(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 104205865 B
(45)授权公告日 2017.10.13

(21)申请号 201380017737.8
(22)申请日 2013.03.15
(65)同一申请的已公布的文献号
申请公布号 CN 104205865 A
(43)申请公布日 2014.12.10
(30)优先权数据
13/434,399 2012.03.29 US
(85)PCT国际申请进入国家阶段日
2014.09.29
(86)PCT国际申请的申请数据
PCT/US2013/031894 2013.03.15
(87)PCT国际申请的公布数据
WO2013/148304 EN 2013.10.03
(73)专利权人 阿尔卡特朗讯公司
地址 法国布洛涅-比扬古
(72)发明人 Y·任 L·奥戈尔曼 J·R·张 T·L·伍德
(74)专利代理机构 北京市中咨律师事务所 11247
代理人 杨晓光 于静
(51)Int.Cl.
H04N 21/8358(2006.01)
G06K 9/46(2006.01)
H04L 9/32(2006.01)
(56)对比文件
CN 102187366 A,2011.09.14,
CN 101977319 A,2011.02.16,
US 2010128789 A1,2010.05.27,
US 2003056010 A1,2003.03.20,
CN 1695343 A,2005.11.09,
J.Dittmann.Content-based Digital Signature for Motion Pictures Authentication and.《IEEE International Conference on Multimedia Computing and Systems》.1999,
审查员 肖然

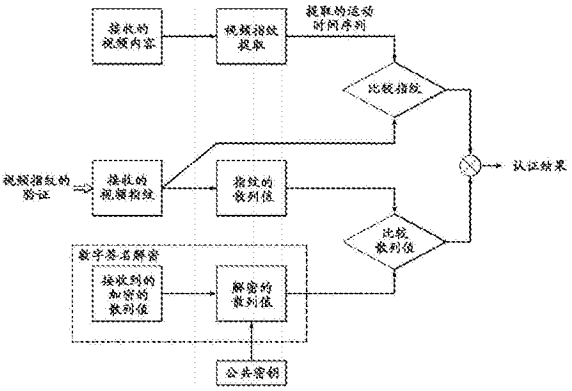
权利要求书3页 说明书18页 附图16页

(54)发明名称

用于认证视频内容的方法和装置

(57)摘要

一种用于认证视频内容的方法，该方法包括：在通信网络中的接收节点处接收来自发射节点的数字签名、无保证的视频指纹和无保证的视频内容；在所述接收节点处确定所述数字签名是否与所述无保证的视频指纹一致，以验证该无保证的视频指纹；以及在所述接收节点处确定所述无保证的视频指纹是否与所述无保证的视频内容一致，来以容忍所述无保证的视频内容中预定量的损失的方式验证该无保证的视频内容。在验证了所述无保证的视频指纹和所述无保证的视频内容的情况下，该无保证的视频内容被认证以供在所述接收节点的后续使用。一种与所述方法相关的接收节点，该接收节点包括输入模块、指纹验证模块、内容验证模块和控制器模块。



CN 104205865 B

1.一种用于认证视频内容的方法，该方法包括：

在通信网络中的接收节点处接收来自发射节点的数字签名、无保证的视频指纹和无保证的视频内容，其中，所述无保证的视频指纹是原始视频指纹的接收版本，其中，所述原始视频指纹在所述发射节点传输所述原始视频指纹之前使用指纹识别算法从原始视频内容中取得，其中，所述指纹识别算法基于突出特征点的移动的轨迹来导出所述原始视频指纹，所述轨迹从所述原始视频内容的采样视频帧中检测到；

在所述接收节点处确定所述数字签名是否与所述无保证的视频指纹一致，以验证所述无保证的视频指纹；以及

在所述接收节点处确定所述无保证的视频指纹是否与所述无保证的视频内容一致，以便以容忍所述无保证的视频内容中预定量的损失的方式验证所述无保证的视频内容，其中，验证所述无保证的视频内容包括：通过在所述接收节点处使用所述指纹识别算法处理所述无保证的视频内容，生成新的视频指纹；

其中，如果所述无保证的视频指纹和所述无保证的视频内容被验证，则所述无保证的视频内容被认证以供在所述接收节点处的后续使用。

2.根据权利要求1所述的方法，其中，所述数字签名是在由所述发射节点传送该数字签名之前，使用加密算法和私有密钥来从原始散列值中产生的；以及

其中，所述原始散列值是在对所述原始散列值进行加密之前，使用散列算法从所述原始视频指纹中取得的。

3.根据权利要求1所述的方法，结合验证所述无保证的视频指纹，该方法还包括：

在所述接收节点处使用解密算法和公共密钥来对所述数字签名进行解密，以获取与原始散列值有关的解密的散列值；

在所述接收节点处使用所述散列算法来处理所述无保证的视频指纹，以获取与所述原始散列值有关的新的散列值；以及

在所述接收节点处将所述新的散列值与所述解密的散列值进行比较，以使得在所述新的散列值与所述解密的散列值相匹配的情况下，所述无保证的视频指纹被验证。

4.根据权利要求2所述的方法，结合验证所述无保证的视频内容，该方法还包括：

在所述接收节点处，通过使用所述指纹识别算法处理所述无保证的视频内容，来生成新的视频指纹；

在所述接收节点处，使用复杂性不变距离测量算法来确定所述无保证的视频指纹与所述新的视频指纹之间的距离度量；以及

在所述接收节点处，比较所述距离度量与预定的阈值，以使得在该距离度量不超过所述预定的阈值的情况下，所述无保证的视频内容被验证。

5.根据权利要求4所述的方法，结合使用所述指纹识别算法，该方法还包括：

从所述无保证的视频内容中选择视频帧的样本，并按照连接的时间顺序排列该样本视频帧；

检测每个样本视频帧中的突出特征点；

针对每个样本视频帧中的每个突出特征点，计算与所述连接的时间顺序的下一样本视频帧中的对应的突出特征点有关的光学流动的角向；

将每个样本视频帧的突出特征点的角向分布到针对每个样本视频帧的对应的角度范

围面元中；

随着所述连接的时间顺序，将针对所述样本视频帧的每个角度范围面元中的值连接，以形成针对每个角度范围面元的直方图；以及

将针对所述角度范围面元的直方图集合进行标准化，以形成建立所述新的视频指纹的对应的运动时间序列集合。

6.根据权利要求5所述的方法，结合使用所述指纹识别算法来建立所述新的视频指纹，该方法还包括：

使用线性分段算法来压缩每个运动时间序列，以将对应的直方图转换成对应的线性分段序列；以及

至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从每个压缩的运动时间序列中提取主斜坡，以形成由所提取的主斜坡表示的用于所述新的视频指纹的对应的运动时间序列集合。

7.一种用于认证视频内容的方法，该方法包括：

从源设备接收视频内容；

通过使用指纹识别算法处理所述视频内容，来生成视频指纹；

使用散列算法处理所述视频指纹，以获取原始散列值；

使用加密算法和私有密钥对所述原始散列值进行加密，以获取与所述原始散列值有关的数字签名；

至少临时将所述数字签名、视频指纹和视频内容存储在发射节点处的存储设备中；以及

在一个或多个通信会话中，将所述数字签名、视频指纹和视频内容从在通信网络中的发射节点传送至接收节点；

其中，结合使用所述指纹识别算法，该方法还包括：

从所述视频内容中选择视频帧的样本，并按照连接的时间顺序排列该样本视频帧；

检测每个样本视频帧中的突出特征点；

针对每个样本视频帧中的每个突出特征点，计算与所述连接的时间顺序的下一样本视频帧中的对应的突出特征点有关的光学流动的角向；

将每个样本视频帧的突出特征点的角向分布到针对每个样本视频帧的对应的角度范围面元中；

随着所述连接的时间顺序，将针对所述样本视频帧的每个角度范围面元中的值连接，以形成针对每个角度范围面元的直方图；以及

将针对所述角度范围面元的直方图集合进行标准化，以形成建立所述视频指纹的对应的运动时间序列集合。

8.根据权利要求7所述的方法，其中，所述接收节点在接收到来自所述发射节点的所述数字签名、视频指纹和视频内容之后，能够确定解密的散列值是否与所接收到的视频指纹一致，以验证所接收到的视频指纹，以及确定所接收到的视频指纹是否与所接收到的视频内容一致，来以容忍所接收到的视频内容中预定量的损失的方式验证该接收到的视频内容。

9.根据权利要求7所述的方法，结合使用所述指纹识别算法来建立所述视频指纹，该方

法还包括：

使用线性分段算法来压缩每个运动时间序列，以将对应的直方图转换成对应的线性分段序列；以及

至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从每个压缩的运动时间序列中提取主斜坡，以形成由所提取的主斜坡表示的用于所述视频指纹的对应的运动时间序列集合。

用于认证视频内容的方法和装置

背景技术

[0001] 本发明涉及用于认证视频内容的方法和装置，该视频内容可以在传输期间被有意更换，以适应多种接入设备、网络架构和通信协议。在各种实施方式中，发射节点、接收节点或者两者实施这一过程。该过程的各种实施方式通过分别验证对应的视频指纹和视频内容，来使用视频指纹和视频内容的加密数字签名认证该视频内容。这里公开的用于认证视频内容的过程的各种实施方式容忍在接收节点处的视频内容中的预定量的损失(loss)。例如，这里描述的方法和装置许可从移动和固定的摄像头到政府安全机构、军事机构、新闻机构以及公众的广泛的即时视频的访问。

[0002] 出于保全和安全的目的，在例如道路、城市人行横道、机场、地铁、军事基地、校园和商店的不同地方中安装了公共监督摄像头。早在十年前，这些视频供给(feed)是私有的，仅可由单个实体(例如，警察、军队或私营保安公司)查看。然而，越来越普遍的是，公共监督视频无阻碍(in the clear)地被发送以使得由多个安全实体(例如，警察、消防员、救护车、国土安全部等)使用，并且使能对各种使用的公共访问(例如，对于众包(crowd-sourcing)安全任务，获取关于交通阻塞的信息，等等)。无阻碍的视频内容未被加密，以使得能够开放访问，或者至少比实际加密的视频内容更广泛地接入。因此，需要内容认证对抗包括源数据修改和中间人修改的恶意攻击。例如，攻击者可以拦截视频流，并且可以通过对帧进行重排序或者注入预制的视频中的一些来消除罪证。认证确保在接收方(即，接收者)端(例如，安全控制站)接收到的视频内容与在视频摄像头捕捉的或由在发送方端处的另一源提供的原始视频内容相同。例如，这与LTE移动视频的安全性有关，该LTE移动视频能够用于公共安全和第一响应方通信。

[0003] 存在对视频内容认证的多个解决方案。通常来说，它们能够被分为三类：1)对称加密，2)使用非对称加密的数字签名，以及3)水印。然而，这些现有的解决方案中没有一个解决方案能够满足当今对在大范围的接收者之间来认证视频的需要，其中，在视频通信的源和接收方(即，接收者)端两者上使用大范围的设备。

[0004] 对称加密不能满足，这是因为其需要许多不同的安全机构来分布和共享单个解密密钥。在安全性方面，公知的是密钥管理问题。分布太多的密钥必然降低系统安全性。更具体地，对称加密包括完全分层加密和选择性或基于置换的加密。在完全分层加密中，视频内容被压缩，并且之后被加密。该方式通常导致计算量大且速度慢，这使得其不适用于即时视频认证。选择性的和基于置换的加密选择性地对字节进行加密，或使用排列(arrngment)来对视频内容进行加扰。这种类型的方式典型地被设计用于特定的视频格式，例如，H.264或MPEG。例如，在MPEG中，对称加密用于基于I帧、P帧和B帧之间的关系来选择和置换字节。总的来说，该方式不是格式兼容的。

[0005] 使用非对称加密的数字签名通常使用对于认证数据而言是非常安全的加密方法。然而，取决于加密计算的本质，这要求接收到的数据要与源数据一致；否则，其将不能认证。视频传输(特别是通过无线信道)的问题在于原始内容可能由于信道中的噪声而被更换，或者由于设备性能(例如，由于移动设备的较小屏幕)而改变视频的大小。因此，即使数据不被

恶意更换，接收到的数据可能不与原始的完全相同，在这种情况下，其将错误地不认证(即，错误拒绝)。

[0006] 非对称加密和数字签名能够通过对帧应用哈尔(Haar)小波滤波器、离散余弦转换(DCT)或小波转换来获取，并且之后基于所获取的参数来生成散列(hash)值。实施加密安全的现成的摄像头的示例为来自加利福尼亚州圣何塞市的思科系统公司的思科视频监控2500系列IP摄像头。其包括使用高级加密标准(AES)的基于硬件的非对称加密。

[0007] 非对称加密和数字签名的变形基于加密校验和，其提供对全部帧、周期性的帧、分组或周期性的分组进行数字签名的校验和。该加密校验和解决方案提供修改检测和消息完整性校验。其能够处理在传输期间视频分组损失的情况。然而，对于视频被有意更换的情况，例如，对于在4G移动情况下的尺寸缩减或转码，或者对于HTTP自适应的比特率流传输，加密校验和将不能匹配更换的视频，除非该校验和在每个修改节点处被重新应用。这在专有网络中是可能的，然而，这是不标准的，并且将引起相当复杂的(并且潜在地不安全的)密钥管理来在所有节点处分布和安全地维护加密密钥。

[0008] 水印能够避免对称加密和非对称加密的问题，并且因此，是对于当前问题的有效解决方案。然而，水印具有其自身的缺陷。由于水印被嵌入到原始视频中，其必须更换该视频。对水印的权衡是嵌入的水印的无感知性对从视频中提取水印以执行认证的能力。在当前的问题中，不期望更换视频，并且期望对认证成功进行最大化。在这些情形下，不期望在视频中嵌入水印。数字水印将信息嵌入到视频帧中来验证真伪。水印技术针对未压缩和压缩视频(例如，H.264)存在。

[0009] 基于前述内容，期望用于认证视频内容的过程允许使用多个网络架构之间的多个用户设备以及通信协议来访问多个人员，同时能够检测视频内容在何时被意外更换、秘密更换或以欺骗意图被更换。为了准许这种宽访问，该过程必须能够容忍已经在传输期间被正当地且预期地更换的视频内容。

发明内容

[0010] 在一个方面，提供了一种用于认证视频内容的方法。在一个实施方式中，该方法包括：在通信网络中的接收节点处接收来自发射节点的数字签名、无保证的(unsecured)视频指纹和无保证的视频内容；在所述接收节点处确定所述数字签名是否与所述无保证的视频指纹一致，以验证该无保证的视频指纹；以及在所述接收节点处确定所述无保证的视频指纹是否与所述无保证的视频内容一致，以便以容忍所述无保证的视频内容中预定量的损失的方式验证该无保证的视频内容。在验证了所述无保证的视频指纹和所述无保证的视频内容的情况下，该无保证的视频内容被认证以供在所述接收节点的后续使用。

[0011] 在另一方面，提供了用于认证视频内容的装置。在一个实施方式中，该装置包括：输入模块，被配置成经由通信网络接收来自发射节点的数字签名、无保证的视频指纹和无保证的视频内容；指纹验证模块，被配置成确定所述数字签名是否与所述无保证的视频指纹一致，以验证该无保证的视频指纹；内容验证模块，被配置成确定所述无保证的视频指纹是否与所述无保证的视频内容一致，来以容忍所述无保证的视频内容中预定量的损失的方式验证该无保证的视频内容；以及控制模块，与所述输入模块、指纹验证模块和内容验证模块有效通信，并且被配置成控制操作，以使在验证了所述无保证的视频指纹和所述无保证

的视频内容的情况下，该无保证的视频内容被认证以供后续使用。所述无保证的视频指纹是原始视频指纹的接收版本。该原始视频指纹在由所述发射节点传送该原始视频指纹之前，使用指纹识别算法从原始视频内容中取得。

[0012] 在另一方面，提供了一种用于认证视频内容的方法。在一个实施方式中，该方法包括：从源设备接收视频内容；通过使用指纹识别算法处理所述视频内容，来生成视频指纹；使用散列算法处理所述视频指纹，以获取原始散列值；使用加密算法和私有密钥对所述原始散列值进行加密，以获取与所述原始散列值有关的数字签名；至少临时将所述数字签名、视频指纹和视频内容存储在发射节点处的存储设备中；以及在通信网络中，在一个或多个通信会话中，将所述数字签名、视频指纹和视频内容从所述发射节点传送至接收节点。

[0013] 在另一方面，提供了一种非暂时性计算机可读介质。在一个实施方式中，该非暂时性计算机可读介质存储第一程序指令，当由第一计算机运行时，该第一程序指令引发与通信网络相关联的计算机控制的接收节点执行用于认证视频内容的方法。在一个实施方式中，该方法包括：在于通信网络中的接收节点处接收到来自发射节点的数字签名、无保证的视频指纹和无保证的视频内容之后，在所述接收节点处确定解密的散列值是否与所述无保证的视频指纹一致，以验证该无保证的视频指纹；以及确定所述无保证的视频指纹是否与所述无保证的视频内容一致，来以容忍所述无保证的视频内容中预定量的损失的方式验证该无保证的视频内容。在验证了所述无保证的视频指纹和所述无保证的视频内容的情况下，该无保证的视频内容被认证以供在所述接收节点的后续使用。

[0014] 本发明的应用性的进一步的范围将从以下提供的具体实施方式中变得显而易见。然而，应当理解的是，当指示本发明的优选实施方式时，具体实施方式和具体示例仅通过例证的方式给出，因为本发明的精神和范围内的各种变化和修改对于本领域的技术人员而言将变得显而易见。

附图说明

[0015] 本发明以设备的各部分的构造、排列和组合、以及方法的步骤的形式存在，借以取得预期的目标，如在下文更全面地阐述的、在权利要求书中特别指出的、以及在附图中示出的，其中：

[0016] 图1是示出用于认证视频内容的过程的示例性实施方式的功能框图；

[0017] 图2是已经使用指纹识别算法的示例性实施方式分析出的视频内容的示例性样本帧，该指纹识别算法检测特征点，计算该特征点随时间的与下一样本帧有关的光学流动的角向，以及将所述角向分布到角度范围面元(bin)；

[0018] 图3是示出与使用和图2相关联的指纹识别算法的示例性实施方式来生成用于视频内容的指纹有关的、示例性角度范围面元随时间的示例性运动时间序列的图表；

[0019] 图4是示出在线性分段处理之后的图3的示例性运动序列的图表；

[0020] 图5是示出在主斜坡(incline)提取之后的图4的示例性运动序列的图表；

[0021] 图6是示出用于认证视频内容的过程的另一示例性实施方式的功能框图；

[0022] 图7是示出用于生成视频内容的视频指纹的过程的示例性实施方式的功能框图；

[0023] 图8是示出从对各种指纹识别算法的性能的定量比较得出的结果的表格；

[0024] 图9是用于认证视频内容的过程的示例性实施方式的流程图；

[0025] 图10与图9结合是用于认证视频内容的过程的另一示例性实施方式的流程图；

[0026] 图11与图9结合是用于认证视频内容的过程的另一示例性实施方式的流程图；

[0027] 图12与图9结合是用于认证视频内容的过程的另一示例性实施方式的流程图；

[0028] 图13与图9和图12结合是用于认证视频内容的过程的另一示例性实施方式的流程图；

[0029] 图14是用于认证视频内容的接收节点的示例性实施方式的框图；

[0030] 图15是与图14的接收节点相关联的指纹验证模块的示例性实施方式的框图；

[0031] 图16是与图14的接收节点相关联的内容验证模块的示例性实施方式的框图；

[0032] 图17是用于认证视频内容的过程的另一示例性实施方式的流程图；

[0033] 图18与图17结合是用于认证视频内容的过程的另一示例性实施方式的流程图；以及

[0034] 图19是用于认证视频内容的发射节点的示例性实施方式的框图。

具体实施方式

[0035] 这里公开了用于认证视频内容的方法和装置的各种实施方式。示例性实施方式描述了将视频指纹和数字签名结合的视频认证解决方案。在某些实施方式中，视频指纹和数字签名与视频内容分开发送(即，不嵌入在视频内容中)。在其他实施方式中，视频指纹和数字签名可以被嵌入在视频内容中，例如，水印或任意合适的嵌入技术。这次描述的认证过程被配置成检测视频内容何时被意外更换、秘密更换或以欺骗意图被更换，同时仍旧能够认证在传输期间已经被合理地且预期地更换的视频内容。这里描述的各种实施方式依赖于一些认证概念，该认证概念与在1995年2月25日提交的美国专利No.5,799,092中公开的、并被分配给朗讯科技公司的自验证识别卡有关，其全部内容通过引用被结合于此。

[0036] 参考图1，用于认证视频内容的过程的示例性实施方式以从原始视频内容中提取视频指纹为开始。该视频指纹提供对视频内容的独特且简洁的描述。该视频指纹之后被用密码签名，以获取数字签名。例如，该视频指纹可以使用散列函数来被处理以获取散列值。原始散列值可以使用与原始视频内容的源相关联的私有密钥来被加密，以生成所述数字签名。该数字签名具有两个特性：1)其对于原始视频而言是唯一的，以及2)其不能由除该私有密钥的所有者之外的也捕捉该视频内容的真实源的任何人来产生。因此，数字签名是认证视频内容的准确性的强安全措施。

[0037] 如果视频流在传输之前、期间或之后被有意修改(例如，其可以针对4G无线传输(以及其他应用))，针对在某些合理情形下的认证，单独的标准数字签名不能用于认证视频内容，因为接收到的视频内容将必定不与原始视频内容精确匹配。因此，无阻碍(即，未加密)的视频指纹随该数字签名和无阻碍(即，未加密)的视频内容一起被发送至视频接收者。

[0038] 更具体地，在视频发送方(例如，视频捕捉、视频源等)端，用于认证视频内容的过程的示例性实施方式包括生成用于原始视频内容的视频指纹。该视频指纹可以通过保持对视频内容的突出特征的轨迹的追踪以生成运动时间序列来被获取。该原始视频内容可以由周期性采样或随机采样的帧序列来表示。对于每个采样的帧，局部特征检测器(例如，加速分割检测特征(FAST)算法)可以用于检测突出的特征点。对于关于FAST算法的附加信息，参见罗斯腾等人，Machine Learning for High-Speed Corner Detection，欧洲计算机视觉

国际会议论文集,2006,第430-443页,其全部内容通过引用结合于此。

[0039] 可以使用光学流动技术(例如,卢卡斯-卡纳德(Lucas-Kanade)算法)来追踪所检测到的特征点的轨迹。对于关于Lucas-Kanade算法的附加信息,参见卢卡斯等人,An Iterative Image Registration Technique with an Application to Stereo Vision,DARPA成像理解研讨会(Imaging Understanding Workshop),1981,第121-130页,其全部内容通过引用结合于此。

[0040] 特征点移动的方向可以分成特定数目的面元。例如,对于八个面元,每个面元表示45度的方向跨度,以覆盖360度的方向范围(例如,面元1——0-45度;面元2——45-90度等)。该特征点基于角向被聚合到每个面元中。针对每个面元,通过随时间把面元值连接在一起来生成直方图。

[0041] 参考图2,示出了具有检测的特征点及其计算的光学流动的视频帧的示例。在该帧的右上方中显示的直方图表示针对光学流动的方向的面元值。最上面的面元是具有在0度与45度之间的方向的点的数量。每个面元反映从直方图的顶部到底部增加45度的45度范围的点的数量。在该图像中,能够看到突出特征在多个方向上移动。

[0042] 直方图(随时间标准化)形成运动时间序列,其中,视频指纹包括针对每个面元的运动时间序列。例如,对于八个面元,有八个来自视频指纹的运动时间序列。图3示出了时间序列的示例。图4示出了在对该时间序列执行线性分段之后的示例性结果。图5示出了在从所述线段分段中提取主斜坡之后的示例性结果。

[0043] 返回到图1,所提取的视频指纹经过散列函数以生成大校验和的值。例如,该散列函数可以使用被称为SHA-1的加密散列函数或被称为SHA-256的另一加密散列函数来实施。SHA-1使用160个比特,并提供2^{160}的安全性强度。SHA-256使用256个比特,并提供2^{256}的安全性强度。对于关于安全散列算法(SHA)(例如,SHA-1、SHA-256等)的附加信息,参见联邦信息处理标准出版物(FIPS PUB)180-3,安全散列标准(SHS),信息技术实验室,国家标准技术局,2008,32页,其全部内容通过引用结合于此。

[0044] 视频指纹用私有密钥进行加密,并且能够用公共密钥进行解密。换句话说,使用公共密钥,接收者能够对加密的视频指纹进行解密,以获取原始的视频指纹。对于第三方而言,在计算方面不太可能以导致通过认证在发送方处生成的匹配接收者的视频指纹来产生解密视频指纹的方式,来修改加密的视频指纹或未加密的视频指纹,即使该第三方可以访问该公共密钥。例如,能够使用李维斯特-沙米尔-阿德尔曼(Rivest-Shamir-Adelman)(RSA)算法或椭圆曲线加密(ECC)算法来实施公共密钥加密。

[0045] 对于关于RSA算法的附加信息,参见李维斯特等人,A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,美国计算机学会通讯,第21卷,第2号,2月,1978,第120-126页,其全部内容通过引用结合于此。对于关于ECC算法的附加信息,参见:1)科布利茨,Elliptic Curve Cryptosystems,计算数学,第48卷,第177号,1月,1978,第203-209页,或者2)米勒,Use of Elliptic Curves in Cryptography,密码学-加密新进展论文集:计算机科学讲稿,1986,第417-426页。科布利茨和米勒的文档的全部内容通过引用结合于此。

[0046] 来自视频发送方端的输出包括无阻碍视频内容、无阻碍视频指纹和数字签名。有几种方式来向接收方(即,接收者)端发送视频指纹和数字签名:1)以预先计划或附件的形

式与原始视频内容一起发送;2)通过分开的通信路径(例如,安全通道)来发送;或者3)嵌入在原始视频内容中(例如,水印)。

[0047] 参考图6,用于在视频内容传输的接收方(即,接收者)端认证视频内容的过程的示例性实施方式包括两步过程:1)接收到的数字签名被解密,并且所得到的解密散列值与接收到的视频指纹的新的(即,新计算出的)散列值进行比较,以及2)新的(即,新计算出的)视频指纹从接收到的视频内容中生成,并与接收到的视频指纹进行比较。如果该新的散列值与接收到的数字签名精确匹配,并且新的视频指纹与接收到的视频指纹接近匹配,则所接收到的视频内容被认为是认证的原始视频内容。

[0048] 更具体地,在接收方端,用于认证视频内容的过程包括基于视频内容的视频指纹的数字签名进行验证校验,以及基于该视频指纹进行另一验证校验。使用公共密钥来对接收到的数字签名进行解密。接收到的视频指纹使用与在发送方端处使用的散列函数相同的散列函数来被处理,以获取新的散列值。解密的散列值与新的散列值进行比较,以检验接收到的视频指纹和接收到的数字签名的完整性。如果解密的散列值与新的散列值匹配,该过程继续基于视频指纹进行第二验证校验。如果数字签名不匹配,该过程结束,并且接收到的视频内容被认为是未认证的。

[0049] 第二验证校验包括使用与在发送方端处使用的视频指纹识别算法相同的视频指纹识别算法来处理接收到的视频内容,以获取新的视频指纹。所接收到的视频指纹通过应用时间序列的距离度量匹配来与新的视频指纹进行比较。测量距离度量的算法的各种实施方式可以被用于增加这种比较的速度,或者增加这种比较的准确性。

[0050] 通常来说,给定用于接收到的视频内容(例如,Q)和原始视频内容(例如,C)的视频指纹,距离度量用于找到两个视频指纹中对应的时间序列之间的最小相似性距离。视频内容中的各种修改导致运动时间序列中的多复杂性。从这种修改得出的时间序列(可能偏移失真、振幅和相位缩放、扭曲、遮掩)通常具有不同数量的峰值和谷值。通常使用的相似性测量技术(例如,动态时间扭曲或提供对峰值和谷值中的一些的局部校准)不能完全解决这一问题。为了处理匹配运动时间序列中的各种复杂性,复杂性不变距离(complexity-invariant distance)测量算法被用于确定两个时间序列之间的复杂性差异,作为对现有的距离测量的校正因子。对于关于复杂性不变距离测量算法的附加信息,例如参见巴蒂斯塔等人,AComplexity-Invariant Distance Measure for Time Series,关于数据挖掘的工业和应用数学学会(SIAM)会议的论文集,4月28-30,2011,梅萨市,亚利桑那州,第699-710页,其全部内容通过引用结合于此。

[0051] 以经验来看,复杂性不变距离测量算法被发现具有对抗由视频转换引入的噪声的足够的鲁棒。形式上,给定$Q=\{\{\theta_{i,j}:0\leqslant i\leqslant f\}:0\leqslant j\leqslant b\}$和$C=\{\{\tau_{i,j}:0\leqslant i\leqslant g\}:0\leqslant j\leqslant b\}$(假设$g\geqslant f$),两个对应的时间序列$Q_j$、$C_j$之间的距离D可以针对每个直方图面元j($0\leqslant j<b$)来计算,其中,b是面元的总数,如下:

[0052] $D(Q_jC_j)=\min\{D_{CIV}(Q_j,C_{i\ldots i+f-1,j}):0\leqslant i\leqslant g-f\}$

[0053] 在$C_{i\ldots i+f-1,j}=\{\tau_{i,j}:i^*\leqslant i\leqslant i^*+f\}$时产生最大值,其中,$i^*$是最小化的时间校准偏移,$0\leqslant i^*\leqslant g-f$。

[0054] 复杂性不变距离D_{CIV}可以如下被计算:

[0055] $$D_{CIV}(Q_j,C_j)=\frac{\max\{K(Q_j),K(C_j)\}}{\min\{K(Q_j),K(C_j)\}}D_E(Q_j,C_j)$$

[0056] 其中，D_E是欧几里德距离，并且$K(Q_j)$是针对直方图面元j的时间序列$Q_j=\{\theta_{i,j}:0\leq i\leq f\}$的复杂性的测量。例如，$K(Q_j)$可以如下被定义：

[0057] $$K(Q_j)=\sqrt{\sum_{i=0}^{f-2}(\theta_{i,j}-\theta_{i+1,j})^2}$$

[0058] 类似地，$K(C_j)$是针对直方图面元j的对应的时间序列$C_j=\{\tau_{i,j}:0\leq i\leq g\}$的复杂性的测量，并且可以使用相似的符号来定义。

[0059] 直观地，$K(Q_j)$测量序列的导数的均方根(RMS)，从而对具有更大差异的序列给予更多的权重。可以针对每个对应对计算出b个时间序列距离。最终，可以计算出该对应对的分数Δ(Q,C)。该分数Δ(Q,C)是包含大于特定阈值d的多个时间序列距离以及那些距离的平均值的元组。例如，对于，距离＝(D(Q_j,C_j):0≤j<b且D(Q_j,C_j)>d)

[0060] $$\Delta(Q,C)=\left(|\text{距离}|,\frac{\sum\text{距离}}{|\text{距离}|}\right)$$

[0061] 该方法不对d过度敏感，该d可以以试探的方式来确定。针对对应对的分数Δ可以根据|距离|(递增)和平均距离(递减)来排序。匹配的视频应当具有b个平均距离为零的匹配的时间序列。

[0062] 当比较没有时间扭曲的不同长度的两个时间序列时，所述时间序列应当被校准。其可以以线性方式来完成，但是线性技术可能是慢速且低效的。为了进行更有效的比较，主斜坡匹配过程可以用于快速计算两个时间序列之间的时间偏移，以使接收到的视频指纹和新的视频指纹同步。该主斜坡匹配技术对每个时间序列使用线性分段，以近似直方图的时间追踪，并且之后，从线性分段中提取具有较长距离或较深高度的主斜坡。如果两个主斜坡具有相似的长度和高度，则它们是相似的。两个主斜坡的相似性指示比较的直方图之间的潜在校准。基于该潜在的校准位置，比较的视频指纹之间的复杂性不变相似性距离可以被计算。如果该相似性距离小于预定的阈值，则两个视频指纹被认为是复杂性不变匹配的，并且视频内容是经认证的(如果数字签名也匹配)。如果相似性距离不小于该预定的阈值，则接收到的视频内容被认为是未认证的。

[0063] 更具体地，主斜坡匹配技术应用线性分段步骤，其可以使用自底向上的分段算法，通过将时间序列压缩成线性分段序列来近似该时间序列。对于关于自底向上的分段算法的附加信息，参见基奥等人，An Online Algorithm for Segmenting Time Series，关于数据挖掘的IEEEE国际会议的论文集，11月29日—12月2日，2001，第289-296页，其全部内容通过引用结合于此。

[0064] 独个的分段可以彼此之间进行比较。通过将较短的一者向较长的一者滑动来比较两个线性分段，以及计算它们之间的复杂性不变距离，如上面所描述的。然而，通过选择与振幅有关的较高和/或与时间有关的“较长”的线性分段，校准能够被减少或简化。所选择的分段能够被称为主斜坡。主斜坡匹配过程的示例如图3-图5中示出。

[0065] 更具体地，找出主斜坡包括将线性分段序列根据时间划分成长度为p的等间隔。如

果开始时间点处于一间隔内，线性分段被认为是处于该间隔内。从每个间隔中，选择具有最高高度和具有大于一些给定阈值(长度(l))的长度的z个线性分段。注意的是，对于不同长度的视频，较短视频的主斜坡可以被较长视频丢弃。因此，最好选择适用于较短视频的长度p。

[0066] 一旦计算出主斜坡，它们能够被成对比较。如果两个主斜坡具有相似的长度和高度，则它们被认为是相似的(准确的距离测量显得不那么至关重要，只要其不是过度限制)。两个主斜坡的相似性指示比较的时间序列的可能的校准位置i^*。根据那些校准位置来计算复杂性不变距离。由于计算被限制到那些位置，整个比较时间被降低。

[0067] 参考图1和图6，在发送方端和接收方端处执行的视频指纹提取的示例性实施方式使用相同的视频指纹算法。直观地，在每个端处的视频指纹试图捕捉视频的最突出的特征穿越时间的运动轨迹。这可以通过使用光流方向直方图(HOOF)算法提取特征来完成。对于关于HOOF算法的附加信息，参见乔杜里等人，Histograms of Oriented Optical Flow and Binet-Cauchy Kernals on Nonlinear Dynamical Systems for the Recognition of Human Actions，关于计算机视觉和模式识别的IEEE会议，2009，第1932-1939页，其全部内容通过引用结合于此。

[0068] 参考图7，视频指纹算法的示例性实施方式接受视频内容Q作为输入，其标识f个均匀采样的帧的序列$Q=\{q_0,q_1,\ldots,q_{f-1}\}$。光流方向直方图可以针对每个连续的帧对$q_i$、$q_{i+1}$来生成。帧$q_i$中的突出局部特征(即，关键点)可以使用特征检测器算法(例如，FAST)来检测。从帧q_i到q_{i+1}的关键点的光学流动可以通过应用Lucas-Kanade算法来计算。具有现实范围内的量级的轨迹可以被保留。具有相等权重的保留轨迹的方向可以被面元化成b个面元，并且直方图可以被标准化。例如，可以选择八个面元，b＝8个面元。相比于根据错误计算的轨迹的大小的加权通过(更多的)精准轨迹来被减弱相比，具有相等权重的面元化产生更鲁棒的指纹。

[0069] 对于每个连续帧对$\{q_i,q_{i+1}\}$，直方图：$\{\theta_{i,j}:0\leqslant j<b\}$目前存在，其中，$\theta_{i,j}$记录在给定方向上移动的关键点的编号。具有检测到的关键点的帧、它们的光学流动、以及光流方向直方图的示例在图2中示出。面元可以穿越时间被聚合，以产生包括b个时间序列(每个方向面元一个)的最终的指纹：

[0070] $\{\{\theta_{i,j}:0\leqslant i\leqslant f\}:\theta_{i,j}:0\leqslant j<b\}$

[0071] 由于在上文，该技术描述了用于比较从发送方端接收到的视频指纹与在接收方端生成的视频指纹，相比于指纹生成，匹配被认为是在计算量上廉价的。

[0072] 尽管存在额外的计算成本，局部特征检测器能够代替均匀采样的点来追踪局部特征，这是因为：1)所得到的光绪流动更可靠，以及2)视频中的每个帧的最突出的特征的运动为最明确的部分，是符合直觉的。

[0073] 各种现有的局部特征检测器算法被比较，包括尺度不变特征变换(SIFT)算法、加速鲁棒特征(SURF)算法和FAST。对于关于SIFT算法的附加信息，参见洛维，Distinctive Image Features from Scale-Invariant Keypoints，国际计算机视觉期刊，第60卷，发行日为2004年11月2日，第91-110页，其全部内容通过引用结合于此。对于关于SURF算法的附加信息，参见贝等人，SURF:Speeded Up Robust Features，计算机视觉和图像理解，第110卷，发行日为2008年6月3日，第346-359页，其全部内容通过引用结合于此。

[0074] 越过SIFT和SURF而选择FAST是因为其明显运行得更快(由于通过直接像素比较来计算),并产生更多的关键点。附加的关键点是有利的,因为不精确的关键点追踪的效果被减弱。尽管FAST被论证具有较小的鲁棒性,但其足以追踪从帧到帧的细微变化。

[0075] 这里描述的各种方法和装置提供了一种鲁棒的和紧凑的视频指纹技术,该技术使得有效的即时视频认证能够防御监督视频和其他类型的视频内容的内容修改和中间人的攻击。例如,监督视频播放公共安全和国土安全中的较大且关键的部分。这是特别及时的,并且与LTE移动视频的安全性有关,该LTE移动视频可以用于公共安全和第一响应方通信。这里描述的方法还能够用于认证存档视频,该存档视频可以用作用于执法和刑事诉讼的证据。视频指纹提取技术是格式(以及编解码器)模块兼容的。

[0076] 例如,为了论证这里描述的方法在速度和精度方面的鲁棒性和效能。公共可用的视频数据库(MUSCLE VCD基准)被用于进行比较性能分析。该数据库由总长为80个小时的101个视频组成。该数据库提供来自不同节目的视频,例如,体育节目、纪录片、动画片、家庭电影、老式黑白电影、商业广告灯。MUSCLE VCD基准包含地面实况数据ST1的集合,其包括组合起来的持续时间为2小时30分钟的15个查询。它们是从五分钟到一小时长的视频的副本。查询视频经历多次转换,包括调整尺寸、重新编码、有角度地摄录、颜色特性的裁剪和改变、变焦、加噪、模糊、以及改变字幕等等。总的查询时间被测量,包括需要生成针对所有查询视频的签名以及在数据库中搜索它们所需的时间量。测试机器是以2.26GHz运行的具有16GB的RAM的因特尔至强四核处理器。参考图8,证明示出了该过程使用少于十分钟的时间来在ST1中以高准确性搜索所有查询。由该论证团队获取的最佳分数的时间占用44分钟。使用这里描述的方法,对于视频认证,使用基于突出特征点的移动的轨迹的视频指纹,并且根据主斜坡校准进行匹配视频指纹是可行且实际的。

[0077] 这里描述的各种方法和装置能够被实施以提供对视频监督系统的视频内容认证。这里描述的视频内容认证过程能够结合用于计算视频指纹的任意算法来使用。参考能够被实施用于该过程的各个步骤的各种算法,这论证了该过程有多鲁棒。该过程还提供用于与现有的视频认证技术有关的视频内容认证的压缩的视频指纹。

[0078] 根据视频指纹的准确性,描述了用于认证视频内容的过程的另一示例性实施方式,以阐述其如何可以被用于和适于监督。整个过程被归入基于内容的媒体认证方法类,但是用比现有的方法更高水平的特征。局部突出特征在视频内容中从采样的帧中被检测,并且穿越时间捕捉那些特征的运动轨迹,作为运动时间序列。该运动已经用于来自压缩编码(例如,MPEG-4)的短期(2帧)运动矢量。通常地,较高水平的特征被认为引发过高的计算负担;然而,较高水平的特征已经用于降低带宽和错误警示的错误率。由于该更鲁棒的特征(相比于单帧方法或2帧方法)已经被计算,用于认证可以没有额外的计算成本。采样的帧的指纹是特性数量的面元值,其通过将局部特征的运动轨迹的方向面元化成面元来获取。例如,在一个示例性实施中,可以使用八个面元。

[0079] 认证方案适用用于散列匹配的鲁棒方法来代替鲁棒散列。形式上,指纹序列表示如下:

[0080] $F=\{\{f_{i,j}:0\leqslant i<m\}:0\leqslant j<B\}$,

[0081] 其中,F是指纹序列,f是采样的帧的指纹,m是采样的帧序列的长度,以及B是面元的总数。每个帧指纹被数字签名(被散列并且被用私有密钥加密)。该对于视频失真而言不

是鲁棒的，然而，除了数字签名之外，无阻碍(即，未加密)的数字指纹被包括在到接收方的传输中。为了认证视频内容，接收方使用公共种子来对视频指纹进行散列，以获取H_1'。数字签名使用公共密钥来解密。所得到的散列H_2'与H_1'进行比较。用于接收到的视频的视频指纹被计算以获取F_1'。计算出的视频指纹F_1'与接收到的视频指纹F_2'进行比较。如果H_1'＝H_2'，并且相似性距离$D(F_1', F_2') \leq dist$，那么相应的视频内容帧被认证，其中，dist是距离阈值。

[0082] 由于视频指纹被表示为时间序列，$D(F_1', F_2')$能够通过测量时间序列之间的距离来计算。视频传输中的各种修改(由于缩放、转码和分组损失等)导致时间序列中的多复杂性。得出的时间序列(可能偏移失真、振幅和相位缩放等)通常具有不同数量的峰值和谷值。为了处理匹配视频指纹中的各种复杂性，巴蒂斯塔的复杂性不变距离测量可以被实施。该复杂性不变距离测量使用两个时间序列之间的复杂性差异，作为对现有的距离测量的校正因子。复杂性不变距离D_{CIV}可以如下计算：

[0083] $$D_{CIV}\left(F_{1j}, F_{2j}\right) = \frac{\max\left\{K\left(F_{1j}\right), K\left(F_{2j}\right)\right\}}{\min\left\{K\left(F_{1j}\right), K\left(F_{2j}\right)\right\}} D_E\left(F_{1j}, F_{2j}\right)$$

[0084] $$K\left(F_j\right) = \sqrt{\sum_{i=0}^{m-2}\left(f_{i,j} - f_{i+1,j}\right)^2}$$

[0085] 其中，F_{1j}和F_{2j}是针对直方图面元j的两个时间序列，D_E是欧几里德距离，并且$K(F_j)$是时间序列的复杂性的测量。直观地，$K(F_j)$测量序列的导数的RMS，从而对具有更大差异的序列给予更多的权重。

[0086] 在获取到针对B个时间序列的相似性距离之后，可以计算比较的指纹对的分数$\Delta(F_1, F_2)$。该分数$\Delta(F_1, F_2)$是包含大于特定阈值dist的多个时间序列距离以及那些距离的平均值的元组。也就是，对于$D_{total} = \{D_{CIV}(F_{1j}, F_{2j}) : 0 \leq j < B$，和$D_{CIV}(F_{1j}, F_{2j}) > dist\}$，

[0087] $$\Delta\left(F_1, F_2\right) = \left(\left|D_{total}\right|, \frac{\sum D_{total}}{\left|D_{total}\right|}\right)$$

[0088] 该方法不对dist过度敏感，该dist可以以试探的方式来确定。两个相同的视频应当具有以平均距离为0匹配的所有面元。

[0089] 参考图9，用于认证视频内容的过程900的示例性实施方式在902处开始，在该902处，在通信网络中，在接收节点处，从发射节点接收数字签名、无保证的视频指纹和无保证的视频内容。接下来，该过程在接收节点处确定所述数字签名是否与所述无保证的视频指纹一致，以验证该无保证的视频指纹(904)。在906处，该过程在所述接收节点处确定所述无保证的视频指纹是否与所述无保证的视频内容一致，来以容忍所述无保证的视频内容中预定量的损失的方式验证该无保证的视频内容。在验证了所述无保证的视频指纹和所述无保证的视频内容的情况下，该无保证的视频内容被认证以供在所述接收节点的后续使用。

[0090] 在过程900的另一实施方式中，数字签名被预先计划、嵌入或附加到所述无保证的视频内容，以传输至接收节点。在该实施方式中，过程900还包括在所述接收节点处将所述数字签名从所述无保证的视频内容中分离。

[0091] 在过程900的另一实施方式中，无保证的视频指纹被预先计划、嵌入或附加到所述无保证的视频内容，以传输至接收节点。在该实施方式中，过程900还包括在所述接收节点

处将所述无保证的视频指纹从所述无保证的视频内容中分离。

[0092] 在过程900的另一实施方式中，如果无保证的视频指纹未由接收节点验证，无保证的视频内容不被认证用于在接收节点的后续使用。在过程900的另一实施方式中，如果无保证的视频指纹被验证而无保证的视频内容未由接收节点验证，无保证的视频内容不被认证用于在接收节点的后续使用。

[0093] 在过程900的另一实施方式中，在分离的通信会话中，经由不同的通信路径来在接收节点处接收数字签名和无保证的视频内容。在过程900的另一实施方式中，在分离的通信会话中，经由不同的通信路径来在接收节点处接收无保证的视频指纹和无保证的视频内容。

[0094] 在各种实施方式中，所述无保证的视频指纹是原始视频指纹的接收版本。该原始视频指纹在由所述发射节点传送该原始视频指纹之前，使用指纹识别算法从原始视频内容中取得。数字签名在由发射节点传送该数字签名之前，使用加密算法和私有密钥来从原始散列值中产生。在对原始散列值进行加密之前，原始散列值使用散列算法从原始视频指纹中得出。无保证的视频内容是原始视频内容的接收版本。

[0095] 参考图9和图10，用于认证视频内容的过程1000的另一示例性实施方式结合验证无保证的视频指纹(904)来扩展图9的过程900。在该实施方式中，过程1000从图9的904推进到1002，在该1002处，在接收节点处使用解密算法和公共密钥来对数字签名进行解密，以获取与原始散列值有关的解密的散列值。接下来，在接收节点处使用散列算法来处理无保证的视频指纹，以获取与原始散列值有关的新的散列值(1004)。在1006处，在接收节点处将新的散列值与解密的散列值进行比较，以使在新的散列值与解密的散列值相匹配的情况下，该无保证的视频指纹被验证。在该实施方式中，过程1000在1006之后返回到906。在过程1000的另一实施方式中，如果新的散列值与解密的散列值不匹配，则无保证的视频指纹未被验证。

[0096] 参考图9-图11，用于认证视频内容的过程1100的另一示例性实施方式结合使用散列算法(1004)来扩展图10的过程1000。在该实施方式中，过程1100从图10的1004推进到1102，在该1102处，向表示无保证的视频指纹的数据排列应用散列算法，以确定建立新的散列值的校验和的值。在该实施方式中，过程1100在1102之后返回到1006。

[0097] 参考图9和图12，用于认证视频内容的过程1200的另一示例性实施方式结合验证无保证的视频内容(906)来扩展图9的过程900。在该实施方式中，过程1200从图9的906推进到1202，在该1202处，在接收节点处，通过使用指纹识别算法来处理无保证的视频内容，来生成新的视频指纹。接下来，该过程在接收节点处，使用复杂性不变距离测量算法来确定无保证的视频指纹与新的视频指纹之间的距离度量(1204)。在1206处，在接收节点处，该距离度量与预定的阈值进行比较，以使在该距离度量不超过该预定的阈值的情况下，所述无保证的视频内容被验证。在过程1200的另一实施方式中，如果距离度量超过该预定的阈值，所述无保证的视频内容未被验证。

[0098] 参考图9、图12和图13，用于认证视频内容的过程1300的另一示例性实施方式结合使用指纹识别算法(1202)来扩展图12的过程1200。在该实施方式中，过程1300从图12的1202推进到1302，在该1302处，视频帧的样本被从无保证的视频内容中选出，并按照连接的时间顺序排列。接下来，在每个样本视频帧中检测突出特征点(1304)。在1306处，针对每个

样本视频帧中的每个突出特征点，计算与连接的时间顺序的下一样本视频帧中的对应的突出特征点有关的光学流动的角向。接下来，每个样本视频帧的突出特征点的角向被分布到针对每个样本视频帧的对应的角度范围面元(1308)。在1310，随着连接的时间顺序，针对样本视频帧的每个角度范围面元中的值被连接，以形成针对每个角度范围面元的直方图。接下来，针对角度范围面元的直方图集合被标准化，以形成建立新的视频指纹的对应的运动时间序列集合(1312)。

[0099] 在另一实施方式中，结合使用指纹识别算法来建立新的视频指纹，过程1300还包括使用线性分段算法来压缩每个运动时间序列，以将对应的直方图转换成对应的线性分段序列。在该实施方式中，至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从每个压缩的运动时间序列中提取主斜坡，以形成由提取的主斜坡表示的用于新的视频指纹的对应的运动时间序列集合。

[0100] 再次参考图9和图12，在过程1200的另一实施方式中，原始视频指纹、无保证的视频指纹和新的视频指纹中的每个包括通过将对应的直方图变为线性分段序列、并且从该线性分段序列中提取主斜坡而形成的对应的运动时间序列集合。在该实施方式中，结合使用复杂性不变距离测量算法，过程1200还包括将无保证的视频指纹的每个运动时间序列与新的视频指纹的对应的运动时间序列配对。每个成对的运动时间序列至少部分地基于在对应成对的运动时间序列中的相似的主斜坡的识别来被校准。每个校准的运动时间序列之间的距离测量使用复杂性不变距离测量算法来确定。

[0101] 在过程1200的另一实施方式中，原始视频指纹、无保证的视频指纹以及新的视频指纹中的每个包括由对应的直方图形成的对应的运动时间序列集合。在该实施方式中，结合使用复杂性不变距离测量算法，过程1200还包括使用线性分段算法来压缩无保证的视频指纹的每个运动时间序列，以将对应的直方图转换成对应的线性分段序列。至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从无保证的视频指纹的每个压缩的运动时间序列中提取主斜坡，以形成由提取的主斜坡表示的用于无保证的视频指纹的对应的运动时间序列集合。使用线性分段算法来压缩新的视频指纹的每个运动时间序列，以将对应的直方图转换成对应的线性分段序列。至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从新的视频指纹的每个压缩的运动时间序列中提取主斜坡，以形成由提取的主斜坡表示的用于新的视频指纹的对应的运动时间序列集合。无保证的视频指纹的每个运动时间序列与新的视频指纹的对应的运动时间序列配对。每个成对的运动时间序列至少部分地基于在对应成对的运动时间序列中的相似的主斜坡的识别来被校准。每个校准的运动时间序列之间的距离测量使用复杂性不变距离测量算法来确定。

[0102] 参考图14，用于认证视频内容的接收节点1400的示例性实施方式包括输入模块1402、指纹验证模块1404、内容验证模块1406以及控制器模块1408。输入模块1402被配置成经由通信网络1412从发射节点1410接收数字签名、无保证的视频指纹、和无保证的视频内容。发射节点1410可以是通信网络1412中的网络节点，或具有对通信网络1412的接入的用户或计算设备。通信网络1412可以是混合通信网络，其包括任意合适的组合中的各种类型的网络架构、通信协议和技术。指纹验证模块1404被配置成确定所述数字签名是否与所述无保证的视频指纹一致，以验证该无保证的视频指纹。内容验证模块1406被配置成确定所

述无保证的视频指纹是否与所述无保证的视频内容一致，来以容忍所述无保证的视频内容中预定量的损失的方式验证该无保证的视频内容。控制模块1408与所述输入模块1402、指纹验证模块1404和内容验证模块1406有效通信，并且被配置成控制操作，以使在验证了所述无保证的视频指纹和所述无保证的视频内容的情况下，该无保证的视频内容被认证以供后续使用。

[0103] 在接收节点1400的另一实施方式中，数字签名被预先计划、嵌入或附加到所述无保证的视频内容，以进行传输。在该实施方式中，接收节点1400还包括视频处理模块，与输入模块1402和控制器模块1408有效通信。该视频处理模块被配置成将数字签名从无保证的视频内容中分离。

[0104] 在接收节点1400的另一实施方式中，无保证的视频指纹被预先计划、嵌入或附加到所述无保证的视频内容，以进行传输。在该实施方式中，接收节点1400还包括视频处理模块，与输入模块1402和控制器模块1408有效通信。该视频处理模块被配置成将所述无保证的视频指纹从所述无保证的视频内容中分离。

[0105] 在接收节点1400的另一实施方式中，如果无保证的视频指纹未由指纹验证模块1404验证，控制器模块1408被配置以使无保证的视频内容不被认证用于后续使用。在接收节点1400的另一实施方式中，如果无保证的视频指纹被指纹验证模块1404验证而无保证的视频内容未由内容验证模块1406验证，控制器模块1408被配置以使无保证的视频内容不被认证用于后续使用。

[0106] 在接收节点1400的另一实施方式中，由输入模块1402在分离的通信会话中，经由不同的通信路径来接收数字签名和无保证的视频内容。在接收节点1400的另一实施方式中，由输入模块1402在分离的通信会话中，经由不同的通信路径来接收无保证的视频指纹和无保证的视频内容。

[0107] 在接收节点1400的各种实施方式中，所述无保证的视频指纹是原始视频指纹的接收版本。该原始视频指纹在由所述发射节点1410传送该原始视频指纹之前，使用指纹识别算法从原始视频内容中取得。数字签名在由发射节点1410传送该数字签名之前，使用加密算法和私有密钥来从原始散列值中产生。在对原始散列值进行加密之前，原始散列值使用散列算法从原始视频指纹中得出。无保证的视频内容是原始视频内容的接收版本。

[0108] 参考图15，指纹验证模块1404的示例性实施方式包括解密子模块1502、散列子模块1504、比较器子模块1506和用于结合控制器模块1408一起验证无保证的视频指纹的处理器子模块1508。解密子模块1502被配置成使用解密算法和公共密钥对数字签名进行解密，以获取与原始散列值有关的解密的散列值。散列子模块1504被配合成使用散列算法处理无保证的视频指纹，以获取与原始散列值有关的新的散列值。比较器子模块1506被配置成将新的散列值与解密的散列值进行比较，以使在新的散列值与解密的散列值相匹配的情况下，该无保证的视频指纹被验证。处理器子模块1508与解密子模块1502、散列子模块1504和比较器子模块1506有效通信。该处理器子模块1508被配置成控制与对数字签名、无保证的视频指纹、新的散列值和解密的散列值中的一者或多者进行解密、处理和比较有关的操作。在视频验证模块1404的另一示例性实施方式中，如果新的散列值与解密的散列值不匹配，则比较器子模块1506被配置以使无保证的视频指纹未被验证。

[0109] 在视频验证模块1404的另一示例性实施方式中，结合使用散列算法，散列子模块

1504被配置成向表示无保证的视频指纹的数据排列应用散列算法，以确定建立新的散列值的校验和的值。

[0110] 参考图16，内容验证模块1406的示例性实施方式包括指纹识别子模块1602、测量子模块1604、比较器子模块1606、以及用于结合控制器模块1408来验证无保证的视频内容的处理器子模块1608。指纹识别子模块1602被配置成通过使用指纹识别算法来处理无保证的视频内容，来生成新的视频指纹。测量子模块1604被配置成使用复杂性不变距离测量算法来确定无保证的视频指纹与新的视频指纹之间的距离度量。比较器子模块1606被配置成将该距离度量与预定的阈值进行比较，以使在该距离度量不超过该预定的阈值的情况下，所述无保证的视频内容被验证。处理器子模块1608与指纹识别子模块1602、测量子模块1604和比较器子模块1606有效通信。该处理器子模块1608被配置成控制与对新的视频指纹、无保证的视频内容、距离度量、无保证的视频指纹和预定的阈值中的一者或多者进行生成、确定和比较有关的操作。在内容验证模块1406的另一示例性实施方式中，如果距离度量超过该预定的阈值，比较器子模块1606被配置以使所述无保证的视频内容未被验证。

[0111] 在内容验证模块1406的另一示例性实施方式中，指纹识别子模块1602被配置成从无保证的视频内容中选择视频帧的样本，并按照连接的时间顺序排列该样本视频帧。指纹识别子模块1602还检测每个样本视频帧中的突出特征点。指纹识别子模块1602还被配置成针对每个样本视频帧中的每个突出特征点，计算与连接的时间顺序的下一样本视频帧中的对应的突出特征点有关的光学流动的角向。此外，指纹识别子模块1602将每个样本视频帧的突出特征点的角向分布到针对每个样本视频帧的对应的角度范围面元。指纹识别子模块1602还随着连接的时间顺序，将针对样本视频帧的每个角度范围面元中的值连接，以形成针对每个角度范围面元的直方图。指纹识别子模块1602还被配置成将针对角度范围面元的直方图集合进行标准化，以形成建立新的视频指纹的对应的运动时间序列集合。

[0112] 在内容验证模块1406的另一示例性实施方式中，结合使用指纹识别算法来建立新的视频指纹，指纹识别子模块1602被配置成使用线性分段算法来压缩每个运动时间序列，以将对应的直方图转换成对应的线性分段序列。指纹识别子模块1602还至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从每个压缩的运动时间序列中提取主斜坡，以形成由提取的主斜坡表示的用于新的视频指纹的对应的运动时间序列集合。

[0113] 在内容验证模块1406的另一示例性实施方式中，原始视频指纹、无保证的视频指纹和新的视频指纹中的每个包括通过将对应的直方图变为线性分段序列、并且从该线性分段序列中提取主斜坡而形成的对应的运动时间序列集合。在该实施方式中，结合使用复杂性不变距离测量算法，测量子模块1604被配置成将无保证的视频指纹的每个运动时间序列与新的视频指纹的对应的运动时间序列配对。测量子模块1604还至少部分地基于在对应成对的运动时间序列中的相似的主斜坡的识别来对每个成对的运动时间序列进行校准。测量子模块1604还被配置成使用复杂性不变距离测量算法来确定每个校准的运动时间序列之间的距离测量。

[0114] 在内容验证模块1406的另一示例性实施方式中，原始视频指纹、无保证的视频指纹以及新的视频指纹中的每个包括由对应的直方图形成的对应的运动时间序列集合。在该实施方式中，结合使用复杂性不变距离测量算法，测量子模块1604被配置成使用线性分段

算法来压缩无保证的视频指纹的每个运动时间序列，以将对应的直方图转换成对应的线性分段序列。测量子模块1604还至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从无保证的视频指纹的每个压缩的运动时间序列中提取主斜坡，以形成由提取的主斜坡表示的用于无保证的视频指纹的对应的运动时间序列集合。测量子模块1604还被配置成使用线性分段算法来压缩新的视频指纹的每个运动时间序列，以将对应的直方图转换成对应的线性分段序列。此外，测量子模块1604至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从新的视频指纹的每个压缩的运动时间序列中提取主斜坡，以形成由提取的主斜坡表示的用于新的视频指纹的对应的运动时间序列集合。测量子模块1604还将无保证的视频指纹的每个运动时间序列与新的视频指纹的对应的运动时间序列配对。测量子模块1604还被配置成至少部分地基于在对应成对的运动时间序列中的相似的主斜坡的识别来对每个成对的运动时间序列进行校准。此外，测量子模块1604使用复杂性不变距离测量算法来确定每个校准的运动时间序列之间的距离测量。

[0115] 参考图17，用于认证视频内容的过程1700的另一示例性实施方式在1702处开始，在该1702处，从源设备接收视频内容。接下来，通过使用指纹识别算法处理视频内容，来生成视频指纹(1704)。在1706处，使用散列算法处理视频指纹以获取原始散列值。接下来，使用加密算法和私有密钥对原始散列值进行加密，以获取与原始散列值有关的数字签名(1708)。在1710处，数字签名、视频指纹和视频内容至少被临时存储在发射节点处的存储设备中。接下来，在通信网络中，在一个或多个通信会话中，从所述发射节点将数字签名、视频指纹和视频内容传送至接收节点(1712)。

[0116] 在另一实施方式中，结合使用散列算法，过程1700还包括向表示视频指纹的数据排列应用散列算法，以确定建立原始散列值的校验和的值。

[0117] 在过程1700的另一实施方式中，接收节点在接收到来自发射节点的数字签名、视频指纹和视频内容之后，能够确定解密的散列值是否与接收到的视频指纹一致，以验证接收到的视频指纹。在该实施方式中，接收节点还能够确定所述接收到的视频指纹是否与所述接收到的视频内容一致，来以容忍所述接收到的视频内容中预定量的损失的方式验证该接收到的视频内容。在另一实施方式中，如果接收到的视频指纹和接收到的视频内容由接收节点验证，接收到的视频内容被认证以供在接收节点的后续使用。在另一实施方式中，如果接收到的视频指纹未被接收节点验证，接收到的视频内容不被认证以供在接收节点的后续使用。在另一实施方式中，如果接收到的视频指纹被验证，而接收到的视频内容未被接收节点验证，接收到的视频内容不被认证以供在接收节点的后续使用。

[0118] 在过程1700的另一实施方式中，数字签名和视频内容在分开的通信会话中，经由不同的通信路径被传送至接收节点。在过程1700的另一实施方式中，视频指纹和视频内容在分开的通信会话中，经由不同的通信路径被传送至接收节点。

[0119] 在过程1700的另一实施方式中，数字签名被预先计划、嵌入或附加到所述视频内容，以传输至接收节点。在过程1700的另一实施方式中，视频指纹被预先计划、嵌入或附加到所述视频内容，以传输至接收节点。

[0120] 参考图17和图18，用于认证视频内容的过程1800的另一示例性实施方式结合使用指纹识别算法(1704)来扩展图17的过程1700。在该实施方式中，过程1800从图17的1704推

进到1802，在该1802处，视频帧的样本被从视频内容中选出，并按照连接的时间顺序排列。接下来，在每个样本视频帧中检测突出特征点(1804)。在1806处，针对每个样本视频帧中的每个突出特征点，计算与连接的时间顺序的下一样本视频帧中的对应的突出特征点有关的光学流动的角向。接下来，每个样本视频帧的突出特征点的角向被分布到针对每个样本视频帧的对应的角度范围面元(1808)。在1810，随着连接的时间顺序，针对样本视频帧的每个角度范围面元中的值被连接，以形成针对每个角度范围面元的直方图。接下来，针对角度范围面元的直方图集合被标准化，以形成建立视频指纹的对应的运动时间序列集合(1812)。在该实施方式中，过程1800在1812之后返回到1706。

[0121] 在另一实施方式中，结合使用指纹识别算法来建立视频指纹，过程1800还包括使用线性分段算法来压缩每个运动时间序列，以将对应的直方图转换成对应的线性分段序列。在该实施方式中，至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从每个压缩的运动时间序列中提取主斜坡，以形成由提取的主斜坡表示的用于视频指纹的对应的运动时间序列集合。

[0122] 参考图19，用于认证视频内容的发射节点1900的示例性实施方式包括输入模块1902、指纹识别模块1904、散列模块1906、加密模块1908、存储设备1910、输出模块1912以及控制器模块1914。输入模块1902被配置成从源设备1916接收视频内容。指纹识别模块1904被配置成通过使用指纹识别算法处理视频内容，来生成视频指纹。散列模块1906被配置成使用散列算法处理视频指纹以获取原始散列值。加密模块1908被配置成使用加密算法和私有密钥对原始散列值进行加密，以获取与原始散列值有关的数字签名。存储设备1910被配置成至少临时存储数字签名、视频指纹和视频内容。输出模块1912被配置成在通信网络1920中，在一个或多个通信会话中，将数字签名、视频指纹和视频内容传送至接收节点1918。控制器模块1914与输入模块1902、指纹识别模块1904、散列模块1906、加密模块1908、存储设备1910和输出模块1912有效通信，并且被配置成控制与对视频内容、视频指纹和数字签名中的一者或多者进行接收、生成、处理、加密、存储、和传送有关的操作。

[0123] 发射节点1900可以是通信网络1920中的网络节点，或者具有对该通信网络1920的接入的用户或计算设备。类似地，源设备1916可以是通信网络1920中的网络节点，或者具有对该通信网络1920的接入的用户或计算设备。例如，源设备1916可以包括视频捕捉设备(例如，视频摄像头)、视频存储设备(例如，视频内容服务器)、或者两者。发射节点1900和源设备1916可以位于不同的位置，可以共位(例如，安全系统)，或在相同的设备中被组合(例如，移动站、膝上型计算机等)。

[0124] 在发射节点1900的另一实施方式中，结合使用散列算法，散列模块1906被配置成向表示视频指纹的数据排列应用散列算法，以确定建立原始散列值的校验和的值。

[0125] 在发射节点1900的另一实施方式中，接收节点1918在接收到来自发射节点1900的数字签名、视频指纹和视频内容之后，能够确定解密的散列值是否与接收到的视频指纹一致，以验证接收到的视频指纹。在该实施方式中，接收节点1918还能够确定所述接收到的视频指纹是否与所述接收到的视频内容一致，来以容忍所述接收到的视频内容中预定量的损失的方式验证该接收到的视频内容。在另一实施方式中，如果接收到的视频指纹和接收到的视频内容由接收节点验证，接收到的视频内容被认证以供在接收节点1918的后续使用。在另一实施方式中，如果接收到的视频指纹未被接收节点验证，接收到的视频内容不被认

证以供在接收节点1918的后续使用。在另一实施方式中，如果接收到的视频指纹被验证，而接收到的视频内容未被接收节点验证，接收到的视频内容不被认证以供在接收节点1918的后续使用。

[0126] 在发射节点1900的另一实施方式中，数字签名和视频内容在分开的通信会话中，经由不同的通信路径被传送至接收节点。在发射节点1900的另一实施方式中，视频指纹和视频内容在分开的通信会话中，经由不同的通信路径被传送至接收节点。

[0127] 在发射节点1900的另一实施方式中，数字签名被预先计划、嵌入或附加到所述视频内容，以传输至接收节点。在发射节点1900的另一实施方式中，视频指纹被预先计划、嵌入或附加到所述视频内容，以传输至接收节点。

[0128] 在发射节点1900的另一实施方式中，结合使用指纹识别算法，指纹识别模块1904被配置成从视频内容中选择视频帧的样本，并按照连接的时间顺序排列该样本视频帧。指纹识别模块1904还检测每个样本视频帧中的突出特征点。指纹识别模块1904还被配置成针对每个样本视频帧中的每个突出特征点，计算与连接的时间顺序的下一样本视频帧中的对应的突出特征点有关的光学流动的角向。此外，指纹识别模块1904将每个样本视频帧的突出特征点的角向分布到针对每个样本视频帧的对应的角度范围面元。指纹识别模块1904还随着连接的时间顺序，将针对样本视频帧的每个角度范围面元中的值连接，以形成针对每个角度范围面元的直方图。指纹识别模块1904还被配置成将针对角度范围面元的直方图集合进行标准化，以形成建立视频指纹的对应的运动时间序列集合。

[0129] 在发射节点1900的另一实施方式中，结合使用指纹识别算法来建立视频指纹，指纹识别模块1904被配置成使用线性分段算法来压缩每个运动时间序列，以将对应的直方图转换成对应的线性分段序列。在该实施方式中，指纹识别模块1904还至少部分地基于选择针对时间特性和振幅特性中的至少一者大于预定的阈值的线性分段，来从每个压缩的运动时间序列中提取主斜坡，以形成由提取的主斜坡表示的用于视频指纹的对应的运动时间序列集合。

[0130] 再次参考图9-图16，非暂时性计算机可读介质的示例实施方式，该非暂时性计算机可读介质存储第一程序指令，当由第一计算机运行时，该第一程序指令引发计算机控制的接收节点1400执行用于认证视频内容的过程(例如，900、1000、1100、1200、1300)。在一个示例性实施方式中，该过程包括：在于通信网络中的接收节点处接收到来自发射节点的数字签名、无保证的视频指纹和无保证的视频内容之后，在所述接收节点处确定解密的散列值是否与所述无保证的视频指纹一致，以验证该无保证的视频指纹。该过程还在接收节点处确定所述无保证的视频指纹是否与所述无保证的视频内容一致，来以容忍所述无保证的视频内容中预定量的损失的方式验证该无保证的视频内容。在验证了所述无保证的视频指纹和所述无保证的视频内容的情况下，该无保证的视频内容被认证以供在所述接收节点的后续使用。

[0131] 在各种附加的实施方式中，存储在非暂时性计算机可读存储器中的第一指令在被第一计算机运行时，可以引发计算机控制的接收节点1400执行与上面描述的用于认证视频内容的过程900、1100、1200、1300相关联的功能的各种组合。换句话说，上面描述的各种特征可以由存储在非暂时性计算机可读介质中的第一程序指令以任意合适的组合来实施。上面描述的接收节点1400的任意合适的模块或子模块可以包括与对应的程序指令相关联的

对应的计算机和非暂时性计算机可读介质。可替换地，与对应的程序指令相关联的对应的计算机和非暂时性计算机可读介质可以是单个组件，或者是组合组件，该组件与上面描述的接收节点1400中的模块或子模块中的任意合适的组合有效通信。

[0132] 再次参考图17-图19，非暂时性计算机可读介质的示例实施方式，该非暂时性计算机可读介质存储第二程序指令，当由第二计算机运行时，该第二程序指令引发计算机控制的发射节点1900执行用于认证视频内容的过程(例如，1700、1800)。在一个示例性实施方式中，该过程包括：在从源设备接收到视频内容之后，通过使用指纹识别算法处理视频内容，来生成视频指纹。使用散列算法处理视频指纹以获取原始散列值。使用加密算法和私有密钥对原始散列值进行加密，以获取与原始散列值有关的数字签名。数字签名、视频指纹和视频内容至少被临时存储在发射节点处的存储设备中。在通信网络中，在一个或多个通信会话中，从所述发射节点将数字签名、视频指纹和视频内容传送至接收节点。

[0133] 在各种附加的实施方式中，存储在非暂时性计算机可读存储器中的第一指令在被第一计算机运行时，可以引发计算机控制的发射节点1900执行与上面描述的用于认证视频内容的过程1700、1800相关联的功能的各种组合。换句话说，上面描述的各种特征可以由存储在非暂时性计算机可读介质中的第一程序指令以任意合适的组合来实施。上面描述的发射节点1900的任意合适的模块可以包括与对应的程序指令相关联的对应的计算机和非暂时性计算机可读介质。可替换地，与对应的程序指令相关联的对应的计算机和非暂时性计算机可读介质可以是单个组件，或者是组合组件，该组件与上面描述的发射节点1900中的模块的任意合适的组合有效通信。

[0134] 上面的描述仅提供本发明的特定实施方式的公开，并不意图用于限制本发明的目的。如此，本发明不只被限于上面描述的实施方式。而是，公认的是，本领域的技术人员能够想到替换实施方式，该替换实施方式落入本发明的范围。

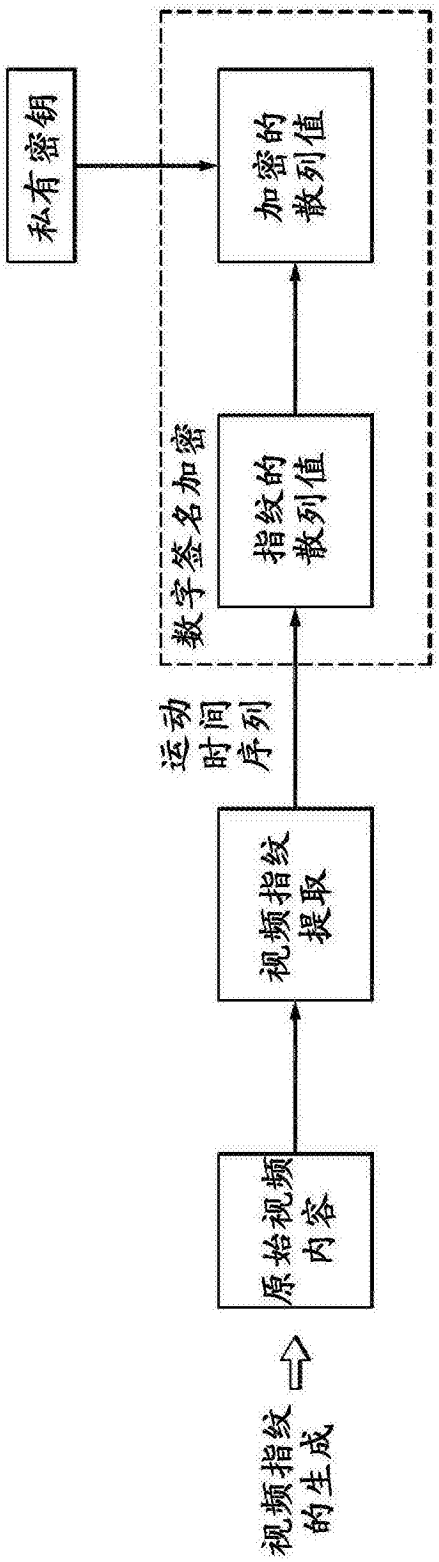


图1

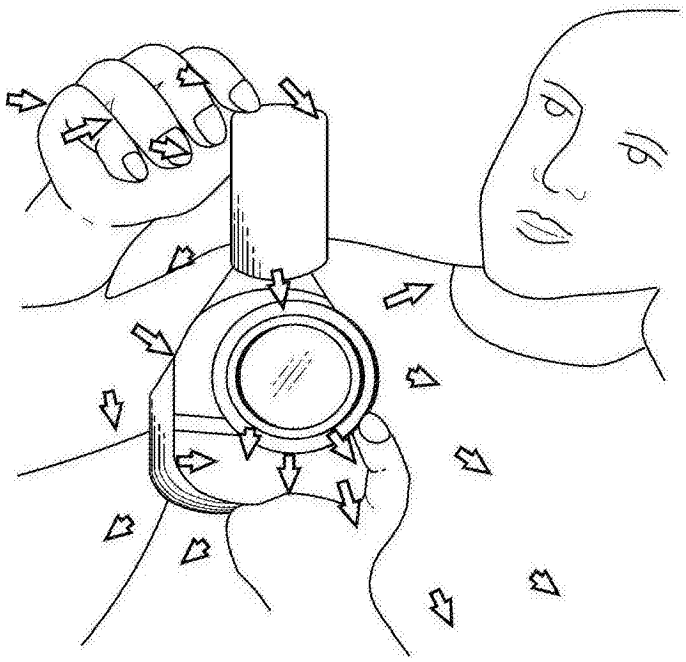


图2

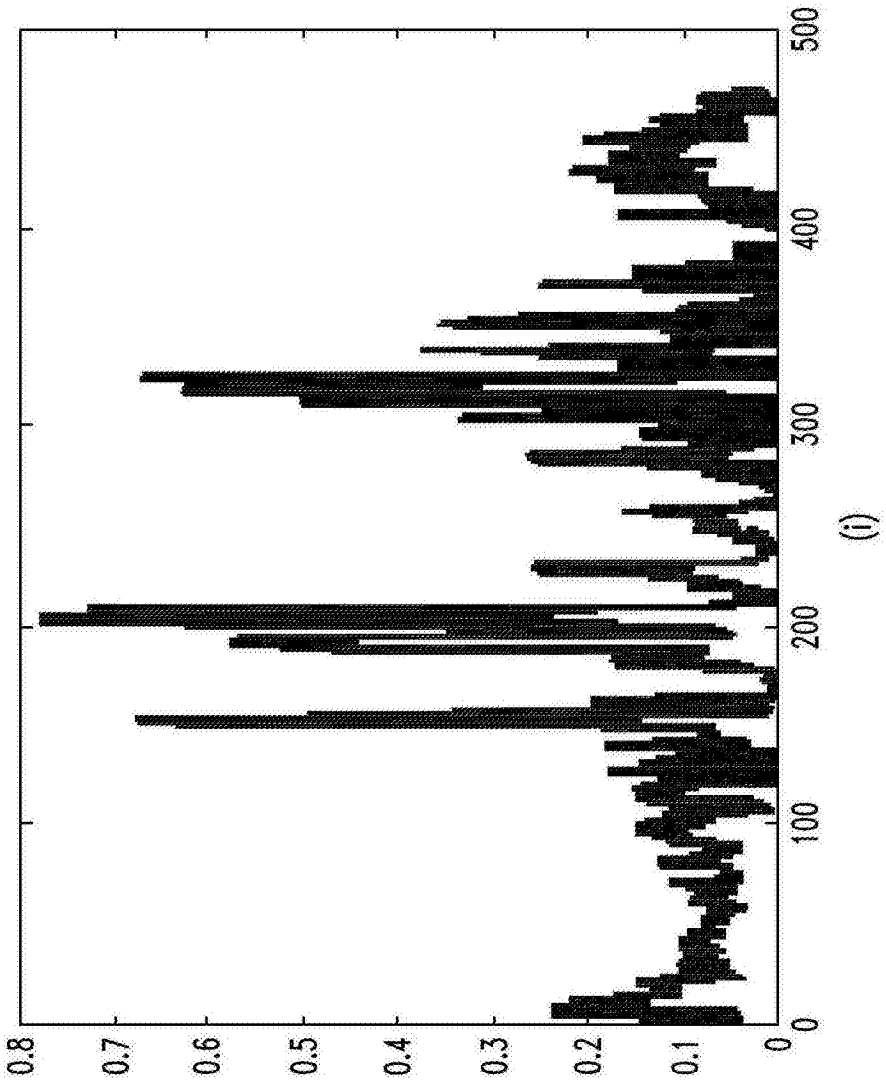


图3

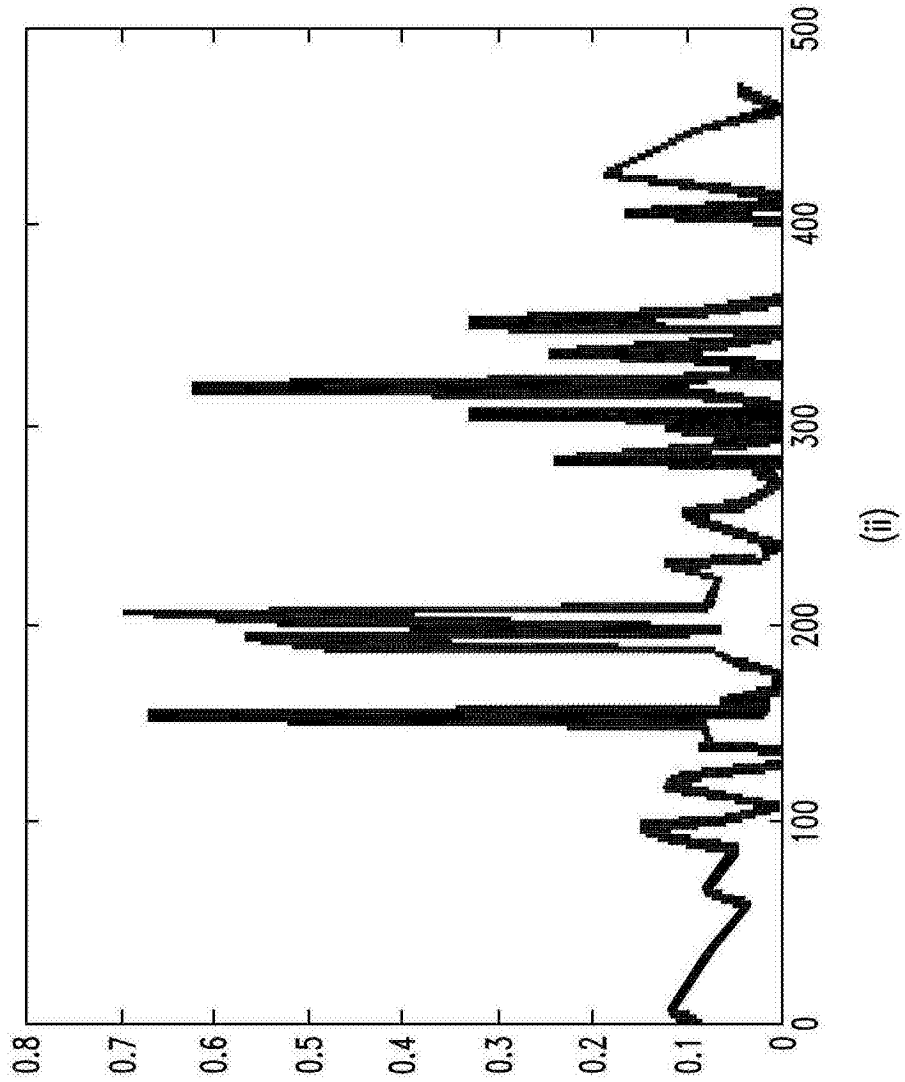


图4

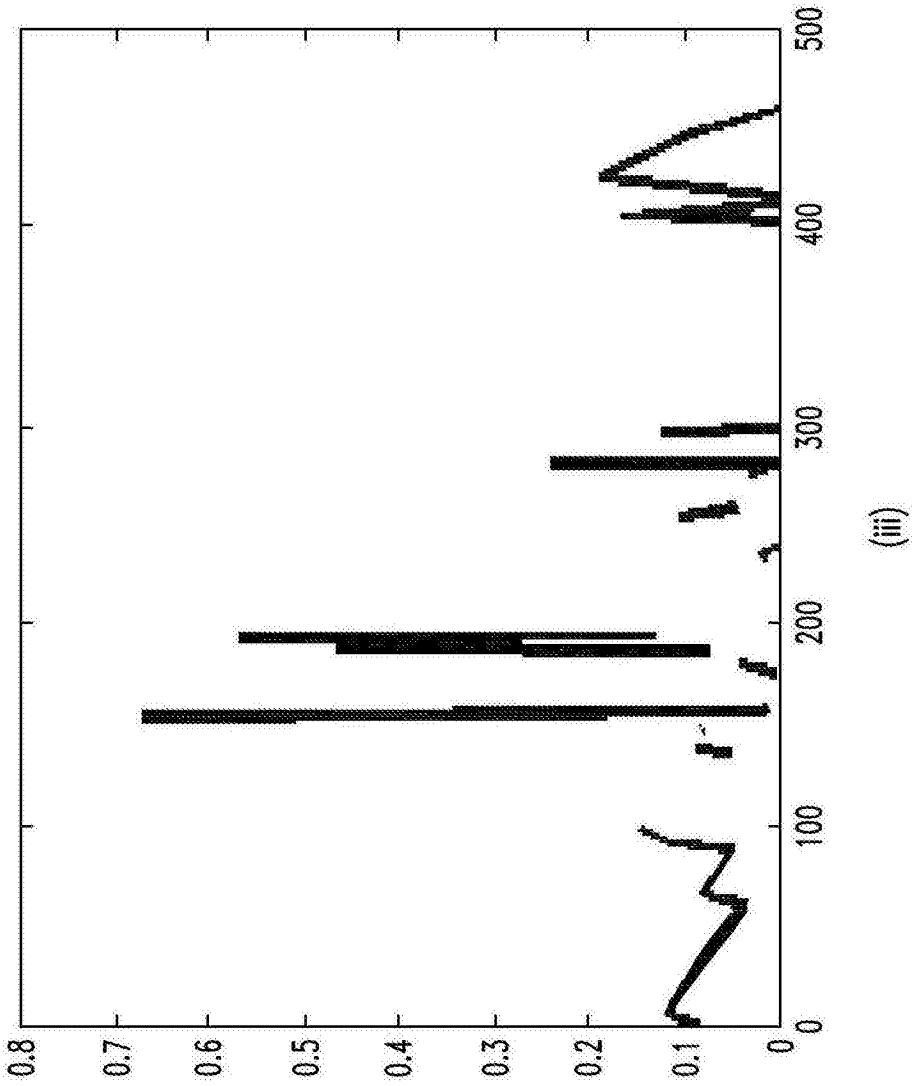


图5

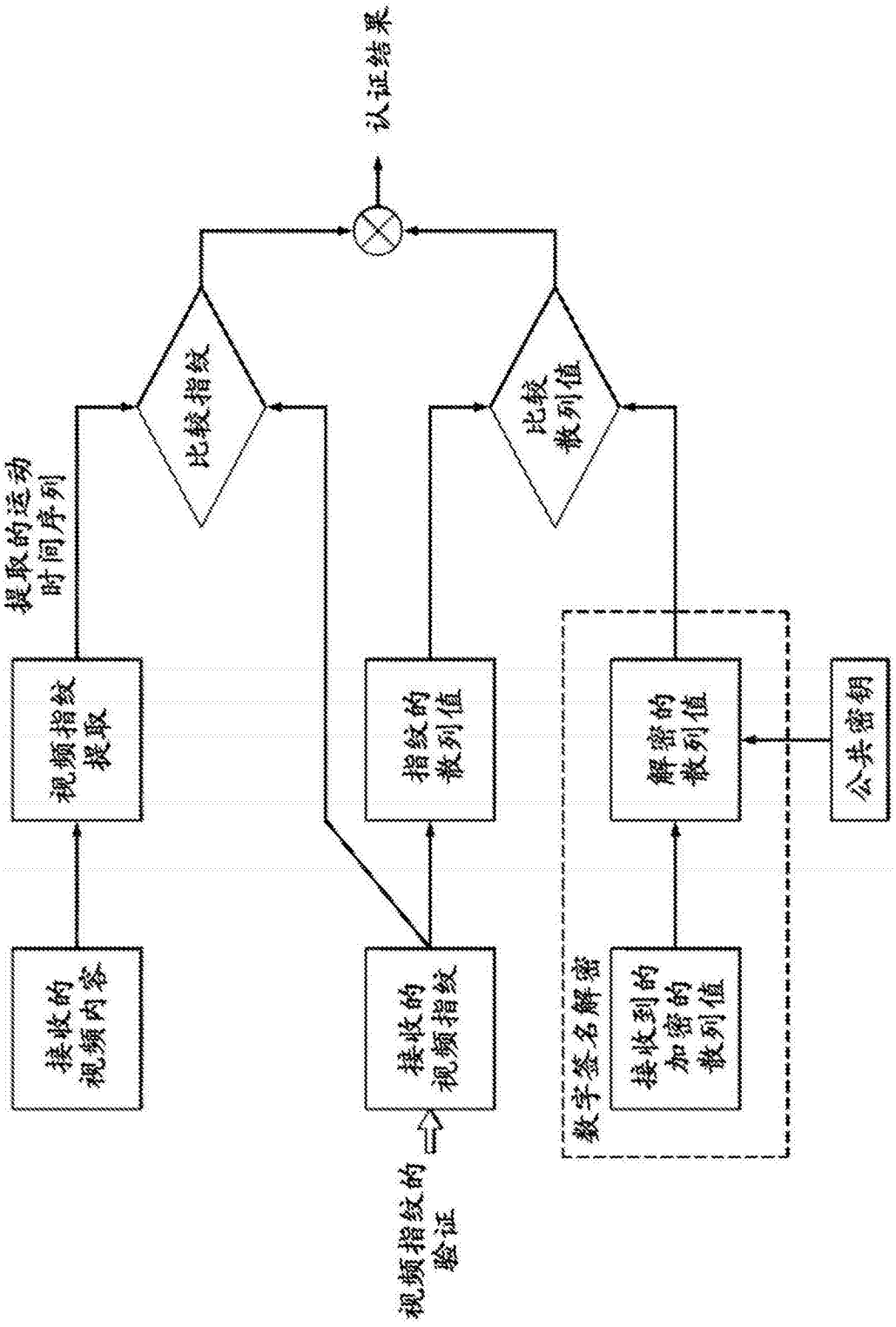

认证结果
比较指纹
比较
数列值
提取的运动
时间序列
视频指纹
提取
指纹的
数列值
解密的
数列值
公共密钥
接收的
视频内容
接收的
视频指纹
数字签名解密
接收到的
加密的
数列值
视频指纹的
验证

图6

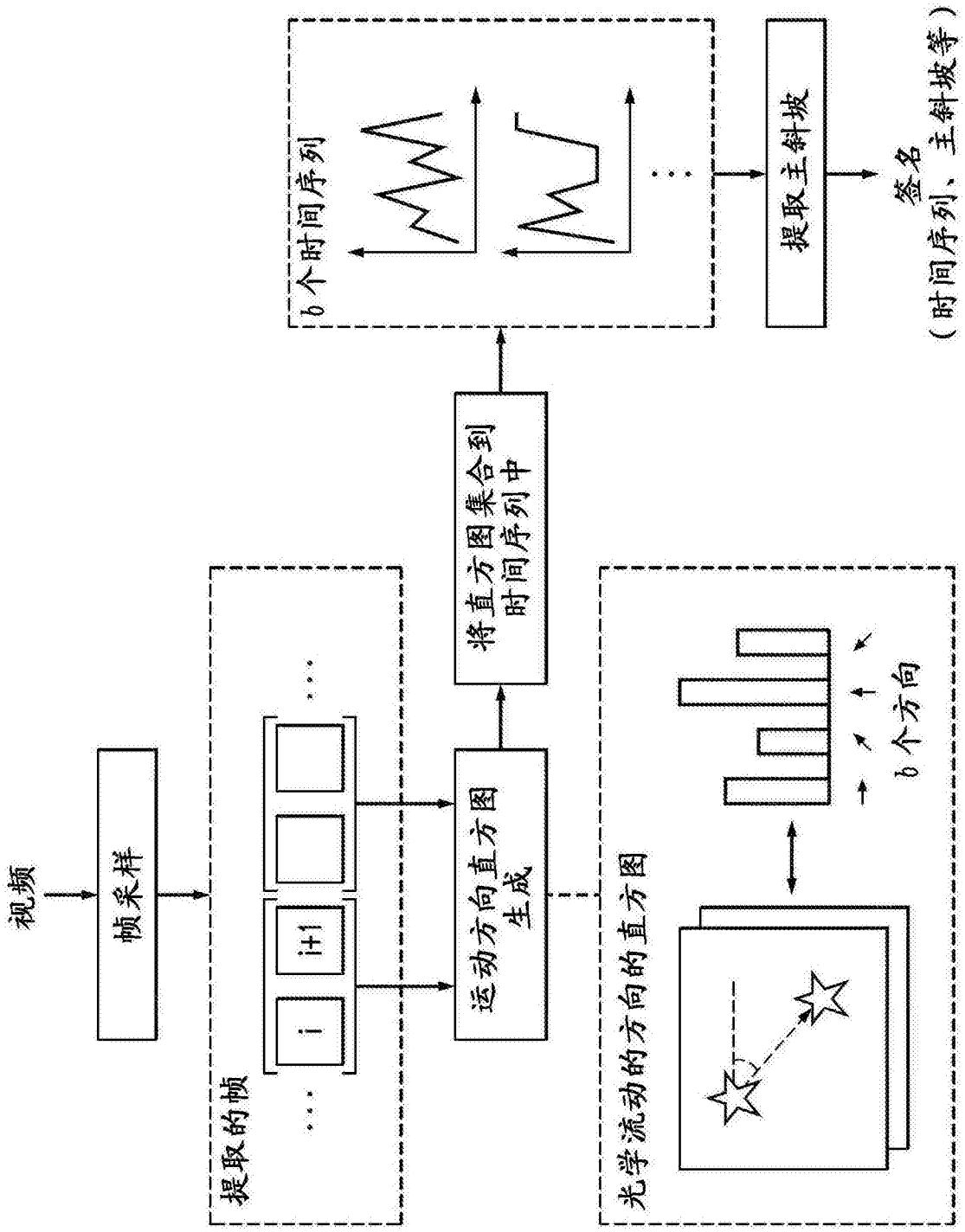

视频
帧采样
提取的帧
i
i+1
运动方向直方图
生成
将直方图集合到
时间序列中
b个时间序列
提取主斜坡
签名
（时间序列、主斜坡等）
光学流动的方向的直方图
b个方向

图7

团队	精度	查询时间
领英	0.86	64 min
中国科学院 -1	0.46	41 min
中国科学院 -2	0.53	14 min
香港城市大学	0.66	45 min
IBM - 1	0.86	44 min
IBM - 2	0.73	68 min
IBM - 3	0.8	99 min
我们的方式	1.0	<10 min

图8

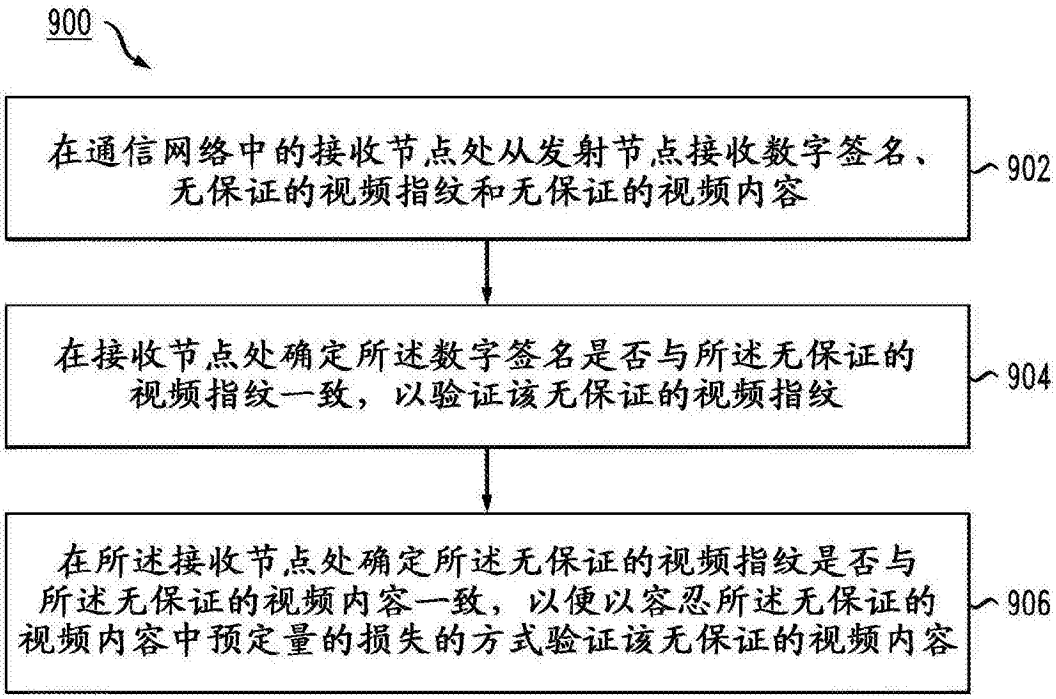


图9

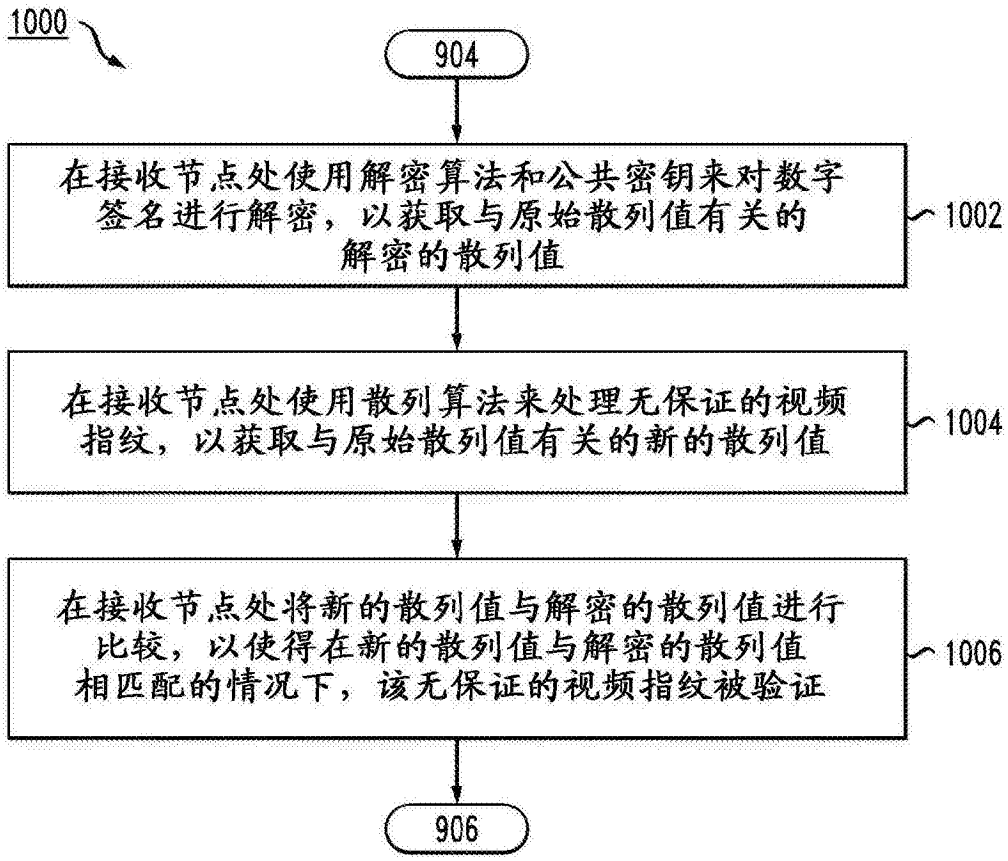

1000
904
在接收节点处使用解密算法和公共密钥来对数字签名进行解密，以获取与原始散列值有关的解密的散列值
1002
在接收节点处使用散列算法来处理无保证的视频指纹，以获取与原始散列值有关的新的散列值
1004
在接收节点处将新的散列值与解密的散列值进行比较，以使得在新的散列值与解密的散列值相匹配的情况下，该无保证的视频指纹被验证
1006
906

图10

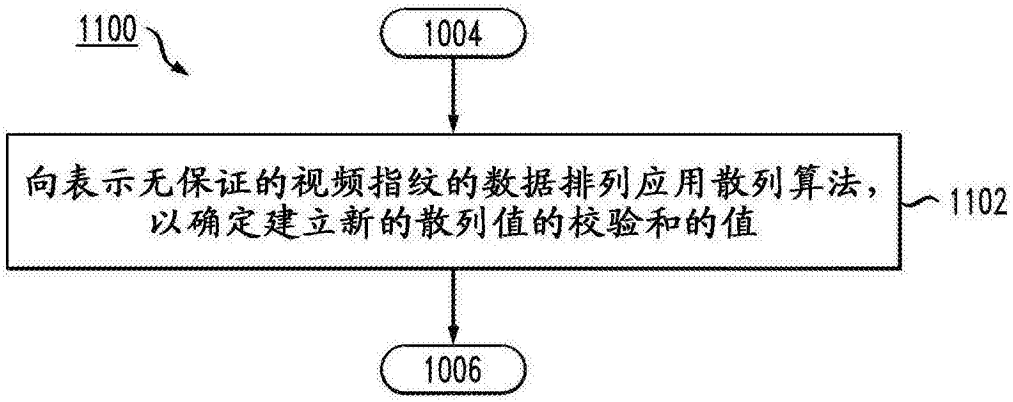

1100
1004
向表示无保证的视频指纹的数据排列应用散列算法，以确定建立新的散列值的校验和的值
1102
1006

图11

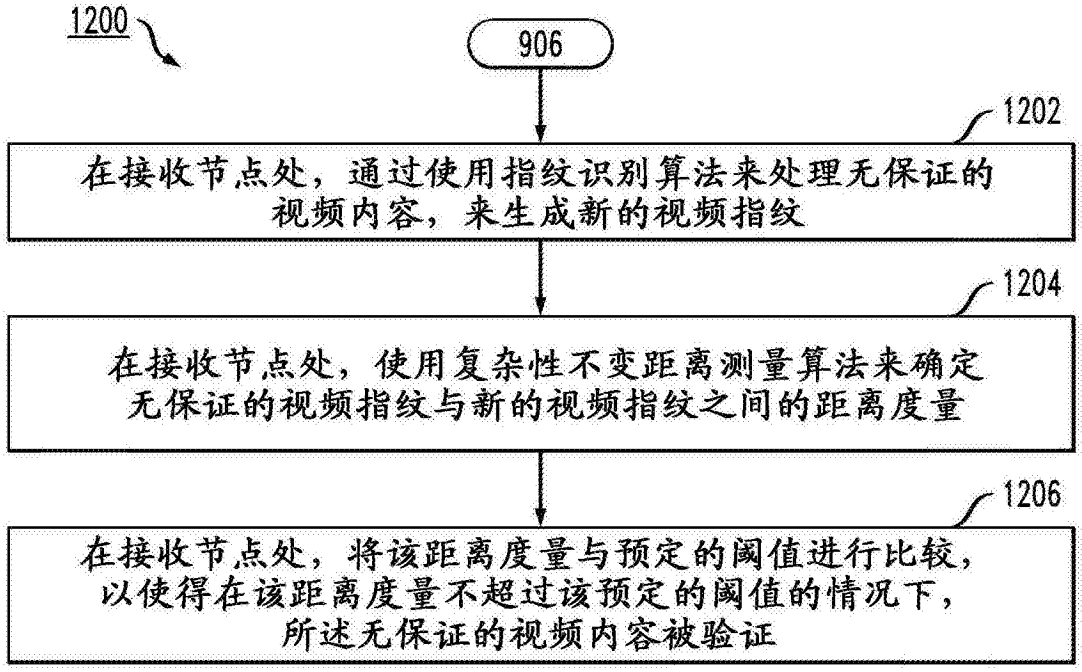

1200
906
1202
在接收节点处，通过使用指纹识别算法来处理无保证的视频内容，来生成新的视频指纹
1204
在接收节点处，使用复杂性不变距离测量算法来确定无保证的视频指纹与新的视频指纹之间的距离度量
1206
在接收节点处，将该距离度量与预定的阈值进行比较，以使得在该距离度量不超过该预定的阈值的情况下，所述无保证的视频内容被验证

图12

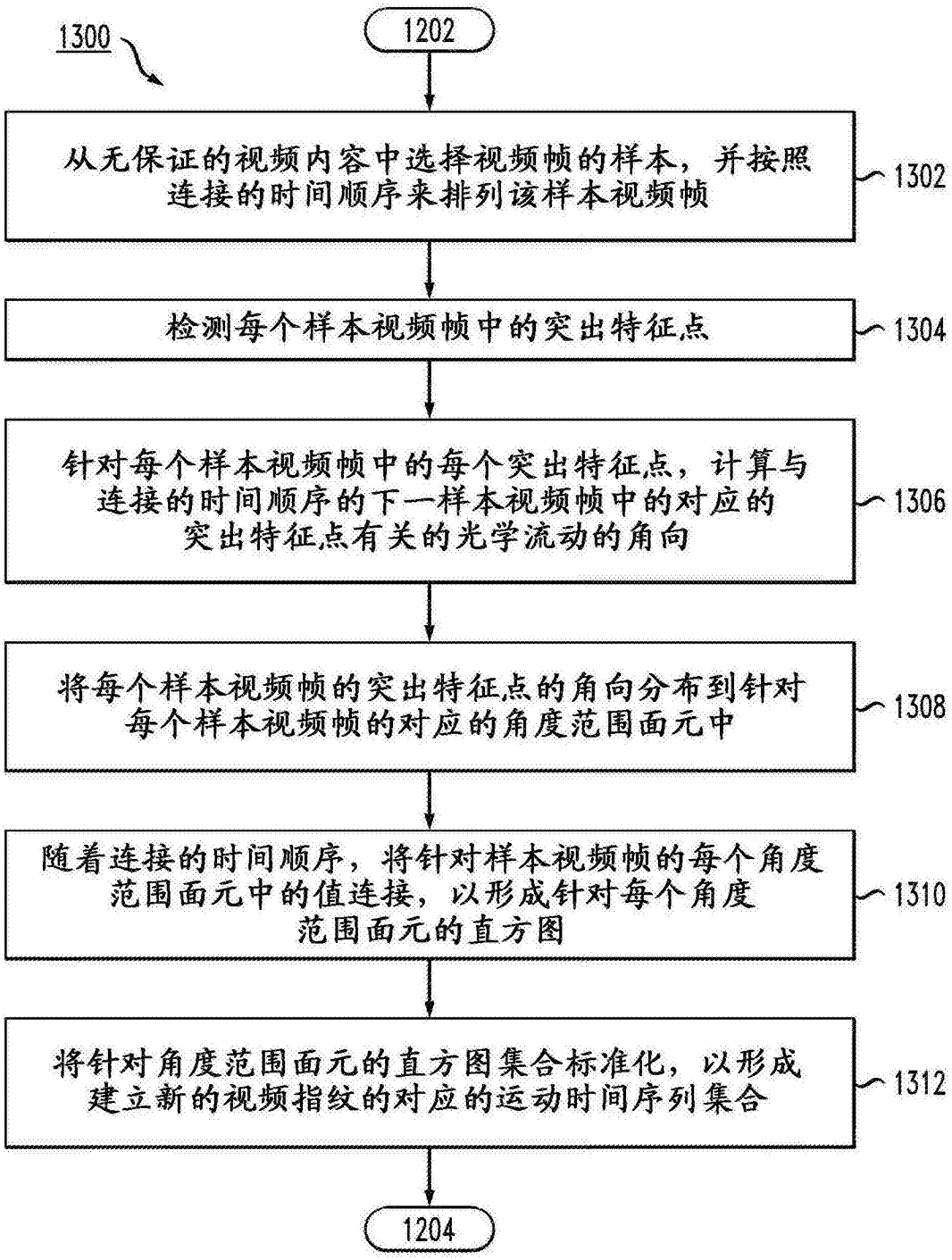

1300
1202
从无保证的视频内容中选择视频帧的样本，并按照连接的时间顺序来排列该样本视频帧
1302
检测每个样本视频帧中的突出特征点
1304
针对每个样本视频帧中的每个突出特征点，计算与连接的时间顺序的下一样本视频帧中的对应的突出特征点有关的光学流动的角向
1306
将每个样本视频帧的突出特征点的角向分布到针对每个样本视频帧的对应的角度范围面元中
1308
随着连接的时间顺序，将针对样本视频帧的每个角度范围面元中的值连接，以形成针对每个角度范围面元的直方图
1310
将针对角度范围面元的直方图集合标准化，以形成建立新的视频指纹的对应的运动时间序列集合
1312
1204

图13

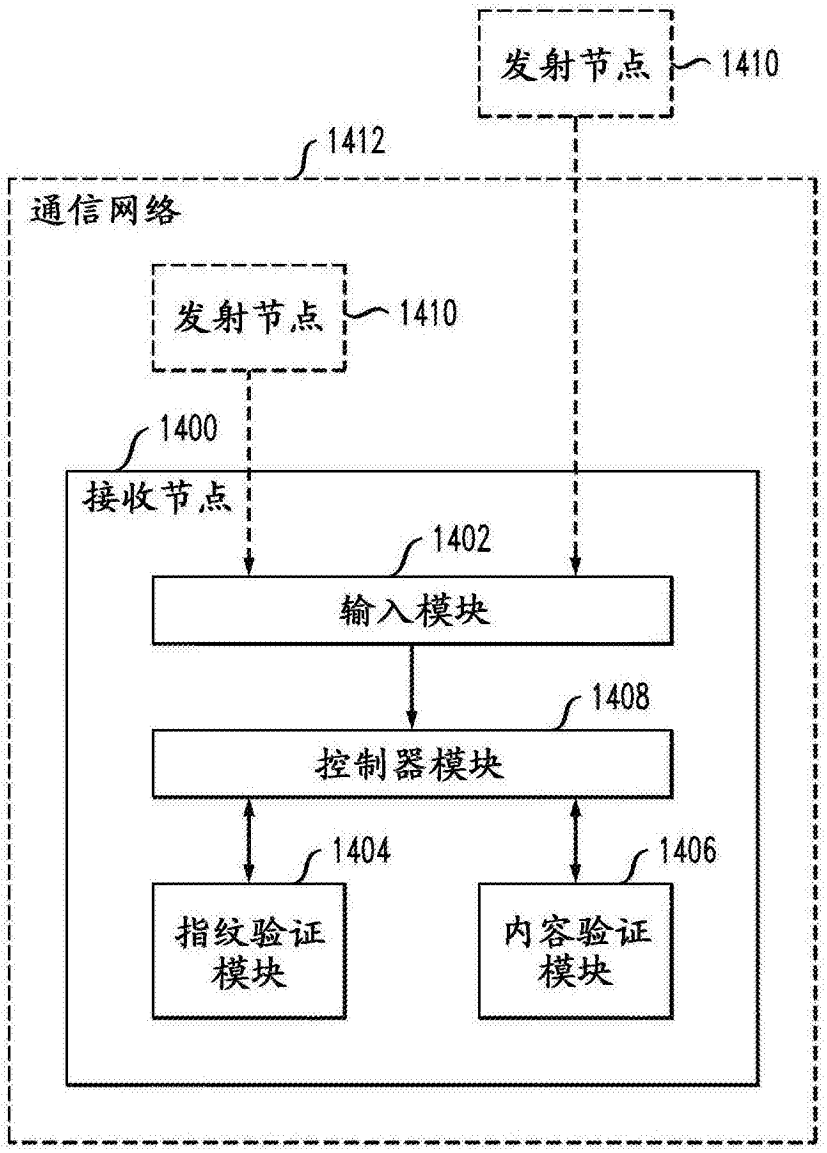

发射节点
1410
1412
通信网络
发射节点
1410
1400
接收节点
1402
输入模块
1408
控制器模块
1404
1406
指纹验证模块
内容验证模块

图14

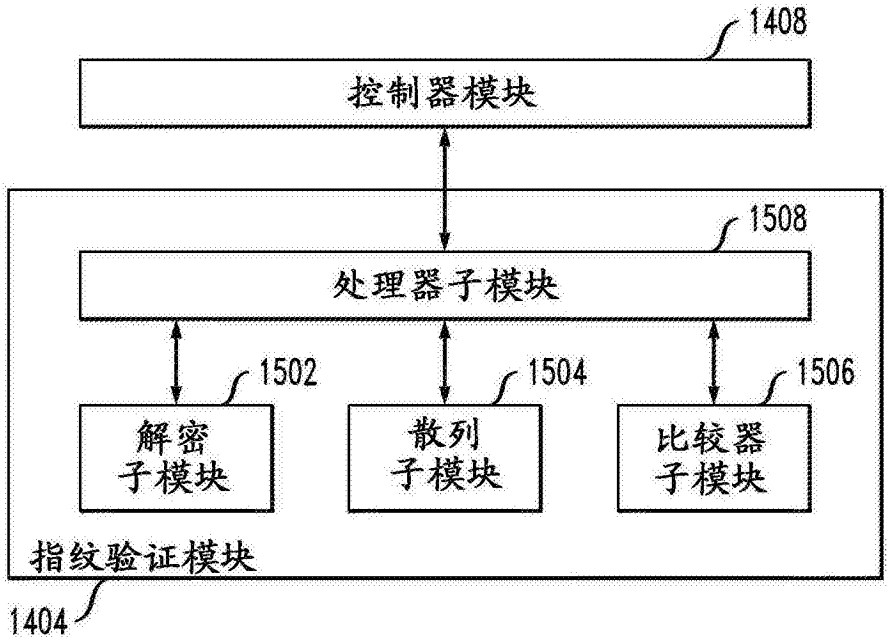

1408
控制器模块
1508
处理器子模块
1502
1504
1506
解密
子模块
散列
子模块
比较器
子模块
指纹验证模块
1404

图15

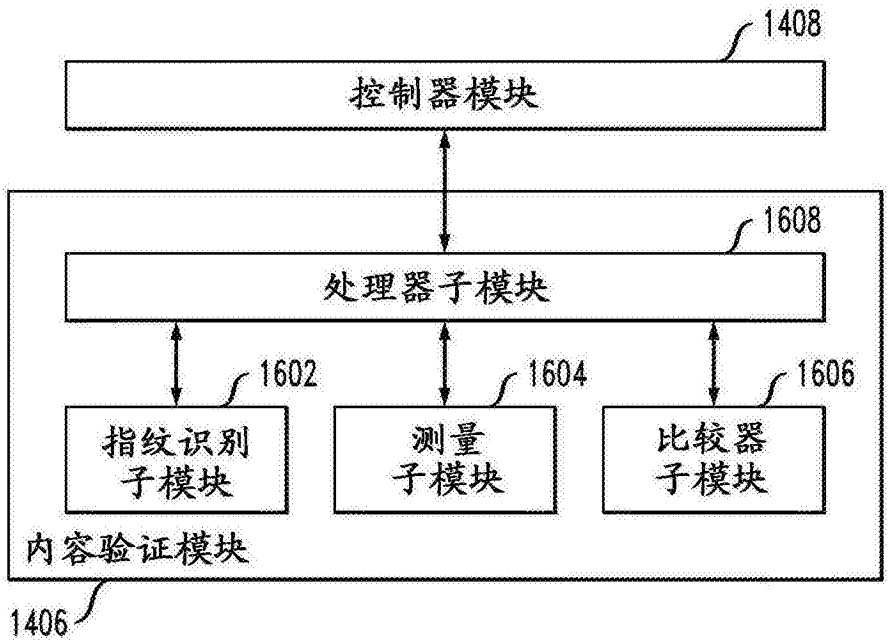

1408
控制器模块
1608
处理器子模块
1602
1604
1606
指纹识别
子模块
测量
子模块
比较器
子模块
内容验证模块
1406

图16

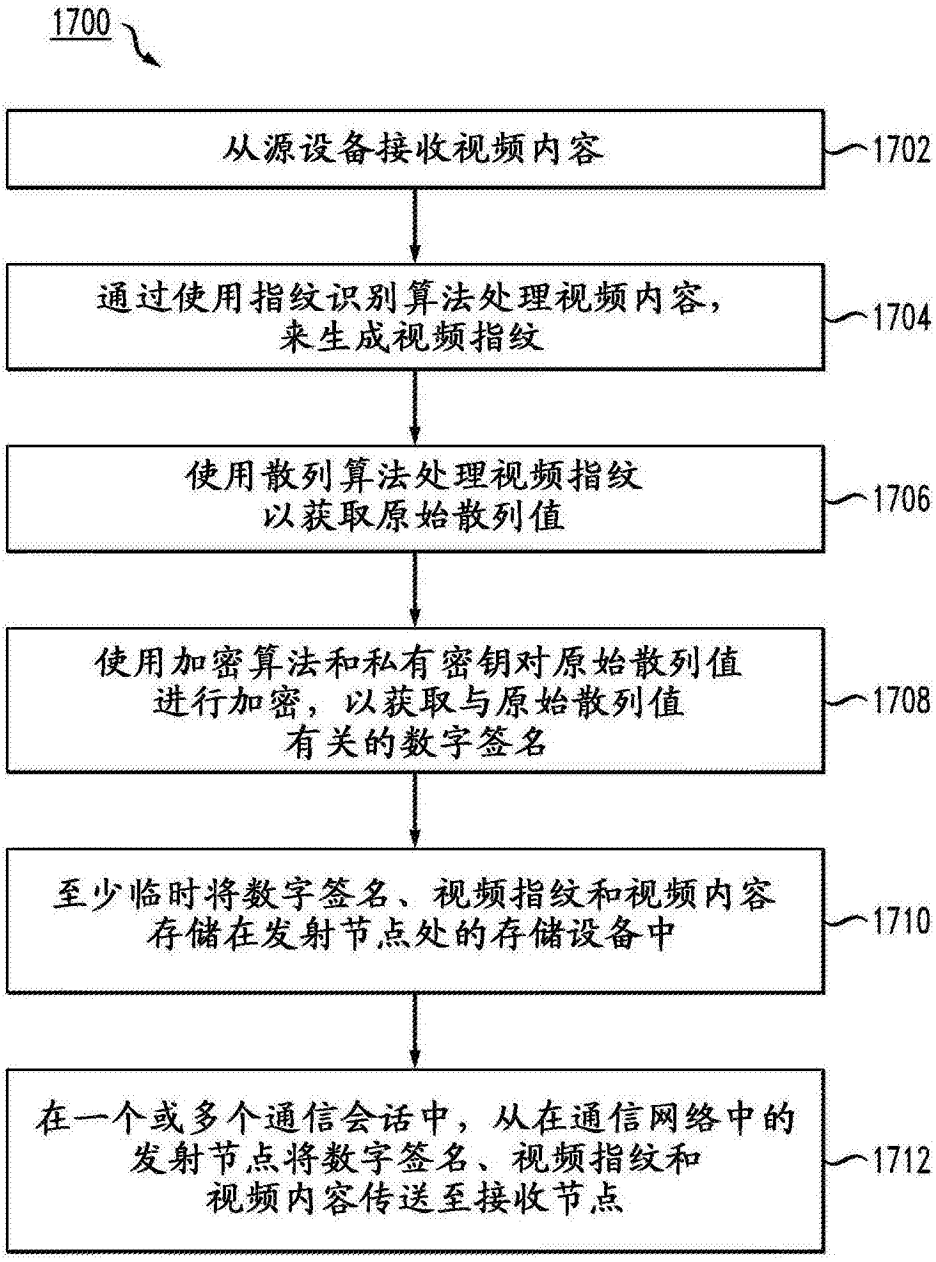

1700
从源设备接收视频内容
1702
通过使用指纹识别算法处理视频内容，来生成视频指纹
1704
使用散列算法处理视频指纹以获取原始散列值
1706
使用加密算法和私有密钥对原始散列值进行加密，以获取与原始散列值有关的数字签名
1708
至少临时将数字签名、视频指纹和视频内容存储在发射节点处的存储设备中
1710
在一个或多个通信会话中，从在通信网络中的发射节点将数字签名、视频指纹和视频内容传送至接收节点
1712

图17

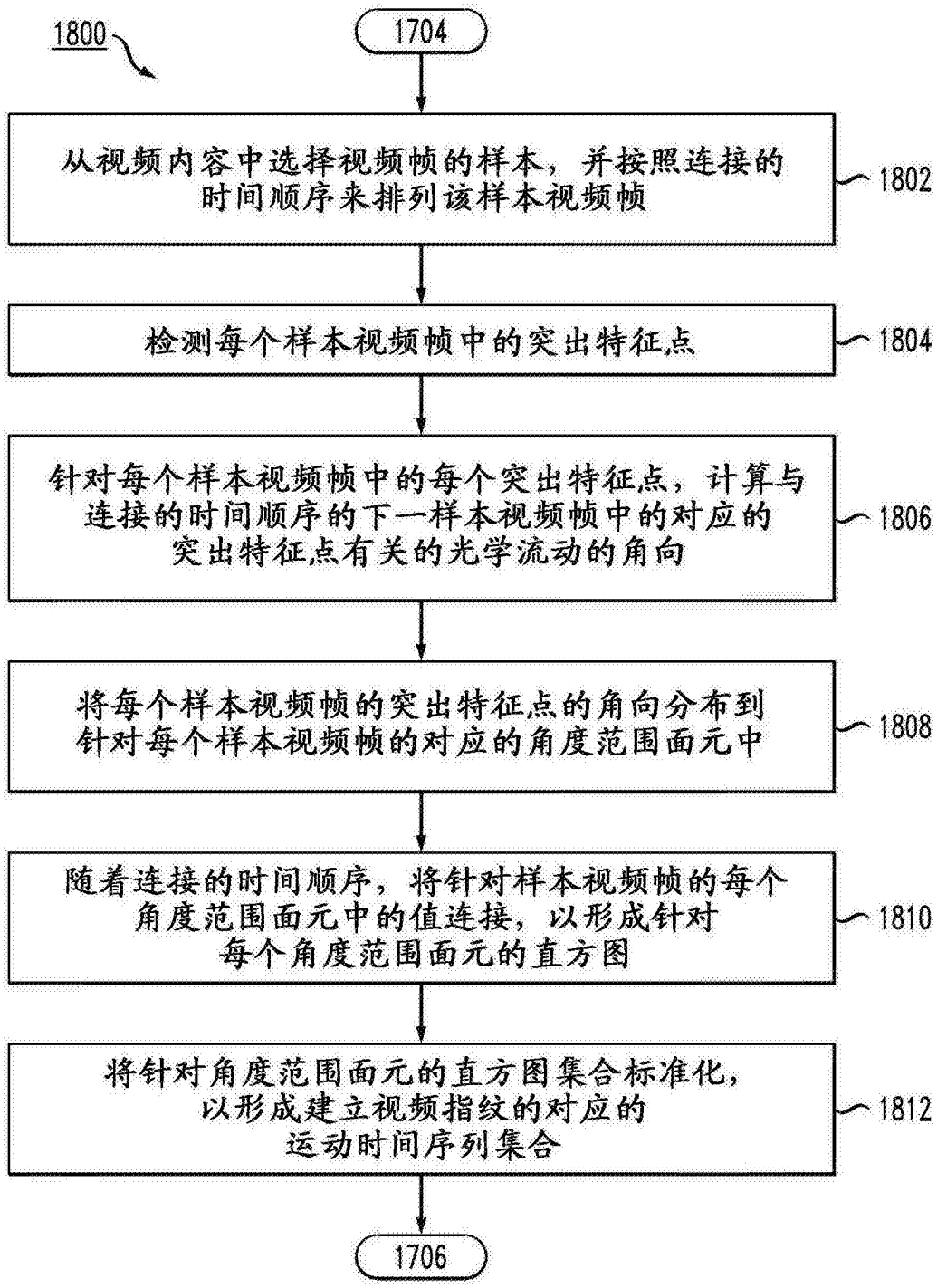

1800
1704
从视频内容中选择视频帧的样本，并按照连接的时间顺序来排列该样本视频帧
1802
检测每个样本视频帧中的突出特征点
1804
针对每个样本视频帧中的每个突出特征点，计算与连接的时间顺序的下一样本视频帧中的对应的突出特征点有关的光学流动的角向
1806
将每个样本视频帧的突出特征点的角向分布到针对每个样本视频帧的对应的角度范围面元中
1808
随着连接的时间顺序，将针对样本视频帧的每个角度范围面元中的值连接，以形成针对每个角度范围面元的直方图
1810
将针对角度范围面元的直方图集合标准化，以形成建立视频指纹的对应的运动时间序列集合
1812
1706

图18

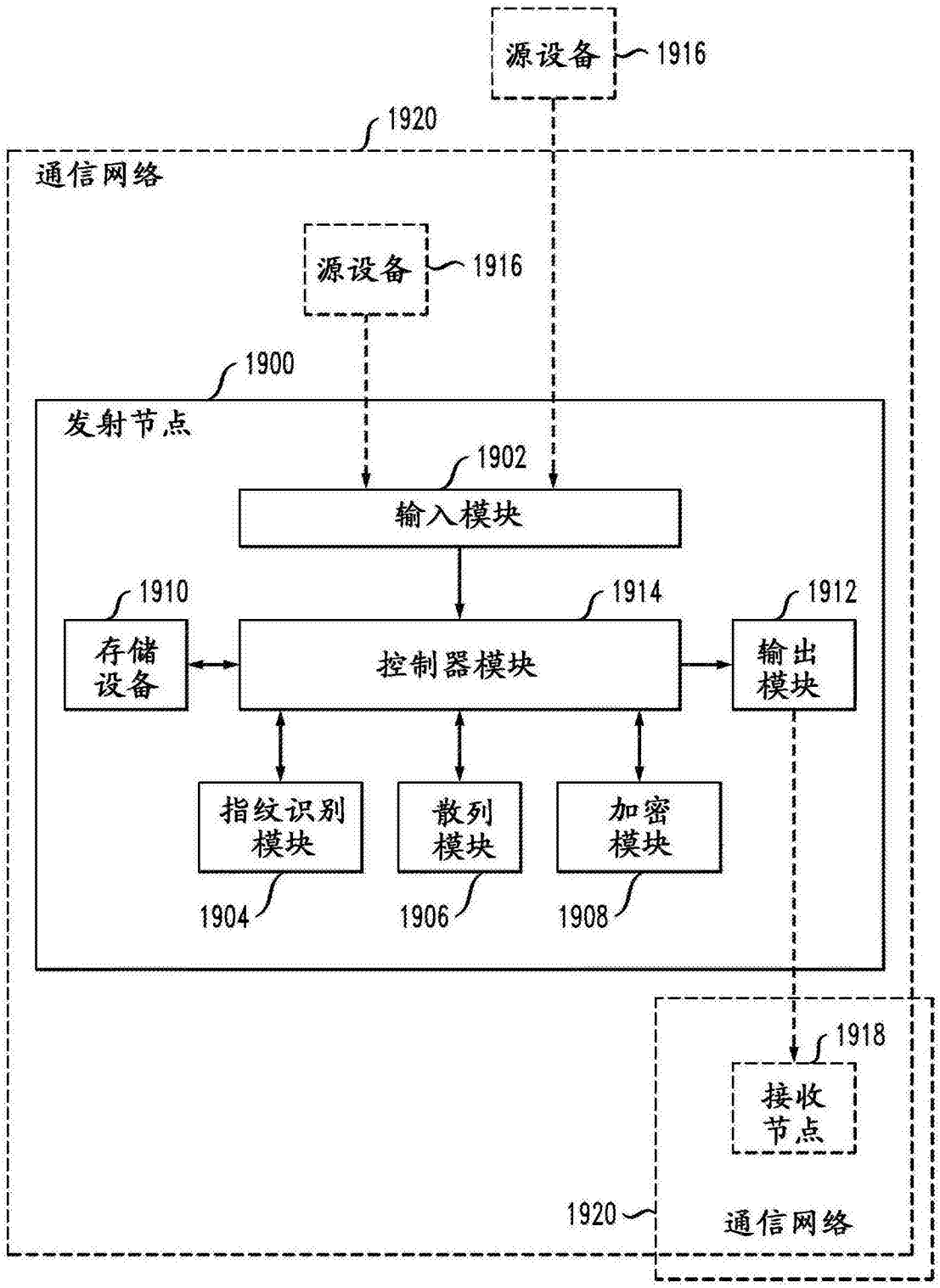

源设备
1916
1920
通信网络
源设备
1916
1900
发射节点
1902
输入模块
1910
存储设备
1914
控制器模块
1912
输出模块
指纹识别模块
散列模块
加密模块
1904
1906
1908
1918
接收节点
1920
通信网络

图19