第 32 卷 第 18 期 计 算 机 工 程 2006 年 9 月
Vol.32 № 18 Computer Engineering September 2006
·安全技术· 文章编号：1000—3428(2006)18—0160—03 文献标识码：A 中图分类号：TP309

一种新的基于三级加密的流媒体 DRM 模型

吴俊军，王 娟
（华中科技大学机械学院，武汉 430074）

摘 要：分析了流媒体数字版权保护（DRM）的一般框架及其存在的问题，结合流媒体的特点，提出了一种新的基于三级加密的流媒体 DRM 模型——时分变码流媒体 DRM。介绍了时分变码流媒体 DRM 的框架、流程，以及时分变码加密机制，并分析了时分变码流媒体 DRM 的特点。该模型具有很好的安全性、实时性和可升级性。

关键词：流媒体；数字版权保护；数字版权

A New Model for Streaming Media DRM Based on Triple Level Encryption

WU Junjun, WANG Juan
(College of Mechanism, Huangzhong University of Science and Technology, Wuhan 430074)

【Abstract】This paper discusses the general framework of existent streaming media digital rights management (DRM) and its deficiency, presents a new model for streaming media DRM by adapting to the property of streaming media. The new model is based on triple level encryption. The new model's framework, process flow and encryption mechanism are described. The new model's characteristic is analyzed and the new model is proved to be secure, real-time and upgradeable.

【Key words】 Streaming media; Digital rights management (DRM); Digital rights

流媒体是指在Internet/Intranet中使用流式传输技术的连续时基媒体[1]，如音频、视频或多媒体文件。它在播放前并不下载整个文件，只将开始部分内容存入内存，其他的数据流随时传送随时播放，大大缩短了用户的等待时间，节省了大量的磁盘空间。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。数字版权保护技术(Digital Rights Management, DRM)是保护数字版权的有效手段。结合流媒体实时性的特点，本文提出了一种新的基于三级加密的流媒体 DRM 模型——时分变码流媒体 DRM。

1 流媒体 DRM 一般框架

实现DRM主要有2种技术：加密技术和数字水印技术[2~4]。数字水印产品在应用方面还不成熟，容易被破坏或破解，而且数字水印方法只能在发现盗版后用于取证或追踪，不能事前防止盗版。所以目前流媒体DRM仍然采用比较成熟的加密技术，实现流媒体内容端到端的安全。主流的流媒体系统目前都已拥有了DRM的解决方案，如RealSystem的RMCS（RealSystem Media Commerce Suite）[5]、MediaService的MDRM(Microsoft Digital Rights Management)[6]等，它们都遵循流媒体版权保护的一般框架。

流媒体版权保护系统主要包括媒体拥有者及其制作服务器、数字媒体授权中心、媒体分发服务器和授权用户 4 大部分。其一般框架如图 1 所示。

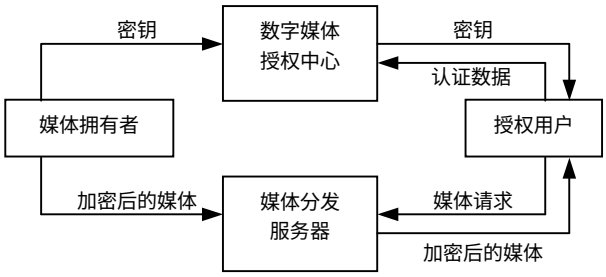

图 1 流媒体版权保护系统的一般框架

基于该框架建立的版权保护系统的运作过程如下[5~8]：

(1)系统建立数字媒体授权中心，保存数据的解密密钥，并对用户的身份进行认证和授权。

(2)媒体拥有者制作、编码、加密流媒体数据。

(3)媒体拥有者将加密后的数据发送到媒体分发服务器，同时将相应的解密密钥(可能与加密密钥不同)安全地发送给数字媒体授权中心进行安全存储。

(4)用户根据所请求的媒体分发服务器中媒体数据的相关信息到数字媒体授权中心进行用户认证。

(5)用户安全地从数字媒体授权中心获得解密密钥，并从媒体分发服务器获得所请求的媒体数据。

(6)用户使用解密密钥对媒体数据进行解密，然后以在线或下载方式收看。该一般框架只考虑了在服务器上的安全存储和密钥在传输过程的安全性，对版权的保护随着解密密钥

作者简介：吴俊军(1972—)，男，副教授，主研方向：智能卡，CIMS，CAD/CAM，网格制造，信息安全；王 娟，硕士

收稿日期：2005-09-09 **E-mail：**wjj@whty.com.cn

安全地发送到授权用户就停止了，没有保证媒体数据在播放过程中及播放结束后的安全性。

该一般框架对流媒体数据的加密是静态的、一次性的，它事先将流媒体数据加密、打包，存放在服务器上，没有充分利用流媒体流式传输的时基性特点。

2 时分变码流媒体 DRM 模型

为了更好地满足流媒体 DRM 的安全性、实时性，本文提出一种新的流媒体版权保护方法——时分变码流媒体 DRM。时分变码流媒体 DRM 框架如图 2 所示。

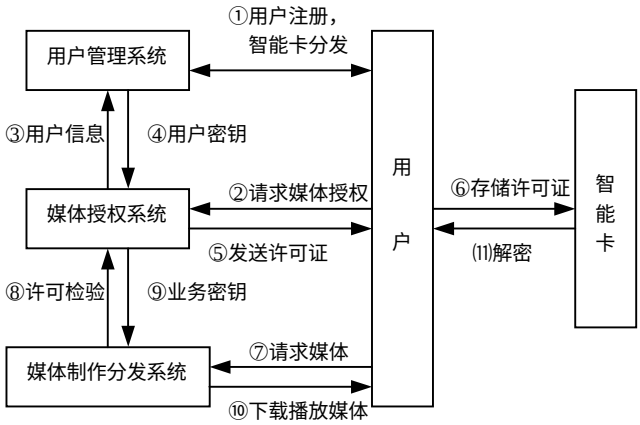

图 2 时分变码流媒体 DRM 框架

2.1 系统构成

时分变码流媒体 DRM 系统主要包括 4 大部分：用户管理系统，媒体授权系统，媒体制作分发系统和用户。各部分的主要任务是：

(1)用户管理系统：主要负责用户的注册、认证、智能卡发放和更新、记账收费等。

(2)媒体授权系统：产生业务密钥，从用户管理系统得到用户密钥，用用户密钥加密业务密钥，并连同使用权限一起产生许可证，发送给用户。

(3)媒体制作分发系统：产生控制字 CW(Control Word)，用 CW 加密流媒体数据产生加密数据流；从媒体授权系统得到业务密钥，用业务密钥加密 CW 产生授权控制信息 ECM（Entitlement Control Message）；将两种信息复用，形成用于下载的数据流。

(4)用户：使用智能卡保存自己的用户密钥；当收到许可证时，用智能卡存储许可证；当要播放流媒体时，必须使用智能卡解密流媒体。

2.2 系统流程

(1)用户向用户管理系统申请账户注册，注册成功后，用户管理系统产生一对非对称密钥，即用户密钥。私钥存储在智能卡中分发给用户，公钥存储在用户管理系统中。用户向媒体授权系统请求媒体权限。媒体授权系统将用户信息以及用户请求的媒体服务信息发送给用户管理系统。用户管理系统根据用户信息认证用户，根据用户请求的服务信息对该用户记账、收费，并将用户密钥发送给媒体授权系统。

(2)媒体授权系统产生业务密钥，用用户密钥加密业务密钥，根据用户请求的服务类型，产生许可证，把许可证发送给用户。

(3)用户接收许可证，将它存储在智能卡中。

(4)用户依据许可证信息向媒体制作分发系统请求下载媒体。

(5)媒体制作分发系统将用户的许可证信息发送给媒体授权系统检验。

(6)媒体授权系统检验许可证，将业务密钥发送给媒体制作分发系统。

(7)媒体制作分发系统产生控制字 CW，用 CW 加密流媒体，用业务密钥加密 CW 形成授权控制信息 ECM，把加密的流媒体和 ECM 信息流复用，形成供下载的流媒体数据流。用户下载流媒体数据，使用智能卡解密，实时播放流媒体。

同流媒体 DRM 一般框架相比较，时分变码流媒体 DRM 使用智能卡存储用户密钥和许可证，业务密钥和控制字的解密都在智能卡中进行，流媒体除了在播放中有一小部分以明文的形式在内存缓冲中存在，其余的时间总是以密文的形式存在，可以保证流媒体在播放中和播放后的安全。

流媒体具有实时性的特点，因此在传输时对流媒体实时加密是可行的。时分变码流媒体 DRM 对流媒体内容的加密，是用户请求媒体服务并得到流媒体使用许可证后，在下载流媒体时实时进行的。除了具有实时性，时分变码流媒体 DRM 对流媒体的加密还具有动态性，这是通过时分变码加密机制实现的。

3 时分变码流媒体 DRM 加密机制

时分变码流媒体 DRM 采用时分变码三级加密机制。从第 2 节已知，该加密机制用到 3 种密钥：控制字 CW，业务密钥和用户密钥。“时分变码”中的“码”是指密钥。所谓“时分变码”，是指在流媒体边加密边下载播放的过程中，控制字 CW 每隔 5s~10s 随机变化 1 次。

3.1 加密过程

在时分变码流媒体 DRM 系统中，流媒体内容发送端对流媒体的加密方式如图 3 所示。

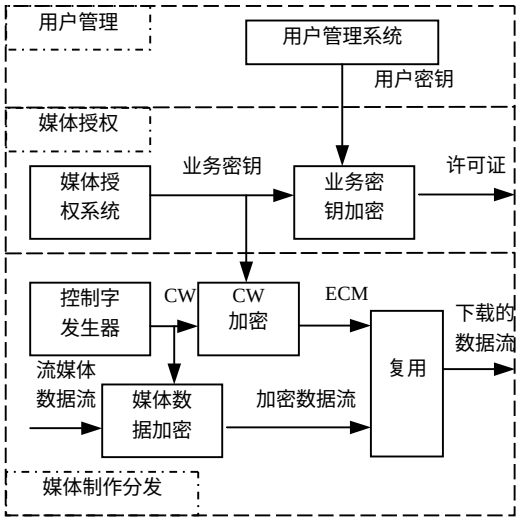

图 3 时分变码加密机制加密过程

用用户密钥加密业务密钥，并结合用户的使用权限，产生使用许可证。用 CW 加密流媒体数据流；用业务密钥加密 CW，产生 ECM 信息；将加密的流媒体数据流和 ECM 信息复用，形成用于用户下载的数据流。

3.2 解密过程

用户端对流媒体的解密过程如图 4 所示。

(1)用户首先要得到使用许可证，并将其存储在智能卡中。

(2)当下载流媒体并播放时，先将下载的数据流解复用，得到 ECM 信息和用 CW 加密的流媒体数据流，ECM 信息被发送到智能卡中。

(3)智能卡先用用户密钥从许可证中解密出业务密钥，然后用业务密钥从 ECM 信息中解密出 CW，并将 CW 输出。

(4)用 CW 解密加密数据流，实现流媒体的播放。

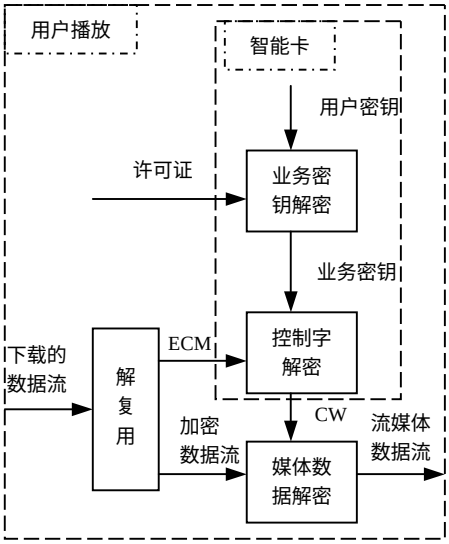

图 4 时分变码加密机制解密过程

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。如果用户请求的服务不是只播放一次的话，它可以将下载的媒体内容保存下来，以后每次播放时，都要用智能卡来解密，同时智能卡中的许可证也将随之改变，当使用权限到期，许可证将自动删除，从而实现流媒体的版权保护。

3.3 加密算法及密钥更新

时分变码加密机制使用的加密算法，其安全性是逐级升高的。控制字 CW 对流媒体数据的加密采用序列密码加密算法；业务密钥对控制字的加密采用对称分组加密算法；用户密钥对业务密钥的加密采用公钥加密算法。根据所用加密算法的不同，3 种密钥的产生和更新也不同。

(1)控制字 CW：用控制字发生器随机产生，每隔 5s~10s 更新一次。控制字 CW 变化时，ECM 信息也随之变化。

(2)业务密钥：用户每次请求媒体授权时随机产生。一旦用户对该媒体的使用权限到期，业务密钥也随之过期，即每次流媒体服务的周期就是相应的业务密钥的生命周期。

(3)用户密钥：用户向用户管理系统注册时产生。它是一对公钥密钥，公钥保存在用户管理系统中，私钥保存在用户的智能卡中，随智能卡分发给用户。智能卡的有效期即为用户密钥的生命周期，一般比较长。

4 时分变码流媒体 DRM 的特点分析

流媒体具有实时性，而DRM系统需要具有安全性、可升级性[4,7~9]，因此流媒体DRM需具有安全性、实时性、可升级性等特点。下面从这 3 方面分析时分变码流媒体DRM。

4.1 安全性

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。

在时分变码流媒体 DRM 中，CW 是动态变化的，每隔 5s~10s 变换一次，即使一个控制字被破解，也只是破解了流媒体的一个小片断，对于整个流媒体来说是杯水车薪。业务密钥是跟每次的服务相关的，对于同一个流媒体，每个用户、每次服务的业务密钥都不同，如果业务密钥被破解，其他用户的业务密钥并不受影响。用户密钥是公钥密码，破解的难度比较大。因此，3 种密钥的生命周期，保证了整个系统在时间上的安全性。

时分变码流媒体 DRM 使用智能卡存储用户密钥和许可证，并使用智能卡实现对业务密钥和控制字的解密，控制字对流媒体的解密通过一个解密模块来实现。这种方式可以保证流媒体在下载、播放和播放后的安全。随着技术发展，对流媒体的解密也可能会在智能卡中进行，这样整个解密过程对用户都是透明的，安全性更高。

4.2 实时性

时分变码流媒体DRM用序列密码对流媒体数据进行加密，序列密码加密简单快速、实时性强[7]，正好满足流媒体实时性的要求。CW的数据量不大，而且对称加密算法速度比较快，因此ECM信息的产生和解密所花费的时间不会影响流媒体的实时性。公钥加密算法比较慢，但是在流媒体播放时，对业务密钥的解密仅进行一次，也不会影响流媒体的实时性。

4.3 可升级性

时分变码流媒体 DRM 的升级主要是通过密钥发生器和密码算法的升级来实现的。当密钥发生器被破解或密码算法不能满足安全性要求时，可以选用更高级的密钥发生器和更安全的密码算法来升级系统。同时，用户只需更换智能卡、下载升级的解密模块即可。

5 结束语

本文提出了流媒体 DRM 的一种新方案——时分变码流媒体 DRM，该方案同流媒体的特点相适应，具有较好的安全性、实时性、可升级性。该方案采用时分变码加密机制，可以满足流媒体版权保护在传输、播放和播放后的安全性。随着加密算法速度的提高和智能卡安全性的加强，本方案的实现将更具优势。

参考文献

1 陈　红, 贾学东, 平西建. 流媒体 DRM 技术分析[J]. 信息工程大学学报, 2004, 5(1):70-72.

2 Torrubia A, Mora F J, Marti L. Cryptography Regulations for E-commerce and Digital Rights Management[J]. Computers & Security, 2001, 20(8): 724-738.

3 Jonker W, Linnartz J P. Digital Rights Management in Consumer Electronics Products[J]. Signal Processing Magazine, 2004, 21(2): 82-91.

4 Eskicioglu A M, Delp E J. An Overview of Multimedia Content Protection in Consumer Electronics Devices[J]. Signal Processing: Image Communication, 2001, 16(7): 681-699.

5 RealSystem Media Commerce Suite Technical White Paper[Z]. http://docs.real.com/docs/drm/DRM_WP1.pdf.

6 Architecture of Windows Media Rights Manager[Z]. http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx.

7 Hwang S O, Yoon K S, Jun K P. Modeling and Implementation of Digital Rights[J]. The Journal of Systems and Software, 2004, 73(3): 533-549.

8 Eskicioglu A M, Town J, Delp E J. Security of Digital Entertainment Content from Creation to Consumption[J]. Signal Processing: Image Communication, 2003, 18(4): 237-262.

9 Lin E I, Eskicioglu A M, Lagendijk R L. Advances in Digital Video Content protection[J]. Proceedings of the IEEE, 2005, 93(1): 171-183.