



(12) 发明专利

(10) 授权公告号 CN 1682486 B

(45) 授权公告日 2013.08.21

(21) 申请号 03821379.6

H04N 21/435(2011.01)

(22) 申请日 2003.09.08

H04N 21/6334(2011.01)

(30) 优先权数据

60/409,675 2002.09.09 US

(56) 对比文件

US 5809147 A, 1998.09.15, 全文.

CN 1254475 A, 2000.05.24, 全文.

(85) PCT申请进入国家阶段日

2005.03.09

CN 1333973 A, 2002.01.30, 说明书第3页第24行-第5页第9行,第5页第24行-第6页第6行,第6页第18行-第7页第17行、图1,图2.

(86) PCT申请的申请数据

PCT/US2003/027774 2003.09.08

说明书第3页第24行-第4页第26行,第5页第24行-第6页第6行,第6页第18行-第7页第17行、图1,图2.

(87) PCT申请的公布数据

W02004/023717 EN 2004.03.18

US 5420866 A, 1995.05.30, 全文.

US 5870474 A, 1999.02.09, 全文.

(73) 专利权人 索尼电子有限公司

地址 美国新泽西州

审查员 阎洁

(72) 发明人 B·L·坎德洛尔

(74) 专利代理机构 北京东方亿思知识产权代理

有限责任公司 11258

代理人 宋鹤

(51) Int. Cl.

H04N 21/434(2011.01)

H04N 5/913(2006.01)

H04N 21/2347(2011.01)

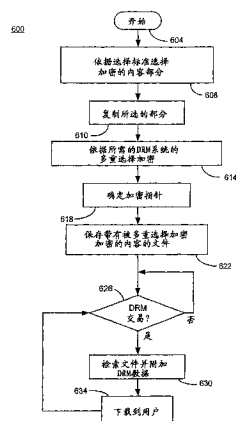
权利要求书3页 说明书7页 附图6页

(54) 发明名称

用于多数字权利管理的内容分配

(57) 摘要

一种允许使用多数字权利管理方案 (DRM) 的方法与设备。检查表示数字内容的未加密数据,以至少识别用于加密的内容段。复制被识别的内容段,然后使用与第一 DRM 关联的第一加密方法加密,产生第一加密段。使用与第二 DRM 关联的第二加密方法加密副本,产生第二加密段。产生一组指向第一与第二加密内容段的指针。然后创建包括第一和第二加密内容段、指针与未加密内容以及 DRM 权利数据的文件,以产生被选择加密的允许多 DRM 的文件。



1. 一种允许使用多种数字权利管理方案 (DRM) 的方法,包括:  
检查表示数字内容的未加密数据,以至少识别用于加密的内容段;  
复制被识别的内容段,来产生被识别的内容段的第一副本和第二副本;  
使用与第一 DRM 关联的第一加密方法加密被识别的内容段的第一副本,产生第一加密内容段;  
使用与第二 DRM 关联的第二加密方法加密被识别的内容段的第二副本,产生第二加密内容段;  
产生指向第一加密内容段的第一指针;  
产生指向第二加密内容段的第二指针;以及  
在数字内容中用第一加密内容和第二加密内容代替被识别的内容段,并插入第一与第二指针,以产生被部分加密的允许双 DRM 的文件。
2. 根据权利要求 1 的方法,其中内容包括数字化的音频。
3. 根据权利要求 1 的方法,其中内容包括数字化的视频。
4. 根据权利要求 1 的方法,进一步包括向文件附加数据,以允许在第一 DRM 下的数字权利。
5. 根据权利要求 1 的方法,进一步包括向文件附加数据,以允许在第二 DRM 下的数字权利。
6. 根据权利要求 1 的方法,其中第一和第二指针包括识别被加密的内容段起始位置的字节偏移量。
7. 根据权利要求 1 的方法,其中第一和第二被加密的内容段具有由加密量所定义的持续时间。
8. 根据权利要求 1 的方法,进一步包括向文件附加数据,以允许在第一 DRM 和第二 DRM 中的至少一个下的数字权利;并向用户传送该文件。
9. 一种允许使用多种数字权利管理方案 (DRM) 的编码器,包括:  
检查表示数字内容的未加密数据,以至少识别用于加密的内容段的装置;  
复制被识别的内容段,来产生被识别的内容段的第一副本和第二副本的装置;  
第一加密器,使用与第一 DRM 关联的第一加密方法加密被识别的内容段的第一副本,产生第一加密内容段;  
第二加密器,使用与第二 DRM 关联的第二加密方法加密被识别的内容段的第二副本,产生第二加密内容段;  
产生指向第一加密内容段的第一指针的装置;  
产生指向第二加密内容段的第二指针的装置;  
在数字内容中用第一加密内容和第二加密内容代替被识别的内容段,并插入第一与第二指针,以产生被部分加密的允许双 DRM 的文件的装置。
10. 根据权利要求 9 的编码器,其中内容包括数字化音频和数字化视频中的至少一个。
11. 根据权利要求 9 的编码器,进一步包括用于向文件附加数据的装置,以允许在第一 DRM 和第二 DRM 中的至少一个下的数字权利。
12. 根据权利要求 9 的编码器,其中第一和第二指针包括识别被加密的内容段起始位置的字节偏移量。

13. 根据权利要求 9 的编码器,其中第一和第二被加密的内容段具有由加密量所定义的持续时间。

14. 根据权利要求 9 的编码器,进一步包括向文件附加数据的装置,以允许在第一 DRM 和第二 DRM 中的至少一个下的数字权利;向用户传送该文件。

15. 根据权利要求 9 的编码器,在被编程的通用计算机中实现。

16. 一种在多数数字权利管理方案 (DRM) 情形下使用数字内容的权利的方法,包括:

执行交易以获得内容的数字权利;

接收的数字内容包含:

未加密的内容段,

使用与第一 DRM 关联的第一加密方法对被选择用于加密的内容段的第一副本加密而产生的第一加密内容段,

使用与第二 DRM 关联的第二加密方法对所述被选择用于加密的内容段的第二副本加密而产生的第二加密内容段,

指向第一加密内容段的第一指针,

指向第二加密内容段的第二指针,

以及允许在第一 DRM 和第二 DRM 中的至少一个下的数字权利的 DRM 数据;

确定可从 DRM 数据中获得有效的数字权利;以及

解密第一和第二加密段之一,以允许内容播放。

17. 根据权利要求 16 的方法,其中内容包括数字化音频和数字化视频的至少一个。

18. 根据权利要求 16 的方法,其中第一和第二指针包括识别被加密的内容段起始位置的字节偏移量。

19. 根据权利要求 16 的方法,其中第一和第二被加密的内容段具有由加密量所定义的持续时间。

20. 一种允许使用多个数字权利管理方案 (DRM) 的其中一个的数字内容的权利的解码器,包括:

执行交易以获得内容的数字权利的装置;

用于接收数字内容的装置,数字内容包含:

未加密的内容段;

使用与第一 DRM 关联的第一加密方法对被选择用于加密的内容段的第一副本加密而产生的第一加密内容段;

使用与第二 DRM 关联的第二加密方法对所述被选择用于加密的内容段的第二副本加密而产生的第二加密内容段;

指向第一加密内容段的第一指针;

指向第二加密内容段的第二指针;以及

允许第一 DRM 和第二 DRM 中至少一个下的数字权利的 DRM 数据;

DRM 验证器,确定从 DRM 数据中可获得的有效的数字权利;以及

解密器,解密加密段之一,以允许播放该内容。

21. 根据权利要求 20 的解码器,其中内容包括数字化音频和数字化视频的至少一个。

22. 根据权利要求 20 的解码器,其中第一和第二指针包括识别被加密的内容段起始位

置的字节偏移量。

23. 根据权利要求 20 的解码器,其中第一和第二被加密的内容段具有由加密量所定义的持续时间。

24. 根据权利要求 20 的解码器,在被编程的通用计算机中实现。

## 用于多数字权利管理的内容分配

### [0001] 相关文件的交叉引用

[0002] 本申请涉及 Candelore 等于 2002 年 10 月 18 日提交的 U. S. 专利申请序号 10/273, 905, 题为“基于视频码片与活动区的双重部分加密”, Candelore 等于 2002 年 10 月 18 日提交的序号 10/273, 903, 题为“星形部分加密”, Candelore 等于 2002 年 10 月 18 日提交的序号 10/274, 084, 题为“码片掩码与渠形部分加密”, Candelore 等于 2002 年 10 月 18 日提交的序号 10/274, 019, 题为“视频场景变化检测”的文献, 上述文献在此引入作为参考。

[0003] 本申请还涉及 Candelore 在 2002 年 9 月 9 日申请的 U. S. 临时专利申请序号 60/409, 675 并要求其优先权。该申请同样在此引入作为参考。

### [0004] 版权声明

[0005] 该专利文献公开的一部分包括了受版权保护的材料。版权所有者不反对在该专利文献或者专利公开以专利局专利文件或者记录形式出现时对其复制再现, 然而在别的方面却保留其全部著作权的权利。

## 技术领域

[0006] 本发明通常涉及数字权利管理的领域。更特别地, 本发明涉及为允许多个数字权利管理方案 (DRM) 的目的而对多重加密的数字化视频特别有用的多重加密方法与设备。

## 背景技术

[0007] 在诸如音乐和电影等音频和 / 或视频内容的传统分配中, 通过包括该著作的物理媒体的所有权来管理版权作品的权利。媒体的所有权为越权使用提供限制障碍。虽然对这种传统“包装媒体”的侵权行为过去和现在都很普遍, 但是在内容的数字分配环境中这个问题被显著地倍增。内容的所有者已经发明各种方法以帮助保护这种被集体称为数字权利管理 (DRM) 的内容。DRM 不仅包含已经用于保护内容的多种加密方案, 还包含许可使用已经被创建的内容的各种方案, 以及针对该内容的权利监控与跟踪。

[0008] 目前在市场上有几种 DRM 形式。也许主导的 DRM 形成了 Microsoft Windows<sup>®</sup> 操作系统媒体播放器的一部分, 这被称为“互惠的”。另一个广泛使用的 DRM 方案被嵌入 Real Network 公司的 real Player<sup>®</sup>。目前微软公司的 DRM 解决方案与压缩算法紧密联系。DRM 解决方案通常在个人电脑 (PC) 平台上执行。因此, DRM 解决方案被设计成能检测软件篡改, 并因此尽力扰乱执行软件运行。

[0009] 上述两个 DRM 实例仅是两个日益增长和发展的技术领域。可以连续预期进一步的 DRM 体现, 以提供对内容的更大保护, 阻止那些非法盗用内容的人。

[0010] 不幸地, 由于有多种 DRM 类型可用, 用户必须获得支持各种 DRM 方案的多组软件 (或插件), 或者限制对于那些希望在他们计算机中支持的 DRM 的内容消费。

## 附图说明

[0011] 在附加权利要求中记载了本发明的特征, 其被认为是新颖的。然而就本发明本身

而言,通过参考下列发明的详细说明能更好地理解结构和操作方法以及其目的与优势,在发明的详细说明中结合附图描述了本发明的一些示范性实施例,其中:

[0012] 图 1 是符合本发明某些实施例的、包括数字权利管理的数字内容分配系统框图。

[0013] 图 2 举例说明符合本发明某些实施例的示范性文件结构。

[0014] 图 3 举例说明符合本发明某些实施例的视频数据的字节偏移安排。

[0015] 图 4 举例说明符合本发明某些实施例的音频数据的字节偏移安排。

[0016] 图 5 举例说明符合本发明某些实施例的视频或音频数据内容中的示范性 DRM 安排。

[0017] 图 6 是显示符合本发明某些实施例的编码带有多种 DRM 内容的方法流程图。

[0018] 图 7 是显示符合本发明某些实施例描述的获取和重放有多种 DRM 的内容的流程图。

[0019] 图 8 举例说明符合本发明某些实施例的内容供应商服务器系统。

[0020] 图 9 是符合本发明某些实施例的重放计算机框图。

### 具体实施方式

[0021] 虽然本发明允许多种不同形式的实施例,但在图中显示并在此详细描述特定实施例。应当理解,本公开被认为是本发明原理的实例,而不打算将本发明限制为所显示和描述的实施例。在下面的描述中,相同的参考数字用于描述几幅视图中相同、相似或对应的部分。

[0022] 在此术语“加扰 (scramble)”和“加密”以及其变化被用作同义语。在此经常使用的术语“视频”不仅仅包含真实的视觉信息,而且在对话(例如,“磁带录象机”)的意义上不仅包含视频信号还包含相关的音频与数据。本文件通常使用“双选择加密”实施例的实例,但是本领域技术人员应该认识到可以使用本发明实现多部分加密而不背离本发明。在此术语“部分加密”与“选择加密”被用作同义语。

[0023] 上面提到的、被共同拥有的专利申请描述了在此通常称为部分加密或者选择加密的方法的各种方面。更特别地,在所描述的系统中使用两个(或更多)加密技术加密特殊选择的数字内容的选定部分,而不加密内容的其它部分。通过适当地选择要被加密的部分,可以有效地加密内容,以便在多种解密系统中使用,而不必加密所有选择的内容。在一些实施例中,使用多种加密系统有效地加密内容仅需要几个百分点的数据系统开销。这导致在电缆或者卫星系统的单个系统中可以利用来自多个制造商的机顶盒或者其它条件存取(CA)接收机的其它实施例,因此使电缆或者卫星公司自由地竞争购买机顶盒的供应商。

[0024] 本发明将类似的选择加密技术应用于多数字权利管理的问题中。上述专利申请描述的部分加密处理利用任何适合的加密方法。然而,使用在上述参考的专利申请中描述的技术,将这些加密技术有选择地应用于数据流,而不是加密所有数据流。通常,但不限于,选择加密处理利用了信息的智能选择来进行加密,以便整个节目不必经历双重加密。通过适当地选择进行加密的数据,可以有效地加扰和隐藏节目资料,防止那些希望随意修改系并非法再现商业内容而不付费的人。用于表示音频与视频数据的 MPEG(或者类似的格式)数据利用帧与帧之间信息冗余的高度可靠性来进行加密。某些数据可以作为表示色度与亮度数据的“锚”数据传送。然后那些数据经常在屏幕简单移动,以通过发送描述该块运动的运

动矢量来产生后续帧。色度与亮度数据的变化同样被编码为变化,而不是记录绝对的锚数据。因此,例如加密这些锚数据或者它关键数据可以有效地使得视频不可观看。

[0025] 本发明的某些实施例通过复制与加密对解密余下的带有第一与第二 DRM 的内容重要或者关键的内容,从而允许第二(或者多种)数字权利管理(DRM)解决方案。复制内容不必附加大幅增加的带宽开销。不同于陆地与卫星广播流,通过因特网传递并最后通过 PC 解密的内容不必限制为 188 字节的分组。对于陆地和卫星流来说,通常根据传送标题中的加扰比特以每个分组为基础执行硬件解密。用软件进行内容解密可以有更多颗粒性和选择。

[0026] 依据某些本发明的实施例,将要加密的选定视频数据可能是一个或者下列组合(上述申请中有更详细的描述)的任何一种:出现在视频帧活动区的视频码片标题,表示视频帧活动区的数据,在视频帧内的星形数据,表示场景变化的数据,I 帧分组,包括 I 帧之后第一 P 帧中的运动矢量的分组,具有码片内标记(intra\_slice\_flag)指示符设置的分组,具有码片内(intra\_slice)指示符设置的分组,包括内编码(intra\_coded)宏块的分组,用于包括内编码宏块的码片的数据,来自视频码片标题之后的第一宏块的数据,包括视频码片标题的分组,锚数据,和用于逐行刷新视频数据的 P 帧数据,在视频帧中纵向与/或横向渠形排列的数据,和任何使得视频和/或音频难于被利用的其它选定数据。上述参考的专利申请中公开了几个这种技术以及其它的技术,本发明可以使用任何一个(或者其它的技术)来仅加密内容的一部分。

[0027] 现在参考图 1,举例说明按照本发明某些实施例的内容传递系统 100。在该系统中,数字内容供应商 104 通过因特网向用户提供例如音频或者视频内容的内容,到用户的个人计算机系统 112,例如通过下载或者流传送。例如,计算机系统 112 是具有视频显示器 116 和驱动扬声器一组扬声器(如扬声器 120L 和 120R)的立体声(或者其它多声道的)系统的多媒体计算机系统。个人电脑 112 使用任何适合的操作系统工作,并具有用于重放音频和/或视频内容(在下文中,“媒体播放器”)的一个或多个软件程序。

[0028] 数字内容供应商可以作为可寻址网点操作,充当内容的在线分配器。在该实例中,网点具有存储内容的内容数据库 130,该内容可以由具有例如连接到因特网的计算机 112 的用户以不同的方式购买。为提供简单化的实例,而非限制本发明的范围,数字内容供应商 104 被描述为具有使用两个数字权利管理系统(显示为 134 的 DRM A 和显示为 138 的 DRM B)供应内容的能力。在传统的数字内容供应商方案中,仅使用单个 DRM 系统,并使用关于特殊 DRM 系统的加密方案以加密形式保存内容。

[0029] 依照某些按照本发明的实施例,保存在内容数据库 130 中的内容用按照内容供应商的双重(多重)DRM 的双重(通常多重的)选择加密存储。这样,数字内容供应商 104 不负担与存储分别属于多种 DRM 的内容有关的需求和成本。也不需要在使用指定 DRM 动态加密内容的计算能力。

[0030] 内容可以被安排作为类似于图 2 中描述的文件传递到用户。在该文件结构中,被传递给用户的文件与多重加密的选定部分一起存储。在一个实例中(而不限于此),如果内容作为 MPEG 数据存储,可以加密全部 MPEG I 帧或者视频码片标题,以实现实际水平的加密,而不必加密整个文件。还可以无限制地使用任何其它适合的选择加密方案。只要音频和/或视频的选定部分被选择进行加密,便复制与加密选定的部分。在该实例中,在一种情

况下按照 DRM A 的加密方案加密选定的部分,在另一种情况按照 DRM B 加密。然后重新组装该内容,以被复制的加密内容代替原始的明文内容。(注意在其它的方案中,内容可以被加密地存储或者不加密地存储,被处理和构造的文件“即时 (on the fly)”传递给用户。)

[0031] 在音频/视频内容的实例中,内容作为音频内容 206 和视频内容 210 存储。文件更进一步包括一组指向被加密的选定音频内容部分的音频加密指针 212。同样地,文件更进一步包括一组指向被加密的选定视频内容部分的视频加密指针 218。DRM A 数据部分 222 提供数据,该数据是解码器解码那些使用加密方案 DRM A 进行加密的内容所必需的。同样地,DRM B 数据部分 226 提供数据,该数据是解码器解码使用加密方案 DRM B 进行加密的内容所必需的。识别部分 230 识别在文件中可用的内容和 DRM 方案。

[0032] 在图 3 中举例说明视频数据 210 与视频加密指针 218 之间的关系。存储指向文件中被加密的视频数据部分的指针。这种加密的部分被显示为 304、308 和 312。这种加密部分与显示为 320、324、328 和 332 的不加密(不用密码)存储的数据部分交替。当然,这种实例是简化以后的,因为仅显示少量加密段,而没有显示可能很大的加密段。在该例图中,举例说明每个加密段有相同的尺寸(例如,加密量(encryptionquanta)),但是这不解释作为限制。

[0033] 音频数据 206 与音频加密指针 212 之间的关系类似于图 4,并在其中举例说明。存储指向文件中被加密的音频数据部分的指针。这种加密的部分被显示为 404、408 和 412。这种加密部分与显示为 420、424、428 和 432 的不加密存储的数据部分交替。此外,因为与那些显示大量的加密段相比较而言,仅显示少量加密段,所以这个例图相当简单。在该例图中,加密段被显示为具有不同的尺寸,这是通过指定每个加密段的长度实现的。

[0034] 在各种情况下,如果希望可以预先确定将被加密的字节数来作为加密量,以便加密指针可以只是一个存储器偏移位置的序列。然后,通过预定的加密量(例如,8 字节)来确定被加密的数据量。在其它的实施例中,加密指针部分不仅包括开始偏移量还包括结束偏移量,或者开始偏移量和多个字节。

[0035] 图 5 描述加密内容的示范部分,其在加密内容的开始部分举例说明了字节偏移位置。数据的下一段是被 DRM A 加密的内容 502,其持续一段时间,这段时间由加密量确定(或者在加密指针中预先确定或者编码)。加密内容 506 的下一段被 DRM B 的加密方案加密,其持续一段时间,这段时间仍由加密量定义。通过使用预先确定的加密量,简化了加密指针。通过指定被加密段的尺寸,通过改变尺寸以实现更灵活的加密方案,这是以牺牲加密指针的效率为代价实现的。注意在预定加密量的情况下,可以加密多种连续段以实现更长加密内容段的效果。

[0036] DRM 典型地核实用户已经为观看内容付费。允许在一段时间或者对一个观看事件观看。当用户付款时,这个动作启动了内容的解密,经常是向用户传送解密密钥以允许解密。为了允许两个或更多 DRM 并行运作,在付款与密钥管理操作和内容解密之间应该有明确的分离。媒体播放器应该允许选择任何一个 DRM。通过使用选择的加密,大部分内容可以明文发送,而只加密发送某些关键的或者重要的内容(解压余下的内容所需要的)。关键或者重要的内容被复制,一组内容在一种 DRM 下加密,而另一组在另一个 DRM 下加密。

[0037] 通过因特网传递的电影与音乐可以用 UDP 分组打包,以通过 IP 网络传递。一旦在 PC 中重新组合,文件可以基本上准确。视频与音频两者可以是大的被分组的基本流(PES)



文件。

[0038] 为了实现本发明的某些实施例,应当对媒体播放器如何识别被加密的内容进行协商。在某些实施例中,如果使用加密量,应将其标准化,或者应当协定最小公分母。加密的颗粒性应该标准化(例如,来自视频与音频帧不同部分的比特能合并以进行加密吗?这对于信号更为复杂,除非反复选择相同比特。)然而,这些问题更适合作标准化谈判的主题,对理解指导本发明的概念和原则不重要。

[0039] 可以使用多种处理方法中的任何一种处理方法创建上述的文件。此外,尽管举例说明音频/视频内容,但通过省略视频加密指针和视频内容,所示的文件结构可以容易地修改为仅用于音频。在图6中描述创建这种文件的一个处理方法作为起始于604的处理600。在608,采用选择标准来选择将被多选择加密的内容段。使用的选择标准可以是如上所述的、前面引用的专利申请中描述的、在别处描述或者新创的任何一种,而没有任何限制。只要选中内容段,在610中所采用的DRM系统有几种,则被复制几次。例如,在数字内容供应商104中创建一组复制的选定数据。

[0040] 然后,在614多重加密选定的内容,使得选定数据的每一组复制集合在每种DRM加密方案下被加密。在内容供应商104的实例中,选定的内容段被复制。一组选定段在DRM A下被加密,复制组在DRM B下加密。然后,在618创建一组加密指针,作为确定被加密部分尺寸的偏移量和可能信息,文件在此时被保存在内容数据库130直到用户希望获得对该内容的数字权利。替换地,可以用明文的(或者加密的)形式保存内容,而在用户购买之后创建向用户传送的文件。

[0041] 当用户购买该内容的权利时,在626执行数字权利管理的交易,其中用户为某些权利付费。这些权利可包括在特别的时间周期观看或者观看次数的权利。可以在该交易期间向副本、放声机或者其它DRM的属性强加限制。当交易完成时,则在630从内容数据库中检索包含被购买内容的文件,附加有定义被购买权利的DRM数据。然后在634,文件被下载或者流传送到用户。用户因此按照符合在626的交易中获得的DRM权利的方式播放内容(在计算机112或者在其它的播放设备)。

[0042] 因此,符合本发明某些实施例的允许使用多种数字权利管理方案(DRM)的方法包括:检查表示数字内容的未加密数据,以至少识别用于加密的内容段;使用与第一DRM关联的第一加密方法加密被识别的内容段,以产生第一加密段;使用与第二DRM关联的第二加密方法加密被识别的内容段,以产生第二加密段;产生指向第一加密内容的第一指针;产生指向第二加密内容的第二指针;在数字内容中用第一加密内容与第二加密内容代替被识别的内容段,插入第一与第二指针,以产生被部分加密的允许双DRM的文件。当购买数字权利时,启动该权利的DRM数据被附加到文件中,并将文件发送到用户。

[0043] 在图7中起始于702的处理方法700举例说明了被用户使用的、依照符合本发明某些实施例的处理方法,在702之后,用户在706经由数字权利获取交易获得内容中的数字权利。用户能因此在710通过下载或流传送接收多种DRM文件。当在714用户希望开始播放时,在718读取DRM数据,使得在用户计算机或其它播放设备中的软件可以确定由用户获得的数字权利是否有效(即,没有到期或否则用尽)。如果在722软件确定数字权利已经到期或用尽,在726中断播放并在730结束处理。

[0044] 如果在722验证用户的数字权利,在734软件读取文件的加密指针,并在738开始

读取内容。如果在 742 加密内容,在 746 依照被选择用于播放(取决于播放软件和/或播放机器)的 DRM 方案解密该内容。如果内容未加密或被解密,控制转到 750,在此,内容被播放或者被缓存来播放。如果在 754 没有到达文件结尾,控制返回到 738,读取内容的下一段。当在 754 到达文件的结尾,在 730 停止处理。

[0045] 因此,依照符合本发明的某些实施例,一种使用对于属于多个数字权利管理方案(DRM) 其中之一的数字内容权利的方法,包括执行交易以获得对该内容的数字权利;接收的数字内容包含:未加密的内容段、使用与第一 DRM 关联的第一加密方法加密的第一加密内容段、使用与第二 DRM 关联的第二加密方法加密的第二加密内容段、指向第一加密内容段的第一指针;指向第二加密内容段的第二指针、以及允许至少在第一 DRM 和第二 DRM 其中之一的数字权利的 DRM 数据;确定可从 DRM 数据中获得有效的数字权利;解密第一和第二加密段其中之一,以允许内容的播放。

[0046] 图 6 的处理 600 可以在任何适合编程的通用处理器中执行,该处理器被用作为多 DRM 编码器,如图 8 的计算机 800。计算机 800 具有一个或多个中央处理器单元(CPU)810,一个或多个相关总线 814 被用于按照已知的方法将中央处理器单元 810 连接到随机存取存储器 818 和非易失性存储器 822。提供诸如显示器和打印机之类的输出设备 826,以便应数字内容供应商要求显示和/或打印,以及提供诸如图形用户界面(GUI)的用户界面。同样地,可能提供诸如键盘、鼠标和可移动的媒体阅读器 830 等输入设备,以便由操作者输入信息。计算机 800 还合并内部和/或外部附属的盘或其它用于存储大量信息的大容量存储器 834,上述信息包括但不限于操作系统、多种 DRM 加密方法以及内容(最可能存储在海量的附属存储器中)。计算机系统 800 还有用于连接到因特网的接口 838,用于为用户的内容请求提供服务。虽然被描述为单个计算机,但是数字内容供应商可以利用多个链接的计算机执行在此描述的功能。

[0047] 图 7 的处理 700 可以在作为解码器/解密器和 DRM 验证器操作的任何适当编程的通用处理器中执行,诸如图 9 所描述的计算机 900。计算机 900 可以是典型的个人电脑设备,其具有一个或多个中央处理器单元(CPU)910,一个或多个关联总线 914 被用于按照已知的方法将中央处理器单元 910 连接到随机存取存储器 918 和非易失性存储器 922。提供诸如显示器适配器和显示器的输出设备 926 以便应用户要求显示输出(可能包括视频内容的播放),以及提供诸如图形用户界面(GUI)的用户界面。还可以附带音频适配器和音频系统 928,用于播放音频或音频/视频内容。同样地,可能提供诸如键盘、鼠标和可移动的媒体阅读器 930 等输入设备,以便操作者输入信息。计算机 900 还结合了内部和/或外部附属的盘或其它用于存储大量信息的大容量存储器 934,上述信息包括但不限于操作系统、DRM 验证和解密软件、媒体播放器软件以及被下载的内容。计算机系统 900 还有用于连接到因特网的接口 938,以便例如购买内容。

[0048] 因此,本发明的某些实施例向数字内容供应商提供了容易地供给在多种数字权利管理方案下的内容而不必完全加密每个潜在 DRM 系统的内容。这允许减少数字内容供应商所需的存储容量(用于存储或多个被完全加密的内容副本)或者处理能力(即时加密)。因为内容供应商使用较低成本就可以容纳多种 DRM,所以通过利用本发明的实施例,可以给予用户大量内容而不需要购买或在他或她的个人电脑上加载多种 DRM 系统与媒体播放器。

[0049] 本领域的技术人员将会认识到已经基于编程处理器(例如,计算机 800 和 900)

的使用,以示范性实施例描述了本发明。然而,本发明将不限于此,因为本发明可以使用诸如专用硬件和 / 或专用处理器等硬件组件等价物,其等价于被描述和要求保护的本发明。同样地,通用计算机、基于微处理器的计算机、微控制器、光学计算机、模拟计算机、专用处理器和 / 或专用硬布线逻辑可用于构造等价于本发明实施例的替换物。此外,尽管已经依据提供播放机制的通用个人电脑描述了本发明,但是可以在专用机器中播放而不背离本发明。

[0050] 本领域的技术人员将理解可以使用例如只读存储器 (ROM) 设备、随机存取存储器 (RAM) 设备等磁盘存储器以及其它的存储器形式实现上述实施例的程序步骤和相关数据;还可以使用光存储器元件、磁存储器元件、磁光的存储元件、闪速存储器、磁心存储器和 / 或其它等价的存储器技术而不背离本发明。这种替换的存储设备应该被认为是等价的。

[0051] 如在此的实施例中描述的,使用执行编程指令的编程处理器实现本发明,上文概括描述的编程指令形式可以被存储在任何适合的电子存储媒体中,或通过任何适合的电子通信媒体传送,或否则出现在任何计算机可读的传播介质或传播介质中。然而,那些本领域的技术人员将理解所述处理可以在不背离本发明的情况下以多种变化和在多种适合的编程语言中实现。例如,执行某些操作的顺序经常是不同的,可以不背离发明地添加附加的操作或者删除操作。可以不背离本发明地添加和 / 或增强错误捕捉,在用户界面和信息放映时可以有多种变化。这种变化是预期的,并被认为是等价的。

[0052] 包含本发明某些方面的软件代码和 / 或数据可能出现在任何计算机可读的媒体、传输介质、存储介质或传播介质中呈现,它们包括但不限于,诸如上述的电子存储器,以及载波、电子信号、数据结构(例如,树、链接列表、表格、分组、帧等等)、光信号、传播信号、广播信号、传输介质(例如,电路接线、电缆、双绞线对、光纤电缆、波导、天线,等等)及其它存储运载或传递代码和 / 或数据的媒体。这种媒体既可以存储软件和 / 或数据或用于从一个位置向另一个位置传送代码和 / 或数据。在该示范性实施例中,已使用的 MPEG 分组、码片、表格及其它数据结构不应该被认为是限制,因为可以同样使用其它数据结构而不背离本发明。

[0053] 虽然已经结合特定实施例描述了本发明,但显然按照上文描述的多种替换物、修改、取代和变化对本领域的技术人员显而易见。因此,本发明意图包含落在附加权利要求范围内的全部替换物、修改和变化。

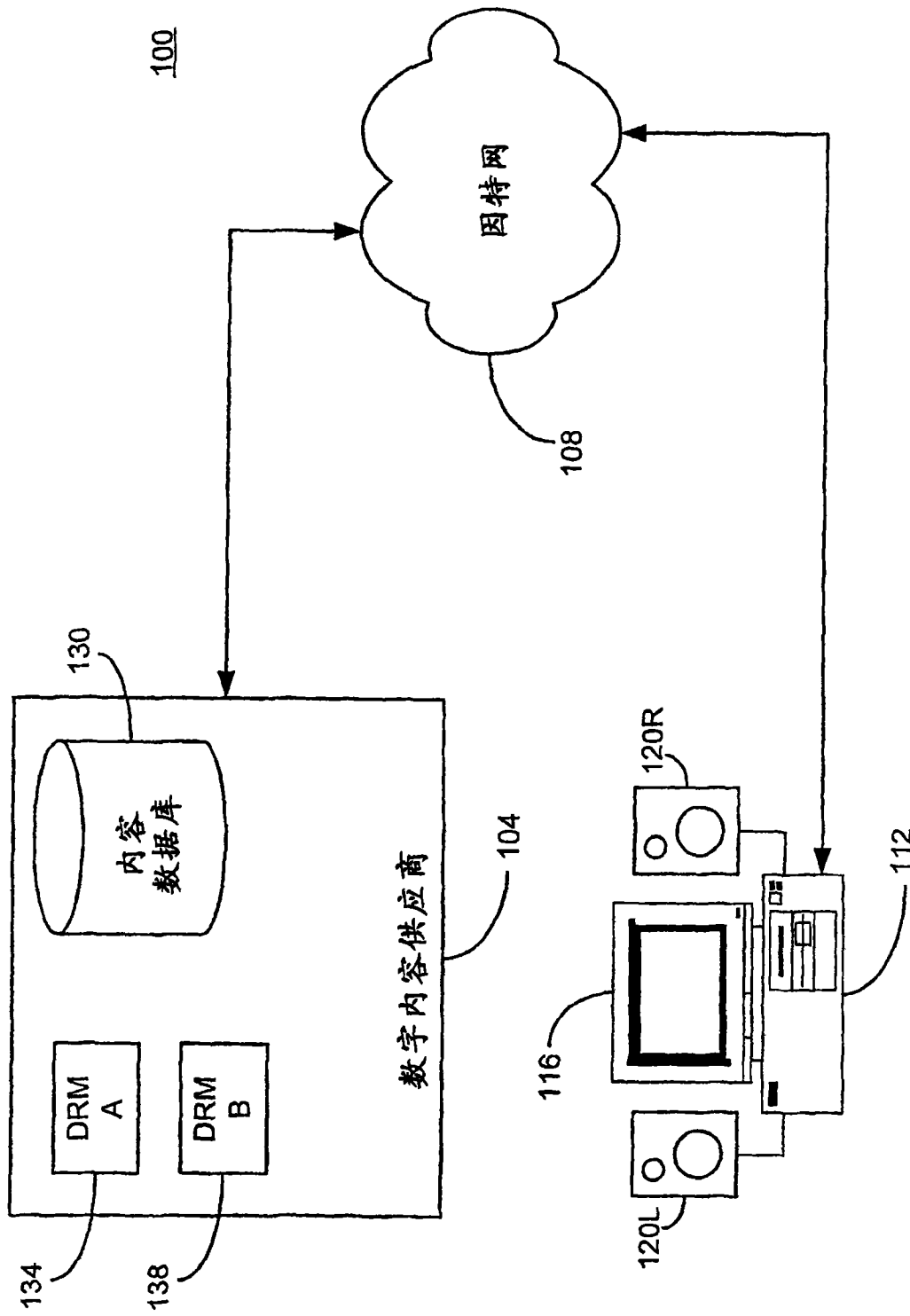
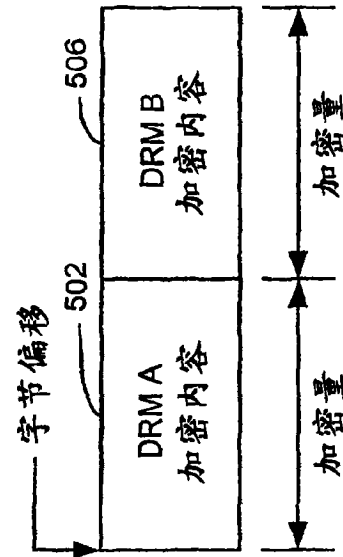
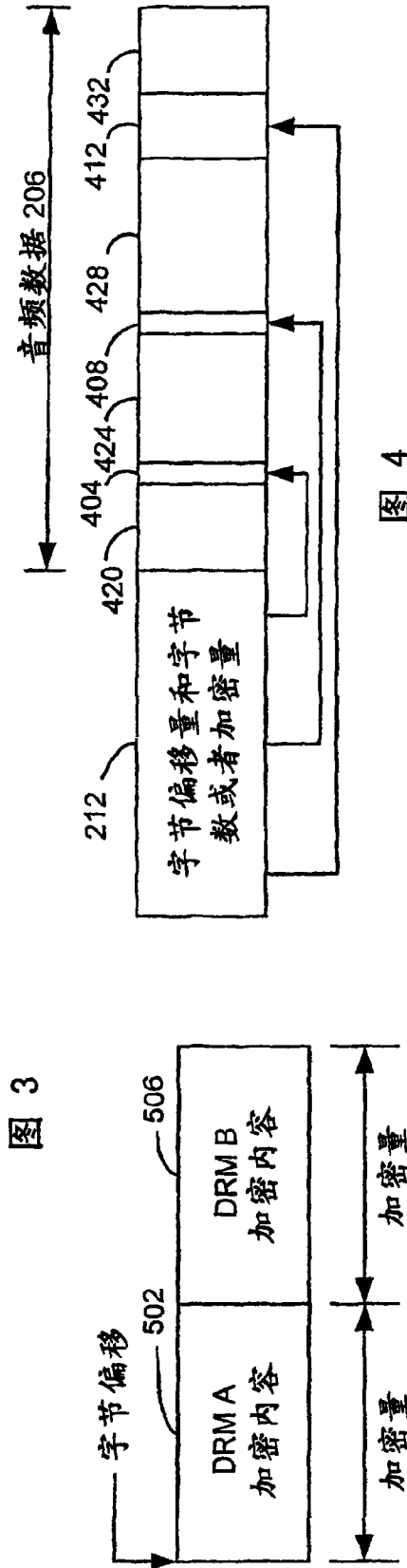
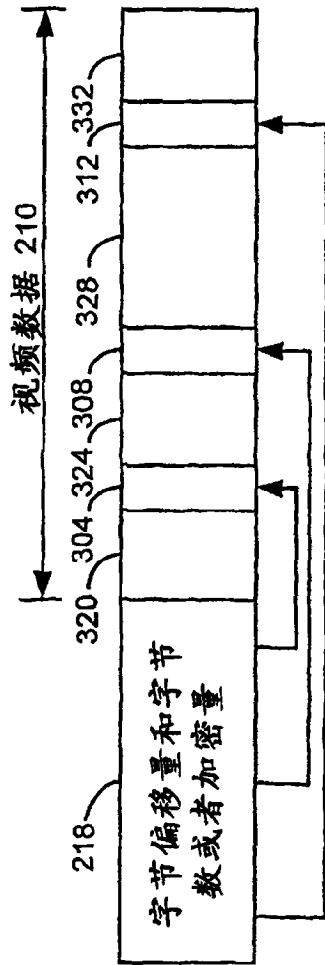
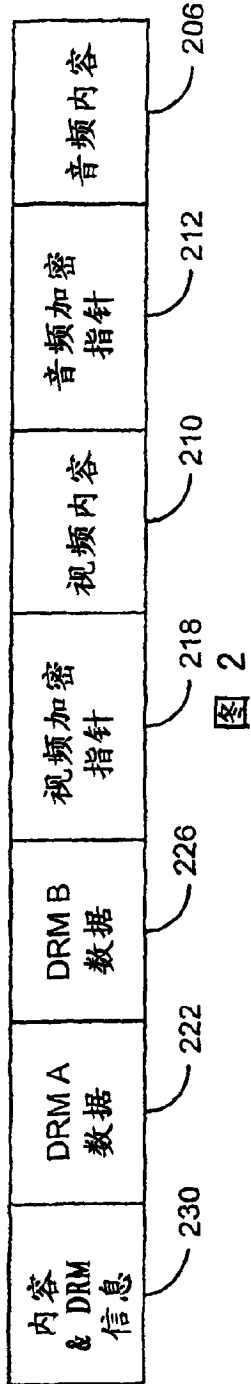


图 1



600

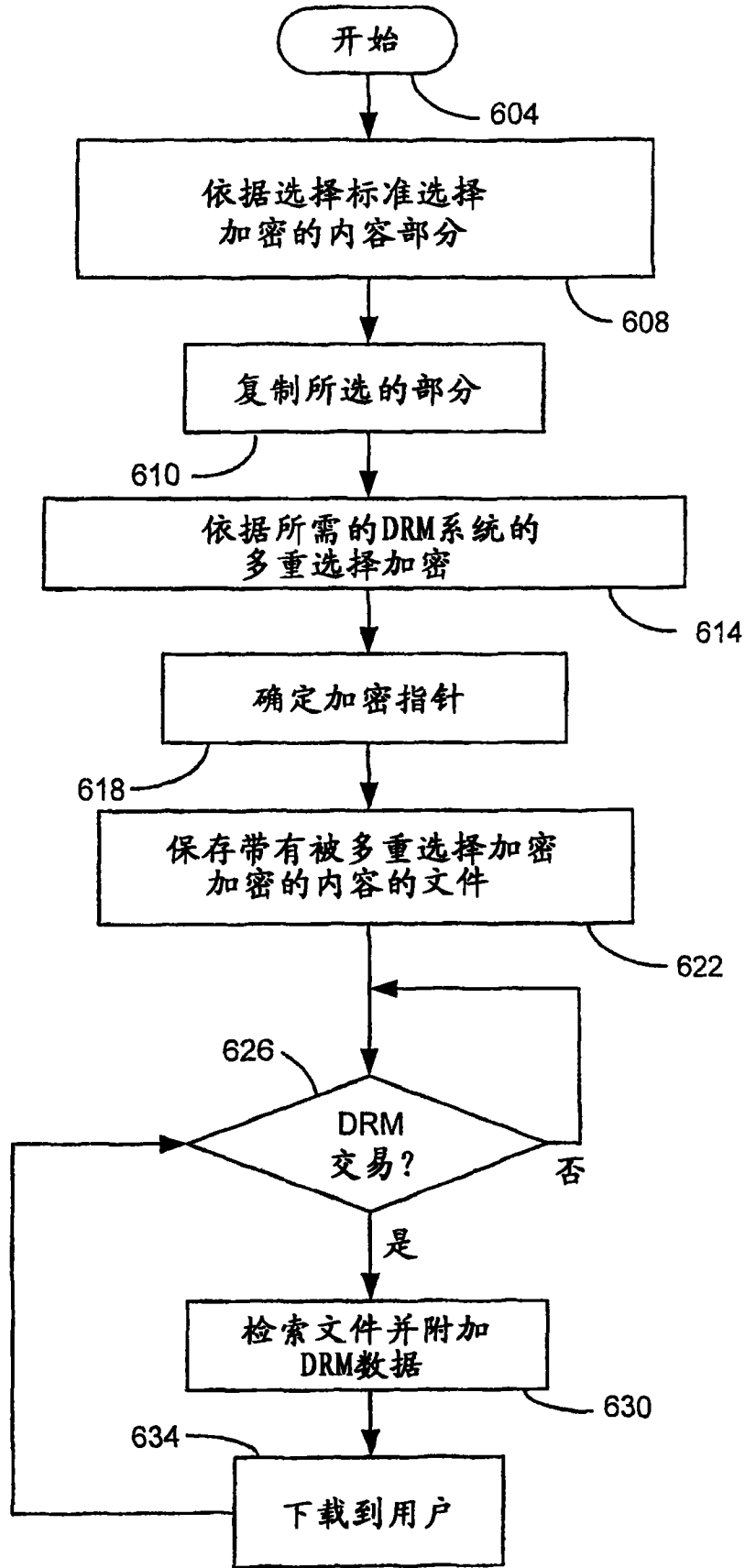


图 6

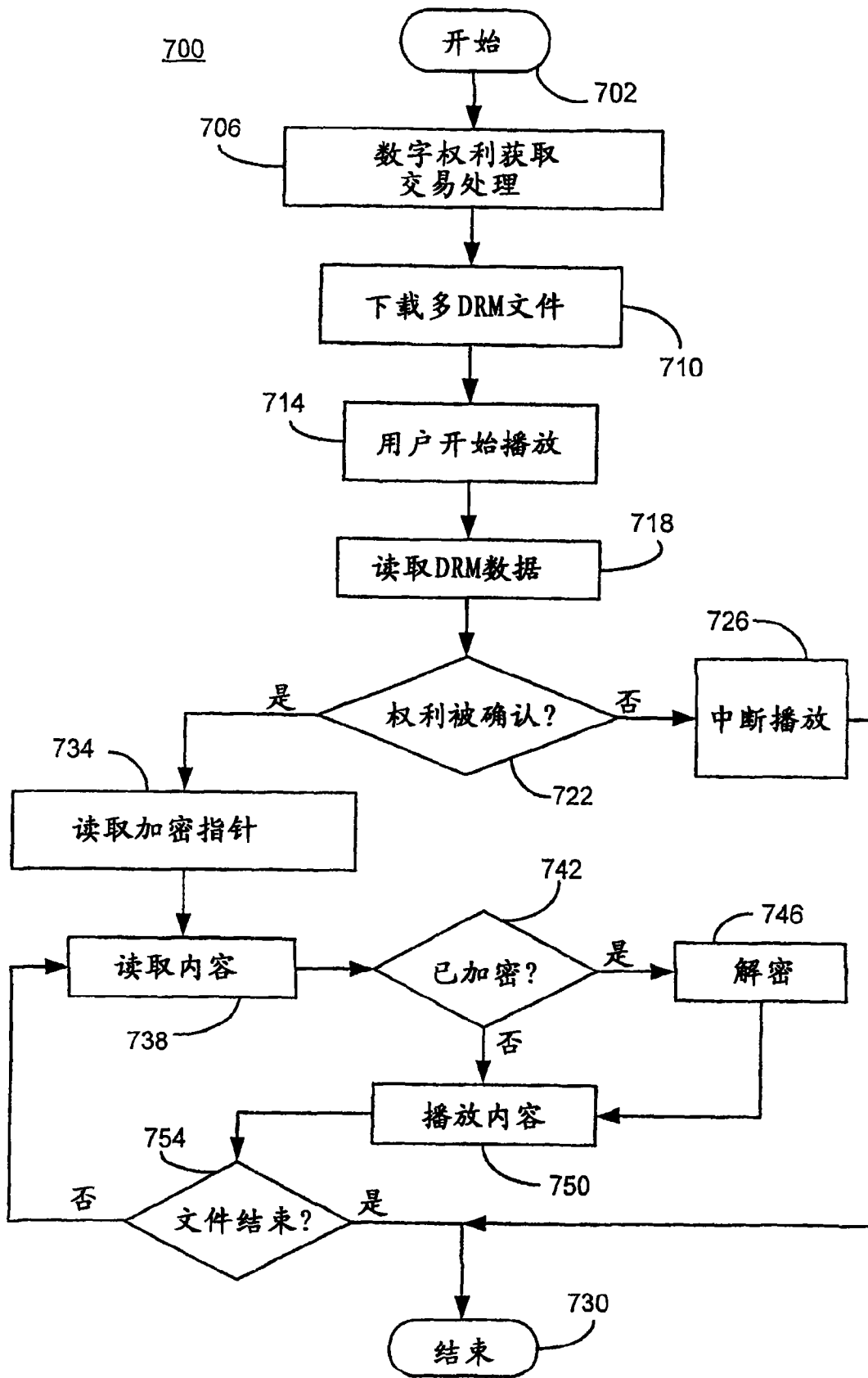


图 7

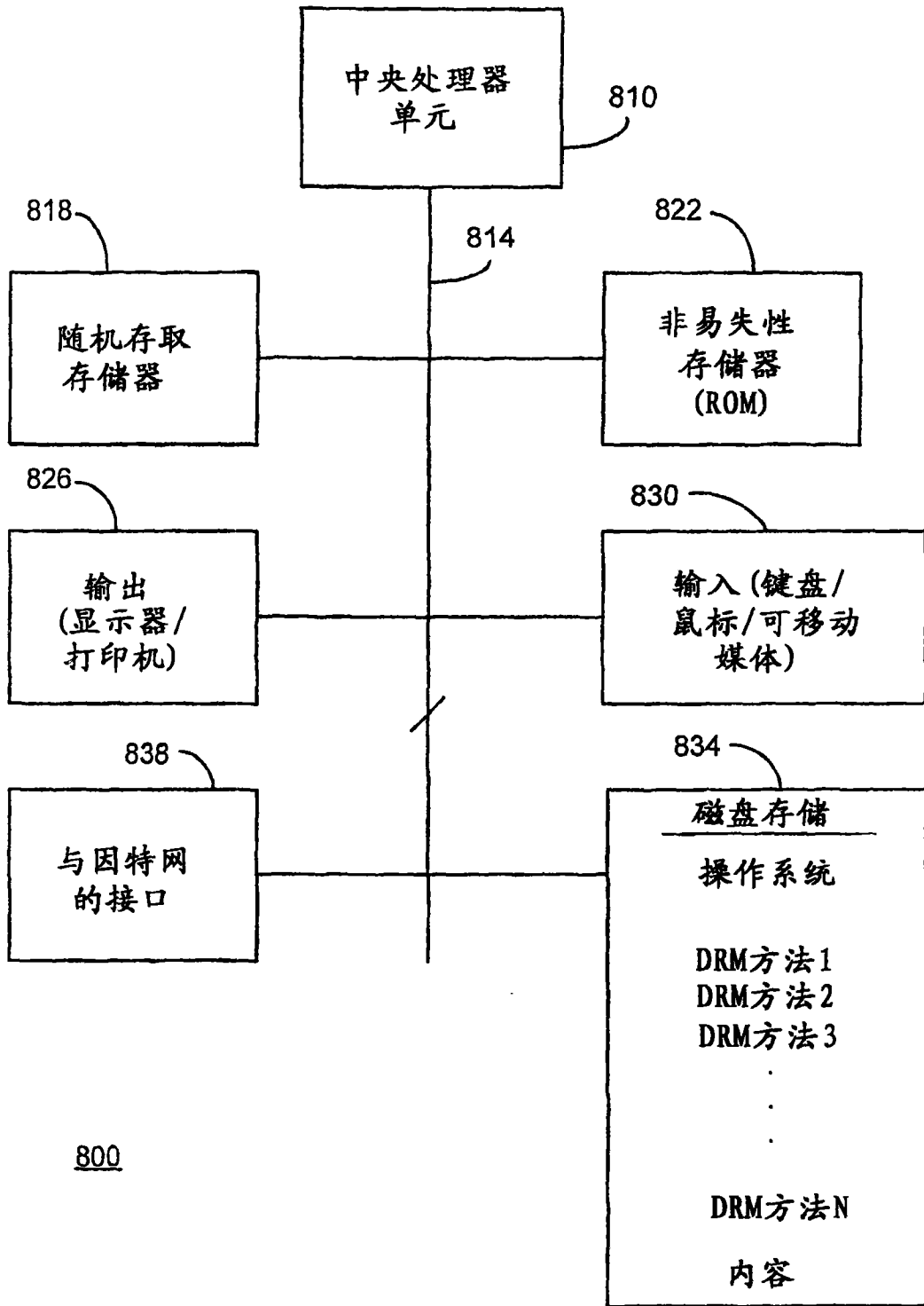


图 8



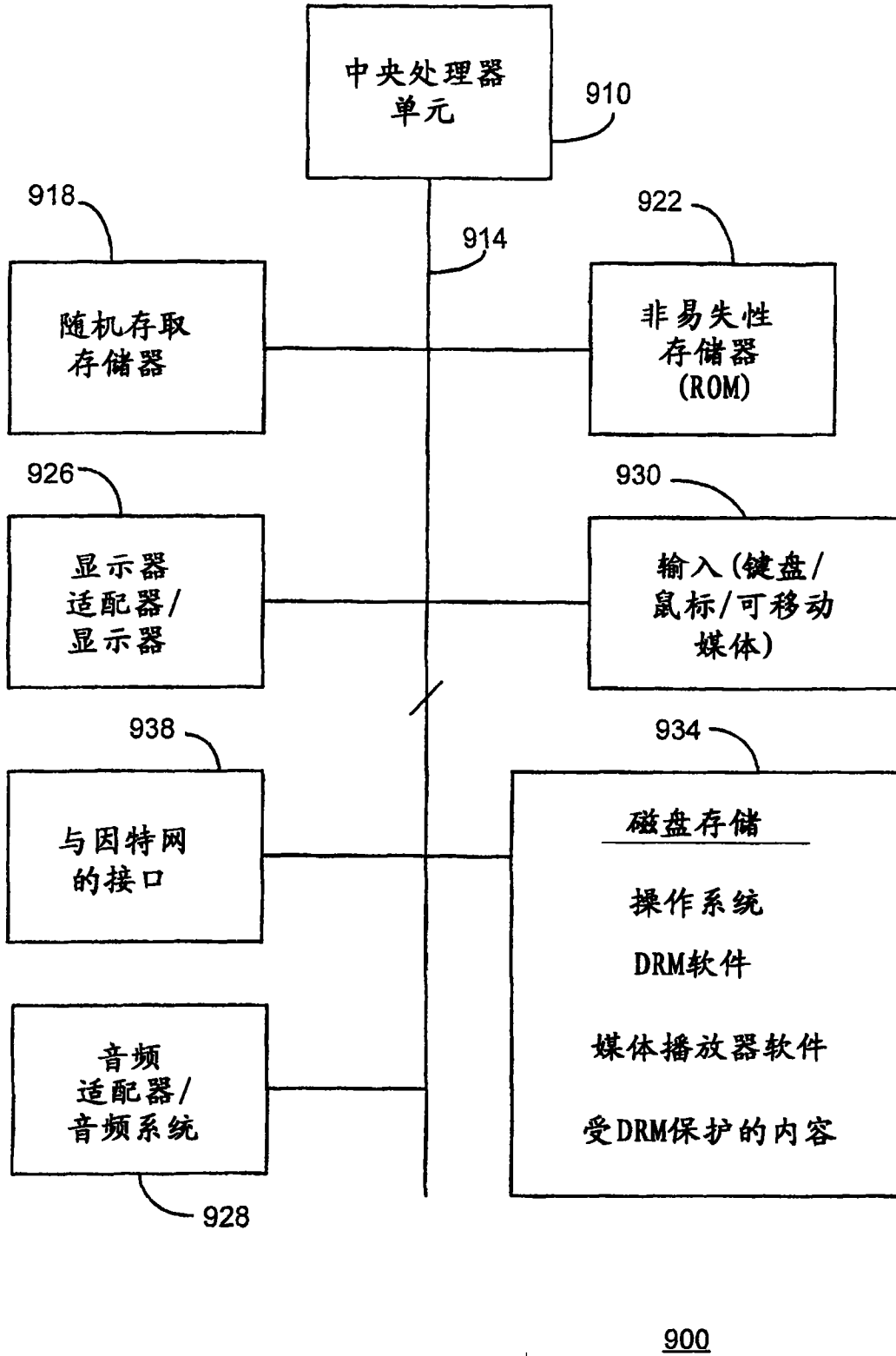


图 9