(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116233568 A
(43)申请公布日 2023.06.06

(21)申请号 202211493213.3

(22)申请日 2022.11.25

(30)优先权数据
21212291.5 2021.12.03 EP

(71)申请人 安讯士有限公司
地址 瑞典浪德

(72)发明人 比约恩·沃尔克
斯蒂芬·伦德贝里

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
专利代理师 梁洪源 康泉

(51)Int.Cl.
H04N 21/835(2011.01)
H04N 19/169(2014.01)
H04L 9/32(2006.01)

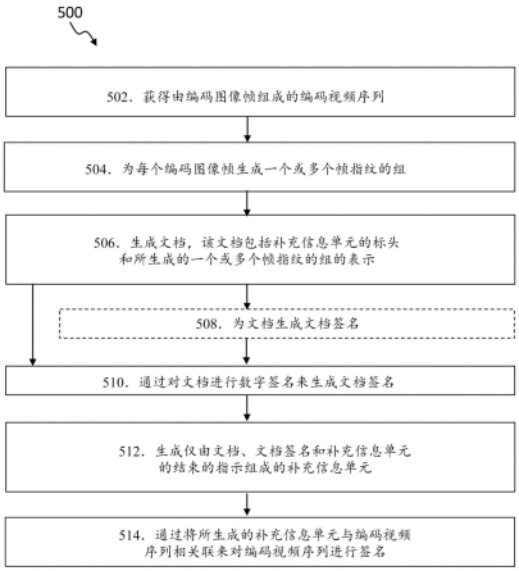
权利要求书2页 说明书11页 附图9页

(54)发明名称

用于对编码视频序列进行签名的方法和装置

(57)摘要

用于对编码视频序列进行签名的方法和装置,包括:获得(502)由编码图像帧组成的编码视频序列;为每个编码图像帧生成(504)一个或多个帧指纹的组;生成(506)文档,该文档包括补充信息单元的标头和所生成的一个或多个帧指纹的组的表示;通过对文档进行数字签名来生成(510)文档签名;生成(512)仅由文档、文档签名和补充信息单元的结束的指示组成的补充信息单元;以及通过将所生成的补充信息单元与编码视频序列相关联来对编码视频序列进行签名(514)。



CN 116233568 A

1.一种对编码视频序列进行签名的方法,所述方法包括:

获得由编码图像帧组成的编码视频序列;

为每个编码图像帧生成一个或多个帧指纹的组,其中,帧指纹是编码图像帧的唯一标识符;

生成文档,所述文档包括补充信息单元的标头以及所生成的一个或多个帧指纹的组的表示;

通过对所述文档进行数字签名来生成文档签名;

生成仅由所述文档、所述文档签名和所述补充信息单元的结束的指示组成的所述补充信息单元;和

通过将所生成的补充信息单元与所述编码视频序列相关联来向所述编码视频序列提供签名。

2.根据权利要求1所述的方法,进一步包括:

为所述文档生成文档指纹;并且其中,为所述文档生成所述文档签名包括:

通过对所述文档指纹进行数字签名来生成所述文档签名。

3.根据权利要求1所述的方法,其中,所述文档进一步包括以下中的一项或多项:被包括在所述补充信息单元中的有效载荷的有效载荷大小值、所述有效载荷的标识符、与所述编码视频序列有关的元数据、与捕获所述视频序列的相机有关的相机信息以及非对称加密密钥对的公钥。

4.根据权利要求1所述的方法,其中,所生成的补充信息单元通过对所述编码视频序列的参考而与所述编码视频序列相关联,并且在与传输所述编码视频序列的信道不同的信道上被传输。

5.根据权利要求1所述的方法,其中,通过在所述编码视频序列的结束处添加生成的补充信息,将所生成的补充信息单元与所述编码视频序列相关联。

6.根据权利要求1所述的方法,其中,所述编码视频序列包括编码图像帧的与第一图片组相关联的第一部分以及编码图像帧的与第二图片组相关联的直接随后的第二部分,其中,所生成的补充信息单元是为编码图像帧的所述第一部分生成的,并且其中,通过在与编码图像帧的所述第一部分相关联的所述第一图片组之后添加所生成的补充信息单元,将所生成的补充信息单元与所述编码视频序列相关联。

7.根据权利要求6所述的方法,其中,通过将生成的补充信息在与编码图像帧的所述第二部分相关联的所述第二图片组之前添加到所述编码视频序列,将所生成的补充信息单元与所述编码视频序列相关联。

8.根据权利要求6所述的方法,其中,通过将生成的补充信息作为与编码图像帧的所述第二部分相关联的所述第二图片组的一部分添加到所述编码视频序列,来将所生成的补充信息单元与所述编码视频序列相关联。

9.根据权利要求1所述的方法,其中,所述编码图像帧包括至少一个帧内帧和一个或多个预测的帧间帧,其中,通过规定时间视频压缩的视频编码格式对所述至少一个帧内帧和所述一个或多个预测的帧间帧进行编码。

10.根据权利要求9所述的方法,其中,所生成的一个或多个帧指纹的组的所述表示包括:所述至少一个帧内帧的生成的指纹(H_I)和所述一个或多个预测的帧间帧中的每个预测

的帧间帧的生成的指纹(H_P)。

11.根据从属于权利要求6时的权利要求9所述的方法,其中,所生成的一个或多个帧指纹的组的所述表示包括:所述第一图片组的帧内帧的生成的指纹(H_I)、所述第一图片组的每个预测的帧间帧的生成的指纹(H_P)和所述第二图片组的帧内帧的生成的指纹(H_I)。

12.根据权利要求10所述的方法,其中,每个预测的帧间帧的生成的指纹(H_P)通过对源自所述预测的帧间帧的数据和源自所述预测的帧间帧直接地或间接地参考的帧内帧的数据的组合进行哈希来生成,其中,所述预测的帧间帧的所述指纹独立于所述预测的帧间帧直接地或间接地参考的任何其他的预测的帧间帧,其中,源自所述预测的帧间帧的所述数据包括所述预测的帧间帧的图像数据和所述预测的帧间帧的图像数据的生成的第一指纹中的一个,并且其中,源自所述帧内帧的所述数据是所述帧内帧的生成的第一指纹。

13.根据权利要求9所述的方法,其中,所述帧内帧是根据H.26x压缩格式编码的I帧或根据AOMedia Video 1、AV1、压缩格式编码的帧内帧或关键帧,并且其中,所述预测的帧间帧是根据H.26x压缩格式编码的前向预测的帧间帧P帧或双向预测的帧间帧B帧或者根据所述AV1压缩格式编码的帧间帧。

14.一种包括被布置为执行根据权利要求1所述的方法的处理电路的装置。

15.一种非暂时性计算机可读存储介质,其上存储有包括指令的计算机程序,当所述程序由计算机执行时使所述计算机执行根据权利要求1所述的方法。

用于对编码视频序列进行签名的方法和装置

技术领域

[0001] 本公开涉及用于保护视频序列免受未经授权的活动的安全措施的领域。具体地，提出了用于对编码视频序列(encoded video sequence)进行签名的方法和装置。

背景技术

[0002] 视频序列是视频帧的有序序列，并且视频帧由像素组成。如果对共同的场景进行成像，则连续的视频帧将具有强相关性。在给定过去帧的情况下预测一个视频帧的能力是基于预测的编码的基本假设。基于预测的编码可以被描述为特别适用于视频序列的数据压缩技术。

[0003] 用作预测其他帧的参考的视频帧被称为参考帧。在没有来自其他帧的信息的情况下编码的帧被称为帧内编码帧、帧内帧、I帧或关键帧。使用来自一个或多个参考帧的预测的帧被称为帧内编码帧或帧间帧。P帧是使用来自单个先前参考帧(或用于每个区域的预测的单个帧)的预测的帧间帧，并且B帧是使用来自两个参考帧(一个先前帧和一个后续帧)的预测的帧间帧。帧有时被称为图片。国际电信联盟ITU-T H.264(2021年8月)建议书“通用视听服务的高级视频编码”规定了一种视频编码标准，其中使用了前向预测帧和双向预测帧。

[0004] 图1图示出由I帧和P帧组成的基于预测的编码视频序列的片段。如上所提及，I帧是具有通过预限定的关联解码操作可以被解码为解码后的视频帧(或视频帧的解码后的部分)的独立可解码的图像数据的数据结构。就其自身而言，P帧是一种数据结构，其关联的解码操作不仅参考P帧自身的图像数据，而且还参考至少一个其他I帧或P帧。从概念上稍微简化地来讲，P帧中的图像数据表示相对于它先前的I帧或P帧编码的视频帧的变化或移动。如果解码操作成功，则从P帧和I帧解码的视频帧通常无法区分。

[0005] 帧间相关性在图1中指示为指向负时间方向t的弧形箭头。在所描绘的简单示例中，每个P帧参考紧接先前的I帧或P帧。如果第一P帧参考第二P帧，则第二P帧必然地参考至少一个进一步的I帧或P帧。在本公开中，第一P帧被称为直接参考第二P帧并且间接参考至少一个进一步的I帧或P帧。因为I帧中的图像数据是独立可解码的，所以参考链(弧形箭头)不继续经过I帧。I帧和后续直接或间接参考I帧的P帧的组合可以被称为图片组，在一些编码格式中被称为GOP。在图1中指示了四个GOP：IPP、IPPPP、IPPP、IPPP。

[0006] 数字签名为通过非安全通道传输的数字消息提供了一层验证和安全。通过数字签名，数字消息的接收者可以验证消息的真实性或完整性。不言而喻，视频数据(例如，视频序列，作为一种特殊情况)可以被数字签名以对视频数据提供一层验证和安全。可以通过对视频数据的指纹而不是视频数据自身进行签名来签名视频数据。在图1的下部中图示出逐帧指纹H_I,H_P的使用，其中每个指纹可以是该视频帧的图像数据的哈希或者该视频帧的图像与可选的进一步信息的结合的哈希。GOP的签名S1、S2、S3、S4通过对该GOP中的指纹的组合进行数字签名来获得。如图1中所图示，如果I帧指纹H_I既作为其自身GOP的一部分被签名，又作为先前GOP的签名的一部分被签名，则可以进一步保护视频序列的安全性以防止未经授权的替换、移除或插入完整的GOP。注意，上排中的直向下箭头表示哈希函数，并且下排中的

箭头表示数字签名。

[0007] 然而,即使如上所描述对视频序列进行数字签名,视频序列仍可能暴露于欺诈性操纵,因为例如,在视频序列中的第一GOP之前数据可能被添加到视频中。进一步,如果I帧指纹H_I既没有作为其自身的GOP的一部分被签名也没有作为前一个GOP的签名的一部分被签名,则一个或多个GOP可能被删除、添加或替换,但存在无法检测到这种操纵的风险。

[0008] US2008/0291999A1公开了用于标记符合H.264/AVC标准或等效数字视频流的单个视频帧的方法和装置。H.264/AVC视频流中的每个视频帧常规上被划分为NAL单元。每个视频帧通常存在许多NAL单元。在H.264/AVC标准中规定了补充增强信息(SEI)类型。SEI类型包括可以包含任意数据的用户数据未注册类型。在所公开的方法和装置中,该类型的NAL单元被提供在每个视频帧的开始,在与该视频帧相关联的其他NAL单元之前。图2中示意性地图示出这一点。包含在特殊SEI单元中的有效载荷数据(有时称为SEI数据)通常是用于视频内容的使用的下游控制的控制信息。SEI数据的示例是流定位数据,诸如视频帧号;码流码率,诸如正常、快进;解密数据,诸如解密密钥或者密钥导出种子;和验证元素,诸如校验和(checksum)、哈希函数值或签名。因此,SEI数据可以包括解密加密视频帧所需的解密数据,诸如解密密钥或密钥导出种子。进一步,SEI数据可以包括验证签名后的视频帧所需的验证数据,诸如校验和、哈希函数值或签名。

[0009] 在US2008/0291999A1中声明了,SEI NAL单元自身可以被加密和/或被签名(被验证),使得其中包含的信息不容易被未经授权的用户访问。这可以被理解为:1)整个SEI可以被加密和/或被签名,或者2)SEI中包含的信息可以被加密和/或被签名。

[0010] 如果该声明被理解为1)整个SEI可以被加密和/或被签名,US2008/0291999A1既没有解释如何完成SEI的加密和/或签名(验证)使得其中包含的信息不容易访问,也没有解释在哪里存储或者如何传输对加密后和/或签名后的SEI进行解密和/或验证所需的SEI解密数据和/或SEI验证数据。进一步,如果整个SEI要被加密,则这种加密后的SEI的接收者将无法将它识别为SEI,因为它已被加密。此外,接收者将无法忽略加密后的SEI并处理序列中的下一个NAL单元,因为接收者不知道加密后的SEI的长度。因此,该声明不能被理解为整个SEI被加密或者被签名。

[0011] 因此,该声明应被理解为2)SEI中包含的信息可以被加密和/或被签名。SEI中包含的信息被理解为SEI数据,并且因此,SEI数据似乎可能被加密和/或被签名(被验证)。如果SEI数据与视频帧的加密和签名类似地被加密和/或被签名,则假设SEI可以在有效载荷中包括对加密后和/或签名后的SEI数据进行解密和验证所需的解密数据和/或验证数据。图3示意性地图示出根据现有技术的SEI。现有技术的SEI由标头、关于有效载荷大小的信息、通用唯一标识符(UUID)、有效载荷(例如,SEI数据)和指示SEI结束的停止位组成。可替代地,假设解密数据和/或验证数据通过另一传输信道传输到接收者。因此,假设在US 2008/0291999 A1中公开的SEI的有效载荷,除了加密后和/或签名后的SEI数据之外,还可以包括对加密后和/或签名后的SEI数据进行解密和/或验证所需的解密数据和/或验证数据,或者这样的解密数据和/或验证数据从另一传输通道发送。

[0012] 这样的解决方案会产生安全风险,其中只有一部分有效载荷(即SEI数据)被加密和/或被签名,因为有可能篡改SEI的其他部分,诸如增加有效载荷的大小,从而使得可以在使用签名后的SEI数据和加密数据和/或验证数据进行加密和/或验证时在SEI中引入附加

的数据而不会引起注意。

[0013] 示例说明了用于对编码视频序列进行签名(例如,数字签名)的可用方法的缺点。

发明内容

[0014] 本公开的一个目的是提供具有防止未经授权的视频帧的替换、移除或插入的机制的用于对编码视频序列进行签名(例如,数字签名)的方法和装置。进一步的目的是提供机制来检测编码视频序列的操纵的发生。

[0015] 这些和其他目的由独立权利要求所限定的本发明实现。

[0016] 在本发明的第一方面中,提供了一种对编码视频序列进行签名的方法。该方法包括:获得由编码图像帧组成的编码视频序列;为每个编码图像帧生成一个或多个帧指纹的组;生成文档,该文档包括补充信息单元的标头和所生成的一个或多个帧指纹的组的表示;通过对文档进行数字签名来生成文档签名;生成仅由文档、文档签名和补充信息单元的结束的指示组成的补充信息单元;以及通过将所生成的补充信息单元与编码视频序列相关联来对编码视频序列进行签名。

[0017] 在本公开中,术语“指纹”应被理解为数据项的唯一标识符。数据项的指纹可以通过对数据项或数据项的子集进行哈希(即通过对数据项或数据项的子集执行哈希操作)获得。可替代地,可以通过对数据项或数据项的子集执行诸如校验和(checksum)操作的不同的操作来获得指纹。获得数据项的指纹的又一替代方案是对数据项或数据项的子集进行数字签名。数据项可以是对视频帧进行编码的图像数据或图像数据的一部分。可能地,数据项可以与诸如加密盐(cryptographic salt)或者时间戳的其他数据进行组合。

[0018] 进一步,在本公开中,术语“帧指纹”应被理解为帧的指纹,例如编码图像帧的指纹。当编码图像帧可以由多个单元(例如,H.26x编码格式的网络抽象层(NAL)单元或者AV1编码格式的开放比特流单元(OBU))组成时,可以为多个单元中的每一个生成帧指纹,并且因此,可以为每个编码图像帧生成一个或多个这样的帧指纹的组。

[0019] 每个NAL单元包括指定NAL单元的类型的标头,例如,NAL单元是否与诸如帧内帧或帧间帧的编码图像帧有关,或者NAL单元是否与补充信息单元有关。除了标头之外,每个NAL单元还包括有效载荷。每个OBU具有提供被包含在OBU中的数据(有效载荷)的识别信息的标头(AV1比特流和解码过程规范,https://aomediacodec.github.io/av1-spec/av1-spec.pdf)。

[0020] 在本公开中,术语“文档”应被理解为文本文件或诸如字节流或比特流的另一数据结构。术语“文档签名”是指文档的数字签名,并且通过文档签名可以验证文档的真实性。此外,在本公开中,术语“补充信息单元(SIU)”应被理解为被配置为包括关于或与编码视频序列有关的补充信息的单元或消息。补充信息单元例如可以是H.26x编码格式的补充增强信息(SEI)消息或AV1编码格式的元数据开放比特流单元(OBU)。补充信息单元的标头包括补充数据,诸如补充信息单元的指示,即,将补充信息单元指示为补充信息单元的指示。通过读取指示,解码器将知道要解码的单元的类型。

[0021] 所生成的一个或多个帧指纹的组的表示可以是或者包括来自所有所生成的一个或多个帧指纹的组的帧指纹的组或列表或者来自所有所生成的一个或多个帧指纹的组的帧指纹的一部分的组或列表。可替代地,表示可以是或者包括来自所有所生成的一个或多

个帧指纹的组的帧指纹的一个或多个哈希或者来自所有所生成的一个或多个帧指纹的组的帧指纹的一部分的一个或多个哈希。

[0022] 通过表述“通过将生成的补充信息单元与编码视频序列相关联来对编码视频序列进行签名”,应理解,包括文档和文档签名的生成的补充信息单元与编码视频序列相关联,以对编码视频序列进行签名(例如,数字签名)。这也可以表述为编码视频序列被提供有签名,这是由于包括文档和文档签名的生成的补充信息单元与编码视频序列的关联。签名后的编码视频序列和关联的补充信息单元的接收者将使用补充信息单元的文档和文档签名来验证编码视频序列。文档和文档签名可以被称为编码视频序列的签名。如将在本公开中描述的,所生成的补充信息单元可以以不同方式与编码视频序列相关联。通过生成仅由文档、文档签名和补充信息单元的结束的指示组成的补充信息单元;并且通过将所生成的补充信息单元与编码视频序列相关联来对编码视频序列进行签名,将不可能在没有检测的情况下例如使用文档操纵补充信息单元。原因是如果在文档签名生成之后文档被修改了,则无法通过文档签名正确地验证文档。例如,如果文档和文档签名在装置处生成并且在传输给接收者之前由装置包含在与编码视频序列相关联的补充信息单元中,并且如果SEI在传输之后但在它到达接收者之前被修改,接收者将无法使用接收到的文档签名验证文档的真实性。如果文档的真实性无法被验证,接收者将了解编码视频序列已暴露于某种未经授权的活动,并且可以采取必要的行动。

[0023] 在详细描述和从属权利要求中给出了关于本发明第一方面的实施例的进一步细节。

[0024] 在本发明的第二方面中,提供了一种被布置为执行本文中所公开的方法的装置。概况地说,本发明的第二方面共享第一方面的效果和优点,并且可以通过相应程度的技术变化来实施。

[0025] 本发明的第三方面涉及一种包含指令的计算机程序,该指令用于使计算机执行本公开中描述的方法。计算机程序可以存储或分发在数据载体上。如本文中使用的,“数据载体”可以是诸如调制的电磁波或者光波的瞬态数据载体或者非瞬态数据载体。非瞬态数据载体包括易失性和非易失性存储器,诸如磁的、光学的或固态类型的永久和非永久存储介质。这样的存储器可以是固定地安装的或便携式的,仍然在“数据载体”的范围内。

[0026] 通常,权利要求中使用的所有术语均应根据它们在技术领域中的普通含义进行解释,除非本文另外明确地限定。所有对“一/一个/该元件、设备、组件、装置、步骤等”的引用都应开放地解释为指元件、设备、组件、装置、步骤等的至少一个实例,除非另外明确地声明。除非明确地声明,否则本文中公开的任何方法的步骤不必按照所描述的确切顺序执行。

附图说明

[0027] 现在参照附图以示例的方式描述各个方面和实施例,在附图中:

[0028] 图1示意性地图示出基于预测的编码视频序列的片段,以及伴随的逐帧指纹和从这些生成的签名;

[0029] 图2示意性地图示出视频序列的片段,其中每个视频帧之前是根据现有技术的SEI;

[0030] 图3示意性地图示出根据现有技术的SEI;

[0031] 图4示意性地图示出根据本发明实施例的被布置为执行对编码视频序列进行签名的装置；

[0032] 图5是根据本发明的实施例的用于对编码视频序列进行签名的方法的流程图；

[0033] 图6A至图6D分别示意性地图示出编码视频序列、补充信息单元、文档的第一示例和文档的第二示例；并且

[0034] 图7A至图7E示意性地图示出签名后的编码视频序列的实施例。

具体实施方式

[0035] 现在将在下文中参照附图更充分地描述本公开的各方面，其中示出了本发明的某些实施例。然而，这些方面可以以许多不同的形式体现并且不应被解释为限制性的；相反，这些实施例以示例的方式提供，使得本公开将是彻底的和完整的，并且将本发明的所有方面的范围充分地传达给本领域技术人员。相同的附图标记在整个描述中指代相同的元件。

[0036] 为了实现上述目的，本发明描述了用于对编码视频序列进行签名的方法和装置。具体地，通过将编码视频序列与特殊的补充信息单元相关联来对编码视频序列进行签名，该补充信息单元被生成为仅由文档、文档签名和补充信息单元的结束的指示组成。补充信息单元可以是H.26x编码格式的SEI消息或AV1编码格式的元数据OBU。由于补充信息单元仅包括这三个组件而没有其他组件，因此不可能在不检测的情况下操纵补充信息单元的内容(例如，更改文档)，因为任何篡改都将导致文件验证失败。因此，补充信息单元的接收者将理解已经对补充信息单元的内容进行了操纵。下面将更详细地描述用于对编码视频序列进行签名的方法和装置。

[0037] 参照图5，将描述对编码视频序列进行签名的方法500。方法500可以应用于由使用基于预测的编码进行编码的编码图像帧(encoded image frames)组成的任何编码视频序列。例如，编码图像帧可以包括至少一个帧内帧和一个或多个预测的帧间帧。至少一个帧内帧和一个或多个预测的帧间帧可以通过规定时间视频压缩的视频编码格式来编码。帧内帧可以是根据H.26x压缩格式进行编码的I帧或根据AV1压缩格式进行编码的帧内帧或者关键帧。预测的帧间帧可以是根据H.26x压缩格式进行编码的前向预测的帧间帧P帧或者双向预测的帧间帧B帧或根据AV1压缩格式进行编码的帧间帧。

[0038] 对编码视频序列进行签名的方法500可以由适当地布置的通用可编程计算机(例如，具有相关的输入和输出接口)来执行，并且具体地通过如图4中示意性地图示出的装置400来执行。装置400包括被布置为执行方法500的动作的处理电路410。例如，处理电路410可以包括被配置为执行方法500的动作的生成组件412和签名组件414。装置400进一步包括存储器420和适于与外部存储器490进行双向通信的输入-输出接口430，在一些实施例中和在一些操作阶段期间，外部存储器490可以存储要签名的编码视频序列。这可能是装置400被包括在被配置为提供存储的编码视频序列的签名作为外部服务的视频管理系统中的实施例的情况。装置400和外部存储器490然后可以由不同实体或由共同的实体拥有和操作。装置400的(内部)存储器420可以适合于用于存储具有用于执行方法500的软件指令的程序421，用于存储用于生成签名的密码信息(例如，私钥)以及支持各种内部管理程序的日志、配置文件和数据。计算机程序421可以包括指令，当程序由计算机执行时，该指令使计算机执行方法500的动作。装置400可以被提供为本地计算机或服务器，或者可以被实现为基于

网络(云)处理资源的分布式方式。为了提供编码视频序列的本地签名,装置400可以集成在诸如数字相机的相机440(例如,适于监控应用和/或监视应用的监控相机)中。在一些实施例中,其中装置400被包括在相机440(例如,捕获视频序列的相机)中,装置400可以被布置为与相机440的编码器450通信,并且被配置为直接地从编码器450接收编码视频序列,并在将签名后的编码视频序列传输到接收者(诸如包括解码器470的客户端装置460)或传输到外部存储器490用于存储之前,对编码视频序列进行签名。客户端装置460可以被配置为对签名后的编码视频序列进行验证和解码。应理解,装置400的其他布置也是可能的,并且解码器450可以是与相机440和装置400分开地布置但被布置为与它们通信的外部编码器。

[0039] 应当注意,图4中图示出的相机440还可以包括与例如图像捕获和图像处理有关的其它组件,这些组件在常规的相机系统中是常见的并且其目的和操作对于本领域普通技术人员来说是众所周知的。为了清楚起见,这样的组件已从图4的图示和描述中省略。可以根据常规的视频编码格式对编码视频序列进行编码。与本发明的各种实施例一起工作的一些常见的视频编码格式包括:高效视频编码(HEVC),也被称为H.265和MPEG-H Part 2;高级视频编码(AVC),也被称为H.264和MPEG-4Part 10;多功能视频编码(VVC),也被称为H.266、MPEG-I Part 3和未来视频编码(FVC);VP9、VP10和AOMedia Video 1(AV1),仅给出几个示例。H.264、H.265和H.266编码格式在本公开中有时被称为H.26x编码格式。术语“编码格式”和“压缩格式”在本公开中可互换使用。上述视频编码格式规定了根据图像内帧和图像间帧实现的时间视频压缩。

[0040] 用于对编码视频序列进行签名的方法500从动作502开始,其中获得由视频序列的编码图像帧组成的编码视频序列。图6A示意性地图示出包括表示为I1-I3的三个帧内帧和表示为P1-P8的八个帧间帧的编码视频序列。装置400可以被配置为从外部存储器490或从编码器450获得(例如,检索或接收)编码视频序列。因此,获得编码视频序列的动作可以包括取得对存储视频数据的存储器(例如,外部存储器490)的访问、下载视频数据和/或接收具有视频数据的传输。

[0041] 在动作504中为每个编码图像帧生成一组一个或多个帧指纹。如前所提及,指纹是数据项的唯一标识符,并且因此,帧指纹是图像帧的指纹,具体是编码图像帧的指纹。特定的帧指纹可以被接收者用来验证特定的编码图像帧的真实性,特定的帧指纹是为特定的编码图像帧生成的。

[0042] 编码图像帧的帧指纹可以通过哈希(即通过对编码图像帧或编码图像帧的一部分执行哈希操作)来获得。可以将加密盐(cryptographic salt)添加到要对其执行哈希操作的数据中,从而可以减少需要的哈希操作的数量。哈希操作的替代是通过对编码图像帧或编码图像帧的一部分执行不同的操作(诸如校验和操作)来获得指纹。获得编码图像帧的指纹的另一种替代是对编码图像帧或编码图像帧的一部分进行数字签名。

[0043] 由于编码图像帧可以由诸如NAL单元或OBU的多个单元组成,因此可以为每个这样的单元生成帧指纹,从而为每个编码图像帧生成多个帧指纹的组。然而,应当理解,即使编码图像帧由多个单元组成,也不必为该编码图像帧生成多个帧指纹,而是为编码图像帧生成的帧指纹的组可以仅包括一个帧指纹。装置400被配置为例如通过处理电路410的生成组件412生成一个或多个帧指纹的组。

[0044] 在编码视频序列包括至少一个帧内帧和一个或多个预测的帧间帧的实施例中,所

生成的一个或多个帧指纹的组的表示包括:至少一个帧内帧的生成的指纹(H_I)和一个或多个预测的帧间帧的每个预测的帧间帧的生成的指纹(H_P)。

[0045] 可以使用相同的或两个不同的哈希函数来生成帧内帧和预测的帧间帧的各自的指纹H_I,H_P。在一个实施例中,使用相对更安全的哈希函数(例如,1024位)生成帧内帧的指纹H_I,并且使用具有较低的计算成本的、相对更简单的哈希函数(例如,256位)生成预测的帧间帧的指纹H_P。如果预测的帧间帧的指纹H_P依赖于帧内帧的指纹,则可以使用更简单的哈希函数以计算精简的方式来生成,而不会显著地降低整体安全级别。

[0046] 编码视频序列可以包括第一图片组和第二图片组。在这样的实施例中,该方法可以包括识别第一图片组和第二图片组的子动作。进一步,所生成的一个或多个帧指纹的组可以包括第一图片组的帧内帧的生成的指纹(H_I)、第一图片组的每个预测的帧间帧的生成的指纹(H_P)和第二图片组的帧内帧的生成的指纹(H_I)。

[0047] 每个预测的帧间帧的生成的指纹(H_P)可以通过对源自预测的帧间帧的数据和源自预测的帧间帧直接地或间接地参考的帧内帧的数据的组合进行哈希来生成。预测的帧间帧的指纹可以独立于预测的帧间帧直接地或间接地参考的任何进一步的预测的帧间帧。进一步,源自预测的帧间帧的数据包括预测的帧间帧的图像数据和预测的帧间帧的图像数据的生成的第一指纹中的一个。此外,源自帧内帧的数据是帧内帧的生成的第一指纹。

[0048] 指纹计算可以表示为:

[0049] $H_P = h(\{\lambda, \pi\})$,

[0050] 其中,h是哈希函数,λ是源自帧内帧的数据,并且π是源自帧间帧的数据。考虑到要签名的视频数据的敏感性和/或考虑到如果视频数据被未经授权方操纵的风险值,哈希函数(或单向函数)可以是提供被认为足够的安全水平的密码哈希函数。三个示例是SHA-256、SHA3-512和RSA-1024。哈希函数应该是预定义的(例如,应该可重现),使得在指纹被验证时指纹可以被重新生成。花括号符号{•}指代通用数据组合运算,其可能包括线性地(并列)或各种交错排列地连接数据。组合运算可以进一步包括对数据的算术运算,诸如按位或、异或、乘、除或模运算。

[0051] 进一步的发展处理帧间帧直接地或间接地参考两个帧内帧的情况。然后,除了源自帧间帧自身的数据π之外,还基于源自这两个帧内帧的数据λ_1,λ_2的组合生成帧间帧的指纹:

[0052] $H_P = h(\{\lambda_1, \lambda_2, \pi\})$.

[0053] 在动作506中,生成文档,该文档包括补充信息单元的标头和所生成的一个或多个帧指纹的组的表示。文档610在图6C中示意性地图示出为包括标头611和帧指纹的表示612。帧指纹的表示612可以被称为图6C中图示出的文档610的有效载荷。如前所提及,文档可以是文本文件或另一数据结构,并且补充信息单元可以是包括补充信息的单元或消息。补充信息单元的标头包括补充数据,诸如补充信息单元的指示,以表明它是补充信息单元。如下面将描述的,补充信息单元在动作512中生成。因此,应该注意,在动作506中补充信息单元尚未生成,但是在动作506中仍然可能知道关于补充信息单元的标头,即关于要生成的补充信息单元的标头。例如,在动作506中,装置400可以设置标头包括补充信息单元的指示。如前所提及,应当理解,补充信息单元的指示表面补充信息单元作为补充信息单元,并且对于所有的补充信息单元都相同。进一步,并且同样如前所提及,所生成的一个或多个帧指纹的

组的表示可以是或包括来自所有所生成的一个或多个帧指纹的组或其一部分的帧指纹的组或列表。可替代地，表示可以是或包括来自所有所生成的一个或多个帧指纹的组或其一部分的帧指纹的一个或多个哈希。可替代地，表示可以是帧指纹和帧指纹的哈希的组合。装置400被配置为例如通过处理电路410的生成组件生成文档。

[0054] 在一些实施例中，除了上述标头和表示之外，文档还包括进一步的信息。在这样的实施例中，文档可以包括以下一项或多项：被包括在补充信息单元中的有效载荷的有效载荷大小值、有效载荷的标识符、与编码视频序列有关的元数据、与捕获视频序列的相机有关的相机信息和非对称加密密钥对的公钥。标识符可以识别文档中包含的有效载荷的类型。例如，标识符可以识别或指示有效载荷与签名后的编码视频序列有关。进一步，标识符可以是诸如通用唯一标识符(UUID)的唯一标识符。在图6D中图示出除了标头611和表示612之外还包括上述所有的进一步信息的文档610的示例。如所图示的，这样的文档610包括标头611、表示612、有效载荷大小值613、标识符ID 614、与编码视频序列有关的元数据615、相机信息616和公钥617。标识符ID 614是被包含在补充信息单元中的有效载荷的标识符，并且可以是UUID。元数据615可以包括描述例如如何解释相机信息616和/或帧指纹612的表示的信息或者描述相机信息616和/或帧指纹612的表示的语法。在一些实施例中，表示612、元数据615、相机信息616和/或公钥617被包含在子文档中。可能还包括标识符ID 614的子文档可以被称为图6D中所图示的文档610的有效载荷。作为文档，子文档可以是文本文件或另一数据结构。在这样的实施例中，文档610可以包括标头611、有效载荷大小值613、标识符614和子文档。

[0055] 在一些实施例中，在动作508中生成文档的文档指纹。文档指纹是文档的指纹。文档指纹可以通过对文档(即对文档的内容)或文档的一部分进行哈希(即通过执行哈希操作)来获得。可替代地，指纹可以通过对文档或文档的一部分执行不同的操作(诸如校验和操作)来获得。获得文档的指纹的又一种替代方案是对文档或文档的一部分数字签名。处理电路410可以被配置为例如通过生成组件412生成文档指纹。

[0056] 在动作510中，通过对文档进行数字签名来生成文档签名。在包括如上所描述在动作508中生成文档指纹的一些实施例中，在动作510中生成的文档签名是通过对文档指纹进行数字签名生成的。文档签名可以被称为编码视频序列的签名或编码视频序列的片段的签名。编码视频序列的片段可以是图片组。文档签名可以例如通过非对称加密生成，即，使用来自与接收者预先共享公钥的密钥对中的私钥，使得接收者能够验证签名。装置400被配置为例如通过处理电路410的生成组件412生成文档签名。

[0057] 在动作512中，补充信息单元被生成为仅由文档、文档签名和补充信息单元的结束的指示组成。补充信息单元是与构成编码图像帧的多个单元相同类型的单元。也就是说，补充信息单元是H.26x编码格式的NAL单元和AV1编码格式的OBU。图6B图示出由文档610、文档签名620和补充信息单元600结束的指示630组成的生成的补充信息单元600。补充信息单元的结束的指示可以是诸如结束位的显式的指示，或者可以是诸如在补充信息单元中达到预定的位数的隐含的指示。应当理解，文档、文档签名和补充信息单元的结束的指示是补充信息单元的仅有的组件。从而实现了对补充信息单元的内容的任何篡改都将被检测到，因为篡改将导致对文档真实性的不成功验证。因此，补充信息单元的接收者将理解已经做出了对补充信息单元的内容的操纵。装置400被配置为例如通过处理电路410的生成组件412生

成补充信息单元。

[0058] 如前所提及，补充信息单元可以是H.26x编码格式的SEI消息或AV1编码格式的元数据OBU。通常，SEI包含解码编码图像帧所不需要的信息。然而，需要根据本发明的补充信息单元来验证编码图像帧的真实性。如先前所描述的，生成的补充信息单元由文档、文档签名和结束的指示组成。由于文档包括所生成的一个或多个帧指纹的组的表示，因此需要文档来验证编码图像帧。如果由于文档的内容的操纵而无法使用文档签名来验证文档，则可能无法验证编码图像帧的真实性。因此，当为整个编码视频序列生成一个单独的补充信息单元时，文档包括整个编码视频序列的所生成的一个或多个帧指纹的组的表示，并且因此，需要文档来验证编码图像帧。如果由于文档的内容的操纵而无法使用文档签名来验证文档，则可能无法验证编码图像帧的真实性。相应地，当为每个图片组生成一个补充信息单元时，需要成功地验证每个补充信息单元的文档，以能够验证该图片组的编码图像帧的真实性。

[0059] 在动作514中，通过将所生成的补充信息单元与编码视频序列相关联来对编码视频序列进行签名。装置400被配置为例如通过处理电路410的签名组件414对编码视频序列进行签名。为了对编码视频序列进行签名，所生成的补充信息单元可以以不同的方式与编码视频序列相关联，一些方式将在下面描述。

[0060] 在一些实施例中，所生成的补充信息单元通过对编码视频序列的参考与编码视频序列相关联，并且在与传输编码视频序列的信道不同的信道上被传输。所生成的补充信息单元和编码视频序列可以通过时间戳彼此相关联。例如，如果所生成的补充信息单元和编码视频序列具有相同或相应的时间戳，则它们被认为彼此相关联。因此，即使没有与编码视频序列一起传输，只要接收者能够接收到所生成的补充信息和编码视频序列两者并验证签名，所生成的补充信息单元就可以对编码视频序列进行签名。传输(较小)补充信息单元的信道可以是第一通信信道，诸如安全通信路径，并且传输(较大)编码视频序列的信道可以是第二通信信道，诸如任意通信路径。可替代地，通过编码视频序列和数据格式之外的补充信息单元之间的关联(例如，通过形成包括编码视频序列和补充信息单元两者并且其中编码视频序列被传输到预期的接收者的数据结构(容器))，所生成的补充信息单元与编码视频序列相关联。这些替代方案的优势在于它们不需要修改编码视频序列的权力(例如，视频数据的所有者授予的授权)，并且因此，它们可以由对编码视频序列没有写访问权限的实体执行。

[0061] 在一些替代实施例中，通过在编码视频序列的结束处添加生成的补充信息，将生成的补充信息单元与编码视频序列相关联。这在图7A中示意性地图示出，其中补充信息单元SIU被添加在编码视频序列IPPPIPPPPIPP的结束处。

[0062] 有时编码视频序列包括若干图片组。在这样的实施例中，编码视频序列的签名可以说是由多个子签名组成，即由被提供给编码视频序列的不同片段的多个补充信息单元组成。这允许在播放期间进行连续的签名验证。它还支持对实时视频流进行编码的视频数据进行签名，这在视频监控应用中特别有用。

[0063] 例如，编码视频序列可以包括编码图像帧的与第一图片组相关联的第一部分以及编码图像帧的与第二图片组相关联的直接随后的第二部分。对于这样的编码视频序列，可以为每个组生成补充信息单元。因此，所生成的补充信息单元可以是为编码图像帧的第一

部分生成的。进一步，可以通过在与编码图像帧的第一部分相关联的第一图片组之后添加所生成的补充信息单元来将所生成的补充信息单元与编码视频序列相关联。即使在本公开中参考了图片组，也应理解可以使用诸如一组帧、帧组、一套图片和一套帧的其他术语。在一些编码格式中，第一图片组和第二图片组可以被称为第一GOP和第二GOP。这在例如图7B、图7C、图7D和图7E中示意性地图示出，其中为编码图像帧的与第一图片组GOP1相关联的第一部分生成的补充信息单元SIU1通过添加在编码视频序列之后而与编码视频序列相关联。对于分别为图片组GOP0(未示出)、GOP2和GOP3生成的补充信息单元SIU0、SIU2和SIU3也是如此。

[0064] 除了如上所提及的在第一图片组之后添加之外，还可以通过将所生成的补充信息单元添加到在与编码图像帧的第二部分相关联的第二图片组之前的编码视频序列来将所生成的补充信息单元与编码视频序列相关联。因此，补充信息单元可以被添加在第一图片组之后但在第二图片组之前。换句话说，所生成的补充信息单元可以被添加在编码视频序列的第一图片组和第二图片组之间。这也可以被表达为在第一图片组之后(例如，在最后一个帧间帧之后)但在第二图片组之前(例如，在随后的帧内帧之前)，将补充信息单元插入到编码视频序列中。这在图7B中示意性地图示出，其中补充信息单元SIU1被添加在图片组GOP1和GOP2之间。对于被添加在图片组GOP2和GOP3之间的补充信息单元SIU2也是如此。

[0065] 可替代地，并且除了如上所提及的在第一图片组之后添加之外，还可以通过将生成的补充信息作为与编码图像帧的第二部分相关联的第二图片组的一部分添加到编码视频序列来将生成的补充信息单元与编码视频序列相关联。因此，补充信息单元可以被包括在第二图片组中。这在图7C和图7D中示意性地图示出，其中补充信息单元SIU1被包括在图片组GOP2中。

[0066] 由于补充信息单元与构成编码图像帧的单元的类型相同，因此可以在编码视频序列中的所期望的位置处(例如，按顺序)将补充信息单元添加到编码视频序列，而不需要接收方处的特殊解码器对编码视频序列进行解码。

[0067] 拥有已按上述方式签名的编码视频序列的接收者可以通过以下过程验证其真实性：

[0068] 1、尝试通过使用发送者生成文档签名的私钥的公钥来验证包含在补充信息单元中的文档签名。因此，当使用公钥和接收到的文档成功地验证接收到的文档签名时，可以验证接收到的文档的内容是正确的。例如，当使用公钥和接收到的文档的哈希成功地验证接收到的文档签名时，接收到的文档的内容被验证为是正确的；

[0069] 2、如果文档签名被成功地验证并且由此证明文档是正确的(例如，未经操纵)，则尝试验证包含在文档中的指纹；

[0070] 3、如果文档中的所有指纹被成功地验证，则断定与补充信息单元相关联的编码视频序列是真实的(验证)。

[0071] 通常，步骤2中的验证包括复制被认为由发送者执行的指纹操作，即重新计算指纹。就其自身而言，步骤1中的验证通常与非对称签名设置有关，其中签名和验证是与私钥/公钥相对应的不同加密操作。在不脱离本发明的范围的情况下，对称和/或非对称验证操作的其他组合是可能的。

[0072] 本文中描述的文档签名是数字签名。在一些实施例中，文档签名通过证明数字消

息或文档从被签名的时间起没有被有意或无意地修改而起作用。文档签名通过生成消息或文档的唯一哈希并使用发送者的私钥对其进行加密来实现这一点。所生成的哈希对于消息或文档是唯一的，并且更改它的任何部分都会完全改变哈希。一旦完成，消息或数字文档就被数字签名并发送给接收者。然后接收者生成他们自身的消息或数字文档的哈希，并使用发送者的公钥对发送者的哈希(包含在原始消息中)进行解密。接收者将他们生成的哈希与发送者的解密哈希进行比较;如果它们匹配，则消息或数字文档未被修改并且发送者被证实。

[0073] 以上主要参考几个实施例描述了本公开的各个方面。然而，如本领域技术人员容易理解的，在所附专利权利要求所限定的本发明范围内，除上述公开的实施例之外的其他实施例同样是可能的。

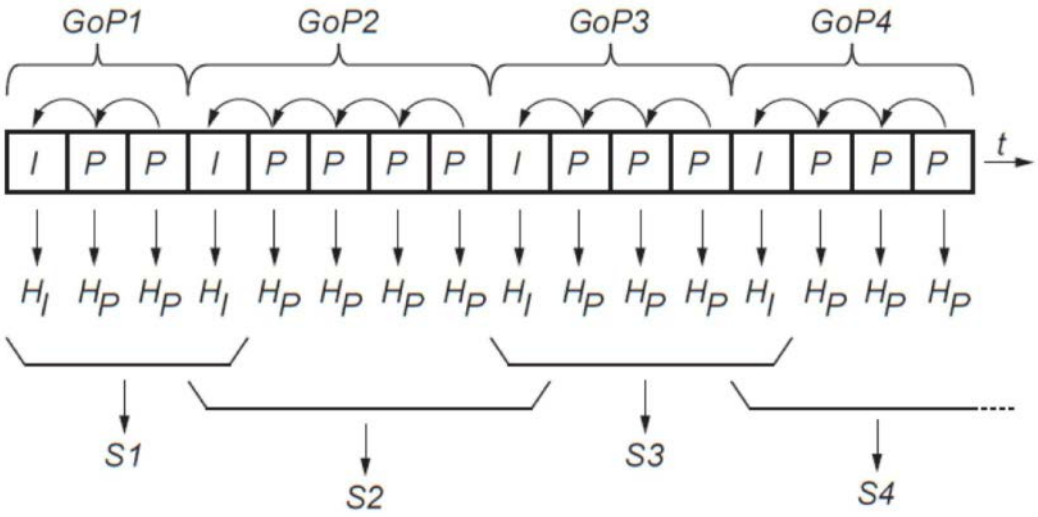

GoP1
GoP2
GoP3
GoP4
I P P I P P P P I P P P I P P P
t
HI HP HP HI HP HP HP HP HI HP HP HP HI HP HP HP
S1
S2
S3
S4

图1


NAL
单元
多个
NAL单元
SEI
视频帧
SEI
视频帧
SEI
视频帧

图2

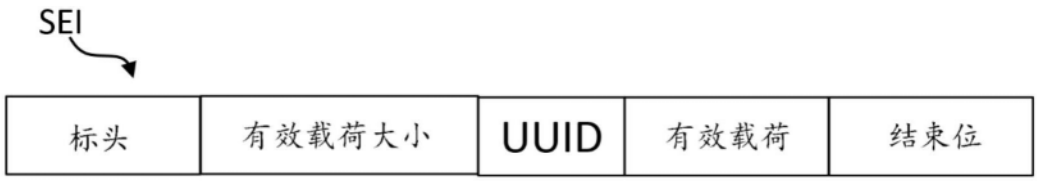

SEI
标头
有效载荷大小
UUID
有效载荷
结束位

图3

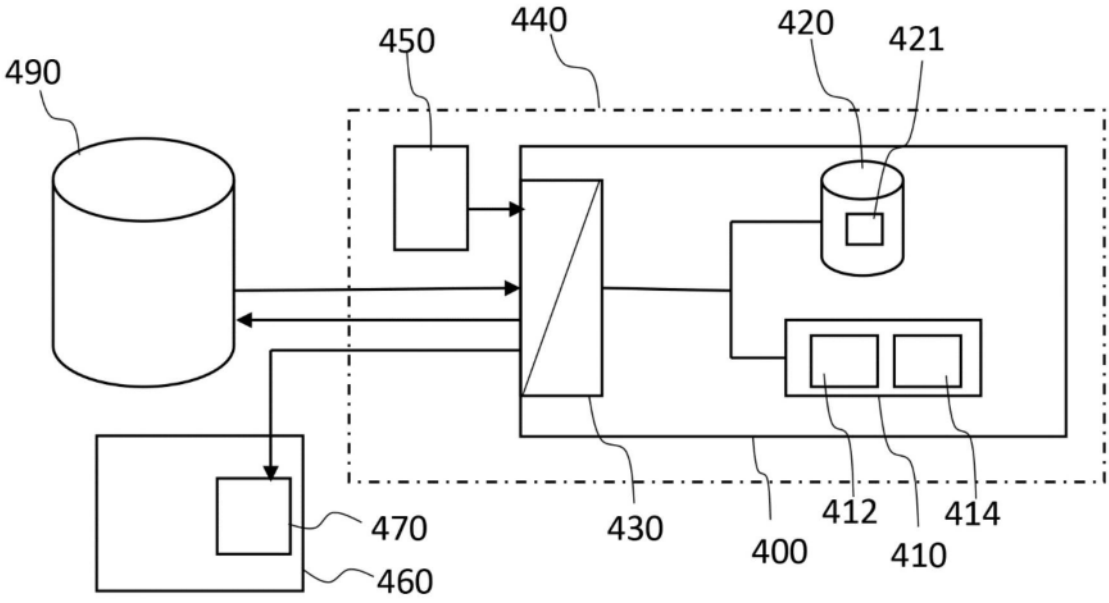


图4

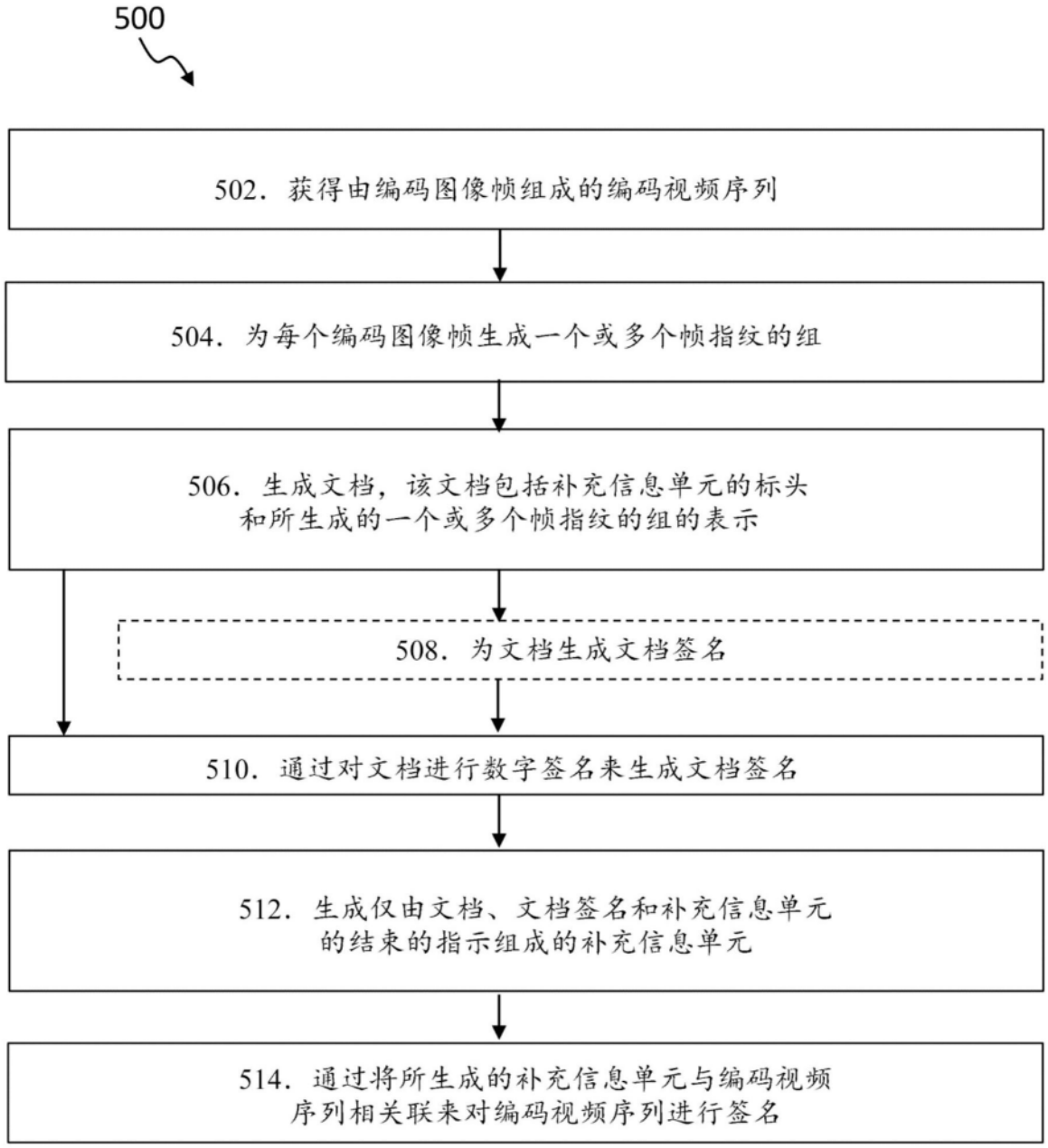

500
502. 获得由编码图像帧组成的编码视频序列
504. 为每个编码图像帧生成一个或多个帧指纹的组
506. 生成文档，该文档包括补充信息单元的标头和所生成的一个或多个帧指纹的组的表示
508. 为文档生成文档签名
510. 通过对文档进行数字签名来生成文档签名
512. 生成仅由文档、文档签名和补充信息单元的结束的指示组成的补充信息单元
514. 通过将所生成的补充信息单元与编码视频序列相关联来对编码视频序列进行签名

图5

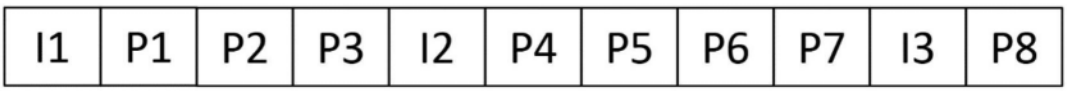

I1
P1
P2
P3
I2
P4
P5
P6
P7
I3
P8

图6A

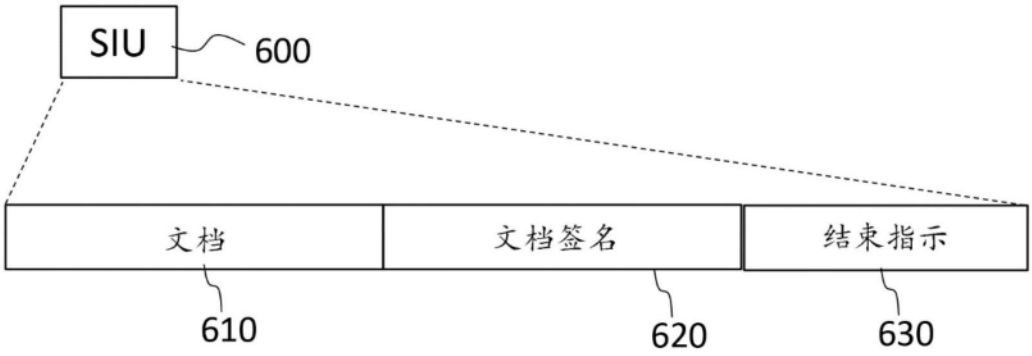

SIU
600
文档
文档签名
结束指示
610
620
630

图6B

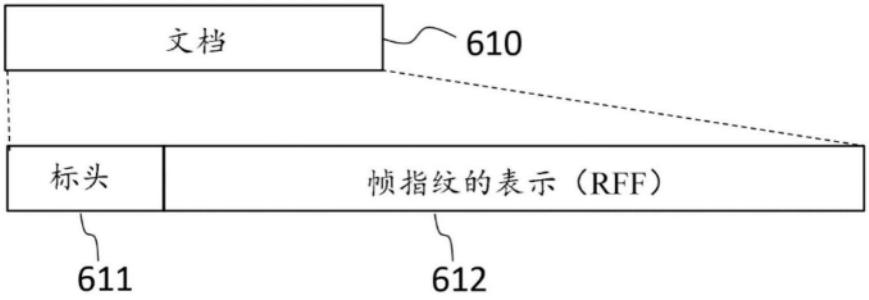

文档
610
标头
帧指纹的表示（RFF）
611
612

图6C

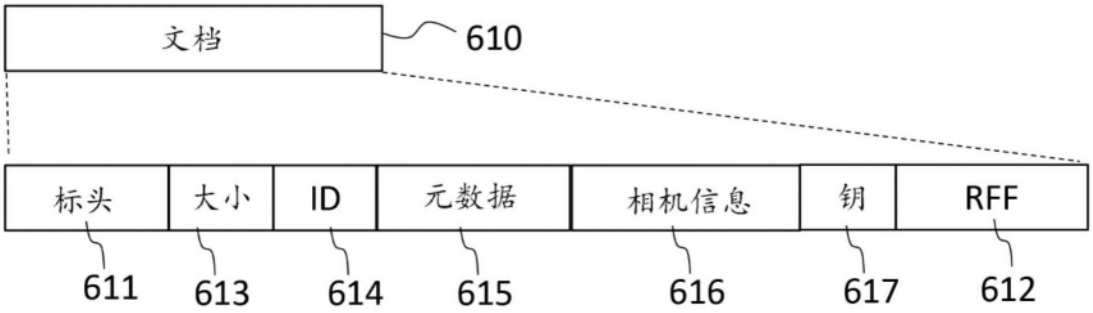

文档
610
标头
大小
ID
元数据
相机信息
钥
RFF
611
613
614
615
616
617
612

图6D

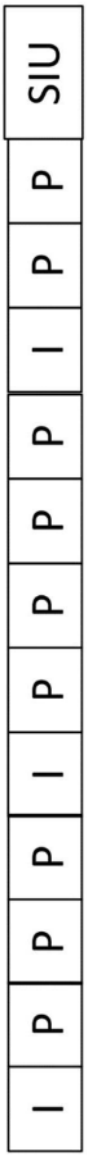


图7A

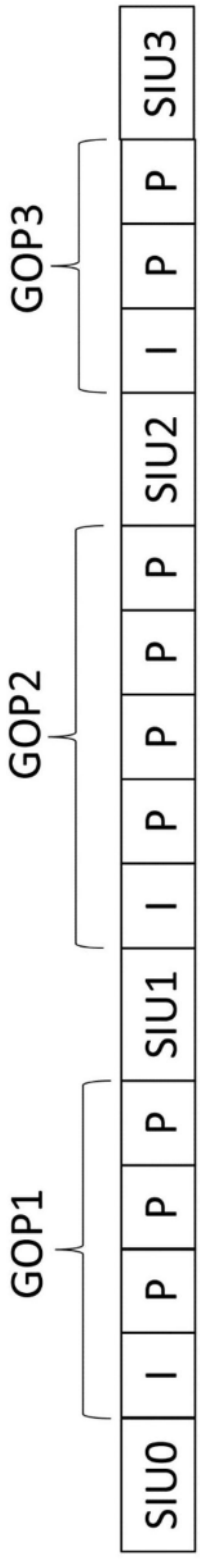


图7B

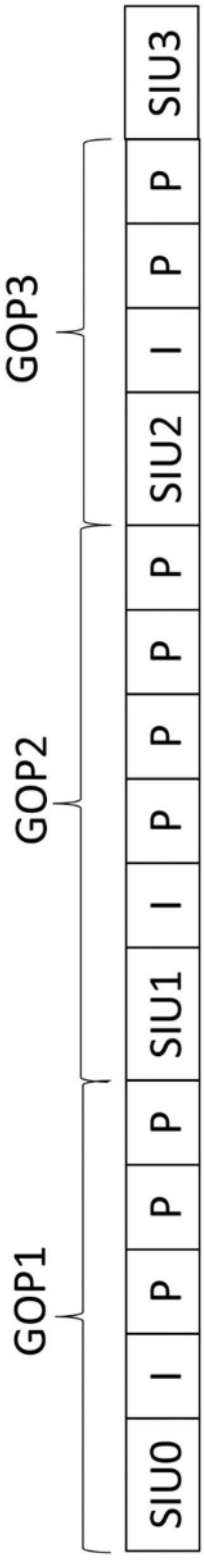


图7C

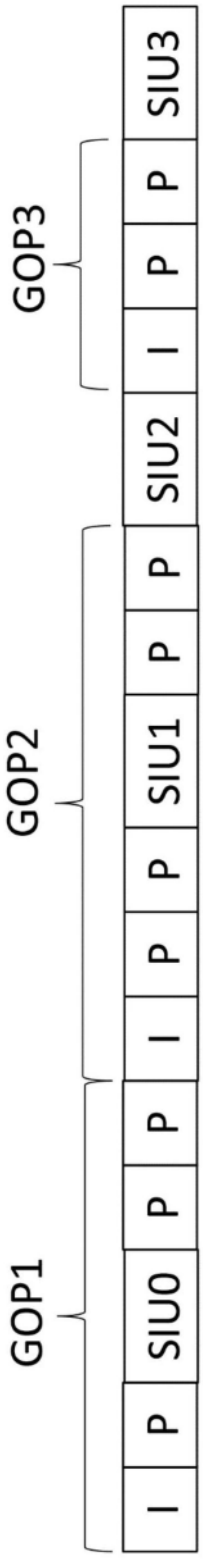


图7D

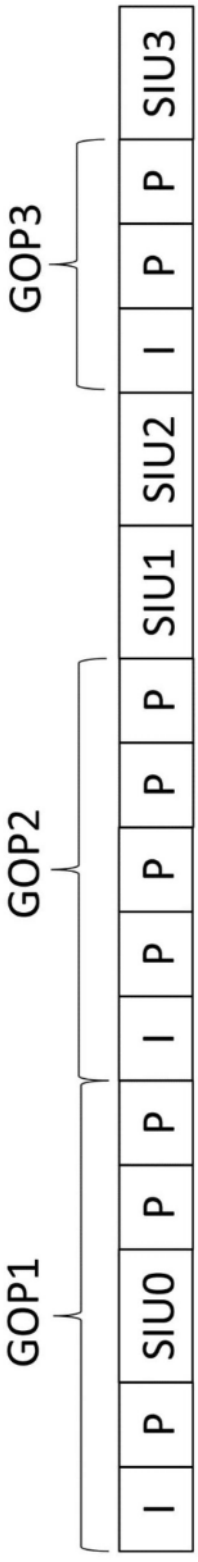


图7E