基于感知Hash的医学体数据鲁棒水印技术

李京兵　黄梦醒　周又玲　著

科学出版社

基于感知 Hash 的医学体数据鲁棒水印技术

李京兵　黄梦醒　周又玲　著

科学出版社
北京

内 容 简 介

数字水印是近年来信息安全领域的热点问题，本书主要包括以下内容：数字水印概论、基础理论、基于感知 Hash 的医学体数据鲁棒水印算法、基于感知 Hash 的医学体数据多水印算法。

全书详细地介绍了医学图像抗几何攻击的多种水印算法的实现方式，可作为通信与信息类、计算机类、电子工程类及相关专业的本科生、研究生教材或教学参考书，也适合于从事信息安全及知识版权保护工作的学者、技术人员、管理人员及法律工作者阅读。同时，本书还可作为安全系统、文本检索、多媒体通信、图像处理和模式识别等领域科技人员的参考资料。

图书在版编目 (CIP) 数据

基于感知 Hash 的医学体数据鲁棒水印技术 / 李京兵，黄梦醒，周又玲著. —北京：科学出版社，2015.11

ISBN 978-7-03-046293-0

Ⅰ. ①基… Ⅱ. ①李… ②黄… ③周… Ⅲ. ①三维－医学影像－水印－鲁棒设计－研究 Ⅳ. ①R445 ②TP309.7

中国版本图书馆 CIP 数据核字 (2015) 第 268009 号

责任编辑：任 静 / 责任校对：郭瑞芝

责任印制：徐晓晨 / 封面设计：华路天然工作室

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

北京教图印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2016 年 1 月第 一 版 开本：720×1 000 1/16

2016 年 1 月第一次印刷 印张：10 1/4

字数：200 000

定价：58.00 元

（如有印装质量问题，我社负责调换）

前　言

伴随着数字化信息时代的来临，计算机网络和多媒体技术的迅猛发展，各大医院也开展了信息化建设。同时，医疗信息技术的逐步发展，使得影像存档和通信系统、电子病历和医院信息系统日益普及。医学数字成像技术广泛用于放射医疗、心血管成像，并且在眼科和牙科等其他医学领域得到越来越深入和广泛的应用，原始的胶片图像存储方法正慢慢被数字化医学图像取代。医学数字成像技术和互联网技术的迅速发展，为远程医疗、远程诊断、学术交流带来了便利，有效地解决了医疗资源分布不均的问题。在医疗信息可以更快、更高效地在公共网络上传递的同时，也面临着一些安全问题。数字水印技术为解决这种信息安全问题提供了有效的手段。数字水印技术将标志性数字信息嵌入医学图像中，其特有的鲁棒性和安全性保证了在经历信息交流过程的数据处理后，仍能完整可靠地提取水印标志，使得远程医疗诊断、远程手术所需的相关患者资料在互联网上传输时，可以有效地保护患者的隐私，避免患者的资料被篡改，从而起到鉴别内容真伪、保护版权等作用，在判断病情、手术设计、医患沟通和医学教学等方面具有很高的研究价值。

数字水印技术作为信息隐藏技术的一个重要分支，是目前信息安全领域的前沿课题，其研究涉及信息学、密码学、数学、计算机科学、模式识别等多种学科。数字水印技术自 1993 年提出以来，发展已有二十多年了，各种算法层出不穷，但目前数字水印仍然是一个未成熟的领域，还有许多难题没有解决，特别是在抗几何攻击、多水印等方面还有许多瓶颈问题没有解决。本书针对这些问题，特别是抗几何攻击的医学图像水印算法提出了自己的算法，并成功申请了八项国家发明专利，读者可在此基础上举一反三。

本书以三维医学体数据作为研究对象，根据图像处理理论，从感知 Hash 技术和水印技术的特性出发，通过统计、分析大量的实验数据，在变换域利用体数据的感知 Hash 值，实现了体数据的水印嵌入与提取，这些基于图像(体数据)特征的算法具有抗几何攻击能力，它们将三维变换、混沌置乱和感知 Hash 进行了有机结合。本书提出的水印算法在医学图像抗常规和几何攻击等方面，都有一定的突破，并据此成功申请了多项国家发明专利。这些算法均基于感知 Hash 和变换域。本书使用了感知 Hash、混沌置乱、Arnold 置乱和全局三维离散余弦变换(DCT)、离散傅里叶变换(DFT)、离散小波变换(DWT)以及它们的结合体——小波余弦变换(DWT-DCT)、小波傅里叶变换(DWT-DFT)。创造性的工作如下。

1. 提出了四种基于感知 Hash 的医学体数据鲁棒水印算法

本书共提出了四种基于感知 Hash 的医学体数据鲁棒水印算法，分别为基于三维 DCT 感知 Hash 的医学体数据鲁棒水印算法、基于三维 DFT 感知 Hash 的医学体数据鲁棒水印算法、基于三维 DWT-DCT 感知 Hash 的医学体数据鲁棒水印算法、基于三维 DWT-DFT 感知 Hash 的医学体数据鲁棒水印算法。这些算法都是首先对医学体数据进行全局三维变换，选取低频部分的系数，再进行三维逆变换，然后在逆变换后的系数中提取一个鲁棒的感知 Hash 值，并将水印序列与该感知 Hash 值相关联，利用感知 Hash 值的鲁棒性实现数字水印的抗几何和常规攻击。并且与以往的水印算法相比，这些算法嵌入和提取水印的速度快，并且没有嵌入容量的限制，故有较高的实用价值，为医学水印的研究提供了一条新的途径。

2. 提出了四种基于感知 Hash 的医学体数据多水印算法

提出了四种医学体数据多水印算法，分别为基于三维 DCT 感知 Hash 的医学体数据多水印算法、基于三维 DFT 感知 Hash 的医学体数据多水印算法、基于三维 DWT-DCT 感知 Hash 的医学体数据多水印算法、基于三维 DWT-DFT 感知 Hash 的医学体数据多水印算法。它们都是利用医学体数据感知 Hash 值的鲁棒性进行水印的嵌入与提取，该算法将三维变换、混沌置乱和感知 Hash 有机结合。实验证明这些算法都具有理想的抗几何和常规攻击能力。与常规的医学体数据水印算法相比，这些算法有较高的鲁棒性，并且多水印的嵌入不影响原始体数据的体素数据值，没有嵌入容量的限制，是一种零水印方案，从而较好地保护了三维医学体数据。

总之，本书突破了传统的医学水印嵌入思想，创造性地提出了利用医学图像的感知 Hash 值来进行水印的嵌入与提取。并将感知 Hash、第三方概念、Logistic Map、Tent Map、Arnold 置乱和零水印技术有机结合成一体，较好地解决了医学水印的抗几何攻击、安全性等难题。

本书作为国内第一部关于基于三维变换感知 Hash 的医学体数据数字水印技术的专著，提出了一些基于三维变换感知 Hash 的抗几何攻击的新算法，其内容不但涵盖了图像感知 Hash，还覆盖了更加可视化的三维体数据。这些算法将数字水印、感知 Hash、第三方概念和混沌置乱有机地结合在一起，有效地解决了医学图像水印发展所遇到的一些难题。

本书共 4 章。第 1 章介绍了数字水印的背景知识、发展历史和现状等，介绍了目前研究的医学图像水印算法的发展历史和现状，并概括了基于感知 Hash 的数字水印算法的发展情况；第 2 章介绍了数字水印算法所需要的基础理论；第 3 章内容为基于感知 Hash 的医学体数据鲁棒水印算法；第 4 章内容为基于感知 Hash 的医学体数据多水印算法。附录 A 为数字水印常用名词英汉对照；附录 B 为简写符号对照

表；附录 C 为数字水印研究相关网址。

本书可以作为专业课程的指导书，也可作为课程设计和毕业设计指导书，同时还可以作为数字水印研发人员的入门参考书。

本书在编写过程中，参考了国内外出版的大量文献和网站资料（这些资料在本书中已尽量列出，若有遗漏深表歉意），在此对本书所引用文献的作者深表感谢。

海南大学的李京兵主要负责全书的组织、统稿及第 4 章的撰写；海南大学的黄梦醒和周又玲主要撰写了第 2 章，并负责全书整理；海南软件职业技术学院的韩宝如撰写了第 1 章、第 3 章和附录。

此外海南大学的李雨佳、胡艳芳等参加了本书的编写和整理，特此感谢。

本书的出版得到了海南大学 211 办公室高水平专著出版专项资金、国家自然科学基金（项目编号：61263033）、海南省高等学校科学研究专项项目（Hnkyzx2014-2）、海南省国际科技合作重点项目（KJHZ2015-04，KJHZ2014-16）、海南省高等学校优秀中青年骨干教师基金（2014-129）的资助和海南省自然科学基金（项目编号：614241）的资助。

由于作者水平有限，书中难免出现各种不足之处，欢迎大家批评指正。作者联系方式为Jingbingli2008@hotmail.com。

目　录

第 1 章　数字水印概述

1.1　背　　景

伴随着全球科技日新月异的进步，人们已步入数字化信息时代，在人们的日常生活中，很多东西都已经具有了数字化的意义。特别是随着互联网的发展与普及，人类在互联网上可以自由地遨游，获取人们想要的东西。1996 年，全球互联网用户不到 4000 万，1998 年就达到了 1 亿，2000 年互联网用户超过 2 亿，到 2005 年全球在线的互联网的用户达到了 10 亿，截至 2011 年，全球互联网使用人数已突破 20 亿。与此同时，数字图像、音频、视频等数字媒体也快速发展，人们可以通过 Internet 发布自己的多媒体作品(包括图像、音频、视频、动画等)，传递重要信息。另外，通过互联网进行数字媒体的复制、下载、发布变得非常方便。这给人们的生活和工作提供了便利条件，提高了工作效率。但另一方面，互联网也为数字媒体的盗版提供了方便。一些人在没有获得数字媒体所有者授权的情况下，随意复制和传播有版权保护的数字媒体出版物，并从中牟取巨大的非法利益。例如，有些数字媒体还没有公开发行或刚发行，几乎同时人们在互联网上就可以免费下载、复制。这大大侵犯了数字媒体版权所有人和制作人的利益，抑制了该产业的蓬勃发展。此外，一些政府文件、银行账单和个人的信用资料在网上被恶意篡改，使得电子商务、电子政务不能顺利地推广应用。因此，在互联网时代，数字媒体的版权保护和认证问题变得日益重要，信息安全成为越来越重要的课题。为此，2006 年 3 月 27 日联合国大会通过决议，确定每年的 5 月 17 日为“世界信息社会日”。2006 年的“世界信息社会日”关注网络安全问题，呼吁“让全球网络更安全”。国际电信联盟秘书长赵厚麟指出，“让全球网络更安全”的内涵包括：提升社会各界对信息技术作为推动经济和社会发展的有力工具的认识，宣传误用信息技术可能造成的严重后果，同时建立相关的规章制度来抗击网络犯罪；提高年轻人和老年人的网络安全意识，推动他们积极参与本地区或跨地区的网络安全活动；采取适当的防范措施，防止滥用网络侵犯个人隐私。互联网是一把双刃剑，在给人们提供各种方便的同时，也存在着许多安全隐患，为数字媒体的盗版、侵权提供了方便。在世界各国政府日益重视知识产权的今天，如何在互联网上保护数字媒体的版权，已成为数字世界中一个非常紧迫的课题，并且它还关系到我国能否真正落实保护知识产权的国策，从而鼓励人们去科技创新，实时发明创造、建立创新型社会，获得更多的自主知识产权，以便在国际经济舞台上占有一席之地。

随着计算机技术的发展，基于传统密码学的版权保护技术日益暴露出存在的缺点和不足。首先，随着计算机硬件技术的提高，计算机处理能力不断提升，仅利用增加密钥长度来实现保密的可靠性并不高。更重要的是一旦传输的文件被非法拦截者破解，那么无论被复制、篡改，它将显得无能为力，这样它的安全性无法得到有效的保障；其次，人们在网上发布的图片、文本、音频和视频等数字多媒体信息，通常情况下，除了少数部分内容需要进行保密外，大多数内容都还是以正常的交流为目的，但如果仅为了版权保护，而将信息全部转换成大多数人看不懂的密文，则失去了信息传播和共享的意义；此外，一旦人们获得了密钥，那么就能轻易地破解其中的内容，此时加密的密文在人们面前就完全成为了明文，这样人们同样可以方便地复制和随意地传播，与版权保护的初衷相悖，显然这在现实应用中存在着一定的弊端。

作为信息隐藏学的一个重要分支，近年来发展起来的数字水印技术则为传统密码学技术存在的问题提供了一个有效的解决方案，因此数字水印也成为国际学术界研究的前沿热点。数字水印技术是利用信号处理的方法在多媒体数据中嵌入具有特殊意义的标识信息(也称为水印)，以此来达到版权保护的作用，通常情况下，这种嵌入了标识信息的宿主媒体数据在主观感觉上不会引起明显的质量下降，不易被察觉。人们只有使用专用的检测器才能检测并分析宿主媒体数据中是否存在着水印，并且水印应该具有一定的抗有意或无意攻击能力，也就是嵌入的水印既能满足不可见性，又能很好地达到稳健性的要求，正是由于数字水印具有这些优势，其在人们日常生活中的应用非常广泛，尤其是版权保护方面。虽然数字水印技术并不能完全阻止盗版发生，但它可以有效地对保护的媒体数据进行真伪鉴别，为非法复制导致的版权纠纷提供有效而强有力的证据，并以此为依据打击一些非法盗版者，起到了保护知识产权的重要作用。由此可见，数字水印技术有其非常积极的现实意义和广阔的应用前景。

1.1.1　数字水印技术

数字水印(digital watermarking)是一种有效的数字产品版权保护和数据安全维护技术[1-7]，是信息隐藏技术研究领域的一个重要分支。其在信息隐藏中的位置如图 1.1 所示[8]。

1. 信息隐藏技术

信息隐藏(information hiding)目前成为国际信息技术研究领域的一个新兴的研究方向[8]，信息隐藏技术是研究如何将某一信息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隐藏的信息。由于含有隐藏信息的媒体发布是公开的，而

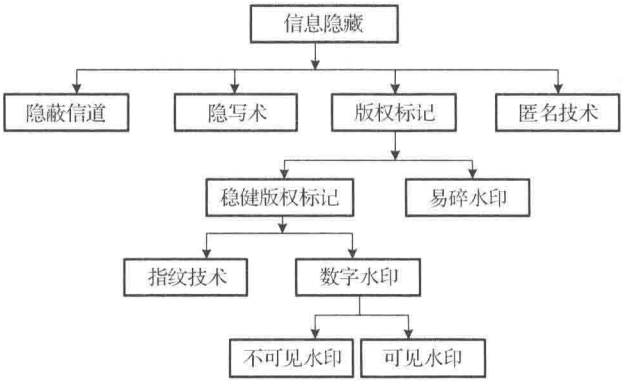

图 1.1　数字水印技术在信息隐藏中的位置

可能的检测者难以从公开的信息中判断隐藏信息是否存在，从而达到保证信息安全的目的。信息隐藏学作为隐蔽通信和知识产权保护等的主要手段正得到广泛的研究与应用。信息隐藏学和传统的密码技术并不完全一样，密码技术主要研究将机密信息(明文)进行特殊的编码，形成不可识别的密码形式(密文)进行传递；而信息隐藏主要研究如何将一个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。信息隐藏技术由于其具有的特点和优势，已成为当今多媒体信息安全技术的一大重要研究热点。

信息隐藏技术的一个重要应用是数字水印技术，关于该方面的应用本书将在后面章节中详细介绍，除此之外，还有以下应用。

(1)信息隐藏技术在军事上有重要用途。因为在现代战争中，信息战是不可避免的，那么在信息战中，若用常规的加密技术，密码的内容被加密成编码，形成一些不易识别的密文来进行传输，但这非常容易引起敌方的注意，敌人通过对信号的检测和定位，很快就会对发送装置进行攻击和破坏，但若通过信息隐藏技术，把重要信息隐藏在普通的图像等数字媒体中来发送，就不易引起对方的注意，从而使得发送装置免遭攻击。因此从国防安全的战略角度考虑，信息隐藏技术的研究意义重大。国家安全部门需要深入了解信息隐藏技术的原理，以便检测和跟踪那些对国家安全造成威胁的秘密信息的传递。

(2)互联网犯罪分子在进行网络犯罪时利用这一技术，通过频繁地改变身份和使用代理服务器，并在离线时抹去计算机中留下的踪迹，以防止计算机安全部门的追查。

(3)法律和相应部门需要深入了解信息隐藏技术的原理及其弱点，以便对妨碍国家和公共安全的秘密信息传递和其他行为进行检测和追踪。

信息隐藏主要工作原理如下：待隐藏的信息称为秘密信息，公开信息则称为载体信息(cover message)，而信息隐藏过程一般由密钥(key)来控制，通过嵌入算法将

秘密信息隐藏到公开信息中，而隐蔽载体(隐藏有秘密信息的公开信息)则通过信道传递，最后检测器利用密钥从隐蔽载体中恢复/检测出秘密信息[8,9]，信息隐藏模型如图 1.2 所示。

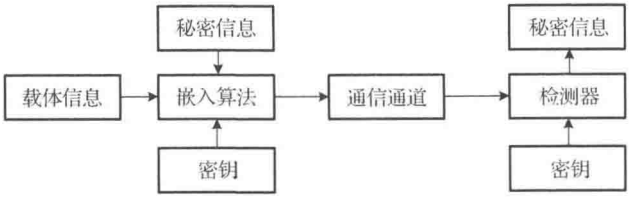

图 1.2　信息隐藏模型

此外，需要注意的是，解决信息安全问题，不仅需要加密算法和安全协议等技术手段，而且需要第三方认证等其他保密措施，是一个系统工程。

2. 数字水印技术

数字水印技术是通过一定的算法将一些标志性信息直接嵌入多媒体内容当中，但不影响原内容的价值和使用，并且不能被人的感知系统觉察到，只有通过专用的检测器或阅读器才能提取。这些标志性的水印信息可以是作者的序列号、公司标志、特殊意义的文本等，用来识别文件、图像或音乐制品的来源、版本、原作者、拥有者、发行人、合法使用人对数字产品的拥有权，可作为鉴定、起诉非法侵权的证据。

与加密技术不同，数字水印技术并不能够阻止盗版活动的发生，但它可以判别对象是否受到保护，监视被保护数据的传播，进行真伪鉴别，解决版权纠纷，并为法庭提供证据。

用于版权保护的数字水印的两大主要特性是鲁棒性(稳健性)和不可见性。鲁棒性就是当水印图像受到一定程度的常规和几何攻击后，照样可以提取出相应的水印；不可见性，就是嵌入的水印用肉眼不易发现。

1.1.2　数字水印的历史

一般认为，数字水印起源于古老的水印技术。这里提到的“水印”技术是指传统水印，即印在传统载体上的水印，如纸币上的水印、邮票和股票上的水印等，将它们对着光照，可以看到其中隐藏的图像。这些传统的“水印”用来证明其内容的合法性。

早在 1282 年，纸水印便在意大利 Fabriano 镇出现，这些纸水印是通过在纸模中加细线模板制造出来的。纸在存在细线的区域会略微薄一些，更透明一些。到了 18 世纪，在欧洲和美国制造的产品中，纸水印已经变得相当实用了。水印被用作商标，记录纸张的生产日期，显示原始纸片的尺寸。大约也是这个时期，水印开始用

于钱和其他文件的防伪措施。纸水印的存在既不影响美感，也不影响纸张的使用。中国是世界上最早发明造纸术的国家，也是最早使用纸币的国家。宋真宗在位时(公元 998—1022 年)，四川民间发明了“交子”。交子正面都有持票人的印记，有密码画押，票面金额在使用时填写，可以兑换，也可以流通。可以说，交子上的印文既包含水印技术也包含消隐技术。

伪造促进了水印技术的发展。英国人威廉·康格里夫发明了一种制造有色水印的技术，方法是在造纸过程中把经过染色的物质插入纸币中。由此制成的水印极难伪造，英格兰银行自身也因它们太难制造而拒绝使用这种水印。另一个英国人威廉·亨利·史密斯发明了一种更实用的技术取代了精细线模式。该模式用一种浅的浮雕雕刻制造早期水印，并把水印嵌入纸模中，由此产生的铸模表面的多变性创造出一种具有不用灰度阴影的漂亮水印，这就是今天 20 美元钞票的杰克逊总统面部上所使用的基本技术。

事实上，正是由于纸水印和消隐技术的特性才真正启发了在数字环境下水印的首次使用。数字水印作为一门技术加以研究可以追溯到 1954 年，当时 Muzak 公司的埃米利·希姆布鲁克(Emil Hembrooke)为带有水印的音乐作品填写了一份题为“声音和相似信号的辨别”的专利[10]。此发明被 Muzak 公司用到了 1984 年前后。1961 年美国专利局这样描述了该项发明[11]，“此发明使得原创音乐的辨认成为可能，从而可以建立一套阻止盗版的方法”。直到 20 世纪 90 年代初期，数字水印才作为一个研究课题受到了足够的重视。

1993 年，澳大利亚的 Tirkel[12]所撰写的《Electronic water mark》一文首次使用了“water mark”这一术语。这一命名标志着数字水印技术作为一门正式研究学科诞生。后来二词合二为一就成为“watermark”，而现在一般都使用“digital watermarking”一词表示“数字水印”。本书后面出现的“水印”一般指的都是数字水印。

数字水印技术自 1993 年[13]被提出以来，由于其在信息安全和经济上的重要地位，发展较为迅速，世界各国的科研机构、大学和商业集团都积极地参与或投资支持此方面的研究。例如，美国财政部、美国洛斯阿拉莫斯国家实验室、欧洲电信联盟、德国国家信息技术研究中心、日本 NTT 信息与通信系统研究中心、美国麻省理工学院、美国南加利福尼亚大学、英国剑桥大学、瑞士洛桑联邦理工学院、微软公司、朗讯贝尔实验室等都在进行这方面的研究工作。IBM 公司、日立公司、NEC 公司、Pioneer 公司和 Sony 公司五家公司还宣布联合研究基于信息隐藏的数字水印。美国的 Digimarc 公司于 1995 年率先推出了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 公司的 Photoshop 4.0 以上版本和 Corel Draw 图像处理软件中，这是一个基于 Internet 的水印认证系统，网上注册后可以实时地告诉注册用户的版权保护的图像在哪些网站上。Alpha 公司是

专门从事计算机图形学、图像处理、计算机视觉等专业软件开发的企业，其开发的数字水印产品 EIKONAmark 较好地解决了多次图像水印问题，可以添加 50 个以上不同的水印。另外，2001 年在瑞士成立的 AlpVision 公司，推出了 Lavellt 软件，能够在任何扫描的图片中隐藏若干字符，这些字符标记可以作为原始文件出处的证明和文档的保护与跟踪。MediaSec 公司的 SysCop 用水印技术来保护多媒体内容，欲杜绝非法复制、传播和编辑。

国际学术界陆续发表了许多关于数字水印技术方面的文章。几个有影响的国际会议(如 IEEE ICIP、IEEE ISCAS、ACM Multimedia 等)和一些国际权威学术期刊也相继出版了数字水印的专辑。1996 年 5 月，国际第一届信息隐藏学术研讨会(International Information Hiding Workshop，IHW)在英国剑桥大学牛顿数学科学研究所召开，至今该研讨会已举办了十一届。在 1999 年第三届信息隐藏国际学术研讨会上，数字水印成为主旋律，全部 33 篇文章中有 18 篇是关于数字水印的研究。1998 年的国际图像处理大会(International Conference on Image Processing，ICIP)上，还开辟了两个关于数字水印的专题讨论。我国于 1999 年 12 月 11 日，由北京电子技术应用研究所组织，召开了第一届中国信息隐藏学术研讨会(China Information Hiding Workshop，CIHW)，至今已成功举办了九届，在很大程度上推进了国内水印技术的研究与发展。

另外，数字水印技术也引起了政府和其他一些机构的兴趣并得到了广泛的支持。欧洲的 Tailsman 计划在视频产品中加入水印，OCTALIS(Offer of Contents through Trusted Access Links)项目的目标是建立具有版权保护功能的机制，Certimark 项目则专门研究水印技术。国际标准化组织也在数字水印领域表现了极大的兴趣，如 JPEG2000 和 MPEG4 都结合了水印技术。

随着国际间的信息与技术交流，国内的许多研究所和高校也投入到数字水印的研究中[14-18]，如中国科学院自动化研究所、哈尔滨工业大学、中山大学、北京交通大学、湖南大学、北京邮电大学等。虽然国内在这一领域的研究起步稍晚一些，但与国际领先机构的水平相差甚微。

2001 年 1 月，由国家 863 计划智能计算机专家组织召开了“数字水印技术研讨会”，来自国家自然科学基金委员会、国家信息安全测评认证中心、中国科学院自动化研究所模式识别国家重点实验室、中科院计算所 CAD 开发实验室、北京大学、浙江大学、上海交通大学、国防科学技术大学、复旦大学等多家科研机构的专家学者和研究人员参加了这次会议，这充分反映了我国对这一领域研究的高度重视[9]。2010 年 9 月 1 日在成都召开了第九届全国信息隐藏研讨会(CIHW2010)，这些学术会议的召开很大程度地推进了国内水印技术的研究与发展。另外国家对信息安全产业的健康发展也非常重视，在《2006 年国家自然科学基金项目指南》中，将“数字媒体内容安全关键技术及评测方法的研究”，特别是“抗几何攻击的安全数字图像/

音频/视频水印、几何造型数字水印”，作为重点支持方向之一。在《2007 年国家自然科学基金项目指南》中，把“文本信息隐藏”的研究作为重点支持方向之一。国家 863 计划、973 计划、国家自然科学基金项目等都对数字水印的研究有项目资金支持[19,20]。

现在，国内也已出现了一些生产水印产品的公司和产品，2005 年 7 月 27 日由华旗研究院研制的爱国者数字水印数码相机，可以在相机拍出的照片存储到存储卡之前嵌入水印信息，这样充分地保护了最初捕获到的图像内容。

虽然数字水印在国内的应用还处于初级阶段，但水印公司的创办使得数字水印技术在国内不仅仅只停留在理论研究的层面上，而是从此走上了实用化和商业化的道路，这样更能推动国内水印技术的蓬勃发展，为国内的信息安全产业提供有效、安全的保障。

1.1.3　数字水印的工作原理

数字水印是近年来出现的数字产品版权保护技术。可以标识作者、所有者、发行者、使用者等，并携带有版权保护信息和认证信息，目的是鉴别出非法复制和盗用的数字产品，作为密码学的加密或置乱技术的补充，保护数字产品的合法复制和传播。

数字水印的工作过程主要由水印的嵌入、提取和检测三部分组成(以下图 1.3 原理图中，媒体以图像为例)。

1. 数字水印的嵌入

通过嵌入水印算法，在密钥(K)控制下，将水印信息嵌入要保护的原始图像中，生成水印图像。数字水印嵌入原理如图 1.3 所示。

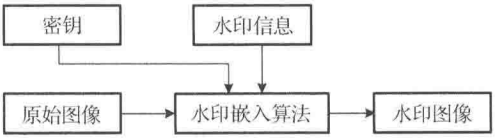

图 1.3　水印嵌入过程

水印嵌入的具体过程就是把水印信号 $W=\{w(k)\}$ 嵌入原始图像 $F=\{x_0(k)\}$ 中，生成含有水印的图像 $X^W=\{x^w(k)\}$。

最常用的嵌入公式如下。

加法准则为

$$x^w(k)=x_0(k)+\alpha x(k) \tag{1.1}$$

乘法准则为

$$x^w(k)=x_0(k)(1+\alpha x(k)) \tag{1.2}$$

式中，α 是嵌入强度。在图像数字水印中，F 可以是像素值(空间域)，也可以是变换域的系数值(变换域)；数字水印研究之初，水印一般直接加在空间域，但其鲁棒性较差，因此现在水印常常嵌在变换域中，如离散小波变换(Discrete Wavelet Transform，DWT)、离散余弦变换(Discrete Cosine Transform，DCT)和离散傅里叶变换(Discrete Fourier Transform，DFT)的变换系数上，水印算法有较好的鲁棒性。

2. 数字水印的提取

水印的提取过程如图 1.4 所示。

虚线方框表示原始图像在提取水印时不是必需的，根据不同的算法有所取舍，不需要原始图像的提取方法为盲水印法，有较大的实用价值。

3. 数字水印的检测

由于水印图像(隐藏对象)可能受到常规或几何攻击，提取出来的水印信息也会发生一些变化，所以要通过计算嵌入水印与提取出的水印相关度，根据其值的大小来判断待测图像中是否含有水印，水印检测过程如图 1.5 所示。

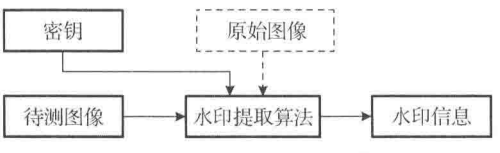

图 1.4　水印的提取过程

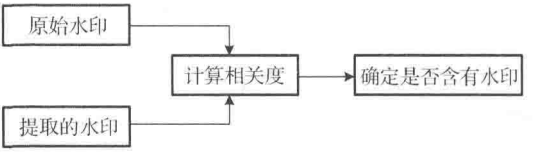

图 1.5　水印检测过程

1.2　数字水印的分类

1. 按数字水印的隐藏位置分类

根据数字水印嵌入的隐藏位置[21,22]，数字水印技术主要分为四类：空间域数字水印、变换域数字水印、分形数字水印和文件结构的冗余部分。

1)空间域数字水印

空(时)间域数字水印技术通过改变空(时)间域的某些像素的灰度值达到隐藏水印的目的。早期学者通过修改像素的最不重要位(Least Significant Bit，LSB)来嵌入水印信息[23,24]。后来陆续地提出了基于统计、序列扩展等空间域水印方案。空间域方法方便、快速，但安全性不高。

2) 变换域数字水印

变换域数字水印技术通过修改变换域系数来隐藏水印，是目前研究最多的一类水印。变换域数字水印又可分为基于 DCT、DFT、DWT 三种。

3) 分形数字水印

Puate 等[25]首先提出基于图像分形压缩的分形水印。图像分形水印是研究图像分形压缩和编码的基础，通过对图像的旋转、缩放、扭曲和反演等变成另一幅自相似图像。

4) 文件结构的冗余部分

这种方式建立在对数据格式和信道的分析上，如网络模型[26]、PDF 或 Word 格式的文件实际上有很多空闲的保留字节，替代这些空闲字节就可方便地嵌入水印。

2. 按数字水印提取过程分类

根据水印提取时是否需要原始载体[8]，水印技术可以是非盲(non-blind)、半盲(semi-blind)和盲(blind)的。非盲水印在提取时需要原始载体和原始水印的参与；半盲水印不需要原始载体，但需要原始水印；而盲水印既不需要原始载体也不需要原始水印。一般来说，非盲水印的鲁棒性要好一点，实现过程比较简单，但从实用的角度来看，盲水印更符合人们的要求，因为水印的提取过程不需要原始图像的参与，但实现过程比较困难。

3. 按数字水印的鲁棒性分类

按照鲁棒性来分，可分为脆弱水印[27-32]、半脆弱水印[33-36]和鲁棒性水印[37-52]。鲁棒性水印是指对含水印的载体进行信号处理(如压缩、剪切、加噪、滤波等)后仍能从载体中提取出水印。脆弱水印主要用于完整性认证，与鲁棒性水印的要求相反，脆弱水印必须对信号的篡改很敏感，人们根据脆弱水印的状态就可以判断数据是否被篡改过。还有一种水印介于二者之间，称为半脆弱水印，对一些操作鲁棒，但对重要数据特征的修改操作是脆弱的。有些水印系统将鲁棒性水印和脆弱水印结合起来，可以对经过恶劣信道或被恶意处理的信息进行恢复[53]。

4. 按数字水印的嵌入方式分类

根据数字水印提取后是否可以完全恢复原始图像，数字水印技术可以分为不可逆水印(irreversible watermark)和可逆水印(reversible watermark)。其中，可逆水印又称为无损水印(lossless watermark)。可逆水印技术是数字水印领域近年来快速兴起的研究方向之一，是当今水印研究的热点。