

(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 1 月 31 日 (31.01.2019)



(10) 国际公布号
WO 2019/020106 A1

(51) 国际专利分类号:

H04M 1/02 (2006.01) **G06K 9/00** (2006.01)
G06F 21/32 (2013.01) **H04L 29/06** (2006.01)

(21) 国际申请号: PCT/CN2018/097396

(22) 国际申请日: 2018 年 7 月 27 日 (27.07.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710627619.9 2017 年 7 月 28 日 (28.07.2017) CN

(71) 申请人: 惠州 TCL 移动通信有限公司 (HUIZHOU TCL MOBILE COMMUNICATION CO., LTD) [CN/CN]; 中国广东省惠州市仲恺高新区和畅七路西 86 号, Guangdong 516006 (CN)。

(72) 发明人: 晁 婷婷 (CHAO, Tingting); 中国广东省惠州市仲恺高新区和畅七路西 86 号, Guangdong 516006 (CN)。

(74) 代理人: 深圳市威世博知识产权代理事务所 (普通合伙) (CHINA WISPRO INTELLECTUAL

PROPERTY LLP.); 中国广东省深圳市南山区高新区粤兴三道 8 号中国地质大学产学研基地中地大楼 A806, Guangdong 518057 (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,

(54) Title: DUAL FINGERPRINT RECOGNITION-BASED AUTHENTICATION METHOD, MOBILE TERMINAL, AND STORAGE DEVICE

(54) 发明名称: 一种基于双指纹识别的验证方法、移动终端及存储装置

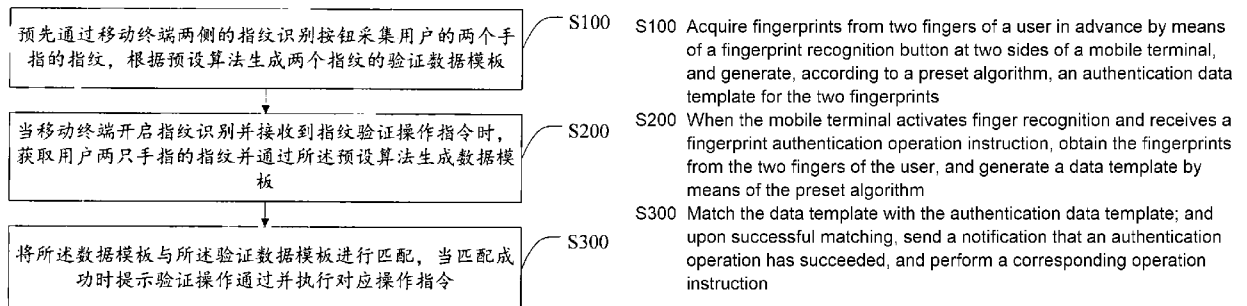


图 1

(57) Abstract: The present invention provides a dual fingerprint recognition-based authentication method, mobile terminal, and storage device. The authentication method comprises: acquiring fingerprints from two fingers of a user in advance by means of a fingerprint recognition button at two sides of a mobile terminal, and generating, according to a preset algorithm, an authentication data template for the two fingerprints; obtaining the fingerprints from the two fingers of the user at the mobile terminal and matching the same with the authentication data template by means of a data template; and upon successful matching, sending a notification that an authentication operation has succeeded, and performing a corresponding operation instruction. The present invention provides a fingerprint recognition chip at two sides of a frame of an electronic device. The invention does not occupy a position on a front screen of the electronic device and avoids the issue of a user unable to find a finger recognition position because the same is disposed on the back of the electronic device, thereby greatly improving the screen-to-body ratio of the electronic device. The use of dual fingerprint authentication also increases security during use of the electronic device.

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))。

(57) 摘要：本发明提供一种基于双指纹识别的验证方法、移动终端及存储装置，所述验证方法包括：预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板；在移动终端获取用户两只手指的指纹并通过数据模板与所述验证数据模板进行匹配，当匹配成功时提示验证操作通过并执行对应操作指令。本发明通过将指纹识别芯片放置于电子设备两侧边框的方式，既不占用电子设备正面的屏幕位置，也避免设置在电子设备背面而使用户找不到指纹识别的位置，大大提高电子设备的屏占比，且双指纹的识别验证增加了电子设备使用的安全性。

一种基于双指纹识别的验证方法、移动终端及存储装置

[1] 【技术领域】

[2] 本发明涉及移动终端指纹识别应用技术领域，具体涉及一种基于双指纹识别的验证方法、移动终端及存储装置。

[3] 【背景技术】

[4] 现在电子支付越来越普遍，电子设备支付很是受到广大用户的青睐。电子设备带来方便、快捷的同时，也存在很大的安全隐患，所以如何确保电子设备支付的安全就值得考虑。

[5] 目前电子设备上用到加密技术基本上有密码、手势和指纹。密码和手势都和人的主观有着密切联系，通过一定的操作还是可以破译，而指纹是人体生物特性，安全系数要比密码和手势高一些。

[6] 当前，指纹识别模块在电子设备上的位置有两种，一种在电子设备正面的下方，一般在Home键的位置；另一种在电子设备反面的上方，一般在后置摄像头下面。在电子设备正面的这种方案，会占据屏幕的位置，使得电子设备的屏占比降低。所以在一些全屏的电子设备上会采用第二种方案，将指纹识别模块放在反面，但这样就无法设计成凸起形状，用户不容易找到指纹识别的位置，用户使用起来不方便。

[7] 因此，现有技术还有待于改进和发展。

[8] 【发明内容】

[9] 本发明要解决的技术问题在于，针对现有技术的上述缺陷，提供一种基于双指纹识别的验证方法、移动终端及存储装置，旨在通过将指纹识别芯片放置于电子设备两侧边框的方式，既不占用电子设备正面的屏幕位置，也避免设置在电子设备背面而使用户找不到指纹识别的位置，大大提高电子设备的屏占比，且双指纹的识别验证增加了电子设备使用的安全性。

[10] 本发明解决技术问题所采用的技术方案如下：

[11] 一种存储装置，其中，存储装置中存储有程序数据，程序数据能够被执行以实

现如下操作：

- [12] 步骤A：预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板；
- [13] 步骤B：当移动终端开启指纹识别并接收到指纹验证操作指令时，获取用户两只手指的指纹并通过预设算法生成数据模板；
- [14] 步骤C：将数据模板与验证数据模板进行匹配，当匹配成功时提示验证操作通过并执行对应操作指令；
- [15] 其中，指纹识别按钮采集的指纹必须不同。
- [16] 一种基于双指纹识别的验证方法，其中，验证方法包括以下步骤：
- [17] 步骤A：预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板；
- [18] 步骤B：当移动终端开启指纹识别并接收到指纹验证操作指令时，获取用户两只手指的指纹并通过预设算法生成数据模板；
- [19] 步骤C：将数据模板与验证数据模板进行匹配，当匹配成功时提示验证操作通过并执行对应操作指令。
- [20] 一种移动终端，其中，移动终端两侧面设置有用采集和识别用户的两个手指指纹的指纹识别按钮；移动终端还包括：处理器、与处理器通信连接的存储器，存储器存储有计算机程序，计算机程序用于被执行时实现基于双指纹识别的验证方法；处理器用于调用存储器中的计算机程序以实现如下操作：预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板；当移动终端开启指纹识别并接收到指纹验证操作指令时，获取用户两只手指的指纹并通过预设算法生成数据模板；将数据模板与验证数据模板进行匹配，当匹配成功时提示验证操作通过并执行对应操作指令。
- [21] 本发明提供一种基于双指纹识别的验证方法、移动终端及存储装置，验证方法包括：预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板；在移动终端获取用户两只手指的指纹并通过数据模板与验证数据模板进行匹配，当匹配成功时提示验证操作通过

并执行对应操作指令。本发明通过将指纹识别芯片放置于电子设备两侧边框的方式，既不占用电子设备正面的屏幕位置，也避免设置在电子设备背面而使用户找不到指纹识别的位置，大大提高电子设备的屏占比，且双指纹的识别验证增加了电子设备使用的安全性。

[22] **【附图说明】**

[23] 图1是本发明基于双指纹识别的验证方法的较佳实施例的流程图。

[24] 图2是本发明基于双指纹识别的验证方法的具体实施流程图。

[25] 图3是本发明的移动终端双指纹识别按钮位置设置结构示意图。

[26] 图4是本发明的移动终端的功能原理框图。

[27] **【具体实施方式】**

[28] 为使本发明的目的、技术方案及优点更加清楚、明确，以下参照附图并举实施例对本发明进一步详细说明。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。

[29] 本发明较佳实施例所述的基于双指纹识别的验证方法，如图1所示，一种基于双指纹识别的验证方法，包括如下步骤：

[30] 步骤S100、预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板。

[31] 本发明的最大改进点在于：在移动终端的两侧的位置设置了两个指纹识别按键，而不是在移动终端正面的下方或者背面的上方；所述移动终端两侧的指纹识别按钮，如图3所示，按钮1是移动终端电源按钮，按钮3是音量调节按钮，按钮2是指纹识别按钮X，按钮4是指纹识别按钮Y。

[32] 具体实施时，如图2所示，所述步骤S100具体包括以下步骤：

[33] 步骤S101、通过移动终端两侧的指纹识别按钮X和指纹识别按钮Y分别采集用户的两个手指的指纹；

[34] 步骤S102、根据采集到的用户的两个手指的指纹，通过预设算法F生成两个指纹的验证数据模板XY，并存储在移动终端的存储器中用于指纹识别时进行匹配。

[35] 进一步地，在实际操作中，在移动终端的两侧的指纹识别按钮X和指纹识别按

钮Y采集用户两个手指的指纹，指纹可以是任意手指（一般是同一只手的拇指和食指），但指纹按钮X和指纹按钮Y采集的指纹必须不同；多次采取指纹根据预设算法F生成两个指纹的验证数据模板XY，并存储在移动终端的存储器中，用于指纹识别时进行匹配，之所以增加一个指纹的采集和识别，就是为了增加指纹识别的安全性。

[36] 步骤S200、当移动终端开启指纹识别并接收到指纹验证操作指令时，获取用户两只手指的指纹并通过所述预设算法生成数据模板。

[37] 具体实施时，如图2所示，所述步骤S200具体包括以下步骤：

[38] 步骤S201、预先在移动终端系统中设置开启指纹识别的验证操作目标，当执行操作目标时提示用户进行指纹输入；

[39] 步骤S202、当收到指纹验证操作指令时，获取用户输入的两只手指的指纹；

[40] 步骤S203、将获取的两只手指的指纹X1和Y1同样通过预设算法F生成数据模板X1Y1。

[41] 进一步地，在实际操作中，在移动终端开启指纹验证操作指令，执行操作时提示用户输入指纹信息，通过移动终端两侧的指纹识别按钮X和指纹识别按钮Y采集用户指纹信息，指纹信息采集完成后，由预设算法F生成数据模板X1Y1，用于和存储在存储器中的验证数据模板XY匹配。

[42] 步骤S300、将所述数据模板与所述验证数据模板进行匹配，当匹配成功时提示验证操作通过并执行对应操作指令。

[43] 另外，当所述数据模板与所述验证数据模板匹配失败时，提示用户验证失败，并提示用户再次输出指纹进行验证。

[44] 具体实施时，如图2所示，所述步骤S300具体包括以下步骤：

[45] 步骤S301、将通过预设算法F生成数据模板X1Y1与所述验证数据模板XY进行匹配；

[46] 步骤S302、当匹配成功时，提示验证操作通过并执行用户的对应操作指令；

[47] 步骤S302、当匹配失败时，提示用户验证失败，并提示用户再次输出指纹进行验证。

[48] 进一步地，在实际操作中，数据模板X1Y1与验证数据模板XY进行匹配时，当

且仅当移动终端两侧的指纹识别均通过验证时，表明验证操作通过，提示用户验证操作通过并执行用户的对应操作指令，主要应用于移动终端的电子支付时使用，如微信、支付宝等进行支付时的验证，还有移动终端中软件的加密，照片的加密等；当匹配失败时，提示用户验证失败，并返回步骤S200再次指纹进行验证；例如用户手指指纹不清晰、手出汗或者手上有水的情况下，匹配多次失败；当匹配失败次数达到预设次数（比如3次，可根据用户的要求进行设置）时，在预设时间（比如1小时）内禁止当前操作，直到预设时间后再次开启指纹识别验证。

- [49] 本发明还提供了一种移动终端，如图4所示，所述移动终端还包括：处理器(processor)10、存储器(memory)20、通信接口(Communications Interface)30和总线40；其中，
- [50] 所述处理器10、存储器20、通信接口30通过所述总线40完成相互间的通信；
- [51] 所述通信接口30用于所述移动终端的通信设备之间的信息传输；
- [52] 所述处理器10用于调用所述存储器20中的计算机程序，以执行上述各方法实施例所提供的方法，例如包括：预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板；当移动终端开启指纹识别并接收到指纹验证操作指令时，获取用户两只手指的指纹并通过所述预设算法生成数据模板；将所述数据模板与所述验证数据模板进行匹配，当匹配成功时提示验证操作通过并执行对应操作指令。
- [53] 本发明还提供一种存储装置，所述存储装置存储有计算机程序，所述计算机程序能够被执行以实现基于双指纹识别的验证方法。
- [54] 综上所述，本发明提供一种基于双指纹识别的验证方法、移动终端及存储装置，所述验证方法包括：预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板；在移动终端获取用户两只手指的指纹并通过数据模板与所述验证数据模板进行匹配，当匹配成功时提示验证操作通过并执行对应操作指令。本发明通过将指纹识别芯片放置于电子设备两侧边框的方式，既不占用电子设备正面的屏幕位置，也避免设置在电子设备背面而使用户找不到指纹识别的位置，大大提高电子设备的屏占比，

且双指纹的识别验证增加了电子设备使用的安全性。

[55] 当然，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硬件（如处理器，控制器等）来完成，所述的程序可存储于一计算机可读的存储介质中，该程序在执行时可包括如上述各方法实施例的流程。其中所述的存储介质可为存储器、磁碟、光盘等。

[56] 应当理解的是，本发明的应用不限于上述的举例，对本领域普通技术人员来说，可以根据上述说明加以改进或变换，所有这些改进和变换都应属于本发明所附权利要求的保护范围。

权利要求书

- [权利要求 1] 一种存储装置，其中，所述存储装置中存储有程序数据，所述程序数据能够被执行以实现如下操作：
- 步骤A：预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板；
- 步骤B：当移动终端开启指纹识别并接收到指纹验证操作指令时，获取用户两只手指的指纹并通过所述预设算法生成数据模板；
- 步骤C：将所述数据模板与所述验证数据模板进行匹配，当匹配成功时提示验证操作通过并执行对应操作指令；
- 其中，所述指纹识别按钮采集的指纹必须不同。
- [权利要求 2] 根据权利要求1所述的存储装置，其中，所述程序数据能够被执行以实现如下操作：
- 当所述数据模板与所述验证数据模板匹配失败时，提示用户验证失败，并提示用户再次输出指纹进行验证。
- [权利要求 3] 根据权利要求2所述的存储装置，其中，所述程序数据还能够被执行以实现如下操作：
- 当所述移动终端检测到用户指纹验证失败的次数达到预设次数时，在一预设时间内禁止当前操作，直到预设时间后再次开启指纹识别验证。
- [权利要求 4] 根据权利要求1所述的存储装置，其中，所述步骤A具体包括：
- 步骤A1：通过移动终端两侧的指纹识别按钮X和指纹识别按钮Y分别采集用户的两个手指的指纹；
- 步骤A2：根据采集到的用户的两个手指的指纹，通过预设算法F生成两个指纹的验证数据模板XY，并存储在移动终端的存储器中用于指纹识别时进行匹配。
- [权利要求 5] 根据权利要求4所述的存储装置，其中，所述步骤B具体包括：
- 步骤B1：预先在移动终端系统中设置开启指纹识别的验证操作目标，当执行操作目标时提示用户进行指纹输入；

步骤B2: 当收到指纹验证操作指令时, 获取用户输入的两只手指的指纹;

步骤B3: 将获取的两只手指的指纹X1和Y1同样通过预设算法F生成数据模板X1Y1。

[权利要求 6] 根据权利要求5所述的存储装置, 其中, 所述指纹验证操作指令包括移动终端解锁、APP解锁以及电子支付验证。

[权利要求 7] 根据权利要求5所述的存储装置, 其中, 所述步骤C具体包括:
步骤C1: 将通过预设算法F生成数据模板X1Y1与所述验证数据模板XY进行匹配;
步骤C2: 当匹配成功时, 提示验证操作通过并执行用户的对应操作指令。

[权利要求 8] 根据权利要求1所述的存储装置, 其中, 所述数据模板与所述验证数据模板进行匹配时, 当且仅当所述移动终端两侧的指纹识别均通过验证时, 表明验证操作通过。

[权利要求 9] 一种基于双指纹识别的验证方法, 其中, 所述验证方法包括以下步骤:
步骤A: 预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹, 根据预设算法生成两个指纹的验证数据模板;
步骤B: 当移动终端开启指纹识别并接收到指纹验证操作指令时, 获取用户两只手指的指纹并通过所述预设算法生成数据模板;
步骤C: 将所述数据模板与所述验证数据模板进行匹配, 当匹配成功时提示验证操作通过并执行对应操作指令。

[权利要求 10] 根据权利要求9所述的基于双指纹识别的验证方法, 其中, 所述步骤C还包括:
当所述数据模板与所述验证数据模板匹配失败时, 提示用户验证失败, 并提示用户再次输出指纹进行验证。

[权利要求 11] 根据权利要求10所述的基于双指纹识别的验证方法, 其中, 当所述移动终端检测到用户指纹验证失败的次数达到预设次数时, 在

一预设时间内禁止当前操作，直到预设时间后再次开启指纹识别验证。

[权利要求 12] 根据权利要求9所述的基于双指纹识别的验证方法，其中，所述步骤A具体包括：

步骤A1：通过移动终端两侧的指纹识别按钮X和指纹识别按钮Y分别采集用户的两个手指的指纹；

步骤A2：根据采集到的用户的两个手指的指纹，通过预设算法F生成两个指纹的验证数据模板XY，并存储在移动终端的存储器中用于指纹识别时进行匹配。

[权利要求 13] 根据权利要求12所述的基于双指纹识别的验证方法，其中，所述步骤B具体包括：

步骤B1：预先在移动终端系统中设置开启指纹识别的验证操作目标，当执行操作目标时提示用户进行指纹输入；

步骤B2：当收到指纹验证操作指令时，获取用户输入的两只手指的指纹；

步骤B3：将获取的两只手指的指纹X1和Y1同样通过预设算法F生成数据模板X1Y1。

[权利要求 14] 根据权利要求13所述的基于双指纹识别的验证方法，其中，所述指纹验证操作指令包括移动终端解锁、APP解锁以及电子支付验证。

[权利要求 15] 根据权利要求13所述的基于双指纹识别的验证方法，其中，所述步骤C具体包括：

步骤C1：将通过预设算法F生成数据模板X1Y1与上述验证数据模板XY进行匹配；

步骤C2：当匹配成功时，提示验证操作通过并执行用户的对应操作指令。

[权利要求 16] 根据权利要求9所述的基于双指纹识别的验证方法，其中，所述数据模板与上述验证数据模板进行匹配时，当且仅当所述移动终端

两侧的指纹识别均通过验证时，表明验证操作通过。

[权利要求 17]

一种移动终端，其中，所述移动终端两侧面设置有助于采集和识别用户的两个手指指纹的指纹识别按钮；还包括：处理器、与处理器通信连接的存储器，所述存储器存储有计算机程序，所述处理器用于调用所述存储器中的计算机程序以实现如下操作：

预先通过移动终端两侧的指纹识别按钮采集用户的两个手指的指纹，根据预设算法生成两个指纹的验证数据模板；

当移动终端开启指纹识别并接收到指纹验证操作指令时，获取用户两只手指的指纹并通过所述预设算法生成数据模板；

将所述数据模板与所述验证数据模板进行匹配，当匹配成功时提示验证操作通过并执行对应操作指令。

[权利要求 18]

根据权利要求17所述的移动终端，其中，所述移动终端还包括：通信接口和总线，所述处理器、所述存储器以及所述通信接口通过所述总线完成相互间的通信，所述通信接口用于所述移动终端的通信设备之间的信息传输。

[权利要求 19]

根据权利要求17所述的移动终端，其中，所述处理器还用于调用所述存储器中的计算机程序以实现如下操作：

当所述数据模板与所述验证数据模板匹配失败时，提示用户验证失败，并提示用户再次输出指纹进行验证。

[权利要求 20]

根据权利要求19所述的移动终端，其中，所述处理器还用于调用所述存储器中的计算机程序以实现如下操作：

当所述移动终端检测到用户指纹验证失败的次数达到预设次数时，在一预设时间内禁止当前操作，直到预设时间后再次开启指纹识别验证。

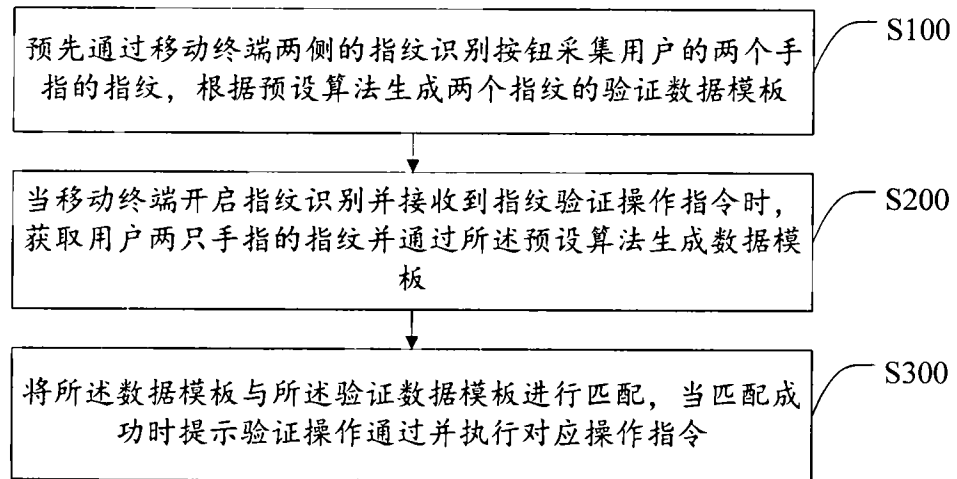


图 1

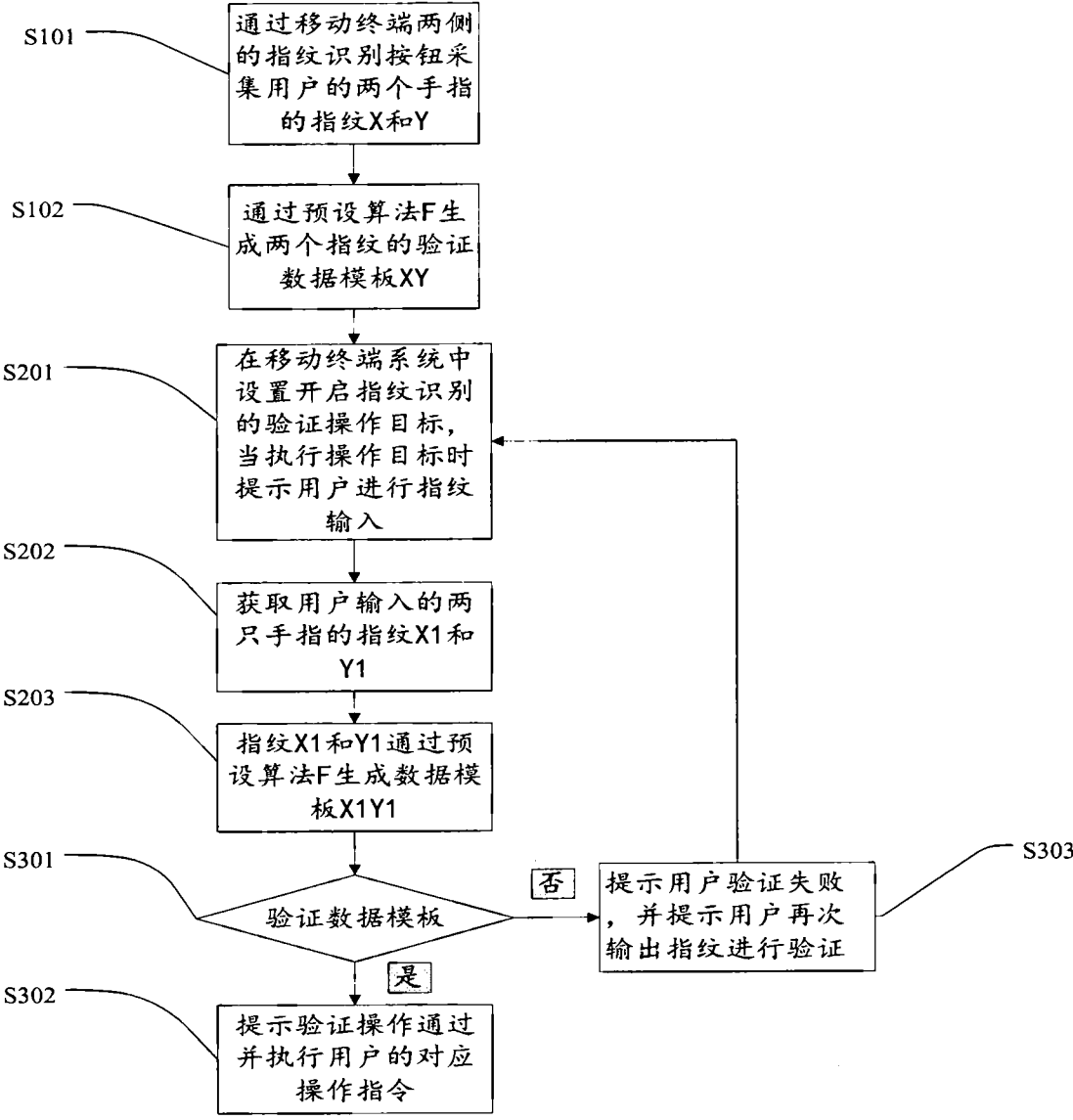


图 2

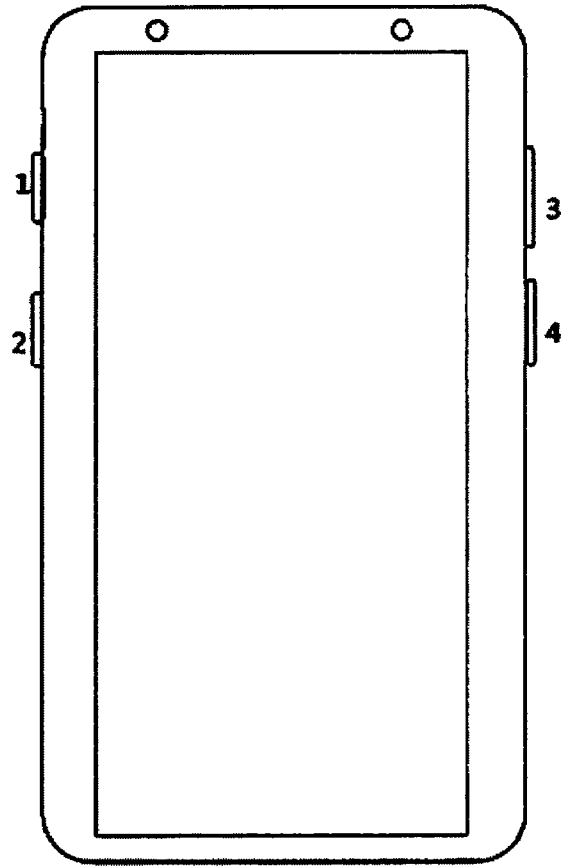


图 3

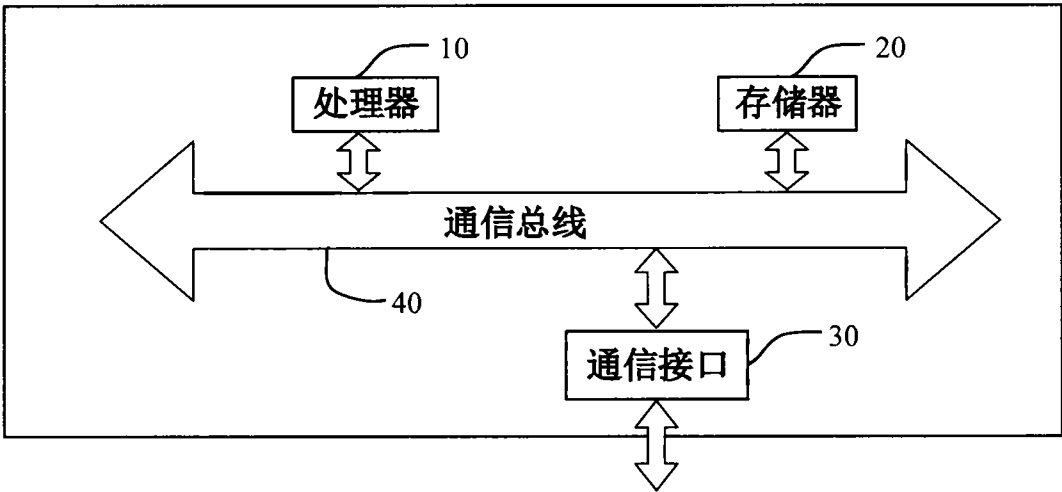


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/097396

A. CLASSIFICATION OF SUBJECT MATTER

H04M 1/02(2006.01)i; G06F 21/32(2013.01)i; G06K 9/00(2006.01)i; H04L 29/06(2006.01)n

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)

H04M; G06F; G06K; H04L

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)

CNTXT; CNABS; CNKI; VEN; USTXT; EPTXT; WOTXT: 终端, 手机, 指纹, 识别, 采集, 侧边, 两侧, 握持, 左侧, 右侧, 验证, 解锁, 支付, terminal, phone, cover, case, side, left, right, dactylogram, fingerprint, finger mark, sensor, validate, rim, unlock, pay

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107360276 A (HUIZHOU TCL MOBILE COMMUNICATION CO., LTD.) 17 November 2017 (2017-11-17) claims 1-10, description, paragraphs [0021]-[0034], and figures 1-4	1-20
X	CN 105654024 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) 08 June 2016 (2016-06-08) description, paragraphs [0046]-[0136], and figures 1-22	1-20
A	CN 105117698 A (NANCHANG O-FILM WISDOM INFORMATION INDUSTRY CO., LTD. ET AL.) 02 December 2015 (2015-12-02) entire document	1-20
A	US 2008226132 A1 (VALIDITY SENSORS INC.) 18 September 2008 (2008-09-18) 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

07 September 2018

Date of mailing of the international search report

10 October 2018

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/097396

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107360276	A	17 November 2017	None			
CN	105654024	A	08 June 2016	None			
CN	105117698	A	02 December 2015	None			
US	2008226132	A1	18 September 2008	US	8175345	B2	08 May 2012

国际检索报告

国际申请号

PCT/CN2018/097396

A. 主题的分类

H04M 1/02(2006.01)i; G06F 21/32(2013.01)i; G06K 9/00(2006.01)i; H04L 29/06(2006.01)n

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)

H04M; G06F; G06K; H04L

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))

CNTXT;CNABS;CNKI;VEN;USTXT;EPTXT;WOTXT: 终端, 手机, 指纹, 识别, 采集, 侧边, 两侧, 握持, 左侧, 右侧, 验证, 解锁, 支付, terminal, phone, cover, case, side, left, right, dactylogram, fingerprint, finger mark, sensor, validate, rim, unlock, pay

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
PX	CN 107360276 A (惠州TCL移动通信有限公司) 2017年 11月 17日 (2017 - 11 - 17) 权利要求1-10, 说明书第[0021]-[0034]段, 图1-4	1-20
X	CN 105654024 A (宇龙计算机通信科技深圳有限公司) 2016年 6月 8日 (2016 - 06 - 08) 说明书第[0046]-[0136]段, 图1-22	1-20
A	CN 105117698 A (南昌欧菲生物识别技术有限公司 等) 2015年 12月 2日 (2015 - 12 - 02) 全文	1-20
A	US 2008226132 A1 (VALIDITY SENSORS INC) 2008年 9月 18日 (2008 - 09 - 18) 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

2018年 9月 7日

国际检索报告邮寄日期

2018年 10月 10日

ISA/CN的名称和邮寄地址

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

受权官员

谢斐

传真号 (86-10)62019451

电话号码 (86-512)88996164

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/097396

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	107360276	A	2017年 11月 17日	无			
CN	105654024	A	2016年 6月 8日	无			
CN	105117698	A	2015年 12月 2日	无			
US	2008226132	A1	2008年 9月 18日	US	8175345	B2	2012年 5月 8日