(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108875688 B
(45)授权公告日 2022.06.10

(21)申请号 201810706117.X
(22)申请日 2018.06.28
(65)同一申请的已公布的文献号
申请公布号 CN 108875688 A
(43)申请公布日 2018.11.23
(73)专利权人 北京旷视科技有限公司
地址 100190 北京市海淀区科学院南路2号A座313
(72)发明人 刘海敏 龙俊洁
(74)专利代理机构 北京睿邦知识产权代理事务所(普通合伙) 11481
专利代理师 徐丁峰 张玮
(51)Int.Cl.
G06V 40/40(2022.01)

(56)对比文件
CN 106575401 A,2017.04.19
CN 106575401 A,2017.04.19
CN 105844203 A,2016.08.10
CN 107181717 A,2017.09.19
CN 101178755 A,2008.05.14
US 2013298192 A1,2013.11.07
JP 2016062457 A,2016.04.25
JP 2013114283 A,2013.06.10
US 2013346311 A1,2013.12.26
US 2013104203 A1,2013.04.25

审查员 彭鼎原

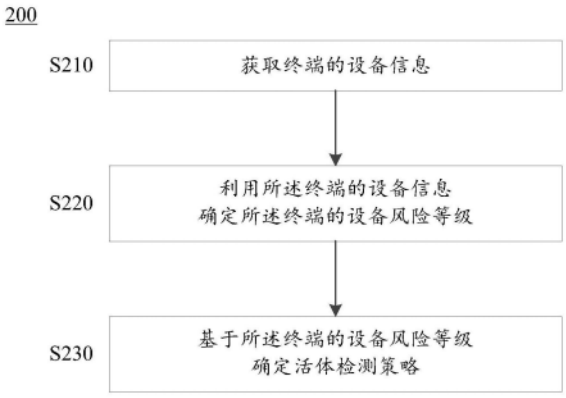
权利要求书2页 说明书12页 附图3页

(54)发明名称

一种活体检测方法、装置、系统及存储介质

(57)摘要

本发明的实施例提供了一种活体检测方法、装置、系统及存储介质。该活体检测方法包括:获取终端的设备信息,所述终端用于获取待检测对象的图像;利用所述终端的设备信息确定所述终端的设备风险等级;基于所述终端的设备风险等级确定活体检测策略。上述技术方案利用终端的设备信息来调整活体检测策略,保证了真实活体以更小成本通过检测,同时让假活体、恶意活体难以通过检测。由此,大大降低了活体检测的安全风险,提升了用户体验,同时防止了恶意请求对系统资源的占用。



CN 108875688 B

1.一种活体检测方法,包括:

获取终端的设备信息,所述终端用于获取待检测对象的图像,其中,所述图像用于活体检测,所述设备信息包括以下一项或多项:设备指纹、设备电量信息以及设备传感器信息;

利用所述终端的设备信息确定所述终端的设备风险等级;

基于所述终端的设备风险等级确定活体检测策略;

其中,所述利用所述终端的设备信息确定所述终端的设备风险等级包括:根据所述终端的设备信息确定所述终端是否是虚拟机,其中,所述虚拟机的设备风险等级为高危风险。

2.如权利要求1所述的方法,其中,所述设备传感器包括以下一个或多个:

陀螺仪传感器、重力传感器、加速度传感器以及磁场传感器。

3.如权利要求1所述的方法,其中,所述设备信息包括设备指纹,所述利用所述终端的设备信息确定所述终端的设备风险等级包括:

对于所述终端的设备指纹属于设备指纹高危黑名单库的情况,确定所述终端的设备风险等级为高危风险;和/或

对于所述终端的设备指纹属于设备指纹风险黑名单库的情况,确定所述终端的设备风险等级为有风险。

4.如权利要求1所述的方法,其中,所述设备信息包括关于所述终端的异常访问次数的信息,所述利用所述终端的设备信息确定所述终端的设备风险等级包括:

对于所述终端的异常访问次数大于第一阈值的情况,确定所述终端的设备风险等级为高危风险;

对于所述终端的异常访问次数不大于第一阈值但大于第二阈值的情况,确定所述终端的设备风险等级为有风险。

5.如权利要求1至4任一项所述的方法,其中,所述基于所述终端的设备风险等级确定活体检测策略包括:

对于所述终端的设备风险等级为高危风险的情况,确定所述活体检测策略为拒绝策略。

6.如权利要求3或4所述的方法,其中,所述基于所述终端的设备风险等级确定活体检测策略包括:

对于所述终端的设备风险等级为有风险的情况,确定所述活体检测策略为随机增加要求所述待检测对象执行的动作数量和/或提升要求所述待检测对象执行的动作难度;和/或

对于所述终端的设备风险等级不是高危风险也不是有风险的情况,确定所述活体检测策略为随机减少要求所述待检测对象执行的动作数量和/或降低要求所述待检测对象执行的动作难度。

7.一种用于活体检测的装置,包括:

获取模块,用于获取终端的设备信息,其中,所述终端用于获取待检测对象的图像,所述图像用于活体检测,所述设备信息包括以下一项或多项:设备指纹、设备电量信息以及设备传感器信息;

风险模块,用于利用所述终端的设备信息确定所述终端的设备风险等级;

确定模块,用于基于所述终端的设备风险等级确定活体检测策略;

其中,所述利用所述终端的设备信息确定所述终端的设备风险等级包括:根据所述终

端的设备信息确定所述终端是否是虚拟机，其中，所述虚拟机的设备风险等级为高危风险。

8.一种用于活体检测的系统，包括处理器和存储器，其中，所述存储器中存储有计算机程序指令，所述计算机程序指令被所述处理器运行时用于执行如权利要求1至6任一项所述的活体检测方法。

9.一种存储介质，在所述存储介质上存储了程序指令，所述程序指令在运行时用于执行如权利要求1至6任一项所述的活体检测方法。

一种活体检测方法、装置、系统及存储介质

技术领域

[0001] 本发明涉及图像处理技术领域，更具体地涉及一种活体检测方法、装置、系统及存储介质。

背景技术

[0002] 随着科技的发展以及自动化程度的提高，诸如生物识别系统的诸多应用系统需要具有活体检测功能，即判断用户是否是有生命的个体。

[0003] 一般活体检测技术利用的是人的生理特征。例如活体指纹检测可以基于手指的温度、排汗、导电性能等信息。活体人脸检测可以基于呼吸、红外效应等信息。活体虹膜检测可以基于虹膜振颤特性、睫毛和眼皮的运动信息、瞳孔对可见光源强度的收缩扩张反应特性等。这些活体检测技术依赖于检测人的生理特征的传感器技术，难以确保活体检测的准确率，也不能有效防止恶意活体对系统的攻击。

发明内容

[0004] 考虑到上述问题而提出了本发明。本发明提供了一种活体检测方法、装置、系统及存储介质。

[0005] 根据本发明一方面，提供了一种活体检测方法，包括：

[0006] 获取终端的设备信息，所述终端用于获取待检测对象的图像；

[0007] 利用所述终端的设备信息确定所述终端的设备风险等级；

[0008] 基于所述终端的设备风险等级确定活体检测策略。

[0009] 示例性地，所述利用所述终端的设备信息确定所述终端的设备风险等级包括：

[0010] 根据所述终端的设备信息确定所述终端是否是虚拟机，其中，所述虚拟机的设备风险等级为高危风险。

[0011] 示例性地，所述设备信息包括以下一项或多项：设备指纹、设备电量信息以及设备传感器信息。

[0012] 示例性地，所述设备传感器包括以下一个或多个：陀螺仪传感器、重力传感器、加速度传感器以及磁场传感器。

[0013] 示例性地，所述设备信息包括设备指纹，所述利用所述终端的设备信息确定所述终端的设备风险等级包括：

[0014] 对于所述终端的设备指纹属于设备指纹高危黑名单库的情况，确定所述终端的设备风险等级为高危风险；和/或

[0015] 对于所述终端的设备指纹属于设备指纹风险黑名单库的情况，确定所述终端的设备风险等级为有风险。

[0016] 示例性地，所述设备信息包括关于所述终端的异常访问次数的信息，所述利用所述终端的设备信息确定所述终端的设备风险等级包括：

[0017] 对于所述终端的异常访问次数大于第一阈值的情况，确定所述终端的设备风险等

级为高危风险；

[0018] 对于所述终端的异常访问次数不大于第一阈值但大于第二阈值的情况，确定所述终端的设备风险等级为有风险。

[0019] 示例性地，所述基于所述终端的设备风险等级确定活体检测策略包括：对于所述终端的设备风险等级为高危风险的情况，确定所述活体检测策略为拒绝策略。

[0020] 示例性地，所述基于所述终端的设备风险等级确定活体检测策略包括：

[0021] 对于所述终端的设备风险等级为有风险的情况，确定所述活体检测策略为随机增加要求所述待检测对象执行的动作数量和/或提升要求所述待检测对象执行的动作难度；

[0022] 对于所述终端的设备风险等级不是高危风险也不是有风险的情况，确定所述活体检测策略为随机减少要求所述待检测对象执行的动作数量和/或降低要求所述待检测对象执行的动作难度。

[0023] 根据本发明另一方面，还提供了一种用于活体检测的装置，包括：

[0024] 获取模块，用于获取终端的设备信息；

[0025] 风险模块，用于利用所述终端的设备信息确定所述终端的设备风险等级；

[0026] 确定模块，用于基于所述终端的设备风险等级确定活体检测策略。

[0027] 根据本发明又一方面，还提供了一种活体检测系统，包括处理器和存储器，其中，所述存储器中存储有计算机程序指令，所述计算机程序指令被所述处理器运行时用于执行上述活体检测方法。

[0028] 根据本发明再一方面，还提供了一种存储介质，在所述存储介质上存储了程序指令，所述程序指令在运行时用于执行上述活体检测方法。

[0029] 根据本发明实施例的活体检测方法、装置、系统及存储介质，通过利用终端的设备信息来调整活体检测策略，保证真实活体以更小成本通过检测，同时让假活体、恶意活体难以通过检测。由此，大大降低了活体检测的安全风险，提升了用户体验，同时防止了恶意请求对系统资源的占用。

[0030] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0031] 通过结合附图对本发明实施例进行更详细的描述，本发明的上述以及其它目的、特征和优势将变得更加明显。附图用来提供对本发明实施例的进一步理解，并且构成说明书的一部分，与本发明实施例一起用于解释本发明，并不构成对本发明的限制。在附图中，相同的参考标号通常代表相同部件或步骤。

[0032] 图1示出了用于实现根据本发明实施例的活体检测方法和装置的示例电子设备的示意性框图；

[0033] 图2示出了根据本发明一个实施例的活体检测方法的示意性流程图；

[0034] 图3示出了根据本发明另一个实施例的活体检测方法的示意性流程图；

[0035] 图4示出了根据本发明一个实施例的用于活体检测的装置的示意性框图；以及

[0036] 图5示出了根据本发明一个实施例的用于活体检测的系统的示意性框图。

具体实施方式

[0037] 为了使得本发明的目的、技术方案和优点更为明显，下面将参照附图详细描述根据本发明的示例实施例。显然，所描述的实施例仅仅是本发明的一部分实施例，而不是本发明的全部实施例，应理解，本发明不受这里描述的示例实施例的限制。基于本发明中描述的本发明实施例，本领域技术人员在没有付出创造性劳动的情况下所得到的所有其它实施例都应落入本发明的保护范围之内。

[0038] 首先，参照图1来描述用于实现根据本发明实施例的活体检测方法和装置的示例电子设备100。

[0039] 如图1所示，电子设备100包括一个或多个处理器102、一个或多个存储装置104。可选地，电子设备100还可以包括输入装置106、输出装置108和数据获取装置110，这些组件通过总线系统112和/或其它形式的连接机构(未示出)互连。应当注意，图1所示的电子设备100的组件和结构只是示例性的，而非限制性的，根据需要，所述电子设备也可以具有其他组件和结构。

[0040] 所述处理器102可以是中央处理单元(CPU)、图形处理器(GPU)或者具有数据处理能力和/或指令执行能力的其它形式的处理单元，并且可以控制所述电子设备100中的其它组件以执行期望的功能。

[0041] 所述存储装置104可以包括一个或多个计算机程序产品，所述计算机程序产品可以包括各种形式的计算机可读存储介质，例如易失性存储器和/或非易失性存储器。所述易失性存储器例如可以包括随机存取存储器(RAM)和/或高速缓冲存储器(cache)等。所述非易失性存储器例如可以包括只读存储器(ROM)、硬盘、闪存等。在所述计算机可读存储介质上可以存储一个或多个计算机程序指令，处理器102可以运行所述程序指令，以实现下文所述的本发明实施例中(由处理器实现)的客户端功能以及/或者其它期望的功能。在所述计算机可读存储介质中还可以存储各种应用程序和各种数据，例如所述应用程序使用和/或产生的各种数据等。

[0042] 所述输入装置106可以是用户用来输入指令的装置，并且可以包括键盘、鼠标、麦克风和触摸屏等中的一个或多个。

[0043] 所述输出装置108可以向外部(例如用户)输出各种信息(例如图像和/或声音)，并且可以包括显示器、扬声器等中的一个或多个。

[0044] 所述数据获取装置110可以采集图像等各种形式的数据，并且将所采集的数据存储在所述存储装置104中以供其它组件使用。数据获取装置110可以是摄像头等。应当理解，数据获取装置110仅是示例，电子设备100可以不包括数据获取装置110。在这种情况下，可以利用其他数据获取装置获取数据，并将所获取的数据发送给电子设备100。

[0045] 示例性地，用于实现根据本发明实施例的活体检测方法和装置的示例电子设备可以在诸如手机、平板电脑、定制终端、个人计算机或远程服务器等的设备上实现。

[0046] 图2示出了根据本发明一个实施例的活体检测方法200的示意性流程图。如图2所示，方法200包括如下步骤：

[0047] 步骤S210，获取终端的设备信息，所述终端用于获取待检测对象的图像。

[0048] 待检测对象可以通过终端发起活体检测请求。该终端可以是手机、平板电脑、定制终端等终端设备，也可能是通过软件模拟出来的各种终端。所述设备信息是关于设备的信

息，例如可以是用于唯一标识出该终端的设备标识、用于检测出该终端为真实设备的特征参数等。

[0049] 在一个示例中，活体检测SDK(Software Development Kit，简称SDK)在终端上进行初始化，其中活体检测SDK为针对活体检测功能的软件开发工具包。可以在活体检测SDK初始化的过程中采集该终端的设备信息。

[0050] 在另一个示例中，活体检测APP安装在终端上，可以在活体检测APP启动的过程中采集该终端的设备信息。

[0051] 上述终端还用于获取待检测对象的图像。例如，可以通过摄像头等装置获取待检测对象的照片和/或视频图像，以用于活体检测。

[0052] 步骤S220，利用步骤S210获取的终端的设备信息确定该终端的设备风险等级。

[0053] 获取到终端的设备信息后，基于设备信息对该终端进行设备风险等级评估判断。如设备信息具有高危风险标识特征，判断该终端的设备风险等级为高危风险；如设备信息具有一般风险标识特征，判断该终端的设备风险等级为有风险；否则该终端为正常设备。在一个实施例中，待检测对象在终端(例如手机、平板电脑、定制终端或虚拟机等终端设备)发起活体检测请求，服务端(例如远程计算机或云端服务器)接收该终端的设备信息，根据该终端的设备信息确定该终端的设备风险等级。在另一个实施例中，待检测对象在终端发起活体检测请求，，终端根据采集到的本终端的设备信息确定本终端的设备风险等级。

[0054] 通过对终端的设备风险等级进行分级评估，可以对来自不同风险等级的终端的活体检测请求进行针对性的处理，以提高系统效率和用户体验。

[0055] 步骤S230，基于步骤S220确定的终端的设备风险等级确定活体检测策略。

[0056] 基于发出活体检测请求的终端的设备风险等级，可以评估当前活体检测请求属于恶意攻击请求的风险等级。由此，可以针对不同设备风险等级确定活体检测策略。例如直接拒绝恶意请求、对可疑的恶意请求随机提高活体检测操作的门槛以及对正常请求随机降低活体检测操作的门槛等。

[0057] 直接拒绝恶意请求可以屏蔽高危风险，同时避免对系统资源的占用。提高活体检测操作的门槛对于可能的恶意请求提升了通过检测的难度。同时随机的活体检测操作要求降低了活体检测操作的可预测性，从而进一步加强了恶意请求通过检测的难度。而对正常请求随机降低活体检测操作的门槛提高了正常请求的通过效率，同时提升了用户体验。

[0058] 通过利用发出活体检测请求的终端的设备信息，调整活体检测策略，保证了真实活体以更小成本通过，同时让假活体、恶意活体难以通过。从而保证了活体检测的准确率。由此，大大降低了活体检测的安全风险，同时防止了恶意请求对系统资源的占用。

[0059] 图3示出了根据本发明另一个实施例的活体检测方法300的示意性流程图。如图3所示，方法300中的步骤S310与方法200中的步骤S210实现的功能、处理方法和过程都类似，在此不再赘述。方法300中的步骤S320、步骤S341、步骤S342、步骤S361以及步骤S362是方法200中的步骤S220的更为具体的实施方式。方法300中的步骤S330以及步骤S351至步骤S355是方法200中的步骤S230的更为具体的实施方式。

[0060] 步骤S320，利用步骤S310获取的终端的设备信息确定该终端是否是虚拟机。虚拟机为通过软件模拟的终端，如虚拟手机终端。虚拟机的设备风险等级为高危风险，是恶意的攻击请求惯用的手段。通过黑客软件等截获真实使用过程中的用户数据，如用户照片、用户

账户数据等。再利用虚拟机使用截获的用户数据伪装成真实用户发出活体检测请求。通过虚拟机发出恶意请求的用户不是真实存在的活体，也称为假活体。

[0061] 示例性地，用于判断终端是否是虚拟机的设备信息可以包括该终端的设备指纹。如同人的指纹具有唯一性从而可以作为人的身份标识，真实的硬件终端也具有可以用于唯一标识出该终端的设备标识，称为该终端的设备指纹。终端的设备指纹例如可以是终端的硬件编号如CPU硬件串码，还可以是国际移动设备识别码(International Mobile Equipment Identity，简称IMEI)以及媒体访问控制地址(Medium Access Control address，简称MAC地址)等设备标识。如果发出请求的终端是真实用户的终端，则该终端的设备指纹将是确定的唯一特定值。而如果发出请求的终端是通过软件模拟的虚拟机，则获取到的终端的设备指纹如IMEI等信息通常为0值。因此，通过判断终端的设备指纹是否为唯一特定值可以检测出该终端是否是虚拟机。

[0062] 示例性地，用于判断终端是否是虚拟机的设备信息还可以包括该终端的设备电量信息。对于一个正常的终端设备，其使用过程中，电量信息是不断变化的。而通过软件模拟的虚拟机的电量将保持不变。因此，通过判断终端的设备电量信息是否一直保持不变可以检测出该终端是否是虚拟机。

[0063] 示例性地，用于判断终端是否是虚拟机的设备信息还可以包括该终端的设备传感器信息。常用的终端，例如手机，往往内置了多个设备传感器。例如陀螺仪传感器、重力传感器、加速度传感器以及磁场传感器等。随着手机的位移，设备传感器信息也随着发生变化。如陀螺仪传感器可以追踪多个方向的位移变化，重力传感器可以追踪重力变化，加速度传感器可以测量手机运动的速度，磁场传感器可以检测磁场强度和方向变化等。而通过软件模拟的虚拟机的设备传感器信息将保持不变。因此，通过判断终端的设备传感器信息是否一直保持不变可以检测出该终端是否是虚拟机。

[0064] 利用终端的上述各种设备信息，可以检测出该终端是否是虚拟机这类设备风险等级为高危风险的设备，从而排除利用虚拟机手段发出的恶意攻击请求。

[0065] 步骤S330，对于经步骤S320确定终端的设备风险等级为高危风险的情况，确定针对该终端的活体检测策略为拒绝策略。例如认为使用虚拟机发出请求的是非活体，直接拒绝该终端的恶意请求。由此，摒除了安全风险，同时有效防止恶意请求对系统资源的占用。

[0066] 方法300还包括步骤S341和步骤S342，终端的设备信息包括该终端的设备指纹，利用终端的设备指纹以及设备指纹黑名单库确定该终端的设备风险等级。

[0067] 在活体识别的各种应用中，如网络身份识别、网络支付认证、安全门禁系统等，各种可疑的行为都会降低终端的信用。根据信用记录情况将发起操作的终端的设备指纹分别加入各级黑名单库。在本实施例中，根据风险程度把设备指纹黑名单库分为两个等级：设备指纹高危黑名单库和设备指纹风险黑名单库。其中，设备指纹高危黑名单库可以包括公安部发布的黑名单、全球共享黑名单，还可以包括实际应用中发起过恶意攻击行为的设备指纹黑名单。设备指纹风险黑名单库可以包括实际应用中发起过可疑攻击行为的设备指纹黑名单。

[0068] 步骤S341，对于终端的设备指纹属于设备指纹高危黑名单库的情况，确定该终端的设备风险等级为高危风险。该终端可能曾经发起过恶意攻击行为，或已被公安部或公众明确列入高危风险黑名单。也即，使用该终端发出请求的可能是有恶意攻击动机的坏人。继

续执行步骤S330，确定针对该终端的活体检测策略为拒绝策略。例如，直接拒绝该终端的请求。由此，摒除安全风险，同时有效防止恶意请求对系统资源的占用。

[0069] 步骤S342，对于终端的设备指纹属于设备指纹风险黑名单库的情况，确定该终端的设备风险等级为有风险。该终端可能发起过可疑攻击行为或发生过其他影响信用的行为。

[0070] 方法300还包括步骤S351。对于终端的设备风险等级为有风险的情况，为了降低安全风险，继续执行步骤S351，确定针对该终端的活体检测策略为随机增加要求用户执行的动作数量和/或提升要求用户执行的动作难度。例如，正常要求用户眨眼2次，可以增加为要求用户眨眼4次。正常只要求眨眼或张嘴动作，可以提升动作难度为右手摸鼻子等。还可以随机组合要求用户执行的动作数量和动作难度，例如要求用户眨眼4次并且张嘴3次，或要求用户眨眼3次并且右手摸鼻子两次，或要求用户张嘴2次并且左手摸鼻子3次等。

[0071] 示例性地，方法300还包括步骤S353、步骤S354以及步骤S355，利用终端采集的待检测对象的图像确定活体检测结果。

[0072] 步骤S353，发送包括上述要求待检测对象执行的动作的信息的指令给对应的终端，以用于指示使用该终端的待检测对象相对应地执行上述要求待检测对象执行的动作。如发送指令如下：请眨眼—>请张嘴—>请眨眼—>请张嘴—>请张嘴。待检测对象根据上述指令执行相应的动作。

[0073] 步骤S354，获取该终端采集的包括该待检测对象执行的动作的视频图像。

[0074] 步骤S355，根据获取到的视频图像确定活体检测结果。例如，如果该视频图像中待检测对象执行的动作与要求待检测对象执行的动作匹配，则该待检测对象的活体检测结果为通过检测，否则为不通过检测。在一个示例中，待检测对象在终端发起活体检测请求，服务端发送上述指令给对应的终端，以指示待检测对象执行活体检测操作，该终端采集包括该待检测对象执行的动作的视频图像发送给该服务端。该服务端根据获取的视频图像确定活体检测结果。

[0075] 在另一个实施例中，待检测对象在终端发起活体检测请求，终端直接发出上述指令指示待检测对象执行活体检测操作，并根据采集到的视频图像确定活体检测结果。

[0076] 通过增加要求待检测对象执行的动作数量和/或提升要求待检测对象执行的动作难度，对于可能的恶意请求提升了通过检测的难度。同时随机的活体检测操作要求降低了活体检测操作的可预测性，进一步加强了恶意请求通过检测的难度。从而对于终端的设备风险等级为有风险的情况，提升了活体检测操作的门槛，降低了活体检测的安全风险。

[0077] 示例性地，方法300还包括步骤S361和步骤S362，终端的设备信息包括关于该终端的异常访问次数的信息，利用该信息确定该终端的设备风险等级。有的恶意攻击会持续不断发出请求，以期通过检测或让被攻击的系统过于忙碌从而无法响应正常的请求甚至系统崩溃。也有想蒙混过关的坏人会多次尝试是否可能通过活体检测。对于新手用户，由于不熟悉如何使用，也可能发起多次重复的请求。上述信息包括特定时间段内频繁发起的请求访问的记录。通过该记录，可以获得同一终端在该特定时间段内频繁发起的异常访问次数。其中，所述特定时间段可以使用默认设置值，例如一天或一个小时，活体检测的管理员也可以修改该设置值。

[0078] 步骤S361，对于终端的异常访问次数大于第一阈值的情况，确定该终端的设备风

险等级为高危风险。从该终端频繁发起的请求很可能是高风险的恶意攻击。继续执行步骤S330，确定针对该终端的活体检测策略为拒绝策略。例如，直接拒绝该终端的请求，由此摒除安全风险，同时有效防止恶意请求对系统资源的占用。其中，第一阈值为高危风险阈值，可以使用默认设置值，例如1000次，活体检测的管理员也可以修改第一阈值。

[0079] 步骤S362，对于终端的异常访问次数不大于第一阈值但大于第二阈值的情况，确定该终端的设备风险等级为有风险。使用该终端的用户可能是想蒙混过关的坏人或不熟悉如何操作的新用户等情况。为了降低安全风险，继续执行步骤S351，确定针对该终端的活体检测策略为随机增加要求待检测对象执行的动作数量和/或提升要求待检测对象执行的动作难度。活体检测操作具体过程如前步骤S353至步骤S355所述，为了简洁，这里不再赘述。其中，第二阈值为一般风险阈值，可以使用默认设置值，例如100次，活体检测的管理员也可以修改第二阈值。

[0080] 方法300还包括步骤S352。对于终端的设备风险等级不是高危风险也不是有风险的情况，也即，该终端为低风险的正常终端。执行步骤S352，确定针对该终端的活体检测策略为随机减少要求待检测对象执行的动作数量和/或降低要求待检测对象执行的动作难度。例如，正常要求待检测对象眨眼2次并且张嘴2次，可以减少为仅眨眼1次或仅张嘴1次，甚至可以不需要执行动作等。通过减少要求待检测对象执行的动作数量和/或降低要求待检测对象执行的动作难度，降低了活体检测操作的门槛，从而提高了正常请求的通过效率，同时提升了用户体验。例如对于有1000个员工的公司使用的刷脸门禁/考勤机。如果要求每个员工眨眼2次并且张嘴2次才能通过活体刷脸验证，每个员工完成上述活体刷脸验证操作的时间为20秒。在上班早高峰期间由于每个员工需要等待活体刷脸验证操作完成方可进入公司，将出现多个员工拥挤在公司门口等待进入公司的情况。根据本发明实施例，正常员工使用的终端经检测为低风险的正常终端，系统随机减少要求待检测对象执行的动作数量和/或降低要求待检测对象执行的动作难度。每个员工进入公司的活体刷脸验证操作为仅需眨眼1次或仅需张嘴1次。对于设备指纹白名单用户，如某员工个人长期稳定使用的同一个手机，甚至不需要执行动作。因而完成活体刷脸验证操作的时间不超过3秒。从而大大提升了正常员工(也即真实活体)通过活体刷脸验证的效率，从公司管理的角度或对员工个人都同时提升了用户体验。另一方面，随机的活体检测操作要求，如上次要求眨眼，下次可能要求张嘴，再下次可能不需要执行动作，也能给正常员工“乏味”的门禁/考勤刷脸操作带来小变化和惊喜，从而进一步提升用户体验。同时随机的活体检测操作要求降低了活体检测操作的可预测性，对于可能的恶意请求增加了通过检测的难度。如盗用员工的手机，使用员工的照片进行刷脸验证，由于不能预期活体检测操作要求的动作，从而不能预先准备好相对应的动作的视频，将很大程度不能通过活体检测，从而降低了安全风险。活体检测操作具体过程如前步骤S353至步骤S355所述，为了简洁，这里不再赘述。

[0081] 上述实施例中的步骤S310至步骤S362给出了一种利用终端的设备信息进行活体检测的方法。本领域技术人员可以理解，上述步骤仅为示例，而非对本发明的限制。如图3所示，先执行虚拟机判断步骤S320，基于终端的设备指纹判断该终端是否是虚拟机。如果不是虚拟机，再执行黑名单检索步骤S341及S342进一步检索该设备指纹是否属于设备指纹高危黑名单库或设备指纹风险黑名单库。如果不属于上述任何一个黑名单库，再执行异常访问判断步骤S361和S362进一步检查该终端是否存在异常访问信息，从而准确判断该终端的设

备风险等级。可选地，上述三种判断方法不必须一一顺序执行。例如，可以跳过虚拟机判断步骤S320，直接执行黑名单检索步骤S341及S342。又例如，执行虚拟机判断步骤S320后，可以不执行黑名单检索步骤S341及S342，直接执行异常访问判断步骤S361和S362。又例如，仅执行异常访问判断步骤S361和S362。可选地，上述三种判断方法可以交换处理顺序。例如，执行虚拟机判断步骤S320后，先执行异常访问判断步骤S361和S362，再执行黑名单检索步骤S341及S342。可选地，上述三种判断方法可以并行执行。根据实际应用场景和系统资源，灵活组合应用上述各种判断方法，取得效果与效率以及成本的综合优选技术方案。

[0082] 在上述实施例中，通过终端发起活体检测请求。本领域普通技术人员可以理解，服务端，例如远程计算机或云端服务器，也可以主动发出活体检测指令给需要进行检测的待检测对象的终端。当终端接收到该活体检测指令后，采集当前终端的设备信息以进行上述活体检测方法的后续步骤。本申请的技术方案对此不做限定。

[0083] 根据本发明另一方面，还提供了一种用于活体检测的装置。图5示出了根据本发明一个实施例的用于活体检测的装置的示意性框图。

[0084] 如图4所示，装置400包括获取模块410、风险模块420和确定模块430。所述各个模块可分别执行上文中所述的用于活体检测的方法的各个步骤/功能。以下仅对该装置400的各部件的主要功能进行描述，而省略以上已经描述过的细节内容。

[0085] 获取模块410用于获取终端的设备信息，所述终端用于获取待检测对象的图像。获取模块410可以由图1所示的电子设备中的处理器102运行存储装置104中存储的程序指令来实现。

[0086] 风险模块420用于利用终端的设备信息确定该终端的设备风险等级。风险模块420可以由图1所示的电子设备中的处理器102运行存储装置104中存储的程序指令来实现。

[0087] 可选地，风险模块420还可以包括虚拟机判断单元。所述虚拟机判断单元根据终端的设备信息确定该终端是否是虚拟机，其中，所述虚拟机的设备风险等级为高危风险。可选地，所述设备信息包括以下一项或多项：设备指纹、设备电量信息以及设备传感器信息。可选地，所述设备传感器包括以下一个或多个：陀螺仪传感器、重力传感器、加速度传感器以及磁场传感器。

[0088] 可选地，所述设备信息包括设备指纹，风险模块420还可以包括黑名单判断单元。所述黑名单判断单元对于终端的设备指纹属于设备指纹高危黑名单库的情况，确定该终端的设备风险等级为高危风险；对于终端的设备指纹属于设备指纹风险黑名单库的情况，确定该终端的设备风险等级为有风险。

[0089] 可选地，所述设备信息包括关于所述终端的异常访问次数的信息，风险模块420还可以包括异常访问判断单元。所述异常访问判断单元对于终端的异常访问次数大于第一阈值的情况，确定该终端的设备风险等级为高危风险；对于终端的异常访问次数不大于第一阈值但大于第二阈值的情况，确定该终端的设备风险等级为有风险。

[0090] 确定模块430用于基于终端的设备风险等级确定活体检测策略。确定模块430可以由图1所示的电子设备中的处理器102运行存储装置104中存储的程序指令来实现。

[0091] 可选地，确定模块430对于所述终端的设备风险等级为高危风险的情况，确定所述活体检测策略为拒绝策略。

[0092] 可选地，确定模块430对于所述终端的设备风险等级为有风险的情况，确定所述活

体检测策略为随机增加要求所述待检测对象执行的动作数量和/或提升要求所述待检测对象执行的动作难度;和/或对于所述终端的设备风险等级不是高危风险也不是有风险的情况,确定所述活体检测策略为随机减少要求所述待检测对象执行的动作数量和/或降低要求所述待检测对象执行的动作难度。

[0093] 本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

[0094] 图5示出了根据本发明一个实施例的用于活体检测的系统500的示意性框图。如图5所示,系统500包括输入装置510、存储装置520、处理器530以及输出装置540。

[0095] 所述输入装置510用于接收用户所输入的操作指令以及采集数据。输入装置510可以包括键盘、鼠标、麦克风、触摸屏和图像采集装置等中的一个或多个。

[0096] 所述存储装置520存储用于实现根据本发明实施例的活体检测方法中的相应步骤的计算机程序指令。

[0097] 所述处理器530用于运行所述存储装置520中存储的计算机程序指令,以执行根据本发明实施例的活体检测方法的相应步骤,并且用于实现根据本发明实施例的用于活体检测的装置中的获取模块410、风险模块420和确定模块430。

[0098] 在一个实施例中,在所述计算机程序指令被所述处理器530运行时使所述系统500执行以下步骤:

[0099] 获取终端的设备信息,所述终端用于获取待检测对象的图像;

[0100] 利用所述终端的设备信息确定所述终端的设备风险等级;

[0101] 基于所述终端的设备风险等级确定活体检测策略。

[0102] 在一个实施例中,在所述计算机程序指令被所述处理器530运行时使所述系统500执行以下步骤:根据所述终端的设备信息确定所述终端是否是虚拟机,其中,所述虚拟机的设备风险等级为高危风险。

[0103] 示例性地,所述设备信息包括以下一项或多项:设备指纹、设备电量信息以及设备传感器信息。

[0104] 示例性地,所述设备传感器包括以下一个或多个:陀螺仪传感器、重力传感器、加速度传感器以及磁场传感器。

[0105] 在一个实施例中,所述设备信息包括设备指纹,在所述计算机程序指令被所述处理器530运行时使所述系统500执行以下步骤:

[0106] 对于所述终端的设备指纹属于设备指纹高危黑名单库的情况,确定所述终端的设备风险等级为高危风险;和/或

[0107] 对于所述终端的设备指纹属于设备指纹风险黑名单库的情况,确定所述终端的设备风险等级为有风险。

[0108] 在一个实施例中,所述设备信息包括关于所述终端的异常访问次数的信息,在所述计算机程序指令被所述处理器530运行时使所述系统500执行以下步骤:

[0109] 对于所述终端的异常访问次数大于第一阈值的情况,确定所述终端的设备风险等

级为高危风险；

[0110] 对于所述终端的异常访问次数不大于第一阈值但大于第二阈值的情况，确定所述终端的设备风险等级为有风险。

[0111] 在一个实施例中，在所述计算机程序指令被所述处理器530运行时使所述系统500执行以下步骤：对于所述终端的设备风险等级为高危风险的情况，确定所述活体检测策略为拒绝策略。

[0112] 在一个实施例中，在所述计算机程序指令被所述处理器530运行时使所述系统500执行以下步骤：

[0113] 对于所述终端的设备风险等级为高危风险的情况，确定所述活体检测策略为随机增加要求待检测对象执行的动作数量和/或提升要求待检测对象执行的动作难度；和/或

[0114] 对于所述终端的设备风险等级不是高危风险也不是有风险的情况，确定所述活体检测策略为随机减少要求待检测对象执行的动作数量和/或降低要求待检测对象执行的动作难度。

[0115] 此外，根据本发明再一方面，还提供了一种存储介质，在所述存储介质上存储了程序指令，在所述程序指令被计算机或处理器运行时使得所述计算机或处理器执行本发明实施例的活体检测方法的相应步骤，并且用于实现根据本发明实施例的用于活体检测的装置中的相应模块。所述存储介质例如可以包括智能电话的存储卡、平板电脑的存储部件、个人计算机的硬盘、只读存储器(ROM)、可擦除可编程只读存储器(EPROM)、便携式紧致盘只读存储器(CD-ROM)、USB存储器、或者上述存储介质的任意组合。所述计算机可读存储介质可以是一个或多个计算机可读存储介质的任意组合。

[0116] 在一个实施例中，所述计算机程序指令被计算机或处理器运行时，使得所述计算机或处理器执行以下步骤：

[0117] 获取终端的设备信息，所述终端用于获取待检测对象的图像；

[0118] 利用所述终端的设备信息确定所述终端的设备风险等级；

[0119] 基于所述终端的设备风险等级确定活体检测策略。

[0120] 在一个实施例中，所述计算机程序指令被计算机或处理器运行时，使得所述计算机或处理器执行以下步骤：根据所述终端的设备信息确定所述终端是否是虚拟机，其中，所述虚拟机的设备风险等级为高危风险。

[0121] 示例性地，所述设备信息包括以下一项或多项：设备指纹、设备电量信息以及设备传感器信息。

[0122] 示例性地，所述设备传感器包括以下一个或多个：陀螺仪传感器、重力传感器、加速度传感器以及磁场传感器。

[0123] 在一个实施例中，所述设备信息包括设备指纹，所述计算机程序指令被计算机或处理器运行时，使得所述计算机或处理器执行以下步骤：

[0124] 对于所述终端的设备指纹属于设备指纹高危黑名单库的情况，确定所述终端的设备风险等级为高危风险；和/或

[0125] 对于所述终端的设备指纹属于设备指纹风险黑名单库的情况，确定所述终端的设备风险等级为有风险。

[0126] 在一个实施例中，所述设备信息包括关于所述终端的异常访问次数的信息，所述

计算机程序指令被计算机或处理器运行时，使得所述计算机或处理器执行以下步骤：

[0127] 对于所述终端的异常访问次数大于第一阈值的情况，确定所述终端的设备风险等级为高危风险；

[0128] 对于所述终端的异常访问次数不大于第一阈值但大于第二阈值的情况，确定所述终端的设备风险等级为有风险。

[0129] 在一个实施例中，所述计算机程序指令被计算机或处理器运行时，使得所述计算机或处理器执行以下步骤：对于所述终端的设备风险等级为高危风险的情况，确定所述活体检测策略为拒绝策略。

[0130] 在一个实施例中，所述计算机程序指令被计算机或处理器运行时，使得所述计算机或处理器执行以下步骤：

[0131] 对于所述终端的设备风险等级为有风险的情况，确定所述活体检测策略为随机增加要求待检测对象执行的动作数量和/或提升要求待检测对象执行的动作难度；

[0132] 对于所述终端的设备风险等级不是高危风险也不是有风险的情况，确定所述活体检测策略为随机减少要求待检测对象执行的动作数量和/或降低要求待检测对象执行的动作难度。

[0133] 根据本发明实施例的活体检测方法、装置、系统及存储介质，通过利用终端的设备信息来进行活体检测，保证真实活体以更小成本通过，同时让假活体、恶意活体难以通过。由此大大降低了活体检测的安全风险，提升了用户体验，同时防止了恶意请求对系统资源的占用。

[0134] 尽管这里已经参考附图描述了示例实施例，应理解上述示例实施例仅仅是示例性的，并且不意图将本发明的范围限制于此。本领域普通技术人员可以在其中进行各种改变和修改，而不偏离本发明的范围和精神。所有这些改变和修改意在被包括在所附权利要求所要求的本发明的范围之内。

[0135] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0136] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。例如，以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个设备，或一些特征可以忽略，或不执行。

[0137] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0138] 类似地，应当理解，为了精简本发明并帮助理解各个发明方面中的一个或多个，在对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该本发明的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如相应的权

利要求书所反映的那样，其发明点在于可以用少于某个公开的单个实施例的所有特征的特征来解决相应的技术问题。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0139] 本领域的技术人员可以理解，除了特征之间相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0140] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0141] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的用于活体检测的装置中的一些模块的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0142] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0143] 以上所述，仅为本发明的具体实施方式或对具体实施方式的说明，本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。本发明的保护范围应以权利要求的保护范围为准。

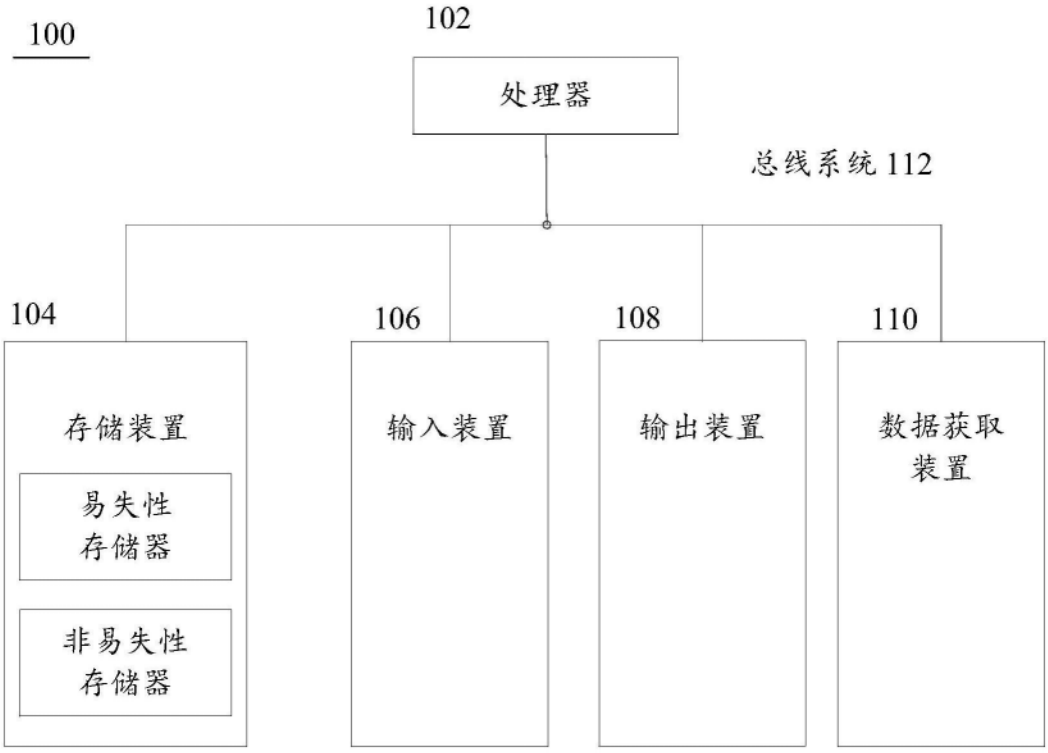

100
102
处理器
总线系统 112
104
106
108
110
存储装置
易失性存储器
非易失性存储器
输入装置
输出装置
数据获取装置

图1

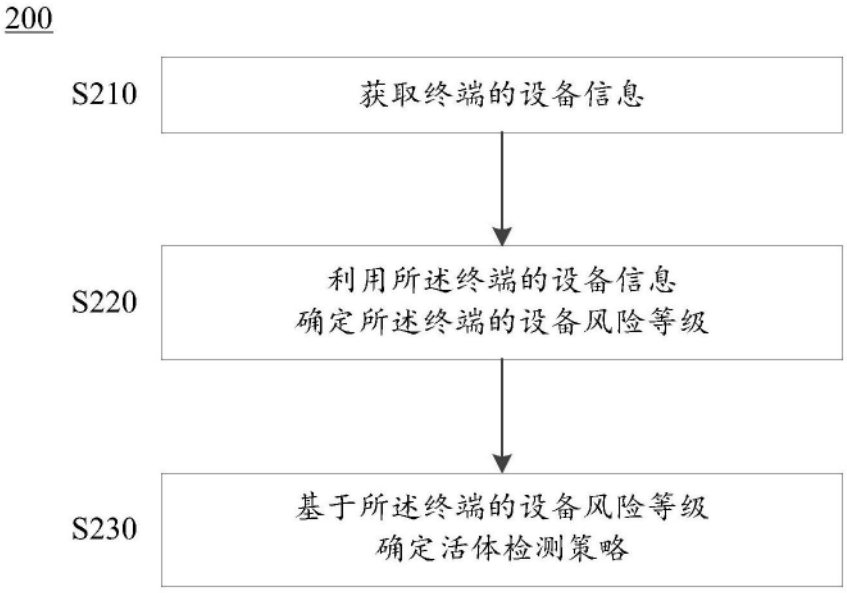

200
S210
获取终端的设备信息
S220
利用所述终端的设备信息
确定所述终端的设备风险等级
S230
基于所述终端的设备风险等级
确定活体检测策略

图2

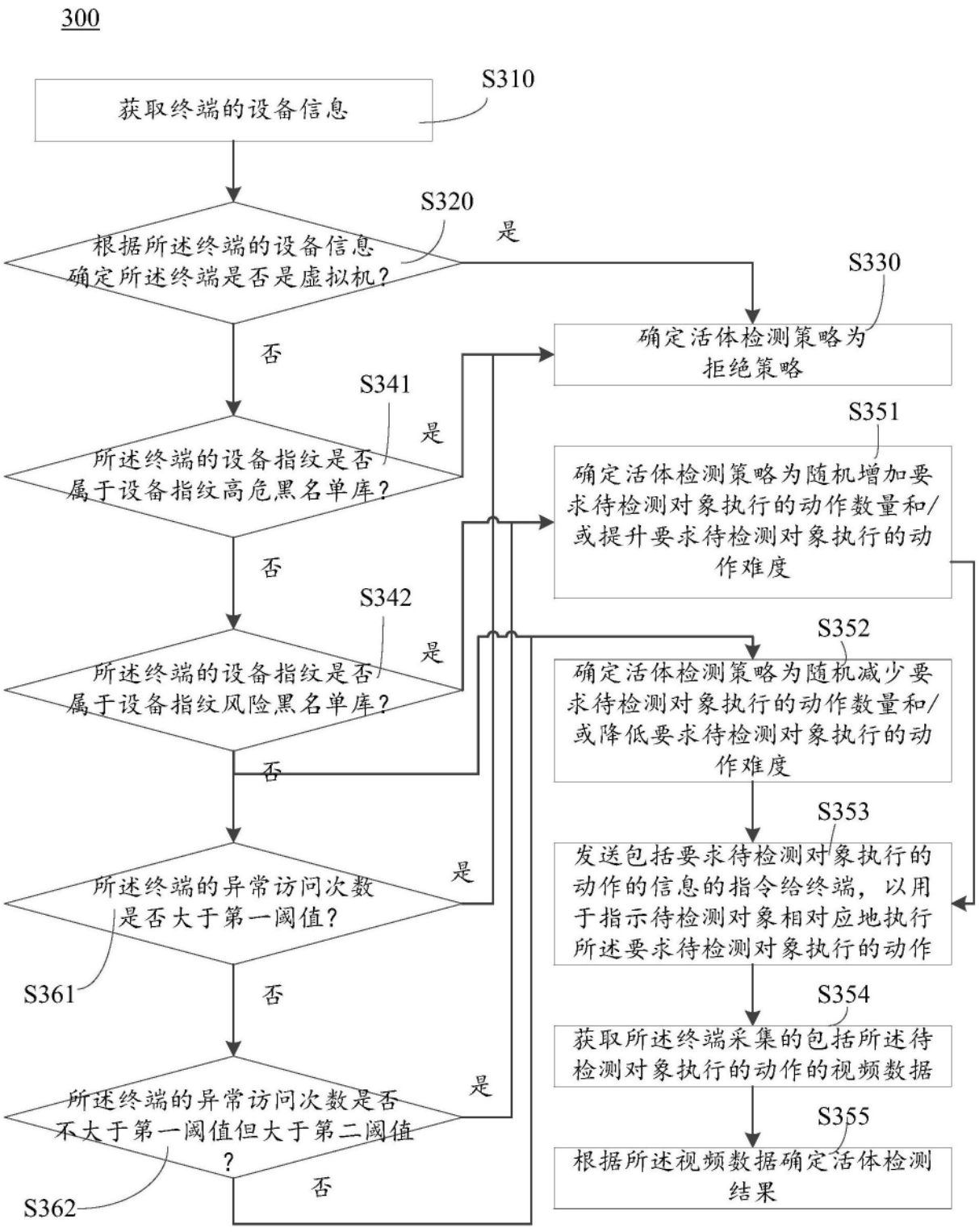

300
S310
获取终端的设备信息
S320
根据所述终端的设备信息确定所述终端是否是虚拟机？
是
S330
确定活体检测策略为拒绝策略
否
S341
所述终端的设备指纹是否属于设备指纹高危黑名单库？
是
S351
确定活体检测策略为随机增加要求待检测对象执行的动作数量和/或提升要求待检测对象执行的动作难度
否
S342
所述终端的设备指纹是否属于设备指纹风险黑名单库？
是
S352
确定活体检测策略为随机减少要求待检测对象执行的动作数量和/或降低要求待检测对象执行的动作难度
否
S353
发送包括要求待检测对象执行的动作的信息的指令给终端，以用于指示待检测对象相对应地执行所述要求待检测对象执行的动作
S361
所述终端的异常访问次数是否大于第一阈值？
是
否
S354
获取所述终端采集的包括所述待检测对象执行的动作的视频数据
S362
所述终端的异常访问次数是否不大于第一阈值但大于第二阈值？
是
否
S355
根据所述视频数据确定活体检测结果

图3

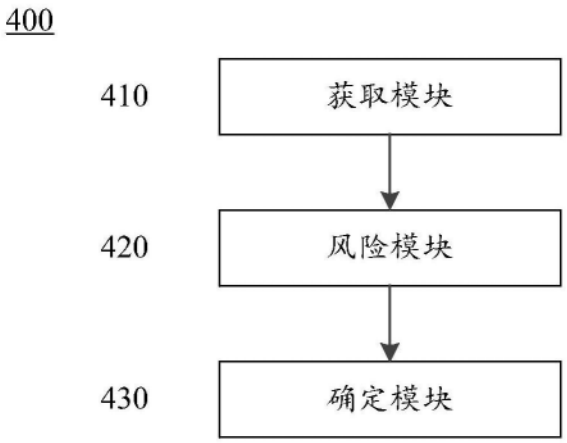

400
410
获取模块
420
风险模块
430
确定模块

图4

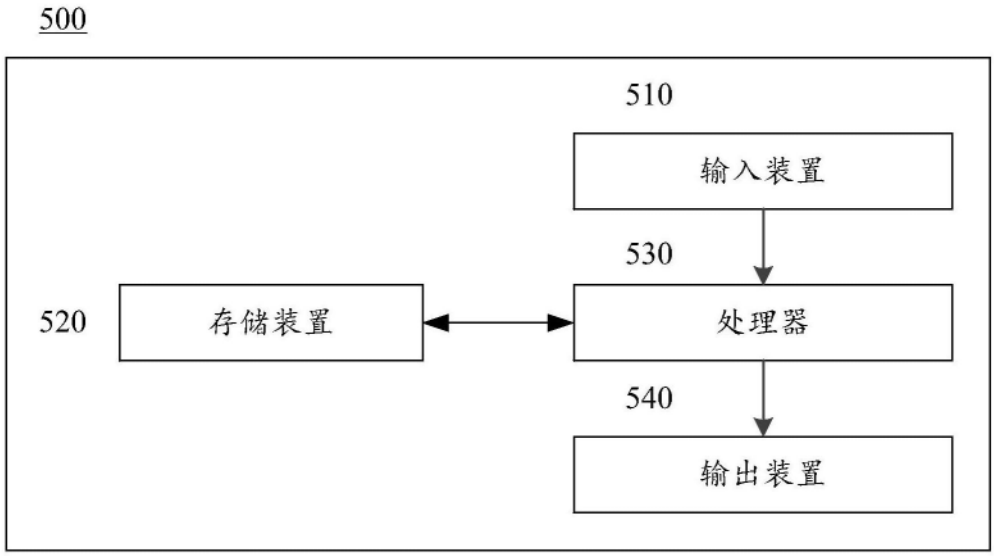

500
510
输入装置
530
520
存储装置
处理器
540
输出装置

图5