



国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

“十二五”国家重点图书出版规划项目
数字出版理论、技术和实践

数字版权保护技术与应用

张立 童之磊 张博 陈立峰 编著



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>



国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

“十二五”国家重点图书出版规划项目
数字出版理论、技术和实践

数字版权保护技术与应用

张立 童之磊 张博 陈立峰 编著

電子工業出版社

Publishing House of Electronics Industry

内 容 简 介

本书以内容产业和版权制度为大背景,以互联网和数字技术为主线条,介绍了数字版权保护技术的各种要素及其相互关系,并介绍了数字版权保护技术在内容产业中的具体应用。本书在全面介绍数字版权保护技术的同时,对其局限性和未来趋势也有所探讨。本书对普通技术工作者了解法律准则和产业知识,对内容生产者了解技术保护措施,均有帮助,可作为一般的版权知识、数字版权保护技术的基础教科书。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

数字版权保护技术与应用 / 张立等编著. — 北京: 电子工业出版社, 2013.9

(数字出版理论、技术和实践)

ISBN 978-7-121-19159-6

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

中国版本图书馆 CIP 数据核字(2012)第 294545 号

策划编辑: 李 弘

责任编辑: 沈艳波

印 刷: 北京天来印务有限公司

装 订: 北京天来印务有限公司

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: 720×1 000 1/16 印张: 20.75 字数: 402 千字

印 次: 2013 年 9 月第 1 次印刷

印 数: 2 000 册 定价: 72.00 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 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线: (010) 88258888。

指导委员会

主 任 孙寿山

委 员（按姓氏笔画排序）

王关义 王志成 方中华 田胜利 朱伟峰 李宏葵

余昌祥 张志强 张增顺 张毅君 郝振省 敖 然

聂震宁 谢俊旗 谢新洲 薛松岩

编辑委员会

主 任 魏玉山

副主任 刘九如

委 员（按姓氏笔画排序）

王 强 王晓光 王德胜 方 卿 邢立强 吕肖庆

刘成勇 刘拥军 刘锦宏 孙 坦 孙广芝 李 弘

沈艳波 张 立 张 峻 张宝元 陈 丹 陈源蒸

郝黎明 秦绪军 徐丽芳 高 昂 黄肖俊 程三国

序

Introduction

数字出版方兴未艾。作为新闻出版业的重要发展方向和战略性新兴产业，数字出版近年来发展迅速，已经成为当前我国新闻出版业转型发展的助推器和新的经济增长点。基于互联网、移动通信网、有线电视网、卫星直投等传播渠道，并以 PC 机、平板电脑、智能手机、电视、iPad 等阅读终端为接收载体的全新数字出版读物，已成为人民群众精神文化生活不可或缺的组成部分。

从毕升的活字印刷到王选的激光照排系统问世，技术元素始终是出版业发展壮大的重要源动力。进入 21 世纪，信息通信技术（ICT）的飞速发展成为新经济发展的主要引擎，使得以思想传播、知识普及、文化传承、科学交流和信息发布为主要功能的出版业可以持续、广泛地提升其影响力，同时大大地缩短了信息交流的时滞，拓展了人类交流的空间。计算机芯片技术、XML 及相关标记语言技术、元数据技术、语义技术、语音识别和合成技术、移动互联技术、网络通信技术、云计算技术、数字排版及印刷技术、多媒体技术、数字权利管理技术等一大批数字技术的广泛应用，不但提升了传统出版产业的技术应用水平，同时极大地扩展了新闻出版的产业边界。

如同传统出版业促进了信息、文化交流和科技发展一样，数字出版的多业态发展也为 20 世纪末期开始的信息爆炸转变为满足个性化需求的知识文化服务提供了技术上的可能。1971 年，联合国教科文组织（UNESCO）和国际科学联盟理事会（ICSU）便提出了 UNISIST 科学交流模型，将出版业所代表的正式交流渠道置于现代科学交流体系的中心位置。进入 21 世纪，理论界又预见到，网络出版等数字出版新业态的出现正在模糊正式交流和非正式交流的界限，更可能导致非正式交流渠道地位的提升。随着以读者（网络用户）为中心的信息交流模式，比如博客、微博、微信和即时通信工具等新型数字出版形态的不断涌现，理论构想正在逐渐变为现实。

通过不断应用新技术，数字出版具备了与传统出版不同的产品形式和组织特征。由于数字出版载体的不断丰富、信息的组织形式多样化以

及由于网络带来的不受时空限制的传播空间的迅速扩展,使得数字出版正在成为出版业的方向和未来。包括手机彩铃、手机游戏、网络游戏、网络期刊、电子书、数字报纸、在线音乐、网络动漫、互联网广告等在内的数字出版新业态不断涌现,产业规模不断扩大。据统计,在2006年,我国广义的数字出版产业整体收入仅为260亿元,而到了2012年我国数字出版产业总收入已高达1935.49亿元,其中,位居前三位的互联网广告、网络游戏、手机出版,总产出达1800亿元。而与传统出版紧密相关的其他数字出版业务收入也达到130亿元,增长速度惊人,发展势头强劲。

党的十七届六中全会为建设新时期的社会主义先进文化做出战略部署,明确要求发展健康向上的网络文化、构建现代传播体系并积极推进文化科技创新,将推动数字出版确定为国家战略,为数字出版产业的大发展开创了广阔的前景。作为我国图书出版产业的领军者之一,电子工业出版社依托近年来实施的一批数字出版项目及多年从事ICT领域出版所积累的专家和学术资源,策划出版了这套“数字出版理论、技术和实践”系列图书。该系列图书集中关注和研究了数字出版的基础理论、技术条件、实践应用和政策环境,认真总结了我国近年发展数字出版产业的成功经验,对数字出版产业的未来发展进行了前瞻性研究,为我国加快数字出版产业发展提供了理论支持和技术支撑。该系列图书的编辑出版适逢其时,顺应了产业的发展,满足了行业的需求。

毋庸讳言,“数字出版理论、技术和实践”系列图书的编写,在材料选取,国内外研究成果综合分析等方面肯定会存在不足,出版者在图书出版过程中的组织工作亦可更加完美。但瑕不掩瑜,“数字出版理论、技术和实践”系列图书的出版为进一步推动我国数字出版理论研究,为各界进一步关注和探索数字出版产业的发展,提供了经验借鉴。

期望新闻出版全行业以“数字出版理论、技术和实践”系列图书的出版为契机,更多地关注数字出版理论研究,加强数字出版技术推广,投身数字出版应用实践。通过全社会的努力,共同推动我国数字出版产业迈上新台阶。



2013年8月

前言

Preface

版权不是与生俱来就与出版或内容创作相伴而生的。手抄本时代，没有版权，出版或内容创作依然存在。中外古代辉煌灿烂的文明成果，与版权无关。当人类社会进入到工业文明时代，特别是欧洲人发明了金属活字印刷机以后，内容作品的批量复制成为可能，批量复制的目的已不仅仅是为了自用或传播，同时还有了商业追求，只有这时版权概念和版权机制才有了诞生的基础。与此同时，出版或内容创作真正进入到产业化生产的时代。所以，严格地说，版权虽肇始于文艺复兴后期，但本质上是工业文明的产物。

版权虽然没有与出版或内容创作相伴而生，但它是否会相伴而终或常生不老呢？没人知道！

版权本身是对内容作品的保护，它通过保护印有内容的介质不被非法复制，从而保护了作品不被非法复制，保障了版权所有者的权益和利益。世界上第一部版权法是诞生于 300 多年前的《安娜法》，它保护的是纸介质的内容作品。随着承载内容的介质形态不断演进，先后出现了底片、胶片、唱片、磁带、磁盘等介质，版权条款也相应地进行了修订和扩充。这些修订和扩充之所以能够适用，是因为介质形态虽然发生了变化，但内容作品的最终形式——出版物，仍然是封装型的，即内容与介质是合一的，内容离不开介质而独立存在。

终于有一天，内容与介质分离了，内容可以与介质分开而独立存在，独立传播，甚至可以在不同介质上呈现。这个时代就是数字化时代。数字化时代，使内容变成了比特流，以比特流的形态在互联网、各种终端设备上传播和被使用。西方甚至有人认为比特流不可保护。所以数字化时代，版权机制受到了前所未有的冲击和挑战。看看今天的互联网，内容泛滥成灾，优秀的作品得不到保护。互联网提供的是“免费的午餐”，互联网本身也成了盗版的天堂。

面对这种形势，单纯靠修订法律已无法适应版权环境发生的变化。尽管美国人制订了《数字千年版权法》，但它的“避风港”条款仍然默认了网络盗版的存在。

数字化时代的另一个特点是用户创作内容，这使盗版有可能成为个人行为，它与封装型出版物时代的印刷厂、光盘生产线这种有组织、成规模，甚至是机构的盗版不同。个人盗版有可能是原版内容的，也可能

是改编后的；有可能是有非法传播目的的，还可能是纯粹提供知识共享的。这一切都使法律的打击对象变得分散、个体和模糊。

数字化时代的第三个特点是，数字作品的复制手段极其简便，简便到只需两个手指动作即可完成，即 **Ctrl+C** 和 **Ctrl+V**。

当法律变得无助的时候，技术也许是无奈之中的唯一选择或补充。这时，数字版权保护技术应运而生。

最初的数字版权保护技术只是单纯的加密封装、限制使用。它好比给数字内容作品加了把锁，只有花钱拿到钥匙的人，才可能打开使用。这是一种预先防范式的保护。这种方式虽然保护了内容作品不被非法侵权，但同时也给消费者带来了困扰，使内容阅读变成了一件麻烦的事情。当消费者因麻烦而放弃阅读时，内容作品的销售便会出现下滑，内容提供商的利益受到打击，作者的利益也受到影响。

于是另一种事后追惩的技术出现了，即数字水印技术。数字水印不影响消费者对内容的使用，但由于内嵌了特殊的痕迹，对非法盗版行为可以追踪打击。

今天，数字版权保护技术已经演变成了具有多种分支形式的数字内容作品的版权保护解决方案，有软件层面的、硬件层面的、内容格式层面的、传输层面的，等等。同时，根据内容产业的发展特征，新的研发探索也在不断尝试，包括版权标准的制定、多种内容粒度的授权机制、灵活的硬件绑定技术、面向不同网络和使用模式的分发技术，以及针对多种媒体形式的版权保护机制等。

如果没有了版权保护，谁还敢把自己的内容作品放到网上供大家使用呢？谁还会进行内容原创呢？如果没有了版权保护，内容生产商将怎样生存和发展呢？内容产业将会成为一种什么样的形态呢？我们都不是预言家。内容产业将来完全有可能演变成另一种模式存在。开源的路径已经为内容产业的新模式掀开了一角。在未来，有些内容也未必会以直接的商业价值存在，它可能是一种新的产业链启动的引擎。纵观国内外内容产业的发展态势，加强版权保护和开放版权两种模式在并行发展，而数字版权保护技术，严格说，是为那些需要保护的内容作品，在现阶段提供一种基本可行的解决方案。本书编写者正是在这个基点上，向读者介绍数字版权保护技术及其在内容产业上的应用。希望这种介绍能使我们的从业者对这个变化的时代，及我们的应对技术有所了解。本书由张立（第1、8章）、童之磊（第4、7章）、张博（第2、3章）、陈立峰（第5、6章）共同编著，张立完成全书统稿工作。

编著者

2013年5月

目 录

Contents

第 1 章	Chapter 1	
	数字版权概述	1
1.1	数字版权保护简介	2
1.1.1	版权的产生	2
1.1.2	技术的进步对版权法律的影响	3
1.1.3	技术措施在版权保护中的应用	4
1.1.4	版权管理的数字化与数字版权管理	6
1.2	数字版权保护技术发展	7
1.2.1	DRM 技术的提出	7
1.2.2	典型的 DRM 体系结构	9
1.2.3	DRM 标准	12
1.2.4	反盗版与盗版之争	15
1.3	数字版权保护技术研发现状	18
1.3.1	数字权利登记注册	18
1.3.2	多粒度授权技术	20
1.3.3	硬件绑定技术	21
1.3.4	多种分发技术	24
1.3.5	富媒体内容版权保护技术	27
1.4	数字版权保护技术市场格局	30
1.4.1	数字版权保护技术产品种类	30
1.4.2	数字版权保护技术市场分类	33

第2章 Chapter 2

数字权利描述语言	37
2.1 数字权利描述语言的体系结构和实体模型	38
2.1.1 DREL 相关概念	39
2.1.2 DREL 体系结构	40
2.1.3 DREL 实体模型	41
2.1.4 DREL 语言模型	43
2.1.5 DREL 的意义	44
2.1.6 国内研究现状	44
2.1.7 现有研究的不足	45
2.2 开放式数字权利语言	46
2.2.1 ODRL 的模型	46
2.2.2 ODRL 权利数据字典语义	52
2.2.3 XML 语法标记	54
2.2.4 ODRL 的扩展定义	54
2.2.5 ODRL 的主要特点与相关应用	55
2.3 可扩展权利标记语言 (XrML)	56
2.3.1 XrML 数字内容传播流程	56
2.3.2 设计原则与目标	56
2.3.3 XrML 优缺点	57
2.3.4 XrML 语法结构组成	58
2.3.5 XrML 核心概念	58
2.3.6 XrML 核心扩展能力	63
2.3.7 XrML 一致性	63
2.3.8 XrML 标准扩展与内容扩展	64
2.3.9 XrML 应用现况	65
2.3.10 XrML 应用实例: MPEG-21	65
2.4 数字权利描述语言的比较	74
2.5 其他数字权利语言	79

第3章 Chapter 3

数字内容信息加密及信息隐藏技术	81
3.1 数字加密	82
3.1.1 加密技术简介	82

3.1.2	加密技术标准 and 格式	86
3.1.3	加密方法	89
3.1.4	密钥的攻击分析	96
3.1.5	密钥的管理	98
3.1.6	相关加密衍生技术	101
3.2	数字摘要	101
3.2.1	基本原理	102
3.2.2	数字摘要的应用	102
3.2.3	相关算法介绍	104
3.3	数字水印	106
3.3.1	概述	106
3.3.2	特征/特点与评价标准	110
3.3.3	研究与发展	113
3.3.4	数字水印的分类	116
3.3.5	数字水印的原理	120
3.3.6	攻击分析	121
3.3.7	数字水印系统模型	124
3.3.8	常见水印算法介绍	128
3.3.9	数字水印的安全性设计	131
3.4	媒体指纹	135
3.4.1	媒体指纹概述	136
3.4.2	媒体指纹的分类	137
3.4.3	媒体指纹的相关研究	140
3.4.4	媒体指纹系统的关键设计点	142
第 4 章	Chapter 4	
	数字标识与认证	145
4.1	版权标识	146
4.2	内容元数据及标识	147
4.2.1	内容元数据	147
4.2.2	内容标识	148
4.2.3	其他标识系统	154
4.3	客户端标识	155
4.3.1	软件标识方案	155

4.3.2 设备标识方案	156
4.4 用户身份认证和识别	157
4.4.1 用户信息认证方式	157
4.4.2 智能卡认证方式	158
4.4.3 生物特征方式	158
4.4.4 PKI 认证方式	160
4.5 用户身份认证的发展趋势	163

第 5 章 | Chapter 5

数字版权保护技术体系	165
5.1 体系模型	166
5.1.1 业务模型	166
5.1.2 数据流模型	168
5.1.3 技术体系与业务系统的关系	169
5.1.4 典型的系统构架	170
5.2 OMA 技术体系	172
5.2.1 信任模型	173
5.2.2 基础下载	174
5.2.3 超级分发	175
5.2.4 流媒体	177
5.2.5 域	178
5.2.6 离线设备支持	179
5.2.7 广告管理	180
5.3 Marlin 技术体系	181
5.3.1 内容获取用例	182
5.3.2 共享与超级分发	186
5.3.3 超级分发	187
5.3.4 使用 OMArilin 进行移动分发	187
5.4 WMRM 技术体系	189
5.4.1 使用的加密算法	190
5.4.2 获取一个证书	192
5.4.3 获取内容密钥	193
5.4.4 解密内容	194

第 6 章 Chapter 6

数字版权交易与保护	197
6.1 数据的安全传输	199
6.1.1 IPSec 安全传输技术	199
6.1.2 SSL 安全传输技术	202
6.1.3 SSL VPN 与 IPSec VPN 技术比较	204
6.2 基于软件的版权保护技术	205
6.2.1 软加密技术	205
6.2.2 硬加密技术	206
6.3 流媒体加密	209
6.3.1 流媒体加密的特点	210
6.3.2 流媒体数据的网络传输方式	211
6.3.3 流式网络传输协议	212
6.3.4 多媒体数据编解码技术	216
6.3.5 数据流化技术	218
6.3.6 流媒体加密技术	221
6.3.7 用分组密码进行流式文件加密	222
6.3.8 用序列密码对媒体流加密	224
6.3.9 流媒体数据加密	225
6.3.10 MPEG-1 加密方法	227
6.3.11 基于 DirectShow 的流媒体加密传输	230
6.4 电子交易安全技术	233
6.4.1 基于 SET 协议的安全电子交易	233
6.4.2 CA 认证系统	237
6.4.3 安全电子交易 (SET) 协议与 CA 认证	243
6.5 数字内容封装与分段控制	245
6.6 内容交易与分发管理	246
6.6.1 超级分发	247
6.6.2 二次分发	248
6.6.3 批量分发	249
6.7 基于可信机制的交易管理	250
6.8 数字版权跟踪	254
6.8.1 完整版权的交易跟踪	254

6.8.2 作品细粒度交易跟踪	255
6.8.3 盗版跟踪	256

第 7 章 | Chapter 7

数字版权保护技术的典型应用	261
7.1 电子图书	262
7.2 原创文学	263
7.2.1 原创模式的数字出版平台	263
7.2.2 原创模式的数字出版服务方式	265
7.3 移动数字音乐	266
7.4 数字电视	267
7.4.1 付费数字电视领域 DRM 应用	268
7.4.2 数字版权保护技术在数字电视领域应用现状	271
7.5 基于智能卡的数字版权保护	272
7.5.1 智能卡技术	272
7.5.2 基于智能卡的数字版权保护系统	273
7.6 Real 公司数字版权保护方案	274
7.7 苹果公司应用版权保护	276
7.8 亚马逊 Kindle 应用版权保护	279
7.9 移动出版业务的数字版权保护	282
7.9.1 应用场景一：客户端的数字内容版权保护应用	283
7.9.2 应用场景二：彩信方式的数字内容版权保护应用	284
7.9.3 应用场景三：WAP 方式的数字内容版权保护应用	285
7.9.4 应用场景四：通过渠道进行内容分发	286
7.9.5 应用场景五：在线阅读	286
7.10 互联网出版应用	287
7.10.1 互联网出版业务	287
7.10.2 互联网出版平台各组成部分	288
7.11 我国政府对数字版权保护技术的重视	289

第 8 章 | Chapter 8

数字版权保护技术发展趋势与思考	291
8.1 数字版权保护技术的局限性	292
8.1.1 产业界对 DRM 的反思	292

8.1.2	DRM 的法律禁区	293
8.1.3	DRM 技术的不足	295
8.2	理论与技术的进步对版权保护的潜在影响	296
8.2.1	本体论的产生	296
8.2.2	语义网、知识库等内容碎片化技术的出现	297
8.2.3	云计算、大数据等内容管理技术的发展	300
8.2.4	P2P 等内容传播技术的崛起	302
8.3	开源与开放催生了新的授权模式	303
8.3.1	互联网的新特征	303
8.3.2	Copyleft 与 CC	305
8.3.3	Open Access 等 Open 系列	306
8.3.4	加强版权保护与开放版权将并存	308
参考文献		311
后记		315

第 1 章

Chapter 1

► 数字版权概述

随着信息技术的飞速发展，信息表达传播的效率和准确度得到了显著提高。但是由于数字媒体内容具有复制、分发便捷的特点，数字媒体产品和内容的侵权、盗版、非法使用日益猖獗，使版权所有者蒙受巨大的经济损失。据不完全统计，全世界每年因盗版而造成的经济损失高达 50 亿美元，美国软件业的盗版损失则达 200 多亿美元，盗版使美国电影业每年的收入减少约 25 亿美元。因此，盗版侵权行为制约着数字出版业可持续发展，在当前复杂的网络环境中实施有效的版权保护措施成为一个迫在眉睫的现实问题。

面对新技术和媒体形式的不断更新，数字内容提供商和内容运营商通常采用这样一种数字保护方法：在满足消费者需求的同时，保护其产品免遭非授权的使用和共享，这种技术称为 DRM (Digital Rights Management)，即数字版权管理或数字版权保护。DRM 的目的是为了保护数字内容的版权，从技术上防止数字内容的非法复制，以一定的计算方法，实现对数字内容的保护，包括电子书、视频、音频、图片等数字内容，最终用户必须得到授权后才能使用数字内容。当前，要推动数字出版产业的不断发展，首先必须保护相关群体利益不受侵害，由此可见，大力研发并推广 DRM 技术是数字出版产业蓬勃发展的核心。