



(12) 发明专利

(10) 授权公告号 CN 102292931 B

(45) 授权公告日 2014. 03. 26

(21) 申请号 200980155365. 9

(22) 申请日 2009. 12. 22

(30) 优先权数据

61/146, 099 2009. 01. 21 US

12/485, 949 2009. 06. 17 US

(85) PCT国际申请进入国家阶段日

2011. 07. 20

(86) PCT国际申请的申请数据

PCT/US2009/069332 2009. 12. 22

(87) PCT国际申请的公布数据

W02010/090689 EN 2010. 08. 12

(73) 专利权人 微软公司

地址 美国华盛顿州

(72) 发明人 Q·S·伯恩斯 R·K·小休斯

J·C·西蒙斯

(74) 专利代理机构 上海专利商标事务所有限公司 31100

代理人 顾嘉运

(51) Int. Cl.

G06F 21/10(2013. 01)

审查员 庞艳

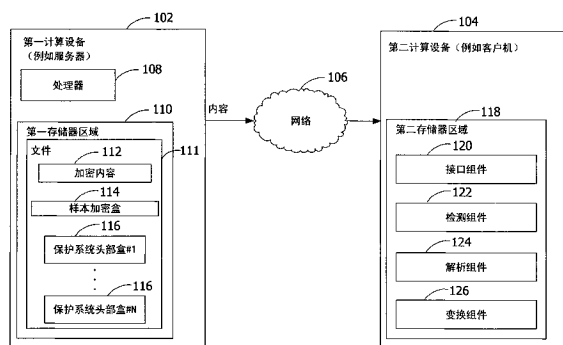
权利要求书2页 说明书9页 附图9页

(54) 发明名称

在单个容器文件中支持多个保护系统的方法和装置

(57) 摘要

在单个容器文件中支持多个内容保护系统。保护系统共享通过文件中的样本加密盒可访问的加密方法。每个保护系统都在保护系统的头部盒中存储用于依照对应的保护系统以解密内容的信息。在一些实施例中，文件中分别的保护系统头部盒对应于每个保护系统。通过使用通常的加密方法和跨保护系统共享加密表达，在文件中支持多个内容保护系统，而不创建内容的附加副本。在一些实施例中，本发明的方面扩展国际标准化组织(ISO)的基本媒体文件格式以在单个容器文件中支持多个数字版权管理(DRM)系统。



1. 一种用于扩展媒体文件格式以在单个容器文件中支持多个保护系统的方法,所述方法包括:

由服务提供者(206)从编码提供者(204)处接收文件(111),其中所述文件(111)被存储在存储器区域中,所述文件包含加密内容(112)、样本加密盒(114)以及多个保护系统头部盒(116),每个所述保护系统头部盒(116)与多个保护系统中的一个或多个相关,所述样本加密盒(114)标识用于加密加密内容(112)的密钥,并且所述多个保护系统头部盒(116)中的每一个包括用于依照多个保护系统中的一个或多个解码加密内容(112)的元数据;

选择服务提供者(206)可用的多个保护系统中的一个或多个;

使用由样本加密盒(114)标识的密钥来将选定的保护系统应用于接收到的文件(111)中的加密内容,以便创建数字版权管理保护的文件,而不创建加密内容的另一个副本;以及将所述数字版权管理保护的文件存储在存储器区域中。

2. 如权利要求1所述的方法,其特征在于,所述样本加密盒包括密钥映射信息以标识密钥。

3. 如权利要求1所述的方法,其特征在于,所述样本加密盒包括密钥标识符。

4. 如权利要求1所述的方法,其特征在于,所述样本加密盒和多个保护系统头部盒启用具有多个保护系统的文件的播放。

5. 如权利要求1所述的方法,其特征在于,所述存储在存储器区域中的文件符合ISO基本媒体文件格式。

6. 如权利要求1所述的方法,其特征在于,还包括:

依照ISO基本媒体文件格式支持在单个容器文件中的多个保护系统;以及

在单个容器文件中存储多个保护系统的元数据以作为ISO基本媒体文件格式的扩展。

7. 一种用于扩展媒体文件格式以在单个容器文件中支持多个保护系统的方法,包括:

接收包含加密内容以及一个或多个加密表达的文件(111),所述加密内容通过所述一个或多个加密表达被加密;

使用所述一个或多个加密表达将多个保护系统应用于所述加密内容,以便从所接收的文件中创建数字版权管理保护的文件,而不创建加密内容的另一个副本;以及

将所述数字版权管理保护的文件传输至一个或多个计算设备以解密所述加密内容,所述解密使用应用的多个保护系统中的至少一个。

8. 如权利要求7所述的方法,其特征在于,所述将多个保护系统应用于加密内容包括将多个保护系统中的每一个的元数据添加加入接收到的文件,所述元数据定义以下的一个或多个:解密密钥,版权对象,以及许可证信息。

9. 如权利要求7所述的方法,其特征在于,所述接收文件包括接收包含密钥映射信息的文件,所述加密内容使用所述密钥映射信息被加密。

10. 如权利要求7所述的方法,其特征在于,所述将多个保护系统应用于加密内容包括:

为多个保护系统中的每一个定义保护系统头部盒;以及

将定义的保护系统头部盒包括在接收到的文件中。

11. 如权利要求10所述的方法,其特征在于,还包括将许可证信息嵌入到保护系统头部盒中。

12. 如权利要求 10 所述的方法,其特征在于,还包括将许可证信息的引用嵌入到保护系统头部盒中。

13. 如权利要求 7 所述的方法,其特征在于,所述接收文件包括从电影工作室处接收与电影对应的文件。

14. 一种用于扩展媒体文件格式以在单个容器文件中支持多个保护系统的系统,所述系统包括:

用于由服务提供者从编码提供者处接收文件的装置,其中所述文件被存储在存储器区域中,所述文件包含加密内容、样本加密盒以及多个保护系统头部盒,每个所述保护系统头部盒与多个保护系统中的一个或多个相关,所述样本加密盒标识用于加密加密内容的密钥,并且所述多个保护系统头部盒中的每一个包括用于依照多个保护系统中的一个或多个解码加密内容的元数据;

用于选择服务提供者可用的多个保护系统中的一个或多个的装置;

用于使用由样本加密盒标识的密钥来将选定的保护系统应用于接收到的文件中的加密内容,以便创建数字版权管理保护的文件,而不创建加密内容的另一个副本的装置;以及
用于将所述数字版权管理保护的文件存储在存储器区域中的装置。

在单个容器文件中支持多个保护系统的方法和装置

[0001] 背景

[0002] 现有的数字版权管理(DRM)系统保护媒体内容和其它文件免受未经授权的使用。为了保护内容,一个 DRM 系统所特有的元数据被存储在具有媒体内容的文件中。设备通过解释元数据和解密内容来提供内容以用于向用户呈现。但是,根据第一 DRM 系统加密的内容不能够被仅支持第二 DRM 系统的设备解密。为了使得加密的内容能够被这一设备解密,现有的系统创建多个版本的内容,其中每个版本根据不同的 DRM 系统被加密。替代地,内容可以由支持第一 DRM 系统的设备解密,并且然后由支持第二 DRM 系统的设备重新加密。还有其它现有的系统包括在第一和第二 DRM 系统之间提供版权映射的服务。

[0003] 概述

[0004] 本发明的实施例支持适用于单个容器文件的多个保护系统。接收包含内容和一个或多个加密表达的文件。内容由加密表达加密。使用来自接收到的文件的加密表达将多个保护系统应用于内容。每个保护系统都保护使用相同加密表达的内容。具有内容以及应用的多个保护系统的文件被传送到一个或多个计算设备以解密。每个计算设备都使用应用的多个保护系统中的至少一个来解密内容。

[0005] 提供本概述以便以简化形式介绍将在以下的详细描述中进一步描述的一些概念。本概述并不旨在标识出所要求保护的主题的关键特征或必要特征,也不旨在用于帮助确定所要求保护的主题的范围。

附图说明

[0006] 图 1 是示出第一计算设备跨网络向第二计算设备提供内容的示例性框图。

[0007] 图 2 是示出内容流从内容提供者通过编码提供者和服务提供者到达消费者的示例性框图。

[0008] 图 3 是示出保护系统应用到内容的示例性流程图。

[0009] 图 4 是示出解码在计算设备上呈现的内容的示例性流程图。

[0010] 图 5 是示出表示片段文件结构的示例性结构的示例性框图。

[0011] 图 6 是示出表示片段文件组织的示例性结构的示例性框图。

[0012] 图 7 是示出用于存储轨道盒的示例性结构的示例性框图。

[0013] 图 8 是示出用于存储媒体信息盒的示例性结构的示例性框图。

[0014] 图 9 是示出用于存储保护的样本条目盒的示例性结构的示例性框图。

[0015] 在全部附图中,相应的附图标记指示相应的部分。

[0016] 详细描述

[0017] 参考附图,公开的实施例至少支持多个保护系统,保护系统诸如在存储用于向用户呈现的媒体内容的文件 111 中的数字版权管理(DRM)系统。文件 111 存储由多个保护系统保护的媒体内容或其它内容的单个副本。部分地为了启用保护系统中的这一互操作性,保护系统使用或共享保护系统常用的加密算法或其它加密方法。此外,跨保护系统共享由保护系统使用的诸如密钥信息等的加密表达。

[0018] 本公开的各方面扩展国际标准化组织(ISO)的基本媒体文件格式以在诸如文件 111 的单个容器文件中支持多个 DRM 系统。在一些实施例中,容器文件包括样本加密盒 114 以及多个保护系统头部盒 116,其中每个保护系统头部盒为一个或多个保护系统所特有。样本加密盒 114 存储或标识保护系统常用的加密方法。每个保护系统头部盒 116 都存储用于与对应的保护系统一起解密内容的数据对象。例如,在一些实施例中,保护系统头部盒 116 中的数据对象用于获取其它数据对象(例如从许可证服务器)以解密内容。数据对象表示在单个文件中同时支持多个保护系统的不透明的元数据。

[0019] 尽管参照作为诸如移动电话或上网本或超便携型等的移动计算设备的计算设备描述本发明,本发明的实施例可以用任何计算设备操作。例如,本发明可以用诸如数码相机、数码摄像机、膝上计算机、机顶盒、游戏控制台(包括手持式游戏控制台)、便携式音乐播放器、个人数字助理、信息装置、以及个人通讯器等设备来操作。

[0020] 再次参考图 1,示例性框图示出第一计算设备 102 跨网络 106 向第二计算设备 104 提供内容。在一些实施例中,第一计算设备 102 是服务器,第二计算设备 104 是客户设备,并且网络 106 是因特网。第一计算设备 102 至少包括第一存储器区域 110 和处理器 108。第一存储器区域 110 存储与例如媒体内容或媒体呈现对应的文件 111。媒体内容包括诸如视频、音频、图像、文本和 / 或图形、或者其序列等的商业或非商业的媒体数据。第一计算设备 102 将具有媒体内容的文件 111 跨网络 106 传输至第二计算设备 104。

[0021] 图 1 中的示例性框图描述由本公开的实施例支持的内容传递场景,该场景包括但不限于,从光盘到计算设备(例如便携式设备或个人计算机)的标准定义或便携式媒体内容的第二会话或数字传递,多媒体内容的渐进下载,跨互联网协议(IP)网络的自适应流传送,或者将多媒体内容侧面装载到便携式设备上。

[0022] 第一计算设备 102 或其它服务器表示媒体内容或与其相关的信息的任何已知或后来开发的源,包括但不限于,数据存储服务器、DRM 服务器、媒体内容服务器(例如用于音乐或视频下载、点播、广播、或广告)、对等服务器等等。第一计算设备 102 可包括一个或多个这类设备。

[0023] 网络 106 表示被配置为支持已知或未来开发的媒体协议的任何数字数据传输基础结构或技术。示例性网络包括但不限于,因特网、蜂窝网络、卫星网络、蓝牙品牌无线网络等。

[0024] 第二计算设备 104 是被配置为从第一计算设备 102 处接收数据的任何计算设备,或这一计算设备的元素。第二计算设备 104 可以被配置为存储和 / 或呈现接收到的数据,或者替代地将接收到的数据传递到另一个设备以用于存储和 / 或呈现。

[0025] 第一计算设备 102 和第二计算设备 104 可以包括诸如收发机、多路复用器、多路去复用器、编码器、解码器、加密器、解密器等组件。

[0026] 在一些实施例中,文件 111 表示用支持多个保护系统的格式存储内容的容器文件。例如,保护系统对应于 DRM 系统。在这些实施例中,文件 111 包括加密内容 112、样本加密盒 114 以及诸如保护系统头部盒 #1 到保护系统头部盒 #N 的多个保护系统头部盒 116。样本加密盒 114 和保护系统头部盒 116 表示由类型标识符和长度所定义的面向对象的构造块。容器盒包含并且分类相关的盒。例如,媒体数据盒是持有用于呈现的媒体内容的容器盒,而电影盒是其子盒定义用于呈现的元数据的容器盒。尽管样本加密盒 114 和保护系统

头部盒 116 被示出包含在诸如附图中所示的特定盒或容器盒中,但是盒表明可以通过其包含的盒或其中的另一个盒传递的信息。此外,盒可以被当作文件 111 中其它盒的子盒。

[0027] 多个保护系统头部盒 116 中的每一个都与一个或多个保护系统相关。任意数量的保护系统头部盒 116 可以被包含在文件 111 中。盒和保护系统由 DRM 标识符或其它保护系统标识符标识。样本加密盒 114 标识用于加密加密内容 112 的密钥。在一些实施例中,样本加密盒 114 存储密钥、密钥标识符和 / 或描述常见或标准的跨保护系统加密的方法的密钥映射信息。每个样本加密盒 114 的密钥可以是不同的。例如,标准加密方法包括以计数器(CTR)模式具有 128 比特密钥大小的高级加密标准(AES)。AES 算法的初始化向量也是保护系统常用的。样本加密盒 114 由保护系统头部盒 116 共享。每个保护系统头部盒 116 都包括依照一个或多个保护系统的用于解码加密内容 112 或授权访问内容的元数据。

[0028] 在其中文件 111 与 ISO 基本媒体文件格式对应的示例中,一些实施例中的保护系统头部盒 116 位于嵌套级别 1,而样本加密盒 114 位于嵌套级别 2。

[0029] 第二计算设备 104 可以访问第二存储器区域 118。第二存储器区域 118、或一种或多种计算机可读介质,存储用于解码和呈现媒体内容至第二计算设备 104 的用户的计算机可执行组件。示例性组件包括接口组件 120、检测组件 122、解析组件 124、以及变换组件 126。这些组件表示用于实现与第二计算设备 104 相关的功能的示例性结构,尽管其它结构也可以被考虑用于实现此处描述的功能。以下参考图 4 描述图 1 所示的示例性组件的操作。

[0030] 一般地,第一存储器区域 110 与第一计算设备 102 相关。例如在图 1 中,第一存储器区域 110 在第一计算设备 102 内。但是,第一存储器区域 110 或其上存储的任何数据可以与第一计算设备 102 本地或远程(例如通过网络可访问的)的任何服务器或其它计算机相关。类似地,第二存储器区域 118 与第二计算设备 104 相关。例如在图 1 中,第二存储器区域 118 在第二计算设备 104 内。但是,第二存储器区域 118 或其上存储的任何数据可以与第二计算设备 104 本地或远程(例如通过网络可访问的)的任何服务器或其它计算机相关。

[0031] 处理器 108 包括任何数量的处理单元,并且被编程为执行用于实现本公开的各方面的计算机可执行指令。指令可以由在第一计算设备 102 内执行的处理器 108 或多个处理器执行,或者由第一计算设备 102 外部的处理器(例如由云服务)来执行。在一些实施例中,处理器 108 被编程为执行诸如各附图(例如图 3 和图 4)中示出的那些指令。

[0032] 再次参考图 2,示例性框图示出内容流从内容提供者 202 通过编码提供者 204 和服务提供者 206 到达消费者。图 2 的示意图示出图 1 中所示示例的示例,其中服务提供者 206 对应于第一计算设备 102,并且消费者设备 208 对应于第二计算设备 104。

[0033] 内容提供者 202 生成包含媒体内容的文件。例如,内容提供者 202 是产生与电影对应的视频文件的电影工作室。生成的视频文件可以用对每个内容提供者 202 专用的被称为夹层格式的格式。内容提供者 202 将视频文件传输至编码提供者 204。编码提供者 204 准备分发至一个或多个服务提供者 206 的视频文件。在这一示例中,编码搭档执行处理以为编码,包括一些实施例中的加密准备夹层内容,并且然后执行编码和加密。使用由内容提供者 202 提供的或者由编码提供者 204 生成的加密密钥进行编码和加密。编码的内容已经准备好分发,但是缺少保护系统(例如 DRM)。将编码的内容发送至服务提供者 206。

[0034] 服务提供者 206 接收编码的内容并且将 DRM A 的头部(例如一个保护系统头部盒 116)添加到视频文件中。具有应用的保护系统的视频文件可以被发送至能够仅由 DRM A 解

密该视频文件的消费者设备 208 或其它设备。替代地或额外地,服务提供者 206 还可以另一个头部 DRM B(例如另一个保护系统头部盒 116)添加到视频文件中。此时,能够使用 DRM A 或 DRM B 来解码视频文件。视频文件被传输到消费者,其中消费者设备 208 可以使用 DRM A 或 DRM B 来解析、解密和解码该视频文件。

[0035] 在一个示例中,内容是电影,并且用户尝试在支持 DRM A 的设备一(Device One)上播放电影。设备一上的播放软件确定电影被加密。播放软件找到与 DRM A 对应的保护专用头部盒。播放软件使用保护专用头部盒中包含的信息以与许可证服务器联系并且检索该电影的许可证。检索的许可证可以被存储在 DRM A 的保护专用头部盒内(例如在其额外的空间)。然后使用 DRMA 解码该电影并且呈现给用户。

[0036] 在进一步的示例中,用户复制电影至支持 DRM B 的设备二(Device Two)。设备二上的播放软件确定电影被加密。播放系统找到与 DRM B 对应的保护专用头部盒。播放软件使用保护专用头部盒中包含的信息以与许可证服务器联系并且检索该电影的许可证。检索的许可证可以被存储在 DRM B 的保护专用头部盒内(例如在其额外的空间)。然后使用 DRM B 解码该电影并且呈现给用户。

[0037] 接着参考图 3,示例性流程图示出将保护系统应用到内容。诸如图 2 中服务提供者 206 的计算设备在 302 处确定是否已经接收到文件。文件包括媒体内容和一个或多个加密表达。媒体内容根据加密表达被加密。在一些实施例中,加密表达包括一个或多个加密密钥、密钥标识符以及密钥映射信息,或者包括描述上述的元数据。在其它实施例中,加密表达包括用于从另一个位置(例如网络服务)获取一个或多个加密密钥、密钥标识符以及密钥映射信息的数据对象。加密表达可以被存储在例如图 1 中所示的一个或多个保护系统头部盒 116 和 / 或样本加密盒 114 中。

[0038] 在 302 处接收到具有媒体内容的文件之后,在 304 处选择多个保护系统。例如,保护系统可以基于文件的预期接受人被选择,或者表示由消费者设备 208 通常使用的保护系统的默认选择。在 306 处,使用一个或多个加密表达以创建 DRM 保护的内容来将选定的保护系统应用于文件中的内容。例如,应用保护系统包括将保护系统的元数据添加或嵌入文件。元数据描述保护系统并且启用内容的解密。在一些实施例中,元数据包括与保护系统相关的解密密钥在一起的与保护系统有关的版权对象或许可证信息(或者许可证信息的引用)。

[0039] 保护系统被应用于内容,而不创建内容另外的副本。因此,单个容器文件(例如文件 111)包括内容和多个选定的、应用的保护系统。

[0040] 在 308 处,DRM 保护的内容被传输至一个或多个计算设备。计算设备使用由计算设备支持的至少一个应用的保护系统来解密内容。替代地或另外地,DRM 保护内容被存储在由计算设备访问的存储器区域。

[0041] 在图 1 的示例中,应用保护系统包括为每个选定的保护系统定义一个保护系统头部盒 116。定义的保护系统头部盒 116 被包括在文件中。在这一示例中,样本加密盒 114 包括包含密钥映射信息和密钥标识符的密钥信息。使用样本加密盒 114 中标识的密钥信息将保护系统应用于内容。

[0042] 接着参考图 4,示例性流程图示出解码在计算设备上呈现的内容。在 402 处,由计算设备接收 DRM 保护的 video 文件。在计算设备上执行的解析器在 404 处检查接收到的文件

中的元数据,以在 406 处确定文件具有应用到其上的保护系统。例如,如果文件采用运动图像专家组 -4 (MP4) 格式,则解析器确定文件已经被加密视频(例如“encv”)或加密音频(例如“enca”)的流类型保护。在这一示例中,解析器检查保护方案信息盒中的方案信息盒或方案类型盒以确定文件中的轨道是否依照本公开的各方面被加密。轨道对应于文件中一组相关的样本。在一些实施例中,解析器在方案类型盒中找到标识保护系统的四字符代码和版本号。

[0043] 在 408 处,在计算设备上执行的应用程序在接收到的视频文件中搜索保护系统头部盒 116,以找到与由计算设备支持的保护系统对应的保护系统头部盒 116。保护系统头部盒 116 用于确保在播放开始之前解密内容的任何许可证可用于计算设备。从样本加密盒 114 处获取密钥标识符。在 410 处,应用程序从与支持的保护系统对应的保护系统头部盒 116 处获取数据,该支持的保护系统使得应用程序能够从与密钥标识符对应的许可证服务器处获取许可证。在 411 处,应用程序然后从许可证中提取出加密密钥,并且解密密钥。在一些实施例中,可以使用已知的公共 - 私人密钥系统来执行解密加密的密钥(例如私人密钥、个性化的密钥、或者其它的非对称密钥)。在 412 处,解密的密钥用于解密轨道,并且向用户呈现解密的内容。

[0044] 在一些实施例中,使用存储在一种或多种计算机可读介质上的计算机可执行组件来实现图 4 中所示的操作。例如,图 1 中所示的组件执行操作。在这一示例中,接口组件 120 接收包含内容以及一个或多个加密表达的文件。内容已经由至少一个加密表达加密。内容进一步具有多个应用其上的保护系统,并且文件包括多个保护系统的每一个的元数据。多个保护系统共享对加密表达的访问。此外,内容根据加密算法被编码。多个保护系统共享加密表达以及加密算法。

[0045] 检测组件 122 检查文件中的方案信息盒以确定内容是否依照本公开的各方面被保护方案保护。检测组件 122 确定哪些保护系统被计算设备支持,并且选择一个支持的保护系统。解析组件 124 从元数据中获取由检测组件 122 选定的保护系统的许可证信息。变换组件 126 基于由解析组件 124 获取的许可证信息以及基于加密表达来解码和解密内容。接口组件 120 向用户呈现解码的内容。

[0046] 接着参考图 5、图 6、图 7、图 8 和图 9,示例性框图示出扩展媒体文件格式以在单个容器文件中支持多个保护系统的本公开的实施例的示例应用。以下示例参考的各已知规范包括但不限于,ISO14496-12、ISO14496-14、ISO14496-1、ISO14496-10、ISO14496-3 以及 ISO/IEC639-3:2007,就各方面而言此处将其全部并入以作为参考。尽管以下描述的示例被定向至 ISO 基本媒体文件格式和 / 或 MP4 格式,但是本发明的各实施例可应用于其它文件格式。

[0047] 为了以下的示例,文件格式可以指电影。电影被逻辑地分为轨道。每个轨道表示媒体的时间序列(例如视频帧)。在每个轨道内,每个时间单元或数据帧被称为样本(例如视频或音频的帧、视频帧的时间连续序列、或音频的时间连续压缩部分)。按顺序隐式地编号样本。音频的帧可以被解压缩为音频样本的序列。每个轨道具有一个或多个样本描述。作为参考,轨道中的每个样本被与描述绑定。描述定义了样本如何被编码(例如标识使用的压缩算法)。

[0048] 在一些实施例中,文件的物理结构和物理媒体的布局都不与媒体内容的时间顺序

绑定。例如，视频帧不需要按照时间顺序被放置在文件中，尽管可以以这种方式放置视频帧。

[0049] 文件中的数据被封装在盒中。元数据，包括定义媒体内容的放置和定时的元数据，被包含在盒中。元数据引用媒体内容（例如视频帧）。媒体内容可以在同一文件中（例如被包含在一个或多个盒中），或者可以在其它文件中。元数据允许依靠诸如超链接（例如统一资源定制器）的引用来参考其它文件。

[0050] 在以下示例中，本发明的各实施例使用具有继承的基于类的标号。类被一致地标识为磁盘上和电线上的结构，如下：类的域以域被指定的相同顺序出现在磁盘结构中，并且父类的域出现在派生类的域之前。此外，当盒包含例如孩子的其它盒时，子盒出现在任何明确指定的域之后并且可以以任意顺序出现（例如兄弟盒可以被重新排序而不违背本发明）。

[0051] 再次参考图 5，示例性框图示出依照本公开的各实施例表示片段文件结构的示例性结构。片段文件结构包括两个顶层盒：元数据的电影片段盒（“moof”），以及样本的媒体数据（“mdat”）盒。在这一示例中，由保护系统共享的样本加密盒 114 被示为电影片段盒的子盒。样本加密盒 114 包括样本专用的加密数据。在图 5 的示例中，样本加密盒 114 具有类型通用唯一标识符（UUID），并且是轨道片段容器盒或样本表容器盒的一部分。

[0052] 以下示出样本加密盒 114 的示例句法。

[0053]

```
aligned(8)    class    SampleEncryptionBox    extends    FullBox('uuid',
extended_type=1, version=0, flags=0)
```

```
{
    unsigned int(8)  AlgorithmID;
    GUID            KID;
    unsigned int(32) sample_count;
    {
```

[0054]

```
        unsigned int(64) SampleIdentifier;
    }[ sample_count ]
}
```

[0055] AlgorithmID 是用于加密轨道的加密算法（例如使用 CTR 模式的 AES128 位）的标识符。KID 是标识用于解密由样本加密盒 114 引用的样本的密钥的密钥标识符。在这一示例中，在样本加密盒 114 中有一个 AlgorithmID 和一个 KID，这意味着每个轨道有一个密钥。在其它实施例中，例如，每个轨道有多个密钥以例如允许密钥轮换广播内容包括加密的轨道中清洁内容的部分的内容，并且允许插入用不同参数加密的内容（例如编辑、广告插入等）。

[0056] Sample_count 是在这一轨道中或轨道片段中样本的数量。SampleIdentifier

用于形成解密样本的初始化向量。用于加密样本数据的 AES CTR 模式加密使用 SampleIdentifier 以作为用 AES 密码加密的 128 位值中的高 64 位,以及使用简单的块计数器(例如在样本开始时从 0 开始)以作为低 64 位。在一些实施例中,给定密钥的 SampleIdentifier 对于每个样本是唯一的,并且初始样本标识符是随机生成的。对于每个添加至文件的保护的样本,递增 SampleIdentifier 以提供熵并确保 SampleIdentifier 是唯一的。

[0057] 再次参考图 6,示例性框图示出表示片段文件组织的示例性结构。电影片段包括特定序列的媒体数据的特定部分。在这一示例中,磁盘格式是片段的 MP4。图 6 中的文件类型盒标识文件为依照本公开的各实施例被编码以使文件类型盒保持固定的长度。诸如 DRM 专用头部盒 #1 到 DRM 专用头部盒 #N 的多个 DRM 专用头部盒 602 (电影盒的子盒)对应于图 1 中所示的多个保护系统头部盒。DRM 专用头部盒 602 包含的数据包括但不限于,许可证服务器引用(例如统一资源定址器)、文件使用的密钥标识符的列表、嵌入的许可证等。DRM 专用头部盒 602 还可以存储或预装载任何数量的嵌入许可证(例如在内容可用于用户之前从服务提供者 206 处)。

[0058] 在一些实施例中,多个 DRM 专用头部盒 602 存在于同一保护系统中。例如,单个文件由两个不同的服务共享,所述两个不同的服务同时使用同一保护系统,但是每个服务使用不同的头部参数(例如不同的服务标识符、不同的许可证获取链接等)。

[0059] 以下示出 DRM 专用头部盒 602 的示例句法。

[0060]

```
aligned(8) class DrmSpecificHeaderBox extends
FullBox('uuid', extended_type=1, version=0, flags=0)
{
    GUID                                DRMID;
    unsigned int(32)                    DataSize;
    unsigned int(8)[DataSize]          Data;
}
```

[0061] DRMID 指定唯一标识该头部所属的保护系统的 UUID。DataSize 指定数据成员的字节的大小。Data 持有保护系统专用的数据。

[0062] 再次参考图 7,示例性框图示出用于存储轨道盒的示例性结构。轨道盒充当用于存储诸如图 8 中所示的媒体信息盒 702 的盒的容器盒。

[0063] 再次参考图 8,示例性框图示出用于存储媒体信息盒 702 的示例性结构。媒体信息盒 702 充当用于存储诸如样本描述盒("stsd")的盒的容器盒。样本描述盒存储包括保护的样本条目盒 802 的盒,该样本条目盒 802 存储加密的样本内容。在图 9 中再次示出样本条目盒。

[0064] 再次参考图 9,示例性框图示出用于存储保护的样本条目盒 802 的示例性结构。保护的样本条目盒 802 充当用于存储诸如保护方案信息盒的盒的容器盒。对比于现有的 ISO 基本媒体文件格式,保护方案信息盒被存储以替代样本描述盒中的样本条目,以注释流被

加密。保护方案信息盒包含方案类型盒(‘schm’),从而方案是可识别的。

[0065] 补充示例

[0066] 此处描述的文件格式表示包括支持交替的音频和视频内容的后期绑定的最小文件格式。这使得支持继承的或出现编码器/解码器(编解码器)的计算设备能够在播放时后期绑定那些流,而不需要增加设备的负载,不需要用额外的下载开销来支持那些编解码器。

[0067] 本公开的各实施例支持片段的和非片段的容器文件。例如,片段的文件格式用于自适应的流,而非片段的文件格式用于来自光盘的数据副本。

[0068] 示例性操作环境

[0069] 作为示例而非限制,计算机可读介质包括计算机存储介质和通信介质。计算机存储介质存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息。通信介质一般以诸如载波或其它传输机制等已调制数据信号来体现计算机可读指令、数据结构、程序模块或其它数据,并且包括任何信息传递介质。以上的任一种的组合也包括在计算机可读介质的范围之内。

[0070] 尽管结合示例性计算系统环境进行了描述,但本发明的各实施例可用于众多其它通用或专用计算系统环境或配置。适用于本发明各方面的公知的计算系统、环境和/或配置的示例包括但不限于,移动计算设备、个人计算机、服务器计算机、手持式或膝上型设备、多处理器系统、游戏控制台、基于微处理器的系统、机顶盒、可编程消费电子产品、移动电话、网络 PCs、小型计算机、大型计算机、包括上述系统或设备中的任一个的分布式计算环境等等。

[0071] 可以在由一个或多个计算机或其它设备执行的诸如程序模块等的计算机可执行指令的一般上下文中来描述本发明的各实施例。计算机可执行指令可以被组织成一个或多个计算机可执行组件或模块。一般而言,程序模块包括但不限于,执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件,以及数据结构。可以利用任何数量的这样的组件或模块及其组织来实现本发明的各方面。例如,本发明的各方面不仅限于附图中所示出并且在此处所描述的特定计算机可执行指令或特定组件或模块。本发明的其它实施例可以包括具有比此处所示出和描述的功能更多或更少功能的不同的计算机可执行指令或组件。

[0072] 本发明的各方面在被配置成执行此处所描述的指令时将通用计算机变换成专用计算设备。

[0073] 此处所示出并描述的各实施例以及此处未具体描述但在本发明各方面的范围内的各实施例构成了用于依照 ISO 基本媒体文件格式在单个容器文件中支持多个保护系统的示例性手段,以及用于存储单个容器文件中的多个保护系统的元数据以作为 ISO 基本媒体文件格式的扩展的示例性手段。

[0074] 此处所示出和描述的本发明的各实施例中的操作的执行或实现的顺序不是必需的,除非另外指定。即,除非另外指定,否则操作可以按任何顺序执行,且本发明的各实施例可以包括比此处所公开的操作更多或更少的操作。例如,构想了在一个操作之前、同时或之后执行另一个操作是在本发明的各方面的范围内的。

[0075] 当介绍本发明的各方面的元素或其实施例时,冠词“一”、“一个”、“该”、“所述”旨在表示有元素中的一个或多个。术语“包括”、“包含”以及“具有”旨在是包含性的,并意味着除所列出的元素以外还可以有额外的元素。

[0076] 已经详细地描述了本发明的各方面,显然,在不偏离所附权利要求书所定义的本发明的各方面的范围的情况下,可以进行各种修改和变化。在不偏离本发明的各方面的范围的情况下,可以对上面的构造、产品以及方法做出各种更改,上面的描述中所包含的和各个附图中所示出的所有主题应该解释为说明性的,而不是限制性的。

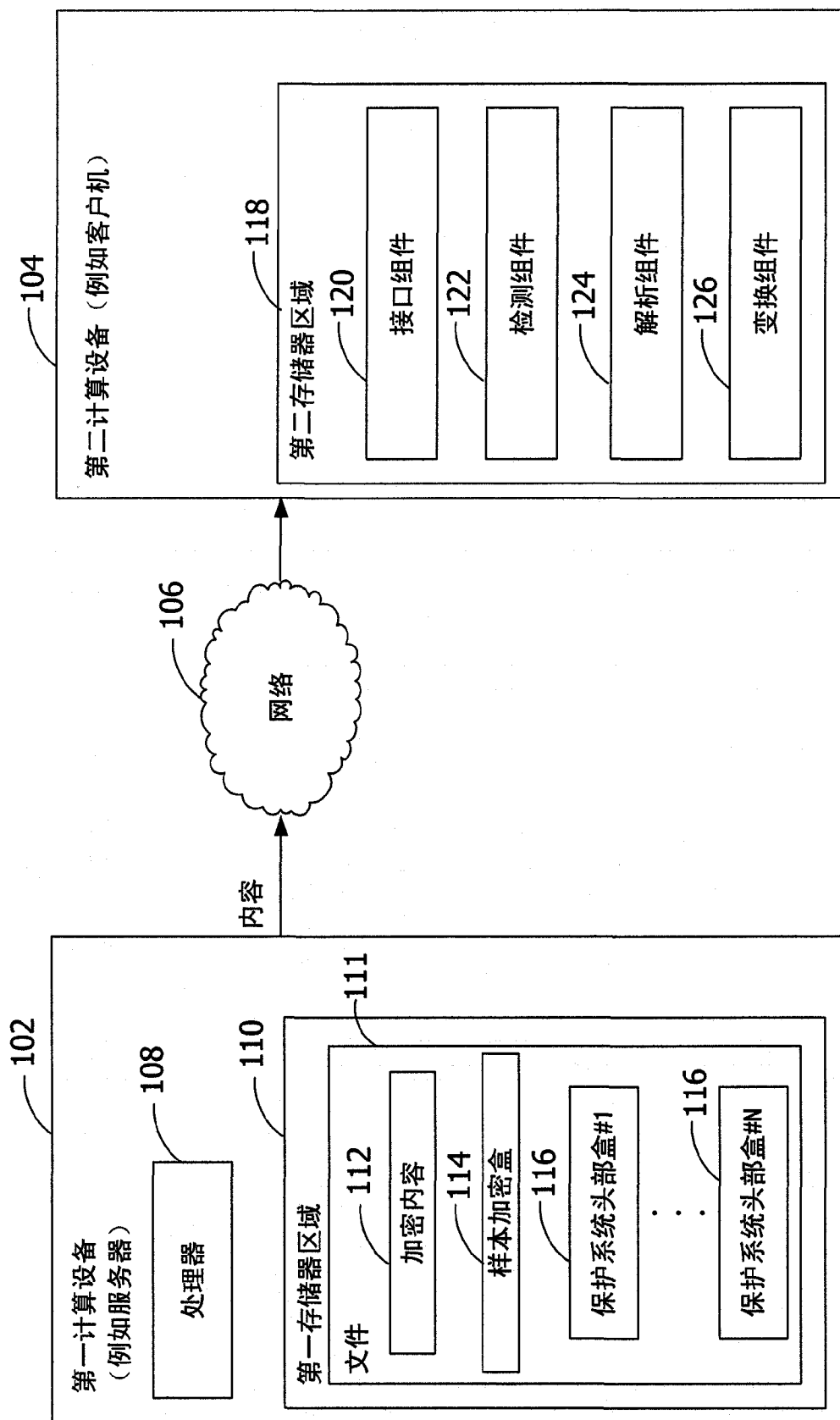


图 1

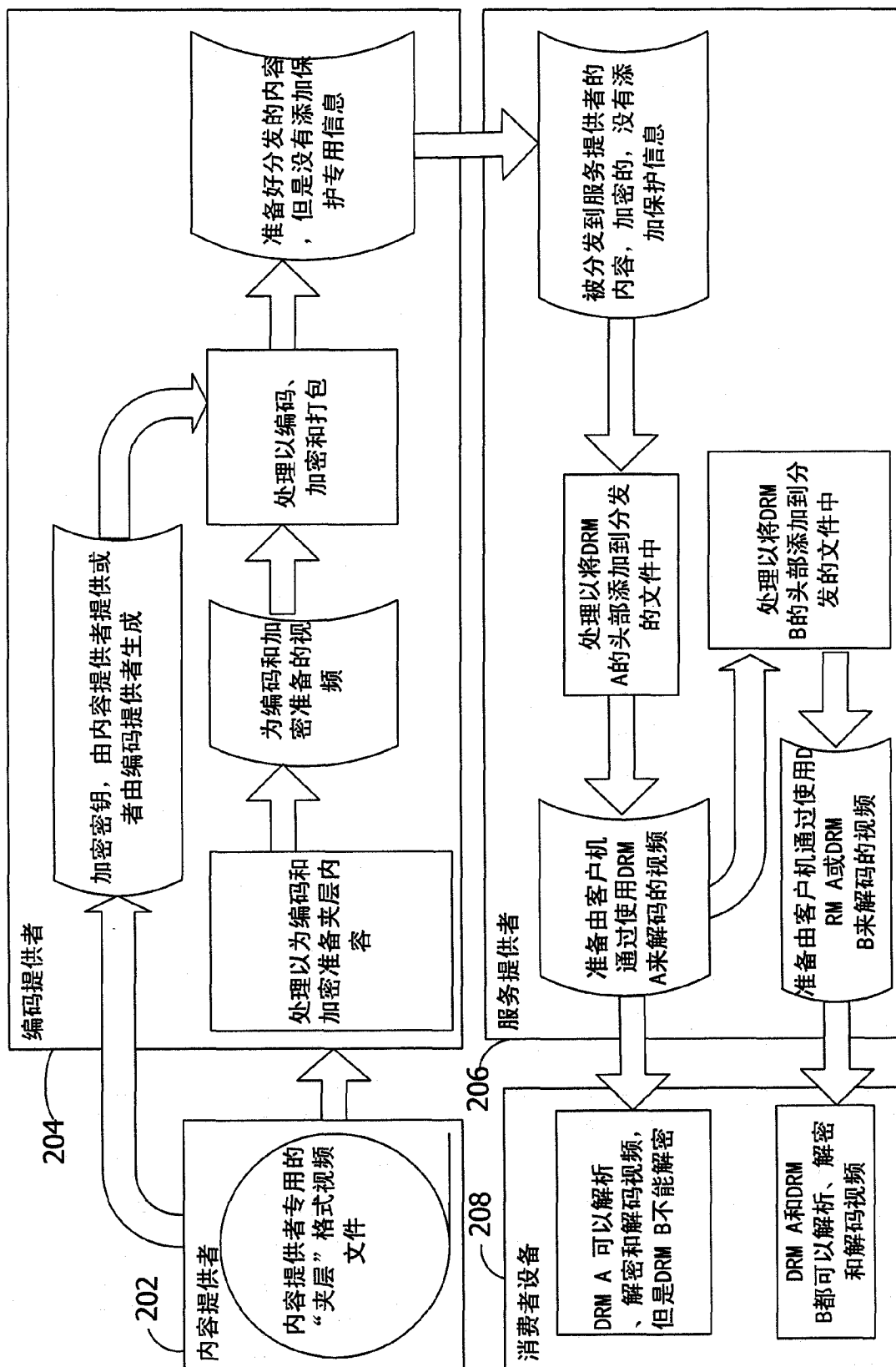


图 2

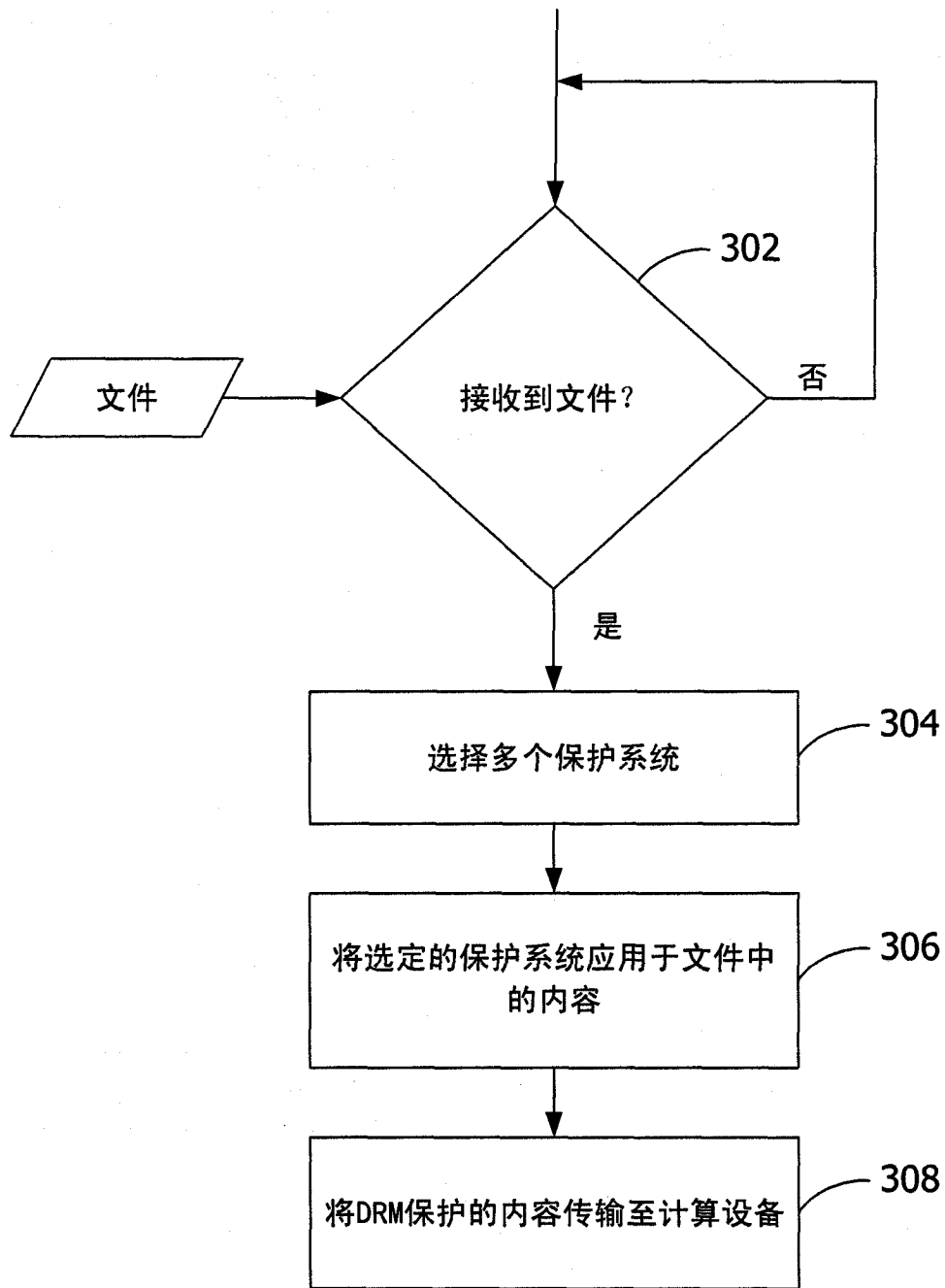


图 3

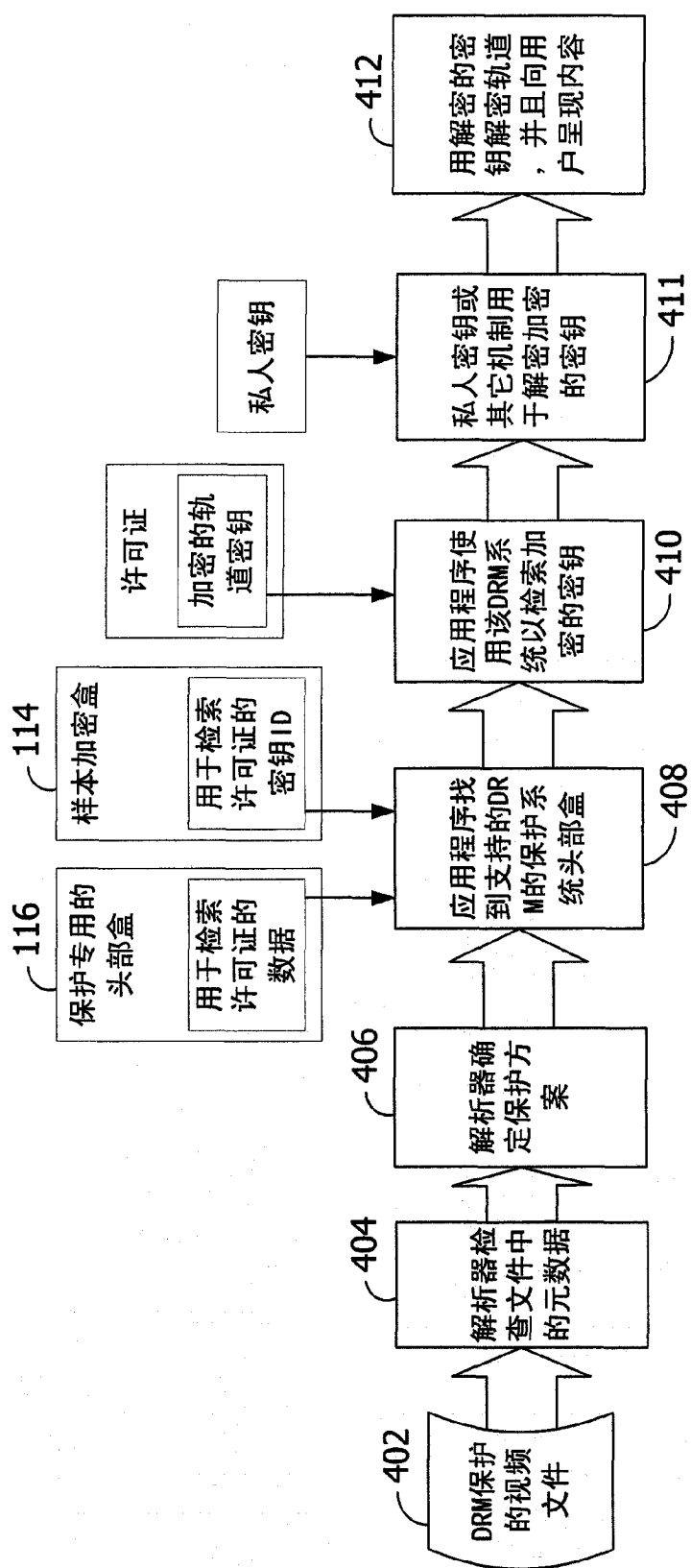


图 4

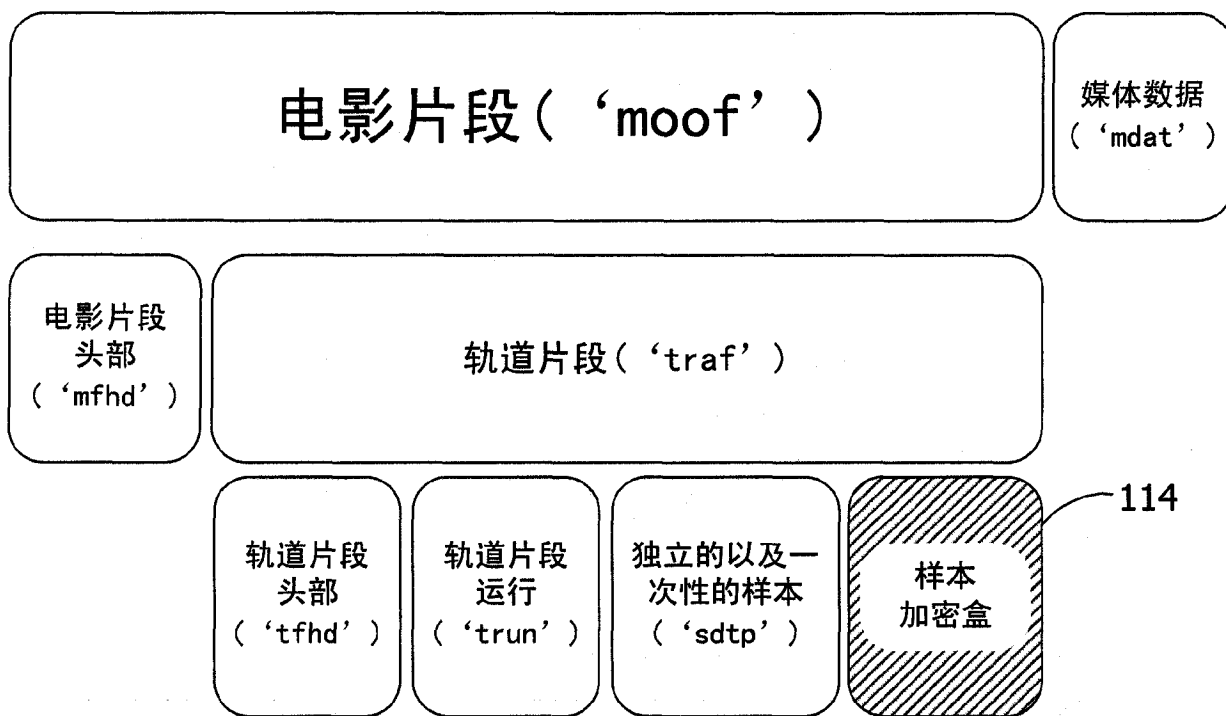


图 5

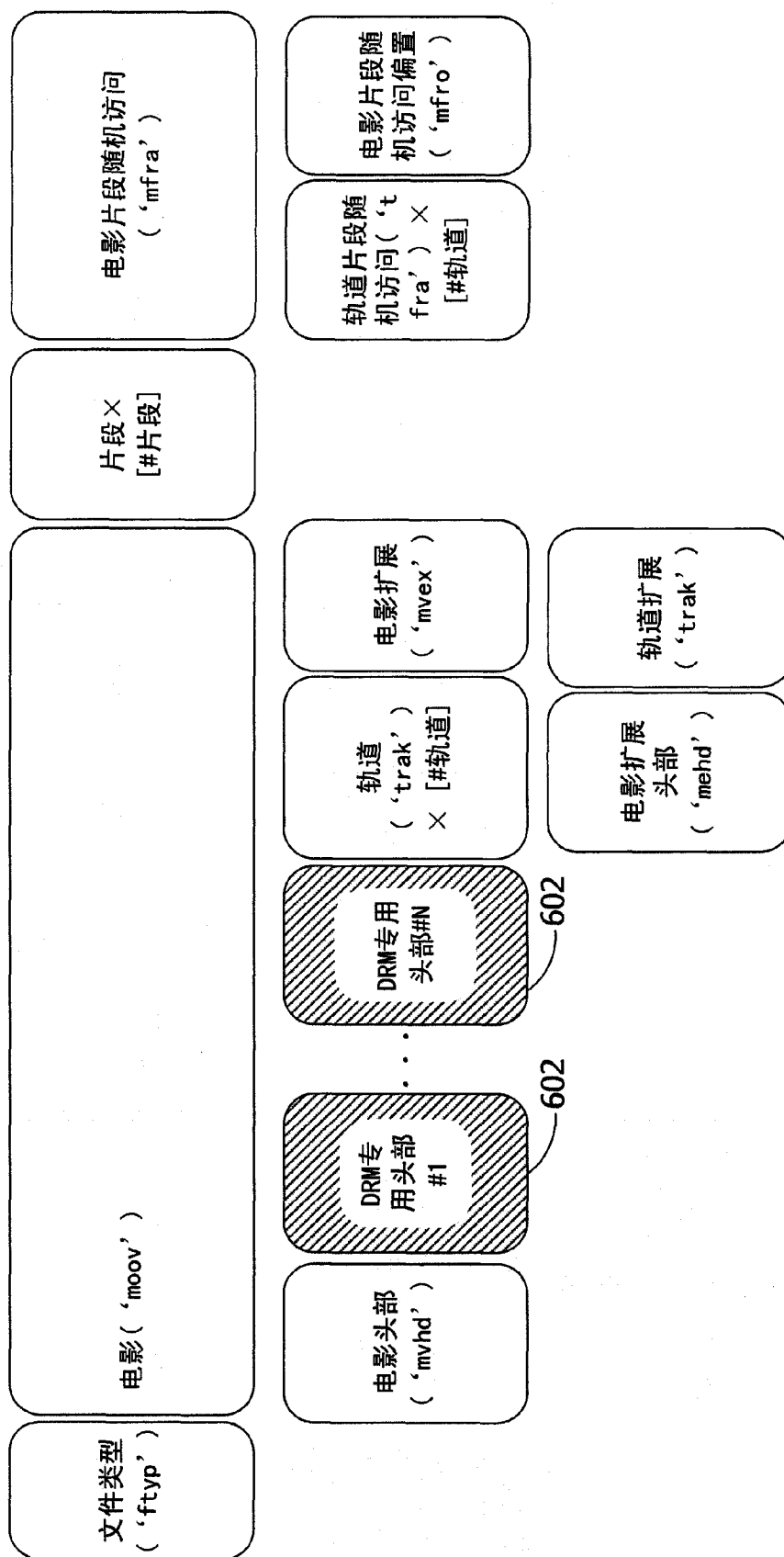


图 6

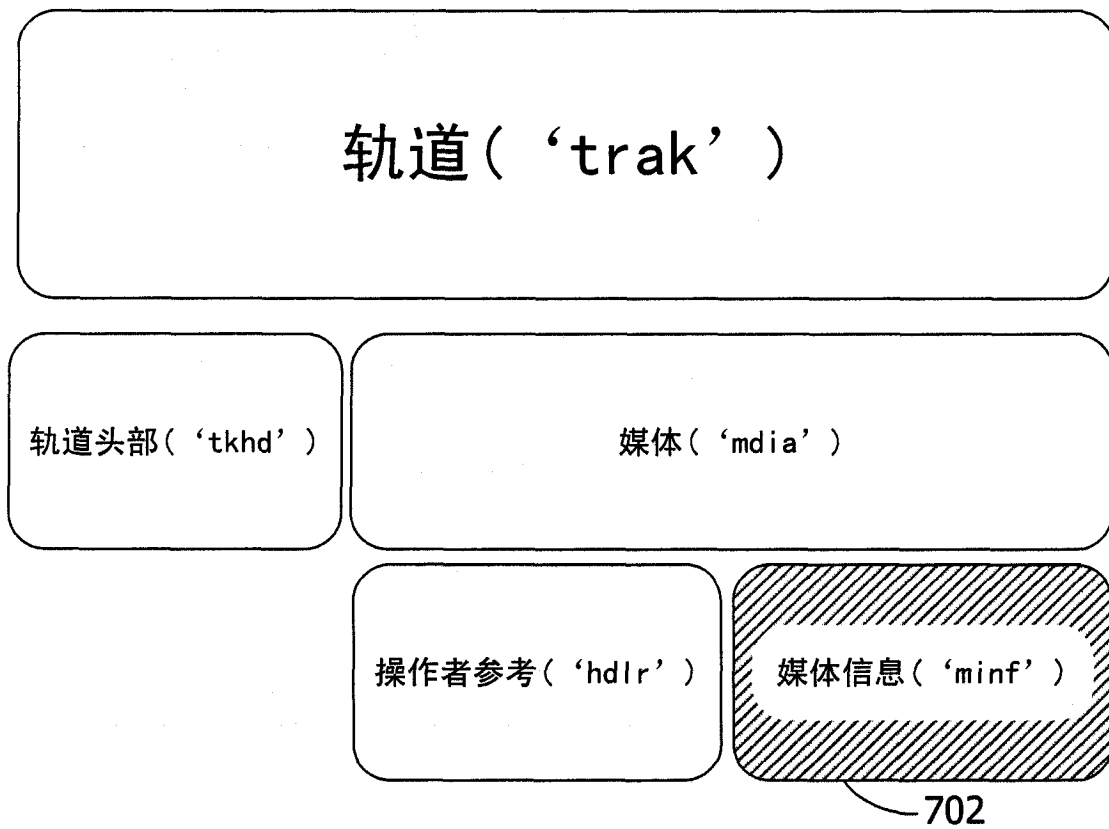


图 7

—702

媒体信息('minf')

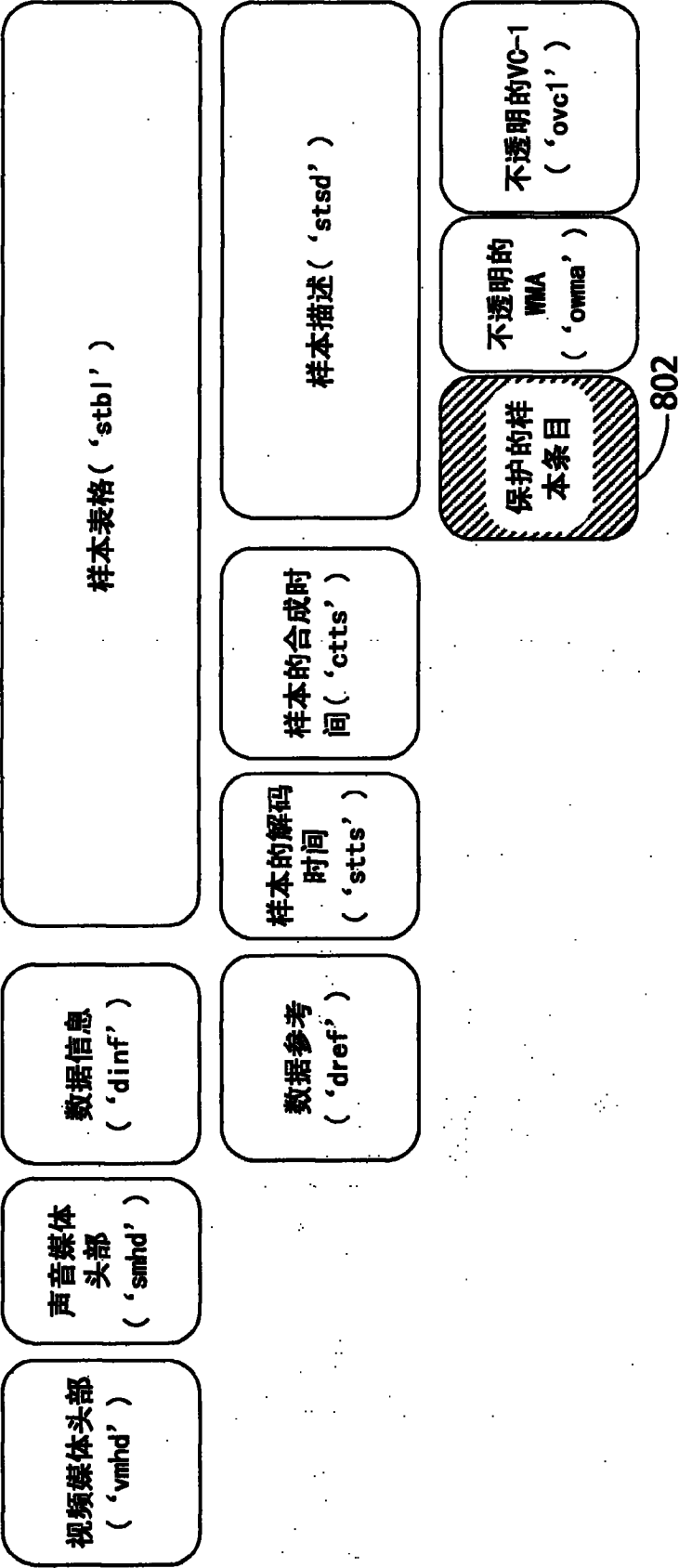


图 8

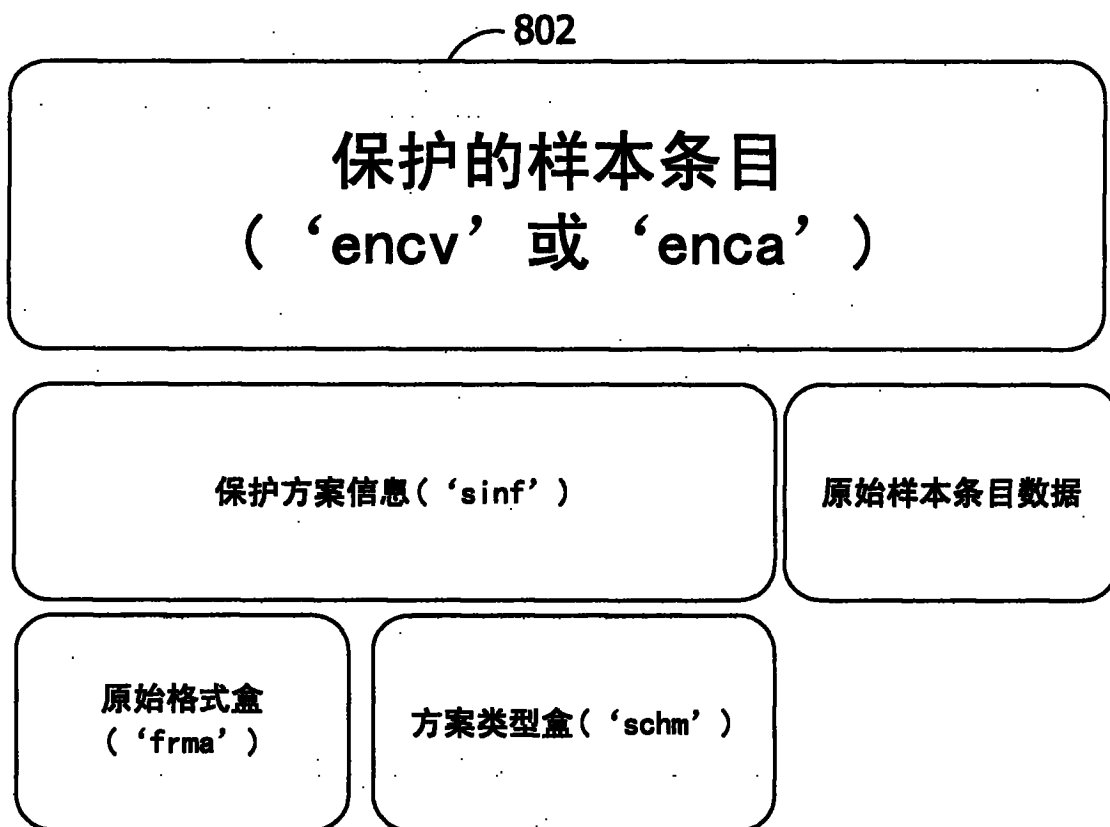


图 9