(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 106548525 A
(43)申请公布日 2017.03.29

(21)申请号 201610409350.2

(22)申请日 2016.06.12

(30)优先权数据
15109081.4 2015.09.16 HK

(71)申请人 英基科技有限公司
地址 中国香港皇后大道东43-59号东美中心2403室

(72)发明人 胡宏基

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 李红爽 栗若木

(51)Int.Cl.
G07C 1/10(2006.01)
H04M 1/725(2006.01)
G06Q 10/10(2012.01)

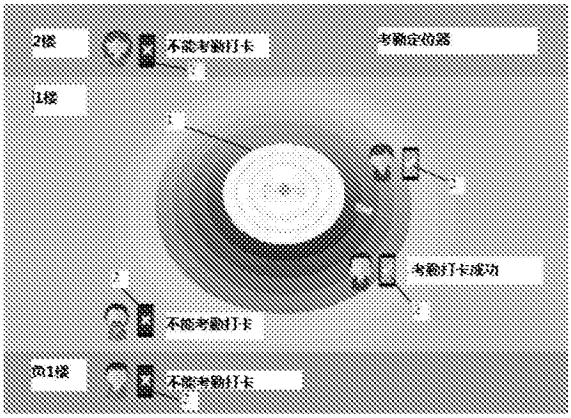
权利要求书3页 说明书4页 附图4页

(54)发明名称

一种打卡系统

(57)摘要

本发明提供一种打卡系统，所述打卡系统包括云端数据库、考勤定位器、和安装有移动应用程式的智能手机，其中，所述云端数据库、所述考勤定位器、和所述智能手机彼此之间进行数据通信，所述考勤定位器以特定的GPS进行登记，并配备蓝牙智能技术；当考勤打卡时，所述移动应用程式可以检测雇员是否在所述考勤定位器5米范围之内；所述移动应用程式使用面部识别，以防他人代打卡。



CN 106548525 A

1.一种打卡系统，其特征在于，所述打卡系统包括云端数据库、考勤定位器、和安装有移动应用程式的智能手机，其中，所述云端数据库、所述考勤定位器、和所述智能手机之间彼此进行数据通信，所述考勤定位器以特定的GPS进行登记，并配备蓝牙智能技术；当考勤打卡时，所述移动应用程式检测雇员是否在所述考勤定位器所在位置的5米范围之内；所述移动应用程式使用面部识别，以防他人代打卡。

2.如权利要求1所述的打卡系统，其特征在于，所述面部识别通过：注册一个雇员的人脸，将所述智能手机中雇员的信息和所述云端数据库中的雇员信息进行匹配，日常考勤打卡，和替换所述雇员的人脸来实现。

3.如权利要2所述的打卡系统，其特征在于，所述注册雇员的人脸包括输入电子邮件地址、密码和人脸识别、验证所述电子邮件地址和所述密码，将所述电子邮件地址、所述密码存入CGG云数据库，将服务器中的人脸下载到所述智能手机中，将加密后的所述人脸和所述电子邮件地址存入所述智能手机和MySQL。

4.如权利要求3所述的打卡系统，其特征在于，一个所述电子邮件地址对应一个用户，所述密码至少为8位长度，同时包括字符和数字。

5.如权利要求2所述的打卡系统，其特征在于，将所述智能手机中雇员的信息和所述云端数据库中的雇员信息进行匹配是通过：雇员输入雇主ID从而添加雇主信息，检查雇主ID是否与所述MySQL的信息匹配，及是否有匹配的电子邮件地址存在，再由雇员确认。

6.如权利要求2所述的打卡系统，其特征在于，所述日常考勤打卡包括人脸验证。

7.如权利要求2所述的打卡系统，其特征在于，所述更换人脸用于防止他人代打卡，所述更换人脸包括：显示当前人脸，将加密的新人脸和电子邮件地址存入所述智能手机和所述CGG云数据库中的所述MySQL，并发送提醒至雇主。

8.如权利要求2所述的打卡系统，其特征在于，所述移动应用程式包括用于断网情况下打卡的算法；手机号码和GPS都标记在考勤打卡记录中。

9.如权利要求2所述的打卡系统，其特征在于，所述考勤定位器使用反欺骗算法，防止改变所述考勤定位器的设定及从所述考勤定位器发出来的信息。

10.一种打卡系统，其特征在于，所述打卡系统包括：云端数据库、考勤定位器、和安装有移动应用程式的智能手机；

其中，所述云端数据库、所述考勤定位器、和所述智能手机之间彼此进行数据通信，所述考勤定位器以特定的GPS进行登记，并配备蓝牙智能技术；当考勤打卡时，所述移动应用程式可以检测雇员是否在所述考勤定位器5米范围之内；所述移动应用程式启动人脸识别，以防他人代打卡；所述人脸识别通过注册一个雇员的人脸、将所述智能手机中雇员的信息和所述云端数据库中的雇员信息进行匹配、日常考勤打卡、和更换雇员的人脸来实现；

所述注册雇员的人脸包括：

输入电子邮件地址、密码和人脸识别，其中，一个所述电子邮件地址对应一个用户，所述密码至少包括8位长度的字符和数字；

验证所述电子邮件地址和所述密码，

将所述电子邮件地址和所述密码存入CGG云数据库，

将服务器中的人脸下载到所述智能手机中，和

将加密后的所述人脸和所述电子邮件地址存入所述智能手机和MySQL；

将所述智能手机中雇员的信息和云端数据库中的雇员信息进行匹配包括：

雇员增加雇主信息，其中，输入所述雇主ID，

检查所述雇主ID是否与MySQL的信息匹配，是否与存在的电子邮件地址匹配，然后由雇员确认；

所述日常考勤打卡包括：人脸验证；

所述更换人脸用于防止他人代打卡，并且包括：

显示当前的人脸，

将加密的新的人脸和电子邮件地址一起存入所述智能手机和所述CGG云数据库中的所述MySQL，和

向雇主发送提醒；

所述移动应用程式包括用于断网情况下的考勤打卡算法；

手机号码和GPS标记在打卡记录中；

所述考勤定位器通过反欺骗算法，防止改变所述考勤定位器的设定及从所述考勤定位器发送出来的信息。

11.一种打卡系统，其特征在于，所述打卡系统包括云端数据库、考勤定位器、和安装有移动应用程式的智能手机；

其中，所述云端数据库、所述考勤定位器、所述智能手机之间彼此进行数据通信，所述考勤定位器以特定的GPS进行登记，并配备蓝牙智能技术；当打卡时，所述移动应用程式检测雇员是否在所述考勤定位器5米范围之内；所述移动应用程式启动人脸识别，以防他人代打卡；所述人脸识别通过注册一个雇员的人脸，将所述智能手机中的雇员信息和所述云端数据库中的雇员信息进行匹配，日常考勤打卡、和替换雇员的人脸来实现；

所述注册雇员的人脸包括：

输入电子邮件地址、密码和人脸识别，其中，一个所述电子邮件地址对应一个用户，所述密码至少包括8位长度的字符和数字；

验证所述电子邮件地址和所述密码，

将所述电子邮件地址和所述密码存入CGG云数据库，

将服务器中的人脸下载到所述智能手机中，和

将加密后的所述人脸和所述电子邮件地址存入所述智能手机和MySQL；

所述将智能手机中的雇员的信息和云端数据库中的雇员信息进行匹配是通过：雇员增加雇主信息，其中，输入所述雇主ID，检查雇主ID是否与MySQL的信息匹配，及是否存在匹配的电子邮件地址，然后由所述雇员确认；

所述日常考勤打卡包括：人脸验证；

所述更换人脸用于防止他人代打卡，并且包括：

显示当前人脸，

将加密的新的人脸和电子邮件地址一并存入所述智能手机和所述CGG云数据库中的所述MySQL，和

向雇主发送提醒；

所述移动应用程式包括用于断网情况下的考勤打卡算法；

手机号码和GPS标记在打卡记录中；

所述考勤定位器通过反欺骗算法，防止改变所述考勤定位器的设定及从所述考勤定位器发送出来的信息；

所述考勤定位器支持1Mbps传输8位组到27位组的数据包，使用先进的低功耗监听模式来实现超低占空比；

所述考勤定位器使用所有蓝牙规范版本通用的自适应跳频技术，最小化来自其他2.4GHz ISM频段无线技术的干扰，和增加链路预算和范围；

所述考勤定位器在所述控制器中放置大量智能信息，让主机长时间休眠，只有当所述主机需要执行动作时，所述控制器才会唤醒所述主机；

所述考勤定位器支持在3毫秒内完成连接设置并开始传输数据，允许所述移动应用程式建立连接，然后在快速中断所述连接之前，在几毫秒内完成短时突发通信，传输已认证数据；

所述考勤定位器对所有数据包使用24bit CRC校验，确保最大程度抵御干扰；

所述考勤定位器对所述数据包使用AES-128加密算法以加强所述数据包的加密和认证；

所述考勤定位器对每个从属设备的每个数据包使用32位接入地址，可连接数十亿设备；

所述考勤定位器包括连接模式和非连接模式；

所述考勤定位器通过小型的纽扣电池提供电能。

一种打卡系统

技术领域

[0001] 本发明涉及打卡系统，尤其涉及包括具备蓝牙智能技术的考勤定位器的打卡系统。

背景技术

[0002] 在现有技术中，传统的打卡系统存在以下方面的限制：1.安装费用高：拉线、安装相应的终端/服务器等花费较高；2.高管理成本：需要在每一个考勤打卡机器中注册(对于多点办公的行业而言)；3.逐一排队打卡：每次只容许一个雇员在一台打卡机上打卡。

[0003] 一些企业尝试着通过手机APP打卡来解决以上问题，但是遇到了新的问题：无法阻止虚假的GPS、他人代打卡。

[0004] 因此，为解决以上问题，急需提供一种低成本、高效率的考勤打卡系统。

发明内容

[0005] 根据本发明的一个实施例，本发明提供的考勤打卡系统包括云端数据库、考勤定位器、安装有移动应用程式的智能手机，其中，所述云端数据库、所述考勤定位器、所述智能手机之间彼此进行数据通信，所述考勤定位器以特定的GPS进行登记，并配备蓝牙智能技术；当考勤打卡时，所述移动应用程式检测雇员是否在所述考勤定位器的5米范围之内；所述移动应用程式使用面部识别，以防他人代打卡。

[0006] 根据本发明的另一实施例，本发明提供的所述打卡系统包括云端数据库、考勤定位器、安装有移动应用程式的智能手机，其中，所述云端数据库、所述考勤定位器、所述智能手机之间彼此进行数据通信，所述考勤定位器以特定的GPS进行登记，并配备蓝牙智能技术；当考勤打卡时，所述移动应用程式检测雇员是否在所述考勤定位器的5米范围之内；所述移动应用程式启动面部识别，以防他人代打卡；所述面部识别通过：注册一个雇员的人脸，将所述智能手机中的雇员信息和所述云端数据库中的雇员信息进行匹配，日常考勤打卡，和替换所述雇员的人脸来实现。所述注册雇员的人脸包括输入电子邮件地址、密码、人脸识别、认证所述电子邮件地址和所述密码，将所述电子邮件地址、所述密码存入CGG云数据库，将服务器中的人脸下载到所述智能手机中，将加密后的所述人脸和所述电子邮件地址存入所述智能手机和MySQL；一个所述电子邮件地址对应一个用户，所述密码至少为8位长度，并且同时包括字符和数字。将所述智能手机中的雇员信息和所述云端数据库中的雇员信息进行匹配的过程包括：雇员增加雇主信息，其中，输入所述雇主ID，检查所述雇主ID是否与MySQL中的信息匹配，是否与存在的电子邮件地址匹配，然后由雇员确认；所述日常考勤打卡包括：人脸验证；所述更换人脸用于防止他人代打卡，并且包括：显示当前的人脸，将加密的新的人脸和电子邮件地址一起存入所述智能手机和所述CGG云数据库中的所述MySQL，和向雇主发送提醒；所述移动应用程式包括用于断网情况下的考勤打卡算法；手机号码和GPS标记在打卡记录中；

[0007] 所述考勤定位器通过反欺骗算法防止改变所述考勤定位器的设定及所述考勤定

位器发送出来的信息。

[0008] 本发明提供的打卡系统允许雇主让许多雇员在同一时间进行考勤打卡动作，通过面部识别和无线感测能有效防止虚假GPS和他人代打卡的问题，无线感测能确保雇员在考勤定位器5米范围内(即雇主要求雇员打卡的指定位置)打卡，提到的5米范围，可以人工进行设置，可以设置1米到30米之间的范围。

[0009] 本发明其他的优点和特征将结合附图进行详细说明。

附图说明

[0010] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明，其中，

[0011] 图1所示为本发明一实施例：打卡系统的应用环境图。

[0012] 图2所示为本发明一实施例：雇员登记面部识别的流程图。

[0013] 图3所示为本发明一实施例：增加雇主的流程图。

[0014] 图4所示为本发明一实施例：考勤打卡进行面部识别的流程图。

[0015] 图5所示为本发明一实施例：更换人脸的流程图。

[0016] 应当理解的是，附图并不是依比例制定的，实施例有时只作概略或局部说明。在一些实施例中，对于理解本发明的非必须具体细节或者致使其他细节难以准确理解的具体细节可能会省略。要留意的是，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

具体实施方式

[0017] 作为一种革新设计，蓝牙智能技术仅仅消耗经典蓝牙无线很小部分的电能。蓝牙智能将蓝牙无线技术扩展到通过微小纽扣电池提供电能的设备，例如手表和玩具。其他，例如运动健身、健康护理、键盘、鼠标、信号灯、可穿戴式娱乐等设备，通过蓝牙智能也得以提升功能。在许多情况下，得益于蓝牙智能，这些设备可以操作超过一年以上才换电池。

[0018] 与早前的说明一样，无线电的范围可以根据应用被优化。市场上大部分的蓝牙设备包括基础30英尺、10米的范围，即经典蓝牙无线电范围，但是，蓝牙规格没有对此作出限制。蓝牙智能技术中，人工设置可以选择优化范围到200英尺或超过200英尺。特别是对于室内感测应用，远范围是必须的。

[0019] 蓝牙智能产品的特点如下：无论从峰值、平均值或闲置模式来看，其耗电量都是极低的；能够在标准纽扣电电池上运行数年之久；低实施成本；多供应商互通性；增强的无线电范围。

[0020] 蓝牙核心规格的优化可透过两个模式实现：双模式和单模式。在双模式中，蓝牙低能量功能是整合在已经存在的经典蓝牙控制器中。这种架构能共享经典蓝牙技术已经存在的无线电和功能，因此，与经典蓝牙技术相比只需要增加很少的成本费用。另外，现有的制造商能在现有的经典蓝牙技术的芯片(例如Bluetooth v2.1+EDR或Bluetooth v3.0+HS的芯片)中使用新的低能量栈，促进了经典蓝牙技术的发展，使得设备具有新的功能。

[0021] 单模式芯片令高度集成及精巧的设备得以出现，单模式芯片具备一个轻量级的连接层，轻量级的连接层可提供低功耗闲置模式操作、简易的设备搜寻，在最低成本下，透过

先进的低功耗和安全加密功能达到可靠的点对多点数据传输。控制器中的连接层可以让已连接互联网的传感器在蓝牙传输时使用蓝牙低功耗资讯流。

[0022] 数据传输:蓝牙智能(低耗能)支持1Mbps传输的8位组到27位组的数据包,使用先进的低功耗监听模式来实现超低占空比。

[0023] 调频:蓝牙智能(低功耗)使用所有蓝牙规范版本通用的自适应跳频技术,最小化来自其他2.4GHz ISM频段无线技术的干扰,增加链路预算和范围。

[0024] 主机控制:蓝牙智能(低功耗)在所述控制器中放置大量智能信息,让主机可以长时间休眠,只有当所述主机需要执行动作时,所述控制器才会唤醒所述主机,由于所述主机比所述控制器更耗电,这样能更大程度地节省电流。

[0025] 通信延迟:蓝牙智能(低功耗)可在3毫秒内完成连接设置并开始传输数据,允许与移动应用程式建立连接,然后在快速拆除所述连接之前,在几毫秒内完成短时突发通信,传输已认证数据。

[0026] 范围:增强的调变指数让蓝牙智能(低功耗)提供的最大范围可超过100米。

[0027] 稳健性:所有数据包都使用24bit CRC校验,最大限度抵御干扰。强安全性:使用AES-128加密算法进行数据加密和认证。

[0028] 拓扑结构:蓝牙智能(低功耗)每个数据包的每个接收都使用32位接入地址,理论上可连接数十亿设备,蓝牙技术的优化可达至在一对一连接的同时,也可透过星型结构支持一对多连接。

[0029] 请参阅附图,具体请参阅图1,图1所示为本发明实施例一种打卡系统的示意图,包括云端数据库,(该云端数据库没有在图1中示出),考勤定位器1、和安装有移动应用程式的智能手机2,要留意的是,允许同时进行考勤打卡的智能手机2的数量可根据实际应用作出更改。其中,所述云端数据库、所述考勤定位器1、所述智能手机2彼此之间进行数据通信以实现考勤打卡过程。所述考勤定位器可向特定GPS(Global Position System)登记,并配备蓝牙智能技术。

[0030] 所述考勤定位器1使用反电子欺骗算法,使得考勤定位器1与使用UUID传统的蓝牙设备区别开来。在这种情况下,非授权的用户不能更改考勤定位器的设定及从考勤定位器发送出来的信息。也就是说,增加了以下3个专有的“服务”权利:在非连接模式,不会对“服务”进行广播;在连接模式,即使在没有应用程序接口的情况下,仍会对“服务”进行广播;在连接模式下,“服务”的数据只能由考勤定位器制造商的专有UUID的所有者进行修改。

[0031] 在一实施例中,当考勤打卡时,所述移动应用程式能检测雇员是否在考勤定位器1的5米范围之内,移动应用程式使用面部识别来防止他人代打卡,所述面部识别通过:注册一个雇员的人脸,将所述智能手机中雇员的信息和所述云端数据库中的雇员信息进行匹配,日常考勤打卡、和替换雇员的人脸来实现。

[0032] 请参阅附图,具体地参阅图2,图2所示是本发明注册雇员的人脸的流程图,注册雇员的人脸的过程包括:输入电子邮件地址,密码和面部识别,其中,一个电子邮件地址对应一个用户,密码至少包括8位长度的字符和数字,验证电子邮件地址和密码,存储电子邮件地址和密码到CGG云数据库中,从服务器中下载人脸到智能手机中和MySQL中。详细来说,在步骤201中,雇员使用智能手机1进行登录。在步骤202中,系统检查雇员是否已经注册。如果雇员已经注册,在步骤203中,系统检查密码是否正确。如果雇员没有注册,在步骤204中,雇

员需要执行注册程序，即：输入电子邮件地址，密码、以及进行面部识别过程。然后，在步骤205中，对输入的数据进行验证，即检查输入的电子邮件地址是否已被他人使用，密码的强度是否足够。在通过验证后，将输入数据存入CGG云数据库。在步骤207中，从服务器中下载人脸到手机中。同时，在步骤208中，存储加密的人脸和电子邮件地址到智能手机和云端数据库中的MySQL中。在步骤209中，引导雇员进入欢迎登录的界面。

[0033] 参阅附图，具体地参阅图3，将智能手机的雇员信息与云端数据库的雇员信息进行匹配是透过输入雇主ID来添加雇主，检查该雇主ID是否与MySQL的信息匹配及是否存在匹配的电子邮件地址，最后由雇员进行确认。在步骤301中，输入雇主ID，在步骤302中，系统检查雇主ID是否与MySQL的信息匹配。如果没有找到匹配的雇主ID，系统会返回步骤301，提示用户输入的雇主ID无效。如果找到匹配的雇主ID，在步骤303a中，系统会进一步检查在相应雇主的雇员档案纪录中是否有匹配的电子邮件地址。如果在相应雇主的雇员档案纪录中未能找到匹配的电子邮件地址，系统进入步骤303b。在步骤303b中，检查在相应雇主的雇员档案纪录中是否有匹配的手机号码。如果能在相应雇主的雇员档案纪录中找到匹配的电子邮件地址或手机号码(在步骤303a或者303b)，在步骤305中，雇员会被要求对相关资料进行确认，例如，“你是<姓名>-<职位>属于<雇主姓名>吗?”。在步骤306中，检查雇员是否已确认在步骤305中显示的相关信息。如果未能在相应雇主的雇员档案纪录中找到匹配的电子邮件地址或手机号码(在步骤303a或者303b)，在步骤307中，系统显示“你现在可以考勤打卡，但是请提醒雇主在工资结算之前匹配你的记录到雇员个人档案中”。

[0034] 参阅附图，具体地参阅图4，日常考勤打卡包括人脸验证。详细来说，在步骤401中，系统会检测人脸，也就是说，截取目前用户的面部数据。在步骤402中，系统检查人脸是否匹配，即把目前截取到的面部资料与雇员注册人脸或更换的人脸后储存的相应资料(参与图2及图5)进行匹配。如果资料匹配，就可以去到步骤403中，进行日常考勤打卡。如果资料不匹配，在步骤404中，系统将提示雇员选择更换登录账号、更换人脸、或者退出考勤打卡过程。

[0035] 参阅附图，具体地参阅图5，更换人脸用于防止他人代打卡，但是允许雇员根据自身的考虑更换自身的面部数据，具体包括：显示目前的人脸，存储加密新人脸和电子邮件地址到智能手机和CGG云数据库的MySQL中，并且发送提醒给雇主。详细来说，在步骤501中，显示当前人脸。然后系统显示询问信息，询问你是否确认更换人脸(雇员更换人脸的消息将会通知给雇主)。然后，在步骤502，系统询问是否继续进入下一步。如果雇员选择进入下一步，在步骤503中存储加密的人脸和电子邮件地址到手机和MySQL中，同时，在步骤504中，发送提醒消息给雇主，最后，在步骤505中，在CGG数据库中删除旧的人脸，并存储新的人脸。

[0036] 另外，特殊算法用于在没有可行网络下进行考勤打卡，但是，打卡过程仍然通过考勤定位器和面部识别进行保护(2重保护)，其次，手机号码和GPS(取决于雇员使用的智能手机)即使在没有网络时也将标记在所述打卡记录中，供雇主进一步的参考。

[0037] 以上实施例仅用于说明本发明，而非对本发明的限制，有关技术领域的技术人员，在不脱离发明的精神和范围的情况下，还可以做出各种变化和变形，因此所有等同的技术方案也属于本发明的保护范畴。

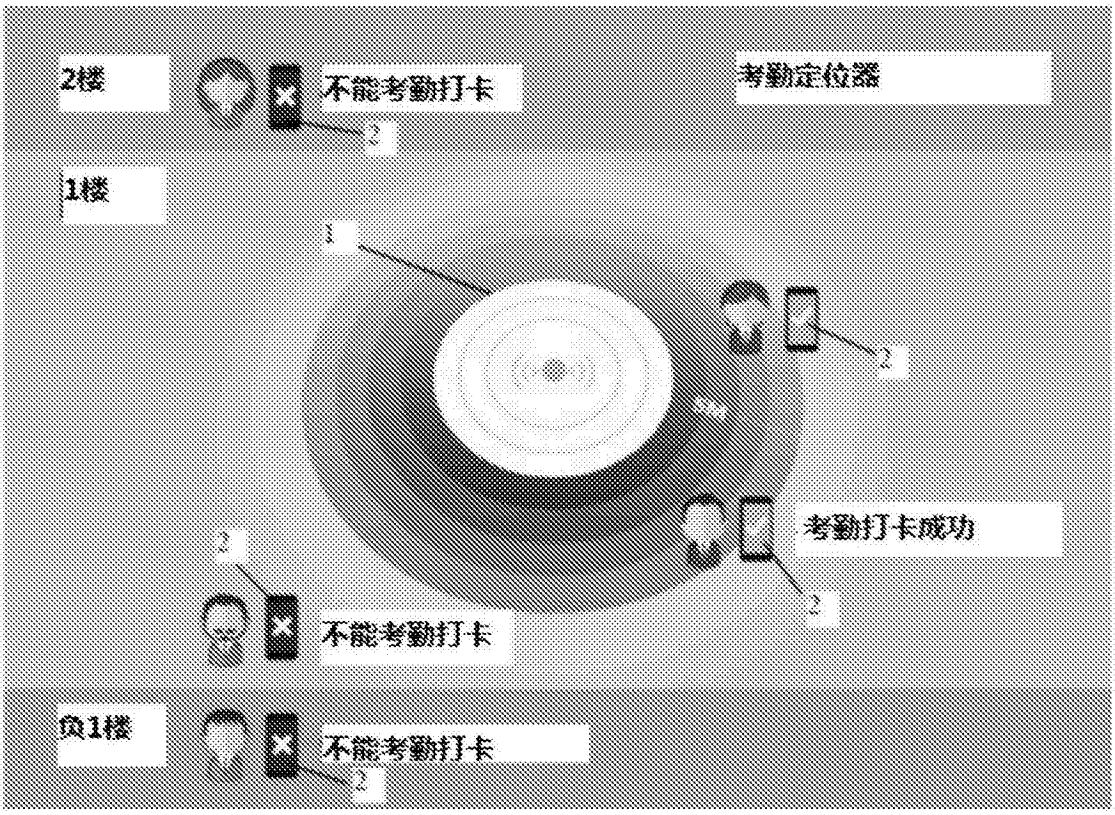


图1

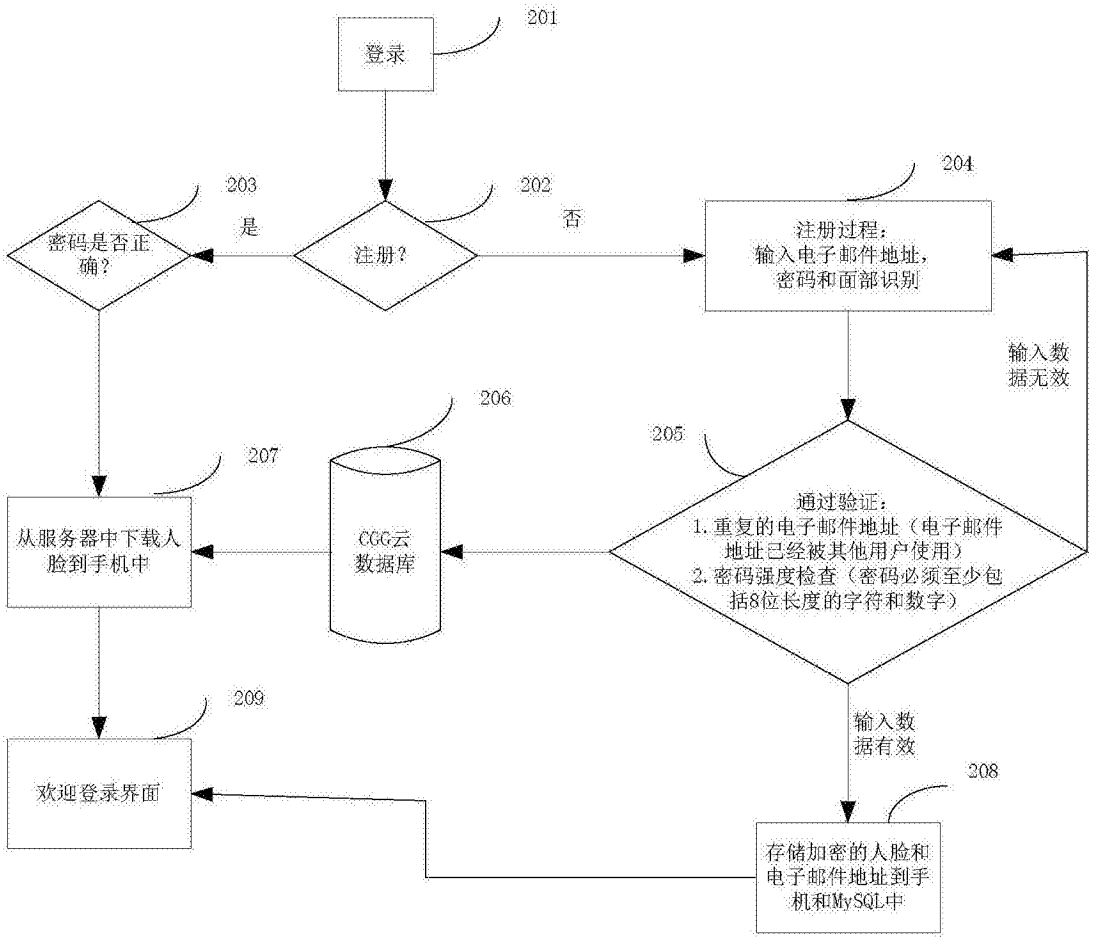

登录
201
注册?
202
否
是
203
密码是否正确?
注册过程:
输入电子邮件地址,
密码和面部识别
204
输入数据无效
通过验证:
1.重复的电子邮件地址(电子邮件地址已经被其他用户使用)
2.密码强度检查(密码必须至少包括8位长度的字符和数字)
205
CGG云数据库
206
从服务器中下载人脸到手机中
207
输入数据有效
存储加密的人脸和电子邮件地址到手机和MySQL中
208
欢迎登录界面
209

图2

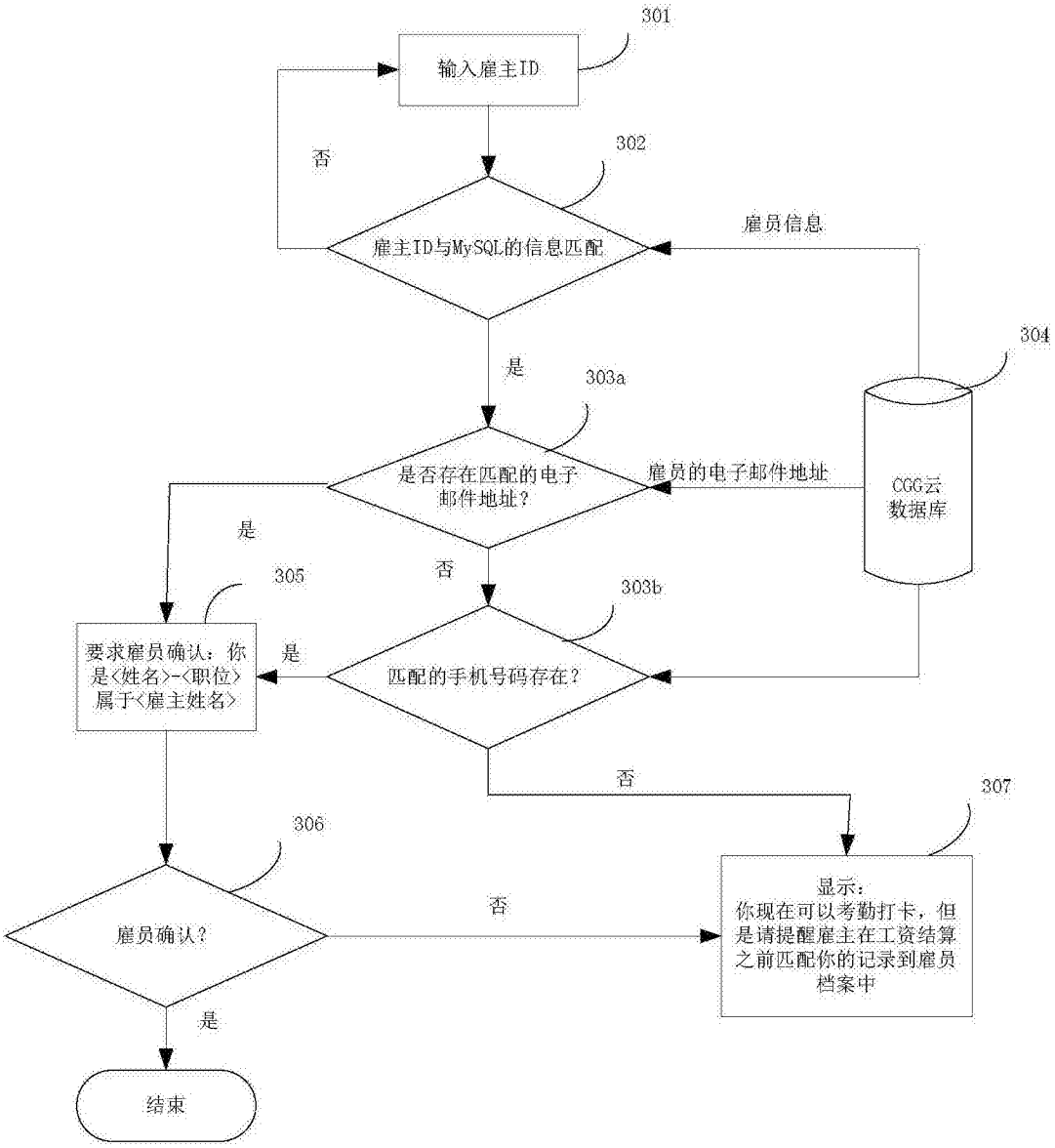

301
输入雇主ID
否
302
雇主ID与MySQL的信息匹配
雇员信息
304
是
303a
是否存在匹配的电子邮件地址？
雇员的电子邮件地址
CGG云数据库
是
否
305
303b
要求雇员确认：你是<姓名>-<职位>属于<雇主姓名>
是
匹配的手机号码存在？
否
307
306
显示：
你现在可以考勤打卡，但是请提醒雇主在工资结算之前匹配你的记录到雇员档案中
雇员确认？
否
是
结束

图3

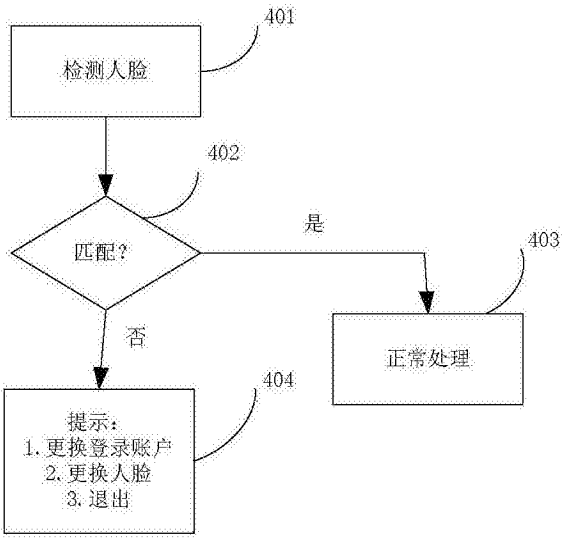

401
检测人脸
402
匹配?
是
403
正常处理
否
404
提示：
1.更换登录账户
2.更换人脸
3.退出

图4

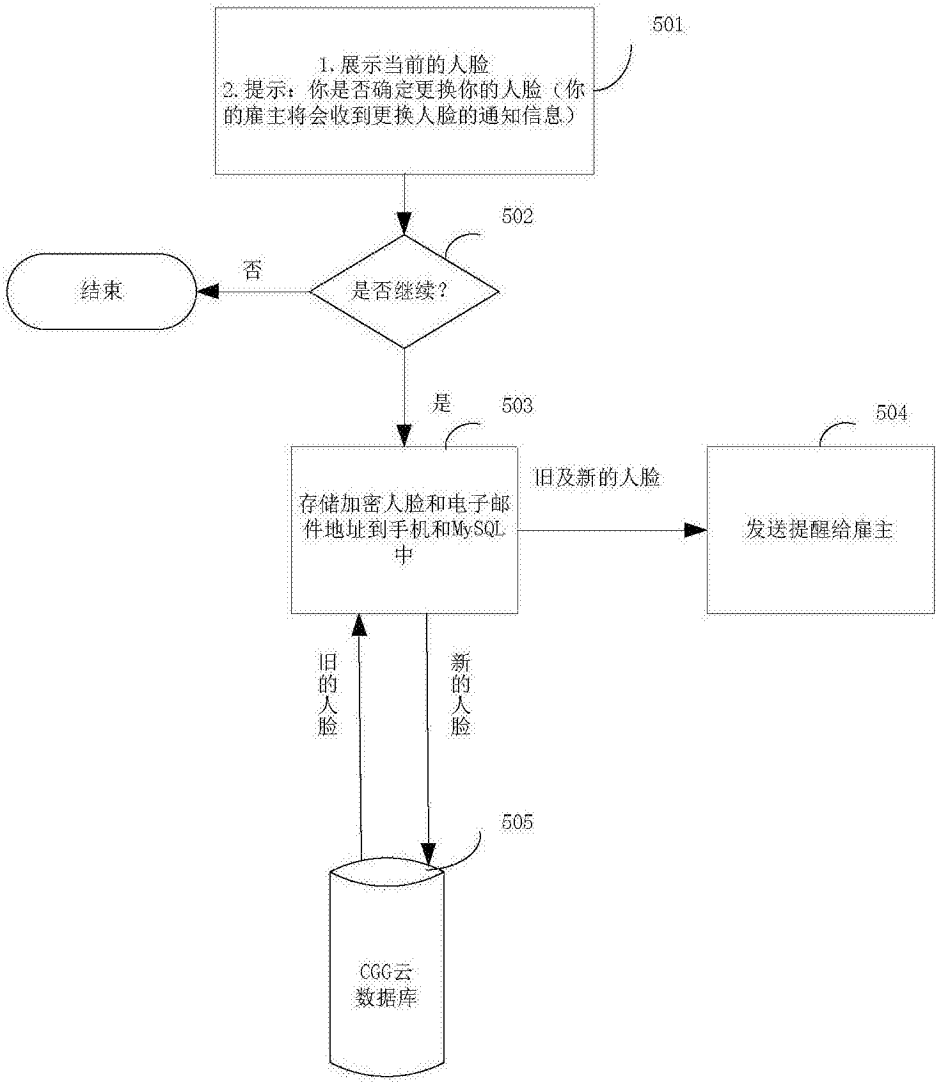

501
1.展示当前的人脸
2.提示：你是否确定更换你的人脸（你的雇主将会收到更换人脸的通知信息）
502
结束
否
是否继续?
是
503
504
存储加密人脸和电子邮件地址到手机和MySQL中
旧及新的人脸
发送提醒给雇主
旧的人脸
新的人脸
505
CGG云数据库

图5