(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 108259507 B
(45)授权公告日 2020.12.08

(21)申请号 201810141722.7

(22)申请日 2013.04.25

(65)同一申请的已公布的文献号
申请公布号 CN 108259507 A

(43)申请公布日 2018.07.06

(30)优先权数据
61/638,332 2012.04.25 US

(62)分案原申请数据
201380022052.2 2013.04.25

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 亚历山大·吉拉德 王新 张少波 刘永亮

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
US 2010023815 A1,2010.01.28
CN 101051906 A,2007.10.10
JP 2012507940 A,2012.03.29
US 7003667 B1,2006.02.21
US 2005097361 A1,2005.05.05
CN 102137089 A,2011.07.27

审查员 任盈之

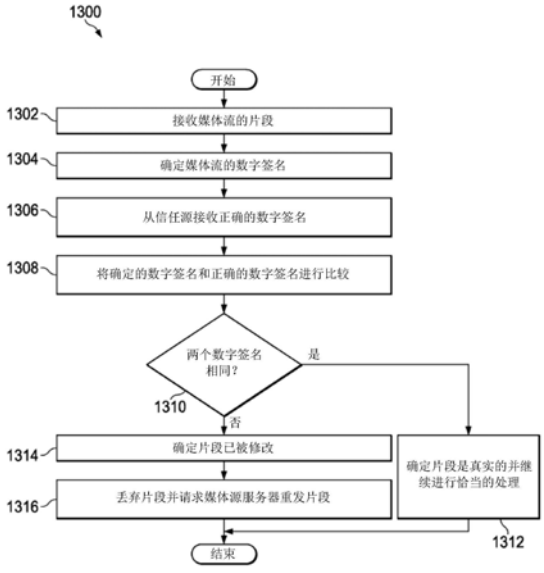
权利要求书2页 说明书13页 附图10页

(54)发明名称

用于自适应流媒体的片段完整性和真实性的系统和方法

(57)摘要

提供了用于自适应流媒体的片段完整性的系统和方法实施例。在实施例中,所述方法包括在数据处理系统处接收媒体流的片段,通过所述数据处理系统确定所述片段的摘要或数字签名,以及通过所述数字处理系统将所述摘要/数字签名与正确的摘要或正确的数字签名相比较以确定所述片段是否已被修改。



CN 108259507 B

1.一种用于验证自适应流媒体的片段完整性和真实性的方法,其特征在于,所述方法包括:

在数据处理系统处根据超文本传输协议或者实时传输协议接收媒体流的片段;

通过所述数据处理系统确定所述片段的摘要或数字签名;以及

通过媒体表示描述中的通用资源定位符获得正确的摘要或正确的数字签名;

通过所述数据处理系统将所述摘要或所述数字签名与所述正确的摘要或所述正确的数字签名相比较以确定所述片段是否已被修改。

2.根据权利要求1所述的方法,其特征在于,所述正确的摘要或数字签名从服务器接收。

3.根据权利要求2所述的方法,其特征在于,服务器为包括所述媒体流的各个片段存储所述正确的摘要或所述正确的数字签名。

4.根据权利要求1所述的方法,其特征在于,所述摘要是加密散列。

5.根据权利要求1所述的方法,其特征在于,所述数字签名是消息认证码。

6.根据权利要求1所述的方法,其特征在于,片段修改包括所述片段相对于所述媒体流中的其它片段的时间顺序的修改。

7.根据权利要求1所述的方法,其特征在于,进一步包括当所述摘要与所述正确的摘要不匹配或所述数字签名与所述正确的数字签名不匹配时,拒绝所述片段。

8.一种用于验证自适应流媒体的片段完整性和真实性的网络部件,其特征在于,包括:

处理器;以及

计算机可读存储介质,所述计算机可读存储介质存储由所述处理器执行的程序,所述程序包括用于进行如下操作的指令:

根据超文本传输协议或者实时传输协议接收媒体流的片段;

确定所述片段的摘要或数字签名;以及

通过媒体表示描述中的通用资源定位符获得正确的摘要或正确的数字签名;

将所述摘要或数字签名与所述正确的摘要或所述正确的数字签名相比较以确定所述片段是否已被修改。

9.根据权利要求8所述的网络部件,其特征在于,所述正确的摘要或正确的数字签名从服务器接收。

10.根据权利要求9所述的网络部件,其特征在于,所述服务器为包括所述媒体流的各个片段存储所述正确的摘要或所述正确的数字签名。

11.根据权利要求8所述的网络部件,其特征在于,所述摘要包括消息认证码。

12.根据权利要求8所述的网络部件,其特征在于,所述摘要包括加密散列。

13.根据权利要求8所述的网络部件,其特征在于,片段修改包括所述片段相对于所述媒体流中的其它片段的时间顺序的修改。

14.根据权利要求8所述的网络部件,其特征在于,所述程序还包括用于进行如下操作的指令:当所述摘要与所述正确的摘要不匹配或所述数字签名与所述正确的数字签名不匹配时,拒绝所述片段。

15.一种用于验证自适应流媒体的片段完整性和真实性的方法,其特征在于,所述方法包括:

在用户设备UE处根据超文本传输协议或者实时传输协议接收媒体流的片段,其中所述媒体流包括超文本传输协议动态自适应流媒体DASH流的多个片段;

通过所述UE确定所述媒体流的所述片段的摘要或数字签名;

通过媒体表示描述中的通用资源定位符获得正确的摘要或正确的数字签名;通过所述UE将所述摘要或数字签名与所述正确的摘要或所述正确的数字签名相比较;以及

通过所述UE确定所述片段是否已被修改。

16.根据权利要求15所述的方法,其特征在于,所述正确的摘要或正确的数字签名从信任源接收。

17.根据权利要求15所述的方法,其特征在于,所述摘要包括消息认证码。

18.根据权利要求15所述的方法,其特征在于,所述摘要包括加密散列。

19.根据权利要求18所述的方法,其特征在于,所述加密散列是安全散列算法SHA,所述SHA包括SHA-256或SHA-512。

20.根据权利要求15所述的方法,其特征在于,确定所述片段是否已被修改包括确定所述片段相对于所述媒体流中的其它片段的时间顺序的修改。

21.一种用于验证自适应流媒体的片段完整性和真实性的用户设备,其特征在于,包括:

处理器;以及

计算机可读存储介质,所述计算机可读存储介质存储由所述处理器执行的程序,所述程序包括用于进行如下操作的指令:

根据超文本传输协议接收媒体流的片段,其中所述媒体流包括超文本传输协议动态自适应流媒体DASH流的多个片段;

确定所述媒体流的所述片段的摘要或数字签名;

通过媒体表示描述中的通用资源定位符获得正确的摘要或正确的数字签名;

将所述摘要或数字签名与所述正确的摘要或所述正确的数字签名相比较;以及

确定所述片段是否已被修改。

22.根据权利要求21所述的用户设备,其特征在于,所述正确的摘要或正确的数字签名从信任源接收。

23.根据权利要求21所述的用户设备,其特征在于,所述摘要包括消息认证码。

24.根据权利要求21所述的用户设备,其特征在于,所述摘要包括加密散列。

25.根据权利要求21所述的用户设备,其特征在于,确定所述片段是否已被修改包括确定所述片段相对于所述媒体流中的其它片段的时间顺序的修改。

用于自适应流媒体的片段完整性和真实性的系统和方法

技术领域

[0001] 本发明涉及用于媒体流的系统和方法,以及在具体实施例中,涉及用于自适应流媒体 的片段完整性和真实性的系统和方法。

背景技术

[0002] 在多系统运营商(MSO)拥有的网络的围墙花园中,一个重要的安全问题是防止非授 权访问和高价值内容复制。随着向开放网络和因特网传递的转变,运营商对他们的分发网 络不再拥有完整的端到端控制。这导致了若干新攻击,虽然未提供对内容的非授权访问, 但这些攻击允许中断业务并对客户端设备进行非授权访问。

[0003] 媒体片段以及它们的描述(例如媒体表示描述(MDP))存储在多个位置,遍及它们的分布网络,它们可缓存在商用内容分发网络(CDN)的节点中,随后可能缓存到接近消 费者的另一CDN的节点,接着缓存在服务提供商的头端处。实际上,除了节点之间的传递 通道上存在的潜在篡改之外,其中一些节点可能是恶意的。

[0004] 首先,该链路中的任一恶意实体均可改变MPD,从而完全劫持整个流会话。这种情况 可通过使用MPD传递超文本传输安全协议(HTTPS)和/或可扩展标记语言(XML)签名 的安全方法来解决。通常情况下,出于该讨论的目的,假定客户端具有正确的MPD并且该 MPD没有被篡改,而恶意实体能够访问MPD并且还能够完全访问网络。

[0005] 考虑三种主要的攻击类型:片段替代、重排序以及修改。完成拒绝服务以提供片段(例 如返回404而非片段)同样总是有可能的,但这种情况仅可通过提供若干可能的下载位置 和/或利用一个以上CDN来解决。

[0006] 直接内容替换或重排序可能在三种情况下发生:当被请求的片段是未加密的,当正被 替代的片段是连续的、加密的并置于同一加密时段(在该时段中片段通过相同的参数加密) (period in time during which segments are encrypted with the same parameter)中,或当目的 是中断呈现而非用一个适用的片段来替代另一片段。

[0007] 攻击的示例是跳过广告(广告被来自电影的下一片段替代)以及服务降级(以低质量 的片段替代高质量的片段)。

[0008] 通常情况下,最容易受攻击的商业模式是当提供的内容缺少支持广告的数字权限管理 (DRM)时,而该商业模式有望成为相当重要的模式。公共频道(例如美国的C-SPAN) 通常也受同样的威胁,在这些公共频道上传输的内容未加密。

[0009] 在未加密的以及在使用部分比特流加密的任意内容中,片段修改总是可能的。在后一 种情况下,加密的字节在未加密的头中发送,因此,例如,可用任意未加密的内容替代实 际保护的基本流。当部分加密的流携带修改客户端行为的未加密指令时,这些指令可用于 修改客户端行为。在全片段加密的情况下,片段修改将致使片段不可用,这可能导致解码 器重置。

[0010] 这种攻击(除加密内容和其它未加密的内容的普通替换)的一个示例是增加‘lmsg’ brand到ISO-FF格式的片段以导致客户端提前退出节目段。另一个有意思的方向

是,如果 存在包含未加密的传递的新MPD通用资源定位符(URL)的消息(虽然这种功能目前还未 标准化),那么就能很容易地用恶意URL代替该URL。

[0011] 当网络内部进行变换(例如重加密)时,恶意实体也可以访问用于对内容进行加密和 解密的密钥。这样,加密内容同样可能发生内容替换。

[0012] 非媒体片段上也可能发生类似的攻击。如果存在初始化和比特流交换片段,修改可致 使整个内容完全或部分不可用,而被修改的索引文件可至少破坏特技模式功能。

[0013] 在某些简单的情况下片段被修改也是可能的,例如由于文件损坏。这样,另外一种常 见的简单情况下的错误是由于使用了不正确的解密密钥。

[0014] 上述讨论仅描述了片段,然而可能从未传递完整的片段,并且比特率交换可能在子片 段级上进行。

发明内容

[0015] 根据实施例,一种用于验证自适应流媒体的片段完整性和真实性的方法包括在数据处 理系统处接收媒体流的片段,通过所述数据处理系统确定所述片段的摘要或数字签名,以 及通过所述数字处理系统将所述摘要或所述数字签名与正确的摘要或正确的数字签名相 比较以确定所述片段是否已被修改。

[0016] 根据另一项实施例,一种用于验证自适应流媒体的片段完整性和真实性的网络部件包 括处理器以及计算机可读存储介质,所述计算机可读存储介质存储由所述处理器执行的程 序,所述程序包括用于进行如下操作的指令:接收媒体流的片段,确定所述片段的摘要或 数字签名,以及将所述摘要或所述数字签名与正确的摘要或正确的数字签名相比较以确定 所述片段是否已被修改。

[0017] 根据另一项实施例,一种用于验证自适应流媒体的片段完整性和真实性的方法包括在 用户设备(UE)处接收媒体流的片段,其中所述媒体流包括超文本传输协议动态自适应 流媒体(DASH)流的多个片段,通过所述UE确定所述媒体流的所述片段的摘要或数字签名,通过所述UE将所述摘要或所述数字签名与正确的摘要或正确的数字签名相比较,以 及通过所述UE确定所述片段是否已被修改。

附图说明

[0018] 为了更完整地理解本发明及其优点,现在参考以下结合附图进行的描述,其中:

[0019] 图1示出了用于传送数据以及维持自适应流媒体的的片段完整性和真实性的实施例系 统;

[0020] 图2示出了片段的表示组;

[0021] 图3示出了片段形成的流的示例;

[0022] 图4示出了动态自适应流媒体的架构;

[0023] 图5示出了表示组的哈希值的码本;

[0024] 图6示出了哈希值的向量形式;

[0025] 图7A-7B示出了片段的广告插入/替换;

[0026] 图8A-8B示出了进行片段替换的内容的修改;

[0027] 图9示出了摘要生成;

[0028] 图10A-10C示出了表示的组合摘要；

[0029] 图11A-11D示出了在组合摘要中定位检索出的片段的摘要；

[0030] 图12示出了检索出的片段的本地摘要/签名；

[0031] 图13示出了用于验证自适应流媒体的片段完整性和真实性的实施例方法的流程图；以 及

[0032] 图14是可用于实施各种实施例的处理系统。

具体实施方式

[0033] 下文将详细论述当前优选实施例的制作和使用。然而，应了解，本发明提供可在各种 具体上下文中体现的许多适用的发明性概念。所论述的具体实施例仅仅说明用以实施和使 用本发明的具体方式，而不限制本发明的范围。

[0034] 通常媒体内容被保护起来避免非授权访问。对于因特网流媒体，已经出现了与篡改媒 体内容有关的额外威胁。实施例提出了用于验证媒体内容的完整性和真实性的方法，媒体 内容通过超文本传输协议(HTTP)动态自适应流媒体(DASH)进行流式传输。

[0035] 实施例使用摘要来验证自适应流媒体片段的完整性和真实性。实施例使用数字签名来 验证自适应流媒体片段的完整性和真实性。实施例请求签名和摘要。实施例验证流式传输 的内容的完整性和真实性。实施例阻止或减少网络内的恶意内容操纵。实施例可用于电缆 /IPTV/电信/移动/无线/互联网视频流媒体、CDN、DASH等领域中支持广告的非DRM自适 应流媒体、安全自适应流媒体，等等。

[0036] 图1示出了用于传送数据以及维持自适应流媒体的的片段完整性和真实性的实施例系 统100。系统100可包括客户端102、媒体源服务器104、认证服务器106、恶意服务器108以及网络110。网络110可包括交换机、路由器、通信信道以及用于将数据从网络110的一 部分发送到网络110的另一部分的其它设备。网络110可包括有线和无线传输构件。客户端102、媒体源服务器104、认证服务器106和恶意服务器108连接到网络110并用于通过网络110发送和接收数据。客户端可以是任意类型的用户设备(UE)，包括个人电脑、笔记本 电脑、平板电脑、智能电话、个人数字助理等。

[0037] 恶意服务器108是在从媒体源服务器104到客户端102的媒体流片段的传输路径中的服 务器。恶意服务器108可能试图修改或替换媒体流的一个或多个片段。例如，恶意服务器 108可能替换不同广告的一个或多个片段或在媒体片段中包含病毒或恶意软件以感染客户 端102或从客户端102获取私人信息。

[0038] 媒体源服务器104用于存储媒体并通过网络110发送媒体流到客户端102。媒体流可包 括媒体流片段。媒体类型可包括视频和音频。各个媒体流片段可使用信息进行编码，客户 端102可从该信息中确定或计算数字签名。数字签名可包括摘要或消息认证码。媒体源服 务器104可为各个片段发送正确的数字签名到认证服务器106，认证服务器106可为媒体流 的各个片段存储正确的数字签名。认证服务器106是信任的认证服务器或信任的源，经客 户端102请求后，认证服务器106向客户端102提供正确的数字签名。客户端102用于确定或 计算各个片段的数字签名，并将确定的数字签名与从认证服务器106接收的正确的数字签 名相比较。如果两个数字签名是匹配的，那么片段未被修改。然而，如果两个数字签名不 匹配，那么客户端102确定片段已被修改并可丢弃该片段，并且/或者请求媒体源服务器

104 重发修改的片段。片段修改可包括用不同的片段替换一个片段，及时重新排列片段相对于 媒体流中的其它片段的暂时位置，和/或片段的部分或全部修改。片段修改可包括插入可 损害客户端102的恶意内容或泄露存储在客户端上的机密用户信息。

[0039] MPD和媒体片段可能都需要合法改变以例如进行动态广告插入。通常，链路中唯一信 任的元素是原始内容提供商或原始内容提供商明确信任的实体。通常有四个选项用来解决 这个问题：

[0040] (1)让信任的实体通过安全信道向客户端提供带外片段摘要；

[0041] (2)使用外部提供的密钥在带内(在媒体或索引片段中)或带外(例如使用HTTP)携带MAC；

[0042] (3)使用认证的加密，尽管这产生了新的非互操作DRM，并且不保持与使用全片段、MPEG-2CA或CENC加密进行编码的内容的兼容性；以及

[0043] (4)对全部片段传输使用HTTPS，尽管该选项明显降低了整个系统的可扩展性。

[0044] 下述实施例提供了以上选项1和2的实施方式，利用带外传输的数字摘要和签名。

[0045] 关于摘要，当恶意实体试图破坏网络或简单地注入病毒文件时，(例如Linux分配器 和文件分享社区)已经遇到了一些问题。在这些情况下，使用加密哈希或摘要来对付攻击， 例如Ubuntu分发提供MD5、安全散列算法(SHA)-1、SHA-256和SHA-512给不同的下载者。

[0046] 如果客户端想要接收摘要，到信任实体的安全信道(例如TLS)对客户端可用，摘要的使用解决了这种情况下的真实性和完整性问题。也就是说，假设第n个片段S(n)和可提供摘要s＝SHA(S(n))的信任实体，如果SHA(S')≠s，那么客户端可拒绝任何不等于S(n)的非法 的片段S'。

[0047] 根据示例实施方式，MPD包括具有语法的补充属性描述符，该语法类似于以下之一：

[0048] <SupplementalProperty schemeIdUri:"urn:mpeg:dash:sea:auth:2013">

[0049] <sea:ContentAuthenticity

[0050] authSchemeIdUri＝"urn:mpeg:dash:sea:sha256"

[0051] authUrlTemplate＝"https://verify.example.com?base＝$base$&range＝$first$-$last$"/>

[0052] </SupplementalProperty>

[0053] 如果只有一个安全信道可用，或需要缓存友好，数字签名可用于提供信任级别。假设 来自信任实体的公钥，可使用键入的散列信息认证码(HMAC)以使消息生效。在这种情况下，当公钥和签名都是未加密的传输时，真实性和完整性都得以保证。MPD自己可通过 使用XML签名来采取同样的方法。

[0054] 例如，MPD包括具有语法的补充属性描述符，该语法类似于以下之一：

[0055] <!--SHA-256digests is available for all(sub)segments-->

[0056] <SupplementalProperty schemeIdUri＝"urn:mpeg:dash:sea:auth:2013">

[0057] <sea:ContentAuthenticity

[0058] authSchemeIdUri＝"urn:mpeg:dash:sea:sha256"

[0059] authUrlTemplate＝"https://verify.example.com?base＝$base$&range＝

$first$-$last$"/>

[0060] </SupplementalProperty>

[0061] 实施例增加额外URL模板用于向信任实体请求片段的摘要值。摘要值是由原始内容提 供商在加密之前为未加密的片段计算的,因此,如果片段被加密,将检测到错误解密密钥 (其将导致错误解密的片段)的使用,并且加密密钥将完全从摘要分离。

[0062] 由于SHA-1不被推荐,可用的两个哈希函数是SHA-256和SHA-512。SHA-256在32位机器(其是在移动设备中使用的绝大多数机器)上的计算复杂度较低,因此在这些机器中SHA-256可能更有用。

[0063] HMAC可在相同的框架内支持;唯一的重大变化是接收公钥。

[0064] 在实施例中,以下语法和语义可用于支持上述的内容认证框架:

[0065]

元素或属性名称	使用	描述
ContentAuthenticity		指定计算片段的真实性标签所必需的信息。
@authSchemeIdUri	M	指定用于计算真实性标签的算法。
@authUrlTemplate	M	指定用于生成URL的模板,该URL用于检索真实性标签值。
@authTagLength	O	指定认证标签的长度,单位为位。如果不存在,标签长度则为@authSchemeldUri 标识的算法中的标签长度。
@keyUrlTemplate	O	指定用于通过使用如ISO/IEC 23009-1:2012, 5.3.9.4.4 中定义的语法和变量替换生成密钥URI的模板。

[0066]

说明： 对于属性：M=必选的；O=可选的；OD=具有默认值的可选；CM=有条件地必选。 对于元素：<minOccurs>...<maxOccurs>（N=无限制） 元素加粗；属性不加粗并在属性前加@。

[0067] 对于URL衍生，摘要和签名URL的衍生构建如下。为给定的媒体、初始化、索引或比特流交换片段，或为子片段构建完整的URL。与ISO/IEC 23009-1附件E中相同的替换变量可用于构建摘要或签名URL模板。如果使用了摘要，https应该用于请求。

[0068]

$<标识符>$	**替换参数**
$$	是一个转义序列，即“$$”由单个“$”代替。
$base$	标识符应由如 RFC3986 中定义的原始 URL 的 scheme“:”hier-part 替换。
$query$	标识符应由如 RFC3986 中定义的原始 URL 的 query 部分替换。如果原始 URL 的 query 部分为空，那么，如果模板字符串中紧靠$query$标识符之前的分隔符不是“？”，或者紧靠$query$标识符之后存在分隔符，那么在模板中包含该标识符将导致移除该

[0069]

	分隔符。
$first$	标识符应由一个范围中的第一字节的字节偏移量替代，并且如果该请求将使用部分 GET 请求执行，标识符应与 RFC2616 的 14.35.1 中 'byte-range-spec' 的 'first-byte-pos' 的值相同。如果 URL 不包含字节范围，$first$的值应为“0”。
$last$	标识符由范围中的最后一个字节的字节偏移量替代；也就是说，包括了指定的字节位置。如果该请求将使用部分 GET 请求执行，标识符应与 RFC2616 的 14.35.1 中 'byte-range-spec' 的 'last-byte-pos' 的值相同。如果 URL 不包含字节范围，$last$的值应为“Inf”。

[0070] 与ISO/IEC 23009-1附件E不同，如果未使用字节范围，变量$first$和$last$具有默认值。不要求与片段或子片段不对应的字节范围请求，并且服务器可忽略这些字节范围请求。

[0071] 对于正数n和m，假设片段S是一个位序列(作为内容块)，表示R＝[S(1),S(2),…,S(n)]是 n个片段的序列，并且表示组A＝[R(1),R(2),…,R(m)]是m个表示的列表。为简单起见，第i 个表示中的第j个片段，A[i][j]，也表示为S(i,j)，i＝1……m并且j＝1……n。可见，表示组A 可被看作片段的m×n矩阵，如图2所示，图2是示出了片段的表示组的图200。

[0072] A定义的(片段)流是n个片段的序列[S(i1,1),S(i2,2),…,S(im,n)]，其中1<ik<m,k＝1, 2……n。如果ik＝x，其中1<x<m,k＝1,2……m，那么一个流被称为非自适应的。在这种 情况下，非自适应流仅仅是表示组A中的一个表示。如果一个流不是非自适应的，那么它 被称为自适应的。如果差分|ik-ik+1|<1,k＝1……n-1，那么一个流被称为平滑的。图3是示 出了由屏蔽片段形成的流的示例的图300。

[0073] 在通用设置中，可以在多源和多汇点图中描述动态自适应流媒体的服务器-客户端系 统架构，其中服务器和客户端之间有大量节点用于提供CDN(内容分发网络)功能以传输 内容片段。表示组A中的片段最初在服务器上是可用的，但是各个服务器可能不一定具有 所有的片段，并且任意片段可能在一个以上服务器上可用。

[0074] 图4是示出了动态自适应流媒体的架构的图400。如果各个客户端根据流中片段的连续 顺序每次仅接收任何流的一个片段，那么该架构的一个系统是流式传输系统，因此，在接 收到片段之后，无需等待接收后续片段，客户端可以以时间推进的方式回放片段。在流式 传输系统中，任何客户端一直接收流的前缀[S(i1,1),S(i2,2),…,S(ik,k)]。

[0075] 如果各个客户端能够接收非表示流，那么流式传输系统是动态自适应的。

[0076] 根据系统使用的片段传输协议(例如http或实时传输协议(rtp))，片段可由服务器 推送到客户端或由客户端从服务器获取。

[0077] 在实施例中，需要确保客户端接收的片段不仅形成了有效的(并且是可能预期的)流 而总体上对流的完整性没有任何篡改，而且各个片段都是真实的，如同原先在服务器上可 用的一样。

[0078] 流的真实性和完整性的一些常见攻击如下：

[0079] (1)修改片段S(i,j)的内容；

[0080] (2)移除或略过一个或多个片段S(ij,j),S(ij+1,j+1),…,S(ik,k)，其中j<k；

[0081] (3)将片段S(i,j)替换为不在表示组A中的另一个片段T；以及

[0082] (4)将片段S(i,j)替换为表示组A中的另一个片段S(p,q)(重排序或再循环)。

[0083] 这些种类的攻击可发生在服务器和客户端之间的传递通道或CDN节点上。

[0084] 在数字安全文献中，哈希函数通常用于保护数字位序列的完整性。这是因为在接收的 片段或接收的流和其原件之间进行直接比较或检查是几乎不可行或非常低效的。相反，通 过预计算片段的哈希值并测试接收的片段是否具有相同的哈希值来进行比较或检查。

[0085] 由于流(其是片段序列)的结构的性质，流的完整性可在片段级别和片段序列级别上 提供。

[0086] 在流式传输系统中，用于完整性保护的简单直接的解决方案是计算所有接收的片段的 哈希值。也就是说，考虑接收的片段为较长连接序列的位，并检查以下是否成立，k＝1……n：

[0087] H([S(i1,1)|S(i2,2)|...|S(ik,k)])＝hSk。

[0088] 这明显涉及太多的冗余计算，并要求预计算太多(n×mn)的哈希值hSk，因为可能会 存在mn个流并且每个流有n个前缀。

[0089] 使用流结构的一个改进的版本是检查每个片段的完整性，随后检查流中片段序列的完 整性。由此得出以下结论：

[0090] H(S(i1,1))＝hi1,1,H(S(i2,2))＝hi2,2……H(S(ik,k))＝hik,k以及H([hi1,1|hi2,2|…|hik, k])＝hSk。

[0091] 然而，检查hSk仍然要进行多次(n×mn)计算。

[0092] 如果动态自适应流式传输系统有信任的(第三)方可以可靠地提供对应于片段S(i,j) 的哈希值hi,j，那么检查接收的片段的完整性可以简化为：

[0093] H(S(i1,1))＝hi1,1,H(S(i2,2))＝hi2,2……H(S(ik,k))＝hik,k。

[0094] 在计算方面，这是最有效的。这是因为当计算随着客户端接收片段而逐步进行时，仅 要求为m×n个哈希值进行m×n次预计算以及为检查流的完整性进行m次计算。

[0095] 但是，假定该信任方可独立联系或通信以提供这些哈希值在实践中可能不现实，

因为 这将引入客户端和该信任方之间额外的通信事务。这产生了其它离线和边线方案。

[0096] 离线方案和边线方案依赖于通过与接收片段的信道不同的信道以全部或按批的形式 向客户端提供预计算的哈希值(只要哈希值变为可用),因此客户端不必请求并接收来自 其它在线服务器的哈希值。

[0097] 如果在客户端(像在视频点播(VOD)的情况下)开始接收片段之前所有片段都可用，所有各个片段S(i,j)的哈希值hi,j可以预计算并在一次通信中(再次,可能通过与获取片段 的信道不同的信道)作为“码本”传递到客户端,如下图所描述的。图5是示出表示组A 的哈希值的码本的图500。

[0098] 在这种情况下,客户端首先需要检查该“码本”的完整性,然后使用该码本像在线情 况一样进行检查：

[0099] H(S(i1,1))＝hi1,1,H(S(i2,2))＝hi2,2……H(S(ik,k))＝hik,k。

[0100] 在许多情况下,在客户端接收这些片段的短时间之前,不是所有的片段都可用(not all segments are available way ahead of time for clients to receive them)。此外,并未预先确定 客户端将接收哪个流,因为客户端可选择根据其网络状况和资源可用性以动态方式接收流 的片段。在这些情形下,随着片段变为可用,仅对哈希值进行计算并提供给客户端。

[0101] 在简单的实际案例中,当客户端接收到片段S(ik,k),(A的第k列中的)所有片段S(i,k)， i＝1,2……m,都可用。这种情形使得可以预计算这些片段的哈希值并将这些哈希值以“向 量”的形式[h1,k,h2,k,…,hm,k]传递给客户端。图6是示出哈希值的向量形式的图600。

[0102] 这样,对于任意k,客户端首先需要检查第k个“向量”的完整性,然后使用它检查是否：

[0103] H(S(ik,k))＝hik,k。

[0104] 有时,当客户端接收到片段S(ik,k),并不知道是否(A的第k列中的)所有片段S(i,k)， i＝1,2……m,都可用。更糟的是,可能不知道是否(A的1到k-1列中的)所有片段都可用，除了客户端已经接收到的片段S(i1,1),S(i2,2),…,S(ik,k)。

[0105] 为了应对这些“非统一”情况,可以使用索引列表(indexed list)方法。这要求当一 些片段S(i,k)变为可用时为所有那些可用片段S(i,k)进行如下预计算

[0106] hi,k＝H(S(i,k))

[0107] 并准备索引列表{(i,k,hi,k)}发送给客户端。在客户端侧,接收到片段S(ik,k)之后,客 户端可检查接收到的列表中是否存在条目(ik,k,hik,k)。如果存在,是否

[0108] H(S(ik,k))＝hik,k。

[0109] 另一个应对“非统一”情况的方法是基于链接。该方法要求当一些片段S(i,k)变为可 用时,不仅为所有那些可用片段S(i,k)计算哈希值

[0110] hi,k＝H(S(i,k))

[0111] 还要为任意两个可用的“邻近”片段计算哈希值

[0112] gi,k,j＝H(hj,k|hj,k-1)。

[0113] 完成这些计算之后,准备两个非索引列表并发送给客户端,一个用于片段哈希值{hj, k},另一个用于“邻近”片段的哈希值{gi,k,j}。在客户端侧,接收到片段S(ik,k)之

后，客户端可计算自己的哈希值

[0114] h＝H(S(ik,k))

[0115] 并检查哈希值是否在片段哈希值的接收列表{hj,k}中。如果是，那么客户端进一步计 算两个“邻近”片段S(ik-1,k-1))和S(ik,k))的哈希值，

[0116] g＝H(hik,k|hik-1,k-1)

[0117] 并检查g是否在“邻近”片段的哈希值{gi,k,j}的接收列表中。如果两个检查都通过了，那么对接收到的片段S(ik,k))的完整性检查是令人满意的。

[0118] 通常情况下，“非统一”实际案例的任意方法可用于“统一”实际案例。例如，索引列表方法相当于“统一”实际案例的“向量”方法，因为索引列表{(i,k,hj,k)}将包括所有(i,k,hj,k)，i＝1,2……m,并成为向量[h1,k,h2,k,…,hm,k]的另一表示。

[0119] 当用于“统一”实际案例，基于链接的方法成为如下：对于k＝1的情况，仅准备了片段的哈希值的一个非索引列表{hi,1|i＝1,…,m}。对于任意k>1的情况，准备了两个非索引列表{hi,1|i＝1,…,m}和{gi,k,j|i,j＝1,…,m}。总体而言，对于整个表示组A，这产 生m×n次哈希值计算和连续片段的所有配对的额外m2×(n-1)次哈希值计算。

[0120] 当用基于链接的方法使“统一”实际案例中的流式传输系统变得平滑时，复杂度可降 低到表示组A的大小的线性顺序O(m×n)，因为这要求m×n次哈希值计算以及连续片段的 所有配对的额外{2×2+(m-2)×3}×(n-1)次哈希值计算。

[0121] 在数字安全文献中，信任方的哈希函数和数字签名通常一起用于提供数字位序列的真 实性。

[0122] 片段内容可出于某种原因(例如商业用途或恶意攻击)而有目的地修改。图7A是示出 了广告插入的图700，图7B是示出了(可能为部分的)内容替换的图702。

[0123] 在DASH中，相同的内容有多个编码版本，并且插入/替换的可能性增大。图8A是示出 了Representations中的进行片段替换的内容的修改的图800(全部或部分替换)。这可在任 意中间节点中发生。

[0124] 在DASH中，在时间-Representation二维空间中，一些片段可进行部分替换。并且，交 换路径并未提前得知，不同组合均有可能。这可能产生组合问题，其中可能性随着表示的 数量和片段的数量而呈指数增长。图8b是示出了交换路径的图802。通常情况下，假定一个片段，实体应该能够用尽可能少的计算和冗余判断该片段是否被修改，该片段是否在原始组内，以及时间顺序是否被改变。

[0125] 动态片段序列的认证包括为各个片段生成签名/摘要，以及按特定顺序连接签名/摘要 以形成消息(组合签名/摘要)。对于一个片段，通过其表示和时间位置从消息中提取其 对应的签名/摘要。将摘要与为片段生成的本地摘要相比以确定该片段是否被以任何方式 (片段自己或时间顺序)修改了。

[0126] 图9是示出了摘要生成的图900。Sij表示来自Representation i的第j个片段。Dij表示片段 Sij的摘要，其反应Sij的特征。摘要Dij的最小位数(示为B)可由表示的数量(示为n:B＝2n+d) 确定，其中d是大于0的整数以确保摘要空间足以从N个表示中区分片段。

[0127] 假定摘要/签名的长度是固定的，并且它们按特定的顺序连接以为如Representation(图 10A)、来自Representation的一组按时间对准的片段(图10B)、或Representation Set(图 10C)形成组合摘要。该组合在时间表示空间中可为不同的顺序：

先时间后表示,或先表 示后时间,如图10a至10c所示。

[0128] 图10A是示出了各个表示的组合摘要的图1000。

[0129] 各个表示均分配有其组合摘要的URL,n个表示就有n个URL。片段无需在表示上保持 一致,当i≠j时,ni可以不等于nj。

[0130] 图10B是示出了来自所有表示的第j个片段的组合摘要1002的图1002。来自表示的每组 片段均分配有其组合摘要的URL,并且其可用时间与片段的可用时间相同。尽管与图10A仅有的微小差别在于组合是按照表示的顺序,这有利于片段通常在表示上保持时间一致以 简单地进行交换的实际案例,同时开始的片段同时或在相近时间可用,它们的摘要/签名 也是如此。

[0131] 图10C是示出了Representation组的组合摘要1004的图1004。给具有n个表示的Representation组的组合摘要分配了URL,该组合摘要可首先按时间顺序然后按表示顺序(如图10C所示),或首先按表示顺序然后按时间顺序(未示出)。片段无需在表示上保 持一致,当i≠j时,ni可以不等于nj。

[0132] 图11A至11D是示出了对于检索出的片段,通过其索引i和j,可从组合摘要中定位片段 的摘要的图1100、1102、1104和1106。请注意,图11d是当片段在表示上保持时间一致(每 个表示包含相同数量的片段)的简化案例。

[0133] 图12是示出了为检索出的片段生成本地摘要/签名的图1200。相比之下,如果S'ij=Sij, 那么认证通过。否则,认证失败。

[0134] 实施例为组合摘要分配了URL。MPD传送组合摘要的URL以表示去何处检索摘要。客户端检索组合摘要。客户端从特定片段中提取摘要。客户端将提取出的摘要与为片段生成的本地摘要相比并得出结论。

[0135] 动态片段序列的认证的实施例方法包括为各个片段生成签名/摘要,以及按特定顺序 连接签名/摘要以形成消息(组合签名/摘要)。对于一个片段,通过其表示和时间位置从 消息中提取其对应部分的签名/摘要。将消息与为片段生成的本地消息相比以确定该片段 是否被以任何方式(组或时间顺序)修改了。该方法可在服务器/存储器/客户端系统上实 施。

[0136] 用于轻量级部分加密的实施例方法包括为各个片段生成签名/摘要以及按特定顺序 (时间表示)连接签名/摘要以形成组合签名/摘要。该方法包括为检索出的片段生成签名/ 摘要,称为A。根据片段的时间位置和Representation,该方法包括生成掩码以从组合签名/ 摘要中提取对应部分,称为B。该方法将A与B进行比较以确定片段是否被修改。

[0137] 在系统/客户端方法中,第一方为片段集生成(具有片段的二维信息的)消息。第二方使用该消息确定检索出的片段是否被修改(集合和时间顺序都未改变)。

[0138] 实施例认证动态序列,使得需要较少的通信(不是每个片段都需要进行通信)。在案 例(a)中提取了N个组合摘要/签名,而在案例(b)中提取了单个组合摘要/签名。实施例认证计算复杂度较低的动态序列。实施例提升了安全性来检测媒体内容是否已被修改、片段是否被修改以及时间顺序是否改变(improved security enabling detection if media content has been modified whether segment is modified or the temporal order is changed)。

[0139] 图13示出了用于验证自适应流媒体的片段完整性和真实性的实施例方法1300的

流程 图。方法1300始于方框1302。在方框1302，客户端接收媒体流的片段。在方框1304，客户 端确定媒体流的数字签名。在方框1306，客户端从信任源接收所接收片段的正确的数字签 名。在方框1308，客户端将确定的数字签名与正确的数字签名相比较，并且在方框1310确定两个数字签名是否相同。如果在方框1310处两个数字签名相同，那么方法1300前进到方框1312。在方框1312，客户端确定片段是真实的并继续恰当地处理该片段，随后，方法1300可结束。如果在方框1310处客户端确定两个数字签名不同，那么方法1300前进到方框1314。在方框1314，客户端确定片段已被修改。

[0140] 方法1300随后前进到方框1316。在方框1316，客户端可丢弃片段并请求媒体源服务器 重发片段，随后，方法1300可结束。

[0141] 图14是处理系统1400的方框图，处理系统1400可以用来实现本文公开的设备和方法。特定设备可以利用所示的所有部件，或仅部件的子集，而集成水平可随设备而异。此外， 设备可以包含部件的多个实例，如多个处理单元、处理器、存储器、发射器、接收器等等。处理系统1400可以包括配备有一个或多个输入/输出设备的处理单元1401，所述输入/输出 设备包括扬声器、麦克风、鼠标、触摸屏、小键盘、键盘、打印机、显示器等等。处理单元可以包括中央处理器(CPU)1402、存储器1408、大容量存储设备1404、视频适配器1410 以及连接至总线1414的I/O接口1412。

[0142] 总线1414可是一个或多个任意类型的若干总线架构，包括存储总线或存储控制器、外 设总线以及视频总线等等。CPU1402可包括任意类型的电子数据处理器。存储器1408可包 括任意类型的系统存储器，例如静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、同步DRAM(SDRAM)、只读存储器(ROM)或其组合等等。在实施例中， 存储器1408可包括在开机时使用的ROM以及执行程序时使用的存储程序和数据的 DRAM。

[0143] 大容量存储设备1404可包括任意类型的存储设备，其用于存储数据、程序和其它信息， 并使这些数据、程序和其它信息通过总线1414访问。大容量存储设备1404可包括如下项中 的一种或多种:固态磁盘、硬盘驱动器、磁盘驱动器、光盘驱动器等等。

[0144] 视频适配器1410和I/O接口1412提供接口将外部输入输出设备耦合到处理单元1401。如图所示，输入输出设备的示例包括耦合到视频适配器1410的显示器1416和耦合到I/O接 口1412的鼠标/键盘/打印机1418。其它设备可以耦合到处理单元1401，并且可以利用附加 的或更少的接口卡。例如，可使用如通用串行总线(USB)(未示出)等串行接口卡将接 口提供给打印机。

[0145] 处理单元1401还包括一个或多个网络接口1406，其可包括以太网电缆等有线链路，和 /或接入节点或者不同网络1420的无线链路。网络接口1406允许处理单元1401通过网络 1420与远程单元通信。例如，网络接口1406可以通过一个或多个发射器/发射天线以及一 个或多个接收器/接收天线提供无线通信。在实施例中，处理单元1401耦合至局域网或广 域网用于数据处理并与远程设备进行通信，远程设备可包括其它处理单元、因特网、远程 存储设施等等。

[0146] 尽管进行了详细的描述，但应理解，可在不脱离由所附权利要求书界定的本发明的精 神和范围的情况下，对本文做出各种改变、替代和更改。此外，本发明的范围不希望限于 本文中所描述的特定实施例，所属领域的一般技术人员将从本发明中容易了解到，过程、机器、制造工艺、物质成分、构件、方法或步骤(包括目前存在的或以后将开发的)可执

行与本文所述对应实施例大致相同的功能或实现与本文所述对应实施例大致相同的效果。因此,所附权利要求书既定在其范围内包括此类过程、机器、制造工艺、物质成分、构件、方法或步骤。

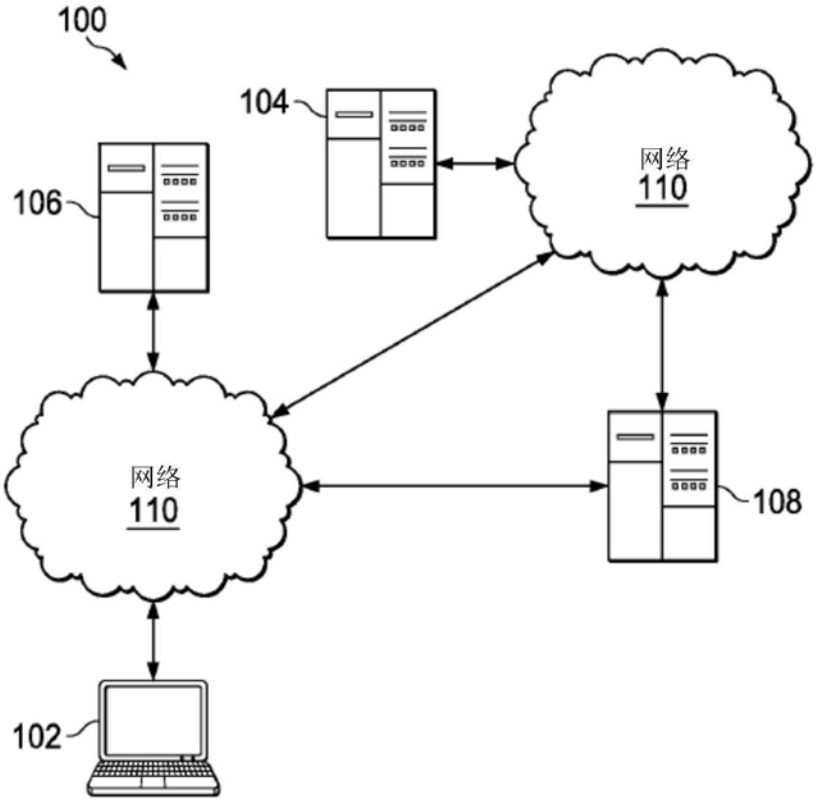

100
104
106
网络
110
网络
110
108
102

图1

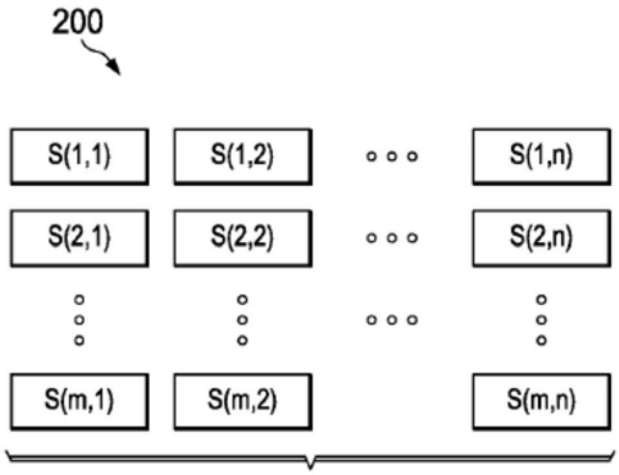

200
S(1,1)
S(1,2)
S(1,n)
S(2,1)
S(2,2)
S(2,n)
S(m,1)
S(m,2)
S(m,n)

图2

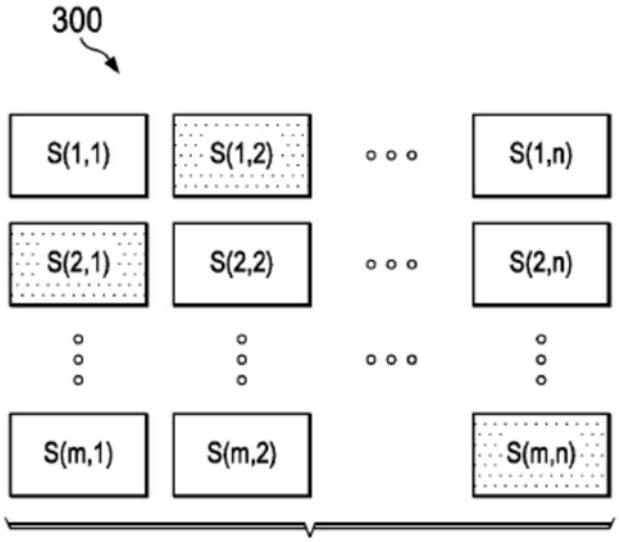

300
S(1,1)
S(1,2)
S(1,n)
S(2,1)
S(2,2)
S(2,n)
S(m,1)
S(m,2)
S(m,n)

图3

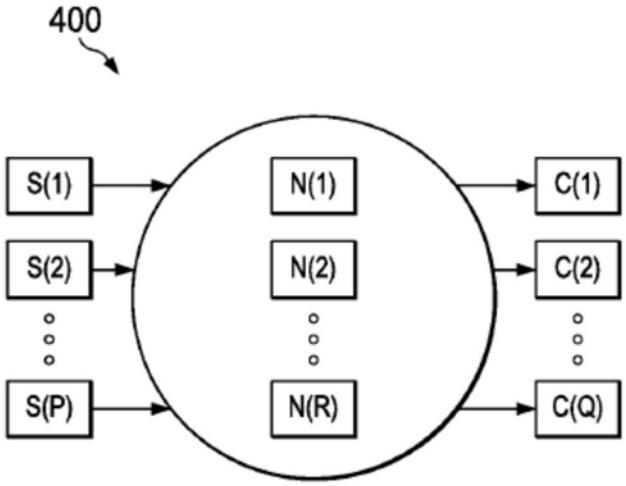

400
S(1)
S(2)
S(P)
N(1)
N(2)
N(R)
C(1)
C(2)
C(Q)

图4

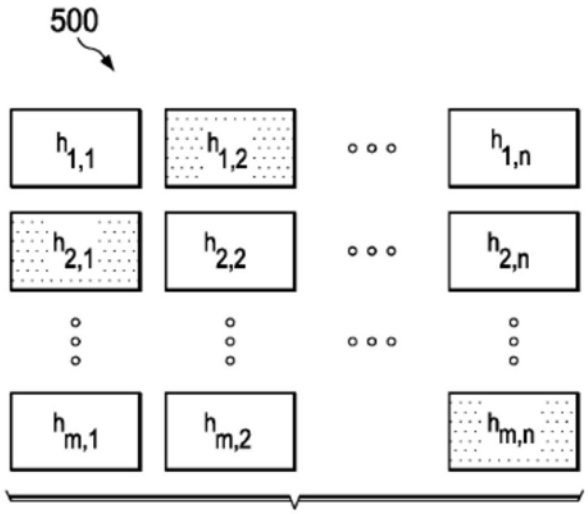

500
h1,1
h1,2
h1,n
h2,1
h2,2
h2,n
hm,1
hm,2
hm,n

图5

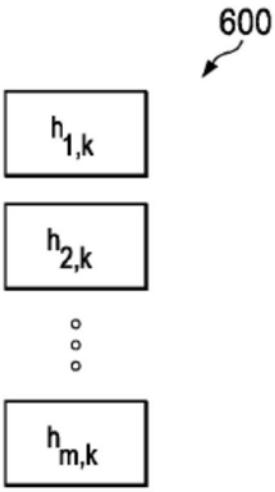

600
h1,k
h2,k
hm,k

图6

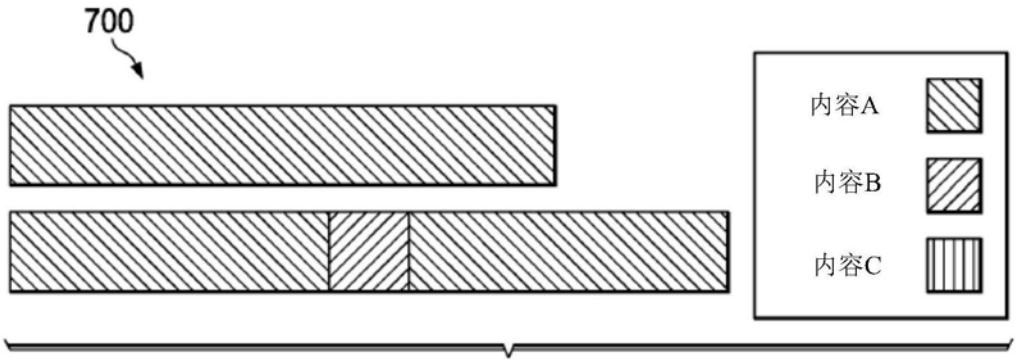

700
内容A
内容B
内容C

图7A

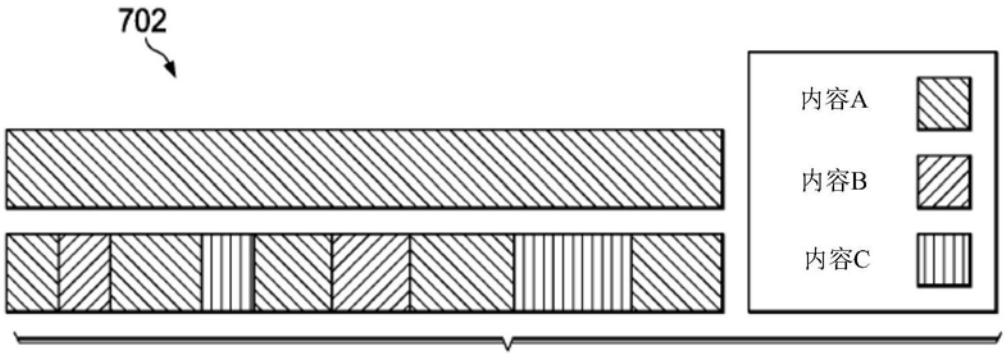


图7B

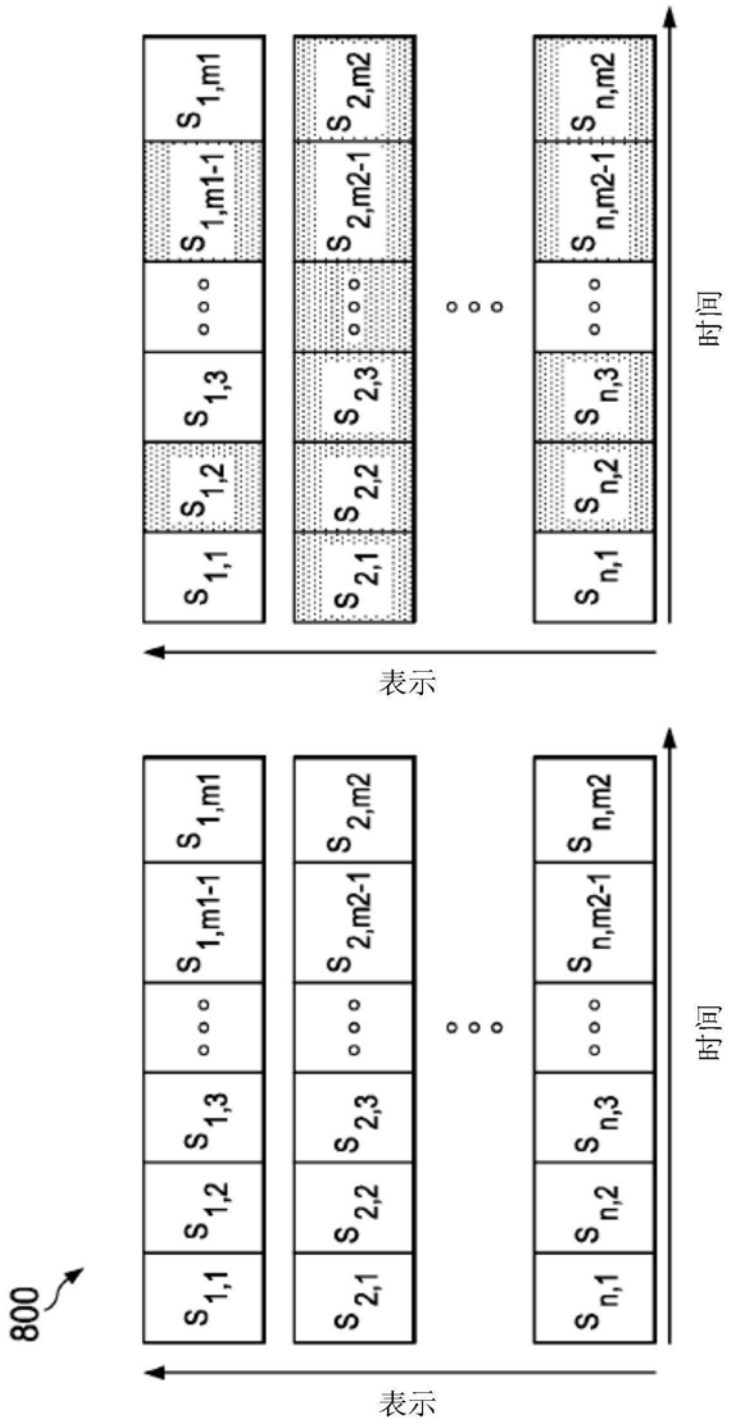

800
$S_{1,1}$ $S_{1,2}$ $S_{1,3}$ ... $S_{1,m1-1}$ $S_{1,m1}$
$S_{2,1}$ $S_{2,2}$ $S_{2,3}$ ... $S_{2,m2-1}$ $S_{2,m2}$
$S_{n,1}$ $S_{n,2}$ $S_{n,3}$ ... $S_{n,m2-1}$ $S_{n,m2}$
表示
时间
$S_{1,1}$ $S_{1,2}$ $S_{1,3}$ ... $S_{1,m1-1}$ $S_{1,m1}$
$S_{2,1}$ $S_{2,2}$ $S_{2,3}$ ... $S_{2,m2-1}$ $S_{2,m2}$
$S_{n,1}$ $S_{n,2}$ $S_{n,3}$ ... $S_{n,m2-1}$ $S_{n,m2}$
表示
时间

图8A

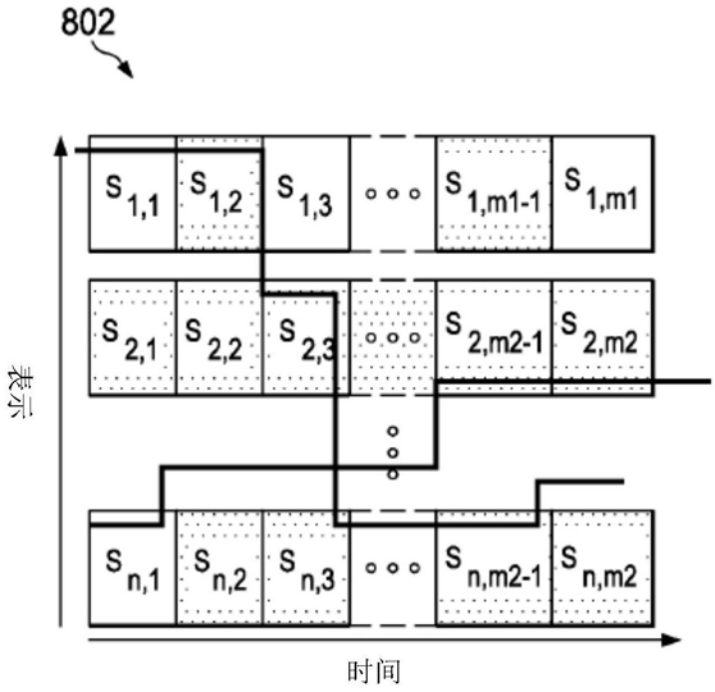

802
S 1,1
S 1,2
S 1,3
S 1,m1-1
S 1,m1
S 2,1
S 2,2
S 2,3
S 2,m2-1
S 2,m2
S n,1
S n,2
S n,3
S n,m2-1
S n,m2
表示
时间

图8B

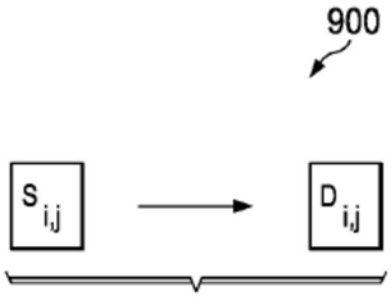

900
S i,j
D i,j

图9

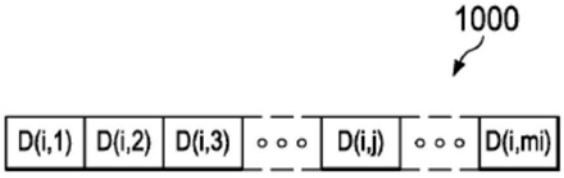

1000
D(i,1)
D(i,2)
D(i,3)
D(i,j)
D(i,mi)

图10A

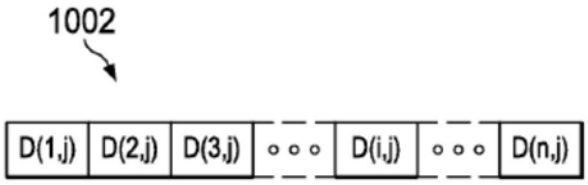


图10B



图10C

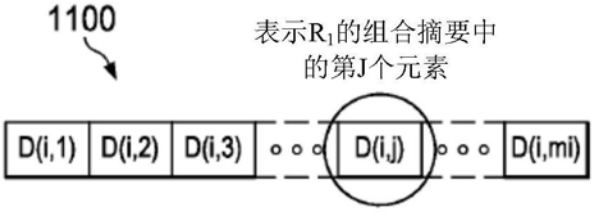


图11A

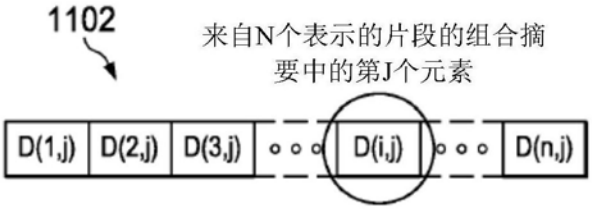


图11B

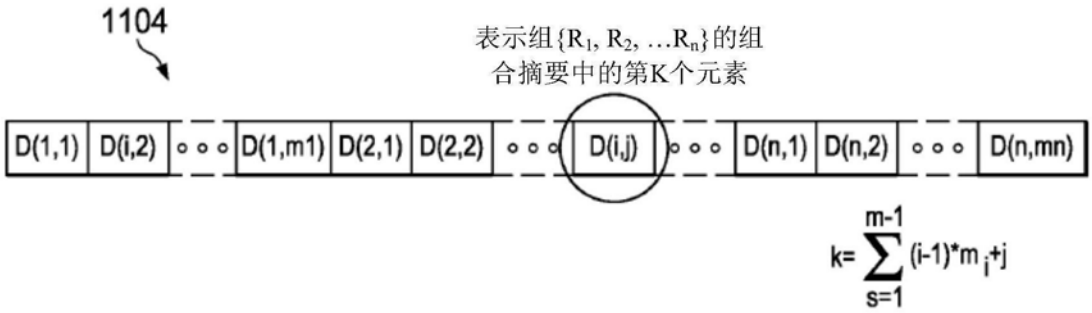


图11C

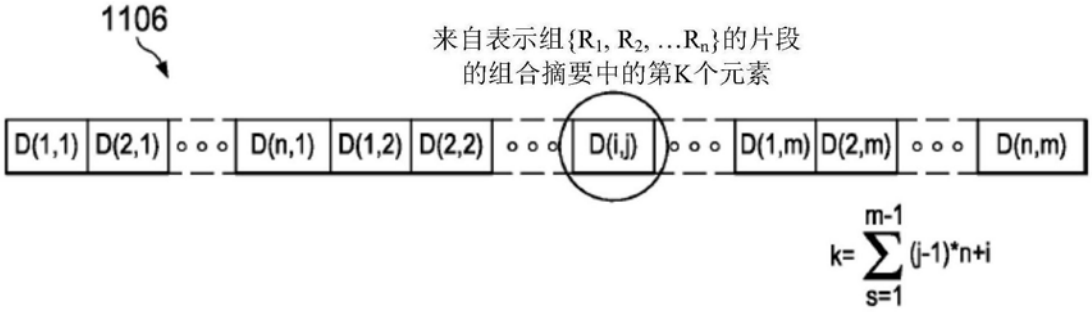


图11D

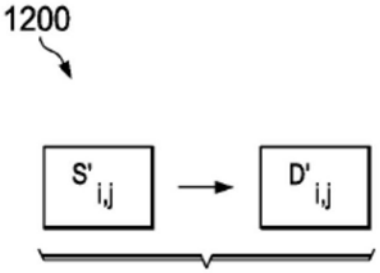


图12

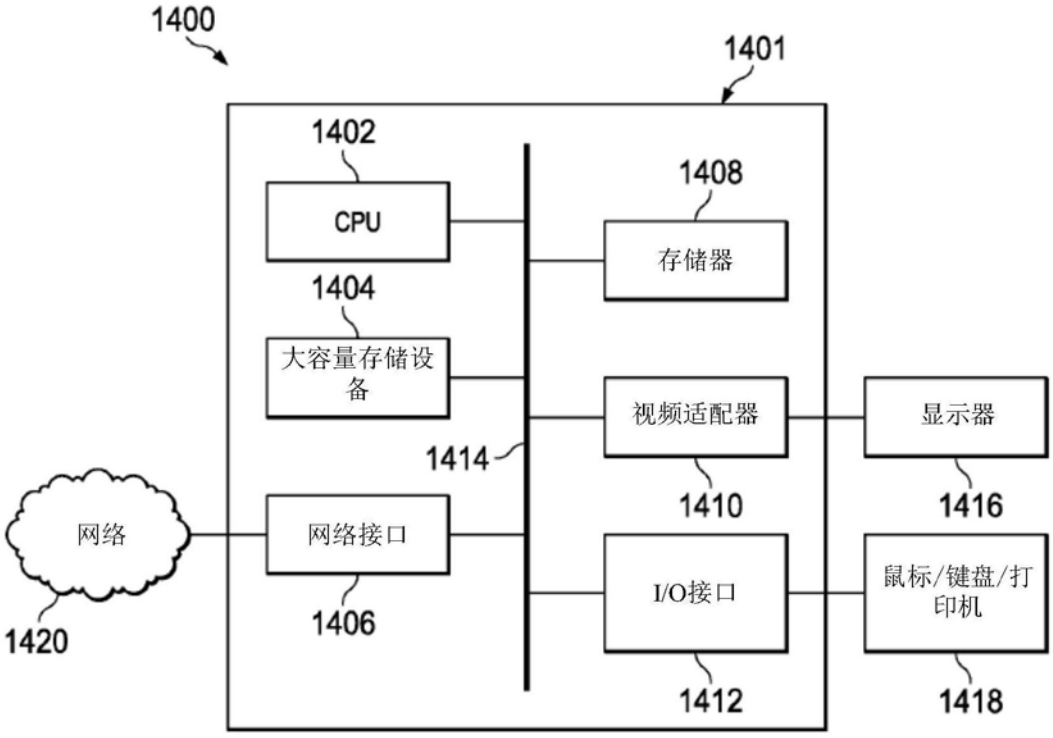

1400
1401
1402
CPU
1404
大容量存储设备
1408
存储器
视频适配器
显示器
1414
1410
1416
网络
网络接口
I/O接口
鼠标/键盘/打印机
1420
1406
1412
1418

图14

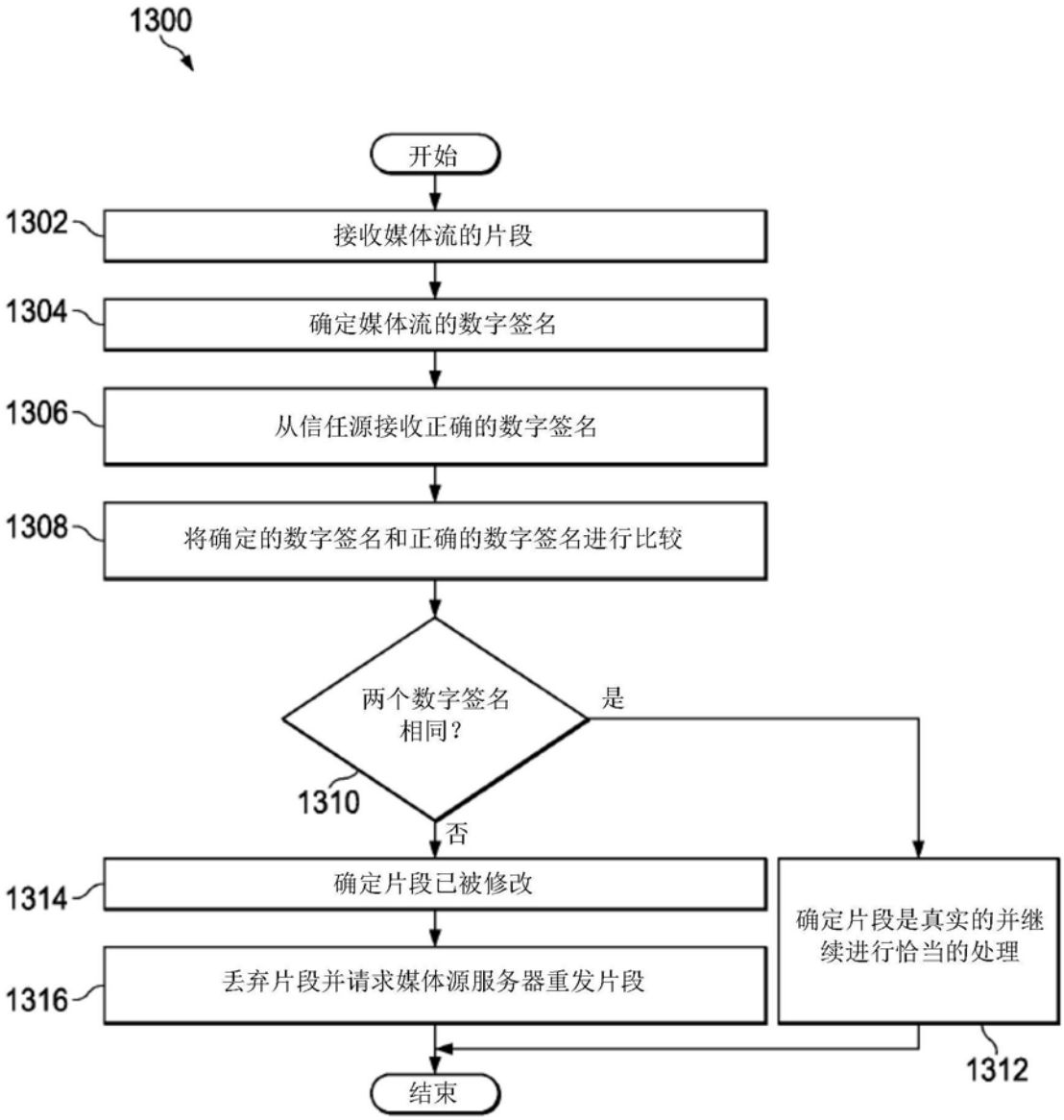

1300
开始
1302
接收媒体流的片段
1304
确定媒体流的数字签名
1306
从信任源接收正确的数字签名
1308
将确定的数字签名和正确的数字签名进行比较
两个数字签名
相同?
1310
是
否
1314
确定片段已被修改
1316
丢弃片段并请求媒体源服务器重发片段
确定片段是真实的并继续进行恰当的处理
1312
结束

图13