



(12) 发明专利

(10) 授权公告号 CN 112001402 B

(45) 授权公告日 2023.10.03

(21) 申请号 202010767513.0

G06Q 20/32 (2012.01)

(22) 申请日 2017.05.11

G06Q 20/36 (2012.01)

(65) 同一申请的已公布的文献号

G06Q 20/40 (2012.01)

申请公布号 CN 112001402 A

H04W 4/80 (2018.01)

(43) 申请公布日 2020.11.27

(56) 对比文件

CN 205375634 U, 2016.07.06

(62) 分案原申请数据

US 2016048667 A1, 2016.02.18

201710331058.8 2017.05.11

CN 102934466 A, 2013.02.13

(73) 专利权人 创新先进技术有限公司

CN 105550863 A, 2016.05.04

地址 开曼群岛大开曼岛西湾路802号木槿
街大展览馆31119号邮箱

CN 105847253 A, 2016.08.10

(72) 发明人 陈力 张鸿 周乐

CN 105871814 A, 2016.08.17

(74) 专利代理机构 北京博思佳知识产权代理有
限公司 11415

US 2013005243 A1, 2013.01.03

专利代理人 周嗣勇

US 2013297425 A1, 2013.11.07

(51) Int.Cl.

US 2014006191 A1, 2014.01.02

G06Q 20/18 (2012.01)

US 2015356563 A1, 2015.12.10

G06Q 20/20 (2012.01)

US 2015371210 A1, 2015.12.24

US 2016335617 A1, 2016.11.17

审查员 刘海艳

权利要求书4页 说明书16页 附图7页

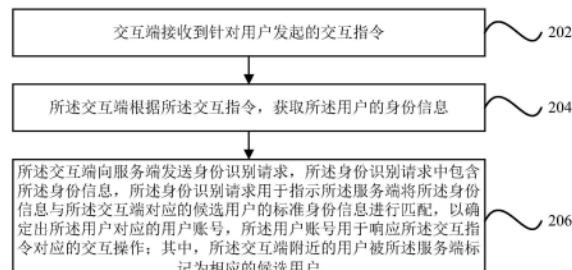
(54) 发明名称

身份认证方法、装置和系统

(57) 摘要

本申请提供一种身份认证方法、装置和系统，该身份认证方法可以包括：交互端接收到针对用户发起的交互指令，获取所述用户的身份信息；所述交互端向服务端发送身份识别请求，所述身份识别请求中包含所述身份信息，所述身份识别请求用于指示所述服务端将所述身份信息与所述交互端对应的候选用户的标准身份信息进行匹配，以确定出所述用户对应的用户账号，所述用户账号用于响应所述交互指令对应的交互操作；其中，所述交互端附近的用户被所述服务端标记为相应的候选用户。通过本申请的技术方案，可以提高对用户的身份识别效率和识别准确度，有助于提升交互效率和安全性。

CN 112001402 B



1. 一种身份认证系统,包括:
 用户客户端、收款端和服务端;
 所述收款端向外发射包含收款端标识信息的近场消息;
 所述用户客户端在接收到所述近场消息时,将所述收款端标识信息、所述用户客户端的已登录用户的用户标识信息和所述近场消息的信号强度发送至所述服务端;
 所述服务端在接收到的所述信号强度大于预设强度的情况下,将所述已登录用户确定为所述收款端对应的候选用户,并在所述收款端标识信息、用户标识信息和信号强度的保存时长超出预设时长时,删除所述收款端标识信息、用户标识信息和信号强度;
 所述收款端接收到针对所述已登录用户发起的交易指令,根据所述交易指令获取所述已登录用户的生物特征信息,并向所述服务端发送包含所述生物特征信息的身份识别请求;
 所述服务端接收到所述身份识别请求,将所述生物特征信息与所述收款端对应的候选用户的标准生物特征信息进行匹配,并确定出所述已登录用户对应的用户账号以用于响应所述交易指令对应的交易操作。
2. 一种身份认证方法,包括:
 交互端向外发射包含交互端标识信息的近场消息;其中,当所述近场消息被用户对应的用户客户端接收到时,所述近场消息用于指示所述用户客户端:将所述交互端标识信息、所述用户的用户标识信息和所述近场消息的信号强度发送至服务端,以由所述服务端在接收到的所述信号强度大于预设强度的情况下,将所述用户确定为所述交互端对应的候选用户;并在所述交互端标识信息、用户标识信息和信号强度的保存时长超出第一预设时长时,删除所述交互端标识信息、用户标识信息和信号强度;
 所述交互端根据接收到的针对所述用户发起的交互指令,获取所述用户的身份信息;
 所述交互端向所述服务端发送包含所述身份信息的身份识别请求,所述身份识别请求用于指示所述服务端将所述身份信息与所述交互端对应的候选用户的标准身份信息进行匹配,以确定出所述用户对应的用户账号以用于响应所述交互指令对应的交互操作。
3. 根据权利要求2所述的方法,还包括:
 当确定出所述用户对应的用户账号时,所述交互端响应于所述交互指令,针对确定出的用户账号实施交互操作。
4. 根据权利要求3所述的方法,所述交互端针对确定出的用户账号实施交互操作,包括:
 所述交互端向所述服务端或区别于所述服务端的其他交互服务端发起交互请求,以相应的由所述服务端或所述其他交互服务端针对所述用户账号实施交互操作。
5. 根据权利要求2所述的方法,所述身份信息包括生物特征信息、所述标准身份信息包括标准生物特征信息。
6. 根据权利要求5所述的方法,所述生物特征信息、所述标准生物特征信息包括以下至少之一:
 人脸信息、指纹信息、掌纹信息、眼纹信息、虹膜信息、步态信息。
7. 根据权利要求2所述的方法,所述候选用户包括在第二预设时长内位于所述交互端附近的用户。
8. 根据权利要求7所述的方法,

通过将任一用户客户端的定位信息与所述交互端的安装位置信息进行比较,确定所述任一用户客户端对应的用户是否位于所述交互端附近。

9.一种身份认证方法,包括:

服务端接收到交互端发送的包含用户的身份信息的身份识别请求,所述身份信息由所述交互端根据针对所述用户发起的交互指令向所述用户获取得到;

所述服务端将所述身份信息与所述交互端对应候选用户的标准身份信息进行匹配;其中,所述交互端附近的用户被所述服务端通过下述方式标记为所述交互端对应候选用户:

所述服务端调取数据库,所述数据库中记录有所述用户对应的用户客户端上传的交互端标识信息、用户标识信息和信号强度;其中,所述用户客户端在接收到所述交互端向外发射的近场消息时,将所述用户的用户标识信息、所述近场消息中包含的、交互端标识信息、所述近场消息的信号强度上传至所述服务端;所述服务端在接收到的所述信号强度大于预设强度的情况下,将所述用户确定为所述交互端对应候选用户,并在所述交互端标识信息、用户标识信息和信号强度的保存时长超出第一预设时长时,删除所述交互端标识信息、用户标识信息和信号强度;

当所述身份信息匹配于所述候选用户对应的标准身份信息时,所述服务端确定所述候选用户对应的用户账号以用于响应所述交互指令对应的交互操作。

10.根据权利要求9所述的方法,所述确定所述候选用户对应的用户账号,包括:

所述服务端根据预先记录的所有用户的用户账号和标准身份信息之间的对应关系,确定对应于所述候选用户的标准身份信息的用户账号。

11.根据权利要求9所述的方法,所述候选用户包括在第二预设时长内位于所述交互端附近的用户。

12.根据权利要求11所述的方法,

通过将任一用户客户端的定位信息与所述交互端的安装位置信息进行比较,确定所述任一用户客户端对应的用户是否位于所述交互端附近。

13.根据权利要求9所述的方法,还包括:

所述服务端将所述用户账号告知所述交互端,以由所述交互端响应于所述交互指令,针对所述用户账号实施交互操作。

14.根据权利要求9所述的方法,还包括:

所述服务端在确定出所述用户账号后,根据所述交互端预先提供的交互数据,针对所述用户账户实施交互操作。

15.根据权利要求9所述的方法,所述服务端将所述身份信息与所述交互端对应候选用户的标准身份信息进行匹配,包括:

所述服务端分别将所述身份信息与各个候选用户对应的标准身份信息进行匹配,并分别得到相应的相似度;

其中,当最高相似度大于预设相似度阈值、且所述最高相似度与次高相似度之间的差值大于预设混淆差值时,所述最高相似度对应的候选用户被确定为匹配于所述用户。

16.一种身份认证方法,包括:

用户客户端接收到交互端发射的包含收款端标识信息的近场消息;

所述用户客户端将所述交互端标识信息、所述用户客户端的已登录用户的用户标识信息和所述近场消息的信号强度发送至服务端,以由所述服务端在接收到的所述信号强度大于预设强度的情况下,将所述已登录用户确定为所述交互端对应的候选用户,其中,在所述交互端标识信息、用户标识信息和信号强度的保存时长超出预设时长时,所述交互端标识信息、用户标识信息和信号强度被所述服务端删除;

其中,当所述交互端获取到针对所述已登录用户的交互指令时,所述已登录用户的身份数息被所述交互端获取并发送至所述服务端,以由所述服务端将所述身份信息与所述候选用户对应的标准身份信息进行匹配,并确定出所述已登录用户对应的用户账号以用于响应所述交互指令对应的交互操作。

17.一种身份认证装置,包括:

消息发射单元,使交互端向外发射包含交互端标识信息的近场消息;其中,当所述近场消息被用户对应的用户客户端接收到时,所述近场消息用于指示所述用户客户端:将所述交互端标识信息、所述用户的用户标识信息和所述近场消息的信号强度发送至服务端,以由所述服务端在接收到的所述信号强度大于预设强度的情况下,将所述用户确定为所述交互端对应的候选用户;并在所述交互端标识信息、用户标识信息和信号强度的保存时长超出第一预设时长时,删除所述交互端标识信息、用户标识信息和信号强度;

信息获取单元,使所述交互端根据接收到的针对所述用户发起的交互指令,获取所述用户的身份信息;

请求发送单元,使所述交互端向所述服务端发送包含所述身份信息的身份识别请求,所述身份识别请求用于指示所述服务端将所述身份信息与所述交互端对应的标准身份信息进行匹配,以确定出所述用户对应的用户账号以用于响应所述交互指令对应的交互操作。

18.一种身份认证装置,包括:

请求接收单元,使服务端接收到交互端发送的包含用户的身份信息的身份识别请求,所述身份信息由所述交互端根据针对所述用户发起的交互指令向所述用户获取得到;

身份匹配单元,使所述服务端将所述身份信息与所述交互端对应的标准身份信息进行匹配;其中,所述交互端附近的用户被所述服务端通过下述方式标记为所述交互端对应的候选用户:

数据库调取单元,使所述服务端调取数据库,所述数据库中记录有所述用户对应的用户客户端上传的交互端标识信息、用户标识信息和信号强度;其中,所述用户客户端在接收到所述交互端向外发射的近场消息时,将所述用户的用户标识信息、所述近场消息中包含的、交互端标识信息、所述近场消息的信号强度上传至所述服务端;所述服务端在接收到的所述信号强度大于预设强度的情况下,将所述用户确定为所述交互端对应的候选用户,并在所述交互端标识信息、用户标识信息和信号强度的保存时长超出预设时长时,删除所述交互端标识信息、用户标识信息和信号强度;

账号确定单元,使当所述身份信息匹配于所述候选用户对应的标准身份信息时,所述服务端确定所述候选用户对应的用户账号以用于响应所述交互指令对应的交互操作。

19.一种身份认证装置,包括:

消息接收单元,使用户客户端接收到交互端发射的包含收款端标识信息的近场消息;

信息发送单元,使所述用户客户端将所述交互端标识信息、所述用户客户端的已登录用户的用户标识信息和所述近场消息的信号强度发送至服务端,以由所述服务端在接收到的所述信号强度大于预设强度的情况下,将所述已登录用户确定为所述交互端对应的候选用户,其中,在所述交互端标识信息、用户标识信息和信号强度的保存时长超出预设时长时,所述交互端标识信息、用户标识信息和信号强度被所述服务端删除;

其中,当所述交互端获取到针对所述已登录用户的交互指令时,所述已登录用户的身份数息被所述交互端获取并发送至所述服务端,以由所述服务端将所述身份数息与所述候选用户对应的标准身份数息进行匹配,并确定出所述已登录用户对应的用户账号以用于响应所述交互指令对应的交互操作。

20.一种电子设备,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器通过运行所述可执行指令以实现如权利要求2-16中任一项所述的方法。

21.一种计算机可读存储介质,其上存储有计算机指令,其特征在于,该指令被处理器执行时实现如权利要求2-16中任一项所述方法的步骤。

身份认证方法、装置和系统

技术领域

[0001] 本申请涉及身份认证技术领域，尤其涉及一种身份认证方法、装置和系统。

背景技术

[0002] 在相关技术中，用户之间可以实现交互操作。在交互操作的实施过程中，一方采用交互设备、另一方采用用户设备，使得该用户设备的使用者获得感兴趣的交互对象，而该交互对象的提供者，可以通过在交互设备与用户设备之间实现的交互操作，从该使用者处获取相应的交互资源。

[0003] 在相关技术中，上述的使用者需要手动操控用户设备，才能够使得该用户设备与交互设备之间完成交互操作。然而，该使用者往往可能处于不利于操作的场景下，比如携带较多的行李等，造成交互效率较低。

发明内容

[0004] 有鉴于此，本申请提供一种身份认证方法、装置和系统，可以提高对用户的身份识别效率和识别准确度，有助于提升交互效率和安全性。

[0005] 为实现上述目的，本申请提供技术方案如下：

[0006] 根据本申请的第一方面，提出了一种身份认证系统，包括：用户客户端、收款端和服务端；

[0007] 所述收款端向外发射近场消息，所述近场消息中包含所述收款端的收款端标识信息；

[0008] 所述用户客户端在接收到所述近场消息时，将所述收款端标识信息、所述用户客户端的已登录用户的用户标识信息和所述近场消息的信号强度发送至所述服务端；

[0009] 所述服务端接收到所述用户客户端发送的收款端标识信息、用户标识信息和信号强度，并在所述信号强度大于预设强度的情况下，将所述已登录用户标记为所述收款端对应的候选用户；

[0010] 所述收款端接收到针对所述已登录用户发起的交易指令，根据所述交易指令获取所述已登录用户的生物特征信息，并向所述服务端发送包含所述生物特征信息的身份识别请求；

[0011] 所述服务端接收到所述身份识别请求，将所述生物特征信息与所述收款端对应的候选用户的标准生物特征信息进行匹配，并确定出所述已登录用户对应的用户账号，所述用户账号用于响应所述交易指令对应的交易操作。

[0012] 根据本申请的第二方面，提出了一种身份认证方法，包括：

[0013] 交互端接收到针对用户发起的交互指令；

[0014] 所述交互端获取所述用户的身份信息；

[0015] 所述交互端向服务端发送身份识别请求，所述身份识别请求中包含所述身份信息，所述身份识别请求用于指示所述服务端将所述身份信息与所述交互端对应的候选用户

的标准身份信息进行匹配,以确定出所述用户对应的用户账号,所述用户账号用于响应所述交互指令对应的交互操作;其中,所述交互端附近的用户被所述服务端标记为相应的候选用户。

[0016] 根据本申请的第三方面,提出了一种身份认证方法,包括:

[0017] 服务端接收到交互端发送的身份识别请求,所述身份识别请求中包含用户的身份信息,所述身份信息由所述交互端根据针对所述用户发起的交互指令向所述用户获取得到;

[0018] 所述服务端将所述身份信息与所述交互端对应候选用户的标准身份信息进行匹配;其中,所述交互端附近的用户被所述服务端标记为相应的候选用户;

[0019] 当所述身份信息匹配于所述候选用户对应的标准身份信息时,所述服务端确定所述候选用户对应的用户账号,所述用户账号用于响应所述交互指令对应的交互操作。

[0020] 根据本申请的第四方面,提出了一种身份认证方法,包括:

[0021] 用户客户端接收到交互端发射的近场消息,所述近场消息中包含所述交互端的交互端标识信息;

[0022] 所述用户客户端将所述交互端标识信息、所述用户客户端的已登录用户的用户标识信息和所述近场消息的信号强度发送至服务端,以由所述服务端在所述信号强度大于预定强度的情况下将所述已登录用户标记为所述交互端对应的候选用户;

[0023] 其中,当所述交互端获取针对所述已登录用户的交互指令时,所述已登录用户的身份信息被所述交互端获取并发送至所述服务端,以由所述服务端将所述身份信息与各个候选用户对应的标准身份信息进行匹配、确定出所述已登录用户对应的用户账号,所述用户账号用于响应所述交互指令对应的交互操作。

[0024] 根据本申请的第五方面,提出了一种身份认证装置,包括:

[0025] 接收单元,使交互端接收到针对用户发起的交互指令;

[0026] 获取单元,使所述交互端获取所述用户的身份信息;

[0027] 发送单元,使所述交互端向服务端发送身份识别请求,所述身份识别请求中包含所述身份信息,所述身份识别请求用于指示所述服务端将所述身份信息与所述交互端对应候选用户的标准身份信息进行匹配,以确定出所述用户对应的用户账号,所述用户账号用于响应所述交互指令对应的交互操作;其中,所述交互端附近的用户被所述服务端标记为相应的候选用户。

[0028] 根据本申请的第六方面,提出了一种身份认证装置,包括:

[0029] 接收单元,使服务端接收到交互端发送的身份识别请求,所述身份识别请求中包含用户的身份信息,所述身份信息由所述交互端根据针对所述用户发起的交互指令向所述用户获取得到;

[0030] 匹配单元,使所述服务端将所述身份信息与所述交互端对应候选用户的标准身份信息进行匹配;其中,所述交互端附近的用户被所述服务端标记为相应的候选用户;

[0031] 确定单元,当所述身份信息匹配于所述候选用户对应的标准身份信息时,使所述服务端确定所述候选用户对应的用户账号,所述用户账号用于响应所述交互指令对应的交互操作。

[0032] 根据本申请的第七方面,提出了一种身份认证装置,包括:

[0033] 接收单元,使用户客户端接收到交互端发射的近场消息,所述近场消息中包含所述交互端的交互端标识信息;

[0034] 发送单元,使所述用户客户端将所述交互端标识信息、所述用户客户端的已登录用户的用户标识信息和所述近场消息的信号强度发送至服务端,以由所述服务端在所述信号强度大于预设强度的情况下将所述已登录用户标记为所述交互端对应的候选用户;

[0035] 其中,当所述交互端获取针对所述已登录用户的交互指令时,所述已登录用户的身份信息被所述交互端获取并发送至所述服务端,以由所述服务端将所述身份信息与各个候选用户对应的标准身份信息进行匹配、确定出所述已登录用户对应的用户账号,所述用户账号用于响应所述交互指令对应的交互操作。

[0036] 由以上技术方案可见,本申请通过由服务器确定出交互端附近的用户并将其标记为候选用户,使得这些用户仅需要向该交互端提供自身的身份信息,即可由服务端自动确定出这些用户对应的用户账号,以便针对确定出的用户账号实施交互操作,一方面无需用户对自身的用户设备进行操作,有助于简化用户操作、提升交互效率,另一方面可以缩小对身份信息的身份识别范围(限制为交互端对应的候选用户),且整个身份识别过程由服务端进行客观匹配而实现、而非人工参与识别,有助于提升对用户身份的识别效率和识别准确度,从而提高交互安全性。

附图说明

[0037] 图1是本申请一示例性实施例提供的一种身份认证系统的架构示意图。

[0038] 图2是本申请一示例性实施例提供的一种基于交互端侧的身份认证方法的流程图。

[0039] 图3是本申请一示例性实施例提供的一种基于服务端侧的身份认证方法的流程图。

[0040] 图4是本申请一示例性实施例提供的一种基于用户客户端侧的身份认证方法的流程图。

[0041] 图5是本申请一示例性实施例提供的一种交易场景的示意图。

[0042] 图6是本申请一示例性实施例提供的一种交易流程图。

[0043] 图7是本申请一示例性实施例提供的另一种交易场景的示意图。

[0044] 图8是本申请一示例性实施例提供的一种基于交互端侧的电子设备的结构示意图。

[0045] 图9是本申请一示例性实施例提供的一种基于交互端侧的身份认证装置的框图。

[0046] 图10是本申请一示例性实施例提供的一种基于服务端侧的电子设备的结构示意图。

[0047] 图11是本申请一示例性实施例提供的一种基于服务端侧的身份认证装置的框图。

[0048] 图12是本申请一示例性实施例提供的一种基于用户客户端侧的电子设备的结构示意图。

[0049] 图13是本申请一示例性实施例提供的一种基于用户客户端侧的身份认证装置的框图。

具体实施方式

[0050] 图1是本申请一示例性实施例提供的一种身份认证系统的架构示意图。如图1所示，该系统可以包括服务器11、网络12、若干用户设备(比如手机13、手机14等)以及交互设备(比如收银台设备15、收银台设备16等)。

[0051] 服务器11可以为包含一独立主机的物理服务器，或者该服务器11可以为主机集群承载的虚拟服务器，或者该服务器11可以为云服务器。在运行过程中，服务器11可以运行某一应用的服务器侧的程序，以实现该应用的相关业务功能，比如当该服务器51运行交互操作的程序时，可以被配置为用于实现交互功能的服务端。

[0052] 手机13-14只是用户可以使用的一种类型的用户设备。实际上，用户显然还可以使用诸如下述类型的电子设备：平板设备、笔记本电脑、掌上电脑(PDAs, Personal Digital Assistants)、可穿戴设备(如智能眼镜、智能手表等)等，本申请并不对此进行限制。在运行过程中，该用户设备可以运行某一应用的用户客户端侧的程序，以实现该应用的相关业务功能，比如当该电子设备运行交互操作的程序时，可以被配置为用于实现交互功能的用户客户端。

[0053] 收银台设备15-16只是可以用于实现交互功能的一种交互设备。实际上，交互设备还可以采用诸如销售终端(point of sale, POS)等，本申请并不对此进行限制。在运行过程中，该交互设备可以运行某一应用的交互端侧的程序，以实现该应用的相关业务功能，比如当该交互设备运行交互操作的程序时，可以被配置为用于实现交互功能的交互端。

[0054] 而对于手机13-14、收银台设备15-16与服务器11之间进行交互的网络12，可以包括多种类型的有线或无线网络。在一实施例中，该网络12可以包括公共交换电话网络(Public Switched Telephone Network, PSTN)和因特网，本申请并不对此进行限制。在另一实施例中，当网络12用于手机13-14、收银台设备15-16之间的交互时，网络12可以包括近场无线通讯网络，例如蓝牙、WIFI、NFC(Near Field Communication, 近场通信)、RFID(Radio Frequency Identification, 射频识别)等，本申请并不对此进行限制。

[0055] 可见，在本申请的技术方案的实施过程中，涉及到用户客户端、交互端、服务端之间的三方交互；其中，从硬件设备的角度而言，用户客户端可以运行于用户设备(如手机13-14)上、交互端可以运行于交互设备(如收银台设备15-16)上、服务端可以运行于服务器11上。下面分别从各方的处理逻辑，以及三方之间的交互过程，对本申请的技术方案进行描述。

[0056] 图2是本申请一示例性实施例提供的一种基于交互端侧的身份认证方法的流程图。如图2所示，该方法应用于交互端上，可以包括以下步骤：

[0057] 步骤202，交互端接收到针对用户发起的交互指令。

[0058] 在本实施例中，交互端可以主动生成交互指令，或者交互端可以接收相关联的其他设备发送的交互指令。

[0059] 步骤204，所述交互端根据所述交互指令，获取所述用户的身份信息。

[0060] 在本实施例中，身份信息是指交互端基于交互指令而获取的该用户的身份信息，该身份信息唯一对应于该用户。

[0061] 在本实施例中，身份信息可以采用任意类型的信息，本申请并不对此进行限制。比如，身份信息可以包括用户输入的密码信息；再比如，身份信息可以包括生物特征信息，则

标准身份信息可以包括标准生物特征信息，例如该生物特征信息与该标准生物特征信息可以包括以下至少之一：人脸信息、指纹信息、掌纹信息、眼纹信息、虹膜信息、步态信息等，本申请并不对此进行限制。

[0062] 步骤206，所述交互端向服务端发送身份识别请求，所述身份识别请求中包含所述身份信息，所述身份识别请求用于指示所述服务端将所述身份信息与所述交互端对应的候选用户的标准身份信息进行匹配，以确定出所述用户对应的用户账号，所述用户账号用于响应所述交互指令对应的交互操作；其中，所述交互端附近的用户被所述服务端标记为相应的候选用户。

[0063] 在本实施例中，服务端可以预先获取并记录所有用户对应的用户账号、标准身份信息等，使得通过将身份信息与标准身份信息进行匹配后，可以根据匹配于该身份信息的标准身份信息，确定该身份信息对应的用户账号（即匹配于该身份信息的标准身份信息对应的用户账号），以便于交互端上的设备客户端针对该确定出的用户账号实施交互操作。

[0064] 其中，服务端可以承载用户的账号注册服务，使得每一用户在注册自身的用户账号时，即可将自身的用户账号、标准身份信息等关联记录于该服务端处，以便于服务端后续通过将标准身份信息与身份信息进行匹配，以对相应的用户进行身份识别。

[0065] 在本实施例中，当确定出所述用户对应的用户账号时，所述交互端可以接收服务端返回的该用户账号，从而响应于所述交互指令，针对确定出的用户账号实施交互操作。其中，交互端在响应于上述交互指令时，可以向服务端发起相应的交互请求，以由该服务端针对该用户账号进行交互；或者，交互端也可以向区别于该服务端的其他交互服务端发起交互请求，以由该其他交互服务端针对该用户账号进行交互。此外，当上述的服务端可以针对该用户账号进行交互时，服务端还可以在确定出该用户账号后，根据交互端告知的交互数据主动完成交互，而不需要交互端单独发送上述的交互请求，甚至不需要将用户账号告知交互端，有助于避免用户账号泄露、防止暴露用户与用户账号之间的关联关系，提升交互安全性。

[0066] 在本实施例中，交互端可以向外发射近场消息，该近场消息中包含所述交互端的交互端标识信息；其中，近场消息可以被基于蓝牙技术而发射，则该近场消息可以为通告帧（Advertising）消息，近场消息还可以基于其他任意的近场通讯技术而发射，比如WIFI、NFC、RFID等，本申请并不对此进行限制。当然，近场消息可以被采用广播方式而发送，即近场广播消息，也可以采用非广播形式的其他方式发送，本申请并不对此进行限制。

[0067] 进一步地，当近场消息被用户对应（如登录）的用户客户端接收到时，该近场消息用于指示该用户客户端：将交互端标识信息（包含于近场消息中）、该用户的用户标识信息和该近场消息的信号强度（如RSSI，Received Signal Strength Indication）发送至服务端，以由服务端在该信号强度大于预设强度的情况下将该用户标记为交互端对应的候选用户，那么由于信号强度与间隔距离呈反相关，可以确保服务端将交互端附近的用户标记为相应的候选用户。

[0068] 在本实施例中，由于用户（及其对应的用户客户端）往往处于运动过程中，因而候选用户可以进一步包括在预设时长内位于交互端附近的用户，以确保“候选用户”的时效性。其中，交互端可以持续、反复发射近场消息，而用户客户端也可以针对接收到近场消息而反复向服务端相关联地发送交互端标识信息、用户标识信息和近场消息的信号强度，使

得交互端对应的候选用户能够得到更新,以确保其时效性。

[0069] 图3是本申请一示例性实施例提供的一种基于服务端侧的身份认证方法的流程图。如图3所示,该方法应用于服务端上;该方法可以包括以下步骤:

[0070] 步骤302,服务端接收到交互端发送的身份识别请求,所述身份识别请求中包含用户的身份信息,所述身份信息由所述交互端根据针对所述用户发起的交互指令向所述用户获取得到。

[0071] 步骤304,所述服务端将所述身份信息与所述交互端对应候选用户的标准身份信息进行匹配;其中,所述交互端附近的用户被所述服务端标记为相应的候选用户。

[0072] 在本实施例中,服务端可以在接收到身份识别请求后,确定交互端对应候选用户;或者,服务端可以预先(例如周期性地)生成交互端对应候选用户,而非在接收到身份识别请求后确定,以降低对身份识别请求的响应延迟。

[0073] 在本实施例中,服务端可以通过多种方式确定交互端附近的用户,以标记相应的候选用户。在一种情况下,服务端可以获取用户客户端的定位信息(例如基于GPS、北斗等定位模块生成的定位信息,或者基于室内定位技术得到的定位信息等),通过将定位信息与交互端的安装位置信息进行比较,以确定该交互端附近的用户。

[0074] 在另一种情况下,服务端可以调取数据库,该数据库中记录有所述用户对应的用户客户上传的交互端标识信息、用户标识信息和信号强度;其中,所述用户客户端在接收到所述交互端向外发射的近场消息时,将所述用户的用户标识信息以及所述近场消息中包含的所述交互端的交互端标识信息、所述近场消息的信号强度上传至所述服务端,以供所述服务端记录至所述数据库;以及,服务端可以接收所述用户上传的交互端标识信息、用户标识信息和信号强度,并在所述信号强度大于预设强度的情况下,将所述用户标记为该交互端对应的候选用户。

[0075] 进一步地,由于用户(及其对应的用户客户端)往往处于运动过程中,因而候选用户可以进一步包括在预设时长内位于交互端附近的用户,以确保“候选用户”的时效性。尤其是对于服务端采用上述基于“数据库”的实施方式时,服务端可以针对数据库中的关联信息进行生命周期管理,例如主动删除数据库中保存时长超出预设时长1的关联信息,以满足“候选用户”的时效性。

[0076] 在本实施例中,当所述身份信息匹配于所述候选用户对应的标准身份信息时,所述服务端可以将所述候选用户对应的用户账号告知所述交互端,以由所述交互端响应于所述交互指令,针对所述候选用户对应的用户账号实施交互操作。其中,服务端可以支持交互功能,则交互端可以通过向该服务端发起交互请求,以由该服务端完成上述的交互操作;或者,当服务端支持交互功能时,服务端可以在确定出上述的用户账号后,无需交互端发起交互请求,即可主动实施上述的交互操作,那么服务端甚至无需将该用户账号发送至交互端,有助于避免用户账号泄露、防止暴露用户与用户账号之间的关联关系,提升交互安全性。

[0077] 在本实施例中,“匹配”可以理解为身份信息与标准身份信息之间的相似度大于预设相似度。其中,当同时存在多个标准身份信息时,服务端可以分别将身份信息与各个候选用户对应的标准身份信息进行匹配,并分别得到相应的相似度;其中,当最高相似度大于预设相似度阈值、且所述最高相似度与次高相似度之间的差值大于预设混淆差值时,即在排除了其他用户的混淆因素的情况下,使得所述最高相似度对应的候选用户被确定为匹配于

所述用户。

[0078] 图4是本申请一示例性实施例提供的一种基于用户客户端侧的身份认证方法的流程图。如图4所示，该方法应用于用户客户端上，可以包括以下步骤：

[0079] 步骤402，用户客户端接收到交互端发射的近场消息，所述近场消息中包含所述交互端的交互端标识信息。

[0080] 步骤404，所述用户客户端将所述交互端标识信息、所述用户客户端的已登录用户的用户标识信息和所述近场消息的信号强度发送至服务端，以由所述服务端在所述信号强度大于预设强度的情况下将所述已登录用户标记为所述交互端对应的候选用户。

[0081] 在本实施例中，当所述交互端获取针对上述已登录用户的交互指令时，所述已登录用户的身份信息可以被所述交互端获取并发送至所述服务端，以由所述服务端将所述身份信息与所述候选用户对应的标准身份信息进行匹配、确定出所述已登录用户对应的用户账号，所述用户账号用于响应所述交互指令对应的交互操作。

[0082] 在本实施例中，交互端可以持续、反复(例如周期性地)发射近场消息，而用户客户端可以在每次接收到近场消息后，均向服务端相关联地发送交互端标识信息、用户标识信息和信号强度，以使得交互端对应的候选用户得以被更新、适应于用户的动态特点。当然，为了降低数据收发导致的功耗，用户客户端可以识别发射近场消息的交互端(例如通过读取近场消息中包含的交互端标识信息等方式)，从而在已经接收到所述交互端发射的近场消息并据此向服务端相关联地发送交互端标识信息、用户标识信息和信号强度后，如果在预设时长2内再次接收到该交互端的近场消息，该用户客户端可以忽略再次接收到的该近场消息；其中，当服务端采用上文描述的生命周期管理机制时，用户客户端采用的该预设时长2应当不大于服务端实施生命周期管理机制的预设时长1，以确保用户客户端处于交互端附近时，服务端必然能够将使用该用户客户端的已登录用户标记为该交互端的候选用户。

[0083] 由以上技术方案可见，本申请通过由服务器确定出交互端附近的用户并将其标记为候选用户，使得这些用户仅需要向该交互端提供自身的身份信息，即可由服务端自动确定出这些用户对应的用户账号，以便针对确定出的用户账号实施交互操作，一方面无需用户对自身的用户设备进行操作，有助于简化用户操作、提升交互效率，另一方面可以缩小对身份信息的身份识别范围(限制为交互端对应的候选用户)，且整个身份识别过程由服务端进行客观匹配而实现、而非人工参与识别，有助于提升对用户身份的识别效率和识别准确度，从而提高交互安全性。

[0084] 在本申请的技术方案中，任何交互操作均可以采用本申请的身份认证方案，并属于本申请技术方案的保护范围之内；例如，交互操作可以包括：信息交互、数据交互、资源交互等。以资源交互为例，在较为具体的场景下，本申请的技术方案可以被应用于交易过程中，比如由卖场提供用于交易的货品资源，而买家提供用于交易的对象资源(如资金、兑换码等)，从而在卖场与买家之间实现货品资源与对象资源之间的资源交互。

[0085] 为了便于理解，下面以上述的交易场景为例，对本申请的技术方案进行说明。如图5所示，假定用户C1前往超市购物，在完成购物时该用户C1携带挑选的货品510前往收银台处，由收银员S1对该货品510进行计价和收款。在货品510上通常设置有价签(例如采用条码等形式)，收银员S1通过收银台设备52上的价签采集装置读取价签(例如条码阅读器等)，并由收银台设备52基于读取价格而发起针对该用户C1的交易指令。

[0086] 当基于相关技术来实施付款时,用户C1需要取出携带的手机51(或其他类型的电子设备),在手机51上展示出付款码(例如采用二维码形式),该付款码的内容与该用户C1的用户账号相关,使得收银台设备52可以针对该用户账号完成交易,即从该用户账号内完成扣款。但是,上述过程需要用户C1专门实施对手机51的各种操作,不仅增加了用户C1的额外负担,而且用户C1并不总是能够顺利完成整个操作,比如图5中的用户C1右手拿着货品510,只能用左手从右边口袋中取出手机51,或者将货品510放下、空出右手再取出手机51,导致用户C1的整个付款过程不顺利,也增加了其他用户的等待时长。

[0087] 而基于本申请的技术方案,用户C1可以在不需要针对手机51执行任何操作的情况下,完成整个付款过程,从而简化用户操作、提升交易效率。在整个付款过程中,可以由手机51、收银台设备52与服务器53之间自动实现交互操作,从而快速完成付款。

[0088] 图6是本申请一示例性实施例提供的一种交易流程图。如图6所示,手机51上运行有预设应用程序的手机客户端、收银台设备52运行有预设应用程序的收银台客户端、服务器53上运行有预设应用程序的服务端,通过手机客户端、收银台客户端和服务端使得手机51、收银台设备52、服务器53能够实现本申请的技术方案;其中,该预设应用程序可以为任意支付应用,当然本申请并不对此进行限制。为了便于理解,下面均以手机51、收银台设备52、服务器53各自实施的处理动作或相互之间的交互操作进行描述,而不再强调手机客户端、收银台客户端和服务端。该交易过程可以包括以下步骤:

[0089] 步骤601,用户C1预先通过手机51上的手机客户端,向服务器53注册对应的用户账号。

[0090] 在本实施例中,用户C1需要在服务器53上拥有唯一对应的用户账号,该用户账号与该用户C1的资金账户相关,以便于通过该用户账号从用户C1的资金账户中扣除/支付相应的资金。通常而言,手机客户端可以在用户C1首次运行时,引导用户C1完成账号注册;当然,用户C1也可以根据实际情况,在其他时机或场景下完成注册操作,本申请并不对此进行限制。此外,用户C1还可以通过诸如PC端或其他设备完成上述的账号注册操作,并在手机51上予以登录;或者,用户C1还可以将自己在其他应用程序中注册的用户账号绑定至该手机客户端对应的应用程序,从而免去账号注册过程、简化用户C1的操作。实际上,任何能够在手机客户端对应的应用程序中,为用户C1构建唯一对应的用户账号的方式,均可以应用于本申请的技术方案,本申请并不对此进行限制。

[0091] 在本实施例中,手机客户端的应用程序可以被预先安装在手机51上,使得该手机客户端可以在该手机51上被启动并运行;当然,当采用诸如HTML5技术的在线“客户端”时,无需在手机51上安装相应的应用程序,同样能够运行该手机客户端,本申请并不对此进行限制。实际上,对于收银台设备52上运行的收银台客户端等,与手机客户端的情况类似,此处不再赘述。

[0092] 步骤602,服务器53关联记录用户账号和标准人脸图像信息。

[0093] 在本实施例中,当用户C1通过手机51运行的手机客户端注册用户账号时,手机客户端可以在注册过程中获取用户C1的人脸图像信息,以作为该用户C1注册的用户账号对应的标准人脸图像信息,即服务器53后续可以将该标准人脸图像信息作为评判标准,识别某一用户的身份是否为该用户C1。

[0094] 当然,对于采用如PC端注册的用户账号,或者虽然在手机客户端注册,但是由于时

间较早而在当时未开通对人脸图像信息的采集功能,或者采用其他应用程序中注册的用户账号等情况下,用户C1也可以在手机客户端内单独开启人脸图像信息的采集功能,并将采集到的标准人脸图像信息关联至用户C1的用户账号,而并不一定在注册用户账号的过程中完成对标准人脸图像信息的采集操作。

[0095] 除了用户C1之外,上述预设应用程序的所有用户,均可以通过与用户C1相类似的方式,在该预设应用程序中获得唯一对应的用户账号,并在服务器53上记录有相关联的标准人脸图像信息。

[0096] 步骤603,收银台设备52向外发射通告帧消息,该通告帧消息中包含该收银台设备52的设备标识信息。

[0097] 在本实施例中,收银台设备52可以基于蓝牙通讯技术,向外发射通告帧消息,该通告帧消息中包含该收银台设备52的设备标识信息,以表明该通告帧消息的来源设备。例如,设备标识信息可以被包含于通告帧消息中的单个字段中,比如UUID(Universally Unique Identifier,通用唯一识别码);或者,设备标识信息可以由通告帧消息中的多个字段同时表征,比如采用UUID、Major(主要)参数、Minor(次要)参数等共同组成收银台设备52的设备标识信息。

[0098] 步骤604,手机51接收到收银台设备52发射的通告帧消息。

[0099] 步骤605,手机51确定接收到的通告帧消息的信号强度、提取通告帧消息中包含的设备标识信息,并根据手机51上登录的用户C1的用户账号,将用户标识信息(对应于用户C1的用户账号,比如该用户账号本身或其他)、设备标识信息与信号强度构成的关联信息上传至服务器53。

[0100] 在本实施例中,以图7所示的交易场景为例。假定用户C1所处的交易场景为超市购物,当用户C1位于收银台设备52处结账时,可能存在用户U1、用户U2等其他用户同样等待该收银台设备52进行结账,而该收银台设备52附近还通常会存在其他收银台设备以及等待这些收银台设备进行结账的其他用户,即收银台设备52周围同时存在很多用户,而收银台设备52需要在用户C1不主动取出手机51并表明身份的情况下,自动识别出该用户C1的身份信息、确定出该用户C1对应的用户账号(其他收银台设备同样需要识别出需要结账的相应用户对应的用户账号,此处不再赘述)。

[0101] 为了实现对用户身份的有效识别,每一收银台设备可以向外发射通告帧消息,该通告帧消息中包含自身的设备标识信息。比如,收银台设备52基于上述的步骤603而发射相应的通告帧消息;当然,收银台设备52可以按照一定周期进行持续性地发射该通告帧消息,以适应于周围用户的动态更新。

[0102] 由于通告帧消息为近场通讯消息,存在一定的覆盖范围M1,使得只有位于该覆盖范围M1内的用户设备,比如以图7所示的收银台设备52为例,位于覆盖范围M1内的用户设备可以包括用户C1的手机51、用户U1的手机71、用户U2的手机72、用户U3的手机73和用户U4的手机74等。通过调整通告帧消息的发射功率等参数,可以控制覆盖范围M1的大小;当覆盖范围M1较小时,可以有效地减少接收到该通告帧消息的用户设备、减小后续确定出的候选用户的数量,从而有助于提升交易效率,但是当用户的站立位置与收银台设备间隔较大时,过小的覆盖范围M1可能导致用户使用的用户设备无法有效接收到通告帧消息,而过大的覆盖范围M1会导致接收到通告帧消息的用户设备过多,可能造成后续的交易效率降低,所以应

当根据实际情况选取恰当的发射功率、形成适当大小的覆盖范围M1。

[0103] 步骤606，服务器53接收到手机51发送的关联信息，并记录接收到的关联信息。

[0104] 在本实施例中，不仅手机51会发送关联信息，所有接收到通告帧消息的用户设备均会向服务器53发送关联信息，以由服务器53进行记录。服务器53可以将接收到的关联信息记录在任意预配置的存储空间，比如可以存储于相关联的数据库中。

[0105] 在本实施例中，服务器53可以采用利于检索的数据结构来记录关联信息，以便于提升后续的数据检索效率，从而提升整体的交易效率。例如，可以创建关联信息表，服务器53将接收到的每一关联信息分别记录为该关联信息表中对应的一条数据，且每条数据的数据结构可以采用：以设备标识信息（如UUID、Major参数、Minor参数等）和用户标识信息为主键、信号强度为值，以便于对该关联信息表中的各条数据实施检索操作。而针对已经创建的关联信息表，服务器53在接收到关联信息时，可以根据该关联信息中包含的设备标识信息和用户标识信息对该关联信息表进行检索，如果存在相匹配的数据，可以根据该关联信息覆盖该数据的值，以实现数据更新；如果不存在相匹配的数据，可以在该关联信息表中添加新的主键，以创建一条新的数据。

[0106] 步骤607，收银台设备52获取交易指令。

[0107] 在本实施例中，收银台设备52可以包含一价格获取装置，该价格获取装置读取用户C1携带的所有货品（如货品510等）的价格后，可以生成针对该用户C1的交易指令，以触发针对该用户C1的交易操作。举例而言，价格获取装置可以包括一条码阅读器，而货品510上可以包含指示其价格的条码，该价格获取装置通过读取该条码，即可获知该货品510的价格；或者，价格获取装置可以包括一RFID阅读器，而货品510上可以包含指示器价格的RFID标签，该RFID标签可以向该RFID阅读器发射价格指示信息（例如货品510的商品信息，或者价格本身），以使其获知货品510的价格；或者，还可以通过其他任意方式获知货品510的价格，本申请并不对此进行限制。

[0108] 当然，价格获取装置并非一定要集成于收银台设备52内部，价格获取装置可以在获知用户C1携带的各个货品的价格后，向收银台设备52发送通知消息，那么收银台设备52可以基于该通知消息而生成交易指令，或者该通知消息本身可以被作为交易指令。

[0109] 步骤608，收银台设备52采集用户C1的人脸图像信息。

[0110] 在本实施例中，收银台设备52可以包括一身份信息采集装置520；当用户C1在收银台设备52处结账时，该身份信息采集装置520可以采集该用户C1的人脸图像信息。

[0111] 在本实施例中，身份信息采集装置520采集任意类型的用户身份信息，但是应当确保服务器53在步骤602中记录有相应信息类型的标准用户身份信息，例如当服务器53记录的标准用户身份信息为标准人脸图像信息时，身份信息采集装置520也应当采集相应的人脸图像信息，而当服务器53记录的标准用户身份信息为标准指纹信息时，身份信息采集装置520也应当采集相应的指纹信息。

[0112] 当然，除了人脸图像信息、指纹信息等生物特征信息之外，其他的非生物特征信息也可以被应用于此处的用户身份信息，本申请并不对此进行限制。

[0113] 步骤609，收银台设备52向服务器53发送身份识别请求，该身份识别请求中包含用户C1的人脸图像信息。

[0114] 步骤610，服务器53确定出收银台设备52对应的候选用户。

[0115] 在本实施例中,服务器53在接收到身份识别请求时,可以确定该身份识别请求来自于收银台设备52,则服务器53以该收银台设备52的设备标识信息为关键字,在记录的关联信息(例如上述的关联信息表)中进行检索,以确定出匹配于该收银台设备52的关联信息。

[0116] 在本实施例中,由于用户设备只有在接收到收银台设备52发射的通告帧消息时,才会向服务器53发送关联信息,而该通告帧消息存在一定的覆盖范围M1,使得对于超出该覆盖范围M1、距离收银台设备52较远的用户,其使用的用户设备必然无法接收到收银台设备52发射的通告帧消息、不会向服务器53发送与收银台设备52相关的关联信息,因而这些用户不会被确定为收银台设备52的候选用户。以图7为例,只有用户C1、用户U1、用户U2、用户U3和用户U4向服务器53上传了与收银台设备52相关的关联信息。

[0117] 在一些情况下,服务器53可以直接将上述的用户C1、用户U1、用户U2、用户U3和用户U4确定为收银台设备52对应的候选用户。

[0118] 而在另一些情况下,服务器53还可以进一步进行筛选。由于关联信息中包含通告帧消息的信号强度,而该信号强度与间隔距离呈负相关,即由于手机51与收银台设备52的间隔距离较小、手机72与收银台设备52的间隔距离较大,因而针对收银台设备52发射的通告帧消息,手机51记录的信号强度较大、手机72记录的信号强度较小。因此,服务器53可以根据各个关联信息中记录的信号强度,筛选出信号强度大于预设强度、即与收银台设备52处于预设间隔距离内的用户,而筛除信号强度小于该预设强度、即与收银台设备52超出预设间隔距离的用户,并将筛选出的用户作为收银台设备52对应的候选用户,以尽可能地减小候选用户的数量。以图7为例,针对上述的用户C1、用户U1、用户U2、用户U3和用户U4,服务器53可以进一步筛除用户U2、用户U3和用户U4,则确定出收银台设备52对应的候选用户为用户C1和用户U1。

[0119] 在本实施例中,交易操作存在一定的时限需求。例如,当用户C2在收银台设备52处进行付款时,用户C2使用的用户设备可以接收到收银台设备52发出的通告帧消息、向服务器53发送相应的关联信息,但是当用户C2完成付款并离开后,如果服务器53始终对该关联信息进行记录,那么用户C2可能被反复确认为收银台设备52的候选用户,这将影响后续用户的交易效率。尤其是,随着收银台设备53处的付款用户越来越多,服务器53确定出的该收银台设备52对应的候选用户也会越来越多,导致交易效率越来越低。

[0120] 因此,服务器53可以引入对记录的关联信息的生命周期管理机制,以适当删除诸如上述的用户C2等发送的关联信息,避免其被误判为候选用户。比如,服务器53可以记录每一关联信息的同时,记录相应的保存时长,并主动删除保存时长达到预设时长的关联信息。由于收银台设备52会持续发射通告帧消息,那么如果用户C2位于收银台设备52附近,其使用的用户设备将由于接收到通告帧消息而向服务器53上传相应的关联信息,使得由该用户C2上传的关联信息得以更新、相应的保存时长也得以更新,那么用户C2将会被确定为收银台设备52对应的候选用户;而如果用户C2离开了收银台设备52附近,其使用的用户设备无法接收到通告帧消息、无法对服务器53上记录的关联信息进行更新,使得该用户C2发送的关联信息在超时(即保存时长达到预设时长)后被服务器53自动删除,则该用户C2将不会被继续确定为收银台设备52对应的候选用户。

[0121] 举例而言,当服务器53采用上述的关联信息表来记录关联信息时,服务器53在将

接收到的关联信息插入为该关联信息表中的一条数据时,可以获取该关联信息的插入时刻的时间戳,并将该时间戳与上述的信号强度一并作为该数据的值。那么,服务器53只需要读取各条数据中记录的时间戳,并结合当前时刻即可确定出相应的保存时长,从而主动删除保存时长达到预设时长的关联信息。

[0122] 步骤611,服务器53将人脸图像信息与候选用户的标准人脸图像信息进行对比,确定出用户C1的用户账号并告知收银台设备52。

[0123] 在本实施例中,服务器53可以通过将人脸图像信息与n个候选用户的标准人脸图像信息进行对比,分别计算出人脸图像信息与每一候选用户的标准人脸图像信息之间的相似度,并得到相应的相似度数组[$\text{sim_score}_1, \text{sim_score}_2, \dots, \text{sim_score}_n$]。

[0124] 在一种情况下,服务器53可以将各个相似度与预设相似度阈值进行比较,如果仅单个相似度大于该预设相似度阈值,可以确定人脸图像信息与该相似度对应的标准人脸图像信息相匹配,从而将该相似度对应的标准人脸图像信息对应的候选用户确定为该用户C1,并将该候选用户对应的用户账号确定为该用户C1的用户账号。

[0125] 在另一种情况下,当存在多个相似度均大于该预设相似度阈值时,服务器53可以选取大于该预设相似度阈值的最高相似度,并确定人脸图像信息与该最高相似度对应的标准人脸图像信息相匹配,从而将该最高相似度对应的标准人脸图像信息对应的候选用户确定为该用户C1,并将该候选用户对应的用户账号确定为该用户C1的用户账号。

[0126] 在又一种情况下,当最高相似度大于该预设相似度阈值时,服务器53进一步计算该最高相似度与次高相似度之间的差值,并在该差值大于预设混淆差值的情况下,确定该最高相似度对应的标准人脸图像信息与人脸图像信息相匹配,且不存在其他存在混淆的标准人脸图像信息,从而将该最高相似度对应的标准人脸图像信息对应的候选用户确定为该用户C1,并将该候选用户对应的用户账号确定为该用户C1的用户账号。

[0127] 在本实施例中,由于服务器53可以确定出收银台设备52对应的候选用户,而这些候选用户均为收银台设备52附近的用户,可以排除在其他收银台设备付款的用户、甚至在其他店面付款的用户等,使得服务器53仅需要将人脸图像信息与数量有限的候选用户的标准人脸图像信息进行对比,便于服务器53将人脸图像信息与每一候选用户的标准人脸图像信息进行一对一的详细比对;相比而言,相关技术中在针对人脸图像信息的识别过程中,往往将待识别的人脸图像信息在包含众多人脸图像信息的图像信息库(例如包含所有在服务器53处注册的用户账号对应的标准人脸图像信息)中进行一对多的检索,然后再对检索到的人脸图像信息进行详细比对,可见:本申请的人脸图像信息的识别过程无需检索等复杂操作,有助于提升人脸图像信息的识别效率,并且由于全程采用一对一的详细比对、避免采用一对多的比对方式,尤其是整个人脸图像信息的识别过程完全由服务器53实现、无需收银员S1等人工参与,有助于提升人脸图像信息的识别准确率、提升交易过程的安全性。

[0128] 步骤612,收银台设备52针对确定出的用户账号,执行相应的扣款操作。

[0129] 在本实施例中,当服务器53承载有支付功能时,收银台设备52可以通过与服务器53之间的交互操作,完成上述的扣款操作。当然,收银台设备52也可以与其他的支付平台进行交互操作,完成上述的扣款操作。

[0130] 步骤613,服务器53向收银台设备52、手机51分别发送扣款成功消息。

[0131] 在本实施例中,收银台设备52处还可以设置一电子闸机或类似装置,在未完成扣

款之前,该电子闸机可以保持关闭状态,以阻止用户C1在未付款的情况下将货品510带离;而在完成扣款后,比如收银台设备52或服务器53向该电子闸机发送开启指令(比如该开启指令可以为专用指令,或者上述的扣款成功消息等),使得该电子闸机切换至开启状态,以便于用户C1顺利通过。

[0132] 综上所述,基于本申请的技术方案,可以在用户无需操控用户设备的情况下,由收银台设备准确获知该用户的用户账号,并高效、准确地实现相应的付款操作,有助于提高交易效率和安全性,以及提升用户体验。

[0133] 图8示出了根据本申请的一示例性实施例的一种基于交互端侧的电子设备的示意结构图。请参考图8,在硬件层面,该电子设备包括处理器802、内部总线804、网络接口806、内存808以及非易失性存储器810,当然还可能包括其他业务所需要的硬件。处理器802从非易失性存储器810中读取对应的计算机程序到内存808中然后运行,在逻辑层面上形成基于交互端侧的身份认证装置。当然,除了软件实现方式之外,本申请并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限定于各个逻辑单元,也可以是硬件或逻辑器件。

[0134] 请参考图9,在软件实施方式中,该身份认证装置可以包括:

[0135] 接收单元901,使交互端接收到针对用户发起的交互指令;

[0136] 获取单元902,使所述交互端根据所述交互指令,获取所述用户的身份信息;

[0137] 发送单元903,使所述交互端向服务端发送身份识别请求,所述身份识别请求中包含所述身份信息,所述身份识别请求用于指示所述服务端将所述身份信息与所述交互端对应候选用户的标准身份信息进行匹配,以确定出所述用户对应的用户账号,所述用户账号用于响应所述交互指令对应的交互操作;其中,所述交互端附近的用户被所述服务端标记为相应的候选用户。

[0138] 可选的,还包括:

[0139] 实施数904,当确定出所述用户对应的用户账号时,使所述交互端响应于所述交互指令,针对确定出的用户账号实施交互操作。

[0140] 可选的,还包括:

[0141] 发射单元905,使所述交互端向外发射近场消息,所述近场消息中包含所述交互端的交互端标识信息;

[0142] 其中,当所述近场消息被所述用户对应的用户客户端接收到时,所述近场消息用于指示所述用户客户端:将所述交互端标识信息、所述用户的用户标识信息和所述近场消息的信号强度发送至所述服务端,以由所述服务端在所述信号强度大于预设强度的情况下将所述用户标记为所述交互端对应的候选用户。

[0143] 可选的,所述候选用户包括在预设时长内位于所述交互端附近的用户。

[0144] 可选的,所述身份信息包括生物特征信息、所述标准身份信息包括标准生物特征信息。

[0145] 可选的,所述生物特征信息、所述标准生物特征信息包括以下至少之一:

[0146] 人脸信息、指纹信息、掌纹信息、眼纹信息、虹膜信息、步态信息。

[0147] 图10示出了根据本申请的一示例性实施例的一种基于服务端侧的电子设备的示意结构图。请参考图10,在硬件层面,该电子设备包括处理器1002、内部总线1004、网络接口

1006、内存1008以及非易失性存储器1010，当然还可能包括其他业务所需要的硬件。处理器1002从非易失性存储器1010中读取对应的计算机程序到内存1008中然后运行，在逻辑层面上形成基于服务端侧的身份认证装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限于各个逻辑单元，也可以是硬件或逻辑器件。

[0148] 请参考图11，在软件实施方式中，该身份认证装置可以包括：
[0149] 接收单元1101，使服务端接收到交互端发送的身份识别请求，所述身份识别请求中包含用户的身份信息，所述身份信息由所述交互端根据针对所述用户发起的交互指令向所述用户获取得到；

[0150] 匹配单元1102，使所述服务端将所述身份信息与所述交互端对应候选用户的标准身份信息进行匹配；其中，所述交互端附近的用户被所述服务端标记为相应的候选用户；
[0151] 确定单元1103，当所述身份信息匹配于所述候选用户对应的标准身份信息时，使所述服务端确定所述候选用户对应的用户账号，所述用户账号用于响应所述交互指令对应的交互操作。

[0152] 可选的，还包括：

[0153] 告知单元1104，使所述服务端将所述用户账号告知所述交互端，以由所述交互端响应于所述交互指令，针对所述用户账号实施交互操作。

[0154] 可选的，还包括：

[0155] 调取单元1105，使所述服务端调取数据库，所述数据库中记录有所述用户对应的用户客户端上传的交互端标识信息、用户标识信息和信号强度；其中，所述用户客户端在接收到所述交互端向外发射的近场消息时，将所述用户的用户标识信息以及所述近场消息中包含的所述交互端的交互端标识信息、所述近场消息的信号强度上传至所述服务端，以供所述服务端记录至所述数据库；

[0156] 标记单元1106，使所述服务端接收所述用户上传的交互端标识信息、用户标识信息和信号强度，并在所述信号强度大于预设强度的情况下，将所述用户标记为所述交互端对应的候选用户。

[0157] 可选的，所述候选用户包括在预设时长内位于所述交互端附近的用户。

[0158] 可选的，所述匹配单元1102具体用于：

[0159] 使所述服务端分别将所述身份信息与各个候选用户对应的标准身份信息进行匹配，并分别得到相应的相似度；

[0160] 其中，当最高相似度大于预设相似度阈值、且所述最高相似度与次高相似度之间的差值大于预设混淆差值时，所述最高相似度对应的候选用户被确定为匹配于所述用户。

[0161] 图12示出了根据本申请的一示例性实施例的一种基于用户客户端侧的电子设备的示意结构图。请参考图12，在硬件层面，该电子设备包括处理器1202、内部总线1204、网络接口1206、内存1208以及非易失性存储器1210，当然还可能包括其他业务所需要的硬件。处理器1202从非易失性存储器1210中读取对应的计算机程序到内存1208中然后运行，在逻辑层面上形成基于用户客户端侧的身份认证装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限于各个逻辑单元，也可以是硬件或逻辑器件。

- [0162] 请参考图13,在软件实施方式中,该身份认证装置可以包括:
- [0163] 接收单元1301,使用户客户端接收到交互端发射的近场消息,所述近场消息中包含所述交互端的交互端标识信息;
- [0164] 发送单元1302,使所述用户客户端将所述交互端标识信息、所述用户客户端的已登录用户的用户标识信息和所述近场消息的信号强度发送至服务端,以由所述服务端在所述信号强度大于预设强度的情况下将所述已登录用户标记为所述交互端对应的候选用户;
- [0165] 其中,当所述交互端获取针对所述已登录用户的交互指令时,所述已登录用户的身份信息被所述交互端获取并发送至所述服务端,以由所述服务端将所述身份信息与所述候选用户对应的标准身份信息进行匹配、确定出所述已登录用户对应的用户账号,所述用户账号用于响应所述交互指令对应的交互操作。
- [0166] 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。
- [0167] 在一个典型的配置中,计算机包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。
- [0168] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。
- [0169] 例如,本申请提出了一种计算机可读介质,其上存储有计算机指令,该指令被处理器执行时实现上述基于交互端侧的身份认证方法。
- [0170] 例如,本申请提出了另一种计算机可读介质,其上存储有计算机指令,该指令被处理器执行时实现上述基于服务端侧的身份认证方法。
- [0171] 例如,本申请提出了又一种计算机可读介质,其上存储有计算机指令,该指令被处理器执行时实现上述基于用户客户端侧的身份认证方法。
- [0172] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。
- [0173] 还需要说明的是,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、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0174] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0175] 在本申请使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0176] 应当理解,尽管在本申请可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本申请范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0177] 以上所述仅为本申请的较佳实施例而已,并不用以限制本申请,凡在本申请的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本申请保护的范围之内。

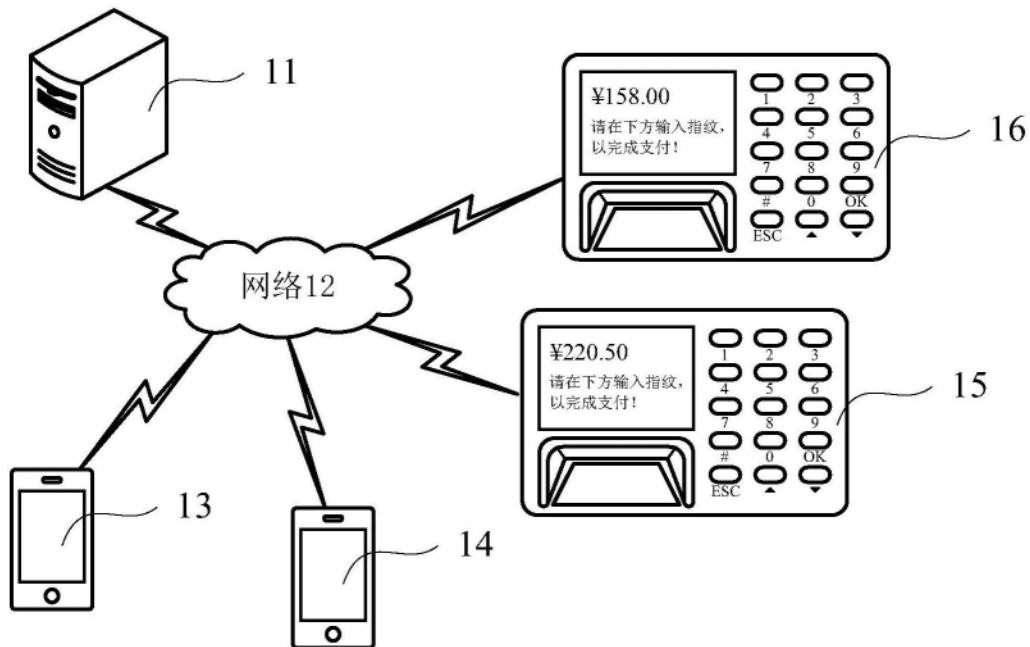


图1

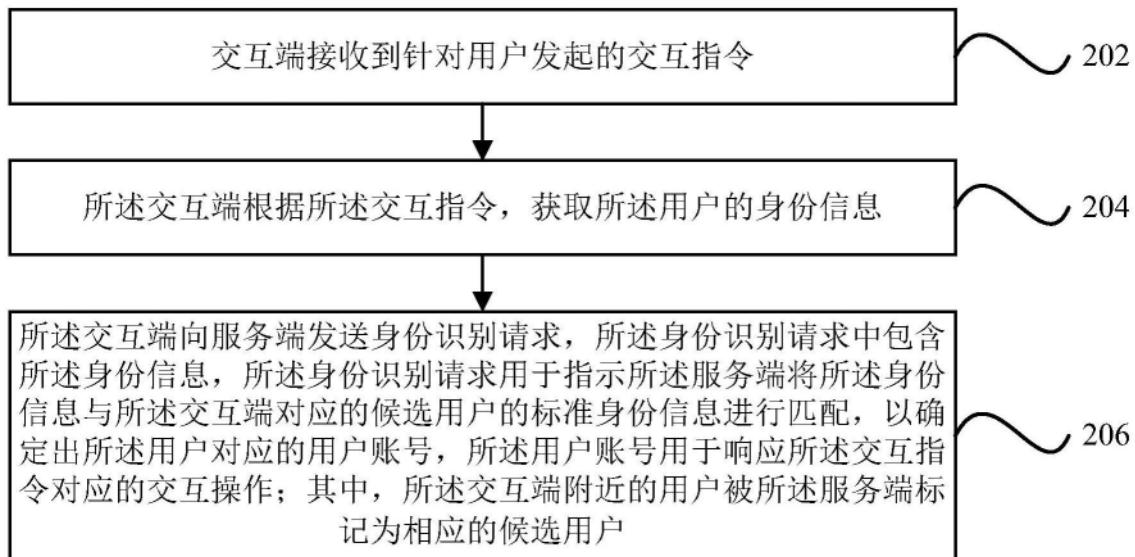


图2

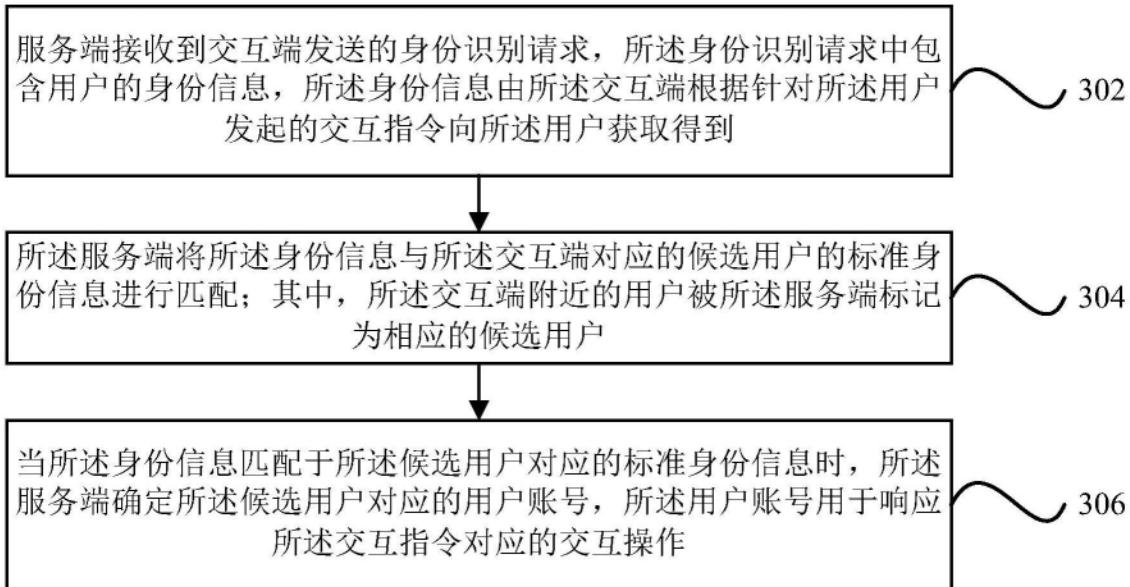


图3

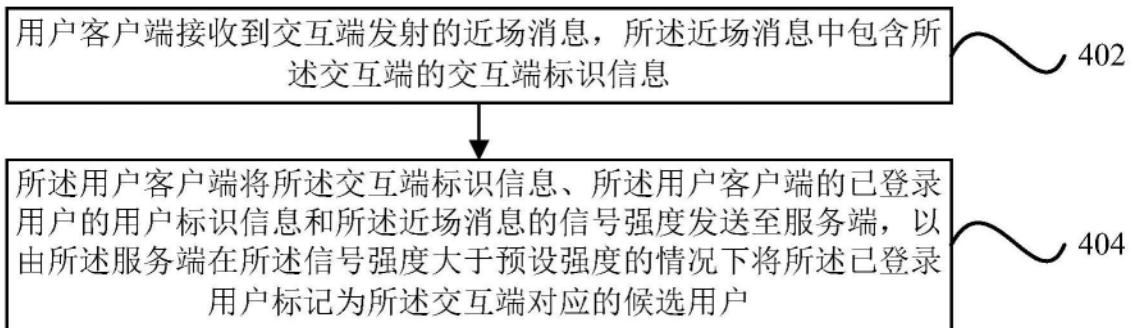


图4

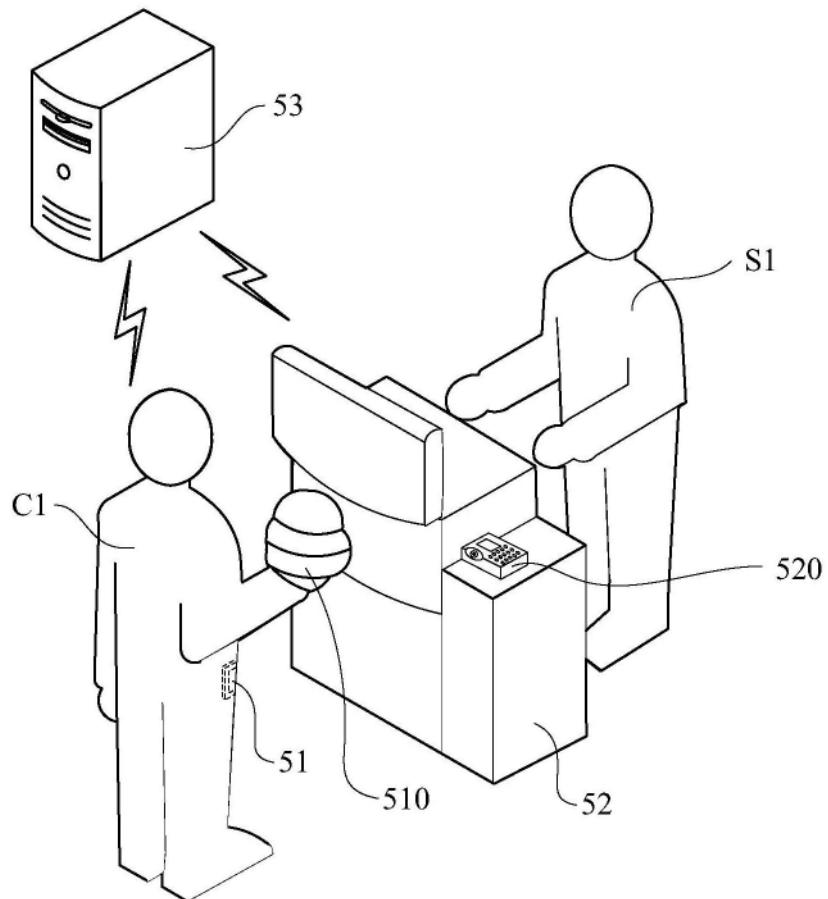


图5

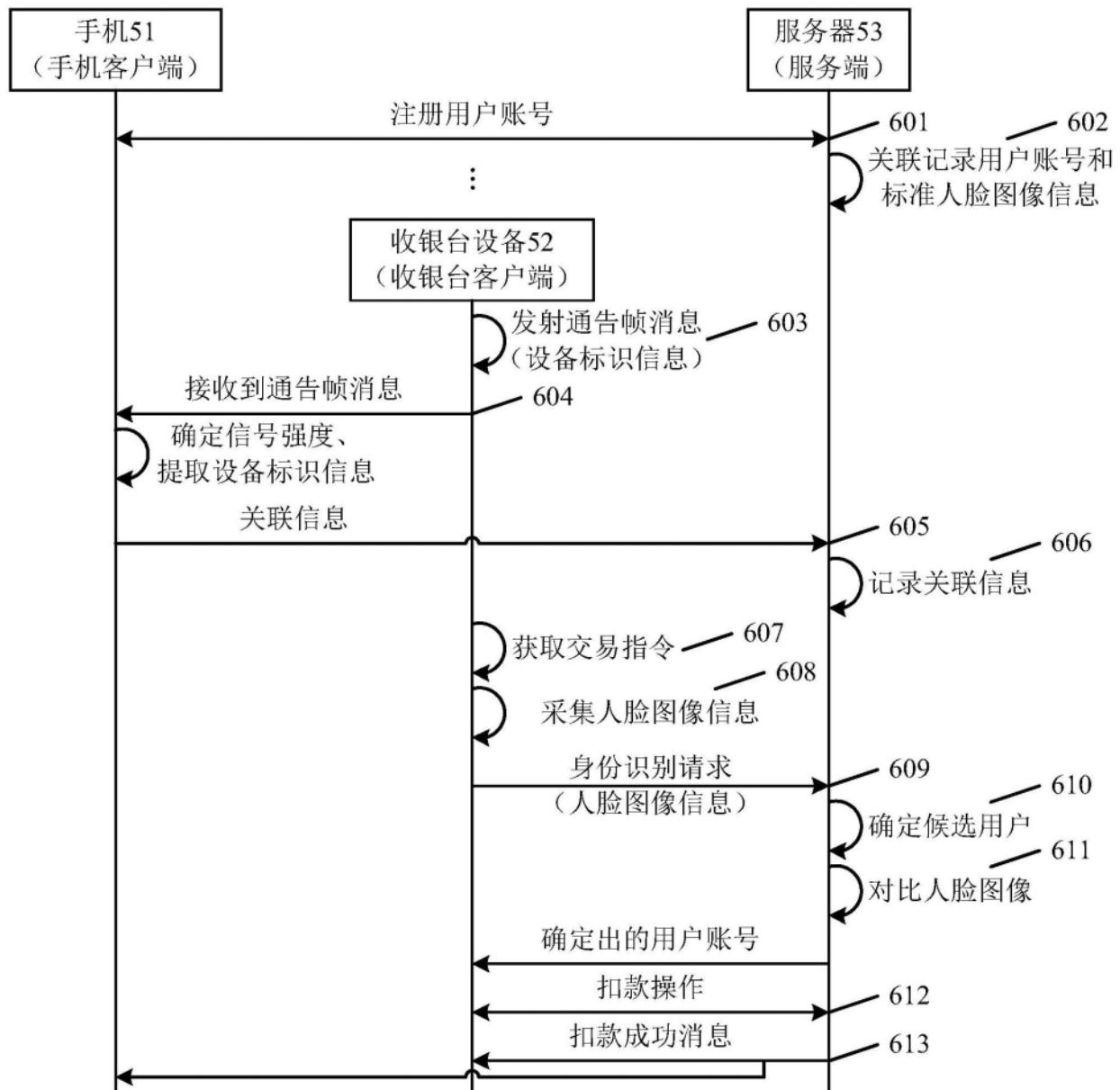


图6

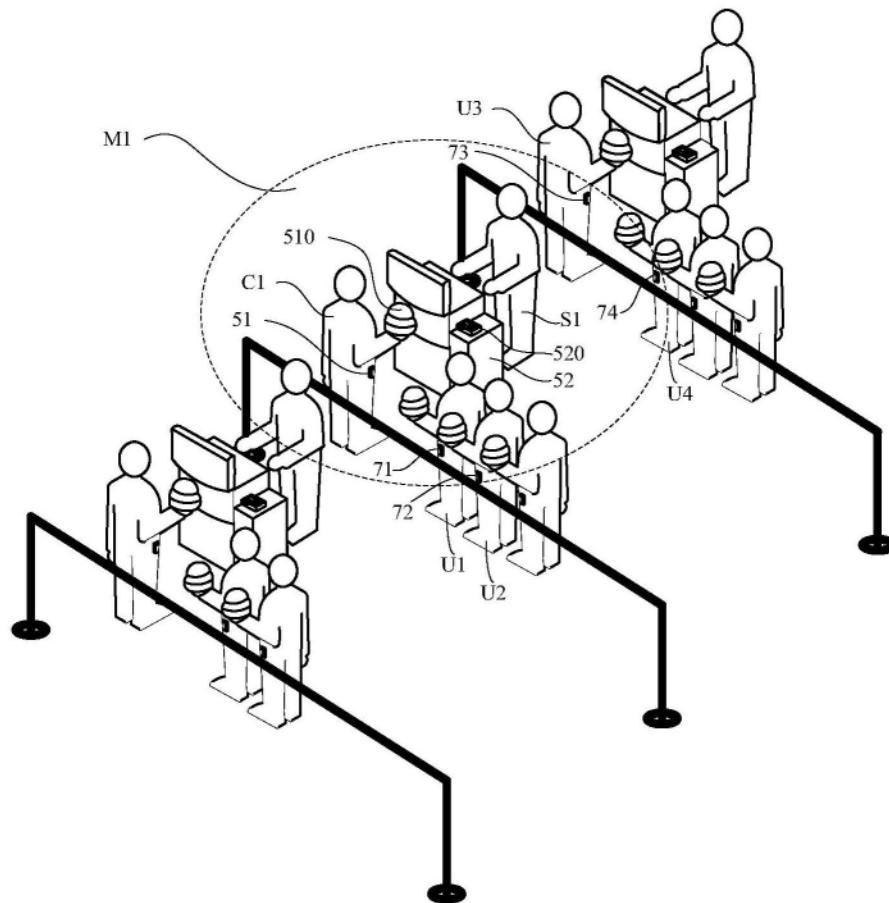


图7

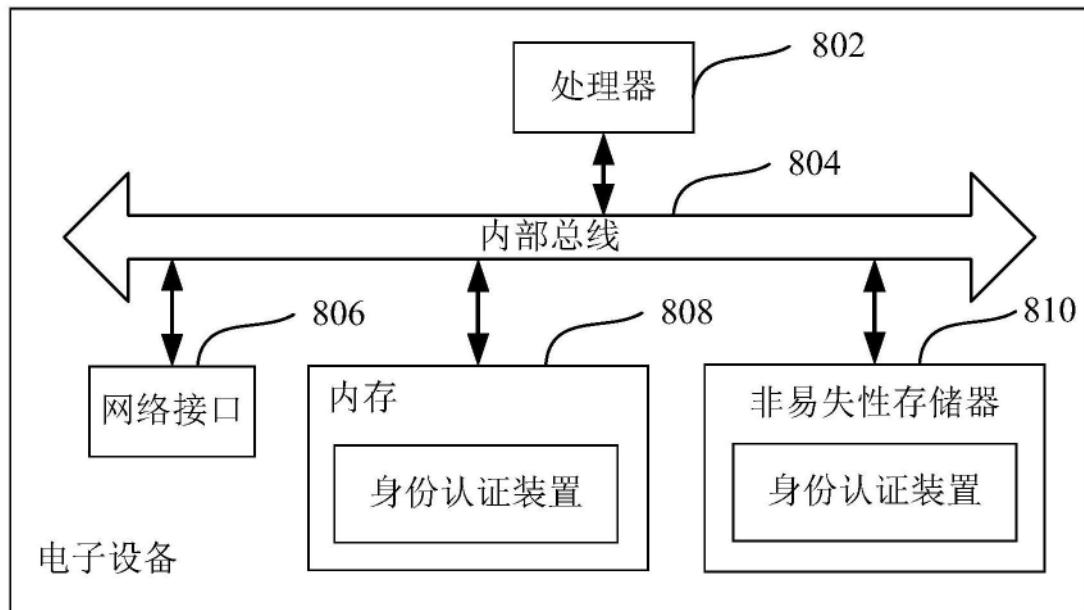


图8

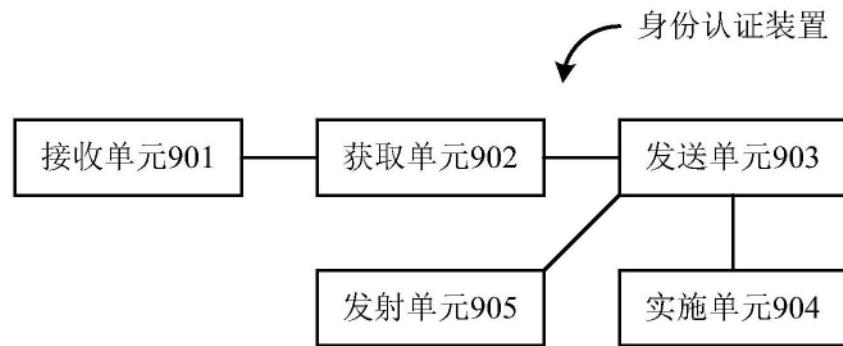


图9

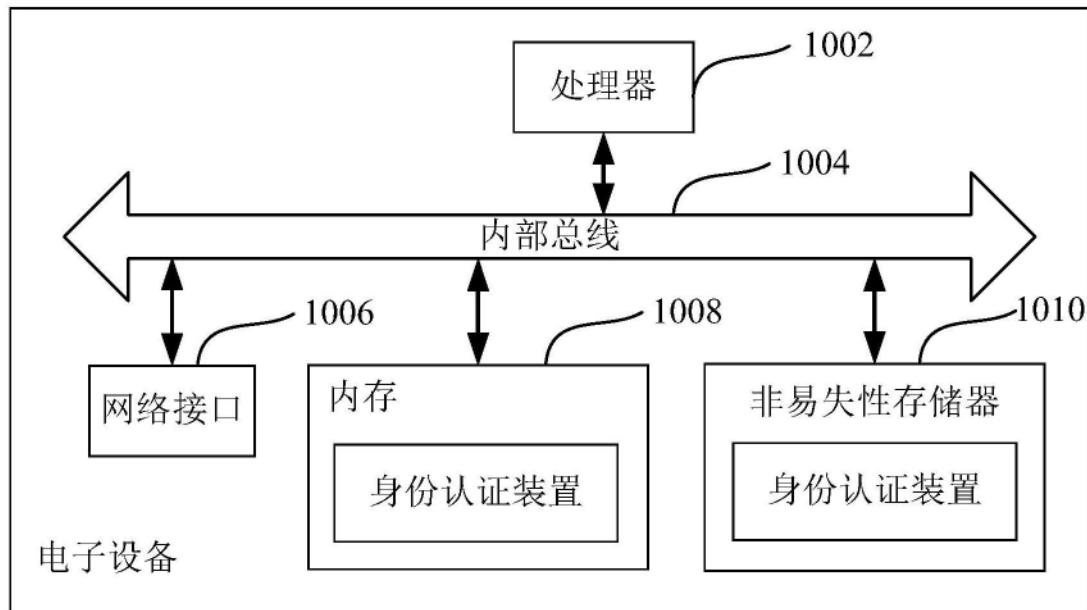


图10

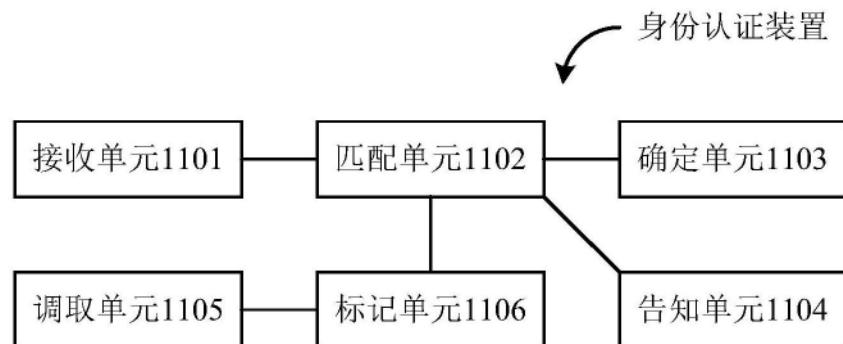


图11

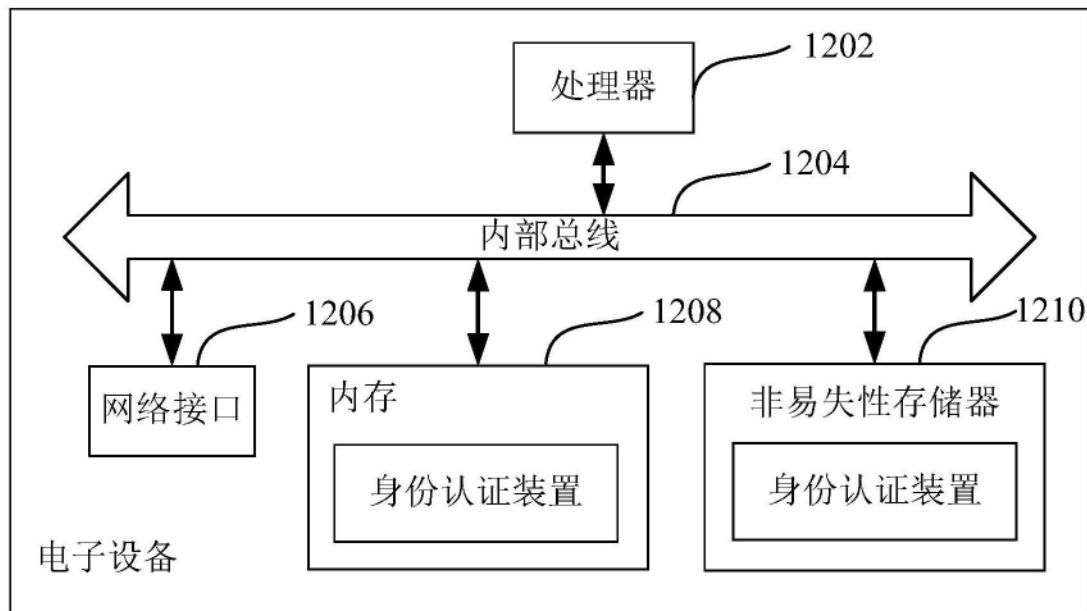


图12

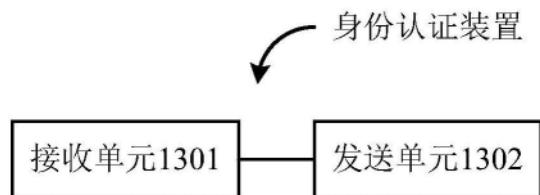


图13