信号与信息处理
技术丛书

数字版权保护技术及其应用

冯柳平 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信号与信息处理技术丛书

数字版权保护技术及其应用

冯柳平　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书重点讲述数字版权保护技术及其应用。全书共分 9 章，包括数字版权管理技术、加密技术与数字签名技术、数字水印技术、数字指纹技术、DRM 标准、权利描述语言、DRM 应用、印刷品防伪技术和抗几何攻击的数字水印算法。

本书内容丰富、层次清晰，可作为高等院校本科、研究生各相关专业的教材，也适合学习数字版权保护技术的人员参考使用。

图书在版编目（CIP）数据

数字版权保护技术及其应用 / 冯柳平编著. —北京：电子工业出版社，2013.8
（信号与信息处理技术丛书）
ISBN 978-7-121-19803-8

Ⅰ. ①数… Ⅱ. ①冯… Ⅲ. ①电子出版物—版权—保护—研究 Ⅳ. ①D913.04

中国版本图书馆 CIP 数据核字（2013）第 046810 号

责任编辑：董亚峰　　特约编辑：王　纲
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：22　字数：565 千字
印　　次：2013 年 8 月第 1 次印刷
定　　价：48.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言

随着互联网和数字化技术的快速发展，网上交易和传播的电子书、音乐、电影、图片、游戏和软件等数字内容越来越多，数字出版物的读者群已经初步形成，数字出版成为出版业未来的发展趋势。但是，由于信息的复制更加快捷简便，盗版现象日益严重，给相关权利人造成巨大的经济损失，挫伤他们使用互联网扩展业务的积极性，并直接威胁数字出版业的健康、可持续发展。

面对有巨大潜力的数字出版市场，如何保护数字作品的版权已成为近年来法律界和 IT 业界的热点问题，同时也是难点问题。传统的版权保护模式已不能满足数字内容版权保护的需要，人们对数字版权保护提出了新的要求，数字版权管理（Digital Rights Management，DRM）技术在这种背景下应运而生。目前常用的数字版权保护技术还有加密技术和数字签名技术、数字水印技术和数字指纹技术等。

DRM 技术是数字网络环境下数字内容交易和传播的重要技术。本书介绍了数字出版领域版权保护的关键技术、相关的标准和应用以及最新进展，使读者在掌握数字版权保护技术基本内容的基础上，对该领域未来的发展趋势及关键技术有所了解。

本书共分为 9 章，第 1 章数字版权管理技术，主要介绍 DRM 系统模型及关键技术，第 2~4 章介绍 DRM 系统的底层技术，包括加密技术与数字签名技术、数字水印技术和数字指纹技术。其中，第 2 章除了介绍常规的加密技术与数字签名技术，还对 DRM 加密技术进行了概述；第 3 章介绍了数字水印的基本概念、分类及性能指标，并对空域和频域主要的数字水印算法和鲁棒性测试软件——Stirmark 基准测试程序进行了描述；第 4 章介绍数字指纹的系统模型、数字指纹编码和数字指纹协议。第 5 章主要介绍 OMA DRM 标准，并对 AVS DRM 标准进行了概述。第 6 章主要介绍当前发展最为完善的两个基于 XML 的权利描述语言——XrML 语言和 ODRL 语言，并对基于逻辑的权利描述语言——LicenseScript 语言的基本内容进行了介绍。目前 DRM 技术的应用领域主要是电子书、流媒体、电子文档等，第 7 章介绍了在这几个领域主要的 DRM 应用。第 8 章印刷品防伪技术，这是数字水印在印刷领域的应用，分析了在打印扫描过程中图像所受到的攻击，包括像素点失真和几何变形，并介绍抗打印扫描的数字水印算法。第 9 章介绍抗几何攻击的数字水印算法，分析了几何攻击对数字水印系统的影响，重点介绍了第二代数字水印——基于图像特征的水印算法，主要包括基于 Harris 特征点和 SIFT 特征点的方法。

本书可作为高等学校信号与信息处理相关专业高年级学生及硕士研究生信息安全技术课程的教材，也可用做信号与信息处理相关专业或相关领域研究人员的参考书。本书约需

40~60 学时讲授。

在本书的编写过程中，参考了国内外有关的数字版权保护技术的众多文献，特别是国内外的研究生学位论文，对某些内容进行了较好的综述与算法描述，参考过的论文在每章的参考文献中已列出，在此对所有参阅与引用了的文献与论文作者表示衷心感谢。

本书得到了高端印刷装备信号与信息处理北京市重点实验室师生的大力支持，尤其是曹鹏教授在本书编写过程中提出了有益的建议，在此表示衷心感谢。研究生徐佳和闻爱华在书稿编排、画图、校对过程中做了大量工作，在此一并致谢。

本书得到了国家自然科学基金项目（No. 61170259）和北京印刷学院重点研究项目（No.E-a-2013-20）的资助，在此特表感谢。

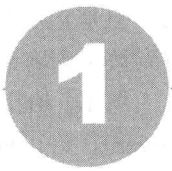
由于编者水平有限，加上数字版权保护技术本身在不断丰富和发展，尽管数易其稿，但书中难免存在不妥乃至错误之处，敬请读者不吝指正。

编　者

2013 年 6 月

目 录

第 1 章



数字版权管理技术

数字版权保护是近年来法律界和 IT 业界一个亟待解决的问题，第一代数字版权保护技术主要致力于对数字内容的安全性与加密技术的开发，在提供数字化和网络化信息服务的同时，有效地阻止对这些信息的非法使用和复制，以达到保护数字知识产权的目的。但随着数字出版的发展和广泛使用，采用传统的加密技术已不能满足数字版权保护的需要。为了更好地保护数字内容的版权，人们提出了一种新的技术——数字版权管理（Digital Rights Management，DRM）技术，即第二代数字版权保护技术，确保数字内容的合法使用和传播。

DRM 技术是在网络及数字化环境下，借助加密与封装技术、PKI 认证、权限管理技术等，使数字内容和权利主体获得对其客体的控制权，从而防止非授权使用，保护权利所有人利益的一种综合性技术体制。DRM 技术对数字内容版权的保护，贯穿数字内容从产生到分发、从销售到使用的整个内容流通过程。文献[1]对 DRM 技术进行了全面的综述。

在网络出版领域，DRM 技术的地位越来越重要。2001 年，DRM 技术被 MIT 的《Technology Review》杂志评为“将影响世界”十大新兴技术之一；随后在旧金山举行的 Seybold 上，DRM 成了一个技术热点，并且人们普遍认为，20 世纪 90 年代中期开始，属于 DRM 的实验阶段，发展到今天，DRM 已经成为一项很重要的技术，特别是数字媒体领域，DRM 成为了必需的技术。

美国计算机协会从 2001 年开始，每年举办一次“ACM Workshop on Digital Rights Management”会议，涉及的内容包括多个方面，主要有 DRM 系统的体系结构、DRM 中对数字内容使用的跟踪和审核、数字内容交易的商业模式及其安全性需求、多媒体数据的加密、身份识别、DRM 系统中的密钥管理、数字内容使用权利的转移问题、数字版权描述等。

越来越多的数字内容通过 DRM 技术保护，实现了数字内容的增值服务。例如，电子书通过 DRM 系统进行网上销售，或者把电子书卖给有 DRM 保护的数字图书馆，使出版社在出版纸书的同时，通过电子书的销售获得更多的收益。在电子书、电子报纸、电子杂志等数字内容的销售方面，DRM 技术发挥了重要的作用。随着移动数据增值业务的迅猛发展，内容提供商通过大量下载类业务及 MMS 等信息类业务传播的音视频和应用软件、游戏等数字内容越来越多，将 DRM 技术引入移动增值业务，可以确保数字内容在移动网内传播，保证内容提供商的利益。移动 DRM 已成为目前全球范围内移动业务研究的热点之一。

1.1 DRM 系统模型

不同的 DRM 系统虽然在所侧重的保护对象、支持的商业模式和采用的技术方面不尽相同，但是它们的核心思想是相同的，都是通过使用数字许可证来保护数字内容的版权。用户得到数字内容后，必须获得相应的数字许可证才可以使用该内容。

图 1-1 给出了典型的 DRM 系统参考体系结构，包括三个主要模块：内容服务器（Content Server）、许可证服务器（License Server）和客户端（Client）[1][2]。

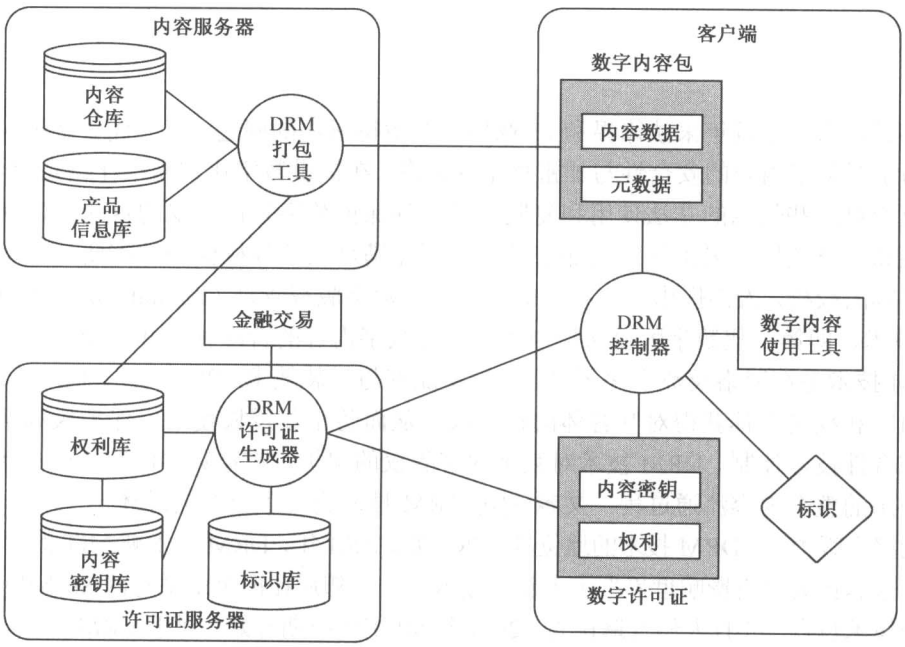


图 1-1 DRM系统参考体系结构

内容服务器通常包括存储数字内容的内容仓库、存储产品信息的产品信息库和对数字内容进行安全处理的 DRM 打包工具。该模块主要实现对数字内容的加密、插入数字水印等处理，并将处理结果和内容标识元数据等信息一起打包成可以分发销售的数字内容。另外一个重要功能就是创建数字内容的使用权利，把数字内容密钥和使用权利信息发送给许可证服务器。

许可证服务器包含权利库、内容密钥库、用户身份标识库和 DRM 许可证生成器，经常由一个可信的第三方——清算中心负责。该模块主要用来生成并分发数字许可证，还可以实现用户身份认证、触发支付等金融交易事务。数字许可证是一个包含数字内容使用权利（包括使用权限、使用次数、使用期限和使用条件等）、许可证颁发者及其拥有者信息的计算机文件，用来描述数字内容授权信息，由权利描述语言描述。大多数 DRM 系统中，数字内容本身经过加密处理。因此，数字许可证通常还包含数字内容解密密钥等信息。

客户端主要包含 DRM 控制器和数字内容使用工具。DRM 控制器负责收集用户身份标识

等信息，控制数字内容的使用。如果没有许可证，DRM 控制器还负责向许可证服务器申请许可证。数字内容使用工具主要用来辅助用户使用数字内容。

当前大部分 DRM 系统都是基于该参考体系结构的，如 Microsoft WMRM、Inter Trust Rights System、Adobe Content Server、RealNetworks RMCS 和 IBM EMMS 等。通常情况下，DRM 系统还包括分发服务器和零售门户网站，特别是支持数字内容网上交易的 DRM 系统。分发服务器存放打包后的数字内容，负责数字内容的分发。零售门户网站直接面向用户，通常作为用户和分发服务器、版权服务器以及（金融）清算中心的桥梁，用户本身只与门户网站交互。

DRM 技术不是密码技术的简单应用，也不是将受保护的内容从服务器传递到客户端并用某种方式限制其使用的简单机制。内容提供者希望通过使用 DRM，保护数字作品的版权，促进数字化市场的发展。因此，用户对 DRM 系统的接受度也是必须考虑的。一个完善的 DRM 系统必须兼顾提供者和使用者双方的需求，具备以下功能[1][2]。

① 提供管理、保护和跟踪数字内容的功能，只有合法的用户才可以使用数字内容。支持对各种形式使用权利的描述、识别、交易、保护、监控和跟踪。

② 提供透明易用的体验环境，保护用户的合法权益和隐私。使用者可以自由选择、购买数字内容，可以在多种设备上使用数字内容。在合法的范围内，可以不受时间、地点、网络状况的限制使用数字内容，可以转卖、赠送或者出借购买的数字内容，支持用户变更数字内容使用设备，支持法律规定的用于保护公众利益的相关权利，如合理使用（Fair Use）。

因此 DRM 需要解决的关键问题包括以下内容[1][2]。

① 数字内容的安全性：保证数字内容在出版发行、分发、使用等整个流通过程中的安全性。数字内容的安全性是数字内容版权保护最基本的要求，主要包括数字内容的机密性、完整性和非否认性。

② 权利描述：描述数字内容授权信息，支持不同商业模式下各种数字内容各类使用权利的描述。

③ 使用控制：控制数字内容的使用，确保只有授权使用者才可以使用受保护的数字内容。同时，用户对数字内容只拥有授予的使用权利，根据使用权利对数字内容进行访问。

④ 合理使用：支持用户对数字内容的合理使用，平衡版权持有人和公众之间的利益。

⑤ 权利转移：支持数字内容使用权利的转移，可以转移到另外一台设备上，也可以暂时或永久地转移给其他用户，使得用户可以更换数字内容使用设备，可以转卖、赠送、出租或者出借数字内容。

⑥ 可信执行：即在不安全的环境中保证程序按照预期的方式执行，程序的执行是安全可信的。

当前大部分 DRM 系统中，数字内容是经过加密、封装、添加水印和签名等处理后分发的，可以认为通过加密等处理的数字内容是安全的。此外，电子商务中的安全交易、电子支付等技术也是影响 DRM 发展的重要因素。

1.2 数字唯一对象标识

1.2.1 DOI 在 DRM 系统中的作用

在 DRM 系统中，每一个被保护的数字内容都有唯一的内容标识，它是鉴别不同数字内容的唯一参考对象。目前用于内容辨识的主要标准有 W3C 的统一资源标识符（Universal Resource Identifier，URI）、数字对象标识符（Digital Object Identifier，DOI）以及 MPEG-21 的数字项目辨识（Digital Item Identification，DII）等。在实际 DRM 系统中应用较多的是 DOI，它是由国际数字对象识别符基金会（International DOI Foundation，IDF）构造的一个框架，为数字环境中的数字对象分配唯一的、永久性的标识，方便该对象的管理和使用[3]。

DOI 是针对数字资源的永久性标识符。DOI 实现了数字资源动态的持久链接，如果数字资源的 URL（Uniform Resource Locator，统一资源定位符）发生了变动，出版商只要向注册代理机构（Register Agent，RA）提交并更新数据即可保证链接的有效性；同时还提供一站式服务，即各出版商通过 DOI 系统实现引文到全文一站式的链接。目前，DOI 国际基金会拥有 8 个注册代理机构，上千万个已经分配并解析的 DOI 号码在美国、欧洲和澳大利亚以及非英语国家的各 DOI 代理注册机构注册，其应用范围已从科技领域拓展到了政府部门领域。

J. Dalziel 在《DRM 环境中的 DOI》[4]中指出，DOI 是一个在数字环境中标识、交易知识产权的系统，它提供了一个管理知识产权内容、链接客户和内容提供商、方便电子交易以及自动化管理所有媒体的版权的框架。利用 DOI 可更容易、更方便地在网络环境中管理知识产权，构建电子商务的自动服务和交易，应用于 DRM 保护出版物的知识产权。

图 1-2 是基于 DOI 的 DRM 系统结构图，从图中我们可以看出，DOI 主要用于信息资源创建与保护以及信息资源发布这两个过程。在信息资源创建与保护的同时，把信息资源的 DOI、元数据及其 URL 向 RA 登记注册，存储这些信息，并由 RA 对其进行管理维护。发布信息资源时，信息资源的 DOI 信息与其一起发布，用户要获取数字资源或有关这一资源的相关信息时，DOI 查询请求就会被传送到 DOI 注册中心，由 DOI 解析系统即 Handle System（句柄系统）解析该 DOI 的 URL 地址，将其 URL 送回给用户浏览器并将结果显示给用户。通过 DOI 和 DRM 的结合，数字资源出版商或所有者可以对数字资源的内容设置权限，达到版权保护的目的。

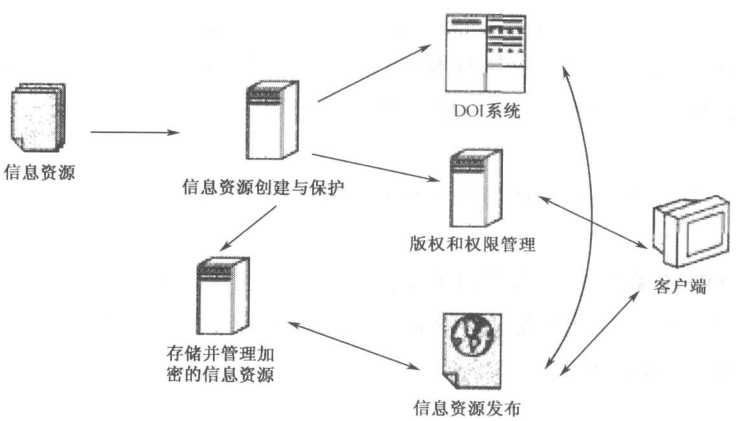


图 1-2　基于DOI的DRM系统结构图

1.2.2　DOI 系统概述

在任何数字环境中，唯一标识符对于信息管理都是非常重要的。如果不和分配者协商，在一个上下文中分配的标识符可能会在另外一个地方（或时间）遇到或者重用，分配者无法保证其他人知道他做的假设。

广义地说，DOI 系统是在数字网络环境下标识和交换知识产权对象的一种开放性系统，它遵从 URI 规范，并为基于数字对象结构公认标准的数字内容管理和数字版权管理提供了框架。这个框架是可扩展的，它有 4 个组成要素：标识符、解析系统、元数据和规则。狭义地说，DOI 是指标识任何数字化对象的一种标识符。DOI 实际上是一种 URI 或 URN（Uniform Resource Name，统一资源名称），即数字网络上的一个实体的名称（不是地址）。它为数字网络上的受控信息提供了一个持久可追溯的鉴别和可互操作的交互系统[5]。

DOI 系统具有以下特点。

① 唯一性：如果被描述的资源被修改或者移动，其标识符并不需要改动。

② 互操作性：能够与其他来源的数据互相操作。

③ 可扩展性：通过对 DOI 管理可增加新的特征和服务。

④ 多元解析：能够针对 DOI 的元数据进行数字内容的多版本、多格式、多镜像解析服务。

⑤ 分布式服务和管理：能够为网络中的任何节点的 DOI 号码提供服务和管理。

⑥ 动态性：元数据、应用和服务的动态更新。

DOI 系统上述特征为用户提供了如下功能：用户可以知道自己拥有哪些资源，需要哪些资源，所需资源位于何处，如何获得所需资源，找到并使用那些存储位置发生变动的资源。

DOI 系统的构建使用了几个现存的基于标准的组件，这些组件组合在一起并进一步开发出了一个协调的系统。整个系统已经为 ISO（ISO TC46/SC49）作为标准所接受。DOI 已经发展为一个由 IDF 管理的跨产业、跨区域、非营利的成果，DOI 广泛应用于科技出版、政府文档、数据等众多领域，DOI 可能用来为数据鉴别提供可互用的通用系统。

1.2.3　DOI 的语法

DOI 标识符是一个唯一的编号，遵循 ANSI/NISO Z39.84-2000 的句法标准，是基于 Handle System 建立的。DOI 由前缀和后缀两部分组成，并用字符“/”分开。其格式为：

```
<DIR><REG>/<DSS>
```

DOI 前缀包括由“.”分隔的两部分。其中<DIR>为目录代码，由 Handle System 赋予固定值 10，这是为了区分其他使用 Handle System 技术的系统；<REG>为登记机构代码，主要是一些大型的出版机构，由 IDF 负责分配号码，一般为四位阿拉伯数字。

<DSS>为 DOI 后缀，由委托命名机构给定。要扩大 DOI 的影响和应用范围，就必须兼顾原有的传统的标识符系统，所以主要编码格式基于一些已存在的标准知识体系，如：期刊及文献内容标识符（Serial Item and Contribution Identifier，SICI）、出版物件标识符（Publisher Item Indentifier，PII）、国际标准图书编码（International Standard Book Number，ISBN）、国际标准期刊编码（International Standard Serial Number，ISSN）等，避免破坏已经建立在上述标