



[12] 发明专利说明书

[21] ZL 专利号 00800909.0

[45] 授权公告日 2004 年 12 月 22 日

[11] 授权公告号 CN 1181488C

[22] 申请日 2000.3.22 [21] 申请号 00800909.0

[30] 优先权

[32] 1999.3.25 [33] US [31] 60/126,167

[32] 1999.12.3 [33] US [31] 09/454,350

[86] 国际申请 PCT/EP2000/002599 2000.3.22

[87] 国际公布 WO2000/058962 英 2000.10.5

[85] 进入国家阶段日期 2001.1.18

[71] 专利权人 皇家飞利浦电子有限公司

地址 荷兰艾恩德霍芬

[72] 发明人 M·A·埃普斯坦

审查员 邓 魏

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 吴立明 傅 康

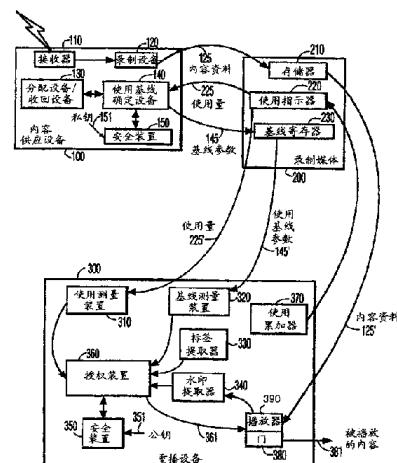
权利要求书 4 页 说明书 10 页 附图 3 页

[54] 发明名称 提供拷贝保护的使用有关的标签

[57] 摘要

拷贝保护资料的每个拷贝带有一种使用限制。一致的重播设备确定该拷贝有多少使用，只在其使用在该拷贝相应的使用限制中时才播放该拷贝保护资料。在本发明的优选实施方案中，拷贝的供应来源包括一种使用总计量，在拷贝保护资料的每个拷贝间分配，从而允许生成拷贝保护资料的不止一个拷贝，或从供应来源的“检出”。当拷贝保护资料的一个拷贝随后被归还，或在供应来源“检入”，与这一拷贝相关的使用分配被归还到使用总计分配中。这样，如果该拷贝保护资料的某个拷贝丢失、损坏或被放错地方，对购买者的损失只是可用使用总计减少了一些。在优选实施方案中，与使用限制相关的参数通过加密方式复制资料进行传递。类似的，在优选实施方案中，与使用限制相关的参数被安全地绑定在拷贝保护资料上，这样非法的供应商不能用非法的资料替代拷贝的资料。

其它的安全方法，如拷贝保护资料的加密、水印、标签，等等，都与以上提到的技术兼容，被包括在本发明的优选实施方案中。



1. 一种重播设备（300），用于播放记录介质（200）中的内容资料（125），重播设备（300）包括：

5 播放器（350），用于基于授权标志（361）播放内容资料（125），使用测量装置（310），用于确定与记录介质（200）相关的使用量，

基线测量装置（320），用于确定至少一个使用基线参数（145），该参数便于确定与内容资料（125）相关的合法期限，

10 授权装置（360），用于基于与记录介质（200）相关的使用量和与内容资料（125）相关的合法期限，来影响授权标志（361），以及

使用累加器（370），用于改进记录介质（200）中的使用指示器（220），以便于确定与记录介质（200）相关的使用量。

15 2. 如权利要求1中的重播设备（300），进一步还包括：

安全装置（350），用于基于与内容资料（125）的供应来源（100）相关的公-私密钥对的公钥来验证该至少一个使用基线参数（145）。

3. 如权利要求2中的重播设备（300），其中：

安全装置进一步还用于基于以下的至少一个鉴定该至少一个使用基线参数（145）：

绑定在该至少一个使用基线参数（145）上的数字签名，该至少一个使用基线参数（145）的密文。

4. 如权利要求1中的重播设备（300），其中：

该至少一个使用基线参数（145）是用一种安全形式绑定到内容资料（125）上的，

安全装置（350），用于鉴定该至少一个使用基线参数（145）与内容资料（125）之间的绑定，

授权装置（360），进一步地还用于根据该至少一个使用基线参数（145）与内容资料（125）之间的所述绑定，影响授权标志（361），

30 5. 如权利要求1中的重播设备（300），其中：

该至少一个使用基线参数（145）被绑定在一个标签上，该标签是基于内容资料（125）水印的哈希值，

授权装置（360）进一步用于根据标签和水印，生成授权标志（361）。

6. 一种内容资料（125）的供应设备（100），包括：
 - 5 录制设备（120），用于将内容资料（125）的一个拷贝录制到记录介质（200）上，
 - 分配设备（130），用于向内容资料（125）的拷贝分配使用总计量的一部分，
 - 10 使用基线测量设备（320），用于确定与记录介质（200）相关的使用量（225）， - 15 基于与记录介质（200）相关的使用量（225）和分配给内容资料（125）这一拷贝的使用总计量的该部分，提供至少一个使用基线参数（145）， - 20 将该至少一个使用基线参数（145）录制在记录介质（200）上，以及
 - 25 安全装置（150），用于以一种安全形式来编码该至少一个使用基线参数（145），进一步还用于将该至少一个使用基线参数（145）绑定在由与内容资料（125）相关的水印的哈希值所生成的标签上。
 7. 如权利要求 6 中的供应设备（100），其中安全装置（150）进一步还用于以一种安全形式来编码该至少一个使用基线参数（145），所述安全形式包含以下的至少一种：
 - 25 绑定在该至少一个使用基线参数（145）上的数字签名，以及使用量（225）的密文。
 8. 如权利要求 7 中的供应设备（100），其中，
 - 25 安全装置（150）进一步还用于将该至少一个使用基线参数（145）绑定在内容资料（125）上。
 9. 如权利要求 6 中的供应设备（100），其中，
 - 分配设备（130）在记录介质（200）随后返回该供应设备时，还进一步地用于收回使用总计量的该部分。
 10. 如权利要求 6 中的供应设备（100），其中，
 - 30 分配设备（130）进一步地，在给定的持续时间后收回使用总计量的该部分。
 11. 一种提供内容资料（125）的方法，该方法包括：

将内容资料 (125) 录制 (560) 到记录介质 (200) 上，
将使用总计量的一部分分配 (520) 给记录介质 (200) 上的内
容资料 (125)，

5 确定 (510) 与记录介质 (200) 相关的使用量 (225)，
基于与记录介质 (200) 相关的使用量 (225) 和使用总计量的
一部分，将至少一个使用基线参数 (145) 记录在记录介质 (200)
上，以便于确定与记录介质 (200) 上的内容资料 (125) 相关的合
法期限，

10 将该至少一个使用基线参数 (145) 绑定在由与内容资料 (125)
相关的水印的哈希值所生成的标签上。

12. 如权利要求 11 中的方法，进一步还包括，

当记录介质 (200) 随后被内容资料 (125) 的供应设备 (100)
处理时，收回使用总计量的该部分。

13. 如权利要求 11 中的方法，进一步还包括，

15 在给定的持续时间后，收回使用总计量的该部分。

14. 如权利要求 11 中的方法，进一步还包括，

将该至少一个使用基线参数 (145) 绑定在内容资料 (125) 上。

15. 如权利要求 11 中的方法，还包括

20 以一种安全形式对该至少一个使用基线参数 (145) 进行编码，
该安全形式包含以下的至少一种：

绑定在该至少一个使用基线参数 (145) 上的数字签名，
该至少一个使用基线参数 (145) 的密文。

16. 一种播放存储在记录介质 (200) 上的内容资料 (125) 的
方法，该方法包括：

25 读取 (610) 与记录介质 (200) 相关的至少一个使用基线参数
(145)，

基于使用基线参数 (145)，决定 (620) 与内容资料 (125) 相
关的合法期限，

读取 (630) 与记录介质 (200) 相关的使用量 (225)，

30 根据合法期限和使用量 (225)，播放 (650) 内容资料 (125)，
以及

在播放 (650) 内容资料 (125) 之后，递增与该存储介质 (200)

相关的所述使用量 (225)。

17. 如权利要求 16 中的方法，进一步还包括，
确定使用基线参数 (145) 的可靠性，其中
播放 (650) 内容资料 (125) 进一步地依赖于使用基线参数 (145)
5 的可靠性。

18. 如权利要求 16 中的方法，进一步还包括，
对内容资料 (125) 的解密，以便上述的播放 (650)。

19. 如权利要求 16 中的方法，进一步还包括，
确定 (640) 与内容资料 (125) 相关的标签的数值，
确定 (640) 与内容资料 (125) 相关的水印，
10 比较 (645) 水印的哈希值与标签的值，以确定与内容资料 (125)
相关的授权，其中，
 内容资料 (125) 的播放 (650) 进一步地还依赖于内容资料 (125)
 的授权。

提供拷贝保护的使用有关的标签

5 技术领域

本发明涉及消费类设备领域，特别是用于防止或阻碍对拷贝保护资料的非法复制的技术。

背景技术

为防止和阻碍对如商业化音乐唱片等拷贝保护资料的非法复制的技术一直在计划和发展中。这些技术一般试图限制从拷贝保护资料的一个合法拷贝上进行复制的数量。同时，该合法拷贝的购买者希望得到为其个人目的对该拷贝进行无限量复制的权利。例如，典型的购买者有权使用多种方法来播放和复制该资料，希望能够用其中任何一种来播放购买的资料，而不受限制。

在本技术中越来越常见的是使用闪存卡来存储资料内容以便在小型的便携设备上重播。这些闪存卡，或者类似的电子存储设备，具有比传统存储介质如磁盘或磁带优越的特性，即它们不含运动的部件，于是更加可靠和鲁棒，而且，一般来说比传统播放器更廉价。还有，这些电子存储设备以及相应的播放器通常比传统的磁盘或磁带及相应播放器小得多，且通常耗电更省，进一步增加了它们用于便携重播系统的适用性。

这些小而不贵的介质用于复制拷贝保护资料的可用性引入了潜在的问题如拷贝保护资料供应商的权利与拷贝保护资料购买者的权利间的平衡。由于该介质很小，打算用于高度便携的应用，该介质丢失、损坏或被放错地方的可能性很大。由此，购买者会希望能够在每次要求替换丢失、损坏或放错地方的拷贝时复制资料内容。相反的，由于介质并不昂贵，对资料内容进行非法的大量复制的可能性很高，资料供应商会期望能够阻止这一非法大量复制。

一种用于限制复制资料内容能力的方法是“检出/检入”系统。在这里，和其中介绍的其它保护方案一样，假设复制和重播设备是“一致的”（conforming）设备，符合用于保护拷贝保护资料的标准。当从一个供应设备向一个便携设备复制一份资料，该一致性供

应设备禁止制作额外拷贝直到含该拷贝的便携设备将其还给供应设备。此方案有许多缺点：如果该便携拷贝丢失、损坏或被放错地方，则它不能被“还给”供应设备，则接下来不能再复制其它拷贝。这样一个潜在的“一次性拷贝”不会被全部消费者接受。相反的，可以5直接从便携拷贝复制材料内容的多个拷贝，从而使本方案失去了保护作用。类似的，尽管允许同时将资料内容复制 N 个拷贝到便携介质上的替代方案可能减轻消费者对拷贝限制的顾虑，这些方案同样被怀疑可能直接从便携介质进行大量的复制。

发明内容

10 本发明的一个目的是提供一种拷贝保护方法和系统，平衡拷贝保护资料内容供应商和该拷贝保护资料内容购买者的权利。本发明进一步的目的是限制由存有拷贝保护资料的介质的丢失所招致的损失的价值。本发明的进一步目的还有限制非法大量生产拷贝保护资料的经济上的可能性。

15 这些及其它的目标是通过将拷贝保护资料的每一拷贝与一使用限制联系在一起实现的。一致的重播设备测定该拷贝已被使用了多少，只当该拷贝的使用在相应的使用限制内时才播放这一拷贝保护资料。在本发明的优选实施方案中，该拷贝的供应源包含“使用总计量”，在拷贝保护资料的每个提供的拷贝间分配，这样允许生成拷贝保护资料的多于一个的拷贝，或从供应源的“检出”。当拷贝20 保护资料的一个拷贝随后被归还，或向供应源“检入”，与该拷贝对应的使用分配被归还到使用总计数值中。在这种方法中，如果拷贝保护资料的某一个拷贝丢失、损坏或被放错地方，对购买者来说，损失的价值只是可用的使用总计的一些减少。在一个优选实施方案中，与使用限制相关的参数用安全的方式借助于该资料的拷贝来传输，这样非法的供应设备不能改变这些参数。类似的，在一个优选实施方案中，与使用限制相关的参数安全地绑定(bind)在拷贝保护资料上，这样非法的供应设备不能用非法的资料来替代复制了的资料。其它的安全方法，如拷贝保护资料的加密、水印、加标签30 (ticketing) 等等，同样与上述的技术是兼容的，被包含在本发明的一个优选实施方案中。

本发明还提供了一种重播设备，用于播放记录介质中的内容资

料。该重播设备包括：播放器，用于基于授权标志播放内容资料；使用测量装置，用于确定与记录介质相关的使用量；基线测量装置，用于确定至少一个使用基线参数，该参数便于确定与内容资料相关的合法期限；授权装置，用于基于与记录介质相关的使用量和与内容资料相关的合法期限，来影响授权标志。还包括使用累加器，用于改进记录介质中的使用指示器，以便于确定与记录介质相关的使用量。

本发明还提供了一种内容资料的供应设备。它包括：录制设备，用于将内容资料的一个拷贝录制到记录介质上；分配设备，用于向内容资料的拷贝分配使用总计量的一部分。该供应设备还包括使用基线测量设备，用于确定与记录介质相关的使用量，基于与记录介质相关的使用量和分配给内容资料这一拷贝的使用总计量的该部分，提供至少一个使用基线参数，将该至少一个使用基线参数录制在记录介质上。以及安全装置，用于以一种安全形式来编码该至少一个使用基线参数，进一步还用于将该至少一个使用基线参数绑定在由与内容资料相关的水印的哈希值所生成的标签上。

此外，本发明还描述了一种提供内容资料的方法。该方法包括将内容资料录制到记录介质上。将使用总计量的一部分分配给记录介质上的内容资料。确定与记录介质相关的使用量。基于与记录介质相关的使用量和使用总计量的一部分，将至少一个使用基线参数记录在记录介质上，以便于确定与记录介质上的内容资料相关的合法期限。以及将该至少一个使用基线参数绑定在由与内容资料相关的水印的哈希值所生成的标签上。

本发明还提供了一种播放存储在记录介质上的内容资料的方法。该方法包括读取与记录介质相关的至少一个使用基线参数。基于使用基线参数，决定与内容资料相关的合法期限。读取与记录介质相关的使用量。根据合法期限和使用量，播放内容资料。以及在播放内容资料之后，递增与该存储介质相关的所述使用量。

附图说明

通过关于所附图中的实例，更详细地对本发明进行阐述，其中：
图 1 所示为根据本发明的使用有关的标签系统的示例框图。
图 2 为根据本发明的示例流程图，用于录制使用有关资料内容。

图 3 为根据本发明的示例流程图，用于播放使用有关资料内容。贯穿这些附图，相同的标号表示相似和相关的特征或功能。

具体实施方式

图 1 所示为根据本发明的使用有关的标签系统的示例框图。该使用有关标签系统包括内容供应设备 100，记录介质 200，及重播设备 300。由于在“安全数字音乐主动（Secure Digital Music Initiative）”（SDMI）中使用，该内容供应设备 100 被称为“SDMI 许可服从模块”（LCM），记录介质 200 被称为“服从 SDMI 的存储介质”（CSM），而重播设备 300 被称为“便携设备”（PD），尽管这里陈述的原理的使用对超过 SDMI 标准的同样适用。

内容供应设备 100 通常是从遥远的地方，如因特网上的一个站点，通过接收器 110，接收到资料内容，尽管内容供应设备 100 也可能是传统的 CD，DVD 或其它媒体播放器设备，设定为可用有限拷贝的方式将其介质中内容的拷贝提供给其它记录介质 200。即，接收器 110 代表所有这样的设备：通过录音机 120 提供录制在记录介质 200 的存储器 210 中的资料内容 125。尽管这一发明适合用于存储器 210，其它存储器存储技术，例如使用磁性或光学的盘、带、棒（rod）等等也都可以。

为了防止对资料内容 125 的大量复制，内容供应设备 100 将有限的使用总计量的一部分分配给资料内容 125 的每个录制在记录介质 200 的拷贝上。当使用总计量完全分配给了记录介质 200，内容供应设备 100 不再进一步提供资料内容 125 的拷贝。当记录介质 200 归还给内容供应设备 100，内容供应设备 100 将分配给这一部分记录介质 200 的使用总计量归还给总的量。即，当每个拷贝被归还，内容供应设备收回被分配给该拷贝的部分，从而补充了使用总计量，可供接下来再次分配。通过这种方式，资料内容的购买者只被限制关于拷贝保护资料的同时在使用中的拷贝数量。

根据本发明，根据已被分配的使用总计量的部分，记录介质 200 被规定了一套“使用基线参数”145，而一致的重播设备 300 执行这一分配，通过从记录介质 200 中依照这次分配的部分播放资料内容 125'。可以使用许多方案量和监控这次分配的使用情况。例如使用总计量可以是重播或演奏资料内容 125' 的总次数，如 50 次演奏，记

录介质 200 可以被分配 10 次演奏。这一分配，10，被存储在记录介质 200 上的基线寄存器中，作为一个使用基线 参数 145，被重播设备 300 递减，或者在每次重播设备 300 演奏资料内容 125' 时，由记录介质 200 递减。当基线寄存器 230 内为 0，就由重播设备 230 或记录介质 200 来禁止进一步的演奏。其它使用量包括测量介质 200 被重播设备 300 播放的时间，测量介质 200 被插入或被拔出重播设备 300 的次数，测量资料内容被录制到介质 200 上后过去的时间，等等。这样的分配、量和这些使用参数的加强对于本领域中的一般技术人员，在考虑到本文中提出的原理后，是很显然的。

当“被删除的”记录介质 200 归还给内容供应设备 100，使用总计量因收回曾被分配给这一记录介质 200 的 10 次演奏而得到补充。这样，记录介质 200 又可被再次分配与它前面接收到的同一资料内容 125 或新的资料内容相关的使用总计量的一部分。注意到使用总计量是与每一个拷贝保护资料内容相关的，可以与其它拷贝保护资料内容的不同，可以不同地进行分配。由于重播设备 300 或记录介质 200 加强了以上所述的使用限制，同时由于一致的播放器 300 期望记录介质 200 包含这一使用限制，从记录介质 200 进行该资料内容非法复制的市场价值很低。即，如果非法拷贝包含了内置于已分配使用的使用基线参数 145 的基线寄存器 230，非法拷贝只有一段有限的可用时间；或者，如果它不包含这一使用基线参数 145，将不能在一致的播放器 300 上使用。这样，根据本发明的原理，通过给资料内容 125 的每个拷贝分配使用参数，购买者被提供了一种可以生成资料内容 125 的多个拷贝的方法，同时，由对资料内容 125 非法大量复制而产生的损害被使用分配的加强而限制。相对的，记录介质 200 上额外消耗的空间对购买者来说是可以接受的，因为只是失去可分配使用总计量的一部分。

以上叙述了本发明的原理，但如以上所述的，并没有排除非法的大量复制。以上叙述中的薄弱环节在于有可能篡改前面提到的使用基线参数。在本发明的优选实施方案中，使用基线参数 145 通过安全装置 150，用一种可核实的形式存储在记录介质 200 上。很多安全技术都可以使用，使用本领域的常用技术。在优选实施方案中，使用基线参数 145 可用拷贝保护资料“可靠来源”相关的私人密钥

151，进行加密或数字签名，或二者同时使用。优选实施方案的重播设备 300 包括相应的安全装置 350，使用指定给“可靠来源”的公私密钥对中与私人密钥 151 对应的公钥 351，鉴定从记录介质 200 读出的使用基线参数 145' 的来源。或者，可以使用一个两层结构，其中嵌入重播设备 300 的第一个公钥用来鉴定内容供应设备 100 给出的第二个密钥。用这种方法，每个可能的内容供应设备的公钥无须事先提供。即，重播的公钥可用于给所有内容供应设备授权。每个内容供应设备会用于所有重播设备制造商这样的授权。通过对使用基线参数 145' 的来源的鉴定，用伪造的使用基线参数 145 代替，在记录介质 200 上存放资料内容 125 的非法拷贝将是无效的。另一方面，对记录介质 200 的“盲目复制”，具有与资料内容 125 相关的被授权的使用分配，会提供一个可用的赝品，因为使用基线参数 145 的可验证形式也会被复制。但是，如上述的，这些伪造的拷贝的经济价值很低，这样就不是非法大量复制的好目标，因为复制的使用基线参数会使记录介质 200 存储器 210 上的内容只有很有限的有效期。

优选实施方案包括其它进一步保护资料内容以防非法大量复制的方法。在重播设备 300 中的授权装置 360 协调这些安全方法和控制，或是用门，重播设备 300 的播放器 390 输出通过一个门 380 播放 381 资料内容。如果所有这些安全测试通过，授权装置 360 插入一个授权标志 361，允许资料内容 125' 变为播放器 390 演奏的内容 381。或者，这些安全方法的部分或全部可在记录介质 200 内加强，尽管如上述的，在记录介质 200 内复制这样的加强设备的费用表示将授权 360 和安全装置 350 放在每个重播设备 300 中更好。

作为额外的安全方法，记录介质包含使用指示器，只是记录介质 200 引起的使用数量。更好地，使用指示器是一个只能增加的计数器，不能减少或被清零。更好地，这一使用指示器包含一个关于其它记录介质的随机数，这样它的数值不能被预先确定。在每次使用记录介质时，使用指示器 220 的值增加。为便于理解，在重播设备 300 中示出了使用累加器 370，尽管使用指示器 220 也可在每次访问存储器 210 时由播放器 300 来增加，或者由每次插入播放器 300，或者多种明确或含蓄地表示使用的任意一种指示方法。例如，如果

用时间来量使用，记录介质 200 或播放器 300 可以包含一个时钟控制系统，周期性地增加使用指示器 220 的值。在优选实施方案中，当资料内容 125 被提供给记录介质 200 时，内容供应设备 100 从使用指示器读取使用量 225。内容供应设备 100 用该使用量 225 来生成使用基线参数 145，从而将使用基线参数 145 绑定在具体的记录介质 200 上。例如，使用基线参数 145 可能含有这一初始的使用量 225 和使用量总计的分配给资料内容这一拷贝的部分。一致的重播设备 300 从记录介质 200 通过基线测量装置 320，读出（和验证）使用基线参数 145，以及通过使用测量装置 310，读出（和验证）使用指示器 220 的当前值。根据本发明的这一方面，重播设备 300 只当当前使用量 225，介于使用基线参数 145 中的使用量的初始和最终值之间时才播放 361 资料内容 125'。通过只增的使用指示器 220，不能仅仅从含有资料内容 125 合法拷贝的记录介质 200 上将使用基线参数 145 复制到其它的记录介质 200 上来生成资料内容 125 的非法拷贝，因为每一记录介质 200 都可能有，或被设计成含有一个统计上唯一的使用量 225。即，例如，使用指示器可以是一个很大的计数器（如 64 位或更大），在制造时初始化为一个随机数，可以采用一些方法来阻止这个计数器用过快的速度递增。这样制造的空白记录介质 200 的购买者不能给它们用同样的使用基线参数，因为每一介质 200 可能含的使用量彼此有本质不同。

在本领域中常用的其它安全技术，也可以应用。如图 1 所示，重播设备 300 含有标签提取器 330 和水印提取器 340。一般来说，水印是被插入资料内容的一致标志，不破坏或从本质上降解资料内容就不能去掉水印。如美国专利申请“标签加密的拷贝保护”中所述，序列号 09/333,628，1999 年 6 月 15 日归档，Michael A. Epstein，律师记录表 PHA23,457，在此引用作为参考，用于控制访问资料内容的权利可以与水印结合起来，典型的是通过单行哈希函数的方法。提供了多种检测标签合法性的规则，是基于与水印的哈希、或多重哈希的数值相比较。如果资料内容 125' 含有水印，但不含合法的标签，授权装置 360 将禁止它的播放 361，尽管它的如上所述的使用量是合法的。通过这种方法，非法得到的资料内容 125 不能被录制在含有合法使用量和参数的记录介质 200 上。为了进一步防止替代的资料

内容 125 被非法录制在含有合法使用量和参数的记录介质 200 上，本发明的优选实施方案将使用基线参数 145 与部分使用总计量被分配的资料内容绑定在一起。例如，上面提到的标签在被装入记录介质 200 的使用基线寄存器 230 中之前，可以包含在被加密或数字签名的使用基线参数 145 中。用赝品替代标签或资料内容或二者的试图，结果会是被与安全装置 350 相连的授权装置 360 拒绝。替代的标签不能通过前面提到的基于可靠供应设备的公钥的验证测试，无论它是否与资料内容匹配，而替代的伪造资料内容不会和与原始资料内容相关的验证标签匹配。

为了完整，根据本发明的多个方面，图 2 所示为录制使用有关资料内容的示例流程图，而图 3 为用于播放这一录制的使用有关资料内容的示例流程图。正如前面提到的，每一讨论到的安全技术减少了非法大量复制拷贝保护资料的经济上的可行性，而多种技术或技术的结合可以达到想要的安全水平。图 2 和图 3 中的技术和测试只作阐述用途。

在录制或潜在录制的开始，在 510 接收到与该存储介质相关的当前使用量。没有在这一流程图中显示的，如果这一记录介质先前从录制设备接收了使用分配，这一分配被归还给与原来录制的资料内容相关的使用总计量中。在 520，使用总计量中与当前提供的资料内容相关的部分被分配给这一记录介质。如果，在 225，由于制作了该资料内容的许多其它拷贝又没有归还，没有可分配的了，录制过程 530-560 被跳过。在 530，基于当前的使用量和分配的使用，检测使用基线参数。这些参数通过例如前面提到的与资料内容相关的标签，或直接绑定在资料内容上，参数的数值和绑定在 540 被保护。保护可以是参数的加密，参数的数字签名，或者二者结合，更好地是基于与资料内容供应商相关的公-私密钥对的私钥。在 550，这组加了密的参数被录制在记录介质上。公-私密钥对的公钥是普遍都知道的，尤其是一致的播放器，要从记录介质读取这些加密的信息的。在 560，资料内容被录制在记录介质上。这一过程继续到 570，其中录制设备可能发出消息，确认录制过程的结束，或者发出消息，报告没有足够的使用分配来录制，等等。

在重播或播放过程的开始，从记录介质中读取使用基线参数，

图 3 中的 610。作为授权的第一次测试，在 615，鉴定这些参数的可信。如上所述，在优选实施方案中，这些参数，用与资料内容的可靠供应商相关的私钥被加密或签名，或二者结合。重播设备使用与该可靠供应商相关的相应公钥，通过解密或鉴定签名，或二者兼具，鉴定这些参数的可信。其它用于鉴定受保护的项目正确性的技术是该领域中常用的。如果，在 615，这些参数没有被鉴定为是可信的，剩下的过程 620—650 被跳过。在 620，由通过鉴定的参数决定合法的使用期间，在 630，从记录介质读取当前使用量。如果在 635，当前使用量不在合法使用期间内，剩下的过程 640—650 被跳过。在 640，检测与该资料内容相关的标签和水印。如上所述，标签最好包含 615 被鉴定的参数。水印典型的是用本领域常用的技术，在读到时从资料内容中抽取出来检测。在 645，比较标签和水印，以鉴定资料内容是被授权播放的；如果不是，在 650 的播放过程被跳过。在 650，播放资料内容。即，如果资料内容是音频记录，生成与记录对应的音频声音；如果资料内容是视听的，生成与记录对应的视听再现；等等。其后，过程继续到 660，其中，显示例如“未授权”消息，作为在 615，635 或 645 测试失败的响应。

上述只是阐述了本发明的原理。可以注意到那些本领域的熟练技术人员将能够设计各种各样的方案，尽管这里没有明确地描述或展示，但体现了本发明的原理，在它的精神和范围内。例如，被分配给每一记录介质 200 的使用限制量的部分可以是用户可选择的，这样用户可以给希望经常使用的介质 200 分配大量的使用，而给要带到丢失或损坏的可能性很大的场合下的记录介质 200 分配较小的使用。同时，分配过程和分配的加强还可随着时间继续发展，基于客户对这些限制的反应。与不断进化的过程一致，内容供应设备 100 和重播设备 300 的功能模块可以被设定成能通过例如从国际互联网站点下载来接收新的操作代码或参数。同样地，应该注意到，限制使用的目的在于防止资料内容的大量复制。与这一目的一致的，部分的以上规则可以放松，从而进一步减轻原始资料内容购买者身上的负担。例如，在某段相当长的时间后，补充使用限制量，适应丢失的介质 200。即，例如，使用限制量可以每月，至少部分地进行补充。这样，即使一位经常丢失记录媒体的购买者也可以得到不断的、

尽管是有限制的供应；相反的，每月的使用限制可以排除有效的大量复制。这些那些的系统配置和优化特征对本领域的普通技术人员，在考虑到本文后，是很显然的，它们包含在下述权利要求的范围内。

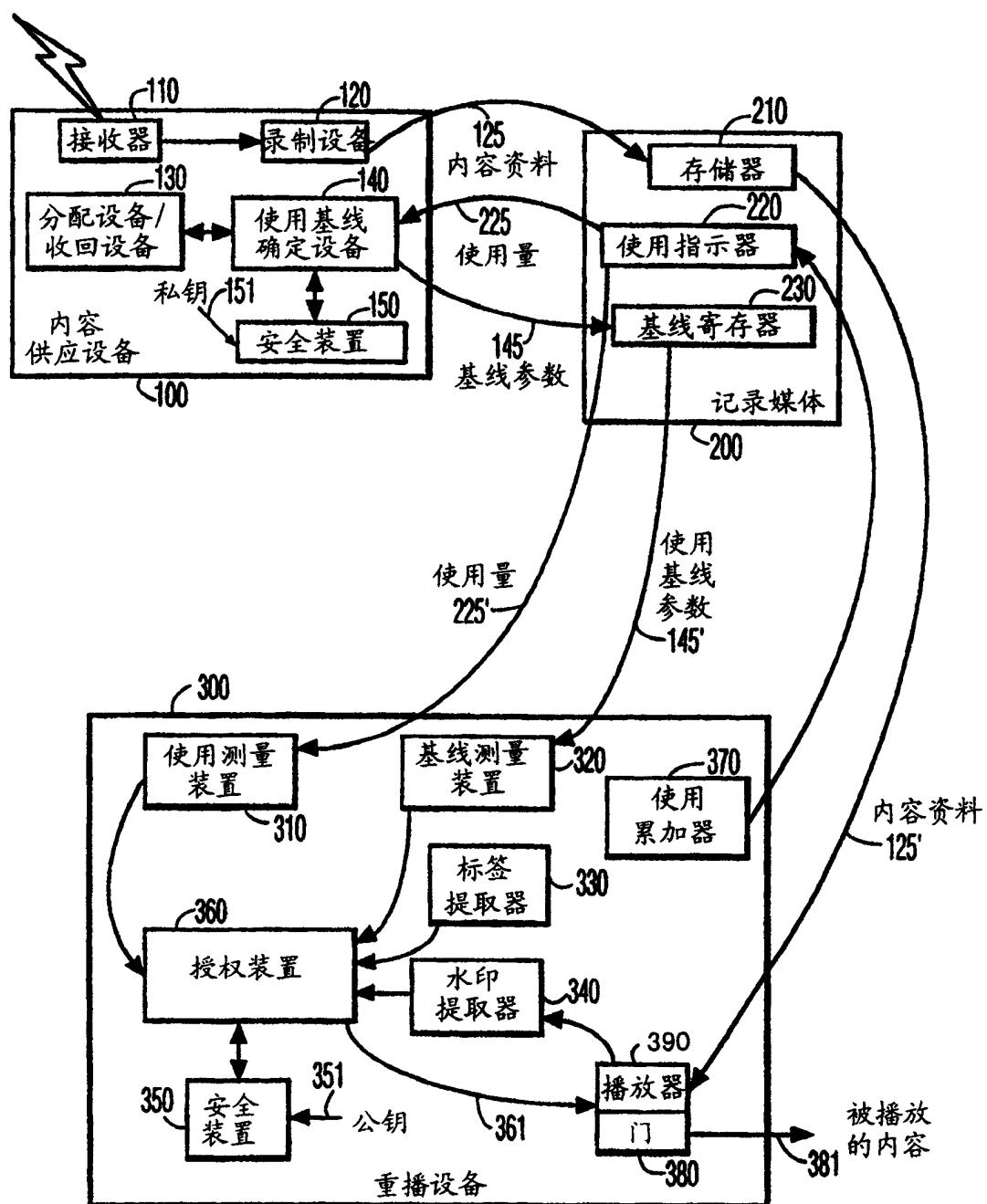


图 1

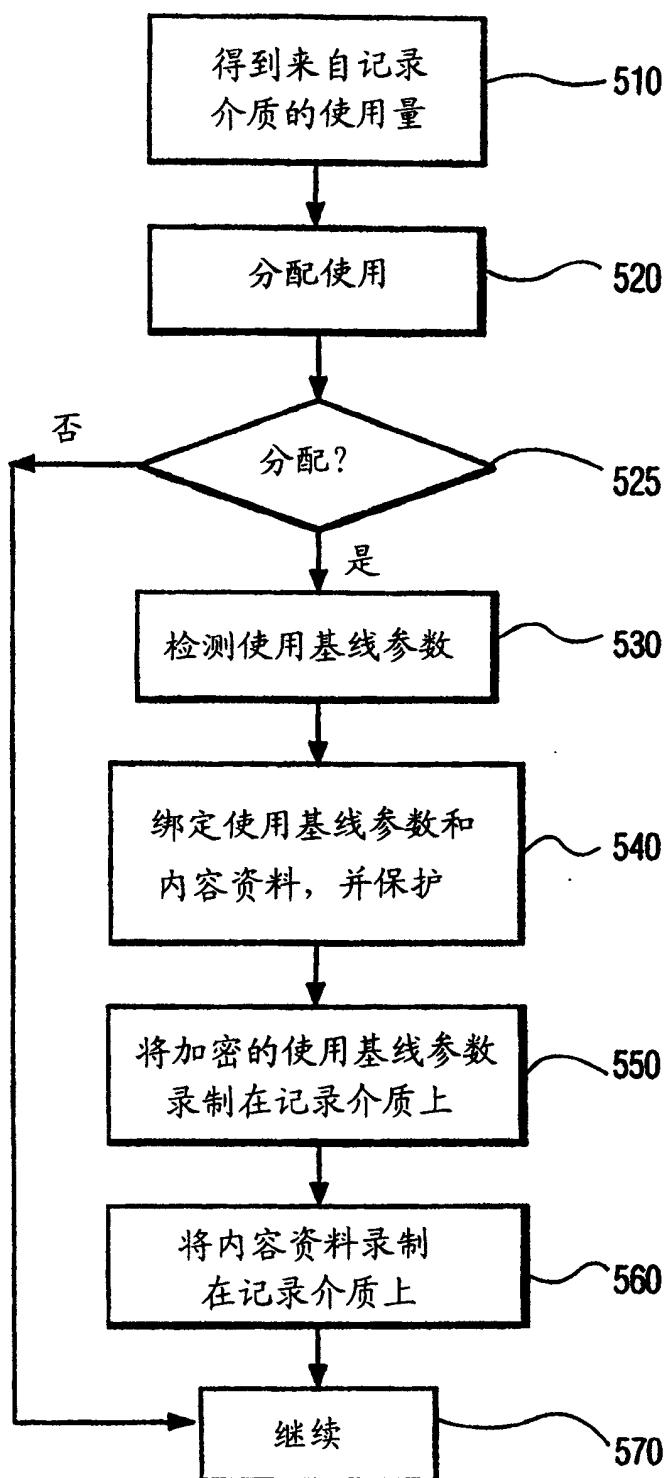


图 2

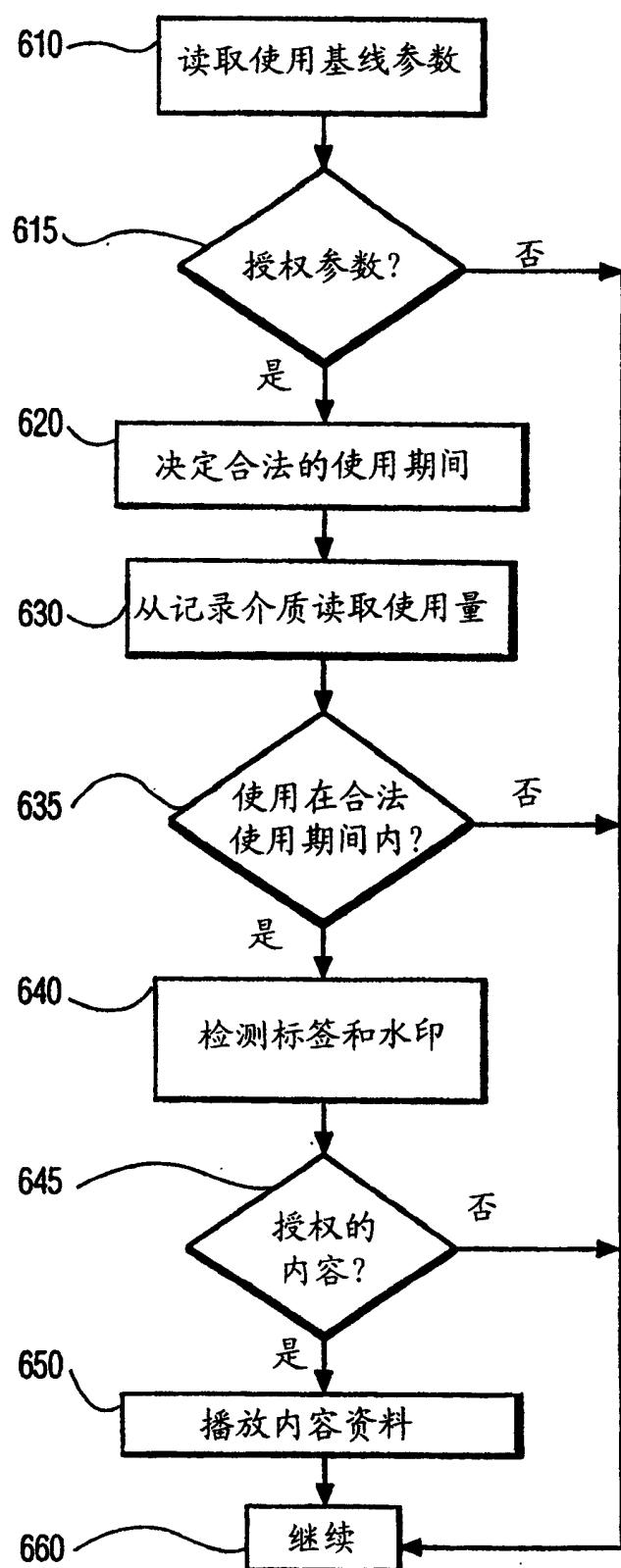


图 3