IMAGE INFORMATION HIDING AND ITS APPLICATIONS

图像信息隐藏及其应用

吕英华 著

科学出版社

图像信息隐藏及其应用

吕英华 著

科学出版社

北京

内 容 简 介

基于图像与视频的信息隐藏技术作为信息安全领域的重要分支近年来得到了广泛关注，并蓬勃发展起来，在信息安全保护方面发挥了重要的影响和作用。本书综合了智能计算、机器学习的理论与方法，从面向应用的角度给出了系列的图像与视频信息隐藏方面的新观点、新方法和新技术。本书内容涵盖数字水印、数字密写及其应用，主要包括信息隐藏基本理论和方法、基于小波变换、奇异值分解、遗传算法和神经网络的水印技术、图像密写及视频水印方法。

本书可供高等院校计算机、信息安全等相关专业的高年级本科生、研究生、教师，以及相关领域的科研人员、工程技术人员使用。

图书在版编目(CIP)数据

图像信息隐藏及其应用/吕英华著. —北京：科学出版社，2014
ISBN 978-7-03-040541-8

Ⅰ. ①图… Ⅱ. ①吕… Ⅲ. ①图象处理—信息管理—研究 Ⅳ. ①TN919.8

中国版本图书馆CIP数据核字（2014）第089894号

责任编辑：任加林 戴薇/责任校对：刘玉靖
责任印制：吕春珉/封面设计：耕者设计工作室

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2014年5月第 一 版 开本：B5（720×1000）
2014年5月第一次印刷 印张：7
字数：105 000
定价：50.00元
（如有印装质量问题，我社负责调换（双青））
销售部电话 010-62134988 编辑部电话 010-62137026（HA08）

前　言

多媒体信息的数字化为多媒体信息的存取提供了极大的便利，同时也极大地提高了信息表达的效率和准确性。随着互联网的日益普及和发展，多媒体信息的利用已达到了前所未有的深度和广度，其发布形式也越加丰富。人们如今可以通过互联网发布自己的作品、重要信息和进行网络贸易等。但是，随之出现的问题也十分严重，如作品侵权更加容易，篡改也更加方便。因此，如何既能充分利用互联网带来的便利，又能有效地保护知识产权和隐秘而重要的信息，受到人们的高度重视。在这种背景下，一门新兴的交叉学科——信息隐藏正式诞生，并成为信息安全的重要分支和主流趋势。目前，信息隐藏作为隐蔽通信和知识产权保护等的主要手段，得到了广泛研究与应用。

信息隐藏技术是利用人类感官系统的敏感特性，将隐密信息以某种方式隐藏在特定的载体中，使之不被察觉或不易被注意到。信息隐藏技术主要分为数字密写技术（steganography）和数字水印（digital watermark）技术。其中，数字密写是指以图像、音频、视频等数字媒体作为掩护，把要发送的秘密信息嵌入到载体信号内部，以不引起外界注意的方式，通过公共信道，特别是互联网进行传递；而数字水印是将能够标志产品的作者、所有者、发行者、使用者或出品时间等信息按照一定的策略嵌入载体信号中，在需要时可通过提取算法将水印从载体数据中检测或提取出来。

本书以作者的多年研究工作为基础，综合了作者从事信息安全，尤其是图像信息隐藏研究的理论成果和教学实践经验，基于智能计算、机器学习的理论与方法，从面向应用的角度给出了系列解决图像信息隐藏的新观点、新方法和新技术。本书内容涵盖数字水印、数字密写及其应用三部分。

全书共分为十章。第 1 章介绍了信息隐藏基本理论和方法。第 2 章给出了基于小波包变换的特征水印算法。第 3 章基于奇异值分解和小波包变换相结合，提出了鲁棒水印算法。第 4 章给出了基于遗传算法的数字水印技术。第 5 章利用机器学习理论，给出了基于人工神经网络的数字水印复原技术。第 6 章提出了基于噪声可见性函数的图像密写方法。第 7 章提出了基于秘密分享的密写算法。第 8 章给出了基于图像内容的密写方法在生物识别中的应用研究成果。第 9 章针对数字视频，提出了基于运动目标分析的视频水印方法。最后在第 10 章

给出了总结与展望。各章节之间紧密配合、前后呼应，具有很强的系统性。同时，书中通过对研究过程和研究方法的讲述，使读者能够在以后的研究工作中得到很大的启发。

本书内容可以满足计算机科学与技术、电子工程、信息技术等相关专业高年级本科生、研究生和研究人员作为科研用书和参考资料的需要。每章所附的参考文献，希望能够帮助读者快速进入相应的研究领域并了解国内外的研究现状。

本书的主要内容是基于作者带领的科研团队在吉林省科技厅重点科技攻关项目（项目编号：20130206042GX、20140204089GX）中的研究与应用的积累与总结。在本书的撰写和整理过程中，本科研团队的其他成员付出了大量的时间和精力，在此对他们的辛勤工作表示衷心感谢！

本书的出版得到了东北师范大学人文学院出版基金的资助，在此表示衷心的感谢！

由于信息隐藏技术发展日新月异，加之作者水平有限，书中难免存在疏漏之处，恳请读者和有关专家批评指正。

目　　录

第1章 信息隐藏

多媒体数据的数字化为多媒体信息的存取提供了极大便利，同时也极大地提高了信息表达的效率和准确性。随着互联网的日益普及，多媒体信息的交流已达到了前所未有的深度和广度，其发布形式也更加丰富。人们如今可以通过互联网发布自己的作品、重要信息和进行网络贸易等，但是随之出现的问题也十分严重，如作品侵权更加容易，篡改也更加方便。因此，如何既充分利用互联网的便利，又能有效地保护知识产权，已受到人们的高度重视。在这种背景下，一门新兴的交叉学科——信息隐藏[1,2]正式诞生。如今，信息隐藏作为隐蔽通信和知识产权保护等的主要手段，正得到广泛研究与应用。

1.1 研究背景、目的和意义

1.1.1 网络时代和信息安全问题

当代的人类文明以网络为代表。实际上，我们早已生活在各种各样的网络中，从电力网、电话网、广播电视网、商业网到交通网。但是，所有这些网络都没有像互联网那样，在如此短的时间内影响如此多的政府、企业和个人。目前，网络已经成为互联网的代名词。在过去的几年中，随着计算机和网络技术的快速发展，互联网的规模急剧膨胀。以中国为例，互联网的用户1997年底为62万户，1998年底为210万户，到2002年初已达1591万户。互联网技术打破了传统的边界概念，使世界变得越来越小，而市场却越变越明显。在网络信息时代，任何产品、技术都要考虑到互联网。电子商务作为网络经济活动全新的技术手段和方法，已成为互联网最广阔的应用领域。电子商务是指在网络环境特别是互联网上进行的商务活动。从交易的参与者来看，电子商务有企业对企业、企业对消费者和消费者对消费者等几种类型。在网络经济时代，各国政府也都面临着角色转换以适应时代要求的新课题，许多国家都先后提出了构建电

子政府的纲领，我国也于1999年启动了“政府上网工程”。网络信息系统将在政府、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。

现有的计算机网络大多数在建设之初都忽略了安全问题，即使考虑了安全，也只是把安全机制建立在物理安全机制上，因此，随着网络的互联程度的不断扩大，这种安全机制对于网络环境来讲形同虚设。另外，目前网络上使用的协议，比如TCP/IP协议，在制定之初也没有把安全考虑在内。开放性和资源共享是计算机网络安全问题的主要根源，它的安全性主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。面对网络信息系统的种种威胁和网络安全与保密的重要性，必须采取有力的措施来保证网络信息的安全与保密。网络安全措施一般分为三类：逻辑上的、物理上的和政策上的措施。面对越来越严重危害计算机网络安全的种种威胁，仅仅利用物理上和政策（法律）上的手段来防范计算机犯罪显得十分有限和困难，因此也应该采用逻辑上的措施，即研究开发有效的网络信息安全技术。即使有了非常完备的安全与保密政策法规，有了非常先进的安全与保密技术，以及天衣无缝的物理安全机制，但是如果这些知识得不到普及，那么所有努力都将是前功尽弃。

人们对信息安全概念的认识在不断更新。20世纪80年代以前，人们把信息安全理解为对信息的机密性、完整性和可获得性的保护，其概念是面向数据的。在20世纪80年代的微机和局域网时代，用户和网络结构比较简单，信息安全是面向网管、面向规约的。20世纪90年代进入了互联网时代，每个用户都可以连接使用乃至控制分布在世界各个角落的上网计算机，故互联网的信息安全强调面向连接、面向用户。由此可见，面向数据的安全概念是信息的保密性、完整性和可获性，而面向使用者的安全概念则是鉴别、授权、访问控制、抗否认性和可服务性以及基于内容的个人隐私、知识产权等的保护。这两者结合就是广义信息安全概念。它是指所有涉及信息的安全性、完整性、可用性、真实性和可控性的相关理论和技术，它是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共信息安全的总和。而狭义信息安全是指信息内容的安全性，即保护信息的秘密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、毛虫、诈骗、盗用等有损合法用户利益的行为，保护合法用户的利益和隐私。信息安全体系结构中的安全服务问题要依靠密码、数字签名、身份验证、防火墙、安全审计、灾难恢复、防病毒、防黑客入侵等安全机制加以解决。其中密码技术和管理是信息安全的核心，安全标准和系统

评估是信息安全的基础。从技术角度看，信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、应用数学、数论、信息论等多种学科的边缘性综合学科。

1.1.2 信息安全技术概述

信息安全技术是一门综合的学科，它涉及信息论、计算机科学和密码学等多方面知识，它的主要任务是研究计算机系统和通信网络中信息的保护方法以实现系统内信息的安全、保密、真实和完整。网络信息安全涉及信息传输的安全、信息存储的安全、对网络传输加密技术、数据完整性鉴定技术；为保证信息存储的安全性，需保障数据库安全和终端安全；信息内容审计，是对进出内部网络的信息进行实时内容审计，以防止或追查可能的泄密行为。对用户的鉴别是对网络中的主体进行验证的过程，通常由三种方法验证主体身份，比如只有该主体具有独一无二的特征或能力，如指纹、声音、视网膜或签名等。

网络信息安全的技术特征主要表现在以下几个方面：

1）完整性，是网络信息未经授权不能改变的特性，即对抗主动攻击，保证数据的一致性，防止数据被非法用户修改和破坏。

2）保密性，是网络信息不被泄漏给未经授权用户的特性，即对抗被动攻击，以保证机密信息不会泄漏给非法用户。

3）可用性，是网络信息可被授权者访问并按需求使用的特性，即保护合法用户对信息和资源的使用不会被不合理的拒绝。

4）不可否认性，也称为不可抵赖性，即网络上所有参与者都不可能否认或抵赖曾经完成的操作和承诺。发送方不能否认已发送的信息，接收方也不能否认已接收的信息。

5）可控性，是对网络信息的传播及内容具有控制能力的特性，即能够对网络信息实施安全监控。

保护信息安全所采用的手段也称作安全机制。所有安全机制都是针对某些安全攻击威胁而设计的，可以按照不同的方式单独或组合使用。网络中采用的安全机制主要有：

1）信息加密和隐藏机制，加密使攻击者无法读懂消息的内容从而达到保护信息的目的；而隐藏则是将有用的信息隐藏在其他信息中，使攻击者无法发现，不仅实现了信息的保密，也保护了通信本身。至今，信息加密仍是保障信息安

全的最基本的手段。信息隐藏则是信息安全领域的一个新方向，它在数字化产品的版权保护等领域的应用中越来越受到人们的重视。

2）完整性保护，用于防止非法篡改，利用密码理论的完整性保护能够很好地对付非法篡改。完整性的另一用途是提供不可抵赖服务，当信息源的完整性可以被验证却无法模仿时，收到信息的一方可以认定信息的发送者，数字签名就可以提供这种手段。

3）认证机制，网络安全的基本机制，即网络设备之间相互认证对方身份，以保证合法用户进行正确的操作并进行正确的审计。

4）审计，防止内部犯罪和事故后调查取证的基础，通过对一些重要的事件进行记录，从而在系统出现错误或受到攻击时能定位错误和找到攻击成功的原因。审计信息应具有防止非法删除和修改的措施。

5）权力控制和存取控制，主机系统必备的安全手段，即系统根据正确的认证，赋予某用户适当的操作权力，使其不能进行越权的操作。该机制一般采用角色管理的办法，针对系统需要定义各种角色，如经理、会计等，然后对他们赋予不同的执行权力。

6）业务填充，在业务空闲时发送无用的随机数据，增加攻击者通过信息流量获得信息的困难。同时也增加了密码通信的破译难度。发送的随机数据应具有良好的模拟性能，能够以假乱真。

1.2 信息隐藏技术简介

随着计算机和通信网技术的发展及普及，数字音像制品以及其他电子出版物的传播和交易变得越来越便捷，但随之而来的侵权盗版活动也呈日益猖獗之势。近年来，数字产品的版权纠纷案件越来越多，因为数字产品被无差别地打印复制是轻而易举的事情，如果没有有效的技术措施来阻止这个势头，必将严重阻碍电子出版物行业及计算机软件业的发展。为了打击盗版犯罪，以上方面要通过立法来加强对知识产权的保护，另一方面必须要有先进的技术手段来保障法律的实施。虽然密码技术可用来解决其中的部分问题，但是密码技术存在着如下的三大缺点：

1）它明确的提示攻击者哪些是重要的信息，容易引起攻击者的好奇和注意，并有被破解的可能。

2）一旦加密文件被破解，其内容就完全透明了。

3）攻击者可以在破译失败的情况下将信息破坏掉，使得合法的接收者也无法阅读信息的内容。目前，信息隐藏技术以其特有的优势解决了密码技术的一些缺陷，开始引起人们的普遍关注。密码技术仅仅隐藏了信息的内容，而信息隐藏技术不但隐藏了信息的内容而且隐藏了信息的存在。人们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，某件数字产品中的版权信息表示版权的所有者，它可以作为侵权诉讼中的证据，而为每件产品编排的产品序列号可以用来识别购买者，从而为追查盗版者提供线索。此外，保密通信、电子商务以及国家安全等方面的应用需求也推动了信息隐藏研究工作的开展。

1.2.1 基本概念

20世纪90年代早期，信息隐藏的应用引起不同研究团体的关注和重视。1996年5月第一届国际信息隐藏学术研讨会[3]在英国剑桥的召开，使这些独立的研究团体走到一起，从而在信息隐藏的一些概念和术语上达成共识。信息隐藏（information hiding）有时也称数据隐藏（data hiding）。从广义上看，信息隐藏有多种含义：一是信息不可见，二是信息的存在性隐蔽，三是信息的接收方和发送方隐蔽，四是传输的信道隐蔽。信息隐藏就是将保密信息隐藏于另一非保密信息载体中，以不引起检查者的注意。这里的载体可以是图像、视频、音频，也可以是信道，甚至是某套编码体制或整个系统。广义上的信息隐藏技术包括数字密写技术、数字水印、数字指纹、隐藏信道、匿名通信等。从狭义上看，信息隐藏就是将某一机密信息秘密隐藏于另一公开的信息中，然后通过公开信息的传输来传递机密信息。狭义上的信息隐藏技术通常就是指数字密写技术与数字水印。

信息之所以能够隐藏在多媒体数据中是因为：

1）多媒体信息本身存在很大的冗余性。从信息论的角度看，未压缩的多媒体信息的编码效率是很低的，所以将这些机密信息嵌入到多媒体信息中进行秘密传送是完全有可能的，并不会影响多媒体信息本身的传送和使用。

2）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只有几十个灰度级；对边缘附近的信息不敏感。利用人的这些特点，可以很好地将信息隐藏而不被察觉。

通常，信息隐藏与信息加密都是把对信息的保护转化为对密钥的保护。信

息隐藏不同于传统的密码学技术。密码技术主要是研究如何将机密信息进行特殊的编码，以形成不可识别的密文进行传递；而信息隐藏则主要研究如何将某一机密信息秘密隐藏于另一公开的载体中，然后通过公开的载体来传递机密信息。对加密信息而言，可能的监测者或非法拦截者可通过截取密文，并对其进行破译，或将密文进行破坏后再发送，从而影响机密信息的安全；但对信息隐藏而言，可能的监测者或非法拦截者则难以从公开的载体中判断机密信息是否存在，难以截获机密信息，从而能保证机密信息的安全。为了增加破译的难度，也可以把加密技术和隐藏技术相结合，即先对待嵌入对象进行加密得到密文，再把密文隐藏到载体对象中。由此可见，传统的以密码学为核心技术的信息安全和隐藏式信息安全技术并不矛盾，而是互补的。

1.2.2 信息隐藏技术的发展

信息隐藏技术主要分为数字密写技术（steganography）和数字水印（digital watermark）技术。其中，数字密写是指以图像、音频、视频等数字媒体作为掩护，把要发送的秘密信息嵌入到载体信号内部，以不引起外界注意的方式通过公共信道，特别是互联网进行传递；而数字水印是将能够标志产品的作者、所有者、发行者、使用者或出品时间等信息按照一定的算法嵌入载体信号中，再通过提取算法将水印从载体数据中检测或提取出来。

数字水印与密写有着密切的联系，有些算法只要稍作改动，便可以相互通用，它们主要的性能指标都包括稳健性、隐蔽性、嵌入量。但由于应用领域的差异，数字水印和密写之间还有一些不同。对于数字水印来讲，上述三项性能的重要性排序是稳健性、隐蔽性、嵌入量。稳健性意味着水印不能被干扰或恶意去除，这是版权确认的保证，因此最为重要；隐蔽性保证了数字产品的商用价值；至于嵌入量，只要能够标识一些必要的信息，并没有过高的要求。而对于密写来说，这三项性能的重要性排序是隐蔽性、嵌入量、稳健性。隐蔽性包括视、听觉隐蔽性和统计上的隐蔽性，意味着临近者无法察觉，所以最为重要；隐蔽通信往往要求高传送率，故嵌入量其次；密写通常应用于无扰信道，所以对稳健性的要求最低。

1.3 数字密写技术

人们最早对密写技术的应用可以追溯到远古时代，一个著名的实例是发生在大约公元前440年的“剃头刺字”的故事[4]，一名叫Histaieus的人筹划着与他的朋友合伙发起叛乱，反抗米堤亚人和波斯人。他找来一位忠诚的奴隶，剃光其头发后，把信息刺在头皮上，等头发长出后把他派到朋友那里。他的朋友将这个奴隶的头发剃掉后获得了这个秘密信息。起义最终获得了成功。随着网络技术、多媒体技术及信息处理技术的迅速发展，人类生活进入到一个全新的数字社会。国际互联网的大力推广，使得各种数字信息资源得以方便而快速地传播。我们可以将重要的资料信息秘密地隐藏于普通的文件中，然后再通过网络等信道传递散发出去。这样伪装后的机密资料，并不像传统加密过的文件那样是一堆乱码，而是看起来和其他非机密性的一般资料无异，因而十分容易欺骗非法拦截者。

国际互联网技术的兴起极大地推动了信息产业的发展，由于网络逐渐普及，使人们的一切活动都通过各种信息系统紧密联系起来。信息的安全保密不仅与国家的政治、军事和外交有关，而且与团体、单位和个人密切相关。大量有关个人的数据（私人存款、医疗记录、财产数据等）都需要在网络上进行处理。信息一旦上网，它将可能被轻而易举地获取。对原始信息的非法复制、蓄意篡改会导致严重的后果，因而近年来无论是官方或是民间，对信息的安全存储、保密传输、真伪验证等问题，都引起了高度的重视。值得强调指出，信息的安全与保密，是整个社会安全与稳定的重要因素。

通常，数字密写系统的构成可以用图1.1表示。掩饰媒体是公开传送信息的载体，可以是文本数据、图像文件、语音文件等等。隐藏过程把要传送的秘密信息通过隐秘密钥并使用某种算法嵌入掩饰媒体，形成表面看来和掩饰媒体完全相同的隐秘对象。隐秘对象通过公开信道传输。接收者接到隐秘对象后，通过隐藏过程的逆过程，分解出秘密信息。数字密写系统的目的是在通信双方之间建立一条秘密通信路径，潜在的攻击者不知道这个通信的存在，任意第三者无法检测到秘密信息，故不能从掩饰媒体和隐秘对象对隐藏数据进行攻击。

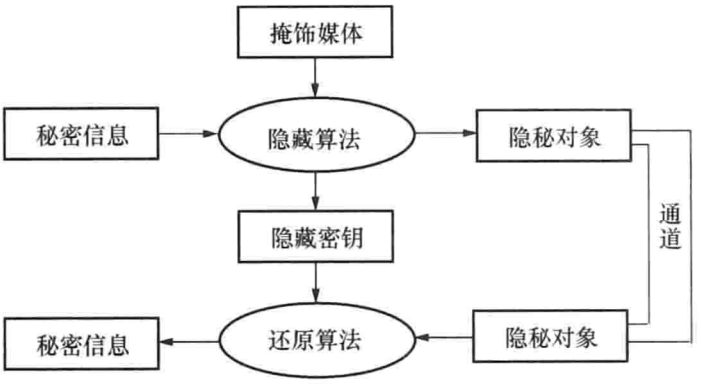

图 1.1 数字密写系统框图

1.4 数字水印技术

随着数字技术和因特网的发展，各种形式的多媒体数字作品（图像、视频、音频等）纷纷以网络形式发表，其版权保护成为一个迫切需要解决的问题。随着我国经济发展，电子商务、网上交易也迅速地发展起来，数字水印可以对这些电子服务提供保护。因此，数字水印技术发展前景非常广阔。由于数字图像很容易被复制，因此数字支票的正确认定就成了难以克服的问题。近年来迅速发展起来的数字水印（digital watermark）[5~7]技术为解决该问题提供了一种新的有效的途径。数字水印技术是指在数字化的数据内容中嵌入不明显的记号，可以是一段文字、标识、序列号等。被嵌入的记号通常是不可见或不可察的，但是通过一些操作可以被检测或者被提取。水印与源数据（如图像、音频、视频数据）紧密结合并隐藏其中，成为源数据不可分离的一部分。由于数字水印是实现版权保护的有效办法，因此如今已成为多媒体信息安全研究领域的一个热点，也是图像处理和信息隐藏技术研究领域的重要分支。在数字水印系统中，隐藏信息的丢失，即意味着版权信息的丢失，从而也就失去了版权保护的功能，也就是说，这一系统就是失败的。由此可见，数字水印技术必须具有较强的鲁棒性、安全性和透明性。

1.4.1 数字水印的分类及主要应用领域

数字水印有很多种分类方法，按照水印嵌入以后的表现形式来分可以分为可见水印与不可见水印[8]，其中不可见水印又可以称为隐含水印，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。可见水印目前研究较少，水印嵌入到图像以后是可以直接看到的，关键的信息被可见水印遮蔽，或者非法用户安全不能够将水印去掉。数字水印按照对图像篡改的敏感性分类，可以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，可以防止恶意的篡改，检测出图像被改动而不需要与原始图像作对比。鲁棒性数字水印是一种抗攻击的数字水印技术，最大限度地防止非法使用者获取、消除嵌入的数字水印。目前对水印的鲁棒性研究是最多的，但是还没有一种绝对安全的数字水印方法，也还没有找到一种抗所有攻击的数字水印方法。其中，对于图像的抗攻击性的研究，现在主要集中在图像处理技术、几何变换、JPEG压缩等上面，而抗图像旋转、剪切是鲁棒性的一个难点。但另一方面，仅研究上述抗攻击方法便判定图像数字水印的安全性是远远不够的。从安全的角度出发，脆弱水印可以具有很高的安全性。按照水印信息嵌入的位置可以分为：空域水印数字算法、变换域数字水印算法。直接改变空域中采样点的幅度值，嵌入水印信息称为空域水印；而改变变换域中的系数，嵌入水印信息称为变换域水印。空域水印数字算法是最早提出的水印方法之一，思想非常简单，但是抗攻击性能较差。变换域数字水印算法技术将水印信息嵌入到变换域系数中。实际上，对应于每种可以将图像作时频分析的变换，都可以找到一种与之相对应的数字水印方法。常见的变换包括离散余弦变换、小波变换、离散傅里叶变换等。另外还可以根据是否需要原始图像或者水印图像来分类，可以分为盲水印、非盲水印；根据水印方法是否可以公开来分类，可以分为公开水印、秘密水印；根据嵌入于检测操作的复杂度来分类，可以分为对称水印和非对称水印等[9]。

数字水印有着广泛的应用，其中主要领域有以下几个方面。

1. 版权保护

数字作品的所有者可用密钥产生一个水印，并将其嵌入原始数据，然后公开发布水印版本作品。当该作品被盗版或出现版权纠纷时，所有者即可以从盗版作品或水印版作品中获取水印信号作为依据，从而保护所有者的权益。

2. 加指纹

为避免未经授权的复制和发行，出品人可以将不同用户的ID或者序列号作为不同的水印（指纹）嵌入到作品的合法复制品中。一旦发现未经授权的复制品，就可以根据此复制品所恢复出的指纹来确定它的来源。