(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 1908922 B
(45)授权公告日 2012.11.07

(21)申请号 200610101464.7
(22)申请日 1997.05.15
(30)优先权数据
60/017722 1996.05.15 US
60/018132 1996.05.22 US
08/689754 1996.08.12 US
08/689606 1996.08.12 US
08/699712 1996.08.12 US
PCT/US96/14262 1996.09.04 US
60/037931 1997.02.14 US
(62)分案原申请数据
97196487.4 1997.05.15
(73)专利权人 英特托拉斯技术公司
地址 美国加利福尼亚州
(72)发明人 V·H·希尔 O·W·西伯特 D·M·范维 R·P·维伯
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张志醒
(51)Int.Cl.
G06F 13/14(2006.01)
G06F 12/14(2006.01)
G11B 20/10(2006.01)
H04L 9/00(2006.01)
(56)对比文件
WO 95/12179 A1,1995.05.04, 全文.
US 5502766 A,1996.03.26, 全文.
审查员 刘彤

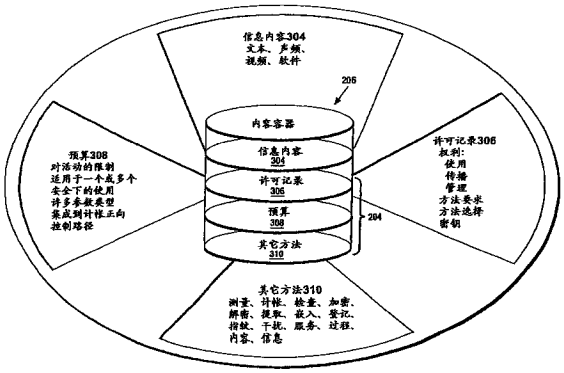
权利要求书 2 页 说明书 35 页 附图 21 页

(54)发明名称

获取DVD盘受控内容或信息的方法及装置、操作DVD设备的方法

(57)摘要

一种用于诸如数字光盘(DVD,也称数字通用盘)的存储介质的权利管理装置,它提供在有限的、大批生产、价格不贵、功能较低的平台-诸如专用的家庭光盘播放器-的充分的复制保护,并且在相同的介质被用于具有更安全的功能的平台时,提供增强的、更灵活的安全技术和方法。一个控制对象(或集)定义多个权利管理规则,例如演播的价格或再传播的规则。低功能的平台只能用控制规则的一个子集,诸如对播放材料的复制或标记的控制。更高级功能的平台能用规则的全部(或不同的子集)。提供保密性强的安全性的方法是,将介质含有的至少部分信息加密,根据控制集和/或其它限制能进行解密。一个安全的"软件容器"可用于保护性地封装(例如采用加密术)各种数字财产内容(例如视频、音频、游戏等等)和控制对象(例如规则集)信息。提供一个用于各种介质和平台的一般使用的标准化容器格式。此外,可以提供一个专用容器给包含DVD节目内容(数字财产)和DVD介质专用规则的DVD介质和设备(例如录制器、播放器等等)。本文披露的技术、系统和方法能兼容到其它保护标准,例如为DVD所采用的CGMA和Matsushita数据保护标准。也可以提供合作权利管理,其中多个连网权利管理装置联合地控制一个或多个这种装置上的一个权利管理事件。



CN 1908922 B

1. 一种用于存取、复制或使用便携式存储介质上存储的受保护的数字信息的电子设备，所述电子设备包括：

配置为从所述便携式存储介质读取受保护的数字信息的视盘驱动器；以及

以通信方式连接到所述视盘驱动器的抗破坏的安全处理单元，所述抗破坏的安全处理单元配置为从便携式存储介质中提取财产标识信息、找出适用的控制集、装入必要的解密密钥、根据需要而使用解密密钥来解密信息、监控用户的输入并根据与受保护的数字信息相关联的、存储在便携式存储介质上的控制集和额外的控制集来确定存储在便携式存储介质上的控制集和额外的控制集是否允许用户已经请求的动作，如果被允许并且在所有必要条件得到满足时，执行所请求的动作以便允许所述电子设备使用受保护的数字信息。

2. 如权利要求 1 所述的电子设备，其中，所述抗破坏的安全处理单元配置为获取所述便携式存储介质上存储的受保护的数字信息的标识信息，且其中所述抗破坏的安全处理单元连接到一个网络，并配置为至少部分基于所述标识信息通过所述网络从远程站点获得控制集。

3. 如权利要求 2 所述的电子设备，其中，所述远程站点包括权利与许可交换所。

4. 如权利要求 1 所述的电子设备，其中，存储在便携式存储介质上的控制集包括一个或多个允许记录、一个或多个预算和 / 或一个或多个方法、或者存储在便携式存储介质上的控制集提供一个或多个加密密钥、一个或多个内容标识符、以及一个或多个应用于不同设备和 / 或设备类的控制。

5. 如权利要求 1 所述的电子设备，其中用于对所述便携式存储介质上存储的一个或多个加密的内容解密密钥进行解密的一个或多个密钥被存储在所述视盘驱动器上。

6. 如权利要求 1 所述的电子设备，其中，所述控制集包括从下列组中选择的一个或多个控制：禁止复制所述受保护的数字信息的控制、只允许复制一次所述受保护的数字信息的控制、允许复制多次所述受保护的数字信息的控制、允许某用户或某类用户播放所述受保护的数字信息的控制和允许某用户或某类用户提取或摘录至少一部分所述受保护的数字信息的控制。

7. 一种存取、复制或使用便携式存储介质上存储的受保护的数字信息的方法，所述方法包括：

从电子设备的用户接收存取、复制或使用受保护的数字信息的请求；

利用所述电子设备的抗破坏的安全处理单元，从便携式存储介质中提取财产标识信息、找出适用的控制集、装入必要的解密密钥、根据需要而使用解密密钥来解密信息、监控用户的输入并根据与受保护的数字信息相关联的、存储在便携式存储介质上的控制集和额外的控制集来确定存储在便携式存储介质上的控制集和额外的控制集是否允许用户已经请求的动作，如果被允许并且在所有必要条件得到满足时，执行所请求的动作以便允许所述电子设备使用受保护的数字信息。

8. 如权利要求 7 所述的方法，其中，存储在便携式存储介质上的控制集包括一个或多个允许记录、一个或多个预算和 / 或一个或多个方法、或者存储在便携式存储介质上的控制集提供一个或多个加密密钥、一个或多个内容标识符、以及一个或多个应用于不同设备和 / 或设备类的控制。

9. 如权利要求 8 所述的方法，其中，控制允许复制一次所述受保护的数字信息用于备

份。

10. 如权利要求 9 所述的方法，其中，访问、复制或使用受保护的数字信息的请求是复制所述受保护的数字信息的请求，所述方法还包括：

确定所述控制允许复制所述受保护的数字信息；

对所述受保护的数字信息进行复制。

11. 一种存取、复制或使用可移动存储介质上存储的受保护的数字内容项的方法，所述方法包括：

在电子设备的驱动器中容纳所述可移动存储介质，所述可移动存储介质存储所述受保护的数字内容项和提供一个或多个控制的控制集，所述控制规定复制一次或禁止复制所述受保护的数字内容项的用法；

从可移动存储介质中提取隐藏的密钥；

存储所述密钥使得解密时不会将所述密钥暴露给所述电子设备；

读取所述控制集；

对所述控制集进行分析；

忽略所述电子设备不能实施的至少一个控制；

维护与所述电子设备能够实施的至少一个控制相对应的允许和 / 或权利管理信息；以及

接收来自用户的请求，

如果所述请求是复制请求，则查询控制来判断是否允许复制，如果被允许，则执行复制存储在可移动存储介质上的受保护的数字内容项，

如果所述请求是使用请求，则从可移动存储介质中读取对应的信息并且根据需要使用所述密钥来解密所读取的信息。

12. 如权利要求 11 所述的方法，其中，所述请求包括复制所述受保护的数字内容项的请求，并且其中所述电子设备能够实施的至少一个控制包括规定能够复制所述受保护的数字内容项的控制，所述方法还包括：

对所述受保护的数字内容项进行复制。

13. 一种电子设备，包括：

用于读取便携式存储介质上存储的受保护的数字信息的视盘驱动器 (80′)；

用于从电子设备的用户接收存取、复制或使用受保护的数字信息的请求的用户接口 (66,68)；

抗破坏的安全处理单元 (72 或 164)，被配置为从便携式存储介质中提取财产标识信息、找出适用的控制集、装入必要的解密密钥、根据需要而使用解密密钥来解密信息、监控用户的输入并根据与受保护的数字信息相关联的、存储在便携式存储介质上的控制集和额外的控制集来确定存储在便携式存储介质上的控制集和额外的控制集是否允许用户已经请求的动作，如果被允许并且在所有必要条件得到满足时，执行所请求的动作以便允许所述电子设备使用受保护的数字信息；以及

向所述用户呈现所述受保护的数字信息的显示器。

获取 DVD 盘受控内容或信息的方法及装置、操作 DVD 设备的方法

[0001] 本申请是 2002 年 12 月 31 日提交的申请号为 02160594.7、发明名称为" 获取 DVD 盘受控内容或信息的方法及装置、操作 DVD 设备的方法"的中国专利申请的分案申请。

[0002] 有关申请和专利的交叉引用

[0003] 本说明书引用下述在先的、普通转让的公开专利的说明书和附图。

[0004] PCT 公开号 WO96/27155,提交日期为 1996 年 9 月 6 日,名称为" 于安全交易管理和电子权利保护的系统和方法",这是基于 1996 年 2 月 13 日提交的 PCT 申请 PCT/US96/02303 和 1995 年 2 月 13 日提交的 Ginter 等人的美国专利申请(系列号为 08/388107)(以下称为 Ginter 等人的专利);

[0005] 美国专利号 4827508,名称为" 法",提交日期为 1989 年 5 月 2 日;

[0006] 美国专利号 4977594,名称为" 法",提交日期为 1990 年 12 月 11 日;

[0007] 美国专利号 5050213,名称为" 法",提交日期为 1991 年 9 月 17 日;

[0008] 美国专利号 5410598,名称为" 法",提交日期为 1995 年 4 月 25 日;

[0009] 欧洲专利号 EP329681,名称为" 法",提交日期为 1996 年 1 月 17 日。

[0010] 此外,本说明书引用下述在先的、普通转让的公开专利的说明书和附图。

[0011] PCT 申请号 PCT/US96/14262,提交日期为 1996 年 9 月 4 日,名称为"

[0012] 式计算以及权利管理的受托基础结构支持系统、方法和技术",它对应于 1996 年 8 月 12 日提交的美国专利申请系列号 08/699712(以下称为 Shear 等人的);

[0013] PCT 申请号 _____,提交日期为 1997 年 ___ 月 ___ 日,名称为" 于在不安全通信通道上安全地传递电子数字权利管理控制信息的隐蔽 式(steganographic)技术",它对应于 1996 年 8 月 12 日提交的 Van Wie 和 Weber 等的美国专利申请系列号 08/689606(以下称为 Van Wie 和 Weber 等人的);以及

[0014] PCT 申请号 _ _ _ _ _ _ _ _ _,提交日期为 1997 年 _ _ 月 _ _ 日,它基于 1996 年 8 月 12 日提交的 Silbett 和 Van Wie 等人的美国专利申请系列号 08/689754,名称为"用加密术保护安全计算环境的系统和方法"(以下称为 Silbert 和 Van Wie 等人的)。

技术领域

[0015] 本发明涉及采用加密术的信息保护技术,更具体来说涉及用加密来管理对便携式介质上存储的信息的权利的技术 - 便携式介质例如是光学介质,诸如数字视盘(亦称"数字多用途盘"和或"DVD")。本发明也涉及根据例如是消费者使用的设备资源(例如个人电脑或独立播放机)、设备的其它属性(诸如是否可以连接和 / 或一般连接着某个信息网络("连接"相对于"未连接"))、以及可用的权利具有可选择应用的信息保护和权利管理技术。本发明进一步部分涉及合作权利管理 - 其中多个联网权利管理设备联合控制一个或多个这种设备上的一个权利管理事件。此外,采用了本发明的重要方面的权利管理,适用于通过广播和 / 或网络下载、和 / 或用 - 无论是与便携式介质独立的还是与便携式介质组合的 - 非便携式存储介质而获得的电子信息。

背景技术

[0016] 能够播放预录制介质中的视频 / 音频的家庭消费电子设备已经使娱乐业得到转变。这种转变是在 20 世纪初由于留声机的发明而开始的 - 留声机首次使消费者得以在家中选择随意的时间收听其喜爱的乐队、管弦乐队或歌手的节目。80 年代初开始有价格不贵的盒式录 / 放机，这引起了电影和广播业的一次深刻变革，产生了崭新的电影、记录片、音乐影视片、体育锻练影视片等家庭消费市场。

[0017] 娱乐业一直在追求向家庭消费者传播内容的最佳介质。由托马斯 . 爱迪生以及其它留声机先驱发明的早期留声机柱面具有复制困难的优点，但是存在各种缺点，例如制造成本高、抗破裂强度低、回放时间非常有限、回放质量相对较低、易受磨损、擦刮或熔化的损害。后来开发的蜡盘和乙烯树脂唱盘能容纳更多音乐，但还是有许多与上述相同的缺点。另一方面，磁带的制造成本很低，能容纳大量的节目内容 （例如 2、4 甚至 6 小时的影像和 / 或声音）。这种磁带再现节目内容的质量相对较高，不易损坏或磨损。然而，尽管磁带比其它介质有许多明显优点，娱乐业却从未将其视为一种理想或最佳介质，原因在于其非常容易复制。

[0018] 磁带有非常灵活的特性，在于录制磁带比较容易。确实，录制磁带的过程近乎与回放预录内容一样容易。由于录制磁带相对容易，所以家庭消费磁带设备制造商一直提供具有双重模式的设备，既能录制磁带又能回放磁带。所以，家庭录音机和录象机传统上都有一个“录制”按钮，允许消费者在空白磁带上录制其自己的节目内容。尽管这种录制功能给予消费者更多的灵活性（例如，能记录幼儿最早说出的话语供下一代以后听，能录制下午播出的肥皂剧供晚上看），但不幸的是，这也是盗版业的温床，非法盗版业每年生产的非法仿制磁带有数百万，涉及金额有数十亿美元。这种非法盗版活动的范围是国际性的，每年都从世界主要娱乐内容制造商手中攫取了巨大的利润。娱乐业必须将这些损失转嫁到诚实的消费者头上，结果导致票房价格更高，录像带和录音带的售价和租金更高。

[0019] 80 年代中期，音频娱乐业开发了光盘，作为对某些这类问题的一种回应。光盘是一种直径数英寸的银色塑料薄盘，能以数字格式存储一个小时或更长时间的音乐或其它音频节目。这类光盘后来也被用于存储计算机数据。这种盘制造成本可以很低，由于采用数字技术记录和恢复信息，所以抗噪音，回放质量极高。由于光盘可用塑料制成，所以重量轻，不易折断，很能容忍用户正常使用造成的损伤（不像以前的乙烯树脂唱片那样，容易刮坏，甚至受到正常操作的留声机的磨损）。并且，由于迄今录制光盘比回放光盘的难度更大，所以，家庭消费设备要具备录制和回放双重功能，同时费用效能与只能回放的设备一样合算，近期还不可能，从而大大减少了非法复制的可能性。由于这些无可比拟的优点，音乐产业已经迅速地接受了这种新的数字光盘技术 - 在短短几年内几乎替换了老的乙烯树脂唱片。

[0020] 确实，由于没有权利管理技术，非授权的复制行为简单容易，广泛流行，这种威胁很明显是导致数字录音磁带 (DAT) 作为音乐传播的介质 - 更重要的是作为家庭录音的介质 - 走向消亡的一个重要因素。录制音乐的权利拥有者强烈反对缺乏权利管理功能的廉价 DAT 技 术的广泛商业化，这是因为数字录制完全忠实于在例如音乐 CD 上的数字源。当然，缺乏权利管理并非是唯一起作用的因素，因为与光盘相比，磁带格式使随机访问困难，例如不按顺序地播放歌曲。

[0021] 视频娱乐业面临着一场与音乐 CD 导致的类似的变革，其基础是在大容量只读式光学介质上分布的数字格式电影。例如，数字光盘技术已经发展到这样的地步，现在除了可以数字化地录制其它信息之外，还可以将一部电影的全部画面（加上伴音）数字化地录制在一张 5 英寸塑料光盘的一面上。同样的光盘也能容纳多个高质量数字声道（例如，录制家庭影院的多声道“环绕”声和 / 或在同一张光盘上录制多种语言的电影对白）。同样的技术使访问电影的个别帧或画面以再现静态图像成为可能，更令人激动的是，它提供了一种前所未有的“随机访问”回放功能，以前的家庭消费设备从未有过这种功能。这种“随机访问”回放功能可用于例如在回放时删除暴力、秽语或裸体内容，使得孩子的父母们按个按钮就能选择一个“R”级影片的“PG”回放版本。“随机访问”功能在允许观众与预先录制内容交互作用方面（例如允许健身爱好者只选择健身影视片中有助于特定某天锻练的那部分内容）也有令人激动的可能。这方面内容例如可阅读 DVD 大会报告汇编中的《新视频程序设计的应用要求》一文（该大会由交互多媒体协会举办，日期 :1995 年 10 月 19 ～ 20 日，地点 :美国加州 Universal 城的 Sheraton Universal 饭店）。

[0022] 光学介质的 DVD 系列产品的部分例子 :

[0023] ● DVD（数字视盘、数字多用途盘），其一个非限定性例子包括能播放 DVD 盘上录制的电影的消费设备 ;

[0024] ● DVD-ROM(DVD 只读存储器），其一个非限定性例子包括与计算机或其它设备相连的一个 DVD 只读驱动器和盘 ;

[0025] ● DVD-RAM(DVD 随机存取存储器），其一个非限定性例子包括一个读 - 写驱动器和光学介质，安装在例如用于家庭录制节目的消费设备中和计算机或用于特定应用的最广范围的其它设备中 ;

[0026] ●当前已知或未知的任何其它大容量光学介质。

[0027] 当然，DVD 系列并非限于用在电影上。与 CD 系列一样，它们也可以用于存储其它种类的信息，例如 :

[0028] ●录音

[0029] ●软件

[0030] ●数据库

[0031] ●游戏

[0032] ●卡拉 OK

[0033] ●多媒体

[0034] ●远程教育

[0035] ●文献

[0036] ●政策和手册

[0037] ●任何种类的数字数据或其它信息

[0038] ●各种数字数据或其它信息的任意组合

[0039] ●任何当前已知或未知的其它用途。

[0040] DVD 用途范围的广泛提出了一个技术挑战 :在这类 DVD 盘上传播的信息内容 - 可能是任何种类的影像、声音或广义来说其它数据或信息，或是它们之间的任何组合 - 如何能够得到充分的保护，与此同时保留、甚至最大程度地提高消费者的灵活性？对新技术

（主要是在影象方面）提出的广泛要求是，就允许复制的程度而言，要么 (a) 允许消费者对节目内容作一级拷贝，留作自用，但禁止消费者制作“拷贝的拷贝”，即对给定的财产作多代拷贝（这样使诚实者保持诚实），要么 (b) 允许对权利所有者不希望复制保护的、或者消费者自己制造的财产作无限制的拷贝。

[0041] 然而，仅仅以不可延伸的方式提供这种简单而有限的复制保护，可能是很目光短浅的－因为不管现在或将来，更加复杂的保护和／或权利管理目标会非常有用（例如：更健全和选择性地应用复制保护技术以及其它保护技术，实现付费观看方式，消费者能够利用增强功能，诸如支付额外费用就能提取节目内容或者交互式地观看节目、接受再传播的信用等等）。此外，在最佳地解决保护和权利管理目标时，例如，根据可用的设备资源和／或设备联网还是不联网，区分并认真对待与通过 DVD 介质提供信息相关的商业机会和成胁是极其有用的。

[0042] 更复杂的权利管理功能也将允许声像制作所和其它的电影和／或唱片的权利所有人更好地管理这些资产，例如，允许被授权方复制数字电影、声像作品－无论是专门的还是任选的作品，用于创作衍生作品，其中例如多媒体游戏。迄今为止提出的保护 DVD 内容的解决方案一般 只是集中在有限的版权保护目标上，未能充分涉及、甚至没有认识到更复杂的权利管理目标和要求。更具体来说，有一种用于 DVD 设备和介质的初始生成的版权保护方案，其基础是最初由 Matsushita 公司开发的一种加密方法和简单的 CGMA 控制代码，后者指明允许的复制类型有：一代复制、不得复制、无限复制。

发明内容

[0043] 要全面解决包括了诸如 DVD 的大容量光学介质的系统中的信息保护和管理问题，其中要求有能解决下述两大类问题的方法和系统：(a) 数－模转换（或相反）；(b) 在联网和不联网的环境中使用这类光学介质。本文披露的发明涉及这些问题和其它问题。例如，就模一数转换（或相反）而言，根据本发明，设想至少有一些用于保护财产和／或描述权利管理和／或控制信息的数字形式的一些信息也可以用模拟信号来传输。例如，从一种格式和／或介质向另一种格式／介质作转换的设备，包含新的上下文中的某些或全部控制和标识信息，或者至少在转换过程中不主动删除这种信息。此外，本发明提供一般提供数字领域的控制、权利管理和／或标识解决方案，并且还提供可在用户设备、计算机以及其它设备中实施的关键重要技术。本发明的一个目的是，提供既在消费电子市场有用又在计算机市场有用的强大的权利管理技术，并且还使将来的技术能力和商务模型演变成为可能。另一个非限定性目的是，提供一种与现有的用于有限功能复制保护和用于加密的工业标准尽可能兼容的，全面的控制、权利管理和／或标识解决方案。

[0044] 本发明提供的权利管理和保护技术，完全满足当前娱乐业要求的对电影的有限复制保护目标，同时还具有灵活性和可扩展性，可以适应范围广泛的更复杂的权利管理选择方案和功能。

[0045] 本发明的一些重要方面（本申请中将另外予以更详细的讨论）包括：

[0046] ●选择与 DVD 介质上记录的信息关联的控制信息（例如规则和使用后果控制信息，其包含非限定性的虚拟传播环境 (VDE) 的要素例），其至少部分基于设备的类别，例如设备的类型、可用资源和／或权利；

[0047] ●允许这类选择控制信息至少部分是在其它设备和/或设备类上所用的控制信息的一个子集，或者是完全不同的控制信息；

[0048] ●保护从DVD设备输出的信息，诸如将Ginter等人的及本申请所披露的权利管理技术应用到在DVD播放器上用IEEE1394端口（或其它串行接口）传输的信号；

[0049] ●在模拟源的基础上创建受保护的数字内容；

[0050] ●反映世界上不同国家和/或地区的不同的使用权利和/或内容可用性；

[0051] ●可靠地管理DVD介质上的信息，使得某些部分可以在一类或多类设备（例如独立的DVD播放器）上使用，而其它部分可以在相同或不同类别的设备（例如独立的DVD播放器或个人电脑）上使用；

[0052] ●可靠地存储和/或传输与付费、检查、控制和/或管理DVD上存储的内容相关的信息，包括与在Ginter等人和Shear等人的专利中所披露的有关的技术；

[0053] ●更新和/或替换在设备操作过程中使用的加密密钥，以修改设备和/或设备类所能使用的信息的范围；

[0054] ●在创建、传播和使用的全部过程中保护信息，其方法例如是，初始保护由数字摄相机采集的信息，在编辑、生产、传播、使用和使用报告的全部过程中继续实行保护和权利管理。

[0055] ●允许由参加并在永久连接的网络或暂时连接的网络中共同工作的多个设备和/或其它系统组成的“虚拟权利机”共享单一和/或多个节点的一些和/或全部权利管理，例如，允许多个这种设备和/或其它系统中的可用资源，以及/或者与使用和/或控制这种设备和/或其它系统的多个当事人和/或组织关联的权利，被应用于音乐会（根据与权利相关的规则和控制），以便管理这种设备和/或其它系统中任何一个或多个上的一个或多个电子事件，这种事件管理例如包括：观看、编辑、分类、编纂、打印、复制、命名、摘选、保存和/或再传播受权利保护的数字内容。

[0056] ●允许对等的设备和/或其它系统之间权利的交换，其中设备和/或其它系统加入永久或暂时连接的网络，并且其中这种权利的交换方式是易货交易的、货币买卖的，以及/或者以价值和/或报酬交换的－其中这种价值和/或报酬是在对等的参加网络的商业和/或消费设备和/或其它系统之间交换的。

[0057] 通用DVD/成本－效用适宜的大容量数字介质权利保护和管理

[0058] 本文描述的本发明可用于商业和/或消费数字信息的提供采用效用－成本适宜的传播介质的任何大容量存储装置，本文所述的DVD应被理解为包括任何这类系统。

[0059] 复制保护和权利管理在实际的DVD系统中是重要的，并且，将来在当前已知或未知的其它大容量存储、回放和录制系统中依然是重要的。提供（或写）在多数DVD介质上的信息有些或者全部都需要保护。这种防复制保护只是权利管理的一个方面。其它方面包括允许权利持有者和其他人管理他们的商业利益（并在潜在的一个时间和/空间距离使它们实现），无论是什么传播介质和/或渠道，也无论接收设备的特定性质如何。这种结合DVD的权利管理解决方案，随着将来一代代可读DVD介质和设备的问世，将变得更加重要。在市场上可以选择录制设备的情况下，以及例如录象、录音和其它数字财产就会从一个设备传输到另一个设备时，此时，权利持有者将希望维护并提出他们的权利。

[0060] 消费设备与计算机的明显结合，网络和调制解调器速度的提高，计算机能力和带

宽的费用的下降，以及光学介质容量的增加，这些因素结合起来创造了一个混合商务模式的世界，在这个世界中，所有各种数字内容都可以在至少偶尔连接的设备和／或计算机上播放的光学介质上传播；在这个世界中，音乐 CD 和初始 DVD 电影销售中常见的一次性购买模式，得到其它模式的补充，后者例如租赁、付费观看、先租后买，等等。消费者可以从同一个或不同的分销者或者其他提供者对这些以及其他模式进行选择。使用费可以在网络和／或连接某种付费清算业务的其它通信渠道上支付。消费者的使用和检查信息可以回流到开发者、分销者和／或其它参与者。现在引入的用于 DVD 的基本复制保护技术不能支持这些和其它复杂模式。

[0061] 随着可写 DVD 设备和介质在市场的出现，其它混合模式也是可能的，例如包括通过卫星与电缆系统传播数字电影。在录制一个电影后，消费者可以选择租赁、租借、付费观看或其它可能的合适模式。随着数字电视的问世，可写 DVD 忠实复制空中节目的能力产生了其它可能的模式和／或权利管理要求。对此，当前为初始只读 DVD 技术而应用的简单的复制保护机制，同样不能满足需要。加密是手段，不是目的

[0062] 加密适用于保护数字格式的知识财产，无论是 DVD 之类的光学介质、磁盘驱动器之类的磁介质、数字设备的活动存储器中，还是正通过计算机、电缆、卫星或其它种类的网络或传输工具传输的知识财产。过去，加密技术由于发送秘密信息。对于 DVD 来说，加密的一个主要目的是要求使用一种复制控制和权利管理系统，以确保只有被权利持有者授权的人才确实能使用加密了的内容。

[0063] 但是，加密与其说是目的，不如说是手段。中心问题是如何设计出方法，在尽可能最大的程度上，保障只有被授权设备和当事人才能解密受保护的内容，以及／或者用其它方法只在权利拥有者和／或受保护内容的其它有关当事人允许的范围内使用信息。

[0064] 本发明提供了强大的权利管理功能。根据本发明提供的一个方面，可以将加密的数字财产存放在 DVD 上的一种抗破坏的软件“容器”中，例如“Digibox”安全容器中，一起存放的还有可以应用和由消费设备实施的关于“不得复制”和／或“复制”和／或“允许复制的次数”的规则。这些相同的规则和／或更灵活和／或不同的规则，可以由计算机设备或其它系统实施，提供更多和／或不同的功能（例如编辑、摘选、一种或多种付费方法、（增加的存储用于详细检查信息的容量等等）。此外，例如“Digibox”安全容器的“软件容器”能存储一定的明文（即不用加密格式的）内容。例如，电影或音乐标题、版权声明、音响样本、电影预告和／或广告都可以明文地存储，并且／或者可由任何适当的应用或设备播放出来。这种信息当提供用于观看、复制和／或其它活动时为了真实性可以被保护。同时，各种有价值的数字财产一电影、影像、图像、文本、软件和多媒体可以至少是部分加密存储的，只能由被授权设备和／或应用使用，只能在被许可（例如经权利所有者同意后）的情况下使用。

[0065] 根据本发明提供的另一个方面（结合 Ginter 等人专利中披露的一些功能）是，DVD 盘上同一个“容器”内可以存储多个规则集。软件然后根据具体情况应用这些规则，具体情况是：例如电影是被消费设备还是计算机播放，特定设备是否有后通道（例如在线连接），播放器位置和／或电影被播放所在的国家和／或其它法律或地理地区，以及／或者设备是否含有能识别并应用这种规则的部件。例如，当信息由消费设备播放时，有些使用规则适用，而当由计算机播放时，其它使 用规则适用。规则的选择取决于权利所有者和／或其它参与者－或者，有些规则可以预先规定（例如根据特定环境或应用来预定）。例如，电影

权利所有者会希望限制复制，保证内容不被摘录，不管该财产所处的是什么情况。这种限制可能只在一定的法律或地理地区应用。另外的办法是，声响制品的权利所有者会希望允许节录预定长度（例如 20 秒内）的内容，这些节录不得用于制作新的商业作品。在有些情况下，政府会要求只有“PG”版的电影和 / 或对等级的电视节目才能在政府辖区内的设备上播放，并且 / 或者如果对 DVD 上录制的内容要求和 / 执行收费的话（例如电影、游戏、数据库、软件产品等的使用付费；和 / 或根据至少部分在 DVD 介质上存储的目录的订单，等等），适用的税费、使用费等等要自动计算和 / 或收取。

[0066] 在微处理器控制下的（或增强的）数字消费设备中，本发明涉及的这种规则的实施，例如只需对中央、控制处理器（或其它 CPU、IEEE1394 端口控制器或其它内容处理控制电路）增加少许设备，和 / 或利用一些 ROM 或快速内存来存储必要的软件。此外，每个 ROM（或能可靠地连接到或集成到是单一制造件的这种控制电路的快速内存或其它内存）例如能存储一个或多个能唯一地标识特定设备、个人身份、管辖区域、设备类和 / 或其它选定参数的数字文件或“证书”。设备例如能被编程为只能将数字财产的复制件以加密格式给另一个数字设备，并只能放置在新的抗破坏的“软件容器”中。容器例如也能带有一个表示现在所发送的是一个复制件而不是原件的代码。设备也可以将接收设备和 / 或设备类的独有的标识符放入相同的安全容器中。结果，例如在一个特定安排中，该复制件只有在欲接收的设备、设备类和 / 或特定地区的设备上是可以播放的，有关使用该复制件的权利会根据这些和 / 或其它变量而不同。

[0067] 接收设备在检测到该数字财产确实是复制件时，例如能被编程为不制作能在消费设备和 / 或其它设备类上播放的其它复制件。如果设备检测到要播放数字财产的设备和 / 或设备类不是原来打算播放的设备，它能被编程为拒绝播放该复制件（如果希望的话）。

[0068] 消费设备中应用的相同规则例如能在具备了提供按照本发明的权利管理保护的计算机上实施。本例中，规则可以规定不得在例如不是消费设备和 / 或设备类的任何设备上播放一定的电影和 / 或其它内容。另一种办法是，这种强大的功能可用于按权利所有者的愿望，规定在计算机上（和 / 或在其它设备和 / 或设备类中）播放时适用的不同使用规则和付费方案，例如根据播放内容所在的不同地理或法律区域进行差别定价。

[0069] 此外，如果有“后通道”(backchannel)- 例如具有双向通信的机顶盒或者附接到网络的计算机 - 本发明考虑如果需要或要求的话对于给定财产的新规则的电子的独立传递。这些新规则例如可以规定折扣、时间有限的销售、广告补贴和 / 或其它需要的信息。前文说过，这些独立传递的规则的确定完全取决于权利所有者和 / 或给定模式中的其它人。

[0070] 下面是关于上述本发明的几个方面的两个具体例子：

[0071] 1. 模拟 - 数字复制的例子

[0072] (a)Bob 有一盘买来（或租借）的 VHS 录像带，他想拷贝一份留作自用。该模拟电影的复制控制代码是内嵌式的，不防碍信号的质量。Bob 有一台可写的 DVD 设备，该设备的配备能提供根据本发明的权利管理保护。Bob 的 DVD 记录器检测到模拟信号中内嵌的控制代码（例如这种记录器可以检测到含有与权利相关的控制和 / 或使用信息的水印和 / 或指纹），创建一个新的安全容器来存放内容规则和描述编码电影，并创建新的控制规则（和 / 或传递到一个安全 VDE 系统以存储并报告某些与使用历史有关的信息，诸如用户姓名、时间等等），所根据的是其检测到的模拟控制代码和 / 或其它信息，它们然后被存放在

Digibox 和 / 或诸如安全数据库的安全 VDE 设备数据存储器中。Bob 随时都能在其 DVD 设备上回放该复制件。

[0073] (b)Bob 将其录制的 DVD 盘给 Jennifer，后者想在带 DVD 驱动器的计算机上播放该盘。她的计算机的配备能提供根据本发明的权利管理保护。她的计算机打开 Digibox，检测出正在使用该复制盘的设备不是记录该盘的设备（因此是未授权的设备），于是拒绝播放该复制盘。

[0074] (c)Bob 再次将其该 DVD 盘给 Jennifer，但后者这一次通过电子方式与制订新规则和使用后果的有关人士取得了联系，该有关人士可能是制片商、分销商和 / 或权利和许可交换站（或者也可能她已经具有了足够的权利来用其播放器播放该复制盘）。有关人士向 Jennifer 发送一个 Digibox 容器，上面载有的规则和后果允许她在其计算机上播放该电影，同时要向她收费，尽管该电影是由 Bob 而不是由制片商或其它价值链参与者录制到 DVD 的。

[0075] 2. 数字—模拟复制的例子

[0076] (a)Jennifer 下班回家，将一盘租借的或自有的 DVD 插入一台与电视相连或者与电视集成的播放器，播放该盘。电影以完全透明的方式被解密，格式由数字转换成模拟，在其模拟电视上显示出来。

[0077] (b)Jennifer 想拷贝一份留作自用。她在含有根据本发明的权利管理保护的 DVD 设备上播放该电影。该设备打开 Digibox 安全容器，访问控制信息，解密该电影。她在盒式磁带录像机上记录模拟信号，得到一个高质量的复制件。

[0078] (c)Jennifer 将该 VCR 拷贝给 Doug，后者希望用该模拟带复制一份自用，但是模拟控制信息使进行复制的 VCR 复制的质量很低，或者不能复制。在另一个非限定性例子中，可以将更全面的权利管理信息编码在模拟输出中，方法是采用上文引用的 Van Wie 和 Weber 专利申请中更详细描述的方法和 / 或系统。

[0079] 根据本发明提供的一个方面，同样的便携式存储介质，例如 DVD，可用于一系列不同的、有一定保护的环境，提供不同的保护功能。每个不同环境都能根据该特定环境所支持的权利管理技术和 / 或功能，使用便携式存储介质中携带的信息。例如，结构简单、价格不贵的家庭消费的盘播放器可以支持复制保护，无需涉及播放器本身功能达不到的较复杂的内容权利。技术功能更强和 / 或更安全的平台（例如可能由网络连接支持的含有安全处理部件的个人电脑，或者“更聪明”的设备），例如可以使用相同的便携式存储介质，并根据更复杂的权利管理技术（例如要求支付额外使用费，提供摘录或选编的选定内容部分的安全提取，等等），提供与介质所含内容的使用相关的增强的使用权利。例如，与便携式存储介质关联的控制集可以适应各种不同的使用功能一越高级或复杂的使用相应地要求只有某些平台才有而其它平台没有的、越高级的保护和权利管理。作为另一个例子，低功能的环境可以忽略（或不启动或不试图使用）控制集中它们不明白的权利，而高功能的环境（它们清楚自己具有的全部功能）例如可以启动被低功能的环境所忽略的权利和对应的保护技术。

[0080] 根据本发明提供的另一个方面，可以对一个独立于介质和平台的安全部件的功能和性能加以伸缩，使得消费电子设备的基本权利管理要求是能应用于更高级平台的一组更丰富功能的子集。该安全部件既可以是一个物理的、硬件部件，也可以是部件的“软件模拟”。根据这个特点，一个介质实例（更确切地说，一个与介质无关的内容版本）能被传递

顾客，不管他们的设备或平台类型如何，内容肯定将得到保护。安全和/或技术功能方面较不高级的平台可以只提供有限的使用内容的权利，而更高级平台则可以根据相应适当的安全条件和安全措施而提供更扩展的权利。

[0081] 根据本发明提供的另一个方面，大批生产、价格不贵的家庭消费的DVD播放器（诸如那些例如构造复杂性最少和组件数最少的播放器），可被改造得与较强和/或安全平台（例如个人电脑）所用的相同的DVD或其它便携式存储介质兼容，而不降低该存储介质与更高级和/或安全平台的结合能提供的高级权利管理功能。根据本发明提供和支持的权利管理和保护装置，于是支持价格不贵的基本复制保护，并能进一步作为商业趋同技术，支持允许根据相同内容的权利的使用由有限资源消费设备的跨接，同时，通过(a)有用于安全权利管理的更大资源的设备和/或(b)与能提供进一步的安全权利管理资源的其它设备或系统连接的设备，充分地保护内容并进一步支持更复杂的安全级和功能。本发明的这个方面允许参与并在永久或暂时连接的网络中合作操作的多个设备和/或其它系统共享在单一或多个节点上发生的至少一个或多个电子事件（例如通过使用Ginter等人专利中描述的保护的处理环境而管理的）的权利管理，并允许与使用和/或控制这种多个设备和/或其它系统的当事人和/或小组关联的权利能按照潜在的与权利相关的规则和控制而被采用。这就例如允许，可通过公司经理的设备得到的权利，可以以某种方式，与一个或多个公司下属职员的权利结合，或者代替后者，条件是他们的计算或其它设备连接成一个暂时连网关系并在适当的范围中操作。一般来说，本发明的这个方面允许DVD分布式权利管理或者封装和发送的受分布式、同等级权利管理保护的内容。无论DVD设备或其它电子信息使用设备是否加入永久或暂时连接的网络，也无论参与分布式权利管理安排的设备和/或其它系统之间的关系是否是暂时的 或是具有更持久的操作关系，这种分布式权利管理都能运行。这样，相同的设备就可以根据设备操作所在的范围而具有不同的权利（例如，在诸如与其它个人和/或小组合作的一个公司环境中，在家庭内部环境和/或与其它外部个人和/或其他当事人合作的家庭环境中，在一个零售店环境中，在学生的教室装置中－其中学生的笔记本在权利管理方面与教室的服务器和/或教师的PC合作，在图书馆环境中－其中多个当事人合作地使用不同的使用检索资料的权利，在工厂楼面－其中的手持设备与控制设备合作，安全并适当地执行专有功能，等等）。

[0082] 例如，将有限资源设备装置，例如DVD设备，与价格不贵的网络计算机(NC)或个人电脑(PC)相连，可以允许权利管理功能和/或当事人和/或设备的特有权利得到增强（或替换），方法是准许权利管理是DVD设备的部分和/或全部权利和/或权利管理功能与网络或个人计算机(NC或PC)的权利或权利管理功能相组合的结果。这种权利由于由可靠（安全）远程网络权利管理机构提供的权利管理功能的可获得性而可以得到进一步的增强、修改或替换。

[0083] 本发明的这些方面能允许同样的设备－本例中是DVD设备－支持断开和连接装置中权利管理功能的不同排列，例如不同程度，并允许从由权利管理设备和/或其它系统组合而产生的权利和/或权利管理功能的可用性产生可用的权利。这可以包括通过使用一个“较不”安全的和/或资源贫乏的设备或系统而得到的部分或全部权利的一个或多个组合，其中“较不”安全的和/或资源贫乏的设备或系统通过与一个“较”安全的或安全“程度不同”的和/或资源丰富的和/或拥有不同权利的设备或系统的连接而得到增强、替换或修

改，其中这种连接采用其中一个设备和／或这两个设备的、描述共享权利管理安排的权利相关规则和控制所确定的权利和／或管理功能。

[0084] 在后一种情况下，连接到逻辑上和／或物理上远程的权利管理功能，能够扩展（例如增加可用安全权利管理资源）和／或改变 DVD 设备或与 NC、个人电脑本地服务器和／或远程权利管理机构相连的 DVD 设备的用户可用的权利的特性。在这种权利增强的情形中，额外的内容部分可以获得，价格可以改变，再传播权利可以改变（例如得到扩展），内容提取权利可以得到增加，等等。

[0085] 这种“连网权利管理”能够允许多个逻辑和／或物理关系形形色色的设备和／或其它系统的权利管理资源的组合，通过与一个或多个“远程”权利管理机构的连接而提供的增强资源，产生更大的权利，或者产生不同的权利。此外，在提供增加的和／或不同的权利管理功能和／或权利的同时，这种基于连接的权利管理安排还能支持多地点的内容可用性，方法是提供远程可用内容－例如在远程的、基于因特网的环球网（world wide web）的、支持数据库的内容存储器中存储的内容－与一个或多个 DVD 盘上的本地内容的无缝集成。

[0086] 在这实例中，用户不仅能体验到增加的或不同的权利，而且能够使用本地 DVD 和补充内容（即从时间观点来说更流行、价格更高、更多样化、或从其它意义上说具有补充性等等的内容）。在这种情况下，DVD 设备和／或 DVD 设备（或与这种设备连接的其它设备或系统）的用户可以将相同的权利、有差异的和／或不同的权利施加到本地或远程可用的内容上，而本地或远程可用的内容的部分本身在由用户和／或设备使用时可以受制于有差异的或不同的权利。这种安排通过采用多个相连装置的权利管理和内容资源，能支持用户在一次内容检索和／或使用活动中可有效获得的被无缝集成的用户内容的机会的全部的极大的增加。

[0087] 这种权利增强的远程管理机构可以用调制解调器直接连接到 DVD 设备和／或其它设备，或者直接或者间接通过使用诸如串行 1394 可兼容的控制器的 I/O 接口连接（例如，通过在 1394 启动的 DVD 设备与本地个人电脑之间的通信，其中，个人电脑充作一个智能同步或异步信息通信接口，连接一个或多个远程管理机构，包括作为增强和／或提供 DVD 设备中权利管理的本地权利管理结构的本地 PC 或 NC 或服务器）。

[0088] 根据本发明提供的另一个方面，参与者和／或参与 DVD 设备或其它系统被提供的、购买的或以其它方法获得的权利，能通过一个或多个永久或暂时连网的设备，在这种对等关系的设备和／或其它系统之间交换。在这种情况下，只要这类设备和／或其它系统参加权利管理系统，例如 Ginter 等人专利中描述的虚拟传播环境，并且采用其中描述的权利转让和其它权利管理功能，则权利就可以被易货交易、出卖、以其它方式有价交换和／或出租。例如，本发明的这个方面允 许当事人交换他们购买了权利的游戏或电影。还是在该例中，某个人可以从邻居购买一部分观看电影的权利，或将从游戏出版商收到的信用转让给另一方以将游戏超级传播到几个熟人，这种信用能被转让（交换）给某个朋友，以买到该朋友的部分权利，一定次数地玩不同的游戏，等等。根据本发明提供的另一个方面，DVD 之类的便携式存储介质含有的内容与一个或多个加密密钥和一个安全内容标识符关联。内容本身（或使用该内容所要求的信息）至少部分用加密法加密－在使用内容之前需要用关联的解密密钥解密该内容。解密密钥本身也可以以加密密钥块的形式被加密。根据所用平台，可以使用不同的密钥管理和存取技术。

[0089] 根据本发明提供的另一个方面，“创建”数字内容（甚至模拟内容）的电子设备-例如数字摄影机/录像机或录音机能够方便地配备适当的硬件和/或软件，以便生成一开始在安全容器内提供的内容。例如，由数字摄影机记录的内容可以被摄影机在其进行记录的同时立即封装入安全容器。摄影机然后就能输出已经封装在安全容器中的内容。这就不需要在晚些时候或在生产阶段封装内容，所以在根据本发明的电子权利管理的总体实现中，节省了一个生产流程步骤。此外，由于在权利管理环境中为了使用而“读”内容这个过程在常规的生产和传播过程的许多阶段都可能发生（例如在编辑和/或DVD或音频盘母盘的所谓“压制”过程中）。相应地，本发明的另一个重要优点是，内容的权利管理基本能扩展到内容生成、编辑、分销和使用的各个阶段，以提供一个能保护整个内容生命周期的权利的无缝的内容保护体系。

[0090] 在一个实施例中，存储介质本身含有密钥块解密密钥，解密密钥隐藏在存储介质中，用一般的存取和/或复制技术一般是取不出来的。这个隐藏的密钥可被驱动器用于对加密的密钥块进行解密一这种解密的密钥块然后被用于有选择地解密介质上的内容和相关信息。驱动器可以以一种安全、抗破坏的方式设计，使得隐藏的密钥不会暴露出驱动器，提供额外一个保护层。

[0091] 根据另一个实施例，视盘驱动器可以存储并保持用于解密一个加密密钥块的密钥。该密钥块解密密钥可以存储在驱动器的密钥存储器中，如果视盘驱动器至少偶尔使用例如由机顶盒提供的通信通道、网络端口或其它通信路线，解密密钥还可以更新。

[0092] 根据另一个实施例，一个虚拟分配环境安全节点包括一个受保护的处理环境，诸如一个基于硬件的安全处理单元。该安全处理节点可以根据传递到介质本身上的安全节点和/或在诸如网络的独立通信通道上传递的安全节点的、由一个或多个安全容器规定的控制规则和方法，控制诸如数字视盘等便携式存储介质上的内容的使用。

[0093] 某些对DVD的常规复制保护当前预见与显然由Matsushita公司首次提出的某些加密技术相结合的CGMA复制保护控制代码。尽管这种方法对数字财产保护的好处是有限的，本发明能够提供补充的、兼容的、并且更加全面的权利管理系统，同时还提供其它和/或不同的选择和解决方案。下面是根据本发明提供的优点的一些其它例子：

[0094] ●完全符合内容提供者需要的高度安全性。

[0095] ●包括分布式权利保护的价值链管理自动化和效率、对价值链参加者的“计时分片”付费解集作用（“piece of tick”paymentdisaggregation）、成本-高效的微观事务管理、以及对至少偶尔连接的设备的脱机微付费和微交易支持的超级传播。

[0096] ●简明、高效的通道管理，包括支持使用可在有限资源、更多资源、独立的和/或连接的设备上传递的相同内容。

[0097] ●可用于任何介质和应用类型和/或所有形式的内容和内容模型-不仅仅是有些现有技术中那样的压缩视频和声响，并支持在各种介质传播系统（例如广播、因特网仓器、光盘等等）间使用相同的或实质上相同的内容容器的复制件，用于在各种不同电子设备（例如数字摄影机、数字编辑设备、录音设备、声响编辑设备、电影院投影仪、DVD设备、广播磁带播放器、个人电脑、智能电视等等）上操作。

[0098] ●通过重要的新的内容收入和/或其它考虑机会和价值链运营效率的提高，使资产管理和收入和/或其它考虑最大化。

[0099] ●能百分之百地兼容其它保护技术，例如 CGMA 保护码和 / 或 Matsushita 对 DVD 复制保护的数据扰乱方法。

[0100] ●能与各种现有的数据扰乱或保护系统使用，提供很高的兼容性和 / 或很高级的功能。

[0101] ●允许 DVD 技术变成形形色色的娱乐、信息商业和计算机世界商务模式的可重用、可编程的资源。

[0102] ●使 DVD 驱动器和 / 或半导体部件的制造商和 / 或分销商和 / 或其它增值参与者，成为正在出现的因特网和内部网的连接世界的物理基础结构的提供者和权利所有者，他们可以要求人们有偿使用加入到商业网络的分布的、物理基础结构的一部分（例如他们提供的一部分）。这些制造商和 / 或分销商和 / 或其它增值参与者能从参加“计时分片”中享受到经济利益，这种利益来自由于参与交易而得到的一小部分收入的积累。

[0103] ●提供自动的国际化、地区化和权利管理，其中：

[0104] -DVD 内容能具有不同规则集的组合，用于根据用户的权利和身份自动使用；

[0105] - 能透明地处理包括税收在内的社会性权利。

[0106] 此外，本发明的 DVD 权利管理方法和装置为介质记录者 / 出版商增加了利益，具体在于：

[0107] ●符合“让诚实的人诚实”的哲学。

[0108] ●能百分之百地兼容其它保护方案，例如 Matsushita 的数据扰乱方法和 / 或 CGMA 编码盘。

[0109] ●能与其它保护方案一起工作和 / 或作为补充，提供期望的程度和 / 或功能，或能用于补充或替换其它方法以提供额外的和 / 或不同的功能或特色。

[0110] ●提供强大的、可扩展的、超越对数字趋同世界的权利管理的有限的复制保护模式的权利管理。

[0111] ●赋予录制 / 出版社创建复杂的资产管理工具的能力。

[0112] ●通过对多媒体环境外的录制财产的控制使用创造重要的商业机会。

[0113] ●独特地将国际化、地区化、超级传播、重企化联系到内容创造过程和 / 或使用控制。

[0114] 本发明的其它发明惠及其它类的权利所有者，例如：

[0115] ●通过价值链和过程层次在全球范围内对数字内容进行持久、透明的保护。

[0116] ●显著降低因复制和传播引起的收入损失。

[0117] ●将“传播”复制和许多形式的版权侵权由战略性的商业威胁转变成重要的商业机会。

[0118] ●与介质和 / 或使用地点和其它权利变量无关的、所有数字内容的单一标准。

[0119] ●跨行业、分销渠道、介质和内容种类的主要规模经济。

[0120] ●能支持 DVD 播放器内的本地使用管理和检查，允许高效率的微交易支持，包括多方微交易和透明的多方微交易。

[0121] ●赋予权利所有者根据具体情况采用最广泛的定价、商务模式和市场策略的能力。

[0122] 本发明对 DVD 和其它数字介质设备制造商有利的其它方面是：

[0123] ●能提供与现有的盘位对位的兼容性。

[0124] ●内容类型独立。

[0125] ●介质独立并且可编程 / 可重用。

[0126] ●高度方便地转变到下一代具有更高密度设备和 / 或可写 DVD 和 / 或其它光学介质格式的设备。

[0127] ●参加用该设备生成的收入流。

[0128] ●对所有数字内容设备的单一可扩展标准。

[0129] ●随时准备面临未来的“趋同”世界，在这种世界里，许多设备在家庭里例如用 IEEE 1394 接口或其它装置相连在一起（例如有些设备非常像计算机，而有些计算机又非常像设备）。

[0130] 本发明的内容向计算机和 OS 制造商提供了许多好处，例如：

[0131] ●例如通过至少一个透明的插件，作为对操作系统的扩展在计算机中实现，不需要改动计算机硬件和 / 或操作系统。

[0132] ●容易无缝地集成到操作系统和设备中。

[0133] ●极其强大的安全性—特别是在用“安全硅片”（即在芯片上制作的硬件 / 固件保护装置）增强时。

[0134] ●将用户设备转变成名副其实的电子商业设备。

[0135] ●提供用于可靠、安全的权利管理和事件处理的平台。

[0136] ●按特殊需要定制的可编程性。

[0137] 本发明提供的其它特点和优点例如包括：

[0138] ●介质上的信息（例如财产和元数据）可以加密也可以不加密。

[0139] ●不同的信息（例如财产和元数据）可用不同的密钥加密。这不仅为防止泄密提供了更多的保护，还支持在复杂的权利管理系统中的选择性的使用权利。

[0140] ●可以在介质上存储加密了的密钥，虽然这并非必要。这些密钥可用于解密受保护的财产和元数据。加密了的密钥之所以可能被使用，是因为这允许信息本身有更多的保密材料，与此同时保持在单一密钥控制下的存取。

[0141] ●可以在介质上存储多组加密了的密钥，要么将不同的密钥组与不同的信息相关联，要么允许多个控制方式使用相同的信息，其中每个控制方式可以用一个或多个不同的密钥去解密它所用的加密密钥集合。

[0142] ●为了支持播放器能访问受权利管理的容器和 / 或内容，可以将加密密钥的解密密钥隐藏在介质中通常访问不到的一个或多个位置上。这种“通常访问不到”的位置物理上对播放器上安装的驱动器开放，对播放器上安装的计算机禁止。这种启动可用不同的固件或驱动器上的跳线等等实现。

[0143] ●播放器存取受权利管理的容器和 / 或内容的能力也可以被一个或多个在播放器内存储的密钥支持，这些密钥能对介质上的某些加密密钥进行解密。

[0144] ●播放器中的密钥可以允许有些播放器播放其他不同的财产。密钥通过网络连接（例如连接到一个个人电脑、一个电缆系统、和 / 或一个调制解调器连接到一个新的和 / 或其他的密钥和 / 或密钥取消信息）被加到播放器和 / 或从播放器删除，或者通过“播放”一个密钥分配 DVD 被自动装入。

[0145] ●控制计算机使用可以得到控制播放器内容和/或权利管理信息的使用的某些或全部相同技术的支持。

[0146] ●控制计算机对内容和/或权利管理信息的使用可以通过一个受托的权利管理系统使计算机接收一个或多个适当的密钥而得到支持。

[0147] ●计算机可以接受允许对介质上某些加密密钥进行解密的其他密钥。

[0148] ●计算机可以接受允许直接对加密数据的一个或多个部分进行解密的其他密钥。这就允许有选择地使用介质上的信息而不暴露密钥(例如能解密任何加密密钥的播放器密钥)。

[0149] 根据本发明提供的另一个方面,提供一个安全的"软件容器",它允许:

[0150] ●用加密方法保护的内容、权利规则和使用控制的封装。

[0151] ●用于运输、储存、和价值链管理的持久保护。

[0152] ●复杂的规则接口结构。

[0153] 元素可以独立地传递,例如关于折扣定价(例如销售定价、特殊用户和小组的折扣、基于使用模式的定价、等等)和/或其他商业模式变化的新控制,可以在财产被传播后传递(这对于大量的财产和物理分配传播介质(例如 DVD、CD-ROM)来说特别有益,因为可以避免再传播的费用,并且消费者可以继续使用它们收藏的盘)。此外,加密数据能被定位在容器"之外"。这就能例如允许使用来自控制和支持"流动"内容以及"遗产"系统(例如 CGMS)的独立存储的数据。

附图说明

[0154] 要更好地透彻理解这些发明具有的这些和其他特点和优点,可结合以下附图阅读对最佳实施例的详细描述:

[0155] 图 1A 表示使用诸如数字视盘之类便携式存储介质的家庭消费电子设备例子;

[0156] 图 1B 表示使用相同便携式存储介质但提供更先进的权利管理功能的安全节点设备的例子;

[0157] 图 1C 表示一例制造受保护光盘的过程;

[0158] 图 2A 表示图 1A 的消费电子设备的一例结构;

[0159] 图 2B 表示图 1B 的安全节点设备的一例结构;

[0160] 图 3 表示图 1A 设备所用数据结构的例子;

[0161] 图 3A 和图 3B 表示控制集定义的例子;

[0162] 图 4A 和图 4B 表示图 1A 设备提供的使用技术的例子。

[0163] 图 5 表示图 1B 由安全节点用来访问存储介质上信息的数据结构的例子;

[0164] 图 6 表示图 1B 安全节点执行的一例使用技术;

[0165] 图 7 是表示 DVD 上含有的一个特殊安全软件容器一个例子的框图;

[0166] 图 8 是表示 DVD 介质上存储的一例安全容器及视频财产内容的框图;

[0167] 图 9 是表示 DVD 介质上含有的一个标准容器的另一个例子的框图,该 DVD 包括一个额外的容器,它有一个例如与安全节点一起使用的更复杂的规则方案;

[0168] 图 10 表示将具有一个容器(它存在该介质上)的 DVD 用于配有安全权利管理节点的 DVD 播放器,该图还显示了将同一个 DVD 与不配有安全权利管理节点的 DVD 播放器使

用；

[0169] 图 11 是一个表示按照本发明在配有权利管理安全节点的 DVD 播放器上使用没有容器的 DVD 与在没有安全节点的 DVD 播放器使用相同的 DVD 的对比框图；

[0170] 图 12 ～ 14 表示网络配置的例子；

[0171] 图 15A ～ 15C 表示一例虚拟权利过程。

[0172] 具体实施方式

[0173] 图 1A 表示的例子是大批量生产的价格不贵的家庭消费电子设备 50，它能使用诸如便携式数字编码光盘之类（例如数字视盘或 DVD）的存储介质 100 上的信息。消费设备 50 包括一个专用光盘播放器 52，在有些实施例中，光盘播放器也可具有向光学介质写数据的能力（可写 DVD 盘，或“DVD-RAM”），光盘播放器与家庭彩色电视 54 相连。一个遥控单元可用于控制该盘播放器 52 和 / 或电视机 54。

[0174] 在一个实施例中，盘 100 可以存储一部长故事影片或其他视频内容。想观看盘 100 中内容的人可以购买或租借该盘，将该盘插入播放器 52，用遥控器 56（和 / 或播放器 52 上可能带有的控制器 58），控制播放器通过家庭彩电 54 回放该内容。

[0175] 在有些实施例中，遥控器 56（和 / 或设备 52 上可能带有的控制器 58）可以控制例如对电影的录制。播放器 52 读取盘 100 所含的数字化视频和音频信息，将其转换为与家庭彩电 54 兼容的信号，并把这些信号提供给家庭彩电。

[0176] 在有些实施例中，电视机 54（和 / 或一个机顶盒）提供视频信号，由设备 52 在可写光学介质 - 例如 DVD-RAM 上录制。电视机 54 根据播放器 52 向电视机提供的信号，在屏幕 54a 上生成图象并通过扬声器 54b 播放伴音。

[0177] 同样的盘 100 也可由图 1B 中的更高级的平台 60 使用。平台 60 例如可以包括与显示监视器 64 相连的个人电脑 62、键盘 66、鼠标器 68 和扬声器 70。在这个例子中，平台 60 也能像专用的盘播放器 52 一样回放盘 100 上存储的内容，并且由于平台中有安全节点 72，所以还能更复杂和 / 或更高级地使用该内容。（在有些实施例中，平台 60 可能也能在可写光学介质，例如 DVD-RAM 上录制内容。）例如，用平台 60 和它的安全节点 72，就有可能交互式地播放电影或其他内容，使得用户可以通过键盘 66 和 / 或鼠标器 68 进行选择，实时地改变通过显示器 64 和扬声器 60 提供的图象。

[0178] 举例来说，平台 60 的用户在显示器 64 上显示的选择项中作出选择，使内容图象的顺序改变（例如提供许多不同结局中的一个，允许用户交互式地控制图象播放流，等等）。计算机 62 可能也能使用并处理数字数据，这些数据例如包括盘 100 上存储的、播放器 52 不能处理的计算机程序和 / 或其他信息。

[0179] 安全节点 72 提供一个安全权利管理设备，它例如允许更侵占性地或彻底地使用盘上存储的内容。例如，专用播放器 52 可以阻止对盘 100 上存储内容的任何复制，或者允许该内容只能被复制一次，然后再也不能复制。而包含安全节点 72 的平台 60 则允许多次复制部分或全部内容 - 当然只有在满足一定条件时才行（例如设备 60 的用户属于特定一类的人，对每次复制保证能按商定的价格支付费用，只复制内容中的特定摘选部分，对每次复制都保持并报告可靠的检查跟踪，等等）（在有些实施例中，专用播放器 52 可以只将受保护内容发送给经认证能可靠地实行权利管理规则并承担使用后果的设备。在有些实施例中，设备认证可以用数字证书，在一个非限制性例子中例如符合 X.509 标准的证书。）因此，本

例中的包含安全节点 72 的平台 60 能用各种灵活、安全的方式使用盘 100 提供的内容，而用专用播放器 52- 或任何其他不含安全节点的设备则不可能。

[0180] 安全的盘创建和传播过程举例

[0181] 图 1C 表示一例安全创建一个用于播放器 50、60 的多媒体 DVD 母盘 100 的过程。本例中，数字相机 350 将光图象（例如照片）转换成代表一个或一序列图象的数字信息 351。本例中的数字相机 350 包括一个安全节点 72A，它在数字信息 351 离开相机 350 之前保护数字信息。实现这种保护的方法例如是，在一个或多个容器内封装数字信息，并且 / 或者将控制与数字信息关联。

[0182] 本例中，数字相机 350 将受保护的数字图象信息 351 提供给一个存储设备，例如一个数字磁带录像机 352。磁带录像机 352 将数字图 象信息（连同任何相关控制信息）存储到一个存储介质上，例如盒式磁带上。磁带录像机 352 也可以包括一个安全节点 72B。本例中的安全节点 72B 能够明白并执行数字相机安全节点 72A 适用的、并且 / 或者与数字信息 351 相关的控制，并且 / 或者能对存储信息施加其自己的控制。

[0183] 相同的或不同的磁带录像机 352 可以将受保护数字信息 351 回放到数字混合控制台 356。数字混合控制台 356 可以混合、编辑、增强或以其他方式处理的数字信息 351，生成代表一个或一序列图象的处理的数字信息 358。数字混合控制台 356 可以接受来自其他设备 - 例如其他磁带录音 / 相机、其他数字相机、字符发生器、图形发生器、卡通片制作器或者任何其他基于图象的设备 - 的其他输入。任何或者所有这类设备也都可以包括安全节点 72，以保护它们生成的信息。在有些实施例中，有些数字信息可以从包括有安全节点的设备中取得，其他数字信息可以从没有安全节点的设备中取得。在另一些实施例中，提供到数字混合器 356 的数字信息有些是受保护的，有些是不受保护的。

[0184] 本例中，数字混合控制台 356 也可以包括有一个安全节点 72C。数字混合控制台安全节点 72C 实施由数字摄象机安全节点 72A 与 / 或磁带录像机安全节点施加的控制，以及 / 或者它可以将它自己的保护加到它产生的数字信息 358。

[0185] 在这一例子中，音频麦克风 361 接受声响，并将之转换成模拟信号。本例中，音频信号被输入到一台数字磁带录音机 362，在图示的例子中，磁带录音机 362 和音频混合器 364 是数字设备。然而，在其他实施例中，这些设备中的其中一个或二者都可以以模拟方式操作。在图示的实施例中，数字磁带录音机 362 将模拟音频信号转换成代表声响的数字信息，并将数字信息（以及任何相关的控制信息）存储到磁带 363。

[0186] 本例中，磁带录音机 362 包括有能将控制信息与磁带 363 存储的信息关联的安全节点 72E。这种控制信息可以与该信息一起存储在磁带 363 中。在另一个实施例中，麦克风 361 可以包括有其自己的能将控制信息与音频信息关联（例如通过将音频信息与控制信息隐蔽式 (steganogrphically) 编码）的内部安全节点 72。磁带录音机 362 可以实施这种由麦克风 361 施加的控制。

[0187] 另一个办法是，麦克风 361 可以按数字方式操作，将音频的数字表示，可能还包括可选地包含在麦克风 361 中的安全节点 72 所提供的控制信息，直接提供给相连的设备，诸如磁带录音机 362。在图 1C 示例中，数字表示可以任选地替代设备之间任意信号的模拟表示。

[0188] 相同的或不同的磁带录音机 362 可以回放磁带 363 上记录的信息 366，并将该信息

提供给音频混合器364。音频混合器364可以混合、编辑或以其他方式处理信息366，生成代表一个或一序列声响的信息368。音频混合器364可以接受来自其他设备－例如其他磁带录音机、其他麦克风、声响发生器、音乐合成器或者任何其他基于音频的设备－的输入。任何或者所有这类设备也都可以包括安全节点72，以保护它们生成的信息。在有些实施例中，有些数字信息可以从包括有安全节点的设备中取得，其他数字信息可以从没有安全节点的设备中取得。在另一些实施例中，提供到音频混合器364的数字信息有些是受保护的，有些是不受保护的。

[0189] 本例中，音频混合器364包括有一个安全节点72F，它实施－如果有的话－由磁带录音机安全节点72E施加的控制，并且/或者实施其自己的控制。

[0190] 数字图象混合器356提供数字信息358到“DVD-RAM”设备360，该设备能写到母盘100和/或写到能由其生成母盘的盘。类似地，音频混合器364可以提供数字信息368到设备360，设备360将图象信息358和音频信息368记录到母盘100上。本例中，设备360可以包括有一个安全节点72D，它实施由数字相机安全节点72A、磁带录像机安全节点72B、数字混合器安全节点72C、磁带录音机安全节点72E和/或音频混合器安全节点72F施加的控制，并且/或者它也可以将其自己的保护信息添加到其写到母盘100的数字信息358中。光盘制造商然后就能用常规光盘批量生产设备，大批生产基于母盘100的光盘100(1)～100(N)，用于通过任何渠道传播（例如通过音像制品店、web网址、电影院等等）。图1A和图1B中所示的消费设备50可以回放盘100-实施向盘100上存储的信息施加的控制。安全节点72就这样，在制造、传播和使用盘100的全部过程中，在由数字相机350生成的图象及由麦克风361生成的声响上保持着端 对端的、持久的安全控制。

[0191] 在图1C的示例中，各种设备互相之间可以通过所谓的“IEEE1394”高速数字串行总线进行通信。在这里，“IEEE 1394”指的是本文引用的下列标准规范中提出的硬件和软件标准：1394-高性能串行总线1995 IEEE标准第1-55937-583-3号（国际电力电子工程协会1995年）。该规范描述了一种自配置、可热插、低成本、可缩放的高速存储器映射数字串行总线。该总线支持100、200或400Mbps的同步和异步传输，并且灵活地支持许多不同的拓扑结构。该规范描述了一个包括有两个电源导线和两对信号双铰线的物理层。该规范进一步描述了包括串行总线管理在内的物理、连接和事务处理层协议。

[0192] 另一方面，也可以用其它适宜的电子通信装置来替代图1C所示的“IEEE 1394”介质，包括其它有线介质（例如以太网、通用串行总线）和/或基于射频(RF)传输的无线介质、红外线信号、和/或任何其它电子通信装置和/或类型。

[0193] 专用播放器结构举例

[0194] 图2A表示专用播放器52的一个结构例子。本例中，播放器52包括一个视盘驱动器80、控制器82(例如包括微处理器84、存储器－诸如只读存储器86和用户接口88)、以及视频/音频处理块90。视盘驱动器80通过与光盘100的光学和物理作用，从该盘读取数字信息。控制器82控制视盘驱动器80根据的是存储在存储器86中并由微处理器84执行的程序指令（并且进一步根据由可连接控制58和/或遥控器56的用户接88所提供的用户输入）。视频/音频处理块90用视频和音频解压之类的标准技术，将视盘驱动器80读取的数字视频和音频信息转换成与家庭彩电54兼容的信号。视频/音频处理块90也可以插入一个表示对该影象节目的所有权和/或保护的可视标记。块90采用一种数字标记来向标

准录制设备指示不得录制该内容。

[0195] 安全节点结构示例

[0196] 图 2B 表示图 1B 所示平台 60 所用的一例结构 - 它在本例中是围绕 - 台个人电脑构建的，但可以包含任意数量的不同类型的设备。本例中，个人电脑 62 可以通过通信块 152 连接到一个诸如因特网的 电子网络 150。计算机设备 62 可以包括视盘驱动器 80（它可以与播放器 52 示例中包含的视盘驱动器 80 相似或相同）。计算机设备 62 进一步可以包括微处理器 154、存储器 156（例如包括随机存取存储器和只读存储器）、磁盘驱动器 158、视频 / 音频处理块 160。此外，计算机设备 62 还可以包括抗破坏的安全处理单元 64 或其它受保护的处理环境。这样，图 1B 中所示的安全节点 72 就可以由安全处理单元 164、微处理器 154 上执行的软件、或者这二者相结合来提供。用仅用软件、仅用硬件或者软硬件混合的方案等不同的实施方法均可以实现安全节点 72。

[0197] 本例中的安全节点 72 可以提供和支持一种采用可再使用内核和权利语言部件的通用权利操作系统。这种可商用的权利操作系统具备未来的先进商业操作系统所需的功能和集成性。在发展中的电子领域，所有参与者都能依赖的通用的、可再使用的电子商业功能，将变得与操作系统的任何其它功能一样重要。此外，除了其它功能外还提供权利与检查操作系统功能的权利操作系统，能够安全地处理与虚拟传播环境相关的较广范围的任务。安全处理单元例如能够提供或支持权利与检查操作系统功能中的许多安全功能。其它的操作系统功能例如能够处理一般的设备功能。整体操作系统例如可以在一开始被设计成包括权利与检查操作系统功能加上其它的操作系统功能，或者，在另一个实施例中，权利与检查操作系统功能可以作为添加件被添加到提供其它的操作系统功能的预先存在的操作系统中。这些特点的任何部分或全部，可以结合本文披露的发明使用。

[0198] 盘数据结构和相关保护举例

[0199] 图 3 表示盘 100 上存储的一些数据结构的例子。本例中，盘 100 可以存储一个或多个受保护形式或无保护形式的财产或其它内容 200。一般来说，本例中，如果财产 200 至少是部分加密的，并且 / 或者使用该财产所需的关联信息至少是部分加密的，并且 / 或者在其它情况下不满足一定的条件就不能使用，则该财产是受保护的。例如，财产 200(1) 可以是用常规安全加密技术全部或部分加密了的。另一个财产 200(2) 可能是完全无保护的，因此可以毫无限制地自由使用。因此，根据本例，盘 100 可以同时存储两种内容，一种是作为受保护财产 200(1) 存储的电影，一种是作为无保护财产 200 (2) 存储的不予保护的对演员和制片人的采访节目或者“影片预告广告”。如本例所示，盘 100 可以存储任意数量的受保护或无保护形式的不同财产 200，数量只受光盘存储容量的限制。

[0200] 在一个实施例中，由盘 100 提供的保护机制可以使用上文引用的 Shear 的专利中描述的保护（和 / 或其它）结构和 / 或技术的任何部分或者全部。Shear 的专利通过非穷尽式举例，描述了解决如何保护数字内容不被非授权使用的问题的方法。例如，Shear 的专利说明书中其中描述了 - 通过客户计算机中的分布控制节点 - 用电子手段“监视”数字内容使用情况的方法。这包括能实现对任何这种使用的后果的装置和方法。

[0201] Shear 的专利说明书中某些要素的非限制性例子包括：

[0202] (a) 加密信息的解密，

[0203] (b) 统计，

[0204] (c) 根据导出的统计信息与内容供应者设定的规则结合得出的使用控制，

[0205] (d) 安全地报告内容使用信息，

[0206] (e) 数据库技术在受保护信息的存储和传递上的使用，

[0207] (f) 预算的本地安全维护，例如包括信用预算，

[0208] (g) 加密密钥和内容使用信息的本地、安全存储，

[0209] (h) 控制处理的本地安全执行，

[0210] (i) 在许多非限制性例子中，光学介质的使用

[0211] 这些特点的任何部分或全部都可以与本文叙述的发明结合使用。

[0212] 授予 Shear 的专利的说明书还涉及数据库内容对用户是本地的还是远程的问题。在端点用户的系统处本地存储并由远程“联机”数据库信息补充的数据库信息，例如能用于增强本地信息，在一个实施例中，本地信息可以存储在光学介质（例如 DVD 和 / 或 CD-ROM）中。例如可用专用的半导体硬件来提供一个安全执行环境，保证数字商业活动有一个安全可靠的基础。

[0213] Shear 的专利其中还描述了通过安全、统计和使用管理功能的使用而进行的数据库使用控制。说明书中尤其描述了一种统计和控制系统，在该系统中，至少部分加密的数据库被发送给用户（例如在光学介质上）。这类光学介质的非限定性例子例如包括 DVD 和 CD-ROM。随后的使用例如能以各种方法进行统计和控制，结果的使用信息可被传输到一个责任方（作为一例）。

[0214] Shear 的专利说明书也描述了根据传输的信息生成帐单。Shear 的专利的其它实施例例如提供了独特的信息安全发明，这些发明例如涉及根据使用模式而受限制的数字内容使用，诸如特定使用种类的数量。这些功能包括监测被使用信息的“邻近性”和 / 或“逻辑相关性”，以确保某人的电子“行为”不逾越其许可的权利。Shear 专利的其它方面尤其还描述了能使组织安全地、局部地管理电子信息使用权利的功能。当一个数据库或数据库的一部分被传递到一个客户地址时，Shear 专利的有些实施例提供例如光学存储装置（其中非穷尽的例子包括 DVD 和 CD-ROM）作为传递机构。这种存储装置能将例如一批视频、音频、图象、软件程序、游戏等，存储在光学介质上，例如 DVD 和 / 或 CD-ROM 上，除此之外还存储其它内容，诸如一批文本文件、文献记录、部件目录、以及各种版权材料和非版权材料。这些特点任何一个或全部都能用于本文中的实施例。

[0215] 一个特定的非限定性实施例例如可能涉及一个准备一批游戏的供应者。供应者准备一个存储游戏相关信息的数据库“索引”，信息内容例如是游戏名称、介绍、制作者标识符、价格、以及在登记或再登记要求之前每个游戏的最多使用次数或总时间。这种信息有些或者全部都可以按加密格式存储在例如光学介质上，光学介质的非限定性例子包括 DVD 和 CD-ROM。供应者于是可以将游戏的有些部分或全部加密，使得除非一个或多个加密部分已被解密，否则游戏就不能使用。一般来说，除非供应者规定的条件得到满足，例如，除非能得到支付使用费用的信用并且反映游戏使用情况的检查信息被存储，否则解密就不会发生。供应者可以决定，例如，哪些用户活动是其允许的，是否为检查和 / 或控制目的而统计这类活动，需要的话，要为所允许的活动设定什么限制。这可能包括，例如，玩游戏的次数以及每次游戏的时间。价格可以打折，其根据的是游戏使用的总时间、当前登记的使用游戏的总次数、顾客是否还登录该同一供应者提供的其它服务，等等。

[0216] 在上面讨论的非限定性例子中，供应者例如会将准备好的游戏与其它有关信息装配在一起，将该集合发布在光学介质上，光学介质 的非限定性例子包括DVD和/或CD-ROM。供应者然后会向预期的顾客销售这种DVD盘。顾客于是可以选择想玩的游戏，然后与供应者联系。供应者于是就能根据其商务模式，将启动信息发给每个授权顾客，其中例如包括使用的启动信息、选定游戏的加密部分的解密密钥（另一个办法是，使用游戏的授权随DVD盘和/或CD-ROM盘一起到达，或者，由用户的安全客户系统根据例如用户参加的检验过的用户类，根据供应者设定的标准自动确定）。采用用户的客户解密与统计机构，顾客于是就能利用这些游戏。该机构然后可以记录使用信息，例如游戏被使用的次数，以及例如每次游戏的时间长度。它能定期地将这种信息传送给游戏供应者，这样实际减少了供应者中央服务器的管理总开销要求。游戏供应者能根据收到的检查信息来收取游戏使用费。这个信息既可以用于顾客收帐，也可以用于从信用提供者收使用费。

[0217] 游戏提供了一种方便的非限定性例子，然而，许多这些相同的思想可以容易地应用于所有种类的内容，所有种类的财产，例如包括：

[0218] ●视频，

[0219] ●数字电影，

[0220] ●音频，

[0221] ●图象，

[0222] ●多媒体，

[0223] ●软件

[0224] ●游戏，

[0225] ●任何其它财产，

[0226] ●任何财产组合

[0227] Shear专利说明书的其它非限定性实施例例如支持安全地控制不同种类的用户活动，例如显示、打印、电子方式存储、通信等等。有些方面进一步对这些不同的使用活动应用不同的控制标准。例如，可以将被浏览的信息与以复制、修改和远程传输为目的读入主计算机的信息区别，不同的活动适用不同的使用费（这样，例如浏览的费用就大大低于复制或打印的费用）。

[0228] Shear专利说明书例如也描述了由出版者和顾客进行的组织内部的信息管理。例如，有一种可选的安全系统可用于允许组织防止使 用全部或部分信息库，除非用户输入了保密码。能支持多层次的保密码以允许按照用户的保密授权级来限制用户的使用。一个实施例例如能用硬件与软件相结合来改进抗破坏能力，另一个实施例可以采用一种完全基于软件的系统。尽管专用硬件/软件系统在某些情况下可以保证抗破坏，对于某些应用来说，在非专用系统上用软件执行实现的技术就能提供足够的抗破坏性能。任何或所有这些特点都可以与本发明说明披露的技术结合使用。

[0229] 图3光盘也可以存储元数据(metadata)、控制及其它信息

[0230] 在本例中，盘100也可以存储有保护和/或无保护形式的“元数据”。播放器52用元数据202来辅助使用盘100存储的一个或多个财产200。例如，盘100可以存贮一个无保护形式的元数据块202(1)和另一个有保护格式的元数据块202(2)。盘100可以存储任何数量的有保护和/或无保护形式的“元数据”块202，数量只受光盘容量的限制。在本例中，

元数据 202 包含用于访问财产 200 的信息。这种元数据 202 例如可以包含用于控制盘 100 上存储的一个或多个财产 200 的回放顺序的帧顺序或“导航”信息。举例来说，无保护元数据块 202 可以只能访问受保护财产 200 的选定部分以生成一个缩略的“电影预告”图象，与此同时，受保护的元数据块 202 可以含有财产 200 的全部视频的图象帧回放顺序。另一个例子是，可以为同一电影财产 200 的不同“剪辑”（例如 R 级版本、PG 级版本、导演剪辑版本等）提供不同的元数据块 202。

[0231] 本例中，盘 100 可以存储用于安全目的的其它数据。例如，盘 100 可以存储控制集 204 形式的控制规则，这些控制规则可以以一个或多个安全容器 206 的形式封装在一起。商业模式参与者能安全地提供代表各自“电子”利益的电子规则和控制。这些规则和控制扩大了一种“虚拟存在™”(Virtual presenct™)，商业参与者可以通过其来按照它们各自互相约定的权利而管理远程的价值链活动。这种虚拟存在可以采用参与者规定的电子条件（例如规则和控制）的形式，电子事件发生之前，这些条件必须满足。这些规则和控制能用于在“下游”电子商业活动期间实施当事人的权利。VDE 内容容器所提供的和 / 或以其它方式使用 VDE 内容容器可获得的控制信息，例如可以构成一个或多个“提议的”电子协议，这种协议用于管理对 这种内容的使用和 / 或使用这种内容的后果，并且能制订涉及多方当事人及其权利义务的协议条款。

[0232] 多方当事人的规则和控制例如可用于形成集中控制集（“合作虚拟存在™”-Cooperative Virtual presence ™)，保证价值链参与者中的电子商业活动与协议一致。这些控制集例如可以规定管理与受保护数字内容（传播的数字内容、设备控制信息等）交互作用的条件。这些条件例如不仅能用于控制数字信息使用本身，也能控制这种使用的后果。结果是，商业参与者的各自利益受到保护，合作、高效与灵活的电子商务模式得以形成。这些模式能与本发明结合使用。

[0233] 盘可以存储加密的信息

[0234] 盘 100 也可以存储一个加密密钥块 208。本例中，盘 100 可以进一步存储一个或多个隐藏密钥 210。本例中，加密密钥块 208 提供一个或多个加密密钥，用于解密一个或多个财产 200 和 / 或元数据块 202。密钥块 208 可以提供不同的加密密钥，用于解密不同的财产 200 和 / 或元数据块 202、或相同的财产和 / 或元数据块的不同部分。于是，密钥块 208 就可以包含许多加密密钥，如果要使用盘 100 存储的所有内容，就要求或可能会要求用到所有密码密钥。尽管图 3 所示的密钥块 208 是与容器 206 分离的，如果需要，它也可以包含在容器内或是容器的一部分。

[0235] 加密密钥块 208 本身要用一个或多个加密密钥加密。为了使播放器 52 能使用盘 100 上存储的任何受保护信息，首先必须将加密密钥块内的对应密钥解密 - 然后用密钥块中解密的密钥去解密对应的内容。

[0236] 本例中，对加密密钥块的解密所需的密钥可以有几个不同的（可能是可选之一的）来源。图 3 所示的例子中，盘 100 存储一个或多个形式为隐藏密钥 210 的解密密钥，用于对介质本身上的密钥块 208 的解密。隐藏密钥 210 例如可以存储在盘 100 上一般访问不到的位置。这个“一般访问不到的”位置例如可以物理上对播放器 52 中安装的驱动器 80 选通，对安装在个人计算机 62 中的驱动器 80 关闭。选通可以由不同的固件、驱动器 80 上的跳线等实现。隐藏密钥 210 可以这样安置在盘 100 上，使得任何物理拷贝该盘的企图导致

不能 拷贝该隐藏密钥。在一个实施例中，隐藏密钥可以按照 J.Hogan 的描述，隐藏在一个或多个块的位流编码序列中（参阅 Josh Hogan 的“DVD 复制保护”，这是作者在第 4 届 DVD 复制保护技术大会上的报告，96 年 5 月 30 日，美国加州 Burbank）。

[0237] 一种可选方法以及 / 或者附加方法是，对加密密钥块 208 的解密所需的密钥可以由盘驱动器 80 提供。本例中，光盘驱动器 80 可能包括一个小型解密部件，例如一个集成电路解密引擎，内含一个存储着密钥的小型安全内部密钥存储器 212。光盘驱动器 212 可以用这个密钥存储器 212 来对加密密钥块 208 进行解密，既不暴露密钥 212 又不暴露解密了的密钥块 208，然后用密钥块 208 中的解密了的密钥对受保护内容 200、202 解密。

[0238] 盘可以存储和 / 或使用安全容器

[0239] 在另一个例子中，解密受保护内容 200、202 所需的的密钥在安全容器 206 内部提供。图 3A 表示可能的一例包括信息内容 304 的安全容器 206（财产 200 和元数据 202 对于该容器来说可以是外部的 - 或者，视盘 100 存储的数据结构全部或多数可以作为逻辑和 / 或实际受保护容器的一部分）。图 3 所示控制集 204 可以包含一个或多个允许记录 306、一个或多个预算 308 和 / 或一个或多个方法 310，如图 3A 所示。图 3B 表示的一例控制集 204 提供一个或多个加密密钥 208、一个或多个内容标识符 220、以及一个或多个控制 222。本例中，不同的控制 222 可以应用于不同的设备和 / 或设备类，诸如播放器 52 和 / 或计算机设备 62，具体视特定平台和 / 或平台类的功能而定。此外，控制 222 也可以应用于不同的财产 200 和 / 或不同的元数据块 202。例如，控制 222(1) 可以允许财产 200(1) 被播放器 52 或计算机设备 62 复制一次作为备份。控制 222(2)（它可能完全被播放器 52 忽略，因为后者的技术和 / 或保密功能不够；但是它可以由计算机设备 62 用于其安全节点 72) 可以允许用户请求，允许公开演出相同的财产 200(1)（例如在酒吧或其它公共场所），并使用户的信用或其它帐户的帐面自动为每次演播借入一定的使用费。第三个控制 222(3) 例如可以允许安全节点 72（而不是播放器 52) 同意一定的用户类（例如核准的广告人和记者）提取或节选受保护财产 200(1) 的某些部分用于宣传。另一个控制 222(4) 例如可以允许视盘 播放器 52 和安全节点 72 二者都能观看财产 200(1) 范围内的某些静态画面 - 但是可能只允许安全节点 72 在支付一定水平的使用费的条件下复制静态画面。

[0240] 光盘和 / 或系统可以利用受托基础结构的例子

[0241] 控制 222 可以含有指向用于一个或多个财产、控制、元数据和 / 或光盘上其它内容的附加控制集的源的指针。在一个例子中，这些附加控制的获得途径可以来自一个受托的第三方，例如一个权利与许可交换站，以及 / 或者来自任何其它由至少一个权利持有人授权提供至少一个附加控制集的价值链参与者。这种权利与许可交换站是几种分布式电子管理与后援服务之一。分布式电子管理与后援服务可称作“分布式商业应用”，其特点之一是它是一种用于电子商业和电子权利和交易管理的管理与后援服务的集成的模块阵列。这些管理与后援服务可以用来为进行金融管理、权利管理、执照许可、规则清算、使用清算、安全目录服务以及其它与在大型电子网络（诸如因特网）和 / 或机构内部内部网、或者甚至家庭内的电子设备网络上工作的交易相关的功能提供安全基础。这些电子设备的非限定性例子包括至少偶尔连接的光学介质设备，例如包含只读和 / 或可写 DVD 播放器和计算机中的 DVD 驱动器和包括例如数字电视和含 DVD 驱动器的机顶盒的趋同设备 (convergent devices)。

[0242] 这些管理与后援服务例如能经改造后适应任何数量的垂直市场中电子商业价值链－包括五花八门的娱乐应用的特殊需要。电子商业参与者例如能用这些管理与后援服务来支持其利益，并且／或者他们还能根据竞争激烈的商务现实来形成并再使用他们的服务。电子商务参与者的其中一些非穷尽的例子包括个人创作者、影视和音乐制作室、分销商、节目收集者，广播者、电缆与卫星经营者。

[0243] 分布式商业应用例如能以最高的效率利用使用管理资源，并且至少在有些实施例中，能够务实地确定规模，最佳地适应电子商业增长的需求。

[0244] 分布式商业应用例如可以包含许多商业应用系统。这些商业应用系统能提供一个基础结构支持网，供整个电子界和／或其许多或全部参与者使用或再使用。不同的支持功能例如能被按层次和／或网络关系集中起来以适应各种商务模式和／或其它目的。模块化支持功能例 如能组合成不同的系列，形成能适应不同的设计实现和目的的不同的商业应用系统。这些商业应用系统例如能分布在许许多多分布程度不一的电子设备中。

[0245] “分布式商业应用”提供的许多附加功能和好处，能与本申请的附图中所示的特定实施例结合起来使用，其中的一些非穷尽性例子包括：

[0246] ●能使电子商业和权利管理高效并切实可行。

[0247] ●提供安全地管理和支持电子交互作用和后果的服务。

[0248] ●提供用于电子商业和其它形式的人类电子交互作用和关系的基础机构。

[0249] ●最优地发挥现代分布计算和网络的效率。

[0250] ●提供电子自动化和分布处理。

[0251] ●支援模块化、可编程、分布式并最佳地计算机化的电子商业和通信基础结构。

[0252] ●提供范围全面的功能组合系列，支援执行各种管理和支持作用的服务。

[0253] ●最大限度地采用电子自动化和分布处理的好处，实现系统和网络资源的最优分配和使用。

[0254] ●高效、灵活、成本－效益高、可配置、可再用、可修改、可推广。

[0255] ●能经济地反映用户的商务和保密要求。

[0256] ●能最优地分布处理－允许商业模式灵活设置、根据需要缩放，适应和满足用户的需要。

[0257] ●能高效地处理各种活动和服务量。

[0258] ●能以分布和集中处理相结合，为每种商业模式定制和运行。

[0259] ●提供能独特地形成并能适应条件变化而重塑的一整套本地、集中和网络化综合功能。

[0260] ●支持通用资源并能再用于许多不同的模式；已设置的基础结构能被具有不同要求的不同价值链再用。

[0261] ●能支持任何数量的商业和通信模式。

[0262] ●高效地运用本地、集中和网络化资源来满足各个价值链的要求。

[0263] ●公用资源的共享分摊了费用，使效率最大化。

[0264] ●支持混合式、分布式、对等、集中式网络功能。

[0265] ●能进行本地、远程和／或中央操作。

[0266] ●能同步、异步地操作，或支持这两种操作模式。

[0267] ●灵活易变，以适应“计算机世界”中瞬时万变的商业机会、关系和约束。

[0268] 这些特点部分或全部都可以与本文披露的本发明结合使用。

[0269] 分布式商业应用提供的优点之一是，为电子商业和其它形式的电子交互作用提供全面的集成的管理与后援服务。分布式商业应用支持的这些电子交互作用，至少在有些实施例中需要使用最宽范围的设备和传播介质，它们的非限定性例子包括，所有当前形式和将来形式的网络与其它通信通道、消费设备、计算机、诸如 WebTV 的趋同设备、以及光学介质，例如 CD-ROM 和 DVD。

[0270] 存取技术的例子

[0271] 图 3、4A 和 4B 表示播放器 52 提供的存取技术的例子。本例中，当盘 100 被装入播放器的光盘驱动器 80（图 4A，框 400）时，播放器控制器 82 可以指示驱动器 80 从盘 100 提取隐藏密钥 210，用它们去解密部分或全部的加密密钥块 208（图 4A，框 402）。本例中，驱动器 80 可以这样存储密钥，使得解密时不会将它们暴露给播放器控制器 82（例如将密钥存储在诸如基于集成电路的解密引擎的安全解密部件内部的密钥存储器 212 中）（图 4A，块 404）。播放器 52 可以控制驱动器 80 从盘 100 读出控制集 204（可以加密也可以不加密）。播放器微处理器 82 可分析控制集，忽略或丢弃那些超过其功能范围的控制 222，并将与它能实施的控制子集（例如“复制一次”控制 222(1)）对应的许可和 / 或权利管理信息保存起来。

[0272] 播放器 52 然后可以等待用户通过控制输入 58 和 / 或遥控器 56 提出请求。如果控制输入是复制请求（图 4A 中判断框 408 的“是”出口），播放器的微处理器 84 就查询控制 222(1)，判断是否允许复制；以及如果允许的话，条件是什么（图 4A 的判断框 410）。然后，如果对应的控制 222(1) 禁止复制（图 4A 中判断框 410 的“否”出口），播放器 52 就拒绝复制盘 100；如果对应的控制 222(1) 允许复制（图 4A 中判断框 410 的“是”出口；判断框 412），就允许复 制（例如控制驱动器 80 顺序访问盘 100 上的所有信息并将信息传送到图中未示出的输出端口）。本例中，播放器 52 在进行复制时，可以在内部的非易失性存储器中（例如控制器存储器 86 中）或控制 222(1) 要求的其它地方存储一个与盘 100 关联的标识符。这个存储的标识符能被播放器 52 用于实施“复制一次”的限制（例如，如果用户试图用同一个播放器多次复制同一个光盘，或有为控制 222(1) 禁止的其它企图时，播放器能拒绝这种请求）。

[0273] 如果用户请求播放或读出一个财产 200（图 4A 中判断框 414 的“是”出口），播放器控制器 82 就可以控制驱动器 80 从选定财产 200 读出对应的信息（例如按元数据 202 规定的顺序），并视需要对读出的信息解密，解密所用的是开始时从密钥块 208 取得后存储在驱动器的密钥存储器 212 中的密钥（图 4A 的框 416）。

[0274] 图 4B 是图 4A 过程的一种变化形式，其适应的情况是，播放器 52 本身提供对加密密钥块 208 解密的解密密钥。本例中，控制器 82 可以提供一个或多个解密密钥给驱动器 80，方法是使用一种安全协议，诸如 Diffie-Hellman 密钥协议，或通过使用驱动器与播放器 52 相连或相连过的与一些其它系统或部件都已知的一个共享密钥（图 4B 的框 403）。驱动器 80 可以用提供的这些密钥来解密图 4A 中框 404 所示的加密密钥块 208，或者也可以用所提供的密钥直接解密受保护财产 2000 和 / 或受保护元数据 202(2) 之类的内容。

[0275] 另一个例子是，播放器 52 可以被编程为将它对加密形式的电影之类的数字财产

的复制件放置在一个抗破坏的软件容器中。该软件容器中含有一个代码，指示该数字财产是复制版而不是原版。发送的播放器 52 也可以将其自己独有的标识符（或者一个意欲接收的设备－诸如另一个播放器 52、盒式录像播放器或设备 50- 所独有的标识符）放置在相同的安全容器中以实现仅在该意欲接收的设备上播放该复制版的要求。播放器 52（或其它接收设备）能被编程为，当检测到数字财产是复制版而不是原版时不作复制（或不额外复制）。需要的话，播放器能用被编程为，拒绝播放未与该播放器的独有标识符一起包装的数字财产。

[0276] 使用模拟编码技术的例子

[0277] 在另一个例子中，更综合的权利管理信息可以由播放器 52 在模 拟输出中编码，方法是采用水印和 / 或指纹方法。现在的“现实世界”有相当的部分都是模拟的而不是数字的。尽管模拟信号无所不在，现有的在模拟领域中管理权利和保护版权的方法要么很原始，或者根本没有。例如：

[0278] ●多代模拟复制中固有的质量恶化并没有阻止几十亿美元的盗版业的盛行。

[0279] ●有些关于录像带复制保护和付费观看保护的方法试图完全防止对商业销售的内容进行复制，或者仅仅允许一代复制。这些方法一般很容易被人克服。

[0280] ●并非所有现有设备都对复制保护信号作出正确的反应。

[0281] ●现有方案局限于例如“允许复制 / 不得复制”这样的控制。

[0282] ●对录音制品的复制保护尚未在商业上实行。

[0283] 有一个与模拟与数字信号之间信息转换相关的问题。即使信息在一开始因采用强大的数字权利管理技术而受到有效保护和控制，相同信息的模拟复制版可能不再受到安全的保护。

[0284] 例如，对于有的人来说，对最初以数字格式发行的节目材料进行模拟录制一般是可能的。有些根据数字原版的模拟录制质量相当好。例如，一种数字通用盘 (DVD) 播放器可以将数字格式的电影转换成模拟格式，并将该模拟信号提供给高质量的模拟家用盒式录像机 (VCR)。家用 VCR 录制该模拟信号。这样，消费者就获得了对原版数字财产的高质量的模拟复制版。人们能再次录制 DVD-RAM 中的模拟信号。许多情况下，这种录制具有相当的质量－并且不再受“付费观看”的约束，或受与数字版的相同内容关联的其它数字权利管理控制的约束。

[0285] 鉴于模拟格式要伴随我们很长的时间，电影制片厂之类的权利所有者、影像出租和分销公司、音乐制作公司和分销商、以及其它价值链参与者会非常喜欢有显著更好的用于模拟电影、影像、声响制品及其它内容的权利管理功能。解决这个问题一般需要有一种方法来确实将权利管理信息与被保护的内容相关联。

[0286] 水印和 / 或指纹与其他权利功能组合后，可以提供“端对端”安全权利管理保护，允许内容提供者和权利所有者确保它们的内容受到足够的保护 -- 不管在内容传播链内部设备的类型、信号格式以 及信号处理的性质如何。这种“端对端”保护允许授权的模拟设备被容易地、无缝地、费用－效能高的集成到现代权利管理结构中。

[0287] 水印和 / 或指纹例如可以含有能够作为虚拟传播环境（“VDE”）的基础的控制信息，在这种虚拟传播环境中电子权利管理控制信息可以在不安全的（例如模拟的）通信通道上传递。这种虚拟传播环境高度灵活方便，适应现有的和新的商业模式，同时也提供前所

未有的灵活度，尤其便于在电子商业和价值链参与者之间建立新的安排和关系－不管内容是以数字和／或模拟格式传播的。

[0288] 水印与分布式对等权利管理技术相结合具有许多优点，其中包括：

[0289] ●用于提供权利管理信息的一种不可删除和不可见的安全技术。

[0290] ●一种将电子商业和／或权利管理控制与模拟内容诸如电影、影像、和声响制品相关联的不可删除的方法。

[0291] ●商业和／或权利管理控制与传播系统的一端到另一端的内容的持久关联，不管信令格式之间转换（例如模－数转换、数－模转换）的数量和类型如何。

[0292] ●规定“不得复制／一次复制／多次复制”权利管理规则、以及更复杂的权利与交易定价模式（例如“付费观看”及其它）的能力。

[0293] ●全部无缝地与全面、通用的电子权利管理解决方案集成的能力。

[0294] ●与授权的模拟和其它非数字和／或非安全信息信号传递机构结合的安全控制信息传递

[0295] ●在内容从模拟转换为数字或反方向转换时提供更复杂和／或更灵活的商业和／或权利管理规则的能力。

[0296] ●将实施新的、更新的或附加商务模式的商业和／或权利管理规则传送到授权的模拟和／或数字设备的灵活能力。

[0297] 这些特点部分或全部都可以与本发明说明书披露的本发明相结合使用。

[0298] 简言之，水印和／或指纹方法可以用“隐蔽式”（“steganographical”）技术，基本上不可删除并且基本上不可看见地在信息信号内部编码权利管理和／或电子商业规则和控制，信息信号例如是模拟信号或模拟信号的数字化（例如取样的）形式，其 中的非限制性例子包括视频和／或音频数据，这种信息信号然后被本地设备解码和使用。这种模拟信息和用速记法编码的权利管理信息的传输手段有很多，其中的非限制性例子包括广播、有线电视和／或物理介质一其中一个非限定性例子为 VCR 磁带。

[0299] 这些特点部分或全部都可以与本发明说明书披露的本发明相结合使用。

[0300] 水印和／或指纹方法至少能使有些权利管理信息在视频和／或其它信息在进行模拟－数字转换和数字－模拟转换后保留下来。这样，在一个实施例中，两个或更多的模拟和／或数字设备可以参与受托的安全权利管理过程和／或事件的端对端组织。

[0301] 功能更强的实施例

[0302] 如上所述，图 3B 中所示的控制集例提供一种全面、灵活和可扩展的控制集，可供播放器 52 和计算机设备 62（或其它平台）使用，这取决于平台的特定技术、安全及其它功能。本例中，播放器 52 由于大批生产消费用品要降低成本和复杂性的要求，所以只有有限的技术和安全功能，因此基本上可以忽略或不启动控制集 204 内提供的控制 222 的某些部分或全部。另一个例子中，由于存储器和／或处理器的成本不断下降，生产商可能要选择增加播放器 52 的技术和安全功能。功能更多的播放器 52 将提供更强大、健全和灵活的权利管理功能。

[0303] 图 5 示出了允许包括安全节点 72 的平台 60 具有使用盘 100 上的信息和／或权利管理信息的增强的和／或不同的功能的装置示例。参见图 5，安全节点 72 可以连接到网络 150，而播放器 52 不可以，这使得安全节点在有关通信安全信息方面具有了另外的极大的

灵活性，诸如检查线索、有关付费要求或定单等信息有关的补偿。安全节点 72 与网络 150 的这种连接（在任何应用中它有可能被其他的通信技术所代替，诸如插入一个可替换的内存条的技术）允许安全节点 72 接受并安全地保存权利管理控制信息，诸如包含额外的控制集 204′ 的额外的容器 206′ 。安全节点 72 除了盘 100 上存储的控制集 204 外还可以使用控制集 204′ 或者用控制集 204′ 代替控制集 204。安全节点 72 也可以保留一个安全的加密密钥存储器 212，由其提供代替盘 100 上存储的任何密钥 208、210 的或密钥 208、210 之外的附加的加密密钥。由于 安全和 / 或技术功能的提高，安全节点 72 就可能使用播放器 52 忽略或不能使用的控制集 204 内的控制 222-- 并且可以在控制集 204′ 的基础上配备进一步的和 / 或增强的权利和 / 或权利管理功能（他们例如可以由用户专门指定并且可以应用于存储在盘 100 上特定的财产 200 和 / 或特定的光盘集）。

[0304] 安全节点存取技术的例子

[0305] 图 6 示出了存取技术的例子（例如它可以由采用安全节点 72 的平台 60 来执行）在本例中其包括，安全节点 72 从盘 100 提取财产标识信息 220（图 6 的框 502），然后寻找适用的控制集和 / 或规则 204（他们可能存储在盘 100 上、安全节点 72 内、安全节点 72 通过网络 150 访问的一个或多个存储位置内、以及 / 或者这些技术的任何或全部的组合）（图 6 的框 504）。安全节点 72 然后装入必要的解密密钥并根据需要用他们来解密信息（图 6 中框 500）。在一个例子中，安全节点 72 从安全容器 206 和 / 或 206 获得必要的密钥，并将它们保存在一个受保护处理环境诸如 SPU 164 中或者保存在一个软件仿真的受保护处理环境中，而不把它们暴露到该环境之外。在另一个例子中，安全节点 72 可以用一个安全密钥交换协议将必要的密钥（或其子集）装入光盘驱动器，供盘驱动器用于解密信息，其方式与在播放器 52 中发生的完全相同，以保持驱动器硬件的完全兼容。

[0306] 安全节点 72 可以监控用户的输入并根据特定的控制集 204、204′ 执行所请求的动作。例如当接到一个用户请求时，安全节点 72 可以查询控制集 204、204′ ，以确定其是否允许用户请求的动作（图 6 中框 508），如果允许，是否执行该请求的操作所需的条件已经得到满足（图 6 中框 510）。本例中，安全节点 72 可以启动为满足任何这种所需条件而必须的操作，这种操作例如，在用户本地存储的电子钱包中记帐，通过网络 150 安全地请求一个帐户记帐、获得和 / 或检查用户证书以确保该用户属于适当的用户类或者他说话算数等等 - 需要的话可使用网络 150（图 6 中框 510）。当所有必要的条件都满足时，安全节点 72 就执行所请求的操作（并且 / 或者用微处理器 154 去执行操作）（例如释放内容），然后生成安全检查记录，该记录可以由安全节点保存，并且 / 或者在这时或以后通过网络 150 报告（图 6 中框 512）。

[0307] 如果所请求操作是要释放内容（例如对该内容进行一次复制），平台 60（或者上例中的播放器 52）就至少部分根据对该内容实施权利的特定控制来执行所请求的操作。例如，该控制可以阻止平台 60 向某些不能用于复制该内容的特定类型的输出设备以外的设备释放内容，或者让它以一种不利于复制的方式释放内容（例如在复制件上嵌入表示复制人身份的“指纹”；有意降低被释放内容的质量，使得对它复制的质量低劣，等等）。一个具体的例子是，一个与平台 60 相连的盒式录像机（图中未予示出）可以是用于进行复制的输出设备。因为当前的模拟设备系列诸如盒式录像机如果进行多代复制，必然会极大地降低质量，因此内容提供者可以提供允许内容被这类模拟设备复制但不允许被数字设备复制的

控制（因为数字设备可以无限制地进行复制而不降低质量）。例如，平台 60 在安全节点 72 保存的数字控制的控制下，只有在盒式录像机向该平台提供一个数字 ID，表示该输出设备是一个盒式录像机时，才可以向盒式录像机释放内容－除非这个数字 ID 确认该输出设备是一个质量较低的模拟设备，否则可以拒绝提供任何输出。此外或者另一种可选办法是，平台 60 可以故意降低向盒式录像机提供的内容的质量，以确保第二代复制的质量不可接受。在另一个例子中，可以由平台 60 用水印和／或指纹技术在模拟输出中编码更全面的权利管理信息。

[0308] 安全容器使用的其它例子

[0309] 图 7 是表示按照本发明，含有一个用于在 DVD 中使用的安全容器 701 的 DVD 介质 700 的一个基本例子。如本例所示，容器 701（“DVD 的 DigiBox”）可以是专门为用于 DVD 和／或其他介质而设计的“标准”容器的专业版，或者也可以是（如图 8 中所示方案）一个完全“标准的”容器。如本例所示，专业容器 701 具有这样的特点，即允许其与内容信息、元数据、以及 DVD 介质 700 上存储的加密和／或保护信息结合使用，其方式如同容器 701 未存在时所用的完全一样。这样，专业容器 701 具备了与 DVD 和／或其它介质上使用的现有数据格式和组织的兼容性。此外，可以将专业容器 701 定制成只支持那些用于支持 DVD 和／或其它介质必须的特点，以便能用比完全支持“标准”容器对象所需要的较不强大或较便宜的计算资源处理和／或控制。

[0310] 本例中，专业“唯 DVD”容器 701 包括内容对象（财产）703，后 者包括一个指向视频标题内容 707 的“外部引用”705，它可以以不包括容器 701 的介质所用的那样的相同方式存储在 DVD 和／或其它介质中。视频标题内容 707 可以包括 MPEG-2 和、或 AC-3 内容 708，以及扰乱（保护）信息 710 和首部、结构和／或元数据 711。外部引用 705 含有的信息能指定（指向、标识和／或描述）为了使用内容和容器 701 上未存储的其它信息而要应用或执行的特定外部过程。本例中，外部引用 705 指定视频标题内容 707 及其部件 708、710 和 711。另一种办法是，容器 701 可以在容器自身内存储视频标题内容的部分或全部，所用格式是容器 701 专用的一种格式和组织，而不是 DVD 和／或其它介质 700 所用的格式。

[0311] 本例中，容器 701 也包括一个控制对象（控制集）705，它规定使用视频标题内容 707 所要运用的规则。如实线箭头 702 所示，控制对象 707“施加到”内容对象（财产）703。如本例所示，规则 704 能规定要施加的保护过程，例如 CGMA 或 Matsushita 数据扰乱过程，并能通过规则 704 所含的外部引用 709，指定在进行保护方案时所用的数据扰乱信息 710。规则 704 中的简短说明“执行 CGMA”表示，该规则要求将用于 DVD 介质上内容的标准 CGMA 保护方案与视频标题内容 707 结合使用，但是一个不同的例子中除了“执行 CGMA”规则之外，还可以在控制对象 705 中规定任意其它规则，或者在控制对象 705 中规定任意其它规则来代替“执行 CGMA”规则，这种任意其它规则包括其它标准 DVD 保护机制，诸如 Matsushita 数据扰乱方案和其它权利管理机制。外部引用 709 允许规则 704 建立在保护信息 710 的基础上，其存储和控制的格式和方式与不含容器 701 和／或只有在处理容器 701 的上下文中才有意义的保护信息的 DVD 相同。

[0312] 图 8 表示一例含有一个“标准”安全容器 801 的 DVD 介质 800。本例中，“标准”容器提供了图 7 容器的所有功能（如果需要的话），但是还可以提供附加的和／或比“唯 DVD”容器上能得到的更广泛的权利管理和／或内容使用功能（例如用使用安全节点的各种不同

平台操作的功能）。

[0313] 图 9 表示一例更复杂的 DVD 介质 800，它具有的标准容器 901 提供图 7 容器的所有功能（如果需要的话），并且能与其它标准容器 902 一样地工作，该其它标准容器 902 无论是位于相同 DVD 介质上还是 来自另一个远程安全节点或网络。本例中，标准容器 902 可以包括一个向标准容器 901 的内容对象 902 施加的补充控制对象 904。同样在本例中，容器 902 可以提供附加的规则，诸如一种允许 / 扩展权利的规则，它允许对 DVD 900 上的内容进行一定次数（例如 5 次）的复制。这种方案增加了在多个平台之间通过访问“后通道”（诸如通过机顶盒或其它能够与另外的网络或计算机双向通信的硬件）对 DVD 内容的权利管理进行控制的灵活性。

[0314] 具用安全容器的 DVD 盘的其它用途

[0315] 图 10 表示使用一个“新的”DVD 盘 - 即介质中包括有特殊的 DVD 安全容器的 DVD 盘。在一个例子中，这种容器在两种可能的情况下使用 ：第一种情况是，使用光盘的是一个“老式”播放器 (DVD 设备，即不配备按照本发明提供权利管理的安全节点的 DVD 设备）；第二种情况是，使用光盘的是一个“新式”播放器 - 即配备按照本发明提供权利管理的安全节点的 DVD 设备。本例中，“新式”播放器内的安全节点配置了必要的功能来处理其它复制保护信息，例如 CGMA 控制码和主要由 Matsushita 公司提出并开发的数据扰乱格式。

[0316] 例如，在图 10 所示的情况下，“新式”播放器（它含有按照本发明的安全节点）能识别安全容器在盘上的存在。播放器于是将该专用 DVD 安全容器从盘上装入驻留的安全节点。安全节点打开该容器，并通过应用来自控制对象的规则，实现和 / 或实施适当的规则和与内容关联的使用后果。这些规则非常灵活。在一个例子中，规则例如可以调用其它保护机制（其中例如，CGMA 保护码和 Matsushita 公司的数据扰乱方法），后者可以在容器的内容（或财产）部分找到。

[0317] 在图 10 所示的另一个例子中，盘上的专用 DVD 容器仍然允许“老式”播放器使用按照常规可以使用的一预定限度数量的内容材料。

[0318] 没有安全节点的 DVD 盘的使用例

[0319] 现在参见图 11，讨论另一种情况。图 11 表示具有两种可能应用的“老式”DVD 盘的使用例 ：第一例中，使用光盘的是一个“老式”播放器 - 即不配备按照本发明提供权利管理的安全节点的 DVD 设备）；第二例中，使用光盘的是一个“新式”播放器（即配备了安全节点）。

[0320] 在第一种情况下，“老式”播放器内按常规方式播 DVD 内容。在第二种情况下，“新式”播放器将会识别出在介质中没有存储一个容器。于是它就在设备的驻留存储器中构建一个“虚拟”容器。为此，它构建一个容器内容对象，并且还构建一个含有适当规则的控制对象。在一个特定例子中，它需要应用的唯一可应用的规则是“执行 CGMA”- 但是在其它例子中，可以采用更多的和 / 或不同的规则。然后将虚拟容器提供给“新式”播放器内的安全节点去执行按照本发明的使用权利管理。尽管图 10 和 11 中没有表示，在 DVD 上下文中使用的虚拟和非虚拟容器中也都可以提供“外部引用”的使用。

[0321] 在至少间或连接的情况下操作时用于共享中介的和组合的权利的示范性装置举例。

[0322] 如上所述，可以将几个不同设备和 / 或其它系统的权利管理资源，按照不同的逻

辑和/或物理关系进行灵活的组合，从而例如产生更多的和/或不同的权利。这种权利管理资源的组合可以通过与一个或多个远程权利管理机构的连接而实现。图 12 ～ 14 是表示权利管理机构在各种上下文中如何使用的一些非限定性例子。

[0323] 例如，图 12 显示一个与局域网 (LAN)1002 连接的权利管理机构中介 1000。LAN 1002 需要的话可以连接到广域网。LAN 1002 将权利管理机构中介 1000 连接任何数量的设备，其中例如播放器 50、个人电脑 60、CD “塔”型服务器 1004。在图示例中 LAN 1002 包括一个调制解调器组（和/或网络协议服务器，图中未表示）1006，它允许膝上型计算机 1008 通过拨号电话线 1010 与权利管理机构中介 1000 相连。另外，膝上型计算机 1008 与权利管理机构中介 1000 的连接也可以采取其它网络和/或通信装置，例如因特网和/或其它广域网 (WANs)。光盘播放器 50A 可以与膝上型计算机 1008 在用户膝上相连。根据以上叙述，图 12 中的任何或所有设备都可以包括一个或多个安全节点 72。

[0324] 权利管理机构中介 1000 可以充当权利的仲裁者和/或调解者。例如，膝上型计算机 1008 和相关的播放器 50A 当处于独立配置时可能只有有限的使用权利。然而，当膝上型计算机 1008 通过调制解调器组 1006 和 LAN 1002 和/或通过其它通信装置连接权利管理机构中介 1000 时，该膝上型计算机就可以获得使用盘 100 的不同的和/或扩展的权利（例如可以访问不同的内容部分，不同的定价、不同的提取和/或再传播权利，等等）。与此类似，播放器 50、设备 60 和设备 1004 也可以通过在 LAN 1002 上与权利管理机构中介 1000 的通信，配备一个增强的和/不同的光盘使用权利集合。最好通过使用上文引用的 Ginter 等人的专利说明书中披露的类型的容器，来确保与权利管理机构中介 1000 的来往通信。

[0325] 图 13 表示另一例在家庭环境内权利管理机构中介 1000 的使用。本例中，膝上型计算机 1008 可以通过高速串行 IEEE 1394 总线和/或通过其它通信装置，与基于家庭的权利管理机构中介 1000 连接。此外，权利管理机构中介 1000 能与下列任何或全部设备相连：

[0326] ●高清晰度电视 1100

[0327] ●一个或多个扬声器 1102 或其它音频传送器

[0328] ●一个或多个个人电脑 60

[0329] ●一个或多个机顶盒 1030

[0330] ●一个或多个光盘播放器 50

[0331] ●一个或多个其它权利管理机构中介 1000A ～ 1000N

[0332] ●任何其它家用或消费设备

[0333] 上述列举的设备任何或全部可以包括一个安全节点 72。

[0334] 图 14 表示权利管理机构中介 1000 的另一例使用。本例中，权利管理机构中介 1000 连接一个网络 1020，诸如局域网、广域网、因特网等等。网络 1020 可以提供权利管理机构中介 1000 与下列任何/或全部设备的连接：

[0335] ●一个或多个连接或偶尔连接的光盘播放器 50A、50B；

[0336] ●一个或多个联网的计算机 1022；

[0337] ●一个或多个盘阅读器塔/服务器 1004；

[0338] ●一个或多个膝上型计算机 1008；

[0339] ●一个或多个诸如权利与许可交换站的商业应用系统（参见上文引用的 Shear 等人的“可靠基础结构...”说明书）；

[0340] ●一个或多个卫星或其它通信上行链路 1026；

[0341] ●一个或多个电缆电视头端 1028；

[0342] ●一个或多个机顶盒 1030（可以连接到卫星下行链路 1032 和 / 或 光盘播放器 50C）；

[0343] ●一个或多个个人电脑设备；

[0344] ●一个或多个便携式光盘播放器 1034（可以通过其它设备连接，直接以及 / 或者偶尔断开）；

[0345] ●一个或多个权利管理机构中介 1000A ～ 1000N；

[0346] ●任何其它所需设备。

[0347] 上述列举的设备任何或全部可以包括一个安全节点 72。权利管理机构中介 1000 能分配和 / 或组合权利，由图 14 所示的任何或所有其它部件使用。例如，权利管理机构中介 1000 能向通过网络 1020 与中介连接的设备提供进一步的安全权利管理资源。图 14 所示的多个设备能参与并在永久或暂时连接的网络 1020 共同工作，共享单一节点的权利管理。与使用和 / 或控制这种多个设备和 / 或其它系统的当事人和 / 或小组关联的权利能按照潜在的与权利相关的规则和控制而被采用。举例来说，可通过公司经理的膝上型计算机 1008 得到的权利，可以以某种方式，与一个或多个公司下属职员的权利结合，或者代替后者，条件是职员的计算机或其它设备 60 以临时联网关系连接到网络 1020。一般来说，本发明的这个方面允许 DVD 分布式权利管理或者以其它方式封装和发送的受分布式、对等权利管理保护的内容。无论 DVD 设备或其它内容使用设备是否加入永久或暂时连接的网络 1020、无论参与分布式权利管理安排的设备和 / 或其它系统之间的关系是否是暂时的或是具有更持久的操作关系，这种分布式权利管理都能运行。

[0348] 例如，膝上型计算机 1008 可以有视设备操作所在上下文而定可获得的不同的权利。例如，在诸如图 12 所示的一个总公司环境中，膝上型计算机 1008 可以有一个权利集合。然而当相同的膝上型计算机 1008 与公司中的其它个人和 / 或小组合作、连接到更综合的网络 1020 时，可以被赋予一个不同的权利集合。当相同的膝上型计算机 1008 如图 13 中例子所示连在一般的家庭环境中时，可以被赋予另一个不同的权利集合。当相同的膝上型计算机 1008 连入其它环境中，可以被赋予更不同的权利集合，这其它环境的非限定性例子为：

[0349] ●与指定个人 / 或小组合作的家庭环境、

[0350] ●零售环境、

[0351] ●作为学生的教室装置、

[0352] ●在图书馆环境中与一个教师合作的教室装置、

[0353] ●工厂楼面、

[0354] ●与能执行专有功能的设备合作的工厂楼面，等等。

[0355] 作为更特定的例子，将诸如图 14 中所示 DVD 设备 50 的有限资源设备装置与价格不贵的网络计算机 (NC) 1022 相连，可以允许权利管理功能和 / 或当事人和 / 或设备的特有权利得到增强（或替换），方法是准许权利管理是 DVD 设备的部分和 / 或全部权利和 / 或权利管理功能与网络或个人计算机 (NC 或 PC) 相组合的结果。这种权利由于由可靠（安全）远程网络权利管理机构 1000 提供的权利管理功能的可获得性而可以得到进一步的增强、或替换。

[0356] 同样的设备一本例中是 DVD 设备 50，于是就能支持断开和连接装置中权利管理功能的不同排列，例如不同程度，并允许从由权利管理设备和 / 或其它系统组合而产生的权利和 / 或权利管理功能的可用性产生可用权利。这可以包括通过使用一个“较不”安全的和 / 或资源贫乏的设备或系统而得到的部分或全部权利的一个或多个组合，其中“较不”安全的和 / 或资源贫乏的设备或系统通过与一个“更加”安全的或安全“程度不同”的和 / 或资源丰富的和 / 或拥有不同权利的设备或系统的连接而得到增强、替换或修改，其中这种连接采用其中一个设备和 / 或这两个设备的、描述共享权利管理安排的权利相关规则和控制的权利和 / 或管理功能。

[0357] 在后一种情况下，连接到逻辑上和 / 或物理上远程的权利管理功能，能够扩展（例如增加可用安全权利管理资源）和 / 或改变 DVD 设备 50 或与 NC 1022、个人电脑 60 和 / 或远程权利管理机构 1000 相连的 DVD 设备的用户的可用权利的特性。在这种权利增强的情形中，额外的内容部分可以获得，价格可以改变，再传播权利可以改变（例如得到扩展），内容提取权利可以得到增加，等等。

[0358] 这种“联网权利管理”能够允许多个逻辑和 / 或物理关系形形色色的设备和 / 或其它系统的权利管理资源的组合，通过与一个或多个“远程”权利管理机构的连接而提供的增强资源，要么产生更大的权利，要么产生不同的权利。此外，在提供增加的和 / 或不同的权利管理功能和 / 或权利的同时，这种基于连接的权利管理安排还能支持 多地点的内容可用性，方法是提供远程可用内容 - 例如在远程的、基于因特网的环球网 (world wide web) 的、支持数据库的内容存储器中存储的内容 - 与一个或多个 DVD 盘 100 上的本地内容的无缝集成。

[0359] 在这个实例中，用户不仅能体验到增加的或不同的权利，而且能够使用本地 DVD 内容和补充内容（即从时间观点来说更流行、价值更高、更多样化、或从其它意义上说具有补充性等等的内容）。在这种情况下，DVD 设备 50 和 / 或 DVD 设备（或与这种设备连接的其它设备或系统）的用户可以将相同的权利、有差异的和 / 或不同的权利施加到本地或远程可用的内容，而本地和远程可用的内容的部分本身在由用户和 / 或设备使用时可以受制于有差异的或不同的权利。这种安排能支持总体上极大地增加用户在一次内容检索和 / 或使用活动中可有效获得的被无缝集成的用户内容的机会。

[0360] 这种增强权利的远程管理机构 1000 可以用调制解调器（见图 12 中的项 1006）直接连接到 DVD 设备 50 和 / 或其它设备，并且 / 或者通过使用诸如串行 1394 可兼容的控制器的 I/O 接口（例如，通过在能用 1394 启动的 DVD 设备与本地个人电脑之间的通信，其中，个人电脑充作一个智能同步或异步信息通信接口，连接一个或多个远程管理机构，包括作为增强和 / 或提供 DVD 设备中权利管理的本地权利管理结构的本地 PC 60 或者 NC 1022）和 / 或通过诸如有线和 / 或无线网络连接的其它数字通信装置，直接或间接连接。参与者和 / 或参与的 DVD 设备 50 或其它系统被提供的、购买的或以其它方法获得的权利能在这种对等相关设备和 / 或其它系统之间交换一只要它们参加一个永久或暂时连接的网络 1020。在这种情况下，只要这类设备和 / 或其它系统参加权利管理系统，例如 Ginter 等人专利中描述的虚拟传播环境，并且采用其中描述的权利转让和其它权利管理功能，则权利就可以被易货交易、出卖、以其它方式有价交换和 / 或出租。例如，本发明的这个方面允许当事人交换他们购买了权利的游戏或电影。还是在该例中，某个人可以从邻居购买一部分观看电

影的权利，或将从游戏出版商收到的信用转让给另一提供信用是为了将游戏超级传播到几个熟人，这种信用能被转让（交换）给某个朋友，以买到该朋友的部分权利，一定次数地玩不同的游戏，等等。

[0361] 虚拟权利过程的例子

[0362] 在图 15A ～ 15C 表示的过程中，两个或更多设备或其它设备的权利管理部件建立一个与一个事件、操作和 / 或其它动作关联的虚拟权利机器环境。该过程有许多启动方式。在一个例子中，设备用户（和 / 或代表用户、用户小组和 / 或自动执行动作的系统的计算机软件）用第一个设备执行一个动作（例如请求该设备播放一个安全容器的内容、提取一部分内容元素、运行一个受保护的计算机程序，授权一个工作流过程步骤、启动机器工具上的一个操作、播放一首歌曲等等），导致与该第一个设备关联的一个权利管理部件的启动（图 15A 中框 1500）。在其它例子中，该过程的启动所根据的是一个自动生成的事件（例如根据一天的某个时间等等），一个随机或伪随机事件和 / 或这类事件与用户启动事件的组合。

[0363] 过程一旦开始，权利管理部件，诸如安全节点 72（例如 Ginter 等人专利中披露的 SPE 和 / 或 HPE）就确定，就该动作而言，该用户可用与该第一个设备关联的哪些权利（图 15A 中框 1502），如果有的话。权利管理部件也确定与完全或部分位于其它设备的用户可用的动作关联的协调和 / 或合作的权利（图 15A 中框 1502）。

[0364] 在一个例子中，执行这些步骤的方法是安全地发送一个请求给权利管理机构服务器 1000，标识出第一个设备、拟执行动作的性质、以及该权利管理机构服务器所需或要求的其它信息。这种其它信息例如包括：

[0365] ●请求的日期和时间、

[0366] ●用户的身份、

[0367] ●网络连接的性质、

[0368] ●可接受的响应延迟等等，以及

[0369] ●任何其它信息。

[0370] 权利管理机构服务器 1000 对该请求的响应是，发回一个列表（或其它合适的结构）到第一个设备。这个列表例如可含有其它设备的标识，它们确实或可能具有与该拟执行的动作相关的权利和 / 或权利相关信息。

[0371] 在另一个实施例中，第一个设备可以将对其它设备的请求通知（例如定时询问）一个网络，该其它设备确实有或可能具有与该拟执行 的动作相关的权利和 / 或权利相关信息。当设备数目相对较少和 / 或不频繁变化时，定时询问是可取的。当权利管理机构服务器 1000 的功能分布于几个设备上时，定时询问也是可取的。

[0372] 本例中，与第一个设备关联的权利管理部件然后可以检查确实有或可能具有与该动作相关的权利和 / 或权利相关信息的设备和 / 或其它设备的用户的安全级（和 / 或类型）（图 15A 中框 1506）。这个步骤例如可以根据 Silbert 和 Van Wie 的专利披露的安全级和 / 或设备类型管理技术以及 Ginter 等人专利披露的用户权利、安全名称服务和安全通信技术来执行。设备和 / 或用户安全级的确定例如可以全部或部分根据设备和 / 或用户类。

[0373] 权利管理部件然后可以决定每个其它设备和 / 或用户是否有足够的安全级，以合作形成与该动作关联的权利集合和 / 或权利相关信息（图 15A 中框 1508）。对每个设备进行评估后，可能有些设备和 / 或用户有足够的安全级，其它则没有。本例中，如果没有足够

的安全级（判断框 1508 的“否”出口），权利管理部件可以创建一个检查记录（例如 Ginter 等人专利披露的格式的检查记录）（图 15A 中框 1510），并结束过程（图 15A 中框 1512）。这种检查记录用于要么立即传输给一个负责的管理机构，要么在本地存储，以后再传输。检查记录步骤例如可以包括，递增一个记录安全级故障的计数器（诸如 Ginter 等人专利中的与概要服务关联的计数器）。

[0374] 如果设备 / 或用户具有要求的安全级（框 1508 的“是”出口），本例中的权利管理部件就根据设备和 / 或用户类和 / 或其它配置和 / 或特点进一步进行判断（图 15B 中框 1514）。这种判断可根据任何数量的因素，诸如：

[0375] ●设备只有通过一个吞吐量不足的网络接口才能访问；

[0376] ●这一类的设备一般其资源根本不足以完成该动作或该动作的相关部分，或者具有可接受的性能、质量或其它特点；

[0377] ●由于各种条件，用户类不适宜（这些条件例如：年龄、安全许可、国籍、司法、或任何其它基于类的或其它的用户特点）；和 / 或

[0378] ●其它因素。

[0379] 举例来说，判断框 1514 的执行的部分方法是，向用户提出一个选择，用户拒绝该选择。

[0380] 如果权利管理部件内的过程确定这种设备和 / 或用户类不适宜（框 1514 的“否”出口），如果需要或希望的话，权利管理部件写一个检查记录（图 15B 中框 1516），然后过程可以结束（图 15B 中框 1518）。

[0381] 但是，如果权利管理部件确定这种设备和 / 或用户类适宜继续（框 1514 的“是”出口），权利管理部件可确定执行第一个设备和其它共同作用的设备上的动作所用的权利和资源（图 15B 中框 1520）。这个步骤的执行，例如可采用 Ginter 等人专利披露的任一或全部处理技术。例如，方法功能可包括能制订一个向各有关设备的请求的事件处理功能，该请求要描述与动作或部分动作相关的、总体或部分潜在地适于被该设备总体或部分处理的信息。本例中，这类请求以及相关的响应可以用 Ginter 等人专利披露的交互方法技术来管理。如果这种交互作用需要更多的信息，或者结果不明确，则权利管理部件例如就可以与用户通信，允许用户进行选择，例如在各种可用的、功能各异的选择中进行选择，并且 / 或者权利管理部件可以进行一个有关资源、权利和 / 或权利相关信息的谈判（例如用 Ginter 等人专利披露的谈判技术）。

[0382] 权利管理部件下一步判断是否有足够的权利和 / 或资源可用于执行所请求的动作（图 15B 中判断框 1522）。如果可用于执行该动作的权利和 / 或资源不够（框 1522 的“否”出口），权利管理部件就写一个检查记录（图 15B 中框 1524），然后结束该过程（图 15B 中框 1526）。

[0383] 本例中，如果有足够的权利和 / 或资源可用（框 1522 的“是”出口），权利管理部件就判断，为了完成整个动作，是否还要处理其它事件（图 15B 中框 1528）。例如，如果得不到完成动作所必须的权利和 / 或资源，可能希望只执行整个动作的一部分。如果需要和 / 或要求更多的事件（框 1528 的“是”出口），权利管理部件会对每一这种事件重复执行框 1520、1522（可能还执行框 1524、1526）。

[0384] 如果有足够的权利和 / 或资源可用于各事件（框 1528 的“否”出口），则如果需要

或要求的话，权利管理部件就向用户提供一个关于对执行该动作所需权利和／或资源其它可用选择对象的选择（图 15B 中框 1530）。另外和／或除此之外的方法是，权利管理部件依靠用户优选信息（和／或缺省信息）代表用户“自动地”作出这种判断（例 如总体费用、性能、质量等等）。在另一个实施例中，可以利用用户类别来过滤或以其它方式辅助在可选方案中作出选择。在另一个实施例中，可以采用人工智能（例如包括专家系统技术）来辅助在可选方案中作出选择。在另一个实施例中，可以将上述（和／或其它）任何或全部技术的组合用于这个选择过程。

[0385] 如果对权利和／或资源没有可以接受的其它选择，或者由于选择过程的其它否定因素（例如，用户按下图形用户界面中的“取消”钮、用户交互作用过程超过了进行选择的规定可用时间等等）（框 1530 的“否”出口），权利管理部件就写一个检查记录（图 15B 中框 1532），然后结束该过程（图 15B 中框 1534）。

[0386] 但是，如果选择过程确定了用于执行动作的一个或多个可接受的权利和／资源组并且所处理的判断是肯定的（框 1530 的“是”出口），权利管理部件就根据所选择的权利和／或资源单独用第一个设备或者第一个设备与任何其它设备（例如权利管理机构 1000 或任何其它相连的设备）的组合执行拟执行的动作，（图 15C 中框 1536）。对拟执行动作的这种合作执行例如包括：

[0387] ●用第一个设备执行该动作的部分或全部；

[0388] ●用第一个设备以外的一个或多个其它设备（例如权利管理机构 1000 和／或一些其它设备）执行该动作的部分或全部；

[0389] ●用第一个设备执行该动作的一部分，一个或多个其它设备执行该动作的一部分；或者

[0390] ●上述方式的任何组合。

[0391] 例如，该步骤可用 Ginter 等人专利中披露的事件处理技术来执行。

[0392] 举例来说，第一个设备可能具有完成特定任务（例如从光盘读取一定信息）所需的全部资源，但是没有完成此任务所需的权利。在这种情况下，第一个设备通过上述步骤来获得其执行该任务所需的其它权利。在另一个示意性例子中，第一个设备可能具有完成特定任务所需的全部权利，但是没有完成此任务所需的资源。例如，第一个设备可能没有足够的硬件和／或软件资源可用于存取、处理或以某些方式使用信息。本例中，步骤 1536 可以部分或全部由某些其它设备、或部分或全部根据第一个设备所提供权利的设备来执行。在另一个例子中，第一个设备要执行一定的动作既缺少必需的权利又缺少必需的资源，可能要依靠一个或多个其它设备来提供这种资源和权利。

[0393] 本例中，权利管理部件在动作结束时，写一个或多个检查记录（图 15C 中框 1538），然后结束该过程（图 15C 中框 1540）。

[0394] 本文描述了一种装置，它不仅充分满足了当前娱乐业对低费用、可规模生产的数字视盘或其它大容量光盘的复制保护方案的要求，而且还提供了用于更先进和／或安全平台的和用于在权利资源较少、较多和／或相异的设备之间的合作权利管理的增强的、可扩展的权利管理功能。尽管本发明是结合目前看来最实际、最可取的实施例而描述的，应当明白，本发明并不局限于所披露的实施例，相反，是旨在包含被本发明的精神和范围包括的各种改进和等价装置。

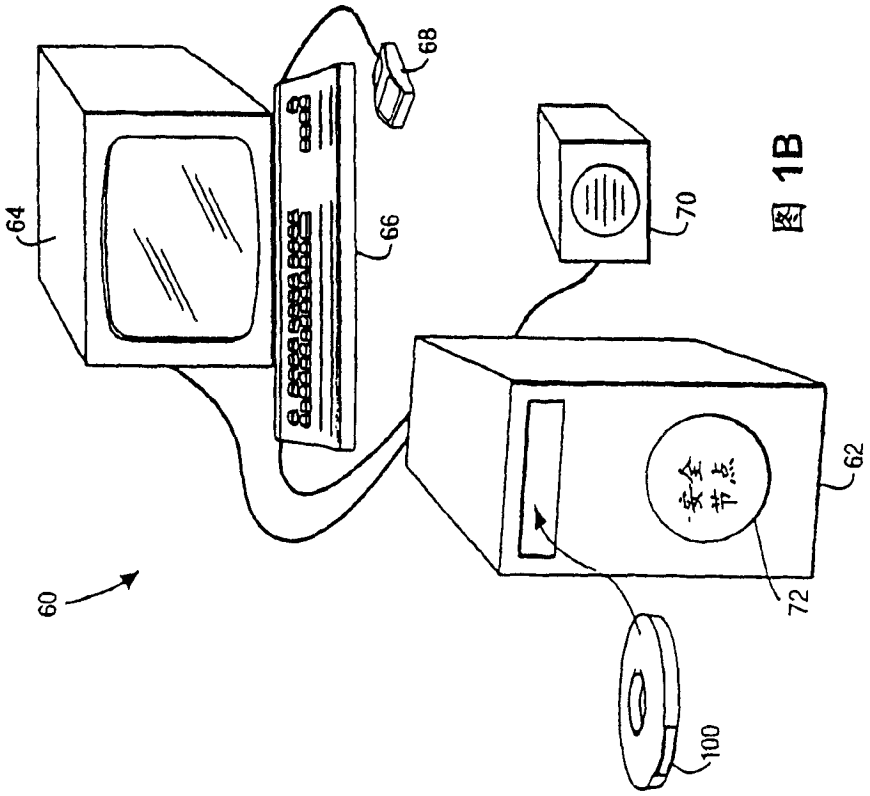


图 1B

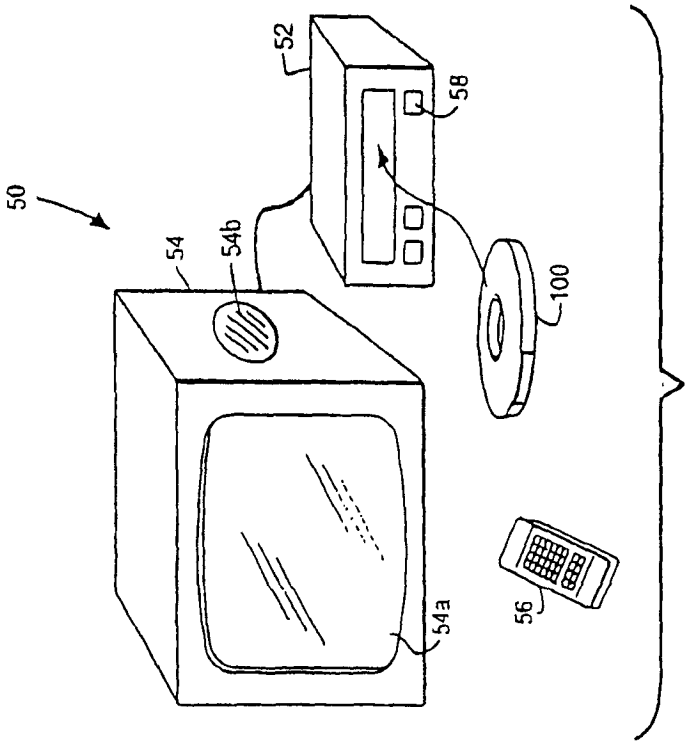


图 1A

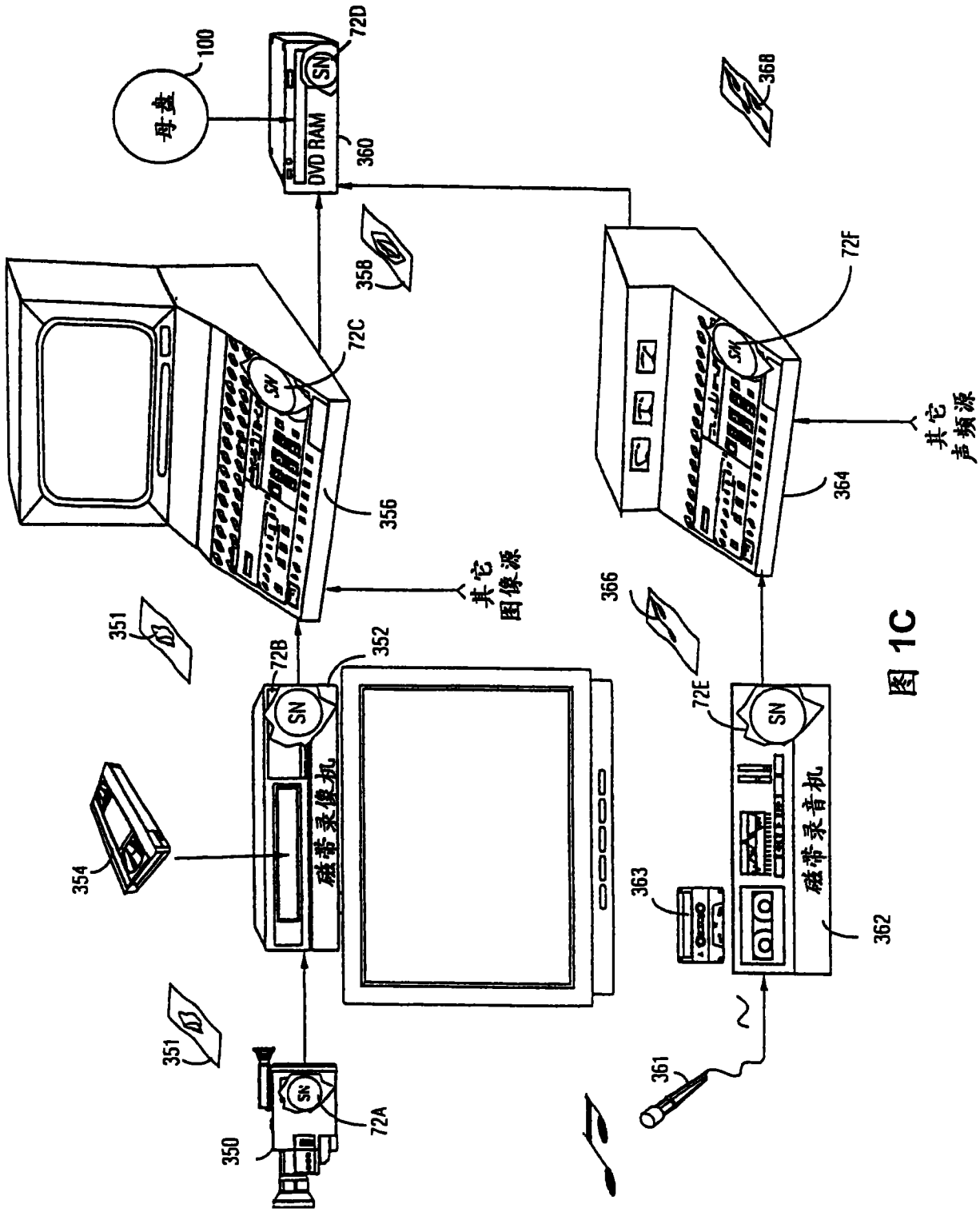

母盘
100
DVD RAM
360
72D
SN
368
358
72C
356
72F
364
其它
声频源
其它
图像源
366
351
72B
352
72E
磁带录像机
磁带录音机
354
363
362
351
361
350
72A

图 1C

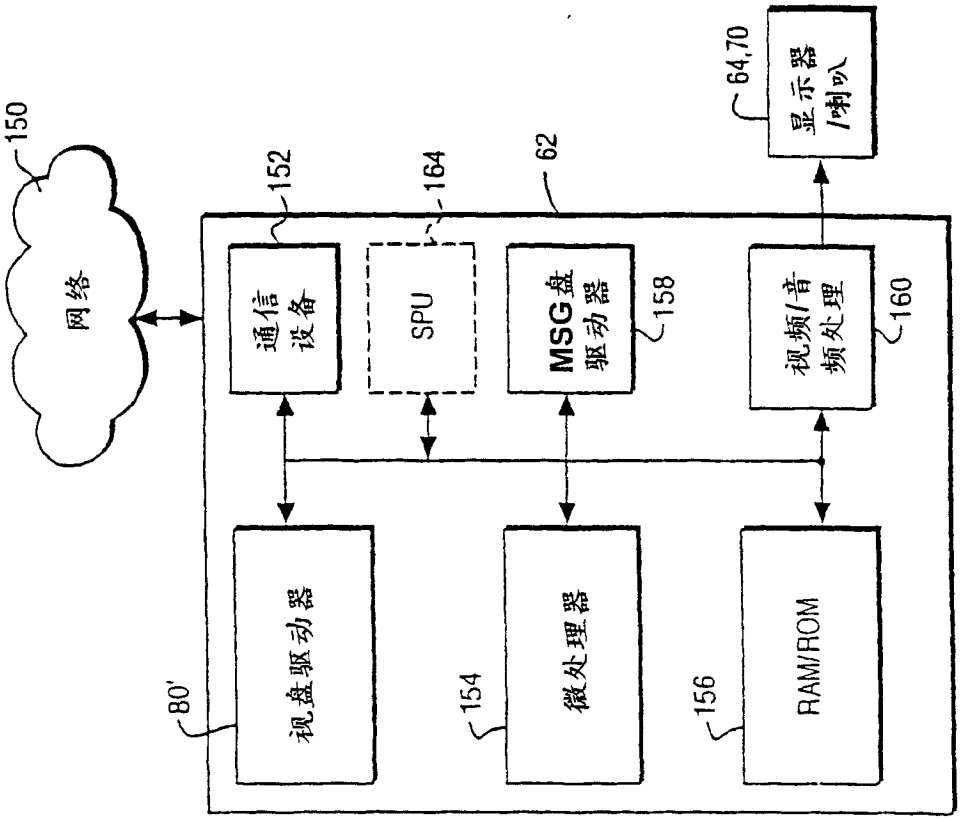


图 2B
安全节点结构例

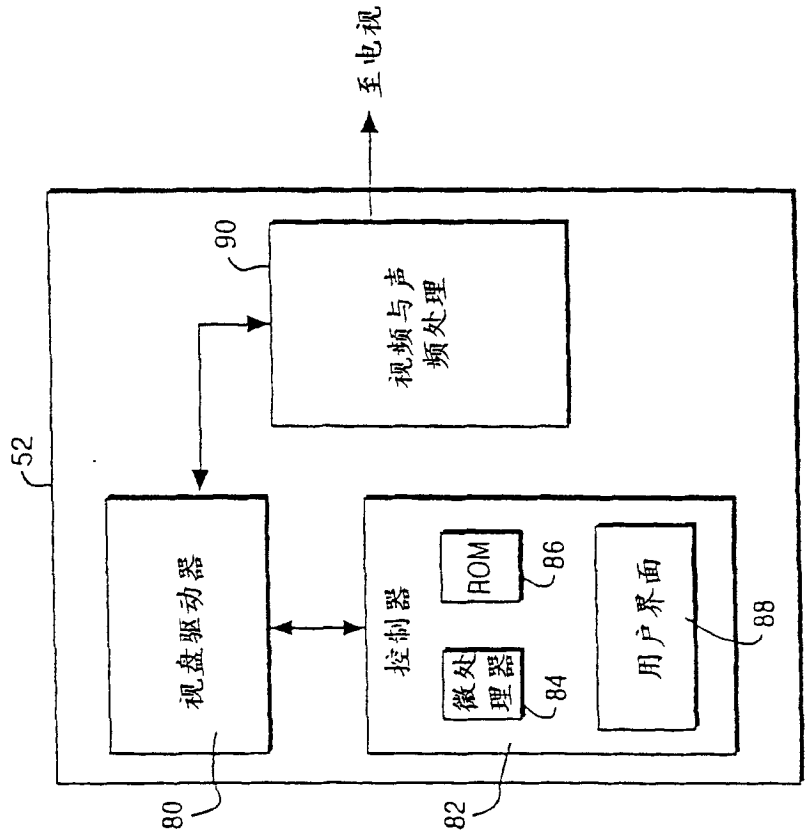


图 2A
播放器结构例

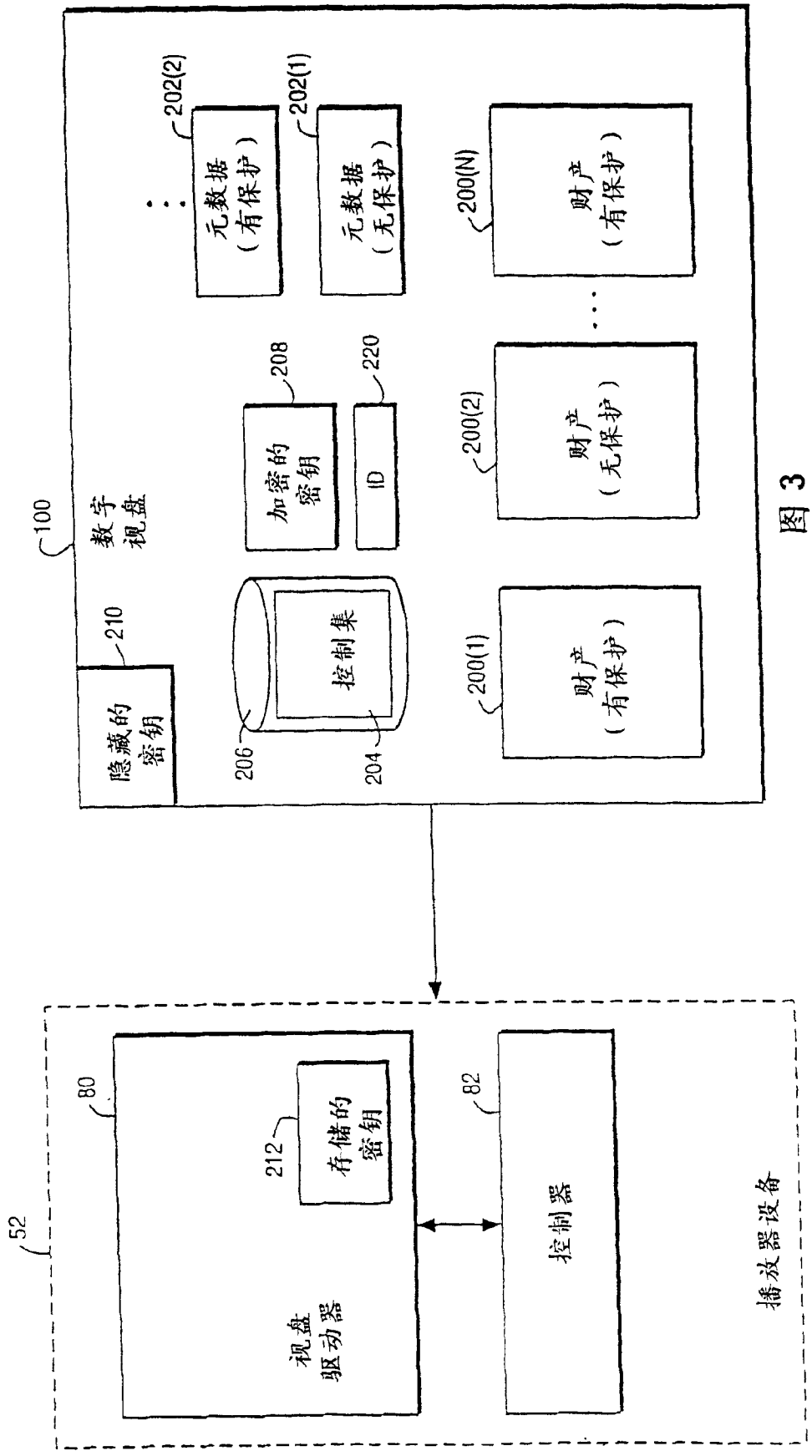

播放器设备
52
视盘驱动器
80
有储的密钥
212
控制器
82
数字视盘
100
隐藏的密钥
210
控制集
206
204
加密的密钥
208
ID
220
元数据（有保护）
202(2)
元数据（无保护）
202(1)
财产（有保护）
200(1)
财产（无保护）
200(2)
财产（有保护）
200(N)

图 3

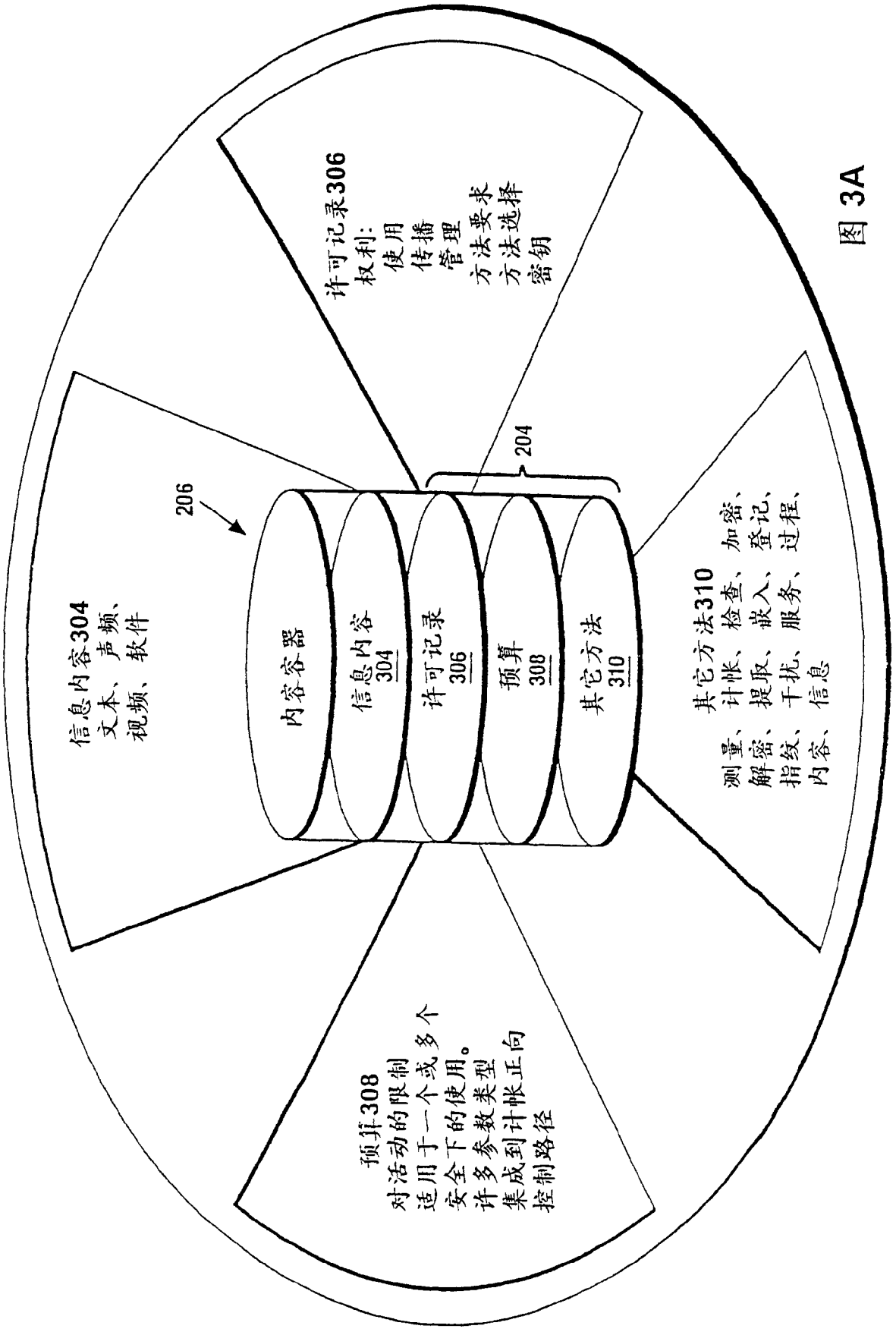

信息内容304
文本、声频、
视频、软件
206
内容容器
信息内容
304
许可记录
306
预算
308
其它方法
310
204
许可记录306
权利:
使用
传播
管理
方法要求
方法选择
密钥
预算308
对活动的限制
适用于一个或多个
安全下的使用。
许多参数类型
集成到计帐正向
控制路径
其它方法310
测量、计帐、检查、加密、
解密、提取、嵌入、登记、
指纹、干扰、服务、过程、
内容、信息

图 3A

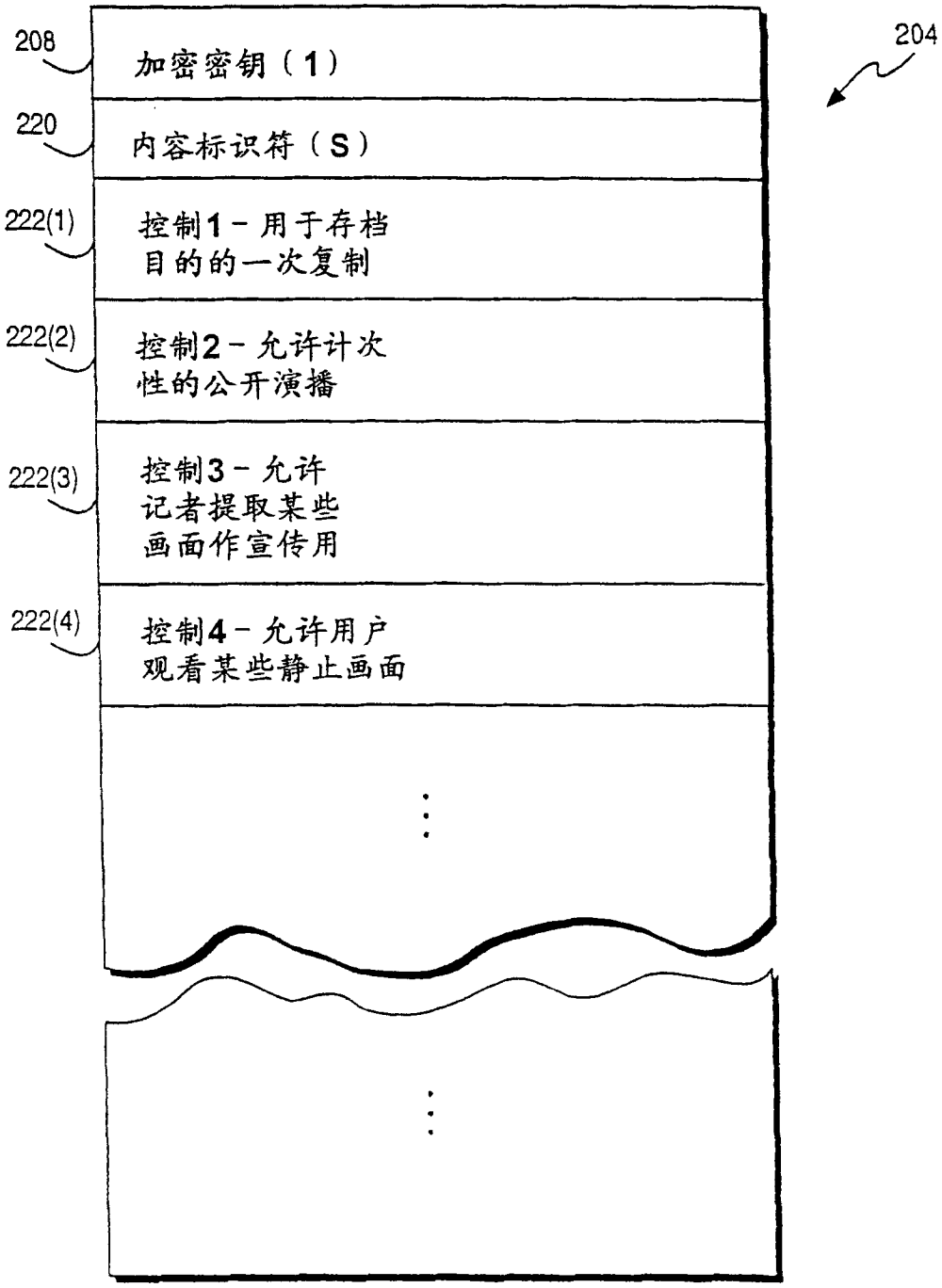

208
加密密钥（1）
204
220
内容标识符（S）
222(1)
控制1－用于存档
目的的一次复制
222(2)
控制2－允许计次
性的公开演播
222(3)
控制3－允许
记者提取某些
画面作宣传用
222(4)
控制4－允许用户
观看某些静止画面

图 3B

控制集例

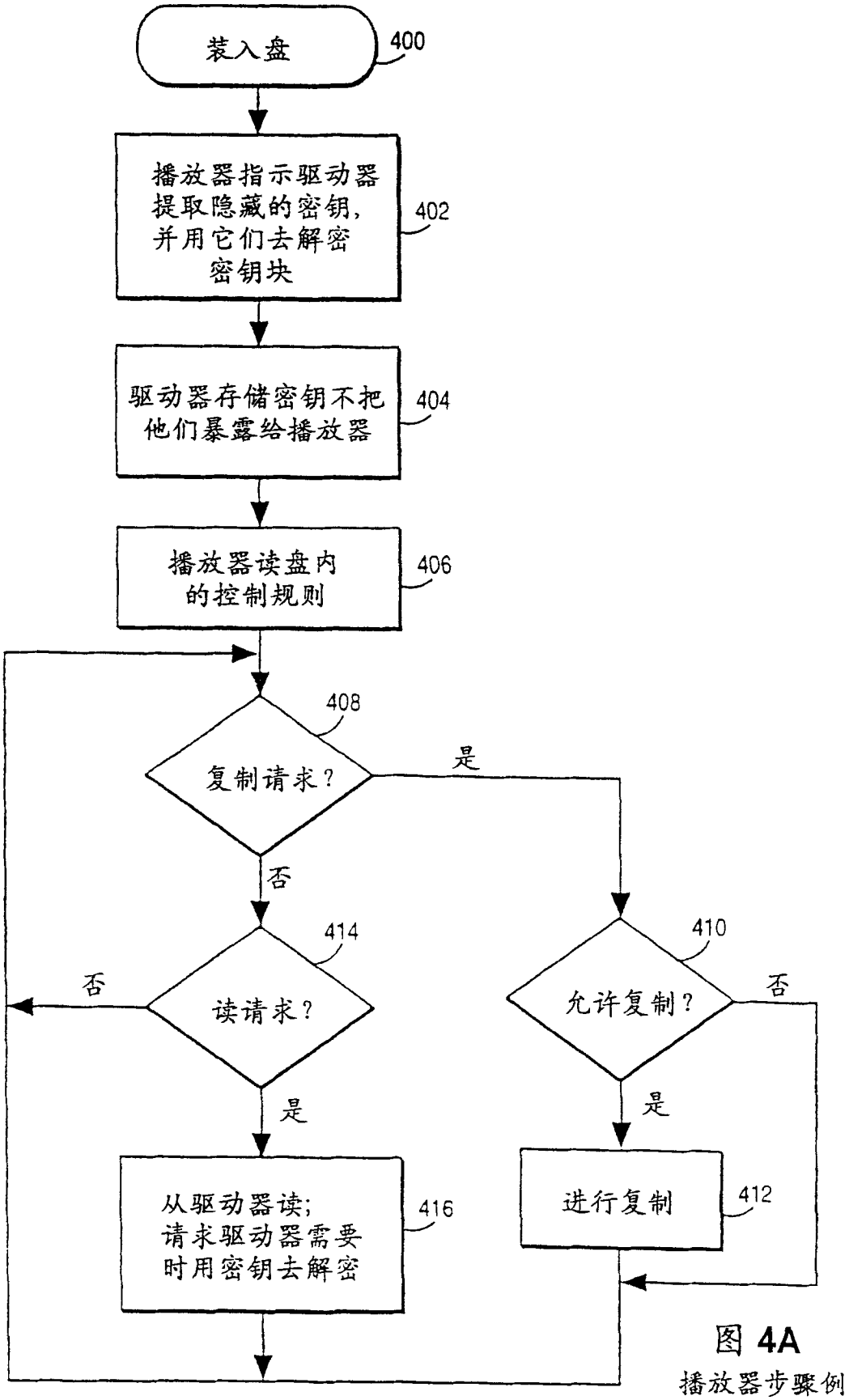

装入盘
400
播放器指示驱动器提取隐藏的密钥，并用它们去解密密钥块
402
驱动器存储密钥不把他们暴露给播放器
404
播放器读盘内的控制规则
406
408
复制请求？
是
否
414
读请求？
否
是
410
允许复制？
否
是
从驱动器读；请求驱动器需要时用密钥去解密
416
进行复制
412

图 4A
播放器步骤例

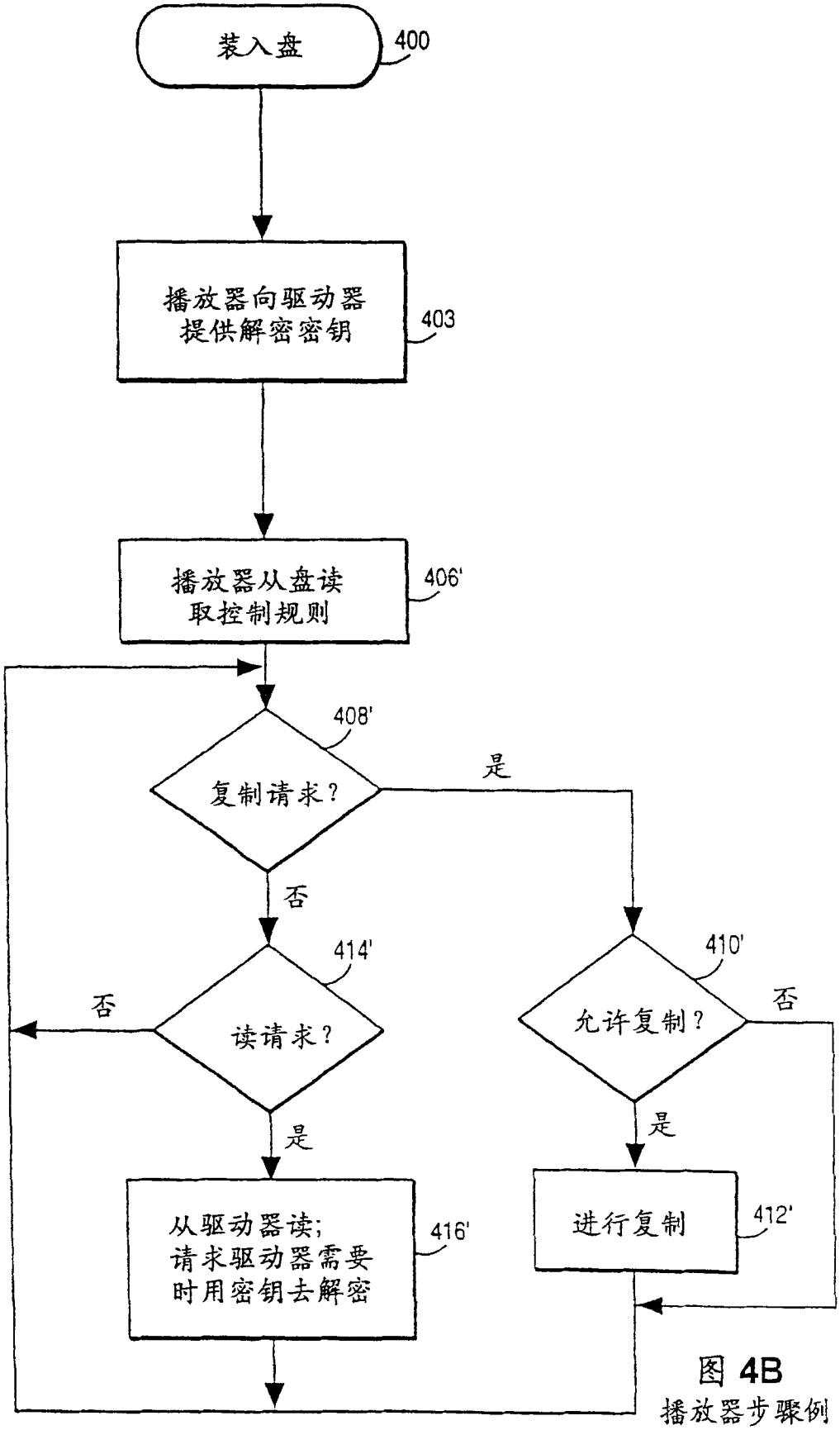

装入盘
400
播放器向驱动器提供解密密钥
403
播放器从盘读取控制规则
406'
408'
复制请求?
是
否
414'
读请求?
否
是
从驱动器读;请求驱动器需要时用密钥去解密
416'
410'
允许复制?
否
是
进行复制
412'

图 4B
播放器步骤例

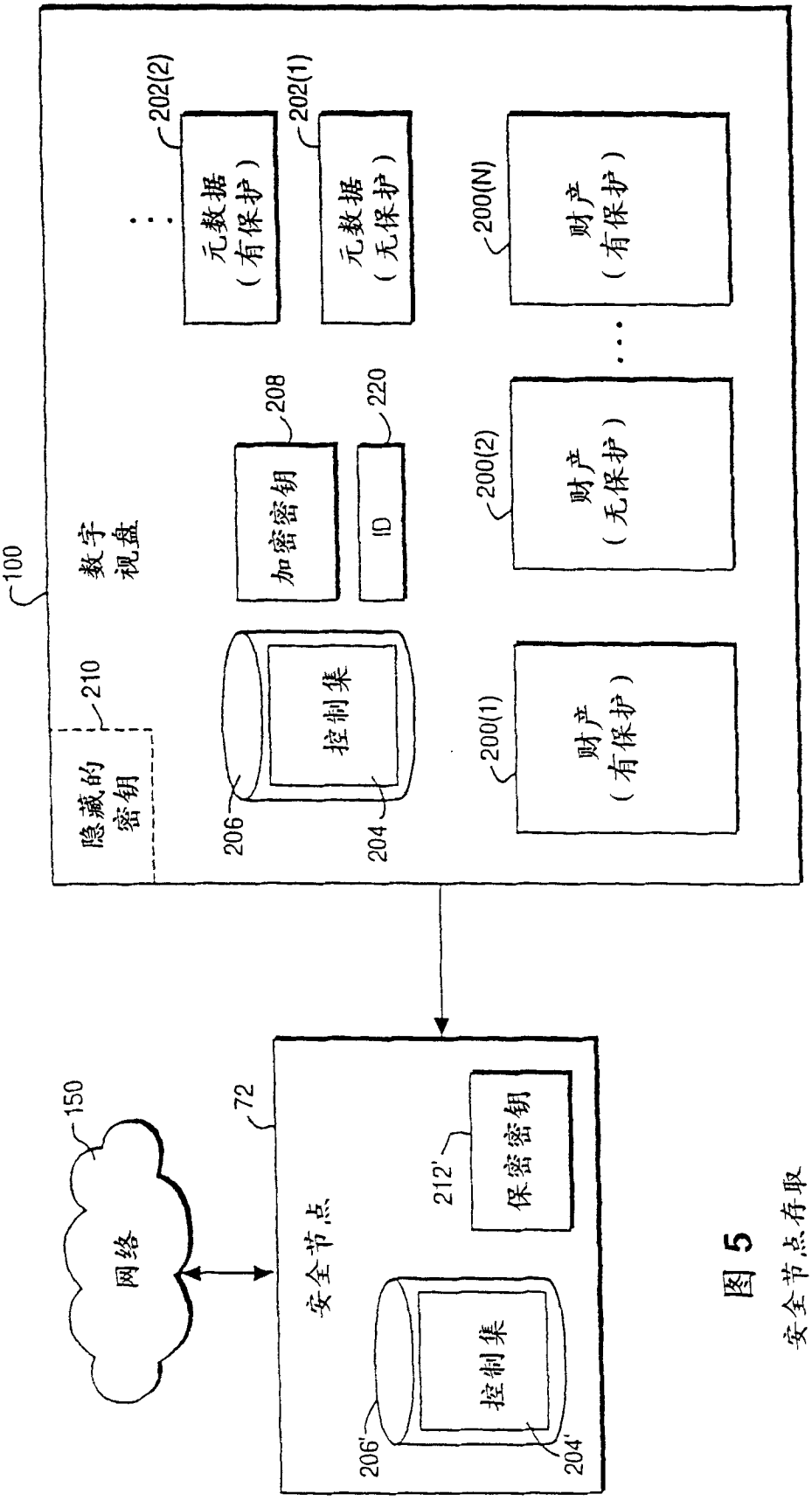

100
数字视盘
隐藏的密钥
210
206
控制集
204
加密密钥
208
ID
220
202(2)
元数据（有保护）
202(1)
元数据（无保护）
200(1)
财产（有保护）
200(2)
财产（无保护）
200(N)
财产（有保护）
150
网络
72
安全节点
212'
保密密钥
206'
控制集
204'

图 5
安全节点存取

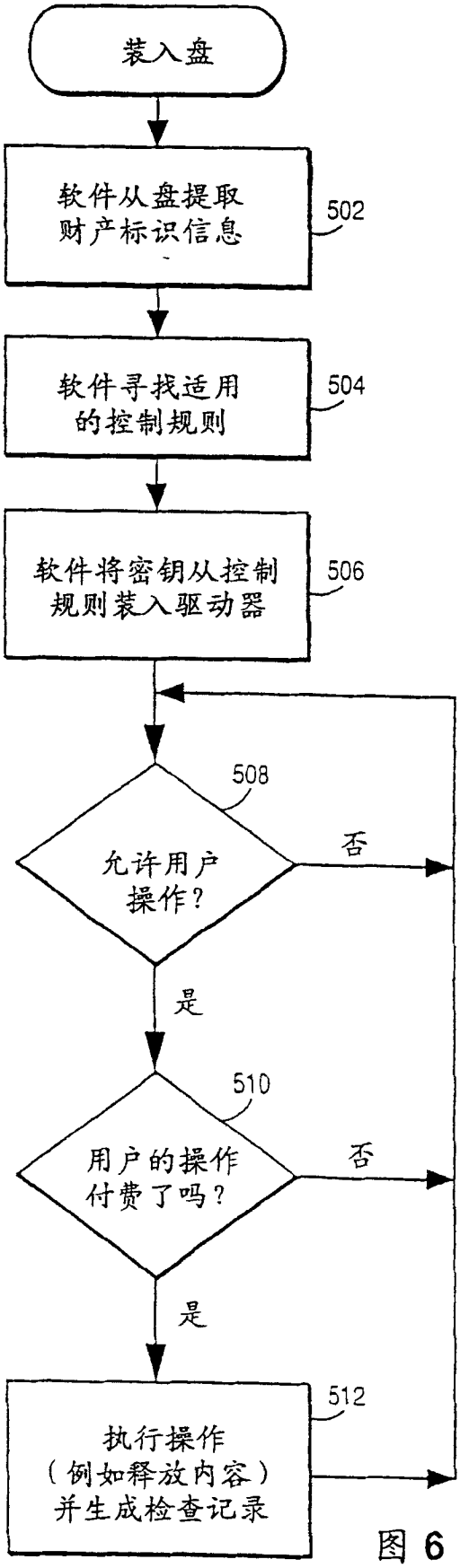

装入盘
软件从盘提取财产标识信息
502
软件寻找适用的控制规则
504
软件将密钥从控制规则装入驱动器
506
508
允许用户操作？
否
是
510
用户的操作付费了吗？
否
是
512
执行操作（例如释放内容）并生成检查记录

图 6

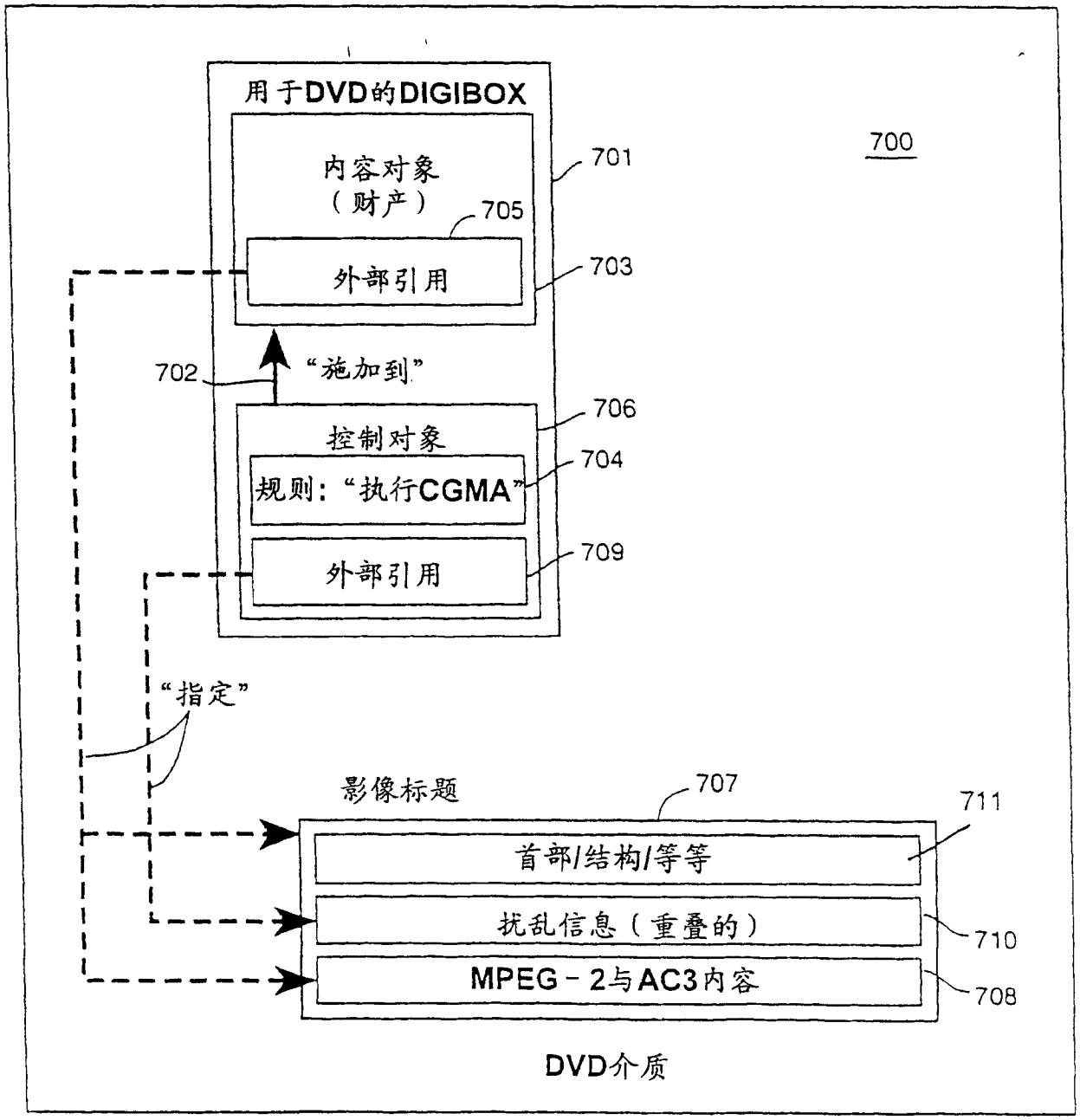

用于DVD的DIGIBOX
内容对象
（财产）
外部引用
“施加到”
控制对象
规则：“执行CGMA”
外部引用
“指定”
影像标题
首部/结构/等等
扰乱信息（重叠的）
MPEG－2与AC3内容
DVD介质
700
701
705
703
702
706
704
709
707
711
710
708

图 7

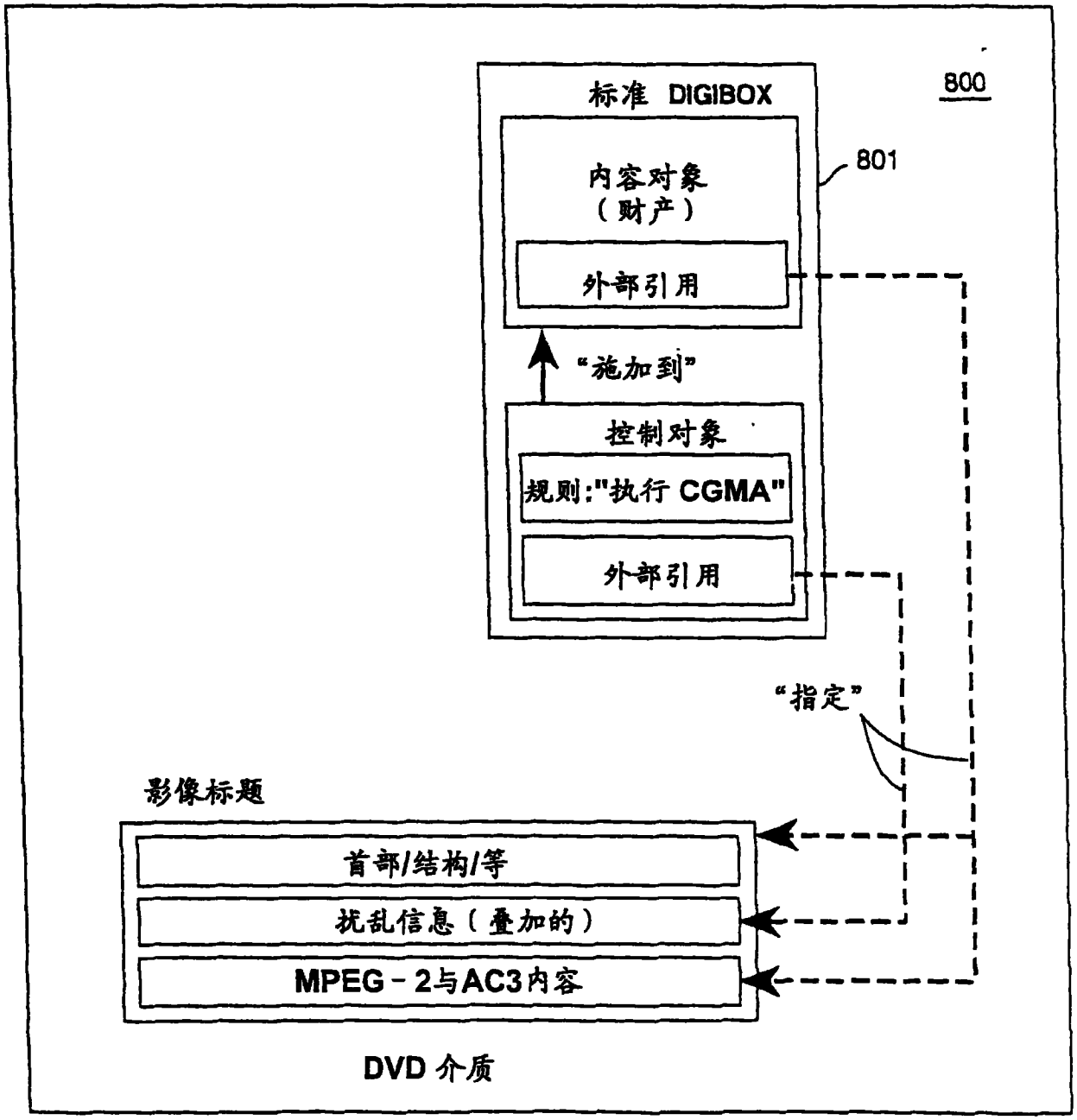

800
标准 DIGIBOX
801
内容对象
（财产）
外部引用
“施加到”
控制对象
规则:"执行 CGMA"
外部引用
“指定”
影像标题
首部/结构/等
扰乱信息（叠加的）
MPEG－2与AC3内容
DVD 介质

图 8

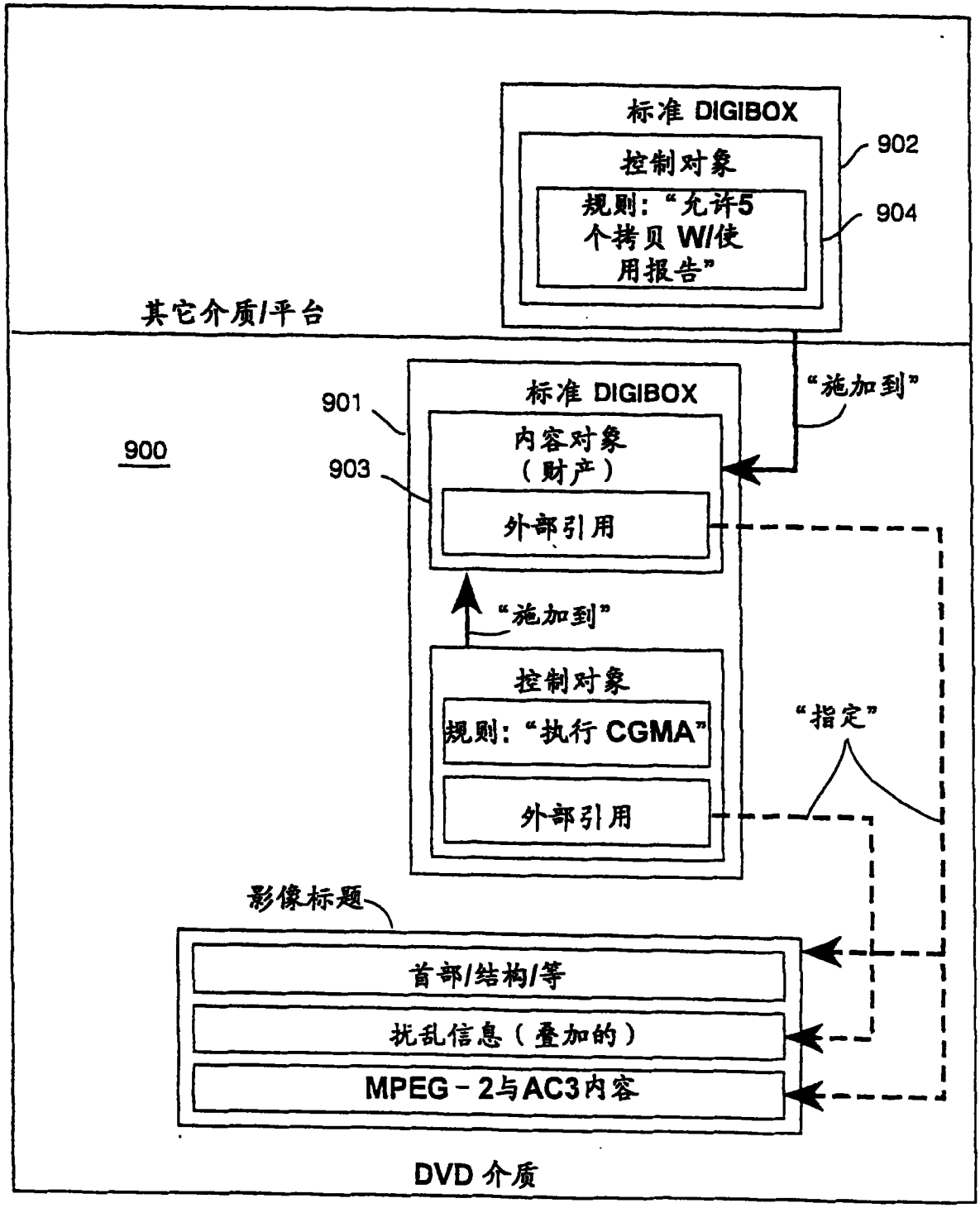

标准 DIGIBOX
控制对象
规则："允许5个拷贝 W/使用报告"
902
904
其它介质/平台
"施加到"
901
标准 DIGIBOX
900
内容对象（财产）
903
外部引用
"施加到"
控制对象
规则："执行 CGMA"
"指定"
外部引用
影像标题
首部/结构/等
扰乱信息（叠加的）
MPEG－2与AC3内容
DVD 介质

图 9

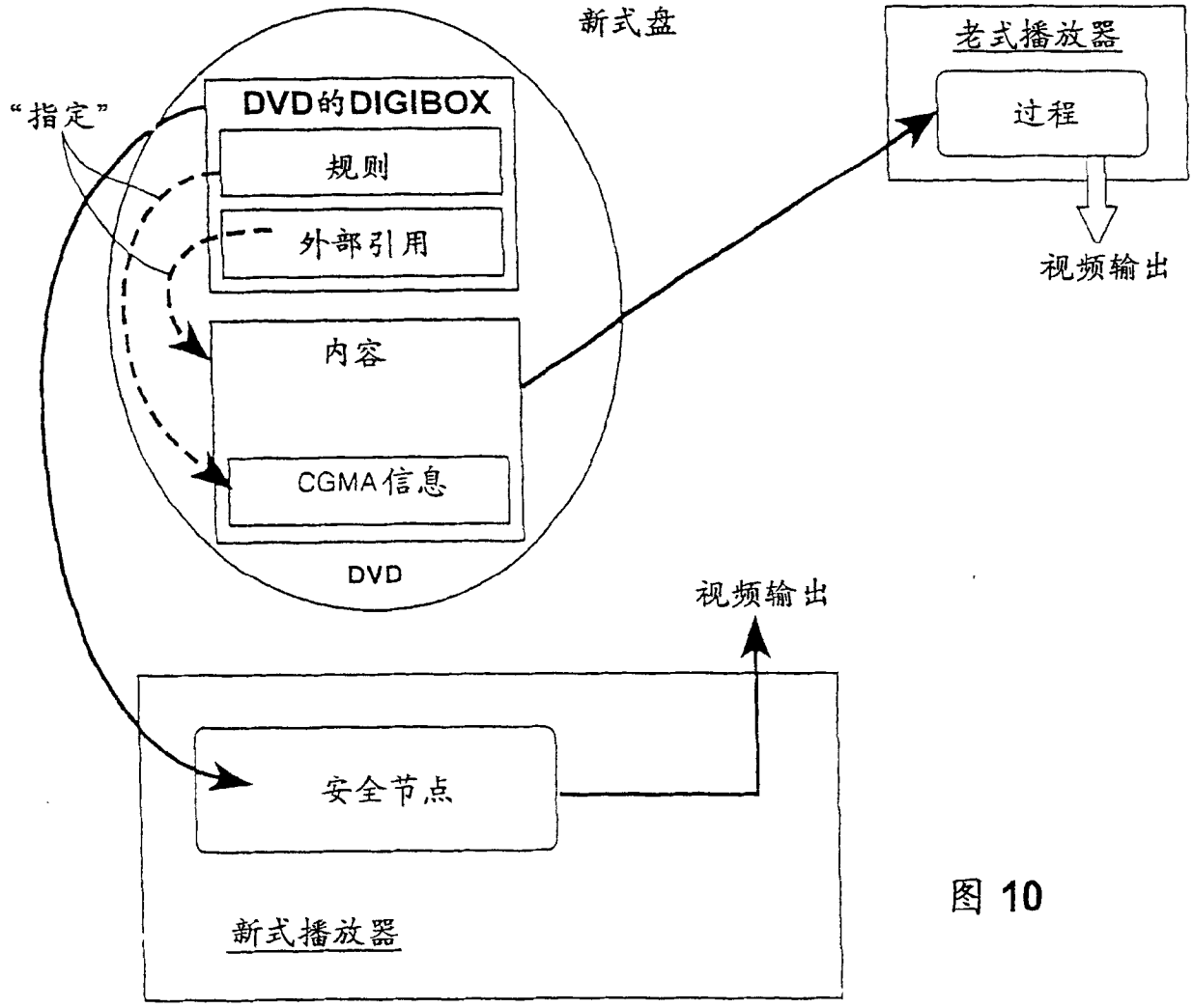

新式盘
"指定"
DVD的DIGIBOX
规则
外部引用
内容
CGMA信息
DVD
老式播放器
过程
视频输出
视频输出
安全节点
新式播放器

图 10

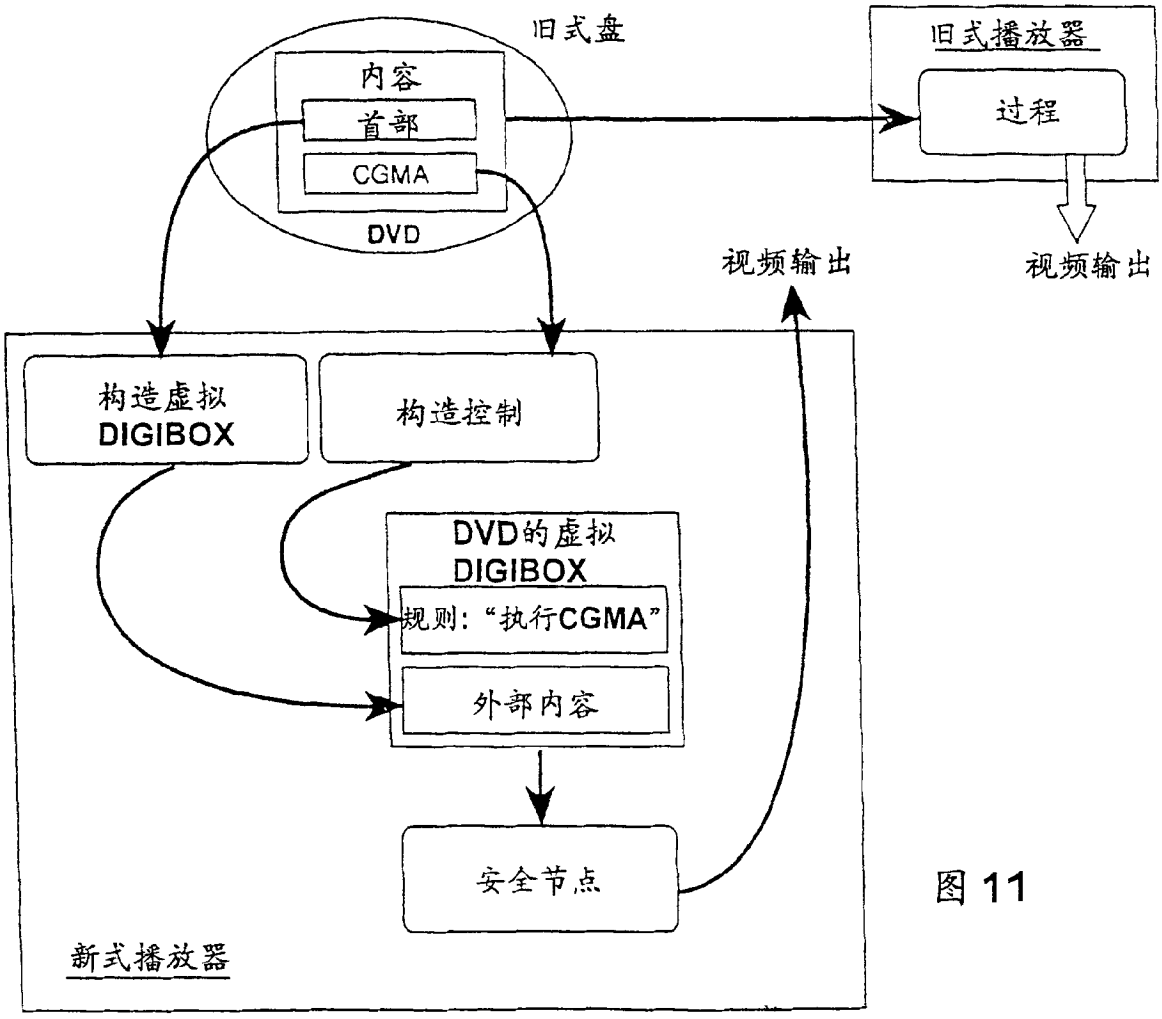

旧式盘
内容
首部
CGMA
DVD
旧式播放器
过程
视频输出
视频输出
构造虚拟
DIGIBOX
构造控制
DVD的虚拟
DIGIBOX
规则："执行CGMA"
外部内容
安全节点
新式播放器

图 11

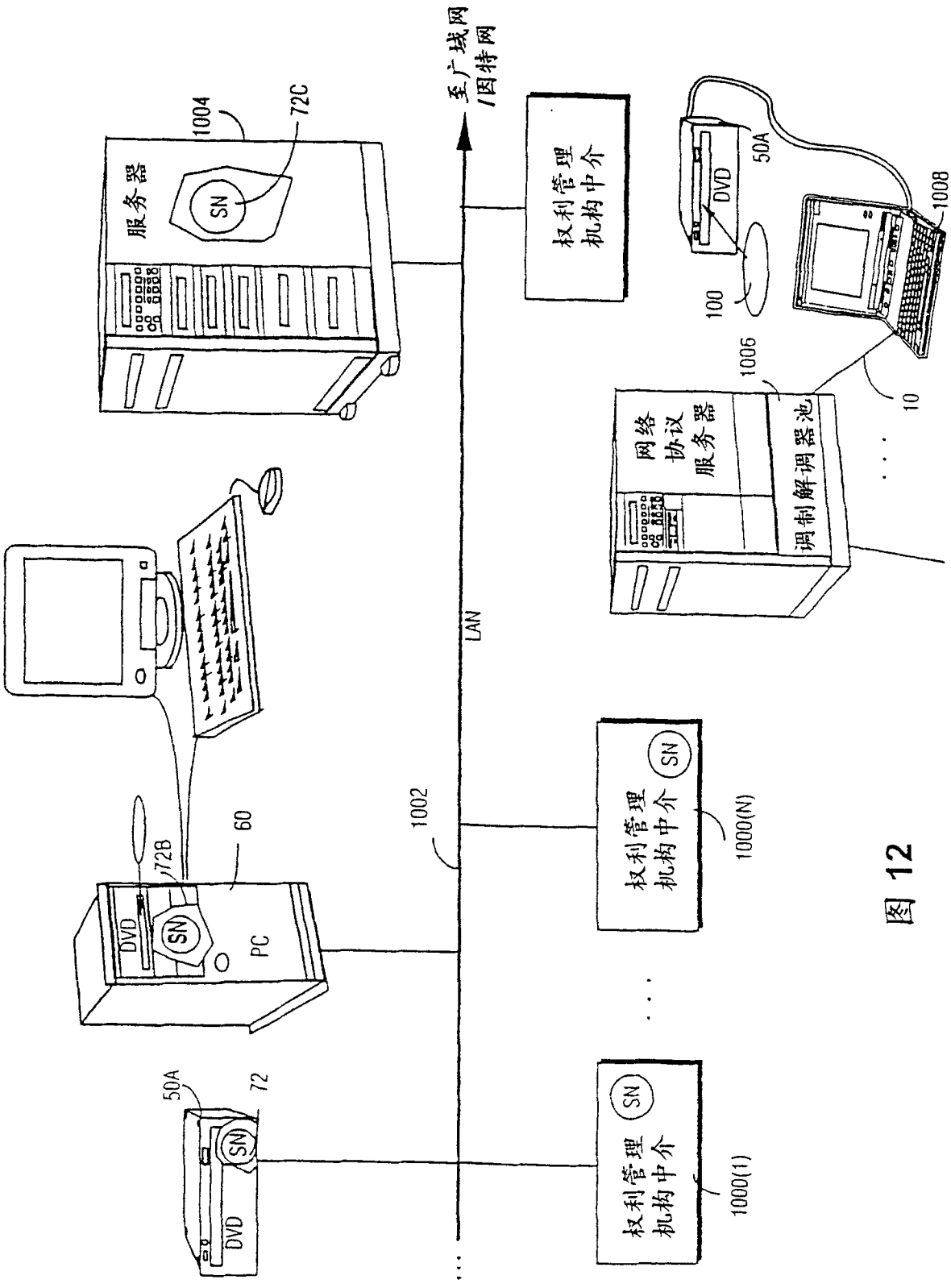

至广域网
/因特网
LAN
服务器
1004
72C
SN
权利管理
机构中介
50A
DVD
100
1008
1006
网络
协议
服务器
调制解调器池
10
72B
60
PC
1002
权利管理
机构中介
1000(N)
50A
72
权利管理
机构中介
1000(1)

图 12

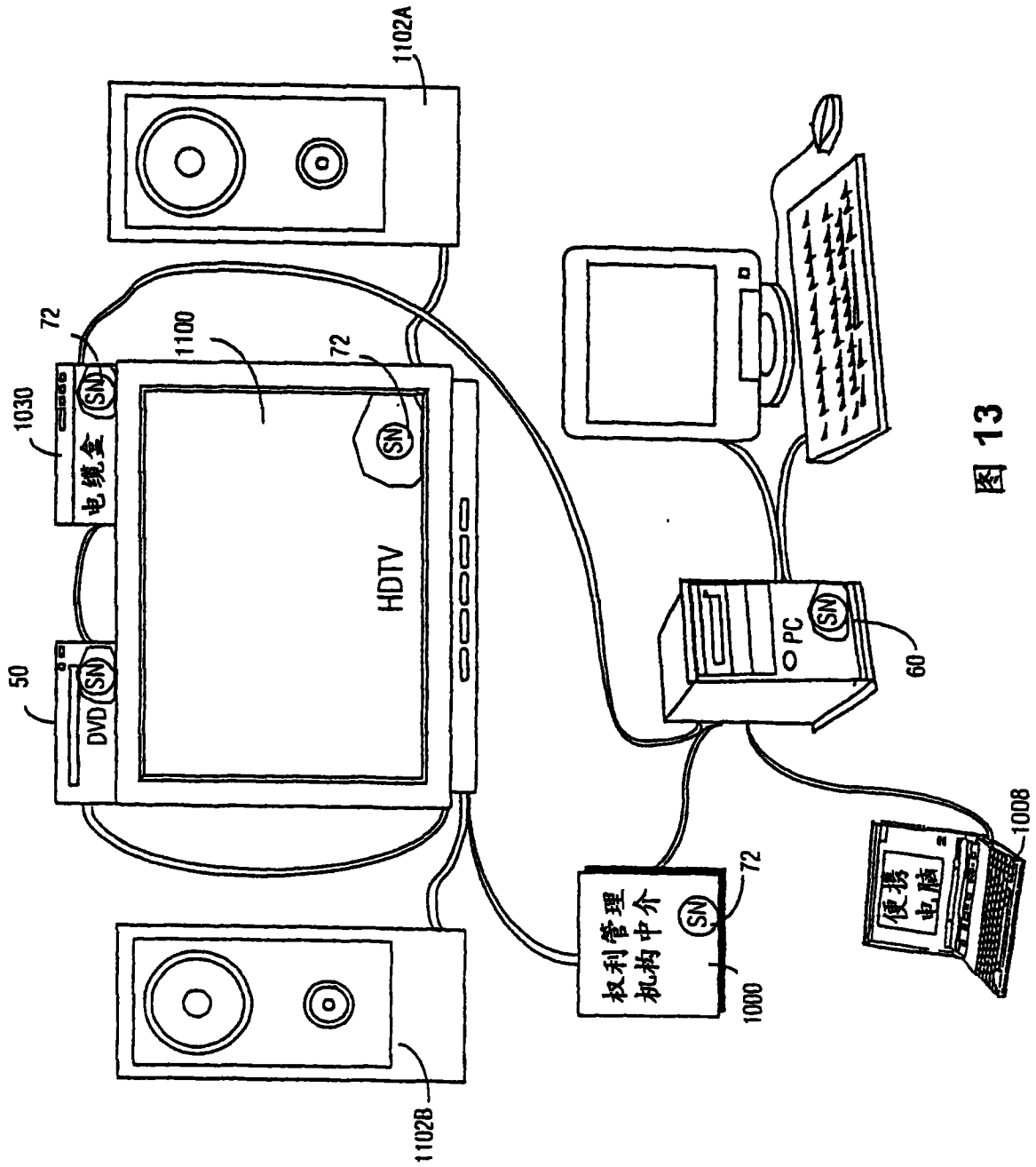

1102A
72
1100
72
1030
电缆盒
SN
HDTV
50
DVD
PC
60
1008
便携电脑
权利管理机构中介
72
1000
1102B

图 13

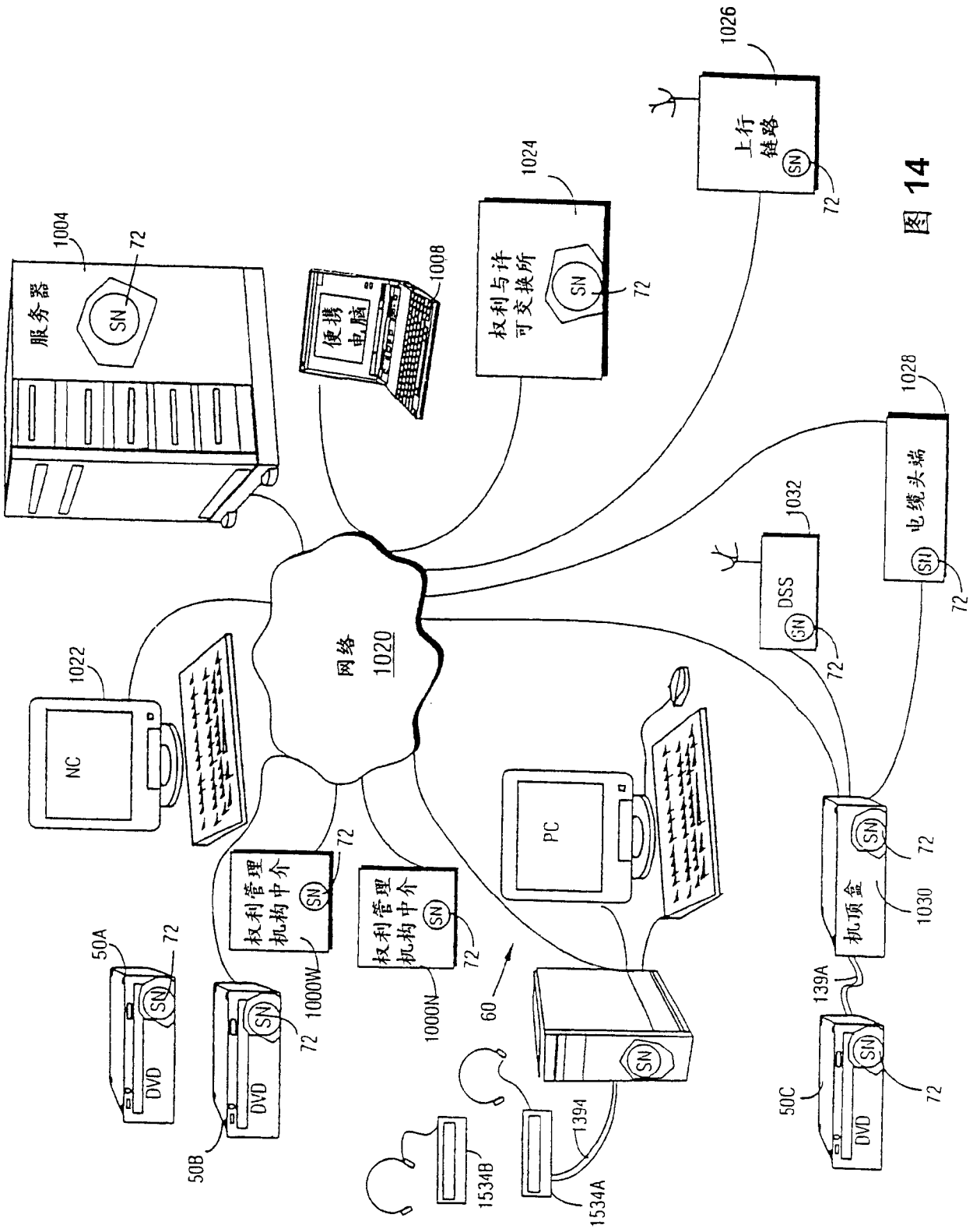

网络
1020
服务器
1004
便携电脑
1008
权利与许可交换所
1024
上行链路
1026
电缆头端
1028
DSS
1032
NC
1022
PC
权利管理机构中介
1000W
权利管理机构中介
1000N
机顶盒
1030
DVD
50A
50B
50C
60
1394
139A
1534A
1534B
SN
72

图 14

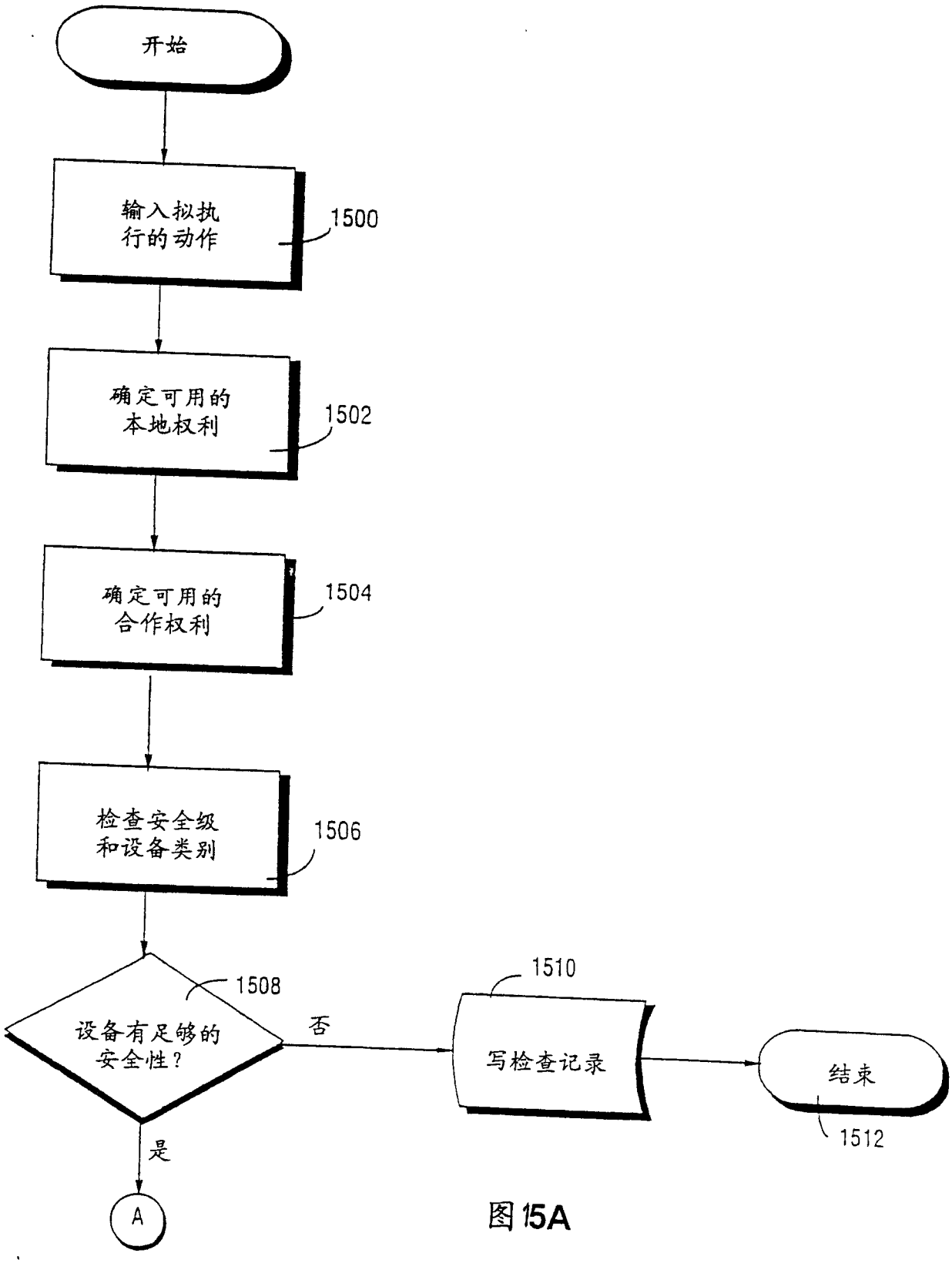

开始
输入拟执行的动作
1500
确定可用的本地权利
1502
确定可用的合作权利
1504
检查安全级和设备类别
1506
设备有足够的安全性？
1508
否
1510
写检查记录
结束
1512
是
A

图 15A

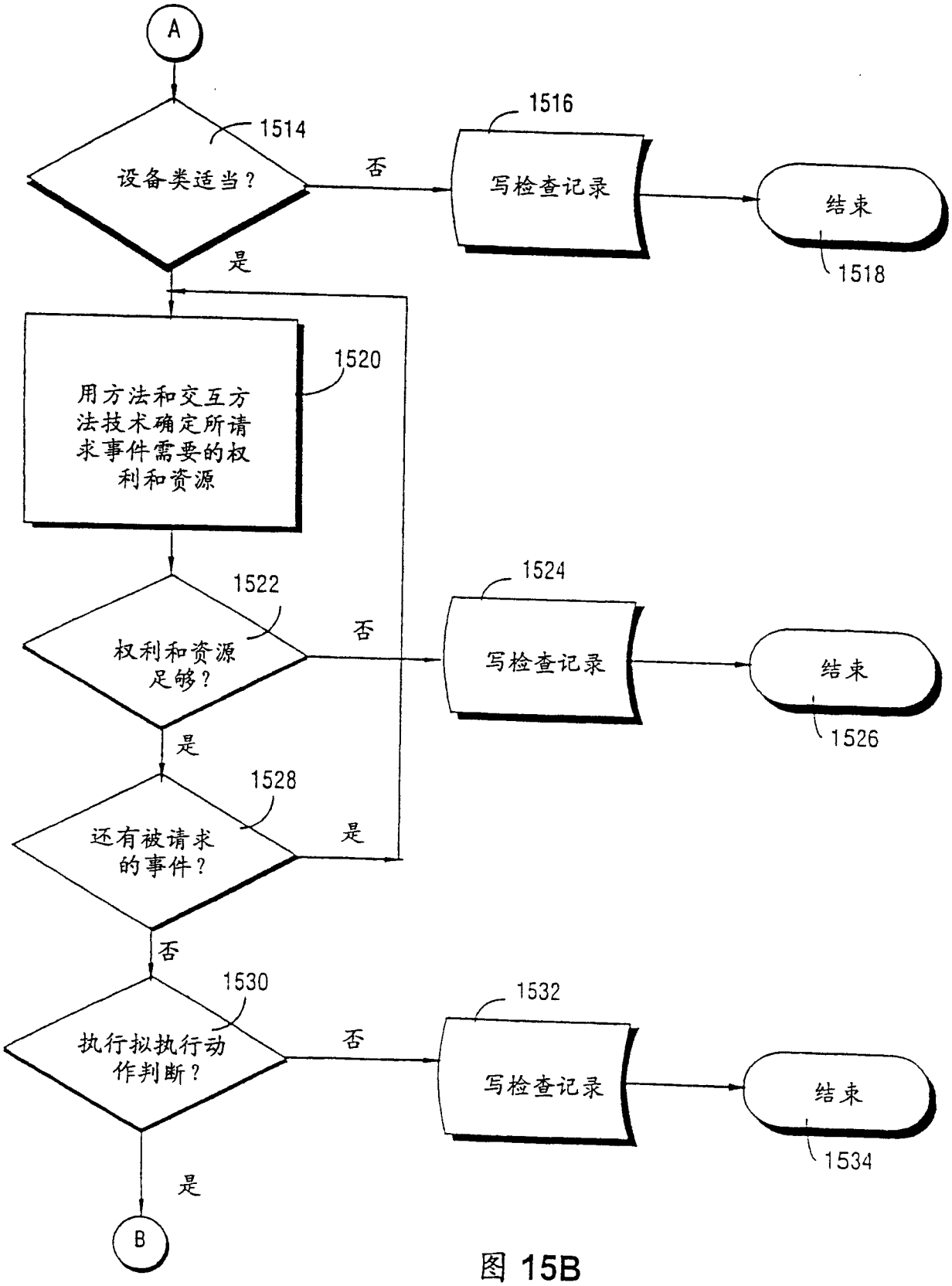

A
1514
设备类适当？
否
1516
写检查记录
结束
1518
是
1520
用方法和交互方法技术确定所请求事件需要的权利和资源
1522
权利和资源足够？
否
1524
写检查记录
结束
1526
是
1528
还有被请求的事件？
是
否
1530
执行拟执行动作判断？
否
1532
写检查记录
结束
1534
是
B

图 15B

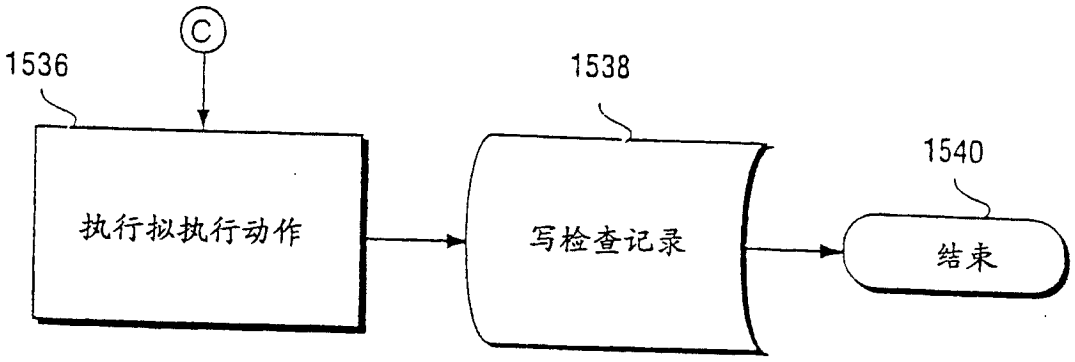


图 15C