(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 11 月 16 日 (16.11.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/193949 A1

(51) 国际专利分类号:
H04N 21/2389 (2011.01)

(21) 国际申请号: PCT/CN2017/083868

(22) 国际申请日: 2017 年 5 月 11 日 (11.05.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610309195.7 2016年5月11日 (11.05.2016) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

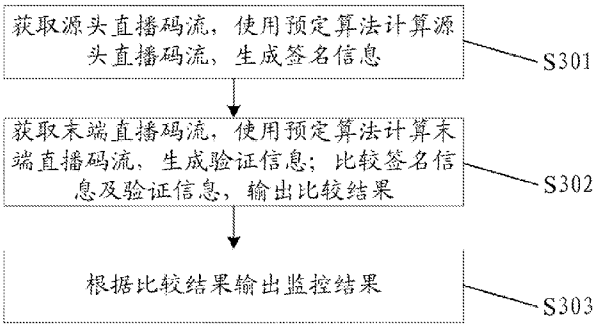
(72) 发明人: 陈正江 (CHEN, Zhengjiang); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 刘志军 (LIU, Zhijun); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 杨斌 (YANG, Bin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 贺镇海 (HE, Zhenhai); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 王雨 (WANG, Yu); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京品源专利代理有限公司 (BEYOND ATTORNEYS AT LAW); 中国北京市海淀区莲花池东路39号西金大厦6层, Beijing 100036 (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, DJ, 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, KH, KN, KP, KR, KW, 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,

(54) **Title:** CODE STREAM TAMPERING MONITORING METHOD AND DEVICE AND COMMUNICATION SYSTEM

(54) **发明名称**: 一种码流篡改监控方法、装置及通信系统



S301 Acquiring a source live broadcast code stream, calculating the source live broadcast code stream using a predetermined algorithm, and generating signature information

S302 Acquiring an end live broadcast code stream, calculating the end live broadcast code stream using a predetermined algorithm, and generating signature information; comparing the signature information and the verification information, and outputting a comparison result

S303 Outputting a monitoring result according to the comparison result

图 3

(57) **Abstract:** Disclosed are a code stream tampering monitoring method and device and a communication system. The method comprises: generating signature information according to a source live broadcast code stream; and generating verification information according to an end live broadcast code stream; comparing the signature information and the verification information, and outputting a comparison result; and outputting a monitoring result according to the comparison result. By means of the implementation of the present application, the tamper-proofing monitoring of a live broadcast code stream based on a digital signature mechanism can be achieved, and there is no need to deploy a dedicated DRM system, thereby solving the problem in the relevant technology that a DRM system needs to be deployed to realize tamper-resistant monitoring.

(57) **摘要**: 本申请公开了一种码流篡改监控方法、装置及通信系统，该方法包括：根据源头直播码流生成签名信息；并根据末端直播码流生成验证信息；比较签名信息及验证信息，输出比较结果；根据比较结果输出监控结果。通过本申请的实施，可以实现基于数字签名机制的直播码流防篡改的监控，不需要部署专用的DRM系统，解决了相关技术需要部署DRM系统才能实现防篡改监控的问题。

WO 2017/193949 A1

[见续页]

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。

(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))。

一种码流篡改监控方法、装置及通信系统

技术领域

本申请涉及通信领域，例如涉及一种码流篡改监控方法、装置及通信系统。

背景技术

直播服务是通过媒体服务器来提供的，用户通过个人的终端接收服务器中的直播码流以观看直播。但是在目前的网络环境中，暴露在公网上为用户提供直播服务的媒体服务器以及其发出的直播码流，存在网络环境安全风险高，由于直播码流是在公网上传输的，会存在攻击者非法篡改直播码流的内容，让用户观看到这些非法的内容，这些内容并不是服务商想提供给用户的。

为了保护媒体服务器的直播码流不被篡改，保障用户观看到正确的直播节目，为用户提供更好的服务，同时，为了保障运营商的合法权益，直播码流的防篡改技术成为目前各大厂商和运营商致力于研究和实施的重点，在相关技术中，为了防止这种情况的发生，通过在系统中部署 DRM（Digital Rights Management，内容数字版权加密保护技术）系统来防御对直播码流的非法篡改。图 1 示出了相关防篡改系统的结构示意图，如图 1 所示，整个防篡改系统分为 DRM 服务器和客户端 agent 两部分，相关技术中，DRM 系统可以实现基本的防篡改功能，然而，DRM 系统部署相对复杂，DRM 前端服务器串接在直播源和 CDN（Content Delivery Network，内容分发网络）之间，增加了可能出现故障的业务节点；同时，需要系统侧和终端侧配合才能实施，而国内运营商一般都没有部署 DRM 系统。

针对上述问题，提出一种码流篡改监控方法，以解决相关技术需要部署 DRM 系统才能实现防篡改监控的问题，是本领域技术人员亟待解决的技术问题。

发明内容

本公开提供了一种码流篡改监控方法、装置及通信系统，以解决相关技术需要部署 DRM 系统才能实现防篡改监控的问题。

本公开提供了一种码流篡改监控方法，其包括：

根据源头直播码流生成签名信息；并根据末端直播码流生成验证信息；

比较签名信息及验证信息，输出比较结果；

根据比较结果输出监控结果。

所述根据源头直播码流生成签名信息，可以包括：获取所述源头直播码流，使用预定算法计算所述源头直播码流，生成所述签名信息；

所述根据末端直播码流生成验证信息，可以包括：获取所述末端直播码流，使用所述预定算法计算所述末端直播码流，生成所述验证信息。

获取源头直播码流可以包括：从直播码流的直播源、和/或内容分发网络中心节点、和/或内容分发网络转码节点，获取直播码流的副本，作为源头直播码流。

获取末端直播码流可以包括：从直播码流的目的终端、和/或目的终端所属组播组的路由设备、和/或目的终端所属组播组的其他设备，获取目的终端所接收到的直播码流的副本，作为末端直播码流。

生成签名信息可以包括：使用预定算法对源头直播码流的数据内容进行加密存储，生成签名信息；生成验证信息包括：使用预定算法对末端直播码流的数据内容进行加密存储，生成验证信息。

数据内容可以包括视频内容、源 IP 地址、传输路径中的至少一个。

根据比较结果输出监控结果可以包括：若比较结果为签名信息与验证信息相同，则输出直播码流未被篡改的监控结果；若比较结果为签名信息与验证信息不同，则输出直播码流被篡改的监控结果，并上报。

本公开提供了一种码流篡改监控装置，其包括：

签名模块，被配置为根据源头直播码流生成签名信息；

验证模块，被配置为根据末端直播码流生成验证信息；比较签名信息及验证信息，输出比较结果；

监控模块，被配置为根据比较结果输出监控结果。

所述签名模块，可以被配置为获取所述源头直播码流，使用预定算法计算所述源头直播码流，生成所述签名信息；

所述验证模块，可以被配置为获取所述末端直播码流，使用所述预定算法计算所述末端直播码流，生成所述验证信息。

签名模块可以被配置为从直播码流的直播源、和/或内容分发网络中心节点、和/或内容分发网络转码节点，获取直播码流的副本，作为源头直播码流。

验证模块可以被配置为从直播码流的目的终端、和/或目的终端所属组播组的路由设备、和/或目的终端所属组播组的其他设备，获取目的终端所接收到的直播码流的副本，作为末端直播码流。

签名模块可以被配置为使用预定算法对源头直播码流的数据内容进行加密存储，生成签名信息；验证模块被配置为使用预定算法对末端直播码流的数据内容进行加密存储，生成验证信息。

数据内容可以包括视频内容、源 IP 地址、传输路径中的至少一个。

监控模块可以被配置为若比较结果为签名信息与验证信息相同，则输出直播码流未被篡改的监控结果；若比较结果为签名信息与验证信息不同，则输出直播码流被篡改的监控结果，并上报。

本公开提供了一种通信系统，其包括本公开提供的码流篡改监控装置。

本公开实施例还提供了一种非暂态计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为执行上述方法。

本公开实施例还提供了一种电子设备，包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器执行上述的方法。

本公开的有益效果：

本公开提供了一种码流篡改监控方法，在源头端，获取源头直播码流，使用预定算法计算源头直播码流，生成签名信息，在用户终端，获取末端直播码流，使用预定算法计算末端直播码流，生成验证信息；比较签名信息及验证信息，输出比较结果，根据比较结果输出监控结果；这样就可以实现基于数字签

名机制的直播码流防篡改的监控，不需要部署专用的 DRM 系统，解决了相关技术需要部署 DRM 系统才能实现防篡改监控的问题。

附图概述

图 1 是相关防篡改系统的结构示意图；

图 2 为本公开第一实施例提供的码流篡改监控装置的结构示意图；

图 3 为本公开第二实施例提供的码流篡改监控方法的流程图；

图 4 是本公开第三实施例提供的通信系统的一种示意图；

图 5 是本公开第三实施例提供的通信系统的另一种示意图；

图 6 是本公开第三实施例提供的码流篡改监控方法的流程图；以及

图 7 是本公开实施例提供的电子设备的结构示意图。

具体实施方式

下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例只是本公开中一部分实施例，而不是全部的实施例。基于本公开中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本公开保护的范围。

现通过实施方式结合附图的方式对本公开做出诠释说明。

第一实施例：

图 2 为本公开第一实施例提供的码流篡改监控装置的结构示意图，由图 2 可知，在本实施例中，本公开提供的码流篡改监控装置包括：

签名模块 11，被配置为获取源头直播码流，使用预定算法计算源头直播码流，生成签名信息；

验证模块 12，被配置为获取末端直播码流，使用预定算法计算末端直播码流，生成验证信息；比较签名信息及验证信息，输出比较结果；

监控模块 13，被配置为根据比较结果输出监控结果。

在实际应用中，预定算法包括但不限于ECC（Error Correcting Code，错误检查和纠正）加密算法、MD5（Message-Digest Algorithm 5，消息摘要算法第五版）加密算法等加密算法；使用加密算法对源头/末端直播码流进行计算处理，是为了避免计算得到的数据被非法攻击篡改，进而失去验证功能。

在一些实施例中，上述实施例中的签名模块11被配置为从直播码流的直播源、和/或内容分发网络中心节点、和/或内容分发网络转码节点，获取直播码流的副本，作为源头直播码流。在实际应用中，签名模块11可以是通过服务器的形式实现，这样，签名模块11就可以直接与直播源、和/或内容分发网络中心节点、和/或内容分发网络转码节点通信，获取需要的副本数据，当然，签名模块11也可以采用作为装置的一部分设置在直播源、和/或内容分发网络中心节点、和/或内容分发网络转码节点等等形式来获取需要的数据。

在一些实施例中，上述实施例中的验证模块12被配置为从直播码流的目的终端、和/或目的终端所属组播组的路由设备、和/或目的终端所属组播组的其他设备，获取目的终端所接收到的直播码流的副本，作为末端直播码流。在实际应用中，验证模块12可以是通过服务器的形式实现，这样，验证模块12就可以直接与目的终端、和/或目的终端所属组播组的路由设备、和/或目的终端所属组播组的其他设备通信，获取需要的副本数据，当然，也可以采用作为装置的一部分设置在目的终端、和/或目的终端所属组播组的路由设备、和/或目的终端所属组播组的其他设备等等形式来获取需要的数据。

在一些实施例中，上述实施例中的签名模块11被配置为使用预定算法对源头直播码流的数据内容进行加密存储，生成签名信息；验证模块12被配置为使用预定算法对末端直播码流的数据内容进行加密存储，生成验证信息。

在一些实施例中，上述实施例中的数据内容包括视频内容、源IP地址、传输路径中的至少一个。传输路径是指视频码流在传输过程中经过的节点标识，若视频码流被篡改，必然需用通过一些没有在传输路径内的节点/设备来篡改数据内容，通过对传输路径的校验可以很快的判断数据是否被篡改。视频内容一般包括视频画面及音频等，源IP地址是视频码流的来源地址，当用户对视频码流的内容感兴趣时，可以根据源IP地址到对应直播源观看，这两个内容一般是篡改的主要对象，通过对其进行比对，可以很快的判断数据是否被篡改。

在一些实施例中，上述实施例中的监控模块13被配置为若比较结果为签名

信息与验证信息相同，则输出直播码流未被篡改的监控结果；若比较结果为签名信息与验证信息不同，则输出直播码流被篡改的监控结果，并上报。

对应的，本公开提供了一种通信系统，其包括本公开提供的码流篡改监控装置。

第二实施例：

图 3 为本公开第二实施例提供的码流篡改监控方法的流程图，由图 3 可知，在本实施例中，本公开提供的码流篡改监控方法包括：

S301：获取源头直播码流，使用预定算法计算源头直播码流，生成签名信息；

S302：获取末端直播码流，使用预定算法计算末端直播码流，生成验证信息；比较签名信息及验证信息，输出比较结果；

S303：根据比较结果输出监控结果。

在一些实施例中，上述实施例中的获取源头直播码流包括：从直播码流的直播源、和/或内容分发网络中心节点、和/或内容分发网络转码节点，获取直播码流的副本，作为源头直播码流。

在一些实施例中，上述实施例中的获取末端直播码流包括：从直播码流的目的终端、和/或目的终端所属组播组的路由设备、和/或目的终端所属组播组的其他设备，获取目的终端所接收到的直播码流的副本，作为末端直播码流。

在一些实施例中，上述实施例中的生成签名信息包括：使用预定算法对源头直播码流的数据内容进行加密存储，生成签名信息；生成验证信息包括：使用预定算法对末端直播码流的数据内容进行加密存储，生成验证信息。

在一些实施例中，上述实施例中的数据内容包括视频内容、源 IP 地址、传输路径中的至少一个。

在一些实施例中，上述实施例中的根据比较结果输出监控结果包括：若比较结果为签名信息与验证信息相同，则输出直播码流未被篡改的监控结果；若比较结果为签名信息与验证信息不同，则输出直播码流被篡改的监控结果，并上报。

第三实施例：

现结合应用场景对本公开进行诠释说明。

本实施例中，在没有 DRM 系统的情况下，提供一种可以及时有效监控直播码流的防篡改的方法。本实施例在没有 DRM 系统的基础上，提出一种基于数字签名机制的直播码流防篡改监控系统和方法。

如图 4 及图 5 所示，所述系统包括：

直播码流签名服务器，被配置为实现上文中的签名模块 11 的功能，被配置为接收直播原始码流，输出直播码流的签名信息。

直播监控服务器，被配置为实现上文中的验证模块 12 的功能，其接收直播码流和直播码流的签名信息，如果发现直播流被篡改，上报告警至管理服务器。

管理服务器，被配置为实现上文中的监控模块 13 的功能，可以负责直播码流防篡改系统的管理，以及设备的运行状态监控。

图 4 及图 5 为本公开中直播码流防篡改系统的 2 种结构示意图。在该架构中，包含了管理服务器、直播源服务器，媒体服务器（内容分发系统）、直播码流签名服务器，直播码流监控服务器，用户客户端等设备。其中，管理服务器、直播码流签名服务器和直播码流监控服务器为新增网元。其中，直播码流签名服务器，接收直播原始码流，输出直播码流的签名信息。其中，直播监控服务器，接收直播码流和直播码流的签名信息，如果发现直播流被篡改，上报告警至管理服务器。其中，管理服务器，可以负责直播码流防篡改系统的管理、以及设备的运行状态监控。其中，直播源服务器为内容提供商向服务运营商提供直播媒体流的源服务器。其中，媒体服务器可以为用户提供直播服务。

在实际的应用中，有 2 种部署方式，如图 4、图 5，这两种防篡改虽然部署方式有差异，但其工作流程是相同的，下面结合图 6，通过实施例对这两种部署方式的直播码流防篡改监控流程进行说明。

如图 6 所示，本实施例提供的防篡改监控方法包括：

S601，管理服务器向直播码流签名服务器下发签名策略信息（包括但不限于需要对哪些频道进行签名等）。

S602，直播码流签名服务器根据策略信息接收直播源或者 CDN 中心/转码节点媒体码流，按照预定算法（包括但不限于 ECC 加密算法、MD5 加密算法等）对码流的数据内容等进行摘要/加密计算，输出直播码流的签名信息。

S603，管理服务器向直播监控服务器下发监控策略信息（包括但不限于需要对哪些频道进行监控等）。

S604，直播监控服务器根据监控策略信息，获取终端获得的直播媒体码流和直播码流签名服务器发出的签名信息，按照预定算法（包括但不限于ECC加密算法、MD5加密算法等）对码流的数据内容等进行摘要/加密计算，输出验证信息，比较签名信息与验证信息，以判断直播流是否被篡改。

S605，直播监控服务器如果发现直播码流被篡改，上报告警至管理服务器。

综上所述，采用本实施例的方法，可以实现基于数字签名机制的直播码流防篡改的监控。

本公开实施例还提供了一种非暂态计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为执行上述任一实施例中的方法。

本公开实施例还提供了一种电子设备的结构示意图。参见图7，该电子设备包括：

至少一个处理器(processor)70，图7中以一个处理器70为例；和存储器(memory)71，还可以包括通信接口(Communications Interface)72和总线73。其中，处理器70、通信接口72、存储器71可以通过总线73完成相互间的通信。通信接口72可以用于信息传输。处理器70可以调用存储器71中的逻辑指令，以执行上述实施例的方法。

此外，上述的存储器71中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。

存储器71作为一种计算机可读存储介质，可用于存储软件程序、计算机可执行程序，如本公开实施例中的方法对应的程序指令/模块。处理器70通过运行存储在存储器71中的软件程序、指令以及模块，从而执行功能应用以及数据处理，即实现上述方法实施例中的码流篡改监控方法。

存储器71可包括存储程序区和存储数据区，其中，存储程序区可存储操作

系统、至少一个功能所需的应用程序；存储数据区可存储根据终端设备的使用所创建的数据等。此外，存储器 71 可以包括高速随机存取存储器，还可以包括非易失性存储器。

本公开实施例的技术方案可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括一个或多个指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本公开实施例所述方法的全部或部分步骤。而前述的存储介质可以是非暂态存储介质，包括：U 盘、移动硬盘、只读存储器（ROM, Read-Only Memory）、随机存取存储器（RAM, Random Access Memory）、磁碟或者光盘等多种可以存储程序代码的介质，也可以是暂态存储介质。

综上可知，通过本公开的实施，至少存在以下有益效果：

本公开提供了一种码流篡改监控方法，在源头端，获取源头直播码流，使用预定算法计算源头直播码流，生成签名信息，在用户终端，获取末端直播码流，使用预定算法计算末端直播码流，生成验证信息；比较签名信息及验证信息，输出比较结果，根据比较结果输出监控结果；这样就可以实现基于数字签名机制的直播码流防篡改的监控，不需要部署专用的 DRM 系统，解决了相关技术需要部署 DRM 系统才能实现防篡改监控的问题。

以上仅是本公开的实施方式而已，并非对本公开做任何形式上的限制，凡是依据本公开的技术实质对以上实施方式所做的任意简单修改、等同变化、结合或修饰，均仍属于本公开技术方案的保护范围。

工业实用性

本申请提供的码流篡改监控方法、装置及通信系统，可以实现基于数字签名机制的直播码流防篡改的监控，不需要部署专用的 DRM 系统，解决了相关技术需要部署 DRM 系统才能实现防篡改监控的问题。

权 利 要 求 书

1、一种码流篡改监控方法，包括：

根据源头直播码流生成签名信息；并根据末端直播码流生成验证信息；

比较所述签名信息及所述验证信息，输出比较结果；

根据所述比较结果输出监控结果。

2、如权利要求 1 所述的方法，其中，

所述根据源头直播码流生成签名信息，包括：获取所述源头直播码流，使用预定算法计算所述源头直播码流，生成所述签名信息；

所述根据末端直播码流生成验证信息，包括：获取所述末端直播码流，使用所述预定算法计算所述末端直播码流，生成所述验证信息。

3、如权利要求 2 所述的方法，其中，所述获取源头直播码流包括：从直播码流的直播源、和/或内容分发网络中心节点、和/或内容分发网络转码节点，获取所述直播码流的副本，作为所述源头直播码流。

4、如权利要求 2 所述的方法，其中，所述获取末端直播码流包括：从直播码流的目的终端、和/或所述目的终端所属组播组的路由设备、和/或所述目的终端所属组播组的其他设备，获取所述目的终端所接收到的直播码流的副本，作为所述末端直播码流。

5、如权利要求 2 至 4 任一项所述的方法，其中，所述生成签名信息包括：使用所述预定算法对所述源头直播码流的数据内容进行加密存储，生成所述签名信息；所述生成验证信息包括：使用所述预定算法对所述末端直播码流的数据内容进行加密存储，生成所述验证信息。

6、如权利要求 5 所述的方法，其中，所述数据内容包括视频内容、源 IP 地址、传输路径中的至少一个。

7、如权利要求 1 所述的方法，其中，所述根据比较结果输出监控结果包括：若比较结果为所述签名信息与所述验证信息相同，则输出直播码流未被篡改的监控结果；若比较结果为所述签名信息与所述验证信息不同，则输出直播码流被篡改的监控结果，并上报。

8、一种码流篡改监控装置，包括：

签名模块，被配置为根据源头直播码流生成签名信息；

验证模块，被配置为根据末端直播码流生成验证信息；比较所述签名信息及所述验证信息，输出比较结果；

监控模块，被配置为根据所述比较结果输出监控结果。

9、如权利要求 8 所述的装置，其中，

所述签名模块，被配置为获取所述源头直播码流，使用预定算法计算所述源头直播码流，生成所述签名信息；

所述验证模块，被配置为获取所述末端直播码流，使用所述预定算法计算所述末端直播码流，生成所述验证信息。

10、如权利要求 9 所述的装置，其中，所述签名模块被配置为从直播码流的直播源、和/或内容分发网络中心节点、和/或内容分发网络转码节点，获取所述直播码流的副本，作为所述源头直播码流。

11、如权利要求 9 所述的装置，其中，所述验证模块被配置为从直播码流的目的终端、和/或所述目的终端所属组播组的路由设备、和/或所述目的终端所属组播组的其他设备，获取所述目的终端所接收到的直播码流的副本，作为所述末端直播码流。

12、如权利要求 9 至 11 所述的装置，其中，所述签名模块被配置为使用所述预定算法对所述源头直播码流的数据内容进行加密存储，生成所述签名信息；

所述验证模块被配置为使用所述预定算法对所述末端直播码流的数据内容进行加密存储，生成所述验证信息。

13、如权利要求 12 所述的装置，其中，所述数据内容包括视频内容、源 IP 地址、传输路径中的至少一个。

14、如权利要求 8 所述的装置，其中，所述监控模块被配置为若比较结果为所述签名信息与所述验证信息相同，则输出直播码流未被篡改的监控结果；若比较结果为所述签名信息与所述验证信息不同，则输出直播码流被篡改的监控结果，并上报。

15、一种通信系统，包括如权利要求 8 至 14 任一项所述的码流篡改监控装置。

16、一种非暂态计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为执行权利要求 1-7 中任一项的方法。

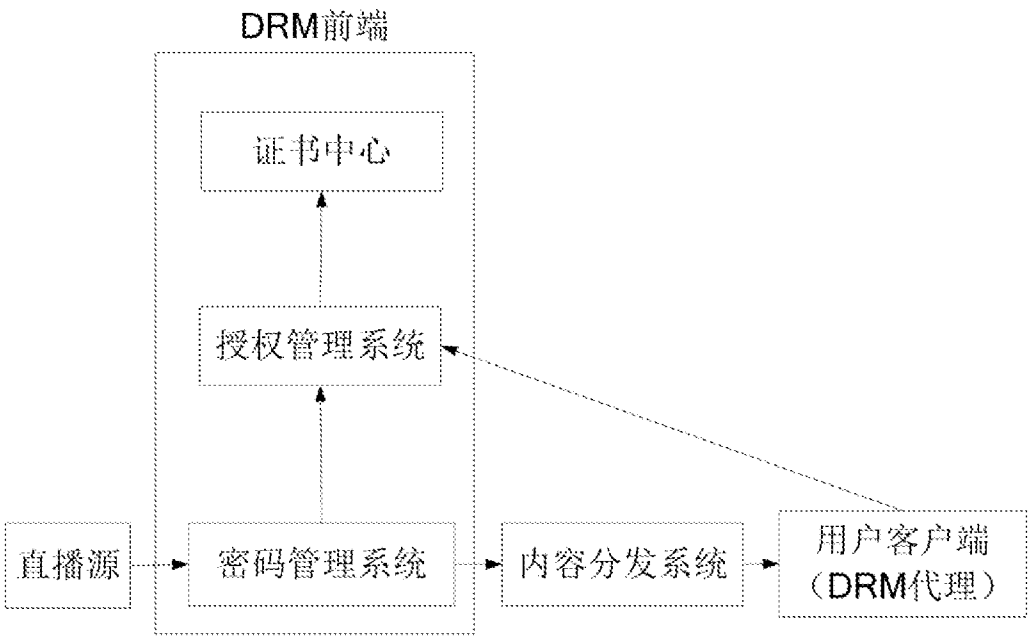

DRM前端
证书中心
授权管理系统
直播源
密码管理系统
内容分发系统
用户客户端
（DRM代理）

图 1

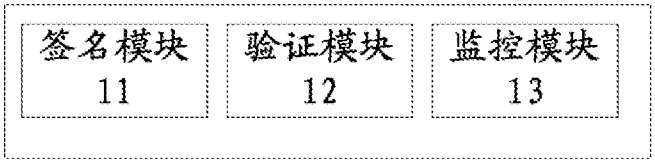

签名模块
11
验证模块
12
监控模块
13

图 2

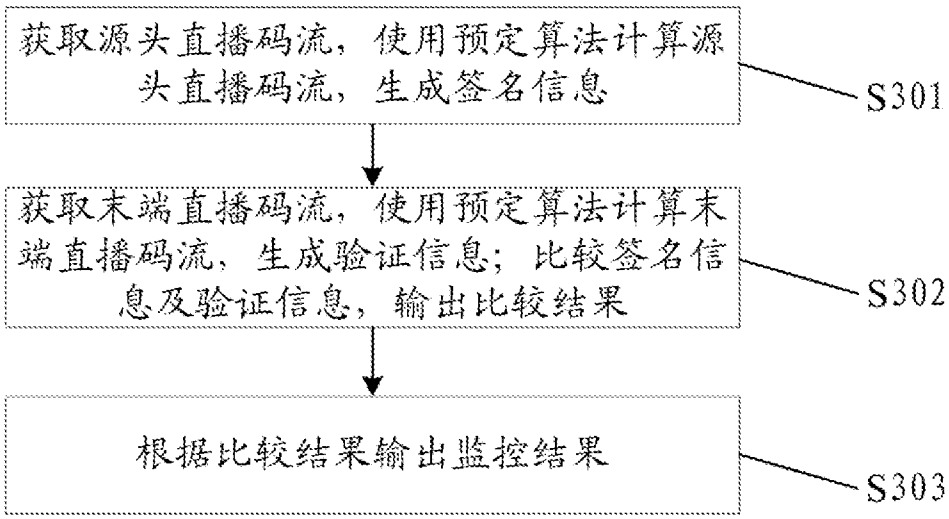

获取源头直播码流，使用预定算法计算源头直播码流，生成签名信息
S301
获取末端直播码流，使用预定算法计算末端直播码流，生成验证信息；比较签名信息及验证信息，输出比较结果
S302
根据比较结果输出监控结果
S303

图 3

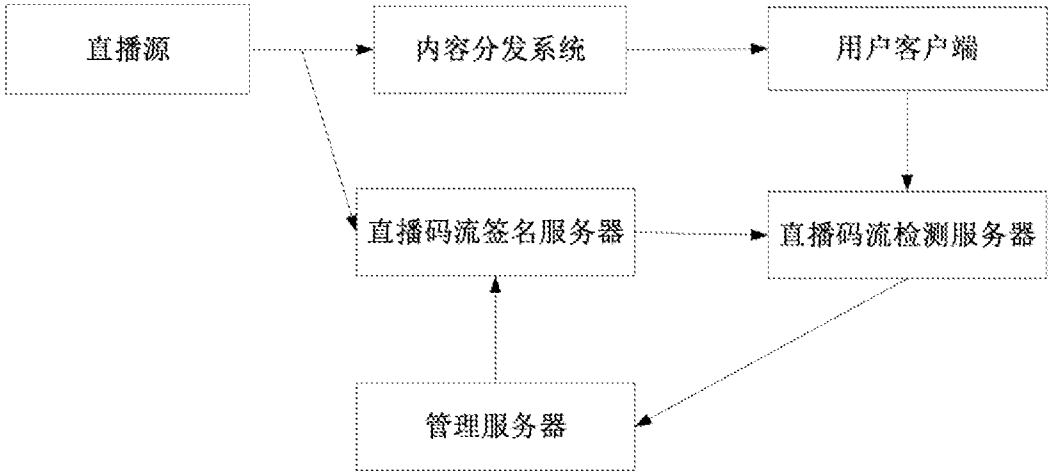

直播源
内容分发系统
用户客户端
直播码流签名服务器
直播码流检测服务器
管理服务器

图 4

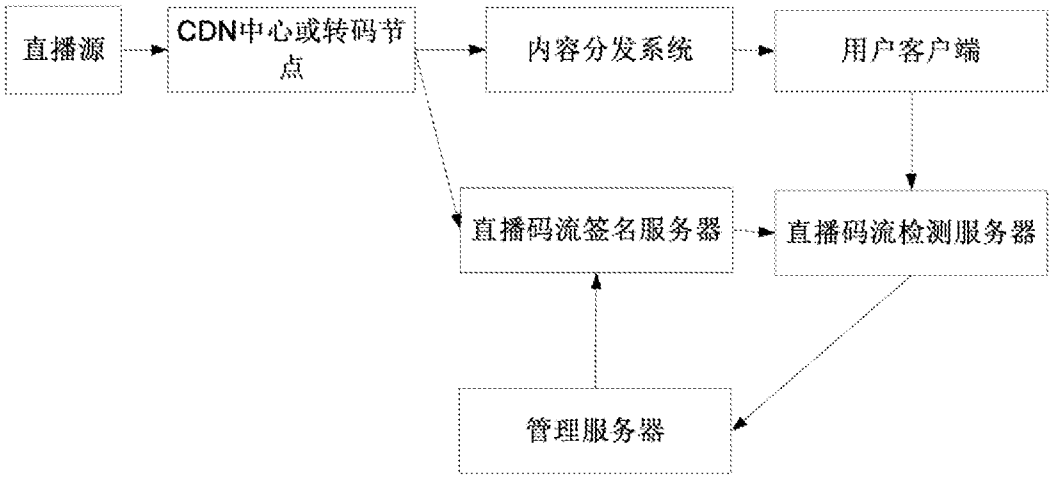

直播源
CDN中心或转码节点
内容分发系统
用户客户端
直播码流签名服务器
直播码流检测服务器
管理服务器

图 5

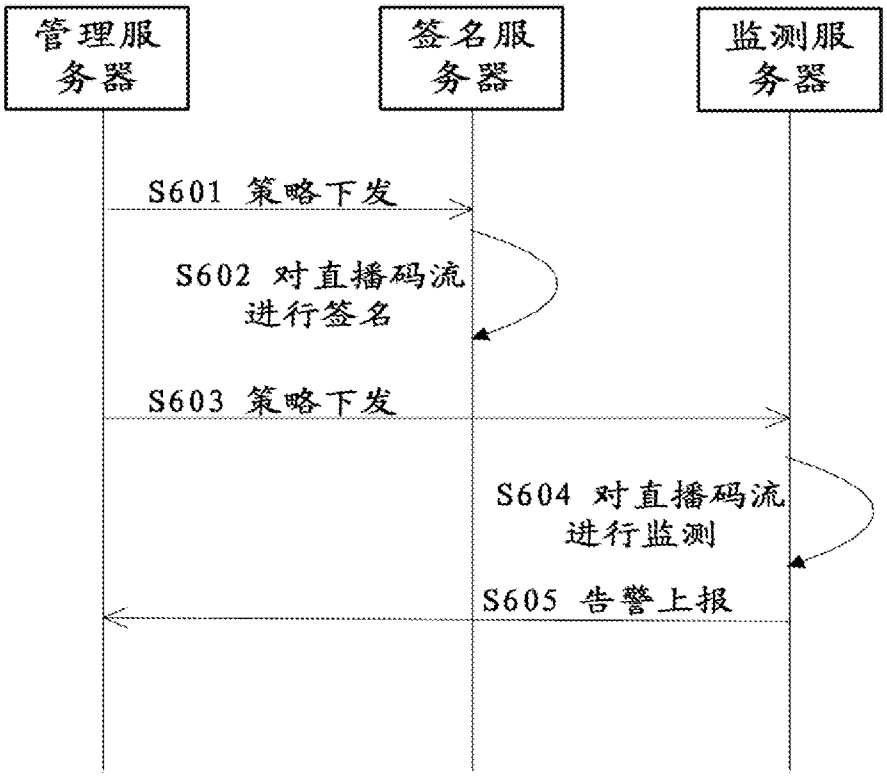

管理服务器
签名服务器
监测服务器
S601 策略下发
S602 对直播码流进行签名
S603 策略下发
S604 对直播码流进行监测
S605 告警上报

图 6

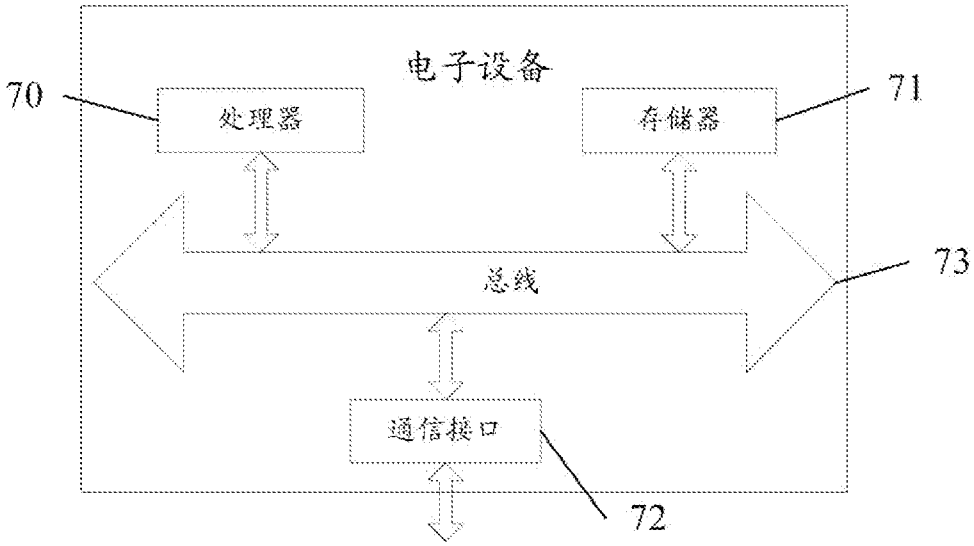

电子设备
70
处理器
存储器
71
总线
73
通信接口
72

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/083868

A. CLASSIFICATION OF SUBJECT MATTER

H04N 21/2389 (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; H04L

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, WPI, EPODOC, GOOGLE, CNKI: live broadcast, live, program, media, video, audio, tamper, juggle, illegal, modification, monitor, detect, signature, watermark, encrypt, verify, CRC, hash, MD5

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104469407 A (SHANDONG TAIXIN ELECTRONICS CO., LTD.), 25 March 2015 (25.03.2015), description, paragraphs [0072]-[0075] and [0096]-[0123], and figure 4	1-16
X	CN 201378857 Y (THE FIRST RESEARCH INSTITUTE OF THE MINISTRY OF PUBLIC SECURITY OF P.R.C et al.), 06 January 2010 (06.01.2010), description, page 3, line 1 to page 5, line 6	1-16
X	CN 104602015 A (XI'AN SUANIER ELECTRONIC TECHNOLOGY CO., LTD.), 06 May 2015 (06.05.2015), description, paragraphs [0036]-[0049]	1-16
A	CN 101282457 A (LU, Jian), 08 October 2008 (08.10.2008), the whole document	1-16
A	CN 1976437 A (ZHEJIANG UNIVERSITY), 06 June 2007 (06.06.2007), the whole document	1-16
A	US 2012148089 A1 (INFOSYS TECHNOLOGIES LIMITED), 14 June 2012 (14.06.2012), the whole document	1-16

☐ 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

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 June 2017 (30.06.2017)	**28 July 2017 (28.07.2017)**
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 **CHEN, Jing** Telephone No.: (86-10) **53318976**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/083868

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104469407 A	25 March 2015	None	
CN 201378857 Y	06 January 2010	None	
CN 104602015 A	06 May 2015	None	
CN 101282457 A	08 October 2008	None	
CN 1976437 A	06 June 2007	None	
US 2012148089 A1	14 June 2012	None	

国际检索报告

国际申请号
PCT/CN2017/083868

A. 主题的分类

H04N 21/2389(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; H04L

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, WPI, EPODOC, GOOGLE, CNKI:直播，节目，媒体，视频，音频，篡改，非法，修改，检测，监测，签名，验证，水印，加密，校验，live, program, media, video, audio, tamper, juggle, illegal, modification, monitor, detect, signature, watermark, encrypt, verify, CRC, hash, MD5

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
X	CN 104469407 A (山东泰信电子股份有限公司) 2015年 3月 25日 (2015-03-25) 说明书第[0072]-[0075]、[0096]-[0123]段，图4	1-16
X	CN 201378857 Y (公安部第一研究所等) 2010年 1月 6日 (2010-01-06) 说明书第3页第1行-第5页第6行	1-16
X	CN 104602015 A (西安蒜泥电子科技有限责任公司) 2015年 5月 6日 (2015-05-06) 说明书第[0036]-[0049]段	1-16
A	CN 101282457 A (陆健) 2008年 10月 8日 (2008-10-08) 全文	1-16
A	CN 1976437 A (浙江大学) 2007年 6月 6日 (2007-06-06) 全文	1-16
A	US 2012148089 A1 (INFOSYS TECHNOLOGIES LIMITED) 2012年 6月 14日 (2012-06-14) 全文	1-16

☐ 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	国际检索报告邮寄日期
2017年 6月 30日	2017年 7月 28日

ISA/CN的名称和邮寄地址	受权官员
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	陈静
传真号 (86-10)62019451	电话号码 (86-10)53318976

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/083868

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	104469407	A	2015年 3月 25日	无	
CN	201378857	Y	2010年 1月 6日	无	
CN	104602015	A	2015年 5月 6日	无	
CN	101282457	A	2008年 10月 8日	无	
CN	1976437	A	2007年 6月 6日	无	
US	2012148089	A1	2012年 6月 14日	无	