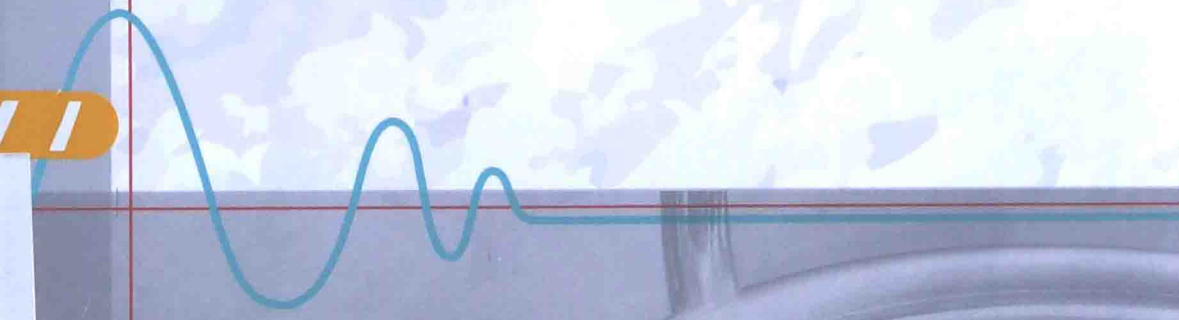
刘绪崇 蒋颖 赵薇 著

基于小波和多尺度几何分析的信息隐藏技术

Information Hiding Technology
Based on Wavelets
and Multiscale Geometric Analysis



湖南大学出版社
HUNAN UNIVERSITY PRESS

刘绪崇 著

基于小波和多尺度几何分析的信息隐藏技术

Information Hiding Technology
Based on Wavelets
and Multiscale Geometric Analysis

湖南大学出版社

内 容 简 介

本书针对传统的数字水印算法容易导致误判和降低水印识别率，且算法过于复杂、难以实现的缺陷，提出了基于二代 Bandelet 图像认证水印算法和基于方向小波几何图像认证算法；针对目前纹理图像隐藏 DEM 数据的已有算法会对纹理图像产生破坏的缺点，提出了基于小波变换的纹理无损隐藏 DEM 数据算法；根据 DEM 数据的特点，提出了基于方向小波的无损三维地形数据水印签名技术和基于 DEM 数据可见三维水印技术；针对水印与载体融合后视觉不太和谐、信息隐藏量小、可见水印容易破坏载体等问题，提出了基于小波系数相对模糊关系的水印算法和基于模糊关系的无损可见水印算法。本书可供信息隐藏技术研究及学习的相关人员参考。

图书在版编目（CIP）数据

基于小波和多尺度几何分析的信息隐藏技术/刘绪崇，蒋颖，赵薇著．—长沙：湖南大学出版社，2014.10

ISBN 978-7-5667-0632-4

Ⅰ.①基… Ⅱ.①刘… ②蒋… ③赵… Ⅲ.①信息系统—安全技术—研究 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2014）第 049635 号

基于小波和多尺度几何分析的信息隐藏技术

JIYU XIAOBO HE DUOCHIDU JIHE FENXI DE XINXI YINCANG JISHU

作　　者：刘绪崇　蒋　颖　赵　薇　**著**
责任编辑：刘　旺　**责任校对**：全　健　**责任印制**：陈　燕
印　　装：虎彩印艺股份有限公司
开　　本：710×1000　16 开　**印张**：7.5　**字数**：150 千
版　　次：2014 年 10 月第 1 版　**印次**：2014 年 10 月第 1 次印刷
书　　号：ISBN 978-7-5667-0632-4/TP·85
定　　价：26.00 元

出 版 人：雷　鸣
出版发行：湖南大学出版社
社　　址：湖南·长沙·岳麓山　　**邮　　编**：410082
电　　话：0731-88822559（发行部），88821174（编辑室），88821006（出版部）
传　　真：0731-88649312（发行部），88822264（总编室）
网　　址：http://www.hnupress.com
电子邮箱：liuwangfriend66@126.com

前　言

随着计算机应用的普及和互联网的飞速发展，信息安全问题已成为影响国家安全、经济发展、社会政治稳定、人民生活的重大问题。信息隐藏技术是信息安全研究领域的研究热点，是一门新兴的交叉学科，在计算机、通信、保密学等领域有着广阔的应用前景。在 1994 年的图像处理会议(ICIP'94)上 Schyndel 提出了数字水印技术，从此掀开了现代信息隐藏技术研究的高潮。我国关于信息隐藏技术的研究从 1999 年开始兴起，其标志是由信息科学领域的何德全、周仲义、蔡吉人 3 位院士联合发起的全国信息隐藏学术研讨会，至今已举行了 11 届。经过多年的努力，信息隐藏技术的研究已经取得了很大进步，已经在人类生活的许多方面得到广泛应用。

目前信息隐藏技术的研究主要集中在隐秘术和数字水印两个方面。隐秘术是研究如何将秘密信息隐藏在不太容易引起注意的消息中，从而使得秘密通信不被觉察；数字水印源于数字媒体作品的版权保护，已成为信息安全领域的最新研究热点。但是，信息隐藏技术无论在理论上还是在应用水平上都还不成熟，缺乏系统性的理论基础和公平统一的性测试与评价体系。本书从分析传统信息隐藏算法的缺陷和不足出发，有针对性地提出新的信息隐藏算法，并从算法的设计、隐藏信息的检测、容量大小和抗攻击性等方面做了很多研究。全书共分为六章：

第一章，绪论。对整个文章的研究背景、立题的依据和主要研究内容进行概述。首先简要介绍了信息隐藏技术和本课题的研究意义。接下来对进行本课题研究所需的必要算法进行综述，指出各个不同算法的优缺点。最后介绍本课题的立题依据和研究内容，并给出本书的结构安排。

第二章，基于几何多尺度分析的图像水印算法。针对传统的数字水印算法容易导致误判和降低水印识别率，而且算法过于复杂难以实现的缺陷，本章提出了基于二代 Bandelet 图像认证水印算法和基于方向小波几何图像认证算法，并对基于局部统计模型自适应噪声强度算法进行改进。前者应用第二代 Bandelet 变换生成图像的几何方向流来刻画图像的纹理和几何特征，后者是利用方向小波变换生成图像的几何方向流来刻画图像纹理和几何特征，上述两个算法都是

利用改进的统计模型自适应噪声强度算法来筛选出纹理丰富的子图，用于信息隐藏。

第三章，纹理无损隐藏 DEM 技术。针对目前已有的纹理图像隐藏 DEM 数据的算法会对纹理图像产生破坏的缺点，本章提出了基于小波变换的纹理无损隐藏 DEM 数据算法。该算法应用基于整数小波变换和极低比特率压缩编码算法，采用直方图平移的无损隐藏算法将压缩的高程数据隐藏到纹理图像中，在提取隐藏信息时采用直方图平移算法可逆地将隐藏在纹理图中的 DEM 数据提取，并实现了纹理图的无损恢复。

第四章，无损 DEM 签名和可见三维水印技术。根据 DEM 数据的特点，提出了基于方向小波的无损三维地形数据水印签名技术和基于 DEM 数据可见三维水印技术。前者是利用方向小波变换来检测三维地形的趋势和走向，将其作为认证水印并隐藏其中，通过修改广义直方图的平移算法实现水印信息的隐藏。后者是将三维水印与 DEM 数据进行三维融合，并记录被三维水印遮蔽的 DEM 数据信息，利用广义直方图平移方法隐藏了被三维水印遮蔽的信息，然后通过广义直方图平移算法可逆地提取出被三维水印遮蔽的信息，用来替换三维水印恢复出原始 DEM 数据。

第五章，基于模糊理论和矩阵理论水印算法。针对水印与载体融合后视觉不太和谐、信息隐藏量小、可见水印容易破坏载体，以及算法本身安全的问题，提出了基于小波系数相对模糊关系的水印算法和基于模糊关系的无损可见水印。前者是采用带参数的整数小波变换获取载体的小波系数，应用 Rabin 方法构造的函数生成模糊关系矩阵，通过近似分量和对角分量的量化噪声余量矩阵的相对关系修改对角分量小波系数，最后对小波系数做小波逆变换得到隐含水印的图像。后者是先将载体与可见水印进行模糊融合，然后利用 RH 算法对遮蔽子图进行加密，最后采用改进的直方图平移方法实现信息隐藏和恢复。

第六章，结束语。对本课题研究工作进行总结，并对下一步的研究方向进行展望。

本书的研究工作得到湖南省工业支撑计划重点项目资金(2013GK2014)、网络犯罪侦查湖南省普通高等学校重点实验室开放资金的资助，得到湖南省公安厅和湖南警察学院纵向项目的资助，以及其他横向研究课题的支撑，特此向支持和关心本研究工作的所有单位和个人表示衷心感谢。此外，还要感谢教育本人多年的师长，感谢各位同仁和同学们的帮助和支持，感谢湖南大学出版社为本书出版付出的辛勤劳动。书中有部分内容参考了有关单位和个人的研究成果，均已在参考文献中列出，在此一并致谢。

由于水平有限，不足之处在所难免，敬请各位读者批评指正。

目　次

第1章 绪 论

1.1 信息隐藏技术

随着信息时代的到来，特别是互联网技术的普及，信息的安全保护问题日益突显，已成为影响国家安全、经济发展、个人利害、社会稳定的重要因素。近年来，国际上开始提出一种关于信息安全的新概念，即在一般的文件中隐藏机密资料，然后再通过网络来传输，隐藏了机密资料的文件即使被非法拦截者从网络上拦截下来，但它们看起来与一般非机密资料非常相似，因而可以逃过拦截者的破解。随之，一门新兴交叉学科——信息隐藏学诞生了。信息隐藏技术作为信息安全领域的最新研究热点，在近几年得到了较快的发展，已经在人类生活的许多方面得到了相当广泛的应用，其驱动力来自信息时代的两大需求——信息安全和版权保护。

信息隐藏技术应用领域广泛，主要应用于数据保密、数据的不可抵赖性、数字作品的版权保护和防伪、数据的完整性保护等。目前，信息隐藏技术研究主要为隐秘术和数字水印两个方面，隐秘术主要研究如何将秘密信息隐藏在不太容易引起注意的信息中，从而使得秘密通信不被觉察；而数字水印则侧重于数字媒体作品的版权保护。

1.1.1 信息隐藏技术的概念

信息隐藏就是把一个有意义的信息（或秘密信息）隐藏于另一公开、普通的信息（或载体）中，非法者不知道这个普通信息中是否隐藏了其他的信息，而且即使知道也难以提取或去除隐藏的信息。信息隐藏所用的载体形式可以是任何一种数字媒体，如图像、声音、视频或一般的文档等，其首要目标是要使加入隐藏信息的目标媒体产生最小的可见性，使人无法看到和听到被隐藏的数据。

信息隐藏与传统的密码学技术是不同的。信息隐藏主要研究如何在一公开

的普通的信息中隐藏某一秘密信息，然后利用公开信息的传输来传递秘密信息。而密码技术主要是研究如何将秘密信息进行特殊的编码，以形成一般人不可识别的密文进行传递。对加密通信而言，监测者或非法拦截者可以通过特别技术或手段截取通信密文，然后对其破译，或将截取密文破坏后再发送出去，影响秘密信息的安全；但对信息隐藏而言，监测者或非法拦截者很难从公开的信息中判断秘密信息是否存在，难以从截获的信息中提取出机密信息，以保证机密信息的安全。

多媒体数据中之所以能够隐藏信息，是基于以下原因：其一，从信息论的角度看，多媒体数据本身存在很大的冗余性，未经过压缩的多媒体数据编码效率也是很低的。其二，人眼或人耳本身对某些信息都有一定的掩蔽效应，如人眼对灰度的分辨率就只有几十个灰度级，对图像边沿附近的信息不敏感等。利用人的这些特点，可以很好地隐藏信息而不被察觉。

1.1.2 信息隐藏技术的特点、分类

1. 信息隐藏技术的特点

信息隐藏与传统的加密技术是不同的，由于信息隐藏的目的不再是限制正常的资料存取，而是在于保证隐藏数据不被非法者侵犯和发现，因此，信息隐藏技术必须考虑正常的信息操作所造成的威胁，即要使秘密资料对正常的数据操作技术（如信号变换操作或数据压缩等）具有免疫能力。根据信息隐藏的技术要求和隐藏目的，该技术应具有以下七个特点：

①鲁棒性。指载体文件的某种改动不会导致隐藏信息丢失的能力。“改动”是指在数据传输过程中的信道噪音、滤波操作、重采样、有损编码压缩、D/ A 或 A/ D 转换等。

②不可检测性。指原始载体与隐蔽载体具有一致的特性。如具有一致的统计噪声分布，肉眼无法区分和识别等，以便使非法拦截者无法判断是否有隐蔽信息。

③透明性。根据人类视觉系统或人类听觉系统属性，经过一系列信息隐藏处理，使载体数据没有明显降质现象，使得隐藏的数据无法被直接察觉。

④恢复性。指经过一些操作或变换后，可能会对原图产生较大的破坏。但采用信息隐藏技术后，即使原来的资料只留下片段数据，技术人员仍能恢复其中的隐藏信息，而且恢复过程不需要原始载体数据。

⑤安全性。指隐藏算法有较强的抗攻击能力，即它必须能够承受一定程度的人为攻击，如噪声、模糊、剪切等，而且不会破坏隐藏信息。

⑥可纠错性。使隐藏信息在经过各种操作和变换后仍能很好地恢复，确保隐藏信息的完整性，一般可采取纠错编码方法。

⑦对称性。指信息的隐藏和提取过程是对称的，包括编码、加密方式，以降低存取难度。

2. 信息隐藏技术的分类

根据不同的标准，信息隐藏技术可作不同分类，通常，信息隐藏技术可按如下几种方式分类：

①按密钥分类。可分为无密钥隐藏和有密钥隐藏两大类。前者又称“纯隐秘术”，指秘密信息在嵌入隐秘载体之前不做任何处理，同时信息嵌入过程也无密钥控制；后者根据密钥体制不同，可将其细分为对称密钥和非对称密钥。

②按载体类型分类。可分为基于文本、图像、音频、视频、超文本、网络层等载体的信息隐藏。

③按嵌入域分类。可分为空域(或时域)方法和变换域方法。前者是指直接用待隐藏的信息替换载体信息中的冗余部分；变换域方法又可细分为离散傅里叶变换(DFT)域、离散余弦变换(DCT)域、离散小波变换(DWT)域等。

④按提取要求分类。可分为盲隐藏和非盲隐藏两类。

⑤按保护对象分类。可分为隐写术和水印技术两类。隐写术的目的是在不引起任何怀疑的情况下秘密地将信息传送，因此它的主要要求是不被检测到和传送信息的大容量等。数字水印技术是指在数字产品中嵌入数字信号，这些数字信号可以是图像、文字、符号、数字等一切可以作为标识或标记的信息，其目的是进行版权保护、所有权证明、指纹和完整性保护等，因此鲁棒性和不可感知性是它必须具有的特性。

1.1.3 数字水印技术

数字水印技术是信息隐藏技术中最重要的分支，是指在数字化的数据内容中嵌入不明显的记号。被嵌入的记号通常是不可见或不可察的，只有通过一些计算操作或专门的检测器才能被检测或者被提取。载体被嵌入水印后就与载体数据紧密结合并隐藏其中，成为载体不可分离的一部分；隐藏的水印可以通过一些操作被提取出，用来保护原有载体的使用价值和商用价值，因此数字水印技术成为版权保护最有效的一种方法。数字水印技术出现得相对比较晚，从 Van Schyndel 在 ICIP'94 会议上发表题为“A digital watermarking”的论文才标志这一领域的开始，而隐写术已经有较深的理论基础，因此在研究数字水印的过程中借鉴了很多隐写术方面取得的成果。

1. 数字水印分类

数字水印有很多种分类方法，因分类的出发点不同就会导致了不同的分类，它们之间是既有联系又有区别的。最常用的分类方法包括以下几类：

(1)按水印外观特性分类

可以将其分为可见水印与不可见水印。不可见水印信息隐含在图像中，是不可见的，必须通过专门的检测设备才能够提取。可见水印是可以看见的水印，就像插入或覆盖在图像上的标识，水印嵌入图像中以后可以直接看到，图像部分信息被可见水印遮蔽，非法用户如要去除水印，除非破坏图像的完整性，从而达到保护版权和数据的目的。

(2)按水印所附载体数据分类

可以将其分为音频水印、图像水印、文本水印、视频水印以及用于三维网格模型的网格水印等。随着数字技术不断发展，将会有更多类型的数字载体出现，因而也会有更多相应载体水印的出现。

(3)按水印的检测过程分类

可以将其分为盲水印、半盲水印和非盲水印。盲水印的检测只需密钥，既不需要原始数据，也不需要原始水印；非盲水印在检测过程中需要原始数据和原始水印的参与；半盲水印则不需要原始数据的参与，但需要原始水印来进行检测。

(4)按数字水印对图像篡改的敏感性分类

可以将其分为脆弱数字水印和鲁棒性数字水印。脆弱数字水印对图像的篡改非常敏感，并且不需要与原始图像作对照就可以判断图像是否被改动，从而便于检测恶意篡改。鲁棒性数字水印是一种抗攻击的数字水印技术，可最大限度地防止非法使用者获取、消除嵌入的数字水印。

(5)按水印信息嵌入的位置分类

可以将其分为空域数字水印、变换域数字水印(包括离散余弦变换、小波变换、重叠式正交变换)。直接在空域中改变采样点的幅度值，嵌入水印信息的算法称为空域水印；改变变换域中的系数，嵌入水印信息的算法称为变换域水印。空域数字水印算法是最早提出的水印方法之一，思想非常简单。Bander 等人提出的 Patchwork 方法和 L. F. Turner 与 R. G. van Schyndel 等人提出的最低有效位算法(LSB)是最早也是最典型的空域水印算法。变换域数字水印技术将水印信息嵌入到变换域系数中，目前该方法是数字水印技术研究的热点。可以说，每一种可以将图像作时频分析的变换，都可以找到与之相对应的数字水印方法，还有一些方法结合了多种变换技术。现在对于变换域水印的研究一般都引入了视觉模型，在不可见性和安全性之间找到平衡点，另外水印嵌入的强度一般也是自适应的。

当然还有很多别的分类方法。如根据水印方法是否可以公开来分类可以将其分为公开水印、秘密水印；根据用途划分可分为版权保护水印、票据防伪水印、篡改提示水印和隐蔽标识水印等；根据嵌入与检测操作的复杂度可分为对称水印和非对称水印。数字水印的主要分类如图 1-1 所示。

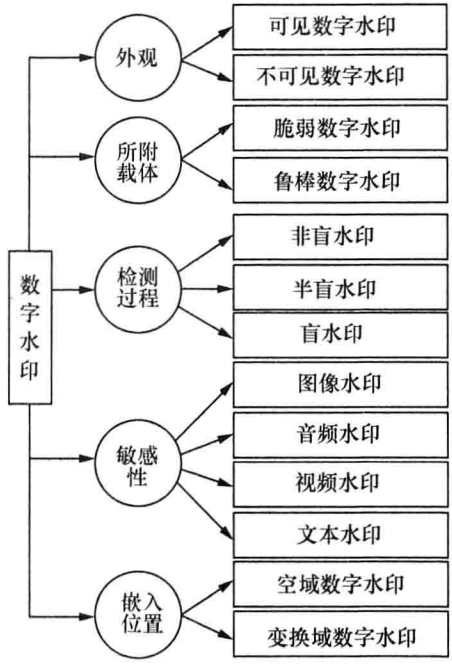


图 1-1 数字水印几种主要的分类方式

目前，在数字水印系统中，隐藏信息的丢失意味着版权信息的丢失，从而也就失去了版权保护的功能。由此可见，数字水印技术除了具备信息隐藏技术的一般特点外，还必须具有较强的鲁棒性、安全性和透明性。

1.1.4 DEM 数据信息隐藏技术

数字地形模型(Digital Terrain Mode，简称 DTM)是以数字的形式按一定的结构组织在一起，表示实际地形特征的空间分布模型。DTM 主要由栅格(Regular Square Grid，RSG)与不规则三角网(Triangulated Irregular Networks，TIN)两种数据格式来表示。前者的优点是充分表现了高程的细节变化，拓扑关系简单，算法实现容易，某些空间操纵及存储方便；前者的不足之处是占用巨大的存储空间，不规则的地面特征与规则的数据表示两者之间的不协调。

后者的优点是高效率的存储，数据结构简单，与不规则的地面特征和谐一致，可以表示线性特征和叠加任意形状的区域边界，易于更新，可适应各种分布密度的数据等；后者的局限性是算法实现比较复杂和困难。这两种格式的数据本质是相同的，都是地形形状大小和起伏特征的数字描述。

按平面上等间距规划采样或内插所建立的 DTM，为栅格数据的 DTM，可以写成矩阵形式：

$$\begin{bmatrix} Z_{00} & Z_{01} & \cdots & Z_{0(n-1)} \\ Z_{10} & Z_{11} & \cdots & Z_{1(n-1)} \\ \cdots & \cdots & \cdots & \cdots \\ Z_{(n-1)0} & Z_{(n-1)1} & \cdots & Z_{(n-1)(n-1)} \end{bmatrix}$$

其中 Z_{ij} 为网格结点 (i,j) 上的地形属性数据，当该属性为海拔高程时，该模型就称为数字高程模型(Digital Elevation Model，缩写 DEM)。地形的 DEM 数据显示如图 1-2 所示：

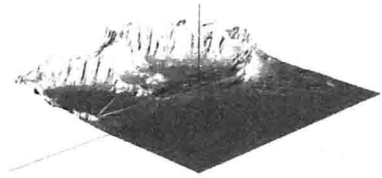


图 1-2　DEM 数据显示

我国已经建成的高精度的 DEM 数据库，对国防建设和经济建设都具有十分重要的意义，属于机密级的数据，如何保护好这些 DEM 数据，或在网络上传输时如何隐藏好这些 DEM 数据，成为迫切需要解决的问题。因此，DEM 数据信息隐藏技术也是本文研究的一个重要内容，包含了 DEM 数字水印技术和 DEM 信息隐藏技术。DEM 数字水印技术是指利用数字水印技术对 DEM 数据进行保护，DEM 信息隐藏技术就是将 DEM 数据秘密地隐藏于另一非机密文件内容之中。本文提出了 DEM 数据水印签名技术和可无损恢复的三维可见水印技术，以及利用纹理图像隐藏 DEM 数据的信息隐藏算法。

1.1.5　信息隐藏技术的发展

信息隐藏学是一门新兴的交叉学科，在计算机、通信、保密学等领域有着广阔的应用前景。信息隐藏的目的是使敌手不知道哪里有秘密，它隐藏了信息的存在形式。这就好比隐形飞机不能被雷达探测到，从而避免了被袭击的危险。众所周知，密码的安全性或不可破译度是靠不断增加密钥的长度来提高的，然而随着计算机计算能力的迅速增长，密码的安全度始终面临着新的挑战。因此信息隐藏技术的出现和发展，为信息安全的研究和应用拓展了一个新的领域。

信息隐藏技术从提出开始就受到了广泛的关注，1994 年的图像处理会议

(ICIP'94)上,Schyndel提出了数字水印技术,从此掀开了现代信息隐藏技术研究的高潮。仅仅过了两年,在ICIP'96上已经出现了以信息隐藏领域中的水印技术(Digital Watermark)、版权保护(Copyright Protection)和多媒体服务的存取控制(Access Control of Multimedia Services)为主要内容的研讨专题。1996年在英国剑桥召开了第一届信息隐藏国际研讨会(First International Workshop on Information Hiding),内容涉及数据隐藏、保密通信、密码学等相关学科领域。截至2009年,共召开了11届信息隐藏国际研讨会,第十一届信息隐藏国际研讨会于2009年6月在德国召开。目前,美国许多著名大学和大公司的研究机构,如麻省理工学院的媒体实验室、明尼苏达大学、普林斯顿大学、南加州大学等,以及NEC公司、IBM公司等,都一直在致力于信息隐藏技术方面的研究,并取得了大量研究成果。与此同时,大量的数字水印应用软件也应运而生,如High Water FBI,Digimarc Corporation,Fraunhofer's SYSCOP等。

国内关于信息隐藏技术的研究从1999年开始兴起,其标志是由我国信息科学领域的何德全、周仲义、蔡吉人3位院士联合发起的全国信息隐藏学术研讨会,至今已举行了11届全国学术会议(CIHW1999,北京;CIHW2000,北京;CIHW2001,西安;CIHW2002,大连;CIHW2004,广州;CIHW2006,哈尔滨;CIHW2007,南京;CIHW2009,长沙;CIHW2010,成都;CIHW2012,北京;CIHW2013,西安)。研讨会集中了国内从事信息隐藏研究的著名专家学者,促进了我国信息隐藏学术的研究及其应用。国内的研究主要是集中在数字水印方面的研究,国家"863计划"、"国家973"项目(国家重点基础研究发展规划)、国家自然科学基金委员会等都对数字水印的研究有项目资金支持。在国内有关信息科学、信息安全、计算机网络及通信等学术会议设立"信息隐藏"或"数字水印"专题进行讨论交流,表明信息隐藏技术已成为学术研究的热点之一。目前,国内从事信息隐藏技术研究的机构主要集中在学校和科研机构,如中国科学院、清华大学、国防科学技术大学、武汉大学、解放军信息工程大学等。

经过多年的努力,信息隐藏技术的研究已经取得了很大进步,隐藏有信息的载体不但经得起人的视觉、听觉等感觉器官检测和仪器设备的检测,而且还能抵御各种人为的蓄意攻击。但总的来说,信息隐藏技术无论在理论上还是在应用水平上都还不成熟,缺乏系统性的理论基础和公平统一的性能测试与评价体系。目前,信息隐藏技术在理论研究、技术成熟度和实用性方面还不能与传统密码技术相比,但它的潜在价值是无法估量的,尤其是在迫切需要解决的版权保护等方面,是根本无法被替代的。在不久的将来,信息隐藏技术在信息安全体系中将发挥极其重要的作用。

1.2 信息隐藏技术的研究意义

随着计算机技术的飞速发展和因特网的日益普及，我国信息化正以一日千里的速度飞速发展，但信息安全却成为影响国家安全、经济发展、社会政治稳定、人民生活的重大问题，利用计算机网络进行犯罪、窃取机密信息的案例屡见不鲜。境内外反动势力时刻准备对我国社会主义政权进行颠覆活动或颜色革命，他们利用互联网进行内外勾结，发布各种反动言论，利用各种渠道打听、获取我国的军事机密、国家政策、经济秘密等。一些西方霸权国家利用自身的信息技术优势，以其先进的信息技术和网络技术手段，极力推行信息霸权、利润霸权、网络资源霸权。还有一些敌对势力在互联网上大力推行他们的“蠕虫计划”，专门针对我国互联网的脆弱性，大肆地在各大门户网站植入木马，让访问网站的计算机“中马”，随意获取“中马”电脑中的数据。因此，信息安全保障已经成为互联网时代国家生存和民族振兴最根本的保障之一。

当前，在互联网上随处可见各种形式的数字作品（图像、视频、音频、作品、书籍等），由于这些数字信息的可复制性，出现了大量的版权争端问题，已经成为政府职能部门关心的重要问题之一。信息隐藏技术中的数字水印成为实现版权保护的最有效的方法之一。数字水印技术可以在原始载体数据中嵌入秘密信息（水印，watermark）来证实该数据的所有权，这种被嵌入的秘密信息可以是一段文字、标识、序列号等，而且要求这种嵌入的水印通常是不可见或不被觉察的，它与原始数据（如图像、音频、视频数据）紧密结合并隐藏其中，能够经历一些不破坏源数据使用价值或商用价值的操作而能保存下来，将作为作品版权保护方面的关键信息。数字水印在版权保护中的作用是指利用隐藏原理使版权标志在被保护的数字作品中不可见或不可听，既不损害原作品，又达到了对作品版权的保护目的。近几年，我国政府部门（如公安部门、版权部门、工商部门）每年查处的侵权案件逐年上升，每年组织联合打击行动，但是涉及版权的各种违法犯罪人数有增无减，主要原因是：第一，作品侵权的利润空间较大，违法犯罪嫌疑人利用各种方式逃避打击；第二，因为产品侵权或盗版的认证难度大，这给侦察办案部门在取证过程中带来很大困难，导致打击不能到位。如果在每个产品中都隐藏了一些有意义的信息（或水印），也就不存在产品的版权认证问题。

在信息时代，人们在方便地获取信息和交流信息的同时，还需要能安全地存储和传输信息。传统的信息加密方法可以加密文本信息，保证其传输的安全，但如果要对图像、视频和声音等多媒体信息进行加密，基于密码学的传统加密方法

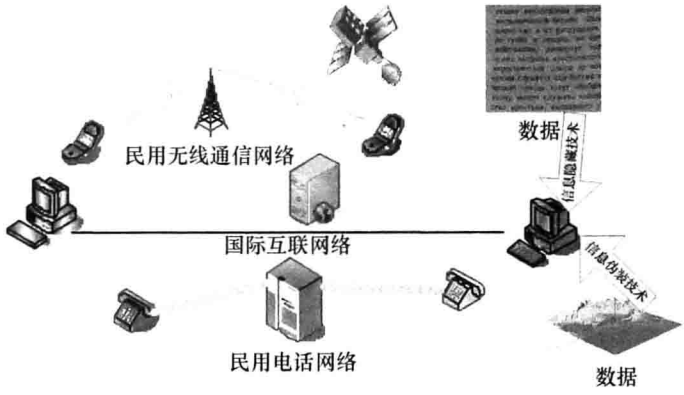


图 1-3 利用公开的信道传输隐藏信息

就显得力不从心了。在军事上，将一幅作战地图或作战指令隐藏在一幅艺术作品中，即使在被敌方截获也无法知道艺术作品中的真正含义。另外，实现在公开信道中安全传输秘密信息，特别是我国现有通信设备条件还比较差，如果能够在没有安全通信信道的条件下实现机密信息的安全传输，就可以利用现有的或民用通信信道传输秘密信息，从而降低实际成本(图 1-3)。因此，信息隐藏技术无论是在军事上还是在经济上都意义重大，它们在军事情报和电子商务等方面有着非常重要的应用前景。

1.3 相关研究工作

本文研究重点是基于小波和多尺度几何分析的信息隐藏和信息检测提取算法及算法在数字高程模型中的应用，需要对已经提出的各信息隐藏算法进行研究。本小节从传统的经典水印算法、多尺度几何分析水印算法、无损信息隐藏算法和自适应容量检测方法进行介绍。

1.3.1 经典水印算法

自 1994 年的图像处理会议上，Schyndel 提出了数字水印技术，从此掀开了现代信息隐藏技术研究的高潮。随后出现了以信息隐藏领域中的水印技术(Digital Watermark)、版权保护(Copyright Protection)和多媒体服务的存取控制(Access Control of Multimedia Services)为主要内容的研讨专题。国内自 1999 年召开第一

次信息隐藏学术研讨会来，至今已举行了 11 届信息隐藏学术研讨会，相关人员已发表很多理论和应用方面的论文，取得了一定的成绩。目前，随着理论研究的进行，国内外相继涌现了数以百计的从事水印技术应用的公司。

数字水印根据加载方法的不同，可以分为空间域水印方法与变换域水印方法。空间域水印方法主要包括最低有效位(LSB)法、纹理映射与 Pathwork 法、文档结构微调法等。目前数字水印方法的研究以变换域数字水印技术为主流，例如，基于 DCT，DWT 或其他具有稀疏表示信号特性的变换，并结合人类视觉系统特性与加密过程的变换域水印方法研究得到研究者普遍重视。与空间域水印方法相比，变换域水印方法具有鲁棒性较高、不可感知性较好以及可隐藏信息量较大等特点。Tirkel 与 Osbomells 等将扩频技术引入到水印研究中，使得水印技术具有与密码学类似的安全性。但是，该类水印方法很难同时满足鲁棒性与感知性的要求。另外，利用 Cox 等人提出的将水印嵌入感知性较强区域的思想，基于感知模型的数字水印方法也得到人们的关注。考虑到每种数字水印技术都存在各自的缺陷，因此，将各种水印技术有机结合，相互取长补短的复合水印技术也得到人们的广泛重视。近年来，人们开始将混沌以及包括细胞自动机、遗传算法、人工神经网络、模糊集合理论以及粗糙集等计算智能技术引入到水印嵌入过程的设计中，并取得了一定效果。目前，数字水印的模型、隐藏数字水印信息的容量(带宽)、算法抗攻击能力与稳健性性能，以及相应水印攻击方法的研究构成各种水印设计方法的研究重点。

1.3.2 多尺度几何分析水印算法

目前，有研究人员从统计学和密码学、差错控制编码的角度研究水印的检测，并取得了一定的研究成果。也有研究人员采用小波变换结合形态学进行图像认证方面的研究，取得了较好的效果。

还有学者利用几何多尺度分析进行图像特征检测和信息隐藏算法的研究，这些算法能够克服传统的水印算法的很多缺陷，是水印研究的一个新的方向。文[8]利用小波变换的低频系数实施均匀标量量化生成低频特征图像作为图像认证的内容，该算法有较强的定位能力，但是抗 JPEG 压缩能力较差。文[7]研究了基于半脆弱水印的内容级视频认证算法，利用 I 帧内块组之间能量不变的特点构造基于内容的特征码。该算法直接利用了统计(能量)比例性，隐藏的特征是没有具体的物理含义的，很难作出直观的分析和判断。文[23]提出了一种结合混沌和图像分块提升小波变换的多功能水印。其采用嵌入一种标识作为可见水印来实现图像的认证，缺点是和需要保护的内容之间没有联系。基于图像