学校代号 10532 学 号 S1310W1047

分 类 号 TP391 密 级



湖 南 大 学 HUNAN UNIVERSITY

**工程硕士学位论文**

**二维码信息隐藏技术研究与实现**

学位申请人姓名\_ 唐 蕾 **培** **养** **单** **位** 信 息 科 学 与 工 程 学 院 **导师姓名及职称** 罗 纲 副 教 授 胡 红 桂 高 级 工 程 师

**学** **科** **专** **业** 计 算 机 技 术 **研** **究** **方** **向** 信 息 隐 藏

**论文提交日期** 2 0 1 5 年 1 1 月 2 日

中国知网 <https://www.cnki.net>

**学校代号：10532**

**学** **号** **：S1310W1047 密** **级：**

**湖南大学工程硕士学位论文**

**二维码信息隐藏技术研究与实现**

学位申请人姓名： 唐 蕾

|  |  |
| --- | --- |
| 导师姓名及职称： | 罗纲副教授胡红桂高级工程师 |
| 培 养 单 位 ： | 信 息 科 学 与 工 程 学 院 |
| 专 业 名 称 ： | 计 算 机 技 术 |
| 论文提交日期： | 2 0 1 5 年 1 1 月 2 日 |
| 论文答辩日期： | 2 0 1 5 年 1 1 月 2 0 日 |
| 答 辩 委 员 会 主 席 ： 赵 欢 教 授 | |

**中国知网** [**https://www.cnki.net**](https://www.cnki.net)

The Research and Implementation on Two-dimensional Barcode Information Hiding

by

TANG Lei

B.E.(Hunan University)2013

A thesis submitted in partial satisfaction of the

Requirements for the degree of Master of Engineering

in

Computer Technology

in the

Graduate School

of

Hunan University

Supervisor

Associate Professor LUO Gang

Senior Engineer HU Honggui

November,2015

中国知网 https://www.cnki.net

中国知网 s://www.cnki.net

摘 要

随着二维码的普及和广泛应用，二维码逐渐成为人们记录信息，传递信息的 重要手段之一，同时针对二维码的信息隐藏的研究也应运而生。二维码信息隐藏 是指在二维码中嵌入一些秘密信息，让第三方在主观上难以察觉秘密信息的存在， 从而达到隐蔽通信的目的。目前，二维码信息隐藏技术的研究还比较少，因此进 行二维码信息隐藏技术的研究很有意义。

本文针对二维码编解码过程的若干关键技术进行了研究，通过深入分析当前 主流二维码所使用的R-S 编码技术的性质，发现了该技术为信息隐藏提供了一个 入口。针对该技术的性质，提出了一种新的二维码信息隐藏算法。本文的主要内 容包括以下几个方面：

首先，介绍了信息隐藏的概念和特点，并介绍了与二维码信息隐藏密切相关 的图像隐藏算法进行了介绍，总结了信息隐藏算法的嵌入和提取框架，重点分析 了当前二维码信息隐藏算法，概括了其存在的问题。

其次，本文针对现有二维码信息隐藏算法存在的问题，提出了一种基于R-S 编码的二维码信息隐藏算法。该算法利用二维码编码技术 R-S 编码所产生的 数据冗余，根据R-S 编码的编码特点将秘密信息合理地嵌入到二维码。通过该算 法，二维码既能够被正常解码，也不会引起任意第三方的怀疑。

最后，本文利用所提出的基于R-S 编码的二维码信息隐藏算法，实现了一个 基于Android 的隐蔽通信系统。该系统通过利用随机数发生器将秘密信息随机的 嵌入到二维码中，具有较好的抗攻击的能力，并且能够使用Android 手机(带摄 像头)提取出秘密信息。由于利用了二维码本身所使用的R-S 编码技术，使得隐 蔽系统能完整保存载体原始信息，不会影响它作为普通二维码的功能，所以该隐 蔽系统具有较好的隐蔽性。

关键词：信息隐藏；信息安全；二维码；R-S 编码

中国知网 <https://www.cnki.net> IⅡ

工程硕士学位论文

Abstract

With the popularity and widespread application of two-dimensional code, two-dimensional code has gradually become an important means of recording and transmitting information.Meanwhile,researches on the two-dimensional code information hiding arise as well.Two-dimensional code information hiding refers to embedding secret information in two-dimensional code to avoid being detected the existence of secret information subjectively by a third party and eventually achieving the purpose of converting communication.At present,researches on two-dimensional code information hiding technology are still few,so it makes sense to do some studies on this new field.

In this paper,the key technologies of the two-dimensional encoding and decoding process has been studied.Based on the deep analysis of the nature of the current mainstream two-dimensional code used in R-S coding techniques,we found that this technique provides an entrance for information hiding.According to the nature of the technology,we proposed a new two-dimensional code information hiding algorithm.The main contents are included as the following aspects:

First,we introduce the concept and characteristics of information hiding and present the image information hiding algorithm which is closely related to the two-dimensional code information hiding.Then we summarize the framework of embedding and extracting information hiding algorithm and pay special attention to the analysis of the current two-dimensional code information hiding algorithm and outlining its problems.

Secondly,based on the existing problems of present two-dimensional code information hiding algorithm,we propose a two-dimensional code based on R-S code information hiding algorithm.The algorithm uses a two-dimensional code technology --data redundancy generated by R-S encoding,according to the characteristics of the R-S encoding,secret information can be embedded reasonably in the two-dimensional code.With this algorithm,two-dimensional code can be decoded properly,without suspicion of any third party.

Finally,with the proposed two-dimensional code information hiding algorithm based on R-S code,a covert communications system based on Android is implemented. Through the use of a random number generator,secret information can embedded

中国知网 <https://www.cnki.net> III

randomly in the two-dimensional code in the system and it has a good anti-attack capability,and the ability to use Android phones with camera to extract the secret information.With the use of R-S code technique in two-dimensional code itself,the system can preserve the original message of cover,and it will not affect its function as a normal two-dimensional code.Therefore,the covert system has a good hiding performance.

Key Words:Information Hiding;Information Security;Two-dimensional code;R-S

code

中国知网 <https://www.cnki.net>

**IV**

工程硕士学位论文

**目** **录**

学位论文原创性声明 I

学位论文版权使用授权书 I

摘 要 II

Abstract IH

目 录 V

**插图索引**  **VII**

**附表索引 VIII**

**第1章** **绪** **论** [**1**](#bookmark2)

**1.1 选题背景** [**1**](#bookmark3)

**1.2 国内外研究现状** [**2**](#bookmark4)

**1.3 本文主要工作** [**4**](#bookmark5)

**1.4 论文结构** [**5**](#bookmark6)

**第2章** **基本原理及相关技术** [**6**](#bookmark7)

**2.1 信息隐藏概述** [**6**](#bookmark8)

2.1.1 信息隐藏常用框架 [7](#bookmark9)

**2.2.2 信息隐藏分析技术** [**7**](#bookmark10)

2.2.3 信息隐藏的特征 [8](#bookmark1)

**2.2.3 信息隐藏的分类** [**9**](#bookmark11)

2.3 图像信息隐藏技术发展现状 [10](#bookmark12)

2.3.1 可逆信息隐藏 [10](#bookmark13)

2.3.2 不可逆信息隐藏 [12](#bookmark14)

**2.3.3 图像质量评价方法** [**13**](#bookmark15)

2.4 二维码 [15](#bookmark16)

**2.4.1 二维码编码技术** [**16**](#bookmark17)

2.4.2 二维码解码技术 [18](#bookmark18)

2.5 小结 [20](#bookmark19)

第3章 基于Reed-Solomon 编码的二维码信息隐藏算法 21

3.1 引 言 21

**3.2 本文提出的二维码信息隐藏算法** **22**

**3.2.1 算法原理** **22**

**3.2.2 算法设计** **23**

中国知网 https :// www.cnki .net V

[3.2.3 信息嵌入 24](#bookmark11)

3.2.4 信息提取 25

3.3 实验结果及其分析 26

3.3.1 不可见性分析 26

3.4.2 鲁棒性分析 27

3.4.3 嵌入容量分析 28

3.4.4 对比分析 29

3.5 小 结 30

第 4 章 Android平台二维码隐蔽通信系统设计与实现 31

4.1 引言 31

4.2 平台简介 31

4.2.1 Java 平台 31

4.2.2 Android 平台 32

4.3 需求分析 32

4.3.1 隐蔽通信模型分析 32

4.3.2 二维码隐蔽通信系统模型分析 32

4.4 系统设计 33

4.4 系统实现 35

4.4.1 载密二维码生成 35

4.4.2 载密二维码识别 37

4.5 系统测试 38

4.5.1 测试目的 38

4.5.2 测试内容 38

**4.5.3 测试方法及结果** **38**

**4.6 系统评价** **42**

**4.7 小结** **42**

结 论 **43**

**本文工作总结** **43**

**需要改进及进一步研究的问题** **44**

参考文献 **45**

**致** **谢** **49**

**附录A 攻读学位期间发表的学术论文** **50**

**VI**

**中国知网** **https :// www. cnki . net**

工程硕士学位论文

**插图索引**

图2.1 信息隐藏常用框架 [7](#bookmark20)

图2.2 隐蔽性、隐藏容量和鲁棒性的关系 [9](#bookmark21)

图2.3 两种常见的二维码 [16](#bookmark22)

图2.4 二维码编码过程 [17](#bookmark23)

图2.5 二维码解码过程 [19](#bookmark24)

图3.1 本文提出的方案 24

图3.2 二维码隐藏信息前后的对比图 27

**图3.3** **不同纠错等级下的嵌入容量** **28**

**图4.1** **系统架构示意图 34**

**图4.2** **载密二维码生成流程图 36**

**图4.3** **载密二维码识别流程图 37**

**图4.4** **中文环境下生成的载密二维码** **39**

图4.5 英文环境下生成的载密二维码 39

图4.6 载密二维码原始信息的可识别性测试结果 40

图4.7中文环境下的载密二维码秘密信息的可识别性测试结果 40

图4.8英文环境下的载密二维码秘密信息的可识别性测试结果 41

图4.9密钥对秘密信息识别结果的影响 41

中国知网 https :// www.cnki . net

VII

**二维码信息隐藏技术研究与实现**

**附表索引**

表3.1 对10条无关载体信息的实验结果 26

表3.2 抗图像压缩与旋转攻击的实验结果 27

表3.3 本文算法与基于PDF 417码的算法的比较 29

表3.4 本文算法与基于DCT 变换的算法的比较 30

表4.1 系统功能需求表 33

表4.2 载密二维码生成所需的主要类类型 36

表4.3 载密二维码识别所需的主要类类型 37

中国知网 https :// www. cnki . net **VIII**

第 1 章 绪 论

1.1 选题背景

二维码是一种用特定的几何图形按一定规律在平面(二维方向)上分布的黑 白相间的图像，也是一种用于在二维空间内记录大量的数据与快速的识别的技术。 二维码具有信息容量大、编码范围广、容错能力强、成本低等特点，通常用来存 储文本信息、特点代码、名片、网址等。目前，二维码已经存在多种码制的国际 标准，被应用到各个领域中，取得了非常高的经济价值。

在国外，二维码的应用发展得比较早，其中以日本、韩国应用得最为广泛。 日本的一些快餐店和便利店的宣传单和优惠券上面都使用二维码，许多超市小票 和电影票都印有二维码，甚至一些人流量比较大的商店也是这样。二维码在韩国 的普及率也是非常高，在多年前韩国就有超过一半的人曾使用二维码，现在在韩 国的各大影院大都使用二维码作为电影入场券，观众只要通过手机在互联网上购 买电影票，在准备进入电影院观影检票口时打开手机里生成的二维码放在扫码设 备下进行扫码就可以完成检票程序，这样既节省了纸张，也不用担心票据丢失。 在一些欧美国家中，二维码也使用得比较普遍。在德国，二维码球票很受用户喜 欢，是最受欢迎的二维码应用之一。在英国、美国、加拿大等地区，二维码不仅 可以在机场作为登机牌使用，也可以作为身份证、驾驶证等证件来使用。

在国内，二维码的应用发展起步比较晚，但是发展速度非常快。早在几年前， 前铁道部就将用户的身份信息与票务信息编码成二维码印制在火车票上，然而真 正将二维码推向普通大众的视野里并成为热点的关键是移动互联网。目前移动互 联应用中有相当一部分都应用了二维码，其中以腾讯公司的微信和阿里巴巴公司 的支付宝最具代表性。微信推出了“拍一拍”二维码添加好友功能，方便用户添加 好友。与此同时，微信通过二维码进入“02O”(Online to Offline)领域，打通线 下商家与用户的壁垒。支付宝推出了二维码支付功能，支付宝用户通过支付宝平 台为收款方生成收款二维码，消费者则使用支付宝移动端的二维码扫描功能扫描 收款二维码，然后跳转到付款页面，消费者只需输入支付密码就可以完成支付， 省去了输入账号名、登录密码等流程，提高了支付效率。

随着二维码技术应用的不断发展和深入，二维码的应用领域会不断扩展，成 为了人类生活当中不可或缺的组成部分。目前，二维码已经走进普通大众的生活 里，给人们的生活带来了快捷、便利的用户体验，人们对二维码的关注逐渐增加， 我们有理由相信二维码在中国的发展前景会更加美好。

中国知网 <https://www.cnki.net> 1

信息隐藏技术，通常也称隐写术或密写术。该技术是将秘密信息隐藏在其他 载体信息中，通过载体的传递来实现秘密信息的传递。与传统的密码技术不同的 是，信息隐藏技术能够使秘密信息避开第三方的注意。它与传统的密码技术相结 合能提供更加强大的保密系统，从而更有效地提高秘密信息传递的安全性。

信息隐藏技术的出现和发展与军事和政治有着密不可分的联系[1]。最早的信 息隐藏技术出现在古希腊战争时期，奴隶主通过将信息写在奴隶的光头上，等奴 隶的头发长起来后再去另一个部落，从而实现部落间的秘密通信。中国古代出现 过用藏头诗传递秘密信息。信息隐藏技术在第一世界大战和第二次世界大战也被 使用过[2]。如今，信息隐藏技术已经成为了信息安全领域的研究热点，引起了各 国安全机构、信息安全公司的高度重视。

图像信息隐藏是信息隐藏的重要组成部分，也是与二维码信息隐藏最为相关 的研究课题。目前图像信息隐藏技术已经取得很多成果，各种图像信息隐藏工具 不断出现，如 EzStego[3]、F5[4]、Hide and Seek for Win95、Jpeg-Jsteg[S]、Mandelsteg[6、 OutGuess[7] 、S-Tools v4 、White Noise Storm[8]等。图像信息隐藏技术是最早从实 验室的摇篮发展成为公司产品的信息隐藏技术，它已经成为国家安全机构和企事 业单位传递秘密信息的重要支撑。然而，图像信息隐藏技术开始大量使用的同时， 对图像信息隐藏分析技术的研究也取得了不少成果[9]。Westfeld 等人提出了针对 PoV(pair of values)嵌入技术的直方图分析法，对信息嵌入后每一对像素灰度、 颜色指数、变换系数进行分析，设计了x² 检验来判断有无密写[10]。Fridrich 等人 提出了RS 分析法，利用图像空间相关性，推导出灵敏的双重统计量来判断有无 密写[11]。不仅如此，很多研究成果很有可能受到密级限制没有公开，信息隐藏分 析技术所取得的进展可能远大于目前我们掌握的信息。所以，对图像信息隐藏技 术进行深入的研究具有非常高的研究价值，为保护国家安全和企业机密提供强大 的技术支撑，对保障国家安全、社会稳定和经济的健康发展具有十分重要的意义。

从目前发表的大量研究论文看，图像信息隐藏研究得最多和最深入的是以自 然图像(风景、人物等)为公开载体的信息隐藏，这主要是自然图像内部相关性 大，存在较大的冗余信息，适合进行信息隐藏。自然图像存在的这些冗余信息， 使得我们可以在其中隐藏信息而不会引起第三方的注意。与自然图像相比，非自 然图像内部几乎不存在相关性，能够用于秘密信息传递的冗余信息非常有限，因 此在非自然图像中隐藏信息比较困难。本课题研究的二维码信息隐藏就是一种非 自然图像信息隐藏。

**1.2国内外研究现状**

信息隐藏技术按载体划分，大致可划分为图像信息隐藏[12]、音频信息隐藏[13]、 视频信息隐藏[14]、文本信息隐藏[15~16]。与文本、音频、视频等数字媒体的隐藏技

中国知网 <https://www.cnki.net> 2

术相比，图像信息隐藏技术研究的比较多，方法更容易实现，所以图像信息隐藏 技术的实际应用往往比较多[17~18]。目前，对于图像信息隐藏方面的研究，主要集 中在自然图像(风景、人物等),根据嵌入域的不同，大致可以分为两类：基于图 像空域的信息隐藏和基于图像变换域的信息隐藏。

1)基于图像空域的信息隐藏技术[19]

这类方法通过对图像的像素进行直接或者间接的修改来进行信息隐藏，比如 基于LSB 的方法[20~22]和基于PVD 的方法[23~24]。数字图像的像素值通常由多个比 特来表示，其中最低位对像素值的贡献最小，称为最低比特位 (Least Significant Bits,LSB) 。 基 于LSB 的方法通过修改最低有效位来隐藏信息，方法比较简单， 隐蔽性比较强。基于PVD 的方法则是利用相邻像素值的差，通过改变差的大小隐 藏信息，方法也比较简单，容量比较大。

**2)基于图像变换域的信息隐藏技术**

这类方法一般先对图像进行信号处理得到图像的变换域信息，然后修改图像 变换域信息来隐藏信息，比如F5[4]和outguess[7]。一方面人类视觉对图像变换域 上的变化不敏感，另一方面图像变换域的变化对图像的视觉效果影响极小，所以 人无法感知图像发生变化的事实。这类方法隐蔽性很高，抵抗统计特性分析攻击 能力也很好，但是嵌入容量较小，方法较复杂。

**以上两类方法基本上是对自然图像信息隐藏的研究，接下来介绍二维码(一** **种非自然图像)信息隐藏的研究状况。**

与自然图像信息隐藏相比，非自然图像信息隐藏的研究要少得多微自然图像 通常与客观世界联系比较紧密，图像内容中包含丰富的信息，存在大量的冗余信 息，这使得它更适合也更容易实现信息隐藏。那些非自然图像(比如密文图像、 二维码)包含的信息就单调得多，图像内部并无明显相关性，且人类视觉系统对 这类图像不能得到有价值或者有意义的内容。因此对非自然图像信息隐藏的研究 不能照搬自然图像信息隐藏的研究成果，而需要根据这类图像特殊的性质，挖掘 图像内部的冗余信息，进而研究出适合该类图像的信息隐藏方法。

**二维码信息隐藏是一种非自然图像信息隐藏。二维码不同于自然图像，自然** **图像通过人的视觉系统就能识别图像的内容，但二维码需要解码设备或解码软件** **才能读取图像的内容，因此二维码与自然图像的差异是显而易见的。**

**尽管二维码的应用已经非常普遍，但是二维码信息隐藏技术的研究并不多。** **从目前公开发表的二维码信息隐藏技术研究的文献来看，已有的二维码信息隐藏** **技术大致可分为两类：**

**1)基于变形技术的PDF417(Portable Data File) 二维码信息隐藏技术[25~27]**  **牛夏牧[25]等人首先提出了一种基于变形技术的PDF417 二维码信息隐藏技** **术。PDF417 码是行排式二维码，对条码符号有严格的技术要求，条码符号的误**

中国知网 <https://www.cnki.net> 3

差是有一定范围的，包括符号字符的允许误差和行间水平错误允许误差。因此该 算法利用PDF417 的这个特点，通过变形技术对条码符号的组成单元宽度进行适 当的调整，以误差累积的方式实现秘密信息的嵌入和提取。该方法不易引起察觉， 且具有较大的嵌入容量，能够抵抗一定的打印扫描攻击。

2)基于变换域的QR(Quick Response)二维码信息隐藏技术[28~29]

这类方法根据自然图像信息隐藏技术的方法，将二维码作为普通图像处理， 首先对二维码图形做变换处理，然后将秘密信息嵌入到变换域的中频系数中，最 后做逆变换处理得到隐藏秘密信息的二维码。提取信息时，同样对载密二维码做 变换处理，然后从变换域的中频系数中提取出秘密信息。该方法延续了传统图像 信息隐藏的方式，易于实现，但抵抗打印扫描攻击的能力较弱，没有充分利用二 维码自身所具有的特点。

综合当前二维码信息隐藏研究的状况，关于二维码信息隐藏算法的研究存在 以下几个问题：

1)基于变形技术的二维码信息隐藏算法只适用PDF417 二维码，并不适用其 他类型的二维码，因此适用范围比较小。

2)基于变换域的QR 二维码信息隐藏技术尽管适用于其他二维码，但是该方 法没有考虑二维码的特殊性，只是借鉴自然图像信息隐藏的方法，因此没 有体现出二维码的优势，抵抗打印和扫描攻击的能力较差。

3)虽然已经出现了两类二维码信息隐藏的方法，但是从整体数量上来看，还 是非常少，因此提出新的二维码信息隐藏算法仍然很有意义。

**1.3** **本文主要工作**

本文针对二维码信息隐藏技术进行研究，以二维码编解码为理论基础，从信 息隐藏的基本原理出发，通过深入分析当前二维码信息隐藏算法，总结归纳其优 缺点，提出了一种新的二维码信息隐藏算法；并利用该算法，实现了一个基于 Android 移动平台的二维码信息隐藏系统。

本文研究内容包括以下几个方面：

(1)深入研究了二维码的编码与解码的规则和流程，根据Google 开源项目 Zxing, 实现了一个基于J2SE 的二维码编解码系统。

(2)提出了一种基于Reed-Solomon(R-S) 编码的二维码信息隐藏算法。该 算法利用R-S 编码产生的冗余，将秘密信息嵌入到二维码中，通过该算法，隐藏 信息后的二维码仍然能正常解码并且不会引起人们的注意。理论分析和实验结果 表明本文提出的算法具有较好的不可见性、鲁棒性和较大的嵌入容量。

**(3)利用本文提出的基于R-S** **编码的二维码信息隐藏算法，设计并实现了一** **个Android平台二维码隐蔽通信系统。该系统由载密二维码生成和载密二维码识**

中国知网 <https://www.cnki.net> 4

别组成：发送者将秘密信息隐藏在二维码中，生成载密二维码；接收者通过使用 Android 智能手机对打印在屏幕或者纸质媒介的载密二维码进行识别，读取秘密 信息。经测试表明，该系统达到了本文设计目标。

**1.4论文结构**

第一章首先介绍了本文研究的背景以及研究现状，然后分析并总结了现有研 究存在的优缺点，其次介绍了本文所做的工作以及本文的研究意义，最后概括本 文的结构。

第二章主要介绍与本文相关的理论知识以及相关技术，分别介绍了信息隐藏的 基本理论与模型，图像信息隐藏技术的研究现状，二维码相关技术，Android 相关技 术 。

第三章介绍了本文提出的基于R-S 编码的二维码信息隐藏算法。首先分析了本 文所提出算法的理论基础表明本文所提出的算法是可行的，然后给出了本文所提出 算法详细的实现步骤，最后从不可见性、鲁棒性和容量三个方面对本文所提出的算 法进行了分析。

**第四章介绍了依据本文提出的算法所设计的一个Android 平台二维码隐蔽通信** **系统。**

**最后是论文的结论，总结了全文的工作，并对未来的研究工作进行展望。**



中国知网 <https://www.cnki.net> 5

**第2章基本原理及相关技术**

互联网的迅速发展，极大地提高了人们进行交流的效率，给人们带来了非常 大的便利，但是在带给人们好处的同时也出现了很多问题，其中安全问题尤为严 重。为了解决这一问题，研究人员提出了许多安全通信的方法，信息隐藏正是其 中之一。信息隐藏是一门历史悠久的学科，现代信息隐藏是集图像信息处理、信 息学、多媒体技术、密码学、模式识别、语言学等多领域的交叉学科。本章主要 介绍了信息隐藏相关的理论，简单介绍了信息隐藏的基本原理，然后介绍了与二 维码信息隐藏密切相关的图像信息隐藏，最后介绍了二维码的相关技术规范。

**2.1** **信息隐藏概述**

信息隐藏，又叫隐写术，是集多学科理论与技术于一身的新兴技术领域，它 是利用人类感觉器官对数字信号的感觉冗余，将秘密信号隐藏在另外一个普通信 号中，隐藏后信号依然表现出普通信号的特征，因此并不会改变普通信号的本质 特征和使用价值。与此同时，人类感知系统并不能察觉出秘密信号的存在，只有 通过特殊制作的提取器才能从该信号中提取出秘密信号。

目前信息隐藏是信息安全领域的重要研究热点[30]。它的起源最早可以追溯到 几千年前古希腊时代。在古欧洲时代，当时的人通过调整部分字母笔划高度，在 部分字母附近挖出微小的孔，用来标注这些特殊的字母，通过这些被标注的字母 隐藏秘密信息。Wilkins 对这种方法做了改进，利用无形的墨水在这些特定字母上 制造微小的斑点来传送信息[1]。在第二次世界大战时期，各国情报人员通过多次 照相缩影、缩小到微粒状，然后将这些微粒粘贴在普通报刊杂志等材料的标点符 号上来传递秘密消息[2]。在我国古代，以藏头诗、藏尾诗、漏格诗以及绘画等形 式信息隐藏层出不穷。

**加密技术广泛地被应用于军事、政府或商业的保密信息通信中。虽然这些加** **密算法以纯数学问题或理论为理论依据，有非常严格的数学理论保证算法的稳定** **性和可靠性，但在互联网技术不断发展中，加密算法也存在一些问题**：

**第一，加密算法的安全性。密码学从诞生开始就一直受到密码分析学的挑战。** **随着超级计算机技术的不断发展，计算机计算能力不断提高，密码分析者能够使** **用高性能的计算机来分析密码算法，这对加密算法产生了重大威胁。**

**第二，通过网络传输数据时，密文容易引起第三方注意，因此更容易受到拦** **截和攻击。由于密文是一堆看似无意义的数据，容易引起攻击者注意和攻击。在** **网络传输数据时，密文有可能被拦截，导致无法及时传递秘密信息，也有可能被**

中国知网 <https://www.cnki.net> 6

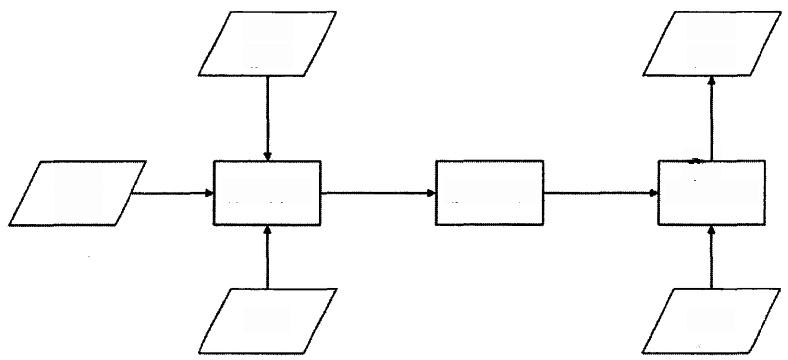
攻击者进行分析，甚至被破译。

第三，加密算法的局限性。加密算法对保密数据的存储和传输具有非常大的 意义，但是它不能解决数字信息的防盗版和版权保护等问题。

在当今互联网浪潮中，现有加密技术已经不能满足人们对数字信息安全性方 面的需求，并且数字内容的保护迫在眉睫，这些激励着研究人员开始将研究视线 转移到了信息隐藏技术上来。

**2.1.1** **信息隐藏常用框架**

一般而言，信息隐藏的常用框架如图2. 1所示，它主要包括嵌入部分和提取 部分[31]。



秘密 信息

提取算法

密钥

秘密 信息

载体 信息

信道传播

嵌入算法

密钥



**图2.1** **信息隐藏常用框架**

秘密信息，是发送方要求保密的信息，有且仅有指定的接收方才可以提取到 该信息；载体信息，是在公开信道传递的信息，对任何第三方都是可见的，通常 是图像、音频、视频等数字媒体。信息隐藏一般都会带密钥，但也可以不带密钥， 信息隐藏中密钥与密码学中的密钥是不一样的，该密钥更多的时候只是用于确定 嵌入位置，嵌入算法将秘密信息嵌入到载体信息特定的嵌入位置中，而提取算法 利用密钥从伪装载体中特定嵌入位置中提取秘密信息。

**2.1:.2信息隐藏分析技术**

信息隐藏分析技术，又叫隐写分析，是信息隐藏的对立技术。我们可以用“盾” 和“矛”来形象地解释信息隐藏和信息隐藏分析技术。信息隐藏是“盾”,用来保护 秘密信息被任何第三方窥探；信息隐藏分析技术则是“矛”,当数据在公开

信道中传输时，任意第三方可以对数据进行监控并拦截，对拦截的数据进行分析，

**确定其中是否存在秘密信息，如果确认存在秘密信息，则尝试破坏或者获取秘密**

信息。

**隐写分析技术通过对公开信道中传输的数据进行捕捉与分析，判断该数据中**

中国**知网** [**https://www.cnki.net**](https://www.cnki.net)7

是否存在秘密信息，并试图提取出该秘密信息的技术。检测秘密信息是否存在是 提取出该信息的前提条件，也是隐写分析要解决的最基本的问题，因此检测秘密 信息的存在性是目前隐写分析研究者最关注的问题。

检测秘密信息存在性的问题可以转化为模式识别当中的分类问题，而且是最 简单的二分类问题。所有被检测对象只属于“存在秘密信息”与“不存在秘密信息” 两者中的一种，因此解决该问题就是要构造一个这样的分类器。

该分类器是为了区分普通载体与隐写载体，主要是通过普通载体和隐写载体 表现出的统计特征进行判断。分类器的一般工作过程为，依据所选取的统计特征， 用标定样本训练分类器，从而构造出了适合当前分类的分类模型，再用测试样本 进行分类，得到分类结果。衡量分类器的性能有三个技术指标，分别是准确率、 虚警率和漏警率。准确率是指正确判断出含有秘密信息样本占所有含秘密信息样 本的比率。虚警率是指错误判断出含有秘密信息样本占所有含秘密信息样本的比 率。漏警率是指本含有秘密信息却未被判断出的样本占所有含秘密信息样本的比 率。

目前隐写分析技术能够做的工作还是比较有限，即使针对单一隐写方法进行 检测，正确率也并非100%,更没有针对所有隐写方法的隐写分析技术。 一般而 言，一种隐写分析技术仅针对一种或者一类隐写方法有效。隐写分析与信息隐藏 是“矛”与“盾”的关系，两者相互对抗，相互促进。一旦有新信息隐藏技术的诞生， 就会有新隐写分析技术的出现。一旦有新隐写分析技术的出现，就会有新信息隐 藏技术的诞生。

**2.1:.3信息隐藏的特征**

与加密技术不同，信息隐藏技术是为了不影响普通载体使用的条件下，对秘 密信息进行隐藏，保证秘密信息不被发现或者破坏，因此信息隐藏技术拥有加密 技术没有的一些特点或要求。依据应用场景的不同，信息隐藏技术所表现的特点 也会有所差异，其基本特征大致有以下三个：

(1)不可见性

不可见性，又常称为隐蔽性，它是指当我们利用嵌入算法嵌入信息后，不会 引起伪装对象和载体产生可感知的差异，也就是说伪装对象与载体应该是不可区 分的，否则就意味这信息隐藏的失败，无法达到隐蔽通信的目的。在某些应用中， 为了获得高鲁棒性和低成本，只要造成的部分失真不会降低原载体的价值，我们可 以接受适度可感知的隐藏。

(2)鲁棒性

鲁棒性是指伪装对象经过若干正常的信号处理或者遭遇攻击者恶意攻击之 后，接收方依然能够通过提取算法从受干扰或者受攻击的伪装对象中提取出秘密

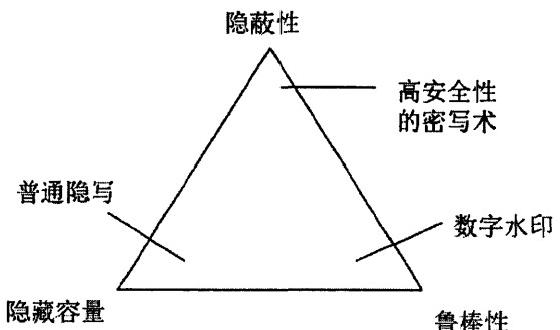
中国知网 <https://www.cnki.net> 8

信息的能力。这些信息处理或者恶意攻击包括常见的信息处理，如数据有损压缩、 图像增强处理、低通滤波处理、二次抽样、二次量化处理、数模之间的转换等； 几何变换，如裁剪、平移、旋转、尺度拉伸、扭曲等操作；文本格式重排版编辑； 噪声干扰；多重水印重叠等。具有较好鲁棒性的信息隐藏技术通常要求在经过这 些变化或者攻击之后，能够从伪装对象中提取出秘密信息。

(3)嵌入容量

嵌入容量是指该信息隐藏算法能够隐藏秘密信息的量的大小，是信息隐藏非 常重要的评价指标。从通信的角度来分析，秘密信息是通信的主体，嵌入容量正是 衡量通信的有效信息量，嵌入容量越大，能够在单次通信中传递的有效信息也就越 多。通常，嵌入容量与不可见性是矛盾的，嵌入的信息量越大，对载体造成的影响 也越大，伪装对象与原始载体的区别也就越大，所以不可见性自然而然就会减低。 因此，我们在具体的信息隐藏过程中，要寻找一个合适的点，既要使得单次通信的 信息量大，又要保证伪装对象和原始载体是不可区分的。

在一个隐蔽通信系统中，不可见性、鲁棒性和嵌入容量是非常重要的评价标 准，它们之间的关系又是相互矛盾的，如图2.2所示。不可见性越高，鲁棒性和 嵌入容量就会相应的降低；鲁棒性升高，不可见性与嵌入容量也会出现降低；嵌 入容量高也就意味着对原始载体的修改量会比较大，会造成鲁棒性和不可见性的 降低。因此要根据具体的应用场景选择合适的组合。



**图2.2隐蔽性、隐藏容量和鲁棒性的关系**

**2** **.** **1** **.4信息隐藏的分类**

信息隐藏分类标准有很多种，根据常见的分类标准，主要有以下几类：

(1)载体类型

根据载体类型不同，分为文档信息隐藏、图像信息隐藏、音频信息隐藏、视 频信息隐藏等。图像是使用范围最广，同时在很多方面上来看都适合信息隐藏， 因此以数字图像为载体的信息隐藏技术是最多的。

中国知网 <https://www.cnki.net> 9