[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04N 7/167
H04N 7/16

[12] 发明专利说明书

[21] ZL 专利号 97180119.3

[45] 授权公告日 2004 年 9 月 22 日

[11] 授权公告号 CN 1168312C

[22] 申请日 1997.10.28 [21] 申请号 97180119.3
[30] 优先权
[32] 1996.11.27 [33] US [31] 08/762,483
[86] 国际申请 PCT/US1997/019374 1997.10.28
[87] 国际公布 WO1998/024236 英 1998.6.4
[85] 进入国家阶段日期 1999.5.27
[71] 专利权人 汤姆森消费电子有限公司
地址 美国印第安纳州
[72] 发明人 H·布拉特 T·E·霍尔朗德
K·E·布里格瓦特 M·S·戴斯
审查员 王素琴

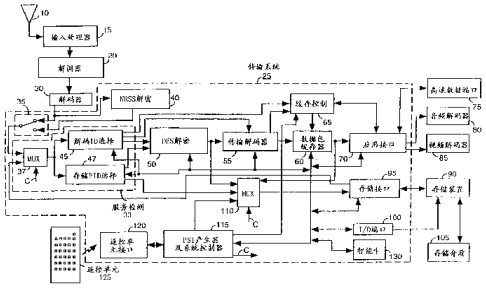
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 王 勇 王 岳

权利要求书 2 页 说明书 18 页 附图 4 页

[54] 发明名称 用于处理加密的视频数据以便产生解密的节目数据的方法

[57] 摘要

一种用来处理加密的视频数据以产生解密的节目数据的方法，该方法处理来自一个输入数据流的节目代表数据，输入数据流包括广播加密密钥和相关广播加密节目数据，包括步骤：利用广播加密算法对在输入数据流中接收的广播加密密钥解密以便提供在解密广播加密节目数据中使用的广播密钥；利用重放算法重新加密广播密钥，以提供在解密由存储介质恢复的加密节目数据时使用的加密重放密钥；以及通过从输出数据中排除广播加密的密钥和将加密重放密钥置于输出数据中，将加密重放密钥与相关广播加密节目数据一起格式化，以形成适于存储在存储介质上的输出数据。



ISSN1008-4274

1. 一种用来处理加密的视频数据以产生解密的节目数据的方法，所述方法处理来自一个输入数据流的节目代表数据，所述输入数据流包括广播加密密钥和相关广播加密节目数据，所述方法包括以下步骤：

利用广播加密算法对在所说输入数据流中接收的所说广播加密密钥解密以便提供在解密所说广播加密节目数据中使用的广播密钥；

利用重放算法重新加密所说广播密钥，以提供在解密由存储介质恢复的加密节目数据时使用的加密重放密钥；以及

通过从输出数据中排除所说广播加密的密钥和将所说加密重放密钥置于所说输出数据中，将所说加密重放密钥与所说相关广播加密节目数据一起格式化，以形成适于存储在存储介质上的输出数据。

2. 根据权利要求 1 的方法，其中所说的格式化步骤包括步骤：

用空数据替代所说的广播加密密钥。

3. 根据权利要求 1 的方法，其中所说的格式化步骤包括步骤：

将数据结构参数置入所说输出数据中，使其与排除所说广播加密密钥和将所说加密重放密钥置入而产生的数据结构兼容。

4. 一种用来处理加密的视频数据以产生解密的节目数据的方法，所述方法自适应处理来自一个输入数据流的节目代表数据，所述输入数据流包括广播加密密钥和相关广播加密节目数据，所述方法包括以下步骤：

接收用户产生的数据，用于选择（a）解密节目输出模式和（b）加密节目输出模式之一；

利用广播加密算法解密在所说输入数据流中接收的广播加密密钥，以提供供在解密所说广播加密节目数据时使用的广播密钥；

在解密节目输出模式，利用所说广播密钥解密所说广播加密节目数据，以便提供用于输出的解密节目数据；

在加密节目输出模式，利用重放算法重新加密所说广播密钥，以提供在解密由存储介质恢复的加密节目数据时使用的加密重放密钥；

将所说加密重放密钥与所说相关广播加密节目数据一起格式

化，以形成适于输出的加密节目数据，以及

从所说解密节目数据和所说加密节目数据中排除所说广播加密密钥以供输出。

5. 根据权利要求 4 的方法，其中所说的排除步骤包括步骤：

用空数据替代所说广播加密密钥。

6. 根据权利要求 4 的方法，还包括步骤：

响应用户产生的数据，将数据结构参数置入所说解密节目输出模式的输出数据中，将不同的数据结构参数置入所说加密节目输出模式的输出数据中。

7.根据权利要求 5 的方法，其中

所说的空数据取代在一个以下数据场中的所述广播加密密钥：MPEG 自适应场；MPEG 打包基本数据流 场；MPEG 数字存储介质控制命令 场；数字卫星系统 辅助数据包数据场；和非 MPEG 数据场。

8. 根据权利要求 4 的方法，其中所说用户产生的数据还识别 a)存储设备，和 b)拟存储的具体节目。

用于处理加密的视频数据以便产生解密的节目数据的方法

技术领域

本发明涉及数字信号处理，尤其涉及条件存取处理、解码、和加密数据包数据的格式化，用于例如由用户广播接收机、卫星或有线电视资料进行的存储。

背景技术

在视频处理和存储应用中，数字视频数据通常被编码以便符合一个已知标准的要求。一个广泛采用的这种标准将MPEG2(运动图象专家组)图像编码标准，以下称作"MPEG标准"。该 MPEG标准包括系统编码部分(ISO/IEC 13818-1，1994年6月10日)和视频编码部分(ISO/IEC 13918-2，1995年1月20日)，以下分别称作" MPEG系统标准"和 " MPEG视频标准"。编码成 MPEG标准的视频数据编码是处在一个打包的数据流的形式，通常包括许多节目信道的数据内容(例如在有线电视中的模拟频道1- 125)。付费服务节目信道，例如HBO™、 Cinemax™和Showtime™，通常是通过例如加密和扰频的方法防止未授权的访问。这些方法可以单独地、重复地或组合地使用，以便提供多个保护级别。

在一个解码器中，对付费服务频道的接入通常是由一个条件接通系统控制，该条件接通系统管理用户的付帐并且根据用户的权利控制节目的解扰以及解密。该条件接通系统可以在多种方式中确定接入是否为已经授权。例如，授权可以从预先编程在一个所谓的"智能卡"上的用户授权信息在解码器内确定。或者，授权可以在一个远距位置确定，并且在解码器中使用从遥控位置发送的用户授权信息实现，就象在一个有线电视中的计节目付费业务那样。该授权信息通常包括用于产生解扰和解密钥的码，用于节目的解扰和解密。但是，该授权信息可以不包括该密钥本身。

加密的和非加密的节目数据的处理以及用于存储、付帐和其它应用的相关加密和扰频码的管理存在许多问题。一个问题是由用户在当以加密的或非加密的方式存储一个节目用于以后时间的观看时所引起的对于维护加密码安全性的需要。再一个问题是提供一个系统，该系统允许对于一个节目的存储或重放，并且允许加密的和非加密的节目

数据的复制保护处理。

发明内容

这些正是根据本发明的一个系统旨在解决的问题。以下所称的"加密"包含扰频功能，其程度是要使得该扰频功能被用于避免未被授权的使用。

在一个处理加密的节目数据以便提供解密的节目数据用于输出的解码器系统中，如果加密密钥从该解码器外露，则在加密密钥的安全性方面将出现泄密。特别是，如果加密密钥或从中可得到密钥的加密码变得可被第三方接触时，安全性将被损害。例如，如果加密密钥从一个解码器输出并且被存储在可移动的存储介质上或者变得可从外部接触，则将出现这种危险性。一旦密钥是可外部存取的，例如在一个存储介质上，它们的安全性就取决于可用的逆向工程和码的破译技术的复杂性。本申请人已经认识到，希望改进一个解码器的禁止一个加密码或密钥的输出的能力。

根据本发明的原理，一个解码器禁止一个加密码或密钥的解密或者非加密的节目输出数据。从包括加密的节目数据和相关的加密码的输入的数据流产生解密的节目代表数据的方法包括对于该加密的节目数据进行解密的步骤。利用加密码对于加密的节目数据解密以便提供解密的节目数据。被形成的一个输出的节目数据流包括解密的节目数据但是不包括该加密码。

按照本发明的特征，加密码被排除在被形成用于支持对解密节目数据的解码并且被包括在该输出节目数据流中的辅助数据之外。

按照本发明的另一个特征，非加密的编码数据取代在输出数据流中的加密码。

本发明提供了一种用来处理加密的视频数据以产生解密的节目数据的方法，该视频解码器用于接收并处理数字视频数据，以供输出以及其后的远程或本地存储，所述方法处理来自一个输入数据流的节目代表数据，所述输入数据流包括广播加密密钥和相关广播加密节目数据，所述方法包括以下步骤：

利用广播加密算法对在所说输入数据流中接收的所说广播加密密钥解密以便提供在解密所说广播加密节目数据中使用的广播密钥；

利用重放算法重新加密所说广播密钥，以提供在解密由存储介质

恢复的加密节目数据时使用的加密重放密钥；以及

通过从所说输出数据中排除所说广播加密的密钥和将所说加密重放密钥置于所说输出数据中，将所说加密重放密钥与所说相关广播加密节目数据一起格式化，以形成适于存储在存储介质上的输出数据。

本发明还提供了一种操作视频解码器的方法，该视频解码器接收并处理数字视频数据，以供输出以及其后的远程或本地存储，所述方法自适应处理来自一个输入数据流的节目代表数据，所述输入数据流包括广播加密密钥和相关广播加密节目数据，所述方法包括以下步骤：

接收用户产生的数据，用于选择（a）解密节目输出模式和（b）加密节目输出模式之一；

利用广播加密算法解密在所说输入数据流中接收的广播加密密钥，以提供供在解密所说广播加密节目数据时使用的广播密钥；

在解密节目输出模式，利用所说广播密钥解密所说广播加密节目数据，以便提供用于输出的解密节目数据；

在加密节目输出模式，利用重放算法重新加密所说广播密钥，以提供在解密由存储介质恢复的加密节目数据时使用的加密重放密钥；

将所说加密重放密钥与所说相关广播加密节目数据一起格式化，以形成适于输出的加密节目数据，以及

从所说解密节目数据和所说加密节目数据中排除所说广播加密密钥以供输出。

附图说明

图1表示一个根据本发明的视频信号接收机系统，用于以用户可选择的、加密或非加密的形式自适应地产生一个节目代表数据流。

图2和3示出一个流程图，用于提供适合于存储在一个可选存储介质上的节目代表数据流，并且用于执行该相关用户的付帐。

图4示出一个处理的流程图，用于从一个选择的存储设备恢复被选择加密或非加密的节目，并且用于依据节目的恢复收帐一个用户。

具体实施方式

图1示出根据本发明的一个视频信号接收机系统，用于以用户可选择的、加密或非加密的形式自适应地产生一个节目代表数据流。虽然该公开的系统是以用于接收表示广播节目的MPEG编码传送数据流的一

个MPEG兼容系统的环境而被描述的，但是它只是实例。本发明的原理还可以被用于包括采用其它类型的编码数据流的非MPEG兼容系统的其它类型的系统。而且，虽然该公开系统被描述为进行广播节目的处理，但是只有一个示范。术语‘节目’被用于表示任何形式的打包数据，例如电话信息、计算机程序、互联网络数据或其它通讯联络。

从总体上看，在图1的视频信号接收机系统中，利用视频数据调制的载波由天线10接收并且由单元15处理。产生的数字输出信号被解调器20解调并且由解码器30解码。来自解码器30的输出由响应来自遥控装置125的命令的传送系统 25处理。系统25提供压缩数据输出，用于存储、更进一步的解码或对于其它装置的通讯联络。系统25包括一个条件接通系统，用于管理用户的付帐以及用于根据用户的授权控制节目的解扰和解密。通过利用遥控装置 125的屏幕上菜单选择，一个视频信号接收机用户选择他希望观看的节目、他希望存储的节目、使用的存储介质的类型以及该节目是以加密的或者非加密形式存储。系统25还提供一个机构用于实现从一个非加密节目的数据流实时或非实时地除去加密码。

视频及音频解码器85和80分别解码来自系统25的压缩数据以便提供用于显示的输出。数据端口75提供了一个接口，用于从系统25到其它装置的压缩数据的通信，例如计算机或高清晰度电视(HDTV)接收机。存储设备90把来自系统25的压缩数据储存在存储介质105上。重放模式中的装置90还支持对于来自存储介质105的压缩数据的检索，用于系统25进行的解码、对于其它装置的通信或存储在一个不同存储介质(为了图的简化没有示出)上的处理。在系统25中的条件接通系统支持解密和付帐，用于程序存储、重放、或包括对于其它装置的通信的更进一步处理。系统 25的条件接通系统对于来自广播信号源的已收数据处理程序所使用的解密和付帐机制不同于对于来自本地存储器信号源的数据播放的处理程序所使用的解密和付帐机制。

详细地考虑图1，通过天线10接收的视频数据调制的载波由输入处理器15转换成数字方式并被处理。处理器15包括射频(RF)调谐器和中频(IF)混频器以及放大级，用于把输入的视频信号降频转换到适合于更进一步处理的较低频带。产生的数字输出信号由解调器20解调并且由解码器30解码。从解码器30输出的信号由传送系统25进一步处理。

经过选择器35，把解码器30的输出或者由NRSS（国家的可更新的标准委员会National Renewable Standards Committee）解扰单元40进一步处理的该解码器30的输出提供到多路复用器(mux)37。选择器35检测一个可插入的、NRSS兼容的解扰卡的存在，并且只要当是该解扰卡当前被插入在该视频信号接收机单元中时(NRSS可移动的条件接通系统被定义在EIA草案文件IS－679，项目PN－3639)，就把单元40的输出提供到mux 37。否则选择器 35把解码器30的输出提供到mux 37。例如，该可插入的解扰卡的存在允许单元40解扰附加的付费服务节目信道，并且把附加的节目服务提供给观众。应该注意，NRSS单元40和智能卡单元130（智能卡单元130将在稍后讨论）共享同一个系统25的接口，使得在任何时间只有或者是一个NRSS卡或者一个智能卡可以插入。另外，该接口可以是单独的，以便允许串联或者并联操作。

从选择器35提供到mux37的数据是在如MPEG系统标准部分2.4定义的MPEG适应打包传送数据流的形式，并且包括一个或多个节目信道的数据内容。包括特定节目频道的单独的数据包是由数据包标识符(PID)识别的。传送数据流包括对于发送进行支持和对于传送编码数据进行解码的辅助数据。这种辅助数据包括节目说明信息(PSI)，用于标识该PID并且汇编单独的数据信息包，以便恢复包括打包数据流的节目信道的全部内容。通过屏幕上的菜单选择，一个视频信号接收机用户利用遥控装置125选择所希望观看的节目、希望存储的节目用于存储的介质，并且选择是否该节目是以加密的或非加密的形式存储。系统控制器115使用经过接口120提供到配置系统25的选择信息，以便选择用于存储和显示的节目，并且产生适合于所选择的存储设备和介质的PSI。经过数据总线并且借助利用控制信号C对于经由mux37和110进行的选择，控制器115以在系统25的单元45、47、50、55、65和95中的控制寄存器值进行设置，来配置系统25的这些单元。而且控制器115是可编程序的，以便允许实时和非实时地从将要被存储或处理的一个非加密节目数据流中除去加密码。该特性通过防止密钥超出系统25之外的输出而增加了加密的安全性，从而限制了第三方的使用。

响应控制信号C，mux37或者从单元35选择传送数据流，或者以重放模式经由储存接口95从存储设备90选择检取的数据流。在正常的、非重放操作情况中，包括用户选择将要观看的节目的数据信息包通过选

择单元45由它们的PID识别。如果在该选择的节目数据包的标题数据中的一个加密指示符指示该数据包是加密的，则单元45将把该数据包提供到解密单元50。否则单元45将提供非加密的数据包到传送解码器55。类似地，包括用户选择用于存储的节目的数据信息包通过选择单元47由它们的PID识别。根据数据包标题加密指示符信息，单元47把加密的数据包提供到解密单元50或把非加密的数据包提供到mux 110。

单元45和47使用PID检测滤波器，该滤波器把由mux37提供的传入数据包的PID与由控制器115预先输入在单元45和47的控制寄存器中的PID相匹配。预先输入的PID被使用在单元47和45中以便标识将要存储的数据信息包和将要被解码使用在提供一个视频图像中的数据信息包。该预先输入的PID被存储于单元45和47的查询表中。该PID查询表被存储器映射到在单元45和 47中的密钥表，把密钥与每一预先输入的PID关联。该存储器映射的 PID和密钥查询表允许单元45和47把包括一个预先输入的PID的加密数据包与实现它们的解密的相关的密钥相匹配。非加密数据包不具有相关的密钥。单元 45和 47都提供识别数据包和它们的相关的密钥到解密器50。在单元45中的 PID查询表也被存储器映射到一个目标表，该目标表把包括预先输入PID的数据包与在数据包缓存器60中的对应目标缓冲区单元相匹配。随着由控制器115指定的 PID，与由用户选择用于观看或存储的节目相关的密钥和目标缓冲区单元地址被预先输入到单元45和47中。

由适应ISO 7816-3的智能卡系统130根据从输入数据流提取的加密码产生密钥。密钥的产生受客户授权的控制，该客户授权是根据预先存储在可插入的智能卡本身上的编码信息确定的(1989年的国际标准化组织文件ISO 7816 - 3定义用于该一个智能卡系统的接口和信号结构）。用户授权信息可以通过在输入数据流中的指令以刷新在该可插入的智能卡上的编码信息的方式而被周期地改变。

该可插入的、ISO 7816 - 3适应的智能卡有利地包括三个算法。其中的两个算法函数被称之为广播加密算法，被指定用于从来自系统25的非重放模式中的输入数据流提取的广播加密码产生加密钥。通过解密在智能卡130自身内的广播加密码，一种广播加密算法产生加密钥。使用在系统25中的第三算法函数用于以系统25的存储和重放模式对于得出的广播加密钥进行加密和解密。该重放算法在可插入的智能

卡中加密和解密广播加密钥。但是，在其它系统中，该重放算法函数可以放置在别处，例如在一个解码器中。

使用在智能卡130中的三个加密算法可以是多种类型的任何一个，并且该重放算法不需要和广播算法是同一个类型。用于示范的目的，广播和重放算法被认为是在联邦的信息标准(FIPS)公布46、74和81（由商业部门全国技术情报服务处提供）中定义的数据加密标准(DES)算法函数。但是，这些算法函数可以是另外的类型，例如Rivest-Shamir- Adlemann（ RSA）函数类型。

存在于该智能卡上的两个广播加密算法的每一个都可以由在该输入数据流中的控制信息所启动。两个广播加密算法被包含在该智能卡中以便允许一个服务提供者在用于全部客户的广播加密算法中实现同时的修改。在该新的算法被使用的日期之前，一个服务提供者通过把具有新算法的一个新智能卡安全地发布到全部客户来改变广播加密算法。在该改变之日期，该服务提供者同时地：通过更新在广播数据流中的控制信息命令该智能卡更改为新的算法；利用新的算法加密节目；并且把更新的加密码插入在广播数据流中。算法中的修改可以由一个服务提供者在一个规则的基础上或按照期望时常地实现，以便保护加密系统的安全性并且防止密码泄露以及未被授权的节目接入。

本发明人已经认识到，使用这样一个包括改变密钥的加密系统提出了以加密方式存储节目的一个问题。具体地说，一旦该智能卡已经改变并且该智能卡算法已经更新，随着一个相关的广播加密码以加密形式存储的节目也许不能够被解密。这是因为在该智能卡上的该新算法是不与利用一个早期版本智能卡相关的加密码兼容的。结果是，该新的智能卡算法不能从该存储加密码得到该需要的广播密钥。存储加密节目的这种装置不能被解密并且一旦一个系统智能卡已经改变，则不能使用。

为了克服这个问题，第三个不同算法，即重放算法被结合在该智能卡上。该第三算法函数，称为重放算法，被使用在用于加密广播密钥的系统25的具体的操作和模式中，以便在系统25的存储和重放模式中构成重放加密码。

一旦由重放算法加密，则该重放加密码可以随着加密节目内容被安全地存储在一个存储介质上。依据加密节目的重放，该重放算法函数

解密该存储的加密码，以便得出源广播密钥，以便启动该加密节目内容的解密。得出的广播密钥被单元 50所用，以便如稍后描述的那样解密该加密的节目内容数据包。这种重放算法不象两个广播算法那样频繁地改变，并且在智能卡的顺序版本中可以被保持无变化。这就使得存储的加密节目能够被解密和使用，尽管在智能卡和广播加密算法中存在改变。

根据这种数据加密标准(DES)，由单元45和47提供到单元50的数据包被加密。图1的系统25的解密单元50在对于这些加密的数据包进行解密中使用这种DES算法函数。在系统25的其它实施中，单元50可以选择使用其它算法函数，例如先前提到的RSA函数。利用由智能卡130经过单元45和47提供的对应密钥，单元50应用已知的技术来解密这种加密的数据包。包括用于显示的节目的来自单元50的解密数据包和来自单元45的非加密数据包被提供到解码器55。包括用于存储的节目的来自单元50的解密数据包和来自单元47的非加密数据包被提供到 mux 110。

单元60包括可由控制器115访问的数据包缓存器。这种缓存器之一被分配来用于保持预定为控制器115所使用的数据，而其它三个缓存器被分配来用于保持预定为应用装置75、80和85所使用的数据包。稍后讨论的更进一步的代替缓存器被用于保持为了取代加密编码数据的数据。在单元60中既由控制器115又由应用接口70执行的对于存储在缓存器中的数据包的存取由缓冲控制单元65控制。单元45把一个目标单元格标志提供到单元65，用于由单元45识别的每一数据包，以便进行解码。该标志指示个别单元60目标位置用于识别的数据包，并且由控制单元65存储在一个内存储器表中。控制单元 65根据FIFO原则确定与存储在缓存器60中的数据包相关的一系列读取和写入指针。这种结合目的标志的写入指针实现来自单元45或 50的一个识别的数据包在单元60中的适合目标缓存器之内的下一个空的位置中的顺序存储。通过控制器115和应用接口70，读取指针实现来自该适当的单元60的目标缓存器的数据包的顺序读出。

由单元45和50提供到解码器55的非加密和解密的数据包包括一个由MPEG系统标准的 2.4.3.2部分定义的一个传送标题。解码器55从该传送标题确定该非加密和解密的数据包是否包括一个适应场(每一

MPEG系统标准)。该适应场包括定时信息，该定时信息包括例如程序时钟基准(PCRS)，该基准实现内容数据包的同步和解码。一旦检测到一个定时信息包，即包括一个适应场的数据包,解码器55就通过在一个中断结构之内设置一个系统中断来通知控制器115该数据包已经被接收。此外,解码器55改变在单元65中的定时数据包目标标志并且把该数据包提供到单元60。通过改变单元65的目标标志,单元65把解码器 55提供的定时信息包转移到指定给控制器115用于保持数据的装置60缓冲位置,而不是指定到应用缓冲器位置。

一旦接收通过解码器55设置的系统中断,控制器115读取该定时信息和PCR值并且将该定时信息和PCR值储存在内部存储器中。连续的定时信息包的PCR值被控制器115使用以便调整系统25的主时钟(27MHz)。在基于PCR和基于主时钟的对连续的定时数据包的接收之间的时间间隔的估算之间的差值由控制器115产生，被用于调整系统25的主时钟(为了简化制图而没示出)。这是通过控制器115把得出的时间估计差值应用来调整用于产生主时钟的一个压控振荡器的输入控制电压实现的。在把定时信息储存在内部存储器之后，控制器115复位该系统中断。

由解码器55从单元45和 50接收的包括音频、视频、标题和其它信息的节目内容的数据包由单元65从解码器55引导到在数据包缓存器60中的指定应用装置缓存器。应用控制单位70从在缓存器60中的指定的缓存器按顺序检取音频、视频、标题和其它数据，并且把这种数据提供到对应的应用装置75、 80和 85。应用装置包括音频与视频解码器80和 85以及高速数据端口75。数据端口75可用来提供例如计算机程序的高速数据到例如一台计算机。另外，端口75可用来把数据输出到一个HDTV解码器。

包括PSI信息的数据包由单元45识别，预定由控制器115缓存在单元60中。以相似于针对包括节目内容的数据包所描述的方式，这种PSI数据包由单元65经单元45、 50以及55直接送到缓存器。控制器115从单元60读取PSI并且储存在内部存储器中。

控制器115使用图2和3的这种处理以便产生适合于存储在介质105上的一个节目数据流，并且针对这种存储而收帐一个用户。控制器115还采用图2和3的这种处理既产生用于存储在介质105上的一个重放加

密码又从将要被存储的节目数据流除去这种源广播加密码。按照先前描述的方式，图2和3的这种数据包标识和指向的处理是由控制器115、控制单位65和PID、单元45和 47的目标和密钥查询表控制的。

这种CPSI(压缩节目说明信息)包括涉及将要被存储的特定节目的信息，而PSI包括涉及在输入到系统25的数据流中的全部节目的信息。结果是,这种CPSI比PSI占用较小存储容量并且引发较小的额外开销。此外,假定给出一个固定的额外开销的约束,这种CPSI可以在一个数据流中比PSI更频繁地重复，并且如此可以得出并且施加该PSI，以便减小节目内容的恢复的等待时间。

在 MPEG系统标准2.4.4部分定义的PSI包括四个非加密单元或信息表。这些是节目结合表(PAT)、节目图表(PMT)、网络信息表(NIT)和条件接通表(CAT)。每个表都是来自由一个特定PID识别的数据信息包形成的。该PMT定义标识包括一个节目的单独的打包数据流的PID标志。这些单独的数据流被称为在 MPEG标准中的基本数据流。基本数据流包括例如视频、用于各种语言的音频以及标题数据流。PAT把节目编号与实现包括该PMT的数据包的标识和汇编的PID相关联。该NIT是可选的和可以被构成和用于定义物理网路参数，例如卫星发送信道频率和转发器信道。CAT包括条件接通信息，例如控制对于根据用户授权的节目的存取的加密码。

在图2的步骤205中,控制器115 (图 1)在系统供电时，随起始步骤200之后执行一个初始化过程。在步骤205中 ,控制器115利用针对PAT和CAT表(分别为PID十六进制值0000和十六进制值0001)的 MPEG定义的PID值加载单元45(图表 1)的 PID检测滤波器.此外,控制器115通过更新该单元45目标表，把PAT和CAT数据包预先指定到在单元60中的控制缓冲器。在单元65的控制之下，由单元45检测的PAT和CAT数据包经过解码器55被引导到单元60中的控制缓冲器。在步骤205中,控制单元65经过一个PSI中断通知控制器115该 PSI数据包存在于单元60中。一经收到该PSI中断,控制器115重复地存取在指定的单元60缓存器中的数据包,并且把完整的CAT和 PAT数据储存在内部存储器中.在从该PAT确定标识PMT和 NIT数据包的PID之后，控制器115重复该处理，以便把完整的PMT和NIT数据存储在内部存储器中。当接收机被开启电源时，一经收到PSI中断，控制器115就连续地存取缓存器60并且捕获在内部

存储器中的PSI数据包。结果是，控制器115捕获在其内部存储器中的PAT、PMT、NIT和CAT数据，包括输入到系统25的传送数据流的完整的PSI。

在图2的步骤210，用户产生的标识一个用户希望存储的节目、以及将要被以加密方式存储的那些节目、以及用于存储的介质和装置的数据(SP、SM、SE)被输入到控制器115(图1)。针对多种原因，用户可以选择加密存储而不选择非加密存储。例如，一个服务提供者可以使得其比较便宜地以加密方式存储，作为在用户复制之后进行数目的限制的一种方式。服务提供者可以经过预先存储的智能卡授权信息，通过控制对于加密节目的存取实现这种方式。输入到控制器115的选择数据由用户通过屏幕上显示的菜单选择，利用遥控装置125经过接口120输入。在步骤 215中，响应输入选择数据(SP)，控制器115从存储的PSI得出针对选择节目的PID。单元47检测滤波器被利用将要被控制器115存储的节目的PID加载。这将启动单元47标识包括被选择用于存储的节目的数据包。在步骤215 ，控制器115还预先利用零数据加载该单元60代替缓存器。该零数据将要被在以加密方式广播的节目中出现的广播加密码所替代。

在图2中的步骤215 ，单元47(图1)把非加密的数据包提供到mux110，并且把加密的数据包(由在分组标题数据中的加密指示符识别)随着相关的广播密钥一道提供到解密单元50。在图2的步骤215中，按照先前描述的方式，在从用于选定节目(SP)的CAT获得的加密码由智能卡130解密而产生广播密钥之后，该广播密钥由控制器115提供到单元47。但是，如果选择数据SE请求被加密存储，则单元47就把将要被存储的加密数据包传递到mux 110。结果是，在图2的步骤 215中 ，响应选择数据SE，包括将要被存储的节目的数据包(SP)或者以加密方式或者以解密方式提供到mux 110。

在步骤217-227中 ，控制器115从完整的节目说明信息形成用于选定用于存储的节目的压缩的节目说明信息(CPSI)，完整的节目说明信息是从输入到系统25的传送数据流捕获的。如果该SE数据要求加密存储，则控制器115随决定步骤217之后执行步骤227。在步骤227中 ，控制器115在智能卡系统130中应用重放算法函数，以便加密在步骤215中先前产生(由广播加密码的解密)的广播密钥，以便形成用于将要被存储

的节目的一个重放加密码。CPSI被形成，以便包括该重放加密码但是排除最初存在于输入到系统25的传送数据流的PSI中的广播加密码。结果是，被形成用于预定用于存储的节目的数据流除去其相关的广播加密码。这就防止了在密钥安全性中的危害，这种危害出现在当密钥被存储在可由第三方访问的可移动的存储介质上的时候。一旦密钥在一个存储介质上是可访问的，则它们的安全性就将依赖存在的逆向工程和密码破译技术。在这种系统中，多个级别的安全性是通过不储存该广播加密码（从广播加密码得出该广播密钥）和通过以加密形式储存该广播密钥的方式而提供的。更进一步，即使该密钥被推导出用于该存储节目，但是它将不提供对于当前广播节目的存取，该广播加密算法针对当前广播节目是有规则地改变的。

如果该SE输入数据不要求加密存储，则控制器115随决定步骤217之后执行步骤227。在步骤225中，控制器115从输入到系统25的传送数据流的PSI形成预定用于存储的节目的CPSI，并且从该CPSI除去加密码。

该描述的加密系统只是示例性的。另外的加密结构可以在数据流的信息区而不是PSI中传送广播和重放加密码。除PSI的产生外，其它加密结构可能还需要以不同间隔产生和插入加密码。如果广播加密码不在PSI中传输，则可能需要以其它数据代替这些码以使它们被从形成的用于将要被存储的节目的数据流中除去。以一定时间相隔出现而不是以CPSI出现的用于代替广播加密码的空数据将在稍后讨论。具体地说，例如当该加密码是在分组标题中传输时，以实时方式，即以数据包的频率对于广播加密码的代替将结合步骤237 - 249讨论。

在步骤230中，根据MPEG句法(MPEG系统标准的2.4.4.3-2.4.4.11)，控制器115把 CPSI数据形成多个部分。在步骤230，控制器115还把标题数据添加到CPSI数据部分，以便格式化和打包用于插入到将要被存储的数据流中的该CPSI数据。根据 MPEG系统标准的2.4.3.2和2.4.3.3部分，控制器115从存储在该控制器 115的内部存储器中的PSI标题数据创建该标题。但是，相对于对应PSI部分的数据，CPSI部分的数据在长度上不同。因此，由控制器115创建包括‘连续性计数’指示符和有效负载单元开始指示符的新标题参数，并且把分别的指示符插入在该标题数据中的分别的指示符中。例如，由控制器115

创建的新的连续计数指示符反映用于该CPSI单元的数据包的数目而不是对应于PSI单元的每一PID数据包的不同编号。例如,由控制器115创建的新的有效负载单元开始指示符标识的是该CPSI部分的第一字节而不是对应于PSI部分的第一字节。

在步骤230之后,图2的流程以图3的步骤237继续进行。在步骤237,控制器115确定广播加密码是否在数据流场而不是该CPSI中被传输。具体地说,控制器 115确定是否广播加密码是在分组标题(每一MPEG系统标准句法部分2.4.3.4)的MPEG兼容适应场中传输。如果是,则控制器115执行步骤249,以便创建包括CPSI数据包和节目内容数据包的一个合成数据流,以空数据替代在分组标题中的广播加密码。该加密码的代替是以数据包频率一个数据包接着一个数据包地执行的。

在步骤249中,在控制器115的控制之下,在步骤215期间(图2)预先输入到在单元60的替代缓存器中的替代数据包数据从单元60提供到mux 110 (图 1)。此外,在步骤249中 ,在步骤230中形成的处于打包形式的MPEG兼容部分的数据被控制器115提供到mux 110(图 1)。如先前结合步骤215讨论的那样,来自单元47或单元50的节目内容数据包的数据流还被提供到mux110。在步骤249中,控制器115利用路径选择信号C在输入到mux 110的节目内容数据流、CPSI数据流和替代数据之间多路复用,以便创建一个合成数据流,由mux110输出到存储接口95。该合成数据流包括节目内容数据包和以空数据替代在分组标题中的广播加密码的CPSI数据包。

控制器 115 根据 PSI 中断信号和来自控制单元 65 (图 1) 的替代定时信号同步将 CPSI 数据包和空数据插入拟存储的节目数据流的过程。PSI 中断表明 PSI 数据包在缓存器 60 中的存在,如结合步骤 205 所讨论的那样。替代定时信号将空数据的插入和广播加密代码在数据包标题中的出现同步起来。按照如此方式, CPSI 的打包部分插入到 PSI 位置以替代 PSI 的相应部分,并且广播加密代码被除去。未加密的 CPSI 数据可以插入被输入 mux100 的加密或未加密的节目内容数据流中,以便产生供存储的加密或未加密节目。

应当注意在步骤 249 执行的广播加密码的替代工作也可以对在数据流场中传送的除 MPEG 数据包标题适应场外的代码进行。此外,加密码可以在除适应场出现的间隔以外的其它间隔被代替。例如, 空数据可以用于替代出现在 MPEG 和非 MPEG 兼容流的多个位置处的加密码: 包

括专有数字卫星系统（DSS™）内的辅助数据包；打包的初步流（PES）场（根据 MPEG 系统标准语法部分 2.5.3.7-2.5.4.2）；数字存储介质控制指令（MSMCC）场（根据 MPEG 系统标准语法附录 A）；以及根据其它数据传输协议比如标准化 CEBus 控制协议（家庭自动化标准 (CEBus)，EIA/IS－60，1989 年 11 月）格式化的非 MPEG 数据包。

如果加密码是以数据包的形式传送的，在数据包中代码本身是序列的仅有的数据项，那么可以从输出数据流中完全省去该携带代码的数据包。这是通过经 PID 选择单元 45 和 47（图 1）丢弃数据包，或者在于步骤 249 执行的多路复用操作期间略去这些数据包而完成的。但是，在输出数据流内的数据结构敏感的参数和数据速率也许需要更新，以反映由于这样的数据包数据略去而引发的数据速率改变。

在步骤249，存储接口（图1）接收拟以打包数据流（下称CPSI流）的形式存储的节目，其中包含CPSI和来自mux110的空数据．在步骤254（图3），在步骤249之后，系统25内的条件接通系统针对节目存储（或向其它之中的传送）向用户收费。通过将收费信息存储在该可插入智能卡自身中而向用户收费。收费信息的存储是由施加重放算法而启动的，但是收费不必与该算法的施加同时进行。该记帐信息表明用户已经存储了一个加密广播节目。该记帐信息是稍后由服务提供者经过电话链路存取的，并且被用于经过一个普通的的付帐处理对于用户收帐。其它付帐机理同样是有可能的。例如，在一个智能卡中可以从一个预先存储的信用和扣除贷款。而且，可能根据存储要求的类型改变付帐量，例如针对存储的一个费用可以只允许存储节目该单一复制或重放，而针对存储的另一费用允许该节目的无限制的复制或重放．要求的存储类型被编码在CPSI数据流本身中的指定的复制保护数据中，或在该CPSI数据流外部的数据包数据中的指定的复制保护数据中．由控制器115使用的用于产生适合于存储在介质105上的节目数据流(CPSI数据流)以及用于针对用户的存储计帐的在图2-3的处理在步骤258结束。

在步骤237中，如果控制器115确定在MPEG兼容的分组标题的适应场中没有广播加密码被传输，则控制器115执行步骤240 － 245．这些步骤对称于步骤249 － 258，除了由于没有广播加密码存在于输入到mux110的数据流表示该节目将要被存储之外，没有必要插入空数据．否则，控制器115执行步骤240，以便经过储存接口95产生用于存储的CPSI

数据流，并且执行步骤244，以相似于结合步骤249和254描述的方式对于进行存储的用户收帐。图2-3的处理的分支在步骤245结束。但是应该注意，在步骤240和249中的CPSI数据流可能被另外提供到其它应用，例如经过接口70的显示或通信而不是经过接口95的存储。

来自mux 110的CPSI由接口95缓冲以便减小数据中的缝隙和比特率的变化。该产生的缓冲数据由存储装置90处理，以便适合于在介质105上的存储。通过经由I/O端口100而使用一个标准化 CEBus控制协议（例如家庭自动化标准(CEBus)， EIA/IS - 60 ，1989年12月），控制器115启动和控制存储装置90 (图 1)的操作。存储装置90是一个线性存储介质DVHS™类型装置而介质105是一个线性顺序访问类型介质，例如录相带。使用已知误差编码技术，例如信道编码、交织和Reed-Solomon编码，存储装置90编码来自接口95的缓冲数据流，以便产生适合于存储的一个编码数据流。单元90在磁带介质105上储存该包括CPSI的产生的编码数据流。

虽然以图1的示范实施例描述在一个线性存储介质上存储数据的一个DVHS™装置，但是存储单元90可以是任何类型的存储器。例如，单元90可以是一个固态的或非线性的装置，用于把数据存储在RAM中或在一个非线性的介质上。非线性介质是一个适应非顺序访问的介质，例如一个视盘介质，包括 CDROM或 DVD。如果单元90和介质105是非线性的或固态类型的存储器系统，则单元90把 CPSI数据从该CPSI数据流分开，并且把该CPSI数据储存在该介质的一个指定目录部分中。这就有利地避免CPSI的重复存储并且减小需要存储器的容量。另外，单元90可能储存如此形成的CPSI数据流并且输入到单元90，包括一个或更多的CPSI数据的重复。

而且，图1的系统25可以包括多个存储/检索路径，支持包括线性、非线性的以及固态类型的各种类型的多个存储装置的操作。在图1中示出单一的存储/检索路径包括单元47、90、95、105和110。通过复制这些单元以便产生并行存储器函数，系统25被迅速地扩展到包括多个存储路径。如先前描述，随着以遥控装置125进行的屏幕上的菜单选择，存储路径和目标为一个特定存储装置的节目由经过接口120输入控制器115的用户产生数据(SP, SM)选择。

使用图4的处理，图1的系统25从重放模式中的存储装置90和介质

105恢复节目。恢复的数据流由系统25处理并且提供到应用装置75、80、和85用于显示或输出。另外，节目数据流可以被存储在其它并行存储装置上(为了简化制图在图1中没示出)。

在图4的步骤505中，在该起始步骤500之后，用户产生的数据(SR、SM)被输入到系统25的控制器115(图1)标识出将要被恢复的节目以及将要从其恢复节目的存储装置(SM)。随着遥控装置125的屏幕菜单选择，用户选择数据经接口120输入到控制器115。为了示范目的假定该用户选择将要从存储装置90(图1)恢复的节目。

在步骤510中，使用如先前讨论的标准化CEBus控制协议，控制器115用经过I/O端口100的命令由装置90从介质105开始恢复选定的节目数据流。装置90解码从介质105恢复的误差编码数据，以便恢复最初提供到装置90用于存储的相应数据。装置 90可以是一个DVHS™线性存储单元或其它存储单元，例如固态RAM或非线性的DVD或 CDROM类型的装置。在步骤510中 ，由装置90到接口95 ，该恢复的解码数据流被传送。经过该标准CEBus，数据传送被控制并且由控制器115同步。接口95缓存从单元90接收的数据，以便调整在数据信息包之间的时间间隔，以便提供一个 MPEG兼容的并且满足MPEG比特率约束的一个缓冲的数据输出。

在步骤515中，使用路径选择信号C，控制器115经过mux37把来自接口95的缓冲输出引导到PID选择单元45和47。在步骤515中，控制器115确定在步骤244和254(图3)编码在指定的复制保护数据中的复制限制是否正被恢复程序操作。根据恢复被允许，控制器115在步骤515中(图4)恢复该重放加密码，即在步骤227(图2)中从用于该选定的节目(SR)的CAT产生的加密码，并且按照先前结合步骤215(图2)描述的方式提供该码到智能卡单元130。在控制器115的控制之下，智能卡130在步骤515中(图4)应用该重放算法以便从重放加密码产生该源广播密钥。在步骤515中，控制器115把该广播密钥提供到在单元45和47中的PID、目标和密钥查询表。

在步骤520中，单元45和 47以及系统25的其余单元处理该重放数据流，或者经过mux110用于存储或经过接口70用于操作使用。随着经由mux 37的选择，来自单元95的重放数据流和来自选择器35的发送数据流都以相似的方式由系统25处理。除密钥产生步骤和CPSI的处理步

骤外，这些数据流都以先前描述的用于发送数据流的方式处理。在重放模式中，智能卡130采用一个重放密钥产生算法而不是广播密钥产生算法。智能卡单元130采用该重放算法函数以便在图2的步骤227中以重放编码算法解密以前编码的该加密码。因此，单元130得出用于该选定的用于重放(SR)节目的源广播密钥。该广播密钥由DES解密单元50使用，以便按照以前描述的用于该发送数据流的方式，在随后步骤520(图4)中解密该加密节目内容的数据包。但是，经 mux 37选定的重放数据流已经包括该CPSI。因此在该重放模式中，控制器115在步骤520中不执行涉及到结合图2-3描述的CPSI的形成。

在图4中示出的示范重放模式中，系统25在步骤520中传输解码该重放的数据流以便提供解码数据到操作解码器80和85用于显示。在这种模式中，系统25根据 MPEG 标准应用包含在该重放数据流中的最新完整的CPSI数据，以便提供一个表示选定节目的SR的传输解码数据流。

利用PID滤波器45和47、解密器50、解码器55、缓存器60和控制单元65，以类似于先前结合图1描述的方式，把该CPSI应用在对于重放数据流进行的传输解码中。除去该CPSI以外，传输解码数据流经由接口70被提供到操作解码器80和85用于MPEG解码和图像重现。在其它模式中，系统25把包括该CPSI的重放数据流提供到其它操作装置，例如提供到高速数据端口75。通过这些操作装置或随后的装置，该CPSI随后被可根据需要用于该重放数据流的传输解码中。如果该重放数据流是将要被存储到一个第二存储装置而不是装置90，则该mux 110将把包括CPSI的数据流经由一个第二存储接口提供到该第二存储装置。而且，该第二存储装置和接口(在图1中都没示出)分别模仿单元90和95的操作及功能。来自接口70、通过应用解码器80和85MPEG解码的数据分别由在单元80和85中的音频和图象重现装置给出。

在步骤527中(图4)，在系统25中的条件接通系统对于该节目重放收帐该用户。通过在该重放算法的操作之时就存储记帐信息，用户在该可插入的智能卡本身之内被收帐。记帐信息表明该用户已经恢复一个加密广播节目。这种记帐信息稍后由服务提供者通过电话链路存取并经过一个普通的付帐处理用于收帐这个用户。如先前描述，其它付帐机理可以同样地被使用。图4的重放处理在步骤530结束。

图1的结构不是唯一的。可以根据本发明的原则得出其它结构以便完成同一个目的。而且,图1结构的单元的功能和图2-4的处理步骤在微处理器的编程指令之内可以整体或部分地实现。此外,本发明的原则适用于系统使用MPEG或非MPEG兼容的电子节目导引，用于传送任何信息，在此处是在MPEG PSI表中传输的信息。本发明原则不被限制为在MPEG兼容的PSI表中的节目指南或PSI。

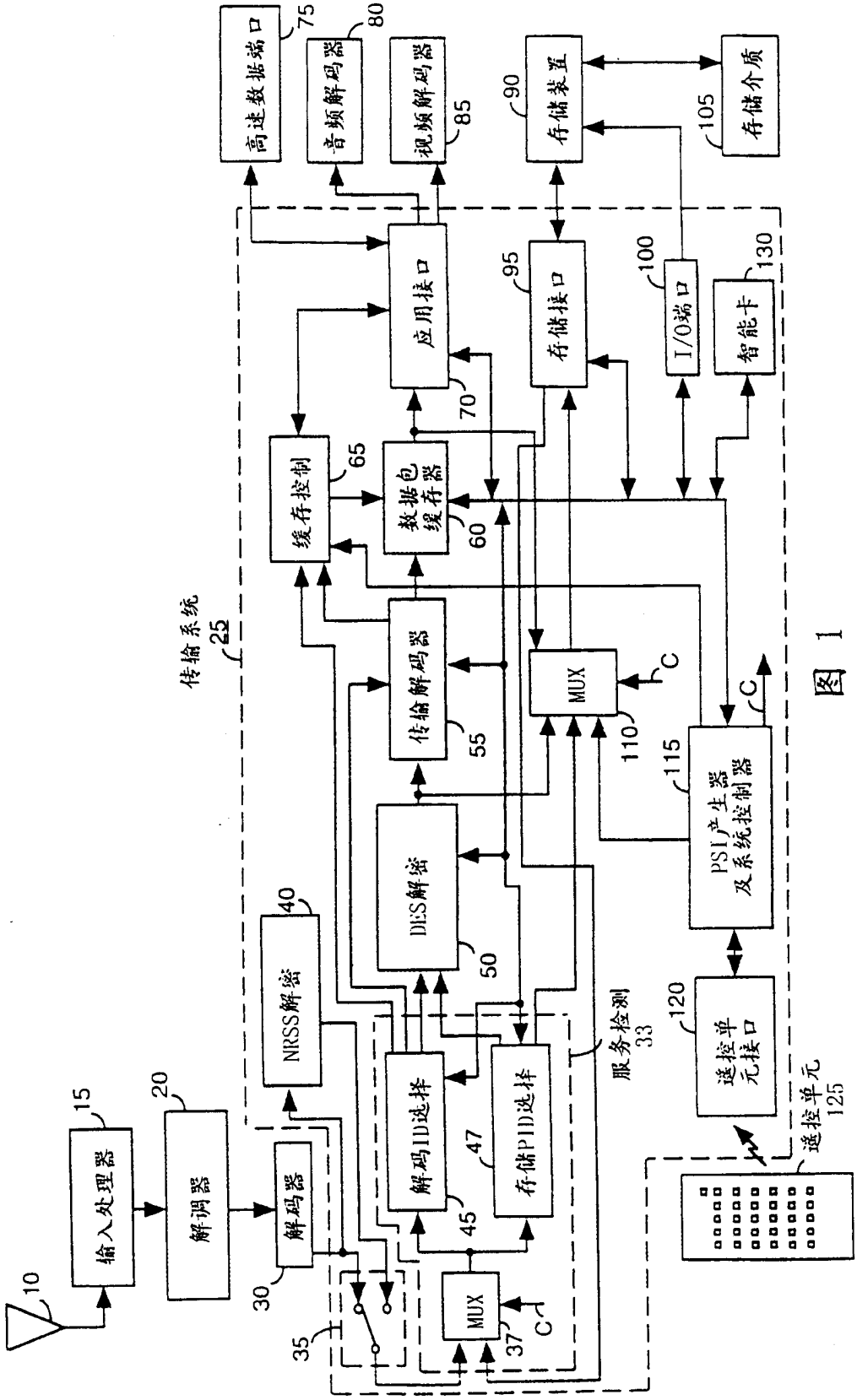

高速数据端口
75
音频解码器
80
视频解码器
85
存储装置
90
存储介质
105
应用接口
70
存储接口
95
I/O端口
100
智能卡
130
缓存控制
65
数据包缓存器
60
传输系统
25
传输解码器
55
MUX
110
C
C
PSI产生器及系统控制器
115
DES解密
50
NRSS解密
40
解码PID选择
47
存储PID选择
45
服务检测
33
遥控单元接口
120
遥控单元
125
输入处理器
15
解调器
20
解码器
30
MUX
37
C
35
10

图 1

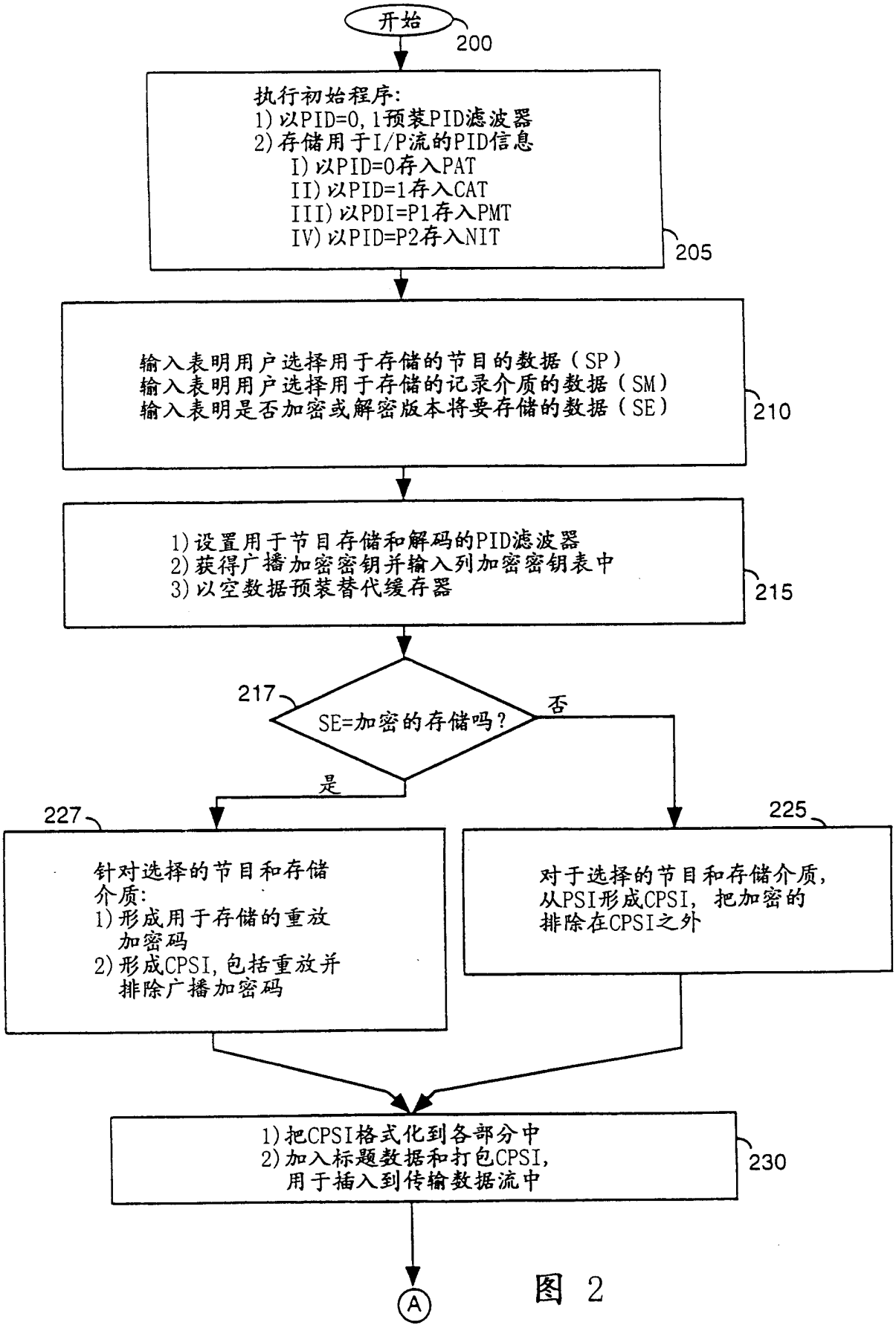

开始
200
执行初始程序:
1)以PID=0,1预装PID滤波器
2)存储用于I/P流的PID信息
I)以PID=0存入PAT
II)以PID=1存入CAT
III)以PDI=P1存入PMT
IV)以PID=P2存入NIT
205
输入表明用户选择用于存储的节目的数据(SP)
输入表明用户选择用于存储的记录介质的数据(SM)
输入表明是否加密或解密版本将要存储的数据(SE)
210
1)设置用于节目存储和解码的PID滤波器
2)获得广播加密密钥并输入列加密密钥表中
3)以空数据预装替代缓存器
215
217
SE=加密的存储吗?
否
是
227
针对选择的节目和存储介质:
1)形成用于存储的重放加密码
2)形成CPSI,包括重放并排除广播加密码
225
对于选择的节目和存储介质,从PSI形成CPSI,把加密的排除在CPSI之外
1)把CPSI格式化到各部分中
2)加入标题数据和打包CPSI,用于插入到传输数据流中
230
A

图 2

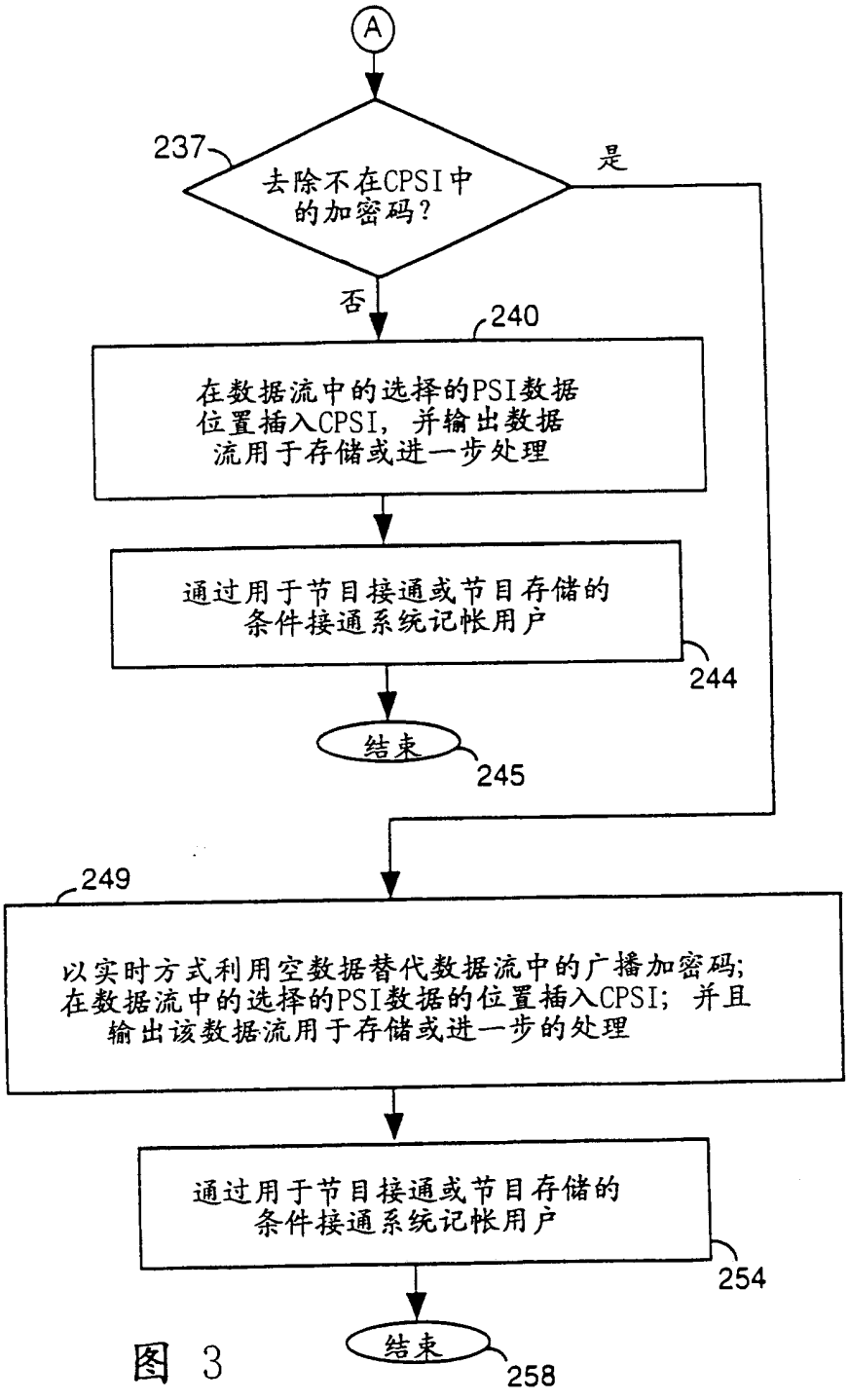

A
237
去除不在CPSI中的加密码?
是
否
240
在数据流中的选择的PSI数据位置插入CPSI，并输出数据流用于存储或进一步处理
通过用于节目接通或节目存储的条件接通系统记帐用户
244
结束
245
249
以实时方式利用空数据替代数据流中的广播加密码;在数据流中的选择的PSI数据的位置插入CPSI；并且输出该数据流用于存储或进一步的处理
通过用于节目接通或节目存储的条件接通系统记帐用户
254
结束
258

图 3

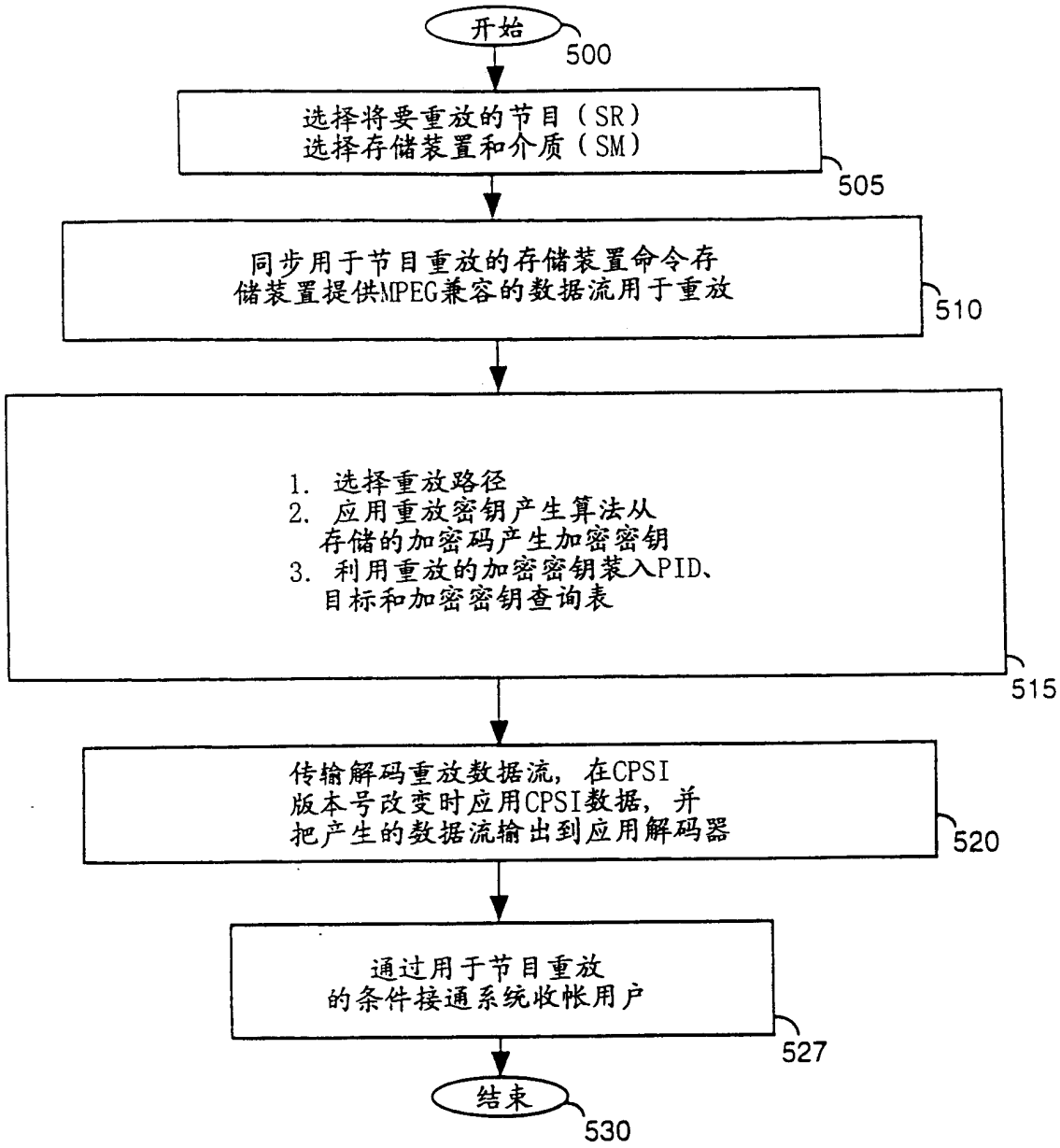

开始
500
选择将要重放的节目（SR）
选择存储装置和介质（SM）
505
同步用于节目重放的存储装置命令存
储装置提供MPEG兼容的数据流用于重放
510
1. 选择重放路径
2. 应用重放密钥产生算法从
存储的加密码产生加密密钥
3. 利用重放的加密密钥装入PID、
目标和加密密钥查询表
515
传输解码重放数据流，在CPSI
版本号改变时应用CPSI数据，并
把产生的数据流输出到应用解码器
520
通过用于节目重放
的条件接通系统收帐用户
527
结束
530

图 4