透视

信息隐藏

张立和　周继军　陈　伟　王　颖　编著

国防工业出版社
National Defense Industry Press

透视信息隐藏

张立和 周继军 陈 伟 王 颖 编著

国防工业出版社
National Defense Industry Press

图书在版编目(CIP)数据

透视信息隐藏/张立和等编著. —北京:国防工业出版社,2007.2

ISBN 978-7-118-04950-3

Ⅰ. 透… Ⅱ. 张… Ⅲ. 信息系统—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2007)第 003126 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号　邮政编码 100044)

天利华印刷装订有限公司印刷

新华书店经售

*

开本 710×960　1/16　印张 11½　字数 203 千字

2007 年 2 月第 1 版第 1 次印刷　印数 1—3000 册　定价 25.00 元

国防书店:(010)68428422　　发行邮购:(010)68414474

发行传真:(010)68411535　　发行业务:(010)68472764

致　　谢

感谢北京大学陈钟教授和北京邮电大学杨义先教授的谆谆教导以及他们在学术、技术等方面给予的大力支持。感谢杨成、李武军、陈明奇、杨晓斌、苏配良等提供的宝贵资料。

向为本书贡献力量的人们表示衷心的感谢！

前　言

信息隐藏技术最初主要用于保密通信。人类在几千年前的远古时代，就把信息纹在奴隶的头皮上、待头发长出加以掩蔽后令其传递信息情报，后来发展到用隐写墨水、显微点以及密电码等技术手段隐藏信息。而今，由于计算机网络技术的发展，为传统的隐藏手段注入了全新活力，出现了许多崭新的信息隐藏技术。信息隐藏技术因为其自身的特点，在隐密通信、版权保护、信息鉴别和内容访问控制等领域得到了广泛的应用。

现代信息隐藏技术是在20世纪90年代发展起来的，并成为当前的热点研究方向。信息隐藏涉及电子工程、信号与图像处理、计算机科学以及密码学等领域，是一门交叉科学。虽然目前还没有形成完整的理论体系，还存在很多有待我们去解决的难题。但是，像数字水印、数字密码、数字图像等技术已经日新月异地蓬勃发展起来了。

本书将从不同的角度，把信息隐藏这门古老而神秘的技术以较为通俗的语言展现给读者。全书共分为5章，第1章介绍了信息隐藏的基本概念、发展及应用；第2章介绍了信息隐藏技术的存在机理和信息隐藏研究所需的数学基础知识；第3章从版权保护、内容认证和权限管理应用角度介绍了数字水印技术，并对相关水印算法进行了综述；第4章介绍了信息隐藏的隐密通信应用及其方法；第5章介绍了用于安全监测领域中的信息隐藏检测技术；最后从实践出发系统地介绍了现有的信息隐藏软件产品。

本书可以作为大学生的课外读物，使他们对信息隐藏有个初步认识，也可以供从事相关领域研究的科研人员阅读参考。

由于作者水平有限，写作时间仓促，书中错误之处敬请读者指正，以便再版时修改和完善，甚为感谢。如果您有何意见或建议，请通过E-mail地址zhoujj@pku.edu.cn和我们联系，我们将及时回复您的问题。

感谢中国博士后科学基金(2005038305)对本书的赞助。

编　者

2007年1月于北京大学畅春园

目　录

第1章 引 言

信息隐藏是一门新的综合性前沿学科，涉及到计算机图形学、信号与信息处理、计算机网络攻防和密码分析等多个学科知识，是国际学术界的研究热点之一。简单地说，信息隐藏技术就是将重要信息隐藏在普通数字媒体中的技术。它主要有两个分支：隐秘术和数字水印。隐秘术是指通过信息隐藏进行秘密通信的技术，这时的重要信息与隐藏该信息的媒体数据没有关系，媒体数据只是重要信息的传输信道，作为重要信息掩人耳目的保护壳；数字水印是指通过信息隐藏进行数字权限管理、内容认证等应用的技术，这时的要隐藏信息与媒体数据有关联性，该信息可能描述了媒体数据的版权归属以及访问控制等内容。

信息隐藏系统通常主要由下述两部分组成：(1)信息嵌入，它利用密钥来实现秘密信息的隐藏。(2)信息检测/提取(检测器)，它利用密钥从隐蔽载体中检测/恢复出秘密信息。在密钥未知的前提下，第三者很难从隐密载体中得到或删除秘密信息，甚至发现秘密信息的存在。如图1-1所示。

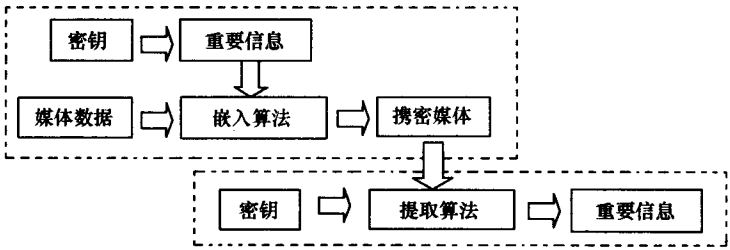

图1-1 一般信息隐藏系统

数字化技术和互联网的发展正在改变着信息传播的载体形式和传播方式，各种数字化产品层出不穷。信息隐藏作为信息安全领域的新生事物，在版权跟踪、网络安全、数据篡改取证、数据防伪上具有不可替代的作用，正逐渐应用于商业、金融、军事和个人消费等领域。

1.1 信息隐藏概述

安全的信息传递通常都是通过加密来完成。密码学在很长时间内都被看做

是外交情报和军事领域内最安全的通信方法和手段，而且商业加密使得有些密码方法也被应用于民间。采用传统密码学理论开发出来的加、解密系统，不管是对称密钥系统（如 DES）还是安全性更高的公开密钥系统（RSA），加密后的数据都是乱码，在信息传递过程中攻击者只能看到这些乱码，而无法破译其中的机密信息，从而达到保密通信的目的。但是这种方法有一个明显的不足，那就是在通信双方之间传输的总是看上去没有任何意义的乱码，这明确地提示给攻击者此时信道中传输的是重要信息的密文，容易引起攻击者的好奇和注意，成为攻击者的攻击目标。而且如果密文被破解，那么其内容就一览无遗了。数字内容产业的蓬勃发展，对版权保护、权限管理及访问控制的需求日益强烈，传统的密码学方法不能完全解决新出现的问题。在这种背景下，具有伪装特点的新兴信息安全学科——信息隐藏应运而生，成为隐蔽通信和信息保护的有效手段，并迅速成为国际上的研究热点。

信息隐藏与信息加密不尽相同，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多了一层保护，因为它不容易引起密码破译者的注意。计算机网络和信息技术的发展使信息隐藏技术得到了空前的应用，它可以将加密后的信息隐藏到任何一种多媒体报文中，这样在网络上传输的信息就变成大家都能够读懂的普通内容掩护信息，因而不会引起攻击者的注意，从而达到麻痹攻击者的目的，即使攻击者预知可能含有信息的载体也很难将隐藏信息提取出来。信息隐藏又称信息伪装，它是利用人类感觉器官对数字媒体的感觉冗余特性，将要传输的秘密信息按照某种算法融入数字媒体的空域、频域或协议结构中并主要通过因特网传输的隐蔽通信技术。信息隐藏具有下述基本特性：

（1）不可感知性。不可感知包含两方面含义：①看不见听不到。因隐藏信息导致图像或音频信号的变化对观察者来讲应该是不可察觉的，隐藏信息的存在不应明显干扰载体数据，不影响载体数据的正常使用。最理想情况是携带信息媒体信号在视觉或听觉上一模一样，至少肉眼或耳朵是无法区分的，这是绝大多数信息隐藏算法应达到的基本要求；②统计不可见。隐藏信息用统计方法是不能恢复的。通过对大量观测样本进行统计分析不会泄漏隐藏内容的有关信息。

（2）密钥安全性。与信息加密技术一样，信息隐藏技术也是把对信息的保护转化为对密钥的保护，因而密码学中对密钥的基本要求也适用于信息隐藏技术，如必须要有足够大的密钥空间，满足 Kerckhoffs 准则等，甚至在设计一个信息隐藏系统时，密钥的产生、发放、管理等也都需要综合考虑。

（3）可恢复性。隐藏有信息的信号在传输过程中，可能会遇到某些情况致使载体信号受到损坏，如网络拥塞、服务质量因素造成丢包等。为了保证隐藏信

息的完整性，信息隐藏技术应具有从部分信号中恢复完整信息的能力。

对于数字水印技术，隐藏的信息主要是与载体内容有关的版权等信息，用于认证载体内容的版权归属、根据隐藏信息描述的权限规则管理载体内容使用。数字水印除了具备上述信息隐藏特性外，还需满足以下特性：

（1）稳健性。隐藏的信息在传输过程中可能会遭到各种有意或无意破坏。以图像为例，在传输过程中信息量比较大，为了节省信道资源，在传递之前都会先将传递的资料进行压缩处理。压缩技术一般可分成两类：无损压缩和有损压缩。无损压缩并不会造成秘密信息的破坏，但压缩率较低；虽然有损压缩技术可能会造成秘密信息的破坏，但因其压缩倍率较高，多媒体多采用有损压缩技术来处理。因此，信息隐藏必须考虑这种来自非恶意操作造成的威胁，使秘密信息对正常的有损压缩技术具有一定的免疫能力。这种免疫力的关键是要使隐藏信息部分不易被有损压缩破坏，也不易被通常的信号变换操作所破坏。实际上稳健性与不可感知性始终是一对矛盾，不存在完全满足这两种要求的隐藏方法。通常只能根据需求的不同有所侧重，采取某种折中，使一方得以较好的满足，而使另一方作些让步。数字水印也应该具有一定的抵抗媒体某种处理而导致隐藏信息丢失的能力，在图像处理过程中类似过滤操作、重新采样、编码、有损压缩、模/数转换等都是常用的信号处理手段。

（2）足够的数据有效载荷。数据有效载荷指在单位时间内或在一个作品中隐藏的水印比特数[1]。对于图像而言，就是指在图像中隐藏的比特数；对于音视频而言，是指在每秒传输数据中隐藏的比特数。当然数据有效载荷所指的比特数是满足稳健性、不可感知性等前提条件的隐藏比特数。不同应用场景对数据有效载荷的要求不同。波音公司对4个有发展前途的且致力于数字电影的公司就其对水印要求进行了问卷调查[2]。认为必须能够满足在标准的400ms～500ms的帧间传输速率下保持水印嵌入实时性，必须有足够的有效荷载量。一般情况下，为了确保高清晰度影片的安全性需要10min～15min的容量。15s的中等清晰度商业广告需要10比特-15比特的有效荷载量植入。

（3）不可抵赖性。水印能为受保护数字产品的版权归属提供完全和可靠的证据。水印系统识别被嵌入到保护对象中的所有者信息（如注册的用户号码、产品标志或其他相关信息等），并能在需要的时候将其提取出来。而且恢复出的水印信息或水印判决的结果应该能够确定地表明所有权归属问题，不会发生多重所有权和所有权抵赖的纠纷。

（4）算法的实时性和低复杂度。在实际应用中，媒体分发服务器可能需要实时检测或嵌入水印信息，如移动网络的消息服务中心每秒钟要处理近百条的多媒体彩信，这就要求在这些媒体中嵌入和检测水印的算法应简单、快速，满足

服务器实时性的要求；另一方面，对于用户也需要无间断的、实时的媒体播放和体验，像在资源有限的设备（如手机终端）中进行水印操作时还要考虑有限的存储空间和计算资源，要根据时间复杂度和空间复杂度的要求对数字水印算法进行设计和选择。

（5）多重水印技术。比如影视节目制作者在给发行者的拷贝中插入有关发行者水印信息，发行者在给使用者的拷贝中插入有关使用者水印信息。如果在发行过程中出现漏洞而发生盗版，只要读取样本中的水印就可以判定在哪个环节出现问题。

1.2 信息隐藏历史

信息隐藏的发展历史可以一直追溯到“匿形术（Steganography）”的使用。“匿形术”一词来源于古希腊文中“隐藏的”和“图形”两个词语的组合。虽然“匿形术”与“密码术（Cryptography）”都是致力于信息的保密技术，但是，两者的设计思想却完全不同。“密码术”主要通过设计加密技术，使保密信息不可读，但是对于非授权者来讲，虽然他无法获知保密信息的具体内容，却能意识到保密信息的存在。而“匿形术”则致力于通过设计精妙的方法，使得非授权者根本无从得知保密信息的存在与否。相对于现代密码学来讲，信息隐藏的最大优势在于它并不限制对主信号的存取和访问，而是致力于签字信号的安全保密性。

信息隐藏起源于古希腊，Herodotus（前 486—前 425）在他的 Histories 一书中曾经描述到[3]：“在古希腊反抗波斯人的战争中，为了安全地传送军事情报，奴隶主剃光奴隶的头发，将情报刻在奴隶的头皮上，待头发长起后再派出去传送秘密消息”。大量这样的技术是在特洛伊战争时期被人们发明和传播的。我国古代也早有利用藏头诗、藏尾诗、漏格诗以及绘画等形式将“密语”隐藏在诗文或画卷中的特定位置的隐蔽消息传递手段。

早期的建筑业艺术家们就已经懂得雕塑和油画等作品从不同角度看上去不尽相同，从而设立了透视图和变形的规则。在 16、17 世纪，这种变形图像提供了一种理想的用于伪装信息的方法。十七世纪的英国人 Wilkins 是资料记载最早使用隐写墨水进行秘密通信的人[4]。早期的隐写墨水是由易于获得的有机物（如牛奶和尿液等）或者“水中溶解盐块”制成，加热后颜色就会变暗而显现出来。后来随着化学工业的发展，在第一次世界大战中人们制造出了复杂的化合物做成隐写墨水和显影剂。但是随着“通用显影设备”的发明，这种方法被摒弃了。因为这种设备可以根据纤维表面的效果判断出纸张的哪一部分被蘸湿过。

第二次世界大战期间，德国军队曾利用微缩原理和照相方法，将秘密文件、

资料情报缩小至数十或数百乃至数千分之一，制成很薄的显微点膜片，然后，再把它们“埋藏”在书报杂志中的某个字及标点符号上，或是将超微膜片藏在邮票、信封内进入邮路传递。对方收到后，按照双方约定好的位置和标记，通过技术手段再重新将显微点还原成像[5]。美国军队则使用了扩频通信技术，将带有秘密信息的载波信号的频谱展宽，使得敌方截获美军通信信号后，频谱仪上呈现一片噪声，达到防止敌方解调信号的目的。

与古代伪装技术同样作用的数字方法在现代信息隐藏中得以使用。如许多信源编码技术，利用人类分辨系统的局限性，将信息隐藏到不会引起人类感知系统察觉的地方。例如频率相近的两个音调同时发声时，高音调会掩饰相对较弱的低音调。人眼对图像复杂纹理区域不如平滑区域敏感，对高频成分不如对低频成分敏感，在编码时对高低频成分分别采用粗细不同的量化，甚至对高频成分舍弃，仍然可以保持良好的视觉图像质量。

1.3 信息隐藏现状与发展趋势

在 1994 年的 IEEE 国际图像处理会议(ICIP'94)上，R. G. Schyndel 等人第一次明确提出了“数字水印”的概念[6]，从此掀起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、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。同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。在美国，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、IBM 等公司都一直在致力于信息隐藏技术方面的研究，并已取得了大量研究成果。国际信息隐藏研讨会迄今为止已举行了 6 届。我国的信息隐藏学术研讨会是于 1999 年由我国信息科学领域的何德全、周仲义、蔡吉人 3 位院士与有关研究单位联合发起的。与此同时，国家 863 计划智能计算机专家组于 2000 年 1 月举办了“数字水印技术学术研讨会”。此次研讨会由中科院自动化所模式识别国家重点实验室和北京邮电大学信息安全中心承办，与会者就数字水印技术的发展动态和趋势进行了全面、深入的探讨。第六届“全国信息隐藏技术学术会议”于 2006 年 8 月在哈尔滨工业大学举行。

除了学术界的研究之外，商业公司也开发出一些信息隐藏软件。如：DiSi-StegaNograph，EZStego，Gif-It-Up v1. 0，Hide & Seek (Colin Maroney)，JPEG-JSTEG (Derek Upham)，MP3Stego (Fabien A. P. Petitcolas，Comput-

er Laboratory, University of Cambridge), Nicetext (Mark Chapman and George Davida, Department of EE & CS, University of Wisconsin Milwaukee)等。一方面这些隐写软件为客户进行秘密通信,防止机密流失提供了通信手段,另一方面也为一些恶意的个人或团伙进行各种非法活动提供了便利。

信息隐藏技术也将是未来信息战对抗的焦点之一,是敌对双方借以获取和破解对方隐蔽通信的制高点。美国已经投入了大量的研究经费进行着针对隐写术工具检测算法的研究,国际上诸多情报机构也为此而绞尽脑汁。作为未来情报战的重要组成部分,信息隐藏技术必将对战争的进程和胜败产生重大影响,因此掌握其发展方向对于指导信息隐藏的研究有着重要意义。将来信息隐藏技术的研究将侧重于以下几个方面:(1)理论体系研究。信息隐藏还没有一个完整的理论体系,许多核心问题还没有解决。如信息隐藏容量的极限是多少?如何更好地隐藏信息?如何对隐藏信息进行检测、恢复、去除等?如何建立统一的信息隐藏理论体系?(2)研究隐写术与隐写分析对抗技术和隐蔽通信与隐蔽信号发现与干扰技术。

在数字水印方面,从1994年开始,国际学术界开始陆续发表有关数字水印的文章,且文章数量呈快速增长趋势。一些有影响的国际会议(如IEEE ICIP、IEEE ICASSP、ACM Multimedia等)以及一些国际权威杂志(如Signal Processing、IEEE Journal of Selected Areas on Communication、Communications of ACM等)相继出版了数字水印的专辑。数字图书馆、网上发行、网络美术馆、写真收藏和彩信等新概念层出不穷;MIDI、CD、VCD、DVD和MP3等数字化产品让人目不暇接。仅靠密码技术是不能完成多媒体数据的加密、认证和保护的,数字水印技术在数据安全中占有不可替代的地位。以DVD为例,参与研究其版权保护水印的就有包括IBM、NEC、SONY在内的数十家大型企业。但是,出版商在利用数字水印保护版权的同时,盗版者也在千方百计地想办法来去除版权标记。为了更好地保护版权,开发出更健壮的水印算法是当前的研究趋势。

德国已经研究了在打印和印刷的纸介质证件中加入隐藏标记的技术,用数字水印防止伪造电子照片。目前,研究该技术的研究所正在开发另一种新的系统,新系统既可在照片上加上牢固的数字水印,也可以经改动让数字水印消失,使任何伪造企图都无法得逞。美国Digimarc公司率先推出了世界上第一个商用数字水印软件,而后又以插件形式将该软件集成到Adobe Photoshop和Corel Draw图像处理软件中。随后,Digimarc公司又推出了一系列数字水印产品。"商标保护(brand protection)"技术通过将保密特征加入到产品包装的设计中,就可以在产品流通链的任何环节中进行产品的认证、辨别原版和复制版、防止产品伪造,并且能够通过供应链来跟踪产品的流通。"安全文档(secure docu-

ment)"技术将 Digimarc 的水印特征加入到重要的文档之中，以此来确认文档的真伪性，辨别原版文档和复制文档，防止未授权的文档复制及确认原始文档的授权应用等。在打印机、复印机中利用数字水印增加控制信息以限制打印的技术也正在研制中。美国财政部已委托麻省理工学院媒体实验室研究在彩色打印机、复印机输出的每幅图像中加入唯一的、不可见的数字水印，通过实时地从扫描票据中判断水印的有无，快速辨识真伪。IBM 东京研究实验室提出了用数据隐藏(data hiding)作为解决方案来鉴定数字化照片的来源，证实数字化照片的完整性，判断照片是否被篡改以及定位篡改的地方。IBM 东京研究实验室与 Yasuda Fire & Marine (YFM)公司联合开发了一种作为安全电子保险索赔的照片安全存档和传输系统的样机。该系统能协助地方服务部门进行汽车损失索赔工作，当索赔服务部门的调解员或修理厂的雇员使用这种安全数码相机和微型闪存器给一辆损坏的汽车拍照片，再利用安全图像编档和传输系统记录这些照片时，服务部门的经理和核算员就能够检查这张照片，并判断它是否用认证的照相机拍摄，是否有任何未被授权的更改。该安全电子索赔处理系统可运行于 Lotus Notes 系统，它能鉴定数字化照片的来源和证实其完整性，以及注册的照片是否来自认证的数码相机和是否被篡改。

数字水印开辟了一条崭新的信息安全途径，它的不可感知的隐蔽性和抵抗各种攻击的能力可以实现数字产品的完整性保护和篡改鉴定，还可用于数字防伪。数字水印必将成为数字作品的版权保护和真伪认证的核心技术措施之一，并在电子商务交易中发挥不可替代的作用。在市场经济飞速发展的今天，对于企业形象和经济利益存在严重损害危险的企业和数字产品创作者来说，这无疑是一个良好的解决方案。数字水印及其应用技术不仅提供了突破性的信息安全防护方式，而且在数字防伪中占据着重要的地位。它对维护国家经济秩序大有益处。表 1－1 所列为 M. Kutter 所整理的一些国际上从事数字水印方面研究的研究小组情况。这些研究小组及公司许多都有有关数字水印及信息隐藏方面的商业软件，读者也可从中免费获得一些软件和源码。

表 1－1　部分信息隐藏软件情况表

名　称	内容	人　员
NEC	_P_I_	Ingemar J. Cox
Università degli Studi di Firenze	LP_I_	Alessandro Piva
IBM	_P_I_	Boon-Lock Yeo
Univ. of Geneva	_P_I_	Joe Ó Ruanaidh
University of Erlangen	_P_I_A	Frank Hartung

（续）

名　称	内容	人　员
MIT-Meadi Lab	_P_I_	Josh Smith Nice
Columbia Univ.	T_P_I_	Marc Schneider Nicely
Purdue Univ.	T_P_I_	Delp & Wolfgang
Curtin University	TL_I_	Sebastien Wong
TU Delft	_LP_I_	Gerhard C. Langelaar
Univ. Thessaloniki ,Greece	_S_I_	Prof. Pitas
Los lamos Nat. Lab.	T_PSI_	Stanford et al
Computer Lab. , U. of Cambridge	_L_SI	Petitcolas

表中的内容栏中各字母的含义如下。T:有关水印信息的指南,L:链接到数字水印主页,P:有文章可下载,S:有软件可下载,I:图像水印,V:视频水印,A:音频水印。

近几年国内许多学者也相继开展了信息隐藏方面的研究,国家有关科技发展部门也日益重视此方面的研究。1999 年国家自然科学基金委员会政策局等组织有关专家,在北京组织召开了“网络计算和信息安全论坛”,强调了研究信息伪装的重要性,与会专家建议国家自然科学基金委员会在“十五”期间应当重点关注包括数字水印在内的网络环境下的信息安全领域的研究。2000 年,又在北京召开了信息安全方面的会议,将信息安全确定为优先资助领域,国家重点基础研究“973”也有信息隐藏方面的专项课题。

1.4　信息隐藏的应用

信息隐藏技术作为一种新兴的信息安全技术已经被许多应用领域所采用,当信息隐藏技术应用于保密通信领域时,称为隐蔽通信或低截获概率通信。当应用于因特网秘密信息传输时常被称为隐写术。作为版权保护的信息隐藏技术通常被称为数字水印技术。

1.4.1　数字内容保护

网络环境下由于数字媒体易于复制、传播的特点使得版权保护的重要性日益突出,因此越来越多的数字视频、声频信号及图像被“贴”上了不可见的标签,这些标签往往携带隐藏了的版权标识或序列号来防止非法拷贝。数字水印技术作为数字产品版权保护的潜在有效手段成为国际学术界与企业界广泛关注的焦

点。数字水印是携带所有者版权信息的数据，被永久地融合到数字产品中。它可以作为版权争端的法律凭证，用来指控盗版者，可以确立版权所有者，识别购买者或者提供有关数字内容的其他附加信息，并将这些信息以人不可感知的方式嵌入到数字图像、数字音频和视频序列中，用于确认所有权，验证数据完整性。具体如下所述。

(1) 证件防伪。数字水印技术可有效防止证件被伪造，以制作个人身份证为例，一般要经过照片扫描、签名、制证机输入、打印和塑封等过程。上述新技术是在打印证件前，在照片上附加一个暗藏的数字水印，处理后的照片用肉眼看与原来完全一样，必须用专门的扫描器才能检测出数字水印。这种方法可以迅速、无误地确定证件的真伪。

(2) 商标保护。该技术通过将保密特征加入到产品包装的设计中，就可以在产品流通链的任何环节中进行产品的认证、辨别原版和复制版、防止产品伪造，并且能够通过供应链来跟踪产品的流通。

(3) 安全文档。将水印特征加入到重要的文档之中，以此来确认文档的真伪性，辨别原版文档和复制文档，防止未授权的文档复制及确认原始文档的授权应用等。包括银行支票、护照、债券、身份证、塑料卡片、邮票、驾照、证书、票据、报表和包装等。

(4) 数据完整性验证。脆弱水印是指对某些处理稳健而对其他处理脆弱的水印。该技术可以验证数据是否被篡改。它与签名等密码技术的区别在于该技术允许根据实际应用场景对数据进行处理，而密码技术则认为对数据的任何处理都是篡改。比如在互联网上传输图像、音视频流这种大数据量时都先要进行必要的压缩，这时在传输之前加入一种能够抵抗压缩的脆弱水印，对数据的任何其他处理都可能导致水印的破坏，从而证明数据的完整性[7]。

1.4.2 隐密通信

把需要传递的秘密信息嵌入到公开的媒体中，这将有效地减少遭受攻击的可能性。如果再结合密码学的方法，即使敌方知道秘密信息的存在，要提取和破译信息也是十分困难的。替音电话技术就是把需要传递的秘密语音信息加密后嵌入到公开线路中的音频中，窃听者听到的是无关紧要的对话。隐蔽通信对稳健性要求较低，主要是需要抵抗未经授权的访问、模数和数模转换等信息传输过程中遇到的正常处理。匿名通信也是信息隐藏在隐蔽通信领域中的应用。所谓匿名通信就是寻找各种途径来隐藏通信消息的主体，即消息的发送者和接收者。在医用数字图像与通信标准中，图像数据与患者姓名、图像拍摄日期和诊断医生等说明内容是相互分离的。有时候会发生患者病情资料被暴露或丢失的现象，