 二维码的编解码过程进行一下简单的介绍，然后重点介绍对本文的研究至关重要的部分。

2.1 QR 二维码的编解码方法概述

每个 QR 码符号都是由最基本的正方形模块组成的一个正方形阵列，它包括功能图形和数据编码区域，其中功能图形由寻像图形、分隔符、定位图形和校正图形组成，不用于数据编码，符号的四周为空白区。图 2.1 为以 QR 码版本 7 符号为例的 QR 码符号的结构图[8]。每个正方形模块代表一个比特，一般情况下，黑色模块代表 0，而白色模块代表 1；如果从数字图像的角度看，每个正方形模块可以对应 1 个、4 个、9 个或 16 个（等依次类推）像素点。

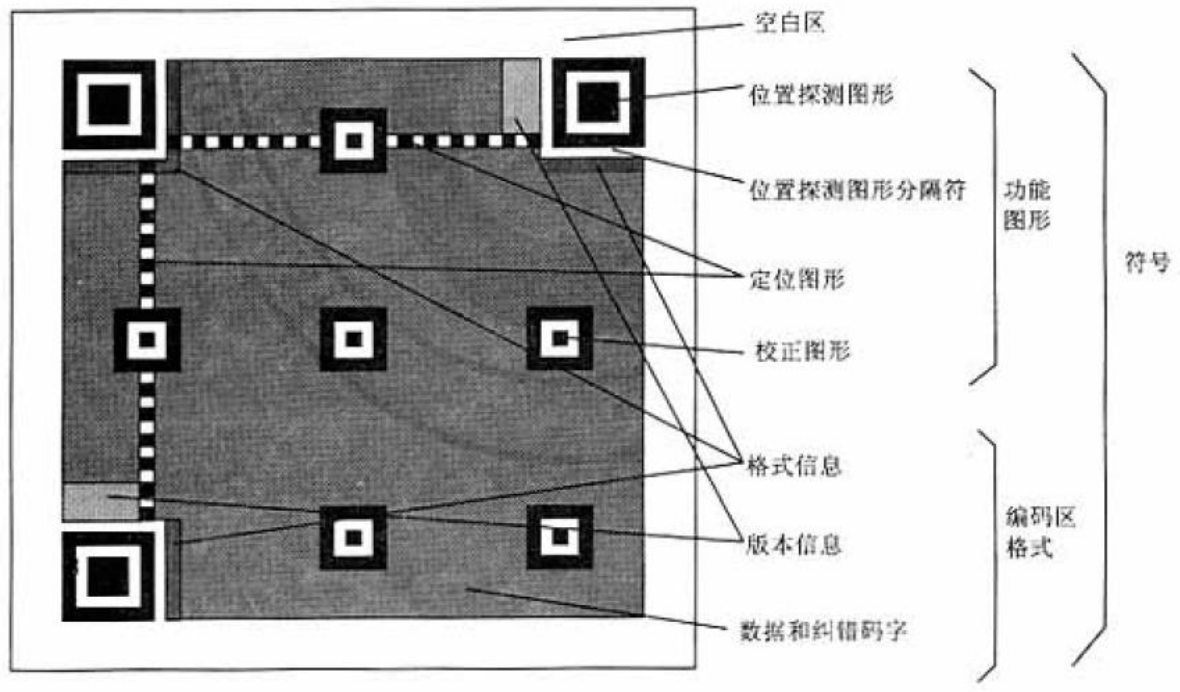

图 2.1 QR 码符号的结构

QR 码符号共有 40 中规格，分别为版本 1、版本 2、…、版本 40。版本 1 的规格为 21×21 模块，版本 2 为 25×25 模块，以此类推，每一个版本符号均比前一个版本每边

增加 4 个模块，直至版本 40，其规格为 177×177 模块，空白区最少要占四个模块宽度（实际上没有这么严格），但并未计入上述规格。通常情况下，QR 码大多是由黑白二色的基本模块组成，而事实上不一定只能是黑白二色，只要保证足够的对比度即可，下面用深色和浅色模块分别对应黑色和白色模块。由于本文主要研究 QR 码的信息隐藏技术，因此无需关注 QR 码的所有细节，故接下来的章节将主要介绍对于本文的研究至关重要的部分。下面简单介绍一下 QR 码各个区域的作用，并且为了尽量保证 QR 码的快速识别特性，一般希望在任何情况下都不对功能图形和格式、版本信息做出任何改变。图 2.2 为 QR 二维码的编解码流程图。

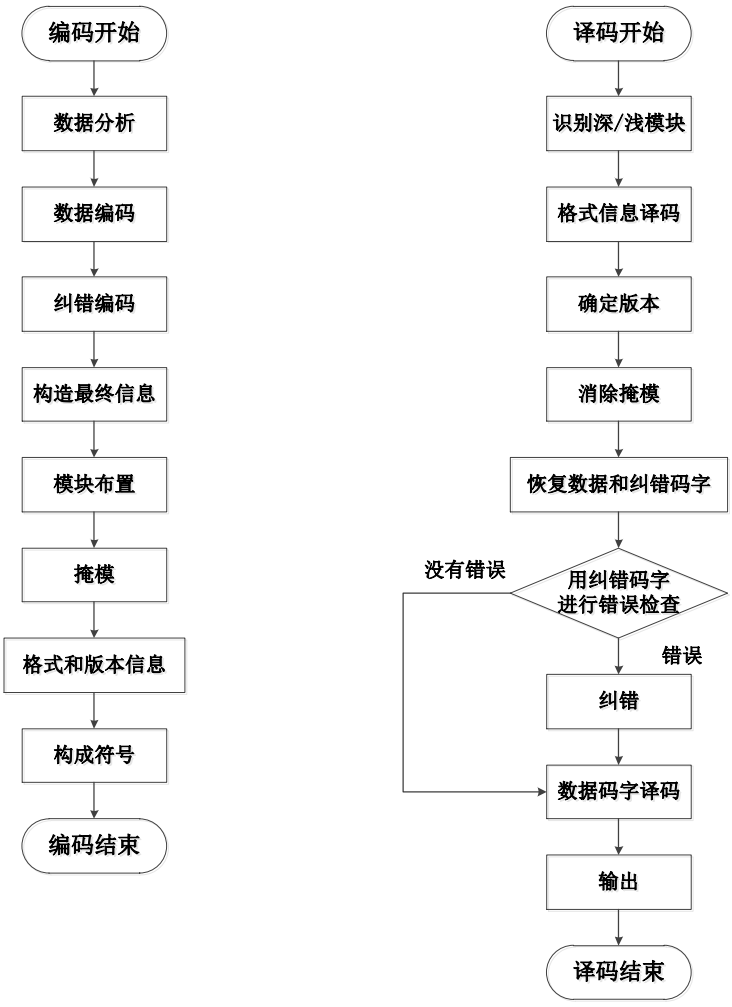

图 2.2　QR 码的编解码流程图

寻像图形：包括三个相同的位置探测图形，分别位于符号的左上角、右上角和左下角，如图 2.1 所示，每个位置探测图形可以看作由 3 个重叠的同心正方形组成，其规格

分别为 7×7 个深色模块、5×5 个浅色模块和 3×3 个深色模块，主要作用是在视场中迅速识别可能的 QR 码符号，并确定符号的位置和方向；

分隔符：每个位置探测图形和编码区域之间均有宽度为 1 个模块的分隔符，如图 2.1 所示，并且全部由浅色模块组成；

定位图形：水平和垂直定位图形分别为一个模块宽的一行和一列，由深色和浅色模块交替组成，且其开始和结尾均为深色模块，如图 2.1 所示，作用是确定符号的密度和版本，并提供决定模块坐标的基准位置；

校正图形：每个校正图形均可以看作由 3 个重叠的同心正方形组成，其规格分别为 5×5 个深色模块、3×3 个浅色模块和一个位于中心的深色模块组成，校正图形的分布情况视符号的版本而定，详情可参考有关文献；

版本和格式信息：用于存储符号的版本、纠错等级和其他有关信息；

数据和纠错码字：真正的数据编码区，本文所做的所有工作都是在这个区域上面进行的。

2.2 QR 码的纠错原理

QR 码采用了迦罗华域 GF(2^8)中的 RS 算法进行差错控制，而在本文中无需知道非常细节的 RS 编解码方法，只需要知道 RS 算法是一种纠错能力非常强的差控编码方法，而纠错能力的提升必然以增加一定的冗余为代价。本文正是利用了这种高冗余性进行设计信息隐藏系统的嵌入容量标准，从而达到隐写的目的，同时又不影响原始 QR 二维码信息的正常读取。实验结果证明，这是一种正确的思路，并且几乎可以达到 QR 码的嵌入容量极限。

确定版本和纠错等级后，功能图形和版本与格式信息的分布情况随之确定，而上节提到，为了保证 QR 码的快速识别特性，需要保证不对这些区域做出任何改变，下面重点介绍 QR 码数据区的相关内容。QR 码首先采用一定的方法将待编码信息转换为二进制比特流，同时分比特流为多个码字，每个码字占 8 比特，然后把所有的码字分为几个合适大小的数据块，采用伽罗华域 GF(2^8)中的 RS 算法在每个数据块内生成纠错码字，并与数据码字共同组成相应数量的纠错数据块，可以任意选取纠错容量大小以内的码字来进行信息的嵌入。

表 2.1 列出了 QR 码符号中前 5 个版本的纠错特性。由于 QR 码版本越高，码字总数越多，而相应的字符布置情况也渐趋复杂，仅仅前五 5 版本的字符布置情况便已非常繁琐，所以本系统仅设计实现了前 5 个版本的有关内容，但是其中采用的方法对于高版本的同样适用。与此同时，为了尽可能的提高嵌入容量，对每个版本也仅选取了纠错等

级最高为 H 的情况，这是因为纠错等级越高，冗余越大，相应的嵌入容量也随之增大；另外，同一版本的低纠错等级完全可以用低版本的高纠错等级替代，因为二者容量差别不大，所以针对研究与设计信息隐藏的方法来说，研究意义也不大。

表 2.1　QR 码符号前 5 个版本的纠错特性

版本	码字总数	纠错等级	纠错码字数	纠错的块数	每一块的纠错代码 (c，k，r)
1	26	L	07	1	(26,19,2)
		M	10	1	(26,16,4)
		Q	13	1	(26,13,6)
		H	17	1	(26,9,8)
2	44	L	10	1	(44,34,4)
		M	16	1	(44,28,8)
		Q	22	1	(44,22,11)
		H	28	1	(44,16,14)
3	70	L	15	1	(70,55,7)
		M	26	1	(70,44,13)
		Q	36	2	(35,17,9)
		H	44	2	(35,13,11)
4	100	L	20	1	(100,80,10)
		M	36	2	(50,32,9)
		Q	52	2	(50,24,13)
		H	64	4	(25,9,8)
5	134	L	26	1	(134,108,13)
		M	48	2	(67,43,12)
		Q	72	2，2	(33,15,9)，(34,16,9)
		H	88	2，2	(33,11,11)，(34,12,11)

1)、纠错容量小于纠错码字数的一半，以减少错误译码的可能性。

2)、约定，(c，k，r)：c=码字总数；k=数据码字数；r=纠错容量。

2.3 QR 码符号的字符布置

实际的通信系统中，在信道编解码模块采用了“交织”的方法可以将突发的连续错误转化为分散的随机错误，从而着重研究应对分散的随机错误的差错控制编码方法，而在 QR 码符号的字符布置中也采用了类似的方法。在这里要特别说明的一点是，布置字符时，首先需要知道各版本的功能图形以及格式和版本信息的字符布置，然后才可以在剩余的纠错数据块中布置字符，当然，其中也存在一定的规律，大致为版本 1 归一类，版本 2~6 归一类，版本 7~13 归一类，版本 14~20 归一类，版本 21~27 归一类，版本 28~34 归一类，版本 35~40 归一类，而其中最大的区别在于校正图形的分布以及版本和格式信息所占用的模块数的不同，阅者可自行查找相关资料。下面以版本 5-H 符号的字符布置为例说明 QR 码符号的字符布置规则，其他各版本符号的字符布置均可按照同样的规则自行画出。

首先根据表 2.1 对每个纠错数据块以及每个块中的数据和纠错码字进行编号，得到表 2.2，然后对表 2.2 按列读取得到最终的码字序列为：D1，D12，D23，D35，D2，D13，D24，D36，…D11，D22，D33，D45，D34，D46，E1，E23，E45，E67，E2，E24，E46，E68，…E22，E44，E66，E88；如果有需要（QR 码各版本符号的字符布置可能存在剩余位），则在序列最后的码字后面加上剩余位 0；然后从 QR 码符号的右下角第一个码字开始向上按列走“几”字形进行码字布置，而对于每个码字的 8 个比特模块具体如何安排，对于本文所研究的内容来说并不重要，便不再赘述。这个过程的难点在于，由于校正图形的存在，会使得排在后面的码字的轮廓呈现不规则的状况，当然也存在一定的规律，本章小结后面会给出版本 1-H~5-H 符号的详细的符号字符布置，其中的规律便一目了然了，而其他版本的字符布置情况均可按照相同的规律自行画出。

表 2.2　版本 5-H 符号的字符布置

块	数据码字					纠错码字			
块 1	D1	D2	……	D11		E1	E2	……	E22
块 2	D12	D13	……	D22		E23	E24	……	E44
块 3	D23	D24	……	D33	D34	E45	E46	……	E66
块 4	D35	D36	……	D45	D46	E67	E68	……	E88

1)、表中 D 系列代表数据码字，E 系列代表纠错码字，分别进行编号；

2)、同一版本的各个纠错数据块的大小可能不同，但不会超过 1 个码字。

采用“交织”的方法的优势在于：可以使得位于同一个纠错数据块中的码字在进行字符布置时分散开来，从而将突发的连续错误转化为分散的随机错误，“变相”提高了纠错能力。具体情况是，可以更好的应对对于 QR 码的某一局部区域进行遮挡、污损的情况，提高 QR 码在局部受损的情况下正确解码的可能性，而这也是 QR 二维码相对于原始的一维条形码的一种优势所在。

2.4 本章小结

本章主要介绍了 QR 码符号的基本组成结构和相关概念、QR 码的纠错原理以及 QR 码符号的字符布置规则，这些都是本系统中所用到的非常重要且最基本的理论基础，有关系统的设计详情请见下章。

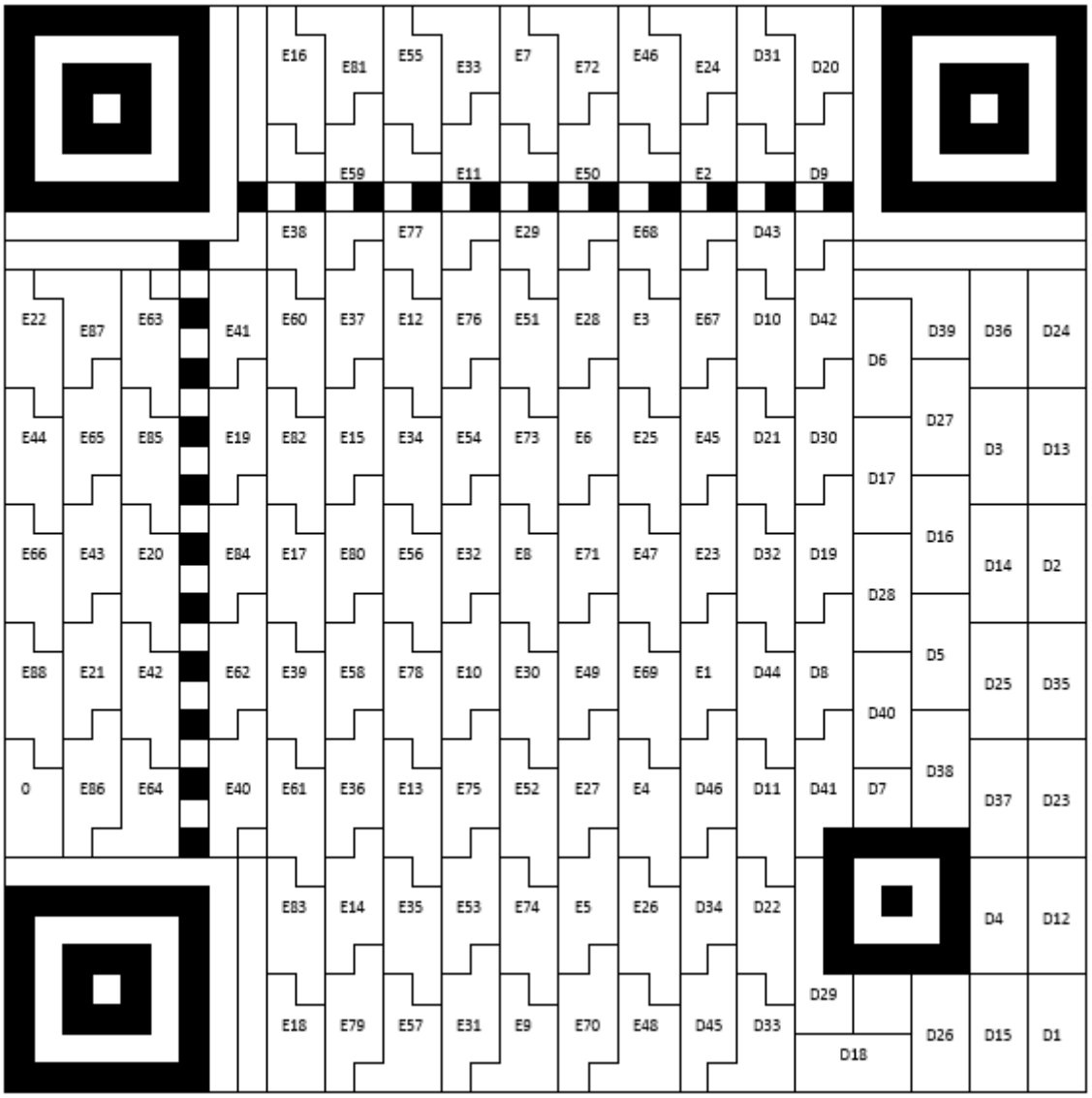

图 2.4　版本 5-H 符号的字符布置

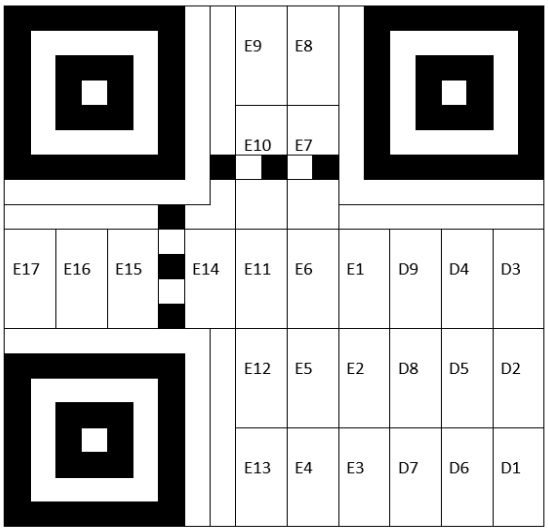

图 2.5　版本 1-H 符号的字符布置

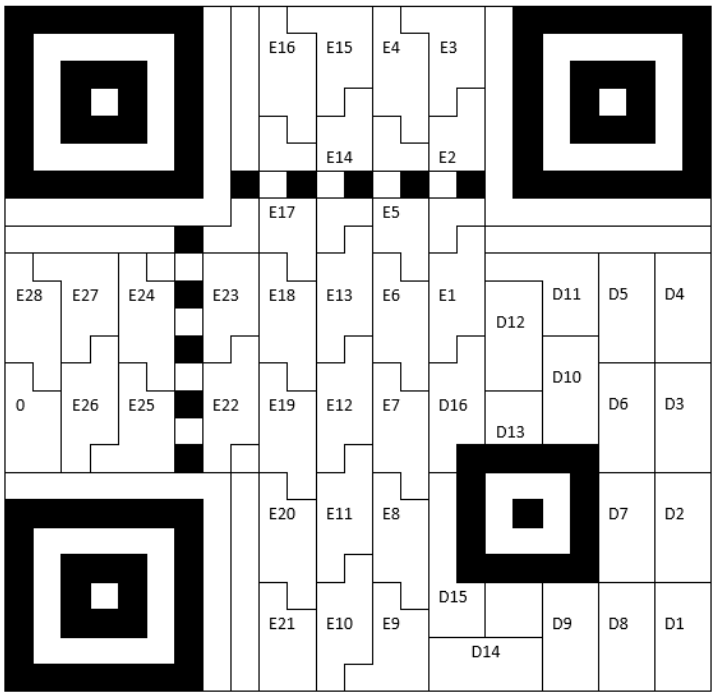

图 2.6　版本 2-H 符号的字符布置

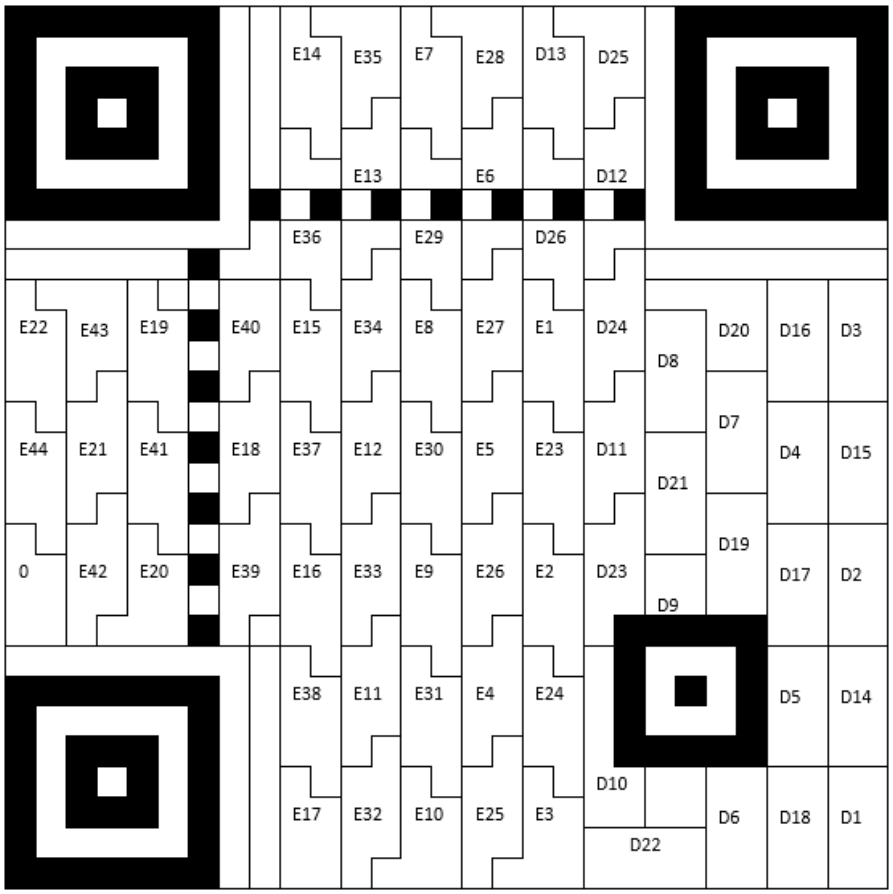

图 2.7　版本 3-H 符号的字符布置

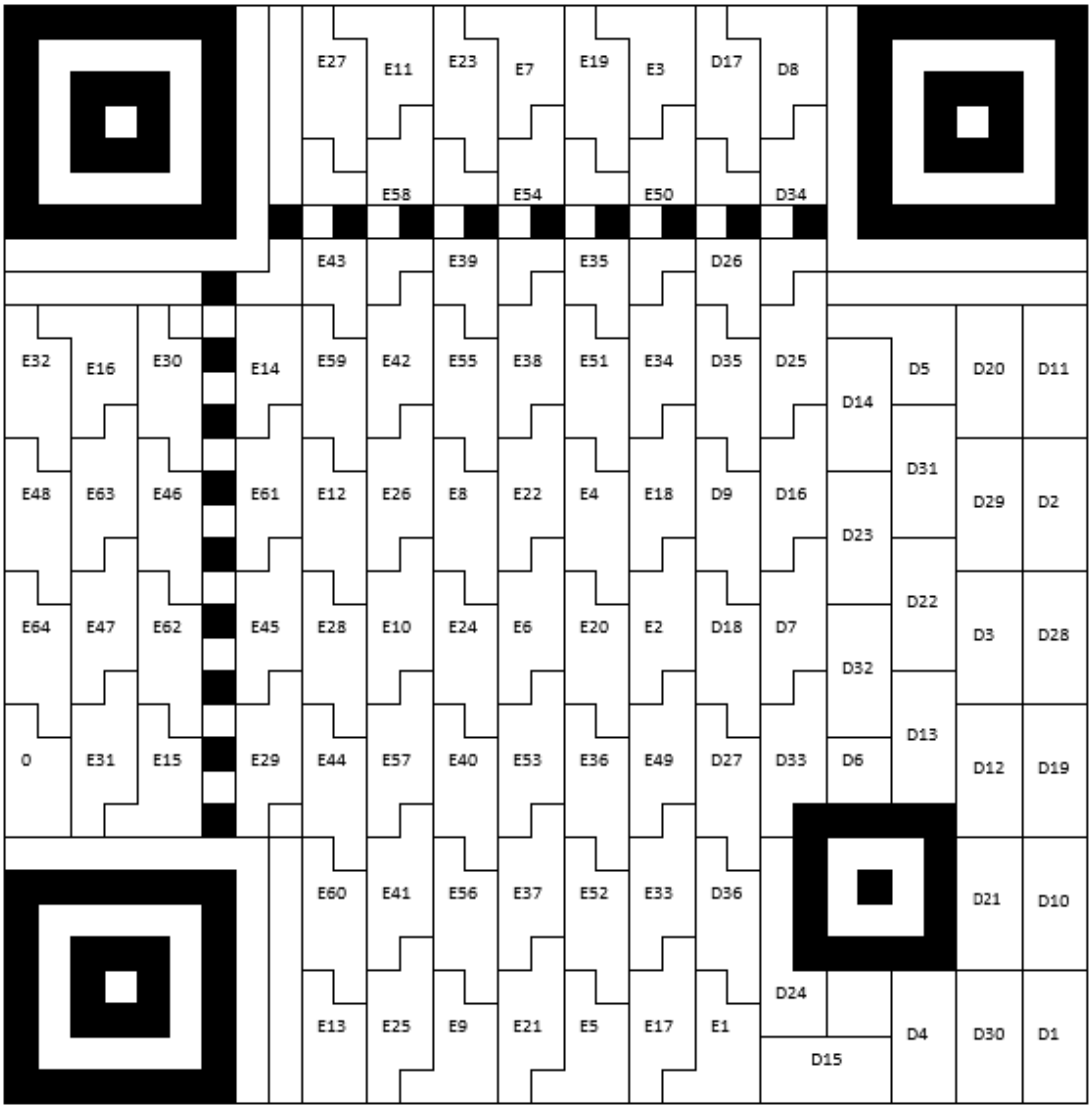

图 2.8　版本 4-H 符号的字符布置

3　基于 QR 二维码的信息隐藏的方案设计

本章主要讲解了基于第二章所述基本原理的具体方案的设计与实现，一共设计并实现了两种方案，第一种方案重点关注信息隐藏系统的嵌入容量问题；然后在第一种方案的基础上，以损失一定的嵌入容量为代价，着重研究减少嵌入秘密信息后 QR 二维码的失真问题，从而提高整个系统的安全性。

3.1　系统概述

图 3.1 为整个系统的设计流程图，图 3.2 为系统的运行主界面，接下来会重点讲解整个系统中的压缩编解码模块和信息的嵌入与提取模块两个核心模块。而在这之前有必要首先说明一些十分重要的有关数字图像简单处理的函数，这些函数的代码量要占到整个系统的 90%以上，同时为整个系统的实现奠定了非常重要的基础。

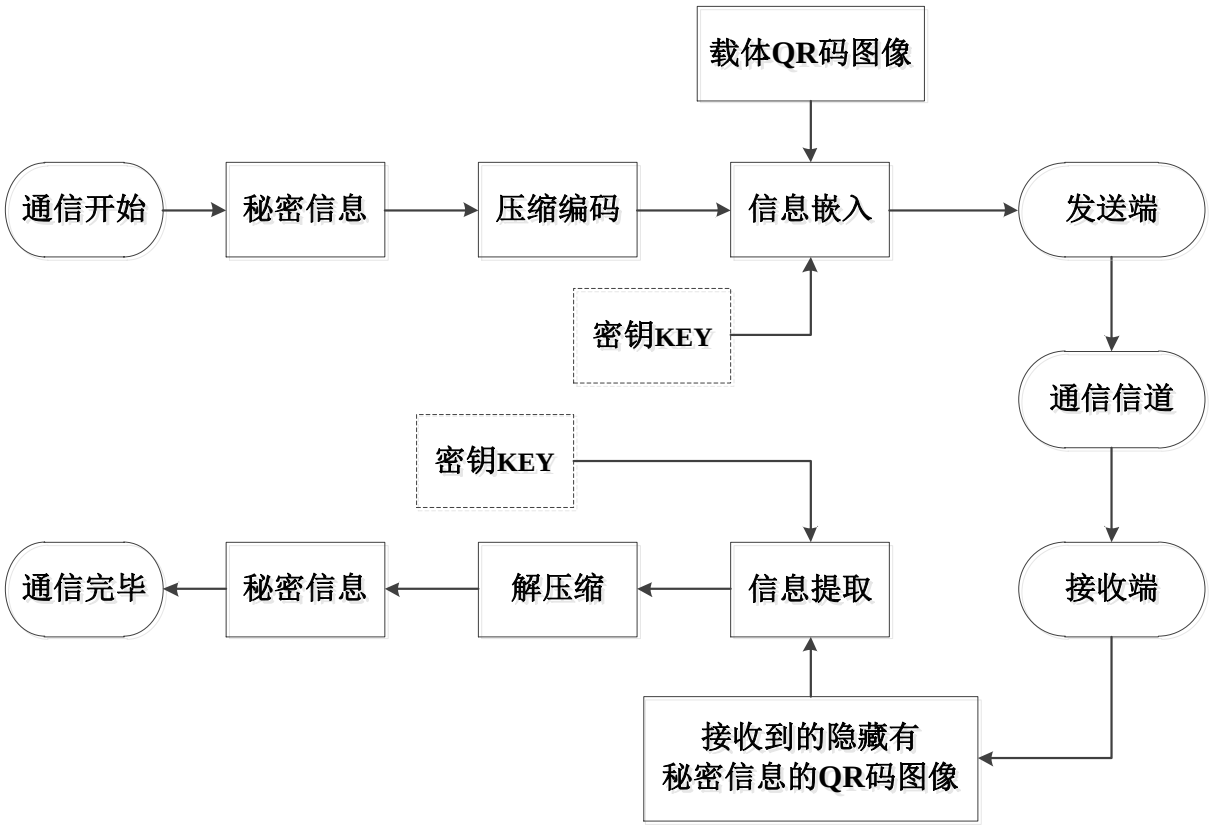

图 3.1　系统流程图

图 3.2　系统的运行主界面

[DispImage]=Version_01_En(Cover,Rep,MRM,SMf)
[DispImage]=Version_02_En(Cover,Rep,MRM,SMf)
[DispImage]=Version_03_En(Cover,Rep,MRM,SMf)
[DispImage]=Version_04_En(Cover,Rep,MRM,SMf)
[DispImage]=Version_05_En(Cover,Rep,MRM,SMf)

上述 5 个函数完成 QR 码前 5 个版本的秘密信息比特流的嵌入，Cover 代表载体 QR 码图像，Rep 代表秘密信息比特流，MRM 代表密钥矩阵，SMf 为模式标志，便于两种方案分别调用，DispImage 代表嵌入秘密信息比特流后的 QR 码图像矩阵，然后使用 imwrite()函数便可输出嵌入秘密信息后的 QR 码图像。

[Message]=Version_01_De(Rec,MRM)
[Message]=Version_02_De(Rec,MRM)
[Message]=Version_03_De(Rec,MRM)
[Message]=Version_04_De(Rec,MRM)
[Message]=Version_05_De(Rec,MRM)

上述 5 个函数完成对应的秘密信息比特流的提取，Rec 代表接收端收到的由发送端处理后的 QR 码图像矩阵，MRM 代表密钥矩阵，这个矩阵可以是事先约定的如第一种

方案便是采取这样的方法，也可以是为了减少失真由发送端的自适应算法得到的，如第二种方案，这时接收端无需知道任何有关信息，所有的信息提取工作均由后台的算法程序自行完成；Message 代表接收端提取出的信息比特流，然后由算术解码程序解码便可得到秘密信息，从而完成秘密信息的传递。下面开始具体讲述两种方案的具体设计思想，其中凡涉及到比特流的嵌入与提取，均是由上述函数实现的，不再赘述。

3.2 压缩编解码模块

3.2.1 三级压缩

三级压缩由以下函数实现：

表 3.1 相关函数与功能

名称	功能
[Warn,KEY]=Z_Str_Agree(Lim,Sel)	按约定字符集输入字符序列，并转换为约定的字符集码，同时提供必要的输入检错。
[Deliver]=Z_Agree_Str(Original)	解码得到的约定字符集序列转换为计算机可识别并输出的 ASCII 码，完成信息传递。
[DecEn,BinEn]=Sue_ArithEnco(EnSeq,Np)	零阶自适应算术编码的编码程序，Np 表示约定字符集的字符总数。
[Original]=Sue_ArithDeco(Stream,Np)	零阶自适应算术编码的解码程序，Np 表示约定字符集的字符总数。

由于整个系统是所有函数的综合搭建与调用，故许多函数参数的设定是为了实现并优化系统功能、方便主函数调用，这里不再具体说明每个参数的意义，下同。

根据第二章所讲解的原理可以知道，一旦 QR 码的版本和纠错等级确定了，冗余量便确定了，而嵌入容量也随之确定，在这种情况下如何提高嵌入容量？本文采用三级压缩的方法将秘密信息进行压缩，从而“变相”提高嵌入容量。

第一级压缩：语言压缩。首先，既然是秘密信息，自然应该是言简意赅的，而非长篇大论、五花八门，例如“US”代表“美国”，“SOS”代表“求救信号”等[9]；

第二级压缩：字符集压缩。上述前提下，使用英文大写 26 个字母、0~9 的数字和几个常用的符号便可完成信息表达，本文选定的字符集如下：｛‘@’ ‘A~Z’ ‘.’ ‘/’ ‘0~9’ ‘:’ ‘空格’ ‘!’｝共 42 个字符，其中‘!’设定为终止符，不作用户输入，且由后台程序自行添加，这样每个字符便可用$\log_2 42 \approx 6$ 个比特表示；

第三级压缩：压缩编码。本文采用零阶自适应算术编码方法对经由上述两级压缩后的秘密信息进行压缩编码，并转换为二进制比特流，最后嵌入 QR 码图像之中。

设定终止符的原因，首先终止符由后台程序自行添加，使系统的应用更为方便；其次，设定终止符后，接收端便无需知道秘密信息的长度，也不会占用不必要的嵌入容量来存储长度信息。

3.2.2 零阶自适应算术编码

为了更为直观、清晰的表述编解码原理，首先列举一个典型例子进行讲解，而实际的算术编解码系统更为复杂；然后说明本文按照实际需要所做出的改进，并主要考虑解码的唯一性以及运算的精度问题两个方面。

——例：假设某信源可以发出三种符号 A，B，C，现对符号序列 BCCB 进行零阶自适应算术编码。

过程分析：初始时刻，对A，B，C三者出现的概率一无所知，可以采用静态模型并认为三者出现的概率相等，暂定$1/3$，而这时每个字符的累积频次均为1，总累积频次为3；将区间$[0, 1)$按概率分布划分给三个字符，如下图所示：

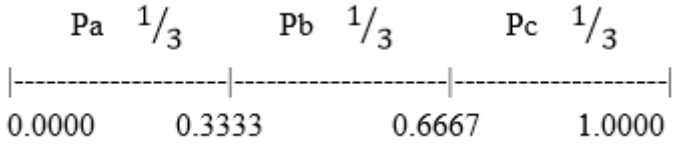

图 3.3 第 1 次概率分布

输入第一个字符 B，落入区间$[0.3333, 0.6667)$，而 B 的累积频次增加 1 变为 2，总累积频次也增加 1 变为 4，同时概率分布更新如下图所示：

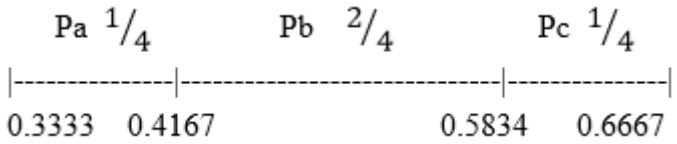

图 3.4 第 2 次概率分布

输入第二个字符 C，落入区间$[0.5834, 0.6667)$，而 C 的累积频次增加 1 变为 2，总累积频次也增加 1 变为 5，同时概率分布更新如下图所示：

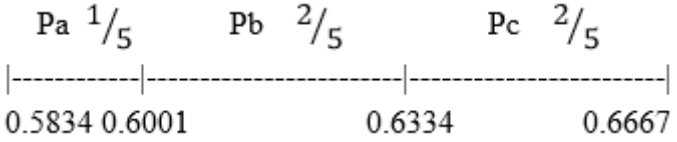

图 3.5　第 3 次概率分布

输入第三个字符 C，落入区间[0.6334, 0.6667)，而 C 的累积频次增加 1 变为 3，总累积频次也增加 1 变为 6，同时概率分布更新如图 2. 4 所示：

输入第四个字符 B，锁定区间[0.6501, 0.6667)，然后在这个区间内任意选择一个实数，例如 0.64，再将其转化为二进制小数，最后去掉小数点得到编码结果为 10100011。

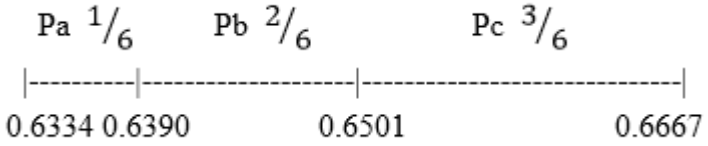

图 3.6　第 4 次概率分布

解码的过程与编码类似，首先假定信源符号 A，B，C 的初始概率均为$1/3$，然后首先将二进制小数转化为十进制小数，也就是 0.10100011B=0.64D，而这时 0.64 首先落入区间[0.3333, 0.6667)（见图 2.1），则输出一位解码 B，同时概率分布更新如图 2.2；这时 0.64 落入区间[0.5834, 0.6667)，输出一位解码 C，同时概率分布更新如图 2.3；0.64 落入区间[0.6334, 0.6667)，输出一位解码 C，同时概率分布更新如图 2.4；0.64 落入区间[0.6390, 0.6501)，输出一位解码 B；这时如果有停止位或者定长，则停止解码，得到解码序列：BCCB。

3.2.3　算法改进

显然，上述简单的编解码过程存在两个非常重要的问题：

第一，当对待编码字符序列的最后一个字符的编码结束并锁定区间后，要如何选定该区间中的某个实数作为最后的编码？而由上述编解码过程可以看出，位于区间内的任何一个实数都可以作为最后的编码，这便导致对于同一个待编码符号序列的编码不唯一；

第二，随着待编码符号序列长度的增加，这时为了保证运算精度，区间端点要保留的小数位数势必增加，如果不采用一定的手段，这也就意味着对计算机运算精度要求的提高与编解码时间的增加，而这些都是应当尽量避免的问题。

首先，对于上述第一个问题，虽然编码序列不唯一，但其实只要保证解码序列的唯一性便可达到编码的目的。一种简单的方法是，在字符集中引入终止符，这样，既然是

压缩编码，则大可选择不同编码中最短的一个作为最后的编码序列，如果最短的序列有很多，则任选一个。本文研究了一种无需引入终止符便可保证唯一解码的算法规则，会在后面进行简单介绍。

其次，对于上述第二个问题，考虑这样一种情况：假如在编码的过程当中某个字符落入了某个区间，而这个区间的两个端点的前几个小数位的数值相同，可以确定的是，编码结束后锁定的区间的两端点也一定具有相同的小数位，这时大可把这几个小数位提前提取并输出，这样每次在分布概率区间时都进行一次动态检测并输出相同的小数位，便可保证在编码过程中不会出现存储并处理一个特别长小数的情况，同时对运算精度和时间的要求也有所缓解，并且编码是实时的。

下面简单介绍一下本文研究的保证解码的唯一性的规则：由于前面采用了动态检测并提取相同小数位的方法，则最后的锁定区间的两端点的第一个小数位一定是不同的，这时左端点乘 10 向上取整，右端点乘 10 向下取整，如果差值大于 1，则最后的小数保留一位，其值为二者之间任何一个；如果差值等于 1，则左右端点同乘 100 并按相同的规则取整，如果差值大于 1，最后的小数保留两位，其值为二者之间任何一个；如果差值等于 1，则依次类推。这样，无需引入终止符便可保证解码的唯一性。特别需要注意的两点是：第一，虽然本文仍然在字符集中引入了终止符，但是引入的目的另有考虑；第二，上述规则的制定与本文所采用的解码算法是存在一定联系的，所以仅供参考，下面简单介绍一下本文采用的解码算法。

解码的过程与编码类似，值得一提的是，解码过程似乎一开始就面临处理一个非常长的小数问题，但与编码的实时性类似，解码也可以是实时的，如何实现？对 2.1.1 节列举的典例而言，考虑这样一种情况：需要解码的编码小数值为 0.64，这时如果只看第一位小数 0.6，可以确定的是，无论 0.6 后面的数值情况如何，编码小数值一定落入 $[0.6, 0.7]$的区间之内，再看概率区间的分布情况，这时$[0.6, 0.7]$跨越了两个区间，则无法判断编码小数值究竟落入哪个区间，因为截取的小数精度不足以输出一位解码；然后取前两位小数 0.64，同理，无论 0.64 后面的数值情况如何，编码小数值一定落入区间 $[0.64, 0.65]$，如果这时该区间不再跨越概率分布的多个区间而落入某一区间，则可输出一位解码，同时配合编码过程的动态检测并提取小数位的方法，便可实现解码过程的实时性，并解决了非常长的小数问题。

本文便是基于上述方法在保证了解码的唯一性的同时又缓解了对于运算精度与时间开销的要求，但为了使系统各模块之间更好的磨合，仍有一点不同：在把编码的十进制小数转化为二进制比特流的时候，一般来讲，一个十进制位只需要$\log_2 10 \approx 3.32$个二进制位，本文选择使用 4 个二进制位来表示一个十进制位，这样必然会损失一定的压缩

效果；然而这样做的好处是，程序不致过于复杂，尤其是对于在 QR 码技术的应用方面带来了极大方便，因为 QR 码采用了迦罗华域 GF(2^8)中的 RS 算法进行差控编码，其基本单元为一个码字 8 个比特，为 4 的倍数。

3.3 嵌入与提取模块

3.3.1 第一种方案

表 3.2 列出了实现嵌入与提取策略相关的函数与功能。

表 3.2 相关函数与功能

名称	功能
[Disp,Loss]=Original_En(image,Np,Sel)	第一种方案，由主函数调用， 综合调用各基本函数完成秘密信息的嵌入。
[Message]=Original_De(image,Np)	第一种方案，由主函数调用， 综合调用各基本函数完成秘密信息的提取。
[Refer,Lim,Lc,Lr,Block]=Version_Pick_En(image)	发送端为实现不同版本的 QR 码 图像的分别处理、优化程序结构而设定的函数。
[Refer,Lc,Lr,Block]=Version_Pick_De(image)	接收端为实现不同版本的 QR 码 图像的分别处理、优化程序结构而设定的函数。

由第二章讲解的 QR 码的纠错原理可知，对于每一个纠错数据块而言，只要选取块内任何一个纠错容量内的码字排列进行信息的嵌入，都可保证原始 QR 码信息的正常解码，而嵌入只需要简单替换即可。如何选择码字排列？一种非常简单的方法是采用伪随机序列模拟生成随机数，同时刚好可以利用伪随机序列的伪随机性来设定嵌入与提取策略；较简单的伪随机序列的产生方法是采用数论中基于数环理论的线性同余法，其迭代公式的一般形式为：

$$f(x) = (r \cdot x + b)\ mod\ M \tag{3.1}$$

其离散形式为：

$$s(n+1) = [r \cdot s(n) + b]\ mod\ M \tag{3.2}$$

其中，*s(n)*为 *n* 时刻的随机数种子，*r* 为扩展因子，*b* 为固定扰动项，*M* 为循环模，*mod M* 表示对 *M* 取模。为保证 *s(n)*的周期为 M，r 的取值应满足 r=4k+1，$M=2^p$，k 与 p 的选取应满足：r<M，$r(M-1)+1<2^{31}-1$。通常公式中参数常用取值为 *s(0)=12357*，*r=2045*，*b=1*，*M=1048576*[10]。

而 MATLAB 中的实现方法便是利用 rand()函数，把 rand()函数的初始种子数设定为嵌入与提取密钥，这样密钥的选择也非常方便，不过鉴于第二种方案，最好选择 0 与正整数[11]；本文第一种方案便是采用这种方法设计实现的，虽然十分简单，但是如果不考虑很高的安全性即 QR 码图像的失真，这种方法非常实用，而研究结果表明，这种方法产生的失真度其实是十分可观的。在这里有一点必须要强调的是，方法虽然十分简单，但是真正实现起来是非常复杂繁琐的，核心代码如下：

```
rand('state',KEY);MR=randperm(Lc);
MR=MR(1:Lr);MRM=[]; SMf=0;
for i=1:Block
    MRM=[MRM;MR];
end
```

其中 Block 代表纠错数据块数，Lc 代表纠错数据块的码字数，Lr 代表纠错容量。

为了降低程序的复杂程度，本系统存在一个小小的弊端：不论秘密信息的长度有多少，都要固定修改纠错容量大小的码字排列，同时为了减少这个弊端所带来的影响，本文引入了终止符与填充的机制，填充是借鉴了 QR 码的掩模方法[12]，使选取的码字排列去除秘密信息后的剩余部分对 QR 码的“视觉性”影响程度降为最低，这里的“视觉性”是 QR 码掩模中的概念，即尽量使 QR 码的‘0’与‘1’的比例接近 1:1，且不会出现大面积的全黑或全白区域。本文选择的填充码字为[0 1 0 0 1 0 1 1]，研究结果表明，填充的效果还是非常可观的。核心代码如下：

```
Rep=[];Fill=[0 1 0 0 1 0 1 1];
for i=1:numel(MRM)
    Rep=[Rep,Fill];
end
```

其中 Fill 代表填充码字不唯一，但选取标准应该保证‘0’和‘1’的比例为 1:1。

3.3.2 第二种方案

第二种方案在嵌入与提取策略上面有所改进，第一种方案由于是随机选取码字排列，虽然效果可观，毕竟没有一定的评价标准。第二种方案中引入失真度的标准，以损失一定的嵌入容量为代价降低了 QR 码图像的失真度，从而提高了系统的安全性[13]；同时，也用相同的失真度标准评价了第一种方案，详细的实验结果将在第四章中详细列出，这

里不做过多阐述。失真度的定义为，嵌入秘密信息后的 QR 码图像与原始 QR 码图像的不同像素值个数占原始 QR 码总像素数的比例[14]，实现代码如下：

```
Diff=bitxor(image,Disp);
Loss=length(find(Diff==1))/numel(image);
```

失真度的标准也即意味着要求算法具有自适应的特性[15]，即对于相同的 QR 码载体图像与相同的秘密信息内容，如何选取一种最合适的嵌入策略，使得嵌入秘密信息后所引起的 QR 码图像的失真为最小。首先，这种考虑所面临的第一个问题就是，在接收端是没有任何关于秘密信息的相关信息的，那么接收端要如何提取秘密信息呢？这时就必须以牺牲一定的嵌入容量为代价了，具体做法是，事先约定 QR 码图像的某一固定区域用于存储嵌入策略的相关信息，例如所选取的码字排列、位置信息等，这样接收端收到 QR 码图像时，先从约定的位置提取有关信息，然后根据这些信息进行秘密信息的提取。这就产生了下面两个问题：第一，如何自适应的选取使得 QR 码图像失真度为最小的嵌入策略？第二，嵌入容量与失真度的转换以什么样的比例最为合适？下面，本文主要针对这两个问题阐述第二种方案的设计思想。

表 3.3 列出了实现嵌入与提取策略相关的函数与功能。

表 3.3　相关函数与功能

名称	功能
[DispOp,LossOp]=Optimize_En(image,Np)	第二种方案，由主函数调用，综合调用各基本函数完成秘密信息的嵌入。
[Message]=Optimize_De(image,Np)	第二种方案，由主函数调用，综合调用各基本函数完成秘密信息的提取。
[Refer,Lim,Lc,Lr,Block]=Version_Pick_OpEn(image)	发送端为实现不同版本的 QR 码图像的分别处理、优化程序结构而设定的函数。
[Refer,Lc,Lr,Block,KEY]=Version_Pick_OpDe(image)	接收端为实现不同版本的 QR 码图像的分别处理、优化程序结构而设定的函数。

首先，对于第一个问题，最理想的方法是可以对所有的情况进行穷举遍历，然后选取失真度最小的一种作为最后的嵌入策略[16]。在这里要特别强调两点，第一，这里所说

的理想也是一种简化的情况，例如，考虑这样一种情况，假设在进行比特替换时，某一QR 码码字的‘0’‘1’比例与要进行替换的秘密信息比特流的 8 个比特的‘0’‘1’比例相同，那么总可调整比特流的嵌入顺序使得嵌入这 8 个比特信息后 QR 码图像不会产生任何的失真，但是这样一来，如果把这种情况列入考虑范围之内，不但会使得算法过于复杂甚至难以实现，而且必然会以牺牲相当大的嵌入容量为代价才可能实现，因此本文的两种方案所采用的方法均未考虑单个码字内的比特排列情况，在 2.3 章节中也对这个问题有所提及；第二，在牺牲的嵌入容量部分存储的是嵌入策略信息，例如所选取的码字排列信息、位置信息等，这意味着穷举遍历的过程中存在一定的内在约束，虽然影响可能很小，但也破坏了算法与结果的“理想”性[17]。第二种方案的设计思想是忽略了这些问题的，但在这里有必要进行说明。

其实，即便是上述“非理想”的情况，要想穷举遍历所有的情况也是非常困难的，因为排列组合的运算数值相当巨大，对计算机的运算能力与时间开销的要求非常高，显然，这些都是应该尽量避免的问题[18]。那么究竟如何选择合适的嵌入策略使得失真度尽可能的降低？本文第二种方案采取的方法是将遍历空间缩减到合适大小，并且取得了可观的效果；之所以会产生这样的现象，本文作出的解释如下：QR 码图像本身是二值的，对任何一个像素点都是非黑即白，因此在嵌入秘密信息比特流时，在很多位置上都有很大的概率与 QR 码本身的像素值相同，而这样的替换是不会引起任何失真的，所以，即使替换的是纠错容量大小的码字数量（约为$1/3$），失真度还是很可观的，也正是基于这个原因，第一种方案虽然方法非常简单，但是失真度却不会很高，是相当实用的；既然第一种方案的失真度不是很高，也就意味着实现失真度的大幅降低是非常困难的，也就是说失真度越小，要想再降低失真度将会非常困难，所以即使是第二种方案缩减了遍历空间，仍然取得了可观的效果。

第一个问题解决了，第二个问题的答案也便呼之欲出：如果可接受的嵌入容量的牺牲越大，也就意味着遍历空间的增大，即可能达到的失真度就会越小。但是这种正相关的关系一定不会随着所牺牲的嵌入容量的增大一直维持下去，因为在牺牲的空间存储的是与嵌入策略相关的信息，如码字的排列信息、位置信息等，这些信息与秘密信息的嵌入是存在一定的约束关系的，而随着这些信息量的增加，这种约束关系可能会更加明显，同时由这些信息本身所引起的失真也就不容忽视了[19]。图 3.7 给出了本文对这种关系的大致的预测曲线，仅供参考。

分析：第一种方案的平均失真度大概在 10%左右，对应图 3.7 中的 0.1，严格来说实际上可能达到的最小平均失真度应该没有图 3.7 那么夸张，而随着遍历空间的增大，所需要损失的嵌入容量的上限值接近于 0.5，也就是说，无论遍历空间有多大，只需要损

失大约一半的嵌入容量便足以存储足够的策略信息，具体原因会在下面指出。

本文的第二种方案利用损失的嵌入容量存储密钥信息，这样，遍历空间的相关信息便可以映射到一个密钥矩阵之中[20]，所占比重为$1/Lr$（Lr 为各版本的纠错容量，也就是嵌入容量）；密钥空间的大小设定为256，刚好占用一个码字（如果密钥空间增大为65536，则占用两个码字），对于每一个纠错数据块，密钥可以是相同的（对于第一种方案，可以认为所有的纠错数据块共用一个相同的密钥），也可以是不同的，因此所有的密钥组成一个密钥矩阵，当然这个矩阵是不需要用户事先约定记忆的，是自适应的，遍历空间的大小容易得出，为256^{Block}（Block 为纠错数据块数），而本文也对程序结构进行了调整优化，使得只需执行 Block*256 次循环即可完成遍历，减少了时间开销。

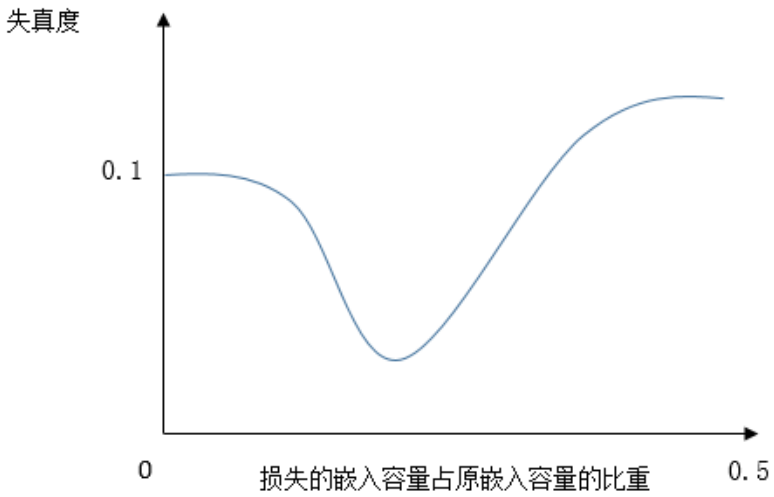

图 3.7　嵌入容量与失真度的转换关系

实际上，上述方法仍然进行了一些取舍：首先，密钥其实是用来生成纠错数据块内的某种码字排列的，但是由于程序实现上的限制，这个排列主要是用 rand()和 randperm()函数生成然后截取而得到的[21]，随着密钥空间的增大，出现重复的可能性就会增大，因此本文实际的遍历空间可能比上述理论值要小一点；再者，随着遍历空间和密钥空间的增大到一定的数值，这时完全可以用码字排列的位置信息来替代密钥矩阵，以减少嵌入容量的损失，这时损失比重便达到上限即大约一半的嵌入容量[22]，对应图 3.7 中的 0.5。本文第二种方案设定的遍历空间较小，选用密钥矩阵更加合适；当然，实际应用时可能根本无需非常大的遍历空间，也就是损失比重不会接近 0.5，但是利用损失的嵌入容量存储位置信息的方法更有可能完成对所有情况的遍历[23]，不失为第三种方案，而第二种方案采取的存储密钥矩阵的方法，无论怎样开销时间，都无法遍历所有的情况。

表 3.4 列出了各版本纠错等级为 H 的采用存储位置信息的方法的嵌入容量的损失情况，仅供参考。

表 3.4　第三种方案的嵌入容量损失情况

版本	Lc	Lr	Lc’	Lr’	每个位置所需 bit 数	位置信息的存放码字（可变）
1	26	8	23	4	5	24~26
2	44	14	38	8	6	39~44
3	35	11	31	6	5	32~35
4	25	8	22	4	5	23~25
5	33	11	29	6	5	30~33

1）表中 Lc、Lr 分别为纠错数据块的码字总数与纠错容量；Lc’、Lr’分别为除去“损失”之外剩余的相应数量。

2）由于版本的尺寸限制，各个纠错数据块的码字总数可能不相同，但相差不会超过一个码字，针对这种情况，本文对各版本所有的纠错数据块均取最小值，多余出的码字直接忽略，这样不但可以简化程序结构，而且对本文的研究的影响微乎其微，不会造成任何严重后果。

由于程序结构的整体性，使得核心代码难以分离，对于第二种方案不再列写。

3.4　本章小结

本章主要讲解了基于第二章所述基本原理的具体方案的设计与实现，在对秘密信息进行压缩编码的基础上，一共设计并实现了两种方案，第一种方案重点关注信息隐藏系统的嵌入容量问题，而第二种方案以损失部分嵌入容量为代价，重点考虑系统的安全性问题。由于论文结构的安排，本章尽量不给出任何结论性的数据参考，以免会降低可读性，接下来的第四章将会详细讨论本系统的运行情况，以及利用该系统所进行的一系列测试，并得出最后的一些结论。

4 实验数据分析与方案评价

本文主要从以下几个方面进行实验设计，首先对压缩编解码模块中所采用的算术编码方法进行压缩率大小的测定，并且在这个基础上，对本系统的嵌入容量进行细致的讨论；然后对嵌入秘密信息后的 QR 二维码图像与原始 QR 二维码图像进行失真度的测定和对比讨论，其中主要包括以下两种情况：一是针对同一秘密信息向不同的 QR 二维码载体图像的嵌入，二是针对向同一 QR 二维码图像嵌入不同的秘密信息。

4.1 实验设计流程

实验一、由于算术编码并非等长码，而本文又对其做出了一定的改进，故难以从理论上计算其压缩率的大小；本文在实现上述系统的基础上，对算术编码的压缩率进行了一系列的测定，测定方法如下：选择一篇英文文献《I HAVE A DREAM》，对 QR 码的前 10 个版本随机选取 10 种其纠错容量大小的该文献中的字符组合进行算术编码，并计算每个版本的平均压缩率，然后根据平均压缩率给出两种方案中每个版本在引入压缩方法后的实际的嵌入容量。

实验二、本文对失真度的测定方法如下：第一，对 QR 二维码的前 5 个版本，针对同一 QR 二维码载体图像与不同的秘密信息（秘密信息的选取方法同上）分别按照两种方案进行嵌入，然后统计失真率（对每个版本每种方案统计 10 次），QR 码载体图像选择编码内容为“大学之道 I have a dream Martin Luther King”，并且按照不同版本的编码容量进行适当的截取和重复；第二，对 QR 二维码的前 5 个版本，针对不同的 QR 二维码载体图像（10 幅）与同一秘密信息分别按照两种方案进行嵌入，然后分别统计失真率，QR 二维码载体图像的选取仍然选用上述英文文献中的不同内容生成不同的 QR 二维码，而秘密信息选择“HTTP://WWW.DLUT.EDU.CN”，并且按照不同版本的嵌入容量进行适当的截取和重复。

实验平台：条码生成网站“HTTP://BARCODE.TEC-IT.COM”，Win7 系统 64 位，软件 MATLAB R2010 b 64 位。

作为示例，图 4.1 给出了第 5 个版本，QR 二维码载体图像的编码信息为“大学之道 I have a dream Martin Luther King”，秘密信息为“HTTP://WWW.DLUT.EDU.CN”，采用第二种方案进行嵌入后得到的 QR 二维码与原始 QR 二维码的编码图像，阅者可自行观察两者两者的区别，而利用普通的 QR 二维码扫码软件扫描得到的信息一定是相同的，“只有”使用本系统才可正确提取秘密信息，从而达到了利用 QR 二维码进行秘密信息的隐藏与传递的目的。

(a). 原始 QR 二维码图像

(b). 嵌入秘密信息后的 QR 码图像

(c). (a)与(b)的比较图

图 4.1　QR 二维码示例图像

图 4.2　提取出的秘密信息

4.2 算术编码的压缩率

4.2.1 压缩率参考

压缩率的定义为数据压缩后的比特长度与压缩前的比特长度之比，为达到压缩的目的，希望压缩率越低越好[24]。计算公式如下：

$$Ra = {}^{L2}/_{L1} \times 100\% \tag{4.1}$$

其中，Ra 代表压缩率，L2 代表数据压缩后的比特长度，L1 代表压缩前的比特长度。

按照 4.1 中设计的实验步骤进行实验并得到的最终结果见图 4.3 和 4.4。图 4.3 是对每个版本随机选取 10 种字符组合（随着版本数的增加，所取字符组合的长度也依次增加，故用版本信息代替长度信息，其余同），然后对每一种组合计算一次压缩率得到的数据统计图；图 4.4 是基于图 4.3 的统计数据对每个版本进行计算平均压缩率，得到平均压缩率的走势图。

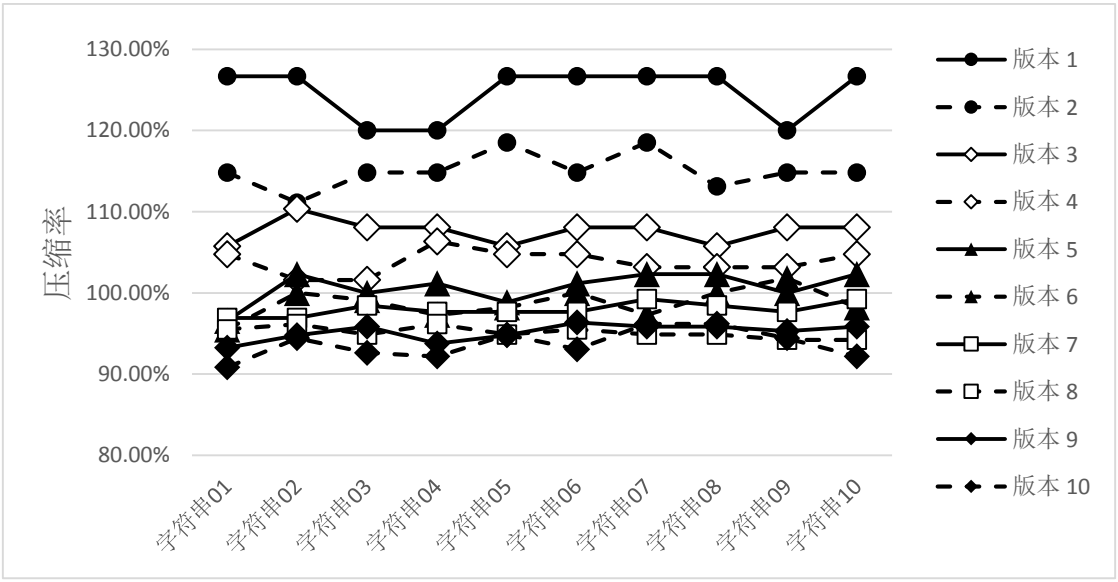

图 4.3 QR 码前 10 个版本的压缩率统计图

从图 4.3 中可以看出，算术编码的压缩率不仅与待编码的信息长度有关，还与待编码的信息内容有关；从图 4.4 中可以看出，随着 QR 码版本的增加也即待编码信息长度的增加，压缩效果越来越明显，而如果待编码信息长度太小，压缩效果是很差的，这点符合许多压缩算法的特点；由于前 5 个版本的嵌入容量略低，采用压缩的方法反而起到相反的效果，但从第 6 个版本开始，压缩的效果便开始显现了。

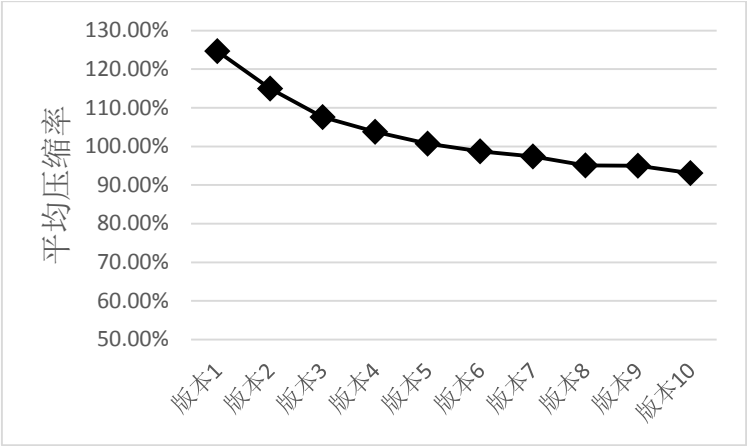

图 4.4　QR 码前 10 个版本的平均压缩率走势图

4.2.2　嵌入容量参考

表 4.1 中列出了 QR 码各版本的嵌入容量，其中第三列是利用原始嵌入容量（比较准确）与图 4.4 中得到的平均压缩率计算得到的。

表 4.1　嵌入容量的确定与对比（参考）

	原始嵌入容量 （单位:字符）	采用压缩方法后的嵌入容量 （单位：字符）
版本 01	10	8
版本 02	18	17
版本 03	29	27
版本 04	42	40
版本 05	58	57
版本 06	74	74
版本 07	86	88
版本 08	104	109
版本 09	128	134
版本 10	149	160

由于算术编码并非等长码，故表 4.1 中第三列的数据仅供参考，但其中的误差是可以接受的，而实际程序中为了保证不出任何差错，取值比较保守。第二种方案中由于在

每个纠错数据块内仅取一个码字用来存储密钥信息，对嵌入容量的影响并不大，故可认为两种方案的嵌入容量是相同的，但随着设计密钥空间的增大，存储密钥所占用的空间就不容忽视了。

4.3 两种方案的失真度分析对比

失真度的定义为嵌入秘密信息后的 QR 二维码图像与原始 QR 二维码图像的不同像素数占原始QR二维码图像总像素数的比例，为了增加安全性，希望失真度越小越好[25]。本文失真度的计算公式如下：

$$Ra = {}^{N2}/_{N1} \times 100\% \tag{4.2}$$

其中，Ra 代表失真度，N2 代表不同像素数，N1 代表原始 QR 码总像素数。

第一，对 QR 二维码的前 5 个版本，针对同一 QR 二维码载体图像与不同的秘密信息（秘密信息的选取方法见 4.1）分别按照两种方案进行嵌入，然后统计失真率（对每个版本每种方案统计 10 次），QR 码载体图像选择编码内容为“大学之道 I have a dream Martin Luther King”，并且按照不同版本的编码容量进行适当的截取和重复，最终得到图 4.5 和图 4.6。

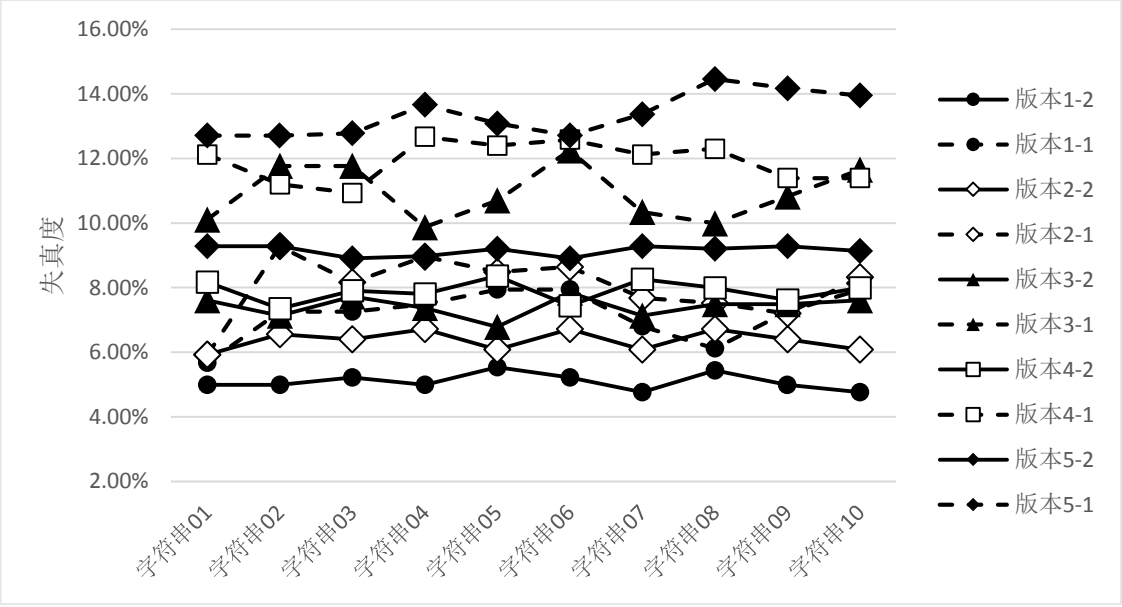

图 4.5 两种方案的失真度分析统计图（一）

图 4.5 中的图例“版本 1-2”代表第一个版本第二种方案，其余类同。从图 4.5 中可以看出，基本上每个版本的每种方案占一个“失真度等级”，为了分析更加直观，下面

着重研究图 4.6 并得出相关结论。

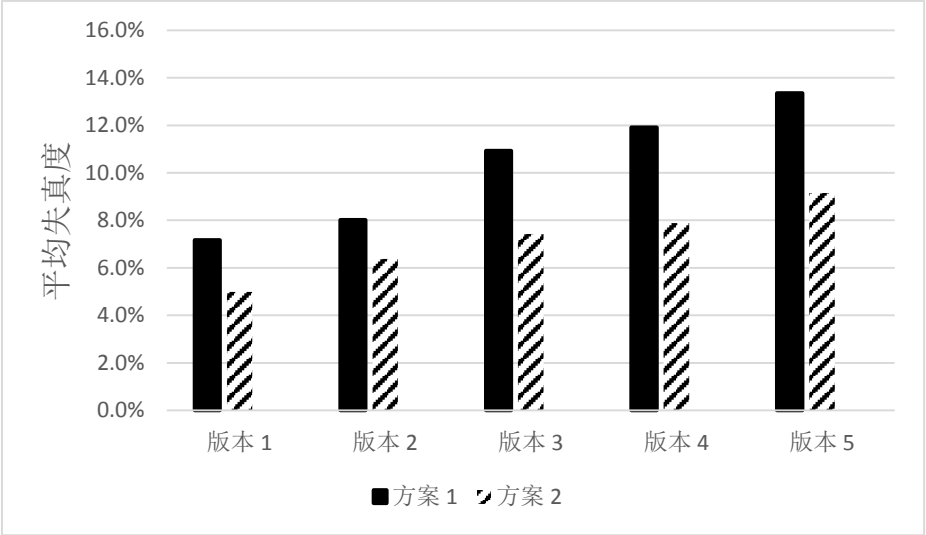

图 4.6　两种方案的平均失真度柱形图（一）

由图 4.6 可以看出，对第一种方案而言，每个版本的平均失真度在$1/10$左右，远低于纠错容量在 QR 码图像中所占的比重（约为$1/3$），还是比较可观的；对每个版本而言，第二种方案的平均失真度要比第一种方案的平均失真度低，差别在$1/3$左右，证明第二种方案的设计思想是正确的。仔细观察图 4.6 还会发现一些奇怪的现象：一是，对每种方案而言，对原始 QR 码图像的改动（像素值直接替换）均为$1/3$左右，然而真正引起的失真度却只有$1/10$；二是，对每个版本而言，在对 QR 码图像的改动均为$1/3$的情况下，失真度却随着版本的增加而逐渐增加。本文做出如下解释：由于 QR 码是二值图像，对每个像素点而言非黑即白，在对像素值进行直接替换时，每个像素均有较大的概率不产生失真，因此实际由替换引起的失真便有可能大幅降低；然而随着版本的增加，QR 码图像总的像素点数随之增加，这时即使单个像素点在替换后不产生失真，但对整个图像的失真度贡献却会逐渐减小。

第二，对 QR 二维码的前 5 个版本，针对不同的 QR 二维码载体图像（10 幅）与同种秘密信息分别按照两种方案进行嵌入，然后统计失真率，QR 二维码载体图像的选取仍然选用 4.1 中提到的英文文献中的不同内容生成的不同的 QR 二维码，而秘密信息则选择“HTTP://WWW.DLUT.EDU.CN”，并且按照不同版本的嵌入容量进行适当的截取和重复，最终得到图 4.7 和图 4.8。

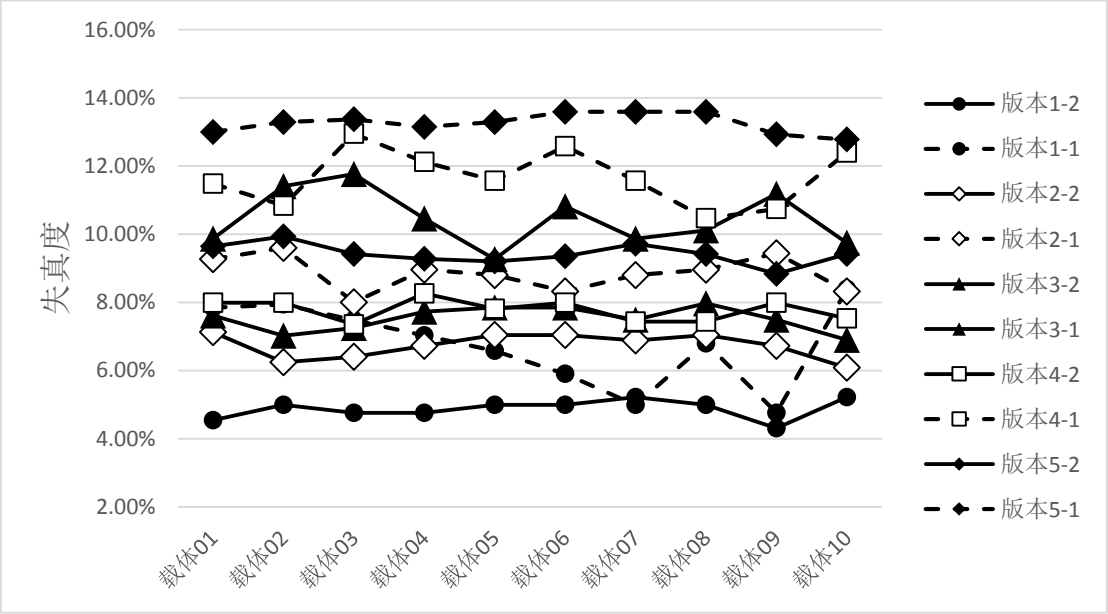

图 4.7　两种方案的失真度分析统计图（二）

图 4.7 中的图例“版本 1-2”代表第一个版本第二种方案，其余类同。从图 4.7 中可以看出，基本上每个版本的每种方案占一个“失真度等级”，这种现象同样在图 4.5 中存在，而类似的，为了分析更加直观，下面着重研究图 4.8 并得出最终的结论。

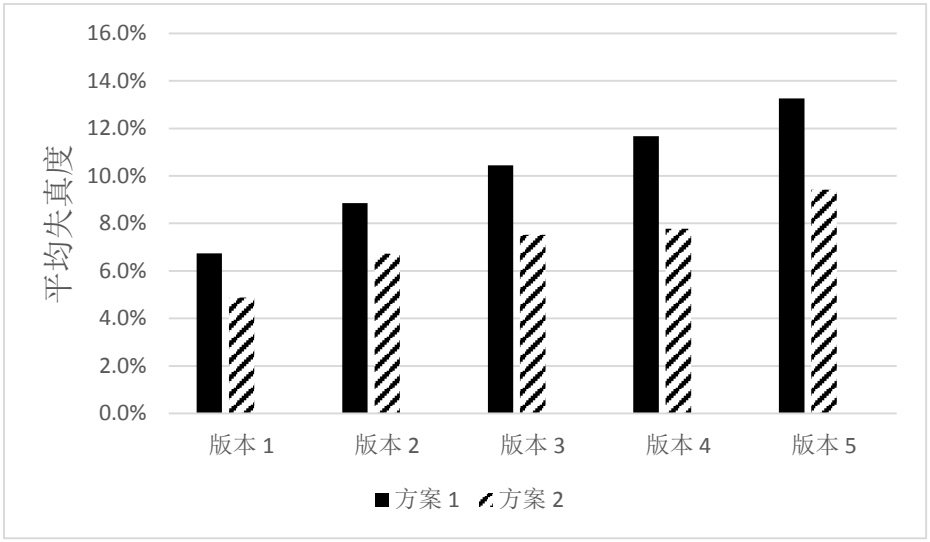

图 4.8　两种方案的平均失真度柱形图（二）

直观看出图 4.7 与图 4.8 的数据和趋势与图 4.5 和图 4.6 大致相同，一定程度上说明本系统存在一定的统计稳定性，而统计稳定性的意义在于，无论是选用哪一种方案、哪一种 QR 码版本、哪一种 QR 码载体（QR 码的编码信息不同）与哪一种秘密信息，在实现秘密通信的基础上，所引起的 QR 码的失真处于使用者的可控制范围之内，也就是说，本文所研究的 QR 二维码的信息隐藏方案具有一定的实际应用价值，而这也是本文研究的根本目的所在。但是由于本人水平有限，在测量方法上可能存在一定的局限和不足。仔细观察图 4.7 会发现版本 1-2 的第 7 个点比版本 1-1 的第 7 个点的值要大，而前者对应第二种方案，后者对应第一种方案，这是不正常的。本文给出的解释是，这种现象只是偶尔出现在版本 1 中，由于版本 1 的嵌入容量较小，第二种方案损失的嵌入容量所占比重虽然仍然很小，但依然有可能对失真度造成一定的影响，不过这种现象一定会随着版本的升高而消失无踪。

4.4 本章小结

本章主要讲解了使用 MATLAB GUI 最终编程实现的信息隐藏系统的运行情况，并且利用该系统对本文所设计的两种不同方案的嵌入容量、安全性等问题进行了一系列的实验设计与数据分析，最终对本文的研究给出了一定的数值参考，并利用图表的形式进行了直观展示，基本达到了本文研究的目的。

结　论

本文主要研究了利用 QR 二维码进行信息隐藏的技术，信息隐藏在信息安全领域是非常重要的一门学科，而研究利用 QR 二维码进行信息的隐藏技术，虽然应用性很强，但应用的广度可能不足，最大的用途可能仅在秘密通信方面；但是鉴于目前 QR 二维码技术非常流行，扫码行为渐趋日常化，本文仍然具有很高的研究价值。

本文所作的主要工作更加着重于实现方法的研究与普适性，由于工作量与时间的限制，并未把所有版本的 QR 二维码囊括进本系统，但是，本系统在编程实现的同时非常注重程序的可扩展性，不断优化和改进程序结构，如果要完成全部的工程，只需要按照相同的方法完成各版本函数的编写然后直接添加即可，无需修改任何主函数或调用部分；当然上述可扩展性还基于研究方法的正确，这点已由对系统的一系列测试结果和数据提供了很好的证明。

参 考 文 献

[1] 张军，熊枫，张丹. 图像隐写分析技术综述[J].计算机工程，2013，39(4):165-168.

[2] 张卫明，李世取，刘九芬. 对空域图像 LSB 隐写术的提取攻击[J].计算机学报，2007，30(9):1625-1631.

[3] Md.Wahedul Islam, Saif alZahir. A Novel QR Code Guided Image Steganographic Technique[C]. International Conference on Consumer Electronics, 2013:586-587.

[4] 冯汉禄，黄颖为，牛晓娇，钱银超.QR 码纠错码原理及实现[J].计算机应用，2011，31(6)：40-42.

[5] 曾子剑.基于 QR 二维码编解码技术的研究与实现[D].四川：电子科技大学，2010.

[6] 韩涛，祝跃飞. 基于 Canny 边缘检测的自适应空域隐写术[J].电子与信息学报，2015，37(5):1266-1270.

[7] Chin-Ho Chung,Wen-Yuan Chen,Ching-Ming Tu. Image Hidden Technique Using QR-Barcode[C]. International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009:522-525.

[8] 国家质量技术监督局.GB/T 18284—2000 快速响应矩阵码[S].2000-12-28.

[9] Pevný T, Filler T, Bas P. Using high-dimensional image models to perform highly undetectable steganography[C]. Proceedings of 12th International Workshop on Information Hiding, 2010: 161-177.

[10] Sartid Vongpradhip, Suppat Rungraungsilp. QR Code Using Invisible Watermarking in Frequency Domain[C]. International Conference on ICT and Knowledge Engineering, 2011: 47-52.

[11] 谢建全，黄大足，谢勃，杨赞伟. 一种大容量的二值图像信息隐藏算法[J].东南大学学报，2007，37(9):10-14.

[12] 刘丽.基于二维码数字水印的产品防伪研究与应用[D].北京：北京邮电大学，2013.

[13] Jantana Panyavaraporn, Paramate Horkaew, Wannaree Wongtrairat. QR Code Watermarking Algorithm Based on Wavelet Transform[C]. International Symposium on Communications and Information Technologies, 2013:791-796.

[14] 陈贵川.基于数据挖掘的二维码防伪防窜货系统分析与设计[D].北京：北京邮电大学，2010.

[15] 刘文彬，刘九芬. 一种针对 LSB 替换隐写的消息定位方法[J].信息工程大学学报，2013，14(6):641-646.

[16] 程永丽.二值图像信息隐藏技术研究[D].天津：天津大学，2007.

[17] Hsiang-Cheh Huang. Reversible data hiding with histogram-based difference expansion for QR code applications[J]. IEEE Transactions on Consumer Electronics, 2011:779-787.

[18] HenrykBlasinski. Per-colorant-channel color barcodes for mobile applications: An interference cancellation framework[J]IEEE Transactions on Image Processing, 2013:1498-1511.

[19] 孟威. 面向文本的自然语言隐写术保密通信系统[J].淮北职业技术学院学报，2015，14(1):141-142.

[20] 李鹏.基于商密二维码和数字水印的防伪图码的研究与设计[D].吉林：吉林大学，2013.

[21] KamonHomkajorn, MahasakKetcham and Sartid Vongpradhip. A technique to remove scratches from QR code images[C]. International Conference on Computer and Communication Technologies(ICCCT 2012), 2012:127-131.

[22] 申载强.二值图像信息隐藏方法研究及设计[D].广东：中山大学，2014.

[23] OrhanBulan, HenrykBlasinski, Gaurav Sharma. Color QR codes:increased capacity via per-channel data encoding and interference cancellation[C]. 19th Color and Imaging Conference Final Program and Proceedings, Society for Imaging Science and Technology, 2011:156-159.

[24] 戴蒙.二值图像信息隐藏技术研究及应用[D].上海：上海师范大学，2004.

[25] Holub V and Fridrich J. Designing steganographic distortion using directional filters[C]. Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), 2012: 234-239.

致　　谢

这里首先感谢指导老师王波的耐心指导以及和谐相处四年的同窗室友周猛、李越、康文辉与本人一起创造的良好的学习氛围，如果没有他们，这人生中的第一篇论文，也许会成为最后一篇论文了。也许正如指导老师王波所说的那样，大学四年，真正清清楚楚可以展现在父母面前的东西，就是这篇凝聚着个人心血与母校情怀、装订精美的论文了，虽然他们也许并不会看懂，但是，这篇论文一定会永远成为家中书架的珍藏，想到他们会时不时戴着老花镜向阳翻阅的神态，吾心甚慰。

大连理工大学，来到这里，对于本人来说，是一种幸运，真心话。毕业之前，你一直是懵懵懂懂的处在校园之中，也许你可以感受到浓郁的学术氛围，感受到学生应有的青春活力，感受到深厚的师生、同学之谊，感受到周围环境的优雅与令人心旷神怡的自然景观与人类社会的完美融合；但也许你从未想过，你有一天会离开，会有不舍，也许你从未考虑过，这学校对你来说究竟意味着什么，你只知道是母校，仅此而已，你从未有所体会。然而，当你面临毕业的时候，或者毕业后的某一天，你一定会知道答案，之所以称作母校，就是因为，不论你于何时何处有所何为，他一直在你身边，只是一直很安静。