(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107038361 A
(43)申请公布日 2017.08.11

(21)申请号 201610896522.3

(22)申请日 2016.10.13

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 吴军 曾晓东 尹欢密 林锋

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
G06F 21/32(2013.01)
G06F 21/44(2013.01)
G06Q 20/40(2012.01)

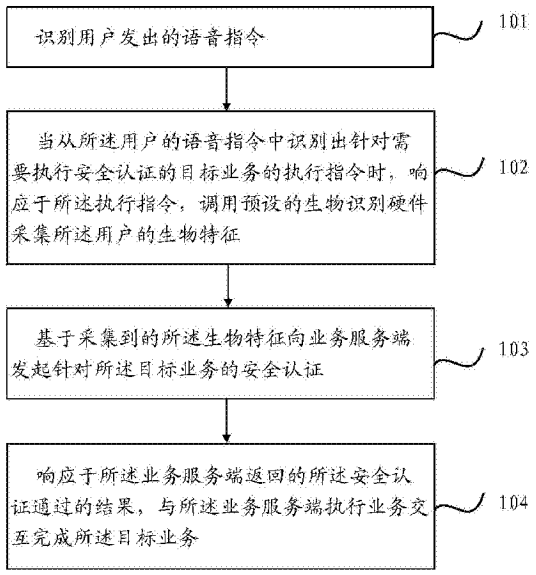
权利要求书2页 说明书11页 附图3页

(54)发明名称

基于虚拟现实场景的业务实现方法及装置

(57)摘要

本申请提供一种新的基于VR场景的业务实现方法，应用于虚拟现实客户端，所述方法包括：识别用户发出的语音指令；当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征；基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证；响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务。本申请可以实现基于语音的快捷交互以及针对目标业务的快捷安全认证。



CN 107038361 A

1.一种基于虚拟现实场景的业务实现方法，其特征在于，应用于虚拟现实客户端，所述方法包括：

识别用户发出的语音指令；

当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征；

基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证；

响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务。

2.根据权利要求1所述的方法，其特征在于，所述识别佩戴虚拟现实的用户发出的语音指令，包括：

通过预设的音频采集硬件采集佩戴虚拟现实终端的用户发出的语音指令；

将所述语音指令上传至业务服务端，以由所述业务服务端针对所述语音指令执行语音识别转换为字符串指令；

接收所述业务服务端返回的针对所述语音指令执行语音识别后得到的字符串指令。

3.根据权利要求1所述的方法，其特征在于，还包括：

当从所述用户的语音指令中识别出针对所述目标业务的取消指令时，响应于所述取消指令，终止所述目标业务；以及，

当从所述用户的语音指令中识别出针对与所述目标业务对应的业务执行方式的切换指令时，响应于所述切换指令，针对与所述目标业务对应的业务执行方式进行切换。

4.根据权利要求1所述的方法，其特征在于，所述调用预设的生物识别硬件采集所述用户的生物特征之前，还包括：

针对所述用户执行活体检测；

当所述用户通过所述活体检测时，在所述虚拟现实场景的用户视野中向所述用户输出采集生物特征的提示。

5.根据权利要求4所述的方法，其特征在于，所述生物特征为指纹；所述生物识别硬件为指纹识别硬件；还包括：

在所述虚拟现实场景的用户视野中输出用于指示所述生物识别硬件在虚拟现实终端上的安装位置的提示。

6.根据权利要求1所述的方法，其特征在于，所述基于采集到的所述生物特征向业务服务端发起针对所述用户的安全认证，包括：

向所述业务服务端发送针对采集到的所述生物特征的验证请求，所述验证请求携带采集到的所述生物特征，以及所述用户的账号信息，以由所述业务服务端在预设的生物特征库中查询与所述用户的账号信息绑定的生物特征样本，并将所述生物特征与该生物特征样本进行匹配，对所述目标业务进行安全认证。

7.根据权利要求1所述的方法，其特征在于，所述目标业务包括支付业务。

8.一种基于虚拟现实场景的业务实现装置，其特征在于，应用于虚拟现实客户端，所述装置包括：

识别模块，识别用户发出的语音指令；

采集模块，当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执

行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征；

认证模块，基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证；

执行模块，响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务。

9.根据权利要求8所述的装置，其特征在于，所述识别模块：

通过预设的音频采集硬件采集佩戴虚拟现实终端的用户发出的语音指令；

将所述语音指令上传至业务服务端，以由所述业务服务端针对所述语音指令执行语音识别转换为字符串指令；

接收所述业务服务端返回的针对所述语音指令执行语音识别后得到的字符串指令。

10.根据权利要求8所述的装置，其特征在于，所述执行模块进一步：

当从所述用户的语音指令中识别出针对所述目标业务的取消指令时，响应于所述取消指令，终止所述目标业务；以及，

当从所述用户的语音指令中识别出针对与所述目标业务对应的业务执行方式的切换指令时，响应于所述切换指令，针对与所述目标业务对应的业务执行方式进行切换。

11.根据权利要求8所述的装置，其特征在于，所述装置还包括：

检测模块，在调用预设的生物识别硬件采集所述用户的生物特征之前，针对所述用户执行活体检测；

输出模块，当所述用户通过所述活体检测时，在所述虚拟现实场景的用户视野中向所述用户输出采集生物特征的提示。

12.根据权利要求11所述的装置，其特征在于，所述生物特征为指纹；所述生物识别硬件为指纹识别硬件；

所述输出模块进一步：

在所述虚拟现实场景的用户视野中输出用于指示所述生物识别硬件在虚拟现实终端上的安装位置的提示。

13.根据权利要求8所述的装置，其特征在于，所述认证模块：

向所述业务服务端发送针对采集到的所述生物特征的验证请求，所述验证请求携带采集到的所述生物特征，以及所述用户的账号信息，以由所述业务服务端在预设的生物特征库中查询与所述用户的账号信息绑定的生物特征样本，并将所述生物特征与该生物特征样本进行匹配，对所述目标业务进行安全认证。

14.根据权利要求8所述的装置，其特征在于，所述目标业务包括支付业务。

基于虚拟现实场景的业务实现方法及装置

技术领域

[0001] 本申请涉及计算机应用领域，尤其涉及一种基于虚拟现实场景的业务实现方法及装置。

背景技术

[0002] VR(Virtual Reality，虚拟现实)技术，是一种综合利用计算机图形系统和各种控制接口，在计算机上生成可交互的三维交互环境，面向用户提供沉浸感的技术。随着VR技术以及硬件的进步，VR技术的应用场景也越来越丰富。

[0003] 然而，VR技术虽然可以面向用户提供逼真的沉浸感，但用户在佩戴VR终端进行沉浸体验时，如果需要在VR场景中执行需要进行安全认证的目标业务(比如支付业务)时，如何快捷的对目标业务进行安全认证，对于提升用户体验将具有十分重要的意义。

发明内容

[0004] 本申请提出一种基于虚拟现实场景的业务实现方法，应用于虚拟现实客户端，所述方法包括：

[0005] 识别用户发出的语音指令；

[0006] 当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征；

[0007] 基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证；

[0008] 响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务。

[0009] 本申请还提出一种基于虚拟现实场景的业务实现装置，应用于虚拟现实客户端，所述装置包括：

[0010] 识别模块，识别用户发出的语音指令；

[0011] 采集模块，当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征；

[0012] 认证模块，基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证；

[0013] 执行模块，响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务。

[0014] 本申请中，通过识别用户发出的语音指令；当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征，并基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证，然后响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务，实现了当用户在虚拟现实场景中执行需要进行安全认证的目标业务时，可以利用语音指令快捷的触发上述目标业务，以及利用虚

拟现实终端搭载的生物特征识别硬件，在该目标业务被触发时，在虚拟现实场景中快捷的完成针对该目标业务的安全认证，从而既可以保障用户在虚拟现实场景中执行的业务的安全性，又可以降低针对业务的安全认证的交互复杂度提升用户的业务体验。

附图说明

[0015] 图1是本申请一实施例示出的基于VR场景的业务实现方法的流程图；

[0016] 图2是本申请一实施例提供的一种基于VR场景的业务实现装置的逻辑框图；

[0017] 图3是本申请一实施例提供的承载所述一种基于VR场景的业务实现装置的VR终端所涉及的硬件结构图。

具体实施方式

[0018] 本申请旨在提出一种用户在佩戴VR终端进行沉浸体验的过程中，通过语音指令这种自然的交互方式，快捷的触发需要执行安全认证的目标业务，以及基于VR客户端搭载的生物识别硬件，对用户在VR场景中对该目标业务进行快捷的安全认证的技术方案。

[0019] VR客户端通过识别用户发出的语音指令；当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征，并基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证，然后响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务，实现了当用户在虚拟现实场景中执行需要进行安全认证的目标业务时，可以利用语音指令快捷的触发上述目标业务，以及利用虚拟现实终端搭载的生物特征识别硬件，在该目标业务被触发时，在虚拟现实场景中快捷的完成针对该目标业务的安全认证，从而既可以保障用户在虚拟现实场景中执行的业务的安全性，又可以降低针对业务的安全认证的交互复杂度提升用户的业务体验。

[0020] 例如，当本申请的技术方案应用于VR场景中的快捷支付场景时，可以通过VR客户端快速的识别出用户发出的语音指令，触发支付业务，并通过VR终端搭载的生物识别硬件，对用户在VR场景中触发的该支付业务，快捷的完成安全认证；一方面，使得用户可以不再需要在VR场景中，执行复杂的交互方式(比如将操作焦点定位到支付界面中)，来触发支付业务；另一方面，使得用户业务可以不再需要在虚拟现实场景中通过复杂的交互方式输入支付密码，对支付业务进行安全认证，从而可以在保证支付安全的前提下，降低用户在触发支付业务，以及对支付业务进行安全认证时的复杂度。

[0021] 下面通过具体实施例并结合具体的应用场景对本申请进行描述。

[0022] 请参考图1，图1是本申请一实施例提供的一种基于虚拟现实场景的业务实现方法，应用于VR客户端，执行以下步骤：

[0023] 步骤101，识别用户发出的语音指令；

[0024] 步骤102，当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征；

[0025] 步骤103，基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证；

[0026] 步骤104，响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服

务端执行业务交互完成所述目标业务。

[0027] 上述VR客户端，是指基于VR技术开发的可以面向用户提供三维沉浸体验的客户端软件；比如，基于VR的APP；上述VR客户端，可以将开发人员开发出的虚拟现实场景模型，通过与VR客户端对接的VR终端，向用户输出，从而使得佩戴VR终端的用户，能够在VR中得到三维沉浸体验。

[0028] 上述目标业务，是指用户在VR场景中执行的，需要进行安全认证的用户业务；

[0029] 例如，在实际应用中，上述目标业务可以是在一些特定的VR场景中的快捷支付业务；比如，VR购物场景中的订单支付、VR直播场景中的打赏、VR游戏场景中的充值以及VR视频场景中的视频点播支付。

[0030] 以下通过VR场景模型创建，目标业务的触发，目标业务的安全认证、以及目标业务的执行四个阶段，对本申请的技术方案进行详细描述。

[0031] 1)VR场景模型创建

[0032] 在本例中，开发人员可以通过特定的建模工具，完成VR场景模型的创建。上述建模工具，在本例中不进行特别的限定；例如，开发人员可以使用诸如Unity、3dsMax、Photoshop等较为成熟的建模工具完成VR场景模型的创建。

[0033] 其中，开发人员在通过建模工具创建VR场景模型的过程中，该VR场景模型，以及该VR场景的纹理贴图，都可来源于现实生活中的真实场景；例如，可以事先通过摄像，采集材质纹理贴图，和真实场景的平面模型，然后通过Photoshop或3dmax等建模工具，来处理纹理和构建真实场景的三维模型，然后导入到unity3D平台(简称U3D)，在U3D平台中通过音效、图形界面、插件、灯光等多个维度进行画面渲染，然后编写交互代码，最后完成VR场景模型的建模。

[0034] 在本例中，开发人员除了需要创建VR场景模型以外，为了使用户能够在VR场景中执行上述目标业务，还可以通过上述建模工具，在上述VR场景模型中，创建一个与上述目标业务对应的2D或者3D的业务界面。

[0035] 例如，在示出的一种实施方式中，上述业务界面，可以是一个基于上述建模工具创建的快捷支付界面；比如，虚拟的收银台界面。用户可以通过特定的交互操作(比如将操作焦点定位到支付界面中)与支付界面进行交互，在VR场景中完成快捷支付。

[0036] 2)目标业务的触发

[0037] 在本例中，当开发人员完成VR场景模型，以及上述业务界面的建模后，上述VR客户端可以将上述VR场景模型以及上述业务界面，通过与上述VR客户端对接的VR终端(比如VR头盔)，向用户输出。

[0038] 其中，需要说明的是，在默认情况下，上述VR客户端可以仅向用户输出上述VR场景模型，用户在VR场景中进行沉浸体验的过程中，可以通过与上述VR客户端进行交互，来触发上述VR客户端执行上述目标业务，在VR场景中输出上述业务界面。

[0039] 在相关技术中，用户在VR场景中触发目标业务时，通常是通过头部姿态或者手势控制操作焦点的移动，将操作焦点定位到VR场景的操作界面上，与操作界面进行交互来实现的。

[0040] 例如，可以在操作界面上提供一用于触发目标业务的虚拟元件(比如虚拟按钮)，用于可以通过将操作焦点定位到该虚拟元件上，来选中该虚拟元件，继而触发上述目标业

务。

[0041] 可见，目前的用于触发目标业务的交互方式，存在过于复杂的问题。

[0042] 在本例中，为了降低用户在触发上述目标业务时的交互复杂度，实现更加自然的交互，上述VR客户端可以搭载语音识别服务，使得用户可以通过语音指令来快捷的触发上述目标业务。

[0043] 在实际应用中，用户在佩戴VR终端进行沉浸体验时，如果需要在VR场景中执行上述目标业务，此时用户可以以语音的形式发出针对该目标业务的执行指令。VR客户端可以通过VR终端搭载的音频采集硬件，采集用户发出的语音指令，当采集到用户的语音指令后，然后基于搭载的语音识别服务对该语音指令进行识别。

[0044] 其中，在示出的一种实施方式中，对用户的语音指令的识别过程，可以在与该目标业务对应的业务服务端上来完成。

[0045] 例如，当上述业务服务端为基于服务器集群构建的业务平台时，可以启用一面向VR客户端提供语音识别服务的语音识别服务器，并面向VR客户端提供访问接口。

[0046] 当VR客户端成功采集到用户的语音指令后，可以基于采集到的该语音指令，构建一个语音识别请求，然后访问上述业务服务端提供的语音识别接口，将该语音识别请求提交至上述业务服务端。

[0047] 上述业务服务端在收到来自VR客户端的语音识别请求后，可以解析该语音识别请求，获取请求中携带的该用户的语音指令，并通过预设的语音识别算法对该语音指令进行识别，将其转换为VR客户端可识别的字符串指令，然后将转换后的字符串指令返回给VR客户端。

[0048] VR客户端在接收到业务服务端返回的字符串指令后，可以识别该字符串指令是否为与上述目标业务对应的执行指令，如果是与上述目标业务对应的执行指令时，可以响应该执行指令，并触发执行上述目标业务的流程。

[0049] 例如，当上述目标业务为基于VR场景的快捷支付业务时，用户在佩戴VR终端进行沉浸体验的过程中，可以发出“开始支付”的语音指令，当通过业务服务端语音识别后，可以将该语音指令转换为VR终端可以识别的字符串指令，由VR客户端进行响应，来触发支付流程。

[0050] 需要说明的是，用户在佩戴VR终端进行沉浸体验的过程中，除了可以通过发出与上述目标业务对应的执行指令对应的语音指令，触发上述目标业务以外，在实际应用中，也可以通过发出其它形式的语音指令，来触发VR客户端针对上述目标业务执行相应的业务控制。

[0051] 在示出的一种实施方式中，当用户通过语音指令触发了上述目标业务后，如果用户需要临时取消该目标业务的执行，还可以通过发出与上述目标业务的取消指令对应的语音指令。当该语音指令被成功识别，转换成VR客户端可识别的字符串指令后，VR客户端可以响应该取消指令，并立即终止该目标业务。

[0052] 例如，当上述目标业务为基于VR场景的快捷支付业务时，用户在佩戴VR终端进行沉浸体验的过程中，当通过发出“开始支付”的语音指令触发了支付业务后，如果用户需要终止支付，可以继续发出“取消支付”的语音指令，当该“取消支付”的语音指令，通过业务服务端语音识别转换为VR终端可以识别的字符串指令后，VR客户端可以响应该“取消支付”的

指令，终止当前的支付流程。

[0053] 在示出的一种实施方式中，当用户通过语音指令触发了上述目标业务后，如果用户需要切换该目标业务的业务执行方式，还可以通过发出与切换上述目标业务执行方式的切换指令对应的语音指令。当该语音指令被成功识别，转换成VR客户端可识别的字符串指令后，VR客户端可以响应该切换指令，针对该目标业务的业务执行方式进行切换。

[0054] 例如，当上述目标业务为基于VR场景的快捷支付业务时，用户在佩戴VR终端进行沉浸体验的过程中，当通过发出“开始支付”的语音指令触发了支付业务后，如果用户需要切换支付方式；比如，将支付方式由当前的“储蓄卡支付”切换为“信用卡支付”，可以继续发出“请使用信用卡支付”的语音指令，当该语音指令通过业务服务端语音识别转换为VR终端可以识别的字符串指令后，VR客户端可以响应该“请使用信用卡支付”的指令，将当前的支付方式由“储蓄卡支付”切换为“信用卡支付”。

[0055] 当然，在实际应用中，除了以上示出的取消目标业务，以及切换目标业务的业务执行方式的业务控制过程以外，如果用户需要针对上述目标业务执行其它形式的业务控制，也同样可以通过发出相应的语音指令来完成；即在本例中，与上述目标业务相关的一切业务控制行为，均可以由用户发出的语音指令来完成。

[0056] 3)目标业务的安全认证

[0057] 在本例中，为了提升用户在VR场景中执行目标业务时，更快捷的对该目标业务进行安全认证，可以利用VR终端搭载的生物识别硬件，来采集业务发起用户的生物特征，来快速的完成对该目标业务的安全认证。

[0058] 其中，上述生物特征，可以是用户指纹；上述生物识别硬件，可以是VR终端搭载的指纹识别硬件。

[0059] 需要说明的是，VR终端搭载的指纹识别硬件，可以是VR终端的硬件架构中内置的指纹识别硬件，也可以是外接的指纹识别模块，或者还可以是与VR终端对接的第三方移动终端(比如智能手机)上内置的指纹识别硬件；比如，当上述VR终端为滑佩式的VR头盔时，用户可以将移动终端插入VR头盔中进行使用，在这种情况下，VR头盔的硬件架构中可以不内置指纹识别硬件，而是直接使用该移动终端中的指纹识别硬件。

[0060] 当然，在实际应用中，上述生物识别硬件，除了以上示出的指纹识别硬件以外，也可以是诸如虹膜识别硬件，声纹识别硬件，或者其它形式的生物识别硬件，在本例中不再一一列举。

[0061] 在以下的实施例中，将以上述生物识别硬件为指纹识别硬件为例进行说明。显然，以上述生物识别硬件为指纹识别硬件为例仅为示例性的，并不用于限定本申请的技术方案。

[0062] 在本例中，在初始状态下，用户可以通过上述VR客户端提前对自己的指纹进行注册，在业务服务端上建立该用户的账号信息与该用户的指纹信息之间的绑定关系。

[0063] 其中，该用户的账号信息，具体可以包括用户在执行上述目标业务时，所使用的业务账号；

[0064] 例如，当上述目标业务为支付业务，上述用户的账号信息，可以是用户的支付账号，用户可以通过指纹注册，将支付账号与指纹信息在业务服务端上进行绑定。

[0065] 当用户完成指纹注册后，后续用户将可以在VR场景中，使用自己的指纹信息，对发

起的目标业务进行快捷的安全认证，而可以不再需要输入诸如业务密码等信息对目标业务进行验证。

[0066] 在示出的一种实施方式中，用户在对指纹进行注册时，在初始状态下，可以使用上述账号信息登录上述VR客户端，然后在VR客户端输出的VR场景的提示下，完成指纹的采集，由上述VR客户端将采集到的指纹信息，与该用户所使用的登录账号通过注册消息的形式发往上述业务服务端。上述业务服务端在收到上述VR客户端发出的注册消息后，可以将该用户的指纹信息作为指纹样本，与该用户的登录账号进行绑定，然后将二者的映射关系存储至预设的特征数据库。

[0067] 其中，在示出的一种实施方式中，为了提升指纹注册过程中的安全性，VR客户端在向业务服务端发送注册消息之前，还可以对用户的指纹注册行为进行身份验证；

[0068] 例如，可以提示用户输入登录密码或者其它能够表征用户身份的信息，对本次执行指纹注册的用户身份进行验证，当验证通过后，再通过VR客户端向业务服务端发送注册消息来完成指纹注册。

[0069] 通过这种方式，可以避免非法用户冒用自己的指纹信息，与另一合法用户的登录账号完成绑定，从而可以提升指纹注册的安全性。

[0070] 当用户在完成指纹信息的注册后，后续当该用户在VR场景中，通过选中上述虚拟元件，成功触发了上述目标业务后，此时VR客户端可以启动基于用户注册的指纹信息，对上述目标业务执行安全认证的流程。

[0071] 在本例中，当佩戴VR终端的用户在VR场景中，通过语音指令成功触发了上述目标业务，此时VR客户端可以调用搭载的指纹识别硬件，来采集该用户的指纹信息。

[0072] 在示出的一种实施方式中，VR客户端在开始采集用户的指纹信息之前，还可以引入针对佩戴VR终端的用户的活体检测流程。

[0073] 在这种情况下，VR终端可以在正式开始采集指纹信息以前，针对佩戴该VR终端的用户进行活体检测，以确定当前VR终端存在使用者。通过这种方式，可以有效的避免，通过诸如指纹图片等作弊手段，仿冒用户的指纹信息来完成非法的业务认证。

[0074] 其中，在本例中，在VR客户端在针对佩戴VR终端的用户进行活体检测的方式，在本例中不进行特别限定；例如，可以通过眨眼识别，心跳识别等技术手段来完成用户的活体检测。

[0075] 当完成针对上述用户的活体检测后，VR客户端可以在VR场景的用户视野中向用户输出一个采集生物特征的提示，以提示用户采集指纹信息，对上述目标业务执行安全认证。

[0076] 例如，当上述目标业务为基于VR场景的快捷支付业务时，VR客户端可以在VR场景的用户视野中，输出一条“请输入指纹完成支付认证”的文本提示消息。

[0077] 在本例中，由于用户在佩戴VR终端进行沉浸体验时，如果要在VR场景中完成指纹信息的检测，将会存在一定的困难；因此，在这种情况下，用户通常将不得不摘下佩戴的VR终端来完成指纹信息的采集。

[0078] 为了解决这种问题，在示出的一种实施方式中，当用户在VR场景中成功触发了上述目标业务后，VR在开始采集用户的指纹信息之前，可以在VR场景中输出一个用于指示指纹采集硬件在该VR终端上的安装位置的提示。

[0079] 其中，输出的该提示，可以是一个静态的提示，也可以是一个动态的提示。

[0080] 在一种实现方式中，VR终端可以在VR场景的用户视野中，输出一个静态的提示标记，提示指纹识别硬件在VR终端上的相对位置；

[0081] 例如，假设VR终端内置的指纹识别硬件，安装在该VR终端的硬件架构中的右上方，则可以在VR场景的右上方输出一个虚拟的闪烁箭头，用于指示该指纹识别硬件在VR场景的用户视野的相对位置，从而可以提示用户将手指向用户视野的右上方移动，来完成指纹的采集。

[0082] 在示出的另一种实现方式中，VR终端可以在VR场景的用户视野中，输出一个动态的提示标记，基于指纹识别硬件在VR终端上的相对位置，引导用户手指移动的方向，来完成指纹采集

[0083] 例如，假设VR终端内置的指纹识别硬件，安装在该VR终端的硬件架构中的右上方，则可以在VR场景中，以当前的操作焦点为起始点，输出一个指向VR场景中用户视野的右上方的动态轨迹，用于指示该指纹识别硬件在VR场景的用户视野的相对位置。在这种情况下，用户可以按照该动态轨迹提示的方向，向指纹识别硬件的安装位置移动，来完成指纹的采集。

[0084] 通过这种方式，可以在VR场景中向用户提示指纹采集硬件的相对位置，使得用户在佩戴VR终端进行沉浸体验时，不需要摘下佩戴的VR终端，就可以快捷的完成指纹信息的采集。

[0085] 在本例中，当VR终端通过调用指纹识别硬件，成功采集到用户的指纹信息时，此时可以基于采集得到的指纹信息与业务服务端进行交互，来完成针对上述目标业务的安全认证。

[0086] 在示出的一种实施方式中，上述业务服务端可以启用指纹识别服务，并面向VR客户端提供指纹识别接口。

[0087] 例如，当上述业务服务端为基于服务器集群构建的业务平台时，可以启用一面向VR客户端提供指纹识别服务的指纹识别服务器，并面向VR客户端提供访问接口。

[0088] 当VR客户端成功采集到用户的指纹信息后，可以基于该用户当前登录VR客户端所使用的账号信息，以及采集到的该用户的指纹信息，构建一个指纹识别请求，然后访问上述业务服务端提供的指纹识别接口，将该指纹识别请求提交至上述业务服务端。

[0089] 上述业务服务端在收到来自VR客户端的指纹识别请求后，可以解析该指纹识别请求，获取请求中携带的该用户的指纹信息以及账号信息，然后将该指纹信息与上述预设的特征数据库中存储的指纹样本，逐个进行匹配，以验证该用户当前使用的账号信息，与上述特征数据库中存储的与该指纹信息绑定的账号信息是否一致。

[0090] 当该用户的指纹信息与上述特征数据库中存储的任一指纹样本完全匹配，此时业务服务端可以进一步验证该用户当前使用的账号信息，与上述特征库中存储的与该用户的指纹信息匹配的指纹样本绑定的账号信息是否一致，然后将验证结果返回给上述VR客户端。

[0091] 其中，上述验证结果即为针对上述目标业务的安全认证结果。上述业务服务端返回给上述VR客户端的验证结果，具体可以是布尔类型的返回值(即false和true)；

[0092] 例如，如果该用户当前使用的账号信息，与上述特征库中存储的与该用户的指纹信息匹配的指纹样本绑定的账号信息一致，可以返回一个返回值true，表明针对上述目标

业务的安全认证通过。

[0093] 相反，如果该用户当前使用的账号信息，与上述特征库中存储的与该用户的指纹信息匹配的指纹样本绑定的账号信息不一致可以返回一个返回值false，表明针对上述目标业务的安全认证失败。

[0094] 其中，需要说明的是，除了以上示出的VR客户端可以将采集到的用户的指纹信息上传至业务服务端，由业务服务端基于该指纹信息对该用户发起的目标业务进行安全认证以外，在实际应用中，针对上述目标业务的安全认证也可以由上述VR客户端在其本地完成。

[0095] 在这种情况下，用户可以在VR客户端本地预留指纹信息完成指纹注册，VR客户端可以采集用户预留的指纹信息，并将该指纹信息与用户的账号信息在本地进行绑定。当用户在VR场景中触发了上述目标业务后，VR客户端可以采集用户的指纹信息，与用户预留的指纹信息进行匹配；如果采集到的指纹信息与用户预留的指纹信息匹配，此时针对上述目标业务的安全认证通过；相反，如果采集到的指纹信息与用户预留的指纹信息不匹配，此时针对上述目标业务的安全认证失败，其具体实现过程不再赘述。

[0096] 4)目标业务的执行

[0097] 在本例中，当VR客户端接收到业务服务端返回的针对上述目标业务的安全认证结果后，如果安全认证通过(比如返回一个true的返回值)，此时VR客户端可以在VR场景中输出与上述目标业务对应的业务界面，并通过该业务界面收集与上述目标业务相关的业务参数，构建一个业务请求，通过访问业务服务端面向VR客户端提供的业务访问接口，将该业务请求提交至业务服务端，与业务服务端执行进一步的业务交互，来完成上述目标业务。

[0098] 例如，当上述目标业务为在VR场景中的快捷支付业务时，此时VR客户端可以输出支付界面，通过支付界面收集诸如用户信息、订单信息、价格信息等与支付业务相关的业务参数，然后构建一个对应支付请求，发送至业务服务端，由业务服务端进行处理，来完成支付流程。

[0099] 通过以上实施例的描述可知，在本例中，用户可以利用语音指令快捷的触发上述目标业务，以及VR客户端还可以利用VR终端搭载的生物识别硬件，对用户在VR实场景中执行的需要进行安全认证的目标业务进行安全认证，从而既可以保障用户在虚拟现实场景中执行的业务的安全性，又可以降低针对业务的安全认证的交互复杂度提升用户的业务体验。

[0100] 以下结合用户在进行VR购物体验时，通过VR终端搭载的指纹识别硬件在VR场景中进行快捷的安全支付的应用场景为例，对本申请的技术方案进行描述。

[0101] 当然，需要说明的是，上述示出的应用场景仅为示例性的，并不用于限定；显然，在实际应用中本申请的技术方案，也可以应用在其它基于VR场景的信息输入场景；

[0102] 例如，用户在VR游戏的场景中，通过指纹快捷的完成游戏币的充值；用户在VR直播场景中，通过指纹快捷的完成打赏；以及用户在VR视频场景中，通过指纹快捷的完成视频的支付点播，等等；在本例中不再一一列举。

[0103] 在该场景下，上述目标业务可以是基于VR场景的快捷支付业务；上述VR客户端，可以是基于VR技术开发的支付客户端；比如，支付宝VR pay；上述业务服务端，可以是支付服务端；比如，基于服务器集群构建的支付宝平台。

[0104] 在初始状态下，用户可以使用支付账号登录该VR客户端，并通过该VR客户端完成

指纹的注册，将自己的指纹与支付账号进行绑定，存储至云端的支付服务端一侧的特征数据库中，其具体的注册过程不再赘述。当注册完成后，后续用户可以在VR场景中通过指纹完成快捷的安全支付。

[0105] 当用户在佩戴VR终端进行VR购物体验时，在VR场景中可以向用户呈现若干可供选择的商品，用户可以通过查看VR场景中提供的商品列表，来选择自己喜欢的商品进行购买。

[0106] 当用户在上述商品列表中，选择了一件满意的商品后，可以通过语音的形式发出针对该商品进行支付的支付指令，来触发VR客户端启动针对该商品的支付流程。当针对该商品的支付流程启动后，VR客户端首先针对用户执行活体检测，在完成活体检测后，可以在VR场景的用户视野中向用户输出一条“请输入指纹完成支付认证”的提示消息。

[0107] 另外，假设指纹识别硬件安装在VR终端的右上方，还可以在VR场景中输出一个指向VR场景中用户视野的右上方的虚拟的闪烁箭头，或者指向VR场景中用户视野的右上方的动态轨迹，以在VR场景中引导用户手指移动方向，完成指纹采集的提示。

[0108] 当用户指纹采集完成后，VR客户端可以基于采集完成的指纹信息和该用户登录VR客户端所使用的登录账号构建验证请求，提交至支付服务端，由支付服务端通过将该用户的指纹信息与该用户注册完成的指纹信息进行匹配；如果相匹配，支付服务端可以进一步匹配该用户当前使用的支付账号，和与该用户与注册完成的该指纹信息绑定的支付账号是否一致；如果一致，此时针对该支付业务的安全认证通过，支付服务端可以向VR客户端返回一个布尔类型的返回值true。

[0109] VR客户端在收到支付服务端返回的安全认证通过的结果后，可以输出支付界面，通过支付界面收集诸如用户信息、订单信息、价格信息等与支付业务相关的参数，然后构建一个对应支付请求，发往支付服务端，由支付服务端来处理该支付请求，完成针对该商品的快捷支付。

[0110] 其中，在实际应用中，为了提升支付的快捷性，还可以引入“小额免认证”的支付流程。在这种情况下，当用户通过语音指令触发了针对选中的商品的支付流程，此时VR客户端可以进一步检查支付金额，并确认支付金额是否低于预设金额(比如200元)，如果支付金额低于预设金额，此时VR客户端可以直接构建支付请求，发往支付服务端，由支付服务端来处理该支付请求，来完成针对该商品的快捷支付；如果支付金额不低于预设金额，再通过采用用户的指纹信息来完成支付业务的安全认证，具体的实施过程不再赘述。

[0111] 通过以上各实施例可知，通过识别用户发出的语音指令；当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征，并基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证，然后响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务，实现了当用户在虚拟现实场景中执行需要进行安全认证的目标业务时，可以利用语音指令快捷的触发上述目标业务，以及利用虚拟现实终端搭载的生物特征识别硬件，在该目标业务被触发时，在虚拟现实场景中快捷的完成针对该目标业务的安全认证，从而既可以保障用户在虚拟现实场景中执行的业务的安全性，又可以降低针对业务的安全认证的交互复杂度提升用户的业务体验。

[0112] 当本申请的技术方案应用于VR场景中的快捷支付场景时，可以通过VR客户端快速的识别出用户发出的语音指令，触发支付业务，并通过VR终端搭载的生物识别硬件，对用户

在VR场景中触发的该支付业务，快捷的完成安全认证；一方面，使得用户可以不再需要在VR场景中，执行复杂的交互方式，来触发支付业务；另一方面，使得用户业务可以不再需要在虚拟现实场景中通过复杂的交互方式输入支付密码，对支付业务进行安全认证，从而可以在保证支付安全的前提下，降低用户在触发支付业务，以及对支付业务进行安全认证时的复杂度。

[0113] 与上述方法实施例相对应，本申请还提供了装置的实施例。

[0114] 请参见图2，本申请提出一种基于VR场景的业务实现装置20，应用于VR客户端；

[0115] 请参见图3，作为承载所述基于VR场景的业务实现装置20的VR终端设备所涉及的硬件架构中，通常包括CPU、内存、非易失性存储器、网络接口以及内部总线等；以软件实现为例，所述基于VR场景的业务实现装置20通常可以理解为加载在内存中的计算机程序，通过CPU运行之后形成的软硬件相结合的逻辑装置，所述装置20包括：

[0116] 识别模块201，识别用户发出的语音指令；

[0117] 采集模块202，当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征；

[0118] 认证模块203，基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证；

[0119] 执行模块204，响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务。

[0120] 在本例中，所述识别模块201：

[0121] 通过预设的音频采集硬件采集佩戴虚拟现实终端的用户发出的语音指令；

[0122] 将所述语音指令上传至业务服务端，以由所述业务服务端针对所述语音指令执行语音识别转换为字符串指令；

[0123] 接收所述业务服务端返回的针对所述语音指令执行语音识别后得到的字符串指令。

[0124] 在本例中，所述执行模块204进一步：

[0125] 当从所述用户的语音指令中识别出针对所述目标业务的取消指令时，响应于所述取消指令，终止所述目标业务；以及，当从所述用户的语音指令中识别出针对与所述目标业务对应的业务执行方式的切换指令时，响应于所述切换指令，针对与所述目标业务对应的业务执行方式进行切换。

[0126] 在本例中，所述装置20还包括：

[0127] 检测模块205(图2中未示出)，在调用预设的生物识别硬件采集所述用户的生物特征之前，针对所述用户执行活体检测；

[0128] 输出模块206(图2中未示出)，当所述用户通过所述活体检测时，在所述虚拟现实场景的用户视野中向所述用户输出采集生物特征的提示。

[0129] 在本例中，所述生物特征为指纹；所述生物识别硬件为指纹识别硬件；

[0130] 所述输出模块206进一步：

[0131] 在所述虚拟现实场景的用户视野中输出用于指示所述生物识别硬件在虚拟现实终端上的安装位置的提示。

[0132] 在本例中，所述认证模块203：

[0133] 向所述业务服务端发送针对采集到的所述生物特征的验证请求，所述验证请求携带采集到的所述生物特征，以及所述用户的账号信息，以由所述业务服务端在预设的生物特征库中查询与所述用户的账号信息绑定的生物特征样本，并将所述生物特征与该生物特征样本进行匹配，对所述目标业务进行安全认证。

[0134] 在本例中，所述目标业务包括支付业务。

[0135] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

[0136] 应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

[0137] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

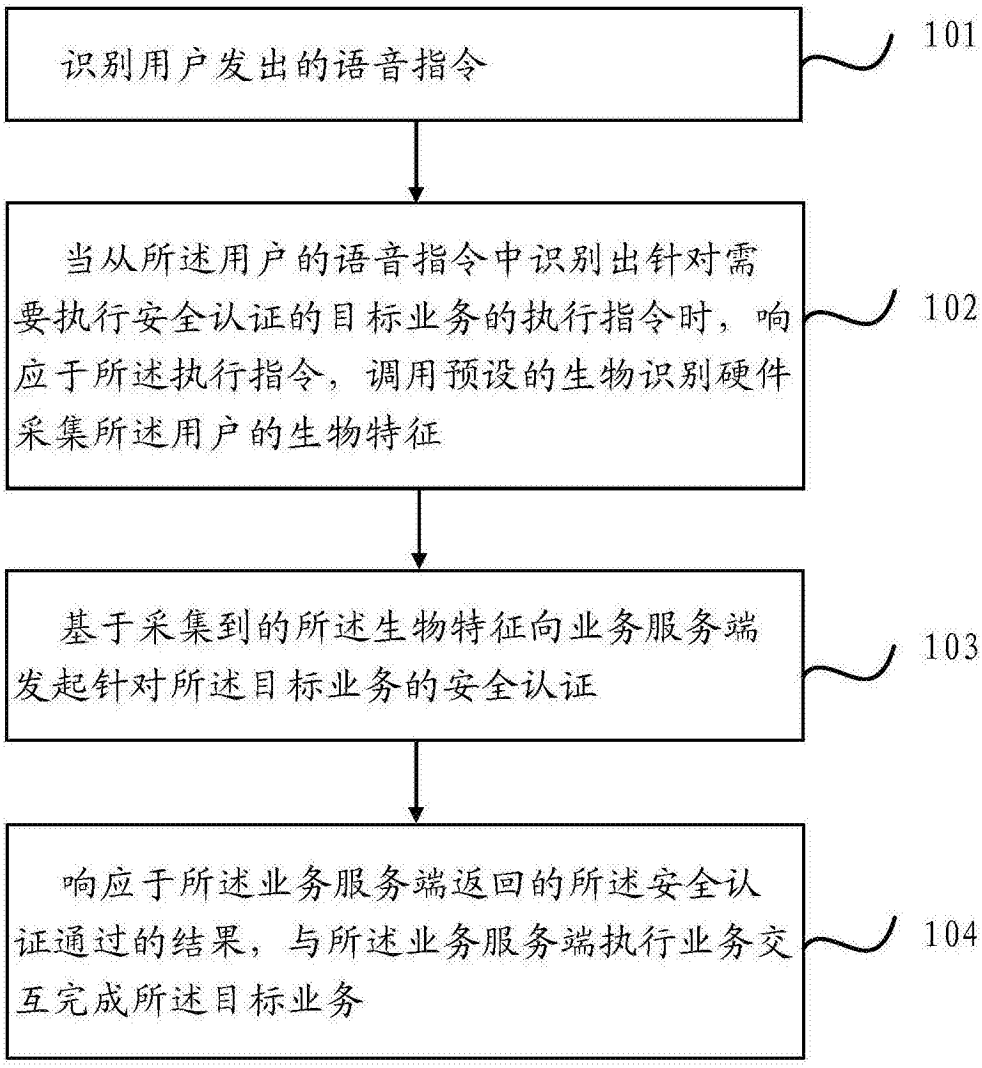

识别用户发出的语音指令
101
当从所述用户的语音指令中识别出针对需要执行安全认证的目标业务的执行指令时，响应于所述执行指令，调用预设的生物识别硬件采集所述用户的生物特征
102
基于采集到的所述生物特征向业务服务端发起针对所述目标业务的安全认证
103
响应于所述业务服务端返回的所述安全认证通过的结果，与所述业务服务端执行业务交互完成所述目标业务
104

图1

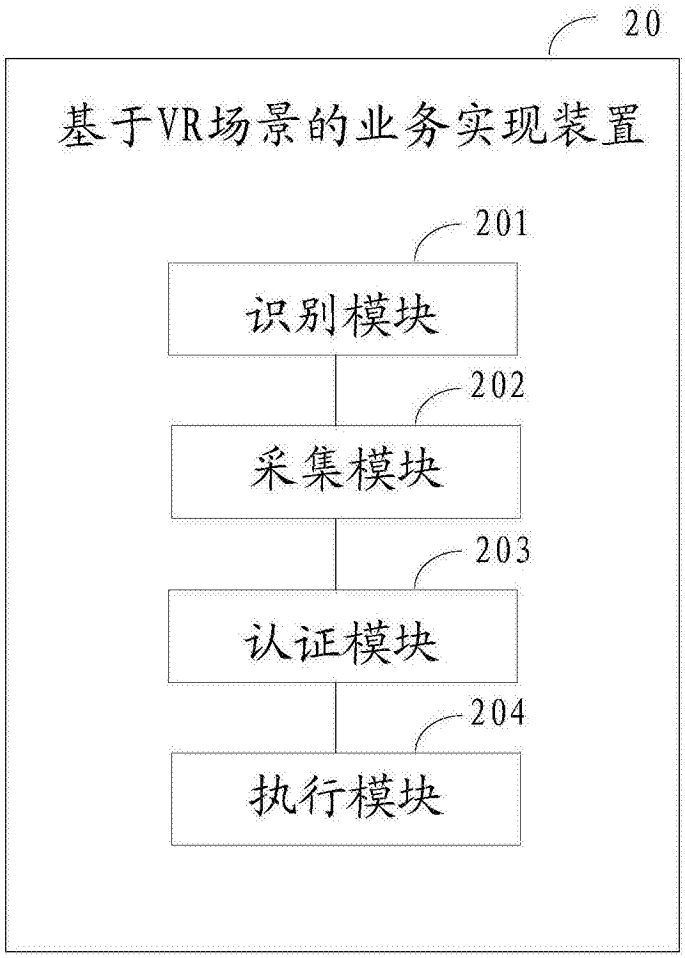


图2

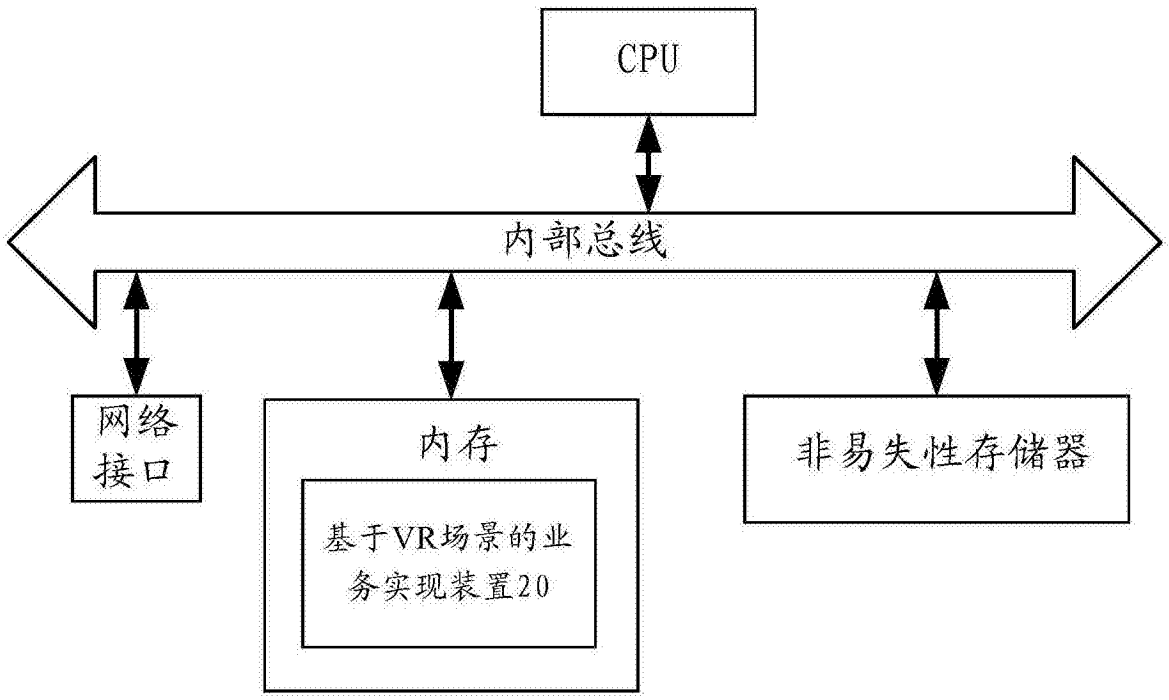


图3