(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 102708314 B
(45)授权公告日 2016.07.06

(21)申请号 201210063003.0
(22)申请日 2007.10.19
(30)优先权数据
10-2007-0020390 2007.02.28 KR
60/852,992 2006.10.20 US
(62)分案原申请数据
200780038543.0 2007.10.19
(73)专利权人 三星电子株式会社
地址 韩国京畿道
(72)发明人 李南杰 金亨灿 金奎百
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王波波
(51)Int.Cl.
G06F 21/10(2013.01)
H04L 29/06(2006.01)
H04L 9/08(2006.01)

(56)对比文件
US 2002/0138442 A1,2002.09.26,
CN 1802617 A,2006.07.12,
CN 1610914 A,2005.04.27,

审查员 姚杰

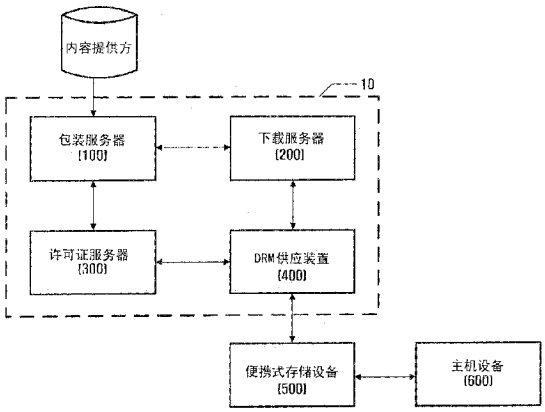
权利要求书1页 说明书8页 附图8页

(54)发明名称

数字权利管理供应装置,系统以及方法

(57)摘要

本发明提供了一种数字权利管理(DRM)供应技术,并且更具体地,提供了能够使用一个或者更多DRM系统轻松提供内容的装置、系统以及方法。DRM供应装置包括:内容下载单元,其从下载服务器下载加密的真实内容以及虚内容,并且其管理下载的真实内容以及虚内容;许可证管理单元,其管理许可证服务器发放的许可证;以及处理单元,其管理下载的真实内容和虚内容、以及发放的许可证。



CN 102708314 B

1.一种包装服务器,包括:

第一包装单元,在内容管理系统中注册内容,产生已注册的内容的数字权利管理DRM首部,产生第一加密密钥,以及使用所述DRM首部和所述第一加密密钥对所述已注册的内容加密;以及

第二包装单元,产生与已加密内容相对应的至少一个虚内容,产生第二加密密钥,并使用所述第二加密密钥对所述虚内容加密,

其中,所述至少一个虚内容是针对多个DRM中的每个DRM,为接收该DRM的许可证而需要的文件,以及所述加密内容的加密密钥(CEK_R)包括在所述虚内容的主体中。

2.根据权利要求1所述的包装服务器,其中,针对每个DRM,产生所述至少一个虚内容。

3.根据权利要求1所述的包装服务器,其中,将所述加密内容和所述至少一个虚内容下载到下载服务器,以及所述下载服务器向DRM供应装置提供针对用户请求的预定内容的加密内容和至少一个虚内容。

4.根据权利要求3所述的包装服务器,其中,所述DRM供应装置请求许可证服务器发放针对所述加密内容的许可证。

5.根据权利要求4所述的包装服务器,其中,所述DRM供应装置在便携式存储设备中存储所述加密内容、所述至少一个虚内容以及所述许可证。

6.一种包装方法,包括

第一包装步骤,在内容管理系统中注册内容,产生已注册的内容的数字权利管理DRM首部,产生第一加密密钥,以及使用所述DRM首部和所述第一加密密钥对所述已注册的内容加密;以及

第二包装步骤,产生与已加密内容相对应的至少一个虚内容,产生第二加密密钥,并使用所述第二加密密钥对所述虚内容加密,

其中,所述至少一个虚内容是针对多个DRM中的每个DRM,为接收该DRM的许可证而需要的文件,以及所述加密内容的加密密钥(CEK_R)包括在所述虚内容的主体中。

7.根据权利要求6所述的包装方法,其中,针对每个DRM,产生所述至少一个虚内容。

8.根据权利要求6所述的包装方法,其中,将所述加密内容和所述至少一个虚内容下载到下载服务器,以及所述下载服务器向DRM供应装置提供针对用户请求的预定内容的加密内容和至少一个虚内容。

9.根据权利要求8所述的包装方法,其中,通过所述DRM供应装置,在存储设备中存储所述加密内容以及所述至少一个虚内容。

数字权利管理供应装置，系统以及方法

[0001] 本申请是申请日为2007年10月19日、申请人为三星电子株式会社的发明专利申请200780038543.0“数字权利管理供应装置，系统以及方法”的分案申请。

技术领域

[0002] 本发明涉及到数字权利管理(DRM)供应技术，并且更具体地，涉及能够使用一个或者更多DRM系统容易地提供内容的装置、系统以及方法。

背景技术

[0003] 通常地，数字权利管理(DRM)技术保护并且管理数字内容创建者的权利。依照于DRM技术，内容供应服务器以加密的形式存储内容，并且当用户发出针对购买加密的内容的请求时，向用户提供加密内容以及用于对加密内容进行解密的密钥信息。DRM技术定义了数字内容能够被回放的次数、数字内容能否被复制、内容能够被复制的次数等。

[0004] DRM功能大致划分如下：数字内容的保护，数字内容的使用规则的管理，以及计费系统的管理。为了保护数字内容，DRM技术对数字内容加密，从而防止在其生命周期中的所有阶段中(即，创建，分发，使用，以及处置)对数字内容的非法分发或者使用。另外，DRM技术使得仅有具有加密密钥的被授权用户能够对加密的内容进行解密并且使用。因此，即使加密的内容被非法的分发了，在没有加密密钥的情况下也不能使用它。

发明内容

[0005] 技术问题

[0006] 尽管如此，多个开发商开发的DRM技术(例如微软(MS)DRM和开放式移动联盟(OMA)DRM)并不彼此兼容。即开发商开发的DRM结构在支持该开发商开发的该DRM结构的硬件或者软件上运行，而不能在其它平台上运行。因此，用户不得不购买支持每个DRM的不同的硬件或者软件。

[0007] 技术解决方案

[0008] 本发明的一方面是使用一种或者更多数字权利管理(DRM)系统来实现内容供应系统。

[0009] 尽管如此，本发明的方面并不受限于本文阐述的方面。通过参考下面给出的本发明的详细描述，本发明的上述和其它方面对于本发明相关领域的普通技术人员来说是显而易见的。

[0010] 根据本发明一方面，提供了一种DRM供应装置，包括：内容下载单元，其从下载服务器下载加密的真实内容、以及虚内容，并且管理下载的真实内容以及虚内容；许可证管理单元，其管理由许可证服务器发放的许可证；以及处理单元，其管理下载的真实内容和虚内容、以及发放的许可证。

[0011] 根据本发明的另一方面，提供了一种DRM供应系统，包括：包装服务器，其对未加密的真实内容执行第一包装处理以及第二包装处理，并且分别生成加密的真实内容、以及虚

内容；下载服务器，其下载加密的真实内容、以及虚内容；许可证服务器，其生成并且发放针对加密的真实内容的许可证；以及DRM供应装置，其接收并且管理加密的真实内容、虚内容、以及许可证。

[0012] 根据本发明的另一方面，提供了一种DRM供应方法，包括：接收加密的真实内容、以及虚内容；以及接收针对加密的真实内容而发放的许可证。

附图说明

[0013] 通过对本发明示例实施例的详细描述以及参照附图，本发明的上述以及其它特性和优点将变得更显而易见，其中：

[0014] 图1示出了根据本发明示例实施例的数字权利管理(DRM)供应系统；

[0015] 图2示出了根据本发明示例实施例的DRM供应系统的许可证绑定结构；

[0016] 图3示出了根据本发明示例实施例的DRM供应系统中包括的包装服务器的操作；

[0017] 图4示出了根据本发明示例实施例的DRM供应系统中的DRM首部(header)的结构；

[0018] 图5示出了根据本发明示例实施例的使用DRM供应系统下载内容的操作；

[0019] 图6示出了根据本发明示例实施例的使用DRM供应系统接收许可证的操作；

[0020] 图7示出了根据本发明示例实施例的DRM供应系统中包括的DRM供应装置；

[0021] 图8示出了根据本发明示例实施例的DRM供应系统中包括的便携式存储设备；

[0022] 图9示出了根据本发明示例实施例的DRM供应系统中包括的主机设备的操作；以及

[0023] 图10示出了根据本发明示例实施例的使用DRM供应系统中包括的信息亭(kiosk)接收DRM内容的操作。

具体实施方式

[0024] 现在将通过参照示出了本发明示例实施例的附图，更全面地描述本发明。尽管如此，本发明可以用多种不同形式体现并且不应当被认为受到本文阐述的示例实施例的限制；而是，提供这些示例实施例使得本公开内容变得全面以及完整，并且向本领域技术人员全面地传达本发明的概念。附图中相似的参照数字代表相似的元件，并且因此它们的描述将被省略。

[0025] 参照附图，在下文中详细描述本发明的示例实施例。

[0026] 图1示出了根据本发明示例实施例的数字权利管理(DRM)供应系统10。参见图1，DRM供应系统10包括包装服务器100、下载服务器200、许可证服务器300、以及DRM供应装置400。DRM供应系统10还可以包括：便携式存储设备500，其通过与DRM供应装置400进行通信，使用内容提供方注册的内容，并且存储内容以其许可证。便携式存储设备500通过连接至主机设备600，回放内容。

[0027] 内容提供方向内容管理系统(CMS)注册要提供的内容。CMS支持对产品(内容)注册、获取以及删除进行管理的功能和设置权利的功能。另外，内容提供方为了向希望使用内容的用户分发内容而注册内容的元信息，设置针对服务商务应用的使用权利，并决定内容的价格。

[0028] 包装服务器100对内容提供方在CMS中注册的真实内容执行第一包装处理以及第二包装处理，并且生成虚内容以及DRM包装文件。此处，包装表示用于保护内容的加密处理。

虚内容表示针对每个DRM(例如微软(MS)DRM以及开放式移动联盟(OMA)DRM)、接收许可证所需的文件。

[0029] 即,为了支持MSDRM以及OMA DRM,包装服务器100对内容包装。稍后参照图3,详细说明第一和第二包装处理。

[0030] 下载服务器200向DRM供应装置400提供(下载)用户请求的内容。在这种情况下,下载的内容是由包装服务器100加密的真实内容、以及虚内容。稍后参照图5,详细说明下载内容的操作。

[0031] 许可证服务器300发放(提供)用于使用加密的真实内容的许可证。此处,基于关于虚内容的信息发放许可证。稍后参照图6,详细说明接收许可证的操作。

[0032] DRM供应装置400向便携式存储设备500提供从下载服务器200以及许可证服务器300接收的内容(例如,加密的真实内容、以及虚内容)。DRM供应装置400可以是信息亭(kiosk)、个人计算机(PC)、便携式多媒体播放器(PMP)、机顶盒,或者移动电话。稍后参照图7,详细说明DRM供应装置400的操作。

[0033] 便携式存储设备500存储DRM供应装置400提供的加密的内容、虚内容以及许可证。便携式存储设备500包括非易失性存储器,例如闪存,其可以读取、写入以及擦除数据,并且能够对数据执行预定的计算。另外,便携式存储设备500可以容易地与主机设备600连接或者从其断开。便携式存储设备500的例子包括智能媒介、记忆棒、CompactFlash(CF)卡,极端数字(extreme Digtial,xD)卡,以及多媒体卡(MMC)。稍后参照图8,详细说明便携式存储设备500的操作。

[0034] 同时,加密的内容、虚内容以及许可证可以是已经存储在便携式存储设备500中了。

[0035] 例如,用户可以购买存储了加密的内容,虚内容以及许可证的便携式存储设备500,并且使用已经存储在便携式存储设备500中的加密的内容、虚内容以及许可证。即,用户可以购买存储了预定内容的便携式存储设备,并且可以在主机设备600一直使用该内容。

[0036] 主机设备600可以连接至便携式存储设备500,并且可以通过使用许可证以及权利对象,来回放内容对象。主机设备600可以是便携式内容回放设备,例如移动电话,个人数字助理(PDA)或者MP3播放器,或者固定的内容回放设备,例如,台式计算机或者数字电视(TV)。稍后参照图9,详细说明主机设备600的操作。

[0037] 图2示出了根据本发明示例实施例的DRM供应系统10的许可证绑定结构。DRM供应系统10使用与相关的DRM系统不同的结构,其中相关的DRM系统一对一地将加密的内容绑定至许可证。

[0038] 参见图2,相关的DRM系统针对每个DRM,绑定加密的内容与许可证文件。因此,对于1Gbyte的视频,需要n乘以1Gbyte容量的存储器。

[0039] 另一方面,根据本发明的DRM供应系统10针对每个DRM,提供加密的真实内容、以及加密的虚内容和许可证文件的大约5Kbytes的包。因此,与相关的DRM系统不一样,由DRM供应系统10提供的内容不需要较大存储空间。

[0040] 即,根据本发明的DRM供应系统10具有分级结构,从而可以同时运行在加载有MSDRM的手机以及加载有OMA DRM的另一手机上。

[0041] 当为了回放内容,相关的DRM系统搜索许可证时,DRM系统读取加密内容的、DRM手

机指定的许可证ID(LID)或者内容ID(CID),并且搜索针对相应许可证的许可证存储数据库(DB)或文件。

[0042] 尽管如此,为了同时支持MSDRM和OMA DRM,DRM供应系统10并不直接将加密的真实内容绑定至相应的许可证。取而代之地,DRM供应系统10包括在加密的真实内容和相应的许可证之间的虚内容。

[0043] 例如,如果主机设备600具有MSDRM,则DRM供应系统10从加密的真实内容读取虚内容的ID,并且然后搜索MSDRM保护的虚内容。

[0044] 然后,如果从虚内容中选择了使用MSDRM加密的文件,DRM供应系统10从相应的虚内容的首部中获取LID,并且从许可证存储DB或文件中获取许可证。虚内容具有用户可以回放或者收听的内容格式。尽管如此,虚内容仅作为媒介,通过它加密的真实内容以及许可证可以被绑定至多个版本的DRM系统。绑定至虚内容的许可证是对针对加密的真实内容的权利进行设置的文件。同时,上述相同的处理可应用于加载OMA DRM系统的手机以及其它DRM系统。

[0045] 图3示出了根据本发明示例实施例的DRM供应系统10中包括的包装服务器100的操作。

[0046] 包装服务器100通过对真实内容进行第一以及第二包装处理,以对真实内容加密,并且生成虚内容以及DRM包装文件。

[0047] 现在描述第一包装处理。第一包装处理包括注册真实内容的第一操作、生成DRM首部的第二操作、生成内容加密密钥(CEK)的第三操作、以及加密真实内容的第四操作。

[0048] 具体地,如果内容提供方向CMS注册真实内容,包装服务器100生成所注册的真实内容的DRM首部。DRM首部包括可以解释内容特点的多种形式的元数据,例如与加密的内容相关联的虚内容名称。另外,DRM首部中包含的信息使用注册至CMS的元数据DB的信息,并且虚内容文件名称是基于注册至CMS的统一资源标识符(URI)而自动生成。另外,虚内容文件名称由不超过255个英文字符的英文字符串构成。

[0049] 现在参照图4,描述包装服务器100生成的DRM首部的结构。

[0050] 参见图4,DRM类型记录于DRM首部的签名域中,并且虚内容的文件名记录于文件名长度域中。DRM加密算法记录于DRM首部长度域中,并且DRM版本信息记录于DRM首部域中。另外,选项信息记录于填充(padding)域中,关于内容长度的信息记录于数据长度域中,并且内容数据信息记录于内容数据域中。

[0051] 再次参见图3,为了加密所注册的真实内容,包装服务器100生成CEK。为了生成所注册的真实内容的CEK(由参照字符CEK_R指示),包装服务器100使用种子值生成16字节CEK,并且对生成的16字节CEK进行基64(base64)编码。此处,种子值使用实时会话密钥值。虽然在本示例实施例中,当信息被包装时,使用“实时”时间信息,但是也可以使用单独管理的随机数表或者其它值。例如,特定音乐文件,例如音乐乐器数字接口(MIDI),可以以随机数表的形式存储于DB中,并且可以用作加密特定的真实内容CEK_R。在这种情况下,CEK_R是可再现内容。

[0052] 接着,使用生成的DRM首部、CEK_R以及对称密钥算法对真实内容加密,并且由此生成加密的真实内容。对称密钥算法使用AES 128比特算法,并且还可以使用其它对称密钥算法。

[0053] 如果第一包装处理完成，则执行第二包装处理。第二包装处理包括生成虚内容的第一操作、生成虚内容的CEK的第二操作、以及包装虚内容的第三操作。虚内容不是例如音乐或者电影等可再现数据，而是用于生成许可证并绑定该许可证至加密的内容的中间文件，该许可证设置加密的内容的权利。如果在第一包装处理中将特定音乐文件用作CEK_R，则虚内容可以是可再现内容。

[0054] 通过使用被用于加密真实内容的CEK_R，自动生成将被支持的DRM包装的目标虚内容。此处，虚内容的主体包括CEK_R。

[0055] 例如，OMA DRM生成MP3格式的虚内容。因此，虚内容具有作为CEK的有效载荷。另外，MSDRM生成Windows媒体音频(WMA)格式的虚内容。MSDRM不仅能生成WMA格式的虚内容，还能生成Windows媒体视频(WMV)以及高级系统格式(ASF)格式的虚内容。同样地，OMA DRM也可以生成多种格式的虚内容。

[0056] 接着，在第二包装处理中生成虚内容之后，为了对虚内容加密，包装服务器100生成CEK。虚内容的CEK由参照字符CEK_D指示。

[0057] 图5示出了根据本发明示例实施例的使用DRM供应系统10下载内容的操作。

[0058] 参见图5，用户或者注册服务器检查用户的便携式存储设备500是否已注册。然后，用户通过因特网在网页上选择用户希望购买的内容，并且请求下载服务器200下载所选的内容(操作①)。

[0059] 因此，下载服务器200请求用户认证服务器(图中未显示)认证用户请求的信息(例如由便携式存储设备500提供的)。如果便携式存储设备500没有注册至用户认证服务器，则用户针对下载所选内容的请求被拒绝。即，下载服务器200仅在用户将便携式存储设备500注册至用户认证服务器之后才下载请求的内容。

[0060] 然后，下载服务器200准备所请求的内容，即，要下载的加密的内容以及虚内容(操作②)。加密的内容是文件，例如运动图像或者音乐，其具有版权，并且虚内容是与针对内容文件的许可证绑定的或者与权利对象绑定的文件。

[0061] 下载服务器200将用户请求的内容传送至DRM供应装置400(操作③)，并且DRM供应装置400将接收到的内容下载至便携式存储设备500(操作④)。

[0062] 然后，下载的内容(即，加密的内容以及虚内容)被存储于内容DB中。由于加密的内容本身并不具有许可证，所以仅当加密的内容与虚内容同时存在时，许可证服务器300才可以被访问。

[0063] 图6示出了根据本发明示例实施例的使用DRM供应系统10接收许可证的操作。在下载内容之后，为了使用内容，用户必须接收针对该内容的许可证。许可证包括用于解密内容的CEK、以及针对内容的多种权利。在本示例实施例中，将描述使用Windows媒体(WM)DRM获取许可证的操作。

[0064] DRM供应装置400分析虚内容的DRM首部(操作①)。通过分析DRM首部，DRM供应装置400获取请求许可证发放所需的URI信息、以及搜索许可证所需的密钥ID(KID)值。

[0065] 然后，DRM供应装置400使用DRM首部以及设备证书，生成挑战数据(操作②)，并且使用超文本传输协议(HTTP)张贴(post)方法将生成的挑战数据传送至许可证服务器300(操作③)。挑战数据包括DRM首部以及设备证书，并且是基64编码的。

[0066] 许可证服务器300对接收到的挑战数据进行基64解码，并且通过分析DRM首部获取

KID。然后，许可证服务器300搜索与获取的KID匹配的CEK，使用设备证书中包括的公钥对CEK加密，并且将加密的CEK插入许可证中(操作④)。此处，使用椭圆曲线密码(ECC)非对称密钥加密方法对CEK加密。

[0067] 许可证服务器300对生成的许可证进行基64编码，并且将基64编码的许可证传送至DRM供应装置400(操作⑤)。此处使用的传送方法是直接许可证获取(DLA)方法。本发明中提出的DRM供应系统10使用DLA方法传送已编码的许可证。

[0068] DRM供应装置400向便携式存储设备500提供基64编码的许可证，并且便携式存储设备500存储该基64编码的许可证。

[0069] 图7是根据本发明示例实施例的DRM供应系统10中包括的DRM供应装置400的框图。

[0070] 参见图7，DRM供应装置400包括内容下载单元410、许可证管理单元420、预览供应单元430、以及处理单元440。

[0071] 内容下载单元410从下载服务器200下载内容，下载的内容存储于便携式存储设备500中。下载的内容包括加密的真实内容、以及两条虚内容(例如，OMA DRM-*.dcf以及MS-DRM-*.wma)，它们作为单条复合内容而被一起管理。

[0072] 许可证管理单元420接收来自许可证服务器300的许可证(或者权利对象)，以使用户能够使用下载的内容。使用OMA DRM方法传送的许可证以及使用MS DRM方法传送的许可证被存储于针对许可证的相应的存储区域中。

[0073] 例如，OMA权利对象存储于权利对象DB中，为了防止权利被随意访问或者修改，配置并且使用加密的存储空间。另外，MS DRM权利对象存储于散列(hash)存储单元中。

[0074] 预览供应单元430在预览屏幕上提供由内容下载单元410应用户的请求而下载的内容。

[0075] 处理单元440管理DRM供应装置400中包括的内容下载单元410、许可证管理单元420以及预览供应单元430的每一个的操作。另外，处理单元440向便携式存储设备500提供由内容下载单元410下载的真实内容和虚内容、以及由许可证管理单元420提供的虚内容的许可证。

[0076] 本文使用的术语“单元”意味着，但不限于，执行特定任务的软件或者硬件组件，例如现场可编程门阵列(FPGA)或者专用集成电路(ASIC)。单元可以有利地配置为驻留在可寻址的存储介质中，并且配置为在一个或者更多处理器上执行。因此，作为示例，单元可以包括组件，例如软件组件、面向对象的软件组件、类组件以及任务组件、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、以及变量。组件和模块中提供的功能可以被组合为更少的组件以及单元，或者进一步被分离成更多的组件以及单元。

[0077] 图8是根据本发明示例实施例的DRM供应系统10中包括的便携式存储设备500的框图。

[0078] 参见图8，便携式存储设备500包括存储空间，即，抗篡改模块(TRM)区域510、DRM区域520、以及用户访问区域530。TRM区域510存储DRM安全信息。即，TRM区域510存储针对每个DRM的便携式存储设备500的序列号，公钥/密钥，证书，设备群密钥，等等。

[0079] TRM区域510可以在便携式存储设备500被制造的时候创建。备选地，当便携式存储设备500在被购买后第一次使用时，可以一次写入TRM区域510。在这种情况下，可以在受到

网络服务器的认证之后写入TRM区域510。对于安全性，希望在制造便携式存储设备500时提前创建TRM区域510。TRM区域510是数据只读区域。存储于TRM区域510的数据可以使用访问便携式存储设备500的特定应用编程接口(API)来读取。

[0080] 访问记录于TRM区域510中的数据的权利必须仅给予DRM代理(图中未显示)，并且必须禁止外部用户移动或者改变数据。

[0081] DRM区域520存储加密的虚内容、以及许可证文件(或者权利对象)。即使DRM区域520对外开放，也不会出现安全问题。但是，如果便携式存储设备500的用户访问DRM区域520，并且移除或者改变其中的文件，则会出现对于DRM代理操作的致命问题。这种文件存储于DRM区域520中。另外，可以使用DRM代理或者特定便携式存储设备提供的API来访问DRM区域520。

[0082] 用户访问区域530存储加密的真实内容，例如视频或者音频，其可以被真正地回放。普通用户可以随意在用户访问区域530中读取或者写入内容。

[0083] 图9示出了根据本发明示例实施例的DRM供应系统10中包括的主机设备600的操作。在本示例实施例中，假定主机设备600也执行DRM供应装置400的功能，并且包括便携式存储设备500。在本示例实施例中，描述使用MS DRM代理来回放加密的内容的操作。

[0084] 参见图9，如果用户选择了所需的内容(操作①)，则内容下载单元410确定DRM是否已经被应用至所选文件。如果所选文件是加密的内容，为了搜索加密的内容的许可证，内容下载单元410搜索虚内容的文件名(操作②)。此处，从DRM首部中读取虚内容的文件名。

[0085] 接下来，通过分析DRM首部，获取请求许可证发放所需的URI信息和搜索许可证所需的KID(操作③)。然后，许可证管理单元420使用获取到的KID，来搜索存储于便携式存储设备500的DRM区域520中的许可证(操作④)。

[0086] 如果许可证不存在或者已经过期，则许可证管理单元420通过许可证下载处理，来请求许可证服务器300发放许可证。如果许可证管理单元420从便携式存储设备500的DRM区域520获取到许可证，则许可证管理单元420将获取到的许可证传送至主机设备600。

[0087] 主机设备600读取许可证中包括的虚内容的解密密钥CEK_D。由于虚内容的解密密钥CEK_D是使用公钥加密的，所以使用存储于TRM区域510中的私钥对该加密的解密密钥进行解密。由此获取解密密钥CEK_D。然后，解密虚内容，并且因此获取加密的真实内容的CEK_R(操作⑤)。

[0088] 接下来，使用CEK_R对加密的真实内容进行解密，并且回放文件(操作⑥)。真实内容是已经使用对称密钥(例如，AES 128比特)加密的。

[0089] 如果加密的真实内容被正常地回放，则主机设备600请求许可证管理单元420更新许可证(例如，更新回放计数)(操作⑦)。

[0090] 图10示出了根据本发明示例实施例的使用DRM供应系统10中包括的信息亭接收DRM内容的操作。首先，用户在使用信息亭下载内容之前必须注册便携式存储设备500。信息亭是DRM供应装置400的示例实施例。

[0091] 用户将便携式存储设备500(例如MMC)连接至信息亭的便携式存储设备接口或者通用串行总线(USB)接口，从信息亭的产品列表中选择所需内容及其许可证类型，并且发出购买请求(操作①)。

[0092] 接下来，信息亭识别用户连接到其上的便携式存储设备500。信息亭包括将用户ID

与便携式存储设备500的序列号匹配的表。因此，信息亭基于连接到其上的便携式存储设备500的序列号，在表中搜索用户ID(操作②)。备选地，信息亭可以通过网络服务器执行认证处理。

[0093] 参见信息亭的内部结构，信息亭包括TRM文件夹、DRM文件夹、以及内容文件夹。TRM文件夹存储将用户ID与序列号匹配的表，并且DRM文件夹存储针对每个用户ID的许可证和虚内容。另外，内容文件夹存储加密的内容。

[0094] 信息亭使用Active X下载共享目录处的内容(操作③)。此处，真实内容以及虚内容被一起下载。

[0095] 如果内容被下载，则信息亭基于找到的用户ID，获取针对用户所选内容的许可证。使用信息亭从许可证服务器300获取针对内容的许可证的处理与以上参照图6所述的获取许可证的处理是相同的，因此对其的详细描述被省略。

[0096] 然后，信息亭提供对下载内容的预览(操作④)。如果用户在信息亭的购买屏幕上选择[回放]功能，则出现预览屏幕。此处，如果用户选择预览的内容类型，则显示内容列表。如果用户选择内容列表右侧的[回放]功能，执行预览功能。针对预览功能，对加密的真实内容进行解密。由于对加密的内容解密的操作已经在参照图9的描述中说明了，因此对其的详细描述被省略。

[0097] 如果完成了预览功能，则将基于找到的用户ID的用户所选内容的许可证、虚内容、以及加密的内容被传送至便携式存储设备500，并且因此完成内容的购买处理(操作⑤)。

[0098] 如上所述，根据本发明的DRM供应装置、系统以及方法提供下列优点中的至少一项。

[0099] 尽管通过参照示例实施例具体显示并且描述了本发明，但是本领域普通技术人员将理解，在不背离由所附权利要求定义的本发明精神和范围的情况下可以做出多种形式以及细节上的变化。示例实施例应当仅被认为是描述性的而非限制性的。

[0100] 工业应用性

[0101] 由于使用一个或者更多DRM(MSDRM，OMA DRM，以及类似的)系统实现内容供应系统，所以可以提供使用统一的加密算法而包装的内容。

[0102] 另外，可以提供DRM内容，其可以被具有不同DRM系统的主机设备回放。

[0103] 无论有版权的真实内容是什么编码格式，提供了针对全部格式的内容的多DRM包装。因此，内容提供方不需要花费额外费用去对内容编码。

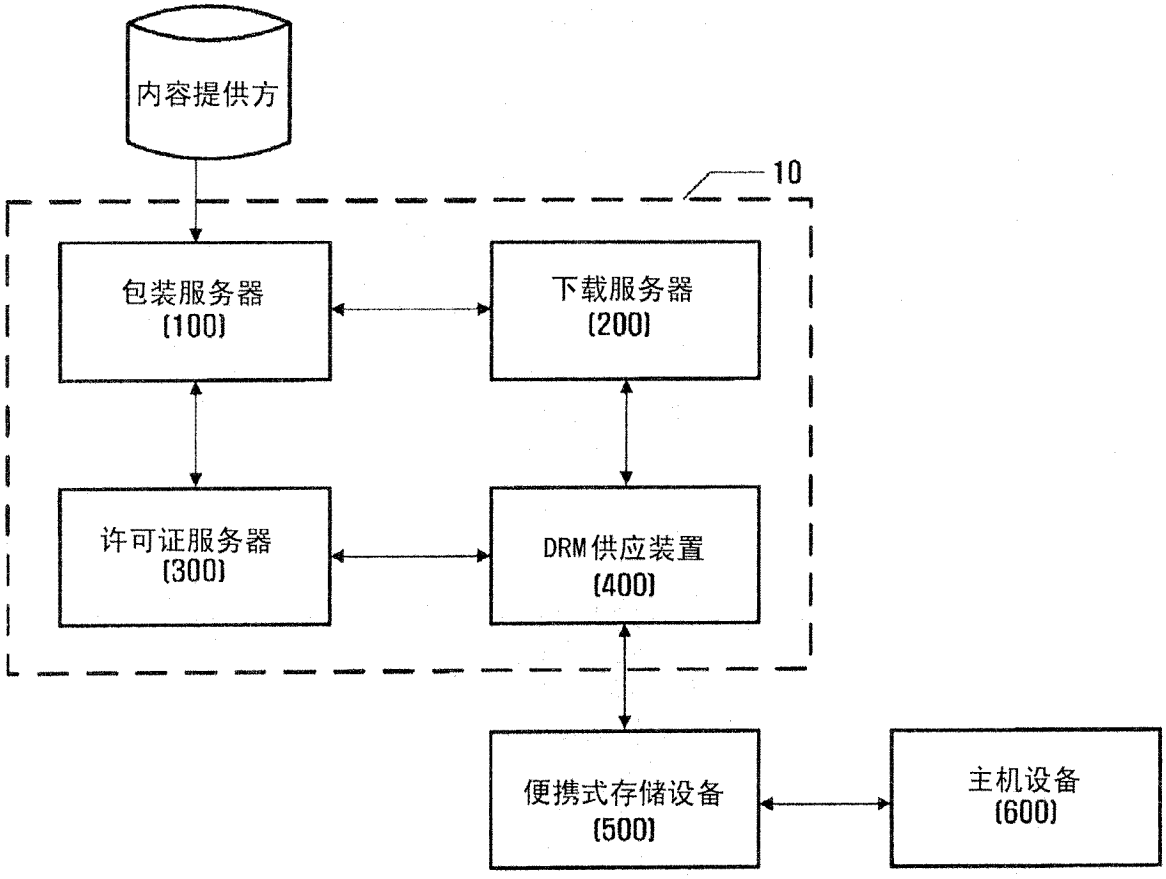

内容提供方
10
包装服务器
(100)
下载服务器
(200)
许可证服务器
(300)
DRM供应装置
(400)
便携式存储设备
(500)
主机设备
(600)

图1

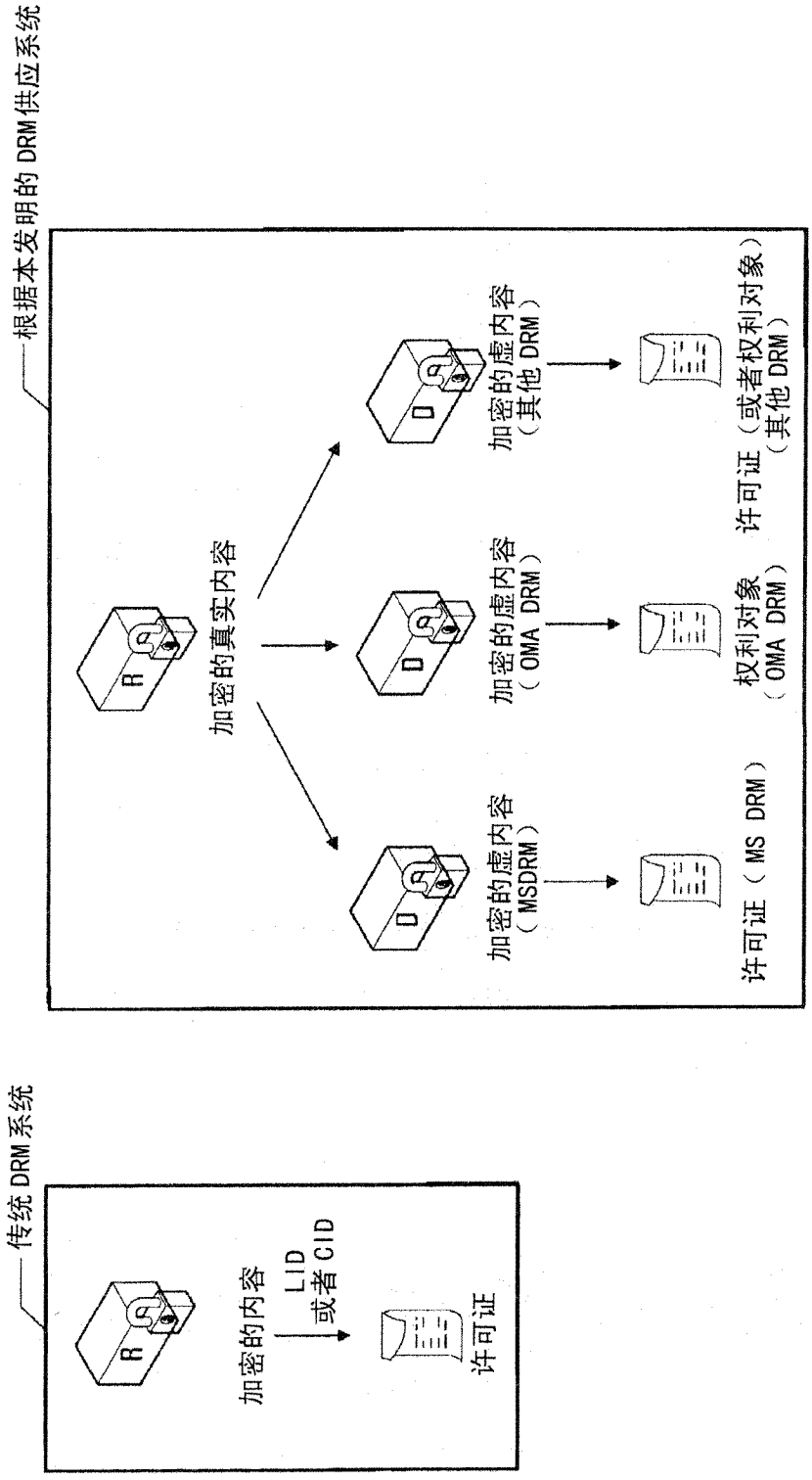

根据本发明的 DRM 供应系统
加密的真实内容
加密的虚内容
（MSDRM）
加密的虚内容
（OMA DRM）
加密的虚内容
（其他 DRM）
许可证（MS DRM）
权利对象
（OMA DRM）
许可证（或者权利对象）
（其他 DRM）
传统 DRM 系统
加密的内容
LID
或者 CID
许可证

图2

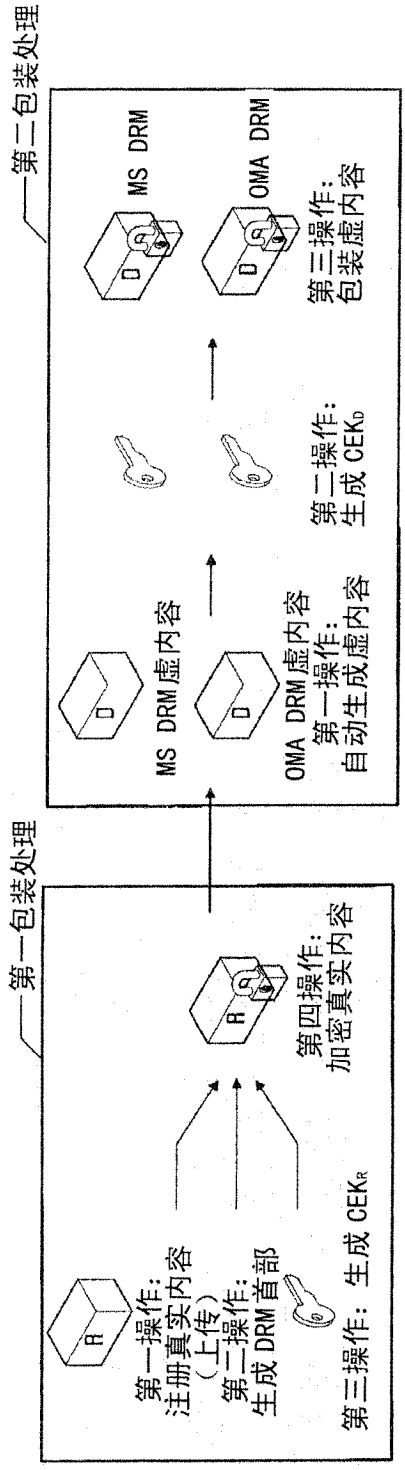

第二包装处理
MS DRM
OMA DRM
第三操作：
包装虚内容
第二操作：
生成 CEKD
MS DRM虚内容
OMA DRM虚内容
第一操作：
自动生成虚内容
第一包装处理
第四操作：
加密真实内容
第一操作：
注册真实内容
（上传）
第二操作：
生成 DRM首部
第三操作：生成 CEKR

图3

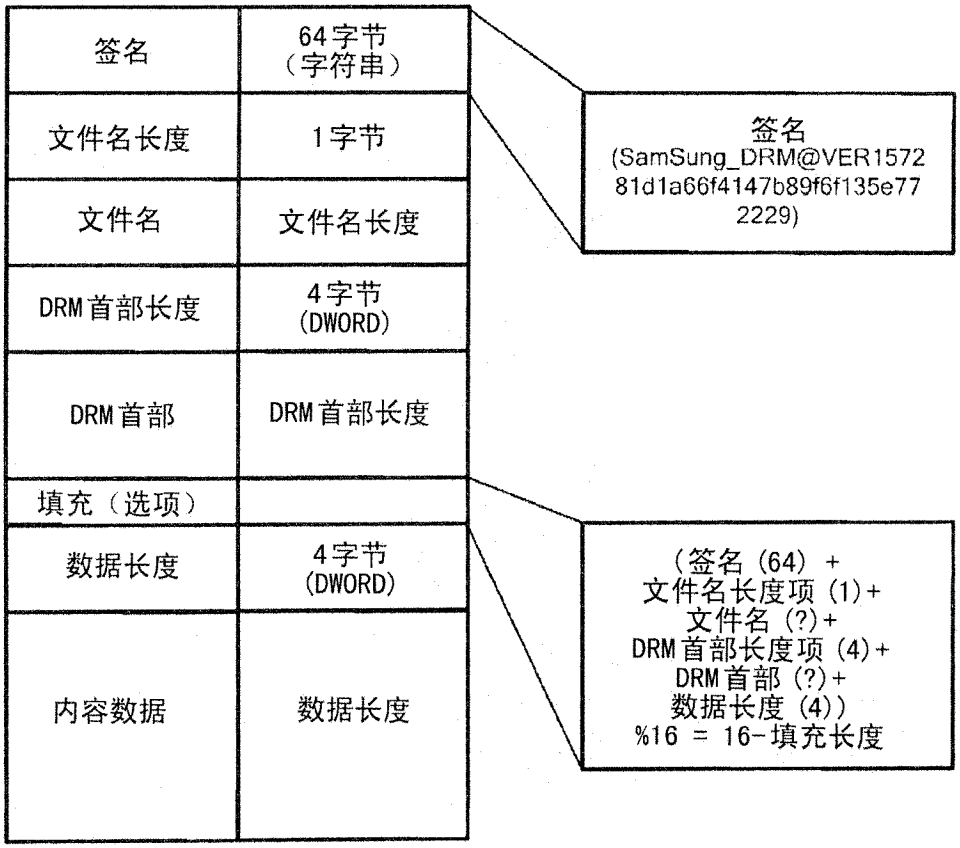

签名
64字节
（字符串）
文件名长度
1字节
文件名
文件名长度
DRM首部长度
4字节
(DWORD)
DRM首部
DRM首部长度
填充（选项）
数据长度
4字节
(DWORD)
内容数据
数据长度
签名
(SamSung_DRM@VER1572
81d1a66f4147b89f6f135e77
2229)
（签名（64）+
文件名长度项（1）+
文件名（?）+
DRM首部长度项（4）+
DRM首部（?）+
数据长度（4））
%16 = 16-填充长度

图4

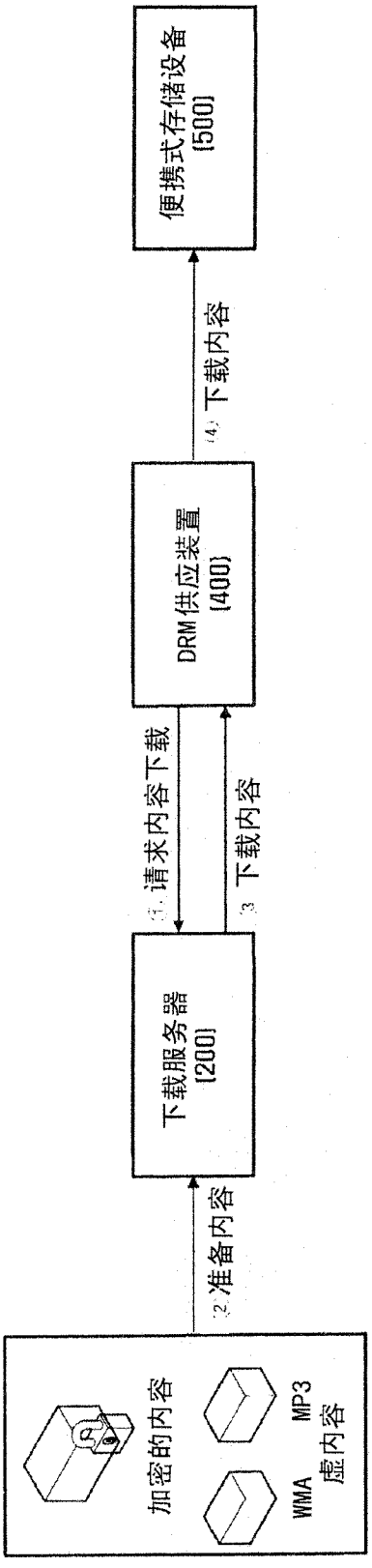

便携式存储设备
[500]
DRM 供应装置
[400]
下载服务器
[200]
加密的内容
MP3
WMA
虚内容
2 准备内容
1 请求内容下载
3 下载内容
4 下载内容

图5

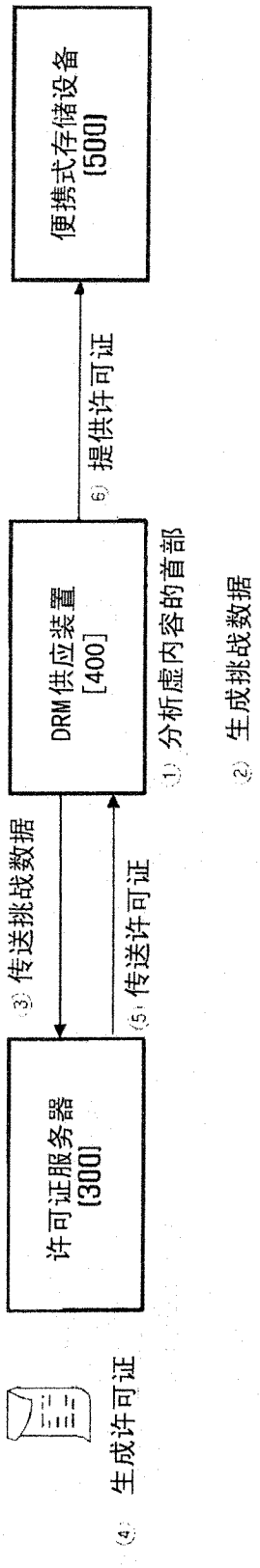

便携式存储设备
[500]
DRM 供应装置
[400]
许可证服务器
[300]
6 提供许可证
1 分析虚内容的首部
2 生成挑战数据
3 传送挑战数据
5 传送许可证
4 生成许可证

图6

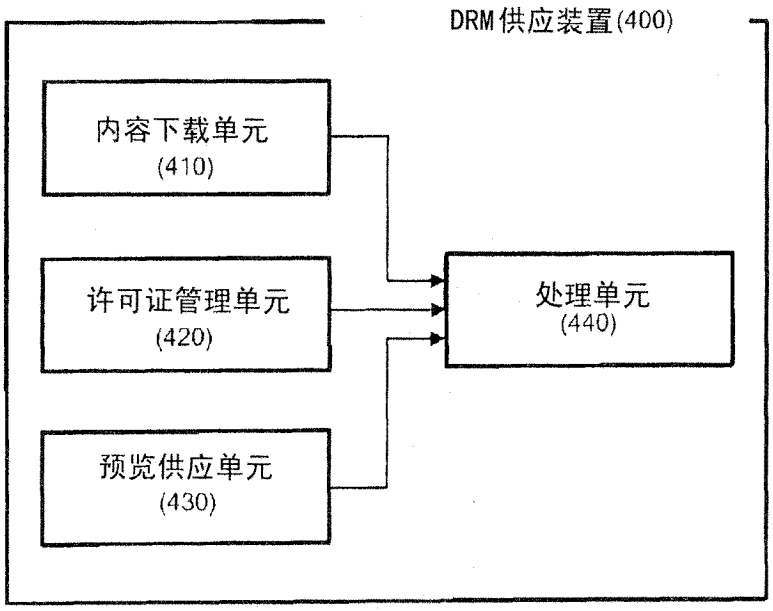

DRM供应装置(400)
内容下载单元
(410)
许可证管理单元
(420)
预览供应单元
(430)
处理单元
(440)

图7

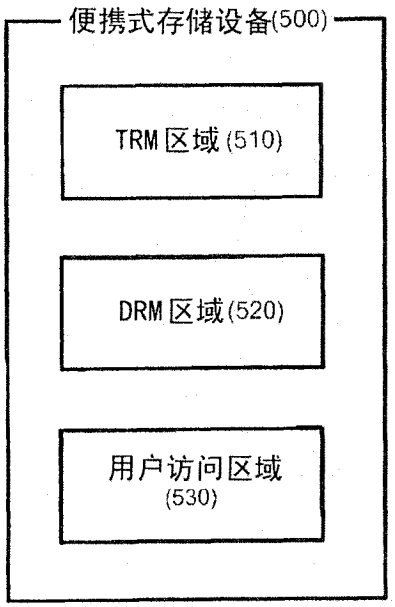

便携式存储设备(500)
TRM区域(510)
DRM区域(520)
用户访问区域
(530)

图8

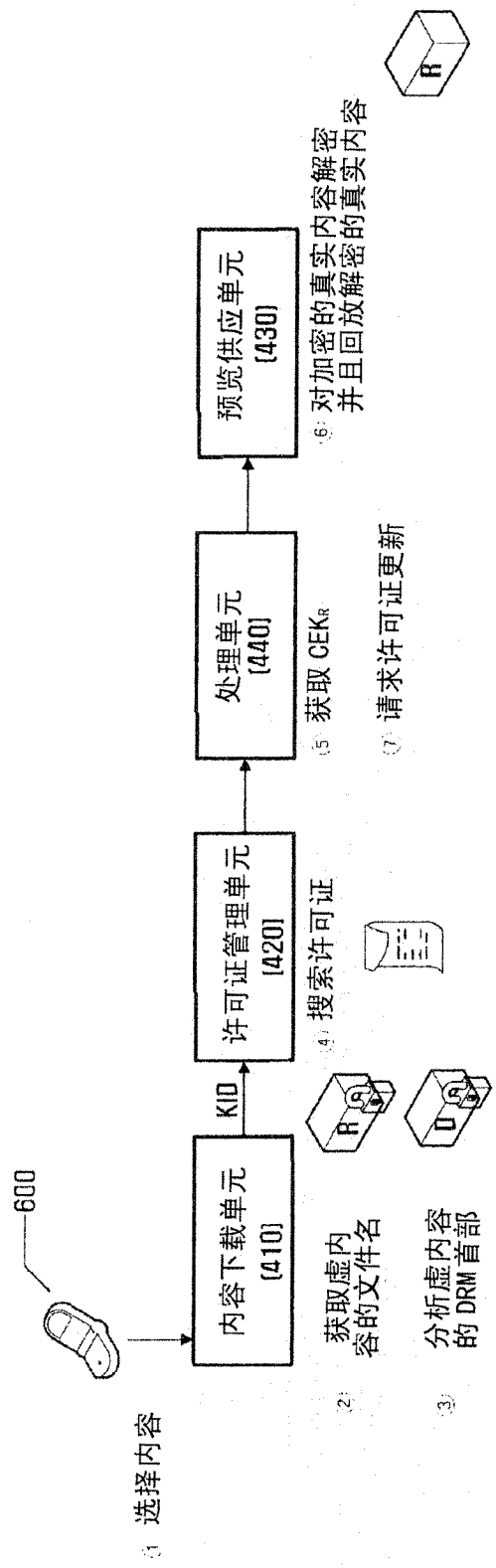

600
内容下载单元 (410)
KID
许可证管理单元 (420)
处理单元 (440)
预览供应单元 (430)
1 选择内容
2 获取虚内容的文件名
3 分析虚内容的 DRM 首部
4 搜索许可证
5 获取 CEKR
6 对加密的真实内容解密并且回放解密的真实内容
7 请求许可证更新

图9

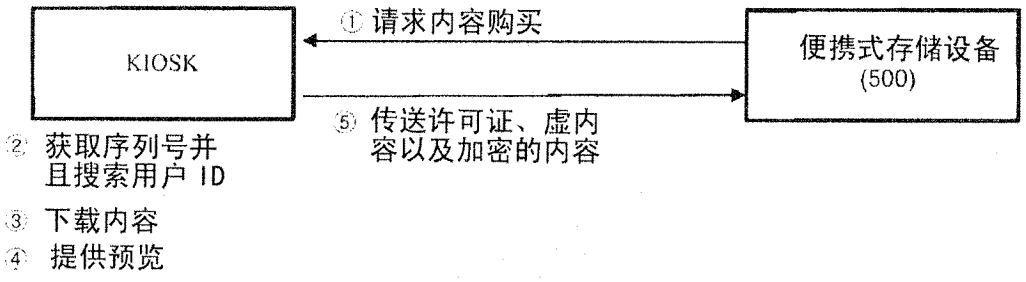

KIOSK
① 请求内容购买
便携式存储设备
(500)
⑤ 传送许可证、虚内容以及加密的内容
② 获取序列号并且搜索用户 ID
③ 下载内容
④ 提供预览

图10