(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 1662980 B
(45)授权公告日 2011.07.13

(21)申请号 03813899.9

(22)申请日 2003.06.11

(30)优先权数据
02077406.3 2002.06.18 EP

(85)PCT申请进入国家阶段日
2004.12.14

(86)PCT申请的申请数据
PCT/IB2003/002574 2003.06.11

(87)PCT申请的公布数据
WO2003/107342 EN 2003.12.24

(73)专利权人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬

(72)发明人 J·P·M·G·林纳茨

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 杨凯 王忠忠

(51)Int.Cl.
G11B 20/00(2006.01)

(56)对比文件
CN 1290395 A,2001.04.04, 说明书第2页第15至23行, 第5页第8至22行, 第6页第8至23行, 第7页第31至32行, 第8页第10至13行, 第8页第19行至第9页第13行、附图1,4,9.
CN 1249510 A,2000.04.05, 说明书摘要.
US 5905798 A,1999.03.18, 说明书第2栏第14至第17行, 第2栏第33至47行, 第3栏第29行至第35行、附图1.

审查员 王宏雨

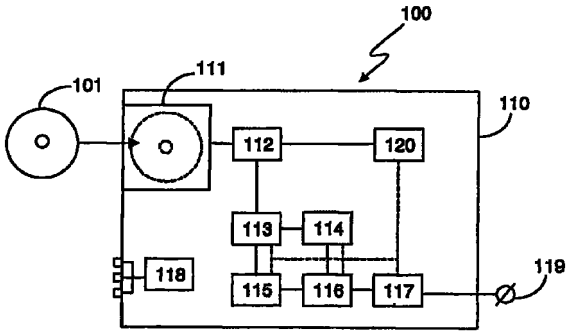
权利要求书 1 页 说明书 8 页 附图 1 页

(54)发明名称

用于安全存储的系统

(57)摘要

一种系统(100),它包括:读取装置(112),用于从存储介质(101)中读取内容数据和控制逻辑数据,所述控制逻辑数据以唯一的方式与存储介质(101)联系;处理装置(113-117),用于处理内容数据并将处理后的内容数据馈送到输出;以及控制装置(120),用于执行控制逻辑数据以及根据正在执行的控制逻辑数据控制处理装置(113-117)。所述联系最好通过所述存储介质(101)的物理参数中的变化来实现,所述变化显现某种调制图形,这种调制图形表示获得对所述控制逻辑数据的访问权所必需的参数。或者,所述联系通过存储介质(101)上含有所述必需参数的集成电路(201)来实现。所述必需参数可以包含解密密钥或认证数据。



CN 1662980 B

1. 一种宿主装置 (110),包括 :

读取装置 (112),用于从存储介质 (101) 中读取内容数据和控制逻辑数据,所述控制逻辑数据以唯一的方式与所述存储介质 (101) 相联系,且包括可执行代码或指令,该读取装置 (112) 进一步被设置来读出用于获得对所述控制逻辑数据的访问的必需参数 ;

不止一个处理装置 (113-117),其耦合到所述读取装置 (112),用于处理所述内容数据,其中如果所述控制逻辑数据包括被设置用于控制所述不止一个处理装置 (113-117) 中的一个或多个处理装置将要被激活的可执行代码或指令且其中包含在所述控制逻辑数据中的可执行代码或指令被设置用于控制所述已被激活的处理装置 (113-117) 的操作,那么所述一个或多个处理装置被激活 ;以及

控制装置 (120),其耦合到所述读取装置 (112),用于执行所述控制逻辑数据并用于根据正被执行的控制逻辑数据来控制那些被激活的处理装置 (113-117),以使宿主装置 (110) 能够确认其被安装在兼容系统 (100) 中,且当该宿主装置 (110) 被安装在兼容系统 (100) 中时,使所述处理装置能够将处理后的内容数据馈送到输出 (119)。

2. 如权利要求 1 所述的宿主装置 (110),其中所述读取装置 (112) 用于读出所述存储介质 (101) 的物理参数的变化,所述变化呈现表示用于获得对所述控制逻辑数据的访问的所述必需参数的调制图形。

3. 如权利要求 2 所述的宿主装置 (110),其中所述控制逻辑数据以加密方式存储在所述存储介质 (101) 上,并且所述必需参数包含对所述加密的控制逻辑数据进行解密所必需的解密密钥。

4. 如权利要求 2 所述的宿主装置 (110),其中所述必需参数包含用于所述控制逻辑数据的认证数据,并且所述控制装置 (120) 用于在执行所述控制逻辑数据之前利用所述认证数据来验证所述控制逻辑数据的真实性。

5. 如权利要求 1 所述的宿主装置 (110),其中所述存储介质 (101) 包括集成电路 (201),所述集成电路包含用于获得对所述控制逻辑数据的访问的必需参数,并且所述读取装置 (112) 用于从所述集成电路 (201) 中读出所述必需参数。

6. 如权利要求 5 所述的宿主装置 (110),其中所述读取装置 (112) 还用于在所述集成电路 (201) 上存储附加参数的值。

用于安全存储的系统

技术领域

[0001] 本发明涉及用于保护存储在移动存储介质（如光学载体）上的内容的系统。

背景技术

[0002] 通过可下载控制软件来实现灵活性的原理已在安全再现(securerendering)领域得到应用。有关此类系统的信息，可参见Bart J.vanRijnsoever、Peter Lenoir和Jean-Paul M.G.Linnartz所著的“数字多媒体内容的可互操作保护”(" Interoperable protection for digitalmultimedia content "，IEEE International Multimedia Conference andExhibit，New York，2000)。

[0003] 随着目前家庭娱乐从模拟平台过渡到数字平台，抵制非法复制的音视频保护越来越成为一个重大问题。在存储介质（如CD和DVD光盘，特别是可录或可重写的）、联网（无处不在的因特网和数字电视）以及压缩（具体为MP3音频和MPEG4视频）方面的技术进步不仅为新的商业模式提供了大量机会，同时也对现有音乐和电影发行行业造成威胁。

[0004] 许多数字电视广播商在条件访问(CA)系统的控制下销售其音像内容。这些系统在传送之前将MPEG-2信号加密，同时将解密密钥发送到付费最终用户的数字TV终端（机顶盒或集成电视机）。这些终端对信号解密，并管理加密密钥和内容访问权。

[0005] OPIMA(多媒体访问的开放平台动议(Open Platform Initiaive forMultimedia Access))是一种允许内容保护系统与多媒体终端之间互操作的规范。OPIMA不限于数字TV，包括例如通过因特网交付音乐。其目的就是要创建内容交付的开放市场。在数字TV和其它应用领域中，内容保护系统易于妨碍了横向市场的发展，在横向市场中，最终用户可以利用他或她的多媒体终端访问所有服务提供商的内容提供。传统上，一个终端只支持一个内容保护系统，这严重限制了可以访问的服务数量。

[0006] 根据OPIMA，通过下载对应的软件模块或插入对应的硬件模块来针对某个特定知识产权管理和保护(IPMP)系统将通用多媒体终端实例化。所述模块实现不同IPMP系统之间所有不同的功能。OPIMA虚拟机(OVM)确保IPMP插件的安全性。这些插件展示内容访问权和最终用户标识，因此它们必须得到，以防护例如最终用户的攻击。OVM实现此保护的方式并不是由OPIMA来定义的，这作为一项留给采纳OPIMA的应用领域的任务。

[0007] OVM实现两个应用编程接口(API)。应用服务API允许独立的应用使用OPIMA。利用该API，诸如软件播放器之类的应用可以请求对URL标识的特定内容项进行访问。

[0008] IPMP服务API允许下载的IPMP插件（或模块）访问多媒体终端的功能。IPMP插件实现应用域中某个特定IPMP系统专用的所有功能。应用域中的通用功能（如传输和可能还有内容解密）都是通过OVM来实现的。OVM还执行大部分再现功能，以确保压缩的数字内容不会在未受保护的接口上被黑客获取。

[0009] 虽然与传统的内容保护系统相比，OPIMA系统允许一定程度的灵活性，但它仍存在多个缺点。其一，这种系统需要可以下载IPMP插件的通信信道。此信道必须是安全的和经过认证的，以使攻击者无法在下载中操纵该插件（例如在该插件中插入病毒或置换代码，

以使攻击者可以未经授权而复制受保护的内容）。还需要返回信道以请求 IPMP 插件。

[0010] 再者，这些插件通常以 Java 语言来实现，并通过 OVM 以 applet 的形式执行。每个内容提供商必须编制具有所有必需功能的自有 IPMP 插件。OPIMA 标准定义了用于应用服务和 IPMP 服务的通用 API，但 OVM 并不提供此 API 中功能的实现。这意味着内容提供商需要做大量重复的工作，而且它暴露出各种安全风险，因为模块是在没有充分安全的情况下发行的。正确地实现安全系统是很难的，因此可以预见，在实现时会发现许多安全漏洞，从而使整个系统似乎并不值得信赖。

[0011] 本发明人意识到，一种类似的技术机制也可以用于不同目的。与为向用户交付内容的设备（如具有在屏幕上显示内容的功能的电视机、移动电话、PC）创造灵活环境的方案不同，可以实现一种用于在光盘等介质上存储和检索内容的灵活解决方案。

[0012] 本发明人意识到另一个缺点，即在当前 OPIMA 的设计理念中，IPMP 插件和内容是通过支持认证的双向网络来交付的。后者可以例如保护插件免受重放攻击 (replay attack)。这使得难以存储内容和与之相关的权利。

发明内容

[0013] 本发明目的是提供一种如前所述的系统，它提供与现有技术系统类似的灵活性，同时更适合于内容的安全存储。本发明的另一个目的在于赋予内容拥有者以可由控制逻辑定义的方式适当选择这些功能的自由。

[0014] 这些和其它目的可根据本发明在一种系统中实现，这种系统包括：读取装置，用于从存储介质中读取内容数据和控制逻辑数据，所述控制逻辑数据以唯一的方式与所述存储介质联系 (link)；处理装置，其连接到所述读取装置以处理所述内容数据并将处理后的内容数据馈送到输出；以及控制装置，其连接到所述读取装置以执行所述控制逻辑数据和根据正在执行的控制逻辑数据控制所述处理装置。

[0015] 这种体系结构的优点是显著的。一方面，所述处理装置可以标准化方式实现。这降低了这些装置中的编程和 / 或安全性错误的风险，并为系统提供固定的基本体系结构和功能。另一方面，通过简单地写入新控制连接数据并将其与内容数据一起存储在与所述存储介质有联系的存储介质上，可以使系统以全新的方式操作。

[0016] 因为控制逻辑数据以唯一的方式与存储介质联系，所以系统不需要安全信道来下载插件，因而更可靠地防止逐比特复制存储介质中的内容。

[0017] 在现有技术的安全存储系统中，许多功能可由本身容纳存储介质的设备来执行。这些功能可以包括解密、再加密、水印检测、利用新水印重新打标 (remark)、读出光盘上的唯一标识符、读取和执行撤销消息、将光盘类型与内容作比较（以防止回放为新闻媒体制作的专业内容以及非法复制到可录介质上）等。本发明提出一种系统，允许内容拥有者拥有以可由控制逻辑数据随意定义的方式选择使用这些功能的自由。

[0018] 在一个实施例中，所述读取装置用于读出所述存储介质的物理参数中的变化 (variation)，所述变化显现一种调制图形 (modulationpattern)，这种调制图形表示获得对所述控制逻辑数据的访问权所必需的参数。在本实施例中，通过如下方式在控制逻辑数据和存储介质之间建立唯一的联系：为访问该控制逻辑数据，要求使用必需参数，所述必需参数是该存储介质的物理组成部分而无法复制到另一个存储介质上。必需参数通过在存储

介质的物理参数中引入变化而编码到该存储介质上，所述变化显现表示所述必需参数的调制图形。

[0019] 存储介质的此类物理参数有时称为存储介质上的“摆动参数 (wobble)”。可参考转让给本发明的同一受让人的美国专利 5724327（代理人案号 PHN13922），它描述创建这种“摆动参数”和在其中存储信息的各种技术。

[0020] 在另一个实施例中，控制逻辑数据经过加密存储在存储介质上，所述必需参数包含对加密的控制逻辑数据进行解密所必需的解密密钥。对于要求使用必需参数以访问控制逻辑数据而言，这是一种非常简单而又有效的技术。没有该参数，则无法恢复控制逻辑数据。并且因为参数无法复制，所以控制逻辑数据必定与存储介质相联系。

[0021] 在另一个实施例中，所述必需参数包含用于所述控制逻辑数据的认证数据；以及所述控制装置用于在执行所述控制逻辑数据之前利用所述认证数据验证所述控制逻辑数据的真实性。对控制逻辑数据加密的一种替代方法是简单地将认证数据存储在存储介质上。复制存储介质时无法复制认证数据，因此对复制的认证无法通过。

[0022] 在另一个实施例中，所述存储介质包括集成电路，它含有获得对所述控制逻辑数据的访问权所必需的参数；所述读取装置用于从所述集成电路中读取所述必需参数。该集成电路有时称为“光盘芯片 (Chipin disc)”。因为每个存储介质都具有其自己的集成电路，所以不可能复制集成电路中具有相同信息的存储介质。于是，可以将来自该集成电路的信息用于实现控制逻辑数据与存储介质之间的联系。

[0023] 在另一个实施例中，读取装置还用于在集成电路上存储附加参数的值。这允许系统跟踪诸如要对内容数据访问施加的使用限制。于是，附加参数可以包含计数器，每次访问之前读取它的值，减去 1 而后再次将其存储。如果计数器到达零值，则系统拒绝对内容数据的访问。当然，该附加参数还可以用于其它目的。

[0024] 本发明的另一个目的是提供一种存储介质，它含有内容数据和控制逻辑数据，所述控制逻辑数据以唯一的方式与所述存储介质联系。此存储介质最好包括光存储介质。

[0025] 在一个实施例中，所述存储介质包括集成电路，所述集成电路包含用于获得对控制逻辑数据的访问权所必需的参数。

[0026] 在另一个实施例中，所述存储介质显现所述存储介质的物理参数中的变化，所述变化显现表示获得对所述控制逻辑数据的访问权所必需的参数的调制图形。

附图说明

[0027] 下面将参考附图阐明本发明的这些和其它方面，附图中：

[0028] 图 1 示意性地显示了根据本发明的包括存储介质和宿主装置的系统；以及

[0029] 图 2 更为详细地显示了包括集成电路的存储介质的一个实施例。

[0030] 在所有这些附图中，相同的引用编号表示相似或对应的功能。附图中显示的一些功能通常实现为软件，因而表示软件实体，如软件模块或对象。

具体实施方式

[0031] 图 1 示意性地显示了根据本发明的包括存储介质 101 和宿主装置 110 的系统 100。宿主装置 110 包括用户可以将存储介质 101 置于其中的插座 111、用于从所述存储介质 101

读取内容数据和控制逻辑数据的读取模块 112、用于处理所述内容数据并将处理后的内容数据馈送到输出 119 的不同处理装置 113-117 以及用户可借以控制宿主装置 110 的操作的用户输入模块 118。宿主装置还包括控制模块 120，下面将对其操作进行描述。

[0032] 在图 1 中，宿主装置 110 实现为光盘驱动器，例如光盘 (CD) 或数字多功能光盘 (DVD) 读取装置。但是，装置 110 还可以容易地实现为软盘驱动器或读取移动硬盘、智能卡、闪速存储器等存储介质的读取装置。包括宿主装置 110 的系统 100 可以是例如光盘播放器、个人计算机、电视机或无线电系统等。

[0033] 可以理解，系统 100 可与根据类似 OPIMA 的原理构建的安全再现系统互操作。在这种实施例中，安全的灵活宿主装置 110 可以与 OPIMA OVM 建立双向通信会话并提供 IPMP 系统。

[0034] 在用户将存储介质 101 置于插座 111 中之后，读取模块 112 被激活。该激活操作可以是自动执行的，也可以是对用户输入模块 118 的用户激活操作如按下按钮的响应。根据本发明，读取模块 112 从存储介质 101 读取控制逻辑数据，并将该控制逻辑数据馈送到控制模块 120。

[0035] 控制模块 120 接收该控制逻辑数据，并试图确定控制逻辑数据真实可信且与存储介质 101 有正确的联系。如果无法确认真实性，控制模块 120 指示错误状态，例如通过向输出 119 提供错误信号或激活宿主装置 110 的前面板上的 LED。

[0036] 在控制逻辑数据和存储介质之间建立唯一联系的一种方法是：要求使用必需参数以访问控制逻辑数据，所述必需参数是存储介质本身的物理组成部分而无法复制到另一个存储介质上。所述必需参数通过在存储介质的物理参数中引入变化而编码到该存储介质上，所述变化显现表示必需参数的调制图形。存储介质的此类物理参数有时称为存储介质上的“摆动参数 (wobble)”。可参考转让给本发明的同一受让人的美国专利 5724327（代理人案号 PHN13922），它描述创建这种“摆动参数”和在其中存储信息的各种技术。

[0037] 存储介质 101 最好是光学可读类型的记录载体，其中信息已经以光学可检测标记的模式记录在其上，且所述光学可检测标记沿其所述轨道与中间区域交错排列。这些变化最好是轨道位置在轨道方向的横向上的变化。

[0038] 在另一个实施例中，具有沿其轨道排列的信息标记的所述记录载体显现由轨道沿线上信息标记的有无造成的第一变化，所述第一变化表示记录在记录载体上的信息信号；以及由与轨道相关联的变化造成的第二变化，所述第二变化显现表示代码的调制图形。

[0039] 用存储介质的物理参数对信息编码的一种替代方法采用调制的预刻槽 (pregroove)（参见授予先锋公司的美国专利 5901123 和授予索尼和先锋公司的美国专利 6075761）。当然其它方法也是可行的。

[0040] 读取模块 112 于是读取存储介质的物理参数中的这些变化，并重建表示所述必需参数的调制图形。随后将该参数提供给控制模块 120。

[0041] 在第一实施例中，控制逻辑数据经加密存储在存储介质上，所述必需参数包含对加密的控制逻辑数据进行解密所必需的解密密钥。没有该参数，则无法恢复控制逻辑数据。因为参数是无法复制的，所以控制逻辑数据必定与存储介质 101 相联系。作为一种附加的安全措施，可以预先在宿主装置 100 中安装必需的解密密钥部分。宿主装置 110 将此部分与包含在必需参数中的解密信息相结合，以获得允许对加密的控制逻辑数据进行解密的完

整的解密密钥。

[0042] 在第二实施例中，必需的参数包含用于控制逻辑数据的认证数据。控制模块 120 在执行控制逻辑数据之前利用该认证数据验证该控制逻辑数据的真实性。认证数据可以比可编码为存储介质的物理参数中的变化的数据的数据量大。在此情况中，可以将认证数据写在存储介质上的某个数据区中，例如写入通常用于存储内容数据的扇区中。然后计算认证数据的加密摘要，并将其编码为物理参数中的变化。因为该摘要（例如采用 MD5 加密哈希函数获得的）将会较短，所以可以以此方式来对该摘要进行编码。此可选方案的更详细的讨论参见国际专利申请 WO 01/95327（代理人案号 PHNL000303）。所述必需参数构成认证数据的加密摘要。

[0043] 在控制逻辑数据与存储介质之间建立唯一联系的另一种方法是采用“光盘芯片 (Chip In Disc)(CID)”方法。此方法可参见例如由本发明的相同申请人提出的国际专利申请 WO 02/17316（代理人案号 PHNL010233）中有所描述。图 2 说明此方法。存储介质 101（本例中为光盘或 DVD 等光学记录载体）配有集成电路 201（有时也称为芯片）。此集成电路包括用于将存储在电路中的信息发送到宿主装置的装置 202。该芯片可以使用由外部电源信号供电的光电二极管 203 为其供电，但也可设想采用电池或其它电源。

[0044] 存储在芯片中的信息可能需要保护，以使未授权的设备无法获得对它的访问权。例如，该信息可以包含内容解密密钥，该密钥应该只提供给符合某种数字版权管理 (DRM) 标准的播放设备。因此，在将存储的信息发送到宿主装置之前最好尝试对宿主装置进行认证。在本发明申请的同一申请人提出的欧洲专利申请序列号 02075983.3（代理人案号 PHNL020192）中描述了一种最适合 CID 型应用的低功率认证方法。

[0045] 类似于采用“摆动参数”的实施例，可以将来自该集成电路的信息用于实现控制逻辑数据与存储介质之间的联系：该信息包含获得对控制逻辑数据的访问权所必需的参数。例如，该信息可以包含解密密钥或认证数据。

[0046] 在另一个实施例中，读取模块 112 还用于在集成电路 201 上存储附加参数的值。此时，为此目的的集成电路 201 包括对应的可重写存储组件 204。这使系统 100 可以跟踪例如要对内容数据访问施加的使用限制。于是，该附加参数可以包含计数器，每次访问之前读取它的值并将其减 1，然后再次将其存储起来。如果计数器到达零值，则系统拒绝对该内容数据的访问。当然，该附加参数还可以用于其它目的。例如，可将其用于保存状态信息。

[0047] 在另一个实施例中，读取模块 112 还用于在存储介质 101 上其它位置存储附加参数的值。例如，存储介质 101 可以包括可重写数字多功能光盘或光盘。这也允许系统 100 跟踪例如使用限制、状态信息或其它信息。

[0048] 读取模块 112 可用于在存储介质 101 上存储控制逻辑数据时重写全部或部分控制逻辑数据。这使系统 100 还可以跟踪例如使用限制、状态信息或其它信息。这里，使用限制可以简单地通过将其赋给控制逻辑数据中的一个变量而实现。这样，只需当在存储介质上存储控制逻辑数据时通过简单地重写该控制逻辑数据中的赋值语句，读取模块 112 就可使使用限制递减。或者，读取模块 112 可以在控制逻辑数据保持在宿主装置 110 的工作存储器中时修改它，随后可以用修改过的控制逻辑数据简单地替换存储介质上的控制逻辑数据。

[0049] 如果控制逻辑数据被修改，则这可能使控制逻辑数据与存储介质之间的联系被破坏。例如，如果认证数据存储在集成电路 201 中或作为存储介质的物理参数中的变化来存

储，则对该控制逻辑数据的修改将使所得控制逻辑数据不再与认证数据匹配。如果认证数据存储在集成电路 201 中，则可以更新该认证数据以反映变更。

[0050] 但是，如果认证数据是作为存储介质的物理参数中的变化来存储的，则无法改变该变化。克服此问题的一个可选方案是将认证数据以加密形式存储在存储介质 101 上的某个可重写区域中。然后将对该认证数据进行解密所必需的解密密钥作为存储介质的物理参数中的变化来存储。读取模块 112 于是可以读取该解密密钥并将其用于对认证数据进行解密。

[0051] 在将修改过的控制逻辑数据写入存储介质 101 之后，读取模块 112 计算新的认证数据（例如，修改后的控制逻辑数据的加密摘要），并利用相应的密钥将其加密，然后将结果写入存储介质 101。

[0052] 如果控制逻辑数据成功解密，和 / 或控制逻辑数据成功通过认证，则控制模块 120 继续执行该控制逻辑数据。在宿主装置 110 中，控制模块 120 控制处理装置 113-117 的操作。控制模块 120 本身根据正在执行的控制逻辑数据来操作。

[0053] 控制逻辑数据不只是获得对内容数据的访问权所必需的密码或解密密钥。确切地说，它包括要由控制模块 120 执行的可执行代码或指令。这些指令可以高级语言，例如解释型脚本语言如 Python 或 Tcl/Tk 的形式提供，也可以低级语言如 Java 字节码的形式提供。当然这些指令本身可以包含一些参数，例如处理装置要执行的某些操作所用的解密密钥或种子。

[0054] 内容处理的第一步通常为 :控制模块 120 激活读取模块 112。读取模块 112 从存储介质 101 读取内容数据，并将其馈送到处理装置 113-117。处理装置 113-117 的输出送至输出 119，然后系统 100 的其它组件可以从该处读取内容（例如，将其作为电影再现或生成音频信号以在扬声器上再现）。最好可以首先让宿主装置 110 确认它安装在兼容系统 100 中。这在输出 119 是数字输出时尤其重要。如果无法确认系统 100 的兼容性，输出 119 上不应出现任何内容。

[0055] 宿主装置 110 可以配备各种各样的处理装置。在图 1 所示示范实施例中，处理装置包括解密模块 113、水印检测模块 114、条件访问模块 115、信号处理模块 116 以及总线加密模块 117。

[0056] 首先，在由控制模块 120 执行的控制逻辑数据的控制下，从存储介质 101 读出的内容由解密模块 113 进行解密。作为该控制的一部分，控制模块 120 可以为解密模块 113 提供解密密钥，也可以就如何获取该解密密钥指示解密模块 113。例如，解密密钥可以存储在存储模块 101 所包含的集成电路中，也可以存储在存储介质 101 上的指定位置。

[0057] 水印检测模块 114 处理解密的内容数据，以查找其中含有嵌入数据的水印。水印可以包含例如数字版权管理数据或内容拥有者的标识。

[0058] 水印检测模块 114 从执行有关如何以及在哪里检测水印的控制逻辑数据的控制模块 120 接收指令。例如，可以指令水印检测模块 114 提取内容拥有者标识，并将该信息馈送到显示模块（未显示）。或者，可以指令水印检测模块 114 检查“不得复制”或“不得再复制”指示符，并在发现此类指示符时通知条件访问模块 115。可能情况还有，控制模块 120 根本不激活水印检测模块 114。

[0059] 由控制模块 120 就如何控制对内容数据的访问向条件访问模块 115 发出指令。可

以指令条件访问模块 115 执行严格的不得复制规则，或不允许许将内容馈送到数字输出端。在此情况中，条件访问模块 115 用信令通知信号处理模块 116 将只生成模拟信号并将其馈送到输出 119。还可以指令条件访问模块 115 将特定类型的水印嵌入到信号中，以馈送到输出 119。

[0060] 信号处理模块 116 负责将内容数据转换成可以出现在输出 119 上的信号。这包括例如生成模拟音频和 / 或视频信号，但也可包括将水印数据嵌入信号，滤掉内容的特定部分，生成该内容的特技播放 (trickplay) 版等。要执行的精确的信号处理或转换操作由控制逻辑数据决定。执行控制逻辑数据的控制模块 120 控制信号处理模块 116 执行的操作。

[0061] 总线加密模块 117 对要在输出 119 上出现的音频和 / 或视频信号加密。例如，宿主装置 110 可以参与执行与系统 100 的另一个组件进行的认证协议。此认证协议的结果是，宿主装置 110 和其它组件共享一个秘密密钥。现在，内容可以用该秘密密钥加密，并以加密的形式出现在输出 119 上。这样，可以从该输出 119 读取数据（例如通过监听输出 119 连接到的总线）的其它组件无法访问该内容。

[0062] 要特别注意的是，处理装置 113-117 均是宿主装置 110 的组件，它们可以部分或全部用软件实现。控制逻辑数据不向宿主装置 110 提供全新的功能，例如不提供全新的解密算法。确切地说，控制逻辑数据通过例如激活或不激活特定的组件，指示应该提取何种类型的数据以及它们应该将该数据提供给其它哪些组件来控制宿主装置 110 的组件的操作。

[0063] 这种体系结构的好处是显著的。一方面，所有处理装置 113-117 可以标准化方式实现。这样降低了这些装置中编程和 / 或安全性错误的风险，并为宿主装置 110 提供固定的基本体系结构和功能。另一方面，通过简单地写入新控制逻辑数据并将其与内容数据一起存储在与所述存储介质相联系的某个存储介质中，可以使宿主装置 110 以全新的方式操作。

[0064] 例如，内容提供商可以将内容数据以加密方式存储在存储介质 101 上。控制逻辑数据包含一些指令，这些指令可将解密密钥馈送到解密模块 113 并使解密模块 113 将解密的内容数据直接馈送到信号处理模块 116。控制逻辑数据还包含一些指令，用于指示信号处理模块 116 生成低质量的模拟输出信号。宿主装置 110 中的其它模块根本未使用。

[0065] 同一个内容提供商以后可能决定实现基于计数器的拷贝保护机制。它将“光盘芯片”添加到存储介质 101 中并更新控制逻辑数据中的指令。在本例中，更新的指令还通过调用内置的“光盘芯片”读取功能来激活条件访问模块 115。添加访问模块 115 现在读出芯片 201 中存储的计数器，检查其值是否大于零，如果大于零，则用信号通知读取模块 112 可以读取内容数据。它还将计数器值减 1。

[0066] 内容提供商还可以选择实施任何其它拷贝保护机制，只要条件访问模块 115 包含必需功能。随后，它只需在控制逻辑数据中写入适当指令，并且可以相信宿主装置 110 会执行它们。

[0067] 应该注意的是，上述实施例说明而非限定本发明，本领域技术人员在不背离所附权利要求书范围的前提下可以设计许多替代实施例。

[0068] 在权利要求中，括号中的任何引用符号不得理解为限制该权利要求。用词“包括”不排除存在不同于权利要求中所列单元或步骤的部件或步骤。单元之前的用词“一个”不排除存在多个这种单元。本发明可以通过包括若干不同单元的硬件以及适当编程的计算机

来实现。

[0069] 在枚举多个装置的装置权利要求中，这些装置中的若干装置可以同一硬件上实现。某些措施在彼此不同的独立权利要求中记载，这一单纯事实并不表示不能组合利用这些措施。

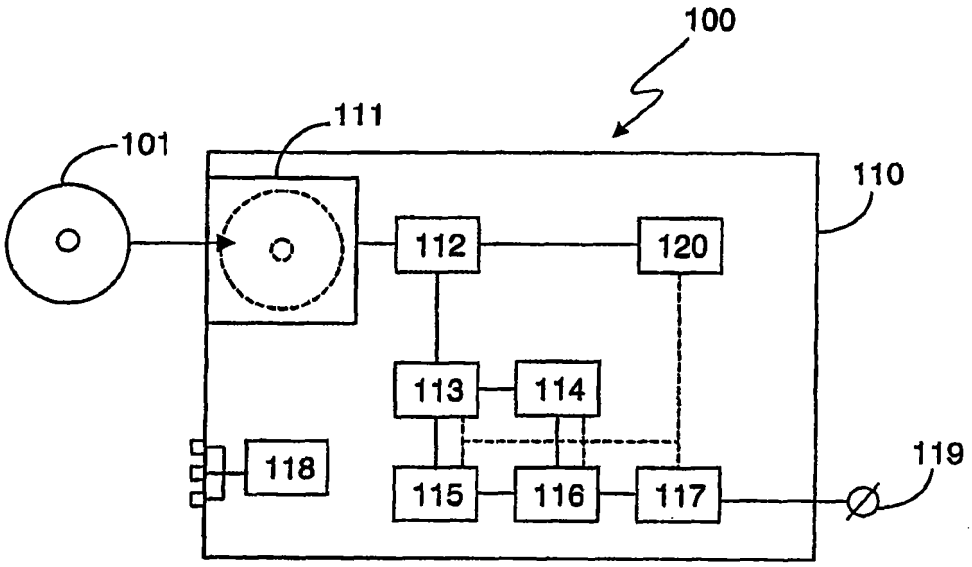

100
111
101
110
112
120
113
114
118
115
116
117
119

图 1

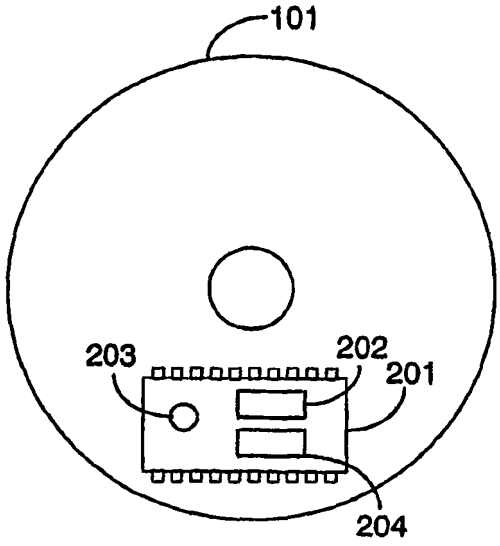

101
203
202
201
204

图 2