

DRM 中流媒体认证的研究与实现

周 岩, 杨宗凯, 刘清堂, 吴 砥
(华中科技大学 电子与信息工程系, 湖北 武汉 430074)

摘 要: 结合现阶段网络应用中流媒体认证技术的实际应用情况和新一代数字版权管理(DRM) 技术, 提出了一个流媒体数字版权认证系统的具体实现方案, 并最终实现了基于该方案的流媒体认证系统。该系统为基于网络服务的流媒体 DRM 系统的最终实现提供了必要的保证。
关键词: DRM; 流媒体; 数字版权; 许可证; 网络服务
中图法分类号: TP393. 09 文献标识码: A 文章编号: 1001-3695(2005) 06-0103-02

Research and Realization of Streaming Media's Recognition in DRM

ZHOU Yan, YANG Zong-kai, LIU Qing-tang, WU Di
(Dept. of Electronic & Information Engineering, Huazhong University of Science & Technology, Wuhan Hubei 430074, China)

Abstract: Combining the actual application situation of the current stream license technology and the new second-generation of DRM technology, and then poses a concrete scheme for the digital right license system. What's more, it realizes the streaming media license system finally according to the scheme. The system offers the necessary guarantee for the final realization of the streaming media DRM system which based on Web service.
Key words: DRM; Streaming Media; Digital Rights; License; Web Service

流媒体是当今新兴起来的一种网络多媒体形式。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。流媒体的出现极大地推动了网上远程教育、电子商务、网上视频点播等技术的飞速发展。随着流媒体应用的日益广阔, 其版权上的问题也就日趋凸显出来。流媒体内容被肆意地盗用、传播, 而内容的所有者以及创作者的正当权益却没有得到应有的保护。随着这些问题带来的负作用日益严重, 当今已经有众多的知名公司和组织投入到了结合数字版权管理(Digital Rights Management , DRM) 技术的受保护内容传播系统的相关研究与开发上来。如 Microsoft, IBM, RealNetworks 以及 SONY 等公司, 这些公司主要从事结合 DRM 技术的整个传播系统以及其组件的开发; MPAA(Motion Picture Association of America) 和 SDMI(Secure Digital Music Initiative) 等组织机构则着眼于发展一些适应特别要求的 DRM 系统, 如 DVD 拷贝的保护以及数字音乐传播的保护。可见 DRM 技术已成为当今网络技术发展的热点之一。

1 流媒体认证系统的设计

第一代 DRM 技术主要集中在资源使用的安全性和加密, 即加密内容和限制内容的发布, 使只有那些购买内容的人才可使用。但这不能有效地处理实时的、更加广泛的 DRM。现今发展的新一代 DRM 技术则覆盖了描述、鉴定、交易、维护、监控和追踪有形或无形资产的各种方式的版权使用形式。新一代 DRM 系统的设计和实施需要考虑两个关键的体系结构, 即功能结构和信息结构。功能结构是提供端到端的 DRM 系统高层模块和组件。信息结构是 DRM 系统包括实体及实体间

的关系。需要强调一点的是, DRM 是“权利的数字化管理”而不是“数字化权利的管理”, 即 DRM 管理的是各种权利, 而不仅仅是管理对数字化内容的许可权。

1.1 流媒体 DRM 系统概述

根据 DRM 系统的功能结构和信息结构, 结合当今流媒体网络版权管理的实际情况, 我们设计实现了一套基于 DRM 技术的流媒体数字版权管理系统, 根据具体功能的不同, 该系统分为三个子系统: 流媒体认证、流媒体编码加密和网上电子交易平台。三个子系统相辅相成, 有效地实现了流媒体的版权管理。

1.2 流媒体认证系统的作用与功能

在整个流媒体 DRM 系统中最为核心的部分便是流媒体认证子系统。流媒体编码加密子系统与网上电子交易平台子系统其实都是为认证子系统提供必要认证信息, 而最终控制流媒体的版权管理则是由流媒体认证子系统来完成。编码加密子系统首先将需要受管理的流媒体按照一定编码规则进行加密, 同时将加密信息如: 内容 ID(区分流媒体的唯一标志)、Key ID(密码编号) 等导入数据库中; 电子交易平台则是将用户的对加密流媒体的申请购买信息以及用户信息存入到数据库中。当用户播放受保护的流媒体文件时, 便会通过网络向认证系统申请播放的许可证, 而认证系统通过数据库的所有存放信息以及获得的用户信息, 对用户权限进行动态的管理, 并将管理信息存入数据库中, 进而实现对流媒体版权的广泛管理(图 1)。

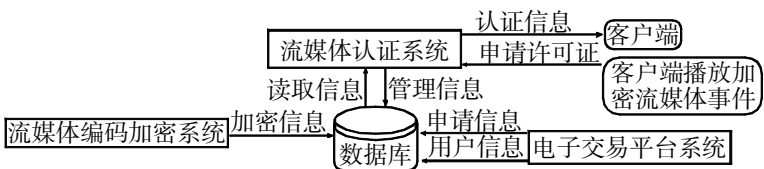


图 1 流媒体 DRM 系统结构图

正是通过流媒体认证系统对使用用户权利有效动态地管理,实时地响应用户的申请,并安全可靠地反馈申请许可,最终实现了整个 DRM 系统对流媒体的监控以及其用户所有的使用形式的追踪管理,从而使整个流媒体 DRM 系统具有了新一代 DRM 系统的重要特性与功能。流媒体认证系统主要实现以下四种功能:

- (1) 当播放受保护流媒体文件或者申请其播放许可证时,可通过网络对使用用户、使用设备来进行认证,并对用户的身份进行有效性判断;
- (2) 可动态地对用户的权限进行有效管理,并可实现对用户使用形式的监控与追踪;
- (3) 可实时记录合理有效用户对流媒体文件的申请、播放等操作并将其存入系统数据库,以方便管理员通过 Web 管理平台进行日后的系统管理与维护工作;
- (4) 可以根据合法用户的不同需求,向用户发送具有与其需求相符的许可证。

1.3 流媒体认证的过程

流媒体的认证过程实质上就是客户端与认证服务器端基于网络服务技术进行的信息交互的过程,如图 2 所示。

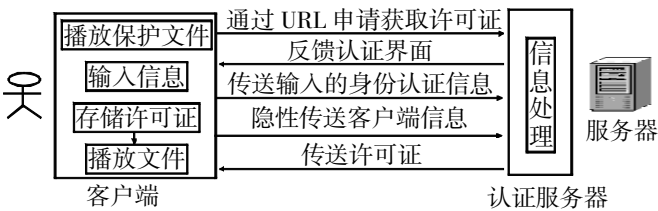


图 2 流媒体认证过程器图

当用户播放受保护流媒体文件时,客户端会通过流媒体中的 URL 信息,连接上认证服务器,同时发送获取许可证的请求信息 Challenge。服务器接收到信息后,便会向客户端反馈回一个认证页面。用户只需要在认证页面中输入其身份认证信息即用户名、密码等(在电子交易平台中获得),并将其提交,同时客户端会隐性传送客户端多种信息。服务器端通过对获得信息的处理,并根据数据库中保存的用户信息,来判断用户的合法性,通过后便会传送相应的许可证到客户端。客户端只需要存储此许可证,即可根据许可证设置的权限来进行播放了。

1.4 流媒体认证实现的原理

在流媒体认证过程中,服务器端接收客户端发送信息后,如何通过对信息的处理来完成对用户的身份认证和生成播放许可证是整个认证过程的关键技术。在服务器端接收到客户端发送的所有信息后,服务器会进行解析信息的工作,从所得信息中获取流媒体文件的密码编号、内容编号和用户信息。结合数据库分析用户信息判断其是否为合法用户,非法用户则不进行许可证生成的操作,并向客户端返回失败信息。确认身份之后,服务器会根据内容编号与用户信息以及数据库中的信息生成权限对象;根据密码编号和数据库信息产生密钥。最后服务器会依据密码编号、密钥、权限对象、客户端信息等创建签发用户指定播放的流媒体文件的许可证,从而完成整个流媒体认证过程。认证实现的基本原理如图 3 所示。

2 流媒体认证系统的实现

流媒体认证系统是建立在开放的标准体系上,允许不同的客户端来使用其提供的服务,这也就为整个流媒体 DRM 系统

提供了很强的扩展性。而且本认证系统提供的认证服务非常灵活,可以适应多种不同的认证方式的认证需求。

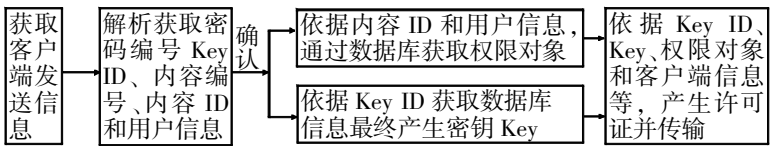


图 3 流媒体认证实现原理图

- (1) 文件播放认证方式。该方式是指当用户播放文件时自动到指定的认证服务器获取许可证,并需要用户身份和密码信息进行认证。认证后,则认证服务器自动传输许可证并存储在用户机器上。该模式一般用于网上视频点播等。
- (2) 单个文件许可证预传输方式。该方式是指用户没有播放文件,而直接通过用户身份和密码认证,以及提供必要的产品标志符获取许可证的方法。认证后,则认证服务器自动传输许可证并存储在用户机器上。该模式一般用于用户已经获得产品,但没有许可证的情况。
- (3) 批量文件许可证预传输方式。该方式是指用户没有播放文件,而直接通过用户身份和密码认证获取批量文件的许可证的方法。认证后,则认证服务器自动传输用户选择的所有媒体文件播放权利许可证存储在用户机器上。该模式一般用于光盘、课件或网络课程等含大量的媒体文件的情况。
- (4) 文件播放许可证默认方式。该方式是指当用户播放文件时自动到指定的认证服务器获取许可证,不需要输入认证信息,认证服务器会自动传输许可证并存储在用户机器上。该模式一般用于样品预览,播放次数有限。

认证系统通过实现以上四种认证方式,也就使得流媒体 DRM 系统可以建立在一个基于网络服务上的更为灵活的版权管理模式之上。而且本认证系统提供了友好的人性化界面,这样在一定程度上提高了系统的可操作性。认证系统用户信息输入界面如图 4 所示,认证系统许可证发放信息提示界面如图 5 所示。



图 4 认证系统用户信息输入界面



图 5 认证系统许可证发放信息提示界面

3 结论

本文通过对 DRM 中流媒体认证的研究,实(下转第 107 页)

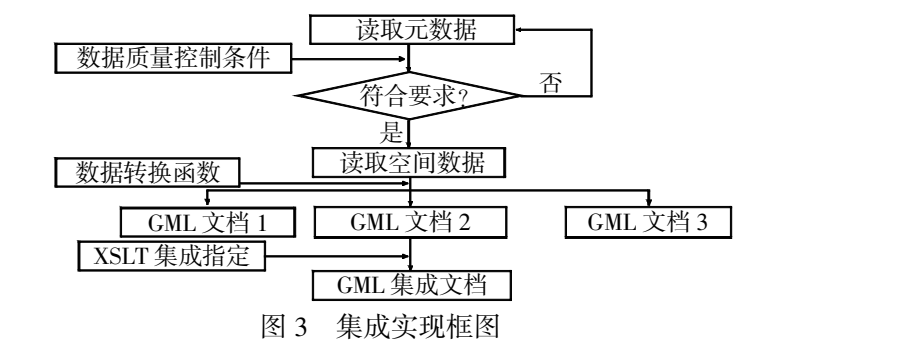


图 3 集成实现框图

3 模型运行结果

当前 GIS 系统使用的空间数据交换格式主要有: ESRI 公司的 Arc/Info Coverage, Shape Files, E00 格式; MapInfo 公司的 MIF 格式; Intergraph 公司的 DGN 等^[1]。本文选用 Arc/Info Shape Files 和 MapInfo 的 MIF 作为实验数据的格式, 利用上述模型和实现原理, 用 VB 语言编程实现了它们到 GML 之间的转换并利用 XML 的 XSLT 技术完成了两者之间的集成。由于 GML 的数据和表达, 目前还没有支持 GML 显示的控件, 而 SVG(可伸缩矢量标记) 与 GML 同属于 XML 体系, 文本式的灵活格式使得它适合于地图、统计图表等文字综合应用的领域, 同时由于体积小、可缩放等优点在网络上也十分流行^[8]。为了检验集成效果, 在实验中将 GML 集成文档转换成 SVG 格式在 IE6.0 浏览器中得到了显示结果。

MapInfo 编辑环境中的实验地图, 包括面状实体(图 4(a)); ArcMap 编辑环境中的实验地图, 包括点状实体和线状实体(图 4(b))。

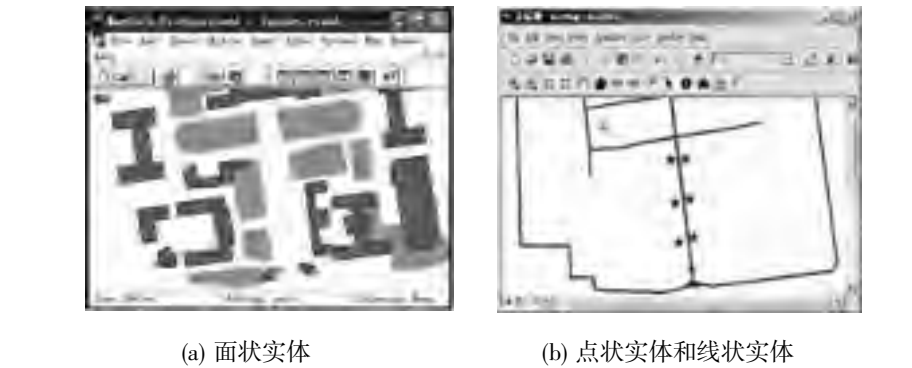


图 4 在 MapInfo 和 ArcInfo 中显示的地图

运用本模型将图 4(a) 中的面元数据与图 4(b) 中的点元、线元数据集成为统一的地理数据在 IE 浏览器中的显示效果如图 5 所示。从试验的结果可以看出, GML 在解决多源空间数据中是一种切实可行的技术, 本文设计的模型是基本有效的。



图 5 IE 中 SVG 表示的集成地图

4 结束语

GML 采用简单的基于文本的地理特征编码, 使地理信息的传输和存储与其可视化分离开来, 不受平台、语言的限制, 在各异构数据源中建立起一个统一的数据接口标准, 为实现地理空间数据的开放式表达和空数据信息的共享和重用提供了一个工具。

参考文献:

[1] 黄杏元, 马劲松, 汤勤. 地理信息系统概论(第 2 版)[M]. 北京: 高等教育出版社, 2001. 87-93.

[2] 宋关福, 钟耳顺, 等. 多源空间数据无缝集成研究[J]. 地理科学进展, 2000, 19(2): 110-115.

[3] 王继周, 付俊娥, 李成名, 等. 基于 GML 的网络 GIS 空间数据交互研究[J]. 计算机应用研究, 2004, 21(1): 64-66.

[4] Geography Markup Language (GML) [EB/OL]. <http://www.open-gis.net/gml>, 2004-06.

[5] 周文生, 毛锋, 等. Web 环境下地理空间数据的开放式表达体系研究[J]. 武汉大学学报(信息科学版), 2004, 29(1): 43-47.

[6] 李军, 费川云. 地球空间数据集成研究概况[J]. 地理科学进展, 2000, 19(3): 204-211.

[7] 飞天工作组. XSLT 和 XPath-XML 转换指南[M]. 北京: 机械工业出版社, 2002.

[8] 刘啸, 毕永年. 基于 XML 的 SVG 应用指南[M]. 北京: 北京科海集团公司, 2001.

作者简介:

旷建中(1974-), 男, 湖南衡山人, 硕士研究生, 研究方向为空间数据集成及 GIS 软件开发等; 马劲松(1969-), 男, 江苏南京人, 南京大学城市与资源学系 GIS 与遥感教研室主任, 副教授, 博士, 研究方向为 GIS 技术与 GIS 软件开发; 蒋民锋(1978-), 男, 江西新余人, 硕士研究生, 研究方向为网络 GIS 及 GIS 技术。

(上接第 104 页) 现了流媒体认证系统。本系统基于网络服务技术, 结合新一代 DRM 系统的设计理念, 为流媒体 DRM 系统提供了灵活多样的认证服务, 同时也为流媒体 DRM 系统日后的扩展提供了先决条件, 从而较好地适应了当今网络流媒体版权管理的需求。该系统可以在杜绝利用网络和计算机非法复制、拷贝、传播流媒体产品的应用中发挥作用, 具有较好的应用发展前景。

参考文献:

[1] O Waller, G Jones, T Whiteley, *et al.* Securing the Delivery of Digital Content over the Internet[J]. Electronics & Communication Engineering Journal, 2002, (10): 239-248.

[2] Sai Ho Kwok. Digital Rights Management for the On-line Music Business[J]. ACM SIGecom Exchanges, 2002, 3(3): 17-24.

[3] Frank Hartung, Friedhelm Ramme, Erisson Research. Digital

Rights Management and Watermarking of Multimedia Content for M-Commerce Applications[J]. IEEE Communications Magazine, 2000, (11): 78-84.

[4] Qiong Liu, Reihaneh Safavi-Naini, Nicholas Paul Sheppard. Digital Rights Management for Content Distribution[Z]. Australasian Information Security Workshop, 2003.

[5] 张福学. 数字版权管理系统的功能和信息结构分析[J]. 情报杂志, 2002, (6): 26-27.

[6] Kim Zwollo. Digital Document Delivery and Digital Rights Management[J]. Information Services & Use, 2001, (21): 9-11.

作者简介:

周岩(1981-), 男, 硕士研究生, 主要研究方向为网络教育; 杨宗凯, 男, 教授, 博士生导师, 主要研究方向为网络教育、电子商务、智能信号处理与应用、宽带网络通信技术; 刘清堂, 男, 博士研究生, 主要研究方向为网络教育; 吴砥, 男, 博士研究生, 主要研究方向为网络教育。