(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110276250 B
(45)授权公告日 2023.06.02

(21)申请号 201910392792.4

(22)申请日 2015.01.12

(65)同一申请的已公布的文献号
申请公布号 CN 110276250 A

(43)申请公布日 2019.09.24

(62)分案原申请数据
201510015237.1 2015.01.12

(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心(邮编KY1-9008)

(72)发明人 曾岳伟

(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 周达 李辉

(51)Int.Cl.
G06V 40/16(2022.01)
G06F 21/32(2013.01)
G06V 40/40(2022.01)

(56)对比文件
CN 103440479 A,2013.12.11
CN 103634120 A,2014.03.12
CN 102622588 A,2012.08.01
CN 101999900 A,2011.04.06
US 2009222388 A1,2009.09.03

审查员 李慧

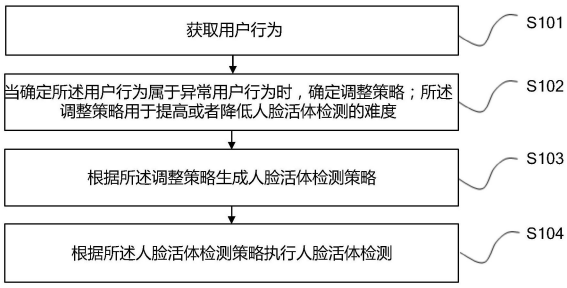
权利要求书2页 说明书11页 附图4页

(54)发明名称

一种人脸活体检测方法和装置

(57)摘要

本发明涉及数据处理领域,特别是涉及一种人脸活体检测方法和装置,所述方法包括:获取第一用户行为和第二用户行为;当确定所述第一用户行为属于正常用户行为且确定所述第二用户行为属于异常用户行为时,获取预置的调整策略;根据所述调整策略在人脸活体检测策略集合中选取目标人脸活体检测策略;其中,所述人脸活体检测策略集合包括多个人脸活体检测策略;根据所述人脸活体检测策略执行人脸活体检测。本发明提供的方法和装置,可以适应不同的业务需求,灵活性强,适应性强,即可以提高系统的安全性,另一方面,也可以提高用户体验的舒适性。



CN 110276250 B

1.一种人脸活体检测方法,包括:

获取第一用户行为和第二用户行为;其中,所述第一用户行为为用户执行第一人脸活体检测策略而形成的行为;所述第二用户行为为用户执行第二人脸活体检测策略而形成的行为;所述第一人脸活体检测策略和所述第二人脸活体检测策略不同;

当确定所述第一用户行为属于正常用户行为且确定所述第二用户行为属于异常用户行为时,获取预置的调整策略;所述调整策略用于提高或者降低人脸活体检测的难度;

根据所述调整策略在人脸活体检测策略集合中选取目标人脸活体检测策略;其中,所述人脸活体检测策略集合包括多个人脸活体检测策略;

根据所述目标人脸活体检测策略执行人脸活体检测。

2.根据权利要求1所述的方法,所述异常用户行为根据以下方式确定:

当确定所述第二用户行为不符合所述第二人脸活体检测策略的通过条件时,确定所述第二用户行为属于异常用户行为;或者,

当未在预设时间内采集到符合所述第二人脸活体检测策略通过条件的第二用户行为时,确定所述第二用户行为属于异常用户行为。

3.根据权利要求1所述的方法,所述第二用户行为为用户历史行为;

所述确定所述第二用户行为属于异常用户行为包括:

根据所述用户历史行为确定所述用户属于高风险用户时,则确定所述第二用户行为属于异常用户行为。

4.根据权利要求1所述的方法,所述第二用户行为为用户在进行人脸活体检测前执行的数据操作;

所述确定所述第二用户行为属于异常用户行为包括:

确定所述数据操作的类型与预设的异常用户行为类型相同时,确定所述第二用户行为属于异常用户行为。

5.根据权利要求1所述的方法,所述确定调整策略包括:

调整人脸活体检测策略集合中各策略的权重,以提高人脸活体检测的难度。

6.根据权利要求1至5任意一项所述的方法,所述人脸活体检测策略包括闭眼、抬头、张口、摇头、微笑策略中的一种或多种。

7.一种人脸活体检测装置,包括:

获取单元,用于获取第一用户行为和第二用户行为;其中,所述第一用户行为为用户执行第一人脸活体检测策略而形成的行为;所述第二用户行为为用户执行第二人脸活体检测策略而形成的行为;所述第一人脸活体检测策略和所述第二人脸活体检测策略不同;

调整单元,用于当确定所述第一用户行为属于正常用户行为且确定所述第二用户行为属于异常用户行为时,获取预置的调整策略;

策略生成单元,用于根据所述调整策略在人脸活体检测策略集合中选取目标人脸活体检测策略;其中,所述人脸活体检测策略集合包括多个人脸活体检测策略;

检测单元,用于根据所述人脸活体检测策略执行人脸活体检测。

8.根据权利要求7所述的装置,所述异常用户行为根据以下方式确定:

当确定所述第二用户行为不符合所述第二人脸活体检测策略的通过条件时,确定所述第二用户行为属于异常用户行为;或者,

当未在预设时间内采集到符合所述第二人脸活体检测策略通过条件的第二用户行为时，确定所述第二用户行为属于异常用户行为。

9.根据权利要求7所述的装置，所述获取单元获取的所述第二用户行为为用户历史行为；

所述调整单元具体用于：

根据所述用户历史行为确定所述用户属于高风险用户时，则确定所述第二用户行为属于异常用户行为。

10.根据权利要求7所述的装置，所述获取单元获取的所述第二用户行为为用户在进行人脸活体检测前执行的数据操作；

所述调整单元具体用于：

确定所述数据操作的类型与预设的异常用户行为类型相同时，确定所述第二用户行为属于异常用户行为。

11.根据权利要求7所述的装置，所述调整单元具体用于：

调整人脸活体检测策略集合中各策略的权重，以提高人脸活体检测的难度。

12.根据权利要求7至11任意一项所述的装置，所述人脸活体检测策略包括闭眼、抬头、张口、摇头、微笑策略中的一种或多种。

一种人脸活体检测方法和装置

[0001] 本申请是申请日为2015年01月12日，申请号为：201510015237.1，名称为“一种人脸活体检测方法和装置”的专利申请的分案申请。

技术领域

[0002] 本发明涉及数据处理技术领域，特别是涉及一种人脸活体检测方法和装置。

背景技术

[0003] 人脸识别技术作为一种有效的身份认证与识别技术，由于其具有方便易用、用户友好性、非接触式等特点，目前得到了广泛的应用。然而，人脸识别系统也容易受到一些非法用户的攻击，如何提高人脸识别系统的安全性成为一个广泛关注的问题。

[0004] 对人脸识别系统的攻击，主要有3类：照片攻击、视频攻击和3D模型攻击。非法分子或者假冒用户在获得合法用户的照片或视频后，使用合法用户的照片或视频作为伪造的人脸试图欺骗系统。为了区分真实人脸以及照片、视频，出现了人脸活体检测技术。这种技术通过系统与用户的交互，利用生成的动作策略让用户做出一些动作，再利用计算机视觉技术判断用户动作是否正确，从而确定采集的是人脸活体，而不是伪造的照片、视频或者3D模型。这种技术从一定程度上提高了人脸识别系统的安全性，但由于人脸活体检测时采用的各种动作策略是固定的，并不能够根据具体的应用场景进行调整，存在灵活度不强，不能满足各种应用场景需求的缺陷。在某些应用场景下，甚至会导致安全性降低，使得系统遭受攻击的风险增大。

发明内容

[0005] 为解决上述技术问题，本发明公开了一种人脸活体检测方法和装置，可以根据不同的应用场景调整人脸活体检测策略以提高或者降低人脸活体检测的难度，灵活性强，适应性强。

[0006] 技术方案如下：

[0007] 根据本发明实施例的第一方面，公开了一种人脸活体检测方法，所述方法包括：

[0008] 获取第一用户行为和第二用户行为；其中，所述第一用户行为为用户执行第一人脸活体检测策略而形成的行为；所述第二用户行为为用户执行第二人脸活体检测策略而形成的行为；所述第一人脸活体检测策略和所述第二人脸活体检测策略不同；

[0009] 当确定所述第一用户行为属于正常用户行为且确定所述第二用户行为属于异常用户行为时，获取预置的调整策略；所述调整策略用于提高或者降低人脸活体检测的难度；

[0010] 根据所述调整策略在人脸活体检测策略集合中选取目标人脸活体检测策略；其中，所述人脸活体检测策略集合包括多个人脸活体检测策略；

[0011] 根据所述人脸活体检测策略执行人脸活体检测。

[0012] 根据本发明实施例的第二方面，公开了一种人脸活体检测装置，所述装置包括：

[0013] 获取单元，用于获取第一用户行为和第二用户行为；其中，所述第一用户行为为用

户执行第一人脸活体检测策略而形成的行为;所述第二用户行为为用户执行第二人脸活体检测策略而形成的行为;所述第一人脸活体检测策略和所述第二人脸活体检测策略不同;

[0014] 调整单元,用于当确定所述第一用户行为属于正常用户行为且确定所述第二用户行为属于异常用户行为时,获取预置的调整策略;所述调整策略用于提高或者降低人脸活体检测的难度;

[0015] 策略生成单元,用于根据所述调整策略在人脸活体检测策略集合中选取目标人脸活体检测策略;其中,所述人脸活体检测策略集合包括多个人脸活体检测策略;

[0016] 检测单元,用于根据所述人脸活体检测策略执行人脸活体检测。

[0017] 本发明实施例的一个方面能够达到的有益效果为:本发明提供的人脸活体检测方法和装置,当确定获取的第一用户行为属于正常用户行为且第二用户行为属于异常用户行为时,可以实时、灵活地调整第一用户行为和第二用户行为所对应的人脸活体检测策略以提高或者降低人脸活体检测的难度,从而适应不同应用场景的需要。例如,在对安全性要求高的应用场景,可以通过提高人脸活体检测的难度,提高系统的安全性;而在对安全性要求不高而用户体验要求高的应用场景,可以通过降低人脸活体检测的难度,给用户较佳的体验。本发明提供的方法和装置,可以适应不同的业务需求,灵活性强,适应性强,即可以提高系统的安全性,另一方面,也可以提高用户体验的舒适性。

附图说明

[0018] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明中记载的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0019] 图1为本发明实施例提供的一种人脸活体检测方法流程示意图;

[0020] 图2为本发明实施例提供的另一种人脸活体检测方法流程示意图;

[0021] 图3为本发明实施例提供的再一种人脸活体检测方法流程示意图;

[0022] 图4为本发明实施例提供的又一种人脸体检测方法流程示意图;

[0023] 图5为本发明实施例提供的人脸活体检测装置示意图。

具体实施方式

[0024] 本发明公开了一种人脸活体检测方法和装置,可以根据不同的应用场景调整人脸活体检测策略以提高或者降低人脸活体检测的难度,灵活性强,适应性强。

[0025] 为了使本技术领域的人员更好地理解本发明中的技术方案,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都应当属于本发明保护的范围。

[0026] 参见图1,为本发明实施例提供的一种人脸活体检测方法流程示意图,所示方法可以包括以下步骤:

[0027] S101,获取用户行为。

[0028] 在一种可能的实现方式中，所述用户行为为用户执行第一人脸活体检测策略而形成的行为。用户在执行人脸活体检测前，系统会随机生成人脸活体检测策略，用户根据系统的提示信息，执行相应的人脸活体检测策略，做出与所述人脸活体检测策略对应的动作或行为，系统通过摄像头采集图像，所述图像可以为一系列的视频帧。例如，用户可以随机生成第一人脸活体检测策略，所述人脸活体检测策略为微笑策略，用户根据系统的提示信息，执行微笑动作，这时系统采集用户行为，获得与用户行为对应的一系列视频帧。系统随机生成的人脸活体检测策略可以包括一种或多种策略，系统获取的用户行为至少包括第一用户行为，所述第一用户行为与第一人脸活体检测策略相对应，具体为用户执行第一人脸活体检测策略而形成的行为。相应地，获取用户行为还可以包括获取第一用户行为和第二用户行为，其中，所述第一用户行为为用户执行第一人脸活体检测策略而形成的行为；所述第二用户行为为用户执行第二人脸活体检测策略而形成的行为；所述第一人脸活体检测策略和所述第二人脸活体检测策略不同。

[0029] 在另外一种可能的实现方式中，系统获取的用户行为为用户历史行为，包括但不限于用户的历史人脸活体检测行为或者其他操作行为。例如，所述用户历史行为可以是用户历史的人脸活体检测行为，例如用户历史上是否有异常的检测记录等，用于评估用户的风险级别是高风险用户还是低风险用户，从而确定如何调整策略以提高或者降低人脸活体检测的难度。其他操作行为可以是用户的历史登陆行为，修改密码行为、交易失败行为、更换绑定手机、解除绑定手机等行为，在此不限定。

[0030] 在另外一种可能的实现方式中，系统获取的用户行为为用户在进行人脸活体检测前执行的数据操作。例如，在一些典型的应用场景下，在用户进行人脸活体检测前，通常会执行登录用户账号的操作或者其他数据操作。

[0031] S102，当确定所述用户行为属于异常用户行为时，确定调整策略；所述调整策略用于提高或者降低人脸活体检测的难度。

[0032] 当用户行为为用户在执行人脸活体检测策略而形成的行为时，所述确定用户行为属于异常用户行为包括：当确定所述用户行为不符合所述第一人脸活体检测策略的通过条件时，确定所述用户行为属于异常用户行为；或者，

[0033] 当未在预设时间内采集到符合所述第一人脸活体检测策略通过条件的用户行为时，确定所述用户行为属于异常用户行为。具体地，可以预先设置人脸活体检测策略的通过条件，当确定获取的用户行为不符合所述人脸活体检测策略的通过条件时，则确定用户的行为属于异常用户行为。此外，还可以预先设置时间条件，例如30S，当系统未在预定时间内例如30S采集到所述第一人脸活体检测策略通过条件的用户行为时，确定所述用户行为属于异常用户行为。这时，当用户因为执行某一人脸活体检测策略而检测不通过超过预设的时间时，则表明有可能系统遭受到了图片或者视频的攻击。这时，就将检测到异常用户行为作为触发调整策略的条件。所述调整策略用于提高或者降低人脸活体检测的难度。

[0034] 在另外一种可能的实现方式中，当获取的所述用户行为为用户历史行为时，所述确定所述用户行为属于异常用户行为包括：根据所述用户历史行为确定所述用户属于高风险用户时，则确定所述用户行为属于异常用户行为。例如，当用户多次登录失败或者在人脸活体检测中不通过或者超时时，确定用户属于高风险用户。

[0035] 在另外一种可能的实现方式中，当获取的所述用户行为所述用户行为为用户在进

行人脸活体检测前执行的数据操作时，所述确定用户行为属于异常用户行为包括：确定所述数据操作的类型与预设的异常用户行为类型相同时，确定所述用户行为属于异常用户行为。所述预设的异常用户行为类型包括：登录失败、修改密码、校验操作、解除绑定手机、更好绑定手机、删除记录等、使用设备异地登录或者使用不同的设备登录等，本发明对此不进行限定。当判断用户在进行人脸活体检测前执行的数据操作与预设的异常用户行为类型相同时，则确定用户具有较高的安全风险，确定用户行为属于异常用户行为。

[0036] 当确定用户行为属于异常用户行为时，确定调整策略具有不同的实现方式。在一种可能的实现方式中，本发明具体实施时，是根据系统预先设置的调整策略确定是提高或者降低人脸活体检测的难度的。具体地，所述预置的调整策略，所述预置的调整策略包括第一策略和第二策略中的至少一者；当所述预置的调整策略为所述第一策略时，提高所述第一人脸活体检测策略的权重；当所述预置的调整策略为所述第二策略时，降低所述第一人脸活体检测策略的权重；其中，所述权重用于表示所述第一人脸活体检测策略在人脸活体检测策略集合中出现的概率。

[0037] 例如，当在安全性要求较高的场合，可以设置预置的调整策略为第一策略，当确定用户行为属于异常用户行为时，可以提高对应异常用户行为的人脸活体检测策略的权重，以增加所述人脸活体检测策略在人脸活体检测策略集合中出现的概率，使得所述策略在后续重新生成人脸活体检测策略时具有较高的出现概率，从而提高人脸活体检测的难度，进而提高人脸活体检测的安全性。

[0038] 当在安全性要求不高但用户体验要求较高的场合，可以设置预置的调整策略为第二策略，当确定用户行为属于异常用户行为时，可以降低对应异常用户行为的人脸活体检测策略的权重，以降低所述人脸活体检测策略在人脸活体检测策略集合中出现的概率，使得所述策略在后续重新生成人脸活体检测策略时具有较低的出现概率，从而降低人脸活体检测的难度，使得用户较容易通过，提高用户的体验。

[0039] 进一步地，当获取的用户行为包括第一用户行为和第二用户行为，且所述第一用户行为和第二用户行为对应不同的人脸活体检测策略时，当确定第一用户行为和第二用户行为其中一者为正常用户行为，另一者为异常用户行为时，则确定调整策略具体为：当预置的调整策略为所述第一策略时，降低对应正常用户行为的人脸活体检测策略的权重，提高对应异常人脸活体检测策略的权重。当所述预置的调整策略为所述第二策略时，提高对应正常用户行为的人脸活体检测策略的权重，降低对应异常人脸活体检测策略的权重。

[0040] 例如，当所述第一用户行为为用户执行第一人脸活体检测策略而形成的行为，所述第二用户行为为用户执行第二人脸活体检测策略而形成的行为，当确定所述第一用户行为属于正常用户行为且确定所述第二用户行为属于异常用户行为时，获取预置的调整策略。当在安全性要求较高的场合，可以设置预置的调整策略为第一策略，降低所述第一人脸活体检测策略的权重，提高所述第二人脸活体检测策略的权重，这样，可以增加对应异常用户行为的第二人脸活体检测策略在人脸活体检测策略集合中出现的概率，使得所述策略在后续重新生成人脸活体检测策略时具有较高的出现概率，从而提高人脸活体检测的难度，进而提高人脸活体检测的安全性。同时，降低对应正常用户行为的第一人脸活体检测策略在人脸活体检测策略集合中出现的概率，使得所述策略在后续重新生成人脸活体检测策略时具有较低的出现概率，从而提高人脸活体检测的难度，进而提高人脸活体检测的安全性。

当在安全性要求不高但用户体验要求较高的场合，可以设置预置的调整策略为第二策略，提高所述第一人脸活体检测策略的权重，降低所述第二人脸活体检测策略的权重，这样，可以增加对应正常用户行为的第一人脸活体检测策略在人脸活体检测策略集合中出现的概率，使得所述策略在后续重新生成人脸活体检测策略时具有较高的出现概率，从而降低人脸活体检测的难度，进而使得用户较容易通过，提高用户的体验。同时，降低对应异常用户行为的第二人脸活体检测策略在人脸活体检测策略集合中出现的概率，使得所述策略在后续重新生成人脸活体检测策略时具有较低的出现概率，从而降低人脸活体检测的难度，进而使得用户较容易通过，提高用户的体验。

[0041] 在另外一种可能的实现方式中，当用户行为为执行相应的人脸活体检测策略而形成的行为时，确定调整策略的依据可以不是依据预置的调整策略，而是引入其他判断条件。例如，确定调整策略包括下述中的至少一者：

[0042] 获取用户历史行为数据，当根据所述用户历史行为数据确定所述用户属于高风险用户时，提高对应所述异常用户行为的人脸活体检测策略的权重；

[0043] 获取用户历史行为数据，当根据所述用户历史行为数据确定所述用户属于低风险用户时，降低对应所述异常用户行为的人脸活体检测策略的权重；

[0044] 获取用户在进行人脸活体检测前的数据操作，当确定所述数据操作的类型与预设的异常用户行为类型相同时，提高对应所述异常用户行为的人脸活体检测策略的权重。

[0045] 需要说明的是，在另外一种可能的实现方式中，当根据所述用户历史行为确定所述用户属于高风险用户或者根据用户在进行人脸活体检测前执行的数据操作的类型与预设的异常用户行为类型相同来确定所述用户行为属于异常用户行为时，所述确定调整策略包括：调整人脸活体检测策略集合中各策略的权重，以提高人脸活体检测的难度。

[0046] S103，根据所述调整策略生成人脸活体检测策略。

[0047] 根据所述调整策略随机生成一个或者多个人脸活体检测策略用于进行人脸活体检测。其中，所述人脸活体检测策略为人脸活体检测策略集合中选取的策略。所述人脸活体检测策略集合包括一个或多个人脸活体检测策略。

[0048] S104，根据所述人脸活体检测策略执行人脸活体检测。

[0049] 在本发明具体实现时，在确定人脸活体检测策略后，执行人脸活体检测的实现可以与现有技术相同，在此不详细叙述。

[0050] 参见图2，为本发明实施例提供的另一种人脸活体检测方法流程示意图。

[0051] 在图2所示的方法中，以随机生成两种人脸活体检测策略、调整策略为根据预置的调整策略而确定为例进行说明。当然，上述方法也可以适用于随机生成3种、4种或多种人脸活体检测策略的情形。本领域技术人员在不付出创造性劳动下获得的其他方式，均属于本发明的保护范围。

[0052] S201，开始人脸活体检测。

[0053] S202，检测设备物理条件是否符合预置条件，如果符合，进入S203；如果不符合，提示用户退出，更换设备。

[0054] 所述预置条件可以包括设备是否具有摄像头、摄像头的像素是否大于设定阈值、设备的环境条件是否满足条件，设备的环境条件可以包括光线强度是否大于设定阈值等。

[0055] S203，随机生成两种人脸活体检测策略。

[0056] 所述人脸活体检测策略可以包括闭眼、抬头、张口、摇头、微笑策略中的一种或多种。闭眼又可以包括闭双眼、闭右眼、闭左眼等。摇头可以包括向右摇头，向左摇头等。具体的人脸活体检测策略可以根据需要设置。在本发明具体实现时，随机生成两种人脸活体检测策略是根据各人脸活体检测策略在人脸活体检测集合中的权重而确定的，所述权重用于表示对应的人脸活体检测策略在人脸活体检测策略集合中出现的概率。权重越高，其出现概率越高，在生成人脸活体检测策略时，被选中的概率也越高。

[0057] 具体地，以默认的人脸活体检测策略包括5种策略为例，系统初始化时，5种策略的权重是一致的，例如均可以设置为20，在随机生成人脸活体检测策略时，5种策略被选中的概率比为1:1:1:1:1。每一种策略可以对应相应的数值范围，例如策略1对应的数值范围为

[0058] [0,20)，策略2对应的数值范围为[20,40)，策略3对应的数值范围为[40,60)，策略4对应的数值范围为[60,80)例如策略5对应的数值范围为[80,100)。在随机生成人脸活体检测策略时，可以随机生成整数，所述整数的取值范围为[0,100)。例如，随机生成的整数为15时，则对应的人脸活体检测策略为策略1;，随机生成的整数为60时，则对应的人脸活体检测策略为策略4。

[0059] 当确定调整策略后，人脸活体检测策略集合中各人脸活体检测策略的权重也相应发生变化，在生成随机整数时的数值取值范围也会发生变化。这时，在调整后的数值范围内随机生成整数，并确定对应的人脸活体检测策略。例如，假设调整后的取值范围为:策略1对应的数值范围为[0,20)，策略2对应的数值范围为[20,40)，策略3对应的数值范围为

[0060] [40,65)，策略4对应的数值范围为[65,85)例如策略5对应的数值范围为[85,105)。在随机生成人脸活体检测策略时，可以随机生成整数，所述整数的取值范围为[0,105)。当随机生成数字60时，对应的策略为策略3，以此类推。

[0061] S204，执行生成的人脸活体检测策略。

[0062] 这时，系统或设备会提示用户执行与生成的人脸活体检测策略对应的动作。用户按照系统提示，做出对应的动作。

[0063] S205，采集用户行为对应的视频帧。

[0064] S206，判断用户行为是否为异常用户行为。

[0065] 其中，用户行为是否为异常用户行为的判断可以包括:判断用户行为是否是人脸；如果是，判断是否是符合人脸活体检测策略的活体动作，当判断结果均为是时，则确定用户行为是正常用户行为，执行S210。当判断结果其中一者为否时，确定用户行为是异常用户行为。执行S207，确定调整策略。

[0066] 其中，用户行为是否为异常用户行为的判断还可以包括:判断是否未在预定的时间内采集到用户行为，如果是，执行S207;如果否，进入S210。

[0067] 当然，也可以在判断用户行为对应的视频帧中是否采集到人脸以及是否是符合人脸活体检测策略的活体动作后，当判断结果其中一者为否时，再进一步判断是否超时，如果超时，则确定为异常用户行为。

[0068] S207，确定调整策略。

[0069] S208，当预置的调整策略为提高安全策略时，提高对应异常用户行为的人脸活体检测策略的权重，进入S203。

[0070] 仍以人脸活体检测策略包括5种策略为例，假设随机生成的人脸活体检测策略为

策略3和策略5，其中，用户在执行策略3时，对应的用户行为被判断为异常行为，如果预置的调整策略为提高安全策略，则提高策略3的权重，例如策略3的权重变为25。这时，其对应的数值范围也会相应调整，调整后的取值范围为：策略1对应的数值范围为[0,20)，策略2对应的数值范围为[20,40)，策略3对应的数值范围为[40,65)，策略4对应的数值范围为[65,85)例如策略5对应的数值范围为[85,105)。在随机生成人脸活体检测策略时，可以随机生成整数，所述整数的取值范围为[0,105)。这样，由于策略3的权重增加，其在随机生成人脸活体检测策略时被选中的概率也增加，从而提高了人脸活体检测的难度，提高了安全性。其中，在提高对应异常用户行为的人脸活体检测策略的权重时，系统可以预先设置调整的幅度以及调整的取值范围。并且，可以设置用户执行人脸活体检测策略的次数阈值，超过次数阈值时，用户在当天不能够进行人脸活体检测，从而提高系统的安全性。

[0071] 进一步的，在另外一种实现方式中，假设在执行策略3之前，预先执行了策略5，而用户执行策略5的用户行为被判断为正常用户行为，那么，当预置的调整策略为提高安全策略时，除了提高对应异常用户行为的人脸活体检测策略的权重之外，还可以降低对应正常用户行为的人脸活体检测策略的权重。由于出现异常行为，说明系统具有较大的被攻击的风险，因此对于较容易通过的策略5，降低其权重，可以降低其被选中的概率，从而提高人脸活体检测的难度，提高系统的安全性。

[0072] S209，当预置的调整策略为提高用户体验策略时，降低对应异常用户行为的人脸活体检测策略的权重，进入S203。

[0073] 仍以人脸活体检测策略包括5种策略为例，假设随机生成的人脸活体检测策略为策略3和策略5，其中，用户在执行策略3时，对应的用户行为被判断为异常行为，如果预置的调整策略为提高用户体验策略，则降低策略3的权重，例如策略3的权重由20变为15。这时，其对应的数值范围也会相应调整，调整后的取值范围为：策略1对应的数值范围为[0,20)，策略2对应的数值范围为[20,40)，策略3对应的数值范围为[40,55)，策略4对应的数值范围为[55,75)例如策略5对应的数值范围为[75,95)。在随机生成人脸活体检测策略时，可以随机生成整数，所述整数的取值范围为[0,95)。这样，由于策略3的权重降低，其在随机生成人脸活体检测策略时被选中的概率也降低，从而提高了人脸活体检测的难度，提高了用户体验。

[0074] 进一步的，在另外一种实现方式中，假设在执行策略3之前，预先执行了策略5，而用户执行策略5的用户行为被判断为正常用户行为，那么，当预置的调整策略为提高用户体验策略时，除了降低对应异常用户行为的人脸活体检测策略的权重之外，还可以提高对应正常用户行为的人脸活体检测策略的权重。由于出现异常行为，说明对应的策略用户具有较大的难度执行，为了提高用户体验，除了降低较难通过的人脸活体检测策略的权重，还可以提高较容易通过的策略5的权重，以提高策略5被选中的概率，从而降低人脸活体检测的难度，提高用户体验。

[0075] S210，判断是否还有未执行的人脸活体检测策略，如果是，进入S204；如果否，进入S211。

[0076] S211，完成人脸活体检测，结束程序。

[0077] 需要说明的是，在本发明实施例具体实现时，当判断用户行为为异常用户行为，在确定调整策略时，除了图2所示实施例中按照预置的调整策略来确定调整策略的方式，还可

以采取其他方式确定调整策略。

[0078] 例如，在一种可能的实现方式中，获取用户历史行为数据，当根据所述用户历史行为数据确定所述用户属于高风险用户时，提高对应所述异常用户行为的人脸活体检测策略的权重。而后，进入S203，重新随机生成人脸活体检测策略。例如，当用户多次登录失败或者在人脸活体检测中不通过或者超时时，确定用户属于高风险用户，这时提高对应所述异常用户行为的人脸活体检测策略的权重，提高人脸活体检测的难度。

[0079] 在另外一种可能的实现方式中，替代S208和S209，可以获取用户历史行为数据，当根据所述用户历史行为数据确定所述用户属于低风险用户时，降低对应所述异常用户行为的人脸活体检测策略的权重。这样，可以提高用户体验。

[0080] 在另外一种实现方式中，替代S208和S209，可以获取用户在进行人脸活体检测前的数据操作，当确定所述数据操作的类型与预设的异常用户行为类型相同时，提高对应所述异常用户行为的人脸活体检测策略的权重。所述预设的异常用户行为类型包括：登录失败、修改密码、校验操作、解除绑定手机、更好绑定手机、删除记录等、使用设备异地登录或者使用不同的设备登录等，本发明对此不进行限定。当判断用户在进行人脸活体检测前执行的数据操作与预设的异常用户行为类型相同时，则确定用户具有较高的安全风险，为了提高系统的安全性，可以通过提高对应所述异常用户行为的人脸活体检测策略的权重，提高人脸活体检测的难度。

[0081] 当然，本领域技术人员可以理解的是，可以对图2所示实施例进行改动或变形，均属于本发明的保护范围。

[0082] 参见图3，为本发明实施例提供的再一种人脸活体检测方法流程示意图。

[0083] S301，获取用户历史用户行为。

[0084] S302，当根据所述用户历史行为确定所述用户属于高风险用户时，则确定所述用户行为属于异常用户行为。

[0085] S303，调整人脸活体检测策略集合中各策略的权重，以提高人脸活体检测的难度。

[0086] 这时，调整权重的策略可以是系统默认的策略，也可以是根据经验确定的、较难被用户执行的策略，即对应异常行为的策略。

[0087] S304，根据调整后的各人脸活体检测策略的权重，随机生成人脸活体检测策略。

[0088] S305，根据所述人脸活体检测策略执行人脸活体检测。

[0089] 在这一实施例中，可以在执行人脸活体检测前，预先获取用户的历史行为，从而确定是提高还是降低人脸活体检测的难度，以提高系统的安全性。

[0090] 参见图4，为本发明实施例提供的又一种人脸体检测方法流程示意图。

[0091] S401，获取用户在进行人脸活体检测前执行的数据操作。

[0092] S402，当确定所述数据操作的类型与预设的异常用户行为类型相同时，确定所述用户行为属于异常用户行为。

[0093] 所述预设的异常用户行为类型包括：登录失败、修改密码、校验操作、解除绑定手机、更好绑定手机、删除记录等、使用设备异地登录或者使用不同的设备登录等，本发明对此不进行限定。当判断用户在进行人脸活体检测前执行的数据操作与预设的异常用户行为类型相同时，则确定用户具有较高的安全风险，确定用户行为属于异常用户行为。

[0094] S403，调整人脸活体检测策略集合中各策略的权重，以提高人脸活体检测的难度。

[0095] 这时，调整权重的策略可以是系统默认的策略，也可以是根据经验确定的、较难被用户执行的策略，即对应异常行为的策略。

[0096] S404，根据调整后的各人脸活体检测策略的权重，随机生成人脸活体检测策略。

[0097] S405，根据所述人脸活体检测策略执行人脸活体检测。

[0098] 在这一实施例中，可以在执行人脸活体检测前，预先获取用户在进行人脸活体检测前执行的数据操作，从而确定是提高还是降低人脸活体检测的难度，以提高系统的安全性。

[0099] 参见图5，为本发明实施例提供的人脸活体检测装置示意图。

[0100] 一种人脸活体检测装置500，所述装置包括：

[0101] 获取单元501，用于获取用户行为。

[0102] 调整单元502，用于当确定所述获取单元获取的用户行为属于异常用户行为时，确定调整策略；所述调整策略用于提高或者降低人脸活体检测的难度。

[0103] 策略生成单元503，用于根据所述调整单元确定的调整策略生成人脸活体检测策略。

[0104] 检测单元504，用于根据所述策略生成单元生成的人脸活体检测策略执行人脸活体检测。

[0105] 进一步的，所述获取单元获取的所述用户行为为用户执行第一人脸活体检测策略而形成的行为；

[0106] 所述调整单元具体用于：

[0107] 当确定所述用户行为不符合所述第一人脸活体检测策略的通过条件时，确定所述用户行为属于异常用户行为；或者，

[0108] 当未在预设时间内采集到符合所述第一人脸活体检测策略通过条件的用户行为时，确定所述用户行为属于异常用户行为。

[0109] 进一步的，所述调整单元具体用于：

[0110] 获取预置的调整策略，所述预置的调整策略包括第一策略和第二策略中的至少一者；

[0111] 当所述预置的调整策略为所述第一策略时，提高所述第一人脸活体检测策略的权重；

[0112] 当所述预置的调整策略为所述第二策略时，降低所述第一人脸活体检测策略的权重；

[0113] 其中，所述权重用于表示所述第一人脸活体检测策略在人脸活体检测策略集合中出现的概率。

[0114] 进一步的，所述获取单元具体用于：

[0115] 获取第一用户行为和第二用户行为；其中，所述第一用户行为为用户执行第一人脸活体检测策略而形成的行为；所述第二用户行为为用户执行第二人脸活体检测策略而形成的行为；所述第一人脸活体检测策略和所述第二人脸活体检测策略不同。

[0116] 进一步的，所述调整单元具体用于：

[0117] 当确定所述第一用户行为属于正常用户行为且确定所述第二用户行为属于异常用户行为时，获取预置的调整策略；所述预置的调整策略包括第一策略和第二策略中的至

少一者；

[0118] 当所述预置的调整策略为所述第一策略时，降低所述第一人脸活体检测策略的权重，提高所述第二人脸活体检测策略的权重；

[0119] 当所述预置的调整策略为所述第二策略时，提高所述第一人脸活体检测策略的权重，降低所述第二人脸活体检测策略的权重；

[0120] 其中，所述权重用于表示所述第一人脸活体检测策略或者所述第二人脸活体检测策略在人脸活体检测策略集合中出现的概率。

[0121] 进一步的，所述调整单元具体用于执行下述中的至少一者：

[0122] 获取用户历史行为数据，当根据所述用户历史行为数据确定所述用户属于高风险用户时，提高对应所述异常用户行为的人脸活体检测策略的权重；

[0123] 获取用户历史行为数据，当根据所述用户历史行为数据确定所述用户属于低风险用户时，降低对应所述异常用户行为的人脸活体检测策略的权重；

[0124] 获取用户在进行人脸活体检测前的数据操作，当确定所述数据操作的类型与预设的异常用户行为类型相同时，提高对应所述异常用户行为的人脸活体检测策略的权重；

[0125] 其中，所述权重用于表示所述人脸活体检测策略在人脸活体检测策略集合中出现的概率。

[0126] 进一步的，所述获取单元获取的所述用户行为为用户历史行为；

[0127] 所述调整单元具体用于：

[0128] 根据所述用户历史行为确定所述用户属于高风险用户时，则确定所述用户行为属于异常用户行为。

[0129] 进一步的，所述获取单元获取的所述用户行为为用户在进行人脸活体检测前执行的数据操作；

[0130] 所述调整单元具体用于：

[0131] 确定所述数据操作的类型与预设的异常用户行为类型相同时，确定所述用户行为属于异常用户行为。

[0132] 进一步的，所述调整单元具体用于：

[0133] 调整人脸活体检测策略集合中各策略的权重，以提高人脸活体检测的难度。

[0134] 进一步的，所述人脸活体检测策略包括闭眼、抬头、张口、摇头、微笑策略中的一种或多种。

[0135] 上述各单元的功能可对应于图1至图4详细描述的上述方法的处理步骤，于此不再赘述。需要说明的是，由于对方法实施例进行详细的阐述，对装置实施例的描述较为简单，本领域技术人员可以理解的是，可以参照方法实施例构造本发明的装置实施例。本领域技术人员在不付出创造性劳动下获取的其他实现方式均属于本发明的保护范围。

[0136] 本领域技术人员可以理解的是，以上对方法和装置实施例进行了示例性说明，以上不视为对本发明的限制，本领域技术人员在不付出创造性劳动下获得的其他实现方式均属于本发明的保护范围。

[0137] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖

非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。本发明可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本发明，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0138] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。以上所述仅是本发明的具体实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

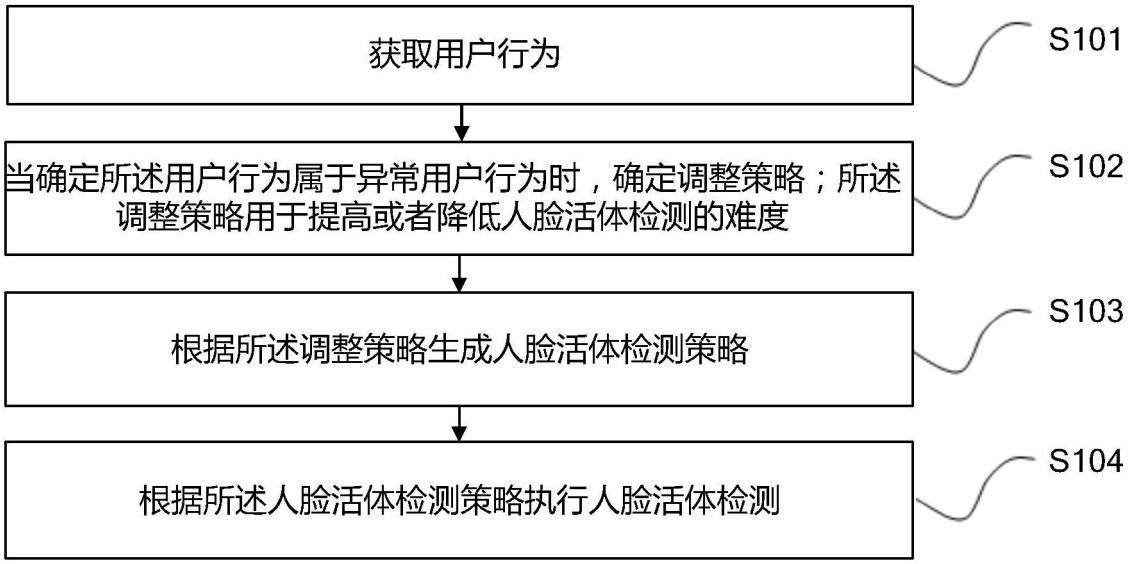

获取用户行为
S101
当确定所述用户行为属于异常用户行为时，确定调整策略；所述调整策略用于提高或者降低人脸活体检测的难度
S102
根据所述调整策略生成人脸活体检测策略
S103
根据所述人脸活体检测策略执行人脸活体检测
S104

图1

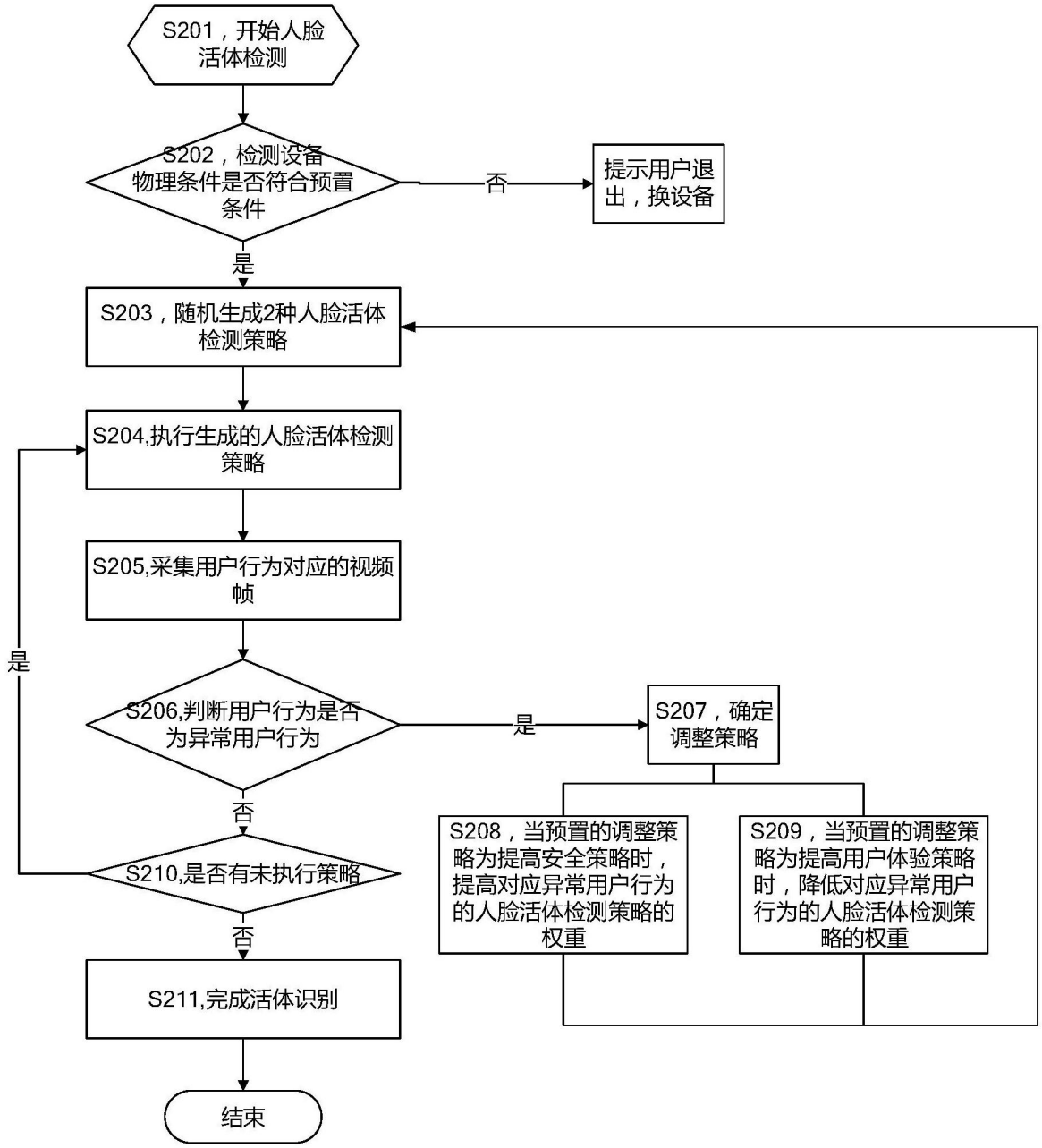

S201，开始人脸活体检测
S202，检测设备物理条件是否符合预置条件
否
提示用户退出，换设备
是
S203，随机生成2种人脸活体检测策略
S204,执行生成的人脸活体检测策略
S205,采集用户行为对应的视频帧
S206,判断用户行为是否为异常用户行为
是
S207，确定调整策略
S208，当预置的调整策略为提高安全策略时，提高对应异常用户行为的人脸活体检测策略的权重
S209，当预置的调整策略为提高用户体验策略时，降低对应异常用户行为的人脸活体检测策略的权重
否
S210,是否有未执行策略
是
否
S211,完成活体识别
结束

图2

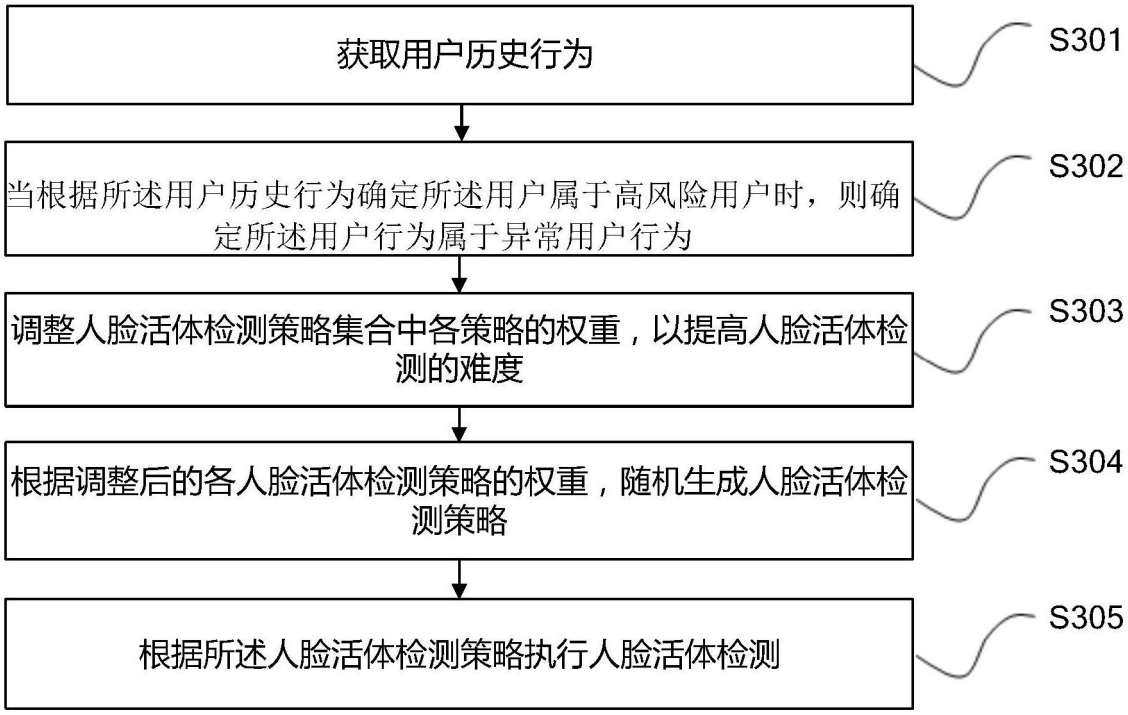

获取用户历史行为
S301
当根据所述用户历史行为确定所述用户属于高风险用户时，则确定所述用户行为属于异常用户行为
S302
调整人脸活体检测策略集合中各策略的权重，以提高人脸活体检测的难度
S303
根据调整后的各人脸活体检测策略的权重，随机生成人脸活体检测策略
S304
根据所述人脸活体检测策略执行人脸活体检测
S305

图3

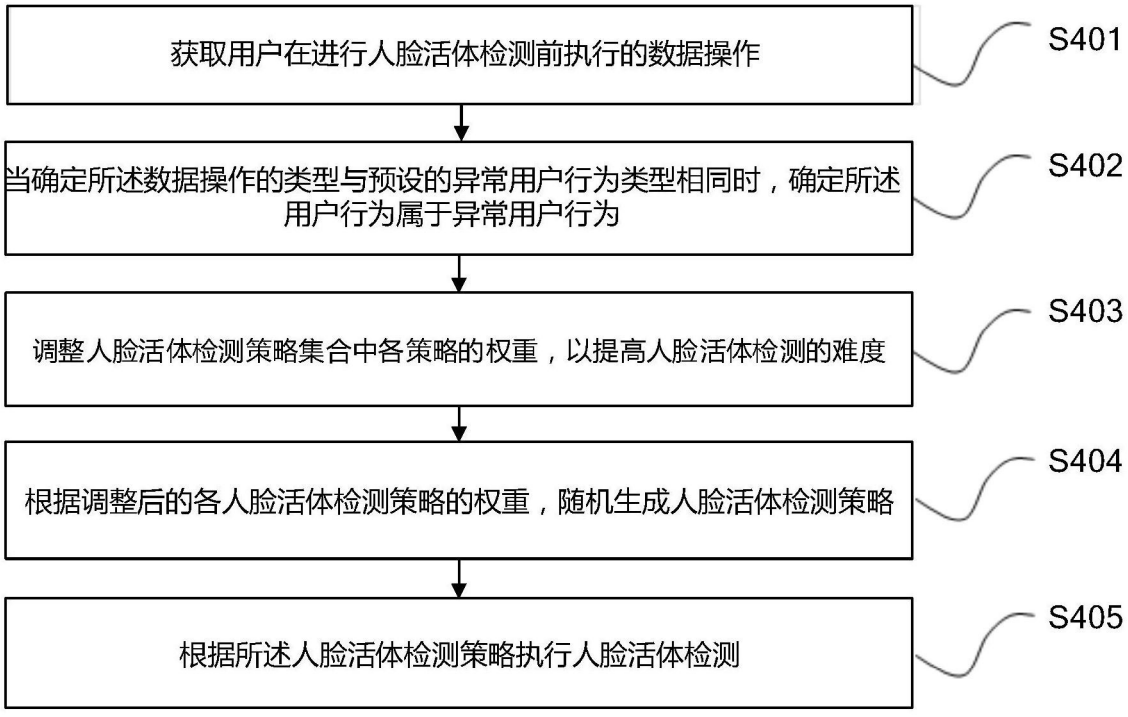

获取用户在进行人脸活体检测前执行的数据操作
S401
当确定所述数据操作的类型与预设的异常用户行为类型相同时，确定所述用户行为属于异常用户行为
S402
调整人脸活体检测策略集合中各策略的权重，以提高人脸活体检测的难度
S403
根据调整后的各人脸活体检测策略的权重，随机生成人脸活体检测策略
S404
根据所述人脸活体检测策略执行人脸活体检测
S405

图4

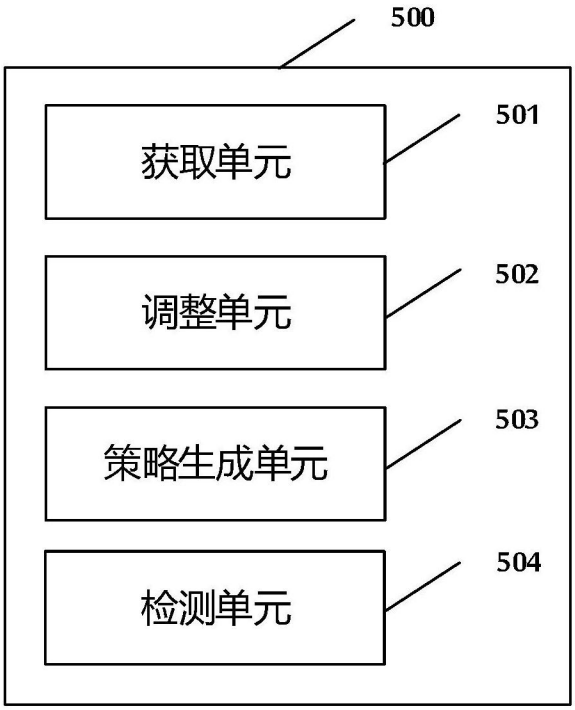


图5