可下载教学资料

http://www.tup.tsinghua.edu.cn

高等学校教材

计算机科学与技术

信息隐藏原理及应用

葛秀慧 田浩 郭立甫 韩缇文 编著

清华大学出版社

高等学校教材

计算机科学与技术

信息隐藏原理及应用

葛秀慧 田浩 郭立甫 韩缇文 编著

清华大学出版社

北京

内 容 简 介

本书全面系统地论述了信息隐藏的概念、分类、应用、理论与原理。书中重点介绍了信息隐藏的基本原理，并分析了与其相关的典型算法，以丰富的实例进行说明，同时提供了部分源代码。另外还详细讨论了数字水印技术与算法，探讨了隐写分析与隐蔽通信。

本书可以作为计算机应用、网络工程、通信与信息系统、信号与处理、信息安全与密码学、电子商务专业的本科生和研究生的教材，也可供从事信息安全研究及应用的学者、技术人员参考。

图书在版编目(CIP)数据

信息隐藏原理及应用/葛秀慧等编著. —北京：清华大学出版社，2008.10
(高等学校教材·计算机科学与技术)
ISBN 978-7-302-18324-2

Ⅰ. 信… Ⅱ. 葛… Ⅲ. 信息系统－安全技术－高等学校－教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2008)第 118316 号

责任编辑：闫红梅　林都嘉
责任校对：焦丽丽
责任印制：杨　艳
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京市清华园胶印厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：10.25　**字　数**：250 千字
版　　次：2008 年 10 月第 1 版　　**印　　次**：2008 年 10 月第1次印刷
印　　数：1～2500
定　　价：18.00 元

高等学校教材·计算机科学与技术

编审委员会成员

（按地区排序）

清华大学	周立柱	教授
	覃　征	教授
	王建民	教授
	刘　强	副教授
	冯建华	副教授
北京大学	杨冬青	教授
	陈　钟	教授
	陈立军	副教授
北京航空航天大学	马殿富	教授
	吴超英	副教授
	姚淑珍	教授
中国人民大学	王　珊	教授
	孟小峰	教授
	陈　红	教授
北京师范大学	周明全	教授
北京交通大学	阮秋琦	教授
北京信息工程学院	孟庆昌	教授
北京科技大学	杨炳儒	教授
石油大学	陈　明	教授
天津大学	艾德才	教授
复旦大学	吴立德	教授
	吴百锋	教授
	杨卫东	副教授
华东理工大学	邵志清	教授
华东师范大学	杨宗源	教授
	应吉康	教授
东华大学	乐嘉锦	教授
上海第二工业大学	蒋川群	教授
浙江大学	吴朝晖	教授
	李善平	教授
南京大学	骆　斌	教授
南京航空航天大学	秦小麟	教授
南京理工大学	张功萱	教授

南京邮电学院	朱秀昌	教授
苏州大学	龚声蓉	教授
江苏大学	宋余庆	教授
武汉大学	何炎祥	教授
华中科技大学	刘乐善	教授
中南财经政法大学	刘腾红	教授
华中师范大学	王林平	副教授
	魏开平	副教授
	叶俊民	教授
国防科技大学	赵克佳	教授
	肖　侬	副教授
中南大学	陈松乔	教授
	刘卫国	教授
湖南大学	林亚平	教授
	邹北骥	教授
西安交通大学	沈钧毅	教授
	齐　勇	教授
长安大学	巨永峰	教授
西安石油学院	方　明	教授
西安邮电学院	陈莉君	副教授
哈尔滨工业大学	郭茂祖	教授
吉林大学	徐一平	教授
	毕　强	教授
长春工程学院	沙胜贤	教授
山东大学	孟祥旭	教授
	郝兴伟	教授
山东科技大学	郑永果	教授
中山大学	潘小轰	教授
厦门大学	冯少荣	教授
福州大学	林世平	副教授
云南大学	刘惟一	教授
重庆邮电学院	王国胤	教授
西南交通大学	杨　燕	副教授

出版说明

改革开放以来，特别是党的十五大以来，我国教育事业取得了举世瞩目的辉煌成就，高等教育实现了历史性的跨越，已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上，高等教育规模取得如此快速的发展，创造了世界教育发展史上的奇迹。当前，教育工作既面临着千载难逢的良好机遇，同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾，是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月，教育部下发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》，提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月，教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件，指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分，精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间（2003—2007 年）建设 1500 门国家级精品课程，利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放，以实现优质教学资源共享，提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展、顺应并符合新世纪教学发展的规律、代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的

前瞻性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1) 高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 高等学校教材·电子信息——高等学校电子信息相关专业的教材。

(4) 高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5) 高等学校教材·信息管理与信息系统。

(6) 高等学校教材·财经管理与计算机应用。

清华大学出版社经过20年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

E-mail: dingl@tup.tsinghua.edu.cn

前言

信息是人类社会和国家发展的重要战略资源。随着科学技术的快速发展，传统媒体内容正在向数字化转变。数据的交换与传输也变得更加快捷。但随之而来的日益严重的知识产权侵犯行为和基于加密的安全措施面临的严峻挑战，使得信息隐藏技术重新焕发活力。

信息隐藏是与数学、密码学、信息论、计算机视觉以及其他计算机应用技术等多学科交叉的学科，是各国研究者所关注和研究的热点。在信息隐藏研究中，可以分为基础理论研究、应用基础研究和应用研究。其中基础理论研究是建立图像信息隐藏的理论框架和若干理论模型，解决安全性度量、通信量分析等基本理论问题，以揭示信息隐藏中若干基本矛盾。信息隐藏的应用基础研究主要针对典型应用需求，研究各种信息隐藏算法和评估体系。信息隐藏的应用研究以图像信息隐藏技术的实用化为目的，研究针对各种应用的实用系统。

信息隐藏利用人类感知及数字媒体自身的冗余，将秘密信息嵌入到载体中，以对载体的使用进行跟踪，从而达到版权保护、完整性认证等目的。作为一门迅速发展的新兴交叉学科，开展其理论与关键技术的研究，具有巨大的军事和经济价值。计算机技术的发展日新月异，信息隐藏技术也不例外，还会不断涌现出新算法、新应用以及新的发展思路。

本书旨在向读者介绍这一充满活力的领域中的基本理论原理及典型算法，并介绍了三个主要分支的研究情况，以期起到抛砖引玉的作用。

本书共分 8 章。第 1 章介绍信息隐藏技术应用分类，以及数字水印及隐写术在信息安全中的地位。第 2 章介绍信息隐藏的基本原理并讨论隐写系统的分类及术语。第 3 章讨论了信息隐藏的预处理，主要涉及相关加密领域的算法及知识。第 4 章介绍隐写术的模型及数字水印模型。第 5 章分析典型的信息隐藏算法，包括位平面算法、调色板算法、空域算法及频域算法，同时还讨论融合算法。第 6 章重点介绍数字水印技术及相关典型算法与技术。第 7 章讨论隐蔽通信，主要探讨 TCP/IP 中的隐蔽通信。第 8 章介绍隐写分析技术及相应评价指标，并分析了通用原形系统的相应算法。

对于这一领域，作者的研究可能只是以管窥豹，仅见其一斑，肯定存在不足之处，希望研究这一领域的同行给予批评和指正。

书中难免会存在问题，欢迎广大读者给予批评指正。

编　者

2008 年 4 月

目 录

第 1 章 简介 …… 1

1.1 引言 …… 1
1.2 隐写术概述 …… 3
1.3 数字水印概述 …… 5
1.4 隐蔽通信概述 …… 7
1.5 信息隐藏的应用 …… 8
1.6 隐写算法综述 …… 10
1.7 隐写分析概述 …… 13
1.8 信息隐藏当前研究现状与存在问题 …… 16
1.9 本章小结 …… 17
1.10 因特网资源 …… 17
1.11 复习题 …… 18

第 2 章 信息隐藏基本原理 …… 19

2.1 信息隐藏的基本原理与分类 …… 19
2.1.1 纯隐写术、密钥隐写术和公钥隐写术 …… 20
2.1.2 文本、音频、图像的隐写 …… 22
2.1.3 音频中的隐写 …… 24
2.2 信息隐藏的主要术语 …… 26
2.3 数字水印系统的构成与分类 …… 28
2.3.1 数字水印系统 …… 29
2.3.2 数字水印、隐写术与加密术的区别 …… 30
2.3.3 数字水印的分类 …… 30
2.3.4 数字水印的特性与术语 …… 31
2.4 本章小结 …… 32
2.5 复习题 …… 32

第 3 章　信息隐藏的预处理 …… 33

3.1　加密的预处理 …… 33
3.1.1　伪随机数发生器 …… 33
3.1.2　RC4 流密码 …… 35
3.2　简单的图像信息伪装技术 …… 37
3.3　置乱 …… 37
3.4　混沌 …… 42
3.5　本章小结 …… 44
3.6　复习题 …… 44

第 4 章　信息隐藏模型 …… 45

4.1　隐写术模型分析 …… 45
4.1.1　Simmons 模型分析 …… 45
4.1.2　通信系统模型分析 …… 46
4.1.3　隐写术的安全模型分析 …… 47
4.1.4　基于通信的水印模型 …… 48
4.2　数字水印空间模型 …… 48
4.3　感知模型 …… 49
4.3.1　人类感知 …… 49
4.3.2　评价的基本指标 …… 50
4.3.3　Watson 感知模型 …… 50
4.4　本章小结 …… 51
4.5　复习题 …… 51

第 5 章　信息隐藏算法 …… 52

5.1　信息隐藏算法概述 …… 52
5.2　位平面算法 …… 53
5.2.1　位平面算法概述 …… 53
5.2.2　位平面算法实现 …… 53
5.2.3　嵌入算法步骤和程序 …… 55
5.2.4　实验和实验结果分析 …… 57
5.3　调色板算法 …… 59
5.3.1　调色板算法原理 …… 59
5.3.2　调色板信息隐藏算法实现 …… 60
5.3.3　调色板信息隐藏算法容量实验 …… 62
5.4　空域信息隐藏算法 …… 65

5.4.1 最低有效位算法原理 …… 65
5.4.2 最低有效位算法实验 …… 66
5.4.3 Hide and Seek 隐写软件分析与实验 …… 67
5.5 频域变换信息隐藏算法 …… 70
5.5.1 离散傅里叶变换 DFT …… 70
5.5.2 离散余弦变换 DCT …… 75
5.6 小波域信息隐藏算法 …… 85
5.6.1 离散小波变换 DWT …… 85
5.6.2 小波变换实现信息隐藏 …… 91
5.7 统计算法 …… 94
5.8 图像融合算法 …… 95
5.9 本章小结 …… 97
5.10 因特网资源 …… 97
5.11 复习题 …… 97

第 6 章 数字水印 …… 98

6.1 数字水印算法概述 …… 98
6.2 空域数字水印算法 …… 99
6.2.1 最低有效位算法 …… 99
6.2.2 Patchwork 算法 …… 100
6.3 变换域算法 …… 102
6.3.1 DCT 算法 …… 103
6.3.2 DWT 算法 …… 105
6.4 可见与不可见数字水印算法 …… 107
6.5 可逆水印概述 …… 110
6.5.1 可逆数字水印现有算法 …… 111
6.5.2 基于纠错编码的差值扩展可逆数字水印 …… 112
6.6 免疫数字水印算法 …… 116
6.6.1 SRIW 形式化描述 …… 116
6.6.2 SRIW 实现方法 …… 117
6.6.3 SRIW 安全性分析及评价标准 …… 118
6.7 多重数字水印 …… 120
6.7.1 多重数字水印概述 …… 120
6.7.2 鲁棒性和脆弱性相结合的双重数字水印 …… 121
6.7.3 基于 CDMA 的多重数字水印算法 …… 124
6.8 本章小结 …… 125
6.9 复习题 …… 125

第 7 章　隐蔽通信 …… 126

7.1　隐蔽通信概述 …… 126
7.2　隐蔽通道 …… 127
7.3　TCP 隐蔽通信 …… 128
7.3.1　TCP 协议概述 …… 128
7.3.2　TCP 隐蔽通信的实现 …… 130
7.4　IGMP 中的隐蔽通信 …… 132
7.5　IP 中的隐蔽通信 …… 134
7.6　本章小结 …… 137
7.7　复习题 …… 137

第 8 章　隐写分析技术 …… 138

8.1　隐写分析概述 …… 138
8.1.1　隐写分析定义 …… 138
8.1.2　隐写分析分类 …… 138
8.2　隐写分析评价指标 …… 140
8.3　隐写分析通用原型系统 …… 141
8.4　隐写分析算法 …… 141
8.4.1　专用隐写分析算法介绍 …… 141
8.4.2　通用隐写分析算法介绍 …… 142
8.4.3　GPC 隐写分析法 …… 143
8.5　本章小结 …… 146
8.6　复习题 …… 146

参考文献 …… 147

第1章

简　介

本章目标

- 理解信息隐藏技术。
- 了解书中讨论重要主题的概况。
- 理解隐写术、数字水印和隐蔽通信。
- 理解隐写术和数字水印在信息安全中扮演的中心角色。

在“引言”之后，本章先介绍信息隐藏的三个重要分支，即隐写术、数字水印和隐蔽通信；然后简要介绍本书的每一部分。

1.1 引　言

随着网络的应用越来越普及，信息安全成为很热门的研究领域，信息安全主要分为两大领域——加密技术与信息隐藏技术，本书主要介绍和研究信息隐藏技术。

信息隐藏是一门交叉学科，它涉及数学、密码学、信息论、计算机视觉以及其他计算机应用技术，是各国研究者所关注和研究的热点。其原理是利用载体中存在的冗余信息来隐藏秘密对象，以实现保密通信或者实现数字签名和认证。信息隐藏与信息加密是不尽相同的，信息加密是隐藏信息的内容，而信息隐藏是隐藏信息的存在性，信息隐藏比信息加密更为安全，因为它不容易引起攻击者的注意。但两者又不能截然分开。信息隐藏打破了传统密码学的思维范畴，从一个全新的视角审视信息安全。与传统的加密相比，信息隐藏的隐蔽性更强，在信息隐藏中，可以把这两项技术结合起来，先将秘密信息进行加密预处理，然后再进行信息隐藏，则秘密信息的保密性和不可觉察性的效果更佳。

信息隐藏技术的推动力有两个方面：第一方面是需要保护知识产权的用户。目前通过互联网，信息能被轻易地传递和复制，这使信息的知识产权变得更难保护。数字水印技术的使用提供了在文档或图像中插入版权提示，用于保护信息的知识产权。数字水印经常是小的图像或文本，在整个文档或图像中不断地重复。相似的技术是嵌入数字指纹和系列号。指纹的优势在于它能用于追踪对源文件的复制以及可以作为起诉的有力工具。

第二方面是对隐藏信息有兴趣的人们，希望以秘密的方式传送信息并且避免第三方接收者的察觉。在这种情况下，隐藏的信息比用来运送它的载体更重要。隐写术经常与加密

术一起用于限制未授权的信息访问。加密术是指通过加密或者以打乱信息的方式来使信息只能到达指定接受者并解密信息。当发送加密的信息时就明显地表明，已经发生了某种形式的通信，并发送了加密的消息，使消息不能被非指定的对象解读。隐写术经常用来隐藏消息的存在。

在信息隐藏中，目前广泛使用的是数字水印技术、隐写术和隐蔽通信。数字水印和隐写术是信息隐藏的两个重要分支。在20世纪90年代早期，与加密技术相比，信息隐藏技术并没有引起学术界的更多关注。但是随着计算机和网络通信技术的发展与普及，数字化的音像制品和其他电子出版物的传播和交易变得越来越便捷，未授权的复制和侵权盗版行为日益严重。在这种大背景下，信息隐藏这一古老的技术重新焕发了活力。研究者首先想到的就是在数字产品中藏入版权信息和产品序列号以防止侵权行为。随着研究的进一步深入，目前信息隐藏技术越来越受到各届的关注，主要是因为版权的拥有者想保护其版权不被盗版，所以信息隐藏中的数字水印技术得到了空前的发展，目前广泛使用于音乐、电影、书籍和软件的防盗版中。

信息隐藏具备的特性如下。

- 不可感知性(imperceptibility)　有时也称为隐蔽性。这一特性是信息隐藏最必要的条件。载入信息的伪装载体与原载体(没有嵌入秘密信息的载体)应当大体上是很接近的，从人的视觉上应该感觉不到任何变化。传统的信息隐藏是将秘密信息嵌入到一般信息中，使得人只看到一般信息，而看不到秘密信息。在不改变原有信息内容的前提下，使一般信息与秘密信息的总体容量远远超过一般信息的容量，这样，传输速度会减慢，也会使人生疑，从而使秘密信息被截获的几率加大。所以，对于信息隐藏而言，重要的是，载体在加载秘密信息前后的大小一般不应变化很大。
- 不可检测性(undetectable)　不可检测性是信息隐藏的目的，如果检测到信息隐藏的存在，说明信息隐藏本身已经失败。
- 容量(capacity)　在保证不可感知性和不可检测性的前提之下，希望载体能嵌入的数据容量越大越好，但容量增大，会降低不可感知性和不可检测性，所以要均衡这三种特性。秘密信息容量越大，隐藏的难度系数越大；图片要比文本更难隐藏；秘密信息与载体信息越接近，保密的效果就会越好。
- 鲁棒性(robustness)　是指嵌入水印后的数据经过各种处理操作和攻击操作以后，不导致其中的水印信息丢失或被破坏的能力。攻击操作一般包括模糊、几何变形、放缩、压缩格式变换、剪切等。
- 安全性(security)　指水印不易被复制、伪造、非法检测和移去，文件格式的变换不会导致水印丢失。
- 复杂性(complication)　指水印的嵌入和提取算法复杂度低，便于推广应用。

在互联网开放的环境中，正在广泛使用着各种信息隐藏工具，信息隐藏工具是一把双刃剑，既可以保护信息的安全，也可为恐怖分子所利用，所以研究信息隐藏有很重要的意义。

下面分别概括性地介绍信息隐藏中的三个重要领域：隐写术、数字水印和隐蔽通信。

1.2 隐写术概述

隐写术(steganography)来自于希腊词根 $\sigma\tau\varepsilon\gamma\alpha\nu\square\zeta$,$\gamma\rho\alpha\varphi\varepsilon\iota\nu$,含义是隐写。它的起源可以追溯到公元前 440 年。隐写术有史可考的第一个记录是希腊史学家 Herodotus 的叙述。在由 Herodotus 写的历史记录中,给出了两个隐写术的例子。第一个是 Demeratus 的例子。在波斯的一个希腊人,为了通知即将到来的入侵,他在木板上写上信息并用腊涂在木板上,信息不见了,信使成功地将空白的木板带到了斯巴达。第二个是 Histiaeus 的例子,他剪去了他最信任的奴隶的头发,然后将信息刺到它的头上。当这个奴隶的头发长出来后,再派他发送这些隐藏的信息。

隐写术的最普通形式是使用看不见的墨水来写消息。在第二次世界大战期间,有很多联军使用这种方法。这些消息经常使用果汁、牛奶或者尿来写,当加热这些消息的载体时,将变黑显示消息。当隐写墨水技术已经很容易地被破解时,人们开始使用 null ciphers,这个词是指未加密的信息,对第三方而言,是很难觉察的。如下面的一个例子:

Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

取每个词中的第三个字母,就得出了其中隐藏的消息:

```
Send Lawyers,Guns, and Money.
```

在第二次世界大战中德军发明了微点技术(microdots),该技术将重要的情报缩小数十倍,伪装成任何印刷品的字母或标点符号,有效地传递大量情报。美国联邦调查局局长胡佛(FBI Director J. E. Hoover)还曾夸赞德国人的发明真是间谍活动的一大杰作。微点技术处理过的情报,需要在接收方使用显微镜能阅读这些情报,对于非知情者而言,通常根本觉察不到通过微点技术处理信息的存在。

隐写术提供了缩微拍摄的可能性,它可以在衣服或行李的间隔中私带秘密。在西班牙对普鲁士的战争中很流行。在 21 世纪,政府已经开始使用隐写术来保护真钞,来防止假钞。它们使用特殊的油墨、染料、嵌入线和微波等来鉴别钞票的真伪。随着 Internet 技术的成长,隐写术也继续发展。

目前隐写术最常见的用法是将秘密信息隐藏到另一个载体中,载体可以是图像、音频、视频和文本或者其他二进制数字编码。隐藏的信息可以是纯文本、密码图像或者其他比特流。网络中使用的大部分文件格式是. bmp,. doc,. gif,. jpeg,. mp3,. txt 和. wav 等。载体和隐藏的信息生成了伪装载体。隐写密钥可以进一步保证隐藏信息的安全性。隐写处理的过程可以概括如下:

```
cover medium + hidden information + stego - key = stego - medium
```

其中掩密密钥(stego-key)可以用于隐藏和对信息解码。隐写术需要特定的软件。使用隐写术的目标是:在传输隐藏信息时避免引起注意。如果引起注意,则隐写失败。

在人类视觉上并不能感知到隐写术处理后的图像质量的下降,因此在互联网上的任何

图像都可以隐藏信息，并且不被怀疑。在美国*USA Today*杂志上的一篇文章写道：恐怖组织使用隐写术进行信息交流而没有被发现。根据美国专家分析，这篇文章缺乏技术信息来支持这个论点。但是在网络快速发展的今天，人们无时无刻不在使用网络进行信息的共享和交流，安全的通信环境是人人所需要的，而使用隐写术正好能够完成个人的安全私密通信。

在数字世界中，隐写术和加密术都是保护信息不被未授权的第三方看到，都是保护信息的很好手段。但是这两种技术都不是无懈可击的，都可能被破解。这就是专家建议使用这两种技术来保护信息的原因所在。此外，隐写术还经常使用在很重要的领域。如在某种情况下，不能自由通信，甚至是在受监控的情况下，为了保护秘密通信而又不想使用加密来引起怀疑的情况下，使用隐写术是一种很好的选择。

隐写术是未来的互联网安全中很重要的一部分，也是在开放的环境中如何保护私密性的关键技术。隐写研究的推动力基本在于自身加密系统的局限性以及需要在开放环境中完全的私密性。经过隐写术处理过的文件，一般察觉不到隐蔽信息的存在，这样只有接收方才能知道隐藏信息的存在并能提取这些秘密消息。可以这样说，隐写术完全满足了人们对私密通信的需求。

下面给出将密文放入一幅.bmp文件中的例子。密文是密钥，密钥是经过加密算法生成的，需要经过Internet这种开放的环境传送出去。通过编写的隐写软件，将密钥嵌入了原始图片。如图1.1和图1.2所示，对读者而言，这两幅图是相同的，但在第二幅图中已经嵌入了密钥，所以对第三方而言，是感觉不到密钥的存在的，这样就达到了秘密传输密钥的目的。当接收者接收到图像，可以用隐写软件提取出密钥。

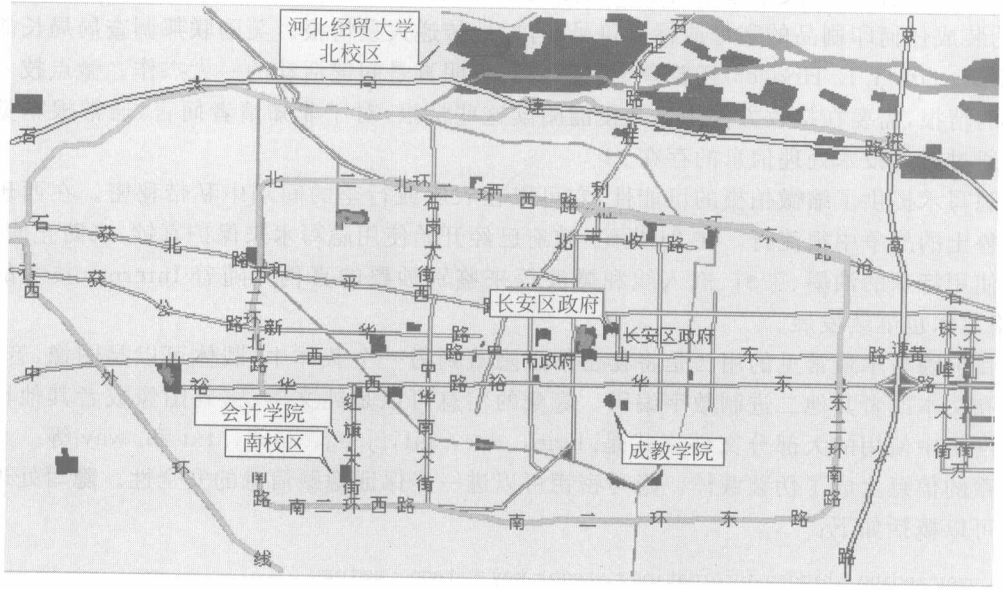

图1.1　原始图像

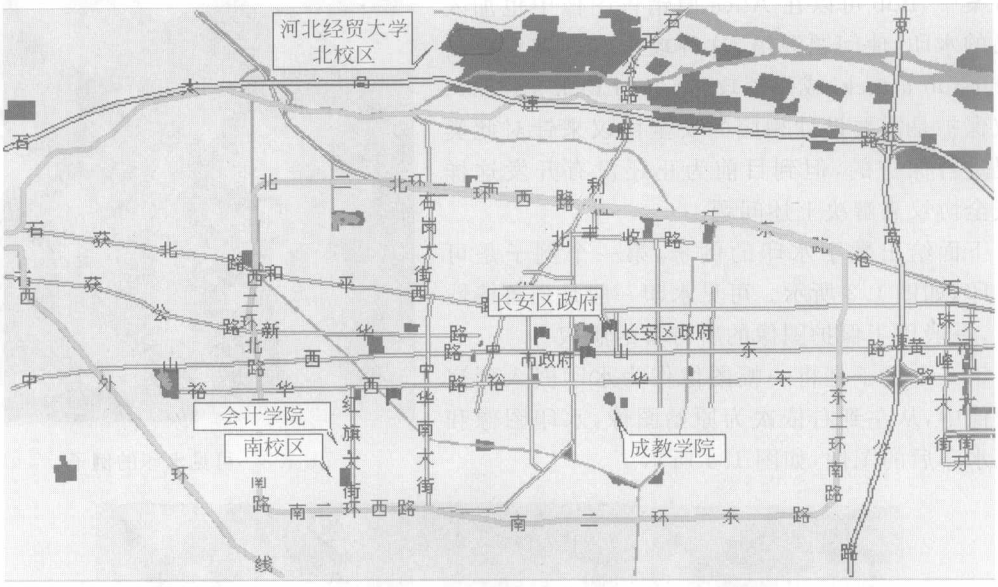

图 1.2　嵌入密钥的图像

1.3　数字水印概述

水印可以追溯到德语词汇“wassermarke”，纸水印在 1282 年出现在意大利，这些最早的水印是通过纸模中加细线模板制造出来的，在有细线的区域，纸更透明、更薄。早期的功能是识别纸的制造商。到 18 世纪，欧洲和美国制造的产品中，纸水印用于纸币和其他文件的防伪。对于数字水印(digital watermarking)，不同的人有不同的理解，但一般而言数字水印就是不可觉察地将秘密信息嵌入载体信号来传送秘密数据。将信息嵌入到其他对象/信号的过程称为嵌入水印。数字水印经常用于版权保护和拷贝保护，其主要应用是图像/视频的版权保护，拷贝保护是指限制或禁止未授权的保护。拷贝保护的最好例子是加密的数字 TV 广播，通过使用许可服务器和访问控制来保护软件的合法使用。版权保护是将版权信息插入到数字对象而对数字对象的质量没有任何损害。当产生数字对象的版权纠纷时，可以从数字对象中提取嵌入信息来证明数字对象的所有者。它可以广泛用于未授权复本的追踪。关于水印最原始的论文是在 13 世纪。由于许多摄影师并不十分信任非可见水印，所以目前的可见水印都是将自己独特的标识直接嵌入到载体之上。在 17 世纪，法国 Claude Lorrain 引入了水印方法来保护自己的版权，在 1710 年英国引入了版权法。

可以通过一个例子来说明如何进行版权保护。Alice 是版权的所有者，她将自己的水印信息嵌入了载体对象，锁定了原载体并开始销售带有水印的图像。Bob 试图将自己的水印嵌入到 Alice 处理过的伪装载体。然后锁定再次嵌入水印的图像并进行销售。为了证明图像的所有者，Alice 和 Bob 都能提取相应的水印来证明自己是拥有者。从前面的叙述中可知，Alice 的销售图像中只拥有自己的水印，而 Bob 销售的图像中还包含 Alice 的水印。这是否就可以表明，Bob 不是销售图像的所有者。但是，情况并非如此简单，在各种不同的水