中国电子教育学会高教分会推荐

普通高等教育电子信息类“十三五”课改规划教材

信息隐藏技术

任 帅　张 弢　编著

西安电子科技大学出版社
http://www.xduph.com

中国电子教育学会高教分会推荐
普通高等教育电子信息类“十三五”课改规划教材

信息隐藏技术

任帅　张弢　编著

西安电子科技大学出版社

内 容 简 介

本书系统地介绍了信息隐藏技术的基础理论、关键技术和实现方法，讲解了信息隐藏技术所涉及的主要学习和研究内容。其主要内容包括信息隐藏技术概念、研究意义和应用领域；对基于数字图像和三维模型的信息隐藏区域和隐藏规则以及相关基础理论；利用优势理论按照空间域/变换域的分类规则进行信息隐藏算法设计；按照对算法性能的贡献点对算法进行分解，将其扩展为一个完整的信息隐藏系统；最后对系统的安全性进行理论和分析案例展示。

本书可作为计算机科学与技术、控制科学与工程、信息与通信工程，尤其是网络空间安全相关学科的研究生和本科生的教材，也可以作为安全领域的科研技术人员的参考书。

图书在版编目(CIP)数据

信息隐藏技术/任帅，张弢编著. —西安：西安电子科技大学出版社，2017.3

ISBN 978-7-5606-4404-2

Ⅰ. ① 信… Ⅱ. ① 任… ② 张… Ⅲ. ① 信息系统—安全技术 Ⅳ. ① TP309

中国版本图书馆 CIP 数据核字(2017)第 039793 号

策　　划　毛红兵
责任编辑　刘炳桢　毛红兵
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西利达印务有限责任公司
版　　次　2017 年 3 月第 1 版　2017 年 3 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印张 9
字　　数　204 千字
印　　数　1～3000 册
定　　价　22.00 元
ISBN 978-7-5606-4404-2/TP

XDUP 4696001-1

中国电子教育学会高教分会

教材建设指导委员会名单

主　任　李建东　西安电子科技大学副校长

副主任　裘松良　浙江理工大学校长

韩　焱　中北大学副校长

颜晓红　南京邮电大学副校长

胡　华　杭州电子科技大学副校长

欧阳缮　桂林电子科技大学副校长

柯亨玉　武汉大学电子信息学院院长

胡方明　西安电子科技大学出版社社长

委　员(按姓氏笔画排列)

于凤芹　江南大学物联网工程学院系主任

王　泉　西安电子科技大学计算机学院院长

朱智林　山东工商学院信息与电子工程学院院长

何苏勤　北京化工大学信息科学与技术学院副院长

宋　鹏　北方工业大学信息工程学院电子工程系主任

陈鹤鸣　南京邮电大学贝尔英才学院院长

尚　宇　西安工业大学电子信息工程学院副院长

金炜东　西南交通大学电气工程学院系主任

罗新民　西安交通大学电子信息与工程学院副院长

段哲民　西北工业大学电子信息学院副院长

郭　庆　桂林电子科技大学教务处处长

郭宝龙　西安电子科技大学教务处处长

徐江荣　杭州电子科技大学教务处处长

蒋　宁　电子科技大学教务处处长

蒋乐天　上海交通大学电子工程系

曾孝平　重庆大学通信工程学院院长

樊相宇　西安邮电大学教务处处长

秘书长　吕抗美　中国电子教育学会高教分会秘书长

毛红兵　西安电子科技大学出版社社长助理

前　言

随着 Internet 的飞速发展，信息传播变得更加方便和快捷，但同时也给信息安全问题带来了巨大挑战。信息隐藏技术以传输的存在性和信息的隐蔽性为信息安全传输提供了可靠的技术手段。

本书以数字图像和三维模型作为信息隐藏载体，讲授基于数字图像和三维模型的信息隐藏技术。本书涉及大量的与信息隐藏技术相关的数字图像和三维模型处理的知识，使得学习者具有完善的信息隐藏技术体系。按照空间域与变换域的技术脉络，详细介绍了基于空间域、变换域以及两者结合的高性能信息隐藏算法设计思路，使得学习者可以掌握并实现具体的信息隐藏算法，符合高等教育高级应用型人才的培养要求。本书还涉及信息隐藏系统架构以及评估方法的讲授，从算法升级到系统，从感性评价上升到理论评估，符合高等教育的理论与实际相结合的复合型创新性人才培养要求。

全书共分 8 章。第一章为绪论，介绍了信息隐藏技术的基本概念，分析了信息隐藏技术较加密和安全信道技术的应用优势，利用实例分析了信息隐藏技术的可行性，介绍了主流的信息隐藏算法分类。在信息隐藏系统方面，重点介绍了信息隐藏系统的特性以及子系统和功能模块，介绍了信息隐藏系统安全性分析的理论基础以及学习与研究思路。第二章为基于数字图像的信息隐藏区域。从数字图像的能量性、结构性以及复杂度特性对信息隐藏区域的生成进行了讲解，系统阐述了与信息隐藏区域生成相关的基础理论。能量性方面的基础理论包括 GHM、CL 和 CARDBAL2 多小波变换、高斯金字塔理论、颜色空间理论。结构性方面的基础理论包括位平面理论、环形解析理论、颜色迁移理论。复杂度特性方面的基础理论包括广义位平面和纹理复杂度判别。第三章为基于三维模型的信息隐藏区域。从三维模型的能量性和结构性对隐藏区域生成进行讲解。能量性方面，首次引进局部高度和 Mean Shift 聚类分析理论用于信息隐藏区域的选择和生成。结构性方面，介绍了使用三维模型骨架理论以及距离变换算法求骨架节点。第四章为基于数字图像与三维模型的信息隐藏嵌入规则，讲授匹配度和信息表达转换理论。匹配度的实现依靠置乱技术，而信息表达转换则介绍颜色场结构法、颜色模矢量场结构法、三维内切球数量表达转换以及三维轮廓表达转换。第五章为基于数字图像的信息隐藏算法，介绍了空间域和变换域在信息隐藏技术中的联合应用方法以及联合应用时变换域生成隐藏区域时必须考虑的生成因素。重点介绍了四种信息隐藏算法：① 基于 $l\alpha\beta$ 与组合广义位平面的信息隐藏算法；② 基于 CL 多小波与 DCT 的信息隐藏算法；③ 基于 GHM 与颜色迁移理论的信息隐藏算法；④ 基于 CARDBAL2 与颜色场结构法的信息隐藏算法。基于数字图像的信息隐藏算法以信息隐藏区域和规则的生成原理为基础，详细给出了算法的应用原理和流程，通过理论分析与实验仿真，验证了算法的有效性。第六章为基于三维模型的信息隐藏算法。分别介绍了基于骨架和内切球解析的三维模型信息隐藏算法以及基于模型点 Mean Shift 聚类分析的三维模型信息隐藏算法。第七章为信息隐藏系统组成，介绍了由 2 个子系统和 9 个功能模

块组成的信息隐藏系统，讲解各个模块的功能设置和理论基础，以及在信息隐藏系统应用中，信息加密方法的选择原则、信息编码原则、载体选择原则、算法选择原则、置乱与优化选择策略，并对预处理子系统中7个模块之间的冲突与协调问题进行相关说明。第八章为信息隐藏系统的安全分析，给出信息隐藏系统安全性分析的基准要素、分析要素、分析的准备工作和分析流程。在简要介绍了现有安全性分析方法的基础上，讲授一种适合对信息隐藏系统进行安全性分析的方法——灰色层次分析法。应用灰色层次分析法提出了一种面向信息隐藏系统的安全性分析模型——基于灰色层次分析法的信息隐藏系统的安全性分析模型，给出了模型的构建和分析流程，并给出实验分析，佐证该模型分析结果的准确性。

本书得到了国家自然科学基金资助项目(61402052，61303041)、陕西省自然科学基础研究计划项目(2014JM2－6105)、中国博士后科学基金资助项目(2015M572510)、陕西省博士后科学基金资助项目、西藏自治区自然科学基金项目(2015ZR－14－20)、长安大学中央高校基本科研业务费专项资金(310832151092)、国家级大学生创新创业训练计划项目(201610710036，201510710044)、全国工程硕士专业学位研究生教育在线课程重大建设项目(课程编号0542)的资助。

本书在“学堂在线”配套慕课(大规模开放在线课程，简称慕课)平台上运行，即配套视频、习题和互动，具有良好的学习效果。读者可登录学堂在线网站 http://www.xuetangx.com/，搜索“信息隐藏技术”在线观看。

由于作者水平所限，书中难免存在诸多纰漏和不足，敬请各位同行专家和广大读者批评指正。

编者著

2016年12月

目　　录

第一章 绪 论

1.1 信息隐藏技术的概念

人类文明数千年，有人类便有了信息的传递。从本能的肢体语言到结绳记事、简笔画、象形文字、烽火、击鼓、孔明灯、飞鸽传书等，无不彰显人类的智慧。人类文明的突飞猛进，大大改观了信息的载体以及传递的方式。特别是数字化的今天，互联网的普遍使用不仅便利了信息交互，更因其开放性的特点，对信息传递的安全性提出了更高的要求，尤其是关系国家安全、军事部署以及重大发展决策的信息传递更是需要加以保护。

随着多媒体技术的进步和网络的发展，越来越多的数字图像和三维模型作为信息载体涌入互联网通信体系。以数字图像和三维模型为载体的信息隐藏技术成为信息安全领域研究的热点。信息隐藏利用数字媒体本身的数据冗余性以及人类感知能力的局限性，借助密码学、混沌理论、编码压缩技术等对信息本身及隐藏位置进行保密，使秘密信息嵌入到公开载体中却不为人知，从而以“存在级”的安全级别去完成信息的安全输出，对信息起到有效的保护。

本书以数字图像和三维模型作为信息隐藏载体，介绍基于数字图像和三维模型的信息隐藏技术。首先，对基于数字图像和三维模型的信息隐藏技术的两个关键问题——信息隐藏区域和隐藏规则进行讲解。其次，根据信息隐藏区域的生成原则以及信息隐藏嵌入规则，按照空间域和变换域的分类方法对信息隐藏算法进行讲授，介绍性能较为全面的信息隐藏算法；此外，将信息隐藏算法按照功能进行细节分解，以系统的思想对算法进行剖析与扩展，提出基于数字图像和三维模型的信息隐藏系统。最后，根据系统结构和功能划分，对信息隐藏系统进行安全性分析研究。

1.2 信息隐藏技术的优势

现阶段，隐秘通信的实现方法主要是加密技术、安全信道技术以及信息隐藏技术等，在考虑代价与安全性的情况下，基于信息隐藏技术的隐秘通信是最为安全、可靠和廉价的实现方法，该方法与加密技术、安全信道技术相比具有明显的优势。

1.2.1 信息隐藏技术较加密技术的优势

加密技术是实现隐秘通信的重要手段之一，通过对明文(秘密信息)进行加密处理形成密文，把原始信息转换成不可读形式，从而实现秘密通信。加密技术最大的特点在于可以

使用公用信道来实现秘密通信，因此得到了广泛的应用。而信息隐藏技术的优势在于，不仅可以应用公用信道，而且可以将明文隐藏到普通的媒体中，使得攻击者难以发现秘密信息的存在，使秘密信息“冠冕堂皇”地从攻击者的监视下溜走，从而真正达到隐秘通信的目的。信息隐藏技术较密码学的应用优势如图 1-1 所示。

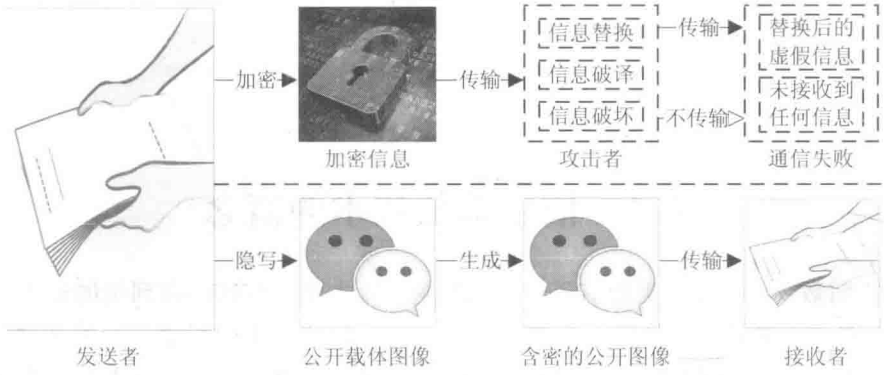


图 1-1　信息隐藏较密码学的应用优势示意

信息隐藏技术的核心思想在于对信息的存在与否进行保密，而对欲隐藏的信息本身并没有要求。通常情况下，为了使秘密通信更加安全，首先将欲隐藏的信息进行加密处理，而后再应用信息隐藏技术将其隐藏在普通载体中，从而实现了比密码学更加可靠的安全传输，达到秘密通信的“双保险”，其原理如图 1-2 所示。

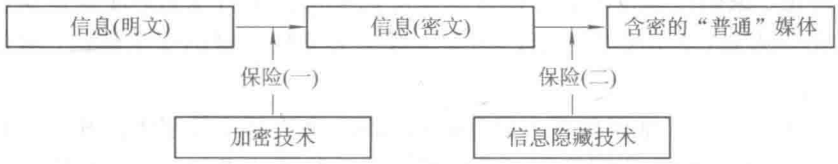


图 1-2　基于信息隐藏技术的隐秘通信“双保险”示意

1.2.2　信息隐藏技术较安全信道技术的优势

安全信道是实现隐秘通信的重要手段之一，它是一种专为发送者和接受者建立的私有信息通道，除了发送者和接受者，其他人无法访问。安全信道虽然安全性好，但需要布设专门的通信链路，因此实现复杂，代价昂贵。另外，实施秘密通信的双方有时根本不具备布设安全信道的条件。安全信道的发送和接收端需要专门的安全管理及隐蔽措施，这样的机制极其容易暴露发送者和接受者的身份，使通信链中断，人员受到危险。

1.3　信息隐藏技术的研究意义以及应用领域

1.3.1　信息隐藏技术的研究意义

1. 完善信息安全体系，提高国家信息安全水平

随着改革开放的不断深入，我国在政治、军事、经济、文化和教育等各个领域都有了

长足的进步和飞速的发展。然而，进步与发展的背后不仅需要人们在研究领域的不懈努力，还需要有安全的信息系统作为支持与保障。随着计算机和网络技术的迅速发展，信息系统更多的是依赖以计算机为基础的计算机网络，因此，计算机网络已经与电力网、电话网、广播电视网、交通网并驾齐驱，成为当代人类赖以生存的网络之一。保证计算机网络中信息传递的安全是衡量网络与信息安全水平的重要指标。

信息隐藏技术为信息安全传递提供了强有力的技术支持。几乎所有的军事信息都涉及国家安全，但也时刻受到窃取与破坏的威胁。应用信息隐藏技术是保障军事信息安全传输与交互的重要技术手段。另外，电子商务、电子政务、电子金融都是网络时代政治和经济活动的全新形式，在自身建立良好的管理体制的基础上，应用信息隐藏技术保障信息的安全传输，可以有效地保护好政务和商业等信息机密，提高政治与经济系统的信息安全。可以肯定的是，信息隐藏技术的进步可以完善信息安全系统，提高国家信息安全水平。

2. 提高信息检测能力，维护国家安全

任何技术本身是没有好坏之分的，关键在于技术使用者应用的目的。如今，信息隐藏技术也被不法分子所利用。不少恐怖组织以 Internet 为联系工具实现散布消息、筹集资金、筹划攻击活动等目的。遍布于全球各个角落的恐怖分子已经开始使用图像、音频和视频文件等作为载体，通过信息隐藏技术来躲避国际反恐机构的监控。如何有效监管 Internet、如何防止不法分子应用信息隐藏技术进行高科技犯罪，成为安全研究领域的重中之重。

深入研究信息隐藏技术，可以进一步了解传递载体在嵌入隐藏信息后所发生的变化，为信息隐藏分析技术提供更多的研究依据，从而更好地对网络进行有效的监管，正所谓“知己知彼，百战不殆!”信息隐藏技术的研究无论在军事上、民用上都有着重要的意义!

1.3.2 信息隐藏技术的应用领域

信息隐藏技术是一种信息处理技术，它的应用范围几乎涵盖了所有涉及到安全通信的领域，尤其是在军事、政治、经济、文化等方面都有着很高的应用价值。

1. 军事方面

现代战争中，即使通信内容已经被加密，但随着数学学科的自身发展和计算机技术的进步，原来加密算法依赖的“计算不可行性”的数学问题可能变得容易求解。而且，敌方也会从加密举动发现端倪，进而启发攻击者进行破解。在某些情况下，虽然敌方不能进行有效的破译，但是可以很容易地对信息加以破坏，使得信息传输失败。所以，战争中更多的是应用信息隐藏技术来实现信息传输，把秘密信息隐藏于敌人难于注意的公开信息中，掩盖了通信存在的事实，使得攻击者难以检测或攻击信号，瞒天过海，达到信息安全传输的目的。

2. 政治方面

随着现代科学技术和传播手段的迅猛发展与广泛运用，舆论彰显出前所未有的独特作用和巨大能量，对社会稳定和国家安全的重要影响日益显现。在政治方面，舆论可以通过生动鲜活、具体直接的内容和形式，持续不断地为政权合法性提供注解和例证，增强人们对现存社会制度和政治秩序的心理认同与支持，不断为政权合法性补给能量。但是，舆论也可以从反方向释放能量，质疑、消解、摧毁现有政权的合法性，引发社会动荡。

从舆论传播的时代特征看，以网络为代表的新兴媒体，已逐渐担负起跨媒体、跨区域、跨层次舆论传播媒介的角色，日趋成为舆论生成的策源地、舆论传播的集散地、舆论交锋的主阵地。在这个阵地上，秘密进行的舆论扩散、反馈、再扩散的速度加快，甚至呈几何级数增长。舆论形成机制和传播方式的变化，加大了舆论传播的离散性、多变性和复杂性，舆情分析和舆论引导的难度都大为增加。对信息隐藏技术的研究，可以提升信息隐藏分析技术水平，使国家对网络隐藏信息进行有效监测，及时了解“隐藏舆情”，提升舆情安全程度，对维护社会安定团结起到十分重要的作用。

3. 经济方面

网络技术与多媒体技术的结合，大大拓宽了网络的应用范围，数字媒体通过网络传输改变了原有媒体发布和物流形式。信息隐藏技术可以有效地保护数字媒体中诸如发行、版权管理以及播放权限等各种问题。另外，在医疗领域，尤其是医学图像系统中，为了防止患者的文字资料与诊断图片分离造成的医疗信息丢失，将患者的姓名等信息嵌入到诊断图片中是很有用的安全措施。还有，信息隐藏技术在进一步实现数字媒体多信息呈现方面，提供了强有力的技术支持。例如，在计算机网络的浏览器中应用隐藏信息可以实现浏览器的智能化；应用信息隐藏技术可以把电影的多种语言配音和字幕嵌到视频图像中携带，在保证视觉质量不受影响的情况下节省了声音的传输信道。与此同时，把电影分级信息嵌入到图像中，可以实现画面放映的等级控制，从而实现电影的分级播放。此外还可以将信息隐藏技术应用到远程教育，实现分级权限的播放。

4. 文化方面

互联网的发展，使得信息的共享方式发生了巨大的变化，人类获取信息的来源越来越多样，如何有效监管与控制信息，使信息的读取和使用权与使用者匹配成为现今需要解决的问题。利用信息隐藏技术，可以在不影响媒体效果的同时，对媒体进行额外的信息标识与控制。例如，对媒体进行内容说明、安全等级标识以及使用权的控制等。

1.4 学 习 重 点

信息隐藏技术的学习主要集中于三点：一是信息隐藏算法；二是信息隐藏系统；三是信息隐藏系统安全性分析。

1.4.1 信息隐藏算法

信息隐藏技术中，最为关键的就是信息隐藏算法的学习。本书在算法部分重点研究数字图像和三维模型的信息隐藏技术。本小节只是对算法的基本原理和分类进行介绍，算法设计将在本书的第五章和第六章进行阐述。

1. 信息隐藏的可行性分析

基于数字图像和三维模型的信息隐藏技术的可行性来自于数字图像和三维模型信号相对于人类视觉的冗余，在人眼无法感知的数据成分中通过修改信号数据进行秘密信息的隐藏，通常是对部分数据(空间域)或描述参数(变换域)做一定的修改或替换来实现一种“非加密”方式的信息隐藏。

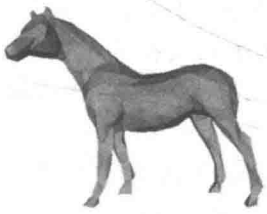
图 1-3 为一个简单的数字图像实例，图(a)大小为 2083 K，经过压缩后，图(b)的数据量仅为原图的 4%左右(92 K)，但是人类视觉系统(Human Visual System，HVS)很难感知到压缩所带来的变化，可见去除冗余对展现图像内容本身没有任何影响。所以认为，对原本压缩过程中欲丢弃的数据进行保留后替换，人类视觉系统是很难识别出图像修改前后的差别的。

(a) 2083K

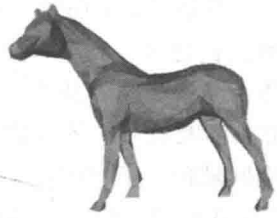
(b) 92K

图 1-3　数字图像冗余实例

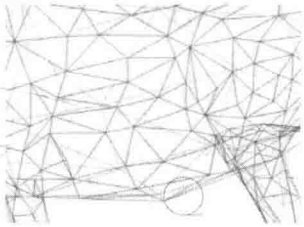
图 1-4 为一个简单的三维模型实例。图(a)为原始未修改的三维图像，图(b)为部分修改后的三维图像。人类视觉无法判断图(a)和图(b)的区别与变化。图(c)为图(a)的局部放大图像，图(d)为图(b)的局部放大图像，借助计算机进行局部放大，才能看到较为明显的区别。



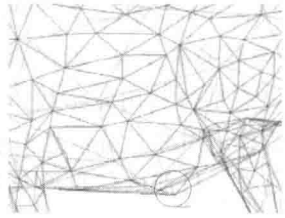
(a) 原始三维模型



(b) 部分修改后的三维模型



(c) 未修改局部放大



(d) 修改后局部放大

图 1-4　三维模型冗余实例

从视觉科学与信号处理的角度来看，信息隐藏可以视为在原始图像下(强背景)叠加隐藏信息(弱信号)。由于 HVS 分辨率的限制，只要叠加的弱信号的信息特性低于 HVS 门限值(对比门限等)，HVS 就无法感受到信号的存在，从而达到信息隐藏的目的，这就是信息隐藏技术的可行性所在。

2. 信息隐藏算法的分类

信息隐藏算法的分类方法众多，典型的大致有以下四种分类方法。

1）按应用对象分类

按照应用对象分类，信息隐藏算法主要分成秘密通信技术、载体标记技术以及额外信息服务技术。秘密通信技术旨在完成信息的秘密传输；载体标记技术则是要完成对载体的注释，例如媒体的所有权或版权等相关信息；额外信息服务技术则是在载体中嵌入一些与载体和载体功能有关的信息数据，使媒体工具(如图像播放器、浏览器)可以提取和执行额外的相关功能，完成分级控制、图像注释以及权限播放等功能。本书主要讲解面向秘密通信的应用。

2）按密钥分类

按密钥分类，信息隐藏算法可分为无密钥信息隐藏和有密钥信息隐藏两大类。无密钥信息隐藏是指秘密信息在嵌入到隐秘载体之前不做任何加密处理，同时信息隐藏过程也无密钥控制，秘密信息的安全保障完全依赖信息隐藏系统的安全性；而有密钥的信息隐藏可以根据加密理论进行信息和嵌入的加密，有密钥的信息隐藏在嵌入和提取时采用相同的密钥，因此也被称为对称信息隐藏技术，反之则被称为非对称信息隐藏技术。

3）按隐藏嵌入域分类

按照隐藏算法所基于的嵌入域进行分类，信息隐藏算法主要分为基于空间域的信息隐藏算法和基于变换域的信息隐藏算法。空间域方法是在数字图像的空间范围内(例如像素值、颜色空间分量、位平面等)直接用隐藏信息来替换载体信息中的冗余部分。变换域方法是把欲隐藏的信息嵌入到载体的一个变换空间(例如离散余弦变换的系数矩阵等)中。当然，现在的一些算法同时基于空间域与变换域。本书算法的讲解是按照隐藏域进行分类展开的。第五章涉及的数字图像信息隐藏算法中，基于 $l\alpha\beta$ 与组合广义位平面的信息隐藏算法是基于空间域的，基于 CL 多小波与 DCT 的信息隐藏算法是基于变换域的，而基于 GHM 与颜色迁移理论的信息隐藏算法和基于 CARDBAL2 与颜色场结构法的信息隐藏算法是基于空间域和变换域联合的。第六章涉及的基于骨架和内切球解析的信息隐藏算法以及基于模型点 Mean Shift 聚类分析的信息隐藏算法均属于空间域信息隐藏算法的范畴。

4）按提取要求分类

根据提取是否利用原始载体可以分成两种信息隐藏算法。若在提取隐藏信息时不需要利用原始载体，则称为盲信息隐藏算法，否则称为非盲信息隐藏算法。考虑到安全以及应用方便的需要，目前的信息隐藏算法大都采用盲信息隐藏算法，本书涉及的信息隐藏算法全部为盲信息隐藏算法。

1.4.2 信息隐藏系统

信息隐藏技术是一项复杂的系统工作，技术的实现涉及到包括嵌入信息本身、载体、隐藏算法和传输条件等各个因素以及相关的综合性问题。下面就信息隐藏系统的特性、组成要素以及要素特性进行阐释。

1. 信息隐藏系统特性

本书讲授的信息隐藏技术主要面向秘密通信应用。信息隐藏系统是支撑秘密通信的专

有应用系统，所以秘密性与通信性是衡量信息隐藏系统的根本特性，而这两个特性中分别包括不可见性和抗分析性以及鲁棒性和容量性，如图 1-5 所示。

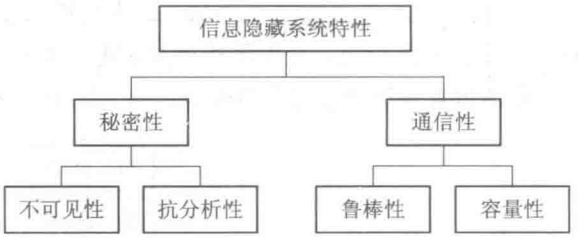


图 1-5　信息隐藏系统特性示意

1）秘密性

秘密性是要求信息隐藏系统可以秘密地传输信息，使有意进行信息截取和破坏的攻击无法找到信息传输迹象，或者无法分析和提取秘密信息。秘密性具体可以概括为系统的不可见性和抗分析性，详细概念见表 1-1 所示。

表 1-1　信息隐藏系统的秘密性概念

秘密性要求	概　念
不可见性	要求不影响对原始载体的理解，即人类感知系统和机器设备都无法发现宿主信息内包含了其他信息，同时不影响宿主信息的感觉效果和使用价值
抗分析性	信息隐藏系统要抵御信息隐藏分析(检测)技术，防止攻击者判断出隐藏信息的存在并成功提取出隐藏的信息内容

注意：不可见性是信息隐藏系统的最基础要求，也是抗分析性的基础。而抗分析性是信息隐藏系统的最高性能要求，在宏观上制约着通信系统的整体性能。

2）通信性

系统的通信性是应用层面上的一个要求，针对这个要求，信息隐藏系统需要满足鲁棒性和容量性，具体概念如表 1-2 所示。

表 1-2　信息隐藏系统的通信性概念

通信性要求	概　念
鲁棒性	鲁棒性指不因载体文件的某种改动而导致隐藏信息丢失的能力。这里所谓的“改动”是指传输过程中可能经历的处理(如信号处理、有损压缩、滤波、调制等)、恶意攻击或者信道中随机噪声的影响
容量性	容量性指载体图像和三维模型能够嵌入的欲隐藏信息的大小

鲁棒性与不可见性在信息隐藏系统中是对立因素，因为通常使用冗余嵌入，即重复嵌入相同的信息来增强鲁棒性，这样就会造成信息嵌入过多，影响不可见性。解决这一对立因素是信息隐藏技术的难点，信息隐藏系统的设计要均衡考虑系统要求。与隐藏容量密切相关的一个概念是信息隐藏率，信息隐藏率是指欲隐藏的信息量与载体信息量的比值。在保证不可见性的前提下，应尽量在载体中隐藏更多的信息，提高信息传输的效率。

2. 信息隐藏系统的组成要素

根据信息隐藏技术的应用目标，一套完整的信息隐藏系统应该包括两个子系统和 9 个功能模块。子系统分别是预处理子系统和嵌入子系统，9 个模块包括信息加密模块、信息编码模块、载体选择模块、算法选择模块、载体解析模块、置乱模块、优化模块、信息嵌入模块以及补丁模块。9 个模块包含在两个子系统中，隶属关系如图 1-6 所示。

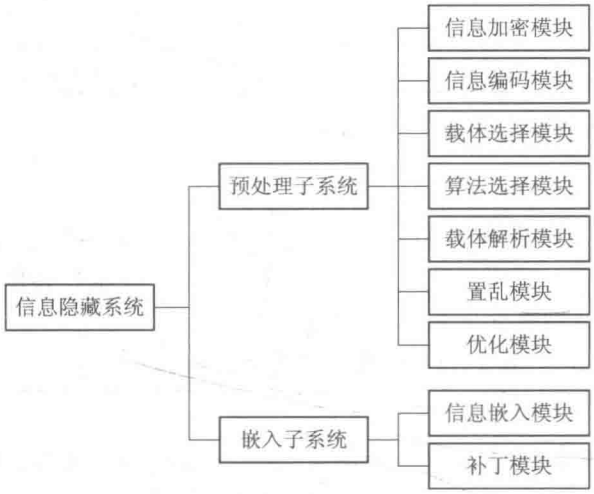


图 1-6　信息隐藏系统的组成要素以及隶属关系

信息隐藏系统中，9 个模块各自发挥其中的作用，表 1-3 是对各个模块做的简要概括。

表 1-3　信息隐藏系统的 9 个模块功能介绍(简述)

信息隐藏系统		功 能 介 绍
预处理子系统	信息加密模块	将欲隐藏的信息进行加密处理
	信息编码模块	将欲隐藏的信息转化成为符合嵌入系统性能条件的信息
	载体图像模块	根据所要隐藏的信息特性和容量等进行载体图像的选取
	算法选择模块	根据欲隐藏信息和载体图像的特性进行隐藏算法的选择
	载体解析模块	根据隐藏规则解析出载体自身所隐含的信息
	置乱模块	对信息进行置乱处理
	优化模块	从调整隐藏顺序(置乱参数)入手对隐藏信息进行优化
嵌入子系统	信息嵌入模块	实现信息的嵌入操作
	补丁模块	根据实际应用需要额外嵌入一些附加信息

1.4.3　信息隐藏系统安全性分析

信息隐藏技术是一门安全学科，应该有专属的性能分析体系，以便信息隐藏系统的设计者和使用者预测和掌握系统的安全程度。目前，信息隐藏系统的安全性分析结果并未按照不可见性、鲁棒性、抗分析性和嵌入容量进行等级划分，因此，分析结果的指导性不强。在实际操作中，性能保障是依靠实验仿真验证，这给信息隐藏系统的设计者和使用者带来