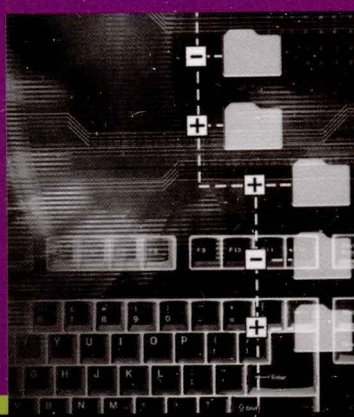
D



多媒体信息安全关键技术研究

胡玉平　韩德志

科学出版社

多媒体信息安全关键技术研究

胡玉平　韩德志　著

科学出版社

北京

前　言

“多媒体”一词最早出现在20世纪80年代美国麻省理工学院(MIT)递交给美国国防部的项目计划报告中，它指文本、图形、图像、声音、视频、动画等多种媒体的综合，通常可以理解成信息表示媒体的多样化。20世纪90年代以来，计算机网络和数字信息处理技术在全世纪范围内得到了迅猛的发展，使得摄影、广告、娱乐、监控、教育和医疗等行业每天都产生大量图像、视频、音频等多媒体数据，从而使数字多媒体产品得到了日益普及和广泛应用。数字产品易于编辑、复制、传输和存储，这一方面促进了人类信息的共享，推动了社会的进步；另一方面在政治、经济、军事等场合，敏感的多媒体信息通过公开信道传输或者存储于面向公众的数据库中，很容易受到信息窃取、数据篡改等攻击。对多媒体信息数据的安全保护目前已成为整个信息安全保护中一个迫在眉睫的现实问题。

目前，多媒体信息安全已成为学术界和企业界所共同关注的研究热点和关键问题。安全功能的复杂性以及攻击手段的层出不穷，迫切需要研究和开发出更多安全、高效、可靠的多媒体信息安全技术和产品。本书在阐述数字水印和密码技术的基础上，围绕多媒体信息安全的关键技术展开了讨论，包括：基于数字水印的版权保护算法研究；基于数字水印的多媒体认证算法研究；基于数字水印的多媒体版权保护协议及其在DRM中的应用研究；内网环境下的多媒体信息存储安全技术；内网一体化安全管理技术。本书大部分成果取自两位作者多年来的研究成果。

全书共分8章。第1章阐述了多媒体信息安全的目标及主要的安全技术，包括数据加密技术、多媒体加密技术、多媒体存储技术的研究现状和发展趋势。第2章阐述了数字水印和密码技术的基本理论，探讨了数字水印和密码技术的联系以及加密技术在数字水印中的应用。第3章结合小波变换、混沌映射、神经网络、奇异值分解的优良特性，研究并设计了4种新颖的图像鲁棒水印算法，这4种方法均为行之有效的图像版权保护方法；研究并设计了一种基于模板嵌入的旋转和缩放估计方法以及一种基于不变质心提取的平移估计方法以检测及校正水印图像所经历的几何变换；研究并设计了一个利用参数替换实现在H.264编码中嵌入盲水印的方法，为在H.264编码中实现水印嵌入提供了一个新的方法。第4章从实用、安全的角度，分析了用于图像认证的半易损水印算法应当满足的条件，在此基础上提出了一种基于奇异值分解的自嵌入图像认证水印算法和一种基于小波域水印的图像认证及恢复算法。第5章研究并设计了一种安全的适用于盗版追踪的买卖交易协议；研究并设计了一种能在数字作品交易过程中保护各方权益的基于数字水印的版权保护协议；探讨了数字水印技术在DRM中的应用方式和所面临的协议攻击问题，构造了一个基

于结合数字水印和 PKI 的安全 DRM 系统。第 6 章针对内网多媒体数据存储安全问题，设计了包括访问认证、I/O 分类、基于元数据的敏感数据保护，以及病毒检测、内容过滤、实时备份和信息的快速检索为一体的综合内网数据安全防护原型系统；并且，根据企业内网海量数据存储系统的特点和数据存储安全需求，我们首先设计多协议安全文件系统（MPSFS）支持不同协议用户的访问，为不同用户提供统一的访问接口，实现用户高效和快速的访问，同时 MPSFS 与身份认证、访问控制和相应安全算法结合充分保证内网数据存储系统的安全性。第 7 章针对我国企事业单位内网海量多媒体信息安全存储存在的问题，开发了内网一体化安全管理系统。该系统融合终端桌面、认证授权、加密和文件管理、监控审计、系统网管、IT 资产和运维管理、移动存储介质管理、决策支持管理、实时报警管理等模块的功能，使各安全模块的灵活配置形成了一个有机的系统，真正实现总体配置、整个网络调控、多层面、分布式的安全系统，实现对终端安全接入，各种网络安全资源集中监控、统一安全策略管理、智能审计，以及多种安全功能产品和模块之间的互动。同时，也能与内网安全存储系统和安全文件管理技术（第 6 章）很好地融合，充分保证企业内网文件数据的安全性。第 8 章在第 6 章和第 7 章介绍的内网一体化安全管理系统结构、组成和相关理论的基础上，从两个方面测试内网一体化安全管理系统：一方面从应用安全角度测试系统对整个内网系统的设备的监控情况；另一方面测试内网一体化安全管理系统对整个内网系统文件访问性能的影响，即读/写性能和 FTP 服务性能的影响，即从实验的角度验证了内网一体化安全管理系统的可靠性。

本书研究工作是国家自然科学基金项目“存储安全中介系统理论、仿真和实现技术研究”（61070154），广东省自然科学基金“超混沌系统建模及其在多媒体信息安全中的应用研究”（S 2011010001581），广东省科技计划“基于相似图像检索的服装网络推广平台的研究与实现”（2010B 01060036）和“基于语义 WEB 的海量网络数据存储系统”（2010B 090400160），广州市科技计划“快速相似图像搜索算法及其在电子商务中的应用研究”（11C42140691）和第十二届广州市难题招贤项目“融合 NAS 和 SAN 的海量网络存储系统”，中国博士后基金科学基金“基于数字水印的图像认证技术研究”（20060390882）和“云存储安全技术研究”（20110490091），以及上海市教育委员会科研创新重点项目（12ZZ153）和上海海事大学科研基金项目（20110014）的研究内容。本书得到广东商学院、科学出版社、上海海事大学、广州中长康达信息技术公司以及广东省电子商务市场应用技术重点实验室的大力支持，在此表示衷心感谢。

在本书的完成过程中，华中科技大学软件学院曹华博士给予了大量的支持和帮助。另外，书中参考了部分国内外同行专家和学者的论文，在此一并向相关作者表示感谢！

限于作者学识水平，书中不足之处在所难免，敬请同行和读者批评指正。

胡玉平　韩德志

2011 年 10 月

目　录

前言 …… i

第 1 章　多媒体信息安全概述 …… 1
1.1　多媒体信息安全的目标 …… 1
1.2　多媒体数据加密技术研究现状 …… 2
1.3　多媒体数字水印技术研究现状 …… 6
1.4　多媒体信息存储安全研究现状 …… 10

第 2 章　数字水印和密码技术 …… 15
2.1　数字水印的基本原理 …… 15
2.2　密码技术的基本原理 …… 24
2.3　数字水印与密码技术的联系 …… 31
2.4　本章小结 …… 34

第 3 章　基于数字水印的版权保护算法研究 …… 36
3.1　研究背景 …… 36
3.2　基于小波变换与混沌映射的自适应水印算法 …… 37
3.3　基于小波树量化与混沌映射的可读水印算法 …… 45
3.4　基于小波变换的空域水印算法 …… 50
3.5　基于神经网络的奇异值分解域公开水印算法研究 …… 55
3.6　水印抗几何攻击方法研究 …… 59
3.7　基于 H.264 编码的视频盲水印嵌入算法研究 …… 70
3.8　本章小结 …… 81

第 4 章　基于数字水印的多媒体认证算法研究 …… 83
4.1　研究背景 …… 83
4.2　用于多媒体图像认证的数字水印系统设计要求 …… 84
4.3　基于奇异值分解的自嵌入图像认证水印算法研究 …… 85
4.4　基于小波域水印的图像认证及恢复算法研究 …… 90
4.5　本章小结 …… 97

第 5 章 基于数字水印的版权保护协议及其在 DRM 中的应用 …… 98
5.1 研究背景 …… 98
5.2 安全有效的数字作品买卖交易协议研究 …… 101
5.3 参与各方权益公平的数字版权保护协议研究 …… 109
5.4 基于数字水印的 DRM 模型 …… 117
5.5 本章小结 …… 126

第 6 章 内网多媒体数据安全存储技术研究 …… 127
6.1 研究背景 …… 127
6.2 内网数据安全存储系统结构 …… 127
6.3 内网数据安全存储系统关键技术的实现 …… 131
6.4 基于共享的多协议安全文件系统的设计 …… 135
6.5 本章小结 …… 147

第 7 章 内网一体化安全管理技术的研究 …… 148
7.1 研究背景 …… 148
7.2 内网安全一体化管理系统结构和组成 …… 149
7.3 内网安全一体化管理系统主要分系统 …… 155
7.4 本章小结 …… 175

第 8 章 内网一体化安全管理系统性能评价 …… 177
8.1 内网设备的监测 …… 177
8.2 系统性能评估 …… 192
8.3 性能测试 …… 195
8.4 本章小结 …… 205

参考文献 …… 206

第1章　多媒体信息安全概述

1.1　多媒体信息安全的目标

近年来，随着 Internet 的发展，多媒体信息安全问题显得愈发重要和突出，它直接威胁到国防及许多重要的经济领域，引起了各级政府及学术界的高度重视[1-3]。多媒体信息安全的目标就是要保证多媒体信息的如下特点[4,5]：

(1) 保密性，除发送方和接收方外，多媒体信息不得被其他人知悉，或对于未授权的用户而言，信息不可用。

(2) 完整性，多媒体数据不被未授权者篡改或损害，多媒体信息系统按多媒体信息安全加密的若干算法研究既定的目标运行，未被非法操纵。

(3) 真实性，通信双方能够认证对方的身份不是假冒的。

(4) 不可否认性，通信双方不能否认自己的行为。

(5) 访问的可控制性，用户依据权限可以对多媒体进行相应操作。

(6) 可用性，多媒体信息服务的连续性、可靠性。

要解决多媒体信息的安全问题，必须综合考虑多个方面因素，并采取相应的安全措施，包括技术措施、管理措施、法律措施等，忽略了其中的任何一个环节，都可能引发安全漏洞。从技术角度来说，“密码＋协议＝信息安全”。而不同类型的多媒体信息系统，可能采取不同的协议和标准，不便建立统一的模型加以研究。因此，一般来需要对图像、视频、音频等多媒体信息进行加密和信息隐藏，以达到信息自身安全的目的。

从学科角度讲，网络环境下的多媒体信息安全是一门多学科交叉的研究课题，涉及数学、密码学、信息论、概率论、计算复杂度理论、计算机网络和信息存储以及其他计算机应用技术等知识领域。从实践角度而言，网络多媒体信息处理过程是一个信息产生源、计算机系统和有线或无线网络传输等各部分协同工作的过程。在协同工作的传输过程中，协同设计的各种文档信息、图像、视频、音频、动画等数字作品，客观上要求在其中嵌入身份标识，以便进行版权保护与身份认证——信息隐藏；或者是利用密钥序列改变原始信息的视听效果，使之成为无意义的信息，从而不被窃取、复制、传播——信息加密。由此可见，目前实现多媒体信息安全的技术主要有三种：信息加密(information encryption)、信息隐藏(information hiding)和信息存储安全，这三项技术既是当前多媒体信息安全领域普遍关注的重大问题，也是该领域研究的热点与难点[1-8]。

1.2 多媒体数据加密技术研究现状

密码技术是信息安全的核心，对于传统的基于密钥体系的加密技术，一直被认为是信息安全领域的支柱技术，并已通过各种算法、协议、标准构成较为完善的应用体系。随着计算机网络不断渗透到各个领域，密码学的应用也随之扩大，例如数字签名认证系统、身份鉴别系统等。

由于多媒体数据具有编码结构特殊、数据量大、实时性要求高等特点，传统的数据加密算法直接应用于多媒体数据时，通常具有较高的计算复杂度，很难满足实时性要求，而且会改变数据格式等，因此早期的多媒体保密方法主要依赖于权限控制针对这种情况，对多媒体数据进行加密的加密算法成为当前亟待研究的课题。

近年来，出现了许多用于多媒体数据的加密方法。根据加密算法与压缩编码过程关系的不同，分为将多媒体数据看成普通数据直接加密的方法、选择性加密方法、将加密过程和压缩编码过程相结合的方法、混沌加密技术 4 种[9]。

1. 直接加密方法

直接加密方法包括对原始多媒体数据直接加密和对压缩后的数据进行加密，这类算法将多媒体用 IDEA、RSA 等算法来加密[9]。如 Kuhn 提出的一种用于付费电视的直接置乱加密算法[10]，这是对原始数据直接加密的方法，不过这类算法更多的是对压缩后的数据进行直接加密；如 Qiao 和 Nahrstedt 提出的一种称为 VEA 的视频加密方法；Li 提出一种基于混沌的块密码的视频数据加密算法；Wee 和 Apostolopoulos 提出的一种适用于流格式视频数据的分层加密方法；易开祥等提出的以混沌流密码为基础构造了图像加密方法；吴敏和单华宁等提出的以混沌为基础构造了用于图像加密的块密码。这些方法利用了传统密码的高强度的优点，可满足高安全性要求，但它的计算复杂度高，加密速度慢，因此难以满足实时性要求，主要适合于多媒体数据存储等实时性要求不高或者安全性要求很高的应用中。

2. 选择性加密方法

选择性加密方法是只选择性地加密一部分数据，在分层的 MPEG 和 H. 263 编码中，码流分为基本层和增强层[11]，基本层对应视频序列的近似数据，增强层增加视频画面的细节效果，此时只加密基本层就可达到加密后的图像无法浏览的效果。选择性加密方法一般在变换域进行，实现图像空域与频域之间的转换可以利用离散余弦变换(DCT)、快速傅里叶变换(FFT)以及小波变换(DWT)等完成，其中 DCT 被认为是对语言和图像的准最佳变换。对图像频域数据只选择 DC 系数进行加密就有较好的加密效果，具有更高的加密效率。

针对多媒体数据通常具有数据量大的特点，目前研究最多的是选择性加密方法，因为视频数据通常比图像和音频具有更多的数据量。根据所加密的数据的不同，可以将视频加密算法分为选择加密不同帧和块、DCT 系数置乱、加密 DCT 系数的符号和运动向量的符号、频率域数据置乱和符号加密相结合、加密数据格式信息等。这类加密方法的优点是可以降低加密的数据量，提高加密效率，缺点是缺少通用的安全性分析方法，算法的安全性得不到保障。例如，仅仅置乱 DCT 块内系数不能保证对已知明文攻击的安全性；仅仅加密 DCT 系数或运动向量的符号，不能保证对穷举攻击的安全性。可见，这种加解密效率的提高是以降低安全性为代价的，因此对于选择性加密算法，关键要解决的是算法的安全性问题。不过，在某些多媒体加密应用中并不要求加密后的信息完全不可理解，例如，在图像传输中可能只要求对其中某个人、物或区域部分加密；在视频点播中可能只要求将原始画面变得模糊，而其中的轮廓可见，此时有选择性地加密是比较合适的。

3. 与编码过程相结合的加密方法

多媒体数据由于数据量大、冗余度高，因此在多媒体数据的存储和传输过程中，数据的高效压缩是必不可少的，对多媒体数据的加密需考虑与数据的压缩相结合。目前公认的关于图像数据压缩编码的国际标准是 JPEG 工作组和 MPEG 工作组推荐的几种图像编码标准算法。因此与编码过程相结合的加密方法主要考虑 JPEG 和 MPEG 两类编码。这类加密方法通常是将编码过程和加密过程相结合，使二者同时进行，其代表有：Sridharan 等提出的将加密过程与快速傅里叶变换过程相结合的语音加密方法；Uehara 提出的将编码和加密相结合，并以小波变换编码中系数置乱的方法；Wen 等提出的使用定长编码 FLC 和变长编码 VLC 进行加密的方法；Tosun 和 Feng 提出的使用前向纠错编码实现加密的方法；Wu 和 Kuo 提出的采用多种 Huffman 树(MHT)的加密方法。这类加密方法能够保持数据格式的相容性，具有较高的加解密效率，但由于采用了不同的统计模型，这类算法通常改变压缩性能，而且，其压缩性能与其安全性存在一定的关系。此外，这类算法对已知明文攻击的安全性相对较低，需要对算法进行改进。

4. 多媒体数据的混沌加密技术

由于广泛使用的图像、视频等多媒体信息的数据量大、冗余度高，在保密通信的实时要求下对传统密码学提出了严峻挑战。在此背景下，一种新型密码技术——混沌密码学[7]引起了国内外学者广泛关注和浓厚的研究兴趣。混沌(Chaos)是一种貌似无规则的运动，是指在确定性非线性系统中，不需附加任何随机因素也可以出现的类似随机的行为(内在随机性)。而高维(超)混沌系统(hyperchaotic system)则是一类维数更高、具有两个以上正 Lyaponuv 指数的更复杂的系统，高维(超)混沌系统相对一维混沌系统具有更高的安全性。混沌作为一

种特别的非线性现象，有许多值得利用的性质，如：混沌信息具有良好的伪随机特性、轨道的不可预测性、对系统初始状态及结构参数的极端敏感性等一系列优良特性。这些特性与密码学的许多要求是相吻合的。数字化混沌信息易于产生和再生，并且人们可以拥有众多的产生混沌信息的混沌系统，这使得数字化混沌密码在计算机多媒体信息的加密方面体现了强大的优势。

混沌科学的倡导者 M. F. Shlesinger 曾说："20 世纪科学将永远铭记的只有三件事，那就是相对论、量子力学和混沌"。混沌中蕴涵着有序，有序过程中也可能出现混沌。混沌研究的进展无疑是非线性科学最重要的成就之一，它正在消除确定论与概率论两个描述体系间的鸿沟，跨越学科界限是混沌研究的重要特点。普适性、标度律、自相似性、分形几何学、符号动力学、重正化群等概念和方法正在超越原来数理学科的狭窄背景，走进化学、生物、信息科学、地学，乃至社会科学的广阔天地。随着计算机技术的发展，混沌的研究被推向深入，这得益于高速计算技术的发展才使得从数值上研究混沌行为成为可能，从而推动了数值混沌研究的蓬勃发展。反过来，数值混沌技术的发展又为解决计算机信息安全问题提供了某些新的技术途径。将混沌系统理论技术应用于多媒体信息加密与内容检测方面，目前正处于发展的初期，展现了良好的应用前景，并越来越受到国内外学界和业界的重视。同时，将混沌理论引入信息安全领域也是当前国际非线性和信息科学两个学科交叉融合的热门前沿课题之一。我国的《国家中长期科学和技术发展纲要(2006～2020)》在支持的重点领域及其优先主题"核心数学及其在交叉领域的应用"的主要研究方向就包括"离散问题、随机问题、量子问题以及大量非线性问题中的数学理论和方法"[7]，混沌应用中的许多基础问题正涉及这样一类的数学理论和方法。因此.结合相关交叉领域开展混沌在多媒体信息加密与内容检测方面的应用基础理论和关键技术研究，也非常符合我国中长期科学和技术发展纲要的要求。特别在当前这种迫切需要信息安全的应用背景下，基于混沌的信息安全技术已成为一门方兴未艾的新技术，对该技术的基础理论和关键应用技术开展深入研究势在必行，这不仅具有深远的学科理论意义，而且具有重要的实际应用价值。

由于混沌在许多应用领域特别是在信息安全领域有极好的应用前景，导致近 20 年来人们对混沌现象的研究产生了很大的兴趣。特别是近 10 年来，许多新的混沌系统和超混沌系统模型被相继提出，如 Chen 系统[12] Lü 系统[13]、统一混沌系统[14]、Liu 系统[15]等典型，以及新近提出的一些典型超混沌系统模型[16-22]。这些超混沌模型可为信息安全领域提供所需的信息源。在超混沌系统建模过程中起关键作用的是混沌反控制技术，所谓混沌反控制(亦称动力系统混沌化)就是对非线性系统施加一类能够使系统产生或加强混沌运动的控制，它属于广义混沌控制的两大方向之一(另一方向是混沌正向控制，即抑制或消除混沌运动)。混沌现象对系统初始条件极为敏感，人们最初认为混沌是不可控的，直到 1990 年 OGY 方法的提出才彻底改变了人们的这种观点，由此激发起来的关于混沌控制的理论、方法

与实验应用研究得到蓬勃开展[23-26]。此外，由于人们早先普遍认为混沌是有害的，需要消除，所以先前的混沌控制目标主要是混沌正向控制。但近年来，人们发现混沌并不都是有害的，在许多场合反而是有益的而且是有巨大应用潜力的，比如在信息加密和信息隐藏领域就是混沌应用颇具潜力的领域之一[27]，混沌的这些应用潜力导致近年来关于系统混沌化的研究迅速崛起[28-32]。因此，有目的地产生或强化混沌现象（即实现混沌化）已经成为当今非线性科学领域一个关键性的研究课题。继 Lorenz 系统和 Rössler 系统等经典混沌系统被发现之后，又有许多新系统被相继建立起来；并且其中一些系统模型已经被应用于信息安全方案的设计。然而，由于许多现有系统模型的性质已广为人知，从而导致使用这些系统构建信息安全方案将降低方案的安全性。因此，不断创建新的混沌系统模型具有实际意义。混沌反控制在理论上非常有吸引力，在技术上却非常有挑战性，因为它涉及非常复杂的混沌现象以及各种相关的高维非自治系统的控制和稳定性[32]，且其研究起步晚。目前，虽然关于离散系统混沌反控制的研究工作已经取得了很大的成功，但对于连续系统，情况则变得非常复杂，尚缺乏有效的理论方法来指导动力系统混沌化的控制系统设计。

直接利用数字化混沌信号进行信息加密是混沌应用的一个方兴未艾的领域。正因为混沌和密码学之间存在着许多天然关联性，自 20 世纪 90 年代以来密码学界开始对混沌理论投入关注，其标志是英国数学家 R. Mhatews 首先提出的混沌加密思想[33]。随之而来，混沌序列加密方法被列为现代密码学的重要研究前沿，并迅速成为现代密码学的一个研究热点。由于混沌加密的效率优势使得其特别适合数字图像等大信息量媒体的加密，而传统的密码学面对图像信息庞大的数据量，往往显得力不从心，失去实用性。因此，近年来人们提出了很多的基于混沌图像加密算法，早期的图像加密大多采用单个的一维混沌系统如著名的 Logistic 系统，但已被证明这种密码系统安全性不高。原因之一是密钥空间不够，不能抵御穷举攻击；二是容易利用相空间重构方法进行混沌系统识别，攻击者只要截获足够长的明文/密文对，就能够破解种子密钥，从而不能抵御已知明文攻击。后来有一些研究者建议使用多个低维混沌系统来加强安全性，但是这种体制大部分是基于数据流的，本质上它和加密文本没有什么区别，没有充分考虑到图像数据自身在存储上的特点。我们认为，实用性强的图像加密方法必须要针对图像特点进行专门设计。在众多的图像加密算法中，J. Fridrich 在文献[34]中提出的一类加密方案比较具有代表性，该方案包括了现代密码体制所倡导的置换、替代、扩散及混乱等基本要素，特别适合于图像加密，其思想很值得借鉴发展。文献[35]借鉴文献[34]的思想提出了用 Cat 映射结合三维 Lorenz 混沌系统的图像加密算法，使密钥空间增大，密文扩散分布性能更好。最近，文献[36]提出了基于一维的标准混沌映射和 Logistic 映射的图像扩散及混乱型加密算法；文献[37]对文献[36]提出的方案进行了改进，使算法增强了抵抗选择明文攻击和已知明文攻击的鲁棒性。文献[38]

提出运用简单的表查询和交换技术代替一维混沌映射迭代的快速图像加密算法，提高了扩散速度。文献[39－40]提出了基于空间或时空混沌的图像加密算法，提高了加密的安全性。总结发现，现有图像加密算法多数使用离散混沌映射，而离散混沌映射一般是低维混沌系统，安全性不是很高。超混沌系统比低维混沌系统复杂性更高，故可给密码系统带来更高的安全性，但高维(超)混沌系统却多为连续混沌系统，其生成密钥流序列的时间开销比低维混沌系统大。因此，如何克服高维系统的这个缺点而发扬其优势，针对图像特点设计专门的加密方案，值得深入研究。

1.3 多媒体数字水印技术研究现状

数字水印是一个隐藏在数字化图像、视频和音频等多媒体中的信息，水印和内容本身集成在一起，在不需要额外的存储空间或新的存储格式的情况下，可以为原始数字媒体提供必要的证明信息和版权保护[41]。其本质在于多媒体数据中存在大量的感知冗余部分，将水印嵌入其中就可以达到隐藏的目的。在现实生活中，有以下两个引起普通关注的问题构成数字水印的主要研究背景[42-43]。

1. 数字产品的版权保护

数字作品(如电脑美术、扫描图像、数字音乐、视频、三维动画)的版权保护是当前的热点问题。由于数字产品的拷贝、修改非常容易，而且可以做到与原作品完全相同，所以原创者不得不采用一些严重损害作品质量的办法来加上文本版权标记，文本的版权标记用于作品所有者鉴别时，存在一些限制。例如，如果我们复印一本书中的几页(在合理使用的限制内)时，可能会忽略复印扉页的版权标记。一位画家使用从杂志广告上合法获得的图片时，可能会剪掉包含版权标记的那部分。这样，随后一个希望使用该作品的守法公民就不可能判断它是否受版权保护，即使判断出该作品受保护，也很难查明创作者的身份或应获得谁的许可。

数字水印可以不被感知而且和包含它们的内容密不可分，所以它们可能比文本版权标记更适合于所有者鉴别。如果作品的使用者拥有水印检测器，即使是在使用了可消除文本版权标志的方法修改了作品后，他们仍能确定包含水印作品的拥有者。Digmarc 的图像水印恰好是为这种用途设计的，他们把水印检测器和 Adobe 公司研制的流行图像处理程序 Photoshop 捆绑在一起，实现了水印检测器的广泛应用。当 Digimarc 的检测器识别水印时，它通过国际互联网与中心数据库联系，并把水印信息作为密钥，从而找出图像所有者的联系信息。

2. 数字作品的篡改问题

通过使用一些技术手段，使得篡改数字作品变得越来越容易。例如图 1－1 显示了使用 Adobe Photoshop 软件对图像进行修改的例子：左边是原始图像，右边

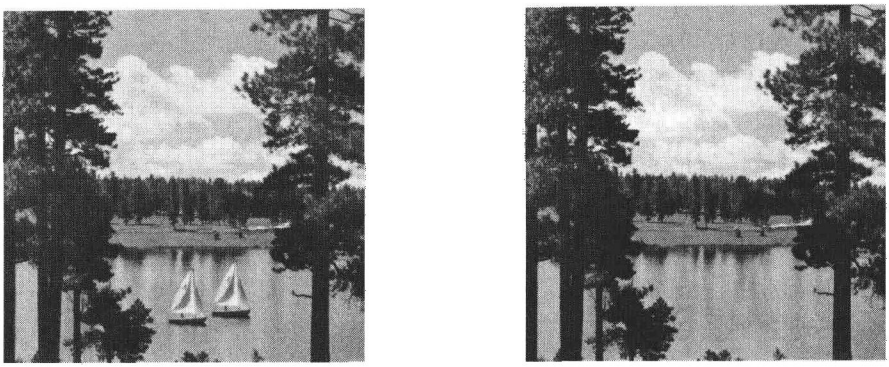


图 1-1　修改图像的简易性：把左边图像中两只小船从场景中去掉，得到右边这幅图像，用 Photoshop 处理大约需要 10 分钟

是修改后的图像。如果这幅图像是法律案件或警察调查中的一条关键证据，篡改会引起很严重的问题。

传统的加密技术也研究了认证信息的问题[44]。解决此问题的一种普通加密途径是这样实施的：首先原始图像发送方利用单向 Hash 函数产生图像的摘要信息，再用其私钥加密，并将加密后摘要（签名）与图像一起传送给接收方，接收方收到图像后，用同样的 Hash 单向函数重新生成图像的摘要信息，并与用发送方公钥解密的摘要进行比较，如果两者相等则图像真实，否则图像被篡改。这种认证方式必须与数字作品一起传送签名，因为在一般的使用中，容易失去签名。例如，考虑一个图像认证系统，它在 JPEG 文件头部存储元数据，如果图像转换为另一文件格式，在文件头就不会有安置签名的空间，这样签名就会丢失。当签名丢失后，作品不能再被认证了。用水印进行内容认证有两个潜在的好处。首先，相关的元数据（如密码签名等）不需要和介质分开存储，这对处理遗留问题的系统是非常重要的，如处理旧的文件时，旧文件格式可能没有多余的空间存储元数据。水印的第二个潜在的优点是：作品被改变时，水印可以和其嵌入的作品获得同样的改变，所以当作品被破坏时，水印也随之改变，这时通过嵌入的水印样本和提取的水印相比较，不仅可以知道作品被修改了，甚至还可以知道在什么时候、什么地方，进行了什么样的修改，而附在文件后的签名却没有这种特性。

从以上两个问题的分析可以看出，数字水印技术与其他的数字产品保护技术相比主要有三个方面的特性：首先，水印是不可感知的，与条形码不同，水印不会减损一幅图像的美观性；第二，水印与嵌入的作品密不可分，和文件头区数据不同，当作品被显示或转化为其他文件格式时水印不会被消除；第三，水印将经历和作品完全相同的变换，这意味着通过查看得到的水印可以获悉作品所经历的变换的一些情况。正因为数字水印的这三个方面的特性，使数字水印在版权保护、复制控制、数据认证、盗版跟踪、数据监控、内容标记等方面能克服其他可选解决方法的局

限性，有着广阔的应用前景。

一般认为，数字水印起源于古老的水印技术，如纸制钱币上的水印、邮票股票上的水印等。数字水印的产生最早可追溯到 1954 年，Muzak 公司的埃米利·希姆布鲁克(Emil Hembrooke)为带有水印的音乐作品申请了一项专利。在这项专利中，通过间歇性地应用中心频率为 1 kHz 的窄带陷波器，认证码就被插入到音乐中。该频率上能量的缺失表征使用了陷波滤波器，而缺失的持续时间通常被编码为点或长划，此认证码使用了莫尔斯电码，此系统被 Muzak 公司在 1964 年前后申请了美国专利。从那时起，人们开始发展大量的水印技术并由此展开了各种各样的应用，但这时的数字水印只是作为一种版权认证的工具，并没有成为一门科学。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，1994，Schyndel 和 Tirkel 等在 IEEE 国际图像处理大会上发表了题为 *a digital watermark* 的论文，这标志着数字水印概念的诞生。

早期的数字水印技术主要针对的是数字图像，在灰度图像的最低有效位 LSB 添加水印，该方法的缺点是鲁棒性很差，对嵌入水印的图像进行按比例缩放、中值滤波等普通操作后，水印就无法正确提取。为了提高水印的鲁棒性，1995 年 Cox 等人提出了一种基于扩频通信的思想，将水印嵌入图像感知上最重要的频域因子中的水印方案[45]，实验结果表明，该方案对各种普通图像处理操作有很好的鲁棒性，Cox 方案已经成为水印技术中一个比较经典的方案，其主要缺陷是水印的提取过程必须有原始图像的参与，即它不是盲水印方案。1996 年 Pitas 提出了一种盲水印方案[46]，通过将图像像素划分成两个子集合，调整其关系嵌入水印，该算法是盲水印算法的一个代表，但很明显该算法是一种空间域算法，其鲁棒性还有待提高。其后一些人员在其基础上进行了改进研究，其中有代表性的是 Voyatzis 等将混沌的方法引入到水印算法中[47]，使得算法的鲁棒性得到了提高；Kundur 等提出了基于离散小波变换的水印算法[48]，通过修改 DWT 系数嵌入水印，并且提出了使用脆弱水印对图像所经受的处理进行估计，进而更有效地对水印进行检测。

对音频水印技术的研究最早见于 1996 年，Bender 等人在文献[49]中提出了 LSB 编码、回声编码、扩频编码和相位编码等 4 种算法；Boney 等[50]将 Cox 方案应用到音频信号中，取得了很好的实验结果，其后，又有研究者对上述算法进行了改进和完善。

对文本文档中嵌入数字水印技术的研究始于贝尔实验室的 Brassil，他于 1995 年首先提出在数字文档中嵌入标记的方法[51]，以保护电子出版物所有者的版权利益。他提出了行位移编码、字位移和特征编码等三种方法。其后，Bender 等于 1996 年提出了一种同字位移编码稍有不同的算法，利用左对齐调整文档时附加空格的方法嵌入水印，另外还提出了一种采用同义词替换的算法。

视频序列是由一系列连续的等时间间隔的静态图像构成，因此可以将某些图

像水印技术的思想直接应用于视频序列，但实际上图像与视频间也存在一些重要的差别，如一个视频水印算法必须考虑某些可能的帧速率转换或丢帧现象，最重要的是：视频水印嵌入时计算复杂度问题会成为首要问题。视频水印算法根据嵌入水印的数据域分为两种：非压缩域和压缩域算法。其中对于非压缩域的水印，Matsui 等于 1994 年提出的一种 DCT 域视频数据嵌入算法[52]，该算法类似于图像水印算法，只是通过 DCT 系数对每一帧视频图像的像素值进行变化，因此对噪声、剪切等处理非常脆弱，而且若攻击者掌握了同一帧视频对象的多个不同水印版本，则可以通过比较得出原始的、未加水印的图像帧；Swanson 等对上述算法进行了改进，利用分块 DCT 变换和频率掩蔽特性相结合嵌入水印[53]，提高了水印的鲁棒性。此外 Swanson 等还提出了一种基于内容的水印技术，并提出了多分辨率的视频水印算法；Langelarr 等首先提出了两种压缩域上的嵌入算法，一种是替换帧内编码块 DCT 系数的变长码的方法，另一种是基于丢弃部分压缩视频流的方法[54]。前一种方法计算量较小，水印嵌入比特率大，但是鲁棒性很差，后一种方法计算较为复杂，水印嵌入比特率低，但水印鲁棒性较强，可以抵抗解码后重新编码的攻击。Hartung 等研究了 MPEG－2 压缩视频域上的水印算法，在保持码率基本不变的情况下，将水印嵌入到 DCT 系数中，并实现了水印的盲检测[55]。他们研究了该算法的鲁棒性，指出其算法对压缩、滤波、轻度旋转具有鲁棒性，对更大程度的旋转，需要采用适当的检测和校正机制，由于去除或插入数据会导致收发双方丢失同步信息，因此还需要同步信息丢失检测及再次同步的机制。

随着数字水印技术研究的不断深入，该技术的应用对象已不仅局限于上述的图像、音频、视频和文本，以图形、三维动画等为嵌入对象的水印技术也已经有了报道。

虽然数字水印技术从正式提出到现在只有短短 10 多年，但人们对数字水印的研究兴趣在不断增长，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。1996 年 5 月 30 日至 6 月 1 日，在英国剑桥牛顿研究所召开了第一届国际信息隐藏学术会议，此次会议把数字水印作为它的一个主要议题，同时，标志着一门新兴的交叉学科——信息隐藏学的诞生。此后，信息隐藏及其数字水印引起了学术界的广泛兴趣，1998、1999、2001、2002 年及 2004～2010 年又分别召开了 11 届国际信息隐藏研讨会议。国际工程学会(SPIE)也从 1999 年起，每年召开一次多媒体信息安全与数字水印大会。此外一些信息安全、密码学、信息处理领域的国际会议上也都有关于信息隐藏及数字水印技术的专题。这些会议的举行，大大加强了研究人员们彼此间的交流，促进了数字水印技术的不断发展。此外，欧美的一些著名大学、知名企业和研究机构，如美国的麻省理工学院、Purdeu 大学、英国的剑桥大学、德国的 Erlangen-Nuremberg 大学、NEC 研究所、IBM 研究所等都投入相当的人力和物力，致力于该项技术的研究，并取得了一些成果，其中美国的 Digimarc 公司于 1995 年就推出了有专利权的水印制作技术，是当时世界 ·

上唯一拥有这一技术的公司，并在 Photoshop 和 CoreDraw 中得到应用，但用其做出来的水印尚不够稳健。1997 年 1 月 7 日该公司又推出了独立的水印软件 Read Marc，利用它可以发现图像是否含有水印及其内容，但效果仍不太理想。此外，英国、日本等也相继在 20 世纪 90 年代初期开始了对这项技术的研究，虽然也没有很完美的产品问世，但对数字水印技术的发展还是起到了巨大的推动作用。

我国数字水印的研究起步于 1998 年，在何德全、周仲义、蔡吉人三位院士的倡导下，由北京电子技术应用研究所、"863 计划"智能计算机系统专家组及其他科研院校主持，分别于 1999、2000、2001、2002、2004、2006、2007、2009、2010 年召开了 9 届国内信息隐藏暨多媒体信息安全学术研讨会，第十届全国信息隐藏暨多媒体信息安全学术大会(CIHW)将于 2012 年 3 月在北京召开。9 届研讨会的召开，为致力于信息隐藏及数字水印研究的专家、学者提供了广泛的交流机会，对推动我国信息隐藏及数字水印技术的研究与应用起到了积极的促进作用。目前国内有许多高等学校和科研院所如清华大学、北京大学、北京邮电大学、中科院自动化所、浙江大学、中山大学、哈尔滨工业大学、北方工业大学等都对数字水印技术进行了深入的研究，在理论上取得了许多可喜的成就。同时，同内有少量公司开始致力于数字水印软件的开发，如：上海阿须数码有限公司、成都宇飞信息工程有限公司。虽然这些公司开发的水印软件还不够完美，但他们的研发工作将促进我国的数字水印研究工作从理论走向应用。

1.4 多媒体信息存储安全研究现状

随着互联网和网络应用的迅速普及，多媒体信息越来越多，海量的多媒体信息多存在企业内网存储系统中，而内网存储系统会面临各种各样的网络攻击和威胁。近年来，针对层出不穷的各种安全威胁，目前国内的政府单位和企业在重点部署了边界安全防范和管理，强化了对来自网络内外部威胁的完善的防护，大部分单位和企业都采取了防病毒、防火墙、VPN、网站防篡改等手段，部分单位还部署了入侵检测、漏洞扫描、安全审计、内容监控、UTM 等设备和系统，来自网络外部的安全威胁大大减小，取得了相当用户的认可和好评[56-76]。

尽管企业界每年花费大量资金防毒防黑，但企业防御失效的另一个容易被忽略的问题是：来自员工、厂商或其他合法使用系统者的内部滥用[76-86]。内网存储安全问题仍然严峻。主要表现在：

(1) 网络内部终端可信与安全与否。漏洞检测和补丁管理缺失，病毒、蠕虫、恶意代码攻击破坏。

(2) 内网机密数据泄露。移动电脑、移动介质和内网设备外联管理混乱，内部重要敏感数据缺乏保护、管理和监控技术手段，或非授权使用。

(3) 违规终端个人行为。各种非工作、非授权的客户端应用软件使用，非正常

网络流量，或其他异常行为。

(4) 系统软硬件资产管理混乱。

目前，多媒体信息多存储在内网存储系统中，针对内网安全存在的问题，迫切需要研究和设计一体化内网安全管理系统：① 对内网的软硬件资产和各终端设备进行统一有效管理；② 即时发现各种非正常网络流量和其他异常用户行为并进行有效控制；③ 能充分保证内网信息存储系统中各种数据信息的安全性[77-79]。

1.4.1　内网多媒体信息存储安全技术发展现状

随着国内信息化程度的快速提高，内网信息安全越来越多受到关注，内网安全产品和厂商短短几年内大量涌现。较为著名的有启明星辰的天珣内网安全风险管理与审计、绿盟的内网安全管理系统、北信源的内网安全及补丁分发管理(VRVEDP)、华软的金盾 CIS5 软件、圣博润公司的 LanSecS 内网安全系统、锐安信息的 NiordSec 内网安平台、明朝万达的 Chinasec(安元)可信网络安全平台等。内网安全提供了传统防火墙、IDS、防病毒系统、专业网管软件所不能提供的防护功能，主体功能包括为：认证、授权管理、访问控制、桌面管理、文档/文件和磁盘加密、移动存储介质管理、防病毒、监控审计等，内网管理的基础是密码技术和认证，功能核心是监控审计、桌面管理、数据安全和访问控制[57-76]。

监控审计类产品是最早出现的内网安全产品，50%以上内网安全厂商推出的是监控审计类产品。监控审计产品主要对计算机终端的网络访问、应用软件使用、系统配置、文件操作以及外设使用等提供集中监控和审计功能，并生成各种类型的报表。监控审计产品一般基于协议分析、注册表监控和文件监控等技术，具有实现简单和开发周期短的特点，能够在内网发生安全事件后，提供有效的证据，实现事后审计的目标，提高内网的可管理性。但监控审计类产品的缺点是不能有效地阻止安全事件的发生，不能从根本上实现提高内网的可信和可控性。

桌面管理类产品针对计算机终端实现一定的管理控制策略，包括外设管理、应用程序管理、网络连接管理、资产管理以及补丁管理等功能，主要是通过限制用户权限、关闭部分服务功能等安全配置管理可有效减少系统漏洞，提高终端防护能力。桌面管理产品通常有监控审计产品类似的终端用户审计功能，桌面监控审计除了使用监控审计类产品的技术外，还可能针对 Windows 系统使用钩子等技术，对资源进行控制，实现对计算机终端资源的有效管理和授权。2008 年，美国联邦政府开始推行和实施联邦桌面核心配置计划(FDCC)，并成为美国国家网络安全综合计划(CNCI)的重要组成部分，实现联邦政府桌面计算机的安全管理实现标准化、自动化，提高信息安全策略的整体部署和防范措施的实施效率。美国联邦政府已强制规定所有使用 Windows 的计算机必须符合 FDCC 的配置要求。

多媒体文档加密类产品也是相对较多的内网安全产品类型，其主要解决特定格式主流多媒体文档的权限管理和防泄密问题。多媒体文档加密技术一般基于文