(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102982256 A
(43)申请公布日 2013.03.20

(21)申请号 201210342302.8

(22)申请日 2006.01.13

(30)优先权数据
10-2005-0112554 2005.11.23 KR
60/643,150 2005.01.13 US

(62)分案原申请数据
200680002172.6 2006.01.13

(71)申请人 三星电子株式会社
地址 韩国京畿道水原市

(72)发明人 吴润相 郑勋任 沈相奎 李硕凤

(74)专利代理机构 北京铭硕知识产权代理有限公司 11286
代理人 郭鸿禧

(51)Int.Cl.
G06F 21/10(2013.01)
G06F 21/60(2013.01)

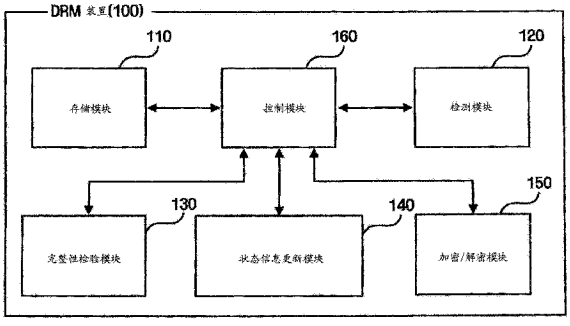
权利要求书 2 页 说明书 10 页 附图 8 页

(54)发明名称

用于数字权利管理的装置和方法

(57)摘要

提供一种数字权利管理(DRM)装置和方法。该DRM装置包括:存储模块,存储具有预定元信息的权利对象(RO);控制模块,当RO检测请求被输入时,提供存储在存储模块中的RO的元信息;完整性检验模块,保持元信息的完整性。



CN 102982256 A

1. 一种数字权利管理装置，包括：

存储模块，存储具有预定元信息的权利对象；

控制模块，当权利对象检测请求被输入时，提供存储在存储模块中的权利对象的元信息；

完整性检验模块，通过使计算的散列值与存储的散列值相等，来保持元信息的完整性，

其中，元信息包括下列至少一种：关于重放预定内容对象的权利对象的消耗限制的限制信息以及关于权利对象的可用性的状态信息，

其中，关于权利对象的可用性的状态信息包括有效状态、无效状态和未识别状态，在有效状态下，权利对象可用，在无效状态下，权利对象不可用，在未识别状态下，权利对象的可用性不能被识别，

其中，所述数字权利管理装置还包括状态信息更新模块，当有效的权利对象被用完并且没有权利对象可用时，状态信息更新模块将关于权利对象的可用性的状态信息改变为无效状态，

其中，权利对象具有除了元信息以外的部分，所述部分被加密，

其中，所述部分包含内容加密密钥，在通过对内容对象进行解密来获得原始内容的过程中使用所述内容加密密钥。

2. 根据权利要求 1 所述的数字权利管理装置，其中，存储模块存储元信息的预定散列值，完整性检验模块使用预定的散列函数计算控制模块提供的元信息的散列值，并且使计算出的散列值与存储在存储模块中的散列值相等。

3. 根据权利要求 1 所述的数字权利管理装置，其中，元信息还包括关于内容对象的重放和再现类型的允许信息。

4. 根据权利要求 1 所述的数字权利管理装置，其中，完整性检验模块计算具有改变的状态信息的元信息的散列值，并且用计算出的散列值更新预先存储在存储模块中的散列值。

5. 根据权利要求 1 所述的数字权利管理装置，其中，当状态信息被设置为处于未识别状态时，状态信息更新模块将检测元信息时的时间信息与限制信息进行比较以确定权利对象是否可用，如果权利对象被确定为处于不可用状态，则将权利对象的状态信息改变为无效状态，其中，完整性检验模块计算具有改变的状态信息的元信息的散列值，并且用计算出的散列值更新预先存储在存储模块中的散列值。

6. 一种数字权利管理方法，包括：

当权利对象检测请求被输入时，提供存储在预定存储介质中的权利对象的元信息；

通过使计算的散列值与存储的散列值相等，来保持元信息的完整性，

其中，元信息包括下列至少一种：关于重放预定内容对象的权利对象的消耗限制的限制信息以及关于权利对象的可用性的状态信息，

其中，关于权利对象的可用性的状态信息包括有效状态、无效状态和未识别状态，在有效状态下，权利对象可用，在无效状态下，权利对象不可用，在未识别状态下，权利对象的可用性不能被识别，

其中，当有效的权利对象被用完并且没有权利对象可用时，关于权利对象的可用性的状态信息被改变为无效状态，

其中，权利对象具有除了元信息以外的部分，所述部分被加密，

其中，所述部分包含内容加密密钥，在通过对内容对象进行解密来获得原始内容的过程中使用所述内容加密密钥。

7. 根据权利要求 6 所述的数字权利管理方法，其中，存储介质存储元信息的预定散列值，并且保持完整性的步骤包括：使用预定的散列函数计算元信息的散列值并使计算出的散列值与存储在存储介质中的散列值相等。

8. 根据权利要求 6 所述的数字权利管理方法，其中，元信息还包括关于内容对象的重放和再现类型的允许信息。

9. 根据权利要求 6 所述的数字权利管理方法，其中，更新步骤包括：

计算具有改变的状态信息的元信息的散列值；

用计算出的散列值更新预先存储在存储介质中的散列值。

10. 根据权利要求 6 所述的数字权利管理方法，其中，当状态信息被设置为处于未识别状态时，所述数字权利管理方法还包括：

将检测元信息时的时间信息与限制信息进行比较，以确定权利对象是否可用；

如果权利对象被确定为处于不可用状态，则将权利对象的状态信息改变为无效状态；

计算具有改变的状态信息的元信息的散列值；

用计算出的散列值更新预先存储在存储介质中的散列值。

用于数字权利管理的装置和方法

[0001] 本申请是申请日为 2006 年 1 月 13 日、申请号为 200680002172.6、发明名称为“用于数字权利管理的装置和方法”的发明专利申请的分案申请。

技术领域

[0002] 与本发明一致的装置和方法涉及数字权利管理，更具体地讲，涉及这样一种数字权利管理，通过该数字权利管理可有效地管理关于权利对象的信息。

背景技术

[0003] 近来，已经积极地研究和开发了数字权利管理（在下文中称为 DRM）。使用 DRM 的商业服务已经被使用或将被使用。由于数字内容的各种特性，诸如拷贝和容易分发数字内容的能力，需要使用 DRM。

[0004] 已经做出一些努力来保护数字内容。通常，数字内容保护集中于防止数字内容的未经许可的访问，仅允许已经付费的人访问数字内容。因此，允许已经对数字内容付费的人对数字内容解密，而不允许没有付费的人对数字内容解密。然而，在这种情况下，当已经付费的人想要将数字内容分发给其他人时，其他人可使用这些数字内容而无需付费。

[0005] 为了解决这个问题，提出了 DRM。在 DRM 中，允许任何人免费访问编码的数字内容，但是需要被称为权利对象的许可来解码和执行数字内容。

[0006] 参照图 1，装置 10 从内容提供商 20 获得数字内容。这里，内容提供商 20 提供的数字内容是加密的格式。为了播放加密的数字内容，需要权利对象 (RO)。

[0007] 装置 10 可从 RO 发布者 30 获得带有许可的 RO 以播放接收的加密的内容。为此，用户应该付费。使用包含在 RO 中的密钥来对加密的数字内容进行解密。

[0008] RO 发布者 30 将权利对象发布详细报告提供给内容提供商 20。RO 发布者 30 和内容提供商 20 可以是同一授权者。

[0009] 在获得 RO 之后，装置 10 消耗该 RO，从而使用加密的数字内容。

[0010] 加密的数字内容可被免费地拷贝或分发给另一装置（未示出）。但是，由于与加密的数字内容不同，RO 包含诸如计数、间隔或拷贝等限制信息，所以 RO 具有对加密的数字内容重复使用或复制的限制。因此，通过使用 DRM 可更有效地保护数字内容。

[0011] 存储有 RO（这在 DRM 中非常重要）的装置应该安全地保护该 RO 不被外部装置试图访问。通常，一方面，通过将 RO 存储在装置的预定安全存储区中，从而以硬件方式保护 RO。另一方面，通过使用各种加密算法在加密状态下存储 RO，从而以软件方式保护 RO。

发明内容

[0012] 技术问题

[0013] 但是，这种基于加密的保护技术可导致装置存储器在读取和写入操作时速度降低。例如，当用户想要搜索存储在装置中的 RO 的信息时，该装置需要对加密的 RO 解密，从解密的 RO 提取信息，然后显示提取的信息，从而导致了对用户请求的慢响应，当 RO 存储在

操作能力低于能重放内容对象的普通装置的便携式存储装置中时，尤其加重了以上问题。

[0014] 技术方案

[0015] 本发明提供一种有效地搜索关于权利对象的信息的方法。

[0016] 当本领域技术人员阅读下面的描述、附图以及权利要求时，本发明以上提到方面以及其它方面、特点和优点对于本领域技术人员将变得清楚。

[0017] 根据本发明的一方面，提供一种数字权利管理 (DRM) 装置，该数字权利管理装置包括：存储模块，存储具有预定元信息的权利对象 (RO)；控制模块，当 RO 检测请求被输入时，提供存储在存储模块中的 RO 的元信息；完整性检验模块，保持元信息的完整性。

[0018] 根据本发明的另一方面，提供一种数字权利管理 (DRM) 方法，该数字权利管理方法包括：当权利对象 (RO) 检测请求被输入时，提供存储在预定存储介质中的 RO 的元信息；保持元信息的完整性。

附图说明

[0019] 通过参照附图来详细地描述本发明的示例性实施例，本发明的上述和其它方面将会变得更加清楚，其中：

[0020] 图 1 是传统的数字权利管理 (DRM) 的概念图；

[0021] 图 2 是根据本发明示例性实施例的 DRM 装置的框图；

[0022] 图 3 是示出根据本发明示例性实施例的数字权利管理方法的流程图；

[0023] 图 4 是示出根据本发明示例性实施例的元信息的完整性被保持的过程的流程图；

[0024] 图 5 是根据本发明示例性实施例的主机装置的框图；

[0025] 图 6 是示出根据本发明示例性实施例的 DRM 系统的示图；

[0026] 图 7 是根据本发明示例性实施例的便携式存储装置的框图；

[0027] 图 8 是示出根据本发明示例性实施例的认证过程的流程图；

[0028] 图 9 是示出根据本发明示例性实施例的主机装置检测存储在便携式存储装置中的权利对象的检测过程的流程图。

具体实施方式

[0029] 可参照下面详细的示例性实施例的描述以及附图来更容易地理解本发明的各方面。但是，可按照多种不同的形式来实施本发明，而不应被理解为限于这里所阐述的示例性实施例。相反，提供这些示例性实施例，以使得本公开透彻和完整，并向本领域技术人员全面传达本发明的构思，并且本发明仅由权利要求所限定。在整个说明书中，相同的标号表示相同的部件。

[0030] 在下文中，将参照附图来详细描述本发明的示例性实施例。

[0031] 在进行详细描述之前，简要地描述本说明书中使用的术语。对术语的描述应该被解释为用于更好地理解说明书和在说明书中没有明确定义的术语，而不是限制本发明的宽广方面。

[0032] - 主机装置

[0033] 主机装置可连接到便携式存储装置，并且使得加密的内容被执行。示例性的主机装置是便携式多媒体装置，诸如移动电话、PDA 或 MP3 播放器、桌上型计算机或数字 TV 等。

[0034] - 便携式存储装置

[0035] 在本发明示例性实施例中使用的便携式存储装置包括非易失性存储器（诸如闪速存储器），数据可被写入到该非易失性存储器中，从该非易失性存储器可读取数据和删除数据，该非易失性存储器可连接到一装置上。这样的便携式存储装置的示例是智能介质、存储棒、致密闪速 (CF) 卡、xD 卡和 MMC。

[0036] - 内容对象

[0037] 内容对象是处于加密状态的数字内容。这里，数字内容的示例包括但不限于，运动画面、静止画面、游戏、文本等。

[0038] - 权利对象

[0039] 权利对象是一种用于使用加密的内容对象的许可。权利对象可包括内容加密密钥、允许信息、限制信息、状态信息和内容对象标识符，内容对象标识符可识别将使用内容加密密钥被播放的内容对象。

[0040] - 内容加密密钥

[0041] 内容加密密钥可具有预定格式的二进制值。例如，可在通过对内容对象进行解密来获得原始内容的过程中使用内容加密密钥。

[0042] - 允许信息

[0043] 允许信息指示内容对象的重放和再现类型。

[0044] 重放的示例包括“播放”、“显示”、“执行”和“打印”。播放分量指示以音频 / 视频格式来表达内容的权利。另外，显示分量指示通过可视装置显示内容对象的权利，打印分量指示产生内容对象的硬拷贝的权利。例如，在内容对象是运动画面或音乐的情况下，显示分量和打印分量中的至少一种可被设置为将被用于播放内容对象的权利对象的允许信息。执行分量指示执行诸如游戏和其它应用程序的内容对象的权利。例如，在内容对象是 JAVA 游戏的情况下，执行分量可被设置为将被用于玩 JAVA 游戏的权利对象的允许信息。

[0045] 同时，复制的示例包括拷贝分量和移动分量。拷贝分量和移动分量是将权利对象从一个装置移动到另一装置并存储该权利对象的权利。移动分量在当前装置中去激活原始权利对象，而拷贝分量在当前装置中不对原始权利对象去激活。这里，去激活可表示权利对象的删除。

[0046] - 限制信息

[0047] 限制信息是指对允许权利对象 (RO) 被重放的限制，并且可设置一条或多条限制信息。限制信息示例可包括计数限制、日期时间限制、间隔限制、累计限制等。

[0048] 这里，计数限制规定授权给内容对象的允许的计数。当计数限制被设置为 10 时，允许主机装置播放内容对象 10 次，直到权利对象的计数限制被耗尽。

[0049] 日期时间限制规定允许的持续时间，并选择性地包含开始元素或结束元素。当消耗具有设置的日期时间限制的权利对象时，主机装置可在日期时间限制的开始项规定的时间 / 日期之后和之前播放内容对象。例如，当开始项被设置为 00:00:00（小时：分：秒）2005-12-01（年 - 月日）时，主机装置不能在 00:00:00 2005-12-01 之前访问并消耗 RO 以播放内容对象。

[0050] 间隔限制规定 RO 可被执行以用于相应的内容对象的时间间隔。当开始元素包含在间隔限制中时，在规定的时间 / 日期之后，在由包含在间隔限制中的持续时间元素规

定的时间段期间允许使用内容对象。例如，对于一周的间隔限制，当主机装置在 00:00:00 2005-12-01 时以及在 00:00:00 2005-12-01 之后消耗 RO 以播放内容对象时，允许消耗 RO 来播放内容对象，直到 00:00:002005-12-08。

[0051] 累计限制规定累计测量的执行权利对象以用于相应的内容对象的时间段的最大时间间隔。当权利对象具有被设置为 10 的累计限制时，主机装置可具有播放内容对象 10 小时的权利对象。在这个示例中，主机装置不受计数或日期时间的限制。

[0052] - 状态信息

[0053] 在限制信息允许的范围内可消耗权利对象。状态信息基于限制信息条件指示权利对象 (RO) 是否可用。每个 RO 的状态信息包括有效状态、无效状态和未识别状态，在有效状态下，RO 可用，在无效状态下，RO 不可用，在未识别状态下，RO 的可用性不能被识别。这里，当 RO 的可用性可能随时间变化时，设置未识别状态。例如，当规定日期时间或间隔时，仅通过限制信息不能得知 RO 的可用性。即，在识别状态信息时，可能另外需要时间信息。在这种情况下，具有日期时间或间隔的每个 RO 的状态信息可被设置为未识别状态。

[0054] - 元信息

[0055] 元信息是指权利对象的预定元数据，并且包括允许信息、限制信息和状态信息中的至少一种。

[0056] - 公共密钥密码术

[0057] 公共密钥密码术也称为非对称密码术，这是因为当在解密数据中使用的密钥和在加密数据中使用的密钥组成不同的加密密钥时进行加密。在公共密钥密码术中，加密密钥包括一对公共密钥和私有密钥。公共密钥不需要被保密，即，公众可容易地访问公共密钥，而私有密钥必须仅由特定装置才能得知。公共密钥加密算法已经对一般公众公开，但是第三人不能得知或很难得知具有加密算法、加密密钥和密码文本的原始内容。公共密钥加密算法的示例诸如 Diffie-Hellman、RSA、El Gamal、Elliptic Curve 等。

[0058] - 对称密钥密码术

[0059] 对称密钥密码术也称秘密密钥密码术，其中，当用于加密数据的密钥和用于解密数据的密钥组成相同的加密密钥时进行加密。尽管作为对称密钥密码术的示例的数据加密标准 (DES) 最为常用，但是最近已经增加了采用先进加密标准 (AES) 的应用。

[0060] - 随机数

[0061] 随机数是具有随机性质的数字或字符的序列。由于产生完全的随机数成本很大，所以可使用伪随机数。

[0062] - 模块

[0063] 模块指的是，但不限于执行特定任务的软件或硬件组件，诸如现场可编程门阵列 (FPGA) 或专用集成电路 (ASIC)。模块可有利地被配置为驻留在可寻址存储介质上，并且被配置为在一个或多个处理器上执行。因此，模块可包括，例如，诸如软件组件、面向对象的软件组件、类组件和任务组件的组件、进程、函数、属性、过程、子程序、程序代码段、驱动程序、固件、微代码、电路、数据、数据库、数据结构、表、数组和变量。设置在这些组件和模块中的功能性可被组合为更少的组件和模块，或者还可被分离为另外的组件和模块。此外，这些组件和模块可被实现为在通信系统的一个或多个 CPU 上执行。

[0064] 当需要时，下面将描述上面具体定义的术语。

[0065] 图 2 是根据本发明示例性实施例的数字权利管理 (DRM) 装置 100 的框图。DRM 装置 100 包括存储模块 110、检测模块 120、完整性检验模块 130、状态信息更新模块 140、加密 / 解密模块 150 和控制模块 160。

[0066] 存储模块 110 包括诸如闪速存储器的存储介质，并且被划分为安全存储区和普通存储区。在安全存储区中存储需要被保护而不被外部装置（未示出）或外部模块（未示出）访问的安全数据，诸如 RO、用于 RO 的元信息的散列值和预定的加密密钥。在普通存储区中存储非安全数据，诸如开放的免费访问的内容对象。

[0067] 存储在存储模块 110 中的每个 RO 可包括元信息。元信息可包括在每个 RO 的固定字段中。例如，可规定元信息被写入与第 a 至第 n 比特相应的字段中。在这种情况下，不考虑 RO 的类型，可从 RO 的固定字段获得每个 RO 的元信息。

[0068] 检测模块 120 根据来自 RO 的请求，检测存储在存储模块 110 中的每个 RO 的元信息。可从外部装置或外部模块施加来自 RO 的请求。

[0069] 完整性检验模块 130 保持元信息的完整性。也就是说，完整性检验模块 130 可通过检验元信息的完整性（例如，外部装置或外部模块对元信息的访问），来防止元信息被改变。例如，完整性检验模块 130 使用预定的散列函数计算外部装置或外部模块访问的元信息的散列值，并将计算出的散列值与存储在存储模块 110 中的散列值进行比较。如果这两个散列值相同，则确定元信息的完整性被保持。这里，存储在存储模块 110 中的散列值可以是当每个 RO 被存储在存储模块 110 中时对该 RO 的元信息计算的散列值。因此，元信息可对外部装置或外部模块开放，但是不能被改变。

[0070] 另外，当包含在任意元信息中的状态信息被状态信息更新模块 140 改变时，完整性检验模块 130 计算具有改变的状态信息的元信息的散列值，并且将计算出的散列值存储在存储模块 110 中。因此，用新计算出的散列值来更新存储在存储模块 110 中的散列值。

[0071] 当包含在由检测模块 120 检测的元信息中的状态信息被设置为未识别状态时，状态信息更新模块 140 将检测元信息时的时间信息与包括在元信息中的限制信息进行比较，由此确定 RO 是否可用。例如，当间隔限制的结束元素被设置为 00:00:002005-11-01，并且元信息检测时间的时间信息指定 00:00:00 2005-11-01 时，RO 被确定为处于不可用状态。可从外部装置或外部模块获得元信息检测时间的时间信息。

[0072] 根据确定结果，如果 RO 被确定为可用，则状态信息更新模块 140 将包括在元信息中的状态信息保持为处于未识别状态。但是，如果 RO 被保持为处于不可用状态，则状态信息更新模块 140 将包括在元信息中的状态信息改变为无效状态。

[0073] 另外，当有效的 RO 被用完并且没有 RO 可用时，状态信息更新模块 140 将包括在元信息中的状态信息改变为无效状态。

[0074] 加密 / 解密模块 150 对预定的数据执行加密和解密。即，当控制模块 160 请求时，加密 / 解密模块 150 对将被发送到外部装置或外部模块的数据进行加密，或者对从外部装置或外部模块接收的数据进行解密。加密 / 解密模块 150 可执行公共密钥加密或私有密钥加密。可存在用于执行这两种加密类型的一个或多个加密 / 解密模块。

[0075] 或者，加密 / 解密模块 150 可产生在与外部装置或外部模块的认证期间所需的预定随机数。同时，存储在存储模块 110 中的每个 RO 可具有除了元信息以外的部分，所述部分被加密 / 解密模块 150 使用包括在 DRM 装置 100 中的独有加密密钥加密。在示例性的实

施例中，RO 的加密部分可以是内容加密密钥。因此，在 RO 应该被提供给外部装置或外部模块的情况下，加密 / 解密模块 150 对 RO 的加密部分进行解密，然后按照认证的外部装置或外部模块能够对 RO 解密的方式对 RO 进行加密。

[0076] 控制模块 160 控制组成 DRM 装置 100 的各个模块 110 至 150 的操作。因此，控制模块 160 用作控制 DRM 装置 100 的整个 DRM 过程的 DRM 代理。另外，控制模块 160 可控制与外部装置或外部模块相关的认证。

[0077] 同时，控制模块 160 将检测模块 120 检测的元信息提供给外部装置或外部模块。在本发明中，“提供元信息”不仅表示“将元信息主动发送到请求元信息的外部装置或外部模块”，而且表示“授权外部装置或外部模块访问元信息”。

[0078] 现在将参照图 3 来描述 DRM 装置 100 的操作过程。

[0079] 图 3 是示出根据本发明示例性实施例的数字权利管理方法的流程图。

[0080] 当在操作 S410 从外部装置或外部模块输入 RO 检测请求时，检测模块 120 在操作 S415 检测存储于存储模块 110 中的 RO 中存储的元信息。

[0081] 在操作 S420，如果元信息包含状态信息，则状态信息更新模块 140 确定状态信息是否被设置为无效状态。

[0082] 其结果是，如果在操作 S420 确定状态信息不处于无效状态，即，处于有效状态，则在操作 S450，控制模块 160 将检测的状态信息提供给外部装置或外部模块。

[0083] 如果在操作 S420 确定状态信息处于无效状态，则在操作 S425，状态信息更新模块 140 将检测元信息时的时间信息与包括在元信息中的限制信息进行比较，并确定包括元信息的 RO 的可用性。

[0084] 如果在操作 S425 确定 RO 可用，则在操作 S445，状态信息更新模块 140 将状态信息保持在未识别状态。在操作 S450，控制模块 160 将元信息提供给外部装置或外部模块。

[0085] 另一方面，如果在操作 S425 确定 RO 不可用，则在操作 S430，状态信息更新模块 140 将状态信息改变为无效状态。这里，在操作 S435，完整性检验模块 130 使用预定的散列函数计算具有改变的状态信息的元信息的散列值。然后在操作 S440，完整性检验模块 130 将计算出的散列值存储在存储模块 110 中。也就是说，在操作 S440，完整性检验模块 130 用对每个 RO 的元信息计算的散列值来更新存储在存储模块 110 中的散列值。之后，控制模块 160 将包括改变的状态信息的元信息提供给外部装置或外部模块。

[0086] 如果在操作 S455 确定有 RO 留在存储模块 110 中，则该过程返回到操作 S415，从而检测模块 120 检测留在存储模块 110 中的 RO 的元信息。

[0087] 上述过程可被重复，直到存储在存储模块 110 中的所有 RO 的元信息被完全检测。

[0088] 在图 3 所示的过程期间，完整性检验模块 130 防止元信息被外部装置或外部模块改变，如图 4 所示。

[0089] 在操作 S510，控制模块 160 提供元信息。当在操作 S520 外部装置或外部模块访问该元信息时，完整性检验模块 130 在操作 S530 保持外部装置或外部模块访问的元信息的完整性。例如，完整性检验模块 130 使用预定的散列函数计算外部装置或外部模块访问的元信息的散列值，并且使计算出的散列值与存储在存储模块 110 中的散列值相等，由此防止未经授权而改变元信息。

[0090] 已经参照图 2 至图 4 描述的 DRM 装置 100 可由多种类型的装置来实现。例如，DRM

装置 100 可以是图 5 所示的主机装置。

[0091] 图 5 是根据本发明示例性实施例的主机装置 200 的框图。

[0092] 主机装置 200 包括 DRM 装置 100。也就是说，主机装置 200 的存储模块 210、检测模块 220、完整性检验模块 230、状态信息更新模块 240、加密 / 解密模块 250 和控制模块 260 分别执行与 DRM 装置 100 的存储模块 110、检测模块 120、完整性检验模块 130、状态信息更新模块 140、加密 / 解密模块 150 和控制模块 160 相同的功能，将省略对其重复的描述。

[0093] 主机装置 200 还包括用户输入模块 215、装置接口模块 225、重放模块 235、显示模块 245 和时间管理模块 255。

[0094] 用户输入模块 215 从用户接收预定的命令或请求。为此，用户输入模块 215 可包括诸如键盘、触摸板或触摸屏的输入装置。因此，用户可通过用户输入模块 215 的输入提出检测存储在存储模块 210 中的 RO 的请求。当输入检测 RO 的请求时，可执行图 3 和图 4 中所示的过程。

[0095] 装置接口模块 225 将数据发送到外部装置（例如，便携式存储装置）/ 从外部装置接收数据。因此，主机装置 200 可通过装置接口模块 225 与外部装置连接。

[0096] 重放模块 235 使用 RO 再现内容对象。例如，重放模块 235 可以是能够再现运动画面的 MPEG 解码模块。

[0097] 显示模块 245 显示重放模块 235 再现的内容对象或控制模块 260 提供的元信息，从而用户能够在视觉上观看（例如，通过播放或执行内容等）使用的内容。可用诸如 PDP、LCD 或有机 EL 的液晶显示面板来构造显示模块 245。

[0098] 时间管理模块 255 管理当前时间信息。

[0099] 从参照图 3 和图 4 的描述中可理解具有上述结构的主机装置 200 检测存储在其的 RO 的检测过程。

[0100] 如以上参照图 3 所述，特别在操作 S425 中，可由时间管理模块 255 提供确定未识别的 RO 的可用性所需的时间信息。可通过显示模块 245 显示在图 3 所示的操作 S450 提供的元信息。

[0101] 在另一示例性的实施例中，用户可将 RO 存储在便携式存储装置中，而不是存储在主机装置 200 中，或者可通过使用主机装置 200 来消耗或检测储在便携式存储装置中的 RO。这里，可由便携式存储装置来实现已经参照图 2 描述的 DRM 装置 100。首先将参照图 6 来描述使用便携式存储装置的 DRM 系统，然后将参照图 7 来描述便携式存储装置的结构。

[0102] 图 6 是根据本发明示例性实施例的 DRM 系统的框图。DRM 系统包括主机装置 200 和便携式存储装置 300。

[0103] 与传统技术相同，用户可从内容提供商 20 获得内容对象，或者可向 RO 发布者 30 付费以购买用于加密的内容的 RO。购买的 RO 可被存储在主机装置 200 中或被传送（移动或拷贝）到便携式存储装置 300。另外，便携式存储装置 300 可在其生产时存储一个或多个 RO。

[0104] 在便携式存储装置 300 存储 RO 的情况下，在主机装置 200 与便携式存储装置 300 连接之后，主机装置 200 消耗存储在便携式存储装置 300 中的 RO 以播放内容对象。在这种情况下，主机装置 200 可具有与参照图 5 所描述的相同的结构并执行与参照图 5 所描述的相同的功能。

[0105] 图 7 是根据本发明示例性实施例的便携式存储装置 300 的框图。

[0106] 便携式存储装置 300 包括 DRM 装置 100。也就是说，便携式存储装置 300 的存储模块 310、检测模块 320、完整性检验模块 330、状态信息更新模块 340、加密 / 解密模块 350 和控制模块 360 分别执行与 DRM 装置 100 的存储模块 110、检测模块 120、完整性检验模块 130、状态信息更新模块 140、加密 / 解密模块 150 和控制模块 160 相同的功能，将省略对其重复的描述。便携式存储装置 300 还包括装置接口模块 370。

[0107] 装置接口模块 370 将数据发送到外部装置 (例如，主机装置 200) / 从外部装置接收数据。因此，便携式存储装置 300 可通过装置接口模块 370 与外部装置连接。

[0108] 当主机装置 200 与便携式存储装置 300 连接以检测存储在便携式存储装置 300 中的 RO 时，可对主机装置 200 和便携式存储装置 300 执行认证。认证是一种基础过程，在该过程中，主机装置和便携式存储装置验证彼此的真实性，由此保持在它们之间交换的数据的安全性，这将参照图 8 来进行描述。

[0109] 图 8 是示出根据本发明示例性实施例的认证过程的流程图。

[0110] 在该示例性的实施例中，数据的下标“H”表示数据被主机装置 200 处理或产生，数据的下标“S”表示数据被便携式存储装置 300 处理或产生。

[0111] 在操作 S610，主机装置 200 将认证请求发送到便携式存储装置 300。当请求认证时，主机装置 200 可将证书 $_H$ 发送到便携式存储装置 300，所述证书 $_H$ 由证书授权者发布给主机装置 200。证书 $_H$ 被证书授权者签有数字签名，并且包含装置 ID_H 和公共密钥 $_H$。另外，在本发明中，当主机装置 200 与便携式存储装置 300 连接时，主机装置 200 和便携式存储装置 300 通过各种有线介质彼此电连接。但是，这仅仅是示例，“连接”还可表示两个装置可在非接触的状态下通过无线介质彼此通信。

[0112] 在操作 S612，便携式存储装置 300 使用证书撤销列表 (CRL) 来验证主机装置 200 的证书 $_H$ 是否有效。如果证书 $_H$ 被登记在 CRL 中，则便携式存储装置 300 可拒绝与主机装置 200 的认证。如果证书 $_H$ 没有被登记在 CRL 中，则便携式存储装置 300 使用主机装置 200 的证书 $_H$ 获得公共密钥 $_H$。

[0113] 如果确定主机装置 200 被验证为认证的装置，也就是说，主机装置 200 的证书 $_H$ 有效，则在操作 S614，便携式存储装置 300 产生随机数 $_S$。在操作 S616，使用公共密钥 $_H$ 来加密产生的随机数 $_S$。

[0114] 在操作 S620，便携式存储装置 300 执行认证响应过程。在认证过程期间，便携式存储装置 300 发送证书 $_S$ 和加密的随机数 $_S$，所述证书 $_S$ 由证书授权者发布给便携式存储装置 300。证书 $_S$ 被证书授权者签有数字签名，并且包含便携式存储装置 300 的 ID_H 和公共密钥 $_H$。

[0115] 在操作 S622，主机装置 200 接收证书 $_S$ 和加密的随机数 $_S$，通过验证证书 $_S$ 来对便携式存储装置 300 进行认证，并且使用它自己的私有密钥 $_H$ 来对加密的随机数 $_S$ 解密。这里，主机装置 200 使用便携式存储装置 300 的证书 $_S$ 来获得便携式存储装置 300 的公共密钥 $_S$。另外，还可使用 CRL 对便携式存储装置 300 执行证书 $_S$ 的验证。

[0116] 如果使用便携式存储装置 300 的证书 $_S$ 将便携式存储装置 300 验证为认证的装置，则在操作 S624，主机装置 200 产生随机数 $_H$。在操作 S626，使用便携式存储装置 300 的公共密钥 $_S$ 来加密产生的随机数 $_H$。

[0117] 之后，在操作 S630，主机装置 200 向便携式存储装置 300 请求认证结束过程。当请求认证结束过程时，主机装置 200 将加密的随机数 $_{H}$ 发送到便携式存储装置 300。

[0118] 在操作 S632，便携式存储装置 300 接收加密的随机数 $_{H}$，并使用它的私有密钥 $_{S}$ 对随机数 $_{H}$ 解密。

[0119] 因此，主机装置 200 和便携式存储装置 300 共享彼此的随机数，即，随机数 $_{H}$ 和随机数 $_{S}$。

[0120] 其结果是，在操作 S640 和 S642，共享彼此的随机数的主机装置 200 和便携式存储装置 300 产生会话密钥。这里，为了使主机装置 200 和便携式存储装置 300 产生它们的会话密钥，可使用相同的算法。因此，主机装置 200 和便携式存储装置 300 共享相同的会话密钥。

[0121] 在完成认证之后，使用主机装置 200 和便携式存储装置 300 的会话密钥对将在主机装置 200 和便携式存储装置 300 之间传输的数据进行加密和解密还可提供数据传输中的确保的安全性。在下面描述的一些示例性的实施例中，除非另外标注，应该理解，主机装置 200 和便携式存储装置 300 使用通过认证产生的每个会话密钥来对彼此传输的数据进行加密和解密。

[0122] 在完成认证过程之后，主机装置 200 可将 RO 移动或拷贝到便携式存储装置 300，或者可消耗存储在便携式存储装置 300 中的 RO 以播放内容对象。

[0123] 在示例性的实施例中，主机装置 200 可发送检测存储在便携式存储装置 300 中的 RO 的请求，这将参照图 9 来描述。

[0124] 图 9 是示出根据本发明示例性实施例的主机装置 200 检测存储在便携式存储装置 300 中的权利对象的检测过程的流程图。

[0125] 当在操作 S710 主机装置 200 的用户输入模块 215 从用户接收到 RO 检测请求时，控制模块 260 通过装置接口模块 225 请求便携式存储装置 300 检测 RO。这里，在操作 S720，控制模块 260 产生 RO 检测请求消息，装置接口模块 225 将产生的 RO 检测请求消息发送到便携式存储装置 300。

[0126] 如果便携式存储装置 300 的装置接口模块 370 从主机装置 200 接收到 RO 检测请求消息，则在操作 S730，检测模块 320 检测存储在便携式存储装置 300 中的 RO 的元信息。

[0127] 在操作 S740，控制模块 360 通过装置接口模块 370 将检测的元信息发送到主机装置 200。这里，在将元信息提供给主机装置 200 之前，便携式存储装置 300 可执行图 3 所示的步骤 S420 至 S445。在这种情况下，可从主机装置 200 获得执行步骤 S425 所需的时间信息。

[0128] 同时，“将检测的元信息提供给主机装置 200”不仅表示“便携式存储装置 300 通过装置接口模块 370 将元信息主动发送到主机装置 200”，而且表示“授权主机装置 200 访问元信息”。

[0129] 如果主机装置 200 的装置接口模块 225 从便携式存储装置 300 获得元信息，则在步骤 S750，显示模块 245 显示所述元信息。

[0130] 这里，如果用户试图通过用户输入模块 215 改变存储在便携式存储装置 300 中的 RO 的元信息，则通过由便携式存储装置 300 的完整性检验模块 330 执行的完整性检验操作可拒绝对元信息的改变。

[0131] 产业上的可利用性

[0132] 如上所述，根据本发明示例性实施例的 DRM 装置和方法可有效检测权利对象的信息。

[0133] 虽然已经参照本发明的示例性实施例具体显示和描述了本发明，但是本领域普通技术人员应该理解，在不脱离由权利要求限定的本发明的精神和范围的情况下，可以对其进行形式和细节的各种改变。因此，应该理解，提供上述示例性的实施例仅仅是为了描述性的意义，而不应被解释为对本发明的范围的任何限制。

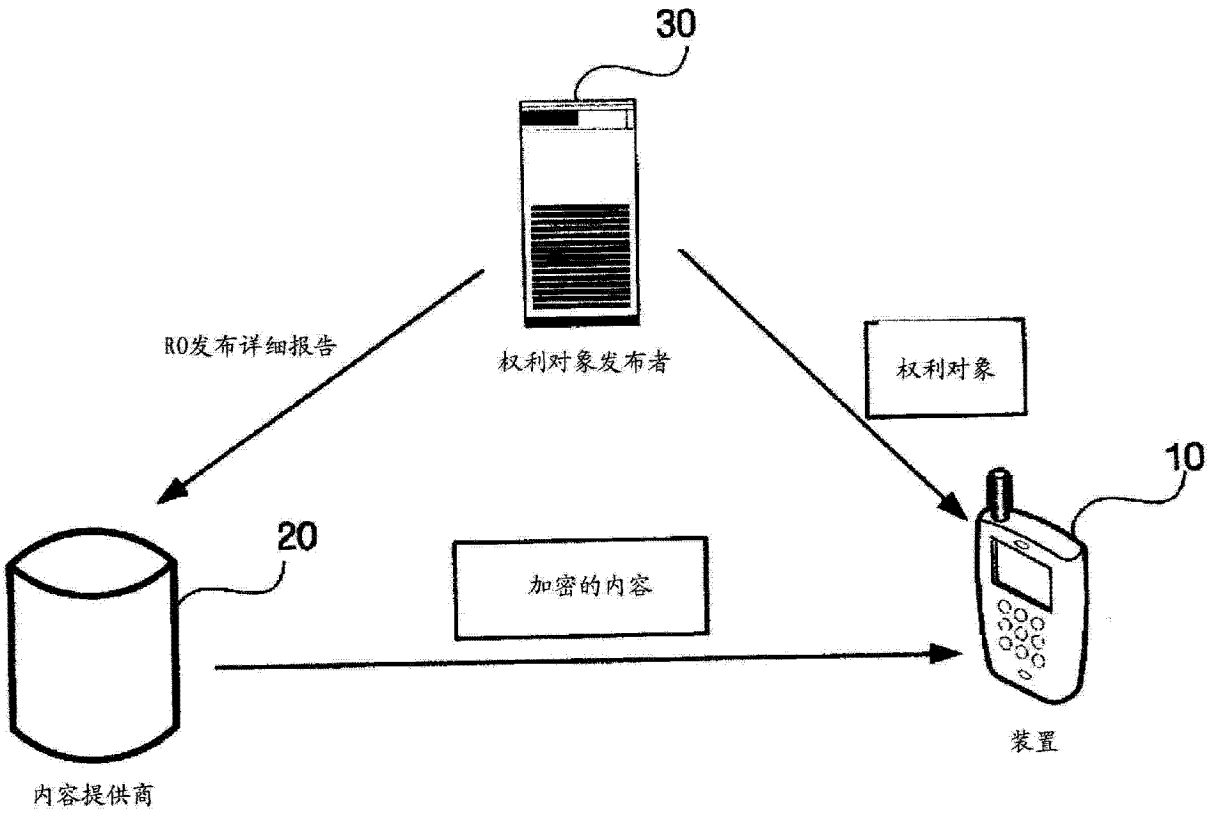


图 1

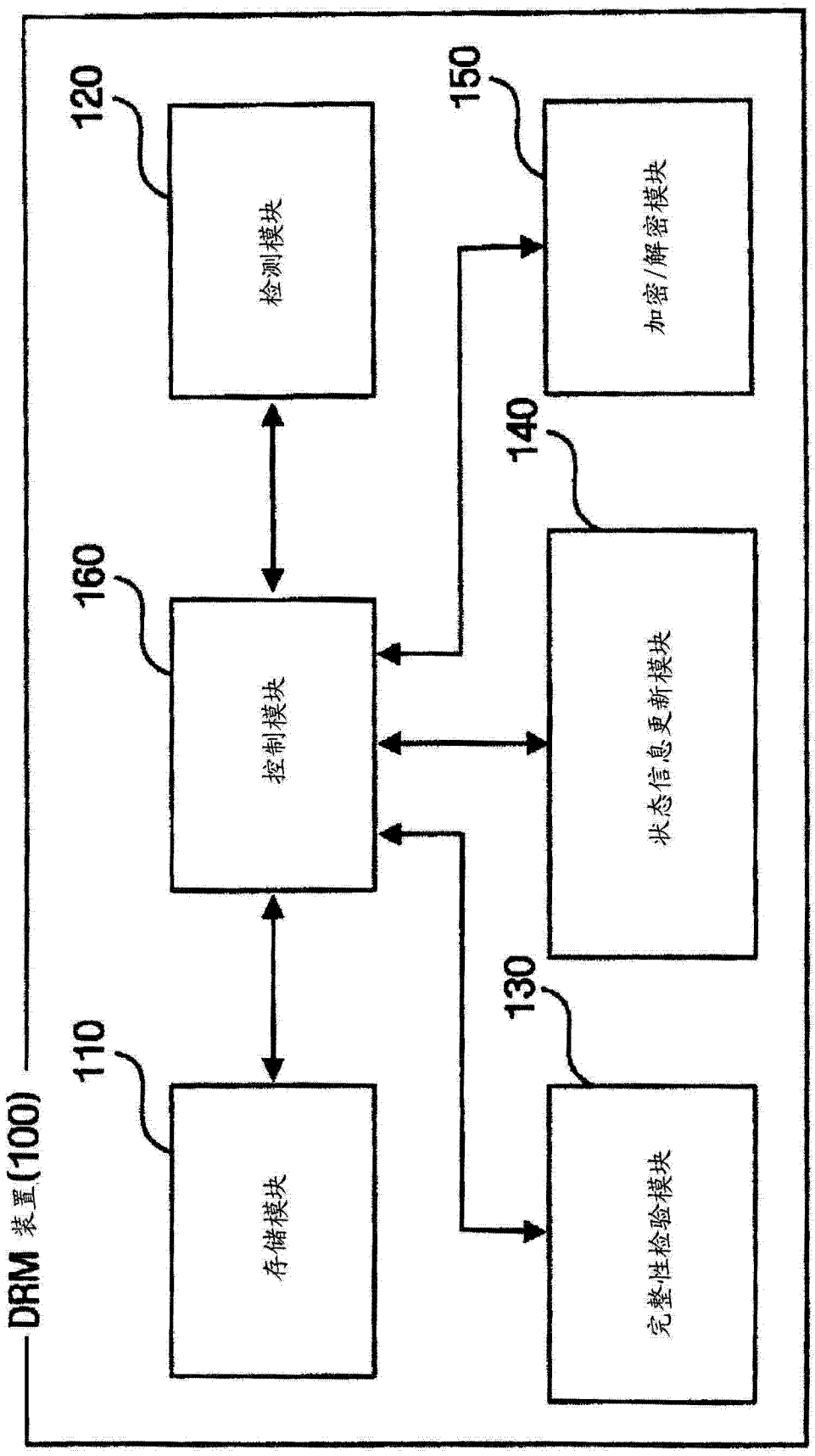

DRM 装置(100)
120
检测模块
150
加密/解密模块
140
160
控制模块
状态信息更新模块
130
110
存储模块
完整性检验模块

图 2

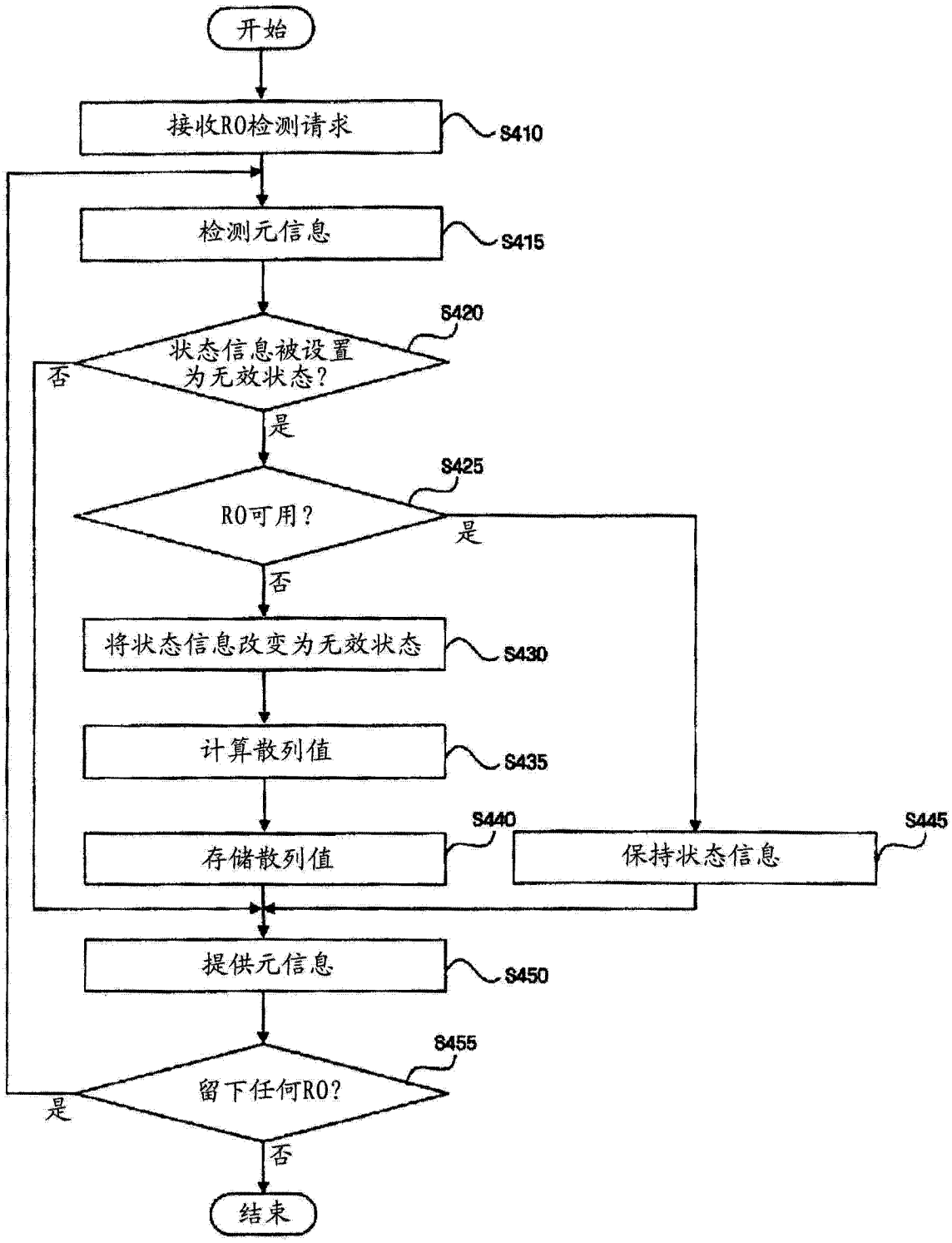

开始
接收RO检测请求
S410
检测元信息
S415
S420
状态信息被设置为无效状态?
否
是
S425
RO可用?
是
否
将状态信息改变为无效状态
S430
计算散列值
S435
S440
存储散列值
S445
保持状态信息
提供元信息
S450
S455
留下任何RO?
是
否
结束

图 3

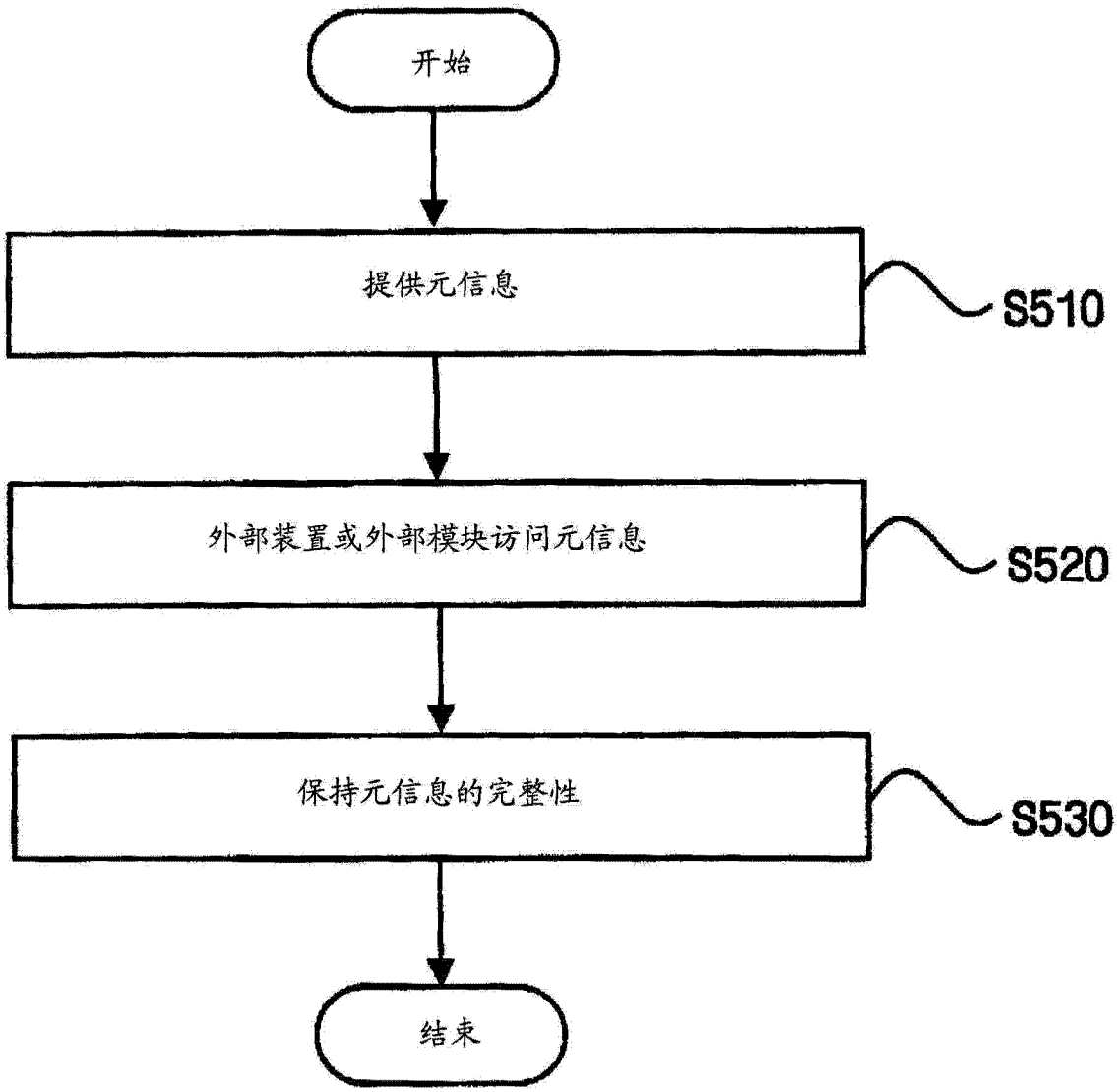


图 4

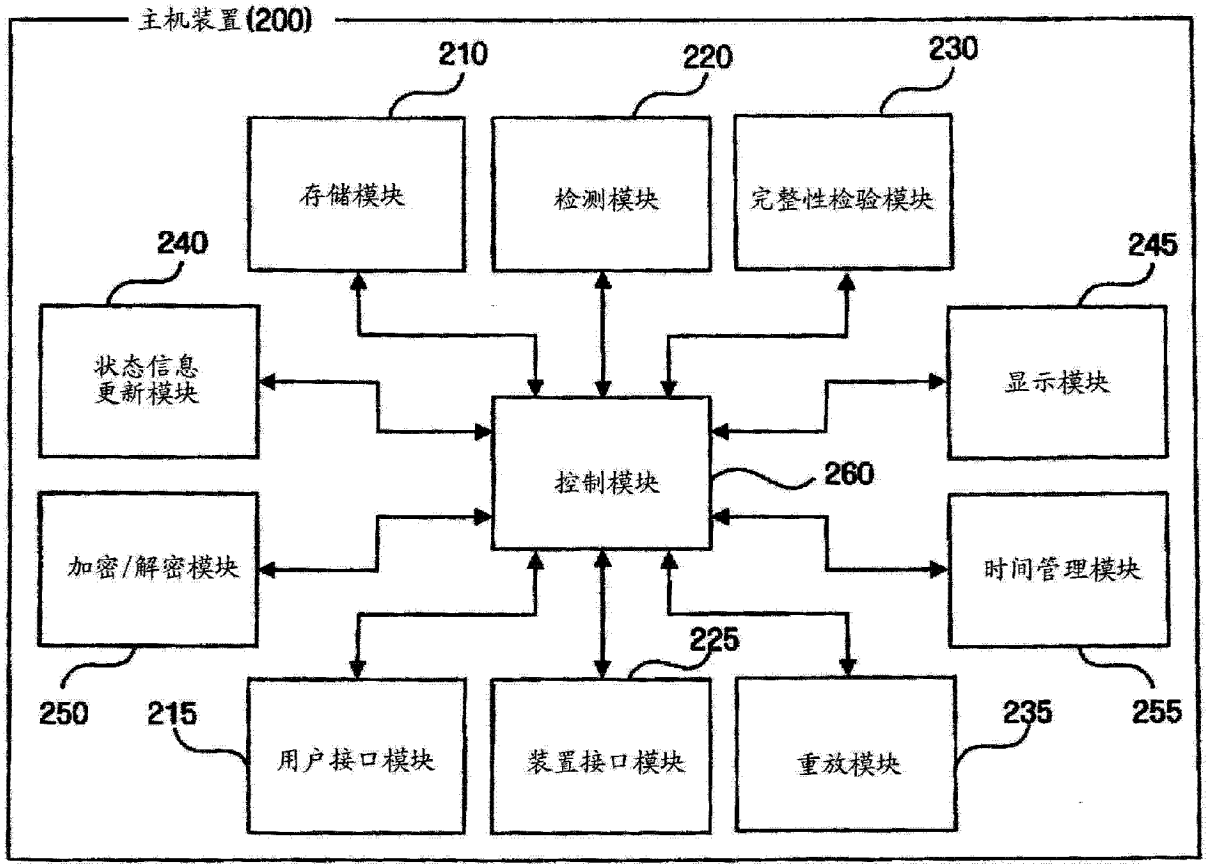

主机装置(200)
210
220
230
存储模块
检测模块
完整性检验模块
240
245
状态信息更新模块
显示模块
控制模块
260
加密/解密模块
时间管理模块
225
250
215
235
255
用户接口模块
装置接口模块
重放模块

图 5

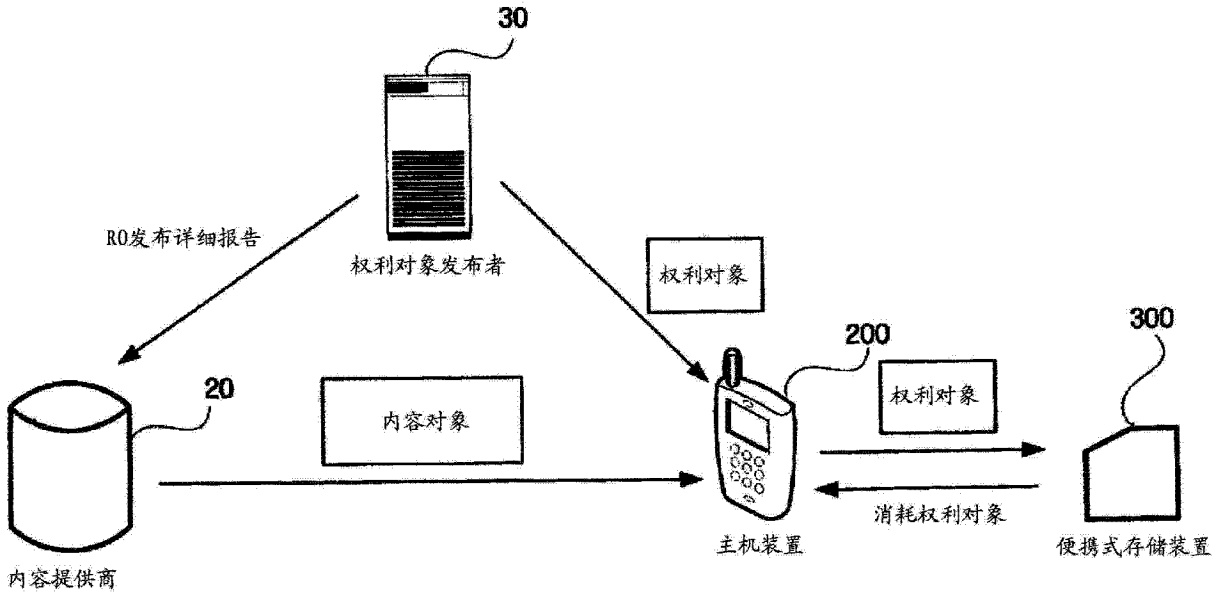

30
RO发布详细报告
权利对象发布者
权利对象
200
300
20
内容对象
权利对象
消耗权利对象
内容提供商
主机装置
便携式存储装置

图 6

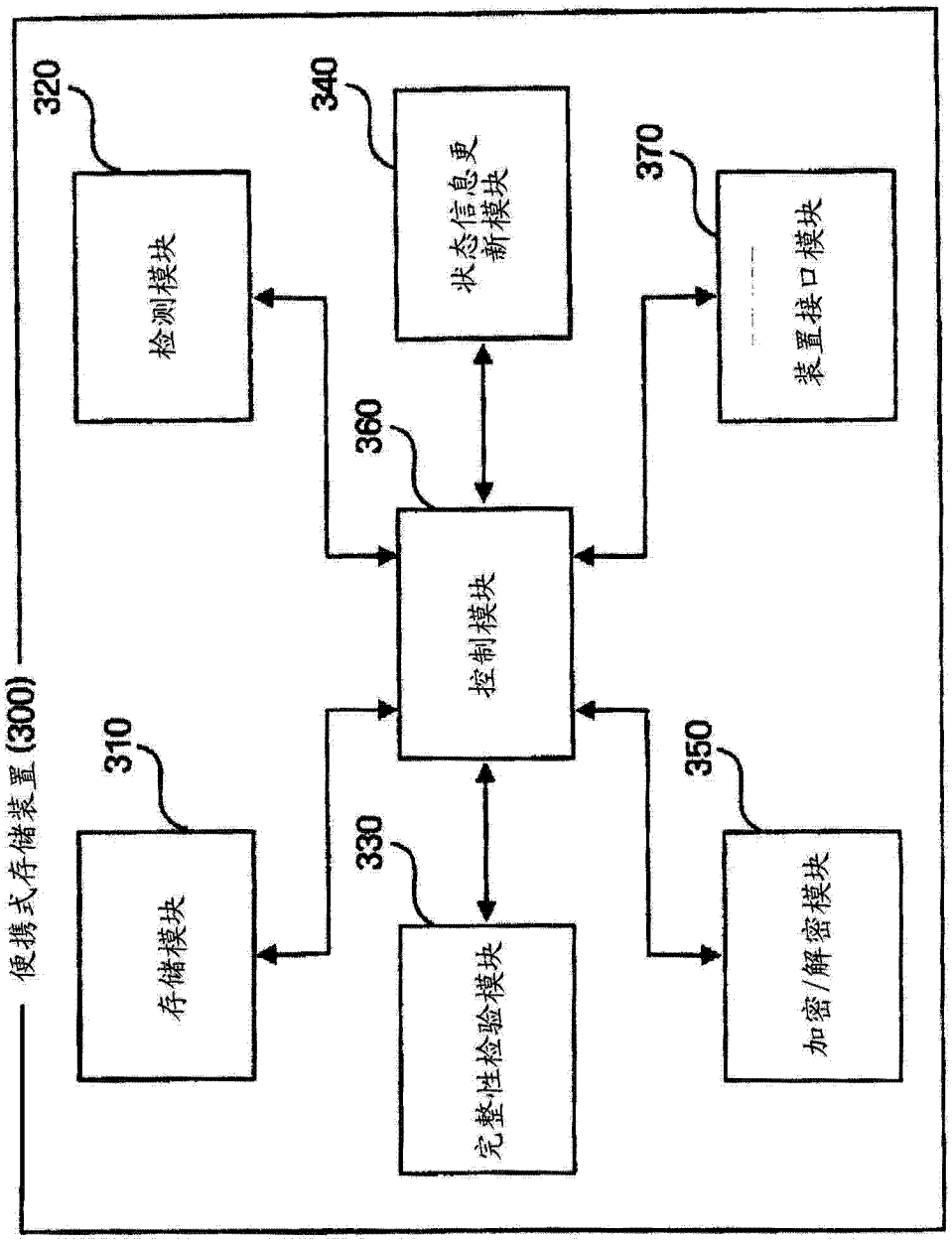

便携式存储装置 (300)
320
检测模块
340
状态信息更新模块
370
装置接口模块
360
控制模块
310
存储模块
330
完整性检验模块
350
加密/解密模块

图 7

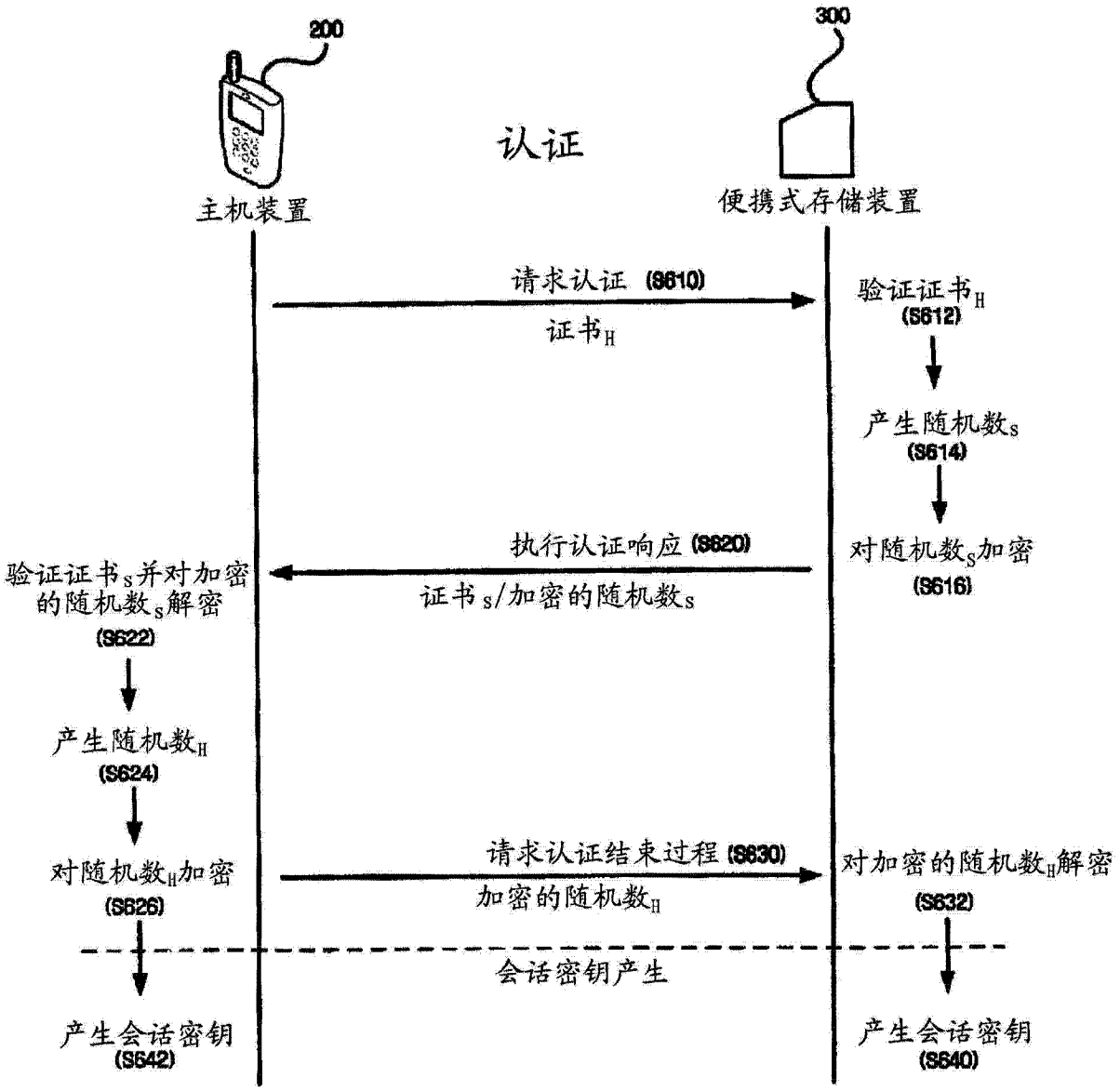

200
300
认证
主机装置
便携式存储装置
请求认证 (S610)
证书H
验证证书H
(S612)
产生随机数S
(S614)
执行认证响应 (S620)
证书S/加密的随机数S
对随机数S加密
(S616)
验证证书S并对加密的随机数S解密
(S622)
产生随机数H
(S624)
对随机数H加密
(S626)
请求认证结束过程 (S630)
加密的随机数H
对加密的随机数H解密
(S632)
会话密钥产生
产生会话密钥
(S642)
产生会话密钥
(S640)

图 8

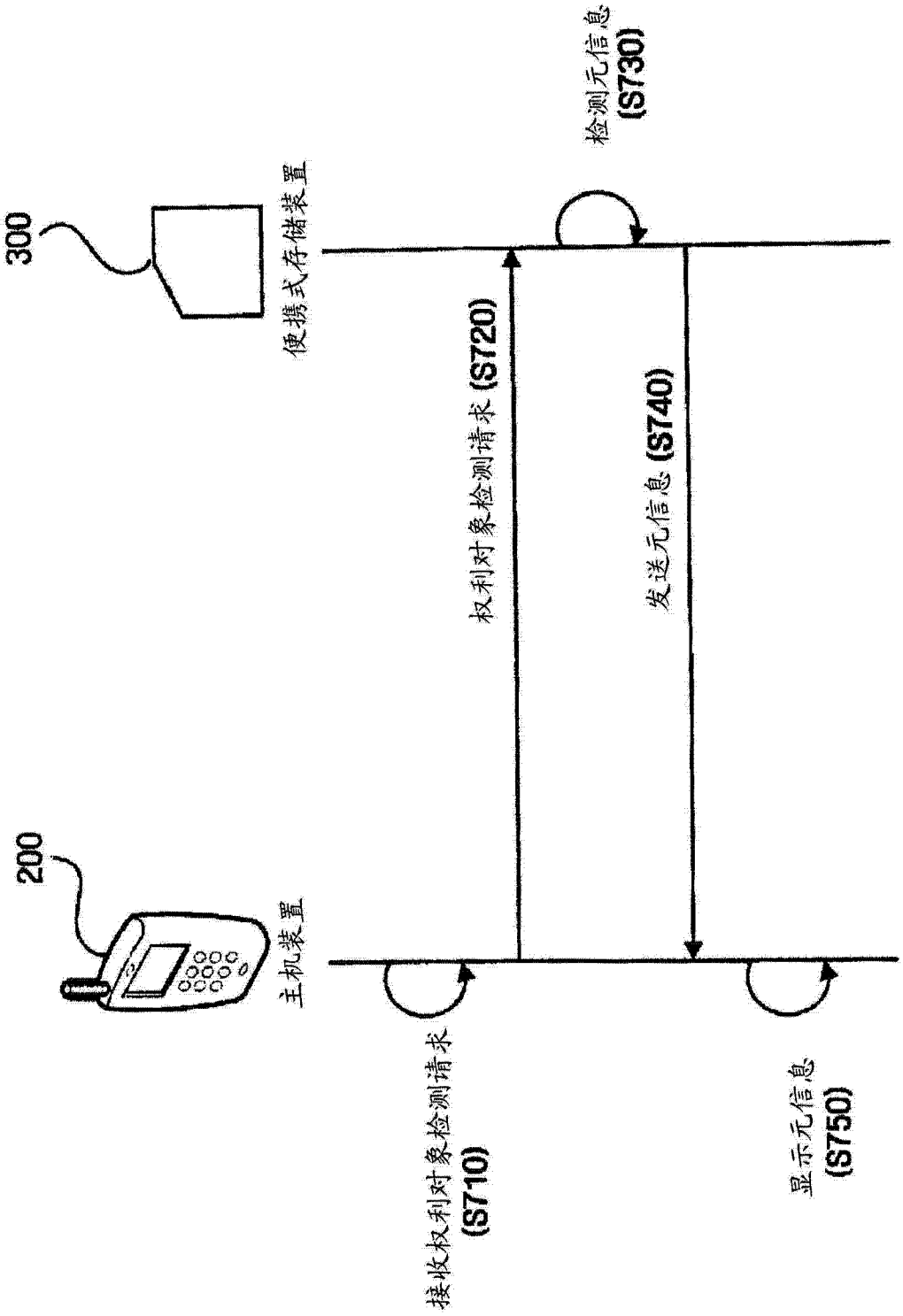

300
便携式存储装置
检测元信息
(S730)
权利对象检测请求 (S720)
发送元信息 (S740)
200
主机装置
接收权利对象检测请求
(S710)
显示元信息
(S750)

图 9