文章编号: 1001- 2486(2004) 06- 0100- 03

数字视频信息分级授权收视系统*

王苏峰, 戴 葵, 侯方勇
(国防科技大学计算机学院, 湖南 长沙 410073)

摘 要: 针对日益严重的数字视频信息安全问题, 提出一种数字视频信息的分级授权收视方案, 其关键是利用现代高强度的密码技术保证数字视频信息传输的安全性和分级授权机制的实现。由于充分利用了成熟的数字视频广播技术, 此分级授权收视系统安全性很高, 系统构建简单, 且成本比较适中。

关键词: 数字视频; 分级授权; 密码; 机顶盒; 智能卡
中图分类号: TP311 文献标识码: A

A Hierarchical Authorization System on Digital Video

WANG Su-feng, DAI Kui, HOU Fang-yong
(College of Computer, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: In order to solve the security problem of digital video, a hierarchical authorization scheme on digital video is presented, which utilizes modern strong cipher to protect digital video's transport and realize hierarchical authorization. Owing to the use of fully mature digital video broadcast technology, the scheme has high security, simple framework, and low cost.

Key words: digital video; hierarchical authorization; cipher; STB; smart card

在军队、国防、政府等相关部门里, 存在着大量的数字视频信息。这些数字视频信息既要供相应级别、特定团体或特定个人收视, 又要保证其安全性, 做到不泄密。目前一般的做法是对数字视频信息进行复制并分发到特定个人或相关单位, 自行收看或者借阅、或组织集体收看。这种做法不足之处很明显, 视频载体分发过多, 其安全性难以控制, 容易造成失密。针对这种不足, 本文提出一种基于数字视频广播条件接收标准[1,2]的数字视频信息的分级授权收视方案。本方案充分利用成熟的数字视频广播技术[3]、高强度密码技术和高可靠性的智能卡技术以及已有的设备和线路, 系统成本比较适中。

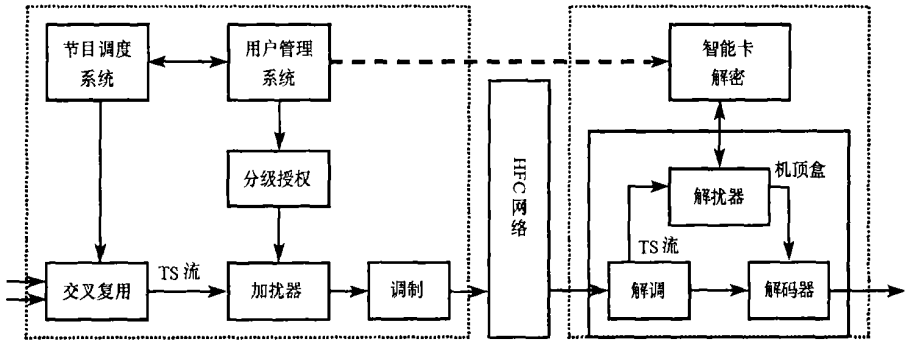

图 1 分级授权收视系统

Fig. 1 A hierarchical authorization system

1 分级授权收视系统的功能结构

分级授权收视系统的基本功能结构如图 1 所示。由图 1 可以看出, 分级授权收视系统由三大部分组

* 收稿日期: 2004- 09- 10
作者简介: 王苏峰(1970—), 男, 博士生。

成:视频前端子系统、传送网络和用户接收子系统。视频前端子系统由节目调度、用户管理和传送流(TS)合成组成,主要功能有:数字视频信息管理、节目播控、交叉复用、传送流(TS)合成、用户分级授权管理、加扰、调制;用户接收子系统由机顶盒和智能卡组成,主要功能有:解调、解密(分级授权)、解扰、解码等。

这种结构充分利用了现有的资源,因为相关单位基本上都自建了有线电视网络系统,有的还有自己的电视台,并且有一定的节目制作能力。因此在现有设备和网络基础上,只需要添加少量的设备:前端需要添加视频服务器、视频数字化设备、DVB 传送流合成部件以及用户管理和分级授权及加扰部分;用户端需要添加机顶盒、智能卡等。

2 分级授权的实现

分级授权是充分利用现代高强度密码技术(3DES、RSA)来实现的,其核心就是利用三层加密机制对数字视频信息进行加密。数字视频信息加扰解扰、加密解密过程如图 2 所示[2]。

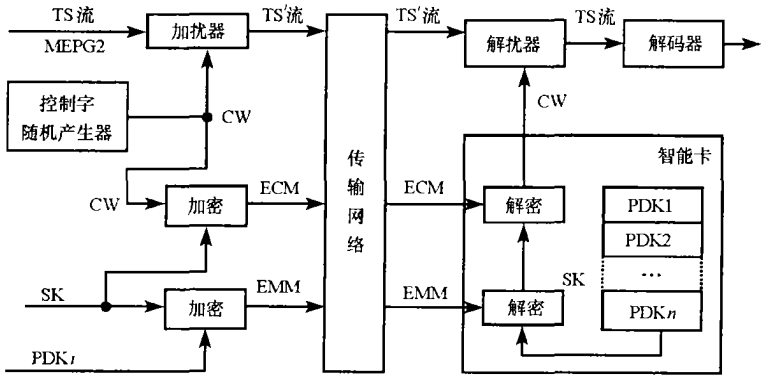

图 2 传送流加解密过程

Fig. 2 The encryption and decryption of TS stream

在发送端,用随机产生的控制字 CW(Control Word)对传送流 TS(Transport Stream)进行加扰计算形成加扰的传送流 TS′。控制字 CW,即传送流的加密密钥,是一组由若干位数字组成的随机数,每隔几秒钟随机变化一次。在接收端要用同样的控制字才能进行解扰,因此分级授权收视系统的核心就是控制字的安全传送。

控制字在对传送流进行加扰的同时,控制字本身也在 ECM 中被业务密钥 SK(Service Key)加密,形成授权控制信息 ECM(Entitlement Control Message),即加密的控制字,ECM 传送流包插入到传送流,大约每隔几秒钟在传送流中出现一次。

同时,用户管理信息(Management Message)包括业务密钥 SK 也被个人分配密钥 PDK(Personal Distribute Key)加密形成授权管理信息 EMM(Entitlement Management Message)。用户管理信息由相关安全部门的用户管理系统形成,用来建立授权用户的名称、级别、单位、地址、智能卡号、当前授权的数据库等等。EMM 传送流包大约每隔几秒钟插入传送流一次。

在接收端,解密由智能卡和解扰器配合完成。要完成解扰功能,需要查找并提取 EMM 和 ECM 传送流包。这就需要利用传送流中一个非常重要的传送流包——MPEG2 的节目特定信息 PSI(Program Specific Information)。PSI 中包含了有关传送流包的包识别码 PID 信息以及 TS 包之间的关系。

PSI 使用 4 个表来定义码流结构,这 4 个表分别是节目关联表 PAT(Program Association Table)、节目映射表 PMT(Program Map Table)、条件接收表 CAT(Conditional Access Table)和网络信息表 NIT(Network Information Table)。节目关联表 PAT 的传送流包 PID 为 0x0000,查找节目信息必须从 PAT 表开始,表中列出了传送流中的节目映射表 PMT 的 PID。PMT 表中又可以找到相应节目的基本码流,还给出了所有 ECM 所在 TS 包的 PID。条件接收表 CAT 的 PID 为 0x0001,它将给出所有 EMM 所在 TS 包的 PID。第四个表是网络信息表 NIT,它给出相应的网络信息,这个表是可选的。

接收端解密的原理如下: 当智能卡插入时, 首先在传送流中寻找条件接收表 CAT, 然后根据 CAT 表中给出的 EMM 包识别码(PID) , 找到相应的加密的 EMM 信息; 智能卡中存有 PDK 等个人分配密钥, 智能卡首先使用 PDK, 对加密的 EMM 解密, 根据解出的 EMM 信息来确定本智能卡是否被授权收看该套节目, 如果没有授权将不能进行后续解密, 也就不能收看该套节目; 如果该卡已被授权, 则启用 EMM 中的业务密钥 SK 对 ECM 解密, 得到控制字 CW; 最后由控制字 CW 对加扰的传送流进行解扰, 得到正常的 MPEG2 传送流, 再由机顶盒中的解码器解码后得到所需的视频信号。

3 智能卡

智能卡对整个分级授权收视系统的安全性起到非常关键的作用。智能卡具有很高的安全性、抗攻击性, 可以保证存放在其中的密钥绝对安全。另外, 智能卡具有自己的操作系统, 使得文件的管理、密钥的管理非常安全方便, 很容易实现分级授权。

在本系统中, 智能卡的作用有两个: 一个是存放授权用户的信息 ——姓名、级别、单位、证件编号、个人分配密钥、级别密钥组、智能卡号等; 另一个就是利用卡上的对应密钥对 EMM 进行解密, 并与卡上的个人信息进行比较, 判断是否授权, 如果授权则继续解密出控制字并送往机顶盒。

智能卡的体系结构如图 3 所示, 采用 SOC 设计技术实现, 其关键技术已掌握或者已经实现。关键部件有: CPU 核、加解密部件(RSA、3DES) 、真随机数发生器(TRNG) 和片内存储器。CPU 核与 8051 单片机兼容, 经过仔细设计, 最高工作频率可达 90MHz; RSA 加密位数为 1024 位, 加解密速度接近 1000 次/s; 真随机数发生器采用全定制电路实现, 其安全性和随机性得到充分保证。

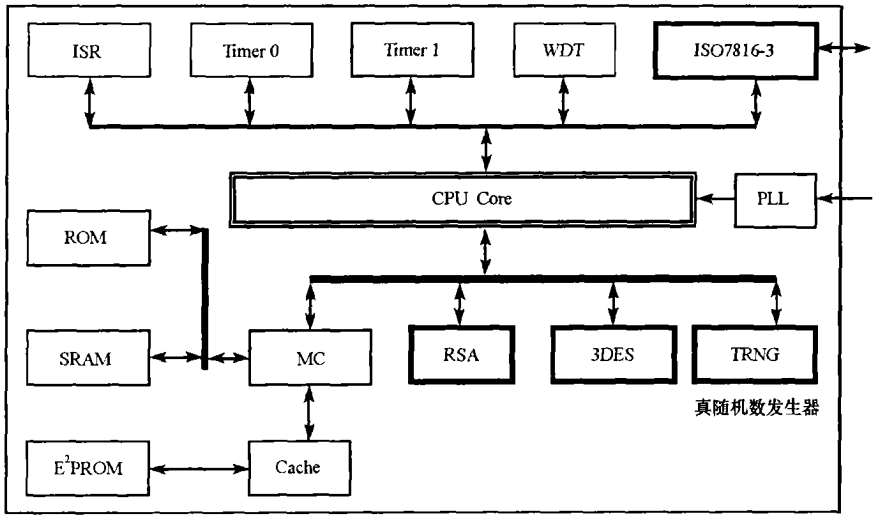

图 3 智能卡的体系结构

Fig. 3 The architecture of smart card

4 结 论

本方案充分利用成熟的数字视频广播技术、高强度密码技术和高可靠性的智能卡技术, 能有效地解决数字视频信息的分级授权收视问题。在本系统中, 视频载体集中存放管理, 数字视频信息传输可靠, 整个系统的安全性很高, 而且整个系统大量采用已有的设备和有线电视传送网络, 系统构建简单, 成本比较适中。

参 考 文 献:

[1] GY/Z175- 2001. 数字电视广播条件接收系统规范[S]. 广电总局行业标准, 2001.

[2] EN 50221. Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications[S]. 欧洲标准局, 1997.

[3] ISO/IEC 13818- 1. 信息技术、运动图像及其伴音信号的通用编码(第一部分) 系统[S]. ISO/IEC, 1994.