(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119646779 A
(43)申请公布日 2025.03.18

(21)申请号 202411677413.3

(22)申请日 2024.11.21

(71)申请人 北京百度网讯科技有限公司
地址 100085 北京市海淀区上地十街10号百度大厦二层

(72)发明人 章志成 王珂欣

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
专利代理师 杜月

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/60(2013.01)
G06Q 30/018(2023.01)

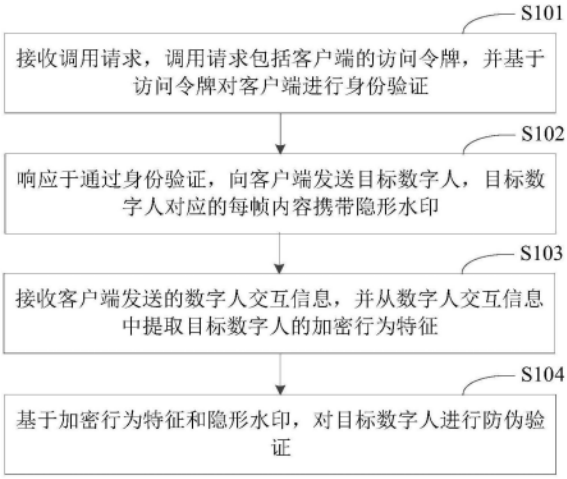
权利要求书5页 说明书13页 附图4页

(54)发明名称

数字人的防伪方法、装置和电子设备

(57)摘要

本公开提出了一种数字人的防伪方法、装置和电子设备,涉及数据处理技术领域,具体为人工智能和虚拟现实等技术领域,方法包括:接收调用请求,调用请求包括客户端的访问令牌,并基于访问令牌对所述客户端进行身份验证;响应于通过身份验证,向客户端发送目标数字人,目标数字人对应的每帧内容携带隐形水印;接收客户端发送的数字人交互信息,并从数字人交互信息中提取目标数字人的加密行为特征;基于加密行为特征和隐形水印,对目标数字人进行防伪验证,由此,本公开基于加密行为特征和隐形水印,对数字人进行防伪验证,有效地解决了数字人的防伪问题,增强了数字人的防伪效果,保证了数字人安全稳定地使用。



CN 119646779 A

1.一种数字人的防伪方法,其中,所述方法包括:

接收调用请求,所述调用请求包括客户端的访问令牌,并基于所述访问令牌对所述客户端进行身份验证;

响应于通过身份验证,向所述客户端发送目标数字人,所述目标数字人对应的每帧内容携带隐形水印;

接收所述客户端发送的数字人交互信息,并从所述数字人交互信息中提取所述目标数字人的加密行为特征;

基于所述加密行为特征和所述隐形水印,对所述目标数字人进行防伪验证。

2.根据权利要求1所述的方法,其中,所述基于所述加密行为特征和所述隐形水印,对所述目标数字人进行防伪验证,包括:

对所述加密行为特征进行解密,得到第一行为特征;

从特征数据库中获取所述目标数字人对应的第二行为特征,并对所述第一行为特征和所述第二行为特征进行特征匹配;

响应于满足所述目标数字人的行为特征未匹配成功和所述数字人交互信息未携带所述隐形水印中至少一项,确定所述目标数字人未通过防伪验证。

3.根据权利要求2所述的方法,其中,所述从特征数据库中获取所述目标数字人对应的第二行为特征,并对所述第一行为特征和所述第二行为特征进行特征匹配之前,还包括:

获取全量的候选数字人,并提取所述候选数字人的第二行为特征,其中所述目标数字人为所述全量的候选数字人中的一个;

基于所述第二行为特征生成所述候选数字人的行为特征集合;

根据所述候选数字人的行为特征集合,生成所述特征数据库。

4.根据权利要求3所述的方法,其中,所述从特征数据库中获取所述目标数字人对应的第二行为特征,并对所述第一行为特征和所述第二行为特征进行特征匹配,包括:

根据所述目标数字人的标识信息,从所述特征数据库中获取所述目标数字人对应的目标行为特征集合;

基于所述第一行为特征与所述目标行为特征集合中的第二行为特征进行匹配;

响应于所述第一行为特征与所述目标行为特征集合中至少一个第二行为特征的匹配度大于设定值,确定所述目标数字人的行为特征匹配成功;

响应于所述第一行为特征与所述目标行为特征集合中每个第二行为特征的匹配度均小于或等于所述设定值,确定所述目标数字人的行为特征未匹配成功。

5.根据权利要求4所述的方法,其中,所述基于所述第一行为特征与所述目标行为特征集合中的第二行为特征进行匹配,还包括:

根据所述数字人交互信息关联的帧号,确定所述第一行为特征关联的帧号;

从所述目标行为特征集合中获取所述帧号所关联的第二行为特征;

根据所述第一行为特征与所述帧号所关联的第二行为特征进行匹配;

响应于所述第一行为特征与所述帧号所关联的第二行为特征的匹配度大于设定值,确定所述目标数字人的行为特征匹配成功;

响应于所述第一行为特征与所述帧号所关联的第二行为特征的匹配度小于或等于所述设定值,确定所述目标数字人的行为特征未匹配成功。

6.根据权利要求1-5中任一项所述的方法,其中,所述向所述客户端发送目标数字人之前,还包括:

获取所述目标数字人的每帧内容的时间戳、所述目标数字人的上传设备标识和创建者标识;

根据每帧内容的所述时间戳、所述上传设备标识和创建者标识,生成每帧内容对应的隐形水印,并在每帧内容和所述数字人模型的纹理中添加所述隐形水印。

7.根据权利要求1-5中任一项所述的方法,其中,所述基于所述访问令牌对所述客户端进行身份验证,包括:

根据所述访问令牌,获取所述客户端对应的多种身份验证信息,所述多种身份验证信息包括所述客户端对应的第一身份关联信息和所述目标数字人对应的第二身份关联信息;

对所述多种身份验证信息分别进行验证,响应于通过多种身份验证,确定所述客户端通过身份验证。

8.根据权利要求1-5中任一项所述的方法,其中,所述方法还包括:

基于所述目标数字人的标识信息,确定所述目标数字人在区块链上的存储位置;

基于所述存储位置对所述区块链进行访问,获取所述目标数字人对应的记录信息,并根据所述记录信息,对所述目标数字人进行版权验证。

9.根据权利要求8所述的方法,其中,所述方法还包括:

响应于所述版权验证未通过,向所述客户端发送与所述调用请求的指示信息,所述指示信息用于指示所述目标数字人未通过版权验证。

10.根据权利要求8所述的方法,其中,所述方法还包括:

向所述区块链存储所述目标数字人的关联信息以生成所述目标数字人的记录信息,所述关联信息至少包括版权信息、创建信息、使用信息和更新信息中的至少一个。

11.一种数字人的防伪方法,其中,所述方法包括:

向服务器发送调用请求,所述调用请求包括客户端的访问令牌,所述访问令牌用于对所述客户端进行身份验证;

接收所述服务器发送的目标数字人并进行展示,所述目标数字人的每帧内容携带隐形水印;

获取输入信息,并从所述目标数字人中提取所述目标数字人的第一行为特征;

根据所述第一行为特征生成加密行为特征,并根据所述加密行为特征和所述输入信息生成数字人交互信息,并向所述服务器发送所述数字人交互信息。

12.根据权利要求11所述的方法,其中,所述方法还包括:

获取所述数字人交互信息所关联的所述目标数字人中的内容帧,并从所述内容帧中提取所述第一行为特征;

确定所述内容帧的帧号,并将所述内容帧的帧号与所述第一行为特征进行关联。

13.根据权利要求11所述的方法,其中,所述向服务器发送调用请求,包括:

获取所述客户端对应的第一身份关联信息和所述目标数字人的第二身份关联信息;

基于所述多种身份验证信息,生成所述访问令牌,并基于所述访问令牌生成所述调用请求。

14.根据权利要求11-13中任一项所述的方法,其中,所述方法还包括:

向区块链存储所述目标数字人的使用信息和更新信息中的至少一个,以更新所述区块链上存储的所述目标数字人的记录信息。

15.根据权利要求14所述的方法,其中,所述方法还包括:

基于所述目标数字人的标识信息,确定所述目标数字人在区块链上的存储位置;

基于所述存储位置对所述区块链进行访问,获取所述目标数字人的记录信息。

16.根据权利要求11-13中任一项所述的方法,其中,所述方法还包括:

接收所述服务器发送与所述调用请求的指示信息,其中所述指示信息用于指示所述目标数字人未通过所述服务器基于区块链上的所述目标数字人的记录信息进行的版权验证。

17.一种数字人的防伪装置,包括:

身份验证模块,用于接收调用请求,所述调用请求包括客户端的访问令牌,并基于所述访问令牌对所述客户端进行身份验证;

发送模块,用于响应于通过身份验证,向所述客户端发送目标数字人,所述目标数字人对应的每帧内容携带隐形水印;

特征提取模块,用于接收所述客户端发送的数字人交互信息,并从所述数字人交互信息中提取所述目标数字人的加密行为特征;

验证模块,用于基于所述加密行为特征和所述隐形水印,对所述目标数字人进行防伪验证。

18.根据权利要求17所述的装置,其中,所述验证模块,用于:

对所述加密行为特征进行解密,得到第一行为特征;

从特征数据库中获取所述目标数字人对应的第二行为特征,并对所述第一行为特征和所述第二行为特征进行特征匹配;

响应于满足所述目标数字人的行为特征未匹配成功和所述数字人交互信息未携带所述隐形水印中至少一项,确定所述目标数字人未通过防伪验证。

19.根据权利要求18所述的装置,其中,所述从特征数据库中获取所述目标数字人对应的第二行为特征,并对所述第一行为特征和所述第二行为特征进行特征匹配之前,所述装置,用于:

获取全量的候选数字人,并提取所述候选数字人的第二行为特征,其中所述目标数字人为所述全量的候选数字人中的一个;

基于所述第二行为特征生成所述候选数字人的行为特征集合;

根据所述候选数字人的行为特征集合,生成所述特征数据库。

20.根据权利要求19所述的装置,其中,所述验证模块,用于:

根据所述目标数字人的标识信息,从所述特征数据库中获取所述目标数字人对应的目标行为特征集合;

基于所述第一行为特征与所述目标行为特征集合中的第二行为特征进行匹配;

响应于所述第一行为特征与所述目标行为特征集合中至少一个第二行为特征的匹配度大于设定值,确定所述目标数字人的行为特征匹配成功;

响应于所述第一行为特征与所述目标行为特征集合中每个第二行为特征的匹配度均小于或等于所述设定值,确定所述目标数字人的行为特征未匹配成功。

21.根据权利要求19所述的装置,其中,所述验证模块,用于:

根据所述数字人交互信息关联的帧号,确定所述第一行为特征关联的帧号;

从所述目标行为特征集合中获取所述帧号所关联的第二行为特征;

根据所述第一行为特征与所述帧号所关联的第二行为特征进行匹配;

响应于所述第一行为特征与所述帧号所关联的第二行为特征的匹配度大于设定值,确定所述目标数字人的行为特征匹配成功;

响应于所述第一行为特征与所述帧号所关联的第二行为特征的匹配度小于或等于所述设定值,确定所述目标数字人的行为特征未匹配成功。

22.根据权利要求17-21中任一项所述的装置,其中,所述向所述客户端发送目标数字人之前,所述装置,用于:

获取所述目标数字人的每帧内容的时间戳、所述目标数字人的上传设备标识和创建者标识;

根据每帧内容的所述时间戳、所述上传设备标识和创建者标识,生成每帧内容对应的隐形水印,并在每帧内容和所述数字人模型的纹理中添加所述隐形水印。

23.根据权利要求17-21中任一项所述的装置,其中,所述身份验证模块,用于:

根据所述访问令牌,获取所述客户端对应的多种身份验证信息,所述多种身份验证信息包括所述客户端对应的第一身份关联信息和所述目标数字人对应的第二身份关联信息;

对所述多种身份验证信息分别进行验证,响应于通过多种身份验证,确定所述客户端通过身份验证。

24.根据权利要求17-21所述的装置,其中,所述装置还用于:

基于所述目标数字人的标识信息,确定所述目标数字人在区块链上的存储位置;

基于所述存储位置对所述区块链进行访问,获取所述目标数字人对应的记录信息,并根据所述记录信息,对所述目标数字人进行版权验证。

25.根据权利要求24所述的装置,其中,所述装置还用于:

响应于所述版权验证未通过,向所述客户端发送与所述调用请求的指示信息,所述指示信息用于指示所述目标数字人未通过版权验证。

26.根据权利要求24所述的装置,其中,所述装置还用于:

向所述区块链存储所述目标数字人的关联信息以生成所述目标数字人的记录信息,所述关联信息至少包括版权信息、创建信息、使用信息和更新信息中的至少一个。

27.一种数字人的防伪装置,用于:

第一发送模块,向服务器发送调用请求,所述调用请求包括客户端的访问令牌,所述访问令牌用于对所述客户端进行身份验证;

接收模块,用于接收所述服务器发送的目标数字人并进行展示,所述目标数字人的每帧内容携带隐形水印;

获取模块,用于获取输入信息,并从所述目标数字人中提取所述目标数字人的第一行为特征;

第二发送模块,用于根据所述第一行为特征生成加密行为特征,并根据所述加密行为特征和所述输入信息生成数字人交互信息,并向所述服务器发送所述数字人交互信息。

28.根据权利要求27所述的装置,其中,所述装置,用于:

获取所述数字人交互信息所关联的所述目标数字人中的内容帧,并从所述内容帧中提

取所述第一行为特征；

确定所述内容帧的帧号，并将所述内容帧的帧号与所述第一行为特征进行关联。

29.根据权利要求27所述的装置，其中，所述第一发送模块，用于：

获取所述客户端对应的第一身份关联信息和所述目标数字人的第二身份关联信息；

基于所述多种身份验证信息，生成所述访问令牌，并基于所述访问令牌生成所述调用请求。

30.根据权利要求27-29所述的训练装置，其中，所述装置，用于：

向区块链存储所述目标数字人的使用信息和更新信息中的至少一个，以更新所述区块链上存储的所述目标数字人的记录信息。

31.根据权利要求30所述的训练装置，其中，所述装置，用于：

基于所述目标数字人的标识信息，确定所述目标数字人在区块链上的存储位置；

基于所述存储位置对所述区块链进行访问，获取所述目标数字人的记录信息。

32.根据权利要求27-29所述的训练装置，其中，所述装置，用于：

接收所述服务器发送与所述调用请求的指示信息，其中所述指示信息用于指示所述目标数字人未通过所述服务器基于区块链上的所述目标数字人的记录信息进行的版权验证。

33.一种电子设备，其特征在于，包括处理器和存储器；

其中，所述处理器通过读取所述存储器中存储的可执行程序代码来运行与所述可执行程序代码对应的程序，以用于实现如权利要求1-10或权利要求11-16中任一项所述的方法。

34.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1-10或权利要求11-16中任一项所述的方法。

35.一种计算机程序产品，包括计算机程序，所述计算机程序在被处理器执行时实现根据权利要求1-10或权利要求11-16中任一项所述的方法。

数字人的防伪方法、装置和电子设备

技术领域

[0001] 本公开涉及数据处理技术领域,具体为人工智能和增强现实等技术领域,尤其涉及一种数字人的防伪方法、装置和电子设备。

背景技术

[0002] 随着虚拟现实和元宇宙等技术的发展,数字人已经广泛应用于多个领域,但是数字人的形象、行为和声音等内容很容易被复制、篡改或未经授权使用,然而,相关技术中的数字人的防伪方法,无法有效地解决数字人的防伪问题。

发明内容

[0003] 本公开提出了一种数字人的防伪方法、装置、电子设备、存储介质和计算机程序产品。

[0004] 根据本公开的第一方面,提出了一种数字人的防伪方法,包括:接收调用请求,所述调用请求包括客户端的访问令牌,并基于所述访问令牌对所述客户端进行身份验证;响应于通过身份验证,向所述客户端发送目标数字人,所述目标数字人对应的每帧内容携带隐形水印;接收所述客户端发送的数字人交互信息,并从所述数字人交互信息中提取所述目标数字人的加密行为特征;基于所述加密行为特征和所述隐形水印,对所述目标数字人进行防伪验证。

[0005] 根据本公开的第二方面,提出了一种数字人的防伪方法,包括:向服务器发送调用请求,所述调用请求包括客户端的访问令牌,所述访问令牌用于对所述客户端进行身份验证;接收所述服务器发送的目标数字人并进行展示,所述目标数字人的每帧内容携带隐形水印;获取输入信息,并从所述目标数字人中提取所述目标数字人的第一行为特征;根据所述第一行为特征生成加密行为特征,并根据所述加密行为特征和所述输入信息生成数字人交互信息,并向所述服务器发送所述数字人交互信息。

[0006] 根据本公开的第三方面,提出了一种数字人的防伪装置,包括:身份验证模块,用于接收调用请求,所述调用请求包括客户端的访问令牌,并基于所述访问令牌对所述客户端进行身份验证;发送模块,用于响应于通过身份验证,向所述客户端发送目标数字人,所述目标数字人对应的每帧内容携带隐形水印;特征提取模块,用于接收所述客户端发送的数字人交互信息,并从所述数字人交互信息中提取所述目标数字人的加密行为特征;验证模块,用于基于所述加密行为特征和所述隐形水印,对所述目标数字人进行防伪验证。

[0007] 根据本公开的第四方面,提出了一种数字人的防伪装置,包括:第一发送模块,向服务器发送调用请求,所述调用请求包括客户端的访问令牌,所述访问令牌用于对所述客户端进行身份验证;接收模块,用于接收所述服务器发送的目标数字人并进行展示,所述目标数字人的每帧内容携带隐形水印;获取模块,用于获取输入信息,并从所述目标数字人中提取所述目标数字人的第一行为特征;第二发送模块,用于根据所述第一行为特征生成加密行为特征,并根据所述加密行为特征和所述输入信息生成数字人交互信息,并向所述服

务器发送所述数字人交互信息。

[0008] 根据本公开的第五方面,提出了一种电子设备,包括:至少一个处理器;以及与所述至少一个处理器通信连接的存储器;其中,所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行上述第一方面或第二方面提出的数字人的防伪方法。

[0009] 根据本公开的第六方面,提出了一种存储有计算机指令的非瞬时计算机可读存储介质,其中,所述计算机指令用于使所述计算机执行上述第一方面或第二方面提出的数字人的防伪方法。

[0010] 根据本公开的第七方面,提出了一种计算机程序产品,包括计算机程序,所述计算机程序在被处理器执行时实现上述第一方面或第二方面提出的数字人的防伪方法。

[0011] 应当理解,本部分所描述的内容并非旨在标识本公开的实施例的关键或重要特征,也不用于限制本公开的范围。本公开的其它特征将通过以下的说明书而变得容易理解。

附图说明

[0012] 附图用于更好地理解本方案,不构成对本公开的限定。其中:

[0013] 图1为本公开一实施例的数字人的防伪方法的流程示意图;

[0014] 图2为本公开另一实施例的数字人的防伪方法的流程示意图;

[0015] 图3为本公开另一实施例的数字人的防伪方法的流程示意图;

[0016] 图4为本公开一实施例的数字人的防伪装置的结构示意图;

[0017] 图5为本公开一实施例的数字人的防伪装置的结构示意图;

[0018] 图6为本公开一实施例的电子设备的示意性框图。

具体实施方式

[0019] 以下结合附图对本公开的示范性实施例做出说明,其中包括本公开实施例的各种细节以助于理解,应当将它们认为仅仅是示范性的。因此,本领域普通技术人员应当认识到,可以对这里描述的实施例做出各种改变和修改,而不会背离本公开的范围和精神。同样,为了清楚和简明,以下的描述中省略了对公知功能和结构的描述。

[0020] 数据处理(Data Processing)是对数据的采集、存储、检索、加工、变换和传输,数据是对事实、概念或指令的一种表达形式,可由人工或自动化装置进行处理,数据经过解释并赋予一定的意义之后,便成为信息。

[0021] 人工智能(Artificial Intelligence,简称AI)是新一轮科技革命和产业变革的重要驱动力量,是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。

[0022] 增强现实(Augmented Reality,简称AR)技术是借助光电显示技术、交互技术、多种传感器技术和计算机图形与多媒体技术将计算机生成的虚拟环境与用户周围的现实环境融为一体,使用户从感官效果上确信虚拟环境是其周围真实环境的组成部分。增强现实具有虚实结合、实时交互、三维注册的新特点。

[0023] 图1为本公开一实施例的数字人的防伪方法的流程示意图。如图1所示,该方法包括:

[0024] S101,接收调用请求,调用请求包括客户端的访问令牌,并基于访问令牌对客户端进行身份验证。

[0025] 需要说明的是,本公开实施例的数字人的防伪方法的执行主体可为具有数据信息处理能力的硬件设备和/或驱动该硬件设备工作所需必要的软件。可选地,执行主体可包括工作站、服务器,计算机、用户终端及其他智能设备。其中,用户终端包括但不限于手机、电脑、智能语音交互设备、智能家电、车载终端等。

[0026] 需要说明的是,客户端通过获取客户端对应的第一身份验证信息和目标数字人的第二身份验证信息,基于多种身份验证信息,生成访问令牌Token,并基于访问令牌生成调用请求。

[0027] 在本公开实施例中,客户端生成调用请求后,向服务器发送调用请求,相应地,服务器通过接收调用请求,对调用请求进行解析,以获取调用请求中包括的客户端的访问令牌。

[0028] 在本公开实施例中,在获取到访问令牌后,可以根据访问令牌,获取客户端对应的多种身份验证信息,多种身份验证信息包括客户端对应的第一身份验证信息和目标数字人对应的第二身份验证信息,对多种身份验证信息分别进行验证,响应于通过多种身份验证,确定客户端通过身份验证。

[0029] S102,响应于通过身份验证,向客户端发送目标数字人,目标数字人对应的每帧内容携带隐形水印。

[0030] 其中,数字人(Digital Human)指的是运用数字技术创造出来的、与人类形象接近的数字化人物形象,数字人可以应用于游戏、影视、直播、虚拟社交等多个领域。

[0031] 需要说明的是,在客户端通过身份验证后,即表明客户端具备合法权限可以使用目标数字人,可以在目标数字人对应的每帧内容中添加隐形水印,并向客户端发送目标数字人。

[0032] 需要说明的是,相关技术中,往往在数字人中添加静态水印,但是数字人往往是动态的,现有的静态水印只能应用于数字人的单帧内容,无法覆盖数字人的动态交互场景,易被用过屏幕录制等方式进行绕过。

[0033] 在本公开实施例中,可以获取目标数字人的每帧内容的时间戳、目标数字人的上传设备标识和创建者标识,根据每帧内容的时间戳、上传设备标识和创建者标识,生成每帧内容对应的隐形水印,并在每帧内容和数字人模型的纹理中添加隐形水印。

[0034] 需要说明的是,针对目标数字人的动态交互场景,例如:目标数字人的展示和互动场景,通过在目标数字人在每帧内容和数字人模型的纹理中添加隐形水印,可以随着目标数字人的动作变化进行更新,即隐形水印为动态水印,目标数字人的每帧内容包含对应的隐形水印信息,例如:时间戳、上传设备标识和创建者标识,确保即使通过视频录制的方式也无法进行绕过。

[0035] S103,接收客户端发送的数字人交互信息,并从数字人交互信息中提取目标数字人的加密行为特征。

[0036] 需要说明的是,在数字人进行互动时,为了确保目标数字人的每次行为都是合法授权的,可以接收客户端发送的数字人交互信息,并从数字人交互信息中提取目标数字人的加密行为特征。

[0037] 可选地,在获取到数字人交互信息后,可以根据目标数字人的标识信息,从数字人交互信息中提取与目标数字人关联的加密行为特征。

[0038] 其中,目标数字人的加密行为特征包括但不限于目标数字人的动作特征、面部特征和对话语音特征等。

[0039] S104,基于加密行为特征和隐形水印,对目标数字人进行防伪验证。

[0040] 在本公开实施例中,在获取到加密行为特征和隐形水印后,可以基于加密行为特征和隐形水印,对目标数字人进行防伪验证。

[0041] 可选地,可以对加密行为特征进行解密,得到第一行为特征,从特征数据库中获取目标数字人对应的第二行为特征,并对第一行为特征和第二行为特征进行特征匹配,根据特征匹配结果和隐形水印,确定目标数字人是否通过防伪验证。

[0042] 举例而言,响应于满足目标数字人的行为特征未匹配成功和数字人交互信息未携带隐形水印中至少一项,确定目标数字人未通过防伪验证;响应于满足目标数字人的行为特征匹配成功和数字人交互信息携带隐形水印中的全部项,确定目标数字人通过防伪验证。

[0043] 在本公开实施例中,在确定目标数字人未通过防伪验证后,可以向客户端发送与调用请求的指示信息,指示信息用于指示目标数字人未通过防伪验证。

[0044] 本公开提出的数字人的防伪方法,通过接收调用请求,调用请求包括客户端的访问令牌,并基于访问令牌对客户端进行身份验证,响应于通过身份验证,向客户端发送目标数字人,目标数字人对应的每帧内容携带隐形水印,接收客户端发送的数字人交互信息,并从数字人交互信息中提取目标数字人的加密行为特征,基于加密行为特征和隐形水印,对目标数字人进行防伪验证,由此,本公开基于加密行为特征和隐形水印,对数字人进行防伪验证,有效地解决了数字人的防伪问题,增强了数字人的防伪效果,保证了数字人安全稳定地使用。

[0045] 图2是根据本公开第二实施例的数字人的防伪方法的流程示意图。

[0046] 如图2所示,在图1所示实施例的基础上,本公开实施例的图案生成方法具体可包括以下步骤:

[0047] S201,接收调用请求,调用请求包括客户端的访问令牌。

[0048] 步骤S201的相关内容,可参见上述实施例,这里不再赘述。

[0049] 上述实施例中的步骤S101“基于访问令牌对客户端进行身份验证”具体可包括以下步骤S202和S203。

[0050] S202,根据访问令牌,获取客户端对应的多种身份验证信息,多种身份验证信息包括客户端对应的第一身份关联信息和目标数字人对应的第二身份关联信息。

[0051] 在本公开实施例中,在获取到访问令牌后,可以对访问令牌进行解析,以获取客户端对应的多种身份验证信息。

[0052] 其中,第一身份关联信息包括但不限于客户端对应的设备标识信息、账号信息和账号信息对应的授权信息等。

[0053] 其中,第二身份关联信息包括但不限于数字人对应的开发者的身份信息、平台应用程序编程接口(Application Programming Interface,简称API)信息和授权使用设备信息。

[0054] S203,对多种身份验证信息分别进行验证,响应于通过多种身份验证,确定客户端通过身份验证。

[0055] 在本公开实施例中,可以对客户端对应的第一身份关联信息进行验证以及对目标数字人对应的第二身份关联信息进行验证,响应于第一身份关联信息通过验证且第二身份关联信息通过验证,即确定客户端通过身份验证。

[0056] S204,响应于通过身份验证,向客户端发送目标数字人,目标数字人对应的每帧内容携带隐形水印。

[0057] S205,接收客户端发送的数字人交互信息,并从数字人交互信息中提取目标数字人的加密行为特征。

[0058] 步骤S204和S205的相关内容,可参见上述实施例,这里不再赘述。

[0059] 上述实施例中的步骤S104“基于加密行为特征和隐形水印,对目标数字人进行防伪验证”具体可包括以下步骤S206和S208。

[0060] S206,对加密行为特征进行解密,得到第一行为特征。

[0061] 在本公开实施例中,在获取到加密行为特征后,可以通过解密算法,对加密行为特征进行解密,以得到第一行为特征。

[0062] S207,从特征数据库中获取目标数字人对应的第二行为特征,并对第一行为特征和第二行为特征进行特征匹配。

[0063] 在本公开实施例中,可以预先生成特征数据库,以从特征数据库中获取目标数字人对应的第二行为特征,并对第一行为特征和第二行为特征进行特征匹配。

[0064] 可选地,可以获取全量的候选数字人,并提取候选数字人的第二行为特征,其中目标数字人为全量的候选数字人中的一个,基于第二行为特征生成候选数字人的行为特征集合,根据候选数字人的行为特征集合,生成特征数据库。

[0065] 在本公开实施例中,可以根据目标数字人的标识信息,从特征数据库中获取目标数字人对应的目标行为特征集合,基于第一行为特征与目标行为特征集合中的第二行为特征进行匹配,响应于第一行为特征与目标行为特征集合中至少一个第二行为特征的匹配度大于设定值,确定目标数字人的行为特征匹配成功,响应于第一行为特征与目标行为特征集合中每个第二行为特征的匹配度均小于或等于设定值,确定目标数字人的行为特征未匹配成功。

[0066] 需要说明的是,本公开对于设定值的设置不作限定,例如:设定值可以为95%、又例如:设定值可以为98%。

[0067] 在本公开实施例中,可以根据数字人交互信息关联的帧号,确定第一行为特征关联的帧号,从目标行为特征集合中获取帧号所关联的第二行为特征,根据第一行为特征与帧号所关联的第二行为特征进行匹配,响应于第一行为特征与帧号所关联的第二行为特征的匹配度大于设定值,确定目标数字人的行为特征匹配成功,响应于第一行为特征与帧号所关联的第二行为特征的匹配度小于或等于设定值,确定目标数字人的行为特征未匹配成功。

[0068] 其中,第一行为特征关联的帧号可以为当前帧的帧号、还可以为在当前帧之前的前N帧的帧号。

[0069] 举例而言,针对设定值为98%以及第一行为特征X_1关联的帧号为当前帧第M帧,从

目标行为特征集合中获取第M帧所关联的第二行为特征X_2,响应于第一行为特征X_1与第二行为特征X_2的匹配度为99%,此种情况下,第一行为特征X_1与第二行为特征X_2的匹配度大于设定值98%,即确定目标数字人的行为特征匹配成功。

[0070] 举例而言,针对设定值为98%以及第一行为特征X_1关联的帧号为当前帧第M帧,从目标行为特征集合中获取第M帧所关联的第二行为特征X_2,响应于第一行为特征X_1与第二行为特征X_2的匹配度为90%,此种情况下,第一行为特征X_1与第二行为特征X_2的匹配度小于设定值98%,即确定目标数字人的行为特征未匹配成功。

[0071] S208,响应于满足目标数字人的行为特征未匹配成功和数字人交互信息未携带隐形水印中至少一项,确定目标数字人未通过防伪验证。

[0072] 需要说明的是,当数字人交互信息中未携带隐形水印中至少一项时,此种情况下,目标数字人未通过隐形水印校验,当数字人交互信息中携带隐形水印中全部项时,此种情况下,目标数字人通过隐形水印校验。

[0073] 需要说明的是,响应于满足目标数字人的行为特征匹配成功和数字人交互信息携带隐形水印中全部项,确定目标数字人通过防伪验证。

[0074] 需要说明的是,每个数字人的版权、创建、更新(例如:修改)和使用通过区块链技术在区块链进行记录存储,形成不可篡改的版权链。

[0075] 在本公开实施例中,在目标数字人使用过程中,可以基于目标数字人的标识信息,确定目标数字人在区块链上的存储位置,基于存储位置对区块链进行访问,获取目标数字人对应的记录信息,并根据记录信息,对目标数字人进行版权验,以确保目标数字人的每次使用都是合法授权的。

[0076] 可选地,可以向区块链存储目标数字人的关联信息以生成目标数字人的记录信息,关联信息至少包括版权信息、创建信息、使用信息和更新信息中的至少一个。

[0077] 在本公开实施例中,响应于版权验证未通过,向客户端发送与调用请求的指示信息,指示信息用于指示目标数字人未通过版权验证;响应于版权验证通过,可以向客户端发送与调用请求的指示信息,指示信息用于指示目标数字人通过版权验证。

[0078] 综上,本公开提出的数字人的防伪方法,接收调用请求,调用请求包括客户端的访问令牌,根据访问令牌,获取客户端对应的多种身份验证信息,多种身份验证信息包括客户端对应的第一身份关联信息和目标数字人对应的第二身份关联信息,对多种身份验证信息分别进行验证,响应于通过多种身份验证,确定客户端通过身份验证,响应于通过身份验证,向客户端发送目标数字人,目标数字人对应的每帧内容携带隐形水印,响应于通过身份验证,向客户端发送目标数字人,目标数字人对应的每帧内容携带隐形水印,对加密行为特征进行解密,得到第一行为特征,从特征数据库中获取目标数字人对应的第二行为特征,并对第一行为特征和第二行为特征进行特征匹配,响应于满足目标数字人的行为特征未匹配成功和数字人交互信息未携带隐形水印中至少一项,确定目标数字人未通过防伪验证,并根据目标数字人对应的记录信息,对目标数字人进行版权验证,由此,本公开通过多重验证方式有效地解决了数字人的防伪问题,当目标数字人在多个平台使用时,可以实现目标数字人跨平台的同步防伪验证,防止在未经授权的平台上使用或篡改目标数字人,增强了数字人的防伪效果,确保目标数字人内容的真实性、唯一性和版权归属。

[0079] 图3为本公开一实施例的数字人的防伪方法的流程示意图。如图3所示,该方法包

括:

[0080] S301,向服务器发送调用请求,调用请求包括客户端的访问令牌,访问令牌用于对客户端进行身份验证。

[0081] 需要说明的是,本公开实施例的数字人的防伪方法的执行主体可为具有数据信息处理能力的硬件设备和/或驱动该硬件设备工作所需必要的软件。可选地,执行主体可包括工作站、服务器,计算机、用户终端及其他智能设备。其中,用户终端包括但不限于手机、电脑、智能语音交互设备、智能家电、车载终端等。

[0082] 在本公开实施例中,可以获取客户端对应的第一身份验证信息和目标数字人的第二身份验证信息,基于多种身份验证信息,生成访问令牌,并基于访问令牌生成调用请求。

[0083] 在本公开实施例中,在生成调用请求后,可以向服务器发送调用请求,调用请求包括客户端的访问令牌,服务器可以基于访问令牌对客户端进行身份验证。

[0084] 需要说明的是,数字人在创建和发布时,会与客户端对应的第一身份验证信息和目标数字人的第二身份验证信息进行绑定,在数字人每次使用时,基于第一身份验证信息和目标数字人的第二身份验证信息,生成访问令牌Token,确保具备合法权限的客户端才能使用数字人。

[0085] 其中,第一身份验证信息包括但不限于客户端对应的设备标识信息、账号信息和账号信息对应的授权信息等。

[0086] 其中,第二身份验证信息包括但不限于目标数字人对应的开发者的身份信息、平台应用程序编程接口API信息和授权使用设备信息。

[0087] 需要说明的是,目标数字人可以在多个不同平台同时进行使用,例如:直播平台、游戏平台和虚拟社交平台,通过获取目标数字人对应的平台API信息,服务器通过与平台API信息对接,可以跨平台地同步对数字人进行防伪验证。

[0088] S302,接收服务器发送的目标数字人并进行展示,目标数字人的每帧内容携带隐形水印。

[0089] 在本公开实施例中,在服务器接收调用请求后,其中调用请求包括客户端的访问令牌,并基于访问令牌对客户端进行身份验证,响应于客户端通过身份验证后,向客户端发送目标数字人,相应地,客户端可以接收服务器发送的目标数字人进行展示。

[0090] S303,获取输入信息,并从目标数字人中提取目标数字人的第一行为特征。

[0091] 需要说明的是,通过输入信息驱动目标数字人,实现与目标数字人的交互,以从目标数字人中提取目标数字人的第一行为特征。

[0092] 需要说明的是,本公开对于输入信息的形式不作限定,例如:输入信息的形式可以为文本、语音等多种形式。

[0093] 需要说明的是,本公开对于从目标数字人中提取目标数字人的第一行为特征不作限定,可以根据实际情况进行选取。

[0094] 可选地,可以获取预训练的行为特征提取模型,基于预训练的行为特征提取模型,从目标数字人中提取目标数字人的第一行为特征。

[0095] 在本公开实施中,可以获取数字人交互信息所关联的目标数字人中的内容帧,并从内容帧中提取第一行为特征,确定内容帧的帧号,并将内容帧的帧号与第一行为特征进行关联。

[0096] S304,根据第一行为特征生成加密行为特征,并根据加密行为特征和输入信息生成数字人交互信息,并向服务器发送数字人交互信息。

[0097] 需要说明的是,在获取到第一行为特征后,可以通过加密算法对第一行为特征进行加密,以生成加密行为特征。

[0098] 在本公开实施例中,可以向区块链存储目标数字人的使用信息和更新信息中的至少一个,以更新区块链上存储的目标数字人的记录信息,并基于目标数字人的标识信息,确定目标数字人在区块链上的存储位置,基于存储位置对区块链进行访问,获取目标数字人的记录信息。

[0099] 在本公开实施例中,服务器发送与调用请求的指示信息,相应地,客户端接收服务器发送与调用请求的指示信息,其中指示信息用于指示目标数字人未通过服务器基于区块链上的目标数字人的记录信息进行的版权验证。

[0100] 本公开提出的数字人的防伪方法,向服务器发送调用请求,调用请求包括客户端的访问令牌,访问令牌用于对客户端进行身份验证,接收客户端发送的目标数字人并进行展示,目标数字人的每帧内容携带隐藏水印,获取输入信息,并从目标数字人中提取目标数字人的第一行为特征,根据第一行为特征生成加密行为特征,并根据加密行为特征和输入信息生成数字人交互信息,并向服务器发送数字人交互信息,由此,本公开通过向服务器发送数字人交互信息,服务器可以从数字人交互信息中提取目标数字人的加密行为特征,并基于加密行为特征和隐形水印,对目标数字人进行防伪验证,有效地解决了数字人的防伪问题,增强了数字人的防伪效果,确保了数字人的合法使用,无需额外的验证操作即可实现数字人的唯一性与版权归属,保证了数字人安全稳定地使用。

[0101] 本公开的技术方案中,所涉及的用户个人信息的收集、存储、使用、加工、传输、提供和公开等处理,均符合相关法律法规的规定,且不违背公序良俗。

[0102] 根据本公开的实施例,本公开还提供了一种数字人的防伪装置,用于实现上述的数字人的防伪方法。

[0103] 图4是根据本公开一实施例的数字人的防伪装置的框图。

[0104] 如图4所示,数字人的防伪装置400,包括:身份验证模401、发送模块402、特征提取模块403和验证模块404。

[0105] 身份验证模块401,用于接收调用请求,所述调用请求包括客户端的访问令牌,并基于所述访问令牌对所述客户端进行身份验证;

[0106] 发送模块402,用于响应于通过身份验证,向所述客户端发送目标数字人,所述目标数字人对应的每帧内容携带隐形水印;

[0107] 特征提取模块403,用于接收所述客户端发送的数字人交互信息,并从所述数字人交互信息中提取所述目标数字人的加密行为特征;

[0108] 验证模块404,用于基于所述加密行为特征和所述隐形水印,对所述目标数字人进行防伪验证。

[0109] 在本公开的一个实施例中,所述验证模块404,用于:对所述加密行为特征进行解密,得到第一行为特征;从特征数据库中获取所述目标数字人对应的第二行为特征,并对所述第一行为特征和所述第二行为特征进行特征匹配;响应于满足所述目标数字人的行为特征未匹配成功和所述数字人交互信息未携带所述隐形水印中至少一项,确定所述目标数字

人未通过防伪验证。

[0110] 在本公开的一个实施例中,所述从特征数据库中获取所述目标数字人对应的第二行为特征,并对所述第一行为特征和所述第二行为特征进行特征匹配之前,所述装置400,用于:获取全量的候选数字人,并提取所述候选数字人的第二行为特征,其中所述目标数字人为所述全量的候选数字人中的一个;基于所述第二行为特征生成所述候选数字人的行为特征集合;根据所述候选数字人的行为特征集合,生成所述特征数据库。

[0111] 在本公开的一个实施例中,所述验证模块404,用于:根据所述目标数字人的标识信息,从所述特征数据库中获取所述目标数字人对应的目标行为特征集合;基于所述第一行为特征与所述目标行为特征集合中的第二行为特征进行匹配;响应于所述第一行为特征与所述目标行为特征集合中至少一个第二行为特征的匹配度大于设定值,确定所述目标数字人的行为特征匹配成功;响应于所述第一行为特征与所述目标行为特征集合中每个第二行为特征的匹配度均小于或等于所述设定值,确定所述目标数字人的行为特征未匹配成功。

[0112] 在本公开的一个实施例中,所述验证模块404,用于:根据所述数字人交互信息关联的帧号,确定所述第一行为特征关联的帧号;从所述目标行为特征集合中获取所述帧号所关联的第二行为特征;根据所述第一行为特征与所述帧号所关联的第二行为特征进行匹配;响应于所述第一行为特征与所述帧号所关联的第二行为特征的匹配度大于设定值,确定所述目标数字人的行为特征匹配成功;响应于所述第一行为特征与所述帧号所关联的第二行为特征的匹配度小于或等于所述设定值,确定所述目标数字人的行为特征未匹配成功。

[0113] 在本公开的一个实施例中,其中,所述向所述客户端发送目标数字人之前,所述装置400,用于:获取所述目标数字人的每帧内容的时间戳、所述目标数字人的上传设备标识和创建者标识;根据每帧内容的所述时间戳、所述上传设备标识和创建者标识,生成每帧内容对应的隐形水印,并在每帧内容和所述数字人模型的纹理中添加所述隐藏水印。

[0114] 在本公开的一个实施例中,所述身份验证模块401,用于:根据所述访问令牌,获取所述客户端对应的多种身份验证信息,所述多种身份验证信息包括所述客户端对应的第一身份关联信息和所述目标数字人对应的第二身份关联信息;对所述多种身份验证信息分别进行验证,响应于通过多种身份验证,确定所述客户端通过身份验证。

[0115] 在本公开的一个实施例中,所述装置400,用于:基于所述目标数字人的标识信息,确定所述目标数字人在区块链上的存储位置;基于所述存储位置对所述区块链进行访问,获取所述目标数字人对应的记录信息,并根据所述记录信息,对所述目标数字人进行版权验证。

[0116] 在本公开的一个实施例中,所述装置400,用于:基于所述目标数字人的标识信息,确定所述目标数字人在区块链上的存储位置;基于所述存储位置对所述区块链进行访问,获取所述目标数字人对应的记录信息,并根据所述记录信息,对所述目标数字人进行版权验证。

[0117] 在本公开的一个实施例中,所述装置400,用于:向所述区块链存储所述目标数字人的关联信息以生成所述目标数字人的记录信息,所述关联信息至少包括版权信息、创建信息、使用信息和更新信息中的至少一个。

[0118] 本公开提出的数字人的防伪装置,通过接收调用请求,调用请求包括客户端的访问令牌,并基于访问令牌对客户端进行身份验证,响应于通过身份验证,向客户端发送目标数字人,目标数字人对应的每帧内容携带隐形水印,接收客户端发送的数字人交互信息,并从数字人交互信息中提取目标数字人的加密行为特征,基于加密行为特征和隐形水印,对目标数字人进行防伪验证,由此,本公开基于加密行为特征和隐形水印,对数字人进行防伪验证,有效地解决了数字人的防伪问题,增强了数字人的防伪效果,保证了数字人安全稳定地使用。

[0119] 根据本公开的实施例,本公开还提供了一种数字人的防伪装置,用于实现上述的数字人的防伪方法。

[0120] 图5是根据本公开一实施例的数字人的防伪装置的框图。

[0121] 如图5所示,数字人的防伪装置500,包括:第一发送模块501、接收模块502、获取模块503和第二发送模块504。

[0122] 第一发送模块501,向服务器发送调用请求,所述调用请求包括客户端的访问令牌,所述访问令牌用于对所述客户端进行身份验证;

[0123] 接收模块502,用于接收所述服务器发送的目标数字人并进行展示,所述目标数字人的每帧内容携带隐藏水印;

[0124] 获取模块503,用于获取输入信息,并从所述目标数字人中提取所述目标数字人的第一行为特征;

[0125] 第二发送模块504,用于根据所述第一行为特征生成加密行为特征,并根据所述加密行为特征和所述输入信息生成数字人交互信息,并向所述服务器发送所述数字人交互信息。

[0126] 在本公开的一个实施例中,所述装置500,用于:获取所述数字人交互信息所关联的所述目标数字人中的内容帧,并从所述内容帧中提取所述第一行为特征;确定所述内容帧的帧号,并将所述内容帧的帧号与所述第一行为特征进行关联。

[0127] 在本公开的一个实施例中,所述第一发送模块,用于:获取所述客户端对应的第一身份关联信息和所述目标数字人的第二身份关联信息;基于所述多种身份验证信息,生成所述访问令牌,并基于所述访问令牌生成所述调用请求。

[0128] 在本公开的一个实施例中,所述装置500,用于:向区块链存储所述目标数字人的使用信息和更新信息中的至少一个,以更新所述区块链上存储的所述目标数字人的记录信息。

[0129] 在本公开的一个实施例中,所述装置500,用于:基于所述目标数字人的标识信息,确定所述目标数字人在区块链上的存储位置;基于所述存储位置对所述区块链进行访问,获取所述目标数字人的记录信息。

[0130] 在本公开的一个实施例中,所述装置500,用于:接收所述服务器发送与所述调用请求的指示信息,其中所述指示信息用于指示所述目标数字人未通过所述服务器基于区块链上的所述目标数字人的记录信息进行的版权验证。

[0131] 本公开提出的数字人的防伪装置,通过接收调用请求,调用请求包括客户端的访问令牌,并基于访问令牌对客户端进行身份验证,响应于通过身份验证,向客户端发送目标数字人,目标数字人对应的每帧内容携带隐形水印,接收客户端发送的数字人交互信息,并

从数字人交互信息中提取目标数字人的加密行为特征,基于加密行为特征和隐形水印,对目标数字人进行防伪验证,由此,本公开基于加密行为特征和隐形水印,对数字人进行防伪验证,有效地解决了数字人的防伪问题,增强了数字人的防伪效果,保证了数字人安全稳定地使用。

[0132] 根据本公开的实施例,本公开还提出了一种电子设备、一种可读存储介质和一种计算机程序产品。

[0133] 图6示出了可以用来实施本公开的实施例的示例电子设备600的示意性框图。电子设备旨在表示各种形式的数字计算机,诸如,膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动装置,诸如,个人数字处理、蜂窝电话、智能电话、可穿戴设备和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例,并且不意在限制本文中描述的和/或者要求的本公开的实现。

[0134] 如图6所示,设备600包括计算单元601,其可以根据存储在只读存储器(ROM)602中的计算机程序或者从存储单元608加载到随机访问存储器(RAM)603中的计算机程序,来执行各种适当的动作和处理。在RAM 603中,还可存储设备600操作所需的各种程序和数据。计算单元601、ROM 602以及RAM 603通过总线604彼此相连。输入/输出(I/O)接口605也连接至总线604。

[0135] 设备600中的多个部件连接至I/O接口605,包括:输入单元606,例如键盘、鼠标等;输出单元606,例如各种类型的显示器、扬声器等;存储单元608,例如磁盘、光盘等;以及通信单元609,例如网卡、调制解调器、无线通信收发机等。通信单元609允许设备600通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

[0136] 计算单元601可以是各种具有处理和计算能力的通用和/或专用处理组件。计算单元601的一些示例包括但不限于中央处理单元(CPU)、图形处理单元(GPU)、各种专用的人工智能(AI)计算芯片、各种运行机器学习模型算法的计算单元、数字信号处理器(DSP)、以及任何适当的处理器、控制器、微控制器等。计算单元601执行上文所描述的各个方法和处理,例如数字人的防伪方法。例如,在一些实施例中,数字人的防伪方法可被实现为计算机软件程序,其被有形地包含于机器可读介质,例如存储单元608。在一些实施例中,计算机程序的部分或者全部可以经由ROM 602和/或通信单元609而被载入和/或安装到设备600上。当计算机程序加载到RAM 603并由计算单元601执行时,可以执行上文描述的数字人的防伪方法的一个或多个步骤。备选地,在其他实施例中,计算单元601可以通过其他任何适当的方式(例如,借助于固件)而被配置为执行数字人的防伪方法。

[0137] 本文中以上描述的系统和技术的各种实施方式可以在数字电子电路系统、集成电路系统、场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、芯片上系统的系统(SOC)、负载可编程逻辑设备(CPLD)、计算机硬件、固件、软件、和/或它们的组合中实现。这些各种实施方式可以包括:实施在一个或者多个计算机程序中,该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释,该可编程处理器可以是专用或者通用可编程处理器,可以从存储系统、至少一个输入装置、和至少一个输出装置接收数据和指令,并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至少一个输出装置。

[0138] 用于实施本公开的方法的程序代码可以采用一个或多个编程语言的任何组合来编写。这些程序代码可以提出给通用计算机、专用计算机或其他可编程数据处理装置的处理器或控制器,使得程序代码当由处理器或控制器执行时使流程图和/或框图中所规定的功能/操作被实施。程序代码可以完全在机器上执行、部分地在机器上执行,作为独立软件包部分地在机器上执行且部分地在远程机器上执行或完全在远程机器或服务器上执行。

[0139] 在本公开的上下文中,机器可读介质可以是有形的介质,其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合地使用的程序。机器可读介质可以是机器可读信号介质或机器可读储存介质。机器可读介质可以包括但不限于电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备,或者上述内容的任何合适组合。机器可读存储介质的更具体示例会包括基于一个或多个线的电气连接、便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或快闪存储器)、光纤、便捷式紧凑盘只读存储器(CD-ROM)、光学储存设备、磁储存设备、或上述内容的任何合适组合。

[0140] 为了提出与用户账号的交互,可以在计算机上实施此处描述的系统和技术,该计算机具有:用于向用户账号显示信息的显示装置(例如,CRT(阴极射线管)或者LCD(液晶显示器)监视器);以及键盘和指向装置(例如,鼠标或者轨迹球),用户账号可以通过该键盘和该指向装置来将输入提出给计算机。其它种类的装置还可以用于提出与用户账号的交互;例如,提出给用户账号的反馈可以是任何形式的传感反馈(例如,视觉反馈、听觉反馈、或者触觉反馈);并且可以用任何形式(包括声输入、语音输入或者、触觉输入)来接收来自用户账号的输入。

[0141] 可以将此处描述的系统和技术实施在包括后台部件的计算系统(例如,作为数据服务器)、或者包括中间件部件的计算系统(例如,应用服务器)、或者包括前端部件的计算系统(例如,具有图形用户账号界面或者网络浏览器的用户账号计算机,用户账号可以通过该图形用户账号界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如,通信网络)来将系统的部件相互连接。通信网络的示例包括:局域网(LAN)、广域网(WAN)和互联网。

[0142] 计算机系统可以包括客户端和服务器。客户端和服务器一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。服务器可以是云服务器,也可以为分布式系统的服务器,或者是结合了区块链的服务器。

[0143] 根据本公开的实施例,本公开还提供了一种计算机程序产品,包括计算机程序,其中,所述计算机程序被处理器执行时实现本公开上述实施例所述的数字人的防伪方法的步骤。

[0144] 应该理解,可以使用上面所示的各种形式的流程,重新排序、增加或删除步骤。例如,本公开中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行,只要能够实现本公开公开的技术方案所期望的结果,本文在此不进行限制。

[0145] 上述具体实施方式,并不构成对本公开保护范围的限制。本领域技术人员应该明白的是,根据设计要求和其他因素,可以进行各种修改、组合、子组合和替代。任何在本公开

的精神和原则之内所作的修改、等同替换和改进等,均应包含在本公开保护范围之内。

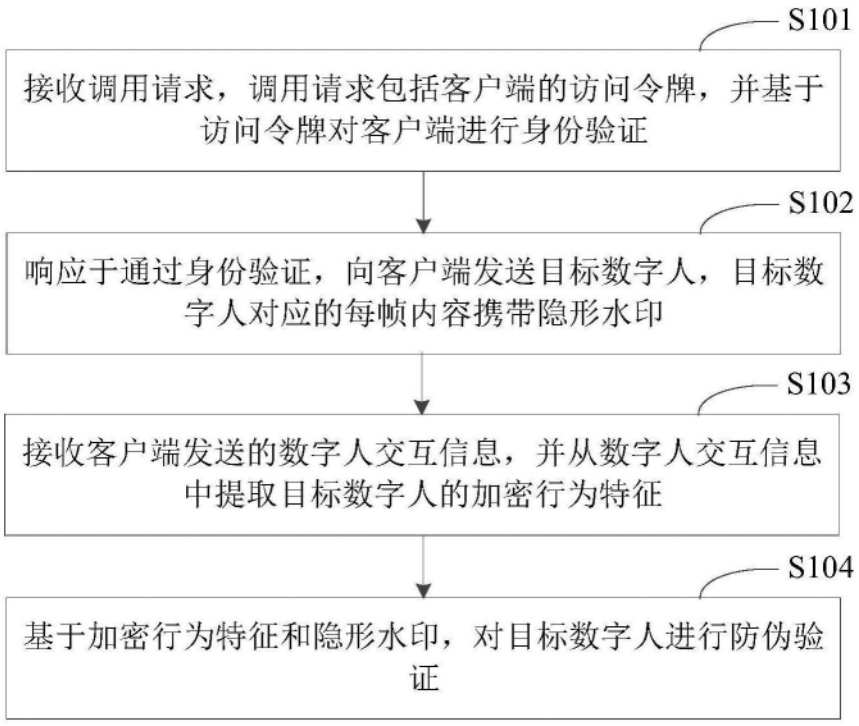

S101
接收调用请求，调用请求包括客户端的访问令牌，并基于访问令牌对客户端进行身份验证
S102
响应于通过身份验证，向客户端发送目标数字人，目标数字人对应的每帧内容携带隐形水印
S103
接收客户端发送的数字人交互信息，并从数字人交互信息中提取目标数字人的加密行为特征
S104
基于加密行为特征和隐形水印，对目标数字人进行防伪验证

图1

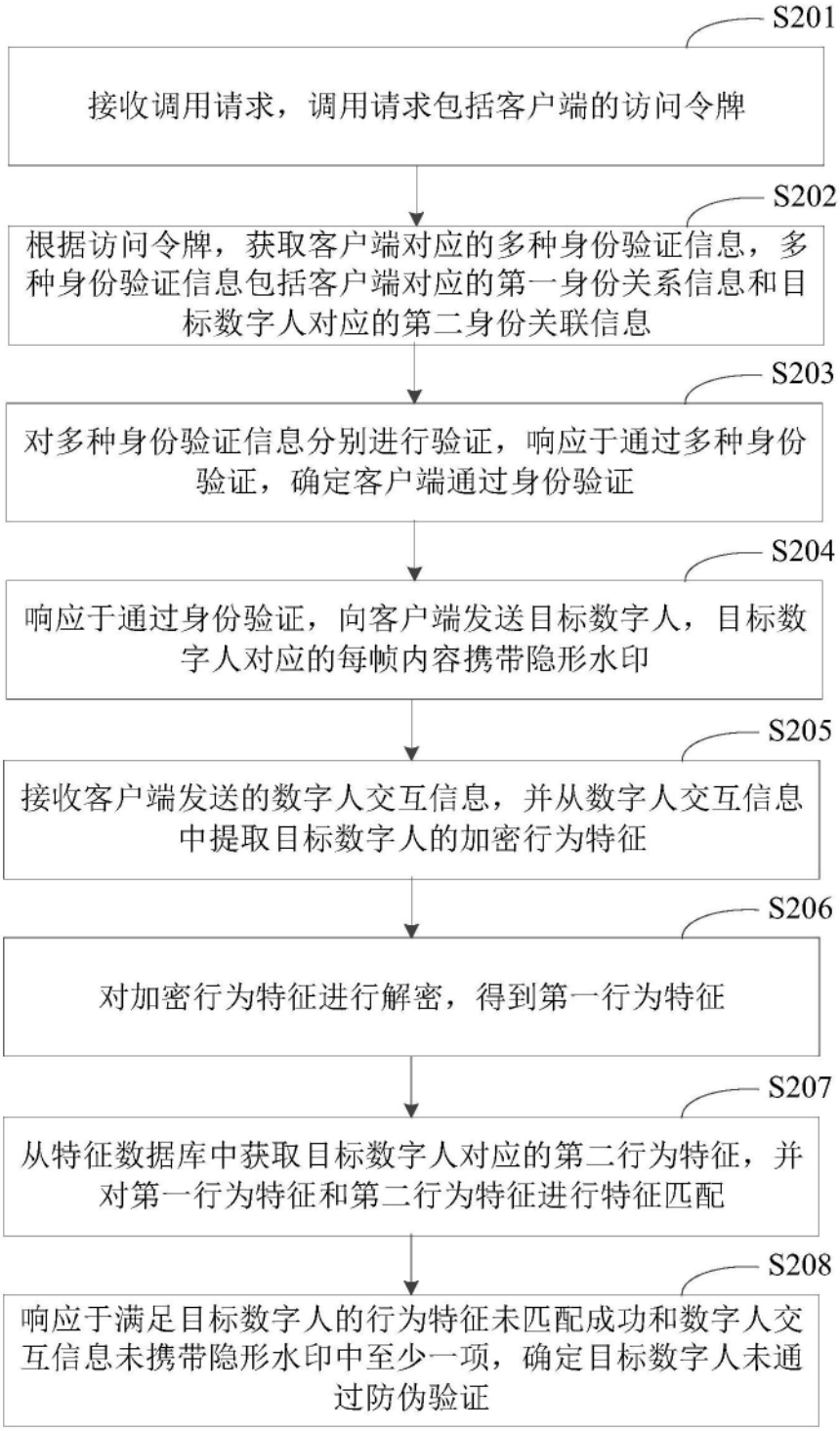

S201
接收调用请求，调用请求包括客户端的访问令牌
S202
根据访问令牌，获取客户端对应的多种身份验证信息，多种身份验证信息包括客户端对应的第一身份关系信息和目标数字人对应的第二身份关联信息
S203
对多种身份验证信息分别进行验证，响应于通过多种身份验证，确定客户端通过身份验证
S204
响应于通过身份验证，向客户端发送目标数字人，目标数字人对应的每帧内容携带隐形水印
S205
接收客户端发送的数字人交互信息，并从数字人交互信息中提取目标数字人的加密行为特征
S206
对加密行为特征进行解密，得到第一行为特征
S207
从特征数据库中获取目标数字人对应的第二行为特征，并对第一行为特征和第二行为特征进行特征匹配
S208
响应于满足目标数字人的行为特征未匹配成功和数字人交互信息未携带隐形水印中至少一项，确定目标数字人未通过防伪验证

图2

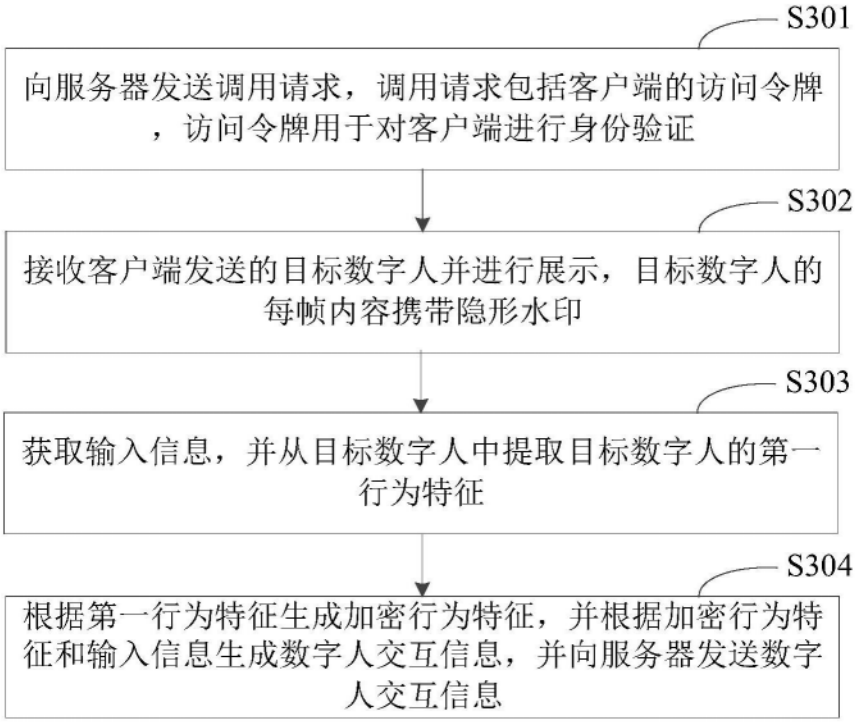

S301
向服务器发送调用请求，调用请求包括客户端的访问令牌，访问令牌用于对客户端进行身份验证
S302
接收客户端发送的目标数字人并进行展示，目标数字人的每帧内容携带隐形水印
S303
获取输入信息，并从目标数字人中提取目标数字人的第一行为特征
S304
根据第一行为特征生成加密行为特征，并根据加密行为特征和输入信息生成数字人交互信息，并向服务器发送数字人交互信息

图3

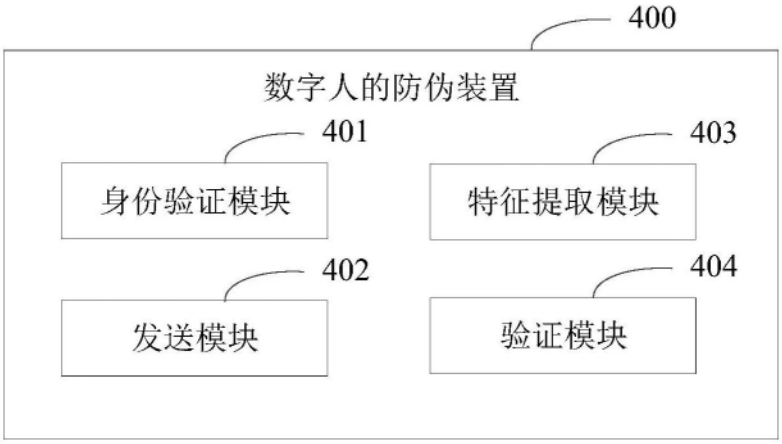

400
数字人的防伪装置
401
身份验证模块
403
特征提取模块
402
发送模块
404
验证模块

图4

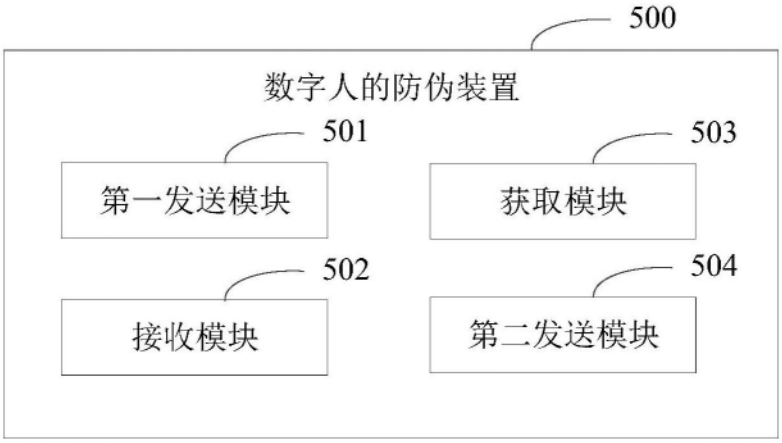

500
数字人的防伪装置
501
第一发送模块
503
获取模块
502
接收模块
504
第二发送模块

图5

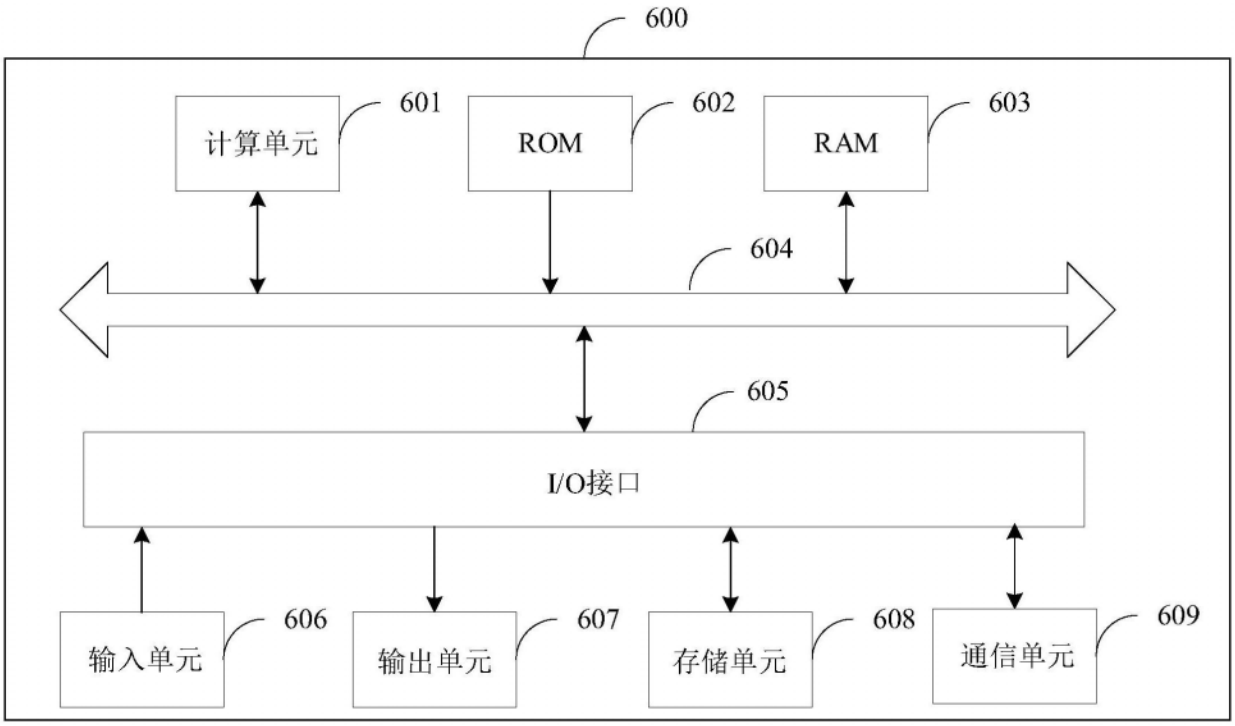

600
计算单元
601
ROM
602
RAM
603
604
605
I/O接口
输入单元
606
输出单元
607
存储单元
608
通信单元
609

图6