

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 3 月 21 日 (21.03.2019)



(10) 国际公布号
WO 2019/052414 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2018/104774

(22) 国际申请日: 2018 年 9 月 10 日 (10.09.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710826063.6 2017年9月14日 (14.09.2017) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛
大开曼资本大厦一座四层 847 号 邮箱,
Grand Cayman (KY)。

(72) 发明人: 及

(71) 申请人 (仅对US): 赵豪(ZHAO, Hao) [CN/CN]; 中国浙江省杭州市余杭区文一西路969号3号楼5楼
阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司(CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲2号渔阳置业大厦B座605, Beijing 100029 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,

(54) Title: AUTHENTICATION METHOD, DEVICE, VR TERMINAL AND VR SERVER BASED ON VR SCENE

(54) 发明名称: 基于VR场景的认证方法、装置、VR终端及VR服务端

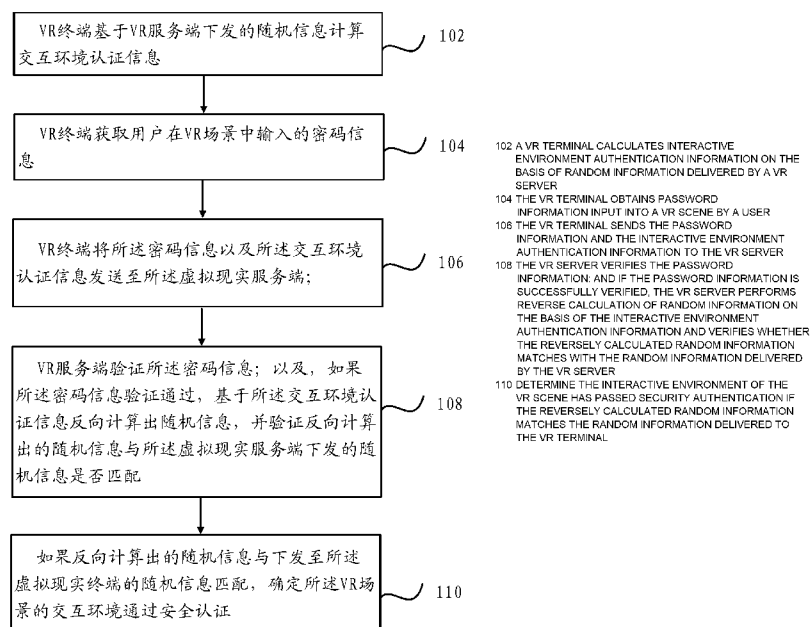


图 1

(57) Abstract: The present specification provides an authentication method based on a VR scene comprising: calculating interactive environment authentication information on the basis of random information delivered by a VR server; and obtaining password information input into the VR scene by a user; sending the password information and the interactive environment authentication information to the VR server, such that the VR server performs reverse calculation of the random information on the basis of the interactive environment authentication information after the password information has been verified, and matches the reversely calculated random information against the random information delivered to the VR client in order to perform security authentication on the interactive environment of the VR scene.

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告 (条约第21条(3))。

(57) 摘要: 本说明书提供一种基于VR场景的认证方法, 包括: 基于虚拟现实服务端下发的随机信息计算交互环境认证信息; 以及, 获取用户在虚拟现实场景中输入的密码信息; 将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端, 以由所述虚拟现实服务端在所述密码信息验证通过后, 基于所述交互环境认证信息反向计算出随机信息, 并将反向计算出的所述随机信息与向虚拟现实客户端下发的随机信息进行匹配, 以对所述虚拟现实场景的交互环境进行安全认证。

基于 VR 场景的认证方法、装置、VR 终端及 VR 服务端

技术领域

本说明书涉及计算机应用领域，尤其涉及一种基于虚拟现实场景的认证方法、装置、VR 终端设备以及 VR 服务端设备。

5 背景技术

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。由于 VR 交互的特点是能够接管用户的全部视野，面向用户提供“沉浸式体验”，因此 VR 技术是目前比较受关注的用户和机器交互方式，
10 很多互联网企业都在积极扩展和自己相关的 VR 业务场景；比如，VR 购物、VR 支付、VR 娱乐，等等。

发明内容

本说明书提出一种基于虚拟现实场景的认证方法，应用于虚拟现实终端，所述方法包括：

15 基于虚拟现实服务端下发的随机信息计算交互环境认证信息；以及，
获取用户在虚拟现实场景中输入的密码信息；

将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端，
以由所述虚拟现实服务端在所述密码信息验证通过后，基于所述交互环境认证信息反向计算出随机信息，并将反向计算出的所述随机信息与向虚拟现实
20 客户端下发的随机信息进行匹配，以对所述虚拟现实场景的交互环境进行安全认证。

本说明书还提出一种基于虚拟现实场景的认证方法，应用于虚拟现实服务端，所述方法包括：

获取虚拟现实终端发送的交互环境认证信息以及用户在虚拟现实场景中
25 输入的密码信息；其中，所述交互环境认证信息基于下发至所述虚拟现实终

端的随机信息计算生成;

验证所述密码信息; 以及, 如果所述密码信息验证通过, 基于所述交互环境认证信息反向计算出随机信息, 并验证反向计算出的随机信息与所述虚拟现实服务端下发的随机信息是否匹配;

- 5 如果反向计算出的随机信息与下发至所述虚拟现实终端的随机信息匹配, 确定所述虚拟现实场景的交互环境通过安全认证。

本说明书还提出一种基于虚拟现实场景的认证装置, 应用于虚拟现实终端, 所述装置包括:

计算模块, 基于虚拟现实服务端下发的随机信息计算交互环境认证信息;

10 以及,

第一获取模块, 获取用户在虚拟现实场景中输入的密码信息;

发送模块, 将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端, 以由所述虚拟现实服务端在所述密码信息验证通过后, 基于所述交互环境认证信息反向计算出随机信息, 并将反向计算出的所述随机信息
15 与向虚拟现实客户端下发的随机信息进行匹配, 以对所述虚拟现实场景的交互环境进行安全认证。

本说明书还提出一种基于虚拟现实场景的认证装置, 应用于虚拟现实服务端, 所述装置包括:

第二获取模块, 获取虚拟现实终端发送的交互环境认证信息以及用户在
20 虚拟现实场景中输入的密码信息; 其中, 所述交互环境认证信息基于下发至所述虚拟现实终端的随机信息计算生成;

验证模块, 验证所述密码信息; 以及, 如果所述密码信息验证通过, 基于所述交互环境认证信息反向计算出随机信息, 并验证反向计算出的随机信息与所述虚拟现实服务端下发的随机信息是否匹配;

25 确定模块, 如果反向计算出的随机信息与下发至所述虚拟现实终端的随机信息匹配, 确定所述虚拟现实场景的交互环境通过安全认证。

本说明书还提出一种虚拟现实终端设备, 包括:

处理器；

用于存储机器可执行指令的存储器；

其中，通过读取并执行所述存储器存储的与机器学习模型的训练的控制逻辑对应的机器可执行指令，所述处理器被促使：

- 5 基于虚拟现实服务端下发的随机信息计算交互环境认证信息；以及，
获取用户在虚拟现实场景中输入的密码信息；

将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端，
以由所述虚拟现实服务端在所述密码信息验证通过后，基于所述交互环境认
证信息反向计算出随机信息，并将反向计算出的所述随机信息与向虚拟现实
10 客户端下发的随机信息进行匹配，以对所述虚拟现实场景的交互环境进行安全认证。

本说明书还提出一种虚拟现实服务端设备，包括：

处理器；

用于存储机器可执行指令的存储器；

- 15 其中，通过读取并执行所述存储器存储的与机器学习模型的训练的控制逻辑对应的机器可执行指令，所述处理器被促使：

获取虚拟现实终端发送的交互环境认证信息以及用户在虚拟现实场景中
输入的密码信息；其中，所述交互环境认证信息基于下发至所述虚拟现实终
端的随机信息计算生成；

- 20 验证所述密码信息；以及，如果所述密码信息验证通过，基于所述交互环境认证信息反向计算出随机信息，并验证反向计算出的随机信息与所述虚拟现实服务端下发的随机信息是否匹配；

如果反向计算出的随机信息与下发至所述虚拟现实终端的随机信息匹配，
确定所述虚拟现实场景的交互环境通过安全认证。

- 25 在本说明书中，实现了虚拟现实服务端在基于用户输入的密码信息完成用户身份认证的基础上，可以进一步基于与密码信息同步发送的交互环境认证信息，对虚拟现实场景的交互环境进行安全认证，来确定当前的交互环境

是否为合法的交互环境，进而可以降低用户在非法的 VR 交互环境中进行业务交互而面临的安全性风险。

附图说明

图 1 是本说明书一实施例示出的一种基于 VR 场景的认证方法的流程图；

5 图 2 为本说明书示出的一种用户在输入密码字符后对操作焦点进行偏移的示意图；

图 3 是本说明书一实施例示出的一种用户在 VR 场景中完成快捷支付的交互示意图；

图 4 是本说明书一实施例示出的一种 VR 终端与 VR 服务端进行交互完
10 成 VR 支付环境的安全认证的示意图；

图 5 是本说明书一实施例提供的承载一种基于 VR 场景的认证装置的 VR 终端所涉及的硬件结构图；

图 6 是本说明书一实施例提供的一种基于 VR 场景的认证装置的逻辑框图；

15 图 7 是本说明书一实施例提供的承载另一种基于 VR 场景的认证装置的 VR 服务端所涉及的硬件结构图；

图 8 是本说明书一实施例提供的另一种基于 VR 场景的认证装置的逻辑框图。

具体实施方式

20 在实际应用中，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，在 VR 场景中完成信息输入通常会存在困难；因而，越来越多的 VR 终端设备，开始面向用户提供一些更加人性化的信息输入方式；

例如，以头戴式的 VR 终端设备为例，当用户需要在 VR 场景中执行信
25 息输入密码时，通常可以在 VR 场景中输出一个包含若干输入字符的输入界

面，而用户则可以通过头部动作与 VR 场景进行交互，来控制 VR 场景中的视觉焦点（即操作焦点），通过视觉焦点来触发选中输入界面中相关的输入字符，进而完成该输入字符的输入操作；比如，在一种实现方式中，用户通过可以将视觉焦点停留在输入界面中相关的输入字符一定时长来选中该输入字符（也可以通过其它的交互方式来选中，本说明书中对选中方式不进行限定），然后触发完成该输入字符的输入操作。

而随着 VR 技术的不断普及，VR 技术在面向用户提供“沉浸式体验”的同时，由于 VR 技术具有接管用户的全部视野的特点，一旦 VR 终端的用户视野（即通过用户佩戴 VR 终端向用户输出的可视化 3D 界面）被恶意的程序劫持后，用户在 VR 场景中输入的诸如密码信息等隐私信息就有可能面临泄露的风险；而且，由于 VR 场景中的用户视野，不同于传统 APP 的屏幕交互界面，如果用户视野被劫持，在 VR 场景下用户完全没有能力觉察到被劫持。因此，如何来准确识别出 VR 场景的 VR 交互环境是否合法，确保用户在 VR 场景中输入信息（尤其是一些诸如支付密码等隐私信息）的安全，则具有十分重要的意义。

有鉴于此，在本说明书中，提出一种在 VR 场景下，在基于用户输入的密码信息的基础上，进一步对用户当前所处的 VR 场景的交互环境进行安全认证的技术方案。

在实现时，VR 终端可以基于 VR 服务端下发的随机信息计算交互环境认证信息，并获取用户在虚拟现实场景中输入的密码信息，然后将所述密码信息和交互环境认证信息一起发送至 VR 服务端。

而 VR 服务端在收到 VR 终端发送的密码信息和交互环境认证信息后，可以首先对密码信息进行验证，并在所述密码信息验证通过后，基于所述交互环境认证信息反向计算出随机信息，然后通过将反向计算出的所述随机信息与向虚拟现实客户端下发的随机信息进行匹配，来对所述虚拟现实场景的交互环境进行安全认证；如果反向计算出的所述随机信息与向虚拟现实客户端下发的随机信息匹配，表明当前的 VR 场景的交互环境为合法的交互环境，

用户在当前的 VR 场景中的业务操作不存在安全风险；反之，如果反向计算出的所述随机信息与向虚拟现实客户端下发的随机信息不匹配，则表明当前的 VR 场景的交互环境为非法的交互环境，用户在当前的 VR 场景中的业务操作存在安全风险。

5 通过这种方式，实现了虚拟现实服务端在基于用户输入的密码信息完成用户身份认证的基础上，可以进一步基于与密码信息同步发送的交互环境认证信息，对用户执行密码信息输入的虚拟现实场景的交互环境进行安全认证，来确定当前的交互环境是否为合法的交互环境，进而可以降低用户在非法的 VR 交互环境中进行业务交互而面临的安全性风险。

10 例如，以在 VR 场景下的快捷支付业务为例，当用户在 VR 场景中通过输入支付密码完成一笔快捷支付交易时，如果用户佩戴的 VR 终端被恶意程序劫持（比如基于 VR 场景的钓鱼、诈骗、页面劫持等攻击行为），此时用户在 VR 场景中发起的支付交易就有可能面临安全风险；比如，用户输入的支付密码泄露，或者将交易资金转入一个非法的账户造成经济损失等。在这
15 种情况下，如果 VR 服务端能够基于 VR 终端发送的交互环境认证信息，在后台准确识别出当前 VR 场景的交互环境是否合法，则能够及时的终止用户在 VR 场景中发起的支付交易，降低用户在 VR 场景中发起的支付交易的安全性风险。

下面通过具体实施例并结合具体的应用场景对本说明书进行描述。

20 请参考图 1，图 1 是本说明书一实施例提供的一种基于虚拟现实场景的认证方法，执行以下步骤：

步骤 102，VR 终端基于 VR 服务端下发的随机信息计算交互环境认证信息；

步骤 104，VR 终端获取用户在 VR 场景中输入的密码信息；

25 其中，需要说明的是，上述步骤 102 和步骤 104 的执行顺序可以互换。

上述 VR 终端，包括任意形态的可以面向用户提供 VR 三维沉浸体验的终端设备；比如，头戴式的 VR 终端设备。

其中，在上述 VR 终端上，可以预先搭载基于 VR 技术开发的客户端软件（比如 APP）或者操作系统，VR 终端可以通过搭载的客户端软件或者操作系统，将开发人员预先开发的 VR 场景模型向用户输出，从而使得佩戴 VR 终端的用户，能够在 VR 场景中得到三维沉浸体验。

5 同时，在上述 VR 终端上，还可以搭载相关的传感器，并通过搭载的这些传感器来检测用户在 VR 场景中执行的交互操作，进而可以基于感应到的交互操作来理解用户的意图，实现用户与 VR 场景之间的交互；

例如，在实际应用中，VR 终端可以内置重力传感器和加速度传感器，并通过内置的重力传感器和加速度传感器来跟踪和识别用户的头部动作，进而可以理解用户的意图，与用户进行交互；而对于用户而言，在佩戴 VR 终端的过程中，可以通过头部动作控制 VR 场景中的操作焦点（即视觉焦点）的移动，在 VR 场景中触发相应的动作与 VR 场景进行交互；比如，用户可以通过头部动作控制视觉焦点的移动，将视觉焦点停留在 VR 场景中提供的虚拟元素（比如虚拟按钮）上一定时长，来选中该虚拟元素，并触发与该虚拟元素对应的执行动作。

10
15

在说明书中，用户在 VR 场景中进行沉浸体验的过程中，可以通过在 VR 场景中执行特定的交互操作，与 VR 场景进行交互，来触发目标业务；其中，上述目标业务具体可以包括需要对用户身份进行认证的业务；比如，上述目标业务可以包括任意形式的需要用户输入密码信息对自身身份进行认证的安全性业务。

20

而对于 VR 终端而言，可以预先定义若干种用于在 VR 场景中触发目标业务的预设交互操作。当用户在与 VR 场景进行交互的过程中，VR 终端可以通过搭载的传感器来检测用户所执行的交互操作，并确定检测到的交互操作是否匹配上述预设交互操作。如果检测到的交互操作匹配上述预设交互操作，则可以立即在 VR 场景中触发目标业务。

25

其中，需要说明的是，以上描述的用于在 VR 场景中触发目标业务的预设交互操作，可以涵盖在 VR 领域中任意类型的交互方式，在本说明书不进

行特别限定。

例如，在一种实施方式中，上述目标业务具体可以是基于 VR 场景的快捷支付业务；在这种情况下，可以在 VR 场景中提供一个用于发起支付的“支付”按钮，而上述预设交互操作则可以是用户通过控制操作焦点的移动，来选中该“支付”按钮的操作；比如，在一种通用的交互方式中，用户可以通过头部动作控制视觉焦点的移动，将视觉焦点停留该“支付”按钮上一定时长，来选中该“支付”按钮，进而触发在 VR 场景中的快捷支付业务。

在本说明书中，当 VR 终端检测到用户在虚拟现实场景中触发了目标业务时，可以向 VR 服务端发送一个业务请求。而在 VR 服务端一侧，可以预先搭建一个用于生成随机信息的随机算法，当 VR 服务端收到 VR 终端发送的一个业务请求后，可以基于该随机算法生成一个随机信息，然后将该随机信息加密下发至 VR 客户端。

当 VR 客户端在收到 VR 服务端加密下发的随机信息后：

一方面，可以对该随机信息进行解密并存储，然后将该随机信息作为计算参数，来计算交互环境认证信息；

另一方面，可以在 VR 场景中输出一个密码输入界面，用户可以与 VR 场景进行交互，通过控制操作焦点的位移（比如，用户可以通过头部动作与 VR 场景进行交互来控制操作焦点的位移），来触发选中密码输入界面中的输入字符，进而完成该输入字符的输入操作。

其中，为了保证密码输入安全，该密码输入界面具体可以是一个由 VR 服务端动态下发的密码输入界面；

例如，上述密码输入界面具体可以是一个由 VR 服务端下发的随机密码输入界面；比如，该随机密码输入界面具体可以是一个包含的输入字符随机的输入界面、界面大小随机的输入界面、所包含的输入字符的大小随机的输入界面、在虚拟现实场景中的展示位置随机的输入界面、以及在虚拟现实场景中的倾斜角度随机的输入界面，等等。

其中，需要说明的是，用户通过与 VR 场景进行交互，来选中密码输入

界面中的输入字符的交互方式，不进行特别限定，在实际应用中，可以包括任意形式的交互方式；例如，在一种实现方式中，用户可以通过将操作焦点停留在输入界面中相关的输入字符一定时长来选中该输入字符，然后触发完成该输入字符的输入操作。

5 在本说明书中，上述交互环境认证信息具体可以是一种隐藏的不可伪造的安全标记，用于标记官方可信的 VR 交互环境。其中，上述随机信息具体可以包括任意形式具有随机性的信息；相应的，上述交互环境认证信息具体也可以涵盖任意形式的基于 VR 服务端下发的随机信息计算生成的不可伪造的安全性信息。

10 在示出的一种实施方式中，上述随机信息可以是预设长度的随机数串；而上述交互环境认证信息则可以是基于上述随机数串映射计算生成的坐标序列；其中，上述坐标序列，具体可以包括用户在与 VR 场景进行交互的过程，操作焦点发生位移时产生的一系列坐标的集合。

15 在这种情况下，在 VR 终端上可以预先搭载用于对随机数串进行映射计算的映射算法，当对 VR 服务端下发的随机数串解密完成后，可以基于该随机算法对该随机数串中的随机数，分别进行映射计算，生成与该随机数串中的随机数分别对应的各映射坐标。

20 其中，对于生成的各映射坐标，可以分别对应用户需要在 VR 场景下输入的密码信息中的一个密码字符；例如，以上述目标业务为快捷支付业务，上述密码信息为 6 位的支付密码为例，在这种情况下，可以通过上述映射算法将上述随机数串中的随机数映射为 6 个与密码字符对应的映射坐标。

其中，需要说明的是，上述映射算法的计算逻辑在本说明书中不进行特别限定，在实际应用中，本领域技术人员可以基于实际的需求来定义；

25 在示出的一种实现方式中，以上述目标业务为 VR 场景下的快捷支付业务，上述密码信息为支付密码为例，上述映射算法则可以是将上述随机数串中的每两位随机数，映射为一个与支付密码中的一个密码字符相对应的映射坐标的算法。即在本说明书中，用于生成上述映射坐标的随机数串的长度取

决于密码信息的字符长度，二者将保持一种相对的关系。

在这种情况下，上述映射算法具体可以用以下公式来表征：

$$x=(\text{int}(\text{challenge}[i*2]) - 4)/10;$$

$$y=(\text{int}(\text{challenge}[i*2+1]) - 4)/10;$$

5 其中， x 表示所述映射坐标的 x 轴坐标值； y 表示所述映射坐标的 y 轴坐标值； challenge 表示上述随机数串； $\text{challenge}[N]$ 表示上述随机数串中的第 N 个数字；比如， $\text{challenge}[i*2]$ 表示上述随机数串中的第 $i*2$ 个随机数； i 的取值范围为 $[0, M-1]$ ；其中， $\text{challenge}[0]$ ，表示上述随机数串中的第一个随机数； M 的取值为所述随机数串的长度值的二分之一（即每两位随机数映射
10 为一个映射坐标）。

例如，以支付宝（Alipay）在 VR 场景下的快捷支付业务为例，支付宝在 VR 场景下的支付密码为 6 位短密码，那么上述随机数串则可以是一个 12 位的随机数字串。在一个例子中，假设上述随机数字串为 152587660579，那么基于上述公式， i 的取值范围为 $[0, 5]$ ，此时可以将 i 在 0~5 之间的每一个
15 数分别代入到上述公式中进行映射计算，得到的映射坐标可以是对该随机数串中的随机数分别进行映射计算，得到计算结果可以如下表所示：

i	$\text{challenge}[i*2]$	$\text{challenge}[i*2+1]$	result
0	$\text{challenge}[0]$	$\text{challenge}[1]$	$[-0.3, 0.1]$
1	$\text{challenge}[2]$	$\text{challenge}[3]$	$[-0.2, 0.1]$
2	$\text{challenge}[4]$	$\text{challenge}[5]$	$[0.4, 0.3]$
3	$\text{challenge}[6]$	$\text{challenge}[7]$	$[0.2, 0.2]$
4	$\text{challenge}[8]$	$\text{challenge}[9]$	$[-0.4, 0.1]$
5	$\text{challenge}[10]$	$\text{challenge}[11]$	$[0.3, 0.5]$

在示出的一种实施方式中，当 VR 终端基于上述映射算法对上述随机数串中的随机数分别进行映射计算，得到与上述密码信息中的各密码字符分别对应的映射坐标后，可以基于这些映射坐标进一步生成坐标序列作为上述交互环境认证信息。
20

其中，在示出的一种方式中，具体可以将通过上述映射计算得到的映射坐标与上述密码输入界面进行结合，将上述映射坐标作为操作焦点的偏移量，

来构建坐标序列作为上述交互环境认证信息。

在实现时，每当用户在上述密码输入界面中输入一个密码字符，VR 终端可以将该密码字符对应的映射坐标作为偏移量，对 VR 场景中的操作焦点执行一次偏移，并记录偏移后的操作焦点的坐标；以此类推，直到用户将完整的密码信息输入完成；例如，以上述密码信息为支付宝的 6 位的支付密码为例，此时操作焦点一共需要执行 6 次偏移，因而 VR 终端需要记录 6 个偏移后的操作焦点的坐标。

其中，为了确保在 VR 服务端一侧能够通过计算还原出上述偏移量，VR 终端可以为操作焦点在密码输入界面中定义一个固定的初始位置。

在这种情况下，每当用户在密码输入界面中输入一个密码字符后，VR 终端可以确定出该初始位置的初始位置坐标，然后将与用户输入的该密码字符对应的映射坐标作为偏移量，对该初始位置坐标执行一次偏移；比如，可以将该初始位置坐标的 X 轴坐标值和 Y 轴坐标值分别作为 X 轴和 Y 轴的偏移分量，对操作焦点的坐标进行偏移。其中，上述初始位置在密码输入界面中的具体位置，在本说明书中不进行特别限定，在实际应用中，上述密码输入界面中的任意位置均可以被定义为上述初始位置；

例如，在一种实现方式中，以用户通过将操作焦点停留在输入界面中相关的输入字符一定时长来选中该输入字符，然后触发完成该输入字符的输入操作的交互方式为例，在这种情况下，可以将该输入字符在密码输入界面中的位置区域的中心位置（即与该输入字符对应的输入按键的区域中心），或者其它便于提取识别的位置定义为上述初始位置；从而，当用户通过控制操作焦点在该输入字符所在的位置区域中提留，触发了该输入字符的输入后，VR 终端可以立即将操作焦点停留到该初始位置，然后从以该初始位置为偏移基准点执行一次偏移，然后记录偏移后的操作焦点的坐标。

其中，VR 终端在对操作焦点进行偏移时的偏移方向，在本说明书中也不进行特别限定，在实际应用中，可以将与用户输入的密码字符对应的映射坐标作为偏移量，对操作焦点执行任意方向的偏移。

例如，请参见图 2，图 2 为本说明书示出的一种用户在输入密码字符后对操作焦点进行偏移的示意图；

如图 2 所示，以上述密码信息为支付宝的 6 位的支付密码为例，假设 6 位支付宝密码为 123456，作为上述交互环境认证信息的坐标序列为：

5 $\{[-0.3, 0.1], [-0.2, 0.1], [0.4, 0.3], [0.2, 0.2], [-0.4, 0.1], [0.3, 0.5]\}$

此时，以上坐标序列中的各坐标分别对应 6 位支付密码中的一个密码字符对应。

假设上述 6 位支付密码中的第一密码字符 1 与映射坐标 $[-0.3, 0.1]$ 对应，当用户控制操作焦点移动到密码输入界面中输入字符 1 所在区域，并触发选
10 中该输入字符 1 完成密码字符 1 的输入后，此时用户佩戴的 VR 终端可以在后台读取该操作焦点在密码输入界面中的初始位置坐标，然后将映射坐标 $[-0.3, 0.1]$ 的 X 轴取值 -0.3 作为操作焦点的 X 轴的偏移分量，将映射坐标 $[-0.3, 0.1]$ 的 Y 轴取值 0.1 作为操作焦点的 Y 轴的偏移分量，在 VR 场景的坐标系中对该初始位置坐标执行一次偏移，将该初始位置坐标的 X 轴的取值，在
15 VR 场景的坐标系中向 X 轴的负方向偏移 0.3 个单位；以及，将该初始位置坐标的 Y 轴的取值，在 VR 场景的坐标系中向 Y 轴的正方向偏移 0.1 个单位。后续，用户在继续输入上述 6 位支付密码中的第二个密码字符 2 时，可以继续控制操作焦点，从输入了密码字符 1 后操作焦点的偏移后的位置，移动到密码输入界面中输入字符 2 所在的区域，继续完成密码字符 2 的输入，以此
20 类推，直到 6 位支付密码输入完成。

在本说明书中，当用户在上述密码输入界面中完成密码信息的输入后，VR 终端可以对已经记录的各偏移后的操作焦点的坐标进行拼接，得到一个坐标序列；比如，可以直接按照各偏移后的操作焦点对应的密码字符在密码信息中的顺序对各偏移后的操作焦点的进行拼接。此时，生成的该坐标序列，
25 即为最终需要提交给服务端进行验证的交互环境认证信息。

通过这种方式，一方面，由于上述映射坐标是基于服务端下发的随机数串计算生成，因此用户在密码输入界面中输入了密码字符后，将与该密码字

符对应的映射坐标作为偏移量，对操作焦点执行一次偏移，相当于对操作焦点执行了一次随机的偏移；因此，可以避免非法用户通过发起重建攻击来窃取用户在密码输入界面中输入的密码信息；

例如，所谓重建攻击，是指非法用户通过非法窃取用户在 VR 场景中执行信息输入的过程中，产生的交互数据（比如用户的头部动作数据），还原出操作焦点在 VR 场景中的位置以及轨迹，进而可以基于已经掌握的密码输入界面中输入字符的布局信息，还原出用户输入的密码字符的攻击手段。由于每当用户在密码输入界面中输入了密码字符后，操作焦点都会执行一次随机的偏移，因此即便非法用户成功窃取到用户在 VR 场景中执行信息输入的过程中，所产生的交互数据，最终还原出的视觉焦点的位置，也仍然与视觉焦点的实际位置存在差异，进而无法基于窃取到的交互数据还原出视觉焦点真实的移动轨迹，可以显著降低通过重建攻击成功窃取到用户输入的密码信息的成功率。

另一方面，通过将上述映射坐标作为操作焦点的偏移量对操作焦点进行偏移，并基于记录的偏移后的操作焦点的坐标，来构建坐标序列作为上述交互环境认证信息的方式，可以避免直接基于生成的映射坐标来构建坐标序列作为交互环境认证信息而面临的安全性风险；

例如，直接将生成的映射坐标进行拼接生成的坐标序列作为交互环境认证信息，相当于对上述映射算法的计算结果不进行任何处理，因此如果直接对通过上述映射算法计算出的各映射坐标进行拼接得到的坐标序列作为交互环境认证信息发送给 VR 服务端，一旦上述映射算法发生泄露，非法用户掌握了上述映射算法，那么就可以通过该映射算法对该交互环境认证信息进行反向计算，还原出 VR 服务端下发的上述随机数串，从而造成安全性风险。

以上以上述交互环境认证信息是基于上述随机数串映射计算生成的坐标序列为例进行了详细说明；

其中，需要补充说明的是，在实际应用中，上述交互环境认证信息除了可以是基于上述随机数串进行映射计算生成的坐标序列以外，也可以是其它

形态的用于标记官方可信的 VR 交互环境的安全性信息；比如，上述交互环境认证信息也可以是基于上述随机信息计算生成的图像、声音等信息，在本说明书中不再进行一一列举。

步骤 106, VR 终端将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端；

在本说明书中，当用户通过与 VR 场景进行交互，在密码输入界面中完成了密码信息的输入；并且，VR 终端基于 VR 服务端下发的随机信息计算生成了交互环境认证信息后，可以获取用户输入完成的密码信息，以及 VR 终端在后台计算生成的交互环境认证信息，然后将获取到的密码信息以及交互环境认证信息发送给 VR 服务端。

例如，以上述交互环境认证信息为基于上述随机信息映射计算生成的坐标序列为例，VR 终端可以将获取到的密码信息和上述坐标序列进行整合生成一个坐标序列串，携带在构建完成的一个响应请求中，返回给 VR 服务端，作为 VR 服务端下发的随机信息的应答。

其中，在实际应用中，VR 终端将获取到的密码信息以及上述交互环境认证信息发送至 VR 服务端时，也可以对该密码信息和上述交互环境认证信息进行加密发送，再由 VR 服务端进行解密；其中，具体的加密方式以及加密算法，在本说明书中不再进行详述。

步骤 108, VR 服务端验证所述密码信息；以及，如果所述密码信息验证通过，基于所述交互环境认证信息反向计算出随机信息，并验证反向计算出的随机信息与所述虚拟现实服务端下发的随机信息是否匹配；

步骤 110, 如果反向计算出的随机信息与下发至所述虚拟现实终端的随机信息匹配，确定所述 VR 场景的交互环境通过安全认证。

在本说明书中，VR 服务端在收到 VR 终端发送的密码信息和交互环境认证信息后，首先可以对该密码信息进行验证；例如，可以将该密码信息与用户在服 VR 服务端上预留的密码信息进行匹配；如果该密码信息验证通过，此时针对该用户的身份认证通过，VR 服务端可以进一步启动对上述交互环

境认证信息的验证。

当然，如果该密码信息验证失败，可以直接终止用户在 VR 场景中发起的上述目标业务，向 VR 终端返回一个业务执行失败的响应消息。

进一步的，当用户通过身份认证后，VR 服务端可以继续对上述交互环境认证信息进行验证，以对用户发起上述目标业务时所处的 VR 场景的交互环境进行安全认证。其中，VR 服务端对上述交互环境认证信息进行验证的过程，与 VR 终端生成上述交互环境认证信息的过程相对应。

在示出的一种实施方式中，仍以上述交互环境认证信息为基于上述预设的映射算法对 VR 服务端下发的上述随机数串得到的映射坐标，与上述密码输入界面进行结合，将上述映射坐标作为操作焦点的偏移量，构建出的坐标序列为例，

在这种情况下，所述交互环境认证信息为用户在虚拟现实场景中输入一个密码字符后，将与该密码字符对应的映射坐标作为偏移量，对所述虚拟现实场景中的操作焦点进行偏移，并拼接各偏移后的操作焦点的坐标得到的坐标序列。其中，上述映射坐标为上述 VR 终端基于上述预设的映射算法对上述随机数串中的随机数分别进行映射计算，生成的与上述随机数对应的映射坐标；各映射坐标分别对应用户输入的密码信息中的一密码字符。

首先，VR 服务端可以分别计算与作为交互环境认证信息的上述坐标序列中的坐标对应的偏移量；

具体的，VR 终端可以将预先定义的上述初始位置通告给 VR 服务端，而 VR 服务端在计算作为交互环境认证信息的上述坐标序列中的坐标对应的偏移量时，可以基于上述初始位置，结合 VR 服务端一侧维护的上述密码输入界面的布局信息，确定出该初始位置在密码输入界面中对应的坐标；此时，该坐标即为 VR 终端一侧的 VR 场景中的操作焦点偏移前在上述密码输入初始位置坐标。

例如，在一种实现方式中，以用户通过将操作焦点停留在输入界面中相关的输入字符一定时长来选中该输入字符，然后触发完成该输入字符的输入

操作的交互方式为例，在这种情况下，VR 终端可以将该输入字符在密码输入界面中的位置区域的中心位置定义为上述初始位置，并将该初始位置通告给 VR 服务端；而 VR 服务端在需要计算作为交互环境认证信息的上述坐标序列中的任一坐标对应的偏移量时，可以基于本地维护的上述密码输入界面的布局信息，确定出与该坐标对应的密码字符在密码输入界面中的位置区域（即与该输入字符对应的输入按键对应的位置区域），然后进一步确定出该位置区域的中心位置的坐标，得到上述初始位置坐标。

当 VR 终端确定出上述初始位置坐标后，可以基于该初始位置坐标以及作为交互环境认证信息的上述坐标序列中的坐标计算对应的偏移量；例如，上述初始位置坐标表征的是操作焦点偏移前的坐标，而上述坐标序列中的坐标表征的是操作焦点偏移后的坐标，因此通过计算操作焦点偏移后的坐标的 X 轴和 Y 轴的坐标取值，与操作焦点偏移前的坐标的 X 轴和 Y 轴的坐标取值，就能够得到操作焦点相对于 X 轴和 Y 轴的偏移量。

其中，由于上述偏移量即为 VR 终端基于上述预设的映射算法对上述随机数串进行映射计算得到的映射坐标，因此 VR 终端在计算出与作为交互环境认证信息的上述坐标序列中的坐标对应的偏移量后，即可以得到 VR 终端基于上述预设的映射算法对上述随机数串进行映射计算得到的原始映射坐标。

在本说明书中，在 VR 服务端一侧，也可以搭载与上述 VR 终端相同的映射算法；当 VR 服务端得到 VR 终端基于上述预设的映射算法对上述随机数串进行映射计算得到的原始映射坐标后，可以基于该相同的映射算法对与各密码字符对应的该原始映射坐标进行反向计算，生成与各原始映射坐标对应的随机数。

例如，仍以以下公式表征的映射算法为例：

$$x=(\text{int}(\text{challenge}[i*2]) - 4)/10;$$

$$y=(\text{int}(\text{challenge}[i*2+1]) - 4)/10;$$

其中，以上公式中各参数的含义，本说明书中不再进行详述；而基于上述映射算法对原始映射坐标进行反向计算，即为将原始映射坐标的 x 轴坐标

值和 y 轴坐标值代入上述公式,反向求解出 challenge[i*2]和 challenge[i*2+1]的过程,具体的计算过程本说明书中不再赘述。

在本说明书中,当通过以上反向计算求解出与各原始映射坐标对应的随机数后,VR 服务端可以将这些随机数进行拼接得到一个随机数串,然后将的得到的该随机数串与 VR 服务端下发至 VR 终端的随机数串进行匹配;如果得到的该随机数串与 VR 服务端下发至 VR 终端的随机数串匹配,表明用户发起上述目标业务时所处的 VR 场景的交互环境通过安全认证,该交互环境为官方可信的 VR 交互环境,此时 VR 服务端可以正常响应并执行 VR 终端发起的上述目标业务,并将业务执行结果反馈给 VR 终端。

反之,如果得到的该随机数串与 VR 服务端下发至 VR 终端的随机数串不匹配,则表明用户发起上述目标业务时所处的 VR 场景的交互环境为通过安全认证,该交互环境为非法的 VR 交互环境,此时该 VR 场景中的用户视野可能被恶意程序劫持,VR 服务端可以直接终止用户在 VR 场景中发起的上述目标业务,向 VR 终端返回一个业务执行失败的响应消息。

可见,通过这种方式,VR 服务端在基于用户输入的密码信息完成用户身份认证的基础上,可以进一步基于与密码信息同步发送的交互环境认证信息,对用户执行密码信息输入的 VR 场景的交互环境进行安全认证,来确定当前的交互环境是否为合法的交互环境,进而可以降低用户在非法的 VR 交互环境中进行业务交互而面临的安全性风险。

以下以上述目标业务为 VR 场景下的快捷支付业务为例,并结合用户在进行 VR 购物体验时,通过在 VR 场景中输出的密码输入界面中输入支付密码,在 VR 场景中进行快捷的安全支付的应用场景,对说明书的技术方案进行描述。

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,也可以应用在其它类似的业务场景中;

例如,用户在 VR 游戏的场景中,快捷的完成游戏币的充值;用户在 VR

直播场景中，快捷的完成打赏；用户在 VR 视频场景中，快捷的完成视频的支付点播；以及用户在 VR 场景中快捷的完成 VR 终端的解锁，等等；在本例中不再一一列举。

在该场景下，上述 VR 终端，具体可以是搭载了基于 VR 技术开发的支付客户端（比如支付宝 VR pay）的头戴式 VR 终端；上述 VR 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。

请参见图 3，图 3 为本说明书示出的一种用户在 VR 场景中完成快捷支付的交互示意图。

在初始状态下，用户可以使用支付账号登录该 VR 终端，并通过在该 VR 终端输出的 VR 场景中设置支付密码，并将设置的支付密码与支付账号进行绑定，存储至云端的支付服务端一侧的安全数据库中。

当该用户在佩戴 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。

请继续参见图 3，当用户在上述商品列表中，选择了一件满意的商品后，可以通过头部动作控制操作焦点的交互方式，通过将视觉焦点在悬浮停留在 VR 场景中预先提供的“立即购买”按钮所在区域之上，并保持停留 N 秒，来触发 VR 客户端启动针对该商品的支付流程。

请参见图 4，图 4 为本说明书示出一种 VR 终端与 VR 服务端进行交互完成 VR 支付环境的安全认证的示意图。

如图 4 所示，当针对该商品的支付流程启动后，此时 VR 终端可以通过搭载的支付客户端向 VR 服务端发起一个支付请求。而上述 VR 服务端在收到上述支付请求后，可以基于搭载的随机算法为 VR 终端生成一个 12 位的随机数串，并将该随机数串加密下发至 VR 终端。

而上述 VR 终端在收到该随机数串后，可以对该随机数串进行解密，并基于搭载的映射算法对该随机数串中的随机数分别进行映射计算，得到 6 个与支付密码中的每一个密码字符分别对应的映射坐标（仍以每两位随机数映

射为一个映射坐标为例)。

请继续参见图 4, 当 VR 终端完成上述映射计算, 可以通过 VR 场景输出由 VR 服务端下发的密码输入框, 并获取用户在该密码输入框中输入的密码字符; 同时, 还可以将计算得到的映射坐标与 VR 服务端下发的密码输入框
5 进行结合, 将上述映射坐标作为操作焦点的偏移量, 来构建坐标序列作为交互环境认证信息。

具体地, VR 终端仍然可以采用每当用户在上述密码输入界面中输入一个密码字符, 将该密码字符对应的映射坐标作为偏移量, 对 VR 场景中的操作焦点执行一次偏移, 并记录偏移后的操作焦点的坐标, 然后对记录的偏移
10 后的操作焦点的坐标进行拼接得到坐标序列作为上述交互环境认证信息的方式, 具体的详细实施过程不再赘述, 可以参考之前实施例的记载。

请继续参见图 4, 当 VR 终端获取到用户输入的支付密码, 以及完成了上述交互环境认证信息的构建后, 可以将上述支付密码和上述交互环境认证信息作为对 VR 服务端下发的随机数串的应答发送给服务端, 由服务端进行
15 验证。

一方面, 服务端首先可以对支付密码进行验证; 如果支付密码验证失败, 可以直接向 VR 终端返回支付失败;

另一方面, 如果支付密码验证通过, 服务端可以进一步对上述交互环境认证信息进行验证。首先, VR 服务端可以通过分别计算与上述交互环境认证信息中的各坐标对应的偏移量, 来消除交互环境认证信息中的各坐标由于
20 操作焦点偏移导致的坐标误差, 还原出与支付密码中的各密码字符对应的原始映射坐标; 其次, 可以进一步基于与 VR 客户端相同的映射算法, 对各原始映射坐标进行反向计算, 得到对应的随机数, 并对得到的随机数进行拼接得到随机数串, 具体的详细实施过程不再赘述, 可以参考之前实施例的记载。

25 当 VR 服务端通过对得到的随机数进行拼接得到随机数串后, 可以将该随机数串与下发至 VR 终端的随机数串进行匹配; 请继续参见图 3 如果得到的该随机数串与 VR 服务端下发至 VR 终端的随机数串匹配, 表明用户发起

上述快捷支付业务时所处的 VR 交互环境为官方可信的 VR 交互环境，此时 VR 服务端可以正常响应并执行 VR 终端发起的上述支付请求，并将支付结果反馈给 VR 终端，由 VR 终端在 VR 场景中向用户输出。

反之，如果得到的该随机数串与 VR 服务端下发至 VR 终端的随机数串
5 不匹配，则表明用户发起上述快捷支付业务时所处的 VR 交互环境可能为非法的 VR 交互环境，此时该 VR 场景中的用户视野可能被非法用户劫持，VR 终端通过 VR 场景输出的购物界面可能是一个钓鱼、诈骗界面，在这种情况下，VR 服务端可以直接终止用户在 VR 场景中发起的上述快捷支付业务，并通过 VR 终端在 VR 场景中向用户输出相应的提示；比如，该提示可以是一
10 条“该笔交易存在安全风险，系统已经帮您终止了该笔交易”的文本提示。

可见，通过这种方式，使得用户在 VR 场景中完成快捷支付时，VR 服务端可以在基于用户输入的密码信息完成用户身份认证的基础上，可以进一步基于与密码信息同步发送的交互环境认证信息，对用户执行密码信息输入的 VR 场景的交互环境进行安全认证，来快速发现用户在 VR 场景下进行快捷支付
15 时可能遭遇的钓鱼、诈骗等攻击行为，从而可以最大程度的保护用户的资金安全。

与上述方法实施例相对应，本说明书还提供了一种基于虚拟现实场景的认证装置的实施例。

本实施例中的基于 VR 场景的认证装置的实施例可以应用在 VR 终端上。
20 装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在 VR 终端的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 5 所示，为本说明书的基于 VR 场景的认证装置所在 VR 终端的一种硬件结构图，除了图 5 所示的处理器、传感器、内存、网络
25 接口、以及非易失性存储器之外，实施例中装置所在的 VR 终端通常根据该 VR 终端的实际功能，还可以包括其他硬件，对此不再赘述。

图 6 是本说明书一示例性实施例示出的一种基于 VR 场景的认证装置的

框图。

请参考图 6，所述基于虚拟现实场景的认证装置 60 可以应用在前述图 5 所示的 VR 终端中，包括有：计算模块 601、第一获取模块 602 以及发送模块 603。

5 其中，计算模块 601，基于虚拟现实服务端下发的随机信息计算交互环境认证信息；以及，

第一获取模块 602，获取用户在虚拟现实场景中输入的密码信息；

发送模块 603，将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端，以由所述虚拟现实服务端在所述密码信息验证通过后，基
10 于所述交互环境认证信息反向计算出随机信息，并将反向计算出的所述随机信息与向虚拟现实客户端下发的随机信息进行匹配，以对所述虚拟现实场景的交互环境进行安全认证。

在本实施例中，所述随机信息为预设长度的随机数串；所述交互环境认证信息为基于所述随机数串映射计算生成的坐标序列。

15 在本实施例中，所述计算模块 601：

基于预设的映射算法对所述随机数串中的随机数分别进行映射计算，生成与所述随机数分别对应的各映射坐标；所述各映射坐标作为每个密码字符对应的偏移量，用于在用户在虚拟现实场景中输入一个密码字符后，对所述虚拟现实场景中的操作焦点偏移该密码字符对应的偏移量；

20 拼接各偏移后的操作焦点的坐标得到所述坐标序列。

在本实施例中，所述计算模块 601 进一步：

确定所述虚拟现实场景中的操作焦点在密码输入界面中的初始位置坐标；
将与该密码字符对应的映射坐标作为偏移量，对所述初始位置坐标执行一次偏移。

25 在本实施例中，所述映射算法用如下公式表征：

$$x=(\text{int}(\text{challenge}[i*2]) - 4)/10;$$

$$y=(\text{int}(\text{challenge}[i*2+1]) - 4)/10;$$

其中， x 表示所述映射坐标的 x 轴坐标值； y 表示所述映射坐标的 y 轴坐标值； challenge 表示所述随机数串； $\text{challenge}[N]$ 表示所述随机数串中的第 N 个数字； i 的取值范围为 $[1, M]$ ； M 的取值为所述随机数串的长度值的二分之一。

5 与上述方法实施例相对应，本说明书还提供了另一种基于虚拟现实场景的认证装置的实施例。

本实施例中的基于 VR 场景的认证装置的实施例可以应用在 VR 服务端上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在 VR 服
10 务端的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 7 所示，为本说明书的基于 VR 场景的认证装置所在 VR 终端的一种硬件结构图，除了图 7 所示的处理器、传感器、内存、网络接口、以及非易失性存储器之外，实施例中装置所在的 VR 终端通常根据该 VR 终端的实际功能，还可以包括其他硬件，对此不再赘述。

15 图 8 是本说明书一示例性实施例示出的一种基于 VR 场景的认证装置的框图。

请参考图 8，所述基于虚拟现实场景的认证装置 80 可以应用在前述图 7 所示的 VR 终端中，包括有：第二获取模块 801、验证模块 802 以及确定模块 803。

20 其中，第二获取模块 801，获取虚拟现实终端发送的交互环境认证信息以及用户在虚拟现实场景中输入的密码信息；其中，所述交互环境认证信息基于下发至所述虚拟现实终端的随机信息计算生成；

验证模块 802，验证所述密码信息；以及，如果所述密码信息验证通过，基于所述交互环境认证信息反向计算出随机信息，并验证反向计算出的随机
25 信息与所述虚拟现实服务端下发的随机信息是否匹配；

确定模块 803，如果反向计算出的随机信息与下发至所述虚拟现实终端的随机信息匹配，确定所述虚拟现实场景的交互环境通过安全认证。

在本实施例中，所述随机信息为预设长度的随机数串；所述交互环境认证信息为基于所述随机数串映射计算生成的坐标序列。

在本实施例中，

所述交互环境认证信息为用户在虚拟现实场景中输入一个密码字符后，
5 将与该密码字符对应的映射坐标作为偏移量，对所述虚拟现实场景中的操作焦点进行偏移，并拼接各偏移后的操作焦点的坐标得到的坐标序列；其中，所述映射坐标为基于预设的映射算法对所述随机数串中的随机数分别进行映射计算，生成的与所述随机数分别对应的各映射坐标；

在本实施例中，所述验证模块 802：

10 分别计算与所述坐标序列中的坐标对应的偏移量，得到与所述密码信息中的各密码字符对应的映射坐标；

基于所述预设的映射算法对与各密码字符对应的原始映射坐标分别进行反向计算，生成与各映射坐标分别对应的随机数。

在本实施例中，所述验证模块 802 进一步：

15 确定所述虚拟现实场景中的操作焦点偏移前在所述密码输入界面中的初始位置坐标；

基于所述初始位置坐标以及所述坐标序列中的坐标计算对应的偏移量。

在本实施例中，所述映射算法用如下公式表征：

$$x=(\text{int}(\text{challenge}[i*2])-4)/10;$$

20 $y=(\text{int}(\text{challenge}[i*2+1])-4)/10;$

其中，x 表示所述映射坐标的 x 轴坐标值；y 表示所述映射坐标的 y 轴坐标值；challenge 表示所述随机数串；challenge[N]表示所述随机数串中的第 N 个数字；i 的取值范围为[1，M]；M 的取值为所述随机数串的长度值的二分之一。

25 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参

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说明书方案的目的。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。

上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是服务器、个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

与上述方法实施例相对应，本说明书还提供了一种 VR 终端设备的实施例。该 VR 终端设备包括：处理器以及用于存储机器可执行指令的存储器；其中，处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中，所述设备还可能包括外部接口，以能够与其他设备或者部件进行通信。

在本实施例中，通过读取并执行所述存储器存储的与数据库损坏的恢复的控制逻辑对应的机器可执行指令，所述处理器被促使：

基于虚拟现实服务端下发的随机信息计算交互环境认证信息；以及，
获取用户在虚拟现实场景中输入的密码信息；

将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端，以由所述虚拟现实服务端在所述密码信息验证通过后，基于所述交互环境认证信息反向计算出随机信息，并将反向计算出的所述随机信息与向虚拟现实客户端下发的随机信息进行匹配，以对所述虚拟现实场景的交互环境进行安全认证；

在本实施例中，所述随机信息为预设长度的随机数串；所述交互环境认证信息为基于所述随机数串映射计算生成的坐标序列。

在本实施例中，通过读取并执行所述存储器存储的与数据库损坏的恢复的控制逻辑对应的机器可执行指令，所述处理器还被促使：

基于预设的映射算法对所述随机数串中的随机数分别进行映射计算，生成与所述随机数分别对应的各映射坐标；所述各映射坐标作为每个密码字符
5 对应的偏移量，用于在用户在虚拟现实场景中输入一个密码字符后，对所述虚拟现实场景中的操作焦点偏移该密码字符对应的偏移量；

拼接各偏移后的操作焦点的坐标得到所述坐标序列。

在本实施例中，通过读取并执行所述存储器存储的与数据库损坏的恢复的控制逻辑对应的机器可执行指令，所述处理器还被促使：

10 确定所述虚拟现实场景中的操作焦点在密码输入界面中的初始位置坐标；
将与该密码字符对应的映射坐标作为偏移量，对所述初始位置坐标执行一次偏移。

在本实施例中，所述映射算法用如下公式表征：

$$x=(\text{int}(\text{challenge}[i*2])-4)/10;$$

15 $y=(\text{int}(\text{challenge}[i*2+1])-4)/10;$

其中，x 表示所述映射坐标的 x 轴坐标值；y 表示所述映射坐标的 y 轴坐标值；challenge 表示所述随机数串；challenge[N]表示所述随机数串中的第 N 个数字；i 的取值范围为[0，M-1]；M 的取值为所述随机数串的长度值的二分之一。

20 与上述方法实施例相对应，本说明书还提供了一种 VR 服务端的实施例。该 VR 服务端包括：处理器以及用于存储机器可执行指令的存储器；其中，处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中，所述设备还可能包括外部接口，以能够与其他设备或者部件进行通信。

在本实施例中，通过读取并执行所述存储器存储的与数据库损坏的恢复
25 的控制逻辑对应的机器可执行指令，所述处理器被促使：

获取虚拟现实终端发送的交互环境认证信息以及用户在虚拟现实场景中输入的密码信息；其中，所述交互环境认证信息基于下发至所述虚拟现实终

端的随机信息计算生成;

验证所述密码信息; 以及, 如果所述密码信息验证通过, 基于所述交互环境认证信息反向计算出随机信息, 并验证反向计算出的随机信息与所述虚拟现实服务端下发的随机信息是否匹配;

- 5 如果反向计算出的随机信息与下发至所述虚拟现实终端的随机信息匹配, 确定所述虚拟现实场景的交互环境通过安全认证。

在本实施例中, 所述随机信息为预设长度的随机数串; 所述交互环境认证信息为基于所述随机数串映射计算生成的坐标序列。

- 10 在本实施例中, 通过读取并执行所述存储器存储的与数据库损坏的恢复的控制逻辑对应的机器可执行指令, 所述处理器还被促使:

分别计算与所述坐标序列中的坐标对应的偏移量, 得到与所述密码信息中的各密码字符对应的映射坐标;

基于所述预设的映射算法对与各密码字符对应的映射坐标分别进行反向计算, 生成与各映射坐标分别对应的随机数;

- 15 拼接生成的各随机数得到所述随机数串。

在本实施例中, 通过读取并执行所述存储器存储的与数据库损坏的恢复的控制逻辑对应的机器可执行指令, 所述处理器还被促使:

确定所述虚拟现实场景中的操作焦点偏移前在所述密码输入界面中的初始位置坐标;

- 20 基于所述初始位置坐标以及所述坐标序列中的坐标计算对应的偏移量。

在本实施例中, 所述映射算法用如下公式表征:

$$x=(\text{int}(\text{challenge}[i*2]) - 4)/10;$$

$$y=(\text{int}(\text{challenge}[i*2+1]) - 4)/10;$$

- 25 其中, x 表示所述映射坐标的 x 轴坐标值; y 表示所述映射坐标的 y 轴坐标值; challenge 表示所述随机数串; $\text{challenge}[N]$ 表示所述随机数串中的第 N 个数字; i 的取值范围为 $[0, M-1]$; M 的取值为所述随机数串的长度值的二分之一。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、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说明书的一般性原理并包括本说明书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
5 实施例仅被视为示例性的，本说明书的真正范围和精神由下面的权利要求指出。

应当理解的是，本说明书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。本说明书的范围仅由所附的权利要求来限制。

10 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

15 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

权利要求书

1. 一种基于虚拟现实场景的认证方法，所述方法包括：

基于虚拟现实服务端下发的随机信息计算交互环境认证信息；以及，
获取用户在虚拟现实场景中输入的密码信息；

5 将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端，
以由所述虚拟现实服务端在所述密码信息验证通过后，基于所述交互环境认证信息反向计算出随机信息，并将反向计算出的所述随机信息与向虚拟现实客户端下发的随机信息进行匹配，以对所述虚拟现实场景的交互环境进行安全认证。

10 2. 根据权利要求 1 所述的方法，所述方法还包括：

当检测到用户在虚拟现实场景中触发了目标业务时，向所述虚拟现实服务端发送业务请求；

获取所述虚拟现实服务端在接收到所述业务请求时，下发的加密后的随机信息；以及，对获取到的随机信息进行解密。

15 3. 根据权利要求 1 所述的方法，所述随机信息为预设长度的随机数串；
所述交互环境认证信息为基于所述随机数串映射计算生成的坐标序列。

4. 根据权利要求 3 所述的方法，所述基于虚拟现实服务端下发的随机信息计算交互环境认证信息，包括：

20 基于预设的映射算法对所述随机数串中的随机数分别进行映射计算，生成与
所述随机数分别对应的各映射坐标；所述各映射坐标作为每个密码字符对应的偏移量，用于在用户在虚拟现实场景中输入一个密码字符后，对所述虚拟现实场景中的操作焦点偏移该密码字符对应的偏移量；

拼接各偏移后的操作焦点的坐标得到所述坐标序列。

25 5. 根据权利要求 4 所述的方法，对所述虚拟现实场景中的操作焦点偏移
该密码字符对应的偏移量，包括：

确定所述虚拟现实场景中的操作焦点在密码输入界面中的初始位置坐标；
将与该密码字符对应的映射坐标作为偏移量，对所述初始位置坐标执行

一次偏移。

6. 根据权利要求 2 所述的方法, 所述目标业务为基于虚拟现实场景的快捷支付业务。

7. 一种基于虚拟现实场景的认证方法, 应用于虚拟现实服务端, 所述方法包括:

获取虚拟现实终端发送的交互环境认证信息以及用户在虚拟现实场景中输入的密码信息; 其中, 所述交互环境认证信息基于下发至所述虚拟现实终端的随机信息计算生成;

验证所述密码信息; 以及, 如果所述密码信息验证通过, 基于所述交互环境认证信息反向计算出随机信息, 并验证反向计算出的随机信息与所述虚拟现实服务端下发的随机信息是否匹配;

如果反向计算出的随机信息与下发至所述虚拟现实终端的随机信息匹配, 确定所述虚拟现实场景的交互环境通过安全认证。

8. 根据权利要求 7 所述的方法, 所述方法还包括:

接收到所述虚拟现实终端在检测到用户在虚拟现实场景中触发了目标业务时发送的业务请求;

响应于接收到的业务请求, 生成所述随机信息; 以及,

将生成的随机信息加密后下发至所述虚拟现实终端。

9. 根据权利要求 7 所述的方法, 所述随机信息为预设长度的随机数串; 所述交互环境认证信息为基于所述随机数串映射计算生成的坐标序列。

10. 根据权利要求 9 所述的方法, 所述交互环境认证信息为用户在虚拟现实场景中输入一个密码字符后, 将与该密码字符对应的映射坐标作为偏移量, 对所述虚拟现实场景中的操作焦点进行偏移, 并拼接各偏移后的操作焦点的坐标得到的坐标序列; 其中, 所述映射坐标为基于预设的映射算法对所述随机数串中的随机数分别进行映射计算, 生成的与所述随机数分别对应的各映射坐标;

所述基于所述交互环境认证信息反向计算出随机信息, 包括:

分别计算与所述坐标序列中的坐标对应的偏移量，得到与所述密码信息中的各密码字符对应的映射坐标；

基于所述预设的映射算法对与各密码字符对应的映射坐标分别进行反向计算，生成与各映射坐标分别对应的随机数；

5 拼接生成的各随机数得到所述随机数串。

11. 根据权利要求 10 所述的方法，所述计算与所述坐标序列中的映射坐标分别对应的偏移量，包括：

确定所述虚拟现实场景中的操作焦点偏移前在所述密码输入界面中的初始位置坐标；

10 基于所述初始位置坐标以及所述坐标序列中的坐标计算对应的偏移量。

12. 根据权利要求 7 所述的方法，所述目标业务为基于虚拟现实场景的快捷支付业务。

13. 一种基于虚拟现实场景的认证装置，所述装置包括：

计算模块，基于虚拟现实服务端下发的随机信息计算交互环境认证信息；

15 以及，

第一获取模块，获取用户在虚拟现实场景中输入的密码信息；

发送模块，将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端，以由所述虚拟现实服务端在所述密码信息验证通过后，基于所述交互环境认证信息反向计算出随机信息，并将反向计算出的所述随机信息
20 与向虚拟现实客户端下发的随机信息进行匹配，以对所述虚拟现实场景的交互环境进行安全认证。

14. 根据权利要求 13 所述的装置，所述随机信息为预设长度的随机数串；所述交互环境认证信息为基于所述随机数串映射计算生成的坐标序列。

15. 根据权利要求 14 所述的装置，所述第一计算模块：

25 基于预设的映射算法对所述随机数串中的随机数分别进行映射计算，生成与所述随机数分别对应的各映射坐标；所述各映射坐标作为每个密码字符对应的偏移量，用于在用户在虚拟现实场景中输入一个密码字符后，对所述

虚拟现实场景中的操作焦点偏移该密码字符对应的偏移量；

拼接各偏移后的操作焦点的坐标得到所述坐标序列。

16. 根据权利要求 15 所述的装置，所述第一计算模块进一步：

确定所述虚拟现实场景中的操作焦点在密码输入界面中的初始位置坐标；

5 将与该密码字符对应的映射坐标作为偏移量，对所述初始位置坐标执行一次偏移。

17. 一种基于虚拟现实场景的认证装置，应用于虚拟现实服务端，所述装置包括：

第二获取模块，获取虚拟现实终端发送的交互环境认证信息以及用户在
10 虚拟现实场景中输入的密码信息；其中，所述交互环境认证信息基于下发至所述虚拟现实终端的随机信息计算生成；

验证模块，验证所述密码信息；以及，如果所述密码信息验证通过，基于所述交互环境认证信息反向计算出随机信息，并验证反向计算出的随机信息与所述虚拟现实服务端下发的随机信息是否匹配；

15 确定模块，如果反向计算出的随机信息与下发至所述虚拟现实终端的随机信息匹配，确定所述虚拟现实场景的交互环境通过安全认证。

18. 根据权利要求 17 所述的装置，所述随机信息为预设长度的随机数串；所述交互环境认证信息为基于所述随机数串映射计算生成的坐标序列。

19. 根据权利要求 18 所述的装置，所述交互环境认证信息为用户在虚
20 拟现实场景中输入一个密码字符后，将与该密码字符对应的映射坐标作为偏移量，对所述虚拟现实场景中的操作焦点进行偏移，并拼接各偏移后的操作焦点的坐标得到的坐标序列；其中，所述映射坐标为基于预设的映射算法对所述随机数串中的随机数分别进行映射计算，生成的与所述随机数分别对应的各映射坐标；

25 所述验证模块：

分别计算与所述坐标序列中的坐标对应的偏移量，得到与所述密码信息中的各密码字符对应的映射坐标；

基于所述预设的映射算法对与各密码字符对应的映射坐标分别进行反向计算，生成与各映射坐标分别对应的随机数；

拼接生成的各随机数得到所述随机数串。

20. 根据权利要求 19 所述的装置，所述验证模块进一步：

5 确定所述虚拟现实场景中的操作焦点偏移前在所述密码输入界面中的初始位置坐标；

基于所述初始位置坐标以及所述坐标序列中的坐标计算对应的偏移量。

21. 一种虚拟现实终端设备，包括：

处理器；

10 用于存储机器可执行指令的存储器；

其中，通过读取并执行所述存储器存储的与机器学习模型的训练的控制逻辑对应的机器可执行指令，所述处理器被促使：

基于虚拟现实服务端下发的随机信息计算交互环境认证信息；以及，

获取用户在虚拟现实场景中输入的密码信息；

15 将所述密码信息以及所述交互环境认证信息发送至所述虚拟现实服务端，以由所述虚拟现实服务端在所述密码信息验证通过后，基于所述交互环境认证信息反向计算出随机信息，并将反向计算出的所述随机信息与向虚拟现实客户端下发的随机信息进行匹配，以对所述虚拟现实场景的交互环境进行安全认证。

20 22. 一种虚拟现实服务端设备，包括：

处理器；

用于存储机器可执行指令的存储器；

其中，通过读取并执行所述存储器存储的与机器学习模型的训练的控制逻辑对应的机器可执行指令，所述处理器被促使：

25 获取虚拟现实终端发送的交互环境认证信息以及用户在虚拟现实场景中输入的密码信息；其中，所述交互环境认证信息基于下发至所述虚拟现实终端的随机信息计算生成；

验证所述密码信息；以及，如果所述密码信息验证通过，基于所述交互环境认证信息反向计算出随机信息，并验证反向计算出的随机信息与所述虚拟现实服务端下发的随机信息是否匹配；

如果反向计算出的随机信息与下发至所述虚拟现实终端的随机信息匹配，

- 5 确定所述虚拟现实场景的交互环境通过安全认证。

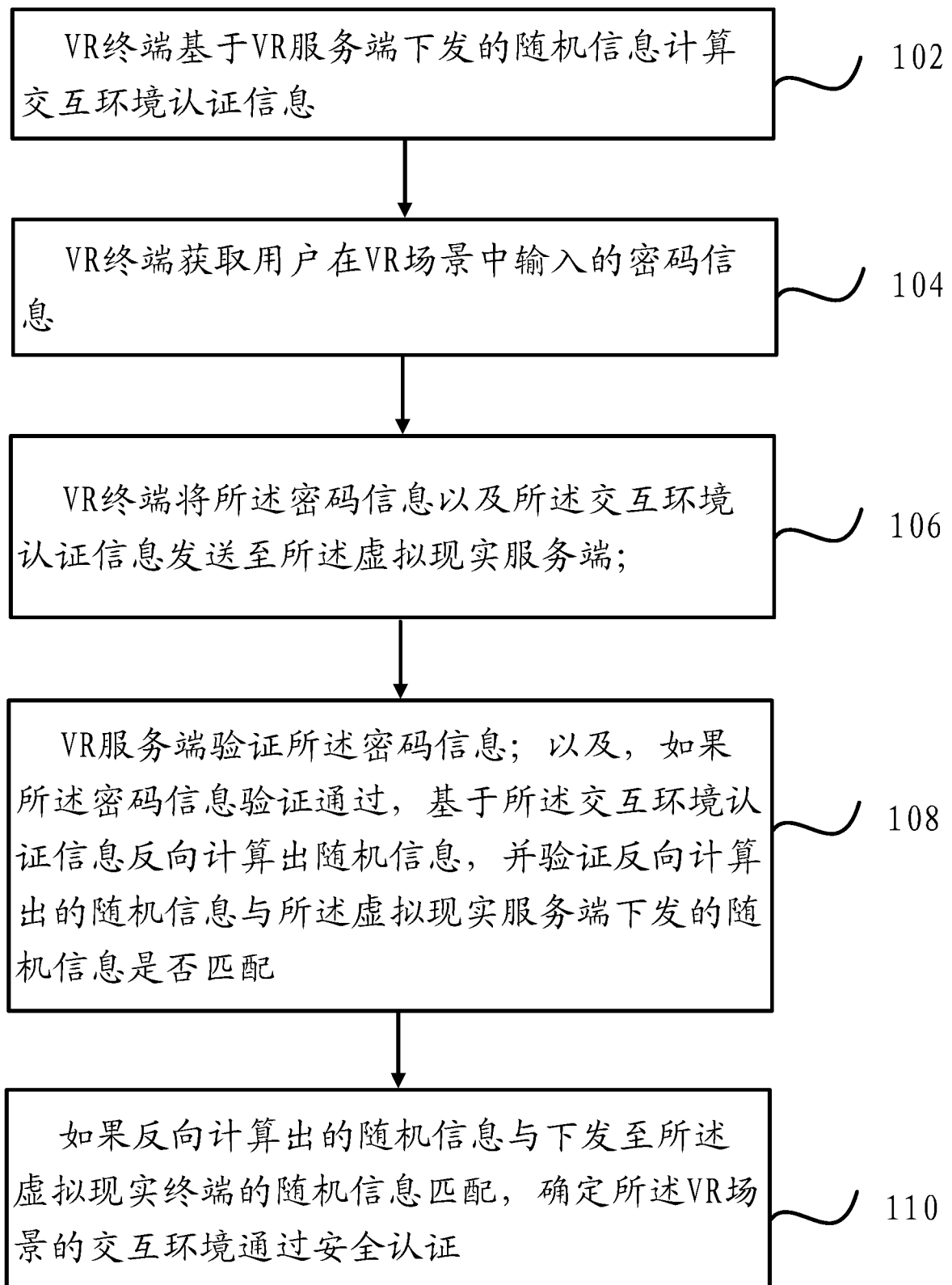


图 1

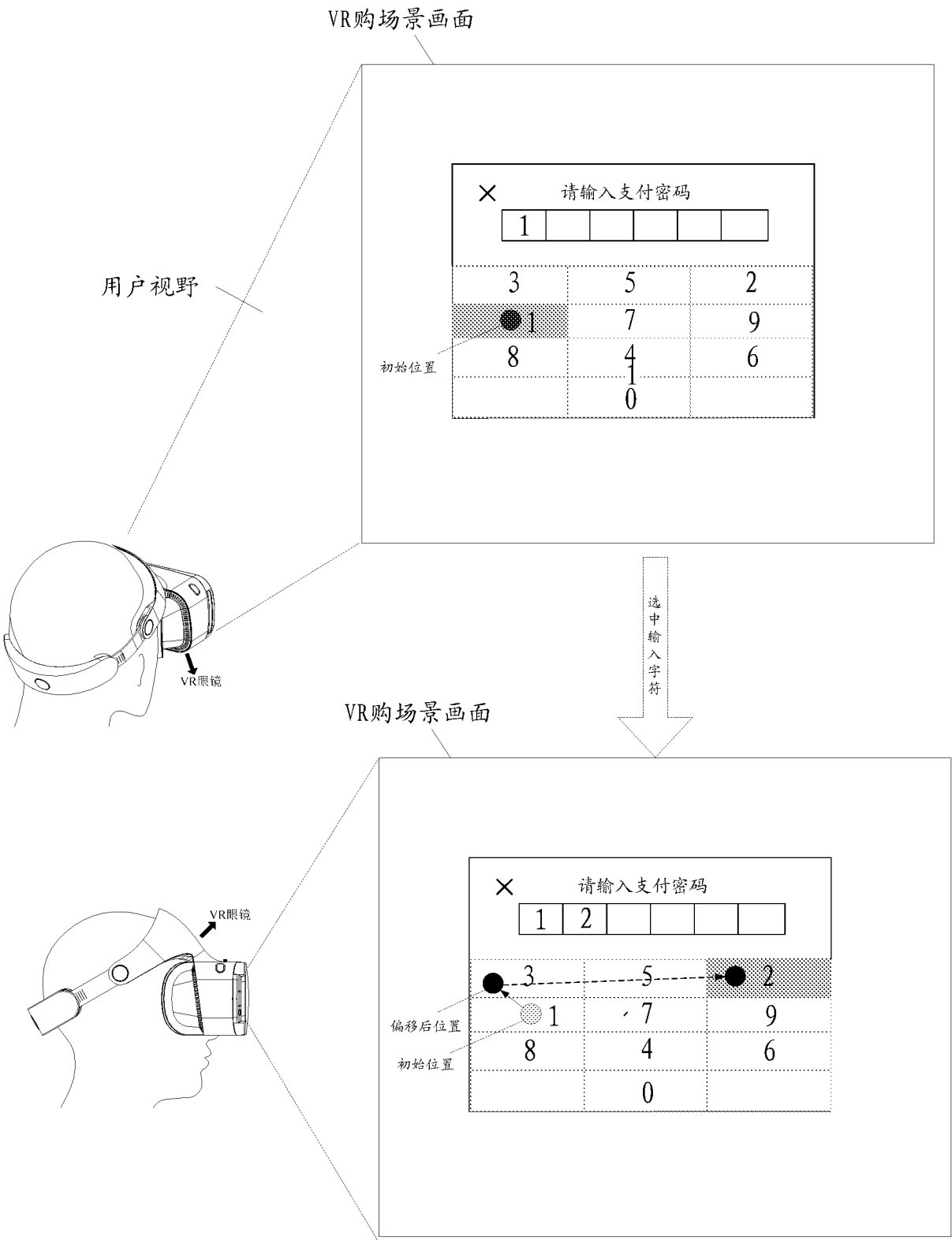


图 2

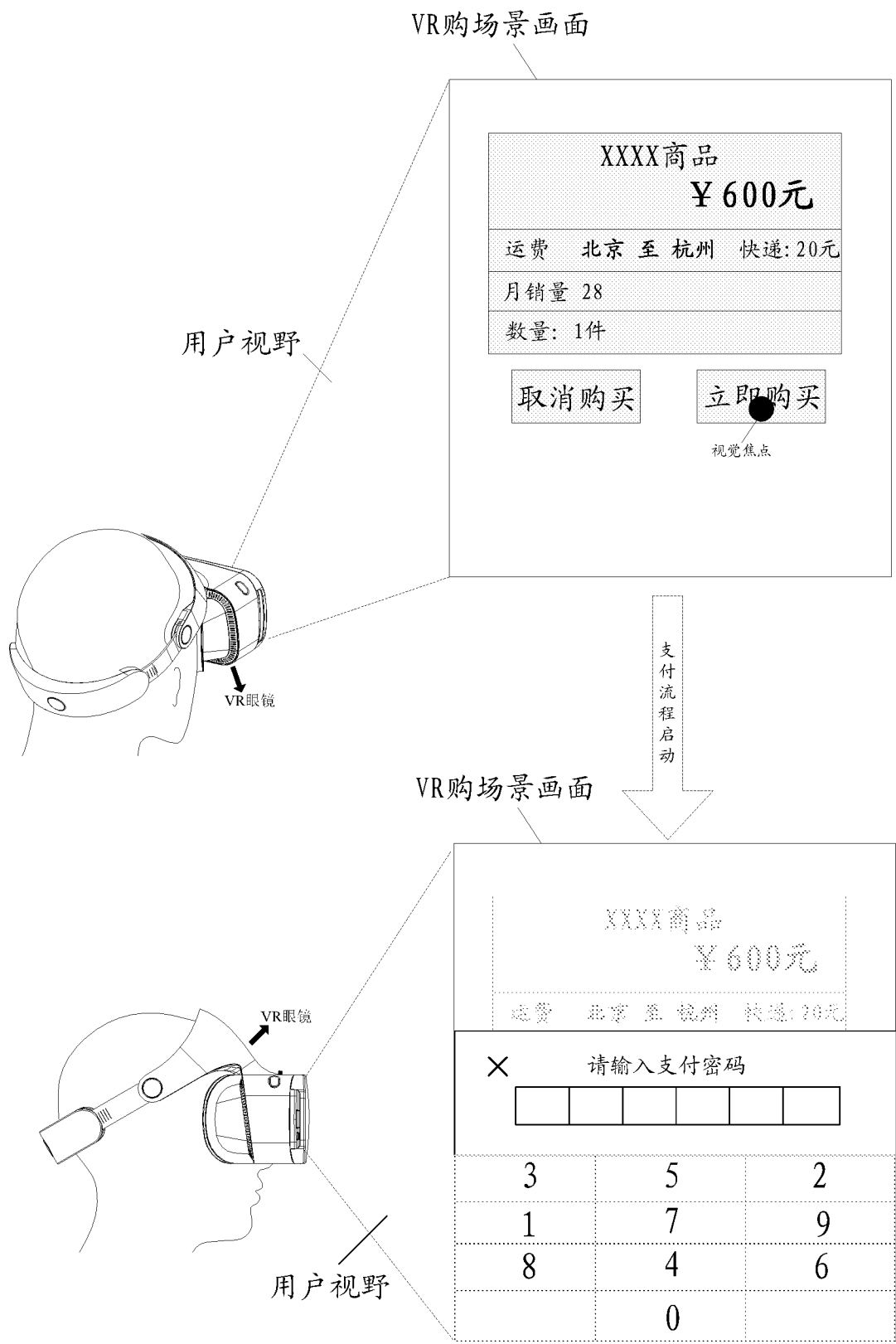


图 3

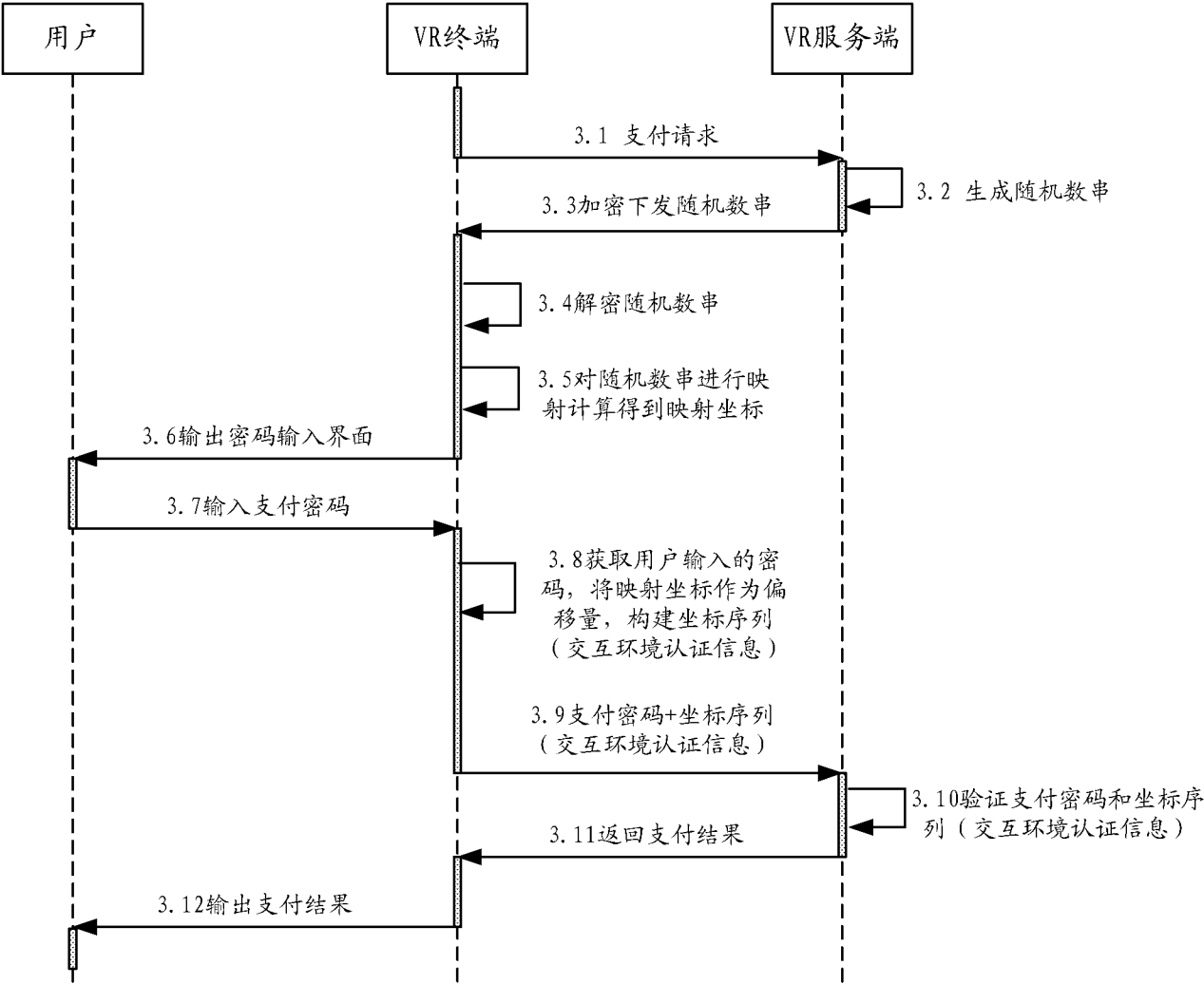


图 4

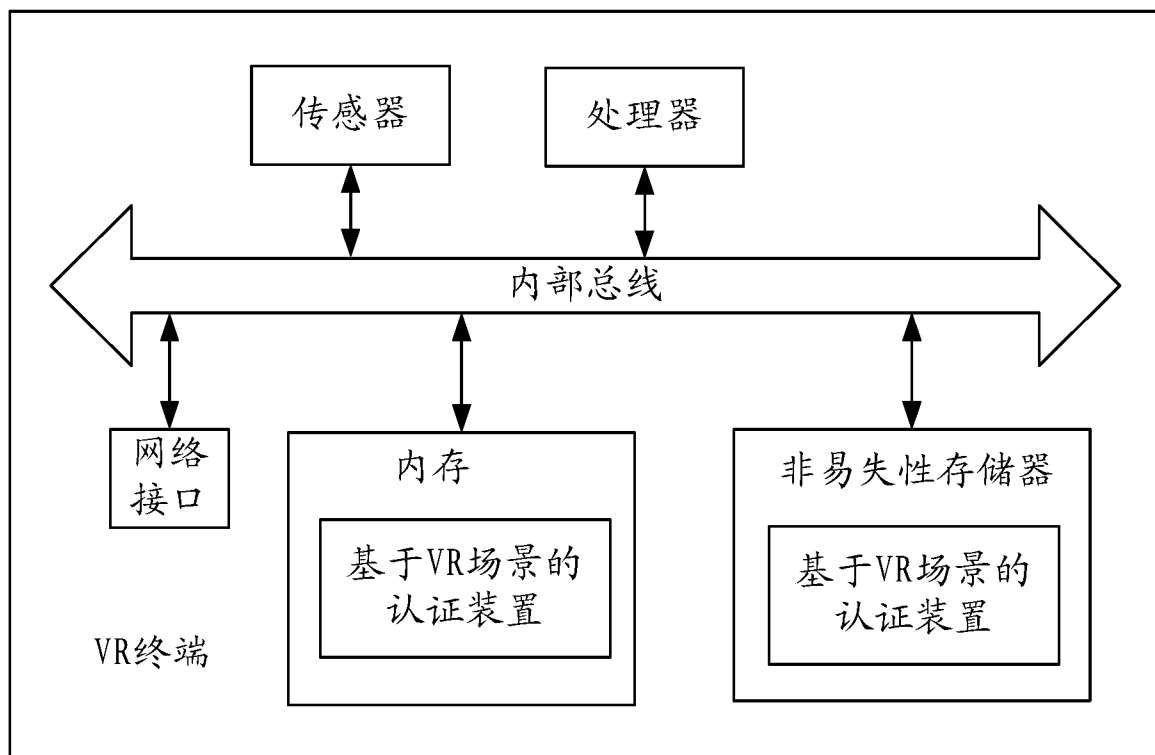


图 5

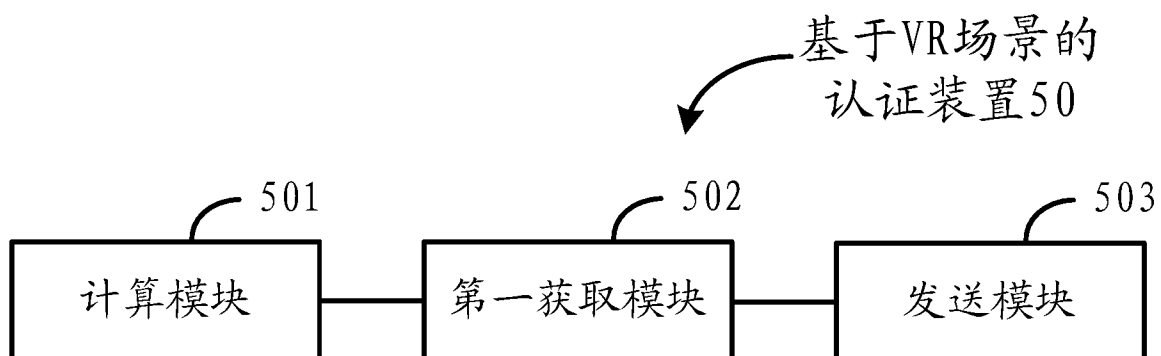


图 6

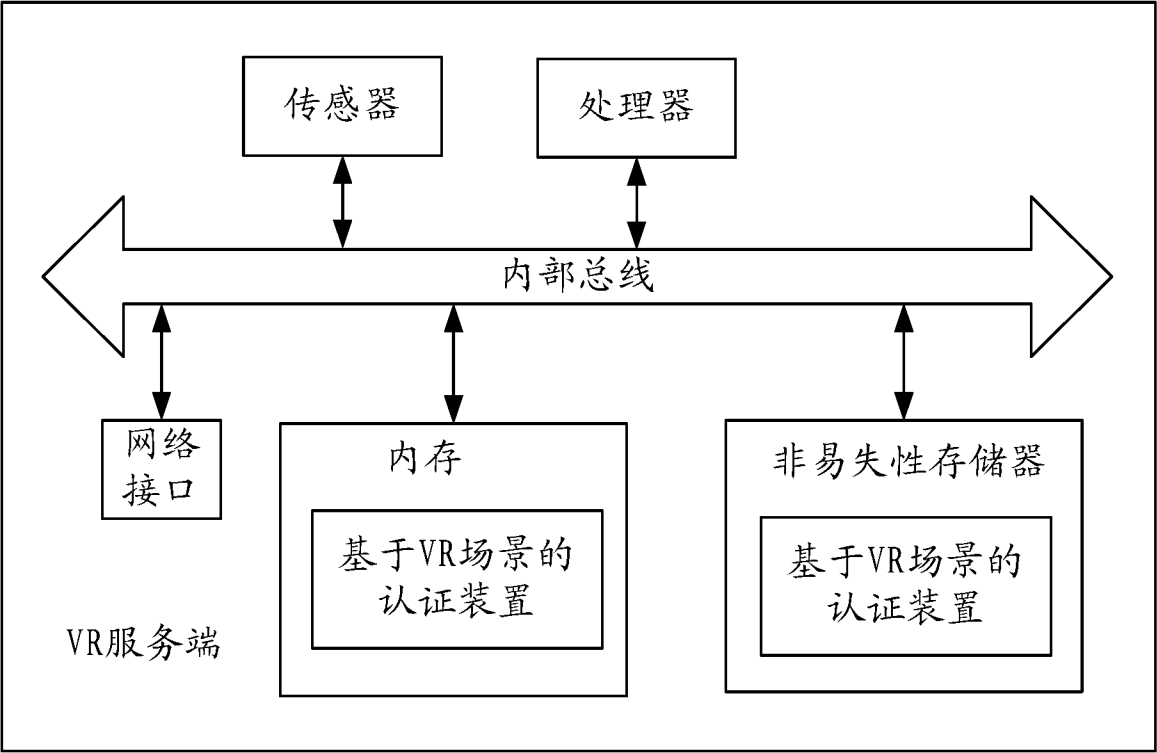


图 7

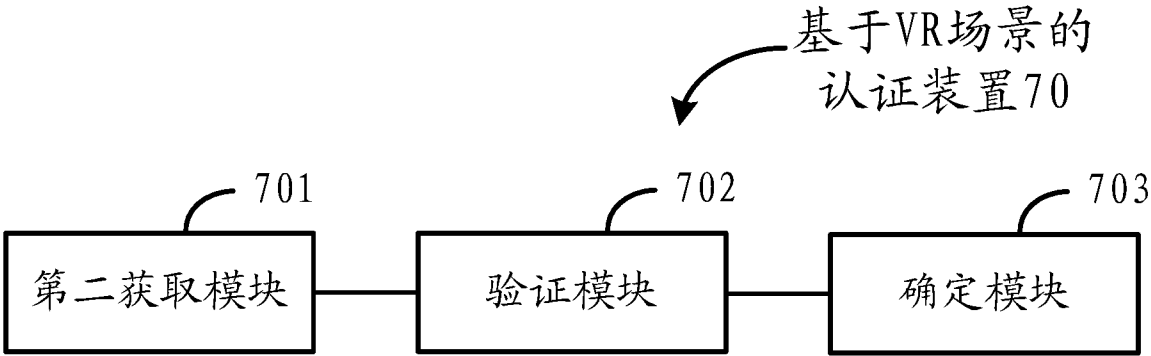


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/104774

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; CNKI; VEN: 虚拟现实, 随机, 认证, 验证, 服务端, 服务器, 密码, 环境, 安全, 坐标, 偏移量, virtual, reality, random, authenticat+, server, password, environment, security, coordinate, offset

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107508826 A (ALIBABA GROUP HOLDING LIMITED) 22 December 2017 (2017-12-22) claims 1-22	1-22
Y	CN 107122041 A (GUANGZHOU ALIBABA LITERATURE INFORMATION TECHNOLOGY CO., LTD.) 01 September 2017 (2017-09-01) description, paragraphs [0001]-[0083]	1-2, 6-8, 12-13, 17, 21, 22
A	CN 107122041 A (GUANGZHOU ALIBABA LITERATURE INFORMATION TECHNOLOGY CO., LTD.) 01 September 2017 (2017-09-01) entire document	3-5, 9-11, 14-16, 18-20
Y	CN 106797564 A (QUALCOMM INC.) 31 May 2017 (2017-05-31) description, paragraph [0009]	1-2, 6-8, 12-13, 17, 21, 22
A	US 8424065 B2 (INTERNATIONAL BUSINESS MACHINES CORP.) 16 April 2013 (2013-04-16) entire document	1-22

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

20 November 2018

Date of mailing of the international search report

29 November 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/104774

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107508826	A	22 December 2017	HK1247752 A0			28 September 2018
CN	107122041	A	01 September 2017	None			
CN	106797564	A	31 May 2017	KR	20170062459	A	07 June 2017
				US	2018295125	A1	11 October 2018
				US	2016094542	A1	31 March 2016
				PE	07392017	A1	04 July 2017
				EP	3198910	A1	02 August 2017
				BR	112017006191	A2	10 April 2018
				US	9998449	B2	12 June 2018
				AU	2015321928	A1	09 March 2017
				JP	2017535998	A	30 November 2017
				WO	2016048575	A1	31 March 2016
				CU	20170034	A7	04 July 2017
				IN201747005219		A	26 May 2017
US	8424065	B2	16 April 2013	US	2011126272	A1	26 May 2011

国际检索报告

国际申请号

PCT/CN2018/104774

A. 主题的分类

H04L 29/06 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNABS; CNTXT; VEN; CNKI; VEN: 虚拟现实, 随机, 认证, 验证, 服务端, 服务器, 密码, 环境, 安全, 坐标, 偏移量, virtual, reality, random, authenticat+, server, password, environment, security, coordinate, offset

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 107508826 A (阿里巴巴集团控股有限公司) 2017年 12月 22日 (2017 - 12 - 22) 权利要求1-22	1-22
Y	CN 107122041 A (广州阿里巴巴文学信息技术有限公司) 2017年 9月 1日 (2017 - 09 - 01) 说明书第[0001]-[0083]段	1-2、6-8、12-13、17、21、22
A	CN 107122041 A (广州阿里巴巴文学信息技术有限公司) 2017年 9月 1日 (2017 - 09 - 01) 全文	3-5、9-11、14-16、18-20
Y	CN 106797564 A (高通股份有限公司) 2017年 5月 31日 (2017 - 05 - 31) 说明书第[0009]段	1-2、6-8、12-13、17、21、22
A	US 8424065 B2 (INTERNATIONAL BUSINESS MACHINES CORP.) 2013年 4月 16日 (2013 - 04 - 16) 全文	1-22

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2018年 11月 20日

国际检索报告邮寄日期

2018年 11月 29日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

李晓茜

传真号 (86-10) 62019451

电话号码 62089456

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/104774

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	107508826	A	2017年 12月 22日	HK1247752 A0			2018年 9月 28日
CN	107122041	A	2017年 9月 1日	无			
CN	106797564	A	2017年 5月 31日	KR	20170062459	A	2017年 6月 7日
				US	2018295125	A1	2018年 10月 11日
				US	2016094542	A1	2016年 3月 31日
				PE	07392017	A1	2017年 7月 4日
				EP	3198910	A1	2017年 8月 2日
				BR	112017006191	A2	2018年 4月 10日
				US	9998449	B2	2018年 6月 12日
				AU	2015321928	A1	2017年 3月 9日
				JP	2017535998	A	2017年 11月 30日
				WO	2016048575	A1	2016年 3月 31日
				CU	20170034	A7	2017年 7月 4日
					IN201747005219	A	2017年 5月 26日
US	8424065	B2	2013年 4月 16日	US	2011126272	A1	2011年 5月 26日

表 PCT/ISA/210 (同族专利附件) (2015年1月)