



[12] 发明专利申请公开说明书

[21] 申请号 97190486.3

[43]公开日 1998年8月12日

[11] 公开号 CN 1190516A

[22]申请日 97.4.30

[30]优先权

[32]96.5.6 [33]EP[31]96201239.9

[86]国际申请 PCT/IB97/00459 97.4.30

[87]国际公布 WO97/42762 英 97.11.13

[85]进入国家阶段日期 98.1.5

[71]申请人 飞利浦电子有限公司

地址 荷兰艾恩德霍芬

[72]发明人 F·L·A·J·肯珀曼

F·博斯韦尔德

[74]专利代理机构 中国专利代理(香港)有限公司

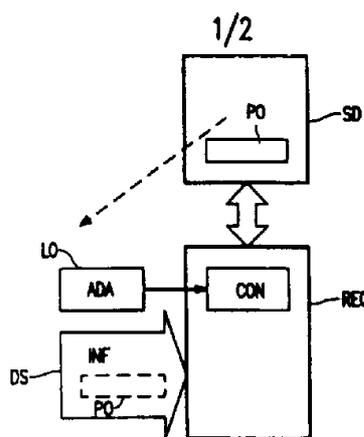
代理人 邹光新 王岳

权利要求书 1 页 说明书 6 页 附图页数 2 页

[54]发明名称 管理信息访问的保密装置

[57]摘要

在一个信息传输的系统中，保密装置（SD）管理一个信息的访问。这个保密装置（SD）提供一个用来指示可以从中取得附加数据（ADA）的一个存储单元（LO）的一个指针（PO），此附加数据（ADA）可以是对要求的信息的一个说明。例如，在一个收费电视系统中，它可以是一个特殊电影的信息，附加数据是这样对它描述的：“4月19日20点30分播出适合12岁以上年龄观看的由詹姆斯邦德导演的动作片。”在这种情况下，可以使用指针（PO）来通知用户，即他的保密装置（SD）允许他收看这个特殊的电影。不过，为了满足各种需要，包含在由指针（PO）指示的存储器（LO）中的附加数据（ADA）可以是软件，例如，游戏或者配置一个与保密装置协同操作的接收器（REC）。



权 利 要 求 书

1.一种保密装置 SD 用来管理一个信息 (INF) 的访问, 其特征在于: 该保密装置 (SD) 提供一个指针 PO 用于指示出可以得到的附加信息 (ADA) 的一个存贮单元 (LO)。

5 2.如权利要求 1 所述的保密装置 SD, 其特征在于: 该指针 (PO) 包括至少一个部分 LB 用于识别由附加数据 (ADA) 构成其一一部分的数据流 (DS1)。

3.如权利要求 1 所述的保密装置 SD, 其特征在于: 该指针 (PO) 包括下面数据部分:

10 一个标记 (LB1) 用来识别一个信息传输系统式网络 (NW);

 一个标记 (LB2) 用来识别一个原始信息传输系统式原始网络 (ONW);

 一个标记 (LB3) 用来在由信息传输系统提供的任何其它数据流 (DS2) 中识别一个数据流 (DS1);

15 一个标记 (LB4) 用来从在该数据流中的任何其它服务 (SV2) 中识别一个服务 (SV1)。

4.如权利要求 1 所述的保密装置 (SD), 其特征在于: 所述指针 (PO) 构成一个用来管理一个访问信息的数据体 (DO) 的一部分。

20 5.与权利要求 1 所述的保密装置 SD 结合使用的一个接收机 (REC), 其特征在于, 该接收机 (REC) 包括一个电路 (CON) 用来检索由指针指示出的附加信息 (ADA)。

25 6.一种包含对其访问可由一个保密装置 (SD) 管理的信息 (INF) 的一个数据流 (DS), 其特征在于: 该数据流 (DS) 包括用来在所述保密装置 (SD) 中进行存贮的一个指针 (PO), 该指针指示存有可获得附加数据 (ADA) 的一个存贮单元 (LO)。

7.一种控制一个信息传输系统的方法, 该传输系统包含至少一个管理一个信息 (INF) 的访问的保密装置 (SD), 其特征在于: 所述访问包括以下步骤: 提供给该保密装置 (SD) 一个指针 (PO), 该指针指示出从其中可以得到附加数据 (ADA) 的一个存储单元。

说明书

管理信息访问的保密装置

5 本发明涉及一种利用保密装置对信息的访问进行管理的装置。此信息可以提供为加密的形式。在这种情况下，所述保密装置根据该信息是否具有代表一种访问信息资格的数据体来决定是否允许对该信息进行解密。

10 美国专利 USA 5,235,415 描述了一个用于允许付费电视用户访问电视节目/或广播节目的方案。在用户手中持有的保密装置例如一个智能卡中存有描述所述节目的费用的数据和帐目状态。该装置包括一个键盘，用于对所涉及节目发请求信息。作为该请求内容的一个功能一个模块使用代码转换表将包含在保密处理器中的数据转换成易懂的信息，该代码转换表有规律地在电视或广播信号中传输。

15 本发明的目的是，利用一个比现有技术适应性更高的保密装置来对信息访问进行管理。权利要求 1，5，6，7 分别定义了一个本发明的保密装置，一个接收装置，一个数据流和对一个信息传递存取系流进行控制的方法。从属权利要求定义了为更好地实现本发明而可以选择使用的附加技术特征。

20 下述方面是本发明所要考虑的。一个信息供应商可能想及时地在一个确定位置提供给他的用户一个新型号的保密装置，事实上，在几乎同一时间里更新所有用户的旧的保密装置，这是几乎不可能的。这样，会存在新和旧的保密装置同时使用的一个过渡期。

25 在现有技术中，如果在新的保密装置中使用新的码和/或格式用于其内包含的数据，就会出现某些实际问题。例如，一个信息供应商将不得不传输两种不同类型的代码转换表，即一个代码转换表将旧代码形式的数据转换成可理解的信息，另一个代码转换表转换新的代码形式的数据。需要提高传输能力才能传输两种不同类型的代码转换表，但这可能是很难实现的，或者是根本不可能的。

30 依照本发明，在一个保密装置中提供一个指针，用来指示从其中可获得附加数据的一个存储位置，该附加数据可以是对要求的信息的一个说明。例如，在一个收费电视系统中，可以是一个关于一个特殊电影信

息的说明“4月19日20点30分，播出适合12岁以上观众收看的，电詹姆斯邦德导演的动作片”。因为信息供应商希望公众了解他们何是提供节目，从而鼓励购买，因此这样的说明将是易懂的形式通知公众的。可以使用指针来通知一个用户，即他的保密装置允许他收看这个特殊电影。那样就不需要代码转换表。因此，本发明具有比现有技术更高的适应性。

下面是本发明的其它优势。与现有技术截然不同，本发明不需要按照代码转换表使用一个专用的模块来转换存于保密装置中的数据。在大多数情况下，本发明任何用来获得附加信息的硬件和/或软件是相当简单的，该附加信息存于由指针指示的存储单元中。再者，这些硬件和/或软件可以全部或者大部分地用于包括数据检索和/或数据恢复等其它功能，例如，一个电子节目指南的功能。因而，本发明可实现相等的成本效益。

从由指针指示的存储单元中的获得的附加数据，可以是任何类型的数据。例如，该附加信息可以是软件，它可与其访问由保密装置控制的信息有某种关系也可以没有。该附加信息也可以是软件，软件提供保密装置与一个与它连接的装置间的接口。这样，本发明在能够提高由该保密装置构成的一个装置的功能的同时，还提供保密装置本身的一种功能。

下面结合附图来表示本发明和附加技术特征，此附加技术特征可以有选择地使用来更好地实现本发明。

附图：

图1表示本发明的基本特征的框图。

图2-4是表明可以选择地使用来更好地完成本发明的附加技术特征的框图。

图5是表示按照本发明的关于付费电视系统的一个实施例的框图。

首先，对使用的参考符号做一些说明，各图中用一种相同的识别代码来表示相似的实体。在单个图中可以显示各种相近实体。这种，为了区分相近实体就需在识别代码上加个数字。如果相似的实体的个数是个游动系数，则这个添加的数字要放在括号中。在说明书和权利要求书中，如果可以很明显地表示，则可以省略掉参考符号的任何添加数字。

图1从各个方面示出本发明的基本特征，即关于一个保密装置SD，

一个接收装置 REC 和一个数据流 DS。该保密装置 SD 管理一个信息 INF 的访问，它能提供一个指针 PO 用来指示从其中可以获得附加数据 ADA 的一个存储单元 LO。接收装置 RFC 与保密装置 SD 协同操作。它包括一个电路 CON 用来检索附加数据 ADA，该 ADA 存于由指针 PO 指示的存储单元 LO 中，该存储单元 LO 最好放在保密装置 SD 之外。该信息 INF 可以以一种数据流 DS 的形式提供给该接收装置 RFC。这样，就可能已经通过数据流 DS 将该指针 PO 传输给保密装置 DS 而在其中存储起来。

原则上，该附加数据 ADA 可以是任何类型的数据，我们将列举三种类型的 ADA 为例子做说明。

首先，该附加数据 ADA 可以是对提供的信息的一个说明。例如，在一个付费电视系统中，可以包括关于一个特殊电影的信息的一个说明：“4月19日20时30分，播出适合12岁以年龄的观众收看的，由詹姆斯邦德导演的动作片。”可以用指针 PO 来通知用户，即那个用户的保密装置 SD 包含一个允许他收看该电影的一个数据体。之后，该指针 PO 可以和这个数据体联合起来，或者甚至形成它的一部分，我们将在下述讨论这些更详细的细节。

第二，该附加数据 ADA 可以是用于在保密装置 SD 与一个需要和它协作的一接收装置 REC 间提供一个接口的软件。例如，该接收装置 REC 可以是一个通用的基顶盒 (settop)，它可以与属于例如不同付费电视系统操作装置的不同类型的保密装置协作。之后，可以提供给该基顶盒一个通用接口，这个通用接口需设置提供该通用基顶盒与一个特殊保密装置间的一个通讯链路。这样，指针 PO 可以指示一个存储单元，该单元用于设置通用接口的软件，因而，该保密装置和该基顶盒可以一个希望的方式协同操作。

第三，附加数据 ADA 可以是位于用户端的用于增强功能的软件。该软件与其访问受控于所述保密装置 SD 的一个信息 INF 有某种关系。例如，该附加数据可以是用来玩游戏的软件，它可以涉及付费电视系统中的某个节目或事件。

图 2 示出下述附加特征。指针 PO 至少包括一个 LB 部分，它用来识别由附加数据 ADA 构成它的一个部分的一个数据流 DSI。图 2 的特征考虑到下述方面。在某时刻，一个用户可能想获得他的探密装置 SD

中有关某种数据体的附加数据 ADA，而此时，他的接收装置 REC 可能调谐到一个数据流 DS2，该数据流不是由他所希望的附加数据 ADA 构成一部分的那一个。图 2 示出的特征允许该接收装置 REC 自动地调谐到包含他所希望的附加数据 ADA 的数据流 DS1 上，然后可以从该数据流 DS1 中检索出他所需要的附加数据 ADA。由此，图 2 的特征给用户提供了方便。

图 3 示出下述附加特征。指针 PO 由下面各部分组成。

一个标记 LB1 用来识别一个信息传输系统或者网络 NO；

10 一个标记 LB2 用来识别一个原始信息传输系统或者始终网络 ONW；

一个标记 LB3 用来从由信息传输系统中提供的任何其它的数据流 DS2 中识别出数据流 DS1；

一个标记 LB4 用来从在该数据流中的任何其它服务 SV2 中识别一个服务 SV1，一个服务是由信息供应商提供的不同片段的信息的集合。

15 例如，在付费电视系统中，体育节目的一个集合可以构成一个服务。

图 3 的特征允许从在该保密装置中有关一种资格的一个数据体到在一个 MPEG 型数据流中（MPEG 为运动图象专家组的缩写）的服务信息产生反向链路。

图 4 示出上下述附加特征。指针 PO 构成该保密装置 SD 的一个数据体 DO 部分。这样就可以有效地利用保密装置里的有用数据存贮功能并容易地访问指针 PO。不过，图 4 的特征看起来似乎很特征。一方面，指针 PO 是未编码而公开的，另一方面，访问管理的不能受到干扰的特征又必须对数据体加密。不过，我们考虑到不全部地对数据体进行编码，并不影响对信息访问进行管理。因为除了有关的信息商以外没有人能够在保密装置中存贮这些数据体。之后，可以在该指针 PO 上叠加一个保密检验码来构成数据体。可以根据该指针 PO 本身与一个属于服务提供商的并存贮在该保密装置里的合成密钥来生成该检验码，如果要给该保密装置 SD 一个数据体，如果它检验到加在该指针上的密码是正确的，则它就存贮所述数据体，反之则拒绝。

30 图 5 示出依照本发明的一个付费电视系统的例子。它由下述主要部分构成：一个操作服务中心 OSC，和在一个用户端的，一个基顶盒 STB，一个用户接口 UIF，和一个以一种智能卡 SC 形式的保密装置。该基顶

盒 STB 包括一个高频端 FRE, 一个数字滤波器 FIL, 一个解密器 DES, 一个控制器 CON 和一个包含 EPG 软件的存储器 MEM。该顶端设置盒 STB 可以耦合到图 5 未标出的一个图象显示器上。

图 5 所示系统是这样操作的, 该操作服务中心 OSC 以加密的形式
5 利用一个 MPEG 型数据流 DS 传输电视节目给基顶盒 STB, 该 MPEG 型数据流 DS 包括资格信息 EMM, 此资格信息是关于有资格收看某种节目的一个用户或一组用户的信息, 该 MPEG 数据流 DS 还包括服务信息数据 SID, 例如, 在欧洲专利的通讯标准 300468。该服务信息数据 SID 包括下列描述的部分。节目提供商, 节目, 这些节目的编制目录定
10 时。用独特的标识符 1D(1)… 1D(N)来区分不同的节目的说明。另外, 该服务信息数据 SID 也包含标识符 IDS 来专门识别该 MPEG 数据流 DS 和它的原形。

在用户端, 该高频端 FRE 调谐到 MPEG 数据流 DS。滤波器 FIL 从该 MPEG 数据流 DS 中提取服务信息数据 SID 和资格信息 EMM。控
15 制装置 CON 可以用 EPG 软件来处理该服务信息数据, 从而以可视的方式通知该用户当前和将来的节目。该控制装置 CON 也可以把该资格信息 EMM 传输给智能卡 SC。在该智能卡 SC 中处理该资格信息 EMM 来得到资格数据体 EDO(1)… EDO(N), 然后这些数据体就存在该智能卡 SC 中。为提供某个节目时, 一个资格数据体 EDO 可以用于控制一个来
20 自允许解密 DES 的开关。于是, 根据包含在智能卡 SC 中资格数据体 EDO 来访问节目。为了知道用户他是否有资格收看一个特殊节目, 该资格数据体 EDO(1)… EDO(N)还包含指针 PO(1)… PO(N)。这些指针可能已经通过例如资格信息 EMM 传输了。

用户可以用以下方式对所有他有资格看的节目进行浏览, 他可以通过
25 用户接口 UIF 来安排这样一个浏览。作为响应, 控制器 CON 通过读存在智能卡 SC 里的所有指针 PO (1) … PO (N) 来对 SC 进行检测。然后, 该控制器 CON 根据专门识别数据流的标识符 IDS 检查该高频端 FRE 是否调谐到所希望的 MPEG 数据流 DS。如果高频端 FRE 没有调谐到该 MPEG 数据流, 该控制器 CON 能依照指针 PO (1) … PO
30 (N) 调谐高频端 FRE, 该指针包括用来指示所希望的 MPEG 数据流 DS 的一个数据部分。一旦, 正确地调谐好高频端 FRE, 该控制器 CON 将利用包含在其中的标识符 ID (1) … ID (N) 将指针 PO (1) …

PO (N) 与服务信息数据 SID 联接起来。相应地，它将读那些关于节目的服务信息数据 SID 的部分，这些节目是该用户有资格收看的。利用 EPG 软件来将该服务信息数据 SID 中的有关部分转换成可视信息，这样，用户便可实现他已预定的浏览。

5 上述的附图和说明，仅仅显示出本发明的有限的部分。显然，还有许多可选择的方案属于从属权利要求。因而，下面将做结论性论述。

在各种部件中都有许多种实际的功能扩展和功能元件的扩展。因此，这些附图仅仅用图表的方式表示并且分别仅用本发明的一个实施例的框图来表示。例如，参照图 1，保密装置 SD 就可以构成接收机 REC 的一个整体部分。

10

使用保密装置 SD 可以访问任何类型的信息 INF。例如，该信息可以是音乐或是软件。它还可以是个混合信息，例如，由视像，音乐和软件合成的信息。

15

可使用任何方式让用户得到信息 INF 和附加数据 ADA。例如，该信息可以存在数据库中，该数据库可通过 internet 网或其它方法进行访问。它也可以存储于一个载体上，例如在用户可购买或免费得到的 CD - ROM 上。当然，额外数据 ADA 也可通过上述方法获得。

20

任何类型的接收机 REC 都可以与保密装置 SD 协作。例如，该接收机 REC 可以是与能传递数据的一个网络相接的一个计算机终端，例如，该网络是电话网。

指针 PO 可以由任何数量的单元构成。例如，以图 3 为参照，该指针 PO 可额外包括一个更多的标记 LB5，它用来识别服务 SV1 中的任何其它节目。

括号内的任何参考标记不应用来限制涉及的权利要求。

25

说明书附图

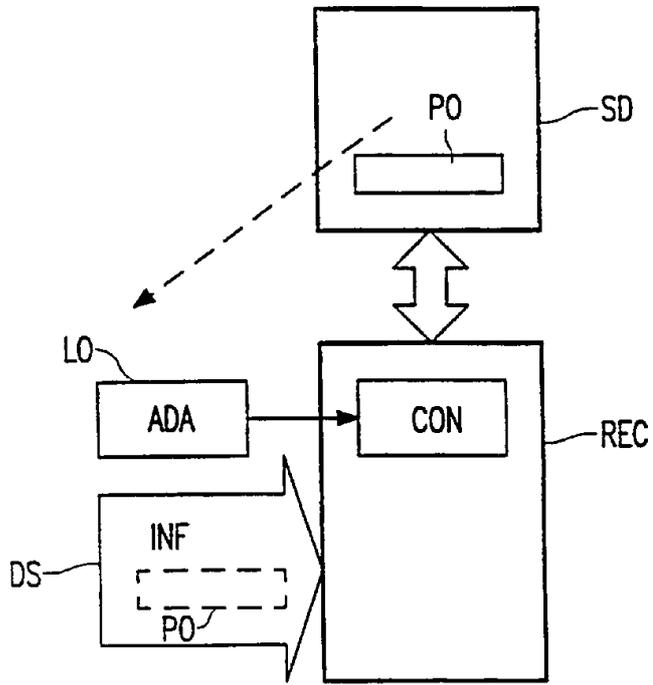


图 1

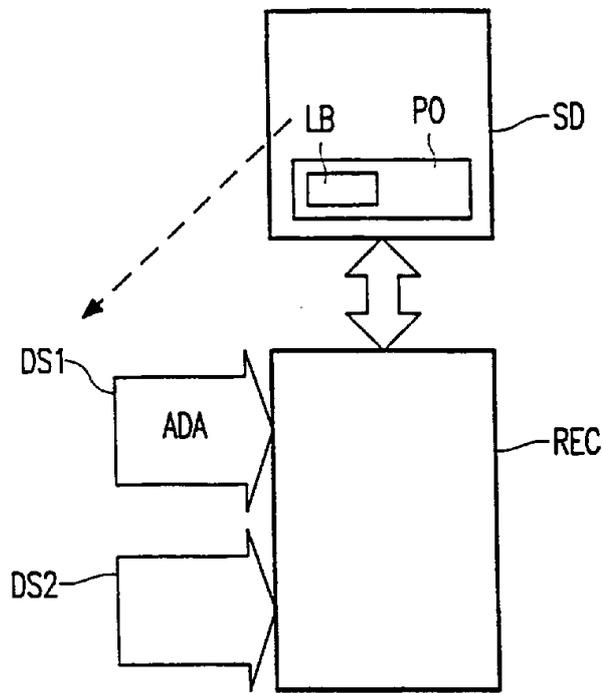


图 2

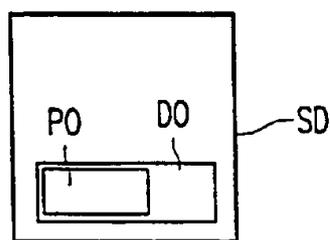


图 4

