数字版权管理技术及应用研究进展

范科峰[1],莫 玮[2],曹 山[3],赵新华[2],裴庆祺[1]
(1. 西安电子科技大学计算机网络与信息安全教育部重点实验室,陕西西安 710071;
2. 中国电子技术标准化研究所,北京 100007; 3. 桂林电子科技大学电子工程学院,广西桂林 541004)

摘 要: 随着信息与通信技术的飞速发展,数字媒体内容的分发、复制与编辑变得越来越普遍.数字内容的版权管理和内容保护可以减少内容盗版和不规范使用行为.本文介绍了数字版权管理技术的基本原理,综述了关键技术,分析了国内外应用情况,并讨论了几个具有挑战性的问题.最后,总结了全文,并展望了该技术领域的研究重点和发展方向.

关键词: 数字内容; 内容安全; 数字版权管理; 标准化
中图分类号: TN319 **文献标识码**: A **文章编号**: 0372-2112 (2007) 06-1139-09

Advances in Digital Rights Management Technology and Application

FAN Ke-feng[1,2],MO Wei[2],CAO Shan[3],ZHAO Xin-hua[2],PEI Qing-qi[1]
(1. *Key Laboratory of CNIS, MOE, Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *China Electronics Standardization Institute, Beijing* 100007, *China*;
3. *School of Electronics Engineering, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*)

Abstract: With the rapid development of ICT technologies, the distribution, copying, and editing the digital media content is more and more easy. The copyright management and content protection of digital content may decrease the content piracy and abnormal usage. In this paper, the basic principal of DRM (digital rights management) is introduced firstly. The key technologies of DRM are summarized in detail secondly. The DRM applications of main scenarios are analyzed thirdly. In addition, several challengeable problems are discussed. Finally, the key research interest and development tendency are expected.

Key words: digital content; content security; digital rights management; standardization

1 引言

数字媒体内容保护通常包括文本、图像、音频、视频等媒体介质.数字技术的迅速发展和广泛应用,互联网、电信移动网络等新兴传输方式和手机、机顶盒、电脑等多媒体终端极大地拓展了数字媒体内容的传输范围.由于数字媒体具备易于无损复制、分发等特性,借助数字技术和互联网随意批量复制和发行受知识产权保护的数字媒体产品和内容的现象普遍存在.如果缺乏对数字媒体的版权管理和内容保护将导致严重的负面现象,由此滋生的大量盗版及不规范使用行为不但会对数字媒体产业造成巨大的冲击,而且也会对我们的经济、社会和文化造成多重的伤害.目前,数字版权保护方面的问题已经引起了各国政府、法律、媒体和工业等各方的共同关注.实际的经验和近年来的探讨表明,仅凭法律手段难以保护数字内容的版权,相关技术手段也是极其重要的.

工业界越来越清晰地认识到,缺少数字版权保护机制的数字化网络无法对数字内容进行有效保护,整个数字内容产业的有序发展将因此受到严重阻碍.因此,出现了数字版权管理技术(Digital Rights Management,以下简称 DRM),它是一项涉及到技术、法律和商业各个层面的系统工程.它为数字媒体的商业运作提供了一套完整的实现手段.DRM 技术确保了数字媒体内容能够被合法的使用.DRM 使各个平台的内容提供商们,无论是因特网、多媒体还是交互数字电视,提供更多的内容,采取更灵活的节目销售方式,同时有效地保护知识产权.DRM 不仅仅指版权保护,同时也提供了数字媒体内容

收稿日期:2006-02-02;修回日期:2006-03-20
基金项目:国家自然科学基金(No. 60672112);信息产业部电子发展基金(No. FZ2004-04);信息产业部电子行标研究项目(No. B1220076800);北京市教委科技计划项目(No. KM200610772008);西电科大研究生创新基金(No. 创 05001)

的传输、管理和发行等一套完整的解决方案,因此 DRM 是一个系统概念,它包含数字版权信息使用,受版权保护的数字媒体内容的管理和分发. 关于 DRM,一个比较公认的定义是"DRM 是对有形和无形资产版权和版权所有者关系的定义、辨别、交易、保护、监控和跟踪的手段[1]. 自 DRM 技术诞生之日起,产业界和学术界进行了大量的研究,国外的如 Microsoft[2]、IBM[3]、Thomson[4]、Philips 等,国内的如华为公司、北大方正、和高校[5,6]等也进行了体系结构和关键算法的研究.

本文对数字版权管理技术研究进展情况进行了综述,重点就 DRM 的基本原理、涉及到的关键技术、应用情况及存在的问题进行了分析,并指出 DRM 的研究重点领域与发展方向.

2 基本概念

2.1 基本特点

DRM 是对数字媒体进行版权管理的系统性方法. 按 W3C 组织的建议,DRM 涉及数字内容使用权限的描述、认证、交易、保护、监测、跟踪,以及对使用权拥有者之间关系的管理. DRM 已经发展到第二代. 第一代 DRM 侧重于对内容加密,限制非法复制和传播,确保只有付费用户才能使用. 第二代 DRM 在第一代的基础上,在权限管理方面有了较大的拓展. 用户、授权和内容是 DRM 系统的三个基本要素. 设计和建立数字版权管理应遵循的基本原则是:简单、灵活和开放[7].

数字版权管理价值链的组成包括:(1) 内容创作者、(2) 版权拥有者和管理机构、(3) 内容代理、发行商、(4) 注册与认证、(5) 数字版权管理方案提供商、(6) 支撑信息系统提供商、(7) 内容仓储管理、(8) 应用开发者、(9) 存储和传输服务、运营、(10) 网络服务提供商、(11) 接入服务提供商、(12) 硬件终端设备制造,(13) 软件终端开发.

数字版权管理应贯穿数字媒体的整个生命周期,包括:内容制作、内容存储、内容发行、内容接收、内容播放、内容显示等.

2.2 基本原理

数字版权管理的原理是:使用技术手段,对数字内容在分发、传输和使用等各个环节进行控制,使得数字内容只能被授权使用的人,按照授权的方式,在授权使用的期限内使用. DRM 的功能模型主要分为三个部分:内容服务器、许可证服务器和客户端[8],如图 1 所示. 上述三个模块是 DRM 的核心功能,必须协同工作,才能构成完整的数字版权管理系统. 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 封装块;许可证服务器包含权利库、内容密钥库、用户身份标识库和许可证生成器,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和触发支付等金融交易事务;客户端主要包含控制器和数字内容使用工具,并负责和许可证服务器进行交互.

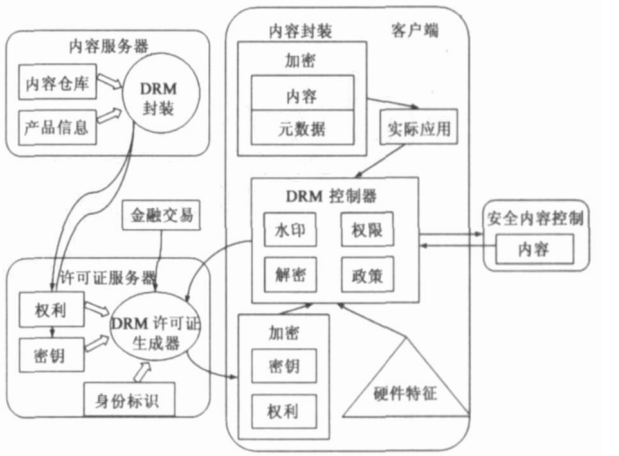

图 1 DRM 基本结构

3 关键技术

3.1 内容安全

3.1.1 数据加密

密码技术是信息安全技术领域的主要传统技术之一,它是基于香农信息论及密码学理论的技术,现有的数字内容的保护多采用加密的方法来完成,即首先将多媒体数据文件加密成密文后发布,使得其在传递过程中出现的非法攻击者无法从密文获取机要信息,从而达到版权保护和信息安全的目的. 加密被广泛的研究[9,10],加密技术对于设备认证和从一个设备到 DRM 系统的安全传输很有用. 以数据加密和防拷贝为核心的 DRM 技术基本上以密码学理论为基础,采用的传统方法是将文件加密成密文的密钥系统或公钥系统,提高加密、解密系统密级的方法是不断增加密钥的长度. 只有授权用户才能得到解密的密钥,而且密钥是与用户的硬件信息绑定的. 加密技术加上硬件绑定技术,防止了非法拷贝,这种技术能有效地达到版权保护的目的.

当前国内外大部分计算机公司和研究机构的 DRM 技术采用这种以数据加密和防拷贝为核心的 DRM 技术方法,针对各个应用领域,有不同的 DRM 系统[2~4]. 但是,这种方法在实际中变得越来越不安全. 在加密视频数据方面有缺陷:一是密文脆弱,必须从头到尾无误的解密,如果密文被修改或传输丢失,那么解密过程即使使用正确的私钥也不能恢复出密文;另一个问题是加解密的计算费用,这在实时应用和低造价的消费电子设备中尤其重要. 另外这种将文件加密成密文的方法,在将密文解开后就失去了保密意义;加密的密文还容易引起许多好事者的兴趣,触发他们积极破译的激

情[9,10].

3.1.2 数字水印

数字水印技术[10,11]是目前信息安全技术领域的一个新方向,是一种可以在开放网络环境下保护版权和认证来源及完整性的新型技术,创作者的创作信息和个人标志通过数字水印系统以人所不可感知的形式嵌入在多媒体中[12],人们无法从表面上感知水印,只有专用的检测器或计算机软件才可以检测出隐藏的数字水印[13].水印可以定义为不被感知地在内容中嵌入信息的操作行为[14].数字水印在 DRM 中的应用有:广播监控、所有者鉴别、所有权验证、操作跟踪、内容认证、拷贝控制和设备控制[15].

(1)广播监控:通过识别嵌入到作品中的水印来鉴别作品是何时何地被广播的;

(2)所有者鉴别:嵌入代表作品版权所有者身份的水印;

(3)所有权验证:在发生所有权纠纷时,用水印来提供证据;

(4)操作跟踪:用水印来鉴别合法获得内容但非法重新发送内容的人;

(5)内容认证:将签名信息嵌入到内容中以待日后检查内容是否被篡改;

(6)拷贝控制:使用水印来告知录制设备不能录制什么内容;

(7)设备控制:使用水印来制造设备,比如 Digimarc 公司的 MediaBridge 系统.

3.1.3 内容封装技术

3.1.3.1 InterTrust 的 DigiBox 技术

DigiBox 技术[16]当前处于领先地位,DigiBox 的结构是一种安全的内容封装方案,一个 DigiBox 能够拥有一个或多个可任意使用的内容.权限描述能在一个 DigiBox 中传送,也能在不同的 DigiBox 中传送.在 DigiBox 中,例如头信息和总体信息这些高层元素用一个传输密钥加密;如果需要,内容能被其他的密钥加密.在 DigiBox 中的部分用公开密钥算法加密,优点是防止任意两个密钥之间的互相可计算;缺点是要求在不同的参入方中分配密钥(密钥管理).进一步要求每个主机有一个称为 InterRight 点的安全存储,加密算法用三重 DES 和 RSA,完整性认证要使用加密的哈希函数.一旦 DigiBox 打开,按照掌管控制的原则,有两种不同的信息流会发生,一方面是计费的目的;另一方面是会根据 DigiBox 的控制集要求收集返回的用户使用信息,而且使用用户意识和同意这一信息反馈圈的作用.现在正在 DigiBox 的内容中集成水印技术[17].

3.1.3.2 IBM 的 Cryptolope

IBM 的 Cryptolope[18]技术的特征是用安全加密技术封装要保护的信息技术内容.Cryptolope 是一种基于 Java 的软件,它由 3 个部分组成,首先 Cryptolope Builder 是一种在打包的工具,它允许构造加密的软件包,包中有使用的商业规则和内容,这一部分的工具是为内容提供者使用.第二部分是为信息的消费者设计的,它的 Cryptolope Player 是访问 Cryptolope 内容的解释器,它通过一个 HTML 的解释器与第三部分的 Cryptolope Clearing Center 交互.第三部分是可信任的第三方,它提供密钥管理,付费系统和事件登陆和使用测量.这种方法面临的主要的问题是这是一个封闭的所有权系统,用户被迫在 IBM 的 InfoMarket 网络环境中使用,这也是 Cryptolope 技术暂时未被广泛接受的原因.这项技术成功的要素是要能提供更多的商业伙伴,需要将版权保护与金融机构,内容提供商等都密切地联系起来.

3.1.4 移动代理技术

采用移动代理来保护知识产权有两种,一是将内容作为移动代理,另一种是将内容交易双方之间签订的数字条约作为移动代理.两种方法在安全性上都还有很多的问题.前一种没有考虑将内容作为代理的对虚假终端攻击的问题.后一种方法没有考虑对内容与用户身份的认证问题.但是移动代理为版权保护技术提供了新的思路[19].

3.2 权限描述

数字内容的版权管理与整个内容的传播流程密切相关.第一代数字版权管理仅仅实现了安全利用和资源加密的静态方式的管理,而上世纪 90 年代后期发展起来的第二代数字版权管理方案,更全面地、动态地管理信息流程,协调各方的权利与义务,使各方利益得到合理的保障.如何实现新的数字权益管理,由微软和施乐合资的 ContentGuard[20]发布的基于 XML,面向数字权益管理的 XrML 标记及相关的 XrML SDK 体系,为描述和实现第二代数字权益管理提供了完整的解决方案.并于 2002 年 4 月提交给国际结构信息标准发展组织 OASIS,目前 XrML 已成为数字版权管理的事实标准.ContentGuard 提出的实现方案包括两部分:对数字权益描述建立数字权益管理文档;对数字权益的执行和对流程的控制.XrML 继承了 XML 的优点,使用了微软的 DCOM 组件技术有较好地跨平台特性,它能确保数字权益管理的信息的完整性并能实现实体的验证[21~23].

3.2.1 数字权限描述

数字权限描述(REL)是行为方在某条件下对特定资源享有的某种权利.因而它包括四大元素:行为方主体(principal)、权利(right)、资源(resource)和条件(condition)[25].

(1)主体:该类封装关于被授权人的认证,是一对一的状态;

(2) 条件:该类指定了权利约束;

(3) 权利:该类是主体对某些资源执行的动作即主体对于相关资源可以执行的一种或一类行为;

(4) 资源:该类是授权主体执行权利的对象.

其关系模型如图 2 所示:

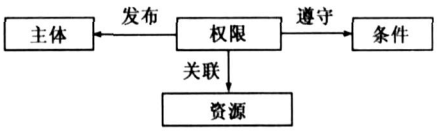

图 2 权限描述的基本结构

3.2.2 授权和许可

以上四要素组成权限描述即 XrML 文档被封装成授权(Grant),每个授权有专门命名.每份许可包含一份或多份授权.每个授权应是一个最基本但完整的权益,而许可可以认为是一组权益,因此 XrML 实现的数字权益保护体系中用四元素来表述形成授权、授权组成许可,系统运作也就是许可(申请)获得许可(确认)的动态过程[24].如图 3 所示:

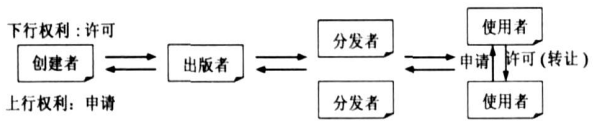

图 3 主体要求的申请和许可的关系

3.3 身份认证

身份认证是 DRM 系统的一个重要组成部分,是实施权限管理的基础.身份认证技术多种多样,从最简单的用户名密码、硬件标志技术到公钥基础设施(PKI)技术,甚至生物识别技术.在复杂性、实时性和安全性方面,不同的身份认证技术差异很大.身份认证是指一方证明另一方身份的过程,是证实被认证对象是否属实和有效的一个过程,其基本思想是通过验证被认证对象的属性来达到确认被认证对象是否真实有效的目的.在单机或封闭环境下,身份认证相对简单,被认证对象的属性主要有口令、智能卡或者声音、指纹、虹膜等生物特征识别技术[25,26]:

(1) 口令核对法是鉴别用户身份最常用的方法,系统核对用户输入的用户名和口令与系统内已有的合法用户的用户名和口令是否匹配来验证用户的身份,它实现方便,使用简单,但是安全性低,网络环境下,口令被明文传输会使身份认证极不安全;

(2) 硬件唯一标志认证技术也被称为硬件绑定技术,用户只有在特定硬件存在的情况下才能使用系统资源.获取硬件唯一标志的方法有很多:CPU ID,但是只有一部分 CPU 可以获取;硬盘 ID;网卡硬件地址,USB 设备 ID 绑定等.

(3) 智能卡是由一个或多个集成电路芯片组成的集成电路卡,智能卡可存储用户的个人化参数和秘密信息.基于智能卡的认证方式是一种双因子的认证方式,若没有智能卡用户就不能访问系统资源,即使智能卡丢失,入侵者仍需猜测个人身份识别码(PIN),才能从智能卡中读取秘密信息,进而利用该秘密信息与主机之间进行认证.

(4) 生物特征识别[27]一般通过:(*a*) 图像预处理,包括图像平滑、尖锐化处理、二值化、轮廓化等;(*b*) 图像分割,分割的目的是把图像空间分成一些有意义的区域.可以以逐个像素为基础去研究图像分割,也可以利用在规定领域中的某些图像信息去分割;(*c*) 图像特征提取,特征提取是图像识别中最关键的一步,必须根据不同的物体采取不同的方法.(*d*) 图像模式匹配,采集图像并提取特征,和数据库中的特征数据进行比较,并输出结果.生物特征认证在 DRM 应用中,需要有相应的生物特征提取仪器,如指纹仪、摄像仪、扫描仪和语音输入器等.生物特征识别包括单生物特征模式和多生物特征模式,典型的单生物特征和多生物特征结合的应用模型如图 4 所示:

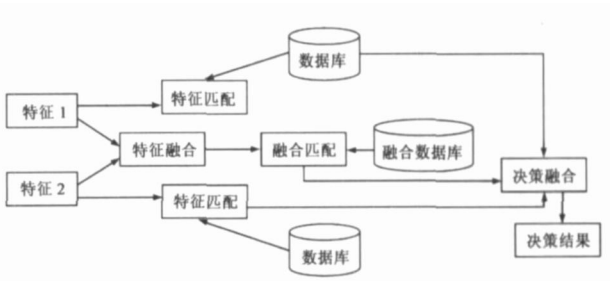

图 4 生物特征与非生物特征结合的应用模型

但是开放的网络环境下,身份认证面临的威胁主要有认证信息的截获、篡改及重放等,对认证的安全性、可靠性、透明性(用户应该感受不到认证服务的存在)以及可扩展性(当和不支持认证机制的系统通信时,应该保持一切不受影响)方面具有很高的要求.

3.4 密钥管理

密钥管理是加密和水印技术中关键的一步[28].密码学和水印的安全性依赖于密钥的保密性,而不是加密算法、水印嵌入和提取的复杂性,即 Kerckhoff 原则[29].然而,安全密钥管理和交换协议的实现对实际的 DRM 系统而言常常会增加复杂度.密钥管理包含多个问题,如密钥产生、密钥的安全交换、密钥安全存储、密钥吊销、密钥契约,和密钥验证[30].对于包含多个设备和网络的视频 DRM 来说,安全密钥交换是其中重要的管理问题.经典的密钥交换和认证协议可以用在 DRM 系统中进行设备间的安全密钥交换.多播和广播网络为密钥管理和视频安全传输提供了几大挑战[31,32].一个挑战是向一组用户或群密钥管理传递时的接入控制.当新用户加入多播网或用户离开网络时的安全性

的保持.另一个挑战是在多播和广播内容发布中所有的接收机获取同样的视频.这是内容跟踪和指纹识别中的一个问题,对每个用户具有个性化的视频拷贝.有学者提出对每个接收机分配一个独特的二进制串,然后通过多播方式对每个接收机发送两份拷贝.两份拷贝各嵌入不同的水印.另一种方法是建议修改网中发送的含水印的视频.缺点是该方法需要网络基础设施的支持,这是许多网络所没有的.

4　应用情况

DRM 的应用领域广泛,大体可分为电子书,包括电子文档、多媒体、移动、广播电视、家庭网络、P2P 等.典型的应用示意图如图 5 所示.

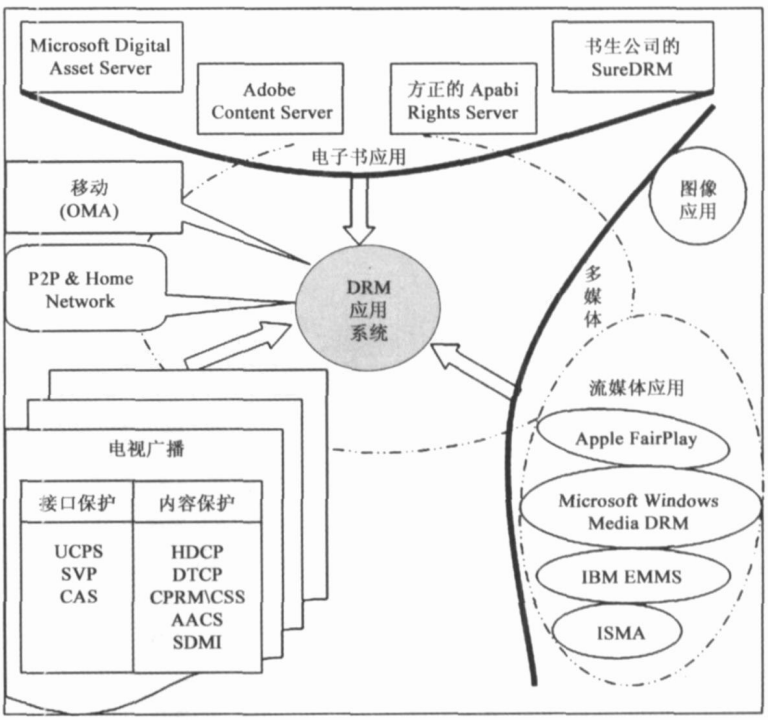

图 5　不同应用领域中的 DRM 技术体系

4.1　电子书、电子文档

对于电子书的 DRM[33]保护 Microsoft DAS、Adobe Content Server(原 Glassbook Content Server)等等,国内的 eBook DRM 系统有方正 Apabi 数字版权保护技术、书生的 SEP 技术、超星的 PDG 等[34].

4.2　多媒体

4.2.1　图像

目前已有的保护图像的方法是数字水印技术,把版权信息通过数字水印技术加入图像后,如果发现有人未经许可而使用该图像,可以通过软件检测图像中隐藏的版权信息,来证明该图像的版权.目前国外的数字水印技术开发商有美国的 Digimarc Corp.及英国的 High Water Signum Ltd.Digimarc 提供的版权管理服务属于前述的第一种方式,它利用数字水印技术在静止图像中嵌入版权信息,High Water Signum 基本上也提供相同的服务.国内现有的以华旗公司自主研发的数字水印系统"爱国者版神"较为知名.爱国者数字水印技术作为新一代数字水印技术,集成抗攻击、抗压缩、易损性和抗重复添加等最新的信息隐藏技术于一体.

4.2.1　流媒体

流媒体是指在 Internet/ Intranet 中使用流式传输技术的连续时基媒体,如音频、视频或多媒体文件.流媒体的实时性使得流媒体技术日益流行,广泛应用于多媒体新闻发布、在线直播、网络广告、电子商务、视频点播、远程教育、远程医疗、网络电台、实时视频会议等互联网信息服务的方方面面.流媒体为互联网的音视频传输带来巨大便利的同时,其自身也更容易被非法拷贝和非法传播,从而损害流媒体拥有者的合法权益.主流的流媒体系统目前都已拥有了 DRM 的解决方案,如 Real System 的 RMCS(Real System Media Commerce Suite)[35]、Media Service 的 MDRM(Microsoft Digital Rights Management)[36]等,它们都遵循流媒体版权保护的一般框架.对于流媒体的 DRM 主要有 IBM 的 EMMS 和 Microsoft Windows Media DRM.另外,由 IBM,Apple,Sun,Cisco,Philips 等于 2000 年 12 月发起成立了 ISMA[37],目标是加速基于 IP 技术的音视频及数据流媒体开放标准的产业化应用.目前已发布 ISMA1.1(MPEG4 基本音视频 Profile0/ 1)、ISMA2.0(AAC-HE 和 AVC 高效音视频 Profile2/ 3/ 4)、ISMACrypt1.1(RTP 承载加密的 AVC 流)等标准,并计划引入 OMA DRM2.0[38]和 REL 作为其 DRM 实现.

4.3　移动

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,其版权及相关利益必须得到保证.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.目前,国际上针对移动 DRM 开展了大量的研究工作,其中,OMA 制定的移动 DRM 标准得到了广泛的支持和认同.2005 年 6 月 14 日,OMA 公布了最新的 OMA DRM V2.0,制定了基于 PKI 的安全信任模型,给出了移动 DRM 的功能体系结构、权利描述语言标准、DRM 数字内容格式(DCF)和权利获取协议(ROAP).OMA 的 DRM 规范主要包括 DRM 系统、数字内容封装和版权描述三大部分:

(1)系统部分(DRM):关注消息交互,密钥交换以及

设备管理等;

(2) 数字内容封装部分(DCF):定义数字内容的封装格式和一些与使用相关的头信息;

(3) 版权描述语言部分(REL):定义对数字内容使用的限制、许可信息和对应的密钥信息等.

当前,已经出现了支持 OMA DRM 的移动设备,如 Nokia 6220 手机. 国内的掌上书院支持移动 DRM,掌上书院是目前使用最为广泛的手机电子书阅读软件之一,它使用的电子书格式为 UMD. 随着 3G 移动技术以及 OMA DRM 的发展,DRM 在移动领域的应用研究将更进一步,市场上将会出现更多的移动 DRM 系统和产品.

4.4 电视广播

在数字电视广播系统中,数字版权保护技术主要应用在数字内容的传输和使用、数字内容制作管理、各类硬件设备、运营商等各环节上. 国际上如 HDCP, DTCP, CPRM, SDMI, SVP, CAS 等,我国数字电视产业联盟刚完成的 UCPS(数字音视频接口统一内容保护技术规范). 目前,联邦通讯委员会(Federal Communications Commission, FCC)已经批准了多项适合用于在数字电视领域的内容保护技术规范.

4.5 P2P 与家庭网络

P2P(Peer to Peer)网络凭借其低成本、高容错能力、资源丰富以及配置灵活等等优点得到了广泛的应用,除了 Skype、BT、eDonkey 等几种比较主要的 P2P 应用外,互联网上还有大量基于 P2P 的业务协作工具、分布式计算、流媒体等多种能够带来丰厚利润回报的业务. 但是同时由于它的灵活性给数字版权保护带来了极大的挑战,目前针对于 P2P 的应用提出了很多种 DRM 的应用模型[39~41],对于整个 P2P 的数字版权保护提出了一些列实用型模型. Thomson 的 SmartRight 系统[42,43]就是一个创新的、可更新的、端到端的用于家庭网络的版权保护方案.

5 挑战性的问题

5.1 互操作问题

在商业环境中,创作者、生产商、发行商需要互相沟通. 制片人和使用者需要频繁地在不同的场合使用不同来源,不同格式的作品资源,这就需要发展的系统具有较强的兼容性. DRM 在产生之日起,由于不同的产业集团各自的利益驱使,形成了互不兼容的版本. 像目前苹果公司的 iTunes 和微软的基于 Windows 平台的媒体播放器采用了不同的 DRM 技术,且不能兼容. 2004 年 Koenen[44]等提出了典型的三种解决 DRM 系统间交互的途径:全局标准化,在线转换,按需下载. DMP 致力于将多种 DRM 系统互通,互换密钥,试想互操作. 需要非常强的政策支持. 因为目前商用 DRM 的种类较少,此想法优先进行但是略超前. 这方面的开发工作包括:

(1) 数字对象标志符(The Digital Object Identifier, DOI),DOI 系统类似于用来识别物品的条形码,注册代理机构为每一个数字对象分配识别号码并记录描述该对象的元数据,假如能够用相对简单的办法跟踪对象和版权所有者情况,那么元数据就可以被不断更新.

(2) 版权表述语言(Rights Expression Languages),为了表述使用数字内容的法律条款,人们发明了许多形式的表述语言. 这些语言具有通用性,可以被用在网站、文本文件、图片、音乐、PDF 文档和流媒体中. 这些表述语言中比较有名的是 Open Digital Rights Language Initiative (ODRL) 和 Extensible Rights Makeup Language (XrML). 互操作是当前 DRM 产业面临的最重要的问题. Heileman[45]提出了一种新的层次化的研究 DRM 系统交互性的模型. 其观点是互联网协议在 OSI 的分层模型下,可把复杂的问题简化. 他把 DRM 系统的交互性划分为三个方面:DRM 执行单元的上层,下层和物理层. 层间的通信协议可以实现标准化.

5.2 标准化问题

标准化的 DRM 就是指整个内容产业链上的不同角色,包括:创作者、发布者、零售商、支付网关,及客户端负责解码任务的 DRM 执行单元都遵守同样的标准. RUMP[46]2004 年在提出了"DRM 系统能否标准化"的观点. 他认为可行的方法是对现有规范中的某些关键模块进行标准化,不能依赖于庞大的 DRM 模型,而依赖于实际的构建于那些模型上的规范,但他没有给出实现的方案. 在实际应用方面,许多公司已经提供了 DRM 解决方案,这其中比较著名的有 Intertrust[47],Microsoft 公司的 Media Player10, IBM 的 EMMS, Apple 的 Itune 等. 但是这些实现方案互相之间并不兼容,因此有不少研究都提出了 DRM 的标准化问题. 在现在大部分系统中,DRM 系统的重点在于保护版权所有者和销售商的利益,却往往忽视了用户的利益,这些 DRM 系统有可能强制用户暴露个人隐私信息. 因而,现在已有研究注重于保护个人隐私,兼顾版权所有者和用户双方权益的方案 DRM 的应用范围也越来越广泛.

对于 DRM 系统,必须要分析其分布链上的潜在安全隐患,同时要鉴别在这条链路的每一个点上,什么工具必须作为反措施来实现. 基于此,要求 DRM 中的数字水印技术必须在鲁棒性、安全性、不可见性、复杂度、容量和验证的可能性及不可逆性等这些重要性质之间做出折中,以达到较好的效果. 而 DRM 中的数字水印技术也应该从这些参数中进行比较. 图 6 给出了水印算法评估基准(benchmark)系统的框架[48]. 水印基准的作用就是要对这些参数进行一个公平和自动的评价. 水印基准研究最初是由 F. Petitcolas, R. Anderson 和 M. Kuhn 等人以 Stirmark 系统开始,做了开创性的工作. Stirmark 系

统至今仍是一个公用的、自动化的基准评价系统.除了 Stirmark 以外,还发展了 Optimark、Checkmark 和 Certimark 等水印基准评价系统[49].

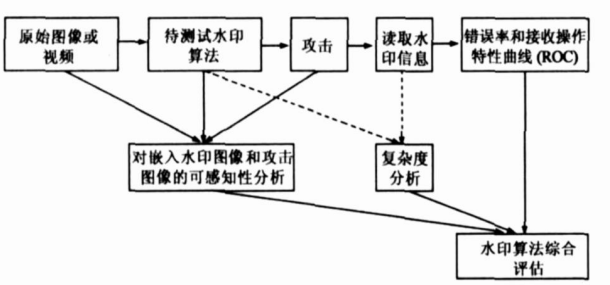

图 6　水印算法评估系统框架

5.3　安全性问题

安全性是 DRM 最基本的要求.安全是相对而言的,攻破密码算法和密钥只是时间的问题,如果从时间上、空间上及从所付出的代价上让破解没有价值的话,系统便是安全的.对于一个密码的最基本的要求,便是安全性.然而,在一个 DRM 系统中,安全性问题并不是选择密码的主要标准.

目前 DRM 系统的安全瓶颈在于用户端软件和 License 的保护.传统密码学中研究的安全问题大多是防止第三者窃密,即 Alice 与 Bob 通信,不能让第三者 Malice 知道通话内容.这里,Alice 和 Bob 是互相信任的,他们之间可以共享密码,而只要保证 Malice 得不到密码即可.然而在 DRM 中的安全问题却很特殊,对于产品发行者来说没有谁是可信任的,因为即使是通过合法途径获得产品的用户,仍然可能复制自己的产品并传播给他人.然而产品发行者却必须把密码交给他所不信任的人.所以,在 DRM 中加解密技术只是用来安全传递产品和密钥,而要防止终端用户通过解密获得原始产品,则还需要其他技术的支持.这些技术的目的在于实现在 DRM 中,不是把密钥交给不可信任的用户,而是交给可信任的程序或设备,然后保证合法用户只能通过这个程序或设备来使用产品.支持 DRM 的数字产品发行系统中,要让终端程序能正常使用加密产品,必须让其拥有解密能力及知晓所有解密所需数据.然而因为在普通的个人计算机上,用户对机器有完全的操控权.因此,一切终端程序知道的,用户也能想办法知道,终端程序能做到的,用户也能想办法做到.正因为如此,有的研究者认为在没有专门硬件支持下,在普通个人计算机上要绝对防止用户通过解密获得原始产品是不可能的.但是我们仍然可以通过多种技术使得程序尽可能安全,也就是说尽可能增加用户通过破解程序来获得未加密的原始产品的困难.

5.4　评测技术

DRM 的评测技术是公认的难题,尚未见到统一测试方案的报道.现有的大多基于水印技术.对 DRM 关键技术进行功能和性能测试,以确保它的安全性、可用性和互操作性.以 IPTV 的 DRM 技术方案测试为例说明,见表 1 和表 2.

表 1　IPTV 数字版权保护解决方案的关键技术及其主要测评指标

关键技术	主要测评指标
资源的安全与保护	加密的强度、数字水印的鲁棒性、数字签名等等
资源和实体的标识	标识(如 URI)的唯一性
资源声明	是否具有资源声明能力 功能描述项的描述、抽取和显示能力 功能描述是否符合 DOCBIN 及其相关扩展标准
权利描述	权利描述语言的可读性 权利描述语言的语法和语义规则 权利描述语言的灵活性机制 权利描述语言的互操作性机制
任管理	加密机制的安全性 接触的人、设备、程序的可信任性
安全硬件	硬件设备(如:处理器,存储器,智能卡)的安全性

IPTV 数字版权保护解决方案比较典型的系统有两种:一种是 IP + PC,另一种是 IP + STB(机顶盒) + TV(电视接收机).因此需要搭建不同的运行环境,以便从系统级设置端到端的测试关键步骤、关键流程、模拟关键环境.

表 2　IPTV 数字版权保护典型系统及其主要测评指标

典型的 IPTV 的 DRM 系统	主要测评指标
IP + PC	各个模块间的互操作性 是否支持各种商业模式的配置
IP + STB + TV	各个模块间的互操作性 是否支持各种商业模式的配置

6　总结与展望

本文对 DRM 涉及的基本原理、关键技术、应用场景和公认的难题等进行了详细分析和综述.DRM 技术已经历四个阶段:

(1)第一阶段(2000 年前)的重点在于数字内容加密存放和客户端根据许可证使用内容;

(2)第二阶段(2000～2003 年)关注 DRM 服务器和客户端间信任关系的建立和内容密钥、许可证交换机制;

(3)第三阶段(2003～2006 年)主要研究具体应用场景对 DRM 中各组成部分的需求,如为了使 DRM 更具有实用性,数字内容和许可证应封装哪些信息等.

(4)第四阶段(2006～目前)通用的 DRM 技术框架.针对数字电视节目内容、家庭网络的 DRM 技术体系和标准研究等.

未来 DRM 技术发展需考虑多方面的需求:

(1) 与其它具有版权需求的应用领域结合,如家庭网络、IPTV、流媒体播放、软件发布、网络游戏等;

(2) 与运营商的运营环境相结合;

(3) DTV、卫星广播、IPTV 等固定宽带数据业务应用(DRM 可丰富用户体验,如按费用选择图像质量、音频效果等,提供灵活的权限管理能力等);

(4) 与 CA(条件接收)系统融合;

(5) 应用软件的可运营化(用户按需或按使用购买特定功能,满足需要又节省开支);

(6) 应用于消费电子类产品的 DRM 芯片技术;

(7) 内容保护以加密为主,辅助使用数字水印和数字指纹、进行盗版跟踪及审计.

(8) DRM 的身份及内容认证结合指纹、虹膜等生物特征识别技术提高安全性.

我们认为 DRM 能有效保护数字内容产业链中各个环节的利益,能促进数字内容消费体系有序管理,将逐渐成为数字媒体产业的关键性技术基础设施. 我国需要加大 DRM 领域技术的研究力度,并开展相对统一的 DRM 技术标准的研发.

参考文献:

[1] R Iannella. Digital rights management (DRM) architecture[J]. D-Lib Magazine,2001,7(6):6 - 11.

[2] Microsoft Corporation. A Technical Overview of Windows Media DRM 10 for Devices[OL]. http://www.microsoft.com/windows/windowsmedia/forpros/Consumerelectronics/p4skit/p4s-2abDetail.aspx,2006 - 10 - 08/2007 - 03 - 10.

[3] W Bender, D Gruhl, N Morimoto. Techniques for data hiding [J]. IBM System,1996,1(35):313 - 336.

[4] Ingemar J Cox, Joe Killian, F Thomson, Talal Shamoon. Secure spread spectrum watermarking for multimedia[J]. IEEE Trans on Image Processing,1997,6(12):1673 - 1687.

[5] 刘立刚,陈晓苏,胡蕾. 抗协议攻击的版权保护安全方案[J]. 中山大学学报,2004,43(2):83 - 86.

[6] Yuan Zhonglan, Xia Guangsheng, Wen Qiaoyan. Copyright protection protocol for digital media[J]. Journal of Beijing University of Posts and Telecommunications,2005,28(1):102 - 106.

[7] Renato Iannella. Digital rights management (DRM) architectures[J]. D-Lib Magazine,2001,3(6):18 - 23.

[8] John S Erickson. OpenDRM: A Standards Framework for Digital Rights Expression, Messaging and Enforcement[OL]. http://www.ait.utk.edu/drmworkshop/opendrm_20sep02.pdf,2002 - 09 - 02/2007 - 03 - 05.

[9] Feng Dengguo. Research on theory and approach of provable security[J]. Journal of Software,2005,16(10):1743 - 1756.

[10] Cox I J. Secure Spectrum Watermarking for Images, Audio and Video[R]. NJ: NEC Res Inst., Princeton,1995.

[11] 钮心忻. 信息隐藏与数字水印[M]. 北京:北京邮电大学出版社,2004.

[12] ISO/IEC,21000 - 5,2004, International Standards Organization. Information Technology Multimedia Framework (MPEG - 21) Part 5: Rights Expression Language[S].

[13] S Craver, N Memon, B L Yeo, M M Yeung. Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications[J]. IEEE Journal on Selected Areas in Communications,1998,16(4):573 - 586.

[14] Furon T, Duhamel P. An asymmetric watermarking method [J]. IEEE Transactions on Signal Processing,2003,51(4):981 - 995.

[15] S Pereira, J J K O Ruanaidh, T Pun. Secure Robust digital image watermarking using the lapped orthogonal transform[J]. IS&T/SPIE Electronic Imaging,1999,3657(2):21 - 30.

[16] O Sibert, D Bernstein, D Van Wie. DigiBox: A self - protecting container for information commerce[A]. First USENIX Workshop on electronic Commerce[C]. New York: IEEE,1995,103 - 109.

[17] G Boccon Gibod, X Serret Avila. Methods and systems for encoding and protecting data using digital signature[P]. US:6,961,854,2005.

[18] Benjamin J Renaud. Digital Signatures for Data streams and Data Archives[P]. US:6021491,2000.

[19] Z Pu-han, SUN Yu-fang, An intelligent mobile agents-based architecture for network fault detection[J]. Journal of Software,2002,13(7):1209 - 1219.

[20] ContentGuard. eXtensible rights Markup Language (XrML) 2.0 Specification[OL]. http://www.xrml.org,2005 - 10 - 04/2007 - 03 - 08.

[21] ContentGuard. XrML 2.0 Specification&Schema. http://www.xrml.org/get_XrML.asp,2005 - 4 - 23/2007 - 03 - 08.

[22] ECAR Research Bulletin. A Digital Rights Management Ecosystem Model For The Education Community[OL]. http://www.contentguard.com/drmwhitepapers/DRM_Ecosystem_2004_05_10.pdf,2004 - 05 - 10/2007 - 02 - 24.

[23] DRM Standard Activities[OL]. http://www.contentguard.com/drmwhitepapers/DRM_standard_activities.pdf,2006 - 04 - 28/2007 - 02 - 25.

[24] Carl Gunter, Stephen Weeks, Andrew Wright. Models and languages for digital rights [A]. Proceedings of the 34th Annual Hawaii International Conference on System Sciences (HICSS-34)[C]. Washington: IEEE Computer Society,2001. 76 - 81.

[25] S K Warfield, M Kaus, F A Jolesz, R Kikinis. Adaptive, template moderated, spatially varying statistical classification[J]. Medical Image Analysis,2000,4(1):43 - 55.

[26] A J Goldstein, L D Harmon, A B Lesk. Identification of human faces[J]. Proceedings of the IEEE,1971,59(5):748 -

760.

[27] Y Zhu, T Tan, Y Wang. Biometric personal identification based on iris patterns[J]. Acta Automatica Sinica, 2002, 28(1):4 - 5.

[28] A M Eskicioglu. Multimedia security in group communications: recent progress in key management, authentication, and watermarking[J]. ACM Multimedia Systems Journal, Special Issue on Multimedia Security, 2003, 9(3):239 - 248

[29] Loyalka S, Hamoodi S Poiseuille Flow of a rarefied gas in a cylindrical tube: Solution of linearized Boltzmann equation[J]. Physics of Fluids A: Fluid Dynamics, 1990, 2(11):2061 - 2065.

[30] S Schneider, R Holloway. Using CSP for Protocol Analysis: The Needham-Schroeder Public-Key Protocol[M]. Royal Holloway: University of London, 1996, 3. 104 - 110.

[31] D Maughan, M Schertler, M Schneider, J Turner. Internet Security Association and Key Management Protocol [Z]. IETF RFC 2408. 1998. 248 - 253.

[32] I Chang, R Engel, D Kandlur, D Pendarakis, and D Saha. Key management for secure Internet multicast using Boolean function minimization techniques[A]. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings[C]. New York, USA: IEEE, 1999. 689 - 698.

[33] Stephen Mooney, Interoperability - Digital Rights Management and the Emerging EBook Environment[J]. D - Lib Magazine, 2001, 7(1):68 - 72.

[34] Microsoft Corporation. Microsoft DAS[OL]. http://www.microsoft.com/reader/default.mspx. 2004 - 03 - 25/2007 - 03 - 05.

[35] Q Liu, R Safavi-Naini, N P Sheppard. Digital rights management for content distribution[A]. Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003[C]. Australia: ACSW Frontiers, 2003. 49 - 58.

[36] Microsoft Corporation. Architecture of Windows Media Rights Manager[OL]. http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx, 2005 - 04 - 10/2007 - 02 - 23.

[37] ISMA, ISMA 1.0.1, 2004. Internet Streaming Media Alliance Implementation Specification, Version 1.0.1[S].

[38] Open Mobile Alliance (OMA). Open mobile alliance: DRM architecture draft version 2 [OL]. http://xml.coverpages.org/OMADRM - ARCHv202 - 20040315.pdf, 2004 - 03 - 15/2007 - 02 - 23.

[39] K Chorianopoulos, J Barria, T Regner, and J Pitt. Cross media digital rights management for online stores[A]. IEEE International Conference on Automated Production of Cross Media Content for Multi - Channel Distribution[C]. New York: IEEE, 2005. 257 - 260.

[40] P Bellini, P Nesi. An architecture of automating production of cross media content for multi-channel distribution[A]. First International Conference on Automated Production of Cross Media Content for Multi - Channel Distribution[C]. New York: IEEE, 2005. 9 - 11.

[41] P Kumar, G Sridhar, V Sridhar, R Gadh. DMW: A middleware for digital rights management in peer-to-peer networks, database and expert systems applications[A]. Proceedings on Sixteenth International Workshop [C]. New York: IEEE. 2005. 246 - 250.

[42] J P Andreaux, A Durand, T Furon, E Diehl. Copy protection system for digital home networks[J]. Signal Processing Magazine, 2004, 21(2):100 - 108.

[43] A Durand, E Diehl, J P Andreaux. Secure Exportation from a Global Copy Protection System to a Local Copy Protection System[P]. European: EP1552363, 2006.

[44] Koenen R H, Lacy J, Mackay Ml. Enabling security technologies for digital rights management[J]. IEEE Signal Processing, 2004, 92(6):883 - 897.

[45] Pramod A Jamkhedkar, Gregory L Heileman. DRM as a layered system[A]. Proceedings of the 4th ACM workshop on Digital rights management[C]. Washington: ACM Workshop on Digital Rights Management, 2004. 11 - 24.

[46] Rump N Can digital rights management be standardized[J]. IEEE Signal Processing, 2004, 21(2):63 - 70.

[47] D Amdur, InterTrust Challenges IBM digital content metering [J]. Report on Electronic Commerce, 1996, 23(15):16 - 18.

[48] Macq B DittmannJ, Delp EJ. Benchmarking of image watermarking algorithms for digital rights management[J]. IEEE Signal Processing, 2004, 92(6):971 - 984.

[49] Fabien A P Petitcolas, Ross J Anderson, Markus G. Kuhn. Information hiding—A survey[J]. Proceedings of the IEEE, 1999, 87(7):1062 - 1078.

作者简介:

范科峰　男,博士生,中国电子学会高级会员,主持国家标准化委员会、信息产业部电子行业标准研究项目,参与国家自然科学基金项目、信息产业部电子发展基金、北京市教委等科研项目. 已发表学术论文 20 余篇,目前的研究方向:数字版权保护技术与标准化等.
E-mail: fankf@126.com

莫　玮　男,博士,教授,博士生导师,IEEE 高级会员,全国电子测量仪器标准化技术委员会主任委员,中国电子学会学术委员会委员和电子测量学会副主任,曾主持完成国家发展改革委员会专项、国家 863 项目、国家自然科学基金项目、信息产业部、国防等多项科研项目. 目前的研究方向:数字版权保护,智能信息处理与测试技术等. E-mail: kf_fan@163.com