

长江学者论丛

数字水印 理论与技术

■ 杨义先 钮心忻 编著

Theory and Applications
of Digital Watermarking



高等教育出版社
HIGHER EDUCATION PRESS

长江学者论丛

数字水印 理论与技术

■ 杨义先 钮心忻 编著

Theory and Applications
of Digital Watermarking



高等教育出版社
HIGHER EDUCATION PRESS

内 容 提 要

本书从理论和技术两个方面对数字水印相关知识进行了全面、系统的介绍。全书共分六章,分别对数字水印基础理论、图像水印、语音水印、视频水印、软件水印和数字产品产权保护等进行了介绍。全书内容覆盖了包括数字水印原理、数字水印攻击等诸多方面数字水印理论与技术方面的主要内容。

本书可作为信息安全、密码学、信息与计算机科学等专业的研究生和高年级大学生的教学参考书,也可作为上述领域中相关科技工作者的实用工具书或技术培训教材。另外,书中介绍的许多算法、协议、方案等都可直接应用于工程实践,书中提出的许多理论问题将有助于激发更多的后继研究。

图书在版编目(CIP)数据

数字水印理论与技术/杨义先,钮心忻编著. -北京:
高等教育出版社,2006.3
ISBN 7-04-018301-3

I. 数... II ①杨... ②钮... III. 电子计算机-密
码术 IV. TP309.7

中国版本图书馆 CIP 数据核字(2006)第 020464 号

策划编辑 刘 英 责任编辑 刘 英 封面设计 王凌波
责任印制 陈伟光

出版发行	高等教育出版社	购书热线	010-58581118
社 址	北京市西城区德外大街 4 号	免费咨询	800-810-0598
邮政编码	100011	网 址	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landaco.com
经 销	蓝色畅想图书发行有限公司		http://www.landaco.com.cn
印 刷	北京市白帆印务有限公司	畅想教育	http://www.widedu.com
开 本	787×1092 1/16	版 次	2006 年 3 月第 1 版
印 张	24.75	印 次	2006 年 3 月第 1 次印刷
字 数	470 000	定 价	42.00 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

版权所有 侵权必究

物料号 18301-00

“长江学者”学术著作出版资助项目 

“长江学者论丛”编辑出版指导委员会

主任委员：赵沁平 教育部副部长

副主任委员：金国藩 清华大学教授，中国工程院院士

闵乃本 南京大学教授，中国科学院院士

吴树青 北京大学教授，教育部社科委主任

饶子和 清华大学教授，中国科学院院士，长江学者特聘教授

舒德干 西北大学教授，长江学者特聘教授，长江学者成就奖获得者

“长江学者论丛”编辑出版指导委员会办公室

主任：吴德刚 教育部人事司司长

副主任：刘志鹏 高等教育出版社社长

吕玉刚 教育部人事司副司长，教育部人才发展办公室主任

吴向 高等教育出版社副总编辑

序

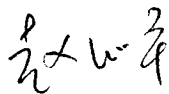
当今世界，科学技术日新月异，知识经济方兴未艾，综合国力竞争日趋激烈。面对日益激烈的国际竞争，立足国情，我国只能走建设创新型国家的发展道路，把提高自主创新能力作为调整经济结构、转变增长方式、提高国家竞争力的中心环节。而科技和人才，特别是创新人才是建设创新型国家和提高自主创新能力的关键。实施科教兴国、人才强国战略，建设创新型国家，构建社会主义和谐社会，高等学校肩负着重大历史使命。教育大计，人才为本。人才问题，始终是高等学校改革与发展的核心问题和头等大事。加快建设高等学校高层次人才队伍，努力培养和造就一批在国际上有重要影响的学术大师、战略科学家和学科带头人，是发展我国高等教育事业的必然要求，也是关系社会主义现代化建设全局的重要任务。

为贯彻落实科教兴国和人才强国战略，推进我国高等学校高层次人才队伍建设，教育部与香港李嘉诚基金会于1998年共同启动了“长江学者奖励计划”。该计划自实施以来，在党和国家领导人的高度重视和关心下，在国家财政等有关部门、高等学校和社会各界的大力支持下，取得了显著成效，在海内外引起了强烈反响。诺贝尔物理学奖获得者杨振宁评价“长江学者奖励计划”是“一个非常了不起的壮举”，“是20世纪末21世纪初中国实施科教兴国战略的一个非常重要的环节。”

长江学者群英荟萃、硕果累累。“长江学者奖励计划”的实施吸引、汇聚和造就了一大批优秀拔尖人才。目前全国88所高等学校聘任727位长江学者，先后有6位优秀学者获得“长江学者成就奖”，31位长江学者被聘为“973”首席科学家，24位长江学者当选为中国科学院、中国工程院院士。在“长江学者奖

励计划”的激励和支持下，长江学者们取得了一批重大科研成果，近年来共有20余篇论文发表在《Nature》、《Science》上，近百项科研成果获得国家自然科学奖、技术发明奖、科技进步奖，其中3项成果获得一等奖，20余项重要成果入选“中国十大科技进展新闻”、“中国基础研究十大新闻”、“中国高校十大科技进展”，有力地支持了国家重大战略的实施，促进了学科建设和科技发展，为培养和造就优秀拔尖创新人才做出了贡献。

编辑出版长江学者学术著作，得到了广大长江学者的积极响应和高等教育出版社的大力支持。希望《长江学者论丛》的出版，进一步提高长江学者在学术领域的影响力，并激励广大学者弘扬长江学者的创新精神，勇攀科学高峰，更好地为促进高校在提高国家自主创新能力、建设创新型国家的伟大事业中，做出更大的贡献。



2006年1月

前 言

数字水印有许多孪生兄弟:信息隐藏、数字指纹、信息伪装、叠像术、替音术等。但是,在所有这些孪生兄弟中,数字水印本身要算是最幸运的了。从近十年前诞生到现在,研究数字水印的学者已经遍布信息安全、密码学、信息与计算科学、通信与信息系统、信号与信息处理、应用数学、控制理论与控制技术、模式识别与智能系统、计算机系统结构、计算机软件与理论、计算机应用技术、军事通信学、软件工程、数字内容、数字媒体设计等领域。在数字水印方面,每年都有大量的论著在国内外发表,有大量的科研成果产生,有众多学术会议在世界各地召开,有许多专利被申请,有不少产品进入市场,有大批优秀专才走出学校等。然而,在这大好形势的背后,数字水印的发展仍然面临种种挑战。

第一,理论研究有待突破。

数字水印这个天生形象而准确的名称及其诱人的应用前景吸引了来自多个领域的首批科学家和工程师,因此,数字水印研究的起点确实具有典型的多科学性和差异性。如今,数字水印方面的研究成果纷繁复杂,理论基础实难统一,甚至名词术语都各不相同。经过近十年的高速发展,从理论角度看,数字水印研究已经到了“从量变到质变”的关键时刻了,如果不有意识地加以引导,将难免出现众多低水平重复性的结果和若干大同小异的学位论文!如果本书能够在引导数字水印理论研究方面起到抛砖引玉的作用,我们将十分高兴。我们认为数字水印理论研究的关键突破点至少包括以下几方面。

1. 数字水印的数学模型建立和隐藏容量分析。香农对通信系统的数学模型建立和信道容量的完整分析是信息论成功的关键,但是,至今在数字水印方面人们不知道如何去刻画数字载体隐藏水印的容量,不知道如何去度量人类感观失真度和水印隐藏量之间的关系,不知道用什么样的数学模型来统一数字水印的研究基础。虽然已经有人开始用游戏理论、信息论、概率论等来试图从攻击的角度建立数学水印模型,但是,到目前为止,还没有深入的结果而且模仿已知理论的色彩还较浓。希望广大的数字水印理论工作者不要再做小修小补式的“新型数字水印算法设计”了,而是,发挥理论优势,勇于攻艰,早日在数字水印容量分析方面取得突破性的成果,从而,建立完整的数字水印基础理论。

2. 数字水印的隐写检测与消除。作为信息安全的一个分支,数字水印也具有明显的“对抗性”。目前,人们的主要精力在于如何将水印完美地隐藏到载体信息中,而少有考虑如何判断某个数字内容中是否含有水印信息,以及如何消除或恢复这些水印信息。虽然已经出现了不少隐写分析方面的优秀成果,但是,这些成果的普适性都还较差,基本上处于“兵来将挡、水来土掩”的水平,远远不能

对付已有的各种数字水印算法的检测要求。

第二,成果应用即将爆发。

如果用“想像无限、应用无限”来形容数字水印也许并不为过。经过过去十年的积累,从应用角度看,数字水印的多种隐藏算法和协议等都已经完全达到了实用化的水平,特别是随着以网络游戏、数字动漫、数字电视、数字电影等为代表的数字内容产业的蓬勃发展,数字水印已经成为各种数字媒体的最有效保护手段之一,巨大的社会需求无疑将引发数字水印的应用高潮,对此,数字水印领域的广大工程师应该有充分的准备,抓住机遇,实现飞跃。如何用鲁棒的数字水印来实现各种数字媒体的产权保护与管理;如何用脆弱的数字水印来完成消息的认证与用户的鉴权;如何用数字水印提供的潜信道来存储与传输必要的隐私信息;如何用数字水印和其他安全技术来建立虚拟社会中的数字诚信体系,建立可信世界;如何用数字水印来增强网络空间中各环节的可生存性;等等。总之,数字水印的应用实在太广泛了,如果数字内容产业领域各专业的工程师们都能够有意识地利用数字水印来解决各自的问题。同时,数字水印工程师们能够积极主动地将数字水印成果推广给其他领域,那么数字水印应用的春天就到来了。希望本书的出版有助于促进这个春天的早日到来。

第三,政策法规不能落后。

各国政府对密码算法都有比较严厉的管制规定,因为,如果密码算法的使用过于泛滥将导致敏感信息传输的失控,将有损强力部门的信息监控力。数字水印虽然不是密码算法,但是,在特殊环境下,数字水印与密码算法可以达到异曲同工的效果。当前,世界各国政府对数字水印都未进行任何形式的监管,但是,这并不意味着政府应该永远无视数字水印的任意使用。如何在促进数字水印的理论与应用健康发展的同时,探索合理的管理规章制度,这对政府管理部门是一个挑战,同样对学术界和工业界也是一个挑战!当数字水印的应用已经“遍地开花”之后,出台数字水印的管理规章将更加困难。希望政府管理部门能够尽早地研究出积极的应对策略。

集中力量应对上述挑战是当前数字水印领域科学家、工程师们和其他相关人员的共同任务,为此,需要首先培养更多的数字水印专家。希望本书能够在促进数字水印的广泛应用,推动数字水印研究的理论水平方面起到积极的作用。

本书的各章(甚至各节)都尽量相对独立,以适应各种需求之读者自由组合并阅读相关章节。比如,信息安全专业或数字内容专业的研究生(包括博士生)或高年级本科生可以从头到尾认真阅读此书的全部内容,这样可以使他们对数字水印有一个比较全面系统的认识,为今后的进一步深造打下基础;理论研究者可以重点阅读第一章,特别是有关数字水印容量和检测部分;对图像、音频、视频软件保护应用感兴趣的读者可分别阅读第二章~第五章;关注数字内容产权保护的读者可阅读第六章和相应的媒体章节。希望本书所列的详细章节目录有助

于读者迅速了解每一章节的主题,并据此迅速找到自己关心的内容。如果我们的这些努力能够提高读者的阅读效率,那么我们就心满意足了。

本书还附有相当详细的参考文献目录,希望如此众多的参考文献能够帮助那些有特殊兴趣的读者直接进入自己的专业领域并了解国际上的相关最新动态。

本书是北京邮电大学信息安全中心和北京邮电大学数字内容研究中心全体成员多年来集体智慧的结晶。在本书写作过程中伍宏涛博士、梁华庆博士、牛少彰博士、夏光升博士、张立和博士、吴志军博士、姚惠明博士、刘郡硕士、苏佩良硕士、郭芬红硕士、胡昌利硕士、杨小兵博士、杨伟硕士、王勇硕士等为本书提供了丰富的资料。特别感谢胡正名教授、徐国爱副教授、李中献副研究员、罗群副教授、卓新建副教授、张茹博士、崔宝江博士、李剑博士、谷利泽博士、辛阳博士、李晖博士、李新博士、张振涛博士、夏光升博士、温巧燕教授、罗守山教授、牛少彰教授。他们同心协力,率领北京邮电大学信息安全中心两百余位研究人员在网络信息安全研究的丰富成果是本书的营养源泉。本书也是国家“973”项目(编号:G1999035804)、国家“863”项目(编号:863-306-ZT05-05-2)、国家自然科学基金项目(批准号:60073049、60473016)、北京市自然科学基金项目(批准号:4042022)和国防科技保密通信重点实验室基金项目(51436060101DZ0801)的成果总结。

由于作者水平有限,书中难免出现各种疏漏和不当之处,欢迎大家批评指正。

作者

2005年4月于北京

目 录

第一章 基础理论	(1)
1.1 数字水印原理	(1)
1.1.1 水印模型	(1)
1.1.2 水印评价指标	(10)
1.1.3 水印分类	(20)
1.1.4 数字水印与信息隐藏	(25)
1.2 数字水印攻击	(29)
1.2.1 未经授权的检测	(30)
1.2.2 未经授权的嵌入	(31)
1.2.3 未经授权的去除	(32)
1.2.4 系统攻击	(32)
1.2.5 一些常见的攻击	(32)
1.3 数字水印容量	(42)
1.3.1 问题描述	(42)
1.3.2 容量的影响因子	(46)
1.3.3 容量公式	(47)
1.3.4 结果分析	(53)
1.4 数字水印检测	(59)
1.4.1 检测分类	(59)
1.4.2 专项检测	(63)
1.4.3 通用检测	(70)
1.4.4 检测系统	(76)
参考文献	(80)
第二章 图像水印	(83)
2.1 普通图像水印	(83)
2.1.1 文件格式数字水印	(83)
2.1.2 图像插值数字水印	(86)
2.1.3 DCT 数字水印	(91)
2.1.4 二值图像数字水印	(95)
2.1.5 模数运算数字水印	(100)
2.1.6 公钥数字水印	(104)
2.1.7 渐进流数字水印	(114)
2.1.8 线性预测数字水印	(118)
2.1.9 Gabor 变换数字水印	(124)

2.1.10 调色板图像数字水印	(129)
2.1.11 G-对角占优数字水印	(133)
2.2 抗打印扫描水印	(138)
2.2.1 打印和扫描对图像的影响	(138)
2.2.2 基于人类视觉特性的图像块分类	(141)
2.2.3 抗几何失真的图像水印	(142)
2.2.4 基于 DCT 系数比较法的印刷水印	(144)
2.2.5 基于 DCT 域数据分类的印刷水印	(149)
2.2.6 应用案例:证件防伪数字图像水印方案	(152)
2.3 图像脆弱水印	(154)
2.3.1 基于数字水印的认证系统	(155)
2.3.2 图像完全级认证的水印算法	(156)
2.3.3 图像内容级认证的水印算法	(156)
2.4 图像鲁棒水印	(161)
2.4.1 基于数据集统计思想的抗数据增删水印	(161)
2.4.2 基于 DCT 的抗图像合并水印	(164)
2.4.3 基于小波变换的抗图像合并水印	(168)
2.4.4 抗综合几何变换的图像水印	(174)
2.4.5 彩信水印实例	(190)
参考文献	(196)
第三章 语音水印	(199)
3.1 语音水印基础	(199)
3.1.1 声音特性与听觉特性	(199)
3.1.2 语音水印的数学模型	(201)
3.1.3 语音水印技术与方案	(202)
3.1.4 语音通信阈下信道	(211)
3.2 基于 HAS 的小波包域数字语音水印	(220)
3.2.1 掩蔽门限的计算	(221)
3.2.2 将 DFT 域的掩蔽门限映射到小波包域	(223)
3.2.3 水印信号的产生与嵌入	(224)
3.2.4 水印信号的检测	(225)
3.2.5 实验结果	(226)
3.3 ABS 语音水印	(226)
3.3.1 ABS 编码与语音水印模型	(227)
3.3.2 ABS 语音水印的加载与提取	(231)
3.3.3 以 G.721(ADPCM)编码为载体的语音水印和提取算法	(232)
3.3.4 以 GSM(RPE-LTP)编码为载体的语音水印和提取算法	(236)
3.3.5 以 G.728(LD-CELP)语音编码为载体的语音水印和提取算法	(239)
3.3.6 以 G.729(CS-ACELP)语音编码为载体的语音水印	(242)

3.3.7 ABS 语音水印的测试结果及分析	(245)
3.4 语音水印应用实例	(247)
3.4.1 基于语音水印的保密通信系统	(247)
3.4.2 基于 PC 的保密通信系统设计与实现	(249)
3.4.3 语音信息隐藏电话	(261)
参考文献	(270)
第四章 视频水印	(273)
4.1 数字视频水印基础	(273)
4.1.1 数字视频水印的性能要求	(273)
4.1.2 数字视频水印的分类	(273)
4.1.3 数字视频水印的应用	(275)
4.1.4 数字视频编码标准 MPEG - 2	(278)
4.2 基于原始视频的水印	(284)
4.2.1 水印的嵌入算法	(285)
4.2.2 水印的提取算法	(286)
4.2.3 水印的公钥提取	(287)
4.2.4 实验结果	(288)
4.2.5 原始视频水印算法仿真与测试流程	(291)
4.3 基于视频编码的水印	(292)
4.3.1 运动速度图与嵌入位置	(293)
4.3.2 嵌入过程	(294)
4.3.3 水印的检测	(296)
4.3.4 实验结果	(297)
4.4 基于压缩视频的水印	(299)
4.4.1 运动速度水印模型	(299)
4.4.2 运动速度水印的嵌入	(300)
4.4.3 运动速度水印的检测	(301)
4.4.4 DCT 系数水印	(305)
参考文献	(309)
第五章 软件水印	(312)
5.1 软件保护概论	(312)
5.1.1 软件安全	(313)
5.1.2 软件水印技术	(317)
5.1.3 软件防篡改	(317)
5.1.4 软件混乱	(318)
5.2 软件水印的特征及分类	(319)
5.2.1 软件水印的理论模型	(320)
5.2.2 软件水印的功能分类	(321)
5.2.3 软件水印的生成分类	(322)

5.2.4 软件水印的攻击	(324)
5.3 静态软件水印	(328)
5.3.1 静态的含义	(328)
5.3.2 静态数据水印	(329)
5.3.3 静态代码水印	(336)
5.3.4 其他静态软件水印	(338)
5.4 动态软件水印	(340)
5.4.1 动态的含义	(340)
5.4.2 Easter Egg 动态水印	(341)
5.4.3 值类型动态数据结构水印	(341)
5.4.4 拓扑类型的动态数据结构水印	(343)
参考文献	(348)
第六章 数字产品产权保护	(350)
6.1 基于数字水印的版权保护协议	(350)
6.1.1 版权注册协议	(351)
6.1.2 水印加载协议	(352)
6.1.3 验证协议	(353)
6.1.4 仲裁协议	(354)
6.2 多媒体产权保护和认证体系	(355)
6.2.1 IMPRIMATUR 多媒体产权保护和认证体系结构	(356)
6.2.2 AQUARELLE 商业模型及其水印协议	(357)
6.2.3 IMPRIMATUR 体系及 DHWM 协议的缺陷	(360)
6.2.4 IMPRIMATUR 体系的改进	(360)
6.3 彩信业务版权管理系统	(362)
6.3.1 DRM 及业界标准	(362)
6.3.2 数字水印版权管理(WDRM)	(365)
6.3.3 OMA 方案	(373)
6.3.4 方案比较	(374)
6.4 DVD 防拷贝方案	(375)
6.4.1 MPEG-2 视频层次化数据结构	(376)
6.4.2 cbp 码	(376)
6.4.3 cbp 修改方案	(377)
6.4.4 cbp 恢复过程	(377)
参考文献	(378)

第一章 基础理论

数字内容的迅速普及使得数字内容的安全性成为备受关注的课题,比如:人们采用密码技术来保证数字内容不被非法阅读;采用数字签名技术来确保数字内容不被冒充和篡改;为了保护数字内容的产权,人们又发明了数字水印技术。

数字水印技术是一种将特制的、不可见的标记,利用数字内嵌的方法隐藏在数字图像、声音、视频等数字内容中,由此来确定版权拥有者、认证数字内容来源的真实性、识别购买者、提供关于数字内容的其他附加信息、确认所有权认证和跟踪侵权行为。如今,数字水印在数字内容的篡改鉴定、数据的分级访问、数据跟踪和检测、商业和视频广播、Internet 数字媒体的服务付费、电子商务认证鉴定等方面具有十分广泛的应用。本章对数字水印基础理论和嵌入技术等进行较为全面的原理性综述。

1.1 数字水印原理

目前,数字水印的研究从结构层次上可分为基础理论研究、应用基础研究、应用技术研究 3 个层次。其中,基础理论研究主要针对感知理论、信息隐藏及其数字水印模型、理论框架等;应用基础研究的主要方向是针对图像、声音、视频等载体,研究相应的数字水印隐藏算法和检测算法;应用技术研究以实用化为主要目的,研究各种多媒体格式的数字水印在实际中的应用。

1.1.1 水印模型

无论从嵌入方法还是从外观形式来看,目前数字水印都是千差万别的,因此,研究水印模型就显得更为重要。

1.1.1.1 数字水印的一般模型

数字水印目前尚未有好的理论模型。所有嵌入水印的方法都由一个水印嵌入系统和一个水印恢复系统组成。

水印信号嵌入模型如图 1.1 所示,其输入是水印信息、载体数据和一个可选的公钥或私钥。水印系统使用一个或多个密钥来确保安全,防止修改和擦除水

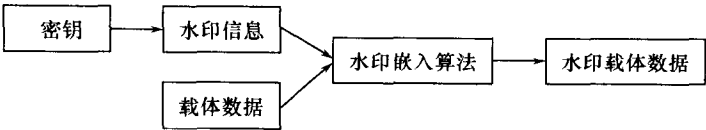


图 1.1 水印信号嵌入模型

印。水印可以是任何形式的数据,比如随机数字序列、图像或文本等。

图 1.2 为水印信号恢复模型,图 1.2 中的虚框部分表示在提取水印信号时,原始载体数据不是必要的。

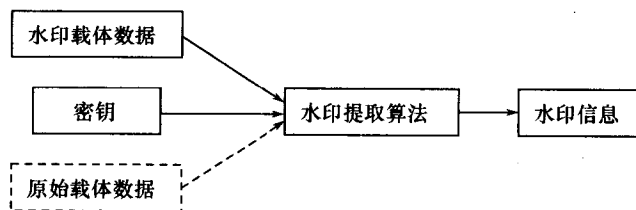


图 1.2 水印信号恢复模型

1.1.1.2 数字水印的通信模型

数字水印从本质上说是一种通信方式(从水印嵌入器向水印接收器传输信息,将水印系统看做信道),因此人们希望套用传统通信模型来研究水印过程。

下面给出基于通信的水印模型。首先引入一些记号。用 c_0 表示原始作品,嵌入水印的作品标记为 c_w ,受噪声/攻击影响的作品标记为 c_n ,嵌入了水印并且带噪声/攻击的作品则标记为 c_{wn} 。图 1.3 和图 1.4 显示了两个水印模型,它们都是由基本通信模型框架映射而来的。图 1.3 的系统采用非盲检测器,检测时需要原始作品,也就是含辅助信息检测器的水印系统;图 1.4 的系统采用盲检测器。在这个映射过程中,把水印系统看成是某种传输信道,水印信息在信道里传输,载体作品也是系统的一部分。

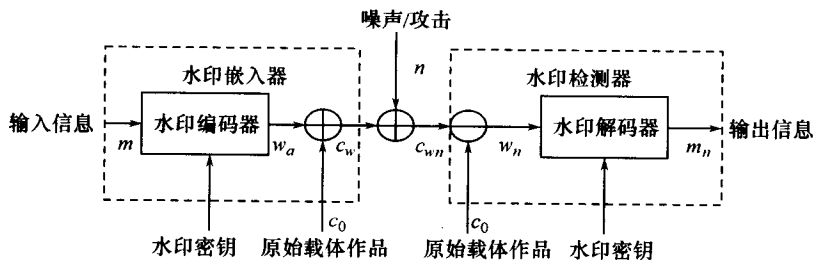


图 1.3 检测时需要原始作品信息的水印系统

不管采用的是含辅助信息的检测器还是盲检测器,嵌入过程都包括两个基本步骤。首先,将水印信息进行编码得到 w_a ,它和载体作品 c_0 的类型一致,维度相等。例如,当给图像添加水印时,水印编码器会产生一个二维的像素模板,它和载体图像的大小一样。当给语音添加水印时,水印编码器会产生一个音频信号。这类映射可以用水印密钥来实现。把 w_a 加到载体作品 c_0 上,便产生了包含水印的作品 c_w 。在上面的 2 个水印系统中,由于水印信息与载体作品的内容

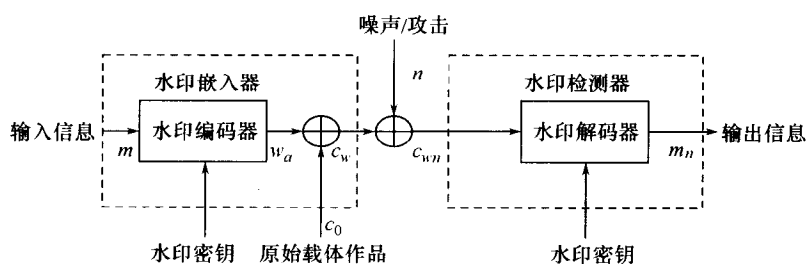


图 1.4 盲检测器的水印系统

无关,这样的嵌入器均属于盲嵌入器(与之相对的是含辅助信息的嵌入器,也就是水印信息与载体作品的内容有关,这样水印系统可以抵抗拷贝攻击)。在嵌入了水印信息后,假设水印作品 c_w 还经历了某些处理过程,包括在作品中加入了噪声以及攻击者试图进行的恶意破坏和删除水印的行为。将这些作用的结果同加性噪声等效仅仅是为了简化模型。

如果采用含辅助信息的水印检测器(如图 1.4 所示),检测过程也包含两个步骤。首先,从接受到的作品 c_{wn} 中减去未加水印的载体作品 w_n ,得到带噪声的水印模型。然后在水印解码器中使用水印密钥对其进行解码。

当水印用于认证时,其目的是检查水印在嵌入作品后,作品是否被修改以及如何被修改。因此上面的两个模型一般不适用于认证系统。下面给出的是水印信息与载体作品有关的水印系统的模型,如图 1.5 所示。

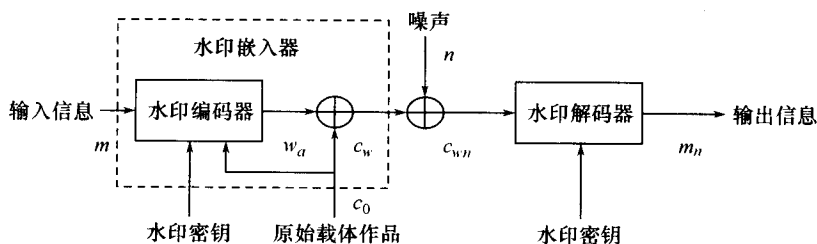


图 1.5 水印作为发送端带边信息的通信

在图 1.5 中, w_a 依赖于 c_0 , 除此之外, 它和图 1.4 所示的模型几乎相同, 唯一的区别是在这个模型中, 水印编码器接收 c_0 作为另一个输入。注意这一改变使得编码器可以赋予 c_w 任何值, 只需让 $w_a = c_w - c_0$ 。进一步考虑到载体作品是传输信道中噪声过程($c_0 + n$)的一部分, 因此这个新模型实际上是发送端携带有边信息的通信系统的一个实例。香农最初研究过这种通信系统。换句话说, 新模型中的嵌入器能够有效利用信道噪声尤其是载体作品 c_0 自身的一些信息。自从香农引进了带边信息的通信这个概念后, 很多人研究了这类通信系统。人们发现, 就一些信道类型而言, 发送端或(和)接受端是否能得到带边信息并不