

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200580031887. X

[51] Int. Cl.

G06F 1/00 (2006.01)
G06K 19/07 (2006.01)
G11B 23/30 (2006.01)
G11B 33/04 (2006.01)

[43] 公开日 2007 年 8 月 22 日

[11] 公开号 CN 101023402A

[22] 申请日 2005.9.8

[21] 申请号 200580031887. X

[30] 优先权

[32] 2004. 9. 21 [33] EP [31] 04022374. 5

[86] 国际申请 PCT/EP2005/054435 2005.9.8

[87] 国际公布 WO2006/032613 英 2006.3.30

[85] 进入国家阶段日期 2007.3.21

[71] 申请人 汤姆森许可贸易公司

地址 法国布洛涅-比郎库尔

[72] 发明人 迪尔克·冈多尔夫 安德烈·谢温措
马尔科·温特

[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 罗松梅

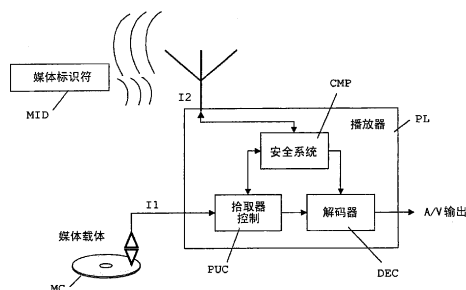
权利要求书 3 页 说明书 13 页 附图 4 页

[54] 发明名称

用于访问受保护数据的方法和装置

[57] 摘要

内容受保护的多媒体数据(例如,商业上可用的视频 DVD)的消费者希望获得这些数据的备份副本,并希望在任意适合的重放设备上自由地播放这些数据,而内容提供商希望保护这些数据不被私自复制。所公开的用于访问来自第一存储介质(MC)(例如,CD)的应用数据的方法使用电子密钥对这些应用数据进行解码或转换。把一个或多个内容标识符附加到应用数据或第一存储介质(MC)。把密钥存储在防止复制的单独的第二存储介质(例如,RFID 标签)上,并把该密钥与内容标识符进行比较。仅当第二存储介质(MID)可用时,才能够进行应用数据的重放或格式转换。由于一次只能使用一个副本,所以这允许对应用数据进行复制、分发或格式转换,而同时保留了数据的内容权力。



1. 一种用于访问从第一存储介质（MC）中检索到的第一数据的方法，包括步骤：

- 通过第一接口（I1）从第一存储介质（MC）中检索第一数据，所述第一数据包含第一内容标识数据和第一应用数据，其中，所述第一应用数据包含AV内容的不同版本或质量等级；

- 通过第二接口（I2）向可拆卸无源设备供电，所述设备包含第二存储介质（MID）；

- 通过所述第二接口（I2）从所述可拆卸设备上的所述第二存储介质（MID）接收第一密钥标识数据；

- 对通过所述第二接口（I2）接收到的所述第一密钥标识数据与通过所述第一接口（I1）检索到的所述第一内容标识数据进行比较（CMP）；

- 基于所述比较，确定所述AV内容的版本或质量等级，其中，所述AV内容具有根据预定规则而与所述第一密钥标识数据相匹配的第一内容标识数据；以及

- 对所述AV内容的所确定的版本或质量等级启用进一步的处理（DEC）。

2. 根据权利要求1所述的方法，其中，对AV内容的所确定的版本或质量等级的进一步处理（DEC）包括：根据所述第一内容标识数据选择解码过程，其中，所述解码过程使用从所述第一内容标识数据中提取的数据作为操作值或参数。

3. 根据权利要求1或2所述的方法，其中，所述进一步处理（DEC）包括：对所述第一应用数据中AV内容的所确定的版本或质量等级的数据进行重新编码，所述方法还包括步骤：

- 把所述第一内容标识数据或第一密钥标识数据附加到所述第一应用数据中重新编码后的部分；以及

- 把所述第一应用数据中重新编码后的部分与附加的标识数据一

同提供给用于存储或呈现的接口。

4. 根据权利要求3所述的方法，其中，所述第一应用数据被加密，以及通过所述第二接口（I2）所接收的所述第一密钥标识数据还包含加密密钥和解密密钥，这两个密钥是相同的，所述方法还包括步骤：

- 从所述第一密钥标识数据中提取加密密钥；以及
- 对所述第一应用数据进行加密或重新编码，并附加所述标识数据，其中，将所提取的加密密钥用于加密或重新编码，以及能够使用解密密钥对所产生的数据进行解密。

5. 根据上述权利要求中任意一项所述的方法，还包括步骤：

- 存储所述第一密钥标识数据，并为对内容标识数据和密钥标识数据进行比较这一步骤检索所存储的密钥标识数据；以及
- 经过预定时间后，删除所存储的密钥标识数据。

6. 根据上述权利要求中任意一项所述的方法，其中，所述第一密钥标识数据包含多个不同的密钥标识符值，以及在确定AV内容的版本或质量等级的步骤中，确定AV内容的版本或质量等级具有与包含在所述第一密钥标识数据中的密钥标识符值中的任意一个相匹配的第一内容标识数据。

7. 一种用于访问从第一存储介质（MC）中检索到的第一数据的装置，所述装置包括：

- 第一接口（I1）和接收装置（PUC），用于从第一存储介质（MC）中检索第一数据，所述第一数据包含第一内容标识数据和第一应用数据，其中，所述第一应用数据包含AV内容的不同版本或质量等级；
- 装置，用于从所述第一内容标识数据中提取第一内容标识符值；
- 第二接口（I2）和接收装置，用于向包含第二存储介质（MID）的无源设备供电，并用于从所述设备上的所述第二存储介质（MID）接收第一密钥标识数据；
- 装置，用于从所述第一密钥标识数据中提取第一密钥标识符值；
- 比较装置（CMP），用于对所述第一密钥标识符值与通过所述第一接口（I1）检索到的AV内容的不同版本或质量等级的第一内容标识符值进行比较；

- 检测装置 (CMP), 用于基于所述比较, 来检测所述AV内容的版本或质量等级, 其中, 所述AV内容具有根据预定规则而与所述第一密钥标识符值相匹配的第一内容标识符值; 以及

- 装置 (DEC), 用于进一步处理所述AV内容, 其中, 针对AV内容的所检测到的版本或质量等级, 所述检测装置 (CMP) 启用所述用于进一步处理的装置质量。

8. 根据权利要求7所述的装置, 其中, 用于对AV内容的所检测到的版本或质量等级做进一步处理的装置 (DEC) 具有选择装置, 所述选择装置根据所述第一内容标识数据来选择解码过程, 以及所述用于进一步处理的装置 (DEC) 使用从所述第一内容标识数据中提取的数据作为操作值或参数。

9. 根据上述权利要求中任意一项所述的方法或装置, 其中, 所述第一应用数据被加密, 所述第一密钥标识数据还包含解密密钥, 以及从所述第一密钥标识符值中提取出所述解密密钥, 并将所述解密密钥用于对所述第一应用数据进行解密。

10. 根据上述权利要求中任意一项所述的方法或装置, 其中, AV内容的不同版本或质量等级具有不同的第一内容标识数据。

11. 根据上述权利要求中任意一项所述的方法或装置, 其中, 所述第二存储介质 (MID) 是只读介质并通过无线接口来访问。

12. 根据上述权利要求中任意一项所述的方法或装置, 其中, 所述第一存储介质 (MC) 和第二存储介质 (MID) 彼此不相连。

13. 根据上述权利要求中任意一项所述的方法或装置, 其中, 通过所述第二接口 (I2) 把加密密钥提供给可拆卸的无源设备 (MC), 以及使用所述加密密钥对所接收的第一密钥标识数据进行加密。

14. 一种媒体封套或罩, 结合了或附加了无源、无线只读存储设备, 所述存储设备上保存标识符值, 其中, 所述标识符值表示用于启用对存储在与所述媒体封套或罩相对应的介质上的内容进行重放的密钥。

用于访问受保护数据的方法和装置

技术领域

本发明涉及用于访问受保护数据的方法和装置。具体地，本发明涉及用于访问从存储介质检索到的版权受保护的数据的方法和装置。

背景技术

商业上可用的多媒体数据受到版权的保护。所有者、音乐和视频产业以及艺术家对防止像CD、DVD、蓝光盘的媒体和像快闪芯片等的其它媒体载体被私自复制特别感兴趣。借助于通常禁止复制的技术手段来防止复制媒体的严格方式受到了消费者的严厉批评，这是由于一些播放设备可能不能够读取这种受保护的盘。消费者继而提出的另一个问题是：不能够创建备份副本以供个人使用。

因此，需要这样一种解决方案，即允许消费者为了个人目的而对例如DVD进行复制，但同时保留内容所有者的版权。

一种已知的解决方案是“突发切断区”，它是一种能够被拾取器（pickup）读取并被写入DVD-ROM盘的特定扇区的条形码。在盘的生产过程中，在单独的处理步骤中为每一个盘独立地完成突发切断区的写入。然而，这个处理步骤增加了生产成本并不允许消费者获得盘的副本，即使为了私人目的也不行。

存在针对可写媒体载体的另一种解决方案，其中，所述可写媒体载体是完全可写或部分可写的。这些可写媒体载体能够保存反映允许消费者进行复制的数目的“计数器”字段。无论何时产生副本，都可以对“计数器”字段的值进行读取、递减和重写。如果这个值达到0，则拒绝更多的复制过程。计数器字段为0意味着已经消耗了所有允许的副本。然而这种解决方案不能用于只读媒体，这是由于它需要媒体载体自身上的可写区域，例如DVD-R/DVD-ROM的组合。此外，所使用的

播放器必须能够通过向这个区域执行写入来改变计数器字段。

另一种解决方案是一种特定的播放器，它具有所存储的本地“计数”值，因而可以限制副本数目。然而，由于它仅适用于特定播放器产生的副本，因此是非常不安全的。

用于内容保护的其它已知方法采用用户专有密钥，这意味着提供商要付出额外的管理努力来维持其顾客的独立密钥，或甚至是设备专有密钥。此外，顾客可能希望根据个人意愿而出售、借出或作为礼品而赠送例如DVD或蓝光盘，这在内容仅能够由用户专有密钥进行访问时是不可能做到的。

发明内容

本发明解决了允许对来自数据存储介质的数据进行复制的上述问题，同时保留了数据的内容权力。因此，本发明防止了对数据（例如像音频、视频的多媒体数据、或程序数据）的未授权使用。具体地，本发明公开了一种使用电子密钥来保护数据的方法，其中，可以容易地复制数据，但是难以复制密钥。此外，本发明解决了允许在不同设备上重放版权受保护的内容的问题。

本发明使用存储在与“媒体载体”相关联、但与其分离的标签上的“媒体标识符”，即把要保护的数据与相应的标识符存储在分离的不同存储媒体上。媒体标识符至少是难以使用商业上可用的设备进行复制，或完全不能进行复制。媒体标识符标签优选地为无源设备。

一种能够对媒体载体的内容进行解码（例如，用于重放）的设备仅当媒体标识符与该设备相连时才允许对数据进行解码。在对来自媒体载体的数据进行解码之前或同时，所述设备必须读取媒体标识符。当媒体标识符可用时，所述设备还可以对来自媒体载体副本的数据内容进行重放。因此，内容的使用变得与物理上的媒体载体无关，并且保护了实际内容的使用而不是物理的数据。

只要用户提供了属于媒体载体的媒体标识符，便可以允许用户制作任意数目的副本并在任意希望的地方使用副本。为了防止对媒体标识符进行复制，把媒体标识符存储在另一种类型的存储介质上而不是

存储在消费者感兴趣的实际数据中。

媒体标识符是例如存储在专用存储设备（例如，智能卡、印刷电路（PEC）或射频标识（RFID）标签）上的码字或解密密钥。优选地，可以使用任意类型的无源存储设备，即没有供电设备但通过组合功率和通信接口从播放器或解码器接收自身操作功率的设备，因而具有无限的使用时间。此外，普通用户难以复制这种设备，而另一方面它们的工业生产成本较低。RFID标签的特定优点是：相应的阅读器不会受到磨损且能够容易地被集成到消费者的电子设备中，由于这些阅读器仅要求RFID标签处于附近的接收范围（例如1米）内的某处而不像专用驱动器那样处于特定位置，所以它们易于操控。

在优选实施例中，对媒体载体上的（例如版权受保护的）数据进行加密，以及媒体标识符标签还包含相应的解密密钥。可以使用标识符对像单段内容（例如，歌曲或视频场景）的数据部分或甚至是编码后的块（例如，如在MPEG中使用的视频编码所使用的帧或图像组（GOP））进行标记，因而要求相应的媒体标识符对于解码是可用的。在一个实施例中，所有的数据部分使用相同的标识符值。在另一个实施例中，数据部分可以使用不同的标识符值。这些标识符值可以从相同的标识符标签中检索到，或可以例如根据可从单一标识符标签中检索到的一个或多个起始值而计算得到。当根据初始标识符值计算得到标识符值时，所需的计算可能取决于也是从媒体标识符中检索到的参数或操作值。例如，可以基于两个初始标识符J1和J2来计算连续GOP的标识符J的序列，例如在简单情况下为 $J_n = J_1 + n * J_2$ 。这防止了使用简单的分析而检测作为盘上最常使用的代码序列的标识符值。

在另一个实施例中，作为整体的数据部分或媒体载体（例如盘）包含标识代码或单独的标识代码，这些代码由拾取器读取并与从媒体识别设备（例如，RFID标签）接收到的一个或多个标识代码进行比较。在当前从盘中检索到的数据部分的标识符具有从媒体标识设备接收到的匹配标识符时，可以启动解码。否则阻止或干扰解码。

本发明更具一般性的观点是定义物理上的“有用资源”和“有用资源标识符”对。这个模型使版权受保护的内容甚至与其呈现形式无关。

在本申请中，术语“媒体载体”用于保持版权受保护数据的存储介质，而术语“有用资源”可以用于这些数据。此外，术语“媒体标识符”和“有用资源标识符”可互换地用于对所述版权受保护数据进行解码所需的数据集和存储在“媒体标识符标签”或“有用资源标识符标签”上的数据集。

为了使这一点更加清楚，考虑如下示例。思考在逻辑上与电影“Finding Nemo”有关的标识符，该标识符存储在DVD盘上。就是说，可以把标识符一次或多次地存储在盘的入口区或视听（AV）数据中。消费者购买具有电影和在物理上分离的标识符的DVD，例如，把标识符存储在RFID标签中。与RFID阅读器相连或包含RFID阅读器、因而能够通过存储在RFID标签上的标识符而对DVD进行解码的DVD播放器或类似的设备可以从DVD中播放电影，或把电影从存储在DVD上的格式（例如6Mbit/s MPEG2）转换为像700kbit/s DIVX5.1的另一种格式，用于在移动设备上进行重放。然而，代码转换器包括与原始版本相同的标识符，从而移动设备也需要访问相同的RFID标签以便对转换后的电影进行解码。此外，如果没有对内容进行加密，则任意的传统设备都可以产生包括标识符的传统DVD副本，但由于传统设备不能访问媒体标识符，所以传统设备也不能对电影进行重放。这允许了消费者自由地使用内容，但禁止了非法流通。

有利地，所有者能够通过复制媒体而多次复制内容，而不会降低对内容进行解码的能力，而内容生产者和/或作者能够确定内容没有被非法复制和流通。

当消费者使用传统的复制过程时，副本仍旧受到内容提供商的控制。由于仅有一个媒体标识符可用，所以一次只能使用副本之一。本发明还包括有用资源格式转换，使复制保护保持对转换为另一格式的副本有效。

作为特定优点，用户不会受到复制保护所要求的任何特定过程的干扰。相反，用户仅需要操控有用资源标识符，而这一点在使用例如RFID标签时是非常舒适的。在这种情况下，用户需要把RFID标签保持在播放器设备周围对于RFID常见的特定范围内，例如20cm或2m。

一种用于提供媒体标识符的非常舒适的方式是把标识符附加到媒体封套上，即装有出售的原始存储介质的包装。

根据本发明，一种用于对从第一存储介质（MC）检索到的第一数据进行访问的装置可以是例如盘播放器或个人计算机（PC）的一部分，包括：

第一接口和接收装置，用于从第一存储介质中检索第一数据，例如来自光盘（CD）、硬盘驱动器（HDD）、记忆棒等的视听数据，第一数据包含第一内容标识数据和第一应用数据；

用于从第一内容标识数据中提取第一内容标识符值的装置，例如微处理器；

第二接口和接收装置，用于向包含第二存储介质的无源设备供电，并用于从所述设备上的第二存储介质接收第一密钥标识数据，例如通过空中接口从RFID标签接收码字；

用于从所述第一密钥标识数据中提取第一密钥标识符值的装置，例如微处理器或多路分解器；

比较装置，例如微处理器或比较器，用于对提取出的第一内容标识符值与第一密钥标识符值进行比较，并用于在两个值相同的情况下产生指示信号；以及

处理装置，例如微处理器或解码器，用于对从第一存储介质接收到的第一应用数据进行处理，其中，在产生所述指示信号时启用处理装置，否则禁用处理装置。

此外，如果第一应用数据被加密且第一密钥标识数据还包含解密密钥，则用于提取第一密钥标识符值的装置还可以提取解密密钥，并把解密密钥提供给用于对第一应用数据进行解密或解码的处理装置。

此外，根据本发明的装置还可以包括：

用于存储第一密钥标识符值的装置，例如存储器，其中，在检索后，比较装置把所存储的密钥标识符值与第一内容标识符值进行比较；

用于测量时间并指示存储了第一密钥标识符值后经过了预定时间的装置，例如，具有零检测器的可加载的下载计数器；以及

用于删除的装置，在存储了第一密钥标识符值后经过了预定时间

的所述指示之后，所述装置删除所存储的密钥标识符值。例如，微处理器可以明确地删除所存储的值，或使用从第二存储介质最新接收到的值来重写所存储的值，以确保第二存储介质仍可访问。

从属权利要求、下文描述和附图中公开了本发明的有利实施例。

附图说明

参考附图对本发明的典型实施例进行描述，其中：

图1是媒体载体封套中的媒体标识符的集成；

图2是能够访问媒体载体和媒体标识符的播放器的结构；

图3是本发明方法的流程图，用于使用从RFID标签接收到的标识符来启用解码器；

图4是访问媒体载体和媒体标识符、并具有用于集成的移动播放器的重新编码器的播放器的结构；

图5是适配器盒中的分离的解码器，用于从传统的播放器中读取编码的AV数据并从媒体标识符中读取标识数据；以及

图6是能够由从授权盒接收到的标识符来启用的播放器中的解码器。

具体实施方式

图1给出的示例示出了怎样把媒体标识符MID集成到媒体载体MC的盒或封套MJ中。根据本发明，保存有用资源（例如，像电影或音乐的视听数据）的媒体载体MC与媒体标识MID在物理上是分离的，其中，媒体标识MID是使用或消耗所标识的有用资源的权力密钥。换句话说，在读取来自第二存储设备MID的第二数据对象时，存储在第一存储设备MC上的第一数据对象可能仅被解码、解密或转换代码。可以把第二存储设备MID在物理上附加到第一存储设备MC或其外壳MJ上。图1示出了优选实施例，例如，媒体标识符MID是附加到相应DVD的封套MJ上的无源射频标识（RFID）标签。由于消费者经常把至少是当前所读取的盘保留在播放器旁，因此这一点尤其有利。媒体标识符MID也可以是放置在媒体封套中的独立项目，从而当读取盘时，能够把媒

体标识符MID从播放器取出并放置在播放器附近。然后，消费者可以从播放器中取走封套，例如用于取出目录单。

在本发明的一个实施例中，媒体标识符MID包含解密密钥或解密密钥的一部分，用于媒体载体MC上的加密数据。使用有用资源/有用资源标识符对的设备可以实现为解码盒，它可以位于播放器、具有显示器的移动设备、PC、网络服务器、机顶盒等的内部。解码盒检查与其相连的有用资源标识符，并且在标识符允许适当权力的情况下开始对有用资源进行解码。否则，优选地，拒绝对有用资源的访问，或至少强力地限制为不可接受的低质量。

媒体标识符或有用资源标识符也可以是使用专用墨水的印刷电路(PEC)，例如由施乐(Xerox)公司开发的墨水。该印刷电路与RFID标签一样具有较低的生产成本并易于集成到盘封套中，而且由于不常用作可写介质而使一般消费者难以复制。这种媒体标识符可以是商店的存货，或者在顾客购买媒体载体时产生。

作为把有用资源标识符与媒体载体分离的优点，可以按照传统方式来生产媒体载体。省略了针对媒体载体的任意分离的处理步骤，例如在DVD-ROM上写入突发切断区。

在使用如RFID的空中接口的情况下，用户甚至不需要使媒体标识符对于解码器盒已知。如图2所示，例如播放器中的解码器盒通过发送射频(RF)信号而自发地检查媒体标识符的可用性，因而向RFID标签供电，并从RFID标签中读取RF应答信号。应答信号所包含的代码能够用于与从盘中读取的标识代码进行比较，从而在两个代码匹配的情况下能够启用解码器，或是在不匹配的情况下禁用解码器；或者，应答信号所包含的代码用作解码器使用的实际解密密钥。在接收范围内存在多于一个的RFID标签时，公知的技术可以用于挑选单个RFID标签并与该标签进行通信。根据本发明的解码设备还可以提供一个专用的位置，其中，必须把当前使用的有用资源标识符放置在该位置，例如驱动器、隔间等。

如果内嵌在媒体载体封套中的媒体标识符是分离地可拆卸的，则这允许所有者把该标识符与原始盘的副本一同携带，这有利于安全性

(即,保护了原始盘),或有利于重新设置或转换目的。用户还可以将具有附加的媒体标识符的原始媒体载体的封套用于复制的盘。

媒体载体上的数据具有逻辑层,该逻辑层与媒体载体周围的媒体标识符相关联,以对内容进行锁定或加密。所述逻辑层可以覆盖全部的媒体,或是媒体上分离的单独部分,例如,CD上单首歌曲或DVD上的单个视频剪辑。还能够通过有用资源周围额外的加密层而禁止解码。解码时需要有用资源标识符。

在一个实施例中,能够在不需要媒体标识符的情况下,以强烈降低的质量对媒体载体的内容进行解码,但是完整质量的解码需要媒体标识符。

本发明的另一方面是允许对有用资源进行重新设置和转换。用户可能希望在他的家中把所有的音频CD存储在单个服务器上。另一方面,只要保证不会发生不受控制的流通,内容创造者可能会容忍这一行为。然而,通过使用媒体标识符(例如,位于服务器附近的RFID标签),可以确保这个条件。

当不能获得媒体标识符时(例如,音频CD的合法或非法副本在汽车的CD播放器中使用时),禁止进行解码。如果该副本是合法的,则用户具有各自的媒体标识符,并需要使汽车的播放器能够访问这些标识符。例如,如果用户在口袋中具有RFID标识符,则该标识符可能处于播放器的检测范围内。然而此时,由于用户的家人不具有标识符标签,所以他们可能不能在家中播放原始CD。这一点对于所有其它的副本都一样。因此,内容提供者能够确定不会发生不受控制的流通。

图3示出了本发明方法的流程图,用于使用从RFID标签接收到的标识符来启用解码器。在第一步骤S1处,从盘中读取数据。在下一个步骤S2处,对所读取的数据进行分析,检测并提取有用资源的ID值。这个ID值优选地被包括在应用数据中,例如,在专用分组中,从而不能把标识符数据与要保护的应用数据分离。这个ID值也可以被包括在盘的引导部分中,从而在把盘插入播放器后,能够容易地找到这个ID值。在下一个步骤S3处,播放器通过专用接口向无源只读存储设备供电,例如,产生电磁场以启用RFID标签或激活智能卡。依据存储设备

的类型,播放器可能需要在独立的步骤S3a处从设备(例如,从智能卡)进行请求,而其它设备在启用时初次发送数据。在步骤S4处从存储设备接收到应答消息,并且在步骤S5处提取出ID值。如果多于一个的存储设备同时做出应答,则通常存在用于在单独的应答消息之间进行区分的已知机制,例如在单独的、统计上修改的延迟后出现的RFID标签应答。在这种情况下,先前的步骤S4、S5被执行若干次。在已经从当前的应答消息中提取出ID值后,把这个ID值与先前步骤S2从盘中读取的ID值进行比较。如果两者相同,或更普遍地,两者根据预定规则而匹配,则在步骤S7处启用解码器,例如,MPEG视频解码器或附加的解扰器。否则,对下一个应答消息进行分析。如果对所有的应答消息进行了分析且没有接收到与盘ID值匹配的值,则在步骤S6处对解码器保持禁用状态。

在本发明的一个实施例中,之后重复上述过程,同时对应用数据进行解码或呈现。例如,在步骤S7处启用解码器后几秒钟时,在步骤S3处再次启用保存媒体标识符的存储设备,并且需要再次发送标识符值。

在本发明的一个实施例中,当可以访问媒体标识符时,能够对有用资源的格式进行转换。图4示出了相应的装置。可以对来自盘的数据(例如DVD视频)进行转换以便存储,并由移动设备(例如,THOMSON Lyra便携式播放器)进行重放。为此,拾取器PU从媒体载体MC中读取数据,控制单元检测这些数据中包括标识符数据,并请求安全系统单元SEC检查这些标识符数据。安全系统单元检查是否可以访问媒体标识符,例如,RFID标签是否处于检测范围中。然后,安全系统按照上文所述的方法从媒体标识符MID中检索媒体标识符值,并把接收到的值与来自盘的标识符数据进行比较。如果它们相等,则安全系统块SEC启用解码器块,该解码器块可以现在就开始对数据进行解码。

同时,安全块SEC启用编码器块EN,编码器块EN可以从解码器块接收输入数据,或是直接从拾取器接收输入数据,这取决于转换的类型。编码器块现在开始对所检索到的数据(除了保持不变的标识符之

外) 进行重新编码。在输出重新编码后的数据之前, 编码器再次添加标识符值, 例如, 作为附加层或附加分组, 从而在媒体标识符不可用的情况下, 也不能够对副本进行解码。当把所复制的数据存储在移动设备上时, 希望收听或观看这些数据的用户需要随身携带媒体标识符标签。

所述转换可能会影响比特速率和编码格式。例如, 可以把PCM编码的音频转换为mp3Pro, 或者把以6Mbit/s的MPEG-2编码的视频转换为以400kbit/s的AVI编码的视频。转换产品仅能够通过有用资源标识符来解码。因此, 避免了不受控制的流通和格式的改变。有用资源标识符也可以规定转换的细节方面。例如, 可以允许单独地对音频CD中的单个音轨进行复制, 但是禁止切除单一音轨的一部分; 或允许把DVD电影的一个章节分开, 但是不能仅把该章节的音频轨道分开。

本发明的另一个实施例是一种适配器机顶盒, 它允许受有用资源标识符保护的有用资源与未集成有保护模型的播放器一起使用。这可以通过如图5所示的在解码之后进行级联的进一步转换来实现。解码被分为两个部分, 并且在两个分离的设备或仪器内执行。第一仪器是标准的、符合当前技术水平的解码器, 它不需要知晓或处理有用资源标识符。第一仪器的输出可以是数字的或模拟的。第二仪器是例如执行有用资源标识适配的机顶盒。它可以具有数字或模拟输入接口, 这取决于与其一同工作的播放器的类型。如果输入接口是模拟的, 则可能需要进行将数据转换(ADC)至数字格式。

这两个仪器可以按照如下方式一同工作: 媒体载体上的内容(例如, 任意类型光盘)具有包封加密, 即, 上文所述的附加的逻辑层。然而传统的解码器将会忽略这个层, 但解码结果的质量会令人烦恼地被扰乱。例如, 由于行扰动或块扰动、或是整个图像的快速抖动而使视频变得不可接受。仅有第二仪器可能实现正确的解扰。这一点通过以下方式实现: 从媒体标识符(例如RFID标签)中读取媒体标识值, 并读取内嵌在来自播放器的数据中的另一个标识符。在模拟信号的情况下, 数据可以内嵌在例如图文电视广播行中, 或是内嵌在非常高或非常低的模拟音频信号中; 在数字信号的情况下, 数据可以是流内的

某些专用分组、或是信令目的的水印。通过这两种信息类型，可以对有用资源与有用资源标识符的匹配进行检查，并且能够执行或拒绝解扰。

本发明方法允许灵活的应用模型。例如，如果伴随着有用资源而提供了多于一个的有用资源标识符（RFID、PEC等），则这允许同时消耗多于一个的副本，例如，一个在客厅一个在车中，或允许使用不同类型的重放设备，即，支持RFID或支持PEC的设备。

此外，为了使已经分发的有用资源对于用户可用，可以单独地出售有用资源标识符。为了广告的目的，可以在不访问媒体标识符的情况下，对媒体载体中的部分内容（例如，CD上的一首歌曲）进行解码。

当本发明方法用于个人计算机（PC）中的内置驱动器时，优选地，可以由内置驱动器自身来检查有用资源标识符。这个过程不需要入和/或出PC的ID承载业务，因而更为安全，这是由于破解标识符代码变得更为困难。

然而如图6所示，可以使用仅用于启用播放器中的解码器的独立的设备（例如，PC 插槽卡），尽管这较不安全。播放器PL中的第一解码器DEC1对所有检索到的数据执行同样的工作，而第二解码器DEC2可以在两个不同的模式下操作。第二解码器DEC2在第一模式下根据第一算法工作，而在第二模式下根据第二算法工作。根据第二算法，可以对受内容保护的数据额外地或不同地进行加扰或加密，而根据第一算法对其它数据进行编码。仅可能由设备STB通过接口IF来将解码器切换到第二模式。设备STB通过接口IF读取第一标识数据，从例如PEC中读取第二标识数据，并把这两个数据进行比较，当它们匹配时，设备STB通过接口IF提供启用信号，该信号用于把第二解码器DEC2切换到第二模式。

此外，下列实施例会是有利的。

在一个实施例中，不同的媒体标识符标签以不同的方式控制重放，例如一个标签用于父母观看，一个标签用于儿童观看。

在一个实施例中，媒体标识符标签包含特定的国家代码，这个代码必须与播放器的国家代码匹配才能进行解码。

在一个实施例中，针对不同的内容质量而设置了不同等级的媒体标识符标签，例如，一个标签用于标准清晰度（SD）视频，而另一个标签用于高清晰度（HD）视频。

在另一实施例中，有用资源可以被视为容器或数据库，而分离的媒体标识符可以用于实现对来自容器的特定项目进行重放。

在一个实施例中，从第二存储介质中检索到的密钥标识数据还包括能够用作操作值或操作标识符的值，这个值修改了解码器或解码器的算法。例如，解码器可以具有不同的预定操作模式，而操作值把解码器切换到当前需要的模式。按照上述方式启用的解码器也可以执行数学操作，其中，从密钥标识数据中检索到的操作值作为操作数。特别地，如上文所述，操作值也可以对用于根据第一密钥标识值来计算第二密钥标识值的算法做出修改或确定。

在一个实施例中，可以对媒体标识符与解码器盒之间的通信自身进行加密，从而不能自由地读取存储在RFID上的密钥。这一点可以通过例如会话加密来实现，其中，把秘密会话密钥传输到RFID标签，这个秘密会话密钥用于在传输期间对加密密钥自身进行加密。为此，媒体标识符标签会需要一些计算能力。

在一个实施例中，播放器把媒体标识符值和/或解密密钥存储一段时间，例如十秒、两个小时或十二小时，从而即使当前不能访问媒体标识符，也能够保持播放器对于相应的有用资源是启用的。可以将这个时间固定为标准时间，或可以存储在媒体标识符标签上，并与媒体标识符值一起下载到播放器上，从而可以为不同的有用资源指定各个时间。在经过这个时间后，自动地删除或重写所存储的值。如果这个时间较短（例如几秒），则用于和媒体标识符进行通信的电磁辐射量减小，因而播放器的功耗减小。如果这个时间在典型音频CD持续时间范围内或更大，则例如，将会在离开家之前启用便携式CD播放器，从而不再需要携带媒体标识符标签。在这种情况下，如果播放器（即，播放器内的安全系统）能够存储与若干CD相关的多个不同的媒体标识符值，则这将是有益的，从而用户可以在各自所允许的时间帧内收听不同唱片。

在本发明的一个实施例中，媒体标识符仅需要启动解码，并且一旦解码启动就可以被取走。在另一个实施例中，定期地（例如，每几个毫秒或每几秒）对媒体标识符的可用性进行检查，并且当不能读取媒体标识符时停止解码。在另一实施例中，媒体标识符必须总是可读的。

原理上，单一的媒体标识符标签也可以为不同的有用资源、甚至是不同的媒体而存储多个不同的标识符值。例如，媒体标识符标签可以包含附加的标识符，这个附加的标识符能够对从因特网下载的数据（例如，奖励音轨等）进行解码。还可以产生包含用于两个或多个媒体（例如，特定的DVD集）的标识符值和/或解密密钥的媒体标识符标签。在这种情况下，播放器内的安全系统把接收到的不同标识符值与当前插入的DVD的标识符值进行比较（这与上文对多个可读取的媒体标识符标签的描述相同），并选择匹配的标识符。

本发明方法还可以用于存储在其它存储媒体而不是盘上的内容数据，例如，存储在便携式MP3播放器的存储器中的MP3编码的音乐。在这种情况下，每一首歌曲都应当具有自己的标识符。

当在例如家庭网络中的中央服务器上保存内容时，也可以使用本发明。在开始向与家庭网络相连的任何设备传送内容之前，服务器可以使用例如RFID检测器来检查媒体标识符。

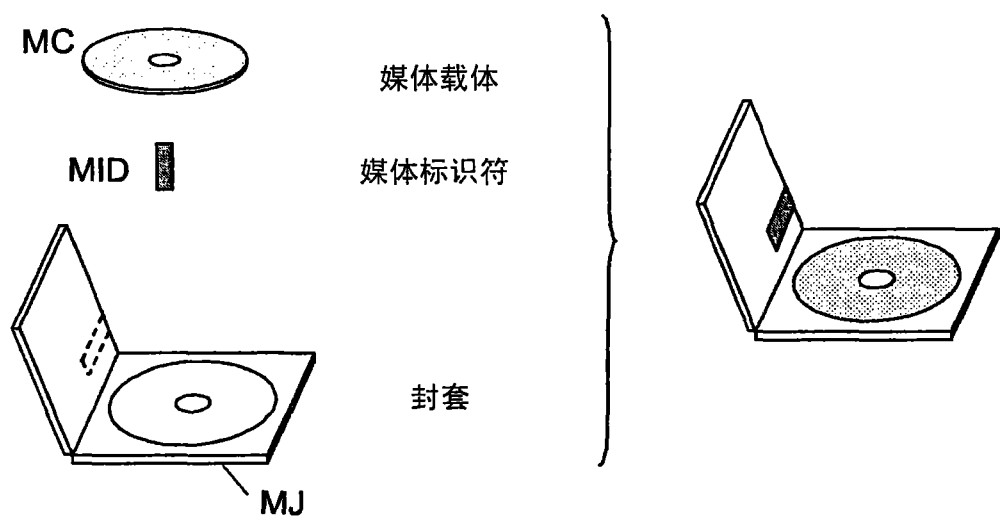


图 1

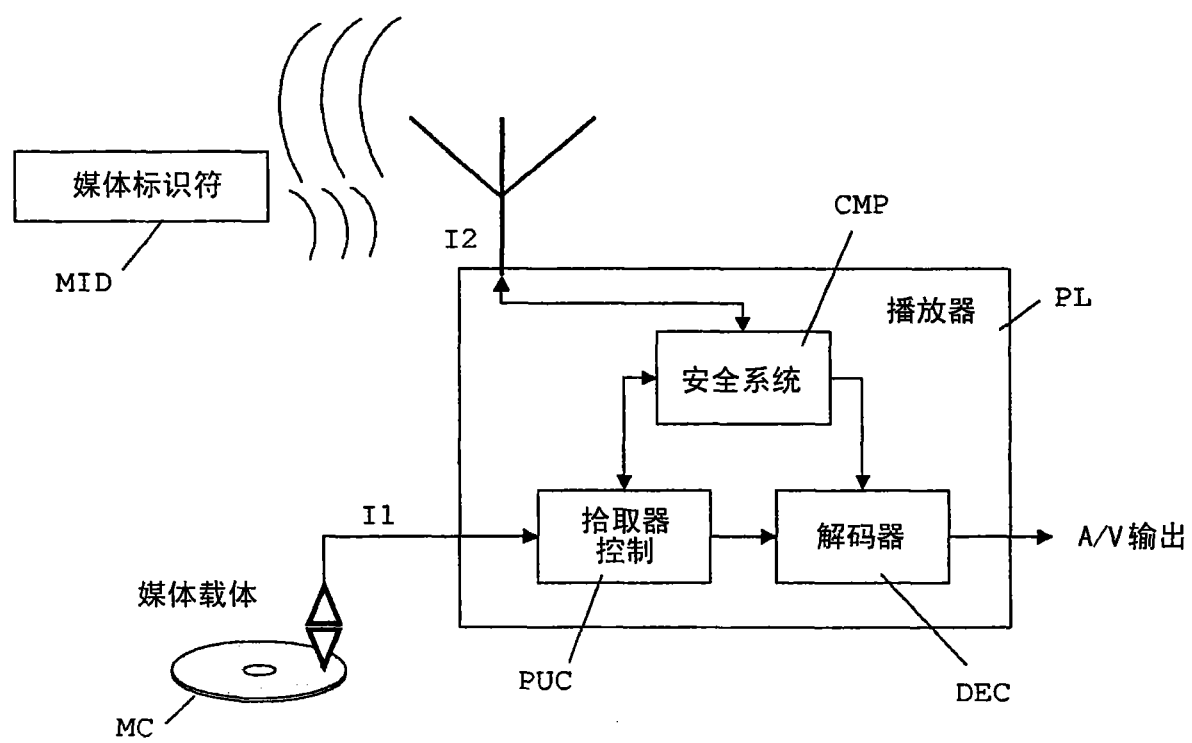


图 2

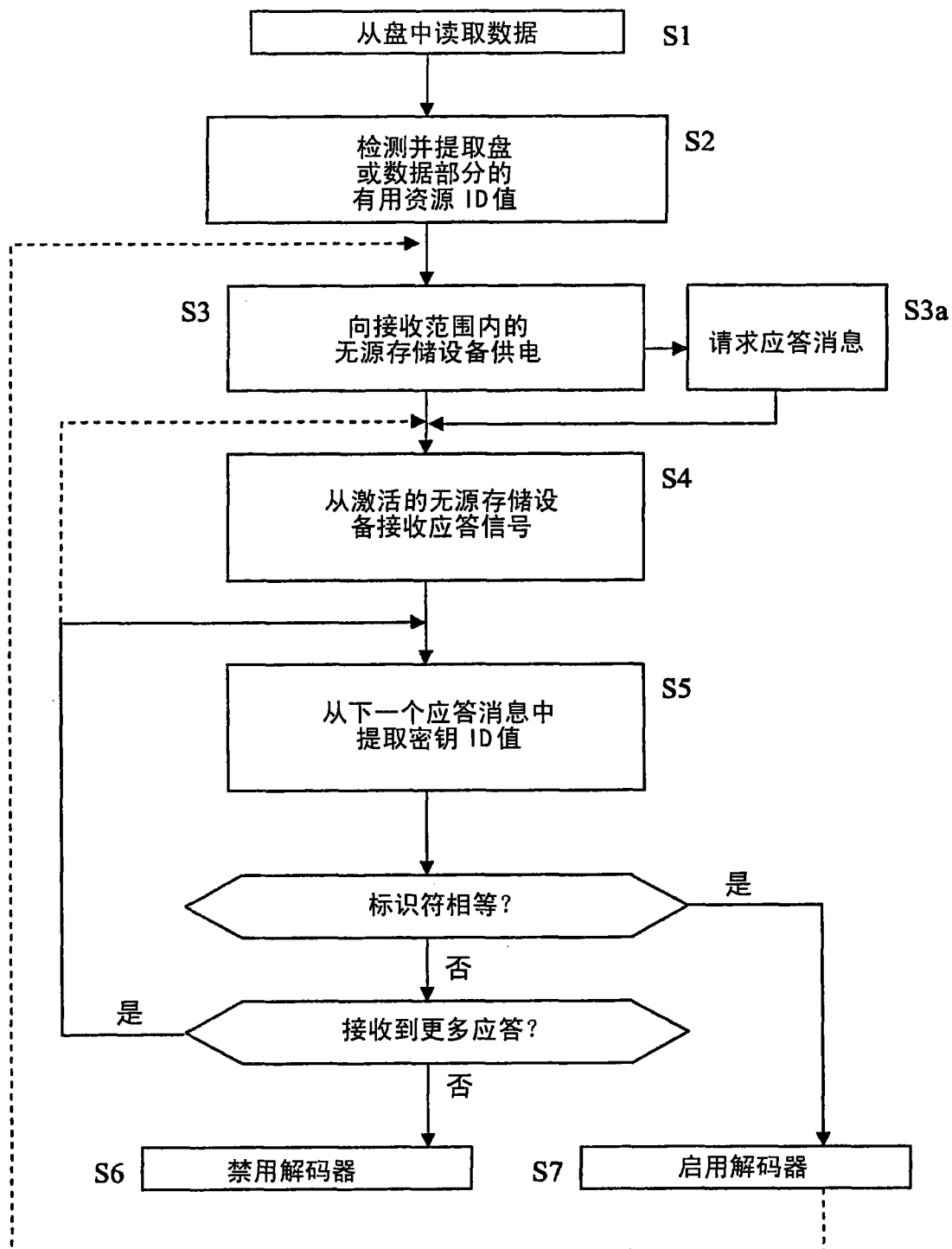


图 3

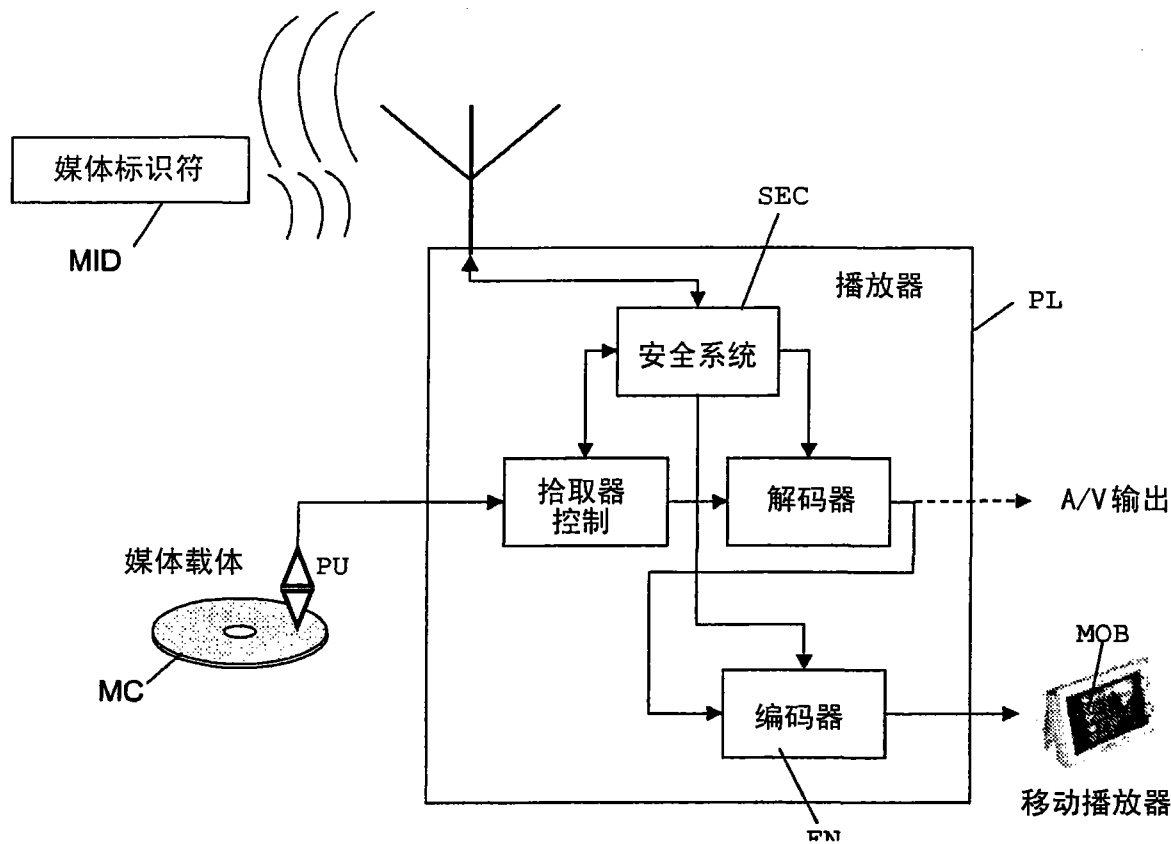


图 4

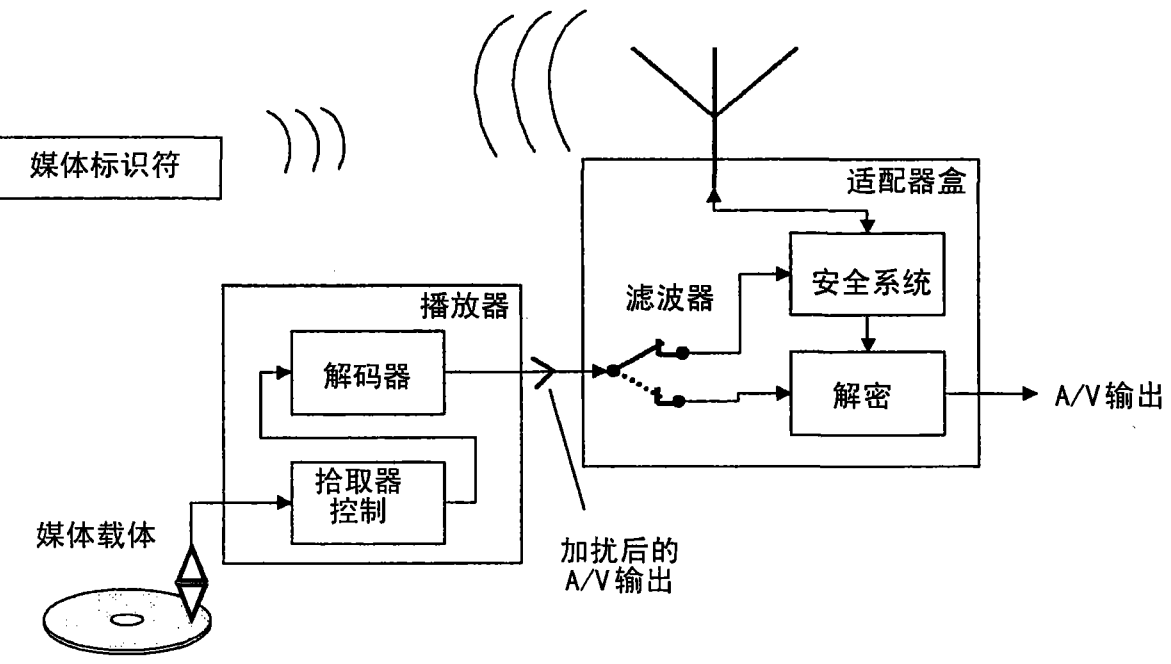


图 5

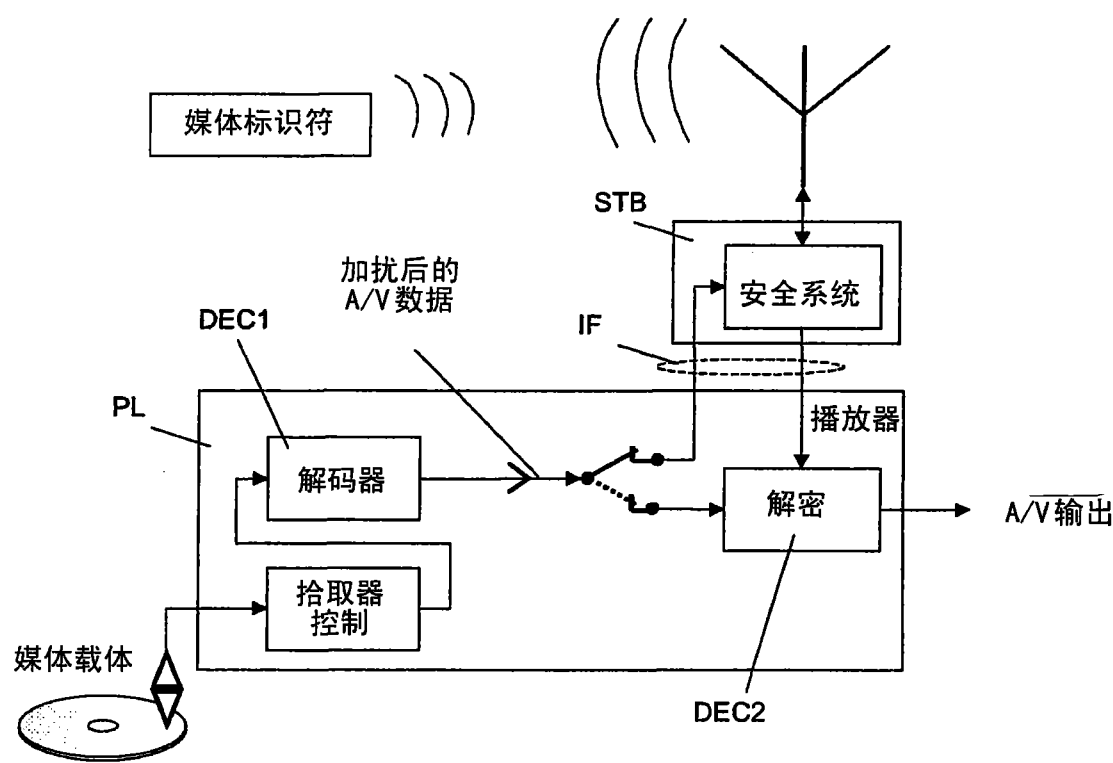


图 6