

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 1 月 26 日 (26.01.2017)



(10) 国际公布号
WO 2017/012419 A1

- (51) 国际专利分类号:
H04N 21/4408 (2011.01)
- (21) 国际申请号: PCT/CN2016/084280
- (22) 国际申请日: 2016 年 6 月 1 日 (01.06.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510428361.0 2015 年 7 月 20 日 (20.07.2015) CN
- (71) 申请人: 深圳 TCL 数字技术有限公司 (SHENZHEN TCL DIGITAL TECHNOLOGY LTD.) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路鲤鱼门街一号前海深港合作区管理局综合办公楼 A 栋 201 室(入驻深圳市前海商务秘书有限公司), Guangdong 518054 (CN)。
- (72) 发明人: 徐坤鹏 (XU, Kunpeng); 中国广东省深圳市前海深港合作区前湾一路鲤鱼门街一号前海深港合作区管理局综合办公楼 A 栋 201 室(入驻深圳市前海商务秘书有限公司), Guangdong 518054 (CN)。
刘锋 (LIU, Feng); 中国广东省深圳市前海深港合作区前湾一路鲤鱼门街一号前海深港合作区管理局综合办公楼 A 栋 201 室(入驻深圳市前海商务秘书有限公司), Guangdong 518054 (CN)。
- (74) 代理人: 深圳市世纪恒程知识产权代理事务所 (CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区南山大道 3838 号设计产业园金栋二层 210-212 (原南头城工业村 11 栋), Guangdong 518052 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[见续页]

(54) Title: STREAM MEDIA DECRYPTION METHOD AND DEVICE

(54) 发明名称: 流媒体解密方法及装置

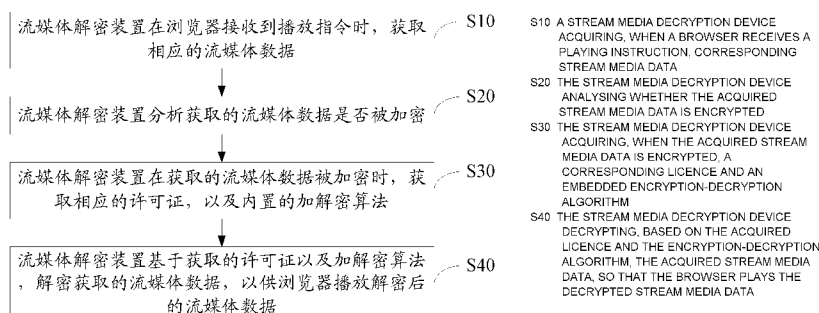


图 1

(57) Abstract: Disclosed is a stream media decryption method. A stream media decryption device is embedded in a browser for running. The stream media decryption method comprises: the stream media decryption device acquiring, when the browser receives a playing instruction, corresponding stream media data; the stream media decryption device analysing whether the stream media data is encrypted; the stream media decryption device acquiring, when the stream media data is encrypted, a corresponding licence and a built-in encryption-decryption algorithm; and the stream media decryption device decrypting, based on the acquired licence and the encryption-decryption algorithm, the stream media data, so that the browser plays the decrypted stream media data. Also disclosed is a stream media decryption device. The present invention can improve the efficiency for decrypting stream media.

(57) 摘要: 本发明公开了一种流媒体解密方法, 将流媒体解密装置内嵌于浏览器运行, 所述流媒体解密方法包括: 所述流媒体解密装置在所述浏览器接收到播放指令时, 获取相应的流媒体数据; 所述流媒体解密装置分析所述流媒体数据是否被加密; 所述流媒体解密装置在所述流媒体数据被加密时, 获取相应的许可证, 以及内置的加解密算法; 所述流媒体解密装置基于获取的所述许可证以及所述加解密算法, 解密所述流媒体数据, 以供浏览器播放解密后的流媒体数据。本发明还公开了一种流媒体解密装置。本发明能够提高解密流媒体的效率。



WO 2017/012419 A1



(84) **指定国** (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ,

CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

流媒体解密方法及装置

[1] 技术领域

[2] 本发明涉及互联网技术领域，尤其涉及流媒体解密方法及装置。

[3] 背景技术

[4] 在互联网技术越来越普及的今天，数字化信息已成为主流传播载体，但数字化信息传播的特点，不利于版权人版权的保护。所以，必须要有一种技术，可以将数字化的文字、音视频文件进行加密处理，针对符合条件的用户，可以得到一个解密该文件的许可证。此种技术以目前微软提供的DRM技术为主流技术，但针对已加密媒体文件的解密方法有多种，各厂商有不同的方式，主要通过浏览器DRM插件状态存在。播放器请求流媒体数据后，解析头信息发现有加密，此时，浏览器会调用DRM插件发送请求以获取许可证，得到许可证后，DRM插件会对播放器后续下载的流媒体数据进行相应的解密处理，解密完成后，把解密后的流媒体数据发送给播放器进行播放。由于流媒体数据从获取到解密需要在浏览器、播放器以及DRM插件中流转，导致现有技术中解密流媒体的效率较低。

[5] 发明内容

[6] 本发明的主要目的在于提供一种流媒体解密方法及装置，旨在提高解密流媒体的效率。

[7] 为实现上述目的，本发明将流媒体解密装置内嵌于浏览器运行，所述流媒体解密方法包括以下步骤：

[8] 所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据；

[9] 所述流媒体解密装置分析所述流媒体数据是否被加密；

[10] 所述流媒体解密装置在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；

[11] 所述流媒体解密装置分析获取的所述许可证是否完整；

- [12] 在所述许可证完整时,所述流媒体解密装置基于获取的所述许可证以及所述加解密算法,解密所述流媒体数据;
- [13] 所述流媒体解密装置将解密后的流媒体数据发送至播放器进行解码处理,并通过浏览器加载呈现解码后的流媒体数据。
- [14] 本发明还提供了一种流媒体解密方法,该流媒体解密方法包括以下步骤:
- [15] 所述流媒体解密装置在所述浏览器接收到播放指令时,获取相应的流媒体数据;
- [16] 所述流媒体解密装置分析所述流媒体数据是否被加密;
- [17] 所述流媒体解密装置在所述流媒体数据被加密时,获取相应的许可证,以及内置的加解密算法;
- [18] 所述流媒体解密装置基于获取的所述许可证以及所述加解密算法,解密所述流媒体数据,以供浏览器播放解密后的流媒体数据。
- [19] 优选地,所述流媒体解密装置基于获取的所述许可证和所述加解密算法,解密所述流媒体数据,以供浏览器播放解密后的流媒体数据的步骤之后,所述流媒体解密方法,还包括:
- [20] 所述流媒体解密装置将解密后的流媒体数据发送至播放器进行解码处理,并通过浏览器加载呈现解码后的流媒体数据。
- [21] 优选地,所述流媒体解密装置基于获取的所述许可证和所述加解密算法,解密所述流媒体数据,以供浏览器播放解密后的流媒体数据的步骤之前,所述流媒体解密方法,还包括:
- [22] 所述流媒体解密装置分析获取的所述许可证是否完整;
- [23] 在所述许可证完整时,执行所述流媒体解密装置基于获取的所述许可证和所述加解密算法,解密所述流媒体数据,以供浏览器播放解密后的流媒体数据的步骤。
- [24] 优选地,所述流媒体解密装置分析获取的所述许可证是否完整的步骤之后,所述流媒体解密方法,还包括:
- [25] 在所述许可证不完整时,所述流媒体解密装置重新获取相应的许可证,直至获取到完整的许可证。

- [26] 优选地，所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据的步骤之前，所述流媒体解密方法，还包括：
- [27] 所述流媒体解密装置在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。
- [28] 此外，为实现上述目的，本发明还提供一种流媒体解密装置，所述流媒体解密装置内嵌于浏览器运行，包括：
- [29] 流媒体获取模块，用于在所述浏览器接收到播放指令时，获取相应的流媒体数据；
- [30] 第一分析模块，用于分析所述流媒体数据是否被加密；
- [31] 加密信息获取模块，用于在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；
- [32] 解密模块，用于基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。
- [33] 优选地，所述流媒体解密装置还包括播放模块，用于将解密后的流媒体数据发送至播放器进行解码处理，并通过浏览器加载呈现解码后的流媒体数据。
- [34] 优选地，所述流媒体解密装置，还包括第二分析模块，用于分析获取的所述许可证是否完整；
- [35] 所述解密模块还用于在所述许可证完整时，基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。
- [36] 优选地，所述加密信息获取模块，还用于在所述许可证不完整时，重新获取相应的许可证，直至获取到完整的许可证。
- [37] 优选地，所述流媒体解密装置，还包括缓存区划分模块，用于在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。
- [38] 优选地，所述流媒体获取模块，还用于解析所述播放指令以获取流媒体内容发布服务器信息，并生成流媒体数据获取请求；将生成的所述流媒体数据获取请求发送至所述流媒体内容发布服务器信息对应的流媒体内容发布服务器，以供流媒体内容发布服务器根据接收到的流媒体数据获取请求返回相应的流媒体数

据。

[39] 本发明通过将流媒体解密装置内嵌于浏览器，所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据；分析所述流媒体数据是否被加密；在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。相较于现有技术，浏览器无需调用额外的DRM插件，避免了流媒体数据在浏览器以及DRM插件之间的重复流转，从而本发明能够提高解密流媒体的效率。

[40] 附图说明

[41] 图1为本发明流媒体解密方法第一实施例的流程示意图；

[42] 图2为本发明流媒体解密方法第二实施例的流程示意图；

[43] 图3为本发明流媒体解密方法第三实施例的流程示意图；

[44] 图4为本发明流媒体解密装置第一实施例的功能模块示意图；

[45] 图5为本发明流媒体解密装置第二实施例的功能模块示意图；

[46] 图6为本发明流媒体解密装置第三实施例的功能模块示意图。

[47] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

[48] 具体实施方式

[49] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[50] 本发明提供一种流媒体解密方法，流媒体解密装置内嵌于浏览器运行，参照图1，在本发明流媒体解密方法的第一实施例中，所述流媒体解密方法包括以下步骤：

[51] S10，所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据；

[52] 需要说明的是，本发明目的的实现在于将流媒体解密装置内嵌于浏览器，并通过流媒体解密装置实现现有DRM插件的功能（如加密判读、许可证获取以及解密等）。内置有流媒体解密装置的浏览器无需额外加载DRM插件，自身即可完成从流媒体数据获取到流媒体数据解密播放的整个过程。具体地，在软件层面

，将流媒体解密装置代码添加至浏览器内核代码中，以实现流媒体解密装置的内嵌。

- [53] 本实施例中，所述流媒体解密装置在所述浏览器接收到播放指令时，解析所述播放指令以获取流媒体内容发布服务器信息（例如，流媒体内容发布服务器的IP地址），并生成流媒体数据获取请求；将生成的所述流媒体数据获取请求发送至所述流媒体内容发布服务器信息对应的流媒体内容发布服务器，以供流媒体内容发布服务器根据接收到的流媒体数据获取请求返回相应的流媒体数据；在接收到流媒体内容发布服务器返回的流媒体数据后，将所述流媒体数据存储至浏览器的数据缓存区中。
- [54] S20，所述流媒体解密装置分析所述流媒体数据是否被加密；
- [55] 所述流媒体解密装置在获取到流媒体数据后，分析所述流媒体数据是否被加密，具体地，解析所述流媒体数据的头文件，在所述头文件中携带有加密信息时，识别所述流媒体数据被加密；在所述头文件中未携带有加密信息时，识别所述流媒体数据未被加密。其中，所述加密信息包括流媒体数据采用的加解密算法，以及许可证颁发服务器等信息。
- [56] S30，所述流媒体解密装置在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；
- [57] 若所述流媒体数据被加密，则所述流媒体解密装置从所述加密信息中解析出所述流媒体数据采用的加解密算法，以及许可证颁发服务器信息（例如，许可证颁发服务器的IP地址）；根据所述许可证颁发服务器信息生成许可证获取请求，并将生成的所述许可证获取请求发送至所述许可证颁发服务器信息对应的许可证颁发服务器，以供所述许可证颁发服务器返回相应的许可证；在接收到所述许可证颁发服务器返回的许可证后，将所述许可证存储至浏览器的数据缓存区中，并与前述流媒体数据关联。
- [58] S40，所述流媒体解密装置基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。
- [59] 在获取到许可证以及内置的加解密算法后，基于获取的所述许可证以及所述加解密算法，解密与所述许可证关联的流媒体数据，以供浏览器播放解密后的流

媒体数据。例如，所述流媒体解密装置获取到的加解密算法为DES算法，则基于获取的所述许可证以及DES算法，解密与所述许可证关联的流媒体数据。

[60] 本实施例提出的流媒体解密方法，将流媒体解密装置内嵌于浏览器，所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据；分析所述流媒体数据是否被加密；在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。相较于现有技术，浏览器无需调用额外的DRM插件，避免了流媒体数据在浏览器以及DRM插件之间的重复流转，从而本发明能够提高解密流媒体的效率。

[61] 进一步地，基于第一实施例，提出本发明流媒体解密方法的第二实施例，参照图2，在本实施例中，S40之后，所述流媒体解密方法，还包括：

[62] S50，所述流媒体解密装置将解密后的流媒体数据发送至播放器进行解码处理，并通过浏览器加载呈现解码后的流媒体数据。

[63] 需要说明的是，浏览器并不具备解码流媒体数据的能力，在播放时，需要调用本地播放器进行解码，然后通过浏览器将解码后的流媒体数据呈现给用户。本实施例中，所述流媒体解密装置在完成对流媒体数据的解密后，将解密后的流媒体数据发送至用户终端本地的播放器进行解码处理，并通过浏览器加载呈现解码后的流媒体数据。例如，当用户在浏览器页面中点击音视频链接后，浏览器直接在页面中为用户呈现相应的音视频，如播放音乐、电影等。

[64] 进一步地，基于第一实施例，提出本发明流媒体解密方法的第三实施例，参照图3，在本实施例中，S40之前，所述流媒体解密方法，还包括：

[65] S60，所述流媒体解密装置分析获取的所述许可证是否完整；若是，则转入执行S40。

[66] 需要说明的是，网络是一个动态的网络设备的集合，包括服务器、路由器、交换机以及用户终端等，可能在某一时间段，由于某种原因造成了特定网络线路的不可达；或者是在某一时间段，某网络设备接收到超过处理能力的大量网络包，造成了数据处理的超时，网络包丢失。而在网络传输过程中，许可证是以多个网络包的形式构成的，任一网络包丢失都会造成最终获取的许可证不完整

，从而造成相应的流媒体数据无法解密，进而导致获取的流媒体数据无法播放，带来不好的用户体验。有鉴于此，本实施例中，所述流媒体解密装置在获取到许可证后，首先分析获取的所述许可证是否完整，若是则基于获取的所述许可证以及内置的加解密算法，对相应的流媒体数据进行解密；否则丢弃获取的所述许可证。

[67] 例如，所述流媒体解密装置在获取到许可证后，通过分析所述许可证的头信息得出该许可证的大小应为512Kb，若获取的所述许可证的实际大小为512Kb，则识别获取的所述许可证完整；若获取的所述许可证的实际大小不为512Kb（网络包丢失），则识别获取的所述许可证不完整。

[68] 基于第三实施例，提出本发明流媒体解密方法的第四实施例，在本实施例中，S60之后，所述流媒体解密方法，还包括：

[69] 在所述许可证不完整时，所述流媒体解密装置重新获取相应的许可证，直至获取到完整的许可证。

[70] 容易理解的是，若所述流媒体解密装置获取的许可证不完整，将会导致流媒体数据不能正常解密，进而导致流媒体数据不能正常播放，影响用户体验。本实施例中，为避免前述问题，所述流媒体解密装置在识别所述许可证不完整时，重新获取相应的许可证，直至获取到完整的许可证，以使得获取的流媒体数据能够正常播放。即所述流媒体解密装置每获取一次许可证，进行许可证完整性的判别，是则进行解密操作，否则丢弃获取的许可证，并再次获取相应的许可证。

[71] 基于上述任一实施例，提出本发明流媒体解密方法的第五实施例，在本实施例中，S10之前，所述流媒体解密方法，还包括：

[72] 所述流媒体解密装置在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。

[73] 需要说明的是，现有技术中，当用户通过浏览器播放流媒体音视频时，浏览器仅获取到流媒体数据的下载地址，然后播放器加载浏览器获取的流媒体数据下载地址下载流媒体数据；播放器在下载流媒体数据后，将下载的流媒体数据发送至DRM插件进行解密；DRM插件在完成对流媒体数据的解密后，将解密后

的流媒体数据返回至播放器；播放器对DRM插件返回的流媒体数据进行解码处理，并将解码后的流媒体数据返回至浏览器，以供浏览器将解码后的流媒体数据呈现给用户。

[74] 本实施例进一步通过在浏览器划分数据缓存区，并由浏览器完成流媒体数据的下载，以及解密；然后将解密后的流媒体数据发送至播放器解码，并接收播放器返回的解码后的流媒体数据，将之呈现给用户，减少了现有的通讯流程，提高了流媒体数据的播放效率；同时，用户能够直接通过浏览器页面进行播放控制（例如，播放、暂停、停止以及音量调整等），带来更好的用户体验。

[75] 本发明还提供一种流媒体解密装置，所述流媒体解密装置内嵌于浏览器运行，参照图4，在本发明流媒体解密装置的第一实施例中，本发明提供一种流媒体解密装置包括：

[76] 流媒体获取模块10，用于在所述浏览器接收到播放指令时，获取相应的流媒体数据；

[77] 需要说明的是，本发明目的的实现在于将流媒体解密装置内嵌于浏览器，并通过流媒体解密装置实现现有DRM插件的功能（如加密判读、许可证获取以及解密等）。内置有流媒体解密装置的浏览器无需额外加载DRM插件，自身即可完成从流媒体数据获取到流媒体数据解密播放的整个过程。具体地，在软件层面，将流媒体解密装置代码添加至浏览器内核代码中，以实现流媒体解密装置的内嵌。

[78] 本实施例中，流媒体获取模块10在所述浏览器接收到播放指令时，解析所述播放指令以获取流媒体内容发布服务器信息（例如，流媒体内容发布服务器的IP地址），并生成流媒体数据获取请求；将生成的所述流媒体数据获取请求发送至所述流媒体内容发布服务器信息对应的流媒体内容发布服务器，以供流媒体内容发布服务器根据接收到的流媒体数据获取请求返回相应的流媒体数据；在接收到流媒体内容发布服务器返回的流媒体数据后，将所述流媒体数据存储至浏览器的数据缓存区中。

[79] 第一分析模块20，用于分析所述流媒体数据是否被加密；

[80] 在流媒体获取模块10获取到流媒体数据后，第一分析模块20分析所述流媒体数

据是否被加密，具体地，第一分析模块20解析所述流媒体数据的头文件，在所述头文件中携带有加密信息时，第一分析模块20识别所述流媒体数据被加密；在所述头文件中未携带有加密信息时，第一分析模块20识别所述流媒体数据未被加密。其中，所述加密信息包括流媒体数据采用的加解密算法，以及许可证颁发服务器等信息。

[81] 加密信息获取模块30，用于在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；

[82] 若所述流媒体数据被加密，则加密信息获取模块30从所述加密信息中解析出所述流媒体数据采用的加解密算法，以及许可证颁发服务器信息（例如，许可证颁发服务器的IP地址）；根据所述许可证颁发服务器信息生成许可证获取请求，并将生成的所述许可证获取请求发送至所述许可证颁发服务器信息对应的许可证颁发服务器，以供所述许可证颁发服务器返回相应的许可证；在接收到所述许可证颁发服务器返回的许可证后，将所述许可证存储至浏览器的数据缓存区中，并与前述流媒体数据关联。

[83] 解密模块40，用于基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。

[84] 在加密信息获取模块30获取到许可证以及内置的加解密算法后，解密模块40基于加密信息获取模块30获取的所述许可证以及所述加解密算法，解密与所述许可证关联的流媒体数据，以供浏览器播放解密后的流媒体数据。例如，所述加密信息获取模块30获取到的加解密算法为DES算法，解密模块40基于加密信息获取模块30获取的所述许可证以及DES算法，解密与所述许可证关联的流媒体数据。

[85] 本实施例提出的流媒体解密装置，内嵌于浏览器，所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据；分析所述流媒体数据是否被加密；在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。相较于现有技术，浏览器无需调用额外的DRM插件，避免了流媒体数据在浏览器以及DRM插件之间的重复流转，从而本发

明能够提高解密流媒体的效率。

[86] 进一步地，基于第一实施例，提出本发明流媒体解密装置的第二实施例，参照图5，在本实施例中，所述流媒体解密装置还包括播放模块50，用于将解密后的流媒体数据发送至播放器进行解码处理，并通过浏览器加载呈现解码后的流媒体数据。

[87] 需要说明的是，浏览器并不具备解码流媒体数据的能力，在播放时，需要调用本地播放器进行解码，然后通过浏览器将解码后的流媒体数据呈现给用户。本实施例中，在解密模块40完成对流媒体数据的解密后，播放模块50将解密后的流媒体数据发送至用户终端本地的播放器进行解码处理，并通过浏览器加载呈现解码后的流媒体数据。例如，当用户在浏览器页面中点击音视频链接后，浏览器直接在页面中为用户呈现相应的音视频，如播放音乐、电影等。

[88] 进一步地，基于第一实施例，提出本发明流媒体解密装置的第三实施例，参照图6，在本实施例中，所述流媒体解密装置，还包括第二分析模块60，用于分析获取的所述许可证是否完整；

[89] 所述解密模块40还用于在所述许可证完整时，基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。

[90] 需要说明的是，网络是一个动态的网络设备的集合，包括服务器、路由器、交换机以及用户终端等，可能在某一时间段，由于某种原因造成了特定网络线路的不可达；或者是在某一时间段，某网络设备接收到超过处理能力的大量网络包，造成了数据处理的超时，网络包丢失。而在网络传输过程中，许可证是以多个网络包的形式构成的，任一网络包丢失都会造成最终获取的许可证不完整，从而造成相应的流媒体数据无法解密，进而导致获取的流媒体数据无法播放，带来不好的用户体验。有鉴于此，本实施例中，在加密信息获取模块30获取到许可证后，第二分析模块60首先分析加密信息获取模块30获取的所述许可证是否完整，若是，解密模块40则基于获取的所述许可证对相应的流媒体数据进行解密；否则第二分析模块60丢弃获取的所述许可证。

[91] 例如，在加密信息获取模块30获取到许可证后，第二分析模块60通过分析所述许可证的头信息得出该许可证的大小应为512Kb，若加密信息获取模块30获取的

所述许可证的实际大小为512Kb，则第二分析模块60识别获取的所述许可证完整；若加密信息获取模块30获取的所述许可证的实际大小不为512Kb（网络包丢失），则第二分析模块60识别获取的所述许可证不完整。

[92] 基于第三实施例，提出本发明流媒体解密装置的第四实施例，在本实施例中，所述加密信息获取模块30，还用于在所述许可证不完整时，重新获取相应的许可证，直至获取到完整的许可证。

[93] 容易理解的是，若加密信息获取模块30获取的许可证不完整，将会导致流媒体数据不能正常解密，进而导致流媒体数据不能正常播放，影响用户体验。本实施例中，为避免前述问题，在第二分析模块60识别所述许可证不完整时，加密信息获取模块30重新获取相应的许可证，直至获取到完整的许可证，以使得获取的流媒体数据能够正常播放。即所述加密信息获取模块30每获取一次许可证，所述第二分析模块60进行许可证完整性的判别，是则供所述解密模块40进行解密操作，否则丢弃获取的许可证，并由所述加密信息获取模块30再次获取相应的许可证。

[94] 基于上述任一实施例，提出本发明流媒体解密装置的第五实施例，在本实施例中，所述流媒体解密装置，还包括缓存区划分模块，用于在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。

[95] 需要说明的是，现有技术中，当用户通过浏览器播放流媒体音视频时，浏览器仅获取到流媒体数据的下载地址，然后播放器加载浏览器获取的流媒体数据下载地址下载流媒体数据；播放器在下载流媒体数据后，将下载的流媒体数据发送至DRM插件进行解密；DRM插件在完成对流媒体数据的解密后，将解密后的流媒体数据返回至播放器；播放器对DRM插件返回的流媒体数据进行解码处理，并将解码后的流媒体数据返回至浏览器，以供浏览器将解码后的流媒体数据呈现给用户。

[96] 本实施例进一步通过缓存区划分模块在浏览器划分数据缓存区，并由浏览器完成流媒体数据的下载，以及解密；然后将解密后的流媒体数据发送至播放器解码，并接收播放器返回的解码后的流媒体数据，将之呈现给用户，减少了现有

的通讯流程，提高了流媒体数据的播放效率；同时，用户能够直接通过浏览器页面进行播放控制（例如，播放、暂停、停止以及音量调整等），带来更好的用户体验。

- [97] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

权利要求书

- [权利要求 1] 一种流媒体解密方法，其特征在于，流媒体解密装置内嵌于浏览器运行，所述流媒体解密方法包括：
- 所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据；
- 所述流媒体解密装置分析所述流媒体数据是否被加密；
- 所述流媒体解密装置在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；
- 所述流媒体解密装置分析获取的所述许可证是否完整；
- 在所述许可证完整时，所述流媒体解密装置基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据；
- 所述流媒体解密装置将解密后的流媒体数据发送至播放器进行解码处理，并通过浏览器加载呈现解码后的流媒体数据。
- [权利要求 2] 一种流媒体解密方法，其特征在于，流媒体解密装置内嵌于浏览器运行，所述流媒体解密方法包括：
- 所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据；
- 所述流媒体解密装置分析所述流媒体数据是否被加密；
- 所述流媒体解密装置在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；
- 所述流媒体解密装置基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。
- [权利要求 3] 如权利要求2所述的流媒体解密方法，其特征在于，所述流媒体解密装置基于获取的所述许可证和所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据的步骤之后，所述流媒体解密方法，还包括：
- 所述流媒体解密装置将解密后的流媒体数据发送至播放器进行解码处理，并通过浏览器加载呈现解码后的流媒体数据。

- [权利要求 4] 如权利要求2所述的流媒体解密方法，其特征在于，所述流媒体解密装置基于获取的所述许可证和所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据的步骤之前，所述流媒体解密方法，还包括：
- 所述流媒体解密装置分析获取的所述许可证是否完整；
- 在所述许可证完整时，执行所述流媒体解密装置基于获取的所述许可证和所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据的步骤。
- [权利要求 5] 如权利要求4所述的流媒体解密方法，其特征在于，所述流媒体解密装置分析获取的所述许可证是否完整的步骤之后，所述流媒体解密方法，还包括：
- 在所述许可证不完整时，所述流媒体解密装置重新获取相应的许可证，直至获取到完整的许可证。
- [权利要求 6] 如权利要求2所述的流媒体解密方法，其特征在于，所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据的步骤之前，所述流媒体解密方法，还包括：
- 所述流媒体解密装置在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。
- [权利要求 7] 如权利要求3所述的流媒体解密方法，其特征在于，所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据的步骤之前，所述流媒体解密方法，还包括：
- 所述流媒体解密装置在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。
- [权利要求 8] 如权利要求4所述的流媒体解密方法，其特征在于，所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据的步骤之前，所述流媒体解密方法，还包括：
- 所述流媒体解密装置在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。

- [权利要求 9] 如权利要求5所述的流媒体解密方法，其特征在于，所述流媒体解密装置在所述浏览器接收到播放指令时，获取相应的流媒体数据的步骤之前，所述流媒体解密方法，还包括：
所述流媒体解密装置在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。
- [权利要求 10] 如权利要求8所述的流媒体解密方法，其特征在于，所述流媒体解密装置分析获取的所述许可证是否完整的步骤之后，所述流媒体解密方法，还包括：
在所述许可证不完整时，所述流媒体解密装置重新获取相应的许可证，直至获取到完整的许可证。
- [权利要求 11] 一种流媒体解密装置，其特征在于，所述流媒体解密装置内嵌于浏览器运行，所述流媒体解密装置包括：
流媒体获取模块，用于在所述浏览器接收到播放指令时，获取相应的流媒体数据；
第一分析模块，用于分析所述流媒体数据是否被加密；
加密信息获取模块，用于在所述流媒体数据被加密时，获取相应的许可证，以及内置的加解密算法；
解密模块，用于基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放解密后的流媒体数据。
- [权利要求 12] 如权利要求11所述的流媒体解密装置，其特征在于，所述流媒体解密装置还包括播放模块，用于将解密后的流媒体数据发送至播放器进行解码处理，并通过浏览器加载呈现解码后的流媒体数据。
- [权利要求 13] 如权利要求11所述的流媒体解密装置，其特征在于，所述流媒体解密装置，还包括第二分析模块，用于分析获取的所述许可证是否完整；
所述解密模块还用于在所述许可证完整时，基于获取的所述许可证以及所述加解密算法，解密所述流媒体数据，以供浏览器播放

解密后的流媒体数据。

- [权利要求 14] 如权利要求13所述的流媒体解密装置，其特征在于，所述加密信息获取模块，还用于在所述许可证不完整时，重新获取相应的许可证，直至获取到完整的许可证。
- [权利要求 15] 如权利要求11所述的流媒体解密装置，其特征在于，所述流媒体解密装置，还包括缓存区划分模块，用于在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。
- [权利要求 16] 如权利要求12所述的流媒体解密装置，其特征在于，所述流媒体解密装置，还包括缓存区划分模块，用于在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。
- [权利要求 17] 如权利要求13所述的流媒体解密装置，其特征在于，所述流媒体解密装置，还包括缓存区划分模块，用于在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。
- [权利要求 18] 如权利要求14所述的流媒体解密装置，其特征在于，所述流媒体解密装置，还包括缓存区划分模块，用于在浏览器划分数据缓存区，所述数据缓存区用于储存流媒体数据、许可证以及解密后的流媒体数据。
- [权利要求 19] 如权利要求17所述的流媒体解密装置，其特征在于，所述加密信息获取模块，还用于在所述许可证不完整时，重新获取相应的许可证，直至获取到完整的许可证。
- [权利要求 20] 如权利要求11所述的流媒体解密装置，其特征在于，所述流媒体获取模块，还用于解析所述播放指令以获取流媒体内容发布服务器信息，并生成流媒体数据获取请求；将生成的所述流媒体数据获取请求发送至所述流媒体内容发布服务器信息对应的流媒体内容发布服务器，以供流媒体内容发布服务器根据接收到的流媒体

数据获取请求返回相应的流媒体数据。

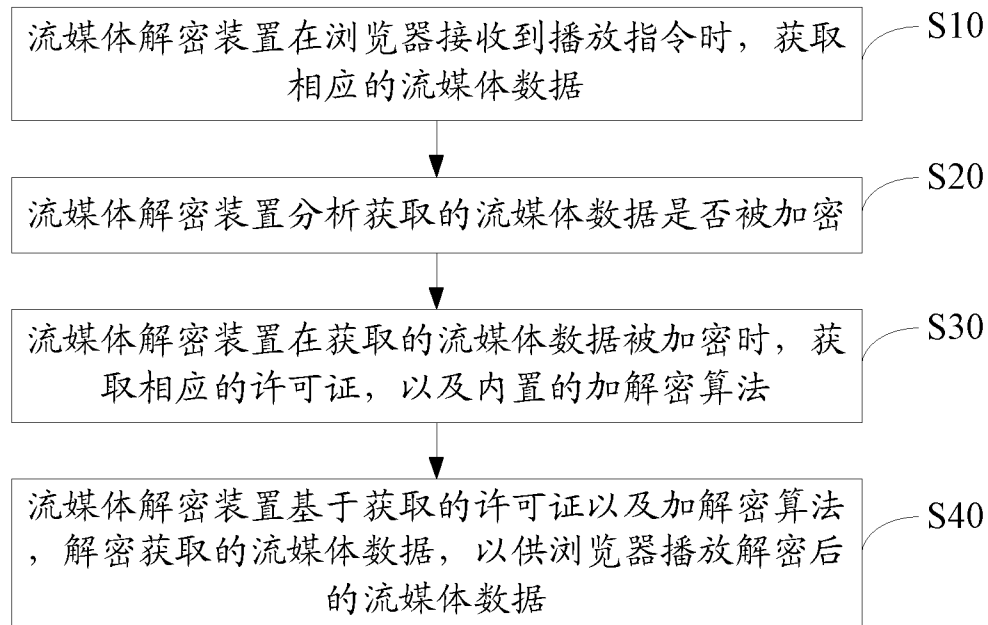


图 1

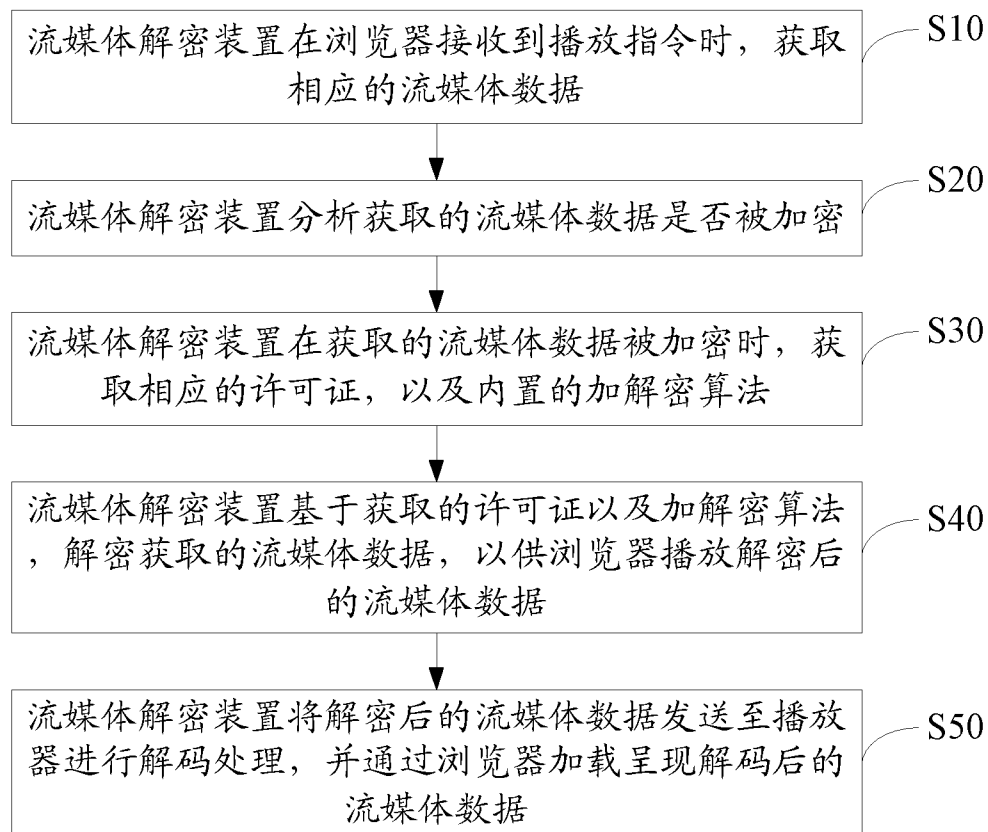


图 2

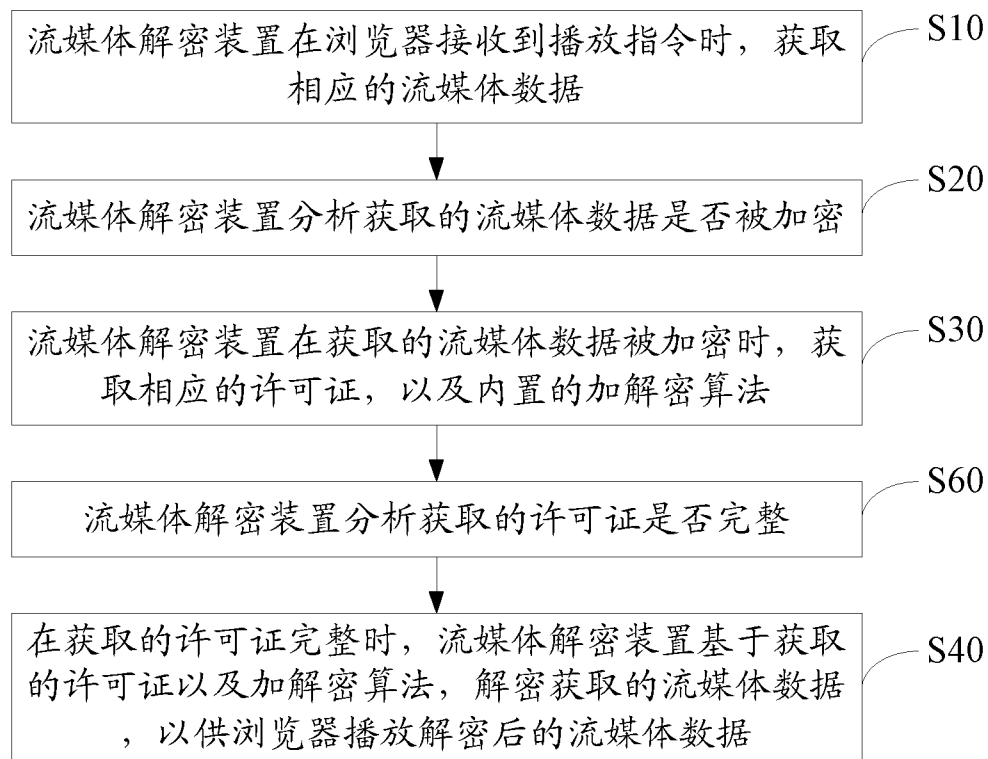


图 3



图 4

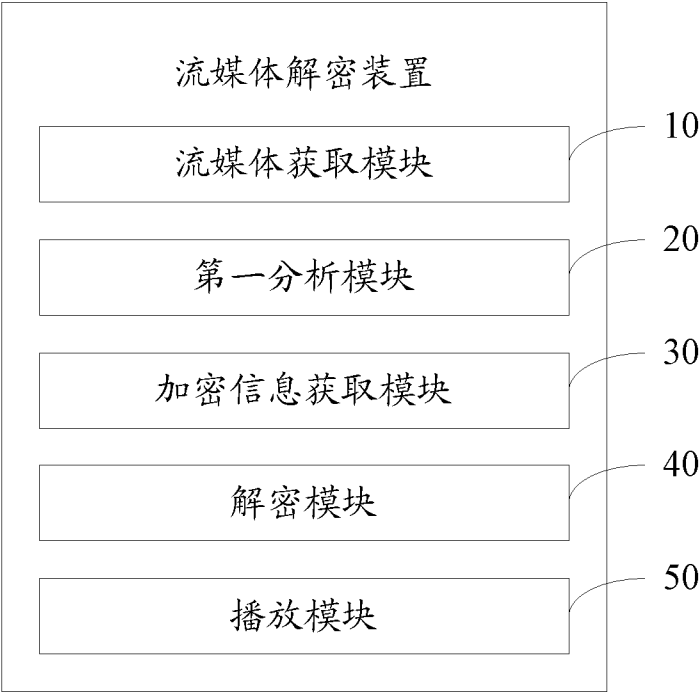


图 5



图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/084280

A. CLASSIFICATION OF SUBJECT MATTER

H04N 21/4408 (2011.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04N; H04W; H04L; H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: certificate, embedded, stream+ media, flow+ media, decrypt+, decipher+, safe+, DRM, digital rights manage+, licence?, integrity, browser?, built in

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105072488 A (TCL DIGITAL TECHNOLOGY (SHENZHEN) CO., LTD.), 18 November 2015 (18.11.2015), description, paragraphs [0037]-[0083]	1-20
Y	CN 102685592 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 19 September 2012 (19.09.2012), claims 1-4, and description, paragraphs [0019]-[0026]	1-20
Y	CN 1462940 A (TOMORROW STUDIO CO.), 24 December 2003 (24.12.2003), claims 1-14	1-20
Y	CN 104427358 A (NETFLIX INC.), 18 March 2015 (18.03.2015), abstract, claims 1-16, and description, paragraphs [0025]-[0030] and [0039]-[0041]	1-20
A	CN 102255886 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 23 November 2011 (23.11.2011), the whole document	1-20
A	US 7991156 B1 (SPRINT COMMUNICATIONS COMPANY L.P.), 02 August 2011 (02.08.2011), the whole document	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	
“A” document defining the general state of the art which is not considered to be of particular relevance	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“E” earlier application or patent but published on or after the international filing date	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	“&” document member of the same patent family

Date of the actual completion of the international search 04 August 2016 (04.08.2016)	Date of mailing of the international search report 24 August 2016 (24.08.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LIU, Cheng Telephone No.: (86-10) 010-62413853

International application No.
PCT/CN2016/084280

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2016/084280

A. 主题的分类

H04N 21/4408 (2011.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04N; H04W; H04L; H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNPAT, CNKI, WPI, EPODOC: 流媒体, 流式媒体, 解密, 安全, 数字版权保护, 许可证, 证书, 完整, 内置, 内嵌, 浏览器, stream+ media, flow+ media, decrypt+, decipher+, safe+, DRM, digital rights manage+, liscence?, integrity, browser?, built in

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 105072488 A (深圳TCL数字技术有限公司) 2015年 11月 18日 (2015 - 11 - 18) 说明书第[0037]-[0083]段	1-20
Y	CN 102685592 A (南京邮电大学) 2012年 9月 19日 (2012 - 09 - 19) 权利要求1-4, 说明书第[0019]-[0026]段	1-20
Y	CN 1462940 A (明日工作室股份有限公司) 2003年 12月 24日 (2003 - 12 - 24) 权利要求1-14	1-20
Y	CN 104427358 A (奈飞公司) 2015年 3月 18日 (2015 - 03 - 18) 摘要、权利要求1-16、说明书第[0025]-[0030]段、第[0039]-[0041]段	1-20
A	CN 102255886 A (南京邮电大学) 2011年 11月 23日 (2011 - 11 - 23) 全文	1-20
A	US 7991156 B1 (SPRINT COMMUNICATIONS COMPANY L.P.) 2011年 8月 2日 (2011 - 08 - 02) 全文	1-20

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 8月 4日

国际检索报告邮寄日期

2016年 8月 24日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

刘成

传真号 (86-10) 62019451

电话号码 (86-10) 010-62413853

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/084280

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	105072488	A	2015年 11月 18日	无			
CN	102685592	A	2012年 9月 19日	无			
CN	1462940	A	2003年 12月 24日	无			
CN	104427358	A	2015年 3月 18日	US	2015074818	A1	2015年 3月 12日
				EP	2846555	A1	2015年 3月 11日
CN	102255886	A	2011年 11月 23日	无			
US	7991156	B1	2011年 8月 2日	US	7382879	B1	2008年 6月 3日

表 PCT/ISA/210 (同族专利附件) (2009年7月)