(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 106464950 A
(43)申请公布日 2017.02.22

(21)申请号 201580030335.0

(22)申请日 2015.04.10

(30)优先权数据
14164465.8 2014.04.11 EP

(85)PCT国际申请进入国家阶段日
2016.12.07

(86)PCT国际申请的申请数据
PCT/CN2015/076354 2015.04.10

(87)PCT国际申请的公布数据
WO2015/154720 EN 2015.10.15

(71)申请人 电视广播有限公司
地址 中国香港

(72)发明人 邓浩唯 罗向荣 谭耀昌 陈曜威

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 梁丽超 刘丹

(51)Int.Cl.
H04N 21/2747(2011.01)
H04N 21/433(2011.01)

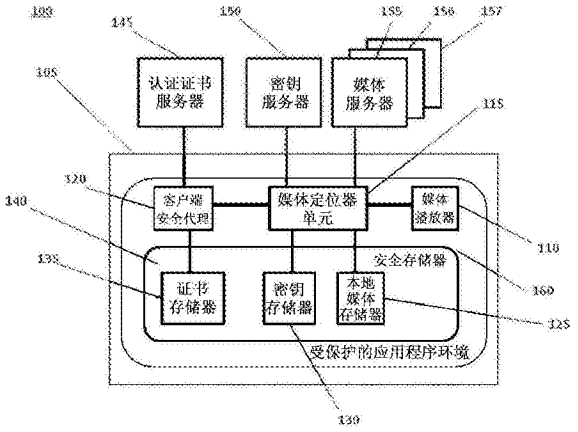
权利要求书2页 说明书11页 附图3页

(54)发明名称

递送和保护媒体内容的方法

(57)摘要

本申请提供了一种在装置上递送媒体内容的方法。在所述装置处接收串流媒体内容的请求。从装置的本地媒体存储器提取所请求的媒体内容的至少第一部分。将所请求的媒体内容的所述至少第一部分递送到装置的媒体播放器以用于回放。与所请求的媒体内容的至少第一部分的递送并行地，将所请求的媒体内容的至少第二部分从远程媒体存储器下载到装置。本申请还提供了一种在装置上保护媒体内容以免未经认证的回放的方法。该方法包括在装置处接收播放媒体内容的请求，其中所请求的媒体内容被加密。该方法还包括获得加密的媒体内容。该方法还包括使用第一加密密钥进一步加密经加密的媒体内容，以便产生双重加密的媒体内容，其中第一加密密钥是所述装置特有的。



CN 106464950 A

1.一种在装置上保护媒体内容以防未经认证的回放的方法,包括:

在所述装置处接收播放媒体内容的请求,其中所请求的媒体内容被加密;

获得所述加密的媒体内容;和

使用第一加密密钥进一步加密所述加密的媒体内容,以便产生双重加密的媒体内容,其中所述第一加密密钥是所述装置特有的。

2.根据权利要求1所述的方法,还包括在所述装置上存储所述双重加密的媒体内容。

3.根据任一前述权利要求所述的方法,还包括:

使用所述第一加密密钥来解密所述双重加密的媒体内容,以便再现所述加密的媒体内容;

在所述装置处接收一个或多个第二加密密钥;和

使用所述一个或多个第二加密密钥解密所述加密的媒体内容,以便产生解密的媒体内容,从而允许所述媒体内容的回放。

4.根据任一前述权利要求所述的方法,其中所述所述第一加密密钥是通过使用所述装置上的应用程序导出的。

5.根据任一前述权利要求所述的方法,其中所述第一加密密钥对于所述装置是唯一的。

6.根据任一前述权利要求所述的方法,其中获得所请求的媒体内容包括从远程媒体服务器下载所请求的媒体内容。

7.根据任一前述权利要求所述的方法,其中获得所请求的媒体内容包括从所述装置的本地存储器中提取所请求的媒体内容。

8.根据前述权利要求中任一项所述的方法,还包括确定与所述加密的媒体内容相关的元数据是否存储在所述装置上,以及:

如果是,则提取所述元数据;或

如果不是,则从远程元数据服务器请求所述元数据并在所述装置处接收元数据。

9.根据任一前述权利要求所述的方法,其中所述加密的媒体内容包括与所述加密的媒体内容相关的元数据。

10.根据权利要求8或9所述的方法,其中所述元数据包括标识所述一个或多个第二加密密钥的位置的数据。

11.根据权利要求10所述的方法,其中所述位置是所述一个或多个第二加密密钥在远程密钥服务器中的位置。

12.根据前述权利要求中任一项所述的方法,其中所述加密的媒体内容包括多个加密的媒体片段,并且其中所述一个或多个第二加密密钥中的每一个与所述多个加密的媒体片段中相应的一个相关联。

13.根据前述权利要求中任一项所述的方法,其中接收所述一个或多个第二加密密钥包括:

从远程密钥服务器请求所述一个或多个第二加密密钥。

14.根据权利要求13所述的方法,还包括:

从访问控制服务器请求认证令牌;

在所述装置处接收所述认证令牌;和

使用所述认证令牌从所述远程密钥服务器请求所述一个或多个第二加密密钥。

15.根据任一前述权利要求所述的方法，还包括：使用所述装置的媒体播放器来执行所述解密的媒体内容。

16.根据前述权利要求中任一项所述的方法，其中获得所述加密的媒体内容包括：

从所述装置的本地存储器提取所述加密的媒体内容的至少第一部分；和

与所述加密的媒体内容的至少第一部分的提取并行地，从远程媒体服务器向所述装置下载所述加密的媒体内容的至少第二部分。

17.根据权利要求16所述的方法，其中所述加密的媒体内容的所述至少第二部分被下载到所述本地存储器，以递送到所述装置的媒体播放器。

18.一种装置，包括：

用于存储媒体内容的存储器；和

处理器，被配置为：

接收播放媒体内容的请求，其中所请求的媒体内容被加密；

获取所述加密媒体内容；和

使用第一加密密钥进一步加密所述加密的媒体内容，以便产生双重加密的媒体内容，其中所述第一加密密钥是所述装置特有的。

19.一种系统，包括：

存储加密的媒体内容的媒体服务器；和

一个装置，被配置为：

接收播放所述加密的媒体内容的请求；

从所述媒体服务器获得所述加密的媒体内容；和

使用第一加密密钥进一步加密所述加密的媒体内容，以便产生双重加密的媒体内容，其中所述第一加密密钥是所述装置特有的。

20.一种其上存储有指令的计算机可读介质，其中所述指令被配置为使得当由计算机执行时，所述指令使得根据权利要求1-17中任一项所述的方法被执行。

递送和保护媒体内容的方法

技术领域

[0001] 本发明涉及保护在装置上的媒体内容以防止媒体内容的未经认证的回放的方法。本发明还涉及在装置上递送媒体内容的方法，并且具体地涉及使用HTTP实时串流递送媒体内容的方法。

背景技术

[0002] 诸如视频和/或音频数据的多媒体可以使用公知的技术串流到最终用户的装置上。媒体内容被从提供商下载或以其它方式提取，并且在下载时同时被递送或呈现给用户。例如，串流视频可以同时下载到用户装置并显示以供观看。类似地，音频内容可以同时下载到用户装置并被回放以供收听。因此，通过串流媒体内容，用户不一定需要首先下载内容，并且仅仅在内容被完全下载时才能访问它以供消费(例如观看、收听等)。

[0003] 使用HTTP作为互联网上的传输协议的媒体串流具有优于其它传统串流传输方法的益处。例如，连接到互联网的许多装置和系统支持HTTP协议。使用HTTP串流传输的视频内容通常被分成被称为片段的小片数据，其中每个片段可以保存几秒的视频数据。因此，一小时视频可以包含数百个片段。只要仅接收到少量片段，媒体播放器就可以开始显示视频内容。此外，HTTP支持自适应比特率串流，其允许媒体播放器根据当前可用于装置的连接带宽，选择在运行中的更高或更低质量的视频。此外，通过使用HTTP，媒体内容也可以被加密。使用这种串流传输方法的串流协议，例如HTTP实时串流传输(HLS)、平滑串流传输和MPEG-DASH，已经在移动装置上被广泛采用。

[0004] 然而，对于高质量媒体内容，串流式媒体是相对带宽密集的，并且通常需要相对快速的互联网连接以便提供令人满意的用户体验。如果连接丢失，例如如果装置离线，则串流可以被中断并且媒体内容可能不再被递送到最终用户，直到连接被重新建立。这显然不利地影响用户体验。因此，本领域中存在在用户将消费媒体内容的任何时间和任何地方更可靠地递送媒体内容的需要。

[0005] 另外，如果在装置上向用户提供的媒体内容受到保护以免发生违背内容提供商的利益的非法复制或重新分发，那也是优选的。存在可以用于防止媒体内容的未认证分发和/或回放的各种加密技术。例如，由苹果公司开发的FairPlay加密系统依赖于用于解密加密的媒体内容所需的主密钥。通过加密该主密钥，如果未认证用户不具有解密加密的主密钥所需的第二“用户”密钥，则能够防止未认证用户获得对媒体内容的访问。

[0006] 然而，在本领域中仍然存在进一步改进和开发用于加密或保护媒体内容免受未经认证的分发和/或回放的方法的需要。本发明的目的是满足这种需要。

发明内容

[0007] 根据本发明的第一方面，提供了一种在装置上串流传输媒体内容的方法。在装置处接收串流媒体内容的请求。从装置的本地媒体存储器提取所请求的媒体内容的至少第一部分。将所请求的媒体内容的至少第一部分递送到所述装置的媒体播放器以用于回放。与

所请求的媒体内容的至少第一部分的递送并行地，将所请求的媒体内容的第二部分从远程媒体存储器下载到装置。

[0008] 媒体内容的一部分可以包括一个或多个媒体片段。因此，媒体内容的片段可以被递送到所述装置的媒体播放器以供回放。如果片段被存储在本地媒体存储器中(例如，如果它们以前已经被下载到装置)，则一旦接收到串流请求并且所述片段已经从本地商店抓取或提取了，则所存储的媒体片段的回放可以马上开始。所请求的媒体内容的其它片段可以从远程媒体存储器下载并作为串流递送到媒体播放器。媒体片段的下载、串流传输和回放可以彼此并行地操作。

[0009] 在一个实施例中，可以确定所述装置的本地媒体存储器是否包括所请求的媒体内容的至少第一部分。可以将所请求的媒体内容的至少第一部分递送到装置的媒体播放器以供回放。可以确定远程媒体存储器是否包括其上存储的所请求的媒体内容的至少第二部分。与所请求的媒体内容的至少第一部分的递送并行，所请求的媒体内容的至少第二部分可以从远程媒体存储器下载到所述装置。

[0010] 因此，该方法可以包括从本地媒体商店或特定远程媒体商店定位每个媒体部分(或片段)及其相应位置。定位可以基于包括在所请求的媒体内容中的元数据。然后可以通过从装置的本地媒体器存储获取它或者通过从远程媒体存储下载它，来将每个媒体片段串流式传输到装置的媒体播放器以供回放。定位、下载和串流式传输功能可以并行操作以向装置的最终用户提供令人满意的回放体验。

[0011] 所述装置可以是能够串流传输媒体内容的任何装置。例如，装置可以是诸如膝上型计算机或平板电脑的便携式装置。该装置可以是诸如智能电话的移动装置，或者可以是能够显示视频的电视或其它装置，或者可以是能够连接到显示装置的机顶盒。或者，装置不需要具有显示器，并且可以被布置为纯粹地串流音频内容。

[0012] 本地媒体存储器可以是用于存储一个或多个媒体文件的所述装置的存储器的一部分。该装置可以包括多于一个物理存储器。远程媒体存储器可以是传统媒体服务器、云上的服务器、或者可以形成一个或多个内容分发网络(CDN)的一部分。可以使用其它类型的远程媒体存储器。

[0013] 所请求的媒体内容的第一和第二部分可以包括任何数量的所请求的媒体内容。例如，从远程存储器下载的媒体内容的程度可以接近100％，在这种情况下，该方法的操作接近传统实时串流传输的操作。或者，可以从本地存储器获取大部分媒体内容，在这种情况下，由于所请求的媒体内容的大部分已经存储在装置上，因此可以优化回放体验的质量。媒体播放器的操作可以不受从本地媒体存储器获取的内容的量以及作为预下载(例如，存储在装置的本地存储器中)的可用内容的量的影响。结果，本发明改进了媒体播放器的媒体串流的位置透明度。

[0014] 所请求的媒体内容的至少第二部分可以被直接下载到本地媒体存储器以递送到媒体播放器。或者，所请求的媒体内容的至少第二部分可被下载并直接递送到媒体播放器。因此，无论每个媒体片段的不同位置如何，媒体片段可以连续地递送到媒体播放器，在串流过程中没有中断。

[0015] 所请求的媒体内容的至少第二部分可以根据串流协议(诸如HTTP实况串流传输(HLS)协议)来下载。所请求的媒体内容的至少第二部分可以从互联网下载。在一些实施例

中，所请求的媒体内容可以从诸如LAN、无线LAN、移动和蜂窝3G/4G/LTE等的其它类型的网络下载。

[0016] 所请求的媒体内容可以包括多个媒体片段。所请求的媒体内容的至少第一部分和所请求的媒体内容的至少第二部分可以各自包括多个媒体片段中的一个或多个。

[0017] 每个媒体片段可以包括用于HTTP传输的媒体内容。此外，除了多个媒体片段之外，所请求的媒体内容可以包括元数据，并且所述元数据可以包括与所请求的媒体内容有关的描述或其它信息，以及所请求的媒体内容中的媒体片段的列表。

[0018] 通过使用所述装置的媒体定位器单元(MLU)，一个或多个解密密钥可以被下载到装置上的本地密钥存储器。具体地，所请求的媒体内容的第一和第二部分中的至少一个可以被加密，并且一个或多个解密密钥可以被布置为解密所请求的媒体内容的第一和第二部分中的至少一个。HLS特别地支持媒体串流的加密。解密密钥可以从远程服务器或其它远程存储器下载。

[0019] 通过使用所述装置的客户端安全代理(CSA)，一个或多个认证证书可以被下载到装置上的证书存储器。解密密钥可以从远程服务器或其它远程存储器下载。

[0020] 将一个或多个解密密钥下载到密钥存储器可以包括首先由MLU请求来自CSA的认证证书，然后所请求的认证证书可以从CSA传送到MLU。

[0021] 尽管加密的媒体内容和解密密钥可以被高速缓存在客户端装置上，但是CSA可以与MLU一起部署以保护媒体内容提供商的利益。CSA可以从公共密钥基础设施认证中心请求X.509客户端证书，并管理用于在不同密钥服务器上认证客户端的证书。

[0022] 因此，如果所述装置第一次尝试从特定远程密钥服务器提取一个或多个解密密钥，则密钥服务器可以通过递送适当的认证证书来请求所述装置的认证。所述装置的CSA可以被布置为提取这样的证书并将其递送到MLU，以用于随后递送到密钥服务器以进行认证。

[0023] 有利地，利用协同操作的MLU和CSA，HLS串流的媒体内容可以通过加密来保护，并且客户端装置可以被认证以允许访问媒体内容。

[0024] 媒体存储器、密钥存储器和证书存储器可以各自位于装置的安全存储器中。安全存储器可以由装置的操作系统(例如Apple iOSTM或Google AndroidTM)或仅允许有效用户访问存储区域的任何其它类似操作环境来保证。

[0025] 虽然媒体内容变得更容易被用户在各种装置上访问和消费，但媒体内容提供商需要对什么人或什么装置可以访问内容的可靠控制。一旦媒体内容被递送到客户端，用户可以重新分发它，或者对媒体内容执行可能违反内容提供商的使用策略的其它动作。

[0026] 因此，根据本发明，可以确定在受保护环境中的安全存储是否已经违规。如果安全存储已经违规，则可以删除媒体存储器、密钥存储器和证书存储器中的至少一个的内容，和/或可以停止所请求的媒体内容的回放。此外，MLU和CSA可以被布置为相互通信。如果MLU和CSA不再相互通信、或者如果通信有疑问，则可以删除媒体存储器、密钥存储器和证书存储器中的至少一个的内容，和/或可以停止回放所请求的媒体内容。

[0027] 因此，CSA可以验证和确保在其操作环境中的安全存储的完整性和安全性，并且可以确认MLU的状态。CSA可以另外检查操作环境的安全策略的维护。如果CSA检测到安全策略被违反了，则CSA可以清除证书存储并通知MLU，并且MLU在从CSA接收到通知时可以停止媒体串流处理，以及清除密钥存储器和本地媒体商店。如果检测到违反使用策略的任何用户

行为或安全环境的其它破坏，则可以删除所有存储的客户端证书、缓存的解密密钥和加密的媒体。

[0028] 另外，MLU可以从CSA接收关于所述装置的受保护的应用环境的状态的周期性更新。当MLU失去与CSA的联系并且不能保证其在安全环境中操作时，可以停止媒体串流传输，并且可以分别清除证书存储器、密钥存储器和本地媒体存储器的内容。

[0029] 解密密钥和/或所请求的媒体内容可以被布置为在下载/提取之后预定的时间段内到期。在到期时，可以停止所请求的媒体内容的回放。另外，在到期时，可以从所述装置中删除解密密钥和/或所请求的媒体内容。

[0030] 根据本发明，还提供了一种布置成执行上述方法的装置，以及包括这种装置的系统。

[0031] 根据本发明的第二方面，提供了一种在装置上保护媒体内容免于未经认证的回放的方法。该方法包括在装置处接收播放媒体内容的请求，其中所请求的媒体内容被加密。该方法还包括获得加密的媒体内容。该方法还包括使用第一加密密钥进一步加密经加密的媒体内容，以便产生双重加密的媒体内容，其中第一加密密钥是所述装置特有的。

[0032] 所请求的媒体内容可以包括适合于在装置上播放的任何媒体文件或文件，诸如但不限于视频数据、音频数据和/或图像数据。媒体内容可以包括在数字媒体文件中。当由所述装置获得时，媒体内容可能已经由远程媒体服务器使用下面更详细讨论的一个或多个第二加密密钥来加密。在能够播放或执行加密的媒体内容之前，所述装置必须首先确定第二加密密钥的位置，以便解密加密的媒体内容。应当注意，术语“加密密钥”和“解密密钥”可以互换使用，因为它们基本上是相同的密钥，但是用于反向操作。

[0033] 一旦在装置处接收到加密的媒体内容，则使用专用于装置的第一加密密钥来执行另一第二加密步骤。使用这种基于装置的加密密钥的第二加密有助于安全或保护媒体内容免受未经认证的分发或回放，因为将双重加密的媒体内容恢复到其单加密状态所需的第一加密密钥是特定于装置的。因此，没有这种装置特定的加密密钥，未认证的装置将不能播放媒体内容。第一加密密钥对于装置可以是唯一的，并且没有其它装置能够再现第一加密密钥。本领域中存在已知的用于产生这种唯一的或装置特定的加密密钥的方法，例如通过在对装置的标识号(例如厂商ID或序列号)使用散列函数的变体。

[0034] 有利地，该方法允许改进保护以防止未认证的加密媒体内容的回放，因为第一加密密钥不需要存储在装置上，而是可以简单地由装置(例如使用合适的应用程序)生成，只要存在对解密双重加密的媒体内容的需求。

[0035] 该方法还可以包括在装置上存储双重加密的媒体内容。双重加密的媒体内容可以存储在所述装置的合适的存储器中，以用于将来的回放，例如每当装置从用户接收到播放媒体内容的请求时。

[0036] 当装置接收到播放加密的媒体内容的请求时，所述装置可以使用第一加密密钥对双重加密的媒体内容进行解密，以便再现加密的媒体内容。该装置然后可以接收一个或多个第二加密密钥。然后，可以使用一个或多个第二加密密钥第二次解密加密的媒体内容，以便产生解密的媒体内容，从而允许媒体内容的回放。

[0037] 有利地，一个或多个第二加密密钥可以远离所述装置存储，以便提高系统的安全性。因此，在加密的媒体内容可以被完全解密用于回放之前，一个或多个第二加密密钥可能

必须首先被装置请求并且在装置处被接收。

[0038] 获得所请求的媒体内容可以包括从远程媒体服务器下载所请求的媒体内容。因此，如果所请求的媒体内容尚未存储在所述装置上，则该装置可以与存储媒体内容的远程服务器通信，以便将所请求的媒体内容下载到装置上。或者，如上所述，双重加密的媒体内容可能已经存储在装置上，在这种情况下，该装置可以从装置的本地存储(例如从合适的存储器)提取媒体内容。

[0039] 如我们已经看到的，为了完全解密双重加密的媒体内容，不仅需要装置特定的第一加密密钥，而且装置还必须访问一个或多个第二加密密钥(所述密钥已经用于第一次加密所述一个或多个密钥媒体内容)。因此，该方法还可以包括确定与加密的媒体内容相关的元数据是否存储在装置上。如果是，则装置可以提取元数据，或者如果不是，则装置可以从远程元数据服务器请求元数据并在装置处接收元数据。

[0040] 加密的媒体内容可以包括与加密的媒体内容相关的元数据。在这种情况下，加密的媒体内容通常包含多个加密的媒体片段(例如要回放的视频或音频数据)以及与加密的媒体片段相关的未加密的元数据。元数据可以包括标识一个或多个第二加密密钥的位置的数据。该位置可以是远程密钥服务器中的一个或多个第二加密密钥的位置。

[0041] 因此，一旦由装置获得(无论其是否已被装置从远程存储位置请求，或者其是否包含加密的媒体内容本身)，所述元数据可以用于访问所需的一个或多个第二加密密钥以完全解密双重加密的媒体内容。

[0042] 接收一个或多个第二加密密钥可以包括从远程密钥服务器请求一个或多个第二加密密钥。特别地，该方法可以包括从访问控制服务器请求认证令牌，在装置处接收认证令牌，以及使用认证令牌从远程密钥服务器请求一个或多个第二加密密钥。因此，装置可以首先获得认证令牌，并且结合识别一个或多个第二加密密钥的位置的元数据，使用认证令牌来获得一个或多个第二加密密钥。

[0043] 应当注意，如果媒体内容被分成多个单独加密的媒体片段，则可以有多于一个的第二加密密钥。在这种情况下，一个或多个第二加密密钥中的每一个可以与多个加密的媒体片段中的对应的一个相关联。因此，元数据可以标识每个单独的第二加密密钥的位置，以便允许对构成媒体内容的全部媒体片段进行解密。

[0044] 一旦装置访问了第二加密密钥，就可以使用第二加密密钥进一步解密加密的媒体内容(已经使用装置特定的加密密钥解密过一次)，以便完全解密媒体内容。该方法然后可以进一步包括使用装置的媒体播放器来执行解密的媒体内容。

[0045] 以与上面结合本发明的第一方面所描述的大致相同的方式，所请求的媒体内容的一部分可以本地驻留在装置的存储器中，并且第二部分可能必须从媒体服务器下载。因此，获得加密的媒体内容可以包括从装置的本地存储器提取加密的媒体内容的至少第一部分。获得加密的媒体内容还可以包括：与提取加密的媒体内容的至少第一部分并行地，从远程媒体服务器向装置下载加密的媒体内容的至少第二部分。加密的媒体内容的至少第二部分可以被下载到本地存储器，以便递送到装置的媒体播放器。

[0046] 根据本发明，还提供了一种布置成执行上述方法的装置，以及包括这种装置的系统。

[0047] 在本公开说明书的范围内，本发明的第二方面的任何特征或元件(即，关于保护媒

体内容免于未经认证的回放的方法)可以与本发明的第一方面的任何特征或元件(即,方法向装置传送媒体内容)组合。

附图说明

[0048] 现在将结合附图描述本发明的具体实施例,其中:

[0049] 图1是根据本发明的实施例的系统的图;

[0050] 图2是示出根据本发明的实施例的递送媒体内容的方法所采取的步骤的串流程图;和

[0051] 图3是示出根据本发明的实施例的保护媒体内容免于未经认证的回放的方法所采取的步骤的串流程图。

具体实施方式

[0052] 本发明的目的是提供一种用于递送和保护媒体内容的改进方法。虽然下面描述了本发明的各种实施例,但是本发明不限于这些实施例,并且这些实施例的变型可以完全落入本发明的范围内,本发明的范围仅由所附权利要求限制。

[0053] 图1示出了根据本发明的实施例的媒体串流系统100。在系统100的客户端或终端用户侧上,系统100包括客户端装置105,例如便携式移动装置。客户端装置105可以是能够进行媒体内容回放的任何其它装置,诸如电视、PC、膝上型计算机、移动电话、机顶盒、音频系统等。

[0054] 客户端装置105包括媒体播放器110、媒体定位器单元115(MLU)和客户端安全代理(CSA)120。媒体播放器110、MLU 115和CSA 120可以包括在客户端装置105的操作系统中的应用程序的一个或多个软件模块中。

[0055] 客户端装置105还包括本地媒体存储器125、密钥存储器130和证书存储器135。本地媒体存储器125、密钥存储器130和证书存储器135驻留在客户端装置105的安全储存器或安全存储器140中。每个存储器不需要驻留在公共安全存储器中,但可驻留在单独的安全存储中。本地媒体存储器125的存储器大小实质上大于传统媒体播放器的存储器缓冲器,使得如果互联网连接丢失并且下载尚未完成,则客户端装置105可以在短时间段内继续媒体内容的回放。媒体播放器110、MLU 115和CSA 120是安全环境中的应用程序的组件。所述应用程序是在诸如Apple iOS、Google Android OS等操作系统的受保护运行时(runtime)环境或受保护的应用程序环境160中的,使得单个组件不能被替换。受保护的应用程序环境160包括安全存储器140,使得当受保护的应用程序环境受损时不能访问存储在其中的数据。

[0056] 在多媒体串流系统100的服务器侧上,提供了认证证书服务器145或公共密钥基础设施证书机构(PKI CA)、密钥服务器150和媒体服务器155。PKI CA 145、密钥服务器150和媒体服务器155可以形成内容分发网络(CDN)的一部分或作为类似云服务器的一部分。它们可以驻留在公共服务器或单独的服务器上。CDN提供对跨互联网复制的媒体内容的方便访问。在其它实施例中,PKI CA 145、密钥服务器150和媒体服务器155可以驻留在联网到客户端装置105的其它用户装置上。另外,PKI CA 145、密钥服务器150和媒体服务器155可以是在互联网上或在MLU 115可访问的专用网络上的任何地方的服务器应用程序,它们中每个都有独立运行的多个服务。媒体内容和媒体片段可以从任何数量的媒体服务器155、156、

157下载。

[0057] 媒体播放器110被布置为根据HLS协议处理和播放其接收的媒体内容，例如媒体片段。例如，媒体播放器110可以处理和显示诸如直播电视串流或电影的视频内容、或诸如音乐曲目或其它音频文件的音频内容。媒体播放器110可以与MLU 115通信，使得媒体播放器110可以接收由MLU115传送给它的媒体内容。为了简化本发明的实施例，媒体播放器110可以是由操作系统提供的标准组件。

[0058] MLU 115是可以从本地媒体存储器125提取媒体内容的客户端装置105的组件。MLU 115还可以从密钥存储器130提取解密密钥。特别地，MLU 115被布置为使用来自密钥存储器130的解密密钥来解密和处理加密的媒体内容，使得即使在离线时，即当从互联网断开时，客户端装置105也能够进行媒体内容回放。MLU 115还被布置为将解密密钥从密钥服务器150下载到客户端装置105，以及将媒体内容从媒体服务器155或媒体服务器155、156、157下载到客户端装置105。所述下载优选地根据HLS协议使用HTTP进行。当下载时，解密密钥存储在密钥存储器130中，并且媒体内容存储在本地媒体存储器125中。不同的密钥可以分别分配给不同的媒体内容，或者分配给媒体内容或多个媒体内容的不同片段。

[0059] 除了确保客户端侧的受保护的运行时环境之外，CSA 120还被布置为通过使用X.509客户端证书在密钥服务器150上认证客户端装置105。可以使用其它形式的客户端证书或认证令牌。X.509客户端证书从PKI CA145获得，由CSA 120下载并本地存储在客户端装置105的证书存储器135中。可能需要不同的客户端证书来播放不同的媒体内容。客户端证书可以由PKI CA 145无效，并且要求MLU 115提供有效的客户端证书以便从密钥服务器150提取解密密钥。

[0060] 现在将根据本发明的实施例描述媒体串流传输系统100的操作方法。

[0061] 在传统的媒体串流技术中，属于提供商的媒体内容被存储在服务器上，并且在客户端装置上运行的客户端应用程序下载媒体内容，同时并行地显示内容。媒体服务器和媒体客户端之间的操作由串流协议规定。

[0062] HLS是使用HTTP传输协议用于在互联网上进行媒体串流的串流协议。HLS支持媒体内容的加密(AES-128)串流。当在加密模式中使用HLS时，通常通过网络服务器向客户端应用程序提供解密密钥。

[0063] 本发明扩展了串流操作以支持媒体内容的预下载以及混合操作模式，根据混合操作模式，预下载的内容和实时串流内容被一起使用。因此，在客户端侧的媒体播放器可以像执行正常的HLS处理那样操作。

[0064] 根据方法200，在步骤205，客户端装置105使用HLS接收串流媒体内容的请求。例如，客户端装置105的用户可以输入打开媒体内容的命令，诸如通过经由在连接到互联网时显示给用户的网页访问链接。该请求可以首先在媒体播放器110处接收然后媒体播放器110将该请求传递给MLU115，或者该请求可以由MLU 115直接接收。

[0065] 在MLU 115处接收到对串流媒体的请求时，在步骤210，MLU 115从本地媒体存储器125提取或抓取任何相关媒体串流片段或其它所请求的媒体内容。这不是从远程服务器搜索和下载整个所请求的媒体内容。在步骤210同时，在步骤215，MLU 115将剩余的所请求的HLS媒体片段从媒体服务器155下载到本地媒体存储器125。

[0066] 例如，所请求的媒体内容可以包括视频的元数据和所请求的媒体内容的多个媒体

片段。元数据可以包含诸如以下信息的信息：媒体片段的细节、媒体片段可以从其下载的媒体服务器的位置、视频是否被加密以及可以提供解密密钥或密钥解密媒体内容的密钥服务器的位置。媒体片段可以由MLU 115根据串流协议来组装。

[0067] 当客户端装置105处于混合操作模式时，多个这样的媒体片段可以形成所请求的媒体内容的第一部分，并且可以存储在本地媒体存储器125中。与所请求的媒体内容有关的任何其它媒体片段形成所请求的媒体内容的第二部分，其可以并行地从媒体服务器155下载到本地媒体存储器125中。

[0068] 因此，所请求的媒体片段中的一个或多个被存储在本地媒体存储器125中。一旦由MLU 115获取，在步骤235，该部分被递送到媒体播放器110以供回放。虽然媒体播放器110正在处理和显示/播放所请求的媒体内容的已经下载的片段，但与实时串流类似，其余片段从媒体服务器155并行地下载到本地媒体存储125。

[0069] 在诸如HLS协议的常规数据串流技术中，如果客户端装置在媒体内容的下载完成之前下线，并且随后在经过一片段时间之后上线，则媒体内容的下载需要重新启动。

[0070] 根据本发明的实施例，如果互联网连接丢失，而媒体内容的下载仍在进行中，则MLU 115继续从本地媒体存储器125获取媒体片段，并将它们传送到媒体播放器110。一旦客户端装置105重新连接到互联网时，MLU115将根据元数据自动地恢复针对未完成的媒体片段的下载处理，并且用户可能不会注意到曾经发生过互联网断开(假设断开不持续太久)，因为回放是连续的。

[0071] 如已经提到的，HLS协议允许串流媒体的加密以提供数字版权管理，使得媒体内容的版权持有者可以控制已经存储在客户端装置105上的媒体的分发和传播。

[0072] 在步骤220，MLU 115确定从本地媒体存储器125提取的所请求的媒体内容是否被加密。如果被加密，则在步骤230，MLU 115访问客户机装置105的本地密钥存储器130。如果必要的解密密钥(或多个密钥)被存储在本地密钥存储器130中，则MLU 115提取解密密钥并在步骤225解密加密的媒体内容然后可以将解密的媒体内容传递给媒体播放器110以供回放(步骤235)。或者，加密的媒体内容可以利用解密密钥传递到媒体播放器110，在这种情况下，媒体播放器110可以在回放之前解密媒体内容。

[0073] 如果必需的密钥未存储在本地密钥存储器130中，则在步骤250，MLU 115访问密钥服务器150。在步骤255，密钥服务器150确定客户端装置105是否被认证以访问所需密钥。如果客户端装置105在密钥服务器150上被认证，则在步骤290，MLU 115可以从密钥服务器150下载或以其它方式提取解密密钥。然后，MLU 115可以解密加密的媒体内容并将解密的媒体内容传递到媒体播放器110。如果MLU未在密钥服务器150上认证，则在步骤260，MLU 115向CSA 120请求相关认证证书。

[0074] 在步骤265，CSA 120访问客户端装置105上的本地证书存储器135，并且在步骤270确定所请求的认证证书是否存储在其上。如果所请求的认证证书存储在本地证书存储器135中，则在步骤280(在下面更详细地描述)，CSA 120提取证书并将其传送给MLU 115。如果在步骤270确定所请求的认证证书没有存储在本地证书存储器135中，则在步骤275，CSA120请求来自PKI CA 145的相关认证证书。在步骤280，CSA 120下载或以其它方式提取认证证书。在步骤285，CSA 120将认证证书传递给MLU115，MLU 115在步骤285将认证证书传递到密钥服务器150。一旦密钥服务器150使用认证证书来认证客户机装置105，在步骤290则由MLU

115下载或以其它方式提取相关解密密钥。然后操作进行到步骤225，其中加密的媒体内容被解密，并且在步骤235，解密的媒体内容最终被传递到媒体播放器110以供回放。上述方法仅仅是特定实施例的说明，并且在不脱离本发明的情况下可以省略/添加许多步骤。

[0075] 为了防止传播下载的媒体内容的非法副本，本地媒体存储器125和密钥存储器130位于由客户端装置105上的操作系统提供的受保护的应用程序环境160的安全存储器140中，所述操作系统例如是已经提到的Apple iOS或Google Android OS。能够建立受保护的应用程序环境160的其它操作系统也可以使用。

[0076] CSA 120周期性地(例如每分钟)验证安全存储器140以及受保护的应用程序环境160的完整性。验证可以基于由操作系统提供的功能来实现。例如，如果客户端装置105是越狱的(jail-broken)或刷机的(rooted)，或者如果安全存储器140被确定为违规的(compromised)，则CSA 120警告MLU 115，并且MLU 115删除本地媒体存储器125和密钥存储器130中的现有数据。另外，停止媒体播放器110对媒体内容的回放。在播放可以继续之前，MLU 115需要来自CSA 120的关于安全存储器140或受保护的应用程序环境160未违规的肯定响应。如果CSA 120确定安全存储装置140的完整性已经被破坏，或者如果CSA 120失去与证书存储装置135的联系，则证书存储装置135的内容也可以被删除。

[0077] MLU 115和CSA 120还被布置为彼此周期性地或连续地通信。如果MLU 115不能建立与CSA 120的连接，则MLU 115不能验证其在受保护的应用程序环境160中运行，因此MLU 115删除本地媒体存储器125和密钥存储器130中的相关媒体文件。此外，媒体内容媒体播放器110停止。当接收到来自CSA 120的肯定响应时，MLU 115可以恢复媒体内容的下载和处理，并且媒体播放器110可以继续回放。

[0078] 根据本发明的另一实施例，CSA 120请求来自PKI CA 145的认证证书，用于从密钥服务器150提取一个或多个解密密钥。认证证书具有定义在其期间相关媒体内容和解密密钥可以本地存储在客户端装置105中的到期日期/时间。媒体内容和解密密钥的有效期可以彼此相关联。当MLU115检测到媒体内容或解密密钥已过期时，它将停止将相关媒体内容串流传输到媒体播放器110并清除本地媒体存储器125中的该媒体内容。认证证书的到期日期可基于PKI CA 145的开放标准和认证证书，例如X.509。MLU115可以检查媒体内容和解密密钥或密钥的到期，即使客户端装置105离线或者在媒体内容的下载完成之后。有利地，当客户端装置105在线时，CSA 120可以利用可从互联网获得的公共时间服务来检查内部装置时钟，以确保装置时钟没有被手动调整。因此，所述数据串流传输方法可以进一步扩展到媒体内容租赁的服务。

[0079] 总之，利用在保护的运行时环境上使用安全存储的MLU 115和CSA120的组合操作，HLS串流传输被扩展为包括预下载和实时串流模式。此外，提取的媒体内容被保护免受非法复制，因为客户端装置向认证中心注册并且在密钥服务器上认证。操作可以对于媒体播放器完全透明。

[0080] 现在将描述根据本发明的另一实施例的媒体串流系统100的另一操作方法(图3中所示的方法300)。应当注意，图3示出了示例方法，并且在不脱离本发明的范围的情况下可以改变步骤的顺序。该方法还可以包括更少或更多数量的步骤。

[0081] 在步骤305，装置105接收播放包括一组媒体片段的媒体内容的请求。在步骤310，媒体定位器单元115确定与所请求的媒体内容有关的元数据是否存储在装置105的存储器

中，例如在本地媒体存储器125中。如果不是，则在步骤315，媒体定位器单元115从媒体服务器155(或者任何数量的媒体服务器155、156和157，如果所述元数据存储在多个服务器上)。如果元数据已经存储在装置105中，则媒体定位器单元115从存储器中提取元数据。一个或多个元数据文件包含视频片段的简要描述，并且对于每个片段，包含相应视频片段加密密钥的位置。

[0082] 一旦获得了元数据文件，在步骤320，媒体定位器单元115确定媒体片段是否存储在本地媒体存储器125中。如果没有，则在步骤325，媒体定位器单元115从媒体服务器155(或者从多个媒体服务器155、156和157，如果媒体片段分布在多个服务器上)下载(加密的)媒体片段。一旦媒体片段被下载，在步骤326，装置105使用装置特定的或基于装置的加密密钥来加密媒体片段。可以使用本领域中已知的技术在装置105处生成装置特定的加密密钥。因为媒体片段已经被加密，所以(已经加密的)媒体片段的加密导致双重加密的媒体片段。注意，如果在步骤320发现媒体片段存储在本地媒体存储器125中，则媒体片段将已经经历了该双重加密。一旦发生了基于装置的加密，双重加密的媒体片段可以存储在本地媒体存储125中以备将来使用。媒体片段的这种双重加密确保了想要播放媒体片段的任何未认证装置将不能这样做，因为它们不具有用于加密媒体片段的相同的装置特定的加密密钥。

[0083] 在步骤330，元数据被更新以指向本地存储的用于由媒体播放器110回放的双重加密的媒体片段。为了实现双重加密的媒体片段的回放，在步骤335，装置105使用装置特定加密密钥来解密双重加密的媒体片段，以便再现加密的媒体片段。在步骤340，客户端安全代理120从认证证书服务器145(其也可以称为访问控制服务器)请求认证令牌。所请求的认证令牌从认证证书服务器145发送到装置105。在步骤350，装置105使用元数据来确定媒体片段加密密钥在密钥服务器150中的位置。认证令牌允许装置105在密钥服务器150上认证。通过使用认证令牌和元数据，装置105从密钥服务器150请求必要的媒体片段加密密钥，并接收返回的所述密钥。最后，在步骤360，装置105使用媒体片段加密密钥来完全解密加密的媒体片段。完全解密后，媒体片段现在准备好在媒体播放器110上回放。

[0084] 注意，如果在本地媒体存储器125中没有找到所请求的媒体片段，则该过程可以以在线串流传输模式操作，由此媒体片段被连续地下载(步骤325)、双重加密(步骤336)、存储在本地媒体存储器、并且被双重解密用于回放(步骤335-360)。或者，在预下载模式中，所请求的媒体片段可能已经被存储在本地媒体存储器125中，在这种情况下不需要下载，并且也不需要双重加密，因为存储的媒体片段已经预先下载。如果媒体片段存在于装置105的存储器中，但装置105不是原始的下载装置，例如，媒体片段已经从另一个装置复制，然后当媒体播放器尝试解密媒体片段时，将会失败，因为它不能产生由原始下载装置产生的相同的装置特定的加密密钥。

[0085] 装置105还可以以混合模式操作，由此一些媒体片段预先下载在啊啊装置的存储器上，并且一些媒体片段在装置存储器上未找到。在这种情况下，该方法沿着图3的串流程图的两个分支操作。

[0086] 媒体定位器单元115可以在运行时切换模式，例如从混合模式到预下载模式或从在线串流模式到混合模式等，而不影响回放。

[0087] 在具有多核处理器的装置上，可以针对不同的媒体片段并行运行不同的步骤。

[0088] 虽然已经结合各种实施例描述了本发明，但是应当理解，本发明不限于这些实施

例，并且这些实施例的改变、修改和变化可以由本领域技术人员执行而不脱离本发明的范围。例如，媒体定位器单元和客户端安全代理可以实现为被设置在计算机或处理器上运行的软件，所述计算机或处理器被配置为执行所述软件。

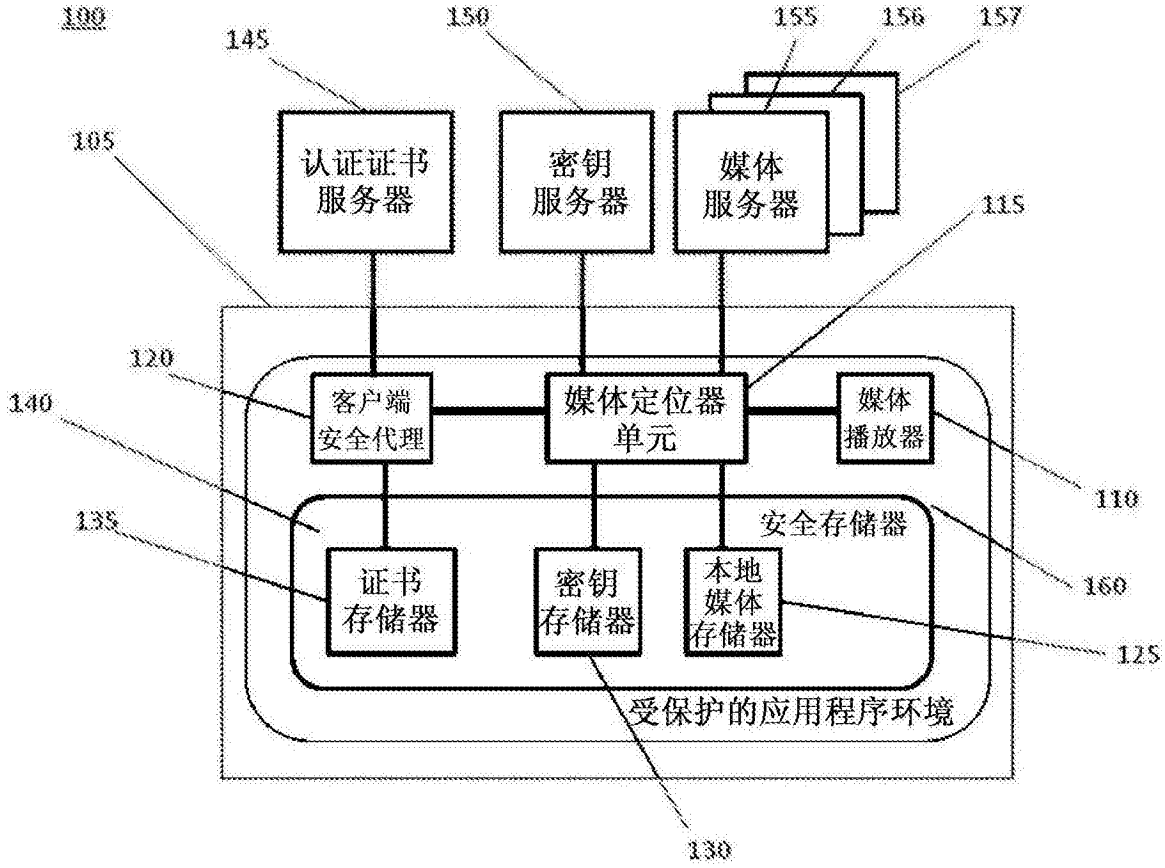

100
145
150
155
156
157
105
认证证书
服务器
密钥
服务器
媒体
服务器
115
120
140
客户端
安全代理
媒体定位器
单元
媒体
播放器
110
135
安全存储器
160
证书
存储器
密钥
存储器
本地
媒体
存储器
125
受保护的应用程序环境
130

图1

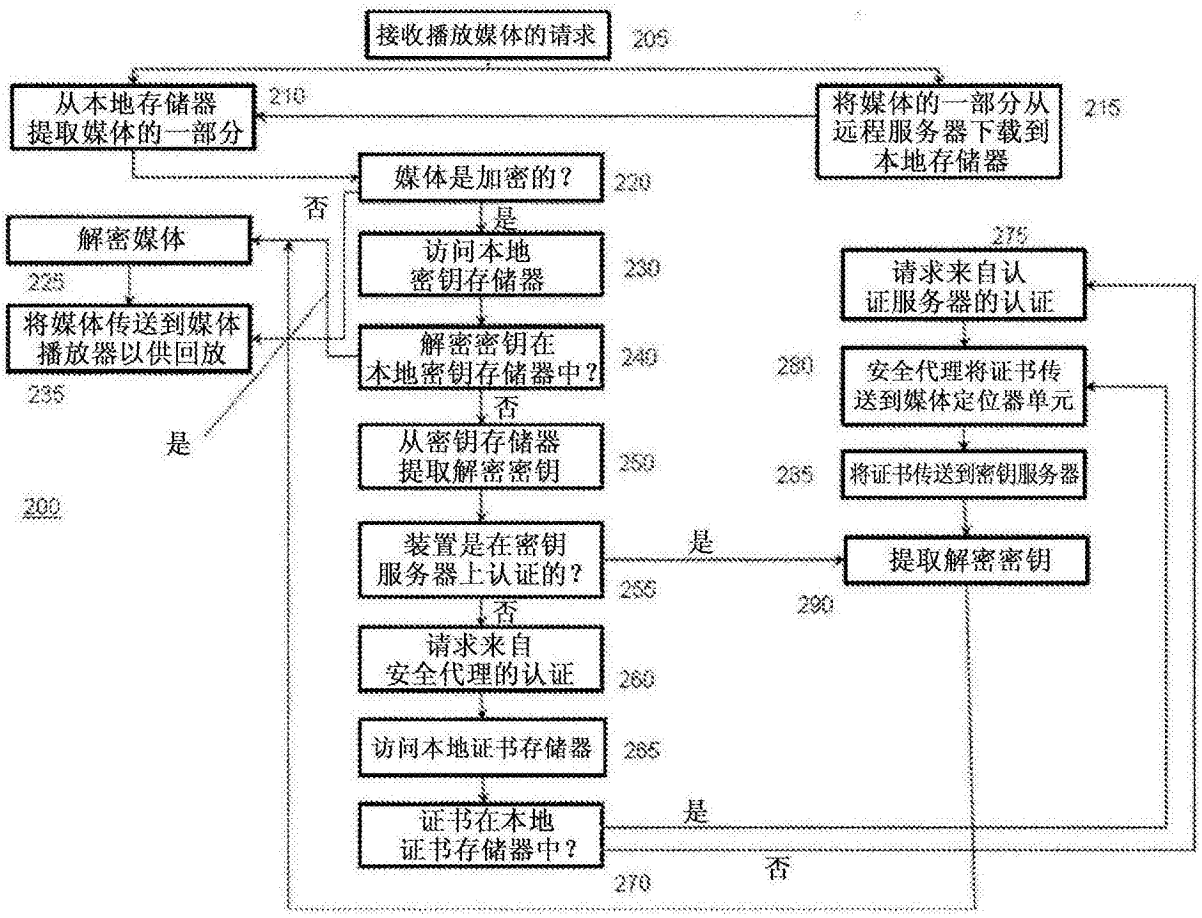

接收播放媒体的请求
205
从本地存储器提取媒体的一部分
210
将媒体的一部分从远程服务器下载到本地存储器
215
媒体是加密的？
220
否
是
解密媒体
225
将媒体传送到媒体播放器以供回放
235
是
200
访问本地密钥存储器
230
解密密钥在本地密钥存储器中？
240
否
从密钥存储器提取解密密钥
250
装置是在密钥服务器上认证的？
255
是
否
请求来自安全代理的认证
260
访问本地证书存储器
265
证书在本地证书存储器中？
270
是
否
275
请求来自认证服务器的认证
280
安全代理将证书传送到媒体定位器单元
285
将证书传送到密钥服务器
290
提取解密密钥

图2

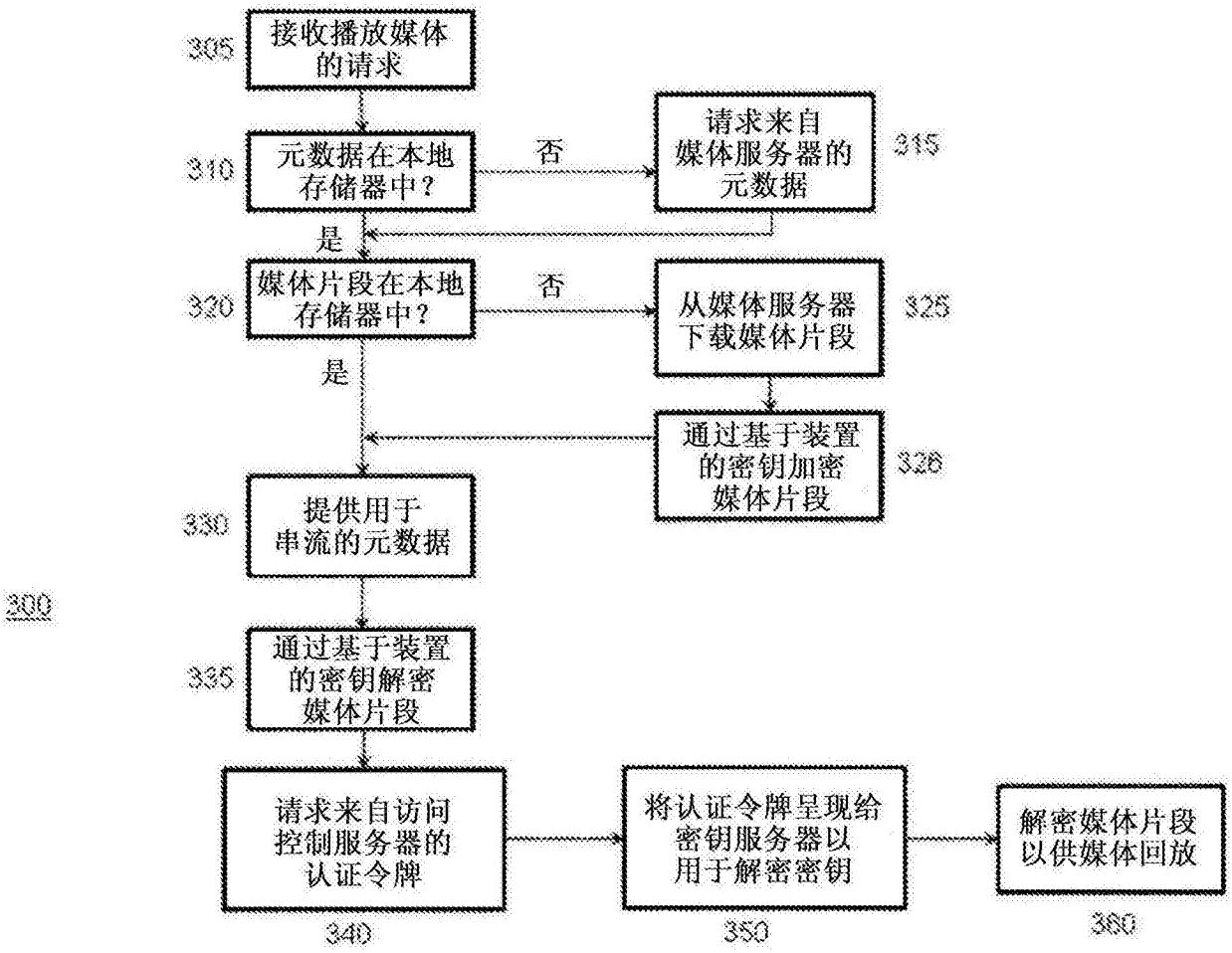

305
接收播放媒体的请求
310
元数据在本地存储器中？
否
315
请求来自媒体服务器的元数据
是
320
媒体片段在本地存储器中？
否
325
从媒体服务器下载媒体片段
是
326
通过基于装置的密钥加密媒体片段
330
提供用于串流的元数据
300
335
通过基于装置的密钥解密媒体片段
340
请求来自访问控制服务器的认证令牌
350
将认证令牌呈现给密钥服务器以用于解密密钥
380
解密媒体片段以供媒体回放

图3