

(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 104683104 A

(43) 申请公布日 2015. 06. 03

(21) 申请号 201310643270. X

(22) 申请日 2013. 12. 03

(71) 申请人 腾讯科技(深圳)有限公司

地址 518044 广东省深圳市福田区振兴路赛  
格科技园 2 栋东 403 室

(72) 发明人 喻欣 金朝林 王小叶 芦姗

(74) 专利代理机构 上海波拓知识产权代理有限  
公司 31264

代理人 吕静

(51) Int. Cl.

H04L 9/32(2006. 01)

H04L 29/06(2006. 01)

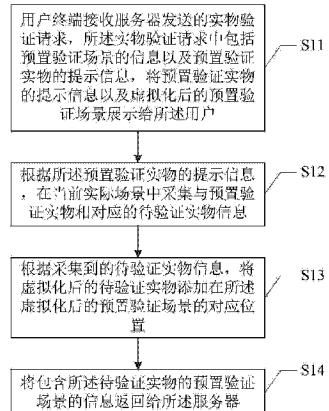
权利要求书4页 说明书16页 附图17页

(54) 发明名称

身份验证的方法、装置及系统

(57) 摘要

一种身份验证的方法，包括：用户终端接收服务器发送的实物验证请求，实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息，将预置验证实物的提示信息以及虚拟化后的预置验证场景展示给用户；根据预置验证实物的提示信息，在当前实际场景中采集与预置验证实物相对应的待验证实物信息；根据采集到的待验证实物信息，将虚拟化后的待验证实物添加在虚拟化后的预置验证场景的对应位置；将包含待验证实物的预置验证场景的信息返回给服务器，以使服务器根据预置验证场景以及预置验证实物对包含待验证实物的预置验证场景进行验证。此外，本发明还提供一种身份验证的装置及系统。上述身份验证的方法、装置及系统可提高身份验证的安全性。



1. 一种身份验证的方法,其特征在于,包括:

用户终端接收服务器发送的实物验证请求,所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息,将预置验证实物的提示信息以及虚拟化后的预置验证场景展示给所述用户;

根据所述预置验证实物的提示信息,在当前实际场景中采集与预置验证实物相对应的待验证实物信息;

根据采集到的待验证实物信息,将虚拟化后的待验证实物添加在所述虚拟化后的预置验证场景的对应位置;以及

将包含所述待验证实物的预置验证场景的信息返回给所述服务器,以使所述服务器根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证。

2. 根据权利要求 1 所述的方法,其特征在于,所述用户终端接收服务器发送的实物验证请求的步骤之前,还包括:

在当前实际场景中采集待验证场景的信息,并将所述待验证场景的信息发送给服务器,以使所述服务器根据预置验证场景对所述待验证场景进行验证。

3. 根据权利要求 2 所述的方法,其特征在于,所述在当前实际场景中采集待验证场景的信息的步骤之前,还包括:

用户终端接收用户所触发的身份注册请求,获取场景信息;

识别经用户确认的场景信息中的实物,将识别的所述实物展示给用户;

响应于所述用户根据展示的所述实物进行的选定操作,获取所述选定操作对应的实物作为所述预置验证实物;

将所述预置验证实物以及所述场景信息发送给所述服务器,其中,所述场景信息中去除所述验证实物的部分作为所述预置验证场景。

4. 根据权利要求 2 所述的方法,其特征在于,所述待验证场景以及所述待验证实物的信息由所述用户终端的图像采集设备采集。

5. 根据权利要求 1 所述的方法,其特征在于,所述根据采集到的待验证实物信息,将虚拟化后的待验证实物添加在所述虚拟化后的预置验证场景的对应位置的步骤,包括:

响应于所述用户对待验证实物的拖曳操作,将虚拟化的所述待验证实物移动至所述虚拟化后的预置验证场景中与所述拖曳操作对应的位置;或者

所述用户终端直接将所述虚拟化后的待验证实物移动至所述虚拟化后的预置验证场景的对应位置。

6. 根据权利要求 1 所述的方法,其特征在于,所述预置验证场景中包含至少一个预置验证实物的提示信息,所述提示信息包括:所述预置验证实物的名称,或者所述预置验证实物在所述预置验证场景中的位置信息。

7. 根据权利要求 6 所述的方法,其特征在于,所述预置验证实物在所述预置验证场景中的位置信息,通过在所述预置验证场景中将与所述预置验证实物对应的位置设置为空白的方式进行展示。

8. 一种身份验证的方法,其特征在于,包括:

服务器向用户终端发送实物验证请求,所述实物验证请求中包括预置验证场景的信息

以及预置验证实物的提示信息；

接收所述用户终端根据所述实物验证请求返回的包含待验证实物的预置验证场景的信息；以及

根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证，将所述验证的结果返回给所述用户终端。

9. 根据权利要求 8 所述的方法，其特征在于，所述服务器向用户终端发送实物验证请求的步骤之前，还包括：

服务器接收用户终端发送的场景信息以及所述预置验证实物的信息，将所述场景信息中去除所述预置验证实物的部分作为所述预置验证场景；

分析提取所述场景信息与所述预置验证实物的特征数据，将分析提取的所述特征数据预置于特征数据库中，以完成身份注册，所述预置验证实物的特征数据包括：所述预置验证实物的实物特征数据以及所述预置验证实物在所述场景信息中的位置数据；以及

将所述身份注册的结果返回给所述用户终端。

10. 根据权利要求 9 所述的方法，其特征在于，所述服务器向用户终端发送实物验证请求的步骤，包括：

向用户终端发送身份验证请求；

接收所述用户终端发送的待验证场景的信息，将所述待验证场景的特征与所述场景信息的特征进行比较；

当所述待验证场景的特征与所述场景信息的特征的相似度大于预置的数值时，向所述用户终端发送实物验证请求。

11. 根据权利要求 10 所述的方法，其特征在于，所述将所述待验证场景的特征与所述场景信息的特征进行比较的步骤包括：

分析提取所述待验证场景的特征数据；

将所述特征数据与预置于所述特征数据库中的所述场景信息的特征数据进行比较。

12. 根据权利要求 8 所述的方法，其特征在于，所述根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证的步骤，包括：

分析提取所述包含所述待验证实物的预置验证场景中的待验证实物的特征数据，所述待验证实物的特征数据包括：所述待验证实物的实物特征数据以及所述待验证实物在所述预置验证场景中的位置数据；

将所述待验证实物的实物特征数据以及所述待验证实物在所述预置验证场景中的位置数据，与预置于所述特征数据库中的所述预置验证实物的实物特征数据以及所述预置验证实物在所述场景信息中的位置数据进行比较。

13. 一种身份验证的装置，运行于用户终端，其特征在于，包括：

接收模块，用于接收服务器发送的实物验证请求，所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息，将预置验证实物的提示信息以及虚拟化后的预置验证场景展示给所述用户；

第一采集模块，用于根据所述接收模块接收的所述预置验证实物的提示信息，在当前实际场景中采集与预置验证实物相对应的待验证实物信息；

处理模块，用于根据所述第一采集模块采集到的待验证实物信息，将虚拟化后的待验

证实物添加在所述虚拟化后的预置验证场景的对应位置；以及

验证模块，用于将所述处理模块处理后的包含所述待验证实物的预置验证场景的信息返回给所述服务器，以使所述服务器根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证。

14. 根据权利要求 13 所述的装置，其特征在于，所述装置还包括：

第二采集模块，用于在当前实际场景中采集待验证场景的信息，并将所述待验证场景的信息发送给服务器，以使所述服务器根据预置验证场景对所述待验证场景进行验证。

15. 根据权利要求 14 所述的装置，其特征在于，所述装置还包括：

场景信息获取模块，用于接收用户所触发的身份注册请求，获取场景信息；

展示模块，用于识别经用户确认的场景信息中的实物，将识别的所述实物展示给用户；

实物获取模块，用于响应于所述用户根据展示的所述实物进行的选定操作，获取所述选定操作对应的实物作为所述预置验证实物；

发送模块，用于将所述预置验证实物以及所述场景信息发送给所述服务器，其中，所述场景信息中去除所述验证实物的部分作为所述预置验证场景。

16. 根据权利要求 14 所述的装置，其特征在于，所述待验证场景以及所述待验证实物的信息由所述用户终端的图像采集设备采集。

17. 根据权利要求 13 所述的装置，其特征在于，所述处理模块包括：

第一处理单元，用于响应于所述用户对待验证实物的拖曳操作，将虚拟化的所述待验证实物移动至所述虚拟化后的预置验证场景中与所述拖曳操作对应的位置；

第二处理单元，用于直接将所述虚拟化后的待验证实物移动至所述虚拟化后的预置验证场景的对应位置。

18. 根据权利要求 13 所述的装置，其特征在于，所述预置验证场景中包含至少一个预置验证实物的提示信息，所述提示信息包括：所述预置验证实物的名称，或者所述预置验证实物在所述预置验证场景中的位置信息。

19. 根据权利要求 18 所述的装置，其特征在于，所述预置验证实物在所述预置验证场景中的位置信息，通过在所述预置验证场景中将与所述预置验证实物对应的位置设置为空白的方式进行展示。

20. 一种身份验证的装置，运行于服务器，其特征在于，包括：

实物验证请求发送模块，用于向用户终端发送实物验证请求，所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息；

第一接收模块，用于接收所述用户终端根据所述实物验证请求返回的包含待验证实物的预置验证场景的信息；以及

验证模块，用于根据所述第一接收模块接收的所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证，将所述验证的结果返回给所述用户终端。

21. 根据权利要求 20 所述的装置，其特征在于，所述装置还包括：

第二接收模块，用于接收用户终端发送的场景信息以及所述预置验证实物的信息，将所述场景信息中去除所述预置验证实物的部分作为所述预置验证场景；

身份注册模块,用于分析提取所述第二接收模块接收的所述场景信息与所述预置验证实物的特征数据,将分析提取的所述特征数据预置于特征数据库中,以完成身份注册,所述预置验证实物的特征数据包括:所述预置验证实物的实物特征数据以及所述预置验证实物在所述场景信息中的位置数据;以及

注册结果发送模块,用于将所述身份注册模块获取的所述身份注册的结果返回给所述用户终端。

22. 根据权利要求 21 所述的装置,其特征在于,所述实物验证请求发送模块包括:

身份验证请求发送单元,用于向用户终端发送身份验证请求;

比较单元,用于接收所述用户终端发送的待验证场景的信息,将所述待验证场景的特征与所述场景信息的特征进行比较;

实物验证请求发送单元,用于当所述待验证场景的特征与所述场景信息的特征的相似度大于预置的数值时,向所述用户终端发送实物验证请求。

23. 根据权利要求 22 所述的装置,其特征在于,

所述比较单元,还用于分析提取所述待验证场景的特征数据,将所述特征数据与预置于所述特征数据库中的所述场景信息的特征数据进行比较。

24. 根据权利要求 20 所述的装置,其特征在于,所述验证模块包括:

分析提取单元,用于分析提取所述包含所述待验证实物的预置验证场景中的待验证实物的特征数据,所述待验证实物的特征数据包括:所述待验证实物的实物特征数据以及所述待验证实物在所述预置验证场景中的位置数据;

比较单元,用于将所述待验证实物的实物特征数据以及所述待验证实物在所述预置验证场景中的位置数据,与预置于所述特征数据库中的所述预置验证实物的实物特征数据以及所述预置验证实物在所述场景信息中的位置数据进行比较。

25. 一种身份验证的系统,其特征在于,包括:用户终端及服务器,

所述用户终端配置有如权利要求 13 至 19 中的任一项所述的装置;以及

所述服务器配置有如权利要求 20 至 24 中的任一项所述的装置。

## 身份验证的方法、装置及系统

### 技术领域

[0001] 本发明涉及计算机通信技术，尤其涉及一种身份验证的方法、装置及系统。

### 背景技术

[0002] 随着移动互联网的发展，越来越多的基于手机等用户终端的应用走进人们的日常生活中，比如通过手机支付购物、手机银行、手机游戏等，这些应用通常涉及货币、游戏装备等个人财产，如果用户的个人帐户被盗，则用户的财产也存在被盗用、交易的风险。现有技术中，一般通过密码对用户的身份进行验证来保护用户的财产安全。但是，密码通常由一串字符组成，规律性较强，容易被非法用户根据用户的个人信息猜测出来或通过破解器暴力破解，因此安全性较低。

### 发明内容

[0003] 有鉴于此，本发明提供一种身份验证的方法、装置及系统，可提高身份验证的安全性。

[0004] 一种身份验证的方法，包括：用户终端接收服务器发送的实物验证请求，所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息，将预置验证实物的提示信息以及虚拟化后的预置验证场景展示给所述用户；根据所述预置验证实物的提示信息，在当前实际场景中采集与预置验证实物相对应的待验证实物信息；根据采集到的待验证实物信息，将虚拟化后的待验证实物添加在所述虚拟化后的预置验证场景的对应位置；以及将包含所述待验证实物的预置验证场景的信息返回给所述服务器，以使所述服务器根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证。

[0005] 一种身份验证的方法，包括：服务器向用户终端发送实物验证请求，所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息；接收所述用户终端根据所述实物验证请求返回的包含待验证实物的预置验证场景的信息；以及根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证，将所述验证的结果返回给所述用户终端。

[0006] 一种身份验证的装置，运行于用户终端，包括：接收模块，用于接收服务器发送的实物验证请求，所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息，将预置验证实物的提示信息以及虚拟化后的预置验证场景展示给所述用户；第一采集模块，用于根据所述接收模块接收的所述预置验证实物的提示信息，在当前实际场景中采集与预置验证实物相对应的待验证实物信息；处理模块，用于根据所述第一采集模块采集到的待验证实物信息，将虚拟化后的待验证实物添加在所述虚拟化后的预置验证场景的对应位置；以及验证模块，用于将所述处理模块处理后的包含所述待验证实物的预置验证场景的信息返回给所述服务器，以使所述服务器根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证。

[0007] 一种身份验证的装置,运行于服务器,包括:实物验证请求发送模块,用于向用户终端发送实物验证请求,所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息;第一接收模块,用于接收所述用户终端根据所述实物验证请求返回的包含待验证实物的预置验证场景的信息;以及验证模块,用于根据所述第一接收模块接收的所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证,将所述验证的结果返回给所述用户终端。

[0008] 一种身份验证的系统,包括:配置有上述装置的用户终端;以及配置有上述装置的服务器。

[0009] 本发明实施例提供的身份验证的方法、装置及系统,通过用户终端根据服务器发送的实物验证请求,在当前实际场景中采集与预置验证实物相对应的待验证实物信息,然后将获取的待验证实物虚拟化后放置在虚拟化的预置验证场景的对应位置,并将放置了虚拟化后的待验证实物的预置验证场景的信息返回给服务器,以使服务器通过分析提取预置验证场景的信息中的待验证实物的特征数据,并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身分进行最终验证,由于是通过当前实际场景中采集的待验证实物的特征数据来进行身份验证,而非法用户通常难以获取到待验证场景与待验证实物的信息,并且也无法通过算法破解的方式获得上述特征数据,因此可提高身份验证的安全性。

[0010] 为让本发明的上述和其他目的、特征和优点能更明显易懂,下文特举较佳实施例,并配合所附图式,作详细说明如下。

## 附图说明

[0011] 图 1 示出了一种用户终端的结构框图。

[0012] 图 2 为本发明第一实施例提供的在用户终端内进行身份验证的方法的流程图。

[0013] 图 3 为本发明第二实施例提供的在用户终端内进行身份验证的方法的流程图。

[0014] 图 4 为本发明第二实施例提供的在用户终端内进行身份验证的方法中用于身份注册的场景信息的示意图。

[0015] 图 5 为本发明第二实施例提供的在用户终端内进行身份验证的方法中用于身份注册的实物信息的示意图。

[0016] 图 6 为本发明第三实施例提供的身份验证的方法的流程图。

[0017] 图 7 为本发明第三实施例提供的身份验证的方法中预置验证场景的示意图。

[0018] 图 8 为本发明第三实施例提供的身份验证的方法中待验证实物被移动后的预置验证场景的示意图。

[0019] 图 9 为本发明第四实施例提供的身份验证的方法的流程图。

[0020] 图 10 为本发明第四实施例提供的身份验证的方法中部分步骤的细节流程图。

[0021] 图 11 为本发明第四实施例提供的身份验证的方法中部分步骤的细节流程图。

[0022] 图 12 为本发明第五实施例提供的身份验证的方法的应用环境图。

[0023] 图 13 为本发明第五实施例提供的身份验证的方法的流程图。

[0024] 图 14 为本发明第六实施例提供的在用户终端内进行身份验证的装置的结构示意图。

[0025] 图 15 为图 14 的装置的存储环境示意图。

[0026] 图 16 为本发明第七实施例提供的在用户终端内进行身份验证的装置的结构示意图。

[0027] 图 17 为本发明第七实施例提供的在用户终端内进行身份验证的装置中部分模块的结构示意图。

[0028] 图 18 为本发明第八实施例提供的身份验证的装置的结构示意图。

[0029] 图 19 为本发明第九实施例提供的身份验证的装置的结构示意图。

[0030] 图 20 为本发明第九实施例提供的身份验证的装置中部分模块的结构示意图。

[0031] 图 21 为本发明第九实施例提供的身份验证的装置中部分模块的结构示意图。

[0032] 图 22 为本发明实施例提供的身份验证的系统的结构示意图。

## 具体实施方式

[0033] 为更进一步阐述本发明为实现预定发明目的所采取的技术手段及功效,以下结合附图及较佳实施例,对依据本发明的具体实施方式、结构、特征及其功效,详细说明如后。

[0034] 本发明实施例所提供的身份验证的方法可应用于用户终端中实现身份验证,用户终端可以包括智能手机、平板电脑、电子书阅读器、MP3 播放器(Moving Picture Experts Group Audio Layer III, 动态影像专家压缩标准音频层面 3)、MP4 (Moving Picture Experts Group Audio Layer IV, 动态影像专家压缩标准音频层面 4) 播放器、膝上型便携计算机、车载电脑、台式计算机等等。

[0035] 图 1 示出了一种用户终端的结构框图。如图 1 所示,用户终端 100 包括存储器 102、存储控制器 104,一个或多个(图中仅示出一个)处理器 106、外设接口 108、射频模块 110、定位模块 112、图像采集设备 114、音频模块 116、触控屏幕 118 以及按键模块 120。这些组件通过一条或多条通讯总线 / 信号线 122 相互通讯。

[0036] 可以理解,图 1 所示的结构仅为示意,用户终端 100 还可包括比图 1 中所示更多或者更少的组件,或者具有与图 1 所示不同的配置。图 1 中所示的各组件可以采用硬件、软件或其组合实现。

[0037] 存储器 102 可用于存储软件程序以及模块,如本发明实施例中的在用户终端内进行身份验证的方法及装置对应的程序指令 / 模块,处理器 106 通过运行存储在存储器 104 内的软件程序以及模块,从而执行各种功能应用以及数据处理,即实现上述的在用户终端内进行身份验证的方法。

[0038] 存储器 102 可包括高速随机存储器,还可包括非易失性存储器,如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中,存储器 102 可进一步包括相对于处理器 106 远程设置的存储器,这些远程存储器可以通过网络连接至用户终端 100。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。处理器 106 以及其他可能的组件对存储器 102 的访问可在存储控制器 104 的控制下进行。

[0039] 外设接口 108 将各种输入 / 输入装置耦合至 CPU 以及存储器 102。处理器 106 运行存储器 102 内的各种软件、指令以执行用户终端 100 的各种功能以及进行数据处理。

[0040] 在一些实施例中,外设接口 108,处理器 106 以及存储控制器 104 可以在单个芯片中实现。在其他一些实例中,他们可以分别由独立的芯片实现。

[0041] 射频模块 110 用于接收以及发送电磁波,实现电磁波与电信号的相互转换,从而

与通讯网络或者其他设备进行通讯。射频模块 110 可包括各种现有的用于执行这些功能的电路元件,例如,天线、射频收发器、数字信号处理器、加密 / 解密芯片、用户身份模块 (SIM) 卡、存储器等等。射频模块 110 可与各种网络如互联网、企业内部网、无线网络进行通讯或者通过无线网络与其他设备进行通讯。上述的无线网络可包括蜂窝式电话网、无线局域网或者城域网。上述的无线网络可以使用各种通信标准、协议及技术,包括但并不限于全球移动通信系统(Global System for Mobile Communication, GSM)、增强型移动通信技术(Enhanced Data GSM Environment, EDGE), 宽带码分多址技术(wideband code division multiple access, W-CDMA), 码分多址技术(Code division access, CDMA)、时分多址技术(time division multiple access, TDMA), 蓝牙, 无线保真技术(Wireless, Fidelity, WiFi) (如美国电气和电子工程师协会标准 IEEE802.11a, IEEE802.11b, IEEE802.11g 和 / 或 IEEE802.11n)、网络电话(Voice over internet protocol, VoIP)、全球微波互联接入(Worldwide Interoperability for Microwave Access, Wi-Max)、其他用于邮件、即时通讯及短消息的协议,以及任何其他合适的通讯协议,甚至可包括那些当前仍未被开发出来的协议。

[0042] 定位模块 112 用于获取用户终端 100 的当前位置。定位模块 112 的实例包括但不限于全球卫星定位系统(GPS)、基于无线局域网或者移动通信网的定位技术。

[0043] 图像采集设备 114 用于拍摄照片或者视频。拍摄的照片或者视频可以存储至存储器 102 内,并通过射频模块 110 发送。

[0044] 音频模块 116 向用户提供音频接口,其可包括一个或多个麦克风、一个或者多个扬声器以及音频电路。音频电路从外设接口 108 处接收声音数据,将声音数据转换为电信号,将电信号传输至扬声器。扬声器将电信号转换为人耳能听到的声波。音频电路还从麦克风处接收电信号,将电信号转换为声音数据,并将声音数据传输至外设接口 108 中以进行进一步的处理。音频数据可以从存储器 102 处或者通过射频模块 110 获取。此外,音频数据也可以存储至存储器 102 中或者通过射频模块 110 进行发送。在一些实例中,音频模块 116 还可包括一个耳机插孔,用于向耳机或者其他设备提供音频接口。

[0045] 触控屏幕 118 在用户终端 100 与用户之间同时提供一个输出及输入界面。具体地,触控屏幕 118 向用户显示视频输出,这些视频输出的内容可包括文字、图形、视频、及其任意组合。一些输出结果是对应于一些用户界面对象。触控屏幕 118 还接收用户的输入,例如用户的点击、滑动等手势操作,以便用户界面对象对这些用户的输入做出响应。检测用户输入的技术可以是基于电阻式、电容式或者其他任意可能的触控检测技术。触控屏幕 118 显示单元的具体实例包括但不限于液晶显示器或发光聚合物显示器。

[0046] 按键模块 120 同样提供用户向用户终端 100 进行输入的接口,用户可以通过按下不同的按键以使用户终端 100 执行不同的功能。

[0047] 第一实施例

[0048] 图 2 为本发明第一实施例提供的在用户终端内进行身份验证的方法的流程图。如图 2 所示,本实施例的身份验证的方法包括以下步骤:

[0049] 步骤 S11,用户终端接收服务器发送的实物验证请求,所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息,将预置验证实物的提示信息以及虚拟化后的预置验证场景展示给所述用户。

[0050] 具体地,首先,用户终端通过预置的客户端程序,响应于用户操作,向服务器发送获取用户操作对应业务的请求,服务器响应用户终端发送的请求,根据预置的规则,向用户终端发送实物验证请求,以验证用户终端的用户的身份是否合法。其中,获取的业务具体可包括:电子支付业务、网络社群业务、即时通讯业务等等。

[0051] 其次,用户终端对接收的实物验证请求中的预置验证场景进行虚拟化处理,将虚拟化后的预置验证场景与图像采集设备当前拍摄的画面进行叠加,然后将叠加后的画面展示给用户,所展示的画面中至少可包含一个预置验证实物的提示信息。可以理解的,虚拟化后的预置验证场景可以三维图片、视频等形式存在。预置验证实物可以是用户在进行身份注册时所确认的验证实物。于本实施例一具体实施方式中,对预置验证场景进行虚拟化处理也可由服务器完成。

[0052] 由于用户在使用用户终端的过程中是活动的,也即用户终端相对于拍摄对象的位置是随时在变化的,比如用户为了获得最佳拍摄效果,会将用户终端靠近拍摄对象或改变拍摄角度等,可以理解的,用户终端在侦测到自身位置发生变化时(也即用户的视角发生变化时),可实时获取用户终端因位置变化而产生的移动数据,然后通过对获取的移动数据进行计算,并根据计算结果对虚拟化后的预置验证场景进行调整,以使虚拟化后的预置验证场景可始终保持与图像采集设备当前拍摄的画面最大限度的叠加在一起,从而可为用户提供较佳的视觉感受。

[0053] 预置验证实物的提示信息可包括:预置验证实物的名称,或者预置验证实物在预置验证场景中的位置信息,或者预置验证实物的名称及其在预置验证场景中的位置信息。预置验证实物的提示信息用于提示用户预置验证实物是什么,或者预置验证实物在预置验证场景中的位置。于本实施例一具体实施方式中,预置验证实物在预置验证场景中的位置信息,可通过在预验证场景中将与预置验证实物对应的位置设置为空白的方式进行展示。

[0054] 步骤 S12,根据所述预置验证实物的提示信息,在当前实际场景中采集与预置验证实物相对应的待验证实物信息。

[0055] 具体地,用户终端根据预置验证实物的提示信息,响应于用户的实物采集操作,通过内置或外设的图像采集设备(例如:摄像头),在当前实际场景中采集与预置验证实物相对应的待验证实物信息。待验证实物的信息可包括待验证实物的影像、画面、图片等等。当前实际场景即为用户终端的用户当前实际身处的生活环境。

[0056] 步骤 S13,根据采集到的待验证实物信息,将虚拟化后的待验证实物添加在所述虚拟化后的预置验证场景的对应位置。

[0057] 于本实施例一具体实施方式中,用户终端对采集到的待验证实物的信息进行识别,获取其中的待验证实物的数据,并根据获取的数据,将待验证实物虚拟化后显示在屏幕中。然后,用户终端可响应于用户对屏幕中显示的虚拟化后的待验证实物的拖曳操作,将虚拟化后的待验证实物移动至虚拟化后的预置验证场景中与拖曳操作对应的位置。于本实施例另一具体实施方式中,用户终端也可在将待验证实物虚拟化后,直接将虚拟化后的待验证实物移动并显示在虚拟化后的预置验证场景的对应位置。

[0058] 上述将预置验证场景与待验证实物的进行虚拟化,将虚拟化后的预置验证场景与图像采集设备当前拍摄的画面进行叠加,以及将虚拟化后的待验证实物的进行移动可通过增强现实技术实现。增强现实技术,也被称之为混合现实技术。它通过计算机图形技术和可

视化技术,将虚拟的信息应用到真实世界,真实的环境和虚拟的物体实时地叠加到了同一个画面或空间同时存在。增强现实提供了在一般情况下,不同于人类可以感知的信息。它不仅展现了真实世界的信息而且将虚拟的信息同时显示出来,两种信息相互补充、叠加。通过利用增强现实技术可以使得身份验证更具有直观性,并且可以防止非法用户通过照片伪造认证,从而可提高身份验证的安全性。

[0059] 步骤 S14,将包含所述待验证实物的预置验证场景的信息返回给所述服务器,以使所述服务器根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证。

[0060] 本发明实施例提供的身份验证的方法,通过用户终端根据服务器发送的实物验证请求,在当前实际场景中采集与预置验证实物相对应的待验证实物信息,然后将获取的待验证实物虚拟化后放置在虚拟化的预置验证场景的对应位置,并将放置了虚拟化后的待验证实物的预置验证场景的信息返回给服务器,以使服务器通过分析提取预置验证场景的信息中的待验证实物的特征数据,并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身分进行最终验证,由于是通过当前实际场景中采集的待验证实物的特征数据来进行身份验证,而非法用户通常难以获取到待验证场景与待验证实物的信息,并且也无法通过算法破解的方式获得上述特征数据,因此可提高身份验证的安全性。

#### [0061] 第二实施例

[0062] 图 3 为本发明第二实施例提供的在用户终端内进行身份验证的方法的流程图。如图 3 所示,本实施例的身份验证的方法包括以下步骤:

[0063] 步骤 S21,用户终端接收用户所触发的身份注册请求,获取场景信息。

[0064] 场景信息具体可以包括即时拍摄的用户生活环境的影像、画面、图片等等。当用户终端之后根据用户的操作,向服务器请求获取预先约定的业务时,该场景信息可以用于用户身份的初步验证以及验证场景的生成。用户终端根据用户的获取场景信息的操作,通过内置或外设的图像采集设备获取与用户的操作对应的场景信息,比如:通过摄像头拍摄获取用户指定的书房一角的图片(如图 4 所示)。由于是利用用户所熟悉并且一般只有用户本人才能出入的生活环境的场景作为身份验证凭证,因此可减少用户的记忆成本,降低身份验证的复杂度,同时提高身份验证的安全性。

[0065] 步骤 S22,识别经用户确认的场景信息中的实物,将识别的所述实物展示给用户。

[0066] 具体地,用户终端可以通过图像识别技术,识别获取的场景信息中的实物,并将识别出的实物展示给用户(如图 5 所示),例如:假设场景信息为拍摄的书房的一角的照片,则用户终端可以通过识别技术识别该照片中的瓷器、书籍、闹钟等实物,然后通过增强现实技术以及虚拟技术,将识别出的实物虚拟化后展示给用户。其中,场景信息经过用户确认。

[0067] 步骤 S23,响应于所述用户根据展示的所述实物进行的选定操作,获取所述选定操作对应的实物作为所述预置验证实物。

[0068] 可以理解的,用户的选定操作对应的实物可以为一个,也可以为多个(两个或两个以上)。

[0069] 步骤 S24,将所述预置验证实物以及所述场景信息发送给所述服务器,以进行身份注册。

[0070] 具体的,用户终端将经用户确认选定的预置验证实物以及场景信息发送给服务

器,以进行身份注册,当服务器成功对该用户终端对应的用户进行身份注册后,服务器将根据该预置验证实物以及场景信息,对用户终端对应的用户进行身份验证。其中,场景信息中去除所述验证实物的部分将作为预置验证场景,在身份验证时由服务器提供给用户终端。

[0071] 步骤 S25,接收服务器发起的身份验证请求,根据所述身份验证请求在当前实际场景中采集待验证场景的信息,并将所述待验证场景的信息发送给服务器,以使所述服务器根据预置验证场景对所述待验证场景进行验证。

[0072] 具体地,首先用户终端通过预置的客户端程序,响应于用户操作,向服务器发送获取用户操作对应业务的请求,服务器响应用户终端发送的请求,根据预置的规则,向用户终端发起身份验证请求。

[0073] 其次,用户终端根据服务器发起的身份验证请求,通过内置或外设的图像采集设备(例如:内置摄像头)在当前实际场景中采集待验证场景的信息,然后将采集的待验证场景的信息发送给服务器,以使服务器根据用户终端在身份注册时发生给服务器的场景信息对待验证场景进行验证。待验证场景的信息可包括待验证场景的影像、画面、图片等等。当待验证场景验证成功后,服务器将会向用户终端发送实物验证请求,以对用户终端的用户的身份做进一步的验证。

[0074] 步骤 S26,接收服务器发送的实物验证请求,所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息,将预置验证实物的提示信息以及虚拟化后的预置验证场景展示给所述用户。

[0075] 步骤 S27,根据所述预置验证实物的提示信息,在当前实际场景中采集与预置验证实物相对应的待验证实物信息。

[0076] 步骤 S28,根据采集到的待验证实物信息,将虚拟化后的待验证实物添加在所述虚拟化后的预置验证场景的对应位置。

[0077] 步骤 S29,将包含所述待验证实物的预置验证场景的信息返回给所述服务器,以使所述服务器根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证。

[0078] 步骤 S26 至步骤 S29 具体可参考第一实施例的相应内容,此处不再赘述。

[0079] 本发明实施例提供的身份验证的方法,通过用户终端根据服务器发送的实物验证请求,在当前实际场景中采集与预置验证实物相对应的待验证实物信息,然后将获取的待验证实物虚拟化后放置在虚拟化的预置验证场景的对应位置,并将放置了虚拟化后的待验证实物的预置验证场景的信息返回给服务器,以使服务器通过分析提取预置验证场景的信息中的待验证实物的特征数据,并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身份进行最终验证,由于是通过当前实际场景中采集的待验证实物的特征数据来进行身份验证,而非法用户通常难以获取到待验证场景与待验证实物的信息,并且也无法通过算法破解的方式获得上述特征数据,因此可提高身份验证的安全性。

[0080] 第三实施例

[0081] 图 6 为本发明第三实施例提供的身份验证的方法的流程图。如图 6 所示,本实施例的身份验证的方法包括以下步骤:

[0082] 步骤 S31,服务器向用户终端发送实物验证请求,所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息。

[0083] 于本实施例一具体实施方式中,预置验证场景可由服务器根据用户终端在身份注册时发送的场景信息以及预置验证实物生成,具体可表现为一幅缺失预置验证实物的场景图像(如图 7 所示)。

[0084] 预置验证实物的提示信息可包括:预置验证实物的名称,或者预置验证实物在预置验证场景中的位置信息,或者预置验证实物的名称及其在预置验证场景中的位置信息。预置验证实物的提示信息用于提示用户预置验证实物是什么,或者预置验证实物在预置验证场景中的位置。

[0085] 步骤 S32,接收所述用户终端根据所述实物验证请求返回的包含待验证实物的预置验证场景的信息。

[0086] 具体地,服务器接收用户终端根据实物验证请求返回的预置验证场景的信息,该预置验证场景的信息中至少包含一个待验证实物,该待验证实物经用户确认已经移动至预置验证场景中的对应位置(如图 8 所示)。

[0087] 步骤 S33,根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证,将所述验证的结果返回给所述用户终端。

[0088] 具体地,服务器根据预置验证场景以及预置验证实物,对包含待验证实物的预置验证场景进行验证。若预置验证实物为多个,可根据预置的验证规则,只要多个待验证实物中至少有一个实物与预置验证实物一致,或当多个待验证实物均与预置验证实物一致时,可最终确认所述用户终端对应的用户身份合法,并将验证的结果返回给用户终端。

[0089] 本发明实施例提供的身份验证的方法,通过服务器向用户终端发送实物验证请求,接收用户终端返回的放置了虚拟化后的待验证实物的预置验证场景的信息,然后通过分析提取预置验证场景的信息中的待验证实物的特征数据,并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身份进行最终验证,由于是通过待验证场景与待验证实物的特征数据来进行身份验证,上述特征数据只能通过分析待验证场景与待验证实物的信息获得,而非法用户通常难以获取到待验证场景与待验证实物的信息,并且也无法通过算法破解的方式获得上述特征数据,因此可提高身份验证的安全性。

#### [0090] 第四实施例

[0091] 图 9 为本发明第四实施例提供的身份验证的方法的流程图。如图 9 所示,本实施例的身份验证的方法包括以下步骤:

[0092] 步骤 S41,服务器接收用户终端的身份注册请求,对所述用户终端的身份进行注册。

[0093] 具体地,如图 10 所示,本步骤具体可包括以下步骤:

[0094] 步骤 S411,服务器接收用户终端发送的身份注册请求。

[0095] 所述身份注册请求中可包含:用户帐号、用于身份注册的场景信息以及所述预置验证实物的信息。服务器接收并存储用户终端发送的用户帐号、用于身份注册的场景信息以及所述预置验证实物的信息,并当后续对该用户终端进行身份验证时,将所述场景信息中去除所述验证实物的部分作为所述预置验证场景返回给该用户终端。

[0096] 步骤 S412,分析提取身份注册请求中包含的场景信息与预置验证实物的特征数据,将分析提取的特征数据预置于特征数据库中,以完成身份注册。

[0097] 具体地,服务器对场景信息与预置验证实物进行几何归一化和灰度归一化处理,

然后提取相关特征数据,特征特殊提取的方法包括但不限于:基于几何特征、局部特征、神经网络等方法的选择。其中,预置验证实物的特征数据可以包括:预置验证实物的实物特征数据(例如:颜色、形状等)以及预置验证实物在场景信息中的位置数据。

[0098] 服务器将提取的场景信息与预置验证实物的特征数据存储于特征数据库中,并将上述特征数据与用户终端对应的用户信息进行关联,以完成身份注册,并将身份注册的结果返回给所述用户终端。

[0099] 步骤 S42,服务器向用户终端发送身份验证请求。

[0100] 具体地,服务器可在接收到用户终端发送的获取预约业务的请求时,响应于该请求发起身份验证,向用户终端发送身份验证请求。该获取预约业务的请求中可包含用户帐号的信息。

[0101] 步骤 S43,接收用户终端发送的待验证场景的信息,分析提取所述待验证场景的特征数据,将所述特征数据与预置于所述特征数据库中的所述场景信息的特征数据进行比较。

[0102] 具体地,服务器接收用户终端发送的待验证场景的信息,首先对接收的待验证场景的信息进行分析,提取待验证场景的特征数据,然后根据用户帐号,从特征数据库中提取与该用户帐号对应的场景信息的特征数据,将分析提取的待验证场景的特征数据与特征数据库中的场景信息的特征数据进行比较,分析二者的相似度是否大于预置的数值。

[0103] 步骤 S44,当所述待验证场景的特征与所述场景信息的特征的相似度大于预置的数值时,向所述用户终端发送实物验证请求,所述实物验证请求中包含所述预置验证场景的信息,以使所述用户终端将虚拟化后的所述预置验证场景展示给所述用户。

[0104] 具体地,服务器将提取的待验证场景的特征与特征数据库中存储的场景信息的特征进行比较,当二者的相似度大于预置的数值(例如:60% 或 80%)时,可判定待验证场景与身份注册时提供的场景信息基本一致,初步验证用户终端对应用户的身分是合法的,并向用户终端发送实物验证请求,以对该用户的身分进行进一步验证,其中实物验证请求中包括预置验证场景的信息,以使用户终端将虚拟化后的预置验证场景展示给用户。该预置验证场景可由服务器根据用户终端在身份注册时发送的场景信息以及预置验证实物生成,具体可表现为一幅缺失预置验证实物的场景图像(如图 8 所示)。

[0105] 步骤 S45,接收所述用户终端根据所述实物验证请求返回的包含待验证实物的预置验证场景的信息。

[0106] 本具体可参考第三实施例的相应内容,此处不再赘述。

[0107] 步骤 S46,根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证,将所述验证的结果返回给所述用户终端。

[0108] 具体地,如图 11 所示,本步骤具体可包括以下步骤:

[0109] 步骤 S461,分析提取所述包含所述待验证实物的预置验证场景中的待验证实物的特征数据。

[0110] 服务器对用户终端根据实物验证请求返回的包含待验证实物的预置验证场景的信息进行分析,提取其中包含的待验证实物的特征数据,该特征数据可以包括:待验证实物的实物特征数据以及待验证实物在预置验证场景中的位置数据。

[0111] 步骤 S462,将分析提取的所述待验证实物的实物特征数据以及所述待验证实物在

所述预置验证场景中的位置数据，与预置于所述特征数据库中的所述预置验证实物的实物特征数据以及所述预置验证实物在所述场景信息中的位置数据进行比较，以对所述用户进行身份验证。

[0112] 具体地，服务器根据用户帐号，从特征数据库中获取对应的预置验证实物的实物特征数据以及该预置验证实物在场景信息中的位置数据，然后将上述数据分别与分析提取的待验证实物的实物特征数据以及待验证实物在预置验证场景中的位置数据进行比较，于本实施例一具体实施方式中，服务器可先将预置验证实物在场景信息中的位置数据与待验证实物在预置验证场景中的位置数据进行比较，若二者的误差值超过预置的第一数值范围，则判定该用户终端对应的用户身份非法，并将身份非法的验证结果返回给用户终端，同时拒绝为该用户终端提供对应的业务；若二者的误差值在预置的第一数值范围内，则继续将预置验证实物的实物特征数据与待验证实物的实物特征数据进行比较，当二者的误差值在预置的第二数值范围内时，判定该用户终端对应的用户身份合法，将身份合法的验证结果返回给用户终端，并为该用户终端提供相应的业务；当二者的误差值超过预置的第二数值范围时，判定该用户终端对应的用户身份非法，并将身份非法的验证结果返回给用户终端，同时拒绝为该用户终端提供对应的业务。由于非法用户通常不熟悉预置验证场景中各个实物的具体位置，因此将待验证实物在预置验证场景中的位置作为身份验证的主要依据之一，可进一步提高身份验证的安全性。

[0113] 本发明实施例提供的身份验证的方法，通过服务器接收用户终端发送的待验证场景的信息，并根据待验证场景的信息对用户终端对应用户的身分进行初步验证，然后在通过初步验证后向用户终端发送实物验证请求，接收用户终端返回的放置了虚拟化后的待验证实物的预置验证场景的信息，然后通过分析提取预置验证场景的信息中的待验证实物的特征数据，并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身分进行最终验证，由于是通过待验证场景与待验证实物的特征数据来进行身份验证，上述特征数据只能通过分析待验证场景与待验证实物的信息获得，而非法用户通常难以获取到待验证场景与待验证实物的信息，并且也无法通过算法破解的方式获得上述特征数据，因此可提高身份验证的安全性。

#### [0114] 第五实施例

[0115] 本实施例可应用于如图12所示的应用环境中，如图12所示，用户终端201、场景处理服务器202以及身份验证服务器203处于有线或无线网络中，通过该有线或无线网络，用户终端201、场景处理服务器202以及身份验证服务器203进行信息交互。

[0116] 图13为本发明第五实施例提供的身份验证的方法的流程图。如图13所示，本实施例的身份验证的方法包括以下步骤：

[0117] 步骤S51，用户终端201响应于用户的身份注册的操作，向场景处理服务器202发送身份注册的请求。

[0118] 身份注册请求中可包括：对应的用户帐号等可唯一标识用户身份的信息，以及用于验证用户身份合法性的场景信息与实物信息。其中场景信息可为用户所熟悉的生活环境的场景画面，由用户终端201根据用户的拍摄指令，通过内置或外设的图像采集设备拍摄获取。实物信息为获取的场景画面中的实物的信息，由用户终端201通过识别拍摄获取的场景画面中的实物并显示给用户，然后根据用户的选择指令获取。由于将用户所熟悉的

生活环境的场景画面作为用户身份验证的依据,不法用户很难像破解现有技术中的密码一样,通过算法对身份验证信息进行破解来通过身份验证,从而可提高身份验证的安全性。

[0119] 步骤 S502 :场景处理服务器 202 对身份注册请求进行处理,存储处理结果。

[0120] 场景处理服务器 202 对身份注册请求进行处理,提取身份注册请求中所包含的用户帐号、场景信息以及实物信息,对场景信息以及实物信息进行识别,获取场景信息的特征数据与实物信息的特征数据(具体可包括:实物的颜色、状态等实物特征数据以及该实物在场景信息中的位置数据等),然后将实物信息的特征数据作为预置验证实物的特征数据,与获取的场景信息的特征数据,以及对应的用户帐号一起存储于特征数据库中。

[0121] S503 :场景处理服务器 202 发送处理结果给身份验证服务器 203,以便身份验证服务器 203 建立注册信息。

[0122] 身份验证服务器 203 将接收的处理结果中的特征数据与用户帐号等用户信息建立对应关系,完成注册流程,然后执行步骤 S504 :将注册结果返回给用户终端 201。

[0123] 步骤 S505 :用户终端 201 向身份验证服务器 203 发送包含用户账号的获取预约业务请求,以获取预约业务。

[0124] 步骤 S506 :身份验证服务器 203 根据获取预约业务请求,向用户终端 201 发起身份验证。

[0125] 除了当接受到获取预约业务请求时以外,身份验证服务器 203 也可在其它情况下主动向用户终端 201 发起身份验证,例如:当检测到用户终端 201 对应的用户帐号出现异常情况时(诸如:被盗用、发布了大量异常信息等情况)。

[0126] 步骤 S507 :用户终端 201 发送待验证场景的信息给场景处理服务器 202。

[0127] 用户终端 201 根据用户的获取指令,通过图像采集设备拍摄获取该获取指令对应的场景的信息,并作为待验证场景发送给场景处理服务器 202。

[0128] 步骤 S508 :场景处理服务器 202 分析并验证待验证场景的信息,分析提取待验证场景的特征数据,并根据用户帐号,查询获取特征数据库中存储的对应的场景信息的特征数据,将待验证场景的特征数据与场景信息的特征数据进行比较,并执行步骤 S509 :将比较结果为做第一验证结果发送给身份验证服务器 203。

[0129] 步骤 S510 :当待验证场景的特征数据与预置验证场景的特征数据的误差小于预置的第一数值时,场景处理服务器 202 发送实物验证请求给用户终端 201。

[0130] 实物验证请求中包含用于实物验证的经虚拟化处理过的,且缺失了该用户终端在身份注册时提交的实物信息的预置验证场景。

[0131] 步骤 S511 :用户终端 201 将接收的实物验证请求中所包含的预置验证场景与图像采集设备当前所拍摄的画面相叠加,并将叠加后的画面展示给用户,然后根据用户的获取指令,通过图像采集设备拍摄获取该获取指令对应的实物,然后对获取的实物进行虚拟化处理后作为待验证实物展示在屏幕当前显示的画面中,并根据用户的拖曳操作,将待验证实物移动至预置验证场景中与拖曳操作对应的位置,再根据用户的确认操作,将包含位置被移动后的待验证实物的预置验证场景的信息发送给场景处理服务器 202。

[0132] 步骤 S512 :场景处理服务器 202 提取接收的预置验证场景的信息中的待验证实物,分析获取该待验证实物的特征数据,具体可包括:颜色、形状等实物特征数据以及待验证实物在预置验证场景中的位置数据,根据用户帐号从特征数据库中查询获取对应的预置

验证实物的特征数据,将预置验证实物的特征数据与待验证实物的特征数据进行比较,以对待验证实物进行验证,并执行步骤 S513 :将比较结果作为第二验证结果发送给身份验证服务器 203。

[0133] 步骤 S514 :身份验证服务器 203 根据第二验证结果向用户终端 201 返回验证结果。当第二验证结果为预置验证实物的特征数据与待验证实物在的特征数据的误差在预置的数值范围内时,确认用户终端 201 通过身份认证,向用户终端 201 发送签名信息。

[0134] 本发明实施例提供的身份验证的方法,通过用户终端根据服务器发起的身份验证请求,获取待验证场景的信息,将获取的待验证场景的信息发送给服务器,以使服务器根据待验证场景的信息对用户终端对应用户的身份进行初步验证,然后根据服务器发送的实物验证请求,获取待验证实物的信息,然后将获取的待验证实物虚拟化后放置在虚拟化的预置验证场景的对应位置,并将放置了虚拟化后的待验证实物的预置验证场景的信息返回给服务器,以使服务器通过分析提取预置验证场景的信息中的待验证实物的特征数据,并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身份进行最终验证,由于是通过待验证场景与待验证实物的特征数据来进行身份验证,上述特征数据只能通过分析待验证场景与待验证实物的信息获得,而非法用户通常难以获取到待验证场景与待验证实物的信息,并且也无法通过算法破解的方式获得上述特征数据,因此可提高身份验证的安全性。

### [0135] 第六实施例

[0136] 图 14 为本发明第六实施例提供的在用户终端内进行身份验证的装置的结构示意图。本实施例提供的身份验证的装置可以用于上述实施例中的身份验证的方法。如图 14 所示,身份验证的装置 60 包括:接收模块 61、第一采集模块 62、处理模块 63 以及验证模块 64。

[0137] 其中,接收模块 61 用于接收服务器发送的实物验证请求,所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息,将预置验证实物的提示信息以及虚拟化后的预置验证场景展示给所述用户。

[0138] 第一采集模块 62 用于根据所述接收模块 61 接收的所述预置验证实物的提示信息,在当前实际场景中采集与预置验证实物相对应的待验证实物信息。

[0139] 处理模块 63 用于根据所述第一采集模块 62 采集到的待验证实物信息,将虚拟化后的待验证实物添加在所述虚拟化后的预置验证场景的对应位置。

[0140] 验证模块 64 用于将所述处理模块 63 处理后的包含所述待验证实物的预置验证场景的信息返回给所述服务器,以使所述服务器根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证。

[0141] 以上各模块可以是由软件代码实现,此时,上述的各模块可存储于存储器 102 内,如图 15 所示。以上各模块同样可以由硬件例如集成电路芯片实现。

[0142] 本实施例对身份验证的装置 60 的各功能模块实现各自功能的具体过程,请参见上述图 1 至图 13 所示实施例中描述的具体内容,此处不再赘述。

[0143] 本发明实施例提供的身份验证的装置,通过根据服务器发送的实物验证请求,获取待验证实物的信息,然后将获取的待验证实物虚拟化后放置在虚拟化的预置验证场景的对应位置,并将放置了虚拟化后的待验证实物的预置验证场景的信息返回给服务器,以使

服务器通过分析提取预置验证场景的信息中的待验证实物的特征数据，并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身份进行最终验证，由于是通过待验证场景与待验证实物的特征数据来进行身份验证，上述特征数据只能通过分析待验证场景与待验证实物的信息获得，而非法用户通常难以获取到待验证场景与待验证实物的信息，并且也无法通过算法破解的方式获得上述特征数据，因此可提高身份验证的安全性。

[0144] 第七实施例

[0145] 图 16 为本发明第七实施例提供的在用户终端内进行身份验证的装置的结构示意图。本实施例提供的身份验证的装置可以用于上述实施例中的身份验证的方法。如图 16 所示，身份验证的装置 70 包括：接收模块 71、第一采集模块 72、处理模块 73、验证模块 74、第二采集模块 75、场景信息获取模块 76、展示模块 77、实物获取模块 78 以及发送模块 79。

[0146] 其中，接收模块 71 用于接收服务器发送的实物验证请求，所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息，将预置验证实物的提示信息以及虚拟化后的预置验证场景展示给所述用户。

[0147] 第一采集模块 72 用于根据所述接收模块 71 接收的所述预置验证实物的提示信息，在当前实际场景中采集与预置验证实物相对应的待验证实物信息。

[0148] 处理模块 73 用于根据所述第一采集模块 72 采集到的待验证实物信息，将虚拟化后的待验证实物添加在所述虚拟化后的预置验证场景的对应位置。如图 17 所示，所述处理模块 73 包括：第一处理单元 731 与第二处理单元 732。其中，第一处理单元 731 用于响应于所述用户对待验证实物的拖曳操作，将虚拟化的所述待验证实物移动至所述虚拟化后的预置验证场景中与所述拖曳操作对应的位置；第二处理单元 732 用于直接将所述虚拟化后的待验证实物移动至所述虚拟化后的预置验证场景的对应位置。

[0149] 验证模块 74 用于将所述处理模块 73 处理后的包含所述待验证实物的预置验证场景的信息返回给所述服务器，以使所述服务器根据所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证。

[0150] 第二采集模块 75 用于在当前实际场景中采集待验证场景的信息，并将所述待验证场景的信息发送给服务器，以使所述服务器根据预置验证场景对所述待验证场景进行验证。

[0151] 场景信息获取模块 76 用于接收用户所触发的身份注册请求，获取场景信息。

[0152] 展示模块 77 用于识别经用户确认的场景信息中的实物，将识别的所述实物展示给用户。

[0153] 实物获取模块 78 用于响应于所述用户根据展示的所述实物进行的选定操作，获取所述选定操作对应的实物作为所述预置验证实物。

[0154] 发送模块 79 用于将所述预置验证实物以及所述场景信息发送给所述服务器，其中，所述场景信息中去除所述验证实物的部分作为所述预置验证场景。

[0155] 优选地，所述待验证场景以及所述待验证实物的信息由所述用户终端的图像采集设备采集。

[0156] 优选地，所述预置验证场景中包含至少一个预置验证实物的提示信息，所述提示信息包括：所述预置验证实物的名称，或者所述预置验证实物在所述预置验证场景中的位置信息。

[0157] 优选地，所述预置验证实物在所述预置验证场景中的位置信息，通过在所述预置验证场景中将与所述预置验证实物对应的位置设置为空白的方式进行展示。

[0158] 本实施例对身份验证的装置 70 的各功能模块实现各自功能的具体过程，请参见上述图 1 至图 13 所示实施例中描述的具体内容，此处不再赘述。

[0159] 本发明实施例提供的身份验证的装置，通过根据服务器发起的身份验证请求，获取待验证场景的信息，将获取的待验证场景的信息发送给服务器，以使服务器根据待验证场景的信息对用户终端对应用户的身份进行初步验证，然后根据服务器发送的实物验证请求，获取待验证实物的信息，然后将获取的待验证实物虚拟化后放置在虚拟化的预置验证场景的对应位置，并将放置了虚拟化后的待验证实物的预置验证场景的信息返回给服务器，以使服务器通过分析提取预置验证场景的信息中的待验证实物的特征数据，并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身份进行最终验证，由于是通过待验证场景与待验证实物的特征数据来进行身份验证，上述特征数据只能通过分析待验证场景与待验证实物的信息获得，而非法用户通常难以获取到待验证场景与待验证实物的信息，并且也无法通过算法破解的方式获得上述特征数据，因此可提高身份验证的安全性。

#### [0160] 第八实施例

[0161] 图 18 为本发明第八实施例提供的身份验证的装置的结构示意图。本实施例提供的身份验证的装置可以用于实现上述实施例中的身份验证的方法。如图 18 所示，身份验证的装置 80 包括：实物验证请求发送模块 81、第一接收模块 82 以及验证模块 83。

[0162] 其中，实物验证请求发送模块 81 用于向用户终端发送实物验证请求，所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息。

[0163] 第一接收模块 82 用于接收所述用户终端根据所述实物验证请求返回的包含待验证实物的预置验证场景的信息。

[0164] 验证模块 83 用于根据所述第一接收模块 82 接收的所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证，将所述验证的结果返回给所述用户终端。

[0165] 本实施例对身份验证的装置 80 的各功能模块实现各自功能的具体过程，请参见上述图 1 至图 13 所示实施例中描述的具体内容，此处不再赘述。

[0166] 本发明实施例提供的身份验证的装置，通过向用户终端发送实物验证请求，接收用户终端返回的放置了虚拟化后的待验证实物的预置验证场景的信息，然后通过分析提取预置验证场景的信息中的待验证实物的特征数据，并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身份进行最终验证，由于是通过待验证场景与待验证实物的特征数据来进行身份验证，上述特征数据只能通过分析待验证场景与待验证实物的信息获得，而非法用户通常难以获取到待验证场景与待验证实物的信息，并且也无法通过算法破解的方式获得上述特征数据，因此可提高身份验证的安全性。

#### [0167] 第九实施例

[0168] 图 19 为本发明第九实施例提供的身份验证的装置的结构示意图。本实施例提供的身份验证的装置可以用于实现上述实施例中的身份验证的方法。如图 19 所示，身份验证的装置 90 包括：实物验证请求发送模块 91、第一接收模块 92、验证模块 93、第二接收模块 94、身份注册模块 95 以及注册结果发送模块 96。

[0169] 其中,实物验证请求发送模块91用于向用户终端发送实物验证请求,所述实物验证请求中包括预置验证场景的信息以及预置验证实物的提示信息。如图20所示,所述实物验证请求发送模块91包括:身份验证请求发送单元911、比较单元912以及实物验证请求发送单元913。其中,身份验证请求发送单元911用于向用户终端发送身份验证请求;比较单元912用于接收所述用户终端发送的待验证场景的信息,将所述待验证场景的特征与所述场景信息的特征进行比较;实物验证请求发送单元913用于当所述待验证场景的特征与所述场景信息的特征的相似度大于预置的数值时,向所述用户终端发送实物验证请求。

[0170] 进一步地,所述比较单元912还用于分析提取所述待验证场景的特征数据,将所述特征数据与预置于所述特征数据库中的所述场景信息的特征数据进行比较。

[0171] 第一接收模块92用于接收所述用户终端根据所述实物验证请求返回的包含待验证实物的预置验证场景的信息。

[0172] 验证模块93用于根据所述第一接收模块92接收的所述预置验证场景以及预置验证实物对所述包含所述待验证实物的预置验证场景进行验证,将所述验证的结果返回给所述用户终端。如图21所示,所述验证模块93包括:分析提取单元931与比较单元932。其中,分析提取单元931用于分析提取所述包含所述待验证实物的预置验证场景中的待验证实物的特征数据,所述待验证实物的特征数据包括:所述待验证实物的实物特征数据以及所述待验证实物在所述预置验证场景中的位置数据;比较单元932用于将所述待验证实物的实物特征数据以及所述待验证实物在所述预置验证场景中的位置数据,与预置于所述特征数据库中的所述预置验证实物的实物特征数据以及所述预置验证实物在所述场景信息中的位置数据进行比较。

[0173] 第二接收模块94用于接收用户终端发送的场景信息以及所述预置验证实物的信息,将所述场景信息中去除所述预置验证实物的部分作为所述预置验证场景。

[0174] 身份注册模块95用于分析提取所述第二接收模块94接收的所述场景信息与所述预置验证实物的特征数据,将分析提取的所述特征数据预置于特征数据库中,以完成身份注册,所述预置验证实物的特征数据包括:所述预置验证实物的实物特征数据以及所述预置验证实物在所述场景信息中的位置数据。

[0175] 注册结果发送模块96用于将所述身份注册模块95获取的所述身份注册的结果返回给所述用户终端。

[0176] 本实施例对身份验证的装置40的各功能模块实现各自功能的具体过程,请参见上述图1至图13所示实施例中描述的具体内容,此处不再赘述。

[0177] 本发明实施例提供的身份验证的装置,通过接收用户终端发送的待验证场景的信息,并根据待验证场景的信息对用户终端对应用户的身分进行初步验证,然后在通过初步验证后向用户终端发送实物验证请求,接收用户终端返回的放置了虚拟化后的待验证实物的预置验证场景的信息,然后通过分析提取预置验证场景的信息中的待验证实物的特征数据,并将该特征数据与预置的特征数据进行比较来对用户终端对应用户的身分进行最终验证,由于是通过待验证场景与待验证实物的特征数据来进行身份验证,上述特征数据只能通过分析待验证场景与待验证实物的信息获得,而非法用户通常难以获取到待验证场景与待验证实物的信息,并且也无法通过算法破解的方式获得上述特征数据,因此可提高身份验证的安全性。

[0178] 本发明实施例还提供了一种身份验证的系统,请参阅图 22,身份验证的系统 300 包括 :用户终端 301 与服务器 302。

[0179] 本实施例中的身份验证的系统中各装置实现功能的具体过程请参阅图 1 至图 13 对应实施例的方法,以及图 14 图至图 21 对应实施例的装置,此处不再赘述。

[0180] 需要说明的是,本说明书中的各个实施例均采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似的部分互相参见即可。对于装置类实施例而言,由于其与方法实施例基本相似,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0181] 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、物品或者装置不仅包括那些要素,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、物品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0182] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成,也可以通过程序来指令相关的硬件完成,的程序可以存储于一种计算机可读存储介质中,上述提到的存储介质可以是只读存储器,磁盘或光盘等。

[0183] 以上,仅是本发明的较佳实施例而已,并非对本发明作任何形式上的限制,虽然本发明已以较佳实施例揭露如上,然而并非用以限定本发明,任何熟悉本专业的技术人员,在不脱离本发明技术方案范围内,当可利用上述揭示的技术内容做出些许更动或修饰为等同变化的等效实施例,但凡是未脱离本发明技术方案内容,依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与修饰,均仍属于本发明技术方案的范围内。

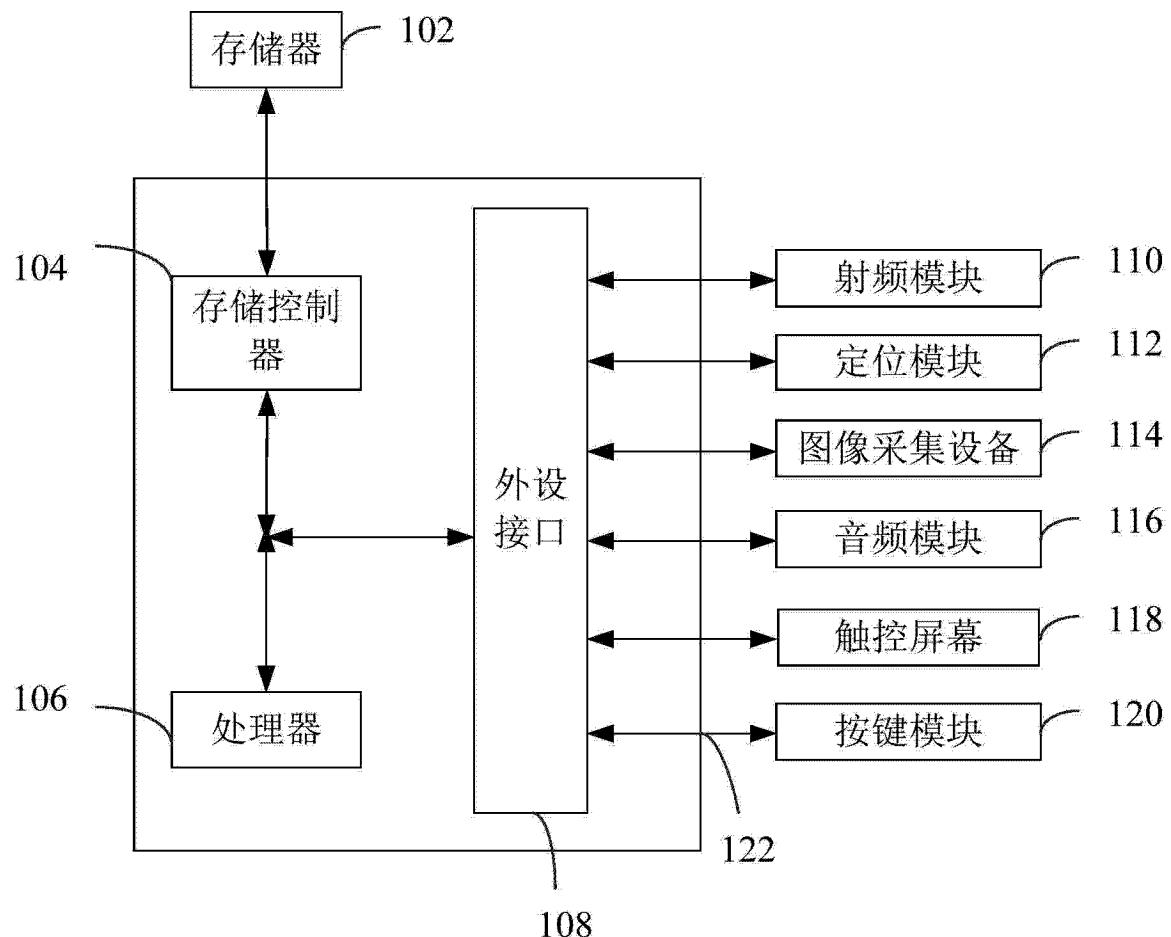


图 1

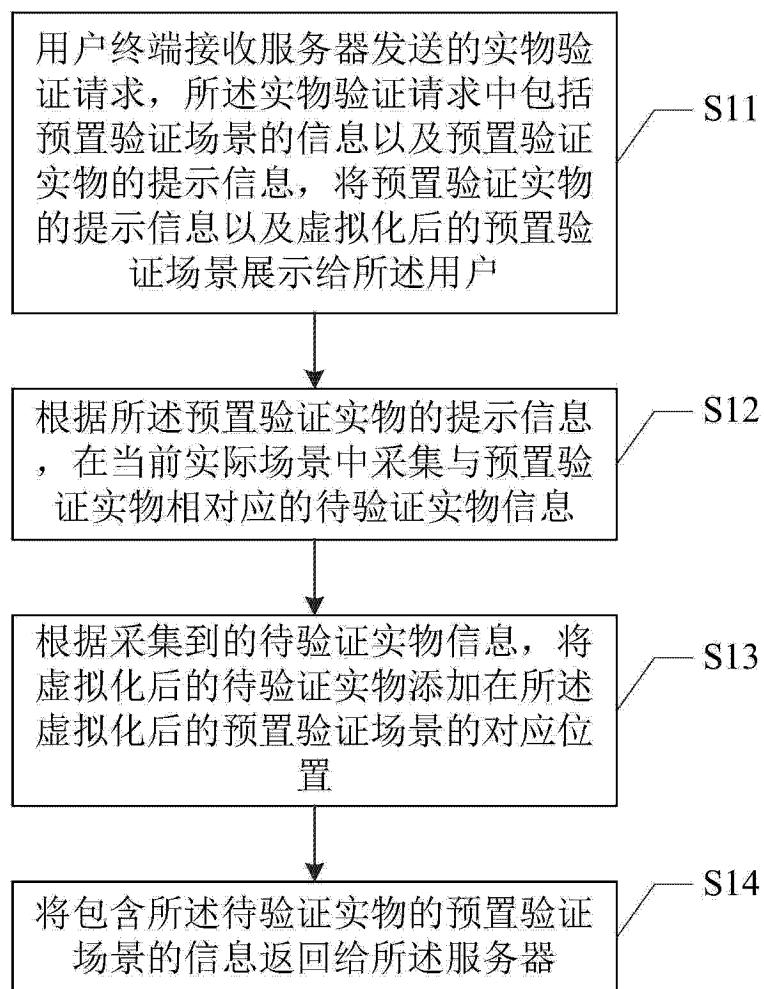


图 2

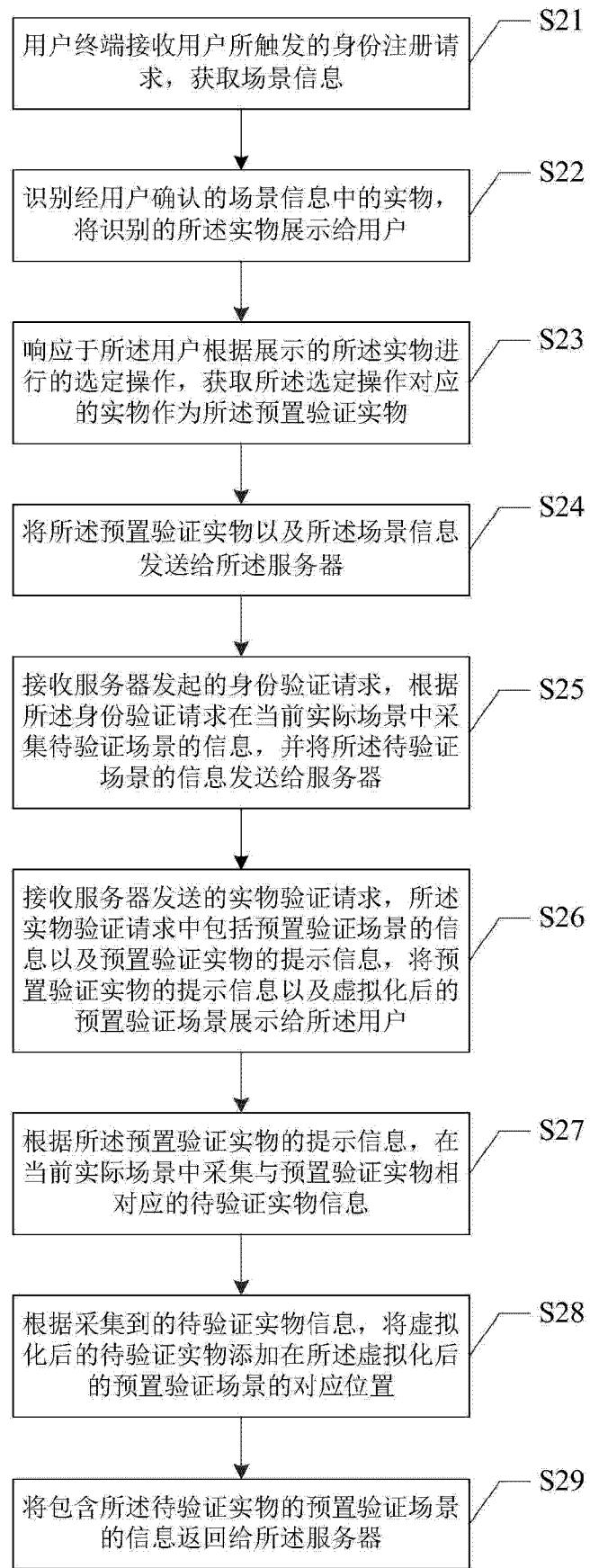


图 3



图 4

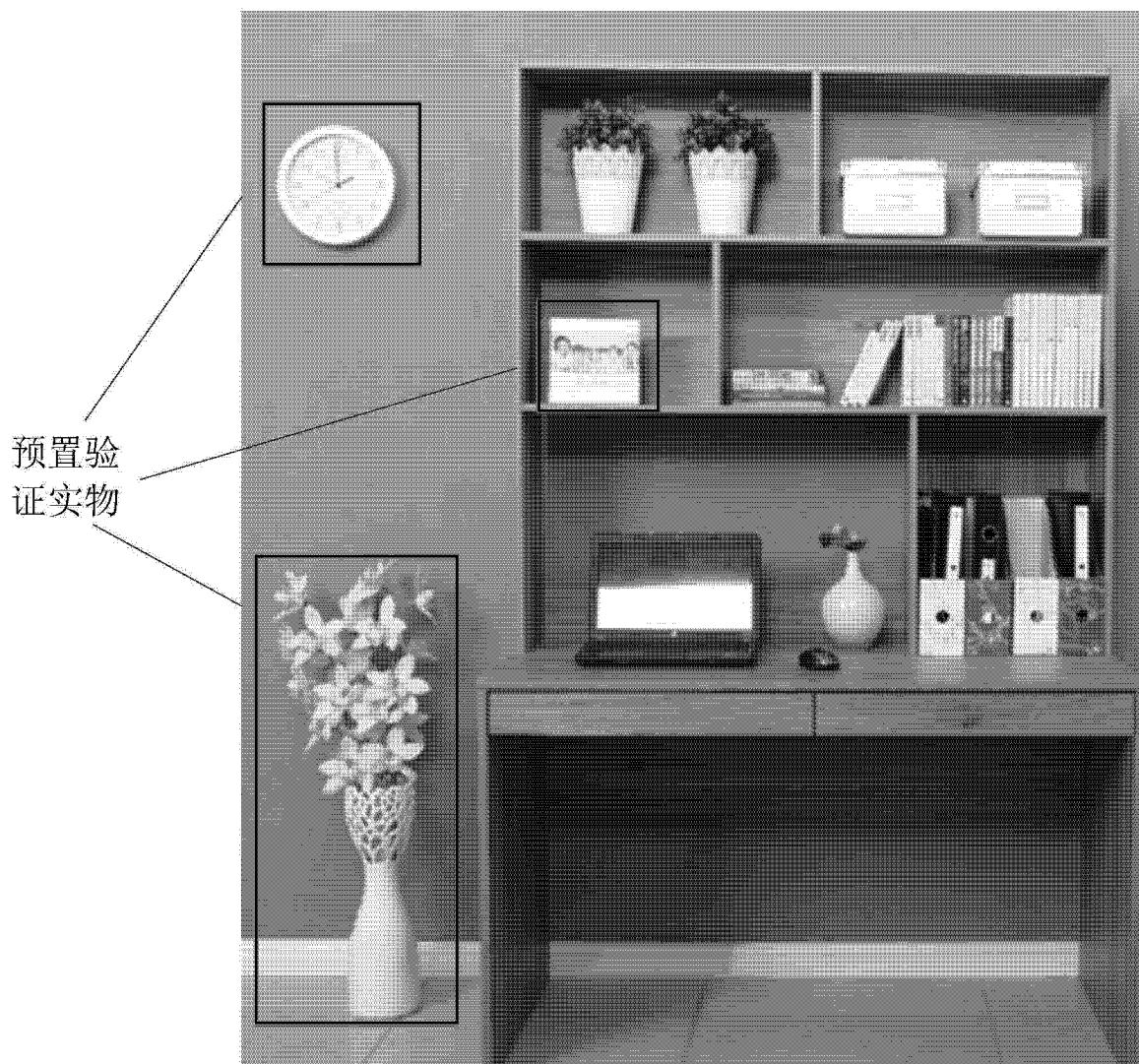


图 5

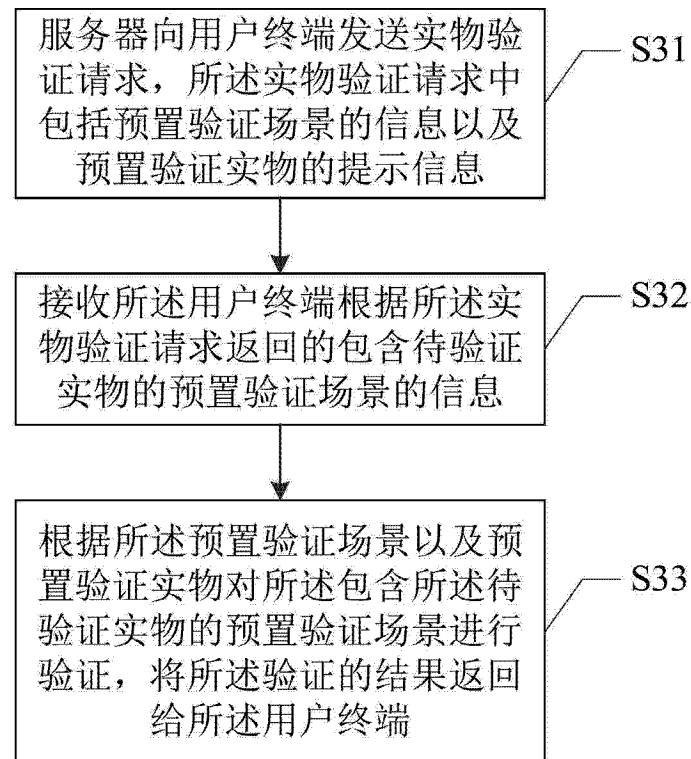


图 6

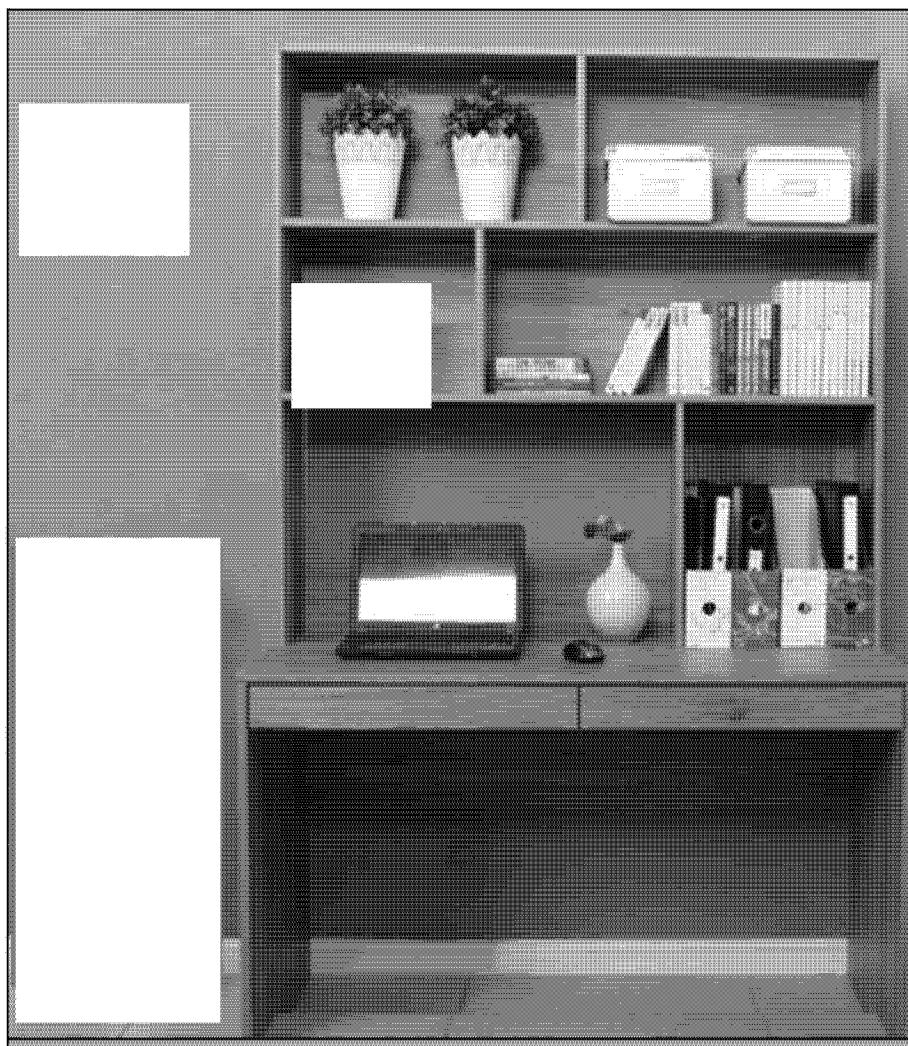


图 7



图 8

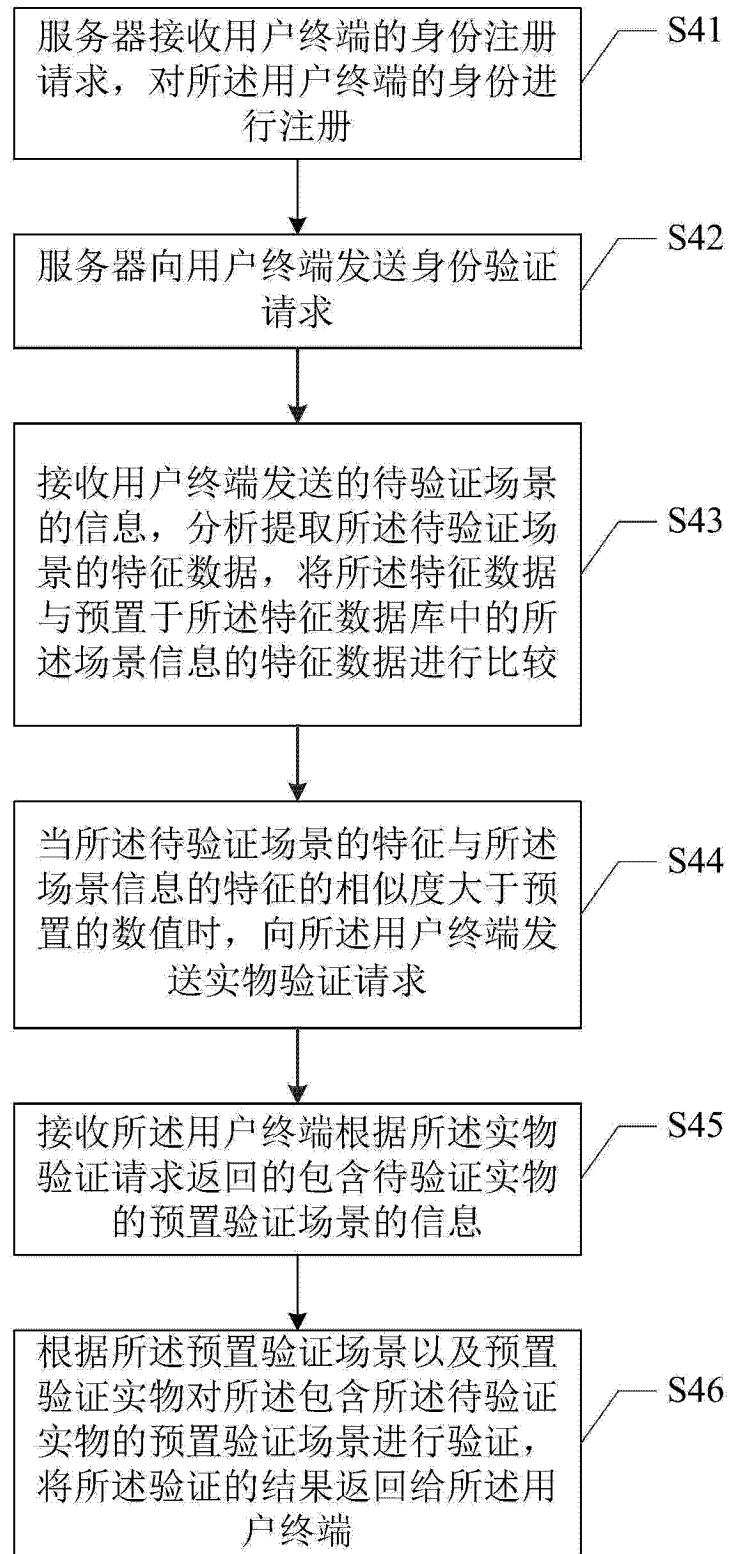
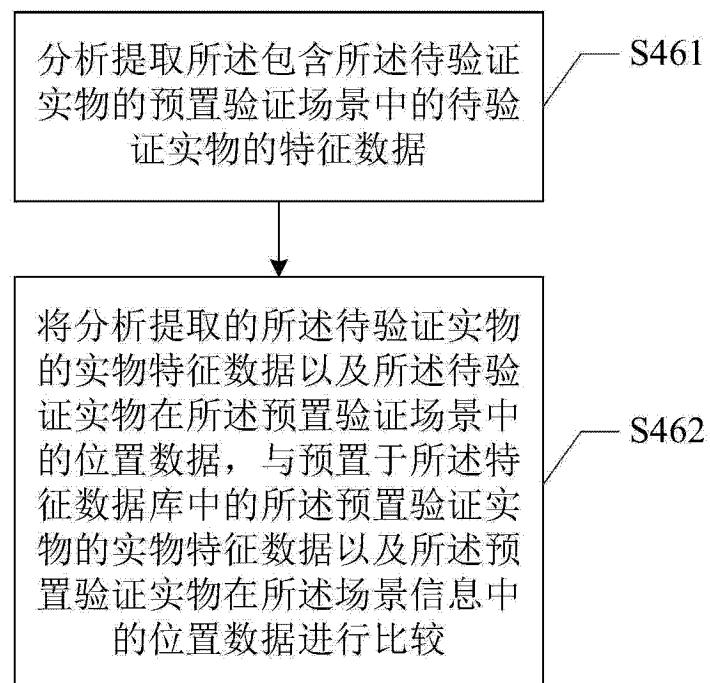
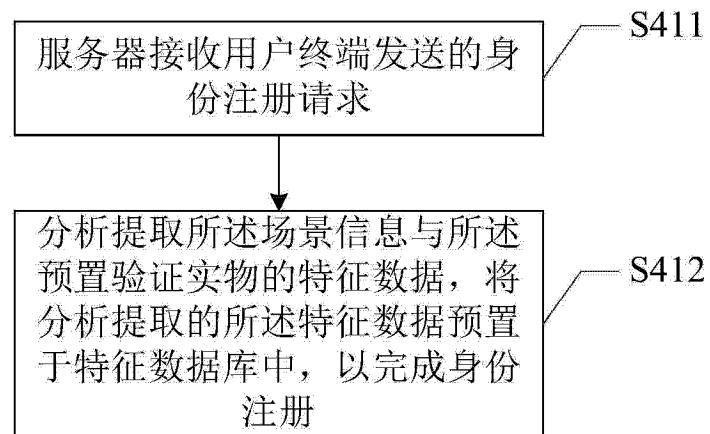


图 9



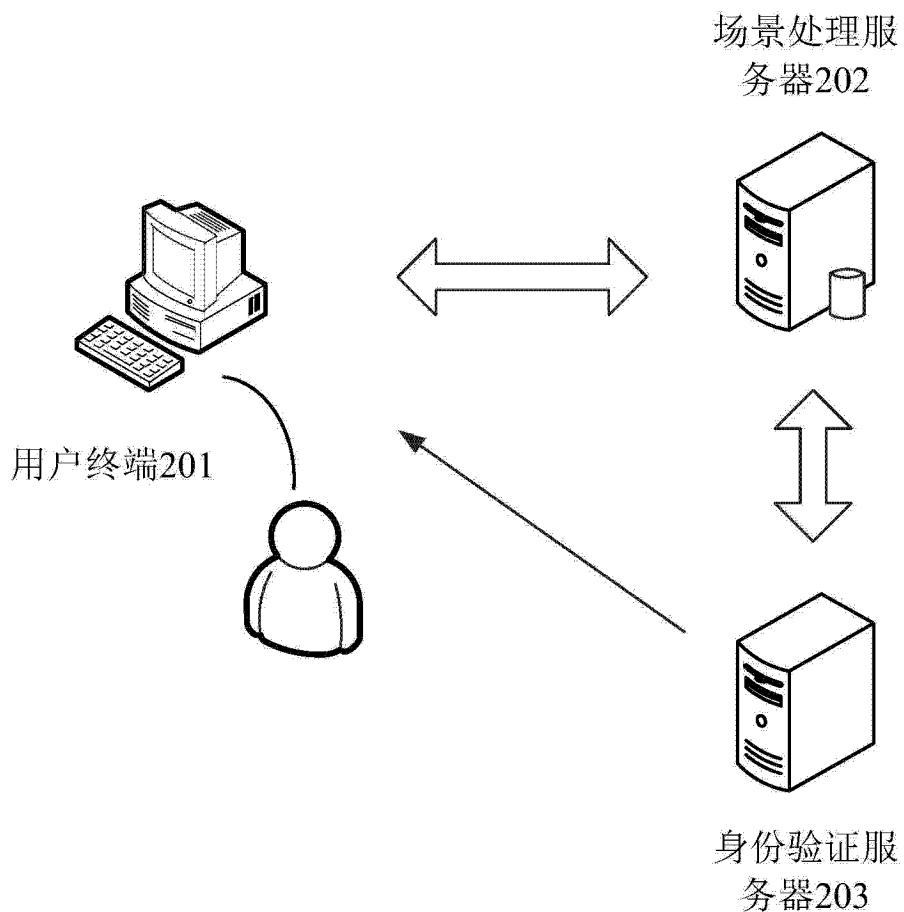


图 12

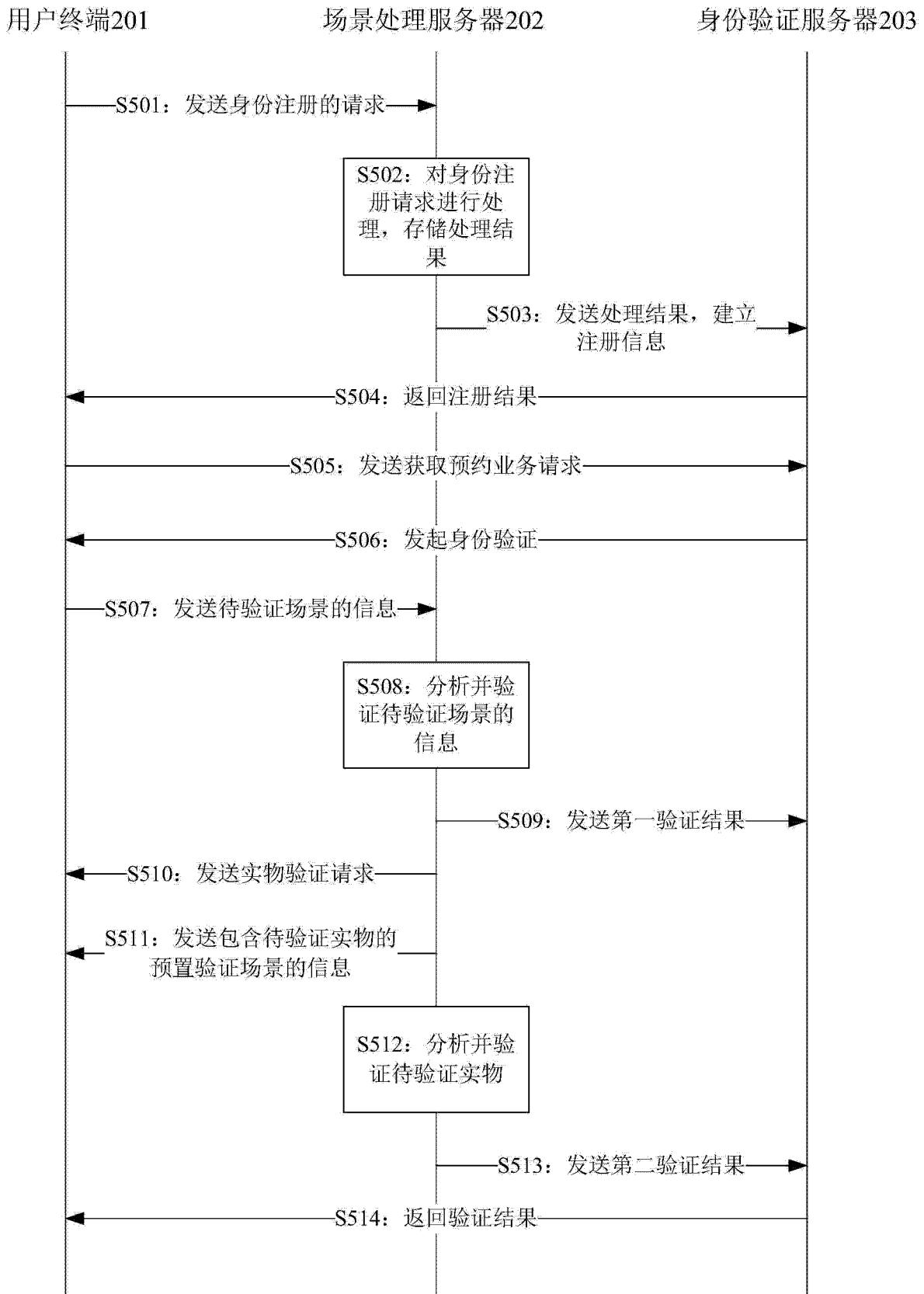


图 13

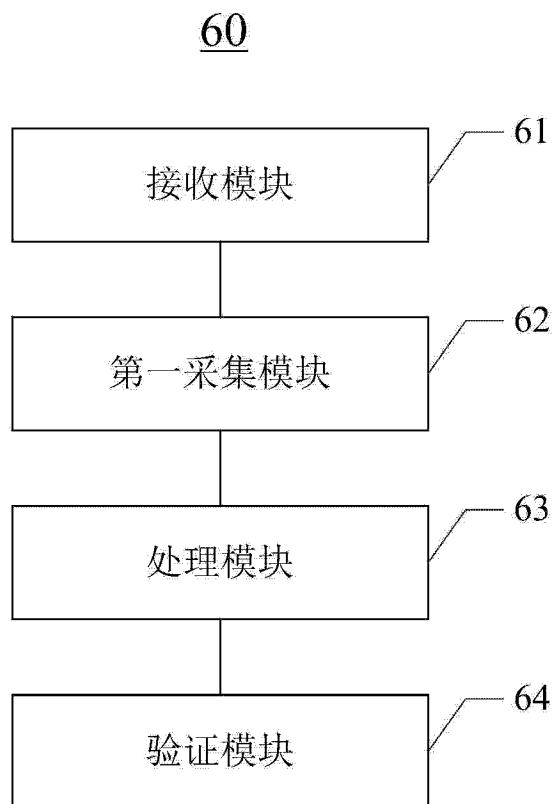


图 14

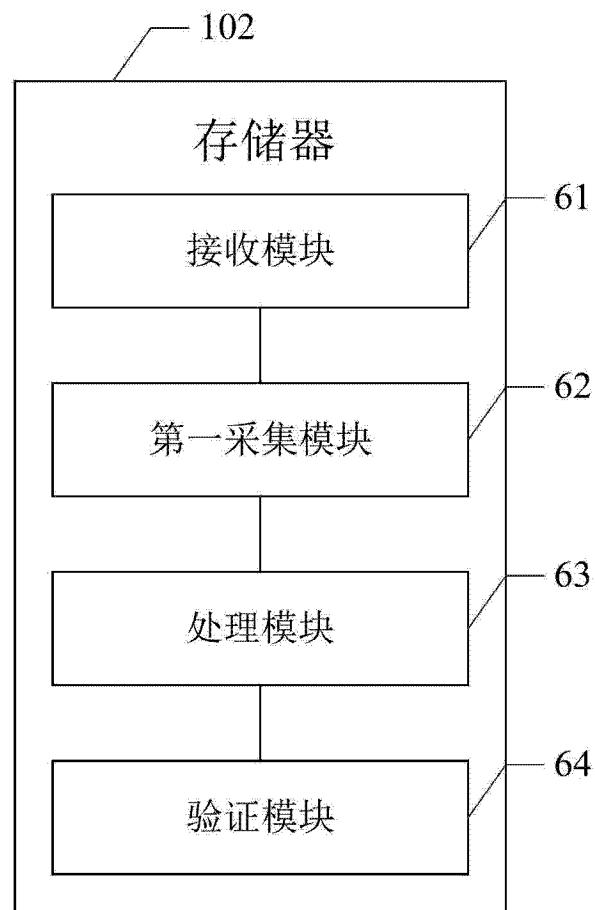


图 15

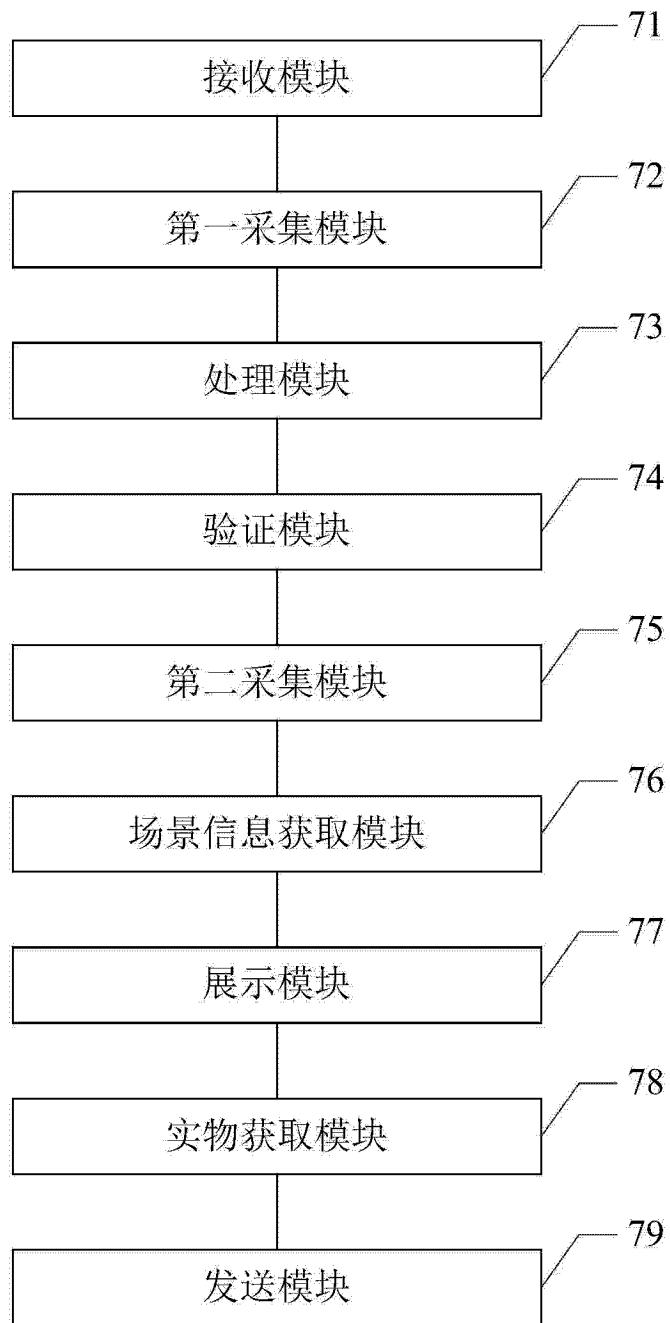
70

图 16

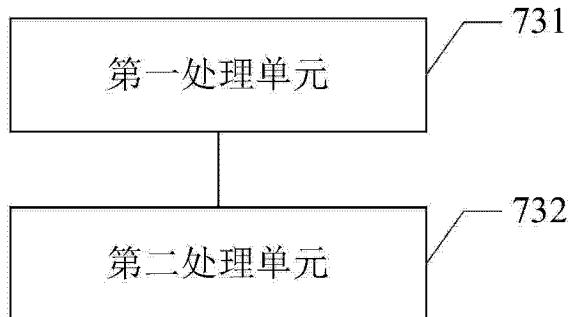
73

图 17

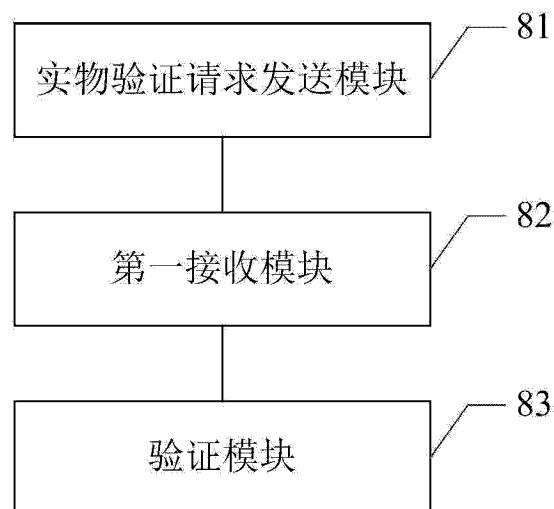
80

图 18

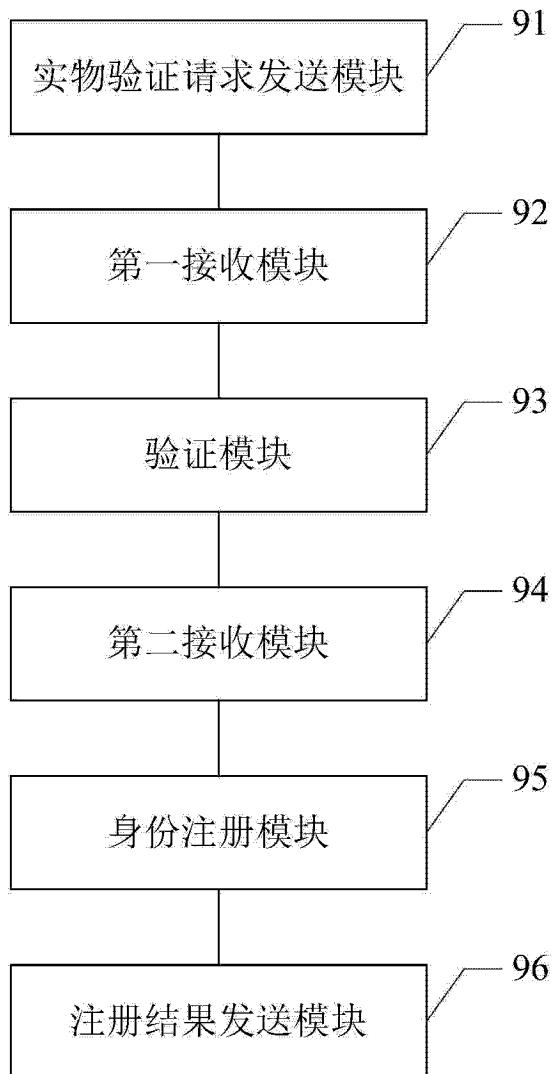
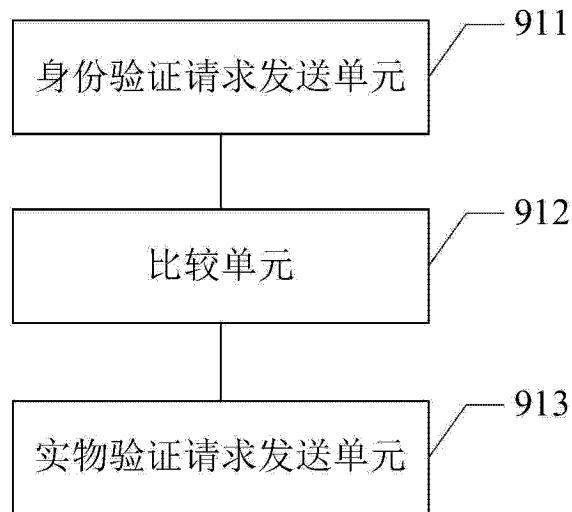
9091

图 20

图 19

93

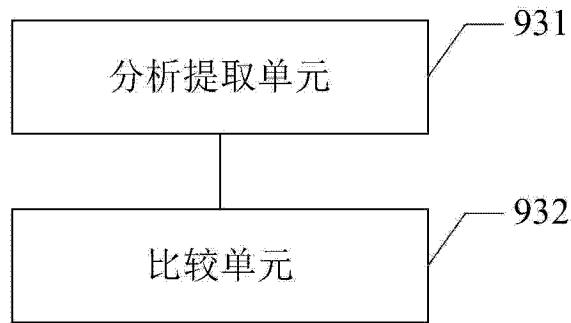


图 21

300

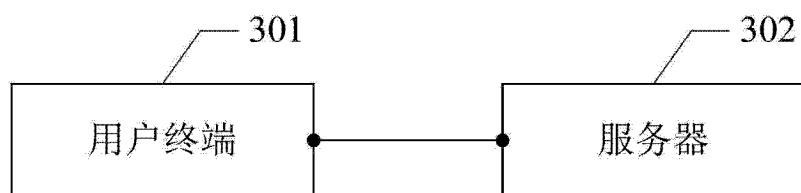


图 22