

文章编号:1001-9081(2005)12-2805-03

一种流媒体数字版权管理系统的实现与设计

王全文,向文

(华中科技大学信息与系统技术研究所,湖北 武汉 430074)

(hustwqw@163.com)

摘要:针对当前流媒体数字版权管理(Digital Rights Management, DRM)的现状,提出了一种基于三层密钥机制的流媒体 DRM 方案。介绍了该系统框架并作了安全性分析,然后对系统的实现方案作了详细的叙述。

关键词:流媒体;数字版权管理;智能卡;DirectShow

中图分类号: TP37 **文献标识码:**A

Design and implementation of DRM system for streaming media

WANG Quan-wen, XIANG Wen

(Institute of Information and System Technology, Huazhong University of Science and Technology, Wuhan Hubei 430074, China)

Abstract: To the current situation of streaming media DRM, a streaming media DRM system based on the three-layer architecture of key was presented. The whole system model was introduced and its security was discussed, and then implementation of the system was described in detail.

Key words: streaming media; Digital Rights Management(DRM); IC; DirectShow

0 引言

流媒体具有实时点播和在线播放等特点,因此对于流媒体的数字版权管理(Digital Rights Management, DRM)技术也不同于传统的版权保护方法,流媒体 DRM 具有实用性、针对性等特点。

目前,国内的一些 DRM 集成商基本上是在微软的 Windows Media DRM 技术基础上制作 DRM 产品。他们或直接应用 DRM 技术,或在流媒体加密技术中再融入第三方的加密技术。这种方法虽然方便、通用,但其技术核心并未公开,并不能在加密、解密等方面做得很彻底。

本文介绍了一种安全的流媒体 DRM 系统的设计和实现,提出了一种基于三层密钥管理思想的实时视频安全传输模式。

1 DRM 系统框架

1.1 DRM 框架模型

我们设计的 DRM 系统主要包括四大部分:用户管理系统、媒体授权系统、媒体加密处理及分发系统和客户端。如图 1 所示。

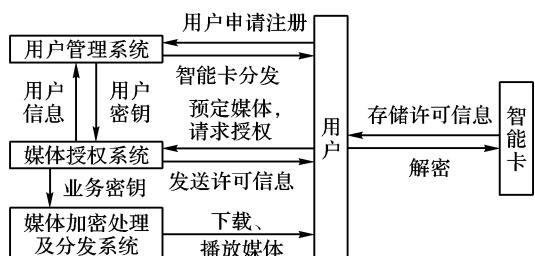


图 1 三层密钥机制流媒体 DRM 框架模型

在这个 DRM 模型中,用户通过网络向用户管理系统申

请用户 ID, 用户管理系统为该用户产生一对非对称密钥,即用户密钥 UK,其私钥存储在智能卡中分发给用户,公钥由用户管理系统保管;当用户向服务器请求媒体播放时,首先要向媒体授权系统请求播放许可,媒体授权系统将用户信息提交给用户管理系统;用户管理系统验证用户的合法性,如果验证为合法则将该用户的 UK 的公钥反馈给媒体授权系统;媒体授权系统将用户所预定的媒体信息以及该业务的业务密钥 SK 发给媒体加密处理及分发系统,同时媒体授权系统将 SK 用 UK 的公钥加密制作成播放许可信息发送给用户;媒体加密处理及分发系统是本 DRM 系统的一个核心部分,它包括一个产生流式密码^[1] CW(Control word)的控制字发生器(随机序列发生器),在这个子系统中,用 CW 加密媒体源,用 SK 来加密 CW 产生 ECM(Entitlement Control Message),然后将 ECM 与用 CW 加密后的媒体进行复用,形成供下载的流媒体数据流;客户端将接收到的许可证信息存储到智能卡中,用智能卡解密得到 CW;最后用 CW 解密媒体数据得到可以播放的源媒体流。

1.2 系统安全性分析

该 DRM 系统的安全性主要依靠三层密钥机制^[2]的安全性,现在就其安全性来进行分析。

1) 操作密钥即控制字 CW

控制字 CW 是该系统中一个至关重要的信息,它被用作 DRM 系统中媒体加密解密的直接密钥。随机序列发生器的初始字序列发生器输出的随机字被用来对码流数据进行加解密操作,在每个控制字的有效区间内加密端和解密端的随机序列发生器都以该控制字为初始种子字来同步产生每一瞬间码流加密的密钥。由于流媒体码流的数据量很大,如果一个控制字被长时间用来对码流进行操作势必会给攻击者提供大量的分析样本,这难免影响到系统的安全性,因此该系统的控

收稿日期:2005-06-20;修订日期:2005-08-25

作者简介:王全文(1981-),男,河南光山人,硕士研究生,主要研究方向:网络与信息安全; 向文(1965-),男,江西景德镇人,教授,主要研究方向:电子商务与信息安全、嵌入式系统及应用。

制字都会几秒钟或者十几秒改变一次。很显然,控制字序列的随机性越高攻击者就越难进行攻击,理想的控制字发生器莫过于真随机序列发生器,这种发生器无论运行多久攻击者都不可能通过以前所有的控制字来推测下一次的控制字。事实上,目前通过计算机或者微处理器所进行的数学运算无法产生真正意义上的随机数,它们所产生的序列不论有多少种状态,但仍然是有限的并且是循环的,因此,在该 DRM 系统中并不必得到一个真正的随机序列,只要它的循环周期足够长就可满足系统的需要。

2) 业务密钥 SK

业务密钥 SK 是用来对 CW 进行加密产生授权控制信息 ECM 的。SK 的更新速度不必很快,该系统中的 SK 可以是一个月更新一次,发送端可根据不同媒体源授权情况的改变来调整 SK。每个媒体源可采用不同的 SK,这使得灵活多样的授权方式成为可能。

3) 用户密钥 UK

用户密钥 UK 是一对非对称密钥,公钥存储在服务端的用户信息管理系统中,而私钥被存储在用户所拥有的智能卡的中。因为智能卡本身的防篡改性,避免了用户与密钥的直接交互,保证了用户私钥的安全。

2 系统实现

2.1 服务端实现

本 DRM 系统服务端有三部分组成:用户管理系统、媒体授权系统和媒体加密处理及分发系统。它们各自任务如下:

用户管理系统:主要负责用户的注册、认证、智能卡分发、数据更新。

媒体授权系统:制作播放许可信息。

媒体加密处理及分发系统:加密媒体源,制作可供下载的流媒体数据流。

1) 用户管理系统

用户管理系统是一个数据库系统,存放着用户信息、媒体信息。通过用户管理系统为新注册的用户提供一个密钥文件,其中包含用户的个人信息(用户 ID、所拥有智能卡的 ID、预定媒体编号)、经加密的用户密钥 UK(RSA 密钥对)以及有效期限。

2) 媒体授权系统

媒体授权系统的核心是一个 RSA 加密程序,用用户密钥 UK 的公钥加密业务密钥 SK。

3) 媒体加密处理及分发系统

媒体加密处理及分发系统是服务端的核心部分,在这里将详细介绍该子系统的实现。图 2 描述的是加密处理及分发系统的主要部分。

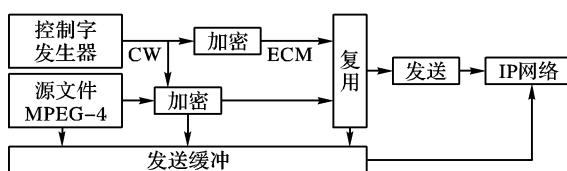


图 2 媒体加密处理及分发系统

在这个系统中,要进行 MPEG-4 数据的流化、加密和发送。对文件的加密应该以数据包为单位进行。发送模块中的发送线程每次将一个数据包从文件缓冲区读到发送缓冲区中,文件的加密过程和复用过程以及发送过程共享该缓冲区。在服务器端和客户端启动数据传输后,就开始了对数据包的

加密、复用和发送,直至播放完毕。首先是将文件的数据包读入发送缓冲区,同时使用控制字发生器产生的 CW 在该缓冲区中加密其中的明文文件,得到密文文件同样写入该缓冲区,然后在将加密 CW 读到该缓冲区中并与该缓冲区中的密文文件进行复用,最后再由发送模块将它传至 IP 网络。

①MPEG-4 码流^[3] 加密方式

在大多数的多媒体 DRM 系统加密媒体数据时不考虑媒体内容的格式,比如说,加密整个媒体数据。然而,这种加密方式并不适合于流媒体内容,因为流媒体服务器不能传输这种改变了媒体本身数据格式的内容。我们采取的加密方式如图 3 所示。Safe header 部分包括 VOP(Video Object Plane)初始码和帧类型信息,这个部分不被加密。Tail 也不被加密,因为它的长度一般是小于 8 的。如果我们对 Tail 部分加密,那么它的长度将会改变,这就改变了整个采样的长度。除了 Tail 部分的采样数据都需要加密。

MP4 Video Sample header		MP4 Video Sample body
Safe header	Encrypted data	Tail
固定尺寸	可变尺寸(CW 字长的整倍数)	小于CW 长度

图 3 MPEG-4 视频采样加密

这样的加密还有一种好处,就是增强了数据安全性。因为这些头数据部分有一定规律的特征无疑将给破译者提供最佳的攻击样本,这会大大降低系统的健壮性。

②ECM 的结构

ECM 信息是插入到媒体数据流中以私有数据的形式发送给用户的。每条 ECM 信息基本上由同步参数字段、控制字字段以及校验字字段组成。同步、参数字段用于标识一条 ECM 信息的开始,此字段不需要加密;控制字字段实际上包含的是加密后的控制字 CW,得到授权的用户可以从该字段解密出控制字;校验字段用于检验前面接收到的两个字段是否存在错误。

我们选取对称加密算法 DES 算法加密 CW,此算法的密钥即业务密钥 SK。

③ECM 与加密文件复用

在研究项目中,我们采用软件实现复用器来实现 ECM 与媒体文件的复用^[4]。

2.2 客户端实现

客户端应用程序主要由网络接收模块、解复用及解密模块和播放模块。如图 4 所示:接收模块把从 IP 网络收到的数据包读到接收缓冲区;解复用器将 ECM 信息从该缓冲区中的数据包中分离出来,用智能卡的解密;除去 ECM 信息的数据包被读到缓冲队列中,用 CW 将其解密;最后播放模块从缓冲队列中取得数据得以播放。

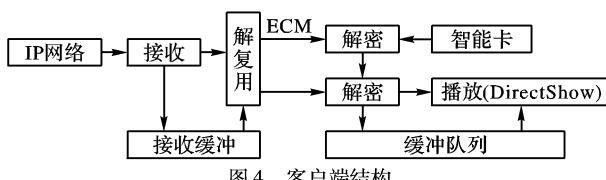


图 4 客户端结构

在上面所示的客户端结构图中,用到了两个辅助技术:智能卡^[5] 和 DirectShow 技术^[6]。

1) 智能卡

在客户端,智能卡担当解密出 CW 的重要角色。智能卡存储器中存有用户密钥以及播放许可信息,首先用这个密钥解密播放许可信息得到业务密钥;然后业务密钥解密 ECM 信

息就得到控制字 CW。

对业务密钥和控制字的解密都是在智能卡中进行的,而且许可证同智能卡绑定在一起,没有智能卡,便无法播放流媒体。即使非法用户得到了下载的数据流,因为没有智能卡以及相应的许可证,仍然无法使用流媒体。所以智能卡是我们 DRM 系统中的关键一环。

2) DirectShow 技术

DirectShow 为开发人员提供了 Direct Show SDK 工具, 使用 SDK 编程可以大大简化流媒体数据的处理过程。DirectShow 提供的是一种开放式的开发环境, 可以根据需要定制自己的组件。DirectShow 系统使用一种叫 Filter Graph 的模型来管理整个数据流的处理过程; 参与数据处理的各个功能模块叫做 Filter; 各个 Filter 在 Filter Graph 中按一定的顺序连接成一条“流水线”协同工作。按照功能来分, Filter 大致分为三类: Source Filters、Transform Filters 和 Rendering Filters。Source Filters 主要负责取得数据, 然后将数据往下传输; Transform Filters 主要负责数据的格式转换、传输; Rendering Filters 主要负责数据的最终去向, 我们可以将数据送给声卡、显卡进行多媒体的演示, 也可以输出到文件进行存储。

在我们的 DirectShow 播放模块中, 首先建立起一个 Source Filters, 用于异步读取从网络过来的数据包, 这个 Filter 是要自己开发的; 包含 MPEG-4 解码器的 Transform Filters 和用于播放的 Rendering Filters, 可以从现有资源获取。

2.3 IP 网络

IP 网络支持单播、组播、广播三种传输方式, 具有很强的灵活性, 同时支持双向数据传输, 很好地解决了上传通道的问

题, 因而可以适应更多的交互式应用。根据流媒体的特点, 采用 UDP 协议由发送端向接收端传送经加密复用的 MPEG-4 数据包。

3 结语

介绍了一种基于三层密钥机制的流媒体 DRM 系统的设计方案, 三层密钥机制本是数字电视 CAS(Conditional Access System) 中的加密体制, 安全性是得到肯定的, 借用它的基本思想设计了适用于 IP 网络的 DRM 系统。然后对该 DRM 系统的服务端及客户端的实现方案做了详细地描述, 不仅提出了一种独特的 MPEG-4 数据包的加密方式, 而且提出了一种安全的视频传输模式, 可以说它基本上是一个完善的 DRM 系统。

参考文献:

- [1] SCHNEIER B. Applied Cryptography, Second Edition : Protocols, Algorithms, and Source Code in C [M]. John Wiley & Sons, Inc., 1996.
- [2] YANG XW, ZHENG ZH. Key Distribution System for Digital Video Signal[A]. Proceedings of ICSP96[C]. 1996. 847 – 850.
- [3] ISO/IEC 14496-2, Coding of Audio-Visual Objects-Part 2: Visual [S]. 2001.
- [4] 苏凯雄, 郭里婷. 数字卫星电视接收技术[M]. 北京: 人民邮电出版社, 2002.
- [5] RANKL W, EFFING W. 智能卡的结构·功能·应用[M]. 北京: 电子工业出版社, 2001.
- [6] Microsoft. DirectX 9 0a SDK[CD]. 2003.

(上接第 2804 页)

灰度), 这时 M_{wav} 的值在 10 单位灰度左右。效果如图 5 所示。

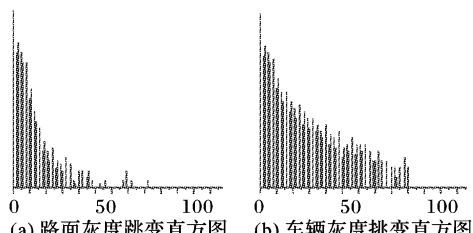


图 4 路面与车辆灰度跳变的直方图

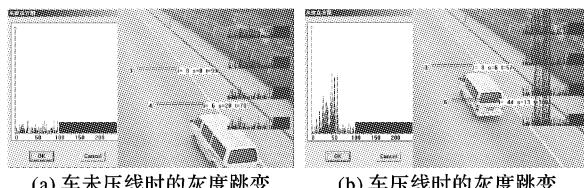


图 5 车未压线和车压线时的灰度跳变

图中曲线是检测区域的灰度跳变信号, 右侧是滤波阈值 M_{wav} 的高度。从图中可以看出设定 M_{wav} 的效果很明显, 无车时路面微小的纹理波动大都可以被滤除。对比之下车辆压线时的灰度跳变信号非常明显。实验结果表明, 采用本方法的虚拟线圈在白天可以达到 95% 的车辆检测率, 漏检率 5%, 由于路面噪音引起的误触发率 4%。

但它也有一定的局限性, 主要表现在以下几个方面: 1) 在帧频率较低时(如每秒钟只有 1、2 帧), 若车辆距离太近可能被认为是一辆车, 只产生一次触发信号。提高帧采集频率便可解决这个问题; 2) 线圈的选取最好选择单纯路面, 如

果线圈区域包括了非常明显的车道线, 那么背景纹理描述子的值会增加, 各等级的扩展系数 n 就应比选择单纯路面时要小, 漏检率和误检率都会有所增加; 3) 在光照变化时, 漏检率和误检率也会增加。在后两种情况下, 应配合其他的检测方法, 以提高系统鲁棒性。

4 结语

本文根据车辆图像比路面纹理变化丰富的特点, 通过统计经滤波的图像灰度跳变来计算纹理描绘子, 从而描述图像纹理特征, 将这种方法应用于虚拟线圈视频测速中, 并提出了相应的决策方法, 应用简便, 效果明显, 可以作为一种主要或辅助的虚拟线圈检测方法。

参考文献:

- [1] GONZALEZ RC, WOODS RE. Digital Image Processing[M]. Second Edition. BEIJING: Publishing House of Electronics Industry, 2003. 536 – 548.
- [2] 蔡平, 刘景堂, 阮秋琦. 复杂场景中基于统计模型检测运动物体的新方法研究[J]. 公安大学学报(自然科学版), 1998. 4, 3 – 11.
- [3] 吴祖林, 沈庆宏, 都思丹, 等. 背景提取基础上运动车辆视频检测[J]. 交通与计算机, 2003, 21(6): 18 – 20.
- [4] MICHALOPOULOS PG, JACOBSON RD, ANDERSON CA et al. Automatic incident detection through video image processing[J]. Traffic Engineering + Control, February 1993 Issue.
- [5] Autoscope. Video detection the atlanta experience[J]. Traffic Technology International. Dec '96/Jan '97 Issue.