

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04N 5/00 (2006.01)

H04N 5/44 (2006.01)

H04N 7/16 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200810073780.7

[43] 公开日 2009年1月28日

[11] 公开号 CN 101355640A

[22] 申请日 2008.9.11

[21] 申请号 200810073780.7

[71] 申请人 敖发良

地址 541004 广西壮族自治区桂林市金鸡路1号
桂林电子科技大学信息与通信学院

[72] 发明人 敖发良 潘 阳 马春波 敖 珺

[74] 专利代理机构 桂林市持衡专利商标事务所有
限公司
代理人 马 兰

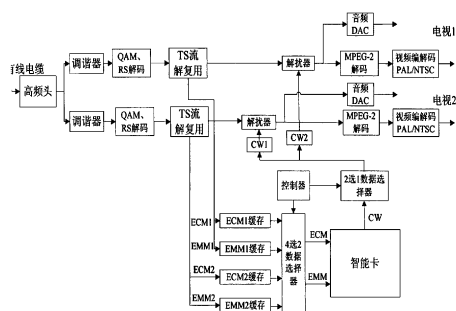
权利要求书2页 说明书11页 附图5页

[54] 发明名称

多显示数字电视机顶盒

[57] 摘要

本发明公开一种多显示数字电视机顶盒，包括一个高频头，至少两路调谐模块、正交幅度解调模块、解复用模块、解码模块，以及一个条件接收模块。调谐器模块、正交幅度解调模块和解复用模块、解码模块都是在单路模块上再简单地增加一路或多路单路模块，从而实现多路不同的信号频道选择输入、模拟信号解调出数字信号和节目流的解复用。而解密解扰模块则不是简单的两个单路的合并，由于智能卡的输入和输出只能是一路信号，所以本发明运用时分复用的原理来处理多路节目信号的解密解扰，以此实现同时在不同的显示器上显示相同或不同的多路节目信号。



1、多显示数字电视机顶盒，其特征在于：包括有
一个高频头，用于接收高频电视信号，并将高频电视信号进行下变频，输出至少两路中频电视信号；
至少两路调谐模块，对高频头输入的中频信号进行滤波以及选频；
至少两路正交幅度解调模块，每路正交幅度解调模块与一路调谐模块相连，负责对滤波以及选频后的电视信号进行解调、解码；
至少两路解复用模块，把同一频道上不同的节目流和信息流分别选出来，并根据观众所选频道把相应节目流传送到相应的解码模块，同时将所选频道的信息流传送到条件接收模块；
一个条件接收模块，接收来自上述各路解复用模块的信息流，即授权管理信息和授权控制信息，并在一个控制字的循环周期内分时处理不同路的授权管理信息和授权控制信息，最后分时输出不同路的控制字信息送对解密流进行解扰；
至少两路解码模块，将条件接收模块解扰出来的电视节目进行音视频解码，同时还原出至少两路相同或不同的音视频流。

2、根据权利要求1所述的多显示数字电视机顶盒，其特征在于：所述条件接收模块包括智能卡、控制器、授权信息选择器、控制字选择器、以及至少两路授权控制信息和授权管理信息的授权信息缓存器、解扰器和节目流缓存器；各路授权信息缓存器分别与不同路的解复用模块相连；控制器分别与授权信息选择器和控制字选择器的控制端相连，用于在一个控制字循环周期内控制授权信息选择器选择其中一路授权控制信息和授权管理信息输入智能卡的输入端，以及控制控制字选择器选择输出智能卡解密出的其中一组控制字输出至相应的解扰器；解扰器与节目流缓存器连接，将每一个控制字循环周期解扰出来的音视频流进行缓存，直至下一个控制字循环周期解扰出来的节目流和信息流的送入。

3、根据权利要求2所述的多显示数字电视机顶盒，其特征在于：所述调谐模块、正交幅度解调模块、解复用模块、音视频解码模块、授权信息缓存器、解扰器和节目流缓存器的路数与所需显示的数字电视节目的路数N相同，其取值在1~3路之间。

4、根据权利要求3所述的多显示数字电视机顶盒，其特征在于：所述授权信息选择器为 $2N$ 选2数据选择器，该授权信息选择器的输入端通过总线与各路授权信息缓存器相连，输出端通过导线与智能卡相连。

5、根据权利要求3或4所述的多显示数字电视机顶盒，其特征在于：所述控制字选择器为N选1数据选择器，该控制字选择器的输入端通过导线与智能卡相连，输出端通过总线与各路解扰器相连。

6、根据权利要求3所述的多显示数字电视机顶盒，其特征在于：所述智能卡将一个控制字循环周期按所需显示的数字电视节目的路数N进行等分，每个 $1/N$ 等分处理一路授权控制信息和授权管理信息。

7、根据权利要求6所述的多显示数字电视机顶盒，其特征在于：所述智能卡的处理每一路授权控制信息和授权管理信息的时间应保证在0.5~1.5秒之间。

8、根据权利要求1所述的多显示数字电视机顶盒，其特征在于：所述各路解复用模块为集成在同一芯片中，构成一个具有多路解复用程序的一个独立模块。

多显示数字电视机顶盒

(一) 技术领域:

本发明属于数字电视接收领域，特别涉及一种多显示数字电视机顶盒。

(二) 背景技术:

随着数字电视的全面推广，数字电视的普及必将是未来广播电视产业的发展趋势。由于从模拟电视到数字电视的转换需要一个较长的过渡时期，为了使现有的模拟电视机能够接收数字电视信号，需要一种转换装置，数字电视机顶盒应运而生。数字电视机顶盒是一种能够接收数字电视信号、完成相应处理并输出模拟的音视频信号，通过模拟电视机播出节目的家用电子产品。数字电视机顶盒的主要功能是完成对数字电视信号的接收，具体讲就是高频头接收来自有线网的高频信号，通过正交幅度解调器完成信道解码，从载波中分离出包含音、视频和其它数据信息的节目流和信息流，然后通过解复用模块则区分不同的节目，提取相应的节目流和信息流，送入解码器和相应的解析软件，完成数字信息的还原，解码器完成音视频信号的解压缩，经视频解码器和音频 D/A 数模拟变换，还原出模拟音视频信号，在常规模拟电视机上显示高质量图像，并提供多声道立体声节目。

对于付费电视，需要加入条件接收模块对节目流和信息流实施解扰，并采用含有识别用户和进行记帐功能的智能卡进行解密，保证合法用户正常收看。条件接收模块的主要目的是控制用户对付费电视的访问和保证经营者的收入，只有与网络经营者有约定的用户才可以获取特殊的服务。在整个条件接收模块的实现中，授权控制信息（ECM）和授权管理信息（EMM）传输的安全性至关重要。条件接收模块解密解扰的过程主要把解复用模块输出的加扰的节目流，用信息流即授权控制信息和授权管理信息进行相应的处理过程。授权管理信息通过智能卡获得授权，然后再对授权控制信息进行解密，解密输出的控制字（CW），再由控制字与加扰的节目流进行解扰，最后输出还原的节目流的音视频流。由于各个条件接收提供商使用各自认为安全的算法，这些算法保证条件接收的安全性和盈利目的，因此现有国内的数字电视机顶盒只能接一台电视机。对于一个家庭来说，每个人的爱好可能都不一样，如果只有一台电视机可以收看，不同爱好的观众要求同时收看不同的电视节目就不能实现了。如果增加电视机的台数，就得增加数字电视机顶盒，还得相应的增加服务费。当前国内电视数字化的推广遇到很大的困难，其中很大的原因就是一台数字电视机顶盒不能连接多台电视机，给用户造成很大不便，用户增加了费用但减少了服务。因此为了解决多台电视共用一个数字电视机顶盒的问题，我们提出新型数字电视机顶盒设计方案，此新型数字电视机顶盒

能使多台电视相互不影响地接收不同的电视节目，给用户更好的服务，从而使电视数字化更顺利地推广。

为实现多路数字电视节目同时收看，存在各自不同的实施方式，如中国发明专利 CN200710118007.3 申请公开的“一拖二数字电视机顶盒”，其数字电视机顶盒采用主从形式，其中主终端包括多个解扰器、多个解码器来进行节目解扰功能，从终端不需要对信息流进行解扰。主从终端间的通信传送的是音视频流和控制字信息。然而这种结构的数字电视机顶盒由于主从终端所处理的信息的不对称，这就需提高主终端芯片 CPU 的速度和容量，因而不只使得主终端的选型和设计的难度加大、生产成本增加，而且一旦主终端出现故障，将会影响整个系统的运行；其次，信息流解扰的过程都在同一个主终端内进行，解扰后节的音视频流就可能出相互干扰的现象，影响数字电视机顶盒的解码效果，最终使得数字电视信号的质量变差。

（三）发明内容：

本发明所要解决的技术问题是提供一种信息处理对称、设计简单、且成本较低的多显示数字电视机顶盒。

为解决上述问题，本发明设计的多显示数字电视机顶盒，包括有：

一个高频头，用于接收高频电视信号，并将高频电视信号进行下变频，输出至少两路中频电视信号；

至少两路调谐模块，对高频头输入的中频信号进行滤波以及选频；

至少两路正交幅度解调模块，每路正交幅度解调模块与一路调谐模块相连，负责对滤波以及选频后的电视信号进行解调、解码；

至少两路解复用模块，把同一频道上不同的节目流和信息流分别选出来，并根据观众所选频道把相应节目流传送到相应的解码模块，同时将所选频道的信息流传送到条件接收模块；

一个条件接收模块，接收来自上述各路解复用模块的信息流，即授权管理信息和授权控制信息，并在一个控制字的循环周期内分时处理不同路的授权管理信息和授权控制信息，最后分时输出不同路的控制字信息送对解密流进行解扰；

至少两路解码模块，将条件接收模块解扰出来的电视节目进行音视频解码，同时还原出至少两路相同或不同的音视频流。

上述方案所述的所述条件接收模块包括智能卡、控制器、授权信息选择器、控制字选择器、以及至少两路授权控制信息和授权管理信息的授权信息缓存器、解扰器和节目流缓存器；各路授权信息缓存器分别与不同路的解复用模块相连；控制器分别与授权信息选择器和控制字选择器的控制端相连，用于在一个控制字循环周期内控制授权信息选择器选择其中一路授权控制信息和授权管理信息输入智能卡的输入端，以及控制控制字选择器选择输出智能卡解密出的其中一组控制字输出至相应的解扰器；解扰器与节目流缓存器连接，将每个控制字循环周期解扰出来的音视频流进行缓存，直至下一个控

制字循环周期解扰出来的节目流的音视频流送入。

根据所需显示的数字电视节目的路数 N ，选择相应个数的调谐模块、正交幅度解调模块、解复用模块、音视频解码模块、授权信息缓存器、解扰器和码流缓存器，即上述各器件的路数与所需显示的数字电视节目的路数 N 相同，其取值在 1~3 路之间。

上述方案中，所述授权信息选择器为 $2N$ 选 2 数据选择器，该授权信息选择器的输入端通过总线与各路授权信息缓存器相连，输出端通过导线与智能卡相连。所述控制字选择器为 N 选 1 数据选择器，该控制字选择器的输入端通过导线与智能卡相连，输出端通过总线与各路解扰器相连。

为了实现两路或两路以上电视节目的同时收看，采用了时分复用原理来处理多路电视信号，为了证明能实现两路节目同时收看，就必须证明智能卡能在一个控制字循环周期内能分时解密两路或两路以上不同的授权控制信息和授权管理信息，即是在一路新的授权控制信息和授权管理信息送入智能卡前，智能卡必须解密出另外一路的控制字。因此本发明的智能卡最好将一个控制字循环周期按所需显示的数字电视节目的路数 N 进行等分，每个 $1/N$ 等分处理一路授权控制信息和授权管理信息。

为了分时处理不同路的授权控制信息和授权管理信息，所述智能卡的处理每一路授权控制信息和授权管理信息的时间应保证在 0.5~1.5 秒之间，以保证在下一个周期的授权控制信息或者授权管理信息到来之前，它能把本周期的内的每一路的授权控制信息和授权管理信息全部都解密出每一路控制字。

根据单路的解复用模块设计原理，可以简单地把或两路以上的单路的解复用模块叠加一起。各个独立的单路解复用模块，它们由相同的程序设计而成，并相互不影响地独立地完成一路信号的解复用。因为两路或两路以上的解复用所用的设计程序是一样的，所以最好把两路或两路以上的单路的程序编译在同一芯片中，集成为一个独立的模块，也就是我们所需要的两路解复用模块。

本发明所设计的多显示数字电视机顶盒，其调谐器模块、正交幅度解调模块和解复用模块都是在单路模块上再简单地增加一路以上单路模块，从而实现多路不同的信号频道选择输入、模拟信号解调出数字信号和 MPEG-2 节目流的解复用。而解密解扰模块则不是简单的两个单路的合并，由于智能卡的输入和输出只能是一路信号，所以本发明运用时分复用的原理通过改进条件接收模块的硬件和软件来处理多路节目信号的解密解扰，以此实现同时在不同的显示器上显示相同或不同的多路节目信号。

本发明与现有技术相比，提出一种多显示数字电视机顶盒的设计方案，可以同时连接两台以上模拟电视机，并同时在这两台以上电视机上收看不同的电视节目，并创新性地设有条件接收模块，以减少用户的投入和费用为目的，使两台电视机同时享受视频点播、互动游戏、网上冲浪、在线升级等业务。

（四）附图说明：

图 1 为本发明多显示数字电视机顶盒的一种优选实施例的原理框图。

图 2 为本发明节目选择流程图。

图 3 为单路正交幅度解调模块原理图。

图 4 为本实施解复用模块的软件流程。

图 5 为本实施例智能卡输入端授权控制信息、授权管理信息与输出端控制字的时序关系图。

图 6 为两路条件接收模块的工作流程图。

图 7 为本发明一种三路显示数字机顶盒的组成原理图。

图 8 为本发明一种两遥控器控制的两路显示数字机顶盒的组成原理图。

图 9 为本发明一种单遥控器控制的两路显示数字机顶盒组成原理图。

（五）具体实施方式：

图 1 为本发明多显示数字电视机顶盒的一种优选实施例的原理框图，包括有一个高频头、两路调谐模、正交幅度解调模块、解复用模块、音视频解码模块、以及一个条件接收系统模块构成。下面对上述各个模块进行详细的说明：

1、高频头和和调谐器

数字电视机顶盒输入端为一路电缆接入，45MHz~860 MHz 的高频电视节目信号在这路电缆上面传输。在数字电视信号传输过程中一路 8MHz 的模拟频道可以传输 6~8 套标准清晰度的电视节目，不同电视节目信号可以传在同一模拟频道，也可以传在不同的模拟频道。高频头或高频放大器的作用是对有线网络上传送 45MHz~860 MHz 的高频信号进行接收、放大和变频，一个高频头就可以接收所有的模拟频道，因此只需要一个高频头。数字电视机顶盒输入端只有一根铜轴电缆接入，高频电视信号进入高频头放大后分两路下变频器或混频器或调谐器，输出两路中频信号。调谐器的作用相当于滤波器，用于选择收看节目所在的频道。当所要收看的两个电视节目处在同一模拟频道时，则需要两个频率相同的本振信号加到调谐器上来产生两个频率相同的中频信号；当所要收看的两个电视节目不在同一模拟频道时，则需要两个频率不同的本振信号加到调谐器上来产生两个频率相同的中频信号，这样才能保证有输出两路不同的电视节目信号。

如图 2 为节目选择流程图，要对两台电视机进行遥控，所以数字电视机顶盒需要两个遥控器输入端，一个遥控器控制一台电视机。遥控器通过数字电视机顶盒软件操作系统电子节目指南 EPG 选择电视节目。节目指南所对应的电视节目表被存储在同一内存中，两个遥控器输入选择控制时，把它们的控制信息以先到先得的方式进行读取节目控制信息，分别从内存中的节目关联表 PAT 读取所看节目的节目映射表包的节目标识符 PMT_PID，分别是 PMT1_PID 和 PMT2_PID。因为选择的电视节目不一样，每个电视节目对应的节目映射表包的节目标识符 PMT_PID 值也是不一样的，所以先将它们的值分别

存入不同的两个内存中。解复用模块再读取 PMT1_PID 和 PMT2_PID 的值，通过两路不同的节目标识符值 PID 滤出不同两路节目映射表 PMT 信息，分别是 PMT1 和 PMT2。从节目映射表中找出节目所对应的网络关联表 NIT 信息，分别是 NIT1 和 NIT2。最后把两个节目的网络关联表 NIT 信息分别传送到对应的调谐器控制端，进而控制调谐器选频，选出所看节目所在的频率点。

2、正交幅度解调模块

如图 3 为单路正交幅度解调模块原理图，正交幅度解调模块处于数字电视机顶盒的后半端，负责将前端的数字电视调谐器下变频到中频，通过解调接收专用芯片的处理得到 MPEG-2 输出信号，解调后输出的码流是符合 DVB-C/ITU J83-A 和 ITU J83-C 的标准。正交幅度调制是一种联合振幅、相位调制方式，其振幅和相位都能携带信息因而具有很高的频带利用率。由于已调信号的振幅、相位均有不同的取值，故其星座图的结构形状可以有多种，如圆形、三角形、矩形、六角形等。对于具有相同的 M 进制的正交幅度调制信号来说，由于星座图不同，各点之间最小距离也不同，因而相应的调制方式会有不同的误码性能。由于信道畸变和噪声会引起较高的误码率，必须在对信号判决前用匹配滤波器和均衡对 I、Q 两路基带信号进行波形失真的恢复。经过均衡器对受损信号的均衡，然后经判决器 $L \rightarrow 2$ ($L=4, 16$ 正交幅度) 电平转换后，最后由并/串转换得到原始数据。解调完成后，还要进行差分解码、符号到字节的映射、解卷积交织、RS 解码、同步第一字节再倒置、解扰，才能从基带物理接口得到数据和时钟。

本实施例两个正交幅度解调模块各自为一个独立的模块，没有控制端，只有输入和输出端。一个正交幅度解调模块只能解调一个频率点的电视信号，而本实施例要求不同的两路电视信号，因此要解决两路信号解调时，则需要两个独立的正交幅度解调模块。正交幅度解调模块的输入端接调谐器的输出，即是通过遥控器选择出来的已调制的数字节目流信号，经过正交幅度解调之后输出为数字信号 MPEG-2 传输流。

3、解复用模块

解复用模块的作用是把同一频道上不同的节目流以及信息流分别选出来，并根据观众所选的节目把音视频传送到解扰器，同时也把节目特定信息 (PSI) 信息传送给存储器。解复用模块根据单路的解复用模块设计原理，可以简单地把两个单路的解复用模块叠加一起。两个独立的单路解复用模块，它们由相同的程序设计而成，并相互不影响地独立地完成一路信号的解复用。因为两路所用的设计程序是一样的，所以本实施例的解复用模块把两个单路的程序编译在同一芯片中，集成为一个独立的模块，也就是我们所需要的两路解复用模块。解复用模块的输入端为正交幅度解调的 MPEG-2 传输流信号，输出端为节目的音视频信号和节目数据信息。

本实施例解复用模块的软件流程如图 4 所示，正交幅度解调模块解调出来的两路节目流 TS1 和 TS2 分别进入各自的解复用模块，首先经过同步检测，找出每一帧的帧头 (0x47)，并把找出的每帧存入 FIFO 缓存中，如果 FIFO 的

传输流缓存中有未处理的包，从 FIFO 传输流缓冲区中取出该包，根据节目标识符 PID 的值，如果是 PID=0，表示当前的包是节目关联表 PAT，那么就对该包进行解析，根据选定的节目号，确定需要解码的节目映射表 PMT 包的节目标识符 PID，更新节目标识符 PID 信息表中节目映射表的节目标识符 PID，将节目映射表 PMT 的状态位设定为需要解码。

根据节目映射表 PMT 的状态位，如果不需要解码，就丢弃这个包。如果节目映射表 PMT 的状态位需要解码，进入节目映射表 PMT 包解析子程序，提取出该解码对应的音频，视频传输流包的节目标识符 PID，将提取出的音频，视频传输流包的节目标识符 PID 值对节目标识符 PID 信息表进行更新。

如果节目标识符 PID 等于节目标识符 PID 信息表中的音频、视频节目标识符 PID 值，那么就进入到音频视频处理程序，对音频视频的传输流包进行解包，配置片上 DMA 直接内存存取控制器。由直接内存存取控制器将对应的打包基本流 PES 包的内容，也就是实际的音视频流的码流发送到片外存储器 SDRAM 的音频、视频缓冲区中，供下一级的音频、视频解码器完成解码功能。最终完成 MPEG2 码流的解码过程。因为两路解复用模块的工作程序都是一样，所以在解复用过程中只需要多增加内存的存储容量，并把它们的节目关联表包的节目标识符 PAT_PID、节目映射表包的节目标识符 PMT_PID 和节目流的节目标识符 PID 信息表分别存在不同的缓存中，以便读取和更新。

4、条件接收模块

本发明的关键在于解密出两路不同的控制字，而不同的控制字则又要通过不同的授权控制信息和授权管理信息解密。

通常情况下，在授权控制信息数据包中会传输两个加密后的控制字：当前时刻的加扰控制字和下一周期的加扰控制字。控制字一般 2~10s 更换一次，因此授权控制信息数据包必须在这个时期内分发数次，以确保用户在控制字更换之前收到新的授权控制信息数据包。授权控制信息数据包只与该传输流中的产品数有关，而与用户数无关，所有用户使用相同的授权控制信息数据包。用户数字电视机顶盒收到授权控制信息数据包后会传送给用户智能卡用于解密控制字。

在授权管理信息数据包中传送加密的产品密钥或加密的组密钥，授权管理信息数据包的信息对于每个用户不同。每个用户接收机首先根据自己的用户号 User-ID 或组号 Group-ID 过滤出属于自己的授权管理信息数据包，然后将数据包传送给用户智能卡，用户智能卡解密出组密钥，再由组密钥解密出产品密钥，根据授权控制信息在智能卡内部解密出控制字并送出智能卡外给数字电视机顶盒解扰。一般产品密钥数小时更换一次，含有产品密钥加密信息的授权管理信息数据包几分中分发一次；组密钥数天更换一次，含有组密钥加密信息的授权管理信息数据包数小时分发一次。

由于授权控制信息和授权管理信息数据包都是几秒钟才更换一次，控制字是随着授权控制信息和授权管理信息的变化而改变，一般也是 2~10s 才变化一次，也就是说 2~10s 内节目流解扰的控制字都是同一个控制字。因此假

设智能卡输入端有两路(不同的)授权控制信息和授权管理信息,分别为 ECM1 和 EMM1、ECM2 和 EMM2,在不同的时刻进入智能卡,然后智能卡在不同的时刻分别处理不同的授权控制信息和授权管理信息,最后输出不同的控制字信息进行解扰。本实施例用 1s 作为一个循环周期,每隔 0.5s 处理不同两路的解密过程。一个周期内前 0.5s 从内存中把 授权控制信息 ECM1 和授权管理信息 EMM1 取出输入智能卡进行解密,输出控制字 CW1,并把存入存储器中,同时新的授权控制信息 ECM2 和授权管理信息 EMM2 存入存储器中。后 0.5s 从内存中把授权控制信息 ECM2 和授权管理信息 EMM2 输入智能卡进行解密,输出控制字 CW2,并把存入存储器中,同时新的授权控制信息 ECM1 和授权管理信息 EMM1 存入存储器中。下个周期重复以上的过程,最终可以 1s 钟内输出两个不同的控制字。

因为控制字在 2s 以上才会改变,所以当解扰时,在 2s 时间内从存储器中取出的控制字不会改变。同时在 2s 时间内一路授权控制信息和授权管理信息解密 2 次,保证了授权控制信息和授权管理信息不断地更新,也会保证控制字不断地更新。经过循环处理授权控制信息和授权管理信息,控制字不间断地更新,进而保证了未解扰的传输流不间断地解扰。只有保证两路传输流不断地解扰,才能保证电视节目不间断地播放,最终达到本文所要求的数字电视机顶盒设计方案:一台数字电视机顶盒连接两台电视机,并能同时收看不同的电视节目。如图 5 所示为本实施例智能卡输入端授权控制信息、授权管理信息与输出端控制字的时序关系图。

两路不同的授权控制信息 ECM1 和授权管理信息 EMM1、授权控制信息 ECM2 和授权管理信息 EMM2 来自解复用器输出端,授权控制信息和授权管理信息缓存的作用就是存储授权控制信息和授权管理信息,通常用 FIFO 存储器构成,一个典型的授权控制信息数据包长度 188 字节,而含有产品密钥加密信息的授权管理信息数据包长度是 37 字节,含有组密钥加密信息的授权管理信息数据包长度为 38 字节。通常授权控制信息数据包信息 2s 钟更新一次,通过再找到在节目映射表中的 CA_descriptor,并找出对应的 授权控制信息码流的节目标识符(PID),最后通过授权控制信息的节目标识符 PID 滤出授权控制信息。为了保证授权控制信息不丢失,应采用内存存储,因为它更新很慢,所以只要有 256 字节的内存作为储存信息。同样授权管理信息数据包信息 10s 以上更新一次,它是通过解码器将从中读取智能卡 IC 的 CA_system_ID 及其它智能卡信息,在节目流中找到并过滤出条件接收表(CAT)(PID=0x0001),通过条件接收表中的 CA_descriptor,找出对应该 CA_system_ID 的 CA_PID,此 CA_PID 即为对应该条件的授权管理信息的节目标识符,最后通过授权管理信息的节目标识符滤出授权管理信息。为了保存授权管理信息,使之不丢失,则需要 150 字节的内存。这样保证智能卡处理一路授权控制信息 ECM1 和授权管理信息 EMM1 时,另一路授权控制信息 ECM2 和授权管理信息 EMM2 能完好的保存,并等到它处理时而没有丢失数据。

最后来讨论智能卡的处理速度,为了分时处理不同两路的授权控制信息

和授权管理信息，智能卡的速度不能不考虑。因为智能卡要保证在下一个新的授权控制信息或者授权管理信息到来之前，它能把两路的不同授权控制信息和授权管理信息处理好。智能卡的输出信息控制字 2s 变化一次，控制字的长度是 64bit，而智能卡的数据传输的波特率为 9600bps，也就是智能卡一秒可以处理输出 9600bit 的数据，远远大于两路控制字信息输出的速度。又根据对智能卡中解密算法的硬件 FPGA 仿真，在处理时钟为 5MHz 的 FPGA 中解密一次控制字需要 0.3s 左右，因此在控制字在 1s 时间内变化最多能处理 3 次，能确保解密控制字时也不丢失和更新。因此本发明中提出智能卡在 0.5s 内解密一路授权控制信息和授权管理信息，再在另一 0.5s 内解密另一路授权控制信息和授权管理信息，最后得出两路不同的控制字信息，也是能保证控制字不丢失同时能按要求更新。

控制器的作用是控制输入端授权控制信息 ECM1、授权管理信息 EMM1 或授权控制信息 ECM2、授权管理信息 EMM2 选择输入，输出端则是控制字 CW1 或控制字 CW2 选择输出。TS1' 和 TS2' 为未解扰的 MPEG-2 视频和音频码流，TS1 和 TS2 为解扰之后的视频和音频数据，它们的码流速率在 3mb/s~38.5mb/s 之间，因此也需要至少一秒钟的缓存，需要 38.5mb 大小的内存。控制字的缓存也很重要，控制字可能几秒钟才变化一次，要确保控制字在几秒钟内不丢失，它需要 128bit 的内存作为存储器。

如图 6 为两路条件接收模块的工作流程图，输入端输入未解扰的节目流 TS1' 和 TS2' 码流，分别经过 FIFO 缓存处理，然后节目标识符 PID 检测分辨节目流包属于什么类型的数据包。当检测结果是条件接收表 CAT 的数据包时，又检测是否是授权管理信息或者是授权控制信息，最后滤出授权管理信息 EMM1 和授权控制信息 ECM1、授权管理信息 EMM2 和授权控制信息 ECM2 数据信息。S 方波发生器是周期为 1s 的方波发生器，当 S 为 '1' 时，判断授权管理信息 EMM1 和授权控制信息 ECM1 通过，授权管理信息 EMM1 与 PDK 进行授权解密，解密结果在与业务密钥 SK 进行第二次解密，再经过数据加密标准 DES 算法解密得到控制字 CW1，控制字 CW1 与未解扰的节目流 TS1' 流进行解扰，最后得到音视频 TS1 码流。同理，当 S 为 '0' 时，判断 EMM2 和 ECM2 通过，EMM2 与私有数据 PDK 进行授权解密，解密结果在与 SK 进行第二次解密，再经过 DES 算法解密得到 CW2，控制字 CW2 与未解扰的节目流 TS2' 流进行解扰，最后得到音视频流。

通过以上各个模块的设计，调谐模块、正交幅度解调模块和解复用模块都是在单路模块上再简单地增加至少一路单路模块，从而实现两路或两路以上不同的信号频道选择输入、模拟信号解调出数字信号和 MPEG-2 节目 TS 流解复用。调谐模块、正交幅度解调模块、解复用模块的路数与所需显示的数字电视节目的路数 N 相同，其取值在 1~3 路之间。而解密解扰模块则不是简单的两个或两个以上的单路的合并，因为智能卡的输入和输出只能是一路信号，所以不能同时解密解扰两路节目信号。为了实现两路节目信号解密解扰，本实施例运用时分复用的原理来处理两路节目信号的解密解扰。

4-1 控制模块处理

智能卡要解密两路授权控制信息和授权管理信息,就必须分时循环处理,因为智能卡输出控制字至少 2s 才变化一次,所以把 2s 分为四等分,0.5s 解密第一路信号,下个 0.5s 再解密第二路信号,再一个 0.5s 又回到解密第一路信号,最后的 0.5s 又解密第二路信号。如此循环解密授权控制信息 ECM 和授权管理信息 EMM 信息,就会不丢失,也不会在新的授权控制信息 ECM 和授权管理信息 EMM 到来时不能及时解密。

控制模块的控制程序步骤为:控制模块输出端为 1 时,4 选 2 数据选择器输入端是授权控制信息 ECM1 和授权管理信息 EMM1,输出即为授权控制信息 ECM1 和授权管理信息 EMM1,智能卡输出端输出控制字 CW1;控制模块输出端为 0 时,4 选 2 数据选择器输入端是授权控制信息 ECM2 和授权管理信息 EMM2,输出即为授权控制信息 ECM2 和授权管理信息 EMM2,智能卡输出端为控制字 CW2。

4-2 智能卡对数据的处理

在模块实现之前,先由数字电视机顶盒过滤出两路的授权管理信息 EMM、两路授权控制信息 ECM,并将其保存在内存中,通过控制器控制并将其传输给智能卡,智能卡解密相关数据并回传。保存授权管理信息 EMM 和授权控制信息 ECM 的目的是为了保证解密一路授权管理信息 EMM 和授权控制信息 ECM 信息时,另一路授权管理信息 EMM 和授权控制信息 ECM 信息正在保存或者更新,使之不丢失。

每一路授权控制信息 ECM 和授权管理信息 EMM 都要经过智能卡解密相关数据并回传的过程。当智能卡插入数字电视机顶盒时,解码器将从中读取智能卡的 CA_system_ID 及其它智能卡信息,在 TS 流中找到并过滤 CAT(PID=0x0001),通过 CAT 中的 CA_descriptor,找出对应该 CA_system_ID 的 CA_PID,此 CA_PID 即为对应该 CA 的授权管理信息 EMM 的节目标识符。获取授权管理信息 EMM 码流后,用智能卡中固化的 PDK 解密出 SK。完成以上步骤后,解码器再找到在节目映射表中的 CA_descriptor,并找出对应的授权控制信息 ECM 码流的 PID,用得到的 SK 对授权控制信息 ECM 解密就可以得到 CW,解扰器将 CW 作为输入控制参数,就可对码流数据进行解扰,恢复出原始信号。其具体步骤为:

a. 授权管理信息 EMM 消息的处理

授权管理信息 EMM 消息主要向用户提供收看付费电视的授权和管理信息。

第一步:数字电视机顶盒从智能卡的 0xEF00 中取得 CA_system_ID;

第二步:数字电视机顶盒从 CAT 表中的 CA_descriptor 中找到与该 CA_system_ID 对应的 CA_PID,即为控制解扰该节目的授权管理信息 EMM_PID;

第三步:条件接收模块根据条件接收模块专有的筛选参数和指令设置授权管理信息 EMM 消息筛选器,将授权管理信息 EMM 消息取出送给智能卡;

第四步:智能卡将用存储于 0x0002 中的 PDK 对授权管理信息 EMM 消息解

密，得到授权和管理信息；

第五步：重复“第三步”，等待新的授权管理信息 EMM 消息。

b. 授权控制信息 ECM 消息的处理

授权控制信息 ECM 消息提供了收看加扰节目的收看判据和解扰参数等信息。

第一步：用户通过电子节目指南 EPG 寻找要收看的节目；

第二步：用户选择要收看的付费节目，数字电视机顶盒从该节节目映射表的 CA_descriptor 中找到与该 CA_System_ID 对应的 CA_PID，即为控制该节目解扰的授权控制信息 ECM_PID，建立解扰参数表；

第三步：条件接收模块根据其专有的筛选参数和指令设置授权控制信息 ECM 表段筛选器，将授权控制信息 ECM 消息取出送给智能卡；

第四步：智能卡从授权控制信息 ECM 消息中得到接收判据，与智能卡保存的收视权力比较。如果收看判据不在收视权力范围内，则通过响应信息告诉用户无权收看该节目；

第五步：如果收看判据落在收视权力中，智能卡用解密出的 SK 将授权控制信息 ECM 消息中的解扰参数解密，得到控制字 CW，通过响应信息送给数字电视机顶盒使用；

第六步：数字电视机顶盒将控制字 CW 保存在解扰参数表里；

第七步：数字电视机顶盒收到传输包，如果包头的加扰控制位为“10”或“11”（注：在 DVB 中，“00”表示传输层未被加扰；“01”表示为今后 DVB 预留；“10”表示传输层加扰采用偶密钥；“11”表示传输层加扰采用奇密钥），则根据传输包的 PID 查找解扰参数表，如果加扰控制位的奇偶性与当前控制字奇偶性相同，则用当前控制字解扰；如果奇偶性不同，则更新当前控制字，将下一个控制字设定为当前控制字，并用于解扰；

第八步：数字电视机顶盒将新的授权控制信息 ECM 包传给智能卡，为了避免向智能卡重复传送授权控制信息 ECM 消息，数字电视机顶盒只在更新当前控制字时才向智能卡传送新的授权控制信息 ECM 消息。

4-3 解扰器模块的处理

解扰器在条件接收模块中有着举足轻重的作用。加扰过的节目流，在流经解扰器时必须进行解扰处理后，才能被音、视频解码器正确解码。针对条件接收系统，DVB 标准组织提出一种通用加解扰算法（Common Scramble Algorithm），这种统一的算法规范化各种不同条件接收的前端加扰部分，使同密方式得用（同密方式是指前端使用相同的控制字，但使用不同的加密电路和信息传送方。同时也规范化解码芯片在解扰电路上的设计，使解码芯片可应用在不同的条件接收系统中。虽然是通用加扰算法，但它的技术细节是不公开的，只有签署了 DVB 组织成员的保密协议后才能获取。

对节目流进行解扰，为保证收发两端序列的同步，将伪随机序列发生器的结构和初始状态编成一组数据，称为控制字，首先将智能卡解密得到的控制字输入解扰器；再者使用控制字产生伪随机二进制序列，就像 DVB 传输系

统中的 TS 流在外码编码前(发端)、后(收端)进行的扩散解扰那样,收发两端使用完全相同的伪随机序列;最后调用解扰算法,使用伪随机序列对被加扰的数据流进行恢复。

本实施例不仅限于上述实施例,还可以为

如图 7 所示的三路显示数字机顶盒,包括一台机顶盒有四个输入端和三个输出端,其中一个输入端为接入有线电视,另外三个输入端分别对应着三个遥控器,三个输出端分别接不同的电视机。遥控器 1 控制电视机 1,遥控器 2 控制电视机 2,遥控器 3 控制电视机 3。假设遥控器 1 单独使用时,智能卡只解密一路数据,因此只有电视机 1 有节目输出,电视机 2 和 3 没有节目输出。只有三个遥控同时使用时,智能卡分时解密三路数据,因此三台电视机有节目输出。

或为如图 8 所示的遥控器控制的两路显示数字机顶盒,包括一台机顶盒有三个输入端和两个输出端,其中一个输入端为接入有线电视,另外两个输入端分别对应着两个遥控器,两个输出端分别接不同的电视机。遥控器 1 控制电视机 1,遥控器 2 控制电视机 2。假设遥控器 1 单独使用时,智能卡只解密一路数据,因此只有电视机 1 有节目输出,电视机 2 没有节目输出。只有两个遥控同时使用时,智能卡分时解密两路数据,因此两台电视机有节目输出。

又或为如图 9 所示的单遥控器控制的两路显示数字机顶盒,包括一台机顶盒有两个输入端和两个输出端,其中一个输入端为接入有线电视,另外一个输入端对应着一个遥控器,两个输出端分别接不同的电视机。遥控器能分别控制电视机 1 和电视机 2,此时遥控器需要有一个控制按键,此按键按下时为控制电视机 1,再按下时为控制电视机 2,又再按一次又返回控制电视机 1,如此循环控制电视机 1 和 2。

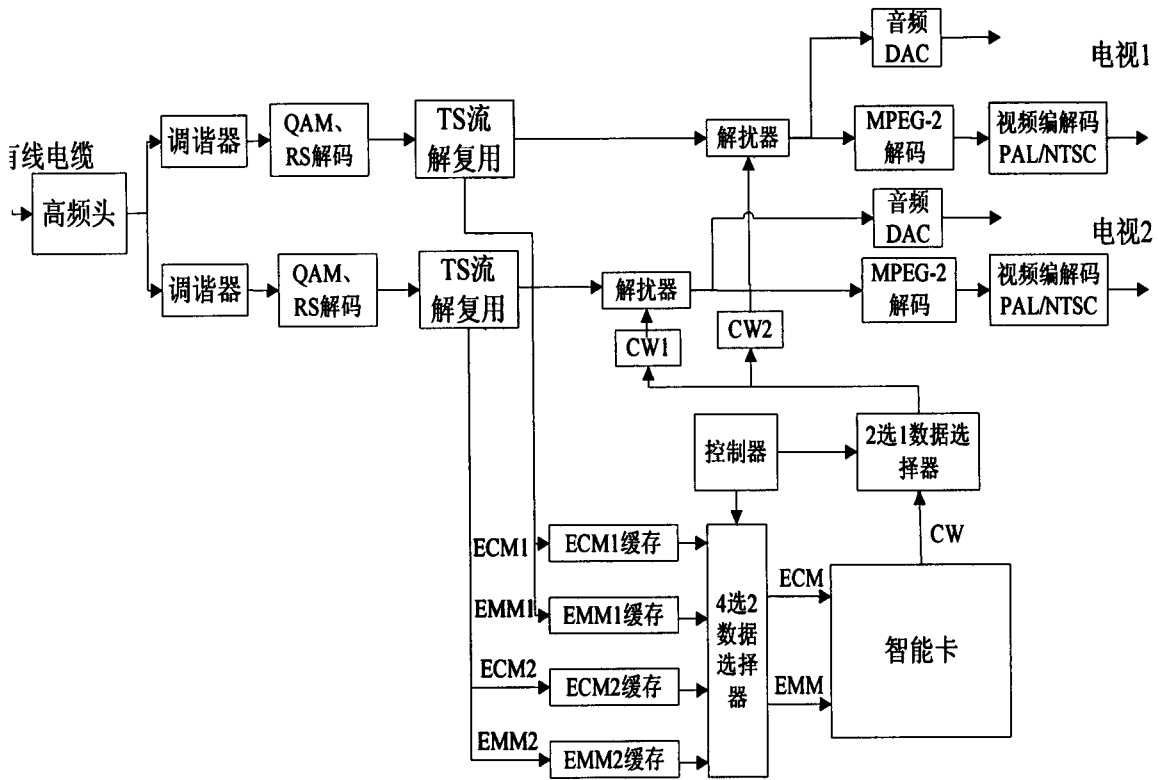


图 1

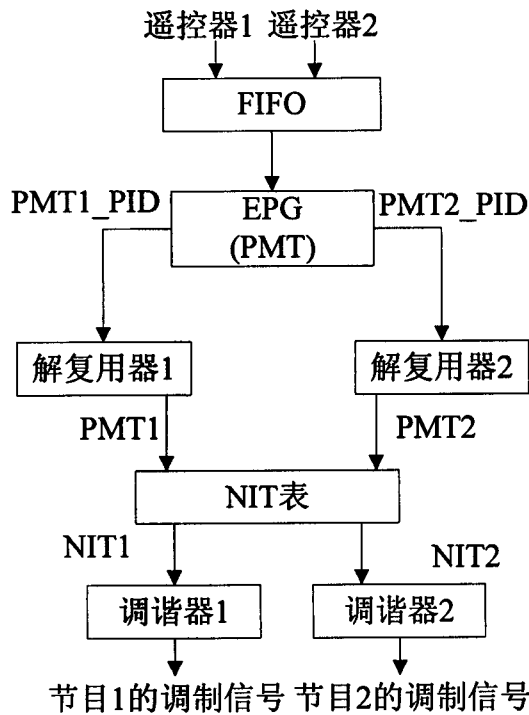


图 2

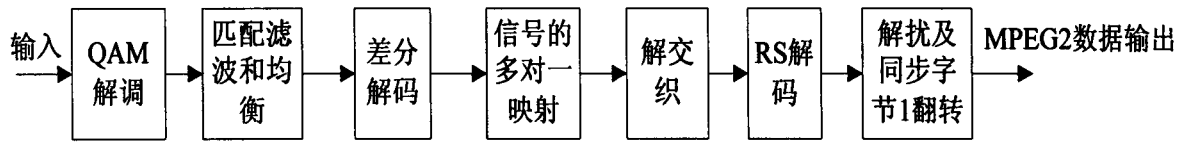


图 3

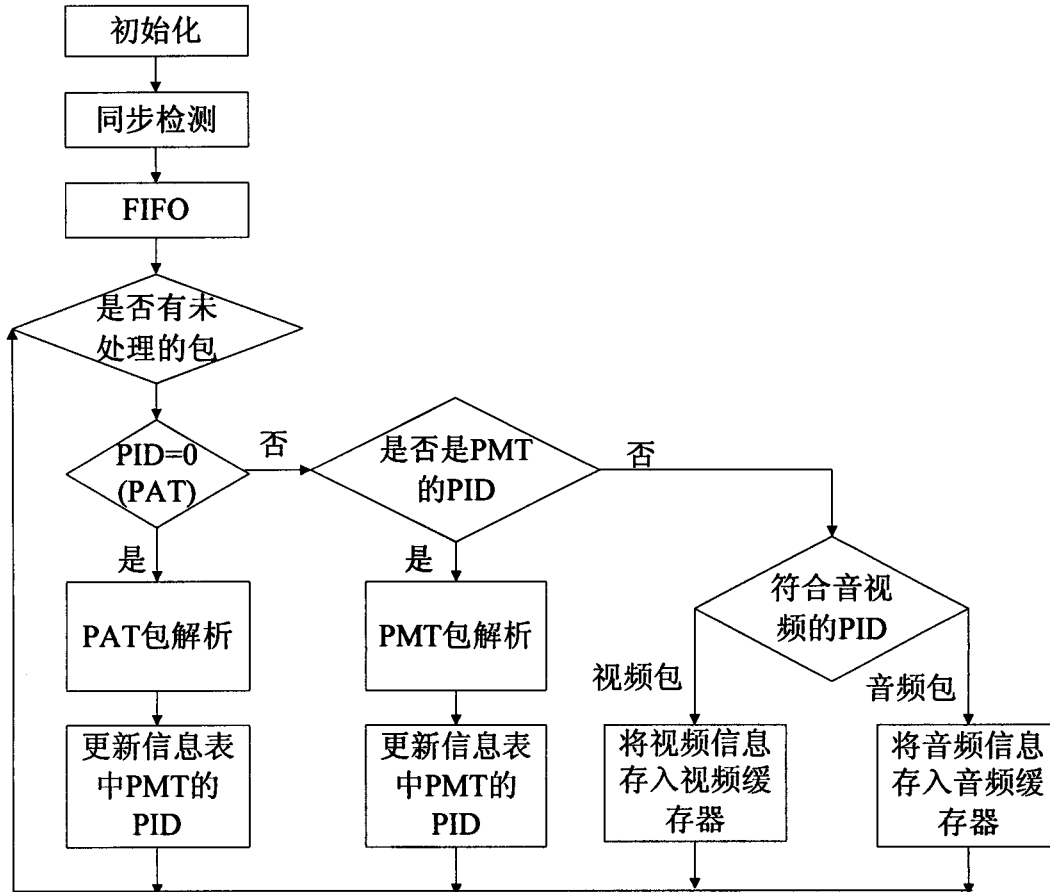


图 4

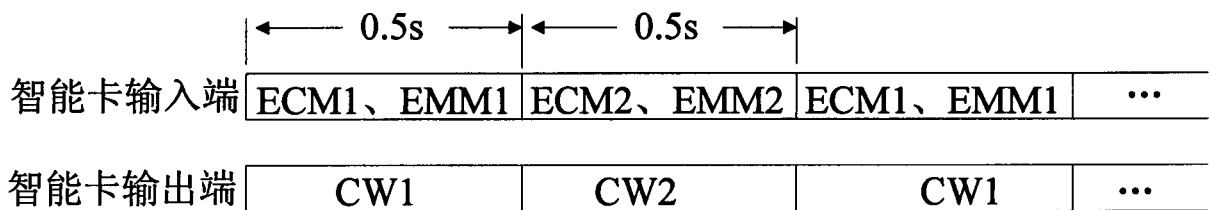


图 5

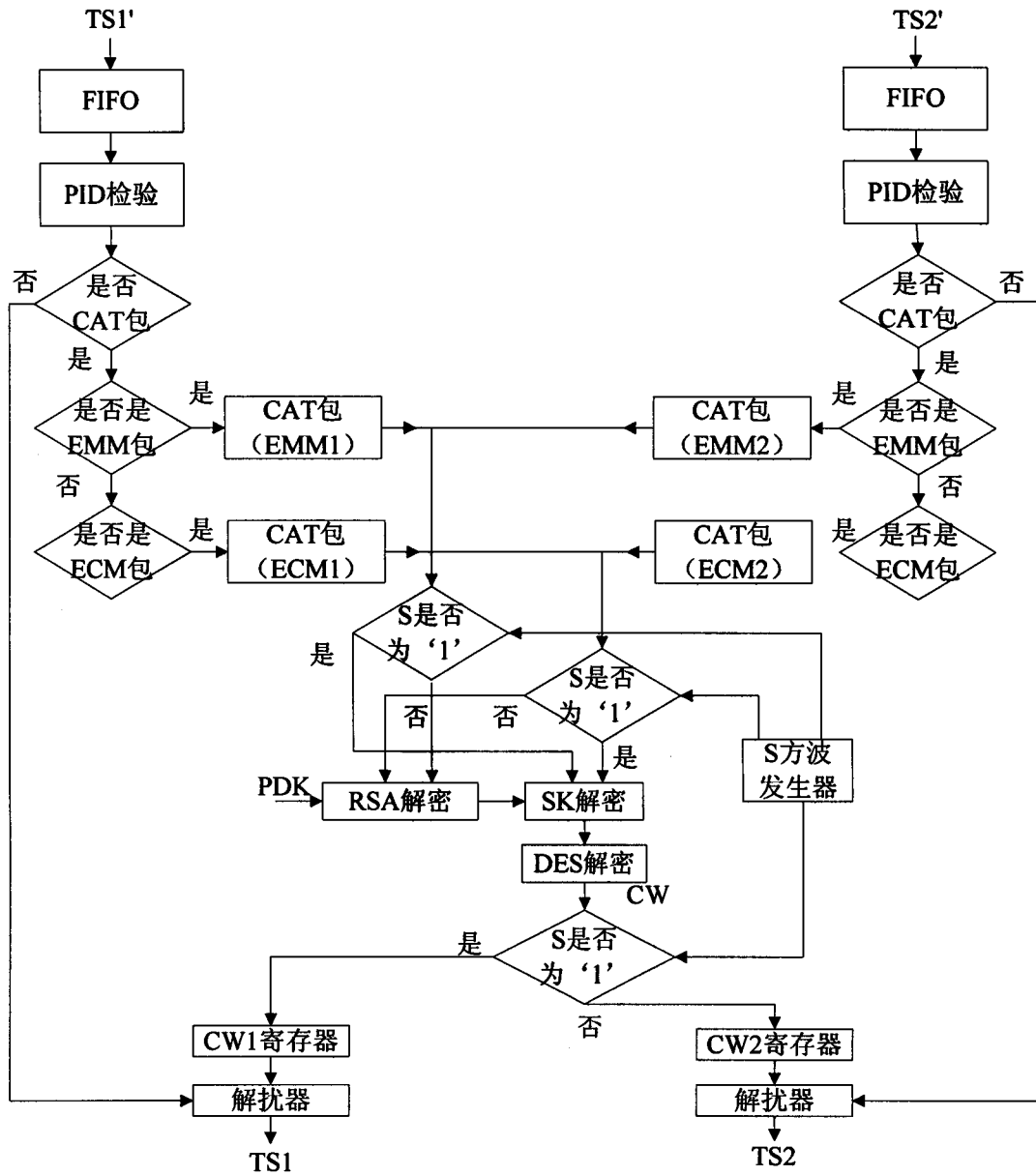


图 6

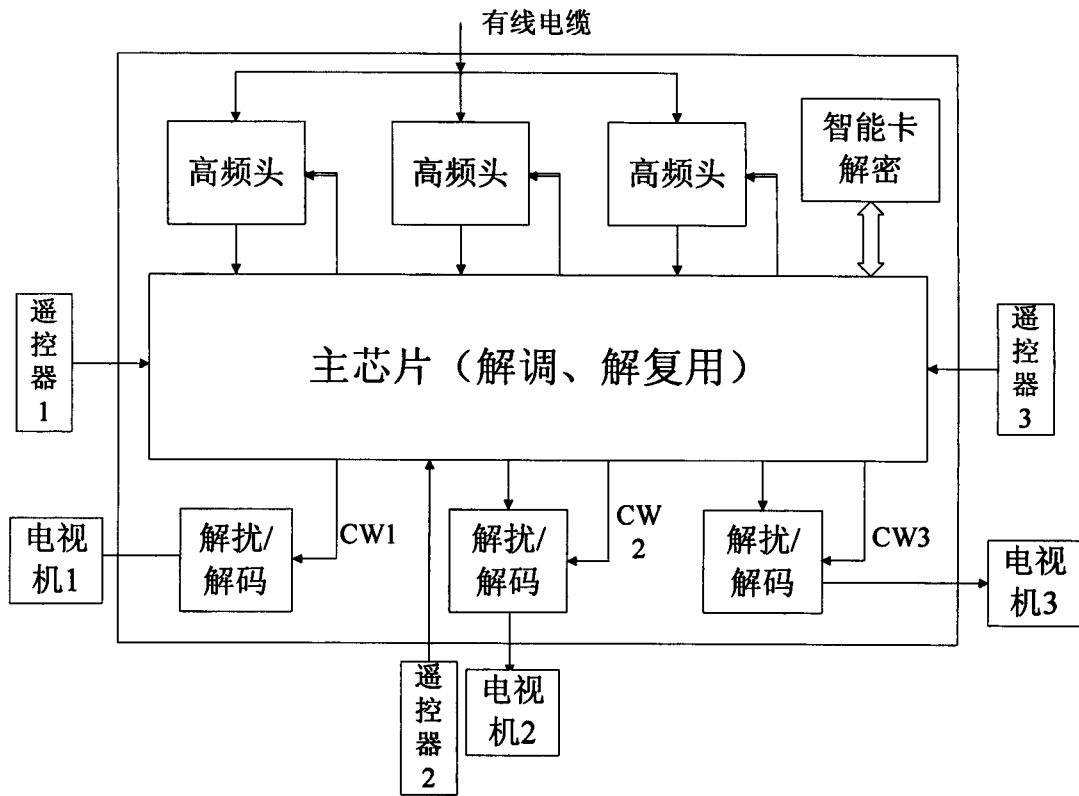


图 7

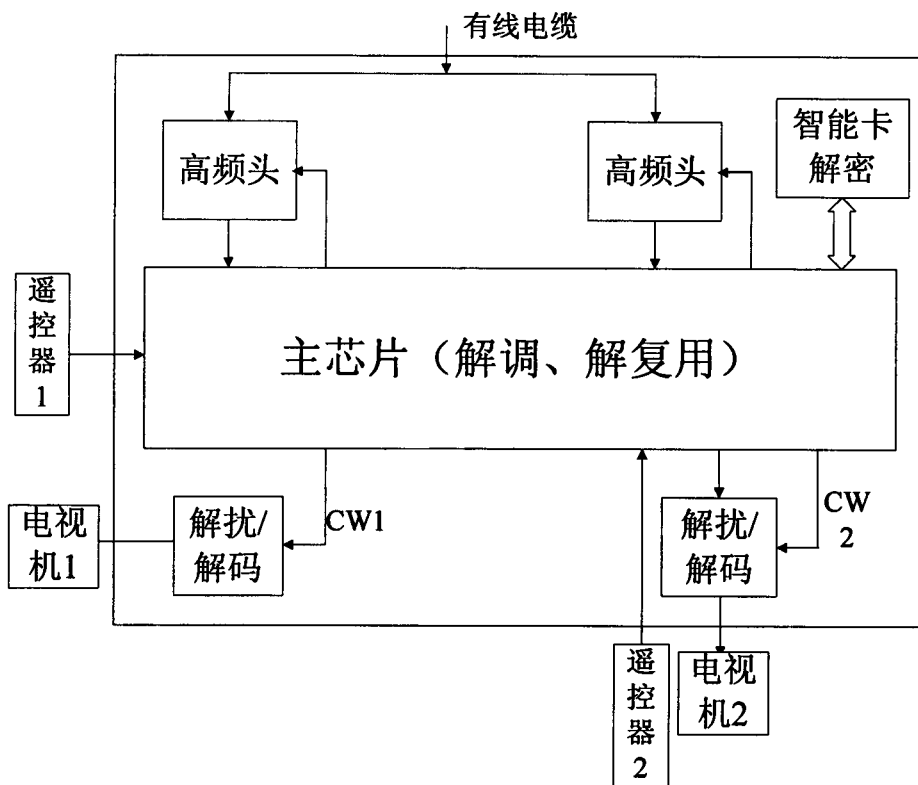


图 8

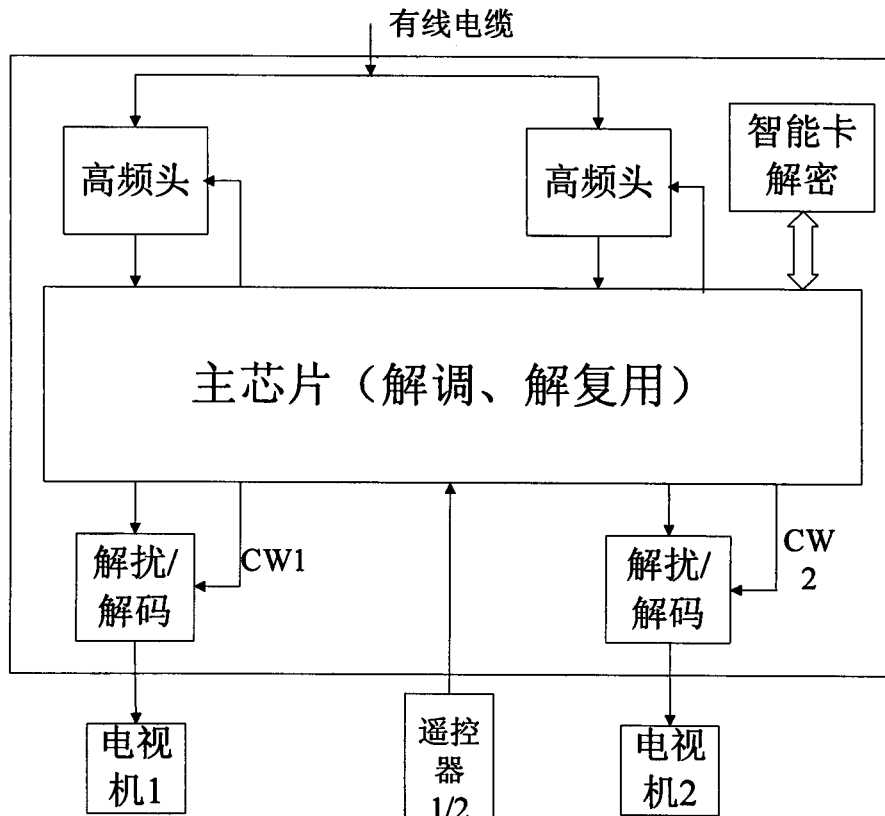


图 9