

(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
2020 年 5 月 7 日 (07.05.2020)



(10) 国际公布号
WO 2020/087527 A1

(51) 国际专利分类号:

G06F 21/32 (2013.01)

(21) 国际申请号:

PCT/CN2018/113803

(22) 国际申请日:

2018 年 11 月 2 日 (02.11.2018)

(25) 申请语言:

中文

(26) 公布语言:

中文

(71) 申请人: 深圳市汇顶科技股份有限公司 (SHENZHEN GOODIX TECHNOLOGY CO., LTD.) [CN/CN]; 中国广东省深圳市福田区腾飞工业大厦B座13层, Guangdong 518045 (CN)。

(72) 发明人: 曹岚健 (CAO, Lanjian); 中国广东省深圳市福田区腾飞工业大厦B座13层, Guangdong 518045 (CN)。

(74) 代理人: 北京同立钧成知识产权代理有限公司 (LEADER PATENT & TRADEMARK FIRM); 中国北京市海淀区西直门北大街32号枫蓝国际A座8F-6, Beijing 100082 (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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

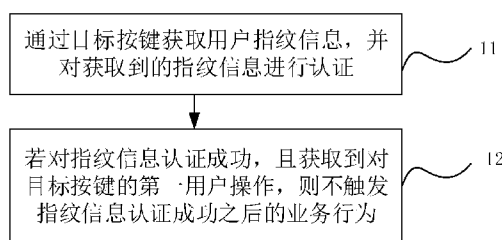
(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),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

(54) Title: FINGERPRINT VERIFICATION METHOD AND APPARATUS, DEVICE AND STORAGE MEDIUM

(54) 发明名称: 指纹认证方法、装置、设备及存储介质



11 Obtain fingerprint information of a user by means of a target button, and verify the obtained fingerprint information

12 If the verification of the fingerprint information is successful and a first user operation for the target button is obtained, not trigger the service behavior after the successful verification of the fingerprint information

图 1

(57) Abstract: The present application provides a fingerprint verification method and apparatus, a device and a storage medium. The method comprises: obtaining fingerprint information of a user by means of a target button, and verifying the obtained fingerprint information; and if the verification of the fingerprint information is successful and a first user operation for the target button is obtained, not triggering the service behavior after the successful verification of the fingerprint information. The security and reliability of a terminal are improved.

(57) 摘要: 本申请提供一种指纹认证方法、装置、设备及存储介质, 包括: 通过目标按键获取用户指纹信息, 并对获取到的指纹信息进行认证; 若对指纹信息认证成功, 且获取到对目标按键的第一用户操作, 则不触发指纹信息认证成功之后的业务行为, 提高了终端的安全性和可靠性。



WO 2020/087527 A1

指纹认证方法、装置、设备及存储介质

技术领域

5 本申请涉及指纹认证技术领域，尤其涉及一种指纹认证方法、装置、设备及存储介质。

背景技术

10 随着信息技术的快速发展，终端(如手机、平板电脑等等)的使用越来越普及。作为终端上的标配技术，指纹识别技术在终端的解锁、唤醒、移动支付等功能中得到广泛应用。尤其是指纹支付功能，不仅可克服了现有技术中数字密码容易被窃取的弊端，而且输入更为快捷。

现有技术中，通过指纹识别进行身份认证，通常是通过手指触摸或点按在指纹采集模块，触发指纹认证模块进行指纹认证，若指纹认证模块认证成功，则触发认证成功后的业务行为。

15 然而，现有技术中，由于指纹识别过程中，指纹认证成功即触发认证成功后的业务行为，针对用户无法判断其安全性的某恶意病毒网页，容易因个人的无意或被强行引导或误导进行指纹验证，造成不必要的人身安全信息泄露或财产损失，终端的安全性较低。

20 发明内容

为克服现有技术中存在的相关问题，本申请提供一种指纹认证方法、装置、设备及存储介质。

第一方面，本申请提供一种指纹认证方法，包括：

25 通过目标按键获取用户指纹信息，并对获取到的指纹信息进行认证；若对指纹信息认证成功，且获取到对目标按键的第一用户操作，则不触发指纹信息认证成功之后的业务行为。

由于本申请实施例，通过在指纹信息认证成功之后，获取到第一用户操作，则不触发指纹信息认证成功之后的业务行为，有效的避免了由于误操作造成违背用户意愿的业务行为，进而提高了终端的安全性和可靠性。

可选的，第一用户操作为用户对目标按键的按下操作。

由于本申请实施例中，第一用户操作为用户对目标按键的按下操作，第一用户操作简单、便捷，且通过第一用户操作，在指纹认证成功后，用户对目标按键执行按下操作，即可不触发指纹信息认证成功之后的业务行为，提高了终端的可操作性。

可选的，若对指纹信息认证成功，且获取到对目标按键的第二用户操作，则触发指纹信息认证成功之后的业务行为。

由于本申请实施例中，在对指纹信息认证成功之后，获取到对目标按键的第二用户操作，则触发指纹信息认证成功之后的业务行为，通过第二用户操作进一步确定触发指纹信息认证成功之后的业务行为，提高了终端的可靠性。

可选的，第二用户操作为用户从目标按键移开手指的操作。

由于本申请实施例中，第二用户操作为用户从目标按键移开手指的操作，第二用户操作简单、便捷，且通过第二用户操作，在指纹认证成功后，通过用户从目标按键移开手指操作，然后触发指纹信息认证成功之后的业务行为，提高了终端的可操作性和可靠性。

可选的，通过目标按键获取用户指纹信息，并对获取到的指纹信息进行认证，包括：

获取合法的用户指纹模板；对用户指纹信息和用户指纹模板进行匹配。

可选的，本申请实施例提供的指纹认证方法还包括：

若对指纹信息认证成功，且获取到对目标按键的第一用户操作，则推送提示信息，以提示用户无法进行业务行为。

可选的，业务行为是用户支付行为。

可选的，目标按键为 Home 键、返回键或者确认键中的任一项。

下面将介绍装置、设备、存储介质及计算机程序产品，其效果可参考方法部分的效果，下面对此不再赘述。

第二方面，本申请提供一种指纹认证装置，包括：

获取模块，用于通过目标按键获取用户指纹信息，认证模块，用于对获取到的指纹信息进行认证；第一处理模块，用于若对指纹信息认证成功，且获取到对目标按键的第一用户操作，则不触发指纹信息认证成功之后的业务

行为。

可选的，第一用户操作为用户对目标按键的按下操作。

可选的，本申请提供的指纹认证装置还包括：

第二处理模块，用于若对指纹信息认证成功，且获取到对目标按键的第

5 二用户操作，则触发指纹信息认证成功之后的业务行为。

可选的，第二用户操作为用户从目标按键移开手指的操作。

可选的，认证模块具体用于：

获取合法的用户指纹模板；对用户指纹信息和用户指纹模板进行匹配。

可选的，本发明实施例提供的指纹认证装置，还包括：

10 推送模块，用于若对指纹信息认证成功，且获取到对目标按键的第一用户操作，则推送提示信息，以提示用户无法进行业务行为。

可选的，业务行为是用户支付行为。

可选的，目标按键为 Home 键、返回键或者确认键中的任一项。

第三方面，本申请提供一种指纹识别模组，包括：目标按键和微控制单
15 元 MCU；

MCU 用于：通过目标按键获取用户指纹信息，对指纹信息进行认证，并将认证结果发送给处理器；若通过目标按键获取到第一用户操作，则将第一用户操作发送给处理器，以使处理器根据认证结果确定对指纹信息认证成功时，根据第一用户操作不触发指纹信息认证成功之后的业务行为。

20 可选的，第一用户操作为用户对目标按键的按下操作。

可选的，MCU 还用于：

若通过目标按键获取到第二用户操作，则将第二用户操作发送给处理器，以使处理器根据认证结果确定对指纹信息认证成功时，根据第二用户操作触发指纹信息认证成功之后的业务行为。

25 可选的，第二用户操作为用户从目标按键移开手指的操作。

可选的，MCU 具体用于：

获取合法的用户指纹模板；对用户指纹信息和用户指纹模板进行匹配。

可选的，MCU 还用于：

30 若对指纹信息认证成功，且获取到对目标按键的第一用户操作，则推送提示信息，以提示用户无法进行业务行为。

可选的，业务行为是用户支付行为。

可选的，目标按键为 Home 键、返回键或者确认键中的任一项。

第四方面，本申请提供一种终端设备，终端设备包括：指纹识别模组和处理器，所述指纹识别模组包括：目标按键和微控制单元 MCU；

- 5 MCU 用于：通过目标按键获取用户指纹信息，并对获取到的指纹信息进行认证，向处理器发送认证结果；若通过目标按键获取到第一用户操作，则将第一用户操作发送给处理器。

处理器用于：若根据认证结果确定对指纹信息认证成功，则根据第一用户操作不触发指纹信息认证成功之后的业务行为。

- 10 可选的，第一用户操作为用户对目标按键的按下操作。

可选的，MCU，还用于若通过目标按键获取到第二用户操作，则将第二用户操作发送给处理器。

处理器，还用于若根据认证结果确定对指纹信息认证成功时，根据第二用户操作触发指纹信息认证成功之后的业务行为。

- 15 可选的，第二用户操作为用户从目标按键移开手指的操作。

可选的，MCU 具体用于：

获取合法的用户指纹模板；对用户指纹信息和用户指纹模板进行匹配。

可选的，MCU 还用于：

- 20 若对指纹信息认证成功，且获取到对目标按键的第一用户操作，则推送提示信息，以提示用户无法进行业务行为。

可选的，业务行为是用户支付行为。

可选的，目标按键为 Home 键、返回键或者确认键中的任一项。

- 25 第五方面，本申请提供一种计算机存储介质，存储介质包括计算机指令，当指令被计算机执行时，使得计算机实现第一方面或第一方面可选方式的指纹认证方法。

第六方面，本申请提供一种计算机程序产品，包括计算机指令，当指令被计算机执行时，使得计算机实现第一方面或第一方面可选方式的指纹认证方法。

- 30 本申请提供一种指纹认证方法、装置、设备及存储介质，包括：通过目标按键获取用户指纹信息，并对获取到的指纹信息进行认证；若对指纹信息

认证成功，且获取到对目标按键的第一用户操作，则不触发指纹信息认证成功之后的业务行为。由于本申请实施例中，在指纹信息认证成功之后，通过获取到第一用户操作，则不触发指纹信息认证成功之后的业务行为，有效的避免了由于误操作造成违背用户意愿的业务行为，进而提高了终端的安全性和可靠性。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图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 是本申请一实施例提供的指纹认证方法的流程示意图；

图 2 是本申请一实施例提供的操作界面示意图；

图 3 是本申请另一实施例提供的指纹认证方法的流程示意图；

图 4 是本申请另一实施例提供的操作界面示意图；

图 5 是本申请一实施例提供的指纹认证装置的示意图；

图 6 是本申请一实施例提供的指纹识别模组的结构示意图；

图 7 是本申请一实施例提供的终端设备的结构示意图。

具体实施方式

为使本申请实施例的目的、技术方案和优点更加清楚，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。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例，例如能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖

不排除他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

随着信息技术的快速发展，终端(如手机、平板电脑等等)的使用越来越普及。作为终端上的标配技术，指纹识别技术在终端的解锁、唤醒、移动支付等功能中得到广泛应用。尤其是指纹支付功能，不仅可解决现有技术中数字密码容易被窃取的问题，而且输入更为快捷。由于指纹识别过程中，指纹认证成功即触发认证成功后的业务行为，针对用户无法判断其安全性的某恶意病毒网页，容易因个人的无意或被强行引导、误导进行指纹验证，造成不必要的人身安全信息泄露或财产损失，终端的安全性较低。为了解决这些技术问题，本申请实施例提供一种指纹认证方法、装置、设备及存储介质。

在介绍本申请实施例之前，下面先对本申请实施例的实施场景进行简单介绍：

场景实例一：

终端显示某恶意病毒网页，网页的前台程序为一个支付页面，此时正在等待验证用户指纹。但是该支付页面被伪装成其他显示形式，用户无法觉察到此页面是一个支付页面，并且该页面没有提供退出按钮。此时用户的习惯性行为是按下 home 键退出该页面，但当用户使用注册指纹手指点击 home 键时，指纹信息认证成功，进而触发指纹认证成功后的支付行为，造成用户不必要的财产损失。

场景示例二：

终端显示某恶意病毒网页，网页的前台程序为一个支付页面，并且无退出按钮，正在等待验证用户指纹。该页面并未伪装成其他形式，用户情急之下通过按下 Home 键退出该页面，但当用户使用注册指纹手指点击 Home 键时，指纹信息认证成功，进而触发指纹认证成功后的支付行为，造成用户不必要的财产损失。

在上述示例应用场景中，或其他类似应用场景下，比如，其他需要用户指纹认证，进而引发用户私人信息泄露等场景，由于指纹认证成功后即触发指纹认证成功后的支付行为，进而造成了用户不必要的损失，为了解决上述问题，本申请提供一种指纹认证方法、装置、设备及存储介质。

基于上述应用场景，下面以具体地实施例对本申请的技术方案以及本申请的技术方案如何解决上述技术问题进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例中不再赘述。下面将结合附图，对本申请的实施例进行描述。

5 实施例一

图1是本申请一实施例提供的指纹认证方法的流程示意图，如图1所示，本实施例以该方法应用于终端来举例说明，该终端可以是移动电话，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等，该方法包括如下步骤：

10 步骤 S11：通过目标按键获取用户指纹信息，并对获取到的指纹信息进行认证。

步骤 S12：若对指纹信息认证成功，且获取到对目标按键的第一用户操作，则不触发指纹信息认证成功之后的业务行为。

针对步骤 S11 进行说明：

15 通过目标按键获取用户指纹信息的过程中，目标按键可以是 Home 键、返回键以及确认键等实体按键，同时，目标按键也可以是虚拟按键，比如悬浮球等，本申请实施例对目标按键的具体按键以及按键形式不做任何限制，只要能够通过目标按键获取到用户的指纹信息即可。可选的，目标按键为 Home 键、返回键或者确认键中的任一项。

20 通过用户对目标按键的相关操作，获取用户指纹信息，其中，用户对目标按键的相关操作可以是用户对目标按键的触摸操作，用户通过相关操作将用户指纹信息反馈至终端设备中的微控制单元，终端对用户指纹信息进行识别与认证。指纹识别即指通过比较不同指纹的细节特征点来进行鉴别，指纹识别技术涉及图像处理、模式识别、计算机视觉、数学形态学、小波分析等
25 众多学科。由于每个人的指纹不同，且同一人的十指之间，指纹也有明显区别，因此指纹可用于身份鉴定。本申请实施例对指纹识别的具体方式不做任何限制，只要能够实现对用户指纹信息进行识别即可。

在一种可能的实施方式中，通过目标按键获取用户指纹信息，并对获取到的指纹信息进行认证，包括：获取合法的用户指纹模板；对用户指纹信息
30 和用于指纹模板进行匹配。

用户在进行指纹认证之前，还需要获取合法的用户指纹模板，获取合法的用户指纹模板可以通过在终端中用户指纹触摸可采集用户指纹模板的目标按键获取，例如，用户可以通过在终端的设置中，使用右手食指对目标按键进行多次触摸，通过重复输入用户指纹信息对用户预设指纹信息进行注册，

5 从而获取合法的用户指纹模板。本申请实施例对获取用户指纹模板的具体方式不做限制，另外，本申请实施例对获取的用户指纹模板的手指以及获取的用户指纹模板数量也不做限制，只要能够实现获取合法的用户指纹模板即可。

通过用户对目标按键的相关操作，获取用户指纹信息之后，还需要对获取到的指纹信息进行认证，具体的，可以通过对用户指纹信息和用户指纹模

10 板进行匹配，由于手指末端正面皮肤上有凸凹不平的纹路，蕴涵大量的信息。这些皮肤的纹路在图案、断点和交点上是不相同的，在信息处理中将它们称作“特征”，而且这些特征具有唯一性和永久性，可以把某个人与其指纹一一对应起来。通过对用户指纹信息和用户指纹模板进行匹配，并可以根据用户指纹信息与用户指纹模板的相似度判断认证结果，若用户指纹信息和用

15 户指纹模板匹配成功，则对用户指纹信息认证成功，若用户指纹信息和用户指纹模板匹配失败，则对用户指纹信息认证失败。本申请实施例对指纹信息认证方式不做任何限制，只要能够实现对获取到的用户指纹信息进行认证即可。

对用户指纹信息认证可以通过终端设备的中央处理器（Central Processing

20 Unit，CPU）实现，也可以通过终端设备的微控制单元（Microcontroller Unit，MCU）来实现，本申请实施例对用户指纹信息认证的具体实现方式不做限制。

对步骤 S12 进行说明：

经过步骤 S11 对获取到的用户指纹信息的认证，其对于用户指纹信息的认证结果可以为对用户指纹信息认证成功或者对用户指纹信息认证失败，若对

25 用户指纹信息认证失败，则不会触发指纹认证成功之后的业务行为，若需要继续执行指纹认证成功之后的业务行为，则需重新获取用户指纹信息并对获取到的指纹信息进行认证，本申请实施例对认证失败后的终端行为不做任何限制。

若对指纹信息认证成功，则需要获取对目标按键的第一用户操作，在对

30 指纹信息认证成功且获取到对目标按键的第一用户操作的情况下，不触发指

纹信息认证成功之后的业务行为，通过对触发指纹信息认证成功之后的业务行为的条件进一步限制，能够有效的避免由于用户误操作等引发的后续业务行为，提高了终端的可操作性以及安全性。例如，在上述示例场景中，在某恶意病毒网页，网页的前台程序为一个支付页面，支付页面为正常支付页面形式或被伪装成其他显示形式，等待用户指纹信息认证，若由于用户使用注册指纹手指触摸或点击 home 键导致指纹信息认证成功，则用户还可以通过第一用户操作，不触发指纹信息认证成功之后的支付行为，从而避免了用户不必要的财产损失。其中，获取对目标按键的第一用户操作可以通过终端设备中的 MCU 实现。

为了不触发指纹信息认证成功之后的业务行为，在一种可能的实施方式中，若对指纹信息认证成功，且获取到对目标按键的第一用户操作，则推送提示信息，以提示用户无法进行业务行为。可选的，业务行为是用户支付行为。下面以提示用户无法进行支付行为为例，对本发明实施例进行介绍，图 2 是本申请一实施例提供的操作界面示意图，如图 2 所示，在支付过程中，需要获取用户指纹信息，其中，界面 201 表示通过目标按键获取用户指纹信息，并对获取到的指纹信息认证成功，若用户想要阻止该次的支付行为，则可以对目标按键执行第一用户操作，其中，界面 202 表示获取到对目标按键的第一用户操作，终端推送提示消息 212，提示用户已阻止当前支付行为。

若对指纹信息认证成功，但没有获取到第一用户操作，则触发指纹信息认证成功之后的业务行为，例如，在正常支付宝付款需要指纹认证的情况下，通过获取用户指纹信息，并对指纹信息认证成功，而且没有获取到第一用户操作，则支付宝付款成功，不影响触发正常情况下的指纹信息认证成功后的业务行为。

第一用户操作可以是对目标按键超过预设时长的触摸操作，可以是对目标按键的长按操作等，本申请实施例对第一用户操作不做具体限制，只要能够在对指纹认证成功且获取到第一用户操作，可以不触发指纹信息认证成功之后的业务行为即可。可选的，第一用户操作为对目标按键的按下操作。在对指纹信息认证成功后，用户对目标按键执行按下操作，则不触发指纹信息认证成功之后的业务行为。例如：在上述实例场景中，某恶意病毒网页，网页的前台程序为一个支付页面，支付页面为正常支付页面形式或被伪装成其

他显示形式，等待用户指纹信息认证，尽管由于用户使用注册指纹手指触摸 home 键导致指纹信息认证成功，但用户还可以通过按下 home 键的操作，阻止终端触发指纹信息认证成功之后的支付行为，从而避免了用户不必要的财产损失。

5 在一种可能的实施方式中，在对指纹信息认证成功之后，为了阻止触发指纹认证成功之后的业务行为，第一用户操作还可以是注册指纹手指触摸目标按键超过预设时长。比如，在对获取到的用户指纹信息认证成功之后，注册指纹手指触摸目标按键超过预设时长，则不触发指纹认证成功之后的业务行为。

10 在本申请实施例中，由于本申请实施例可以通过在指纹信息认证成功之后，获取到第一用户操作，则不触发指纹信息认证成功之后的业务行为，实现了对指纹信息认证成功之后的是否触发相应的业务行为进行人工控制，有效的避免了由于误操作等造成违背用户意愿的业务行为，进而提高了终端的安全性和可靠性。

15 实施例二

在上述实施例一的基础上，图 3 是本申请另一实施例提供的指纹认证方法的流程示意图，本实施例以该方法应用于终端来举例说明，该终端可以是移动电话，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等，如图 3 所示，本申请提供的指纹认证方法
20 还包括：

步骤 S21：若对指纹信息认证成功，且获取到对目标按键的第二用户操作，则触发指纹信息认证成功之后的业务行为。

经过步骤 S11 对获取到的用户指纹信息的认证，若对指纹信息认证成功，则需要获取对目标按键的第二用户操作，在对指纹信息认证成功且获取到第二用户操作的情况下，触发指纹信息认证成功之后的业务行为，通过对触发指纹信息认证成功之后的业务行为的条件进一步限制，能够有效的避免由于用户误操作等引发的后续业务行为，提高了终端的可操作性以及安全性。例如，在正常支付宝付款需要指纹认证的情况下，通过获取用户指纹信息，并对指纹信息认证成功，而且获取到对目标按键的第二用户操作，则支付宝付款成功，不影响触发正常情况下的指纹信息认证成功后的业务行为。图 4 是
25 30 付款成功，不影响触发正常情况下的指纹信息认证成功后的业务行为。图 4 是

本申请另一实施例提供的操作界面示意图，如图 4 所示，例如，在正常支付宝付款需要指纹认证的情况下，需要获取用户指纹信息，并对指纹信息进行认证，界面 401 表示通过目标按键获取用户指纹信息，并对获取到的指纹信息认证成功，在正常支付的情况下，用户对终端执行第二用户操作，用户界面 402 表示在对指纹信息认证成功之后，获取到对目标按键的第二用户操作，则触发指纹信息认证成功之后的支付行为。在触发指纹信息认证成功之后的业务行为之后，还可以通过推送消息 412，提示用户支付成功。

第二用户操作可以是对目标按键的触摸操作，可以是对目标按键的按下操作等，本申请实施例对第二用户操作不做具体限制，只要能够在对指纹认证成功且获取到第二用户操作，可以触发指纹信息认证成功之后的业务行为即可。可选的，第二用户操作为用户从目标按键移开手指的操作。例如，在正常支付宝付款需要指纹认证的情况下，通过获取用户指纹信息，并对指纹信息认证成功，而且用户从目标按键移开手指，则支付宝付款成功，不影响触发正常情况下的指纹信息认证成功后的业务行为。获取对目标按键的第二用户操作可以通过终端设备中的 MCU 来实现。

本申请实施例对第一用户操作和第二用户操作不做具体限制，只要终端能够根据第一用户操作或第二用户操作进行相应的不触发或触发指纹认证成功之后的业务行为即可。

在本申请实施例中，由于本申请实施例可以通过在指纹信息认证成功之后，获取到第二用户操作，则触发指纹信息认证成功之后的业务行为，有效的避免了由于误操作等造成违背用户意愿的业务行为，进而提高了终端的安全性和可靠性。

实施例三

本申请实施例还提供一种指纹认证装置，图 5 是本申请一实施例提供的指纹认证装置的示意图，本实施例以该方法应用于终端来举例说明，该终端可以是移动电话，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等，如图 5 所示，本申请实施例提供的指纹认证装置包括：

获取模块 51，用于通过目标按键获取用户指纹信息，认证模块 52，用于对获取到的指纹信息进行认证；第一处理模块 53，用于若对指纹信息认证成功

功，且获取到对目标按键的第一用户操作，则不触发指纹信息认证成功之后的业务行为。

可选的，第一用户操作为用户对目标按键的按下操作。

可选的，本申请提供的指纹认证装置还包括：

- 5 第二处理模块 54，用于若对指纹信息认证成功，且获取到第二用户操作，则触发指纹信息认证成功之后的业务行为。

可选的，第二用户操作为用户从目标按键移开手指的操作。

可选的，目标按键为 Home 键、返回键或者确认键中的任一项。认证模块具体用于：

- 10 获取合法的用户指纹模板；对用户指纹信息和用户指纹模板进行匹配。

本申请实施例体用的指纹认证装置，还包括：

推送模块 55，用于若对指纹信息认证成功，且获取到对目标按键的第一用户操作，则推送提示信息，以提示用户无法进行业务行为。

可选的，业务行为是用户支付行为。

- 15 本申请实施例提供的指纹认证装置可用于执行上述的指纹认证方法，其内容和效果可参考方法部分，本申请实施例对此不做限制。

实施例四

本申请提供一种指纹识别模组，图 6 是本申请一实施例提供的指纹识别模组的结构示意图，如图 6 所示，本申请提供的指纹识别模组包括：目标按

- 20 键 61 和微控制单元 MCU62。

MCU62 用于：通过目标按键 61 获取用户指纹信息，对指纹信息进行认证，并将认证结果发送给处理器；若通过目标按键 61 获取到第一用户操作，则将第一用户操作发送给处理器，以使处理器根据认证结果确定对指纹信息认证成功时，根据第一用户操作不触发指纹信息认证成功之后的业务行为。

- 25 可选的，第一用户操作为用户对目标按键 61 的按下操作。

可选的，MCU62 还用于：

若通过目标按键 61 获取到第二用户操作，则将第二用户操作发送给处理器，以使处理器根据认证结果确定对指纹信息认证成功时，根据第二用户操作触发指纹信息认证成功之后的业务行为。

- 30 其中，MCU62 的个数可以为一个或两个以上，例如，MCU62 的数量为

1 个, 则该 MCU62 用于获取用户指纹信息且对指纹信息进行认证, 并将认证结果发送给处理器, 还用于获取第一用户操作, 并将第一用户操作发送给处理器, 还用于获取第二用户操作, 并将第二用户操作发送给处理器。再例如, MCU62 的数量为 2 个, 则可以为第一个 MCU62 用于获取用户指纹信息且将
5 指纹信息进行认证, 并将认证结果发送给处理器, 第二个 MCU62 用于获取用户指纹信息且对指纹信息进行认证, 并将认证结果发送给处理器, 还用于获取第一用户操作, 并将第一用户操作发送给处理器, 还用于获取第二用户操作, 并将第二用户操作发送给处理器, 本发明对 MCU62 数量为两个时, 每个 MCU62 负责的工作不做限制, 只要能够实现本申请技术方案即可。再
10 例如, MCU62 数量为 3 个, 则可以为第一个 MCU62 用于获取用户指纹信息且将指纹信息进行认证, 并将认证结果发送给处理器, 第二个 MCU62 用于获取用户指纹信息且对指纹信息进行认证, 并将认证结果发送给处理器, 第三个 MCU62 用于获取第二用户操作, 并将第二用户操作发送给处理器。

可选的, 第二用户操作为用户从目标按键 61 移开手指的操作。

15 可选的, MCU62 具体用于:

获取合法的用户指纹模板; 对用户指纹信息和用户指纹模板进行匹配。

可选的, MCU62 还用于:

若对指纹信息认证成功, 且获取到对目标按键 61 的第一用户操作, 则推送提示信息, 以提示用户无法进行业务行为。

20 可选的, 业务行为是用户支付行为。

可选的, 目标按键 61 为 Home 键、返回键或者确认键中的任一项。

本申请实施例提供的指纹识别模组可用于执行上述的指纹认证方法, 其内容和效果可参考方法部分, 本申请实施例对此不做限制。

实施例五

25 本申请一实施例还提供一种终端设备, 图 7 是本申请一实施例提供的终端设备的结构示意图, 如图 7 所示, 终端设备包括: 指纹识别模组 71 和处理器 72, 指纹识别模组 71 包括: 目标按键 711 和微控制单元 712 MCU712 用于:

通过目标按键 711 获取用户指纹信息, 并对获取到的指纹信息进行认证, 向处理器 72 发送认证结果; 若通过目标按键 711 获取到第一用户操作, 则将
30 第一用户操作发送给处理器 72。

处理器 72 用于：若根据认证结果对指纹信息认证成功，则根据第一用户操作则不触发指纹信息认证成功之后的业务行为。

可选的，第一用户操作为用户对目标按键 711 的按下操作。

可选的，MCU712 还用于：

- 5 若通过目标按键 711 获取到第二用户操作，则将第二用户操作发送给处理器 72；

处理器 72，还用于若根据认证结果确定对指纹信息认证成功时，根据第二用户操作触发指纹信息认证成功之后的业务行为。

可选的，第二用户操作为用户从目标按键 711 移开手指的操作。

- 10 可选的，MCU712 具体用于：

获取合法的用户指纹模板；对用户指纹信息和用户指纹模板进行匹配。

可选的，MCU712 还用于：

若对指纹信息认证成功，且获取到对目标按键 711 的第一用户操作，则推送提示信息，以提示用户无法进行业务行为。

- 15 可选的，业务行为是用户支付行为。

可选的，目标按键 711 为 Home 键、返回键或者确认键中的任一项。

本申请实施例提供的终端设备可用于执行上述的指纹认证方法，其内容和效果可参考方法部分，本申请实施例对此不做限制。

实施例六

- 20 本申请一实施例还提供一种计算机存储介质，存储介质包括计算机指令，当指令被计算机执行时，使得计算机实现如上述的指纹认证方法。

实施例七

本申请一实施例还提供一种计算机程序产品，包括：计算机指令，当指令被计算机执行时，使得计算机实现如上述的指纹认证方法。

- 25 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

- 30 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对

其限制；尽管参照前述各实施例对本发明进行了详细的说明，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，或者对其中部分或者全部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发明各实施例技术方案的范围。

权 利 要 求 书

1、一种指纹认证方法，其特征在于，包括：

通过目标按键获取用户指纹信息，并对获取到的所述指纹信息进行认证；

若对所述指纹信息认证成功，且获取到对所述目标按键的第一用户操作，

5 则不触发所述指纹信息认证成功之后的业务行为。

2、根据权利要求1所述的方法，其特征在于，所述第一用户操作为用户对所述目标按键的按下操作。

3、根据权利要求1所述的方法，其特征在于，还包括：

若对所述指纹信息认证成功，且获取到对所述目标按键的第二用户操作，

10 则触发所述指纹信息认证成功之后的业务行为。

4、根据权利要求3所述的方法，其特征在于，所述第二用户操作为用户从所述目标按键移开手指的操作。

5、根据权利要求1-4任一项所述的方法，其特征在于，所述通过目标按键获取用户指纹信息，并对获取到的所述指纹信息进行认证，包括：

15 获取合法的用户指纹模板；

对所述用户指纹信息和用户指纹模板进行匹配。

6、根据权利要求1-4任一项所述的方法，其特征在于，还包括：

若对所述指纹信息认证成功，且获取到对所述目标按键的第一用户操作，则推送提示信息，以提示用户无法进行所述业务行为。

20 7、根据权利要求1-4任一项所述的方法，其特征在于，所述业务行为是用户支付行为。

8、根据权利要求1-4任一项所述的方法，其特征在于，所述目标按键为Home键、返回键或者确认键中的任一项。

9、一种指纹认证装置，其特征在于，包括：

25 获取模块，用于通过目标按键获取用户指纹信息；

认证模块，用于对获取到的所述指纹信息进行认证；

第一处理模块，用于若对所述指纹信息认证成功，且获取到对所述目标按键的第一用户操作，则不触发所述指纹信息认证成功之后的业务行为。

30 10、根据权利要求9所述的装置，其特征在于，所述第一用户操作为用户对所述目标按键的按下操作。

11、根据权利要求 9 所述的装置，其特征在于，还包括：

第二处理模块，用于若对所述指纹信息认证成功，且获取到对所述目标按键的第二用户操作，则触发所述指纹信息认证成功之后的业务行为。

12、根据权利要求 11 所述的装置，其特征在于，所述第二用户操作为用户从所述目标按键移开手指的操作。

13、根据权利要求 9-12 任一项所述的装置，其特征在于，所述认证模块具体用于：

获取合法的用户指纹模板；

对所述用户指纹信息和用户指纹模板进行匹配。

14、根据权利要求 9-12 任一项所述的装置，其特征在于，还包括：

推送模块，用于若对所述指纹信息认证成功，且获取到对所述目标按键的第一用户操作，则推送提示信息，以提示用户无法进行所述业务行为。

15、根据权利要求 9-12 任一项所述的装置，其特征在于，所述业务行为是用户支付行为。

16、根据权利要求 9-12 任一项所述的装置，其特征在于，所述目标按键为 Home 键、返回键或者确认键中的任一项。

17、一种指纹识别模组，其特征在于，包括：目标按键和微控制单元 MCU；所述 MCU 用于：

通过所述目标按键获取用户指纹信息，对所述指纹信息进行认证，并将认证结果发送给处理器；

若通过所述目标按键获取到第一用户操作，则将所述第一用户操作发送给所述处理器，以使所述处理器根据所述认证结果确定对所述指纹信息认证成功时，根据所述第一用户操作不触发所述指纹信息认证成功之后的业务行为。

18、根据权利要求 17 所述的指纹识别模组，其特征在于，所述第一用户操作为用户对所述目标按键的按下操作。

19、根据权利要求 17 所述的指纹识别模组，其特征在于，所述 MCU 还用于：

若通过所述目标按键获取到第二用户操作，则将所述第二用户操作发送给所述处理器，以使所述处理器根据所述认证结果确定对所述指纹信息认证

成功时，根据所述第二用户操作触发所述指纹信息认证成功之后的业务行为。

20、根据权利要求 19 所述的指纹识别模组，其特征在于，所述第二用户操作为用户从所述目标按键移开手指的操作。

21、根据权利要求 17-20 任一项所述的指纹识别模组，其特征在于，所述 MCU 具体用于：

获取合法的用户指纹模板；

对所述用户指纹信息和用户指纹模板进行匹配。

22、根据权利要求 17-20 任一项所述的指纹识别模组，其特征在于，所述 MCU 还用于：

10 若对所述指纹信息认证成功，且获取到对所述目标按键的第一用户操作，则推送提示信息，以提示用户无法进行所述业务行为。

23、根据权利要求 17-20 任一项所述的指纹识别模组，其特征在于，所述业务行为是用户支付行为。

24、根据权利要求 17-20 任一项所述的指纹识别模组，其特征在于，所述目标按键为 Home 键、返回键或者确认键中的任一项。

25、一种终端设备，其特征在于，包括：指纹识别模组和处理器，所述指纹识别模组包括：目标按键和微控制单元 MCU；

所述 MCU 用于：

20 通过所述目标按键获取用户指纹信息，并对获取到的所述指纹信息进行认证，向所述处理器发送认证结果；

若通过所述目标按键获取到第一用户操作，则将所述第一用户操作发送给所述处理器；

所述处理器用于：

25 若根据所述认证结果确定对所述指纹信息认证成功，则根据所述第一用户操作不触发所述指纹信息认证成功之后的业务行为。

26、根据权利要求 25 所述的终端设备，其特征在于，所述第一用户操作为用户对所述目标按键的按下操作。

27、根据权利要求 25 所述的终端设备，其特征在于，

30 所述 MCU，还用于若通过所述目标按键获取到第二用户操作，则将所述第二用户操作发送给所述处理器；

所述处理器，还用于若根据所述认证结果确定对所述指纹信息认证成功时，根据所述第二用户操作触发所述指纹信息认证成功之后的业务行为。

28、根据权利要求 27 所述的终端设备，其特征在于，所述第二用户操作为用户从所述目标按键移开手指的操作。

5 29、根据权利要求 25-28 任一项所述的终端设备，其特征在于，所述 MCU 具体用于：

获取合法的用户指纹模板；

对所述用户指纹信息和用户指纹模板进行匹配。

10 30、根据权利要求 25-28 任一项所述的终端设备，其特征在于，所述 MCU 还用于：

若对所述指纹信息认证成功，且获取到对所述目标按键的第一用户操作，则推送提示信息，以提示用户无法进行所述业务行为。

31、根据权利要求 25-28 任一项所述的终端设备，其特征在于，所述业务行为是用户支付行为。

15 32、根据权利要求 25-28 任一项所述的终端设备，其特征在于，所述目标按键为 Home 键、返回键或者确认键中的任一项。

33、一种计算机存储介质，其特征在于，所述存储介质包括计算机指令，当所述指令被计算机执行时，使得所述计算机实现如权利要求 1 至 8 中任一项权利要求所述的指纹认证方法。

20

1/7

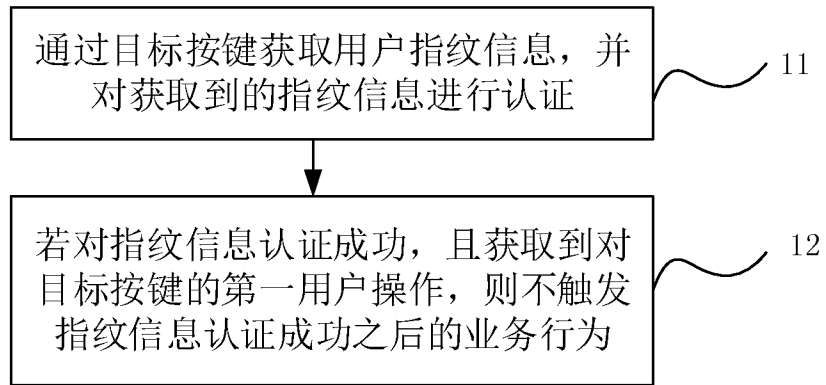


图 1

2/7

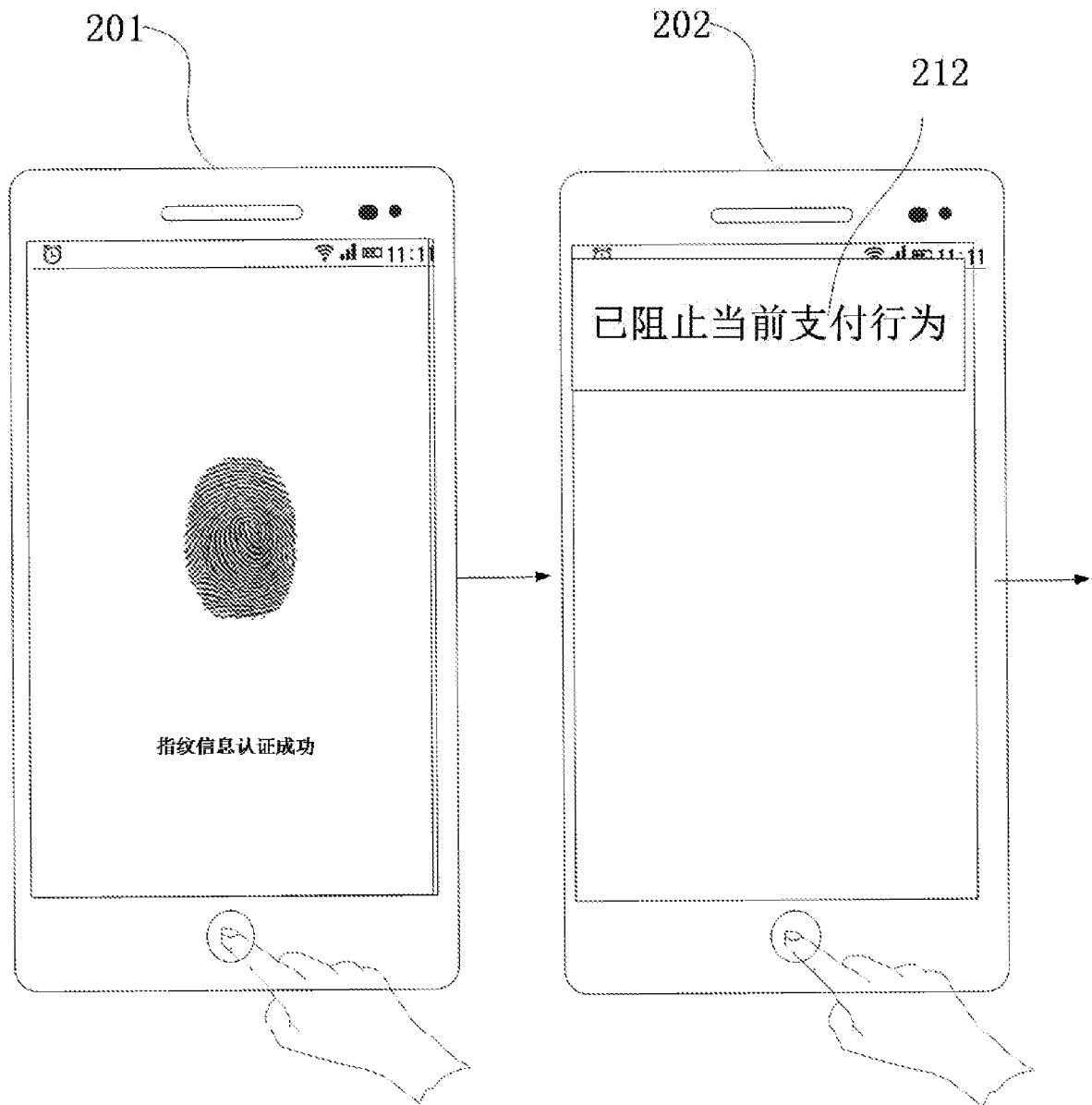


图 2

3/7

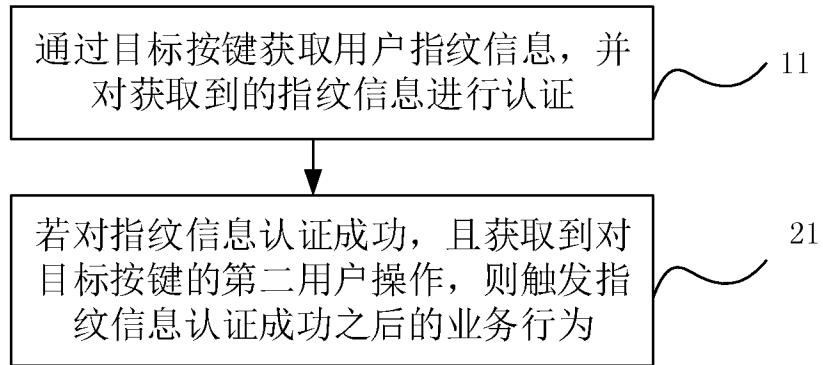


图 3

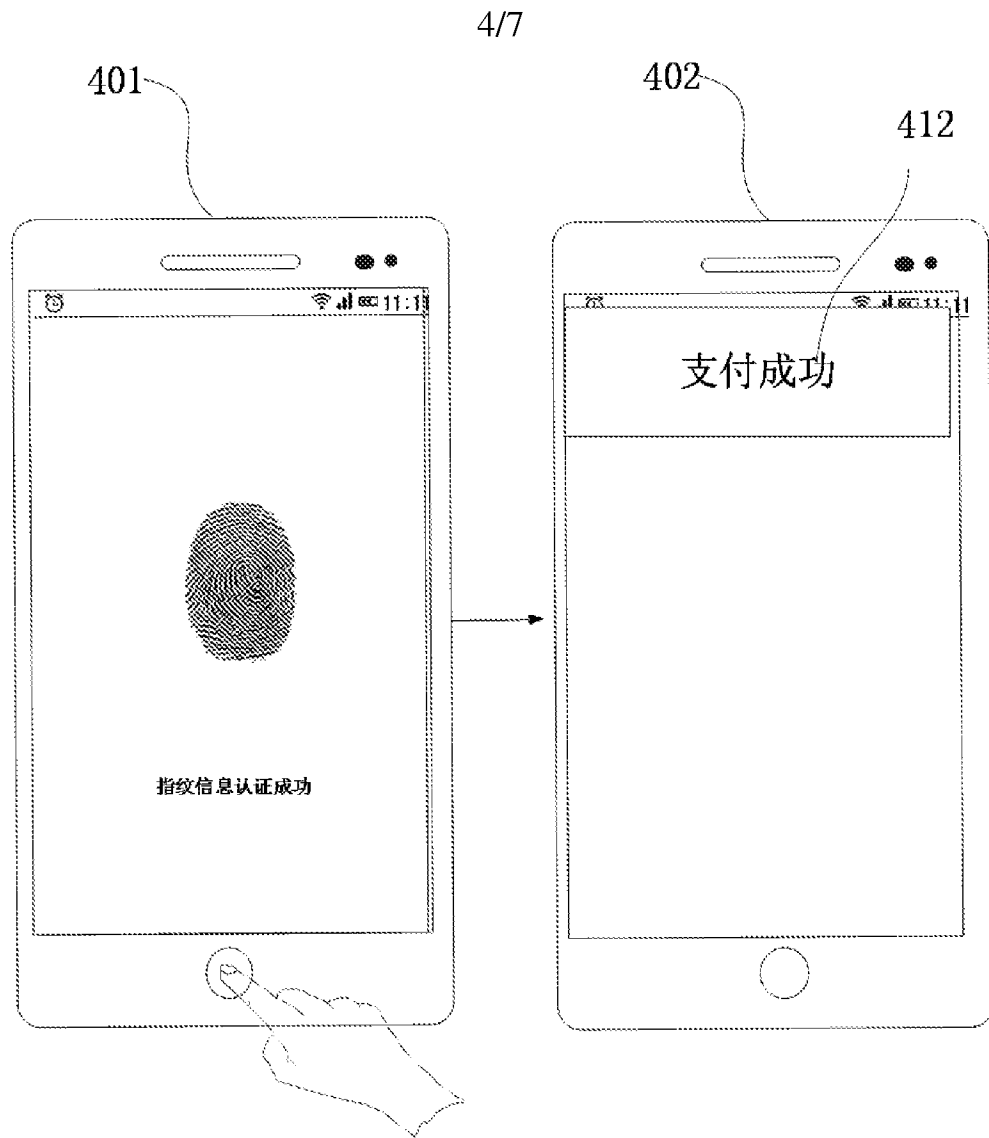


图 4

5/7

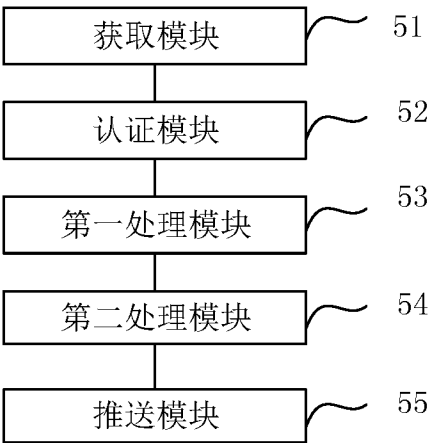


图 5

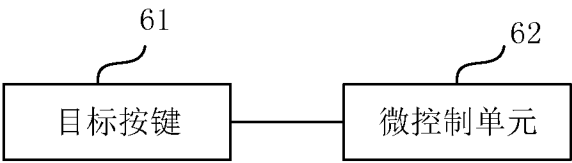


图 6

7/7

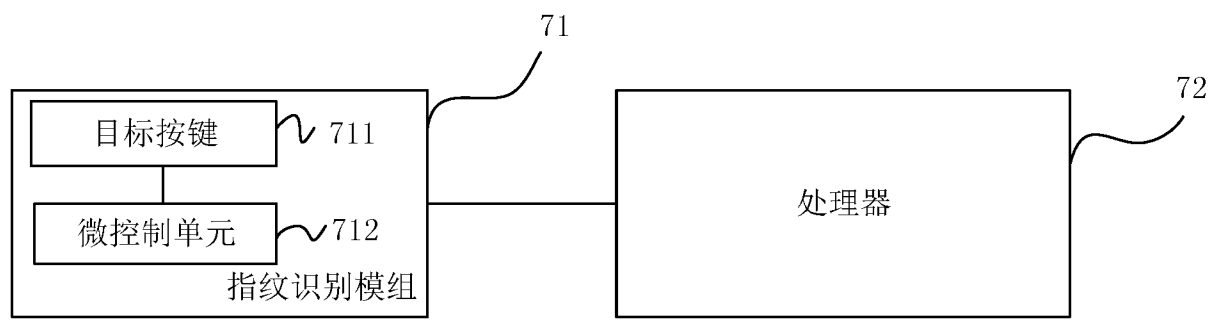


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/113803

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(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)

G06F21/-

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)

USTXT; EPTXT; CNTXT; CNABS; WOTXT; VEN; CNKI: 指纹, 认证, 支付, 按压, 不支付, 拒绝支付, 不触发, 按键, 误操作, 误支付, fingerprint, authenticate, payment, press, not pay, refuse to pay, not trigger, button, misoperation, pay error

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 106062701 A (SHENZHEN SUNWAVE TECHNOLOGY CO., LTD.) 26 October 2016 (2016-10-26) description, paragraphs [0067] and [0082]-[0091], and figures 6 and 7	1-33
Y	CN 105210072 A (LG ELECTRONICS INC.) 30 December 2015 (2015-12-30) description, paragraphs [0050], [0051] and [0062]-[0064], and figure 5	1-33
A	CN 105117631 A (LENOVO (BEIJING) CO., LTD.) 02 December 2015 (2015-12-02) entire document	1-33
A	CN 105989495 A (LI, Ming) 05 October 2016 (2016-10-05) entire document	1-33
A	US 2016335469 A1 (CHIANG, Kuo-Ching) 17 November 2016 (2016-11-17) entire document	1-33



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

“D” document cited by the applicant in the international application

“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

12 July 2019

Date of mailing of the international search report

30 July 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/113803

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106062701	A	26 October 2016	WO	2017177385	A1	19 October 2017
CN	105210072	A	30 December 2015	WO	2014185581	A1	20 November 2014
				US	9098735	B2	04 August 2015
				EP	2997517	A4	04 January 2017
				US	2014341447	A1	20 November 2014
				EP	2997517	A1	23 March 2016
				KR	20140134459	A	24 November 2014
				US	2015324627	A1	12 November 2015
				US	9477873	B2	25 October 2016
				CN	105210072	B	09 February 2018
CN	105117631	A	02 December 2015	CN	105117631	B	31 August 2018
				US	2017060259	A1	02 March 2017
CN	105989495	A	05 October 2016	KR	20180108758	A	04 October 2018
				EP	3428867	A1	16 January 2019
				WO	2017152818	A1	14 September 2017
				US	2019095926	A1	28 March 2019
US	2016335469	A1	17 November 2016	None			

国际检索报告

国际申请号

PCT/CN2018/113803

A. 主题的分类

G06F 21/32 (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)

G06F21/-

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))

USTXT;EPTXT;CNTXT;CNABS;WOTXT;VEN;CNKI:指纹, 认证, 支付, 按压, 不支付, 拒绝支付, 不触发, 按键, 误操作, 误支付, fingerprint, authenticate, payment, press, not pay, refuse to pay, not trigger, button, misoperation, pay error

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
Y	CN 106062701 A (深圳信炜科技有限公司) 2016年 10月 26日 (2016 - 10 - 26) 说明书第67、82-91段及图6-7	1-33
Y	CN 105210072 A (LG电子株式会社) 2015年 12月 30日 (2015 - 12 - 30) 说明书第50-51、62-64段及图5	1-33
A	CN 105117631 A (联想北京有限公司) 2015年 12月 2日 (2015 - 12 - 02) 全文	1-33
A	CN 105989495 A (李明) 2016年 10月 5日 (2016 - 10 - 05) 全文	1-33
A	US 2016335469 A1 (CHIANG, KUO-CHING) 2016年 11月 17日 (2016 - 11 - 17) 全文	1-33

☐ 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 7月 12日

国际检索报告邮寄日期

2019年 7月 30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

传真号 (86-10)62019451

受权官员

夏雪

电话号码 86-(20)-28950718

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/113803

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	106062701	A	2016年 10月 26日	WO	2017177385	A1	2017年 10月 19日
CN	105210072	A	2015年 12月 30日	WO	2014185581	A1	2014年 11月 20日
				US	9098735	B2	2015年 8月 4日
				EP	2997517	A4	2017年 1月 4日
				US	2014341447	A1	2014年 11月 20日
				EP	2997517	A1	2016年 3月 23日
				KR	20140134459	A	2014年 11月 24日
				US	2015324627	A1	2015年 11月 12日
				US	9477873	B2	2016年 10月 25日
				CN	105210072	B	2018年 2月 9日
CN	105117631	A	2015年 12月 2日	CN	105117631	B	2018年 8月 31日
				US	2017060259	A1	2017年 3月 2日
CN	105989495	A	2016年 10月 5日	KR	20180108758	A	2018年 10月 4日
				EP	3428867	A1	2019年 1月 16日
				WO	2017152818	A1	2017年 9月 14日
				US	2019095926	A1	2019年 3月 28日
US	2016335469	A1	2016年 11月 17日	无			

表 PCT/ISA/210 (同族专利附件) (2015年1月)