



(12) 发明专利申请

(10) 申请公布号 CN 102075813 A

(43) 申请公布日 2011. 05. 25

(21) 申请号 201010511656. 1

(22) 申请日 2010. 08. 27

(30) 优先权数据

09168907. 5 2009. 08. 28 EP

(71) 申请人 耶德托存取公司

地址 荷兰霍夫多普

(72) 发明人 A·A·沃斯 A·E·万弗瑞斯特

G·J·德克尔 B·V·科廷

(74) 专利代理机构 中国国际贸易促进委员会专

利商标事务所 11038

代理人 付建军

(51) Int. Cl.

H04N 21/4623(2011. 01)

H04N 21/4367(2011. 01)

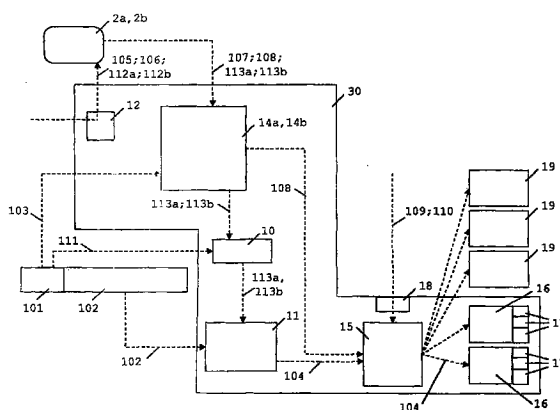
权利要求书 3 页 说明书 7 页 附图 5 页

(54) 发明名称

接收机中数据流的可靠且不可篡改处理

(57) 摘要

本发明涉及接收机中数据流的可靠且不可篡改处理。本发明提供一种用于可能结合智能卡的接收机中数据流的安全且不可篡改处理的方案。分组标识符和与该分组标识符相关联的内容类型标识符以加密的形式被接收并在接收机内安全地处理,以允许处理该数据流的加密的净荷,而不可能在尝试拦截解密后净荷时篡改该内容类型标识符。



1. 一种接收机 (1a) 中的用于处理数据流的方法,所述数据流包括报头和加密的净荷,所述报头包括第一分组标识符,所述方法包括以下步骤:

解密 (1001) 所述加密的净荷以获得解密的净荷;

接收 (1002) 加密的第二分组标识符和加密的第一内容类型标识符;

在安全环境内从所述加密的第二分组标识符获得 (1003) 第二分组标识符;

在所述安全环境内从所述加密的第一内容类型标识符获得 (1004) 与第二分组标识符相关联的第一内容类型标识符;

比较 (1005) 第一分组标识符和第二标识符以获得第一比较结果;

如果第一比较结果与第一预定条件匹配,则基于第一内容类型标识符选择 (1007) 第一解码模块,并将所述解密的净荷路由 (1008) 到第一解码模块以对所述解密的净荷进行解码。

2. 根据权利要求 1 所述的方法,其中,在一个或多个加密的授权消息中接收所述加密的第二分组标识符和所述加密的第一内容类型标识符,并且其中,通过将所述一个或多个加密的授权消息发送 (1009) 到智能卡并经由安全连接从所述智能卡接收 (1010) 第二分组标识符和第一内容类型标识符来获得第二分组标识符和第一内容类型标识符。

3. 一种接收机中的用于处理数据流的方法,所述数据流包括报头和加密的净荷,所述报头包括用于识别所述加密的净荷的第一分组标识符,所述方法包括以下步骤:

解密 (1001) 所述加密的净荷以获得解密的净荷;

在安全环境内从硬编码存储器中获得 (1011) 第二分组标识符;

在所述安全环境内从所述硬编码存储器中获得 (1012) 与第二分组标识符相关联的第一内容类型标识符;

比较 (1005) 第一分组标识符与第二标识符以获得第一比较结果;以及

如果第一比较结果与第一预定条件匹配,则基于第一内容类型标识符选择 (1007) 第一解码模块,并将所述解密的净荷路由 (1008) 到第一解码模块以对所述解密的净荷进行解码。

4. 根据权利要求 3 所述的方法,其中,所述硬编码存储器是接收机的一部分。

5. 根据权利要求 3 所述的方法,其中,所述硬编码存储器是智能卡的一部分。

6. 根据权利要求 1-5 中任一项所述的方法,还包括如下步骤:基于第一内容类型标识符从一组预定义的接口中选择 (1013) 接口,并将第一解码模块的输出限制 (1014) 到所选择的接口。

7. 根据权利要求 1-6 中任一项所述的方法,还包括以下步骤:

接收 (1015) 明文的第三分组标识符和与第三分组标识符相关联的明文的第二内容类型标识符;

如果第一比较结果与第二预定条件匹配,那么比较 (1016) 第一分组标识符和第三分组标识符以获得第二比较结果;以及

如果第二比较结果与第三预定条件匹配,那么基于第二内容类型标识符选择 (1018) 第二解码模块,并将所述解密的净荷路由 (1019) 到第二解码模块以对所述解密的净荷进行解码。

8. 根据权利要求 7 所述的方法,其中

所述数据流是 MPEG2 传输流，
所述报头和所述加密的净荷是所述 MPEG2 传输流中的基本流的一部分，
第三分组标识符和第二内容类型标识符在所述 MPEG2 传输流的节目映射表中接收，
第一解码模块是接收机的安全芯片组中的视频解码器或音频解码器，并且
第二解码模块是所述安全芯片组外部的电视文字广播解码器、字幕解码器或软件小程序。

9. 一种用于处理数据流的接收机 (1a)，所述数据流包括报头 (101) 和加密的净荷 (102)，所述报头 (101) 包括第一分组标识符 (103)，所述接收机 (1a) 包括

解扰器 (11)，被配置为解密所述加密的净荷 (102) 以获得解密的净荷 (104)；

第一输入模块 (12)，被配置为接收加密的第二分组标识符 (105) 和加密的第一内容类型标识符 (106)；

处理器 (13a)；

存储器 (14a)；和

路由器 (15)，

其中，所述处理器 (13a) 被配置为：

从所述加密的第二分组标识符 (105) 获得第二分组标识符 (107) 并从所述加密的第一内容类型标识符 (106) 获得与第二分组标识符 (105) 相关联的第一内容类型标识符 (108)；

在所述存储器 (14a) 中存储第二分组标识符 (107) 和第一内容类型标识符 (108)；

比较第一分组标识符 (103) 和存储在存储器 (14a) 中的第二分组标识符 (107) 以获得第一比较结果；并且

如果第一比较结果与第一预定条件匹配，那么向所述路由器 (15) 提供第一内容类型标识符 (108)，

并且其中，所述路由器 (15) 被配置为：

基于第一内容类型标识符 (108) 选择第一解码模块 (16)；并且

将所述解密的净荷 (104) 路由到第一解码模块 (16) 以对所述解密的净荷 (104) 进行解码。

10. 一种用于处理数据流的接收机 (1b)，所述数据流包括报头 (101) 和加密的净荷 (102)，所述报头 (101) 包括第一分组标识符 (103)，所述接收机 (1b) 包括：

解扰器 (11)，被配置为解密所述加密的净荷 (102) 以获得解密的净荷 (104)；

处理器 (13b)；和

路由器 (15)，

其中，所述处理器 (13b) 被配置为：

从硬编码存储器 (14b) 中获得第二分组标识符 (107) 和第一内容类型标识符 (108)；

比较第一分组标识符 (103) 和存储在硬编码存储器 (14b) 中的第二分组标识符 (107) 以获得第一比较结果；

如果第一比较结果与第一预定条件匹配，那么向所述路由器 (15) 提供第一内容类型标识符 (108)，

并且其中，所述路由器 (15) 被配置为：

基于第一内容类型标识符 (108) 选择第一解码模块 (16) ;并且

将所述解密的净荷 (104) 路由到第一解码模块 (16) 以对所述解密的净荷 (104) 进行解码。

11. 根据权利要求 9 或 10 所述的接收机 (1a, 1b), 其中, 所述处理器 (13a, 13b) 还被配置为基于第一内容类型标识符 (108) 从一组预定义的接口中选择接口 (17) 并将第一解码模块 (16) 的输出限制到所述接口 (17)。

12. 根据权利要求 9-11 中任一项所述的接收机 (1a, 1b), 还包括第二输入模块 (18), 该第二输入模块 (18) 被配置为接收明文的第三分组标识符 (109) 和与第三分组标识符 (109) 相关联的明文的第二内容类型标识符 (110), 并且其中所述处理器 (13a, 13b) 还被配置为:

如果第一比较结果与第二预定条件匹配, 那么比较第一分组标识符 (103) 和第三分组标识符 (109) 以获得第二比较结果; 并且

如果第二比较结果与第三预定条件匹配, 那么基于第二内容类型标识符 (110) 选择第二解码模块 (19), 并将所述解密的净荷 (104) 路由到第二解码模块 (19) 以对所述解密的净荷 (104) 进行解码。

13. 根据权利要求 9-12 中任一项所述的接收机 (1a, 1b), 还包括安全芯片组 (30), 并且其中, 所述解扰器 (11)、所述处理器 (13a, 13b)、所述存储器 (14a, 14b)、所述路由器 (15) 和第一解码模块 (16) 是所述安全芯片组 (30) 的一部分。

14. 一种在根据权利要求 9 的接收机 (1a) 中使用的智能卡 (2a), 包括:

输入模块 (21), 被配置为从接收机 (1a) 接收加密的第二分组标识符 (105) 和加密的第一内容类型标识符 (106);

解密器 (22), 被配置为解密所述加密的第二分组标识符 (105) 以获得第二分组标识符 (107) 并解密所述加密的第一内容类型标识符 (106) 以获得与第二分组标识符 (105) 相关联的第一内容类型标识符 (108); 和

输出模块 (23), 被配置为通过安全连接向所述接收机 (1a) 提供第二分组标识符 (107) 和第一内容类型标识符 (108)。

15. 一种在根据权利要求 10 的接收机 (1b) 中使用的智能卡 (2b), 包括:

硬编码存储器 (24), 包括第二分组标识符 (107) 和与第二分组标识符 (107) 相关联的第一内容类型标识符 (108);

输出模块 (23), 被配置为通过安全连接向所述接收机 (1b) 提供第二分组标识符 (107) 和第一内容类型标识符 (108)。

接收机中数据流的可靠且不可篡改处理

技术领域

[0001] 本发明涉及在可能结合智能卡的接收机中数据流的安全解密和解码。

背景技术

[0002] 在有条件访问 (CA) 系统中的付费电视应用利用加扰 (也称为加密) 来保护数字电视广播流。接收机用于获得相关的解密密钥以在呈现数字电视流之前解扰该流。这样的解密密钥也称为控制字或者 CW。在数字电视台的首端 (head-end) 中, CW 的序列与一个或多个例如音频、视频、字幕、电视文字广播和 / 或小程序 (applet) 的基本流相关联。对于 MPEG2 流, 基本流由 PID (分组标识符) 来识别。通过 CW_stream_Id, CW 的流通常是可识别的。在 MPEG2 标准中, 组成电视服务的 PID 的列表 (MPEG2 术语中的节目流) 包含在明文 PMT (节目映射表) 中。该 CA 系统使用相似的数据结构将 CW_Stream_ID 映射到多个 PID。接收机中的解码器处理 PMT, CA 系统的智能卡处理把 CW_Stream_ID 联系到相关 PID 的信息, 并设置接收机以加载用于解扰基本流的相关密钥。

[0003] 为了防止对明文数字电视流的未授权访问, 在接收机的安全域中, 典型地在安全芯片或芯片组中, 执行数字电视信号的解扰和解码是公知的。

[0004] 在处理 MPEG2 流时, 已知的接收机通常采取以下步骤。接收并解调 MPEG2 分组。从 MPEG2 报头中提取 PID 和加扰控制字段。在接收机的存储器中的 CW 查找表中搜索具有匹配 PID 值的条目, 并且从该表中读取关联的 CW 密钥。加扰控制字段值用于从关联的 CW 密钥中选择需要在解扰器中加载的 CW。使用该 CW 在解扰器中解密 MPEG2 分组的加扰净荷。来自明文 MPEG2 PMT 的信息用于确定分组的 stream_type (流类型)。该 stream_type 是标识内容的类型 (例如音频、视频、字幕、电视文字广播或小程序) 的内容类型标识符。该 stream_type 用于将分组发送到适当的解码模块。

[0005] 对于 MPEG2 流的处理, 接收机通常使用以下输入: 来自 MPEG2 分组报头的 PID 值和加扰控制字段和明文 MPEG2 PMT 信息, 其中具体地为基本流的 PID 和与 PID 相关联的 stream_type。

[0006] 为了确保接收机的预期操作, 所有这些输入数据需要提供准确的信息。因为以明文提供 PMT 和 MPEG2 分组报头, 它们在接收机中处理前可被篡改。这使得攻击者能够改变 PID 值或者 stream_type 值, 例如使得视频和音频基本流看起来像电视文字广播流。通常在接收机的安全域中处理视频流和音频流, 然而, 在解扰后, 在安全域之外处理电视文字广播流。这样篡改输入会使解扰的视频和音频基本流离开安全域, 实现对这些流的未授权访问并且使流的处理不可靠。

发明内容

[0007] 本发明的一个目的是改进数据流的安全处理。

[0008] 根据本发明的一个方面, 提出一种接收机中的用于处理数据流的方法。该数据流包括报头和加密的净荷。该报头包括第一分组标识符。该方法包括解密该加密的净荷以获

得解密的净荷的步骤。该方法还包括接收加密的第二分组标识符和加密的第一内容类型标识符的步骤。该方法还包括在安全环境内从加密的第二分组标识符获得第二分组标识符的步骤。该方法还包括在安全环境内从加密的第一内容类型标识符获得与第二分组标识符相关联的第一内容类型标识符的步骤。该方法还包括比较第一分组标识符和第二标识符以获得第一比较结果的步骤。该方法还包括以下步骤：如果第一比较结果与第一预定条件匹配，则基于第一内容类型标识符选择第一解码模块，并将解密的净荷路由到第一解码模块以对解密的净荷进行解码。

[0009] 根据本发明的一个方面，提出了一种用于处理数据流的接收机。该数据流包括报头和加密的净荷。该报头包括第一分组标识符。该接收机包括解扰器，被配置为解密该加密的净荷以获得解密的净荷。该接收机还包括第一输入模块，被配置为接收加密的第二分组标识符和加密的第一内容类型标识符。该接收机还包括处理器、存储器和路由器。该处理器被配置为从加密的第二分组标识符获得第二分组标识符。该处理器还被配置为从加密的第一内容类型标识符获得与第二分组标识符相关联的第一内容类型标识符。该处理器还被配置为在存储器中存储第二分组标识符和第一内容类型标识符。该处理器还被配置为比较第一分组标识符与存储在存储器中的第二分组标识符以获得第一比较结果。该处理器还被配置为：如果该第一比较结果与第一预定条件匹配，则向路由器提供第一内容类型标识符。该路由器被配置为基于第一内容类型标识符选择第一解码模块。该路由器还被配置为将解密的净荷路由到第一解码模块以对该解密的净荷进行解码。

[0010] 第一预定条件是例如第一分组标识符等于第二分组标识符。

[0011] 因此，把第一内容类型标识符和相关联的第二分组标识符安全地提供给接收机以进行处理，即以加密的从而不可篡改的形式接收。而且，处理解密的净荷依赖于不可篡改的第一内容类型标识符。有利地，这使在接收机中处理前改变内容类型标识符变得相当复杂。

[0012] 权利要求 2 的实施例有利地使得能够将授权控制消息和 / 或授权管理消息用于第一内容类型标识符的安全分配。

[0013] 根据本发明的一个方面，提供一种接收机中的用于处理数据流的方法。该数据流包括报头和加密的净荷。该报头包括第一分组标识符。该方法包括在安全环境内解密加密的净荷以获得解密的净荷的步骤。该方法还包括在安全环境内从硬编码存储器获得第二分组标识符的步骤。该方法还包括从硬编码存储器中获得与第二分组标识符相关联的第一内容类型标识符的步骤。该方法还包括比较第一分组标识符与第二标识符以获得第一比较结果的步骤。该方法还包括如下步骤：如果该第一比较结果与第一预定条件匹配，那么基于第一内容类型标识符选择第一解码模块并将解密的净荷路由到第一解码模块以对该解密的净荷进行解码。

[0014] 根据本发明的一个方面，提供一种用于处理数据流的接收机。该数据流包括报头和加密的净荷。该报头包括第一分组标识符。该接收机包括解扰器，被配置为解密该加密的净荷以获得解密的净荷。该接收机还包括处理器和路由器。该处理器被配置为从硬编码存储器获得第二分组标识符和第一内容类型标识符。该处理器还被配置为比较第一分组标识符与存储在硬编码存储器中的第二分组标识符以获得第一比较结果。该处理器还被配置为：如果第一比较结果与第一预定条件匹配，那么向路由器提供第一内容类型标识符。该路由器被配置为基于第一内容类型标识符选择第一解码模块。该路由器还被配置为将解密的

净荷路由到第一解码模块以对该解密的净荷进行解码。

[0015] 第一预定条件是例如第一分组标识符等于第二分组标识符。

[0016] 因此,将该第一内容类型标识符和相关联的第二分组标识符安全地提供给接收机以进行处理,即从硬编码存储器,由此以不可篡改的形式获得。而且,处理解密的净荷依赖于不可篡改的第一内容类型标识符。这有利地使得在接收机中处理前改变内容类型标识符是不可能的。

[0017] 权利要求 4 的实施例有利地启用接收机内的硬编码存储器。

[0018] 权利要求 5 的实施例有利地启用智能卡内的硬编码存储器。

[0019] 权利要求 6 和 11 的实施例能够有利地限制解码器向预定义接口(例如 HDMI/HDCP 接口、DVI/HDCP 接口、或者 DRM 保护接口)的输出。HDMI、HDCP、DVI 和 DRM 分别是公知的高清多媒体接口、高带宽数字内容保护、数字视频接口和数字版权管理的缩写。

[0020] 权利要求 7 和 12 的实施例对于允许未授权访问的解密的净荷,有利地实现较少的安全处理。第二预定条件是例如第一分组标识符不同于第二分组标识符。第三预定条件是例如第一分组标识符等于第三分组标识符。

[0021] 权利要求 8 的实施例有利地实现 MPEG2 流的安全和不可篡改处理。

[0022] 权利要求 13 的实施例有利地防止在接收机内窃取(tapping)信号。

[0023] 根据本发明的一方面,提供一种在具有一个或多个上述特征的接收机中使用的智能卡。该智能卡包括输入模块,被配置为从接收机接收加密的第二分组标识符和加密的第一内容类型标识符。该智能卡还包括解密器,被配置为解密加密的第二分组标识符以获得第二分组标识符并且解密加密的第一内容类型标识符以获得与第二分组标识符相关联的第一内容类型标识符。该智能卡还包括输出模块,被配置为向接收机提供第二分组标识符和第一内容类型标识符。

[0024] 因此,智能卡能够有利地用于安全地获得第二分组标识符和第一内容类型标识符并安全地将它们提供给接收机。

[0025] 根据本发明的一个方面,提供一种在具有一个或多个上述特征的接收机中使用的智能卡。该智能卡包括硬编码存储器。该硬编码存储器包括第二分组标识符和与第二分组标识符相关联的第一内容类型标识符。该智能卡还包括输出模块,被配置为向接收机提供第二分组标识符和第一内容类型标识符。

[0026] 因此,智能卡能够有利地用于安全地获得第二分组标识符和第一内容类型标识符并安全地将它们提供给接收机。

[0027] 在下文中,将更详细地描述本发明的实施例。然而,应该明白,这些实施例不应被解释为对本发明保护范围的限制。

附图说明

[0028] 将参考附图中示出的示例性实施例更详细地解释本发明的各方面,在附图中:

[0029] 图 1a 示出了本发明的示例性实施例的接收机;

[0030] 图 1b 示出了本发明的示例性实施例的接收机;

[0031] 图 2a 示出了本发明的示例性实施例的智能卡;

[0032] 图 2b 示出了本发明的示例性实施例的智能卡;

- [0033] 图 3 示出了本发明的示例性实施例的接收机和智能卡中的数据流；
- [0034] 图 4a 示出了本发明的示例性实施例的接收机中执行的方法步骤的示意图；
- [0035] 图 4b 示出了本发明的示例性实施例的接收机中执行的方法步骤的示意图；
- [0036] 图 5 示出了本发明的示例性实施例的接收机中执行的方法步骤的示意图。

具体实施方式

[0037] 在 CA 系统中,接收机是接收数据流的设备,从数据流中提取并处理加密的数据分组。该数据流可以作为广播流被接收或者可以源自存储在例如硬盘或者 DVD 盘上的文件。数据分组具有报头和加密的净荷。在接收机中,该加密的净荷被解密和解码以允许在终端用户设备(例如电视、PC 或者音频播放设备)上播放。根据内容的类型,使用特定的解码器。内容的类型是例如音频、视频、字幕、电视文字广播和小程序。一些类型的内容(例如视频流和音频流)由于其价值特点,黑客对其特别有兴趣。

[0038] 数据流是例如符合 ISO 13818-1 标准的 MPEG2 流。MPEG2 流通常包含多个基本流,每个基本流包含具有报头和净荷的数据分组。报头包含分组标识符(PID)。净荷包含属于特定内容类型的内容。根据 MPEG2 标准,PMT 单独地以明文提供给接收机,可能作为净荷内的数据结构。PMT 包含将 PID 联系到称作 stream_type 的内容类型标识符的信息。比较在基本流中接收的 PID 与在 PMT 中接收的 PID,使得可以得到净荷的 stream_type。PMT 为明文的性质使得黑客可以将其篡改。

[0039] 通过安全地向接收机提供输入数据,本发明提供防止这种篡改的保护。除了别的以外,输入数据包括用于可识别净荷的内容类型标识符。输入数据在接收机内使用,在接收机中输入数据被保护以防止篡改。至此,输入数据或者在广播流中被加密,或者代替地在存储器中被硬编码。在使用智能卡来获得输入数据的情况下,可以使用现有技术接收机和智能卡之间安全地交换数据。在接收机内,优选地在安全芯片或安全芯片组内处理净荷和输入数据,确保数据信号不会被窃取。

[0040] 在图 1a 中示出了接收机 1a。通过第一输入模块 12,安全地接收输入数据。接收的输入数据被加密并包含 PID 和与该 PID 相关联的 stream_type。处理器 13a 例如通过在接收机 1a 内解密输入数据或者通过令智能卡解密输入数据,从输入数据获得 PID 和 stream_type。获得的 PID 和 stream_type 存储在存储器 14a 中供以后参考。可以获得多个 PID 和相关联的 stream_type 并存储在存储器 14a 中。可以得到与 stream_type 相关联的 PID 范围,以允许在存储器 14a 中更高效的存储。

[0041] 接收机 1a 还包含用于解密数据分组的加密的净荷的解扰器 11。加密的净荷例如源自 MPEG2 基本流或文件。数据分组具有报头,该报头包含识别净荷的 PID。在解密加密的净荷之后,解密的净荷要由特定的解码器解码。通过比较来自数据分组的报头的 PID 与存储在存储器 14a 中的 PID 来选择解码器。当发现匹配时,从存储器读取相关联的 stream_type 并选择对应的解码器模块 16。stream_type 例如指示要使用的解码器 16,或者 stream_type 允许在表中查找以找到对应的解码器模块 16。可以使用任何其它机制利用 stream_type 找到解码器模块 16。路由器 15 将解密的净荷路由到选择的解码器模块 16,在解码器模块 16 中解密的净荷可被解码。

[0042] 在图 1b 中示出了另选的接收机 1b。在接收机 1b 中,在存储器 14b 中硬编码了 PID

和相关联的 stream_type, 因此不需要通过接收机 1a 中的例如输入模块 12 的输入模块提供。除了通过输入模块 12 安全接收输入数据外, 接收机 1b 以与接收机 1a 相似的方式工作。在图 1b 中, 存储器 14b 在接收机 1b 内部。存储器 14b 可以代替地设置在接收机 1b 可访问的智能卡中。

[0043] 在图 2a 中示出了智能卡 2a, 其可以与如图 1a 中所示的接收机 1a 一起使用以获得 PID 和相关联的 stream_type。输入模块 21 从接收机接收包含加密的 PID 和加密的 stream_type 的加密输入数据。解密器 22 解密该输入数据, 并将由此获得的解密的 PID 和 stream_type 通过输出模块 23 提供给接收机 1a。利用任何公知的智能卡接口技术, 来保护智能卡 2a 和接收机 1a 之间的接口。

[0044] 图 2b 示出了另选的智能卡 2b, 其可以与如图 1b 中所示的接收机 1b 一起使用以获得 PID 和相关联的 stream_type。PID 和相关联的 stream_type 存储在硬编码存储器 24 中, 并通过输出模块 23 提供给接收机 1b。

[0045] 在图 3 中更详细地示出了在本发明的示例性实施例的接收机中如何处理数据。为了简明, 处理器 13a、13b 未示出。数据流用虚线箭头表示。用逗号分隔的附图标记表示替换例。用分号分隔的附图标记表示部件之间的多个数据流。存储器 14a, 14b 或者是硬编码存储器 14b (在此情况下未使用智能卡 2a, 2b), 或者是存储器 14a (在此情况下使用智能卡 2a, 2b) 以从智能卡 2a 中的加密的输入数据获得 PID 和相关联的 stream_type 或者从智能卡 2b 中的硬编码存储器 24 获得 PID 和相关联的 stream_type。

[0046] 在存储器 14a, 14b 中存储了 PID 和相关联的 stream_type。而且, 存储 PID 和相关联的 CW。在接收机中以本身已知的方式接收 CW, 例如在授权控制消息 (ECM) 中接收 CW, 其中在预定义时间帧内两个 CW 关联到一个 PID。这两个 CW 称作奇 CW 和偶 CW, 其使用包含加密的净荷的数据分组报头中的加扰控制字段来选择。如何存储 PID、stream_type 和 CW 的示例在下面的表中示出, 其可以用作信任信息查找表。可以使用任何其它结构来存储这些数据, 只要 stream_type 能够与 PID 相关联并且 CW 能够与 PID 相关联即可。

[0047]

信任信息查找表			
PID	CW_奇	CW_偶	Stream_type
101	CW1	CW2	视频
201-299	CW3	CW4	1
$\{p_{100}\}_{\geq 0}$	CW1	CW2	音频

[0048] 信任信息查找表包含三行数据。在第一行中存储值为“101”的 PID、值为“CW1”的奇 CW、值为“CW2”的偶 CW 以及值为“视频”的 stream_type。因此, CW1 和 CW2 与 PID 101 相关联, PID 101 被关联到 stream_type 视频。在第二行中, PID 范围 201-299 被关联到 CW3、CW4 和 stream_type 1, 其中 stream_type 的值 1 表示例如视频。在第三行中, PID 范围 $\{p_{100}\}_{\geq 0}$, 即 $\{0, 100, 200, \dots\}$, 被关联到 CW1、CW2 和 stream_type 音频。

[0049] 参考图 3, 在下面的示例中, 在 ECM 中接收 PID 和相关联的 CW, 在授权管理消息

(EMM) 中接收 PID 和相关联的 stream_type。通过接收机 1a 的安全域 30 中的第一输入模块 12 接收 ECM 和 EMM, 并通过接收机 1a 和智能卡 2a 之间的安全接口转发到智能卡 2a。在智能卡 2a 中解密加密的奇 CW 112a 和加密的偶 CW 112b, 并通过该安全接口作为解密的奇 CW 113a 和解密的偶 CW 113b 与来自 ECM 的 PID 信息一起被提供给接收机 1a, 在接收机 1a 中它们被存储在存储器 14a 中。加密的 PID 105 和加密的 stream_type 106 也在智能卡 2a 中解密, 并作为解密的 PID 107 和解密的 stream_type 108 被提供给接收机 1a, 在接收机 1a 中它们被存储在存储器 14a 中。当接收到 MPEG2 基本流时, 从基本流的报头 101 中提取数据字段, 并且将基本流的加密的净荷 102 送到解扰器 11 中。从报头提取的数据字段中有: 识别净荷的 PID 103 和识别要使用奇 CW 还是偶 CW 来解密加密的净荷的加扰控制字段 111。

[0050] 在存储器 14a 中查找 PID103 的 CW 113a ;113b, 并基于加扰控制字段 111 的值, 开关 10 向解扰器 11 提供奇 CW 113a 或者偶 CW 113b。解扰器 11 使用提供的奇 CW 113a 或者偶 CW 113b 解密加密的净荷 102。在解密净荷之后, 将 stream_type 108 和解密的净荷 104 一起发送到路由器模块 15。路由器模块 15 使用 stream_type 108 从存储在存储器 14a 中的信任信息查找表中选择用于对解密的净荷 104 进行解码的适当解码器。与现有技术相反, 由此不使用在明文 PMT 中提供的并通过第二输入模块 18 接收的 PID 109 和 stream_type 110 信息。如果 stream_type 为空 (零), 即在存储器 14a 中不可用或者无效, 那么路由器可以被配置为使用来自 PMT 的信息。第二输入模块 18 和第一输入模块 12 可以是同一个输入模块。

[0051] 在安全域 30 中的 stream_type 108 可以包含或者具有用于解码模块 16 的关联的路由信息。这实现了: 例如有价值内容的发送被限制于安全的输出接口 17 (例如 HDMI), 而不是无保护的高质量模拟接口 (例如 SCART 和 S-video)。

[0052] 存在实现加载和提供信任的 stream_type 的多种方式。CA 系统通常提供将 PID 值与由 CW_Stream_ID 参考的 CW 流相关联的机制。这个机制允许几个基本流共享 CW 值。CW_Stream_ID 与 PID 值的关联发生在用于该 CW_Stream_ID 的 CW 序列的发送之前。因此, ECM 至少包含 CW_Stream_ID 和 CW 112a, 112b 的加密版本。CW_Stream_ID 的 PID 列表为附加的信任 stream_type 107 提供了良好的基础。代替单个 PID 值, CW_Stream_ID 关联由 {PID 107, stream_type 108} 对的数组组成。在处理 CW_Stream_ID 关联的列表后, 智能卡 1a 能够使用安全信息加载协议向接收机 1a 的安全域 30 发送信任的 stream_type 108。

[0053] 另选地, 定义特殊数据流, 其包含多个 PID 值 107 的信任 stream_type 108。为了防止对数据的修改, 这个特殊数据流被加密。该特殊数据流在接收机的安全域 30 中的解扰器 (可以是解扰器 11) 中被解密。解析 PID 107 和 stream_type 108 之间的关联并存储在存储器 14a 中以在安全域 30 中使用。

[0054] 另选地, 创建两个单独的 CW 查找表和单独的密钥阶梯 (ladder) 以加载 CW。为了这个目的, 可以使用公知的密钥阶梯模块。一个 CW 查找表包含需要留在安全域 30 内的多个流的信息, 另一个 CW 查找表覆盖允许由安全域 30 之外的解码器 19 解码的基本流。为此目的, 可以使用具有值为 1 或者值为 0 的二元 stream_type。密钥阶梯模块利用嵌入到芯片的一次性可编程存储器结构中的简单密钥层级, 执行安全会话处理以把 CW 113a, 113b 直接加载到芯片的安全域 30 中。

[0055] 可以使用其它另选的方法将 CW 和 stream_type 提供给接收机 1a。

[0056] 图 4a 示出了在本发明示例性实施例的接收机（例如图 1a 中示出的接收机）中执行的方法的步骤。优选地，在接收机 1a 的安全芯片 30 中执行这些步骤。在步骤 1001，把基本流的加密的净荷 102（例如加密的视频净荷）解密成解密的视频 104。在步骤 1002，接收 ECM 或者 EMM，其具有加密的 PID 105 和加密的 stream_type 106。在步骤 1003，解密 PID 105 并存储在存储器 14a 中，在步骤 1004，解密 stream_type 106 并存储在存储器 14a 中。在步骤 1005，将解密的 PID 107 与视频净荷的 PID 103 进行比较。至此，从基本流的报头中提取 PID 103 并与存储在存储器 14a 中的 PID 进行比较。如未发现匹配，则由步骤 1006 指示，那么在步骤 1007，从存储器 14a 中读取与 PID 103（或者 PID 107，在此情况下是相同的）相关联的 stream_type 108 并使用，以选择用于对视频净荷进行解码的视频解码模块 16。在步骤 1008，将解密的视频净荷路由到该视频解码模块 16。

[0057] 图 4b 示出了在本发明示例性实施例的接收机（例如在图 1b 中示出的接收机）中执行的另选方法的步骤。该方法与图 1a 的不同之处在于：不是接收 ECM 或者 EMM 以获得 PID 107 和相关联的 stream_type 108，而是在存储器（例如接收机 1b 的硬编码存储器 14b 或者智能卡 2b 的硬编码存储器 24）中硬编码 PID 107 和 stream_type 109。在步骤 1011，从硬编码存储器 14b 或 24 中读取 PID 107，并在步骤 1012，从硬编码存储器 14b 或者 24 中读取 stream_type。

[0058] 在图 5 中示出了在本发明示例性实施例的接收机（例如图 1a 中示出的接收机）中执行方法的附加可选步骤。除了在图 4a 中示出的步骤之外，在图 5 的示例性实施例中，在步骤 1013 中选择接口 17 以在步骤 1014 中限制解码器 16 的输出。如果在存储器 14a 中没有找到 stream_type，那么接收机 1a 可以被配置为基于在接收机中不安全地接收的输入数据来路由解密的净荷 104，其在这种情况下是例如电视文字广播净荷。例如在 PMT 中接收包含明文 PID 109 和与 PID109 相关联的明文 stream_type 110 的输入数据。在步骤 1015，接收 PMT。在步骤 1016，将来自 PMT 的 PID 109 与电视文字广播净荷 104 的 PID 103 相比较。如果 PID 匹配，则由步骤 1017 指示，那么在步骤 1018 选择接收机的安全域 30 之外的电视文字广播解码模块 19。在步骤 1019，将电视文字广播净荷 104 路由到电视文字广播解码单元 19。

[0059] 如图 5 中所示的附加的可选步骤可以相似地应用于图 4b 的示例。

[0060] 本发明的一个实施例可以被实现为与计算机系统一起使用的程序产品。该程序产品的程序定义实施例的功能（包括在这里描述的方法）并可以包含在各种计算机可读存储介质上。示例性的计算机可读存储介质包括但不限于：(i) 永久存储信息的不可写存储介质（例如，计算机内的只读存储装置，诸如 CD-ROM 驱动器可读的 CD-ROM 盘、闪存、ROM 芯片或者任何类型的固态非易失性半导体存储器）；和 (ii) 存储可更改信息的可写存储介质（例如，磁盘驱动器内的软盘或者硬盘驱动器或者任意类型的固态随机存取半导体存储器）。

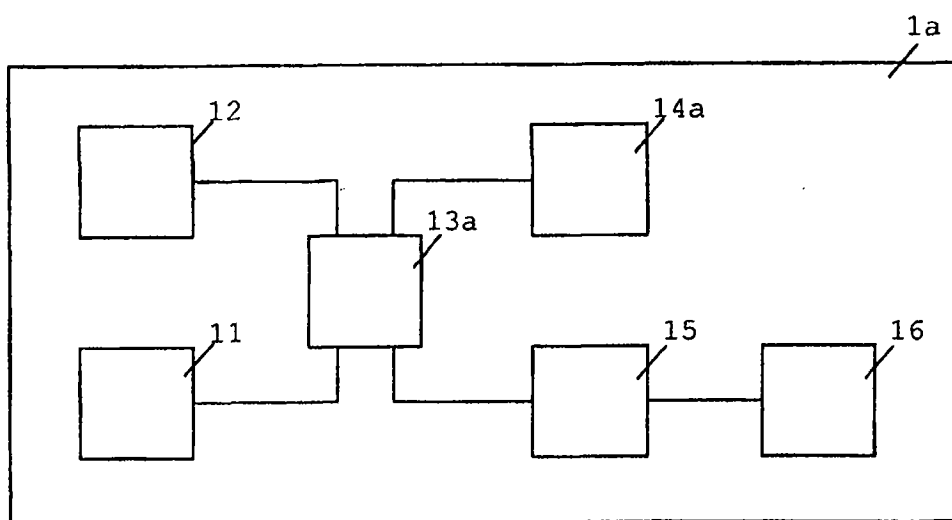


图 1a

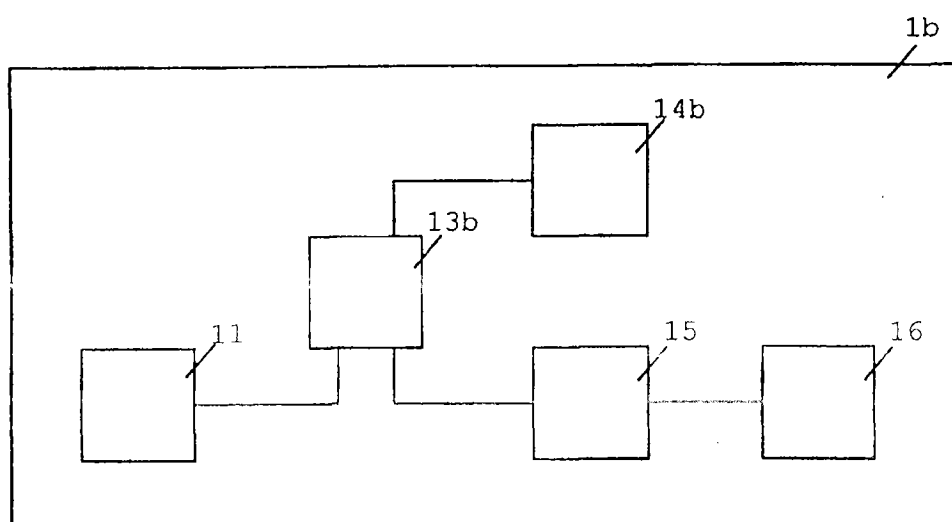


图 1b

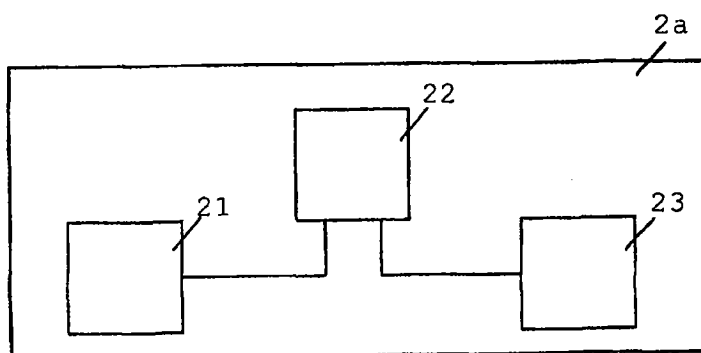


图 2a

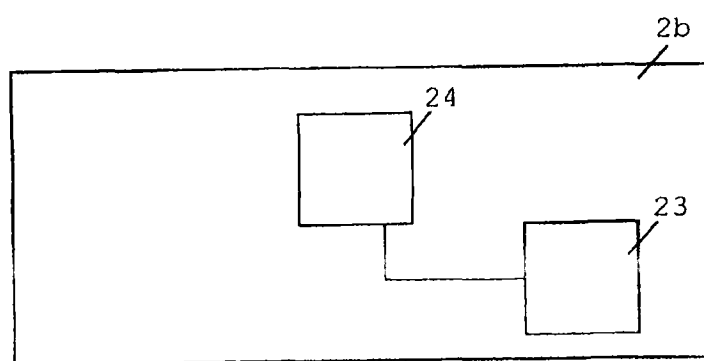


图 2b

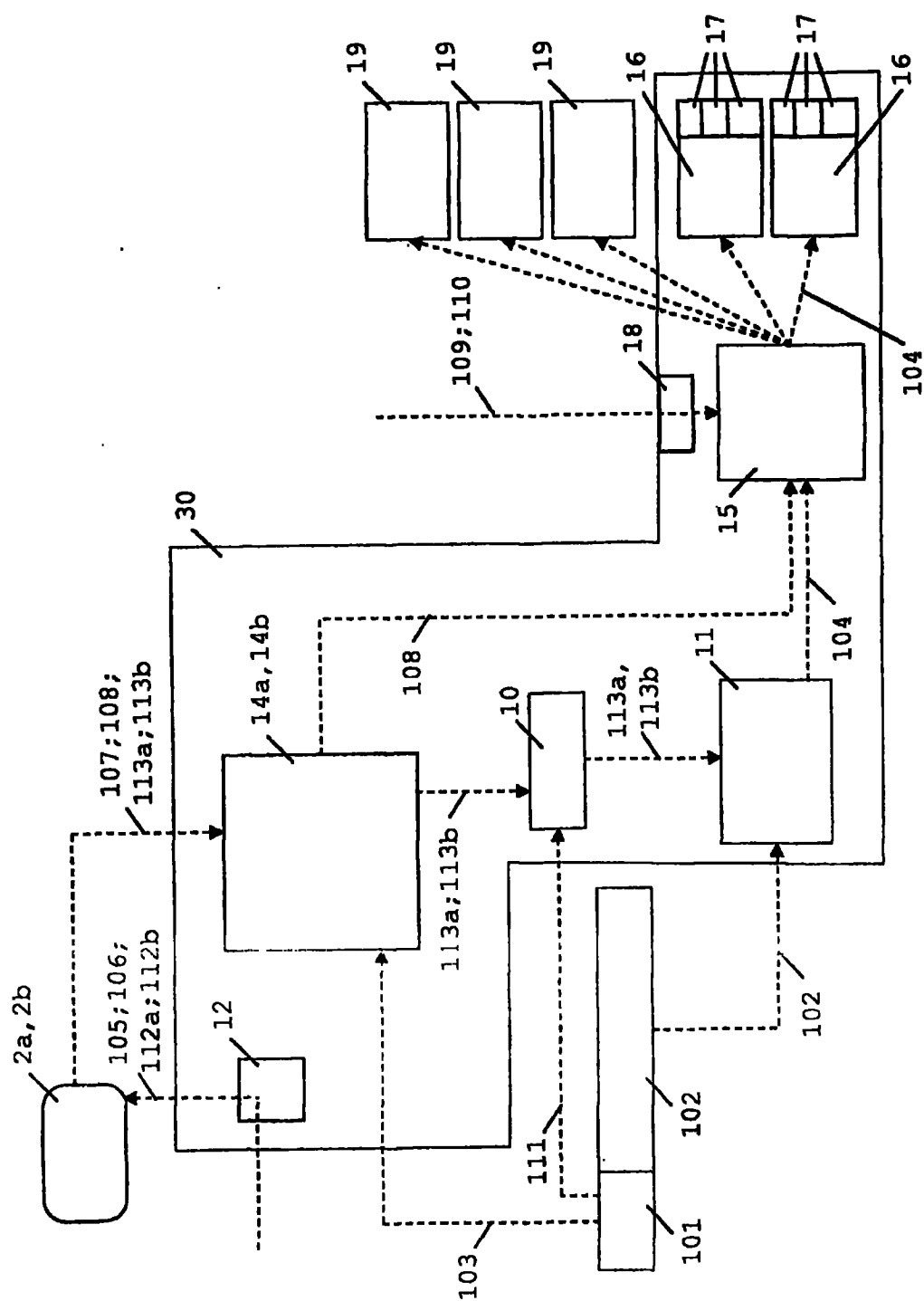


图 3

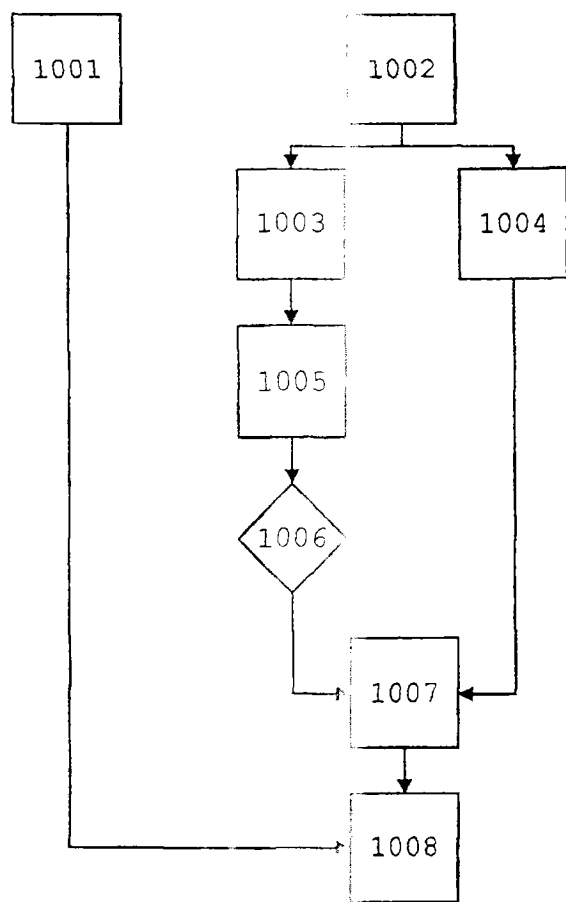


图 4a

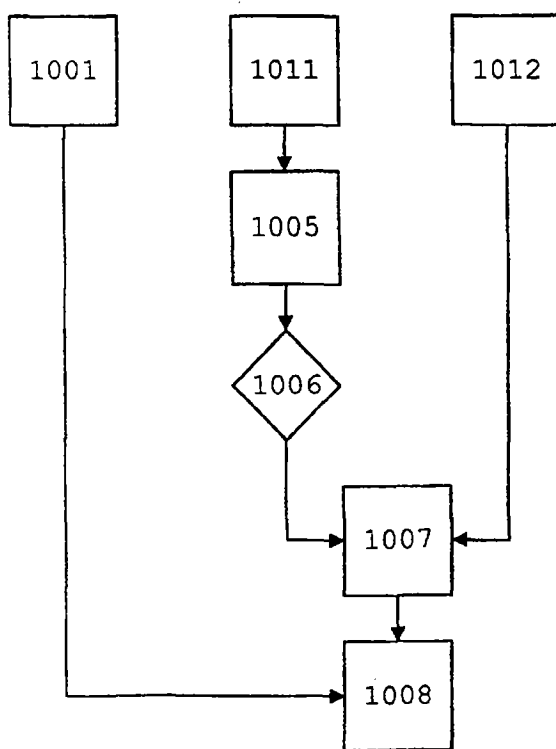


图 4b

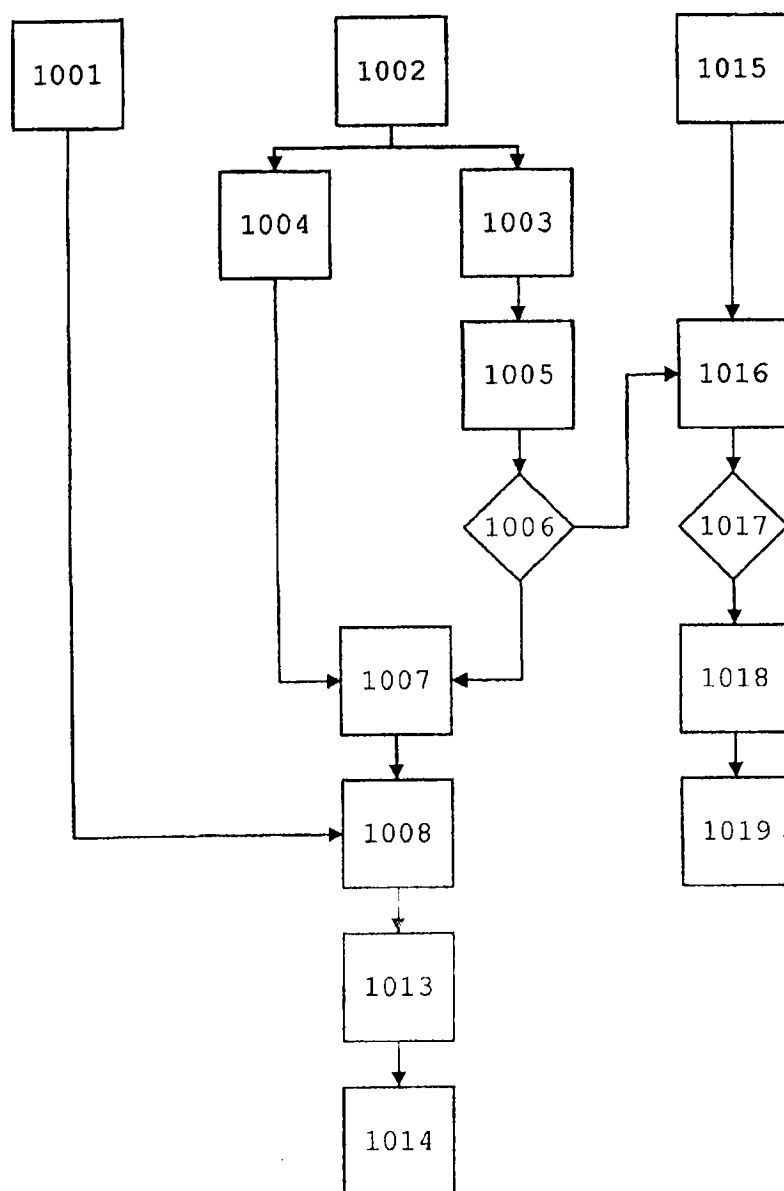


图 5