(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 108427879 A
(43)申请公布日 2018.08.21

(21)申请号 201810241884.8

(22)申请日 2018.03.22

(71)申请人 平安科技(深圳)有限公司
地址 518000 广东省深圳市福田区八卦岭工业区平安大厦六楼

(72)发明人 刘阳 冯心 梁瑾 张瑞光 李俊 黄心官 刘文慧

(74)专利代理机构 深圳市明日今典知识产权代理事务所(普通合伙) 44343
代理人 王杰辉

(51)Int.Cl.
G06F 21/45(2013.01)

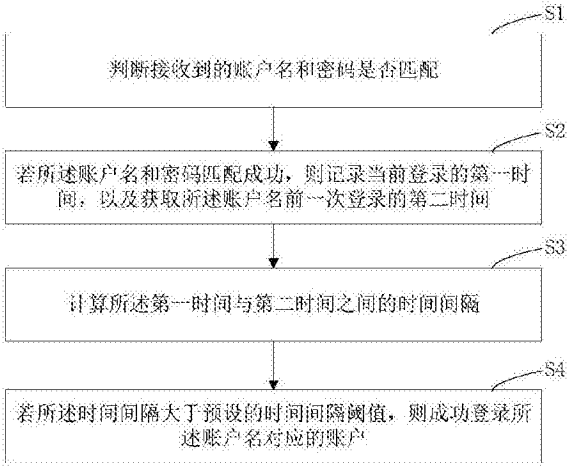
权利要求书2页 说明书10页 附图8页

(54)发明名称

账户安全管理方法、装置、计算机设备和存储介质

(57)摘要

本发明揭示了一种账户安全管理方法、装置、计算机设备和存储介质，其中方法包括：判断接收到的账户名和密码是否匹配；若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间；计算所述第一时间与第二时间之间的时间间隔；其中，若所述第二时间为空，则所述时间间隔为无穷大；若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户。本发明不用为账号解锁问题而引用第三方时间任务管理框架，也无需为初始用户设定额外的标记位，减少开发工作量；不需要在后台进行时间任务管理动作，大大的减少系统资源的开销。



CN 108427879 A

1.一种账户安全管理方法，其特征在于，包括：

判断接收到的账户名和密码是否匹配；

若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间；

计算所述第一时间与第二时间之间的时间间隔；

若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户。

2.根据权利要求1所述的账户安全管理方法，其特征在于，所述若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间的步骤之后，包括：

若所述第二时间为空，则生成强制修改密码指令。

3.根据权利要求2所述的账户安全管理方法，其特征在于，所述生成强制修改密码指令的步骤之后，包括：

接收修改后的密码，以及拍摄修改密码者的第一人脸照片；

将所述修改后的密码、以及所述第一人脸照片分别与所述账户名关联存储在数据库中。

4.根据权利要求3所述的账户安全管理方法，其特征在于，所述成功登录所述账户名对应的账户的步骤之后，包括：

拍摄当前登录者的第二人脸照片；

在所述数据库中调取与所述账户名对应的所述第一人脸照片；

将所述第一人脸照片和第二人脸照片进行比较；

若判定所述第一人脸照片和第二人脸照片为同一人的人脸照片，则开放当前登陆者的全部账户权限；若判定所述第一人脸照片和第二人脸照片为不同人的人脸照片，则根据预设规则关闭当前登陆者的部分账户权限。

5.根据权利要求4所述的账户安全管理方法，其特征在于，所述在所述数据库中调取与所述账户名对应的所述第一人脸照片的步骤之前，包括：

向拍摄区域进行超声波扫描，并接收超声波的反射波；

根据反射波判断拍摄区域的物体的轮廓；

若轮廓符合预设的标准，则判定当前拍摄的图片是真人图片，生成调用所述第一人脸照片的指令。

6.根据权利要求1所述的账户安全管理方法，其特征在于，所述计算所述第一时间与第二时间之间的时间间隔的步骤之后，包括：

若所述时间间隔大于预设的时间间隔阈值，则清空密码输入错误次数的历史数据。

7.根据权利要求1所述的账户安全管理方法，其特征在于，所述判断接收到的账户名和密码是否匹配的步骤之后，包括：

若所述账户名和密码匹配失败，则在密码输入错误次数的历史数据上加一；

判断加一后的所述历史数据是否大于预设错误阈值；

若大于，则锁定所述账户名。

8.一种账户安全管理装置，其特征在于，包括：

判断单元，用于判断接收到的账户名和密码是否匹配；

记录获取单元，用于若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间；

计算单元，用于计算所述第一时间与第二时间之间的时间间隔；

登录单元，用于若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户。

9.一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至7中任一项所述方法的步骤。

10.一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，所述计算机程序被处理器执行时实现权利要求1至7中任一项所述的方法的步骤。

账户安全管理方法、装置、计算机设备和存储介质

技术领域

[0001] 本发明涉及到账户安全管理领域，特别是涉及到一种账户安全管理方法、装置、计算机设备和存储介质。

背景技术

[0002] 登录某些系统、网站时，需要登录账户名和密码，只有密码和账户名对应成功后，才会登录成功。为了系统安全，会限制指定时间内连续输入错误密码的次数，如果连续输入密码错误达到预设次数，则会将该账户名锁定，然后根据设定的方式将账户名解锁，比如常见的，经过指定时间长后，自动恢复正常的设置等。

[0003] 具体的，在账户安全管理上，现有技术存在两种方式，具体如下：

[0004] 1、当登录次数到达设定值时，即锁定账户名，一段时间内不得登录；

[0005] 2、业务系统一般采用管理员创建，而非注册方式生成账户名，管理员创建密码的强度较弱或不方便记忆，需要在初始登录时强制修改密码。

[0006] 上述第一种方式，账户锁定后需自动解锁，一般是在系统中设定定时任务，在设定的时间点内触发解锁任务。而配置定时任务需要在系统中引入第三方框架，同时任务执行过程中需要消耗大量的系统资源，这无疑增加了开发工作量和系统硬件开销，延长了项目开发周期；上述第二种方式，初始化账户，需要额外的标记位标识，同样也会增加开发工作。

[0007] 所以提供一种新的账户安全管理方法，以节约开发工作量是一种亟需解决的问题。

发明内容

[0008] 本发明的主要目的为提供一种无须引入第三方时间任务管理框架的账户安全管理方法、装置、计算机设备和存储介质。

[0009] 为了实现上述发明目的，本发明提出一种账户安全管理方法，包括：

[0010] 判断接收到的账户名和密码是否匹配；

[0011] 若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间；

[0012] 计算所述第一时间与第二时间之间的时间间隔；其中，若所述第二时间为空，则所述时间间隔为无穷大；

[0013] 若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户。

[0014] 进一步地，所述若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间的步骤之后，包括：

[0015] 若所述第二时间为空，则生成强制修改密码指令。

[0016] 进一步地，所述生成强制修改密码指令的步骤之后，包括：

[0017] 接收修改后的密码，以及拍摄修改密码者的第一人脸照片；

[0018] 将所述修改后的密码、以及所述第一人脸照片分别与所述账户名关联存储在数据

库中。

[0019] 进一步地，所述成功登录所述账户名对应的账户的步骤之后，包括：

[0020] 拍摄当前登录者的第二人脸照片；

[0021] 在所述数据库中调取与所述账户名对应的所述第一人脸照片；

[0022] 将所述第一人脸照片和第二人脸照片进行比较；

[0023] 若判定所述第一人脸照片和第二人脸照片为同一人的人脸照片，则开放当前登陆者的全部账户权限；若判定所述第一人脸照片和第二人脸照片为不同人的人脸照片，则根据预设规则关闭当前登陆者的部分账户权限。

[0024] 进一步地，所述在所述数据库中调取与所述账户名对应的所述第一人脸照片的步骤之前，包括：

[0025] 向拍摄区域进行超声波扫描，并接收超声波的反射波；

[0026] 根据反射波判断拍摄区域的物体的轮廓；

[0027] 若轮廓符合预设的标准，则判定当前拍摄的图片是真人图片，生成调用所述第一人脸照片的指令。

[0028] 进一步地，所述计算所述第一时间与第二时间之间的时间间隔的步骤之后，包括：

[0029] 清空密码输入错误次数的历史数据。

[0030] 进一步地，所述判断接收到的账户名和密码是否匹配的步骤之后，包括：

[0031] 若所述账户名和密码匹配失败，则在密码输入错误次数的历史数据上加一；

[0032] 判断加一后的所述历史数据是否大于预设错误阈值；

[0033] 若大于，则锁定所述账户名。

[0034] 本发明还提供一种账户安全管理装置，包括：

[0035] 判断单元，用于判断接收到的账户名和密码是否匹配；

[0036] 记录获取单元，用于若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间；

[0037] 计算单元，用于计算所述第一时间与第二时间之间的时间间隔；其中，若所述第二时间为空，则所述时间间隔为无穷大；

[0038] 登录单元，用于若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户。

[0039] 本发明还提供一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述任一项所述方法的步骤。

[0040] 本发明还提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述任一项所述的方法的步骤。

[0041] 本发明的账户安全管理方法、装置、计算机设备和存储介质，不用为账号解锁问题而引用第三方时间任务管理框架，也无需为初始用户设定额外的标记位，减少开发工作量，缩短开发时间。判断是否解除账户的锁定状态的时间是根据用户的登录时间进行的，解除锁定状态的时间分布较为分散，也不需要在后台进行时间任务管理动作，大大的减少系统资源的开销。

附图说明

[0042] 图1为本发明一实施例的账户安全管理方法的流程示意图；

[0043] 图2为本发明一实施例的账户安全管理方法的流程示意图；

[0044] 图3为本发明一实施例的账户安全管理方法的流程示意图；

[0045] 图4为本发明一实施例的账户安全管理方法的流程示意图；

[0046] 图5为本发明一实施例的账户安全管理装置的结构示意框图；

[0047] 图6为本发明一实施例的账户安全管理装置的结构示意框图；

[0048] 图7为本发明一实施例的账户安全管理装置的结构示意框图；

[0049] 图8为本发明一实施例的账户安全管理装置的结构示意框图；

[0050] 图9为本发明一实施例的计算机设备的结构示意框图。

[0051] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0052] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0053] 参照图1，本发明实施例提供一种账户安全管理方法，包括步骤：

[0054] S1、判断接收到的账户名和密码是否匹配；

[0055] S2、若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间；

[0056] S3、计算所述第一时间与第二时间之间的时间间隔；

[0057] S4、若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户。

[0058] 如上述步骤S1所述，上述账户名是指登录系统对应账户时需要输入的名称内容。上述密码用于验证账户名是否正确。在一个系统中，每一个账户一般设置有一个对应的密码。在一具体实施例中，一个账户可以对应设置多个密码，使用不同的密码登录该账户时，所得到的权限不同。本步骤S1是指，系统接收到当前用户输入的账户名和密码后，判断账户名与密码是否匹配，如果匹配成功，则可以登录系统，如果匹配失败，则会发出错误提示等信息。

[0059] 如上述步骤S2所述，上述第一时间是系统判定上述账户名和密码匹配后记录的时间，该时间可以为用户输入完账户名和密码后点击登录时的时间，也可以是系统判断完账户名和密码是否匹配后的时间，可以根据具体要求进行相应的设置即可。上述第二时间是系统前一次登录的时间，该前一次登录是指用户输入账户名和密码后点击登录的操作，点击登录后无论是否登录成功，均会记录一个时间，这个时间既可以认为是上述的第二时间。

[0060] 如上述步骤S3所述，若所上述第二时间为空，则时间间隔为无穷大；上述第二时间为空，是指当前登录账户为第一次登录账户，即在本次之前并没有登录过上述账户，所以，第二时间是不存在的，因此可以认为第一时间和第二时间的时间间隔为无穷大。

[0061] 如上述步骤S4所述，只要上述时间间隔大于预设的时间间隔阈值，则会成功登录上述账户对应的系统。即，无论用户在登录账户之前，账户处于锁定状态还是非锁定状态，只要账户名和密码匹配，且上述时间间隔大于预设的时间间隔阈值，均会成功登录系统。在另一实施例中，如果时间间隔小于等于上述时间间隔阈值，若是账户名对应的账户处于锁定状态，则无法成功登录账户，如果账户名对应的账户未处于锁定状态，则不会影响用户正

常的登录。

[0062] 参照图2，本实施例中，上述若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间的步骤S2之后，包括：

[0063] S21、若所述第二时间为空，则生成强制修改密码指令。

[0064] S22、接收修改后的密码，以及拍摄修改密码者的第一人脸照片；

[0065] S23、将所述修改后的密码、以及所述第一人脸照片分别与所述账户名关联存储在数据库中。

[0066] 如上述步骤S21所述，如果第二时间为空，则说明账户名对应的账户可能是系统管理员分配的账户，其密码一般较为简单，或者不容易记忆，在后期使用时存在风险，如果密码较为简单，则容易被破解；如果密码不容易记忆，则容易忘记，需要麻烦管理员进行提醒等，所以生成强制修改密码指令，要求用户必须修改密码，而用户自己修改的密码，相对用户而言容易记忆，还可以设置难度较高的密码。

[0067] 如上述步骤S22所述，修改完成密码之后，还会拍摄修改密码者(即上述的用户)的第一人脸照片，第一人脸照片可以用于后期的二级验证或者权限管理等使用。

[0068] 如上述步骤S23所述，将修改后的密码和第一人脸照片分别与账户名关联存储在数据库中，是为了后期根据账户名进行调用密码和第一人脸照片进行比对。

[0069] 参照图2，本实施例中，上述成功登录所述账户名对应的账户的步骤S4之后，包括：

[0070] S41、拍摄当前登录者的第二人脸照片；

[0071] S42、在所述数据库中调取与所述账户名对应的所述第一人脸照片；

[0072] S43、将所述第一人脸照片和第二人脸照片进行比较；

[0073] S44、若判定所述第一人脸照片和第二人脸照片为同一人的人脸照片，则开放当前登陆者的全部账户权限；若判定所述第一人脸照片和第二人脸照片为不同人的人脸照片，则根据预设规则关闭当前登陆者的部分账户权限。

[0074] 如上述步骤S41至S44所述，如果第一人脸照片与第二人脸照片为同一人的人脸照片，说明是账户名对应的主人进行登录，其具有全部的权限。如果第一人脸照片与第二人脸照片不为同一人的人脸照片，则说明是非账户名对应的主人进行的登录，此时，存在两种可能，第一种是用户好友进行登录；第二种是账户被盗。无论是哪一种情况，此时设置了账户的权限，则可以保护账户的安全。在其它实施例中，受到权限限制时，当前操作者可以发送授权管理信息给用户，如果用户接收并回复授权的命令，则可以获取到更大的权限，该权限可以是全部权限，也可以根据用户回复不同的授权命令而给予对应的权限。在一具体实施例中，比如系统为银行的自动取款系统，虽然账户名和密码匹配成功，但是因为上述的人脸比对失败，此时，当前用户的权限是可以查看账户余额，但是不能取款等。

[0075] 参照图3，本实施例中，上述在所述数据库中调取与所述账户名对应的所述第一人脸照片的步骤S42之前，包括：

[0076] S421、向拍摄区域进行超声波扫描，并接收超声波的反射波；

[0077] S422、根据反射波判断拍摄区域的物体的轮廓；

[0078] S423、若轮廓符合预设的标准，则判定当前拍摄的图片是真人图片，生成调用所述第一人脸照片的指令。

[0079] 如上述步骤S421至S423所述，如果当前拍摄的图片是一个海报等照片时，那么海

报等照片必须较为平整的展开，此时其轮廓是一个平面，而如果是真人，其轮廓是一个3d轮廓。即，对拍摄物进行如B超一样的扫描，如果扫描的结果是一个与人头近似的3d轮廓，则认为拍摄的第二照片是一个真人照片，以防止他人利用照片欺骗系统而获取到上述账户的全部权限，提高账户的安全。

[0080] 参照图4，本实施例中，上述计算所述第一时间与第二时间之间的时间间隔的步骤S3之后，包括：

[0081] S31、若所述时间间隔大于预设的时间间隔阈值，则清空密码输入错误次数的历史数据。

[0082] 如上述步骤S31所述，无论当前账号是否处于锁定状态，自动将账号设置到未锁定状态，同时清空之前密码输入的错误次数，此时如果密码正确，则可以登录成功；此时如果密码错误，则重新开始记录登录错误次数。

[0083] 本实施例中，上述判断接收到的账户名和密码是否匹配的步骤S1之后，包括：

[0084] S11、若所述账户名和密码匹配失败，则在密码输入错误次数的历史数据上加一；

[0085] S12、判断加一后的所述历史数据是否大于预设错误阈值；

[0086] S13、若大于，则锁定所述账户名。

[0087] 如上述总部后S11至S13所述，即为若当前次输入的账户名和密码不匹配，则增加一次密码输入错误的次数累计。

[0088] 在本实施例中，在上述计算所述第一时间与第二时间之间的时间间隔的步骤S3之后，包括：

[0089] S301、若上述时间间隔小于等于预设的时间间隔阈值，且上述账户处于锁定状态的情况下，接收预设操作动作强制解除锁定状态。

[0090] 如上述步骤S301所述，其具体的强制解除锁定状态的过程如下：接收预设的强制解除锁定状态的按钮被点击产生的指令，生成邮件输入框；判断输入框内输入的内容是否是预设的内容(该内容是用户在建立账户时输入的内容)；若是，则将该内容发送给指定的邮箱(该邮箱同样是在建立账户时预设的邮箱)；若未收到上述邮箱的反馈(包括反馈超时)，则解除锁定状态失败；若接收到上述邮箱的反馈，则判断邮箱反馈的内容是否符合预设要求(同样是在建立账户设置的内容，该内容与输入上述输入框的内容一般不同)，如果符合要求，则解除锁定状态，否则解除锁定状态失败。本步骤的好处是：如果当前操作者是其它人，那么他不会知道具体发送到那个邮箱，所以其不会登录对应的邮箱进行反馈，同时，即使知道是哪个邮箱，邮箱的密码也不一定知道，进一步提高账户的安全等。

[0091] 进一步地，在上述“判断邮箱反馈的内容是否符合预设要求”的步骤之前，判断登录邮箱的设备是否与当前登录账户的设备相同，若相同，则解除锁定状态失败。也就是，如果要解除锁定状态至少要准备两台不同的设备，否则无法完成解除锁定状态，旨在增加解除锁定状态的难度。本实施例中，还可以判断登录邮件的设备与当前登录账户的设备是否属于同一局域网内，若在同一局域网内，也无法完成解除锁定状态。同样增加解除锁定状态的难度。

[0092] 本实施例中，在判断输入框内输入的内容是否是预设的内容之前，还会判断登录账户的设备所处的地理位置；判断该地理位置是否为预设的指定地理位置；若是，则生成“判断输入框内输入的内容是否是预设的内容”的指令。上述判断位置的方法包括多种，若

登录账户的设备时无线连接网络的设备，则可以通过GPS、wifi定位、基站三角定位等；若登录账户的设备是有限连接网关，则获取网关的位置即可。

[0093] 本实施例中，上述账户安全管理方法，可以在系统的登录程序中编写对应上述方法的应用程序即可，无需在开发的时候引入第三方时间任务管理框架，降低了开放的工作量。判断是否解除账户名的锁定状态的时间是根据用户的登录时间进行的，解除锁定状态的时间分布较为分散，系统无需在后台一直进行时间任务管理工作，大大地减少系统资源的开销。

[0094] 参照图5，本发明还提供一种账户安全管理装置，包括：

[0095] 判断单元10，用于判断接收到的账户名和密码是否匹配。

[0096] 记录获取单元20，用于若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间；

[0097] 计算单元30，用于计算所述第一时间与第二时间之间的时间间隔；

[0098] 登录单元40，用于若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户。

[0099] 上述判断单元10中，账户名是指登录系统对应账户时需要输入的名称内容。上述密码用于验证账户名是否正确。在一个系统中，每一个账户一般设置有一个对应的密码。在一具体实施例中，一个账户可以对应设置多个密码，使用不同的密码登录该账户时，所得到的权限不同。本实施例中，上述系统接收到当前用户输入的账户名和密码后，判断账户名与密码是否匹配，如果匹配成功，则可以登录系统，如果匹配失败，则会发出错误提示等信息。

[0100] 上述记录获取单元20中，上述第一时间是系统判定上述账户名和密码匹配后记录的时间，该时间可以为用户输入完账户名和密码后点击登录时的时间，也可以是系统判断完账户名和密码是否匹配后的时间，可以根据具体要求进行相应的设置即可。上述第二时间是系统前一次登录的时间，该前一次登录是指用户输入账户名和密码后点击登录的操作，点击登录后无论是否登录成功，均会记录一个时间，这个时间既可以认为是上述的第二时间。

[0101] 上述计算单元30中，若上述第二时间为空，则时间间隔为无穷大；上述第二时间为空，是指当前登录账户为第一次登录账户，即在本次之前并没有登录过上述账户，所以，第二时间是不存在的，因此可以认为第一时间和第二时间的时间间隔为无穷大。

[0102] 上述登录单元40中，只要上述时间间隔大于预设的时间间隔阈值，则会成功登录上述账户对应的系统。即，无论用户在登录账户之前，账户处于锁定状态还是非锁定状态，只要账户名和密码匹配，且上述时间间隔大于预设的时间间隔阈值，均会成功登录系统。在另一实施例中，如果时间间隔小于等于上述时间间隔阈值，若是账户名对应的账户处于锁定状态，则无法成功登录账户，如果账户名对应的账户未处于锁定状态，则不会影响用户正常的登录。

[0103] 参照图6，本实施例中，上述账户安全管理装置还包括：

[0104] 生成单元21，用于若所述第二时间为空，则生成强制修改密码指令。

[0105] 修改拍照单元22，用于接收修改后的密码，以及拍摄修改密码者的第一人脸照片；

[0106] 关联存储单元23，用于将所述修改后的密码、以及所述第一人脸照片分别与所述账户名关联存储在数据库中。

[0107] 在上述生成单元21中，如果第二时间为空，则说明账户名对应的账户可能是系统管理员分配的账户，其密码一般较为简单，或者不容易记忆，在后期使用时存在风险，如果密码较为简单，则容易被破解；如果密码不容易记忆，则容易忘记，需要麻烦管理员进行提醒等，所以生成强制修改密码指令，要求用户必须修改密码，而用户自己修改的密码，相对用户而言容易记忆，还可以设置难度较高的密码。

[0108] 在上述修改拍照单元22中，修改完成密码之后，还会拍摄修改密码者(即上述的用户)的第一人脸照片，第一人脸照片可以用于后期的二级验证或者权限管理等使用。

[0109] 在上述关联存储单元23中，将修改后的密码和第一人脸照片分别与账户名关联存储在数据库中，是为了后期根据账户名进行调用密码和第一人脸照片进行比对。

[0110] 参照图6，本实施例中，上述账户安全管理装置还包括：

[0111] 拍摄单元41，用于拍摄当前登录者的第二人脸照片；

[0112] 调取单元42，用于在所述数据库中调取与所述账户名对应的所述第一人脸照片；

[0113] 比较单元43，用于将所述第一人脸照片和第二人脸照片进行比较；

[0114] 权限管理单元44，用于若判定所述第一人脸照片和第二人脸照片为同一人的人脸照片，则开放当前登陆者的全部账户权限；若判定所述第一人脸照片和第二人脸照片为不同人的人脸照片，则根据预设规则关闭当前登陆者的部分账户权限。

[0115] 在上述拍摄单元41、调取单元42、比较单元43以及权限管理单元44中，如果第一人脸照片与第二人脸照片为同一人的人脸照片，说明是账户名对应的主人进行登录，其具有全部的权限。如果第一人脸照片与第二人脸照片不为同一人的人脸照片，则说明是非账户名对应的主人进行的登录，此时，存在两种可能，第一种是用户好友进行登录；第二种是账户被盗。无论是哪一种情况，此时设置了账户的权限，则可以保护账户的安全。在其它实施例中，受到权限限制时，当前操作者可以发送授权管理信息给用户，如果用户接收并回复授权的命令，则可以获取到更大的权限，该权限可以是全部权限，也可以根据用户回复不同的授权命令而给予对应的权限。

[0116] 参照图7，本实施例中，上述账户安全管理装置，还包括：

[0117] 超声扫描单元421，用于向拍摄区域进行超声波扫描，并接收超声波的反射波；

[0118] 轮廓判断单元422，用于根据反射波判断拍摄区域的物体的轮廓；

[0119] 人脸判定单元423，用于若轮廓符合预设的标准，则判定当前拍摄的图片是真人图片，生成调用所述第一人脸照片的指令。

[0120] 在上述超声扫描单元421、轮廓判断单元422和人脸判定单元423中，如果当前拍摄的图片是一个海报等照片时，那么海报等照片必须较为平整的展开，此时其轮廓是一个平面，而如果是真人，其轮廓是一个3d轮廓。即，对拍摄物进行如B超一样的扫描，如果扫描的结果是一个与人头近似的3d轮廓，则认为拍摄的第二照片是一个真人照片，以防止他人利用照片欺骗系统而获取到上述账户的全部权限，提高账户的安全。

[0121] 参照图8，在一实施例中，上述账户安全管理装置，还包括：

[0122] 清空单元31，用于清空密码输入错误次数的历史数据。

[0123] 在上述清空单元31中，无论当前账号是否处于锁定状态，自动将账号设置到未锁定状态，同时清空之前密码输入的错误次数，此时如果密码正确，则可以登录成功；此时如果密码错误，则重新开始记录登录错误次数。

[0124] 在一实施例中，上述账户安全管理装置，还包括：

[0125] 增加单元11，用于若所述账户名和密码匹配失败，则在密码输入错误次数的历史数据上加一；

[0126] 阈值判断单元12，用于判断加一后的所述历史数据是否大于预设错误阈值；

[0127] 锁定单元13，用于若所述历史数据大于预设错误阈值，则锁定所述账户名。

[0128] 在一实施例中，上述账户安全管理装置，还包括：

[0129] 解除锁定单元301，用于若上述时间间隔小于等于预设的时间间隔阈值，且上述账户处于锁定状态的情况下，接收预设操作动作强制解除锁定状态。

[0130] 在上述解除锁定单元301中，其具体的强制解除锁定状态的过程如下：接收预设的强制解除锁定状态的按钮被点击产生的指令，生成邮件输入框；判断输入框内输入的内容是否是预设的内容(该内容是用户在建立账户时输入的内容)；若是，则将该内容发送给指定的邮箱(该邮箱同样是在建立账户时预设的邮箱)；若未收到上述邮箱的反馈(包括反馈超时)，则解除锁定状态失败；若接收到上述邮箱的反馈，则判断邮箱反馈的内容是否符合预设要求(同样是在建立账户设置的内容，该内容与输入上述输入框的内容一般不同)，如果符合要求，则解除锁定状态，否则解除锁定状态失败。本步骤的好处是：如果当前操作者是其它人，那么他不会知道具体发送到那个邮箱，所以其不会登录对应的邮箱进行反馈，同时，即使知道是哪个邮箱，邮箱的密码也不一定知道，进一步提高账户的安全等。进一步地，在上述“判断邮箱反馈的内容是否符合预设要求”的步骤之前，判断登录邮箱的设备是否与当前登录账户的设备相同，若相同，则解除锁定状态失败。也就是，如果要解除锁定状态至少要准备两台不同的设备，否则无法完成解除锁定状态，旨在增加解除锁定状态的难度。本实施例中，还可以判断登录邮件的设备与当前登录账户的设备是否属于同一局域网内，若在同一局域网内，也无法完成解除锁定状态。同样增加解除锁定状态的难度。

[0131] 本实施例中，在判断输入框内输入的内容是否是预设的内容之前，还会：判断登录账户的设备所处的地理位置；判断该地理位置是否为预设的指定地理位置；若是，则生成“判断输入框内输入的内容是否是预设的内容”的指令。上述判断位置的方法包括多种，若登录账户的设备时无线连接网络的设备，则可以通过GPS、wifi定位、基站三角定位等；若登录账户的设备是有限连接网关，则获取网关的位置即可。

[0132] 本发明实施例中的账户安全管理装置，可以在系统的登录程序中编写对应上述方法的应用程序即可，无需在开发的时候引入第三方时间任务管理框架，降低了开放的工作量。判断是否解除账户名的锁定状态的时间是根据用户的登录时间进行的，解除锁定状态的时间分布较为分散，系统无需在后台一直进行时间任务管理工作，大大地减少系统资源的开销。

[0133] 参照图9，本发明实施例中还提供一种计算机设备，该计算机设备可以是服务器，其内部结构可以如图9所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中，该计算机设计的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于存储账户安全管理方法中用到的图片数据等数据。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一

种账户安全管理方法。

[0134] 上述处理器执行上述账户安全管理方法的步骤包括：判断接收到的账户名和密码是否匹配；若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间；计算所述第一时间与第二时间之间的时间间隔；其中，若所述第二时间为空，则所述时间间隔为无穷大；若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户。

[0135] 在一实施例中，上述若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间的步骤之后，包括：若所述第二时间为空，则处理器生成强制修改密码指令。

[0136] 在一实施例中，上述处理器生成强制修改密码指令的步骤之后，包括：接收修改后的密码，以及拍摄修改密码者的第一人脸照片；将所述修改后的密码、以及所述第一人脸照片分别与所述账户名关联存储在数据库中。

[0137] 在一实施例中，上述处理器成功登录所述账户名对应的账户的步骤之后，包括：拍摄当前登录者的第二人脸照片；在所述数据库中调取与所述账户名对应的所述第一人脸照片；将所述第一人脸照片和第二人脸照片进行比较；若判定所述第一人脸照片和第二人脸照片为同一人的人脸照片，则开放当前登陆者的全部账户权限；若判定所述第一人脸照片和第二人脸照片为不同人的人脸照片，则根据预设规则关闭当前登陆者的部分账户权限。

[0138] 在一实施例中，上述处理器在所述数据库中调取与所述账户名对应的所述第一人脸照片的步骤之前，包括：向拍摄区域进行超声波扫描，并接收超声波的反射波；根据反射波判断拍摄区域的物体的轮廓；若轮廓符合预设的标准，则判定当前拍摄的图片是真人图片，生成调用所述第一人脸照片的指令。

[0139] 在一实施例中，上述处理器计算所述第一时间与第二时间之间的时间间隔的步骤之后，包括：清空密码输入错误次数的历史数据。

[0140] 在一实施例中，上述处理器判断接收到的账户名和密码是否匹配的步骤之后，包括：若所述账户名和密码匹配失败，则在密码输入错误次数的历史数据上加一；判断加一后的所述历史数据是否大于预设错误阈值；若大于，则锁定所述账户名。

[0141] 本领域技术人员可以理解，图9中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定。

[0142] 本发明实施例还提供一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时实现一种账户安全管理方法，该方法具体为：判断接收到的账户名和密码是否匹配；若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间；计算所述第一时间与第二时间之间的时间间隔；其中，若所述第二时间为空，则所述时间间隔为无穷大；若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户。

[0143] 上述计算机可读存储介质存储的计算机程序，不用为账号解锁问题而引用第三方时间任务管理框架，也无需为初始用户设定额外的标记位，减少开发工作量，缩短开发时间。判断是否解除账户名的锁定状态的时间是根据用户的登录时间进行的，解除锁定状态的时间分布较为分散，也不需要在后台进行时间任务管理动作，大大的减少系统资源的开销。

[0144] 在一个实施例中，上述若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间的步骤之后，包括：若所述第二时间为空，则处理器生成强制修改密码指令。

[0145] 在一实施例中，上述处理器生成强制修改密码指令的步骤之后，包括：接收修改后的密码，以及拍摄修改密码者的第一人脸照片；将所述修改后的密码、以及所述第一人脸照片分别与所述账户名关联存储在数据库中。

[0146] 在一实施中，上述处理器成功登录所述账户名对应的账户的步骤之后，包括：拍摄当前登录者的第二人脸照片；在所述数据库中调取与所述账户名对应的所述第一人脸照片；将所述第一人脸照片和第二人脸照片进行比较；若判定所述第一人脸照片和第二人脸照片为同一人的人脸照片，则开放当前登陆者的全部账户权限；若判定所述第一人脸照片和第二人脸照片为不同人的人脸照片，则根据预设规则关闭当前登陆者的部分账户权限。

[0147] 在一实施例中，上述处理器在所述数据库中调取与所述账户名对应的所述第一人脸照片的步骤之前，包括：向拍摄区域进行超声波扫描，并接收超声波的反射波；根据反射波判断拍摄区域的物体的轮廓；若轮廓符合预设的标准，则判定当前拍摄的图片是真人图片，生成调用所述第一人脸照片的指令。

[0148] 在一实施例中，上述处理器计算所述第一时间与第二时间之间的时间间隔的步骤之后，包括：清空密码输入错误次数的历史数据。

[0149] 在一实施例中，上述处理器判断接收到的账户名和密码是否匹配的步骤之后，包括：若所述账户名和密码匹配失败，则在密码输入错误次数的历史数据上加一；判断加一后的所述历史数据是否大于预设错误阈值；若大于，则锁定所述账户名。

[0150] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储与一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的和实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可以包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限，RAM一多种形式可得，诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双速据率SDRAM(SSRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0151] 需要说明的是，在本文中，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、装置、物品或者方法不仅包括那些要素，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、装置、物品或者方法所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、装置、物品或者方法中还存在另外的相同要素。

[0152] 以上所述仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

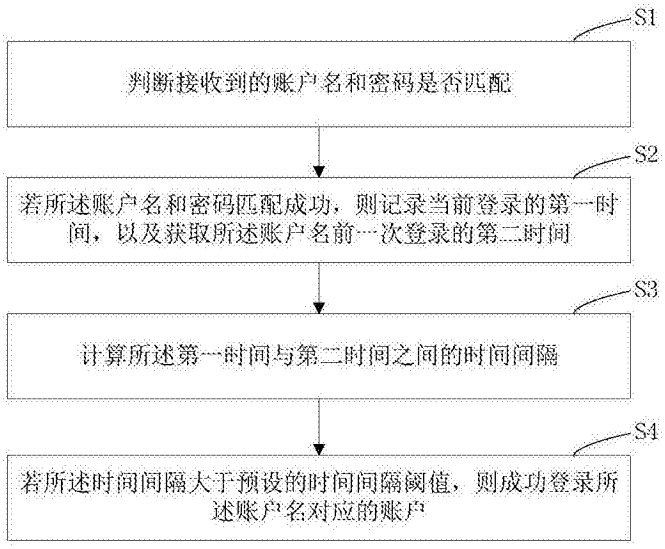

S1
判断接收到的账户名和密码是否匹配
S2
若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间
S3
计算所述第一时间与第二时间之间的时间间隔
S4
若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户

图1

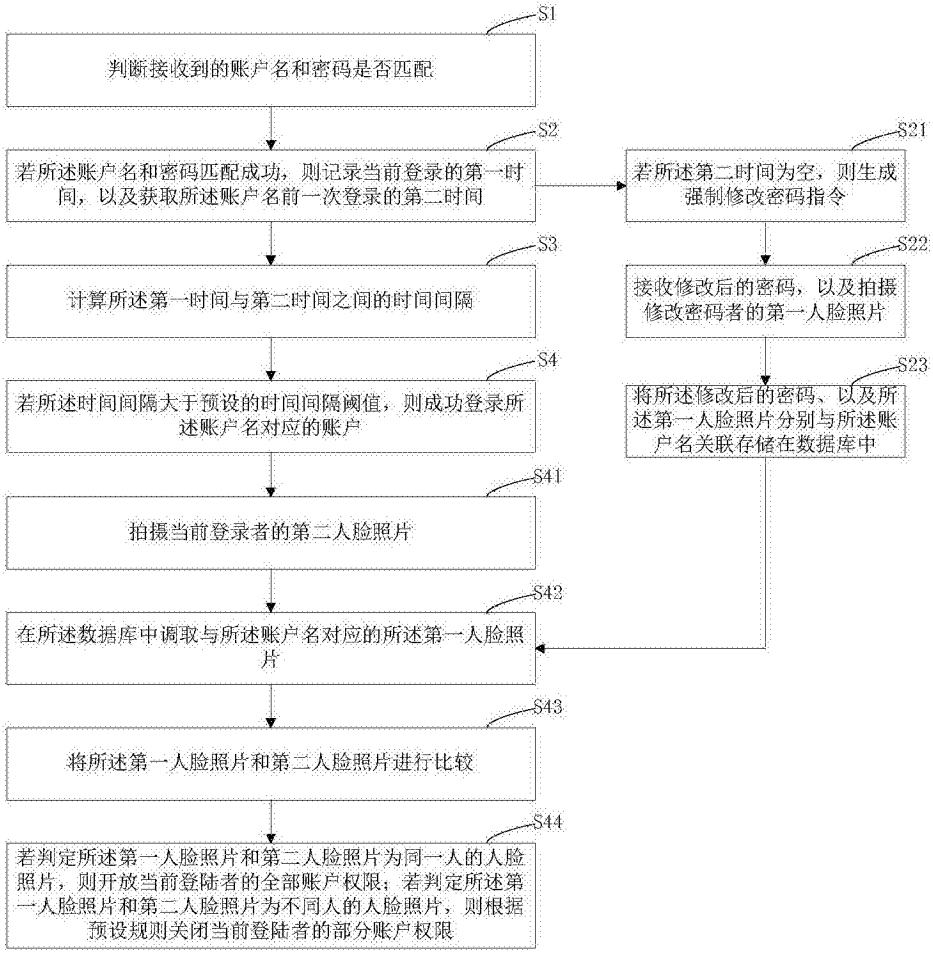

S1
判断接收到的账户名和密码是否匹配
S2
若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间
S21
若所述第二时间为空，则生成强制修改密码指令
S22
接收修改后的密码，以及拍摄修改密码者的第一人脸照片
S23
将所述修改后的密码、以及所述第一人脸照片分别与所述账户名关联存储在数据库中
S3
计算所述第一时间与第二时间之间的时间间隔
S4
若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户
S41
拍摄当前登录者的第二人脸照片
S42
在所述数据库中调取与所述账户名对应的所述第一人脸照片
S43
将所述第一人脸照片和第二人脸照片进行比较
S44
若判定所述第一人脸照片和第二人脸照片为同一人的人脸照片，则开放当前登陆者的全部账户权限；若判定所述第一人脸照片和第二人脸照片为不同人的人脸照片，则根据预设规则关闭当前登陆者的部分账户权限

图2

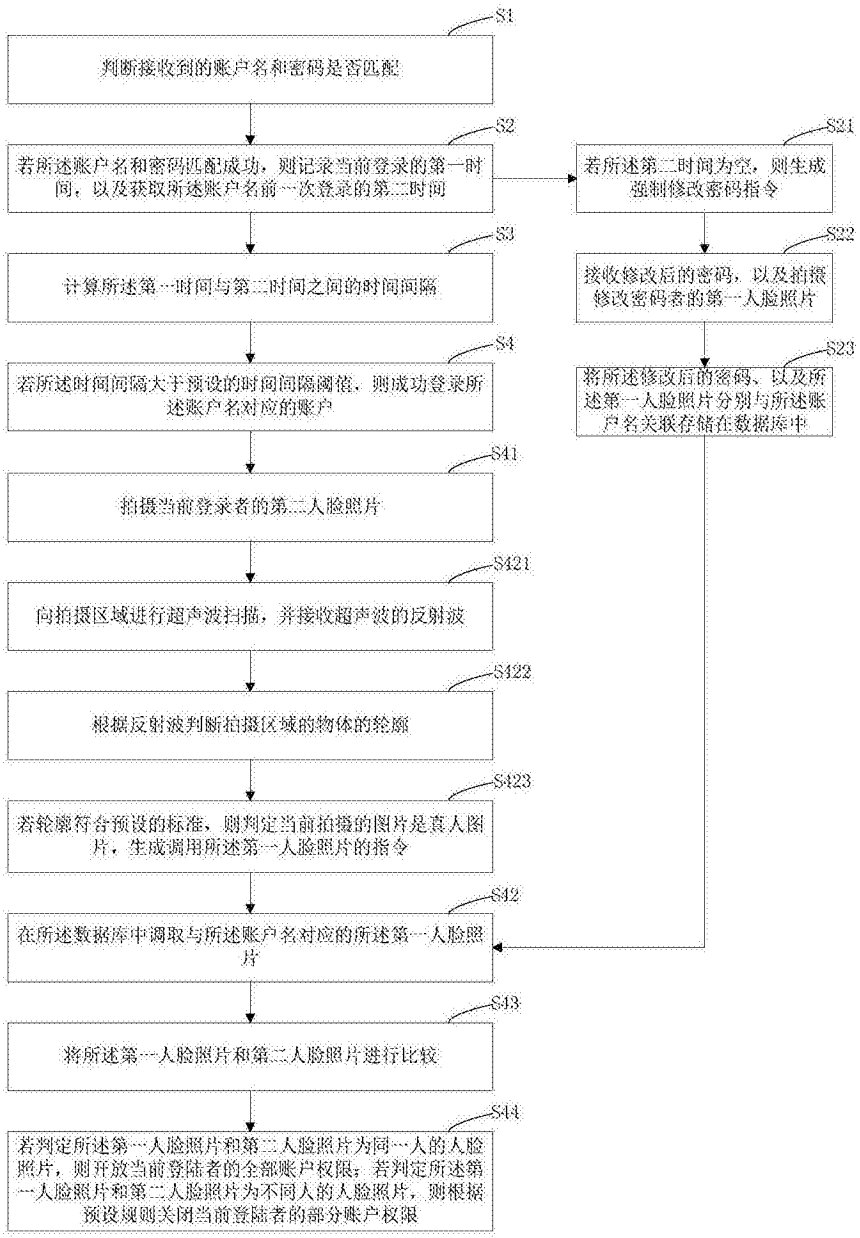

S1
判断接收到的账户名和密码是否匹配
S2
若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名前一次登录的第二时间
S21
若所述第二时间为空，则生成强制修改密码指令
S22
接收修改后的密码，以及拍摄修改密码者的第一人脸照片
S23
将所述修改后的密码、以及所述第一人脸照片分别与所述账户名关联存储在数据库中
S3
计算所述第一时间与第二时间之间的时间间隔
S4
若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户
S41
拍摄当前登录者的第二人脸照片
S421
向拍摄区域进行超声波扫描，并接收超声波的反射波
S422
根据反射波判断拍摄区域的物体的轮廓
S423
若轮廓符合预设的标准，则判定当前拍摄的图片是真人图片，生成调用所述第一人脸照片的指令
S42
在所述数据库中调取与所述账户名对应的所述第一人脸照片
S43
将所述第一人脸照片和第二人脸照片进行比较
S44
若判定所述第一人脸照片和第二人脸照片为同一人的人脸照片，则开放当前登陆者的全部账户权限；若判定所述第一人脸照片和第二人脸照片为不同人的人脸照片，则根据预设规则关闭当前登陆者的部分账户权限

图3

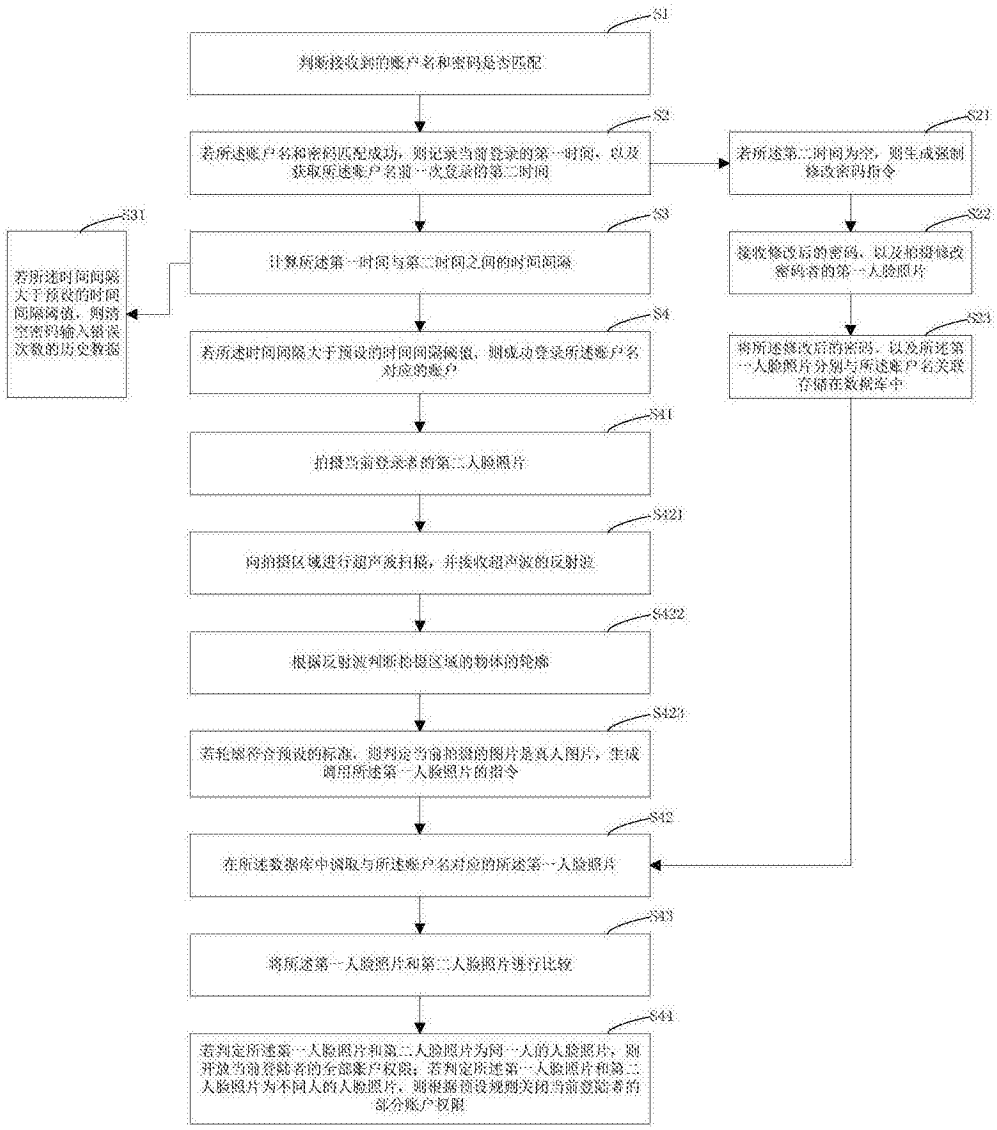

S1
判断接收到的账户名和密码是否匹配
S2
若所述账户名和密码匹配成功，则记录当前登录的第一时间，以及获取所述账户名第一次登录的第二时间
S21
若所述第二时间为空，则生成强制修改密码指令
S22
接收修改后的密码，以及拍摄修改密码者的第一人脸照片
S23
将所述修改后的密码，以及所述第一人脸照片分别与所述账户名关联存储在数据库中
S3
计算所述第一时间与第二时间之间的时间间隔
S31
若所述时间间隔大于预设的时间间隔阈值，则将登录密码输入错误次数的历史数据
S4
若所述时间间隔大于预设的时间间隔阈值，则成功登录所述账户名对应的账户
S41
拍摄当前登录者的第二人脸照片
S421
向拍摄区域进行超声波扫描，并接收超声波的反射波
S422
根据反射波判断拍摄区域的物体的轮廓
S423
若轮廓符合预设的标准，则判定当前拍摄的图片是真人图片，生成调用所述第一人脸照片的指令
S42
在所述数据库中调取与所述账户名对应的所述第一人脸照片
S43
将所述第一人脸照片和第二人脸照片进行比较
S44
若判定所述第一人脸照片和第二人脸照片为同一人的人脸照片，则开放当前登录者的全部账户权限；若判定所述第一人脸照片和第二人脸照片为不同人的人脸照片，则根据预设规则关闭当前登录者的部分账户权限

图4

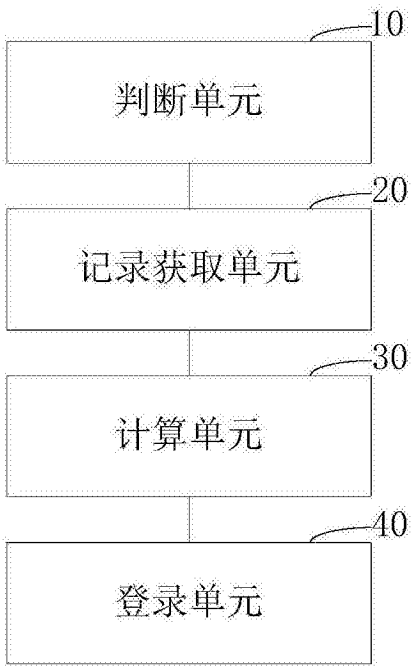


图5


10
判断单元
20
记录获取单元
21
生成单元
30
计算单元
22
修改拍照单元
40
登录单元
23
关联存储单元
41
拍摄单元
42
调取单元
43
比较单元
44
权限管理单元

图6

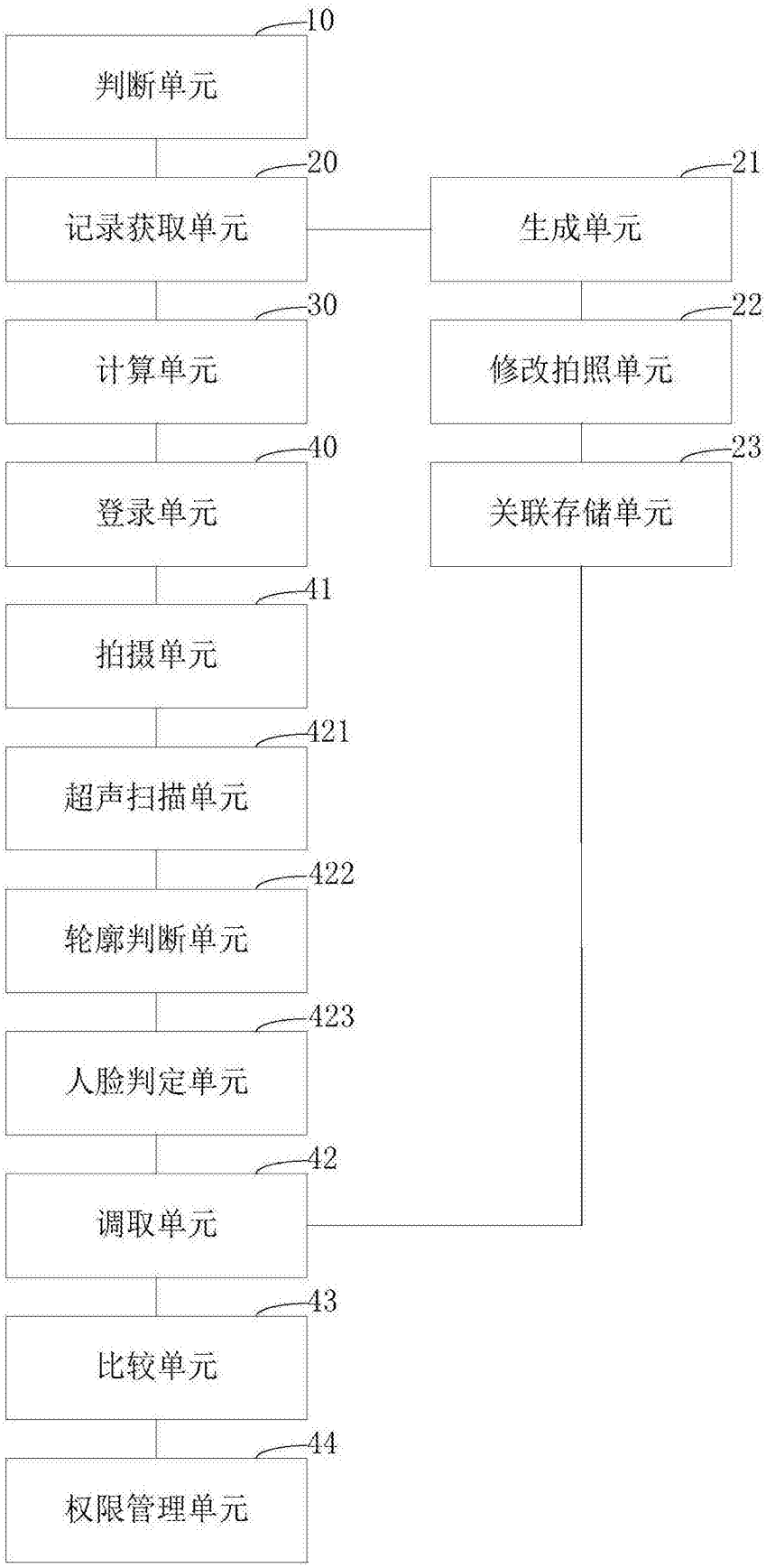

10
判断单元
20
记录获取单元
21
生成单元
30
计算单元
22
修改拍照单元
40
登录单元
23
关联存储单元
41
拍摄单元
421
超声扫描单元
422
轮廓判断单元
423
人脸判定单元
42
调取单元
43
比较单元
44
权限管理单元

图7

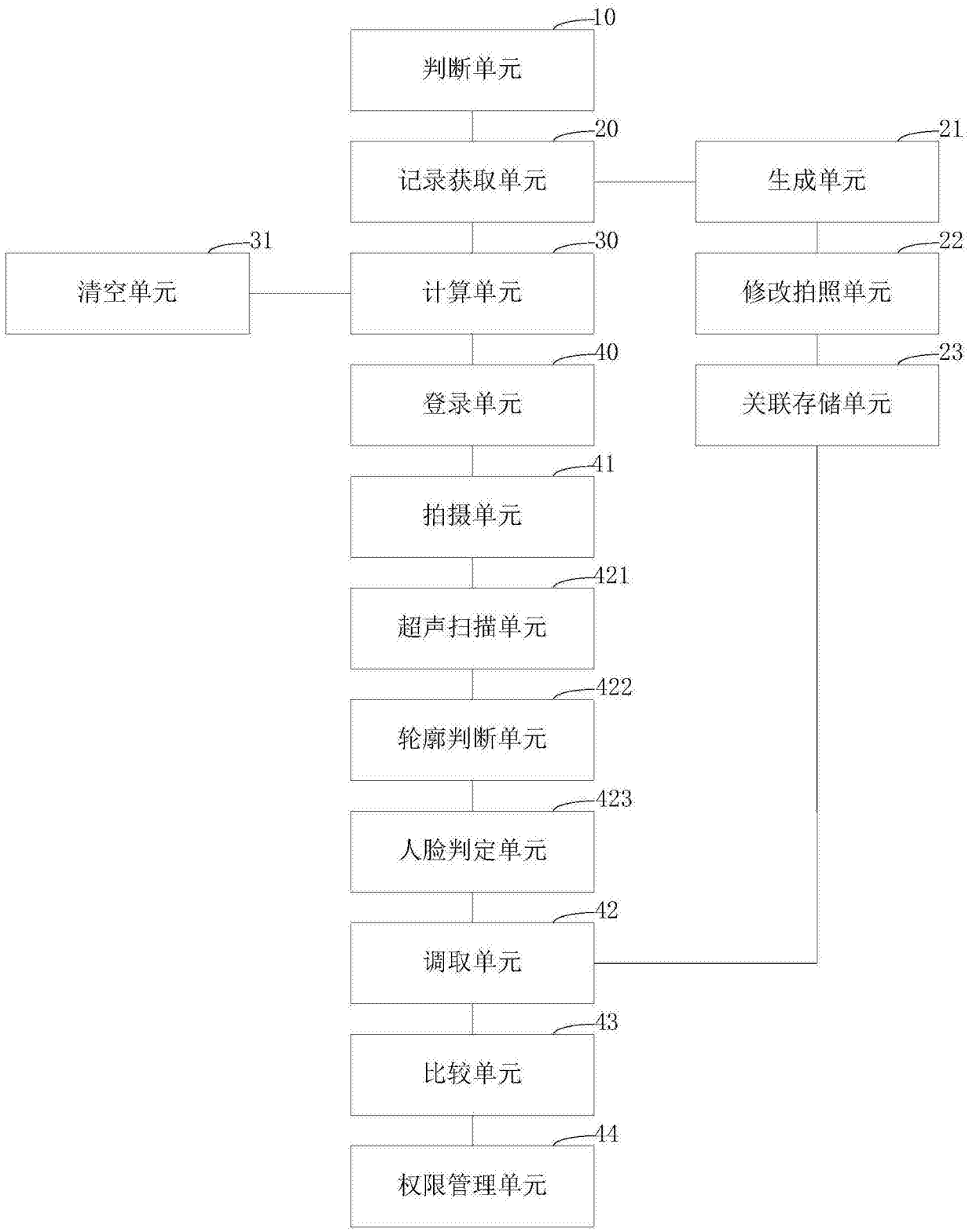

10
判断单元
20
记录获取单元
21
生成单元
31
清空单元
30
计算单元
22
修改拍照单元
40
登录单元
23
关联存储单元
41
拍摄单元
421
超声扫描单元
422
轮廓判断单元
423
人脸判定单元
42
调取单元
43
比较单元
44
权限管理单元

图8

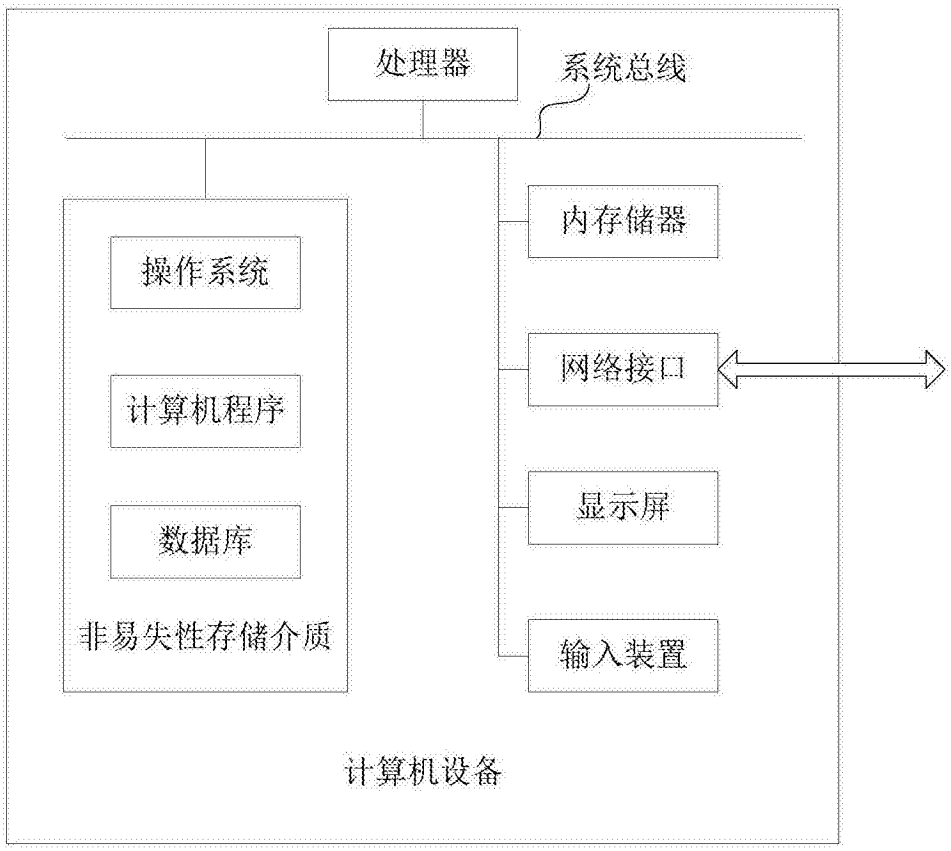


图9