(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1628447 B
(45)授权公告日 2010.04.28

(21)申请号 02828988.9

(22)申请日 2002.11.08

(30)优先权数据
PCT/EP02/05610 2002.05.22 EP

(85)PCT申请进入国家阶段日
2004.11.19

(86)PCT申请的申请数据
PCT/EP2002/014897 2002.11.08

(87)PCT申请的公布数据
WO2003/098895 EN 2003.11.27

(73)专利权人 汤姆森许可贸易公司
地址 法国布洛里

(72)发明人 拉尔夫·舍费尔 阿兰·杜兰德
劳伦特·勒塞纳
弗雷德里克·帕斯奎尔

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 戎志敏

(51)Int.Cl.
H04L 29/06(2006.01)
H04N 7/24(2006.01)
H04N 7/167(2006.01)

(56)对比文件
WO 99/62248 A1,1999.12.02, 全文.
CN 1301442 A,2001.06.27, 全文.
WO 98/43431 A1,1998.10.01, 全文.

审查员 曲桂芳

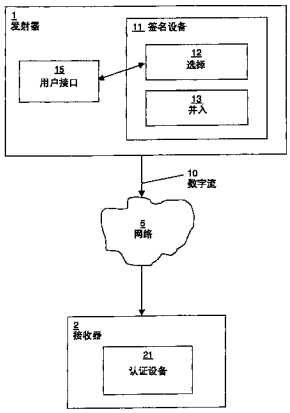
权利要求书 3 页 说明书 13 页 附图 3 页

(54)发明名称

签名和认证设备及方法和相应的产品

(57)摘要

本发明涉及一种设备和一种方法，用于对数字流(10)进行签名，每个数字流(10)包括与视听信息有关的内容和信令。所述设备将加密应用于信令的有选择地确定的描述符，称为认证描述符，以获得签名。本发明还涉及对应的认证设备和方法。应用于对DVB/MPEG数字流、尤其是针对MHP的认证。



CN 1628447 B

1. 一种签名设备 (11)，通过产生通过应用于数字流 (10) 的加密而获得的、要并入所述数字流 (10) 中的至少一个签名，对要通过通信网络 (5) 传输的数字流进行签名，这些数字流 (10) 中的每一个均包括几个信息实体，所述实体包括 ：

- 内容，至少与视听信息相关 ；

- 以及至少一个信令，由与所述内容的源、宿和结构相关的信息集合构成，由于网络要求，所述信令能够可靠地在网络中进行修改，包含被称为描述符的必要数据结构，并主要通过被称为表格的已排列编组构建，

其特征在于所述签名设备 (11) 包括用于在所述信令的描述符中有选择地确定描述符的装置以及用于将所述加密应用于所确定的描述符的装置，所确定的描述符被称为认证描述符，其保持不被网络头端中的重新复用步骤所触及。

2. 根据权利要求 1 所述的签名设备，其特征在于根据 DVB 和 MPEG 标准，构建所述数字流 (10)。

3. 根据权利要求 2 所述的签名设备，其特征在于根据 MHP 标准，构建所述数字流 (10)。

4. 根据权利要求 1 所述的签名设备，其特征在于其设置用于将所述加密应用于任意信令 MPEG/DVB 表格的认证。

5. 根据权利要求 4 所述的签名设备，其特征在于所述设备设置用于将所述加密应用于以下表格中的至少一个的认证 ：节目映射表 PMT、节目访问表 PAT、条件访问表 CAT、网络信息表 NIT、服务描述表 SDT、事件信息表 EIT、时间偏移量表 TOT、应用程序信息表 AIT 和束关联表 BAT。

6. 根据权利要求 5 所述的签名设备，其特征在于所述设备设置用于将所述加密应用于至少一个 AIT 表格的认证。

7. 根据权利要求 1 所述的签名设备，其特征在于其包括使用户能够选择所述认证描述符的装置 (12)。

8. 根据权利要求 1 所述的签名设备，其特征在于其包括用于将所述认证描述符的地址并入所述数字流 (10) 的装置 (13)。

9. 根据权利要求 8 所述的签名设备，其特征在于所述并入装置 (13) 用于将至少一个散列描述符引入每个所述数字流 (10) 中，所述散列描述符包括至少一个摘要值，还包括用于计算所述摘要值的所述认证描述符的地址，所述至少一个摘要值是通过将散列算法应用于至少一个所述认证描述符而得到的，并被用于计算所述签名。

10. 根据权利要求 9 所述的签名设备，其特征在于所述并入装置 (13) 用于根据树结构，将所述散列描述符排列在所述数字流 (10) 中，通过具有较低等级的至少一个其他所述散列描述符来计算至少一个所述散列描述符。

11. 根据权利要求 8 所述的签名设备，其特征在于每个表格包括具有有限大小并分配有号码的至少一个部分，并且每个部分包括将描述符连续引入该部分的至少一个环，所述并入装置 (13) 用于通过至少提及所述部分号码以及出现次数而规定每个所述认证描述符的地址，每个所述认证描述符属于给定部分的至少一个给定环、并具有分别针对这些环中的每一个的至少一个出现次数。

12. 一种签名方法，通过产生通过应用于数字流 (10) 的加密而获得的、要并入所述数字流 (10) 中的至少一个签名，对要通过通信网络 (5) 传输的数字流进行签名，这些数字流

(10) 中的每一个均包括几个信息实体，所述实体包括：

- 内容，至少与视听信息相关；

- 以及至少一个信令，由与所述内容的源、宿和结构相关的信息集合构成，由于网络要求，所述信令能够可靠地在网络中进行修改，包含被称为描述符的必要数据结构，并主要通过被称为表格的已排列编组构建，

其特征在于所述方法包括在所述信令的描述符中有选择确定描述符的步骤以及将所述加密应用于所确定的描述符的步骤，所确定的描述符被称为认证描述符，其保持不被网络头端中的重新复用步骤所触及。

13. 根据权利要求 12 所述的签名方法，其特征在于根据 DVB 和 MPEG 标准，构建所述数字流 (10)。

14. 根据权利要求 13 所述的签名方法，其特征在于根据 MHP 标准，构建所述数字流 (10)。

15. 根据权利要求 12 所述的签名方法，其特征在于其设置用于将所述加密应用于任意信令 MPEG/DVB 表格的认证。

16. 根据权利要求 15 所述的签名方法，其特征在于所述方法设置用于将所述加密应用于以下表格中的至少一个的认证：节目映射表 PMT、节目访问表 PAT、条件访问表 CAT、网络信息表 NIT、服务描述表 SDT、事件信息表 EIT、时间偏移量表 TOT、应用程序信息表 AIT 和束关联表 BAT。

17. 根据权利要求 16 所述的签名方法，其特征在于所述方法设置用于将所述加密应用于至少一个 AIT 表格的认证。

18. 根据权利要求 12 所述的签名方法，其特征在于其包括使用户能够选择所述认证描述符的步骤。

19. 根据权利要求 12 所述的签名方法，其特征在于其包括用于将所述认证描述符的地址并入所述数字流 (10) 的步骤。

20. 根据权利要求 19 所述的签名方法，其特征在于所述并入步骤用于将至少一个散列描述符引入每个所述数字流 (10) 中，所述散列描述符包括至少一个摘要值，还包括用于计算所述摘要值的所述认证描述符的地址，所述至少一个摘要值是通过将散列算法应用于至少一个所述认证描述符而得到的，并被用于计算所述签名。

21. 根据权利要求 20 所述的签名方法，其特征在于所述并入步骤用于根据树结构，将所述散列描述符排列在所述数字流 (10) 中，通过具有较低等级的至少一个其他所述散列描述符来计算至少一个所述散列描述符。

22. 根据权利要求 19 所述的签名方法，其特征在于每个表格包括具有有限大小并分配有号码的至少一个部分，并且每个部分包括将描述符连续引入该部分的至少一个环，所述并入步骤用于通过至少提及所述部分号码以及出现次数来规定每个所述认证描述符的地址，所述每个所述认证描述符属于给定部分的至少一个给定环、并具有分别针对这些环中的每一个的至少一个出现次数。

23. 一种用于通过检查并入在数字流 (10) 中的至少一个签名对通过通信网络 (5) 接收到的所述数字流 (10) 进行认证的认证设备 (21)，所述数字流 (10) 中的每一个均包括几个信息实体，所述实体包括：

- 内容，至少与视听信息相关；

- 以及至少一个信令，由与所述内容的源、宿和结构相关的信息集合构成，由于网络要求，所述信令能够可靠地在网络中进行修改，包含被称为描述符的必要数据结构，并主要通过被称为表格的已排列编组构建，

其特征在于所述认证设备 (21) 包括在所述信令的描述符中有选择确定描述符的装置以及用于将所述认证应用于所确定的描述符的装置，所确定的描述符被称为认证描述符，其保持不被网络头端中的重新复用步骤所触及，以及由其计算所述签名，

所述认证设备 (21) 应用于包括通过根据权利要求 1 到 11 之一所述的签名设备 (11) 所产生的签名的数字流 (10)。

24. 一种用于通过检查并入在数字流 (10) 中的至少一个签名对通过通信网络 (5) 接收到的所述数字流 (10) 进行认证的方法，所述数字流 (10) 中的每一个均包括几个信息实体，所述实体包括：

- 内容，至少与视听信息相关；

- 以及至少一个信令，由与所述内容的源、宿和结构相关的信息集合构成，由于网络要求，所述信令能够可靠地在网络中进行修改，包含被称为描述符的必要数据结构，并主要通过被称为表格的已排列编组构建，

其特征在于所述认证方法包括在所述信令的描述符中有选择确定描述符的步骤以及将所述认证应用于所确定的描述符的步骤，所确定的描述符被称为认证描述符，其保持不被网络头端中的重新复用步骤所触及，由其计算所述签名，

所述认证方法应用于包括通过根据权利要求 1-11 之一所述的签名设备 (11) 所产生的签名的数字流 (10)。

签名和认证设备及方法和相应的产品

技术领域

[0001] 本发明涉及签名(signing)和认证(authentication)设备及方法和相关产品，特别用于DVB(数字视频广播)/MPEG(运动图像专家组)数字流，尤其针对MHP(多媒体家庭平台)标准。

背景技术

[0002] 因此，其特别涉及数字电视领域。数字电视环境包括对不同种类数据的广播或流式传输(streaming)，例如，不同种类的数据包括视听内容(典型为MPEG音频/视频)、互动内容、触发、节目专用信息(与所发送的节目有关的专用信息，简写为“PSI”)、服务信息(使接收器能够自动配置、使用户能够通过EPG-电子节目指南对服务进行浏览的补充信息，简写为“SI”)、专用数据、信令等。通常，将与内容(即PSI、SI和一些专用数据)的源、宿和结构有关的信息整合在信令中。

[0003] 这些数据通常通过MPEG-2传送流进行传送，所述MPEG-2传送流由在PES(分组单元流)中传送的视听流和在MPEG-2部分中传送的其他信息(信令、PSI、SI、互动内容…)构成。一些数字广播网络和宽带网络或多或少地容易受到电子欺骗的攻击。具有良好技术装备的盗版者可以在网络中解译数据、对其进行修改并重新广播(或重新流式传输)这些数据。陆地和微波广播网络比卫星或有线网络更容易受到攻击。因此，问题在于确保MPEG-2网络上的数字数据传输的安全性。

[0004] 事实上，如视听内容、PSI和PI等所列出的一些数据项是纯广播内容，所以对其的盗版会引起用户的烦恼，但至少不会对其有钱财影响。但是，具有返回信道的交互终端可以运行t-commerce(电视商务)或家庭银行应用程序。对这种应用程序的电子欺骗不仅会令用户非常愤怒，而且可能会耗费其大量金钱。

[0005] 数据内容的认证已经是公知的。特别地，参考文献WO-99/49614描述了一种在数字流中发送的数据的认证方法，其中分级地组织数据，至少形成一个根目录单元、子目录单元和文件单元。对文件中的数据进行签名，并将相关文件认证值存储在引用子目录单元中。依次签名此文件认证值，并将相关子目录认证值存储在引用根目录单元中。此公开的其他方案涉及通过产生第二认证值对第二根目录进行认证，以及在封装到传送流的表格或部分中之前认证数据。

[0006] 同样，文件WO-99/62248公开了一种在交互电视系统中实现的方法，用于管理交互电视应用程序的模块。该系统从广播台向多个接收台传输模块，接收台具有模块管理器，存储模块请求，并对与请求相对应的模块的多个信道进行监控。在详细的实施例中，要传输的应用程序由一系列的模块构成，其中每一个均为目录模块。目录模块包含针对应用程序中的每个模块的条目和足够的信息，已允许接收台访问应用程序的所有模块。此外，在接收台中也可以采用认证机制，以确保当前所下载的传送带和/或模块是可信的。

[0007] 此外，如DVB多媒体家庭平台等互动系统规定了如何认证广播应用程序，并且其规定了如何保护通过返回信道传送的数据内容。但是，欺骗操作仍然是可能的，因为可以通

过适当的方式改变信令，从而取消、替换或添加内容，而不会有任何明显的区别。于是，不仅试图提供对内容的认证，还试图提供对信令本身的认证，例如，特别是针对根据 ATVEF（表示高级电视增强论坛）标准而构建的流。

[0008] 但是，这种方法引起了针对 DVB 数字流的特殊问题，因为通常在网络头端 (head-end) 中对流进行重新复用。因此，由于网络要求，PID（分组标识符）甚或如 PMT（表示节目映射表，每个节目一个表格，除与该节目有关的专用信息之外，可能指示构成该节目的 PES 的 PID) 等表格的内容存在被修改的危险。这将意味着再次计算所有散列码和签名，其涉及将专用密钥赋予每个复用器以计算适当的签名。现在，用于向每个复用器提供已验证密钥对的成本将是巨大的。开发这种信令认证策略的技术人员已经发现了这种情况。

发明内容

[0009] 本发明涉及一种设备，用于对要通过通信网络进行传输的数字流进行签名，适用于 DVB 数字流认证，尤其针对 MHP 应用程序，并使得通信更加安全。

[0010] 还涉及一种对应的方法、以及一种设备和一种相关解码器和一种用于对通过通信网络接收到的数字流进行认证的方法，以及对应的软件和数字流。

[0011] 因此，本发明应用于一种设备，通过产生通过应用于数字流的加密而获得的、要并入所述数字流中的至少一个签名，对要通过通信网络传输的数字流进行签名。这些数字流中的每一个均包括几个信息实体，这些实体包括：

[0012] - 内容，至少与视听信息相关；

[0013] - 以及至少一个信令，由与所述内容的源、宿和结构相关的信息集合构成，由于网络要求，所述信令能够可靠地在网络中进行修改，包含被称为描述符的必要数据结构，并主要通过被称为表格的已排列编组构建。

[0014] 根据本发明，所述签名设备用于将加密至少应用于所述信令，更具体地，应用于所述信令的描述符中有选择确定的描述符，被称为认证描述符。

[0015] 所以，与如果信令已经被签名将采用的自然解决方案，即对整个部分（信令的子表格，具有有限大小）应用认证处理相反，选择信令的特定描述符，以进行认证。这种令人惊讶的解决方案的直接优点在于，对于签名，能够选择重新复用步骤并未触及的描述符。因此，可以非常有效地实现防止恶意修改的保护，同时避免由于网络头端中的重新复用而给认证处理带来的巨大复杂性。

[0016] 此外，在重新复用设备中，甚至在针对签名，决定保留在重新复用期间将被修改的一些描述符时，与不得不再次对整个部分进行签名以产生考虑到修改后的描述符的已更新签名相比，更为轻便和快捷。实际上，利用对已修改描述符的明智选择，在发射级获得的大多数信息都能够得到保留，特别是按照由散列得到的未改变摘要值的形式，而只是针对签名，必须重新计算签名信息的一小部分。

[0017] “视听信息”表示音频和 / 或视频信息。

[0018] 优选地，根据 DVB 和 MPEG 标准，更具体地根据 MHP 标准，构建所述数字流。

[0019] 本发明的签名设备可以应用于对 MPEG/DVB 表格的认证，尤其是用于 PSI 表格：PMT、PAT（节目访问表，表示针对每个所发送的节目，节目号与 PMT 传送分组的 PID 之间的链接）、CAT（条件访问表，在至少一个节目具有条件访问的情况下，给出了携带权利管理

消息 -EMM 的 PES 的 PID)，以及用于 DVB-SI 表格 :NIT(网络信息表)、SDT(服务描述表)、EIT(事件信息表)、TOT(时间偏移量表)、AIT(应用程序信息表)、BAT(束关联表)。所述签名设备也可以应用于基于 MPEG2 系统 (ISO/IEC 13818-1) 部分语法的任何 MPEG/DVB 专用表格。

[0020] 有利地，所述签名设备包括使用户能够选择所述认证描述符的装置。例如，该用户是广播组的成员。则，将所选择的描述符中的任何一个标识符并入流中，从而当接收器接收到这些流之前，将所使用的描述符通知给接收器，或者在发射器和接收器之前事先就所选择的描述符达成一致。另一解决方案在于更系统化地确定所选择的描述符，例如，按照特定标准版本。

[0021] 优选地，所述签名设备用于 :

[0022] - 将至少一个最低级签名描述符中的签名引入所述数字流 ;

[0023] - 以及还将包括与该签名有关的证书数据的至少一个证书描述符 ;

[0024] - 以及通过将加密应用于所述最低级签名描述和所述证书描述符的内容而得到的至少一个较高级签名描述符并入所述数字流。

[0025] 这对于安全、灵活地确保如广播公司和制造商等多个参与者之间的互操作性非常有意义。

[0026] 实际上，只要提供几个等级，将能够导致公用密钥基础结构 (PKI)。于是，建立根证书权限 (针对最高级签名)，以及可选地，建立其他证书权限。

[0027] 优选地，所述签名设备包括用于将所述认证描述符的地址并入所述数字流的装置。这是使接收器知道针对签名而使用的描述的有效方式。

[0028] 于是，有利的是，所述并入装置用于将至少一个散列描述符引入每个所述数字流中。所述散列描述符包括通过将散列算法应用于至少一个所述认证描述符而得到的至少一个摘要值 (digest value)，并将其用于计算所述签名。所述散列描述符还包括用于计算所述摘要值的所述认证描述符的所述地址。这些方式提高了认证效率，因为其依赖于用于计算签名并从而用于检验其真实性的传递中间结果。

[0029] 更具体地，所述并入装置优选地用于根据树结构，将所述散列描述符排列在所述数字流中，通过具有较低等级的至少一个其他所述散列描述符来计算至少一个所述散列描述符。摘要值的嵌套计算能够逐渐计算由其最终获得签名的基本值 (即，根摘要值)，同时确保考虑了与多个认证描述符有关的所有必需信息。

[0030] 优选地，所述摘要值具有固定的大小，与现有散列算法中的通常情况相同。

[0031] 同样优选的是具有并入装置的以下实施例，每个表格包括具有有限大小并分配有号码的至少一个部分，并且每个部分包括将描述符连续引入该部分的至少一个环。有利地，这些并入装置用于规定属于给定部分的至少一个给定环、并具有分别针对这些环中的每一个的至少一个出现次数的每个所述认证描述符的地址，通过至少提及 :

[0032] - 该部分号

[0033] - 以及这些出现次数。

[0034] 按照这种方式，能够有效且按照简单的方式识别针对验证而使用的描述符的标识。

[0035] 用于寻址的其他可能传输信息包括 :

[0036] - 该部分的版本号，

[0037] - 和 / 或该部分的类型。

[0038] 在具有所述并入装置的特定实现中，有利地，所述签名设备用于将签名和可能的至少一个摘要值和证书数据以专用数据的形式引入至少一个特定的部分，所述特定部分与包含所述认证描述符的部分相链接。该实现允许将至少一些认证信息与其他信令信号相分离。

[0039] 因此，在优选实施例中，所述特定部分用于包含签名和证书数据，有利地，以签名和证书描述符的形式，以及给出了根摘要值并指向其他部分中的较低级摘要值的根散列描述符。这可能是非常有利的，因为 DVB/MPEG-2 的结构不允许将描述符设置在部分的开始，而这对于所述部分的整个剩余部分都是有效的。即，所有描述符均位于环中的某处，这也是不能与所述部分一起直接发送顶级描述符的原因。

[0040] 在具有特定部分的另一实施例中，不仅将签名和证书数据以及根散列描述符设置在所述特定部分中，而且将所有其他散列描述符设置在所述特定部分中（例如，位于所述部分的顶级）。这对于 DVB/MPEG-2 是可能的，因为寻址机制允许对表格中的描述符进行直接寻址。

[0041] 本发明还涉及一种对应于上述设备的方法，用于通过根据本发明的签名设备的任意实施例来执行。

[0042] 本发明的另一目的是一种用于通过检查并入在数字流中的至少一个签名对通过通信网络接收到的所述数字流进行认证的设备。这些数字流中的每一个均包括几个信息实体，这些实体包括：

[0043] - 内容，至少与视听信息相关；

[0044] - 以及至少一个信令，由与所述内容的源、宿和结构相关的信息集合构成，由于网络要求，所述信令能够可靠地在网络中进行修改，包含被称为描述符的必要数据结构，并主要通过被称为表格的已排列编组构建。

[0045] 根据本发明，所述认证设备用于将认证至少应用于所述信令，更具体地，应用于所述信令的描述符中有选择确定的描述符，被称为认证描述符，由其计算所述签名。

[0046] 优选地，所述认证设备应用于包括通过根据本发明的签名设备所产生的签名的数字流。

[0047] 本发明还涉及一种解码器，其特征在于其包括根据本发明的认证设备。

[0048] 本发明的另一目的是一种对应于本发明的认证设备的认证方法，优选地用于通过根据本发明的认证设备的任意实施例来执行。

[0049] 本发明还涉及一种计算机程序产品，包括当在计算机上执行该程序时，用于执行根据本发明的签名或认证方法的步骤的程序代码指令。

[0050] 术语“计算机程序产品”应当被理解为包括计算机程序的任何物质化，不仅涉及存储支持（磁带、盘、…），还涉及信号（电信号、光信号、…）。

[0051] 本发明还应用于一种包括几个信息实体的数字流，这些实体包括：

[0052] - 内容，至少与视听信息相关；

[0053] - 以及至少一个信令，由与所述内容的源、宿和结构相关的信息集合构成，由于网络要求，所述信令能够可靠地在网络中进行修改，包含被称为描述符的必要数据结构，并主

要通过被称为表格的已排列编组构建，

[0054] - 将至少一个签名并入所述数字流。

[0055] 根据本发明，根据所述信令，计算所述签名，更具体地，根据所述信令的描述符中有选择地确定的描述符，被称为认证描述符。

[0056] 优选地，通过要求保护的签名设备的任意实施例产生所述数字流。

附图说明

[0057] 通过以下参考附图的非限制性实施例，将更好地理解和示出本发明，其中：

[0058] - 图 1 是根据本发明的签名设备和对应的认证设备的示意图；

[0059] - 图 2 示出了 DVB/MPEG-2 单元流，包括视听和专用数据流以及相关表格 (PAT、PMT 和 AIT)，并指出了表格和流之间的链接；

[0060] - 以及图 3 详细示出了图 2 所示的一些表格 (PMT 和 AIT)，与单元流相关，以及与应用程序信息和应用程序流相关。

具体实施方式

[0061] 数字流 10 的发射器 1 通过网络 5 向具有解码能力的接收器 2 发送这些流 10（图 1）。发射器 1 典型地用于广播流 10，例如，网络 5 是宽带或广播网络，以及特别是有线或卫星网络。在另一实施例中，网络 5 由因特网构成。在所示情况下，数字流 10 由 DVB/MPEG-2 流构成，从而特别包括内容和与之相关的信令数据。信令主要由表格构成，并包括描述符。流 10 可以符合 MHP 标准。

[0062] 发射器 1 包括：签名设备 11，用于对要发送的数字流 10 进行签名；以及用户接口 15，特别用于使如广播公司等发送者能够控制签名处理。签名设备 11 用于对信令进行签名，不仅是内容。其包含选择模块 12，使用户通过用户接口 15 选择信令的一些描述符，称为认证描述符，用于信令认证。因此，对其进行加密，以获得相关签名。签名设备 11 还包含并入模块 13，能够将认证描述符的地址并入所发送的数字流 10。

[0063] 每个接收器 2 包括认证设备 21，能够检查所接收到的签名，尤其是用于信令认证的签名。认证设备 21 能够考虑流 10 中所指示的用于认证的认证描述符。

[0064] 现在，将对特别感兴趣的示例进行描述。发送数字电视服务（互动或非互动）信号的重要入口点是在 MPEG-2 系统标准 (ISO/IEC13818-1) 中所规定的 PMT（节目映射表）。在发送互动 MHP 应用程序的信号的情况下，PMT 包含传送 AIT（应用程序信息表）的流的位置和传送应用程序代码和数据的流的位置（对 DSM-CC DSI 消息的指针，DSM-CC 表示“下载服务启动”，ISO/IEC 13818-6 国际标准），如图 2 和图 3 所示。以下的技术方案能够保护互动 MHP 应用程序的信令数据，从而使解码平台能够检查其在传送网络上是否已经被修改。此外，MPEG-2 系统标准禁止对 PMT 的加扰，所以这里并未考虑加扰。

[0065] 信令的保护基于散列码、签名和证书。通过规定三个新的描述符来进行这些密码消息的编码，分别包含以上对象：

[0066] • hash_descriptor

[0067] • signature_descriptor

[0068] • certificate_descriptor.

[0069] 这里针对单独认证的每个部分，单独引入 hash_descriptor 字段，并且我们下面将考虑表格的这个给定部分，无论该表格由多个部分或者只由一个部分构成。另一方面，signature_descriptor 字段应用于表格中的所有 hash_descriptor 字段，以及 certificate_descriptor 字段涉及该表格中的所有 signature_descriptor 字段。

[0070] 对 hash_descriptor 的说明

[0071] hash_descriptor 可以位于 AIT 或 PMT（或任何其他要认证的 MPEG-2 表格）的环中。更具体地，其位于包括要认证的描述符的每个描述符环中。环中的位置并不重要，因为 hash_descriptor 包括能够惟一寻址每个描述符的 descriptor_address 字段。

[0072] hash_descriptor 包含散列码，也称为摘要值，根据 descriptor_address 所指向的描述符进行计算。在 AIT 或 PMT 的情况下，其只包括跟随在与 hash_descriptor 相同的环 (loop) 中的描述符。所指向的描述自身可以位于 hash_descriptor 字段中，从而能够实现类似递归的计算处理。

[0073] hash_descriptor 的语法如下：

[0074]
```
hash_descriptor(){
```

[0075]
```
  descriptor_tag                    8    uimsbf
```

[0076]
```
  descriptor_length                 8    uimsbf
```

[0077]
```
  digest_count                      16   uimsbf
```

[0078]
```
  for(i = 0;i < digest_count;i++){
```

[0079]
```
    digest_type                     8    uimsbf
```

[0080]
```
    descriptor_count                8    uimsbf
```

[0081]
```
    for(j = 0;j < descriptor_count;j++){
```

[0082]
```
      descriptor_address            40   uimsbf
```

[0083]
```
    }
```

[0084]
```
    for(j = 0;j < digest_length;j++){
```

[0085]
```
      digest_byte                   8    bslbf
```

[0086]
```
    }
```

[0087]
```
  }
```

[0088]
```
}
```

[0089] 其中“uimsbf”和“bslbf”分别表示“无符号整数最高有效位优先”和“位串最左位优先”。

[0090] descriptor_tag：hash_descriptor 的标签。

[0091] descriptor_length：hash_descriptor 的长度。

[0092] digest_count：此 16 位数值识别此散列描述符中的摘要值的数量。

[0093] digest_type：此 8 位数值识别可能用于相关描述符的摘要算法。在表 1 中给出了其允许值，其中在 RFC 1321(RFC 表示请求注解；http://www.ietf.org/rfc/rfc1321.txt) 中定义了 MD-5(MD 表示“消息摘要”)，以及在 FIPS-180-1(FIPS 公开 180-1：安全散列标准，国家标准和技术学院，1994 年；http://www.itl.nist.gov/fipspubs/fip180-1.htm) 中定义了 SHA-1(SHA 表示“安全散列算法”)。

[0094] 表 1- 摘要算法的允许值

[0095]

值	摘要长度	算法
0	0	非认证
1	16	MD-5
2	20	SHA-1
其他		保留

[0096] descriptor_count :此 16 位数值识别与摘要值相关的描述符的数量。此字段的数值应当大于零。

[0097] descriptor_address :这是部分中的描述符的普通地址,稍后将进行详细的解释。

[0098] digest_length :此整数值给出了每个摘要值的字节数。其依赖于如图 1 所示的摘要类型。

[0099] digest_byte :此 8 位数值保持摘要值的一个字节。

[0100] 对 signature_descriptor 的说明

[0101] 该描述符的语法如下 :

[0102] signature_descriptor(){

[0103] descriptor_tag 8 uimsbf

[0104] descriptor_length 8 uimsbf

[0105] signature_id 8 uimsbf

[0106] signature_length 8 uimsbf

[0107] for(i = 0 ;i < N ;i++){

[0108] signature specific data

[0109] }

[0110] }

[0111] descriptor_tag :signature_descriptor 的标签。

[0112] descriptor_length :signature_descriptor 的长度。

[0113] signature_id :此 ID(表示“标识符”) 使其能够具有来自多于一个权威机构的签名。

[0114] signature_length :指示跟随环 (following loop) 的长度。

[0115] 字段“signature specific data”包含以下 ASN.1,ASN.1 结构 (表示“摘要语法注释一”语言),是 BER(基本编码规则) 和 DER(区分编码规则) 结构的组合 :

[0116] Signature:: = SEQUENCE{

[0117] certificateIdentifier AuthorityKeyIdentifier,

[0118] hashSignatureAlgorithm HashAlgorithmIdentifier,

[0119] signatureValue BIT STRING}

[0120] certificateIdentifier :如 ITU-T X.509 扩展 (代表国际电信联盟 - 电信标准部分,建议 X.509 :目录认证框架,1997 年) 中所定义,与 AuthorityKeyIdentifier 字段有关。

其识别携带有用于检验签名的已验证公共密钥的证书：

[0121] AuthorityKeyIdentifier:: = SEQUENCE{

[0122] keyIdentifier [0]KeyIdentifier 可选，

[0123] authorityCertIssuer [1]GeneralNames 可选，

[0124] authorityCertSerialNumber[2]CertificateSerialNumber 可选}

[0125] 实施不需要使用 AuthorityKeyIdentifier 的可能出现的密钥标识符元素（“keyIdentifier”）。AuthorityKeyIdentifier 结构包含权限证书发布者标识(authorityCertIssuer) 和相应的权限证书序列号元素 (authorityCertSerialNumber)。

[0126] authorityCertIssuer 字段包含字段“directoryName”,给出了携带有用于检查签名的公共密钥的证书的发布者名称（并因而等于用在 MHP 中的字段 issuerName)。

[0127] hashSignatureAlgorithm :此字段识别所使用的散列算法。由于涉及计算签名所需的加密算法,已经在证明相关密钥的证书中对其进行了描述（在 SubjectKeyInfo 字段中）。因此,只需要散列算法的标识。所支持的算法是 MD5 和 SHA-1,其中经典地通过下式给出标识符（参见 RFC 2379）：

[0128] md5 OBJECT IDENTIFIER:: =

[0129] {iso(1)member-body(2)US(840)rsadsi(113549)

[0130] digestAlgorithm(2)5}

[0131] sha-1 OBJECT IDENTIFIER:: =

[0132] {iso(1)identified-organization(3)oiw(14)secsig(3)

[0133] algorithm(2)26}

[0134] signatureValue :签名的数值,依赖于 MHP 规范的选择。

[0135] 对 certificate_descriptor 的说明

[0136] 与经典的 PKI 技术一样,该描述符包含递归使用的几个证书。特别地,将叶证书首先设置在 certificate_descriptor 中,而最后指示仅针对一致性而包括在其中的根证书。

[0137] 名称为 CertificateFile 的文件包含在 certificate_descriptor 中所提及的证书链中的所有证书,一直到根证书,并包括根证书。在 ETSI TS 102 812 V1.1.1(表示“欧洲电信标准学院,技术规范”）中定义了用于编码证书的简档表 (profile)。

[0138] certificate_descriptor 规定如下：

[0139] certificate_descriptor(){

[0140] descriptor_tag 8 uimsbf

[0141] descriptor_length 8 uimsbf

[0142] signature_id 8 uimsbf

[0143] certificate_here_flag 1 bslbf

[0144] reserved 7 bslbf

[0145] if(certificate_here_flag == 1){

[0146] certificate_cout 16 uimsbf

[0147] for(i = 0 ;i < certificate_count ;i++){

[0148] certificate_length 24 uimsbf

[0149] certificate()

[0150] }

[0151] }

[0152] }

[0153] descriptor_tag :certificate_descriptor 的标签。

[0154] descriptor_length :certificate_descriptor 的长度。

[0155] signature_id :此 ID 对证书和特定的签名进行链接。

[0156] certificate_here_flag :为位字段，当设置为“1”时，表示证书位于此描述符中。否则，应当使用来自应用程序的证书，必须对链接进行定义。

[0157] certificate_count :此 16 位整数带有证书描述符中的证书数。

[0158] certificate_length :此 24 位整数规定了证书的字节数。

[0159] certificate() :此字段带有由 ITU-T X.509 定义的单一“证书”数据结构。

[0160] 在 MHP 平台的情况下，可以使用与用于交互应用程序相同的证书管理。否则，具体建立针对证书管理的机制。

[0161] MPEG/DVB 部分中的描述符的普通寻址

[0162] (hash_descriptor 中的字段“descriptor_address”)

[0163] 现在，将详细描述寻址 MPEG 和 DVB 表格中的描述符的寻址机制。可以使用可变长度寻址机制，其能够以更为紧凑的方式存储地址。但是，在本实施例中，地址具有 40 位的恒定长度，使得处理更为容易。查看目前的 MPEG 和 DVB 规范，可以识别三种不同类型的部分。

[0164] 第一部分类型（此后表示为“type0”）具有以下结构，利用这种 type0 部分构建 PAT、CAT 和 TOT 表格：

[0165] type0_section(){

[0166] table_id

[0167] …

[0168] for(i = 0 ;i < N ;i++){

[0169] descriptor()

[0170] }

[0171] CRC_32

[0172] }

[0173] table_id 给出了表格的表示和代表“循环冗余校验”的 CRC。

[0174] 在 type0 部分的情况下，地址中的字节具有如下含义：

[0175] • 第一字节 :表格中的部分数；

[0176] • 第二字节 :0；

[0177] • 第三字节 :0；

[0178] • 第四字节 :i(N)，此字节寻址 type0 部分环中的描述符。

[0179] 第二部分类型（此后表示为“type1”）具有以下结构，利用这种 type1 部分构建 SDT 和 EIT：

[0180] type1_section(){

[0181] table_id

[0182] …

[0183] for(i = 0 ;i < N1 ;i++){

[0184] …

[0185] for(j = 0 ;j < N2 ;j++){

[0186] descriptor()

[0187] }

[0188] }

[0189] CRC_32

[0190] }

[0191] • 第一字节 :表格中的部分数 ;

[0192] • 第二字节 :0 ;

[0193] • 第三字节 :i(N1),此字节寻址 type1 部分的外环 ;

[0194] • 第四字节 :j(N2),此字节寻址 type1 部分的内环。

[0195] 第三部分类型 (此后表示为“type2”) 具有以下结构,利用这种 type2 部分构建 NIT、BAT、PMT 和 AIT 表格 :

[0196] type2_section(){

[0197] table_id

[0198] …

[0199] for(i = 0 ;i < N1 ;i++){

[0200] descriptor()

[0201] }

[0202] …

[0203] for(j = 0 ;j < N2 ;j++){

[0204] …

[0205] for(k = 0 ;k < N3 ;k++){

[0206] descriptor()

[0207] }

[0208] }

[0209] CRC_32

[0210] }

[0211] 在 type2 部分的情况下,描述符地址需要五个字节 :

[0212] • 第一字节 :表格中的部分数 ;

[0213] • 第二字节 :i(N1),此字节寻址 type2 部分的第一环 ;

[0214] • 第三字节 :j(N2),此字节寻址 type2 部分的外环 ;

[0215] • 第四字节 :k(N3),此字节寻址 type2 部分的内环。

[0216] 顶级描述符

[0217] 通过顶级描述符,理解 certificate_descriptor 和 signature_descriptor 字段,以及指向具有要认证的描述符的部分中的所有其他 hash_descriptor 字段的 hash_descriptor 字段 (即,包含根摘要值的 hash_descriptor)。

[0218] 在本实施例中,在特定的部分中发送这些描述符,所述特定的部分与包含要认证

的描述符的部分相链接。此链接特定部分包含与原始部分相同的 PID 和 Table_ID,但通过被称为“section_syntax_indicator”的特定的指示符与之相区分。对于所有 DVB/MPEG 定义部分,将此 section_syntax_indicator 设置为一,表示部分语法遵循普通部分语法。对于特定扩展,将 section_syntax_indicator 设置为零,表示专用数据出现在给出了特定部分的长度的字段 (private_section_length) 之后。按照其可以包含顶级信息的方式规定这些专用数据。例如,扩展部分具有以下结构 :

[0219] extension_section(){

[0220] table_id 8 uimsbf

[0221] section_syntax_indicator 1 bslbf

[0222] private_indicator 1 bslbf

[0223] reserved 2 bslbf

[0224] private_section_length 12 uimsbf

[0225] reserved 3 bslbf

[0226] version_number 5 uimsbf

[0227] certificate_descriptor()

[0228] signature_descriptor()

[0229] hash_descriptor()

[0230] }

[0231] 在 ISO/IEC 13818-1 中的专用部分定义部分对其进行了规定的字段 private_indicator 是针对未来使用的保留位,以及字段“version_number”扩展部分所属的表格版本 (特别参见 EN 300 468V1.3.1- 针对“欧洲标准”)。

[0232] 示例

[0233] 以下示例示出了可以如何将 AIT 的描述符用于签名。在此示例中,对由几个部分形成的整个表格进行全局认证,而不是像以前那样对每个部分进行单独认证。第一步是选择要认证的描述符。第二步是利用 MD5 摘要算法计算这些描述符的散列码。位于每个包含至少一个认证描述符的环中的 hash_descriptor 包含这些描述符的地址和这些描述符的 MD5 摘要值。由于 hash_descriptor 是可寻址的,不需要具有环中特定的位置。按照这种方式,可以针对 AIT 部分,产生散列码。

[0234] 以下附图示出了在通常 AIT 结构中插入 hash_descriptor(如 ETSI TS 102 812 V1.1.1 所定义) :

[0235]

	位数	标识符
Application_information_section() {		
Table_id	8	uimsbf
Section_syntax_indicator	1	bslbf
Reserved_for_future_use	1	bslbf
…		
Common_descriptor_length	12	uimsbf
for (i=0; i<N1; i++) {		
// hash_descriptor()		
// other descriptor()		
}		
…		
application_loop_length	12	uimsbf
for (i=0; i<N2; i++) {		
application_identifier()		
application_control_code	8	uimsbf
…		
application_descriptors_loop_length	12	uimsbf
for (j=0; j<N3; j++) {		
// hash_descriptor()		
// other descriptor()		
}		
}		
CRC_32	32	rpchof
}		

[0236] 其中“rpchof”表示“余式多项式系数,最高次数优先”。

[0237] 完整的AIT表格可以由几个部分构成,与任何DVB/MPEG表格相同。在已经计算了表格的所有部分的散列码之后,必须产生顶级信息。为此,计算考虑了对应表格的所有hash_descriptor字段的顶级hash_descriptor(根摘要值),其中使用上述描述符寻址机制。下一步是利用与能够在相应certificate_descriptor的叶证书中找到的公用密钥相对应的专用密钥,对此顶级hash_descriptor进行RSA-加密(RSA密码算法表示Rivest-Shamir-Adleman)。此RSA-加密的结果是存储在signature_descriptor中的签名。将这三个顶级描述符存储在相应表格的所谓扩展部分中。在AIT的情况下,表格ID总是0x74,但PID(分组标识符)是列出在相应服务的PMT中的数值。包含顶级描述符的扩展部分具有与要认证的AIT相同的PID和表格ID,但将section_syntax_indicator设置为零:

[0238] extension_section(){

[0239] table-id(0x74) 8 uimsbf

[0240] section_syntax_indicator(0x00) 1 bslbf

[0241] private_indicator 1 bslbf

[0242] reserved 2 bslbf

[0243] private_section_length 12 uimsbf

[0244] reserved 3 bslbf

[0245] version_number 5 uimsbf

[0246] certificate_descriptor()

[0247] signature_descriptor()

[0248] hash_descriptor()

[0249] }

[0250] 版本号表示此扩展部分所属的表格版本。

[0251] 在变体实施例中，所有 hash_descriptor 字段位于 extension_section 中的顶级。

[0252] 在实施中，推荐将 section_syntax_indicator 设置为“不关心”（表示处理流的解复用器通过该位，而与其状态为“1”或“0”无关），从而所需的 DVB/MPEG 部分本身和 extension_section 通过解复用器滤波器。按照这种方式，扩展部分中的顶级描述符直接可用，并能够立即进行认证。

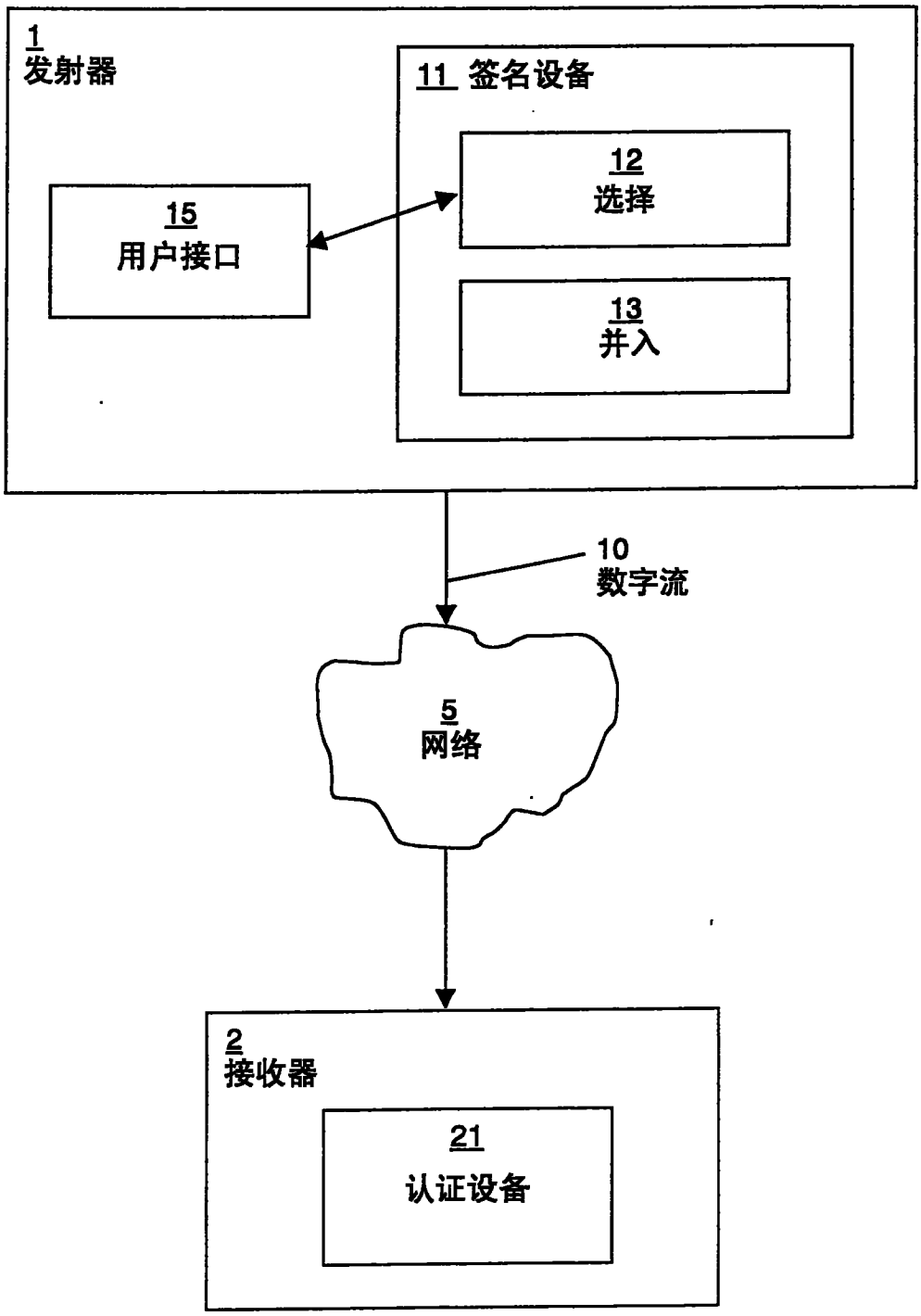


图 1

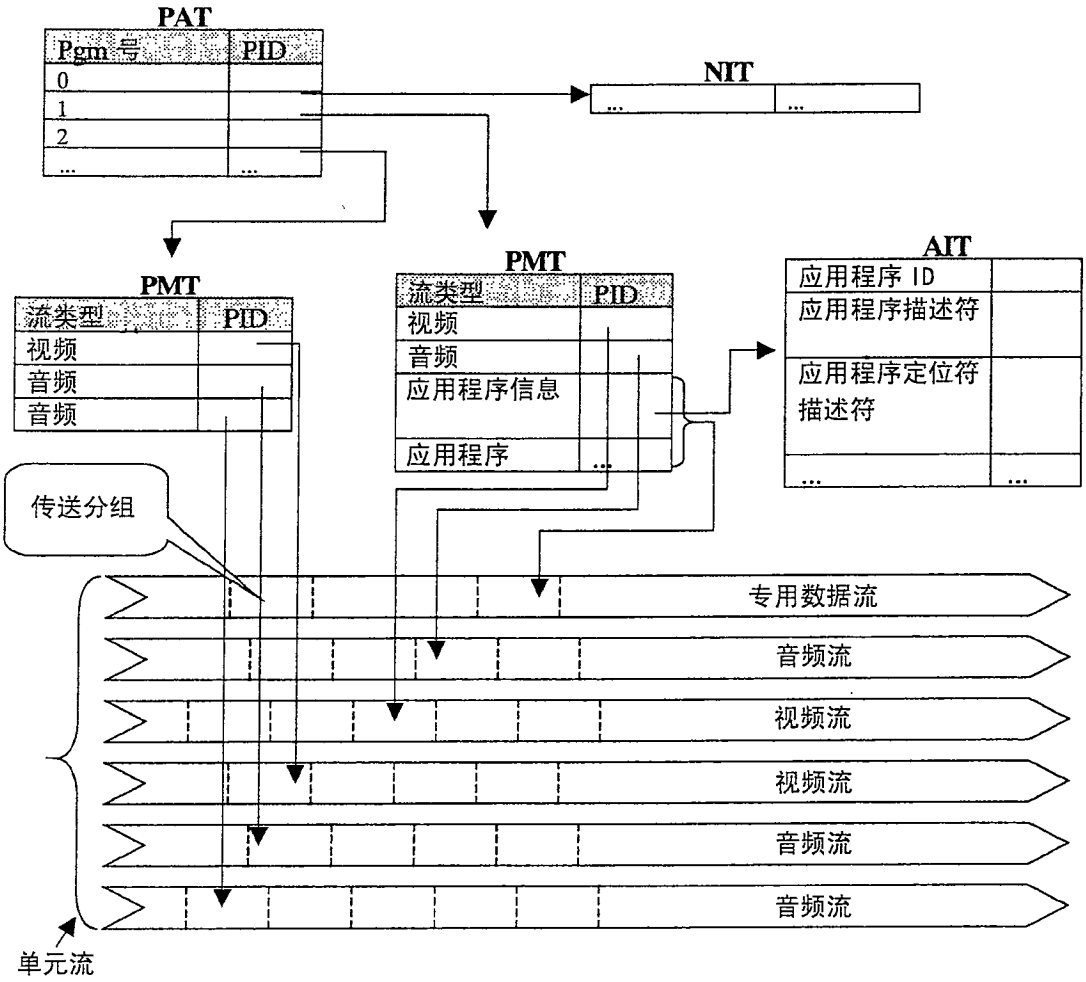

PAT
Pgm 号
PID
0
1
2
...
NIT
...
...
PMT
流类型
PID
视频
音频
音频
PMT
流类型
PID
视频
音频
应用程序信息
应用程序
...
AIT
应用程序 ID
应用程序描述符
应用程序定位符
描述符
...
...
传送分组
专用数据流
音频流
视频流
视频流
音频流
音频流
单元流

图 2

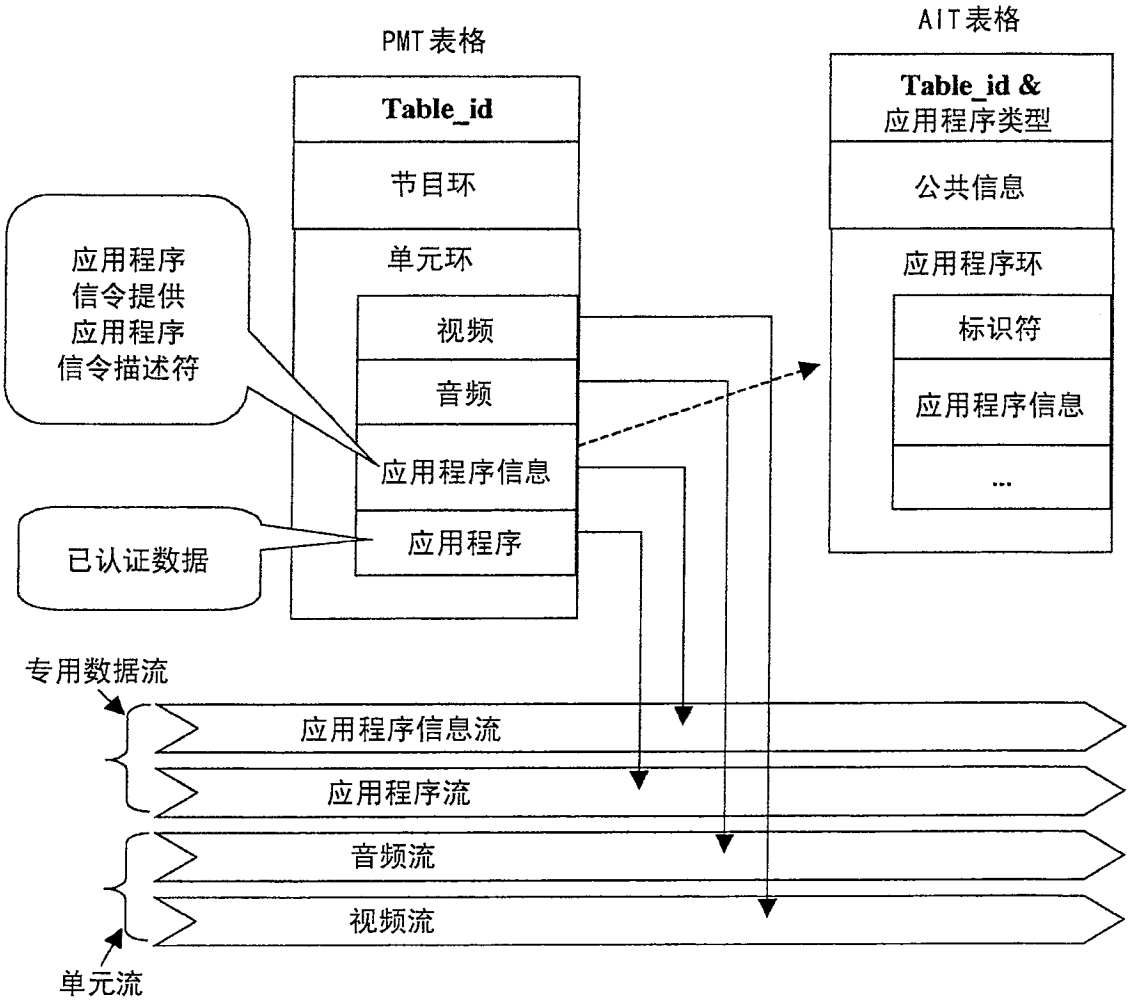

PMT表格
Table_id
节目环
单元环
视频
音频
应用程序信息
应用程序
应用程序
信令提供
应用程序
信令描述符
已认证数据
AIT表格
Table_id &
应用程序类型
公共信息
应用程序环
标识符
应用程序信息
...
专用数据流
应用程序信息流
应用程序流
音频流
视频流
单元流

图 3