数字权益管理技术

张晓林

文摘：本文简要描述数字权益管理的整体机制和技术框架，介绍权益描述语言、数字内容保护技术、权益管理机制等的技术要求和范例系统。

关键词：数字权益，知识产权，描述语言，保护技术，管理机制

Digital Rights Management Technologies

Zhang Xiaolin
Dept. of Information Management, Sichuan University, Chengdu, 610064

Abstract: Based on a brief introduction to the overall framework and its technical structure, the paper describes the requirements and systems of rights description languages, rights protection techniques, and rights management mechanisms.

Keywords: Digital rights management, Intellectual property, Rights description languages, Rights management mechanisms

数字权益管理(Digital Rights Management，以下简称 DRM)是指对数字化信息产品(如图书、 音乐、图像、录像、多媒体文件等)在网络中交易、传输和利用时所涉及的各方权利进行定义、描述、保护和监控的整体机制，是数字化信息环境可靠运行和不断发展的基本保障之一[1]。它包括知识产权保护，但涉及更为多样化对象在数字信息交易利用中更为广泛的活动与权益。

1. DRM 总体框架及其基本要求

DRM 涉及商业运营模式、法律制度、社会文化习惯和技术机制等多方面内容[2]，如图 1 所示。其中商业模式界定数字信息交易利用形式，并界定它们各自对知识产权管理的要求[3]；法律机制包括建立相应法律，如世界知识产权组织 1996 年版权协定[4]、美国数字千年版权法案[5]、欧洲理事会协调信息社会版权及邻接权指令[6]，另外涉及建立守法承诺、违法调查和非法处罚机制；社会文化因素涉及特定社会文化环境关于知识产权保护的社会期望、行为习惯、教育机制等；技术机制则充分利用数字信息网络化交易利用的特点，直接支持和控制知识产权管理的具体操作，并保障商业运营、保障法律实施、支持知识产权保护教育。

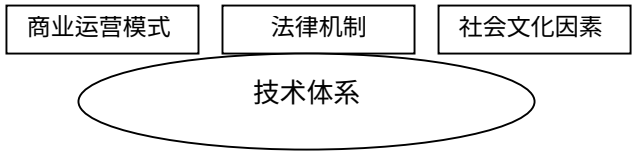

图 1

从总体上讲，DRM 机制需要支持现有法律、保护知识产权及相关利益、促进知识广泛传播和有效利用、促进信息环境健康发展。由于涉及多方参与者，DRM 还涉及不同的具体要求[3,7,8]。例如，从用户的角度，希望保护按现有法律和在传统信息产品交易利用中已获得的权益(例如合理使用和出借、转让权利)，保障数字内容可靠性，保障数字信息交易利用的方便性，保护用户隐私，保障 DRM 机制本身的互操作性、透明性和后向兼容性，并能提供增值服务。从生产出版者角度，希望保护知识产权和收益，支持多种形式灵活组配的商业运营模式，支持对不同细粒度信息内容和内容组合的保护，提供对交易利用流程的监控审计能力及市场跟踪分析能力，保障 DRM 机制下知识产品生产和传递的方便性经济性，保障 DRM 机制的互操作性和可伸缩性。从信息服务机构角度，希望保护信息服务机构在知识产权法律下已获得的权益，支持知识产品借阅、共享和长期保存，保障信息内容可靠性，支持附加增值服务，保护用户隐私，保障 DRM 机制的互操作性和透明性。由于角度不同，上述要求中有一些潜在的冲突，但用户要求(以及基于用户要求的信息服务机构要求)将会主导 DRM 技术发展，因为成功的 DRM 技术必须依靠成功的市场，而且发展的市场会不断突破技术限制、开辟新的知识产权管理方式。

2. DRM 技术体系及其要求

从技术角度，DRM 包括一系列相互联系的技术，图 2 给出了这个技术体系的基本构

成。其中：

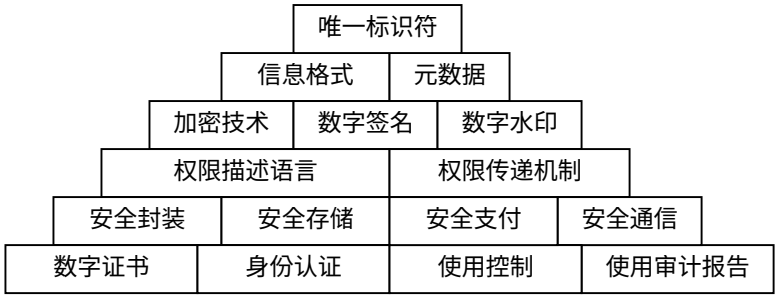

图 2

a. 唯一标识符技术解决 在网络环境下唯一、持久地确认数字信息产品的问题[8]；

b. 信息格式技术通过开 放格式(如 XML、PDF、JPEG、 MPEG、CSS、XSL、PNG 及基于 XML 的 OEB)支持多种信息内容形态的表示、交换和解析；

c. 元数据支持对数字信 息产品内容的定义和描述[10]；

d. 加密技术(包括对称密 钥和非对称密钥技术)、数字签名和数字水印技术支持对数字信息产品的加密、校验和来源认证；

e. 权限描述语言和权限传递机制负责对数字信息交易使用过程涉及的复杂对象的复杂权利进 行定义、描述、以计算机可识别方式标记、传递并检验；

f. 安全封装技术负责将多个数字信息对象及元数据封装在单一文件内以便传递，有时甚至封 装到特定物理载体上(例如智能卡、光盘、存储卡等)，封装过程可能涉及压缩和加密处理；

g. 安全通信、支付和存储技术利用 SSL 和 SET 等技术保障数字信息产品的可靠交易、安全传递 和可靠存储；

h. 数字证书及身份认证技术通过 X509 数字证书和 PKI 认证体系来确立准入控制、验证双方身 份、保障交易或传递的不可抵赖性和可审计性，建立交易与利用各方信任体系。

i. 使用控制与审计技术则在身份验证和权益规定的基础上实施交易或利用授权，并统计报告 交易或使用情况[11]。

这些技术经过一定集成形成相对完整的技术机制，并在相关法律、管理、审计、教育措施支持下实施数字权益管理。

为了保证在复杂的网络环境中有效推行和利用 DRM 机制，人们提出以下技术要求：

a. 信息可利用性，DRM 技术不能影响而应保障信息内容的完整性、可利用性和利用的方便性；

b. 开放性，任何 DRM 技术都应基于开放标准，不专属于某个厂家或机构，不排斥任何一种信息 内容形态或商业运营形式；

c. 平台独立性，DRM 技术机制应能支持各种软硬件系统和包括 WAP 在内的各种网络机制；

d. 底层技术独立性，DRM 技术机制应独立于具体数据格式、加密、数字水印、安全封装和传递 技术，这往往要求它们能选择应用多种格式和技术；

e. 可伸缩可扩展性，DRM 技术机制应支持不同规模的信息系统，能吸纳新内容和技术形态；

f. 内部集成性，DRM 系统应可与内部的知识产品生产系统、资产管理系统、交易管理系统和信 息组织检索系统等无缝链接；

g. 外部集成性，DRM 系统应支持第三方电子商务、身份验证、隐私保护、信息发现技术机制；

h. 灵活实施性，DRM 机制应以多种方式灵活应用于数字信息交易与利用中，例如基于出版商、 基于中介系统、基于信息服务系统、基于用户系统的 DRM 机制等。

上述技术中许多属于通用技术，例如唯一标识符、数据格式、元数据、加密技术、身份认证、安全通信和安全支付等。本文在以下部份将着重讨论 DRM 机制中独特而关键的权限描述语言、内容保护技术和权限保护系统问题。

3. 权限描述语言

数字权限管理首先应准确定义和描述谁拥有什么数字信息产品的什么权限、按照什么

协议和交易方式将哪些权限在什么范围授予给谁。这些信息必须用标准的开放的和计算机可识别的方式描述和标记，DRM 系统才可能自动进行相应的记录、识别、解析和解释，并据此进行权限控制。

权限描述语言实际涉及一个复杂的语言知识体系，首先依赖唯一标识符技术(例如 DOI 或 ISBN/ ISSN/ISWN/ISRC 等)来唯一地标记和确认在数字权限管理中的各个实体(包括信息产品、交易方、交易利用过程及相应的协议)，为各实体建立元数据格式，为描述元数据内容建立通用术语集(数据字典)及转换映射机制，为描述数据字典中概念及其逻辑语义关系建立相应概念集(Ontologies)，然后在此基础上建立权限描述标记语言，并根据元数据格式和标记语言来实际描述和标记关于特定信息产品在特定交易过程中的特定权限(图 3)。

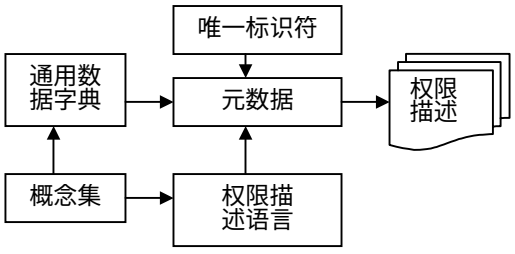

图 3

建立这个体系的首要任务是搜寻权限管理中的各种可能情况，建立相应概念体系，这方面工作起始于 INDECS[12] 计划及现在的 MPEG21[13]，它们分析、确认和定义权限管理涉及的各种实体、过程、概念及其逻辑关系，定义相应元数据词汇，为 DRM 提供一个标准的术语集。另外，国际图联的 FRBR 项目[14]也描述了出版物形态间的逻辑关系。在此基础上，人们正引入和开发相应的元数据，例如 Dublin Core[15]、AAP 电子图书元数据[16]和 ONIX 元数据[17]格式。

利用这些术语及其相互关系，人们致力于建立一个开放性权限描述机制。例如，开放 DRM 框架 (Open DRM Framework)[2]和 PREP(Policy and Rights Expression Platform)[18]框架都提出基于 WEB 的开放式权限描述机制，它们的核心部份是开放式权限描述语言，基于通用数据字典和概念集、并以计算机可识别的标准格式来描述生产者和信息服务系统(作为提供者)的权限管理政策，以及描述用户和信息服务系统(作为用户)的权限管理方式，支持这些信息以开放形式发布和组织，以便能被自动发现、获取和解析，并在此基础上支持自动的权限谈判、权限交易、使用控制。而且，这个语言应可扩展，能不断引入关于新的内容形态、商业模式、交易条件、管理操作的权限规定和术语，能与相关领域共享有关的元数据和概念集。这个语言应通过一系列标准接口允许生产者、用户或信息服务系统使用安全传输、验证、安全存储等方面的标准技术来实施权限控制，甚至可以将语言本身固化嵌入相应技术机制，但应不限制使用某几种专门技术。这个语言还应支持权限管理信息交换协议(Rights Messaging Protocol)，以便人们查询权限管理信息、传递授权标志，而且将包括双 向操作， 例如出版商查询信息服务系统或用户是否具备必要的权限管理机制和能力。

权限描述语言需要定义和描述的具体内容包括[3,8]：

a. 交易利用模式，包括免费使用、免费登记使用、个人购买、机构购买、长期订阅、出租、 出借、购买使用许可、按用户类型或地区销售、按阅读次数或阅读时间销售、按不同内容组合或内容形态销售、按不同阅读设备销售等，而且应能吸纳新的交易模式。

```
<rights>
  <asset>
    <uid idscheme="URI">…</uid>
  </asset>
  <usage>
    <usage-type>
        ……
        <constraint>…</constraint>
    </usage-type>
        ……
  </usage>
  <narrow>…</narrow>
  <rightsholder>
    <party>
        ……
        <role>…</role>
    </party>
    ……
  </rightsholder>
  <admin>
    <party>…</party>
    <datetime>…</datetime>
  </admin>
</rights>
```
表 1

b. 交易利用权益，包括：发行零售商的发行权 限，例如发行地区或用户范围、发行数量、发行交易模式类型、信息内容形态类型、信息内容组合方式、阅读设备类型、价格范围等；图书馆等信息服务机构的服务权限，例如地区或用户范围、服务模式类型(例如只能提供借阅)、提供信息内容形态和组合方式限制、阅读设备限制、拷贝与长期保存限制、附加增值服务限制；用户使用权限，如显示、打印、拷贝、修改、删除、出借、转售等权限。

c. 权益管理权限，例如各交易方在建立用户隐 私保护条款、对不同信息内容组分或不同内容形态建立不同条款、转换内容形态(例如将 PDF 版转换为纯文字版)、析取和重组内容、

集成到其它产品、转换阅读设备、在出版或发行后修改权益条款、设置新条款、嵌入验证信息等方面的权限。

目前，人们已定义若干描述语言来具体描述、标记权限信息，比较主要的有 Open Digital Rights Language(ODRL)[19]和 Extensible Rights Markup Language(XrML)[20]。前者是开放标准，后者属 Xerox 公司所有、需要授权才能使用。两者都基于 XML 语言，表 1 给出基于 ODRL 的一个例子。

4. 数字内容保护技术

数字内容保护技术的目标是保证只有合法用户经过授权后通过合法拥有的技术手段才能利用被保护信息。保护技术类型包括加密封装技术、数字水印技术、专用系统或专用存储载体、内容控制技术(例如采用连续传送播放格式或低分辨率格式等增加复制或拷贝难度)等。由于后两种技术影响信息内容可利用性和使用方便性，现在的发展趋势是以加密封装为主来保护信息内容，基本技术过程可由图 4 表示。

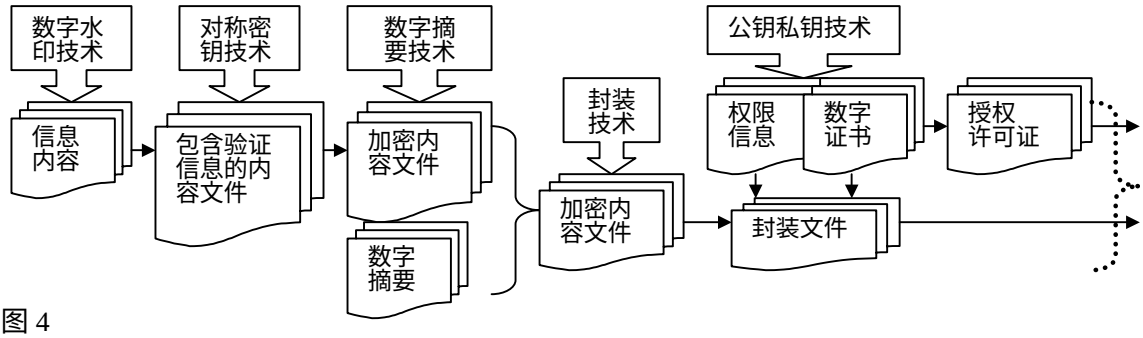

图 4

数字水印(Digital watermarking)技术[21,22-23]是信息隐藏术(Steganography)的一个分支，通常 是隐蔽地将特定信息(例如版权信息、出版者身份、出版物唯一标识符、甚至元数据或权限控制信息)嵌入到公开数字内容中，可通过特别软件或硬件析取、识别和显现，从而鉴别出版物原始作者或提取其它控制信息。与此密切相关的是数字指纹(Digital fingerprinting)技术，专指用隐蔽方 式嵌入特定信息单元鉴别信息(例如出版物复本顺序号)，据此确认数字信息单元的原始拥有者，从而发现泄密者或擅自拷贝传播者。绝大多数数字水印嵌入技术在数字内容编码噪音中嵌入数据，通过特定算法使这些数据按一定方式分布，使其不能被使用者感知、只能由专门解码软件识别。具体方法主要分为基于空间域的嵌入方法(例如在按一定规律分布的像素点最次码位 LSB 嵌入数据)和基于频率域的嵌入方法(例如在离散余弦转换 DCT 中根据各数据块 DCT 系数来嵌入数据)。许多数字水印技术还能自动根据数字内容编码分布特征来调整数字水印“深浅”密度，例如一幅清晰蓝天图像和一幅盛夏花园图像就需要不同深浅的水印。数字水印需要具备一定的健壮性，能抵御过滤、压缩、剪截、旋转、比例转换、格式转换、图像锐化或钝化、甚至统计平均、拼图、加载新水印、重新扫瞄或重新抽样等攻击。数字水印不仅用于数字图像，还用于音频数据(例如 MusiCode 技术)和视频数据(例如 Galaxy/DVD 数字水印建议)。

加密技术是数字内容保护的基础，一般使用对称密钥技术对实际信息内容加密，使用非对称密钥(公钥私钥)技术来传递对称密钥(作为解密密钥)并对有关数字摘要、数字证书或许可证等加密。由于加密技术已相对成熟，请有兴趣的读者参见相关文献。数字摘要(Digital Digest)技术用于保 障数据内容的真实性完整性、防止传输和存储过程的删改。一般可采取诸如 MD5 这样的单向杂凑算法(One-way hush function)对数据内容进行计算形成一个小容量摘要，例如 128bits，即使只有微 小差别的不同数据内容也将产生不同的数字摘要。例如，有人用 MD5 对<双城记>全文生产数字摘要“CABB806969AF220B281474382D88C726”，然后在全文中增加了一个空格，重新生产的数字摘 要为“532CF2E34EC2DDC301D4AC3EF0D3260 ”。数字摘要用内容作者私钥加密后传输。接收者 可利用同样算法对数据内容计算得到一个摘要，并与经内容作者公钥解密后的摘要比较，从而鉴定真实性完整性。数字证书是包含特定对象(可以是个人、机构或机器)的元数据、公钥以及需要传递的对称密钥等的信息集合，被用认证机构(Certification Authority)私钥加密，可用认证机构公 钥解密，用以证明特定对象的身份。

在数字权益管理中，数据内容对称加密密钥、权限管理信息、身份信息、提供者公钥等都可能被组织到一个权限许可证文件中，该文件用特定接收者公钥加密后传递，只有合法接收者用自己的私钥才能解密、从而获得解密密钥和其它必要数据。而且，公钥私钥对往往被用软件甚至硬件形式固化在提供者系统和接收者系统中，这些系统经过一定验证体系注册登记，接收者本人也无法析取出它们的明文形式。

5. 数字权限管理系统

众多的数字内容保护系统已应运而生，例如 IBM 的 Cryptolopes、InterTrust 的 DigiBoxes、NetRights 的 LicenseIt 等，我们这里简要介绍若干相对比较全面的数字权限管理系统。

(1) EBX 系统

EBX 系统(Electronic Book Exchange System)[7]是由出版领域众多公司组成的知识联盟协作提 出的电子图书权限管理机制，其主要技术过程如图 5 所示。

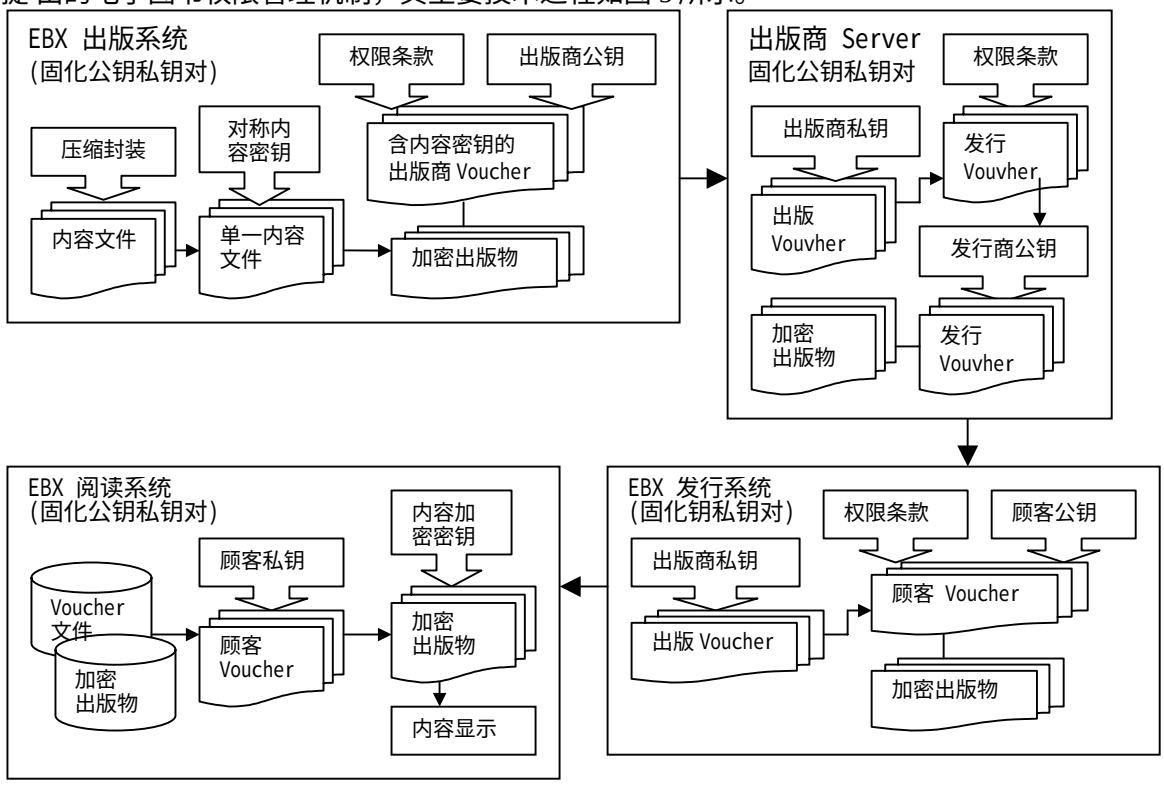

图 5

EBX 主要利用一个许可证文件(Voucher) 来传递权限信息和控制权限执行。许可证中包括数字 内容唯一标识符，内容加密密钥，允许阅读、借阅、出售或转让的复本数量，具体发行或传递权限(例如出售、借阅、转让或修改)、具体使用权限(例如显示、打印、拷贝等)，根据设备、时间、内容类型、内容部份等进一步设置的权限，内容验证编码等。

整个过程开始时，出版商利用专门的 EBX 出版软件(可以是 WEB 服务器嵌入软件)，将所有内容文件封装压缩为一个文件，利用对称加密技术随机产生一个加密密钥对其进行加密。然后出版商按照标准格式建立一个出版许可证，写入出版物信息和权限条款，并将加密密钥封装在该许可证中，最后用出版商公钥对许可证加密，并将加密出版物及其许可证存储到出版商服务器。

发行商利用专门的 EBX 发行软件(可以是 WEB 服务器嵌入软件)购买电子出版物发行权限。当发行商确认购买加密出版物发行权后，出版商服务器用出版商私钥对出版许可证解密，根据购买条件填入发行权限条款，建立发行许可证，并用发行商公钥对发行许可证加密，然后将该许可证和加密出版物传给发行商服务器。

顾客利用专门的 EBX 阅读系统(可以是 WEB 浏览器嵌入软件)来购买和使用电子出版物。当顾客确认购买某出版物后，发行商服务器用发行商私钥对发行许可证解密，根据购

买条件填入顾客使用权限条款，建立顾客许可证(也包含出版物信息和内容加密密钥)，并用顾客公钥对顾客许可证加密，然后将该许可证和加密出版物传给用户。顾客的 EBX 阅读系统将加密出版物和许可证分别存入指定的目录，当顾客阅读该出版物时，EBX 阅读系统取出相应许可证，用顾客私钥解密，取出内容加密密钥，对加密出版物解密并显示有关内容。但是，解密后的顾客许可证和内容文件只存在于计算机内存中，一旦当前阅读过程结束就被清除。

图书馆可利用 EBX 发行系统来购买电子图书(限定复本数量)，可通过管理界面设置“借阅”时间。当读者从图书馆系统中借出一本电子图书时，读者同时获得设置了时间限制的使用许可证，图书馆拥有的该复本许可证自动“暂时”失效，当读者归还使用许可证、或有效时间已到时，读者的使用许可证自动失效，图书馆拥有的该复本许可证恢复有效。

所有系统的公钥私钥对都在制造过程中固化到软件中，所有许可证文件和内容文件都以加密形式存储，在运行过程中自动调用处理，使用者无法截获明文形式的密钥、许可证或内容文件。EBX 还通过其它技术来保证传输和交易的可信赖性，例如基于 SSL(安全套接层)技术保证数据传递的私密性，基于 PKI(Public Key Infrastructure) 进行身份认证和防抵赖。

(2) Adobe PDF Merchant

PDF 是流行的数据内容格式，Adobe 公司推出了 PDF Merchant 系统支持数字权益管理，它由 WebLock、 WebSell、WebBuy 三个分布但相互联系的功能模块组成[24](图 6)。

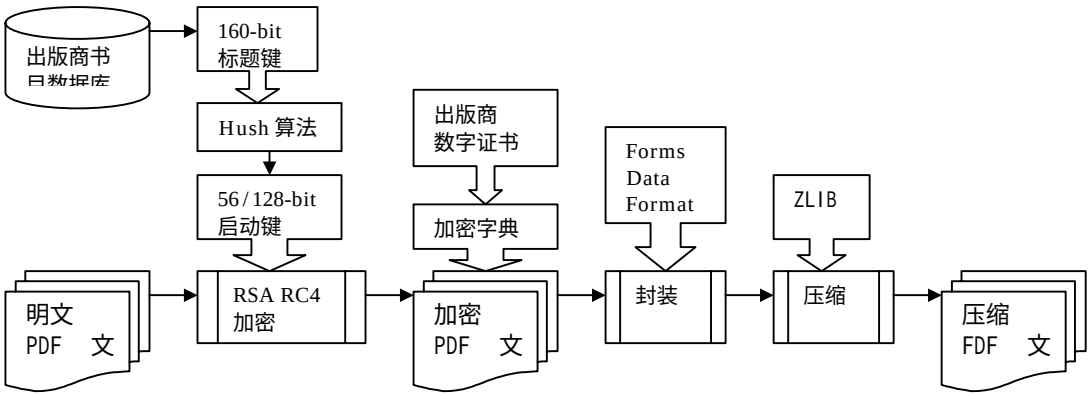

图 6

WebLock 是一个独立的服务器端工具，供出版商对 PDF 格式的出版物(以下称 PDF 文件)进行加密封装处理。具体操作步骤包括：从出版商书目数据库中取出 160 比特的标题键(Title Key)，利用杂 凑算法生成 128 比特(美国)或 56 比特(其它国家)的启动键(Access Key)；将启动键作为加密密钥， 利用 RSA/RC4 工具对原始 PDF 文件加密，形成加密 PDF 文件；为加密 PDF 文件加上加密字典(Encrypt dictionary)，该字典是一个包含若干对象的附加文件，确认必须具备的安全控制机制(例如经过注册的 Adobe 客户端 WebBuy 模块标识号和加密密钥)，字典用出版商数字证书(Digital Certificate) 签署，即用其中的私钥加密；将整个 PDF 密文(包括其加密字典)用 FDF(Forms Data Format)封装， 由于 FDF 文件(MIME 类型为 application/vdn.fdf)被设置为总是存入用户机器，可避免浏览器软件自动打开 PDF 文件。在封装过程中还可使用 ZLIB 压缩工具对已经压缩的 PDF 文件进一步压缩，进一步减少数据量。在这个过程中还可加入使用限制条件，不过许多使用限制是在实际销售过程(即 WebBroker 模块)才根据顾客选择具体规定，所以使用限制条件往往由 WebBroker 以许可证形式体现。

WebSell(又称 WebBroker)也是服务器端工具，销售商可将其作为一个 COM(Component Object Model)对象嵌入自己的 IIS/ASP 系统环境中，负责在数字出版物销售过程中建立和使用许可证、保证对出版物使用实现安全控制，具体功能包括：根据顾客购买条件建立使用权限，将权限数据写入使用许可证(License)文件；请求或自动提取顾客计算机环境参数，捆绑入许可证中；将出版商加密密钥再加密封装入许可证中；利用自己数字证书对许可证文件进行数字签名；向顾客传送经过加密封装的出版物文件和许可证文件。PDF

Merchant 通过将许可证文件与用户计算机的特定环境参数 (Habitat values)相捆绑而保障用户合法获得该文件后可持续对它进行权限管理，可用环境参数包 括：计算机 ID，通常就是 NIC(Network Interface Card)的 MAC 地址；用户确认号，如 Windows 的用 户登记号(往往与其它属性结 合来提高安全程度)；UTC(Universal Time Clock)时间值，用于允许 借阅或出租等功能的系统；存储装置确认号，例如硬盘、网络驱动器号码等。具体使用什么参数可由用户在自己 WebBuy 设置选项中确定，也可由出版商或销售商明确规定，但所有许可证都必须至少捆绑一个环境参数。

WebBuy 是与 Adobe Acrobat 4.05 以上版本阅读器捆绑的客户端嵌入安全处理器，对 PDF 文件进 行解密处理，并根据使用权限控制使用操作。具体控制步骤包括：当顾客调用特定 PDF 文件时，首先在当前 PDF 目录或用户许可证目录下寻找该 PDF 文件的许可证；如果找到，通过它取得开启密钥；利用密钥和 RSA/RC4 算法为 PDF 文件解密；解密后通知用户“授权完成”，启动 PDF 阅读器，根据使用权限进行阅读或其它形式的处理；如果没有找到，用户不能使用该 PDF 文件，WebBuy 将提示用户联机购买相应许可证。使用权限包括打印、修改、选择内容(文字或图像)进行拷贝剪贴、对内容进行批注等，这些权限由许可证文件描述。权限控制机制在 PDF 文件被打开、存储以及用户试图修改与安全有关的阅读器设置时都会自动启动。

PDF Merchant 对一般数据出版使用提供相对安全的整体环境，但捆绑计算机环境参数影响移动 使用能力，而且 PDF 解密密钥在客户端对 PDF 文件解密过程中显性存在于内存中，Adobe 阅读器本身也可能遭到袭击从而允许存储解密后的 PDF 文件。

除此之外，安全数字音乐计划(SDMI)[25]和 MPEG[26]也都提出了自己的 DRM 机制。

6. 结束语

技术上讲，DRM 机制正在逐步成熟，但它也面临许多问题[1]。例如，匿名性与隐私保护、侵蚀读者在法律和传统交易过程已获得合法权益的可能性、可信赖机制与身份验证、技术和系统的互操作性、以及“道高一尺、魔高一丈”的破译密码及保护机制活动等。另外，DRM 机制对图书情报机构将带来深远的影响，也需要及时进行研究。

参考文献

[1] W3C Workshop on Digital Rights Management. Jan 2001 http://www.w3.org/2000/12/drm-ws/
[2] Renato Iannella, Open Digital Rights Management A Position Paper for the W3C DRM Workshop. www.w3.org/2000/12/drm-ws/pp/iprsystems-iannella.pdf
[3] AAP DRM for eBooks: Publishers’ Requirements. 2000.http://www.publishers.org/home/drm.pdf
[4] WIPO COPYRIGHT TREATY, December 20, 1996 http://www.loc.gov/copyright/wipo/treaty1.html
[5] The Digital Millennium Copyright Act. Oct. 1998 http://www.loc.gov/copyright/legislation/hr2281.pdf.
[6] The EC directive on the harmonisation of copyright and neighbouring rights in the information society (copyright directive). (May 1999)
http://europa.eu.int/comm/internal_market/en/intprop/intprop/news/copy2en.pdf
[7] Electronic Book Exchange System Specification v0.8 http://www.ebxwg.org/pdfs/spec.pdf
[8] J. Bormans and N. Rump. Multimedia framework (MPEG-21)Part 1: Vision, Technologies and Strategy. v2.0, ISO/IEC JTC1/SC29/WG11/N4040, March 2001
http://www.cselt.it/mpeg/public/mpeg-21_pdtr.zip.
[9] 张晓林. 数字对象的唯一标识符技术。现代图书情报技术，2001(待发)
[10] 张晓林. 元数据开发利用的标准化框架。现代图书情报技术，2001.2
[11] 张晓林. 虚拟信息资源系统的用户使用管理。现代图书情报技术，2000.5
[12] G. Rust and M.Bide. The <indecs> Metadata Framework: Principles, model and data dictionary. June 2000.
http://www.indecs.org/pdf/framework.pdf
[13] MPEG: Call for Requirements for Rights Data Dictionary and Rights Expression Language. March 2001.
http://www.cselt.it/mpeg/cfp/call_for_requirements(rights_language).htm
[14] IFLA Functional Requirements for Bibliographic Records. 1998 http://www.ifla.org/VII/s13/frbr/frbr.pdf
[15] Dublin Core Metadata Element Set, Version 1.1. 1999 http://dublincore.org/documents/dces/
[16] AAP Metadata Standards for EBOOK. 1.0. 2000. http://www.publishers.org/home/metadata.pdf
[17] ONIX International Release 1.2. 2000. http://www.editeur.org/onixfiles1.2/onixfiles.html
[18] John Erickson, et al. Principles for Standardization and Interoperability in Web-based Digital Rights Management. 01/2001. http://www.w3.org/2000/12/drm-ws/pp/hp-erickson.html
[19] Open Digital Rights Language V0.8. Nov. 2000. http://www.odrl.net/ODRL-08.pdf
[20] Extensible Rights Markup Language http://www.xrml.org/
[21] S. Katzenbeisser, and F. Petiticolas. Information Hiding: Techniques for steganography and digital watermarking. London: Artech House, 2000

[22] The information hiding homepage - digital watermarking & steganography
http://www.cl.cam.ac.uk/~fapp2/steganography/
[23] Fraunhofer Institute for Computer Graphics. Site on Digital Watermarking.
http://www.iis.fhg.de/amm/techinf/ipmp/water.html
[24] K. Abrew. Using Adobe's PDF Merchant for Secure Ebook Distribution
http://www.planetpdf.com/mainpage.asp?webpageid=884，另参见
Adobe Systems Incorporated, Adobe PDF Merchant SDK Reference Manual, December 2, 1999
[25] Secure Digital Music Initiative. http://www.sdmi.org/
[26] R. Koenen. Intellectual Property Management and Protection in MPEG Standards. Jan. 2001
http://www.w3.org/2000/12/drm-ws/pp/koenen.pdf

本文最初发表在《现代图书情报技术》2001 年第 5 期第 3-7 页，续 10 页。