

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 11 月 14 日 (14.11.2019)



(10) 国际公布号
WO 2019/214030 A1

(51) 国际专利分类号:
G06F 21/31 (2013.01)

(21) 国际申请号: PCT/CN2018/094413

(22) 国际申请日: 2018 年 7 月 4 日 (04.07.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810439259.4 2018 年 5 月 9 日 (09.05.2018) CN

(71) 申请人: 平安科技 (深圳) 有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN];
中国广东省深圳市福田区八卦岭八卦三路平安大厦 6 楼, Guangdong 518000 (CN)。

(72) 发明人: 白益仲 (BAI, Yizhong); 中国广东省深圳市福田区八卦岭八卦三路平安大厦 6 楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳众鼎专利商标代理事务所 (普通合伙) (SHENZHEN ZHONGDING INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市龙岗区龙城街道中心城清林路 546 号城投商务中心 4 层/B, Guangdong 518172 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: METHOD AND APPARATUS FOR UNLOCKING MULTIPLE APPLICATIONS USING SHARED PASSWORD, DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 多应用程序共享密码解锁方法、装置、设备及存储介质

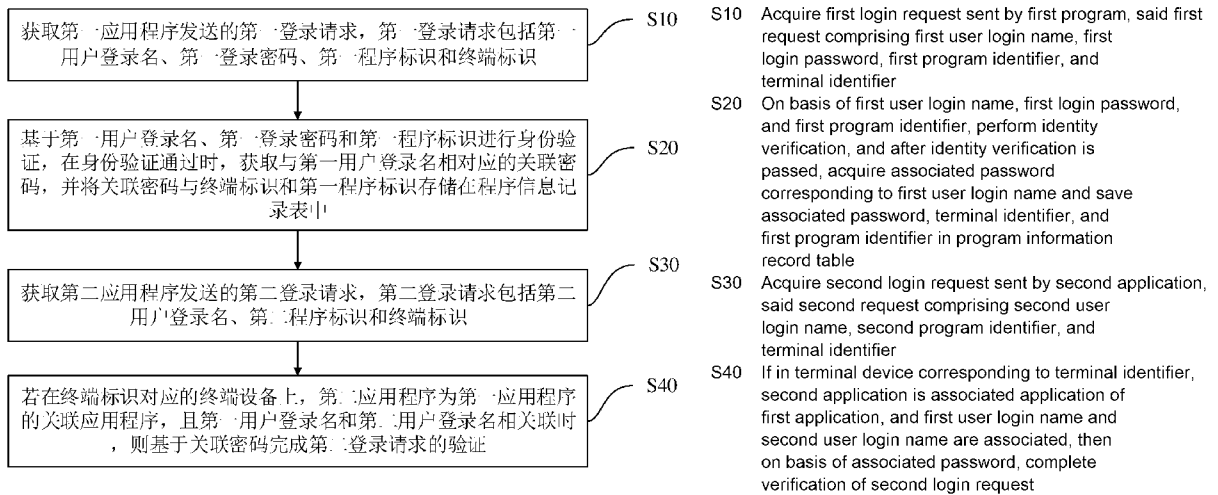


图 1

(57) Abstract: Disclosed in the present application are a method and apparatus for unlocking multiple applications using a shared password, and a device and a storage medium. The method comprises: on the basis of a first user login name, a first login password, and a first program identifier, performing identity verification, and after the identity verification is passed, acquiring an associated password corresponding to the first user login name and saving the associated password, a terminal identifier, and the first program identifier in a program information record table; acquiring a second login request sent by a second application, the second login request comprising a second user login name, a second program identifier, and the terminal identifier; if in the terminal device corresponding to the terminal identifier, the second application is an associated application of the first application, and the first user login name and the second user login name are associated, then on the basis of the associated password, completing verification of the second login request. The present method is able to realize rapid application login, reducing the time required for a user to log in to an application,

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国(除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告(条约第21条(3))。

while ensuring the security thereof.

(57) 摘要: 本申请公开一种多应用程序共享密码解锁方法、装置、设备及存储介质。该方法包括: 基于第一用户登录名、第一登录密码和第一程序标识进行身份验证, 在身份验证通过时, 获取与第一用户登录名相对应的关联密码, 并将关联密码与终端标识和第一程序标识存储在程序信息记录表中; 获取第二应用程序发送的第二登录请求, 第二登录请求包括第二用户登录名、第二程序标识和终端标识; 若在终端标识对应的终端设备上, 第二应用程序为第一应用程序的关联应用程序, 且第一用户登录名和第二用户登录名相关联时, 则基于关联密码完成第二登录请求的验证。该方法可实现应用程序的快捷登录, 节省用户登录多应用程序的登录时间, 同时保证了用户登录应用程序的安全性。

多应用程序共享密码解锁方法、装置、设备及存储介质

本申请以 2018 年 5 月 9 日提交的申请号为 201810439259.4，名称为“多应用程序共享密码解锁方法、装置、设备及存储介质”的中国发明专利申请为基础，并要求其优先权。

技术领域

本申请涉及移动终端领域，尤其涉及一种多应用程序共享密码解锁方法、装置、设备及存储介质。

背景技术

现有的应用程序解锁仅能实现一个应用程序或者平台的登录，当用户使用多个应用程序时需要不同的应用程序进行不同的密码设置，会导致设置的密码过多，出现用户记混密码的情况，从而使得用户无法快捷地登录相应的应用程序。当用户对多个应用程序设置同样的登录密码时，若一个应用程序的登录密码泄露，其他应用程序的登录密码也会泄露，存在安全隐患。同时，在第二个应用程序登录时，可以采用手势密码解锁应用程序，此时，若手势密码设置的比较简单，使得手势密码输入过程中，其手势动作泄露该手势密码，使得该手势密码安全性不高；若手势密码设置的比较复杂时，势必会增加用户操作复杂度，给用户造成不便。

发明内容

本申请实施例提供一种多应用程序共享密码解锁方法、装置、设备及存储介质，以解决用户对多个应用程序设置不同的登录密码时出现登录密码记混的问题，同时解决登录密码复杂、安全性不高的问题。

第一方面，本申请实施例提供一种多应用程序共享密码解锁方法，包括：

获取第一应用程序发送的第一登录请求，所述第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识；

基于所述第一用户登录名、所述第一登录密码和第一程序标识进行身份验证，在身份验证通过时，获取与所述第一用户登录名相对应的关联密码，并将所述关联密码与所述终端标识和所述第一程序标识存储在程序信息记录表中；

获取第二应用程序发送的第二登录请求，所述第二登录请求包括第二用户登录名、第二程序标识和所述终端标识；

若在所述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证。

第二方面，本申请实施例提供一种多应用程序共享密码解锁装置，包括：

第一登录请求获取模块，用于获取第一应用程序发送的第一登录请求，所述第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识；

关联密码获取模块，用于基于所述第一用户登录名、所述第一登录密码和第一程序标

识进行身份验证，在身份验证通过时，获取与所述第一用户登录名相对应的关联密码，并将所述关联密码与所述终端标识和所述第一程序标识存储在程序信息记录表中；

第二登录请求获取模块，用于获取第二应用程序发送的第二登录请求，所述第二登录请求包括第二用户登录名、第二程序标识和所述终端标识；

第二登录请求验证模块，用于若在上述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证。

第三方面，本申请实施例提供一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

获取第一应用程序发送的第一登录请求，所述第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识；

基于所述第一用户登录名、所述第一登录密码和第一程序标识进行身份验证，在身份验证通过时，获取与所述第一用户登录名相对应的关联密码，并将所述关联密码与所述终端标识和所述第一程序标识存储在程序信息记录表中；

获取第二应用程序发送的第二登录请求，所述第二登录请求包括第二用户登录名、第二程序标识和所述终端标识；

若在上述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证。

第四方面，本申请实施例提供一个或多个存储有计算机可读指令的非易失性可读存储介质，其特征在于，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器实现如下步骤：

获取第一应用程序发送的第一登录请求，所述第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识；

基于所述第一用户登录名、所述第一登录密码和第一程序标识进行身份验证，在身份验证通过时，获取与所述第一用户登录名相对应的关联密码，并将所述关联密码与所述终端标识和所述第一程序标识存储在程序信息记录表中；

获取第二应用程序发送的第二登录请求，所述第二登录请求包括第二用户登录名、第二程序标识和所述终端标识；

若在上述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证。

本申请的一个或多个实施例的细节在下面的附图及描述中提出。本申请的其他特征和优点将从说明书、附图以及权利要求书变得明显。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例的描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 是本申请实施例 1 中多应用程序共享密码解锁方法的一流程图；

图 2 是本申请实施例 1 中多应用程序共享密码解锁方法的另一流程图；

图 3 是本申请实施例 1 中多应用程序共享密码解锁方法的又一流程图；

图 4 是图 1 中步骤 S40 的一具体流程图；

图 5 是本申请实施例 2 中多应用程序共享密码解锁装置的一原理框图；

图 6 是本申请实施例 4 中计算机设备的一示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

实施例 1

图 1 示出本实施例中多应用程序共享密码解锁方法的流程图。该多应用程序共享密码解锁方法应用在同一终端设备上登录多个关联应用程序时，多个关联应用程序可以使用一个登录密码完成登录验证过程，从而实现关联应用程序基于一个登录密码完成登录验证的目的。该多应用程序共享密码解锁方法可应用在电脑、智能手机和平板等终端设备上，用于对同一终端设备上的多个关联应用程序通过共享密码进行登录。如图 1 所示，多应用程序共享密码解锁方法包括如下步骤：

S10：获取第一应用程序发送的第一登录请求，第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识。

第一应用程序是安装在终端设备上的一个应用程序。第一登录请求是指登录第一应用程序的请求。在与终端设备通过网络相连的第一服务器获取第一应用程序发送的第一登录请求时，该登录请求还携带有第一用户登录名、第一登录密码、第一程序标识和终端标识。其中，第一服务器是指第一应用程序对应的服务器。第一用户登录名是指登录第一应用程序的用户登录名。第一登录密码是指登录第一应用程序的与第一用户登录名相对应的登录密码。第一程序标识是指用于识别第一应用程序对应的标识，该第一程序标识可以唯一识别出第一应用程序。终端标识是指登录第一应用程序的终端设备的标识，该终端标识包括但不限于移动终端的 IMEI 码(International Mobile Equipment Identity, 国际移动终端设备身份标识)和 SN (Serial Number, 序列号)。

其中，IMEI 码存储在智能手机和平板等终端设备中，一个移动终端设备对应一个 IMEI 码，该 IMEI 码可用于唯一识别移动终端设备。SN 码是产品序列号，用于验证产品的合法身份，一套正版的产品只对应一组产品序列号。用户在移动终端设备上下载应用程序时，

应用程序对应的第一服务器会获取移动终端设备对应的 IMEI 码和 SN 码。

S20: 基于第一用户登录名、第一登录密码和第一程序标识进行身份验证, 在身份验证通过时, 获取与第一用户登录名相对应的关联密码, 并将关联密码与终端标识和第一程序标识存储在程序信息记录表中。

具体地, 当用户在登陆第一应用程序时, 与第一应用程序对应的第一服务器基于第一用户登录名、第一登录密码和第一程序标识进行对用户进行身份验证, 若第一用户登录名、第一登录密码和第一程序标识与第一服务器存储的信息一致时, 则对该用户的身份验证通过。例如, 第一服务器可以先基于第一程序标识确定发送该第一登录请求的第一应用程序, 然后, 查询第一应用程序中所有的用户信息是否存在与第一用户登录名和第一登录密码相匹配的用户信息, 若存在, 则身份验证通过。

在用户的身份验证通过时, 与第一应用程序对应的第一服务器获取一个与第一用户登录名相对应的关联密码。其中, 关联密码是指第一应用程序和其他关联应用程序可以共享同一个密码进行登录的密码。关联应用程序是指预先存储的与第一应用程序相关联的应用程序, 该关联应用程序是由开发商定义的, 可以是同一公司下开发的不同的应用程序。例如, 平安集团开发的车险 APP、寿险 APP 和理财 APP 等属于相互关联的应用程序, 若本实施例中的第一应用程序为车险 APP, 则其关联应用程序为寿险 APP、理财 APP 或者平安集团开发的其他 APP。关联密码具体是指第一应用程序进行身份验证通过后, 在同一终端设备上安装的关联应用程序可以共享的密码。

该关联密码是服务器随机生成的一个密码。在第一服务器获取关联密码后, 第一服务器将关联密码与终端标识和第一程序标识存储在程序信息记录表中。其中, 程序信息记录表是用于记录应用程序信息的表, 包括记录应用程序的下载情况和关联密码。记录应用程序的下载情况包括记录应用程序的第一程序标识、终端标识和下载时间等情况。

将第一应用程序的关联密码、终端标识和第一程序标识存储在程序信息记录表中, 便于后续识别第二应用程序是否为第一应用程序的关联应用程序并完成第二应用程序的第二登录请求的验证。

S30: 获取第二应用程序发送的第二登录请求, 第二登录请求包括第二用户登录名、第二程序标识和终端标识。

第二应用程序是指在同一终端标识对应的终端设备上登录的不属于第一应用程序的应用程序。第二登录请求是指第二应用程序的登录请求。与第二应用程序关联的第二服务器获取第二应用程序发送的第二登录请求, 该登录请求携带有第二用户登录名、第二程序标识和终端标识。其中, 第二服务器是指第二应用程序对应的服务器。第二用户登录名是指第二应用程序对应的用户登录名。第二程序标识是指第二应用程序对应的程序标识, 用于唯一识别第二应用程序。

本实施例中, 若第一应用程序和第二应用程序在开发时, 是同一集团、企业或者开发者开发的关联应用程序, 且第一应用程序和第二应用程序共用一个服务器时, 第一服务器和第二服务器为同一服务器。若第一应用程序和第二应用程序在开发时, 虽然是同一集团、

企业或者开发者开发的关联应用程序，但是第一应用程序和第二应用程序没有共用一个服务器，则需要设置一个关联服务器实现第一服务器和第二服务器之间的信息交互。其中，关联服务器是指是指用于实现第一服务器和第二服务器之间信息交互的服务器，关联服务器与第一服务器和第二服务器相连。

S40:若在终端标识对应的终端设备上，第二应用程序为第一应用程序的关联应用程序，且第一用户登录名和第二用户登录名相关联时，则基于关联密码完成第二登录请求的验证。

第二服务器在获取第二登录请求时，则基于第二登录请求中的第二程序标识查询预先存储的关联应用程序信息表，以确保第二应用程序是否为第一应用程序的关联应用程序。其中，关联应用程序信息表是指用于记录第一应用程序和第二应用程序之间是否存在关联关系的表。在关联应用程序信息表中，每一组关联应用程序信息包括存在关联关系的至少两个程序标识。

本实施例中，当第一服务器和第二服务器为同一个服务器时，关联应用程序信息表存储在该服务器中；当第一服务器和第二服务器不属于同一个服务器时，则关联应用程序表存储在关联服务器中。将关联应用程序信息表存储在关联服务器中，便于对关联应用程序信息表中的数据进行集中管理，避免每个应用程序对应的服务器中都存储一份关联应用程序信息表。根据关联应用程序信息表，可以确定第一程序标识和第二程序标识对应的第一应用程序和第二应用程序是否为关联应用程序。

若确定第二应用程序是第一应用程序的关联应用程序时，则基于预先设置的关联用户名信息表查询用户登录名和第二用户登录名是否关联，在确定第一用户登录名和第二用户登录名相关联时，则将程序信息记录表中关联密码发送给终端标识对应的终端设备。关联用户名信息表是指用于记录用户登录名是否存在关联关系的表。如任一用户预先在车险APP、寿险APP和理财APP上采用各自的用户登录名和登录密码进行登录时，需将所有关联应用程序对应的用户登录名和登录密码存储在关联用户名信息表上，以便在获取第二登录请求的第二用户登录名后，根据该第二用户登录名查询关联用户名信息表，以确定第二用户登录名和第一用户登录名是否相关联。

本实施例中，当第一服务器和第二服务器为同一个服务器时，关联用户名信息表存储在该服务器中；当第一服务器和第二服务器不属于同一个服务器时，则关联应用程序表存储在关联服务器中。将关联用户名信息表存储在关联服务器中，便于对关联用户名信息表中的数据进行集中管理，避免每个应用程序对应的服务器中都存储一份关联用户名信息表。判断第一用户登录名和第二用户登录名的关联性可以确定用户的登录身份，避免不同用户在同一台终端设备登录第二应用程序和第一应用程序，也可获取该关联密码，保证用户的登录安全 and 信息安全。

进一步地，该多应用程序共享密码解锁方法还包括：设置关联密码的有效时间。有效时间是指将关联密码发送给终端标识对应的终端设备后，用于验证关联密码有效的时间，设置关联密码的有效时间可以进一步保障用户的信息安全性。在规定的有效时间内，第二

应用程序对应的服务器获取到终端标识对应的终端设备发送的关联密码后，通过第二登录请求的验证。将关联密码发送给终端标识对应的终端设备，便于用户基于获取的关联密码进行第二应用程序的登录，简化验证的过程，保障用户登录第二应用程序的安全性。

在第二服务器获取第二应用程序的第二登录请求后，第二服务器需将第二登录请求携带的终端标识与存储在第一服务器中的程序信息记录表进行对比，判断第二应用程序的终端标识是否与第一应用程序对应的终端标识一致，若一致，则第二服务器将第二登录请求携带的第二程序标识和第二用户登录名与关联应用程序信息表和关联用户名信息表进行查询比较，当确定第二应用程序为第一应用程序的关联应用程序，且第二用户登录名与第一用户登录名相关联时，第二服务器将关联密码发送给终端标识对应的终端设备。可以理解地，当第一服务器与第二服务器属于同一服务器时，则该服务器将存储在程序信息记录表中的关联密码发送给终端标识对应的终端设备。当第一服务器与第二服务器不属于同一个服务器时，则关联服务器获取第一服务器中存储的关联密码，并发送给第二服务器。在发送关联密码给第二服务器时，该关联密码都会有一对应的有效时间，因此，在发送关联密码时，也会将有效时间发送给第二服务器，第二服务器在规定的有效时间内获取到终端设备发送的关联密码，则第二登录请求的验证通过。

通过判断第二应用程序是否为第一应用程序的关联应用程序，同时判断第二用户登录名和第一用户登录名是否关联，当确定第二应用程序是第一应用程序的关联应用程序并且确定第二用户登录名和第一用户登录名相关联时，则第二登录请求基于获取的关联密码进行第二登录请求的验证。具体地，由于预先配置了关联密码的有效时间，并将关联密码发送给终端标识对应的终端设备后，若在预设时间内用户在关联应用程序上输入第二用户登录名和该关联密码，即可完成第二用户登录名对应的第二登录请求的验证。

该多应用程序共享密码解锁方法实现了多个应用程序只需一个登录密码和关联密码就可以使用户完成在同一终端设备上安装的多个应用程序的登录，解决了多个应用程序设置多个登录密码容易混淆的问题。同时，解决用户对多个应用程序设置同样的登录密码时，若一个应用程序的登录密码泄露，其他应用程序的登录密码也会泄露的安全隐患问题，保证了用户登录应用程序的安全性。

在一具体实施方式中，多应用程序共享密码解锁方法还包括：在登录密码设置界面上配置与第一用户登录名相对应的第一登录密码，第一登录密码包括手势密码。

具体地，登录密码设置界面是指用于设置登录密码的界面。若用户没有注册第一应用程序的第一用户登录名和第一登录密码时，第一应用程序会要求用户进入登录密码设置界面，用户在登录密码设置界面上注册第一用户登录名，同时设置与第一用户登录名相对应的第一登录密码。

第一登录密码包括手势密码，手势密码的设置规则是指基于预先设定的一特定图案的坐标，验证目标图案的坐标是否符合预先设置的匹配规则的一种验证方式。其中，目标图案是指用户选择的用于解锁第一登录密码的图案。预先设置的匹配规则是指用于验证目标图案的位置坐标和初始位置是否匹配的规则。

本实施例中的手势密码包括图片底层、动态坐标层和活动图层。

具体地，该手势密码具体包括三个层，第一层为图片底层，第二层为动态坐标层，第三层是活动图层。其中，图片底层是指用户在手势密码设置界面设置手势密码时，预先选取的含有特定图案的图片层。该特定图案包括有特殊形状的图案，比如纽扣和盘子等，用来帮助用户记忆。动态坐标层是指用于定位第三层活动图层的位置的坐标层，该动态坐标层的坐标是可移动的坐标。活动图层是指用户选取的目标图案所在的图层，活动图层包括圆形轮廓和字符图案等。其中，每个字符图案都位于一圆形轮廓中，该活动图层的字符图案在终端设备屏幕中是可以被全屏拖动的，圆形轮廓的位置坐标由动态坐标层进行定位。

在一具体实施方式中，如图2所示，在登录密码设置界面上配置与第一用户登录名相对应的第一登录密码，具体包括如下步骤：

S51：在图片底层中获取手势密码的初始位置。

初始位置是指在图片底层上选择的特定图案的位置。在设置手势密码时，应先在图片底层任意选择一个特定图案，并确定该特定图案的初始位置。

具体地，在图片底层确定手势密码的初始位置是通过图片底层中选取的特定图案的位置确定的。为了方便地确定特定图案的位置，对图片底层的每一特定图案都会设置一特定的圆形轮廓，通过圆形轮廓的形状和半径大小来确定手势密码的初始位置。圆形轮廓相比于其它形状的轮廓可以更好更完整地反映特定图案的大小，更容易通过圆心确定特定图案的位置。

S52：获取活动图层中的目标图案的位置坐标。

具体地，当确定了手势密码的初始位置后，还需要在活动图层选取目标图案并确定目标图案的位置坐标。该目标图案是用户根据个人喜好选择的图案。其中，目标图案的位置坐标可通过动态坐标层获取。当用户在活动图层上选取了目标图案后，动态坐标层则会基于直角坐标系确定目标图案的位置。

活动图层的字符图案包括但不限于中文大写数字、中文小写数字、阿拉伯数字、生肖和天干地支（十天干、十二地支）等字符图案。具体地，目标字符图案的位置坐标也是通过其对应的圆形轮廓确定的。

S53：基于动态坐标层，判断目标图案的位置坐标与手势密码的初始位置是否符合预先设置的匹配规则；若符合，则与第一用户登录名对应的第一登录密码设置成功。

具体地，在确定手势密码的初始位置后需要对选取的目标图案进行测试验证。该测试验证是指对活动图层上的目标图案的位置坐标和初始位置进行测试验证的过程。若符合匹配规则，则验证成功，第一用户登录名对应的第一登录密码设置成功。匹配规则的验证标准具体为：当目标图案对应的圆形轮廓的圆心坐标和初始位置的某一特定图案的圆心坐标距离小于等于预设值（如预设半径的0.15倍）时，则验证通过。其中，预设半径是指圆形轮廓的半径大小，可以理解地，0.15倍还可以是其他具体数值。

本实施例中的关联密码也可以指手势密码，该关联密码为在系统每次随机分配一定数量的字符图案中选取的与目标图案一致的图案。当用户在登录第二应用程序时，服务器会

给终端标识对应的终端设备上发送一定数量的字符图案，用户需要在终端设备上的多个字符图案中选取与目标图案一致图案，然后移动该目标图案，使得目标图案的位置坐标和初始位置符合预先设置的匹配规则的验证标准，当符合匹配规则的验证标准，则第二应用程序对应的第二登录请求验证成功。

进一步地，在移动活动图层上的目标图案时，目标图案不能单独进行移动，因此，对目标图案进行验证时，需要对活动图层整体进行移动，然后通过计算目标图案的位置坐标与初始位置的坐标是否符合匹配规则的验证标准，若符合匹配规则的验证标准，则第二应用程序对应的第二登录请求验证成功。由于活动图层必须依赖于动态坐标层确定目标图案的位置坐标，而动态坐标层只有一个坐标系，因此，在移动目标图案时，对应的活动图层整体移动，方便基于动态坐标层获取目标图案的位置坐标，用于验证目标图案的位置坐标是否符合匹配规则的验证标准。

通过判断目标图案的位置坐标与手势密码的初始位置是否符合预先设置的匹配规则实现登录密码的设置，若符合匹配规则，则登录应用程序通过。采用该方案实现对应用程序的解锁。使用目标图案完成手势密码的验证，降低了应用程序解锁的操作复杂度。同时，由于目标图案位置的不确定性，提高了手势密码解锁的安全性。

在一具体实施方式中，如图 3 所示，在步骤 S20，获取与第一用户登录名相对应的关联密码的步骤之后，该多应用程序共享密码解锁方法还包括如下步骤：

S21：设置关联密码的有效时间。

若第一应用程序和第二应用程序对应的第一服务器和第二服务器属于同一个服务器时，服务器在获取与第一用户登录名相对应的关联密码后，会对该关联密码设置一个有效时间，用于验证终端设备发送关联密码给服务器的时间是否在有效时间内。

若第一应用程序和第二应用程序对应的第一服务器和第二服务器不属于同一个服务器时，则关联服务器在获取关联密码后会对该关联密码设置一个有效时间用于验证终端设备发送关联密码给服务器的时间是否在有效时间内。

本实施例中的关联密码设置有至少 6 位字符，该字符可以包括阿拉伯数字和/或英文字母随机组合形成的字符串。有效时间设置为 30s，基于这种设置，由于 6 位阿拉伯数字和英文字母的穷举次数在 30s 内是不可能穷举完全的，因此，将关联密码设置为至少 6 位英文字母和/或阿拉伯数字组合的字符串，并对关联密码设置有效时间，可以加大关联密码被破解的难度，提高关联密码验证的安全性。

在步骤 S30，获取第二应用程序发送的第二登录请求的步骤之后，该多应用程序共享密码解锁方法还包括如下步骤：

S22：若第二登录请求的获取时间在有效时间内，则执行基于关联密码完成第二登录请求的验证的步骤。

当第一应用程序和第二应用程序对应的第一服务器和第二服务器属于同一个服务器时，第二登录请求的终端设备在有效时间内，将获取到的关联密码发送给对应的服务器时，服务器会执行基于关联密码完成第二登陆请求的验证的步骤。

当第一应用程序和第二应用程序对应的第一服务器和第二服务器不属于同一个服务器时，关联服务器会将从第一服务器获取到的关联密码和有效时间发送给第二登录请求携带的终端标识的终端设备，同时关联服务器将终端标识和有效时间发送给第二服务器。第二服务器在规定的有效时间内，获取到终端标识对应的终端设备发送的关联密码后，第二服务器执行基于关联密码完成第二登录请求的验证的步骤。

关联密码在有效时间内验证成功后，执行基于关联密码完成第二登录请求的验证的步骤，保证了第二登录请求验证通过的安全性。

S23：若第二登录请求的获取时间超过有效时间，则需要重新执行获取第一应用程序发送的第一登录请求的步骤。

具体地，若第二登录请求的获取时间超过有效时间，则说明基于关联密码对第二登录请求的验证超过了有效时间时，此时，该关联密码失效，无法基于该关联密码对第二登录请求进行验证，因此需要用户重新发送第一登录请求，并在第一登录请求验证通过时，获取关联密码，然后验证第二登录请求中的第二程序标识是否与第一程序标识关联，第一用户登录名是否与第二用户登录名关联。

步骤 S21-S23，通过对关联密码设置有效时间，在有效时间内则执行基于关联密码完成第二登录请求的验证；在超过有效时间，则重新执行获取第一登录请求的步骤，提高了通过关联密码验证第二登录请求的安全性。

在一具体实施方式中，如图 4 所示，步骤 S40，若在终端标识对应的终端设备上，第二应用程序为第一应用程序的关联应用程序，且第一用户登录名和第二用户登录名相关联时，则基于关联密码完成第二登录请求的验证，具体包括如下步骤：

S41：根据第二登录请求中的终端标识，查询程序信息记录表中是否存在与终端标识对应的第一程序标识。

具体地，若第一应用程序和第二应用程序对应的第一服务器和第二服务器属于同一个服务器时，服务器在获取第二登录请求携带的终端标识后，服务器会基于终端标识查询预先存储在服务器中的程序信息记录表，确定该终端标识在程序信息记录表中是否存在与第二程序标识对应的第一程序标识，表示第一应用程序的第一登录请求和第二应用程序的第二登录请求是在同一终端设备上登录的。

若第一应用程序和第二应用程序对应的第一服务器和第二服务器不属于同一个服务器时，第二服务器会将获取的终端标识和第一服务器中存储的终端标识进行比较，若第一服务器中存在有与第二登录请求的终端标识一致的终端标识，则确定第一应用程序的第一登录请求和第二应用程序的第二登录请求是在同一终端设备上登录的。

S42：若存在与终端标识对应的第一程序标识，则基于第二登录请求中的第二程序标识和第一程序标识，查询预先设置的关联应用程序信息表，确定第二程序标识和第一程序标识是否关联。

在确定第一登录请求和第二登录请求来自于同一终端标识对应的终端设备后，则基于第一登录请求中携带的第一程序标识和第二登录请求携带的第二程序标识，查询预先设置

的关联应用程序信息表，确定第二程序标识与第一程序标识是否关联。

可以理解地，在第一应用程序和第二应用程序对应的第一服务器和第二服务器共用同一个服务器时，关联应用程序信息表存储在该服务器上；在第一应用程序和第二应用程序对应的第一服务器和第二服务器不共用一个服务器时，关联应用程序信息表存储在关联服务器上。将关联应用程序信息表存储在关联服务器上，可以避免当第一服务器和第二服务器不属于同一个服务器时，关联应用程序信息表需要在每个服务器上进行存储的问题，方便查询和获取。

S43：若第二程序标识和第一程序标识关联，则在终端标识对应的终端设备上，确定第二应用程序为第一应用程序的关联应用程序。

在基于关联应用程序信息表查询到第二程序标识和第一程序标识关联时，则可以确定第二程序标识对应的第二应用程序和第一程序标识对应的第一应用程序具有关联性，第二应用程序为第一应用程序的关联应用程序。

S44：基于第二登录请求中的第二用户登录名和第一用户登录名，查询预先设置的关联用户名信息表，确定第二用户登录名和第一用户登录名是否关联。

第一应用程序和第二应用程序对应的第一服务器和第二服务器属于同一个服务器时，关联用户名信息表存储在对应的服务器上；第一应用程序和第二应用程序对应的第一服务器和第二服务器不属于同一个服务器时，关联用户名信息表存储在关联服务器上。

具体地，在确定第二应用程序为第一应用程序的关联应用程序后，还需要查询预先设置的关联用户名信息表，确定第二用户登录名和第一用户登录名是否关联，避免不同的用户在同一终端设备上登录关联应用程序，使得用户登录应用程序的安全性受到威胁。

如在一终端设备上，不进行第二用户登录名和第一用户登录名是否关联的验证，则会出现用户 A 在该终端设备上登陆了第一应用程序，用户 B 在该终端设备上登录了第二应用程序，在第二应用程序和第一应用程序相互关联的情况下，该终端设备会收到一关联密码，若用户 B 输入关联密码进行第二登录请求的验证，则会导致用户 A 在第二应用程序中的信息泄露，使得用户 A 的第二应用程序出现登录安全不确定性，因此，在确定第二应用程序为第一应用程序的关联应用程序后，还需要查询预先设置的关联用户名信息表，确定第二用户登录名和第一用户登录名是否关联，才能发送关联密码给该终端设备，保证用户登录的安全性。

S45：若第二用户登录名和第一用户登录名相关联，则基于关联密码完成第二登录请求的验证。

在确定第二用户登录名和第一用户登录名关联，并且第一应用程序和第二应用程序对应的第一服务器和第二服务器属于同一个服务器后，服务器会基于程序信息记录表中的关联密码完成第二登录请求的验证。

在确定第二用户登录名和第一用户登录名关联，并且第一应用程序和第二应用程序对应的第一服务器和第二服务器不属于同一个服务器后，第二服务器会通过关联服务器，获取存储在第一服务器的关联密码，然后发送给终端标识对应的终端设备。终端设备在有效

时间内将关联密码发送给第二服务器完成第二登录请求的验证。

通过步骤 S41-S45 的验证过程,使得第二应用程序可以基于关联密码完成第二登录请求的验证,使得用户不需要输入第二应用程序的登录密码的情况下依然能够完成第二登录请求的验证,方便用户登录。

该多应用程序共享密码解锁方法,通过确定第二应用程序与第一应用程序在同一终端设备上登录,相互之间为关联应用程序,并且第二应用程序对应的第二用户登录名和第一应用程序对应的第一用户登录名关联时,在第一应用程序验证通过时,基于关联密码实现多个应用程序的登录,使得多个应用程序可以共享一个登录密码。用户只需要在终端设备对某一应用程序输入一次登录密码,与该应用程序关联的其他应用程序都可以实现免密码登录,实现多应用程序的快捷登录。登录密码采用手势密码验证,节省了用户登录应用程序的登录时间,方便用户操作。在发送关联密码时,给关联密码设置对应的有效时间,提高了用户登录应用程序的安全性。

应理解,上述实施例中各步骤的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不对本申请实施例的实施过程构成任何限定。

实施例 2

图 5 示出与实施例 1 中多应用程序共享密码解锁方法一一对应的多应用程序共享密码解锁装置的原理框图。如图 5 所示,该多应用程序共享密码解锁装置包括第一登录请求获取模块 10、关联密码获取模块 20、第二登录请求获取模块 30 和第二登录请求验证模块 40。其中,第一登录请求获取模块 10、关联密码获取模块 20、第二登录请求获取模块 30 和第二登录请求验证模块 40 的实现功能与实施例中多应用程序共享密码解锁方法对应的步骤一一对应,为避免赘述,本实施例不一一详述。

第一登录请求获取模块 10,用于获取第一应用程序发送的第一登录请求,第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识。

关联密码获取模块 20,用于基于第一用户登录名、第一登录密码和第一程序标识进行身份验证,在身份验证通过时,获取与第一用户登录名相对应的关联密码,并将关联密码与终端标识和第一程序标识存储在程序信息记录表中。

第二登录请求获取模块 30,用于获取第二应用程序发送的第二登录请求,第二登录请求包括第二用户登录名、第二程序标识和终端标识。

第二登录请求验证模块 40,用于若在终端标识对应的终端设备上,第二应用程序为第一应用程序的关联应用程序,且第一用户登录名和第二用户登录名相关联时,则基于关联密码完成第二登录请求的验证。

优选地,多应用程序共享密码解锁装置还用于在登录密码设置界面上配置与第一用户登录名相对应的第一登录密码,第一登录密码包括手势密码。

优选地,该多应用程序共享密码解锁装置还包括初始密码设置单元 51、目标图案的位置坐标获取单元 52 和第一登录密码设置单元 53。

初始密码设置单元 51,用于在图片底层中获取手势密码的初始位置。

目标图案的位置坐标获取单元 52，用于获取活动图层中的目标图案的位置坐标。

第一登录密码设置单元 53，用于基于动态坐标层，判断目标图案的位置坐标与手势密码的初始位置是否符合预先设置的匹配规则；若符合，则与第一用户登录名对应的第一登录密码设置成功。

优选地，多应用程序共享密码解锁装置还包括有效时间设置单元 21。

有效时间设置单元 21，用于设置关联密码的有效时间。

优选地，在第二登录请求获取模块 30 之后，多应用程序共享密码解锁装置还包括第一有效时间判断单元 22 和第二有效时间判断单元 23。

第一有效时间判断单元 22，用于若第二登录请求的获取时间在有效时间内，则执行基于关联密码完成第二登录请求的验证的步骤。

第二有效时间判断单元 23，用于若第二登录请求的获取时间超过有效时间，则需要重新执行获取第一应用程序发送的第一登录请求的步骤。

优选地，第二登录请求验证模块 40 包括程序信息记录表查询单元 41、关联应用程序信息表查询单元 42、关联应用程序确定单元 43、关联用户名信息表查询单元 44 和第二登陆请求验证单元 45。

程序信息记录表查询单元 41，用于根据第二登录请求中的终端标识，查询程序信息记录表中是否存在与终端标识对应的第一程序标识。

关联应用程序信息表查询单元 42，用于若存在与终端标识对应的第一程序标识，则基于第二登录请求中的第二程序标识和第一程序标识，查询预先设置的关联应用程序信息表，确定第二程序标识和第一程序标识是否关联。

关联应用程序确定单元 43，用于若第二程序标识和第一程序标识关联，则在终端标识对应的终端设备上，确定第二应用程序为第一应用程序的关联应用程序。

关联用户名信息表查询单元 44，用于基于第二登录请求中的第二用户登录名和第一用户登录名，查询预先设置的关联用户名信息表，确定第二用户登录名和第一用户登录名是否关联。

第二登陆请求验证单元 45，用于若第二用户登录名和第一用户登录名相关联，则基于关联密码完成第二登录请求的验证。

实施例 3

本实施例提供一计算机可读存储介质，该计算机可读存储介质上存储有计算机可读指令，该计算机可读指令被处理器执行时实现实施例 1 中多应用程序共享密码解锁方法，为避免重复，这里不再赘述。或者，该计算机可读指令被处理器执行时实现实施例 2 中多应用程序共享密码解锁装置中各模块/单元的功能，为避免重复，这里不再赘述。

可以理解地，所述计算机可读存储介质可以包括：能够携带所述计算机可读指令代码的任何实体或装置、记录介质、U 盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、电载波信号和电信信号等。

实施例 4

图 6 是本申请一实施例提供的计算机设备的示意图。如图 6 所示，该实施例的计算机设备 60 包括：处理器 61、存储器 62 以及存储在存储器 62 中并可在处理器 61 上运行的计算机可读指令 63。处理器 61 执行计算机可读指令 63 时实现上述实施例 1 中多应用程序共享密码解锁方法的步骤，例如图 1 所示的步骤 S10 至 S40。或者，处理器 61 执行计算机可读指令 63 时实现上述各装置实施例中各模块/单元的功能，例如图 5 所示第一登录请求获取模块 10、关联密码获取模块 20、第二登录请求获取模块 30 和第二登录请求验证模块 40 的功能。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。

以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权 利 要 求 书

1. 一种多应用程序共享密码解锁方法，其特征在于，包括：

获取第一应用程序发送的第一登录请求，所述第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识；

基于所述第一用户登录名、所述第一登录密码和第一程序标识进行身份验证，在身份验证通过时，获取与所述第一用户登录名相对应的关联密码，并将所述关联密码与所述终端标识和所述第一程序标识存储在程序信息记录表中；

获取第二应用程序发送的第二登录请求，所述第二登录请求包括第二用户登录名、第二程序标识和所述终端标识；

若在所述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证。

2. 如权利要求 1 所述的多应用程序共享密码解锁方法，其特征在于，在所述获取与所述第一用户登录名相对应的关联密码的步骤之后，所述多应用程序共享密码解锁方法还包括：设置所述关联密码的有效时间；

在所述获取第二应用程序发送的第二登录请求的步骤之后，所述多应用程序共享密码解锁方法还包括：

若所述第二登录请求的获取时间在所述有效时间内，则执行所述基于关联密码完成所述第二登录请求的验证的步骤；

若所述第二登录请求的获取时间超过所述有效时间，则需要重新执行所述获取第一应用程序发送的第一登录请求的步骤。

3. 如权利要求 1 所述的多应用程序共享密码解锁方法，其特征在于，所述多应用程序共享密码解锁方法还包括：

在登录密码设置界面上配置与所述第一用户登录名相对应的第一登录密码，所述第一登录密码包括手势密码。

4. 如权利要求 3 所述的多应用程序共享密码解锁方法，其特征在于，所述手势密码包括图片底层、动态坐标层和活动图层；

所述在登录密码设置界面上配置与所述第一用户登录名相对应的第一登录密码，包括：

在所述图片底层中获取所述手势密码的初始位置；

获取所述活动图层中的目标图案的位置坐标；

基于所述动态坐标层，判断所述目标图案的位置坐标与所述手势密码的初始位置是否符合预先设置的匹配规则；若符合，则与所述第一用户登录名对应的第一登录密码设置成功。

5. 如权利要求 1 所述的多应用程序共享密码解锁方法，其特征在于，所述若在所述终

端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证，包括：

根据所述第二登录请求中的终端标识，查询所述程序信息记录表中是否存在与所述终端标识对应的第一程序标识；

若存在与所述终端标识对应的所述第一程序标识，则基于所述第二登录请求中的第二程序标识和所述第一程序标识，查询预先设置的关联应用程序信息表，确定所述第二程序标识和所述第一程序标识是否关联；

若所述第二程序标识和所述第一程序标识关联，则在所述终端标识对应的终端设备上，确定第二应用程序为第一应用程序的关联应用程序；

基于所述第二登录请求中的第二用户登录名和第一用户登录名，查询预先设置的关联用户名信息表，确定所述第二用户登录名和所述第一用户登录名是否关联；

若所述第二用户登录名和所述第一用户登录名相关联，则基于关联密码完成所述第二登录请求的验证。

6. 一种多应用程序共享密码解锁装置，其特征在于，包括：

第一登录请求获取模块，用于获取第一应用程序发送的第一登录请求，所述第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识；

关联密码获取模块，用于基于所述第一用户登录名、所述第一登录密码和第一程序标识进行身份验证，在身份验证通过时，获取与所述第一用户登录名相对应的关联密码，并将所述关联密码与所述终端标识和所述第一程序标识存储在程序信息记录表中；

第二登录请求获取模块，用于获取第二应用程序发送的第二登录请求，所述第二登录请求包括第二用户登录名、第二程序标识和所述终端标识；

第二登录请求验证模块，用于若所述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证。

7. 如权利要求6所述的多应用程序共享密码解锁装置，其特征在于，所述多应用程序共享密码解锁装置还包括：

有效时间设置单元，用于设置所述关联密码的有效时间；

第一有效时间判断单元，用于若所述第二登录请求的获取时间在所述有效时间内，则执行所述基于关联密码完成所述第二登录请求的验证的步骤；

第二有效时间判断单元，用于若所述第二登录请求的获取时间超过所述有效时间，则需要重新执行所述获取第一应用程序发送的第一登录请求的步骤。

8. 如权利要求6所述的多应用程序共享密码解锁装置，其特征在于，所述多应用程序共享密码解锁装置还用于：在登录密码设置界面上配置与所述第一用户登录名相对应的第一登录密码，所述第一登录密码包括手势密码。

9. 如权利要求8所述的多应用程序共享密码解锁装置，其特征在于，所述多应用程序

共享密码解锁装置还包括：

初始密码设置单元，用于在所述图片底层中获取所述手势密码的初始位置；

目标图案的位置坐标获取单元，用于获取所述活动图层中的目标图案的位置坐标；

第一登录密码设置单元，用于基于所述动态坐标层，判断所述目标图案的位置坐标与所述手势密码的初始位置是否符合预先设置的匹配规则；若符合，则与所述第一用户登录名对应的第一登录密码设置成功。

10. 如权利要求 6 所述的多应用程序共享密码解锁装置，其特征在于，所述第二登录请求验证模块，包括：

程序信息记录表查询单元，用于根据所述第二登录请求中的终端标识，查询所述程序信息记录表中是否存在与所述终端标识对应的第一程序标识；

关联应用程序信息表查询单元，用于若存在与所述终端标识对应的所述第一程序标识，则基于所述第二登录请求中的第二程序标识和所述第一程序标识，查询预先设置的关联应用程序信息表，确定所述第二程序标识和所述第一程序标识是否关联；

关联应用程序确定单元，用于若所述第二程序标识和所述第一程序标识关联，则在所述终端标识对应的终端设备上，确定第二应用程序为第一应用程序的关联应用程序；

关联用户名信息表查询单元，用于基于所述第二登录请求中的第二用户登录名和第一用户登录名，查询预先设置的关联用户名信息表，确定所述第二用户登录名和所述第一用户登录名是否关联；

第二登陆请求验证单元，用于若所述第二用户登录名和所述第一用户登录名相关联，则基于关联密码完成所述第二登录请求的验证。

11. 一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

获取第一应用程序发送的第一登录请求，所述第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识；

基于所述第一用户登录名、所述第一登录密码和第一程序标识进行身份验证，在身份验证通过时，获取与所述第一用户登录名相对应的关联密码，并将所述关联密码与所述终端标识和所述第一程序标识存储在程序信息记录表中；

获取第二应用程序发送的第二登录请求，所述第二登录请求包括第二用户登录名、第二程序标识和所述终端标识；

若在所述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证。

12. 如权利要求 11 所述的计算机设备，其特征在于，在所述获取与所述第一用户登录名相对应的关联密码的步骤之后，所述处理器执行所述计算机可读指令时还实现如下步骤：设置所述关联密码的有效时间；

在所述获取第二应用程序发送的第二登录请求的步骤之后，所述处理器执行所述计算机可读指令时还实现如下步骤：

若所述第二登录请求的获取时间在所述有效时间内，则执行所述基于关联密码完成所述第二登录请求的验证的步骤；

若所述第二登录请求的获取时间超过所述有效时间，则需要重新执行所述获取第一应用程序发送的第一登录请求的步骤。

13. 如权利要求 11 所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还实现如下步骤：

在登录密码设置界面上配置与所述第一用户登录名相对应的第一登录密码，所述第一登录密码包括手势密码。

14. 如权利要求 13 所述的计算机设备，其特征在于，所述手势密码包括图片底层、动态坐标层和活动图层；

所述在登录密码设置界面上配置与所述第一用户登录名相对应的第一登录密码，包括：

在所述图片底层中获取所述手势密码的初始位置；

获取所述活动图层中的目标图案的位置坐标；

基于所述动态坐标层，判断所述目标图案的位置坐标与所述手势密码的初始位置是否符合预先设置的匹配规则；若符合，则与所述第一用户登录名对应的第一登录密码设置成功。

15. 如权利要求 11 所述的计算机设备，其特征在于，所述若所述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证，包括：

根据所述第二登录请求中的终端标识，查询所述程序信息记录表中是否存在与所述终端标识对应的第一程序标识；

若存在与所述终端标识对应的所述第一程序标识，则基于所述第二登录请求中的第二程序标识和所述第一程序标识，查询预先设置的关联应用程序信息表，确定所述第二程序标识和所述第一程序标识是否关联；

若所述第二程序标识和所述第一程序标识关联，则在所述终端标识对应的终端设备上，确定第二应用程序为第一应用程序的关联应用程序；

基于所述第二登录请求中的第二用户登录名和第一用户登录名，查询预先设置的关联用户名信息表，确定所述第二用户登录名和所述第一用户登录名是否关联；

若所述第二用户登录名和所述第一用户登录名相关联，则基于关联密码完成所述第二登录请求的验证。

16. 一个或多个存储有计算机可读指令的非易失性可读存储介质，其特征在于，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器实现如下步骤：

获取第一应用程序发送的第一登录请求，所述第一登录请求包括第一用户登录名、第一登录密码、第一程序标识和终端标识；

基于所述第一用户登录名、所述第一登录密码和第一程序标识进行身份验证，在身份验证通过时，获取与所述第一用户登录名相对应的关联密码，并将所述关联密码与所述终端标识和所述第一程序标识存储在程序信息记录表中；

获取第二应用程序发送的第二登录请求，所述第二登录请求包括第二用户登录名、第二程序标识和所述终端标识；

若在所述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证。

17. 如权利要求 16 所述的非易失性可读存储介质，其特征在于，在所述获取与所述第一用户登录名相对应的关联密码的步骤之后，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器还实现如下步骤：设置所述关联密码的有效时间；

在所述获取第二应用程序发送的第二登录请求的步骤之后，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器还实现如下步骤：

若所述第二登录请求的获取时间在所述有效时间内，则执行所述基于关联密码完成所述第二登录请求的验证的步骤；

若所述第二登录请求的获取时间超过所述有效时间，则需要重新执行所述获取第一应用程序发送的第一登录请求的步骤。

18. 如权利要求 16 所述的非易失性可读存储介质，其特征在于，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器还实现如下步骤：

在登录密码设置界面上配置与所述第一用户登录名相对应的第一登录密码，所述第一登录密码包括手势密码。

19. 如权利要求 18 所述的非易失性可读存储介质，其特征在于，所述手势密码包括图片底层、动态坐标层和活动图层；

所述在登录密码设置界面上配置与所述第一用户登录名相对应的第一登录密码，包括：

在所述图片底层中获取所述手势密码的初始位置；

获取所述活动图层中的目标图案的位置坐标；

基于所述动态坐标层，判断所述目标图案的位置坐标与所述手势密码的初始位置是否符合预先设置的匹配规则；若符合，则与所述第一用户登录名对应的第一登录密码设置成功。

20. 如权利要求 16 所述的非易失性可读存储介质，其特征在于，所述若在所述终端标识对应的终端设备上，所述第二应用程序为所述第一应用程序的关联应用程序，且所述第一用户登录名和所述第二用户登录名相关联时，则基于所述关联密码完成所述第二登录请求的验证，包括：

根据所述第二登录请求中的终端标识，查询所述程序信息记录表中是否存在与所述终端标识对应的第一程序标识；

若存在与所述终端标识对应的所述第一程序标识，则基于所述第二登录请求中的第二程序标识和所述第一程序标识，查询预先设置的关联应用程序信息表，确定所述第二程序标识和所述第一程序标识是否关联；

若所述第二程序标识和所述第一程序标识关联，则在所述终端标识对应的终端设备上，确定第二应用程序为第一应用程序的关联应用程序；

基于所述第二登录请求中的第二用户登录名和第一用户登录名，查询预先设置的关联用户名信息表，确定所述第二用户登录名和所述第一用户登录名是否关联；

若所述第二用户登录名和所述第一用户登录名相关联，则基于关联密码完成所述第二登录请求的验证。

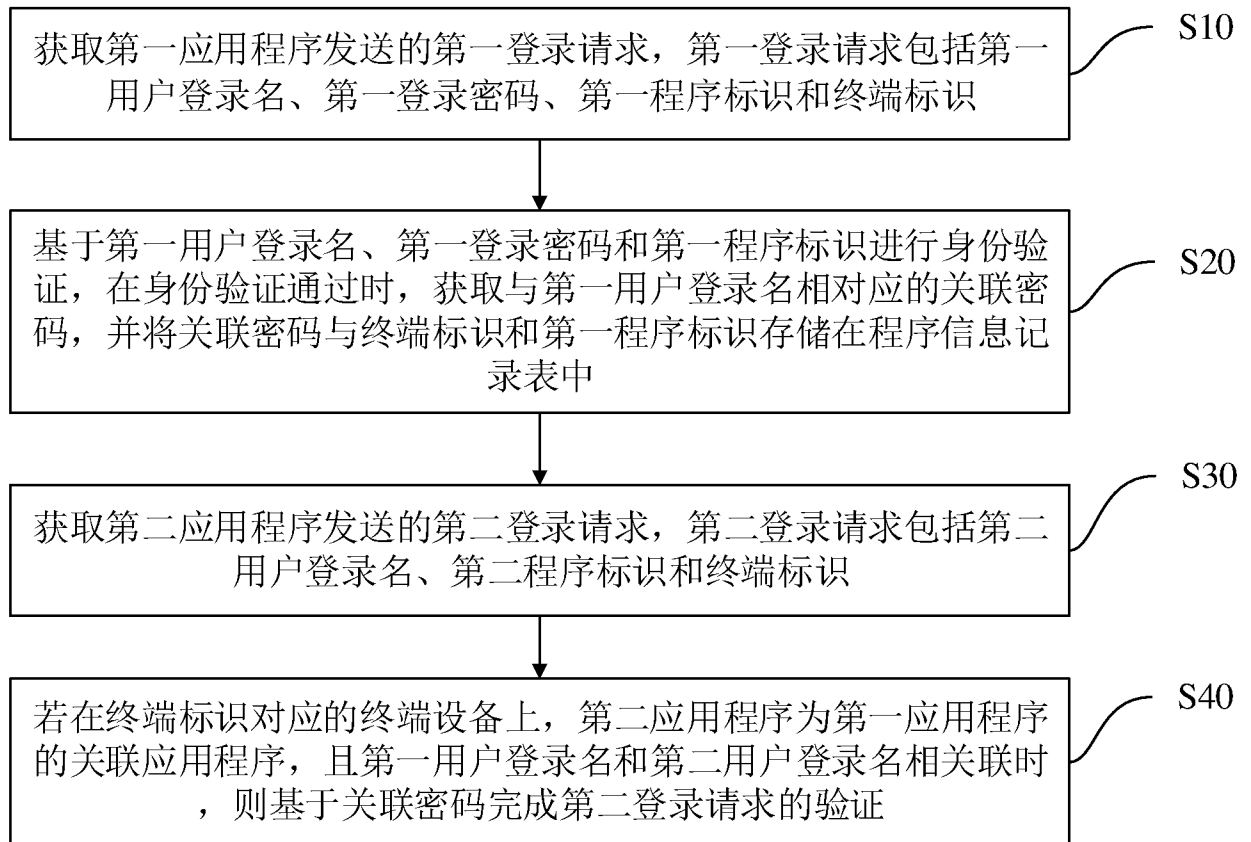


图 1

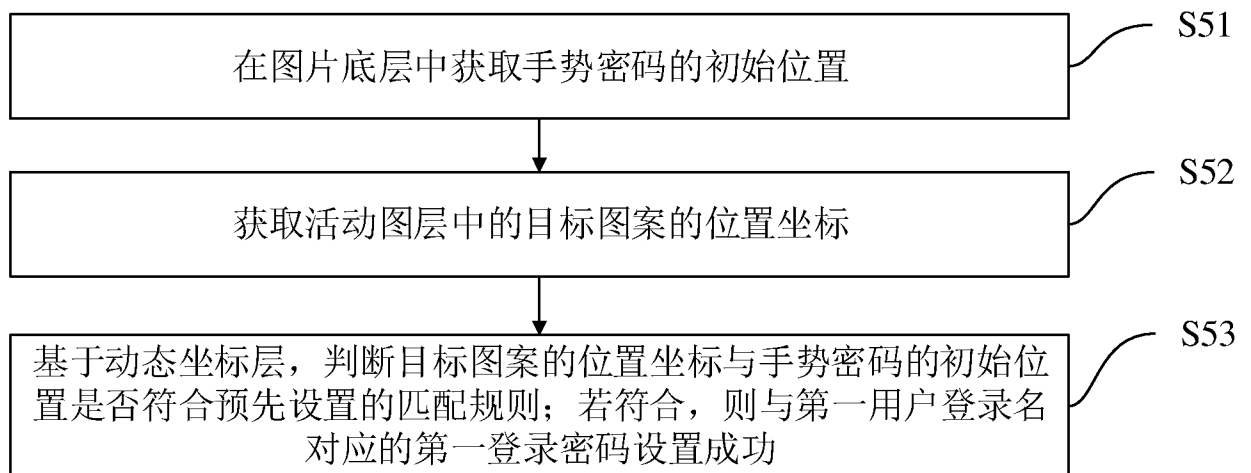


图 2

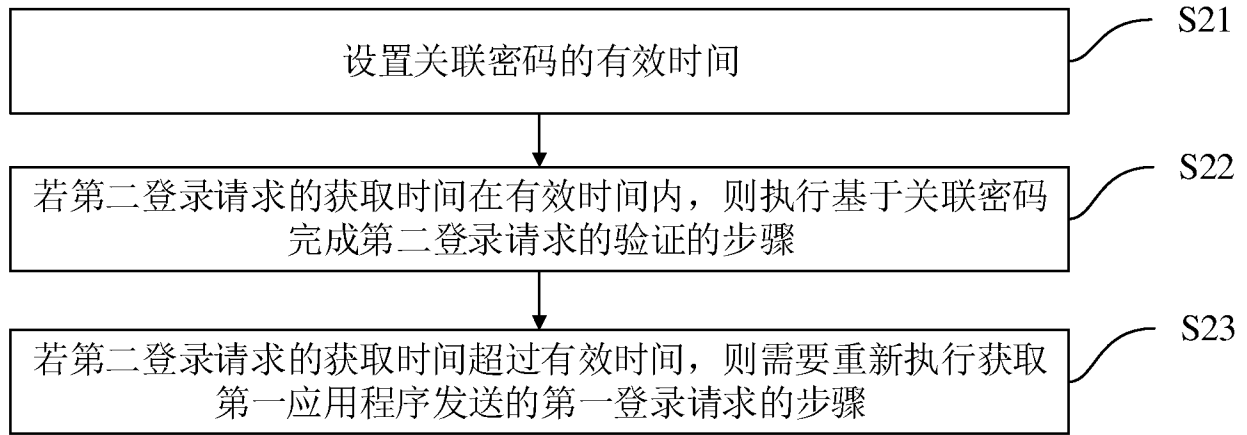


图 3

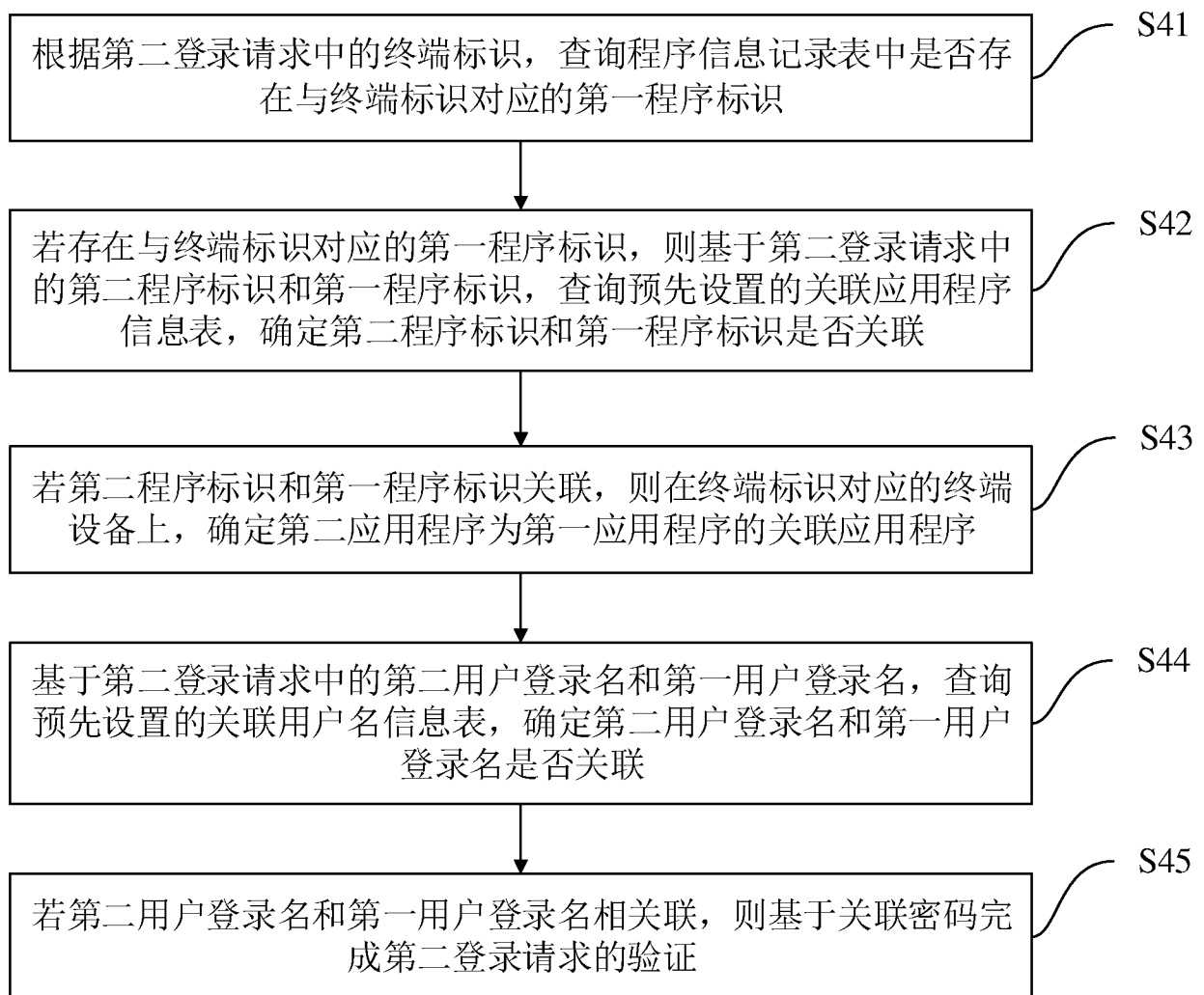


图 4

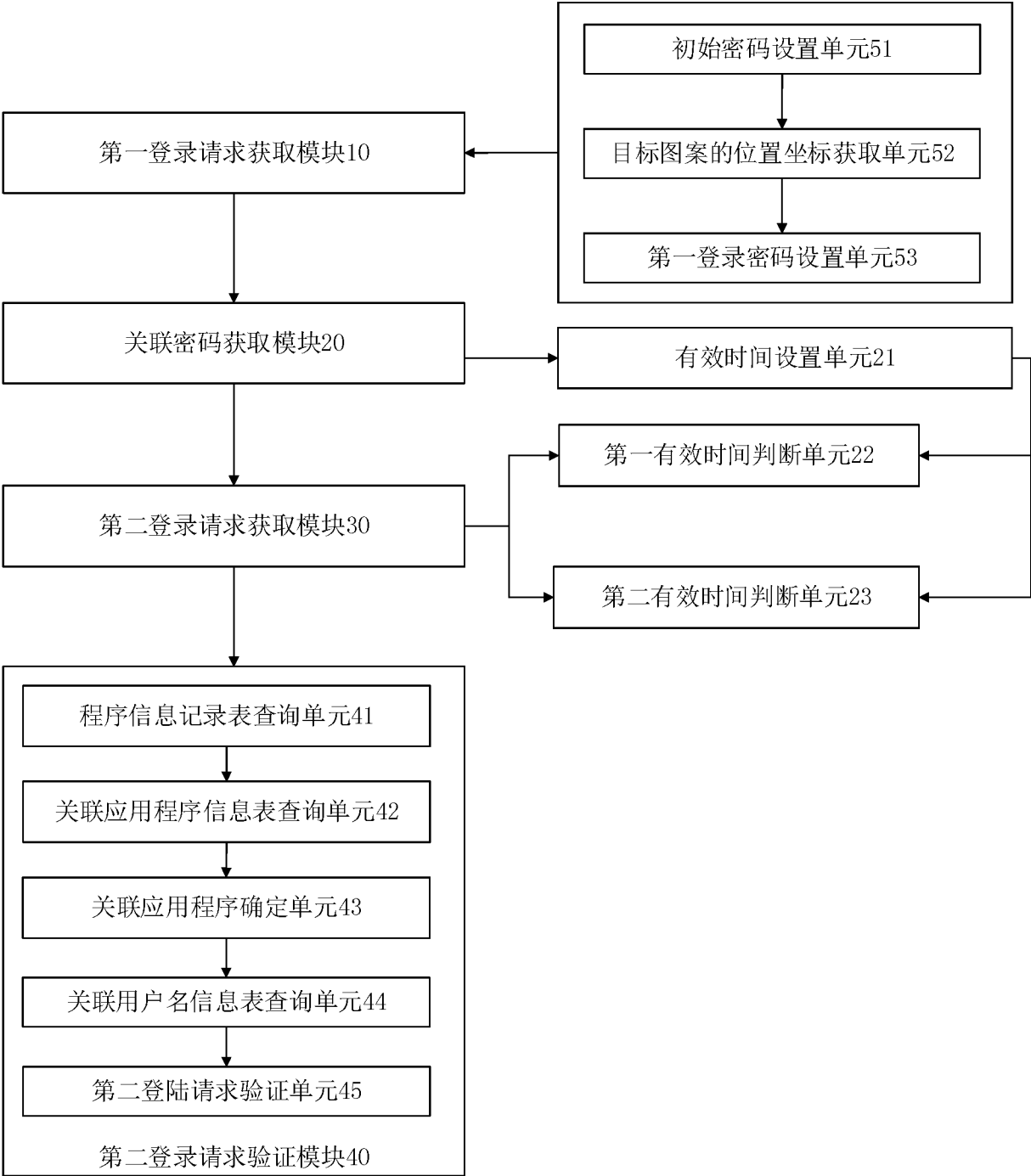


图 5

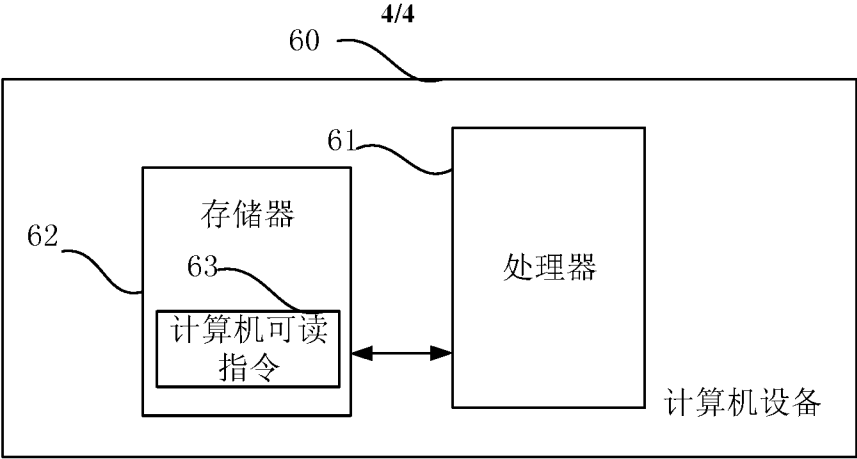


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/094413

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/31(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; TWTXT; TWABS; DWPI; VEN; USTXT; EPTXT; WOTXT; CNKI: 应用程序, 共享, 密码, 登录, 关联, 记录, 标识, 手势, application, APP, share, password, login, associate, record, identification, gesture

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103065080 A (GUANG DONG OPPO MOBILE TELECOMMUNICATIONS CO., LTD.) 24 April 2013 (2013-04-24) description, paragraphs 5-13, 19-36 and 54, and figures 1-3	1-20
A	CN 105227302 A (GUANG DONG OPPO MOBILE TELECOMMUNICATIONS CO., LTD.) 06 January 2016 (2016-01-06) entire document	1-20
A	CN 106330918 A (HANGZHOU DPTECH TECHNOLOGIES CO., LTD.) 11 January 2017 (2017-01-11) entire document	1-20
A	US 2002116648 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 22 August 2002 (2002-08-22) entire document	1-20

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

22 January 2019

Date of mailing of the international search report

13 February 2019

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Authorized officer

Facsimile No. (86-10)62019451

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/094413

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	103065080	A	24 April 2013	CN	103065080	B	20 January 2016
CN	105227302	A	06 January 2016	WO	2017071363	A1	04 May 2017
CN	106330918	A	11 January 2017	None			
US	2002116648	A1	22 August 2002	None			

国际检索报告

国际申请号

PCT/CN2018/094413

A. 主题的分类

G06F 21/31 (2013.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNABS; CNTXT; TWTXT; TWABS; DWPI; VEN; USTXT; EPTXT; WOTXT; CNKI: 应用程序, 共享, 密码, 登录, 关联, 记录, 标识, 手势, application, APP, share, password, login, associate, record, identification, gesture

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 103065080 A (广东欧珀移动通信有限公司) 2013年 4月 24日 (2013 - 04 - 24) 说明书第5-13、19-36、54段, 附图1-3	1-20
A	CN 105227302 A (广东欧珀移动通信有限公司) 2016年 1月 6日 (2016 - 01 - 06) 全文	1-20
A	CN 106330918 A (杭州迪普科技有限公司) 2017年 1月 11日 (2017 - 01 - 11) 全文	1-20
A	US 2002116648 A1 (IBM) 2002年 8月 22日 (2002 - 08 - 22) 全文	1-20

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2019年 1月 22日

国际检索报告邮寄日期

2019年 2月 13日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

房琦

传真号 (86-10) 62019451

电话号码 86-(20)-28950714

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/094413

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103065080	A	2013年 4月 24日	CN	103065080	B	2016年 1月 20日
CN	105227302	A	2016年 1月 6日	W0	2017071363	A1	2017年 5月 4日
CN	106330918	A	2017年 1月 11日	无			
US	2002116648	A1	2002年 8月 22日	无			