

(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
2017 年 1 月 5 日 (05.01.2017)



(10) 国际公布号
WO 2017/000354 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2015/085849
- (22) 国际申请日: 2015 年 7 月 31 日 (31.07.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510369387.2 2015 年 6 月 29 日 (29.06.2015) CN
- (71) 申请人: 宇龙计算机通信科技(深圳)有限公司
(YULONG COMPUTER TELECOMMUNICATION
SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中
国广东省深圳市南山区科技园北区梦溪道 2 号,
Guangdong 518057 (CN)。
- (72) 发明人: 刘东海 (LIU, Donghai); 中国广东省深圳市
南山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。 汪智勇 (WANG, Zhiyong); 中国广东省深圳
市南山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。

(74) 代理人: 广州三环专利代理有限公司 (GUANG-
ZHOU SCIHEAD PATENT AGENT CO., LTD.); 中国
广东省广州市越秀区先烈中路 80 号汇华商贸大厦
1508 室, Guangdong 510070 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,
JP, KE, KG, KN, KP, KR, 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,

[见续页]

(54) Title: FINGERPRINT PASSWORD VERIFICATION METHOD, SYSTEM, AND TERMINAL

(54) 发明名称: 指纹密码的验证方法、系统和终端

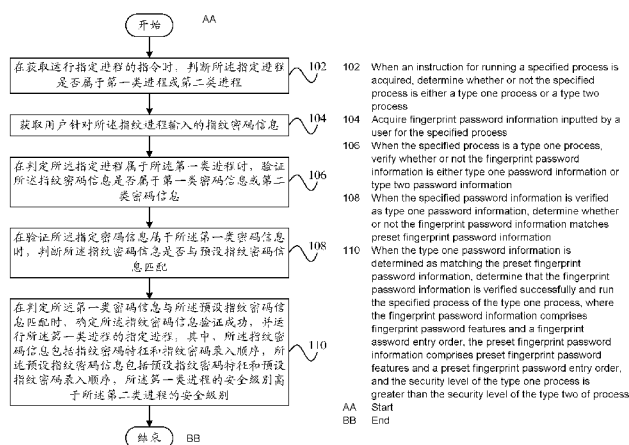


图 1

(57) Abstract: A fingerprint password verification method, system, and terminal. The fingerprint password verification method comprises: when an instruction for running a specified process is acquired, determining whether or not the specified process is either a type one process or a type two process (102); acquiring fingerprint password information inputted by a user for the specified process (104); when the specified process is determined as a type one process, verifying whether or not the fingerprint password information is either type one password information or type two password information (106); when the fingerprint password information is verified as type one password information, determining whether or not the type one password information matches preset fingerprint password information (108); when the type one password information is determined as matching the preset fingerprint password information, determining that the fingerprint password is verified successfully, and running the specified process of a first type of processes (110). The present solution enriches alarm notification solutions for fingerprint passwords while ensuring data security of a terminal and simplifies verification steps for the user.

(57) 摘要:

[见续页]

RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, **本国际公布:**
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, — 包括国际检索报告(条约第 21 条(3))。
TG)。

一种指纹密码的验证方法、系统和终端，其中，指纹密码的验证方法，包括：在获取运行指定进程的指令时，判断指定进程是否属于第一类进程或第二类进程（102）；获取用户针对指定进程输入的指纹密码信息（104）；在判定指定进程属于第一类进程时，验证指纹密码信息是否属于第一类密码信息或第二类密码信息（106）；在验证指纹密码信息属于第一类密码信息时，判断第一类密码信息是否与预设指纹密码信息匹配（108）；在判定第一类密码信息与预设指纹密码信息匹配时，确定指纹密码信息验证成功，并运行第一类进程的指定进程（110）。通过本方案，在保证终端的数据安全的同时，丰富了指纹密码的报警提示方案，简化了用户的验证步骤。

指纹密码的验证方法、系统和终端

本申请要求于 2015 年 06 月 29 日提交中国专利局，申请号为 201510369387.2、发明名称为“指纹密码的验证方法、系统和终端”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明涉及终端技术领域，具体而言，涉及一种指纹密码的验证方法、一种指纹密码的验证系统和一种终端。

10 背景技术

在相关技术中，指纹密码被广泛应用于终端设备的验证功能中，但是，指纹密码的验证过程通常是判断指纹密码信息是否与预设密码信息完全匹配，若匹配，则执行相应的进程，若不匹配，则退出验证过程，上述指纹密码的验证过程导致验证过程过于严格，尤其是对于安全要求低的进程，严格的指纹密码验证过程会增加进程运行的复杂度，另外，虽然进程经过严格的指纹密码的验证，但是在验证失败时，没有任何预警机制，对于用户的数据安全也存在极大隐患。

因此，如何设计一种能够保证数据安全，同时能够安全预警的指纹密码的验证方案成为亟待解决的技术问题。

20

发明内容

本发明正是基于上述技术问题至少之一，提出了一种新的能够保证数据安全，同时能够安全预警的指纹密码的验证方案，通过对于进程类型进行判断，以及对指纹密码信息进行判断，以确定运行进程或进行相应的报警提示，从而在保证数据安全的同时，实现了安全预警的效果。

25

有鉴于此，根据本发明的第一方面的实施例，提出了一种指纹密码的验证方法，包括：在获取运行指定进程的指令时，判断所述指定进程是否

属于第一类进程或第二类进程；获取用户针对所述指定进程输入的指纹密码信息；在判定所述指定进程属于所述第一类进程时，验证所述指纹密码信息是否属于第一类密码信息或第二类密码信息；在验证所述指纹密码信息属于所述第一类密码信息时，判断所述第一类密码信息是否与预设指纹密码信息匹配；在判定所述指纹密码信息与所述预设指纹密码信息匹配时，确定所述指纹密码信息验证成功，并运行所述第一类进程的指定进程，其中，所述指纹密码信息包括指纹密码特征和指纹密码录入顺序，所述预设指纹密码信息包括预设指纹密码特征和预设指纹密码录入顺序，所述第一类进程的安全级别高于所述第二类进程的安全级别。

5

在该技术方案中，通过对于进程类型进行判断，以及对指纹密码信息进行判断，以确定运行进程或进行相应的报警提示，从而在保证数据安全的同时，实现了安全预警的效果。

10

具体地，在进行指纹验证前，已经预先设定进程的类型，如将网银支付进程、私密数据查看进程和安全操作系统的相关进程设定为第一类进程，同时，如将快速拍照进程、录音进程、屏幕解锁进程、通信人信息查看进程和紧急拨号进程设定为第二类进程。

15

另外，用户将自己的指纹设定为第一类指纹信息，其中，第一类指纹信息包括用户对第一类进程中的每个进程设定的一组指纹密码（即预设指纹密码信息，包括指纹特征和指纹录入顺序），用户将亲友的指纹设定为第二类指纹信息。

20

其中，对于第一类进程的安全要求较高，用户在完成一次指纹信息的录入后，在验证过程中包括至少两次判断步骤，也即必须是用户自己的指纹信息，且与预设指纹信息完全匹配时，才能执行第一类进程的指定进程，否则，则需要继续判断是否运行进程或执行相应的报警提示，例如，在获取用户的亲友的指纹或用户自己的指纹后，不需要严格判断即可执行相应的进程，但是，如果既非用户自己的指纹，又非亲友的指纹，无论是第一类进程或第二类进程均主动发出报警提示信息，以保护数据安全。

25

在上述技术方案中，优选地，还包括：在判定所述指定进程属于所述第二类进程时，验证所述指纹密码信息是否属于所述第一类密码信息或所

述第二类密码信息；在验证所述指纹密码信息属于所述第一类密码信息或所述第二类密码信息时，确定所述指纹密码信息验证成功，并运行所述第二类进程的指定进程。

5 在该技术方案中，通过在运行第二类进程时，若获取第一类密码信息或第二类密码信息，均执行相应的进程，则在保证数据安全的同时，简化了用户的验证步骤，也即对于安全级别较低的进程，用户自己的指纹或亲友的指纹均能实现运行进程的功能，从而提升了用户的使用体验。

在上述技术方案中，优选地，还包括：在判定所述指纹密码信息不属于所述
10 所述第一类密码信息，或不属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第一类报警提示信息，其中，所述第一类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

在该技术方案中，通过在指纹密码不属于第一类密码信息或第二类密码信息时，发出第一类报警提示信息，实现了指纹验证过程的主动预警功能，
15 也即在检测到非用户本人或亲友要运行第一类进程或第二类进程时，对用户的数据存在极大的安全隐患，此时，发出强烈的报警提示来提示用户数据威胁，例如，终端同时发出振动提示、提示灯闪烁和铃声提示灯信息。

在上述技术方案中，优选地，还包括：在判定所述指定进程属于所述
20 第一类进程，且所述指纹密码信息属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第二类报警提示信息，其中，所述第二类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

在该技术方案中，通过在判定指定进程属于第一类进程，且指纹密码
25 信息属于第二类密码信息时，确定指纹密码信息验证失败，进一步地实现了指纹验证过程的主动预警功能，也即在检测到用户亲友运行第二类进程时，发出缓和且友好的报警提示，例如，终端发出光学提示信号，以提示亲友不具备运行高安全级别的进程的权限，同时，不会对用户造成严重的干扰。

在上述技术方案中，优选地，还包括：在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第一类密码信息时，在判定所述指纹密码信息与所述预设指纹密码信息不匹配时，确定所述指纹密码信息验证失败，并发出第三类报警提示信息，其中，所述第三类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

在该技术方案中，通过在判定第一类指纹密码信息与预设指纹密码信息不匹配时，确定验证失败且发出相应的第三类报警提示信息，更进一步地实现了指纹验证过程的主动预警功能，也即在判定用户本人运行安全级别较高的进程（第一类进程），但是用户输入指纹的顺序或特征不正确时，提示用户输入错误，其中，还可以在用户输入错误次数大于或等于预设次数时，锁定指纹密码的验证功能。

根据本发明的第二发明的实施例，还提出一种指纹密码的验证系统，包括：判断单元，用于在获取运行指定进程的指令时，判断所述指定进程是否属于第一类进程或第二类进程；获取单元，用于获取用户针对所述指定进程输入的指纹密码信息；验证单元，用于在判定所述指定进程属于所述第一类进程时，验证所述指纹密码信息是否属于第一类密码信息或第二类密码信息；所述判断单元还用于，在验证所述指纹密码信息属于所述第一类密码信息时，判断所述指纹密码信息是否与预设指纹密码信息匹配；所述指纹密码的验证系统还包括：确定单元，用于在判定所述第一类密码信息与所述预设指纹密码信息匹配时，确定所述指纹密码信息验证成功，并运行所述第一类进程的指定进程，其中，所述指纹密码信息包括指纹密码特征和指纹密码录入顺序，所述预设指纹密码信息包括预设指纹密码特征和预设指纹密码录入顺序，所述第一类进程的安全级别高于所述第二类进程的安全级别。

在该技术方案中，通过对于进程类型进行判断，以及对指纹密码信息进行判断，以确定运行进程或进行相应的报警提示，从而在保证数据安全的同时，实现了安全预警的效果。

具体地，在进行指纹验证前，已经预先设定进程的类型，如将网银支

付进程、私密数据查看进程和安全操作系统的相关进程设定为第一类进程，同时，如将快速拍照进程、录音进程、屏幕解锁进程、通信人信息查看进程和紧急拨号进程设定为第二类进程。

5 另外，用户将自己的指纹设定为第一类指纹信息，其中，第一类指纹信息包括用户对第一类进程中的每个进程设定的一组指纹密码（即预设指纹密码信息，包括指纹特征和指纹录入顺序），用户将亲友的指纹设定为第二类指纹信息。

10 其中，对于第一类进程的安全要求较高，用户在完成一次指纹信息的录入后，在验证过程中包括至少两次判断步骤，也即必须是用户自己的指纹信息，且与预设指纹信息完全匹配时，才能执行第一类进程的指定进程，否则，则需要继续判断是否运行进程或执行相应的报警提示，例如，在获取用户的亲友的指纹或用户自己的指纹后，不需要严格判断即可执行相应的进程，但是，如果既非用户自己的指纹，又非亲友的指纹，无论是第一类进程或第二类进程均主动发出报警提示信息，以保护数据安全。

15 在上述技术方案中，优选地，所述验证单元还用于：在判定所述指定进程属于所述第二类进程时，验证所述指纹密码信息是否属于所述第一类密码信息或所述第二类密码信息；所述确定单元还用于：在验证所述指纹密码信息属于所述第一类密码信息或所述第二类密码信息时，确定所述指纹密码信息验证成功，并运行所述第二类进程的指定进程。

20 在该技术方案中，通过在运行第二类进程时，若获取第一类密码信息或第二类密码信息，均执行相应的进程，则在保证数据安全的同时，简化了用户的验证步骤，也即对于安全级别较低的进程，用户自己的指纹或亲友的指纹均能实现运行进程的功能，从而提升了用户的使用体验。

25 在上述技术方案中，优选地，所述确定单元还包括：警报提示单元，用于在判定所述指纹密码信息不属于所述第一类密码信息，或不属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第一类报警提示信息，其中，所述第一类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

在该技术方案中，通过在指纹密码不属于第一类密码信息或第二类密

码信息时，发出第一类报警提示信息，实现了指纹验证过程的主动预警功能，也即在检测到非用户本人或亲友要运行第一类进程或第二类进程时，对用户的数据存在极大的安全隐患，此时，发出强烈的报警提示来提示用户数据威胁，例如，终端同时发出振动提示、提示灯闪烁和铃声提示灯信息。

在上述技术方案中，优选地，所述警报提示单元还用于：在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第二类报警提示信息，其中，所述第二类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

在该技术方案中，通过在判定指定进程属于第一类进程，且指纹密码信息属于第二类密码信息时，确定指纹密码信息验证失败，进一步地实现了指纹验证过程的主动预警功能，也即在检测到用户亲友运行第二类进程时，发出缓和且友好的报警提示，例如，终端发出光学提示信号，以提示亲友不具备运行高安全级别的进程的权限，同时，不会对用户造成严重的干扰。

在上述技术方案中，优选地，所述警报提示单元还用于：在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第一类密码信息时，在判定所述指纹密码信息与所述预设指纹密码信息不匹配时，确定所述指纹密码信息验证失败，并发出第三类报警提示信息，其中，所述第三类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

在该技术方案中，通过在判定第一类指纹密码信息与预设指纹密码信息不匹配时，确定验证失败且发出相应的第三类报警提示信息，更进一步地实现了指纹验证过程的主动预警功能，也即在判定用户本人运行安全级别较高的进程（第一类进程），但是用户输入指纹的顺序或特征不正确时，提示用户输入错误，其中，还可以在用户输入错误次数大于或等于预设次数时，锁定指纹密码的验证功能。

根据本发明的第三发明的实施例，还提出一种终端，包括通信总线、

输入装置、存储器以及处理器，其中：

所述通信总线，用于实现所述输入装置、存储器以及处理器之间的连接通信；

所述输入装置，用于获取用户针对指定进程输入的指纹密码信息；

5 所述存储器中存储一组程序代码，且所述终端调用所述存储器中存储的程序代码，用于执行以下操作：

所述处理器在获取运行指定进程的指令时，判断所述指定进程是否属于第一类进程或第二类进程；

所述输入装置获取用户针对所述指定进程输入的指纹密码信息；

10 所述处理器在判定所述指定进程属于所述第一类进程时，验证所述指纹密码信息是否属于第一类密码信息或第二类密码信息；

所述处理器在验证所述指定密码信息属于所述第一类密码信息时，判断所述指纹密码信息是否与预设指纹密码信息匹配；

15 所述处理器在判定所述指纹密码信息与所述预设指纹密码信息匹配时，确定所述指纹密码信息验证成功，并运行所述第一类进程的指定进程，其中，所述指纹密码信息包括指纹密码特征和指纹密码录入顺序，所述预设指纹密码信息包括预设指纹密码特征和预设指纹密码录入顺序，所述第一类进程的安全级别高于所述第二类进程的安全级别。

在上述技术方案中，优选地，还包括：

20 所述处理器在判定所述指定进程属于所述第二类进程时，验证所述指定密码信息是否属于所述第一类密码信息或所述第二类密码信息；

所述处理器在验证所述指定密码信息属于所述第一类密码信息或所述第二类密码信息时，确定所述指纹密码信息验证成功，并运行所述第二类进程的指定进程。

25 在上述技术方案中，优选地，还包括：

所述处理器在判定所述指纹密码信息不属于所述第一类密码信息，或不属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第一类报警提示信息，

其中，所述第一类报警提示信息包括光学提示信号、振动提示信号和

声音提示信号中的一种或多种的任意组合。

在上述技术方案中，优选地，还包括：

所述处理器在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并
5 发出第二类报警提示信息，

其中，所述第二类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

在上述技术方案中，优选地，还包括：

所述处理器在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第一类密码信息时，在判定所述指纹密码信息与所述预设
10 指纹密码信息不匹配时，确定所述指纹密码信息验证失败，并发出第三类报警提示信息，

其中，所述第三类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

15 通过以上技术方案，通过对于进程类型进行判断，以及对指纹密码信息进行判断，以确定运行进程或进行相应的报警提示，从而在保证数据安全的同时，实现了安全预警的效果。

附图说明

20 图 1 示出了根据本发明的一个实施例的指纹密码的验证方法的流程示意图；

图 2 示出了根据本发明的实施例的指纹密码的验证系统的示意框图；

图 3 示出了根据本发明的实施例的终端的示意框图；

图 4 示出了根据本发明的另一个实施例的指纹密码的验证方法的流程
25 示意图；

图 5 示出了根据本发明的另一个实施例的终端的示意框图。

具体实施方式

为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附

图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

图 1 示出了根据本发明的一个实施例的指纹密码的验证方法的流程示意图。

如图 1 所示，根据本发明的一个实施例的指纹密码的验证方法，包括：步骤 102，在获取运行指定进程的指令时，判断所述指定进程是否属于第一类进程或第二类进程；步骤 104，获取用户针对所述指定进程输入的指纹密码信息；步骤 106，在判定所述指定进程属于所述第一类进程时，验证所述指纹密码信息是否属于第一类密码信息或第二类密码信息；步骤 108，在验证所述指纹密码信息属于所述第一类密码信息时，判断所述指纹密码信息是否与预设指纹密码信息匹配；步骤 110，在判定所述第一类密码信息与所述预设指纹密码信息匹配时，确定所述指纹密码信息验证成功，并运行所述第一类进程的指定进程，其中，所述指纹密码信息包括指纹密码特征和指纹密码录入顺序，所述预设指纹密码信息包括预设指纹密码特征和预设指纹密码录入顺序，所述第一类进程的安全级别高于所述第二类进程的安全级别。

在该技术方案中，通过对于进程类型进行判断，以及对指纹密码信息进行判断，以确定运行进程或进行相应的报警提示，从而在保证数据安全的同时，实现了安全预警的效果。

具体地，在进行指纹验证前，已经预先设定进程的类型，如将网银支付进程、私密数据查看进程和安全操作系统的相关进程设定为第一类进程，同时，如将快速拍照进程、录音进程、屏幕解锁进程、通信人信息查看进程和紧急拨号进程设定为第二类进程。

另外，用户将自己的指纹设定为第一类指纹信息，其中，第一类指纹信息包括用户对第一类进程中的每个进程设定的一组指纹密码（即预设指纹密码信息，包括指纹特征和指纹录入顺序），用户将亲友的指纹设定为

第二类指纹信息。

其中，对于第一类进程的安全要求较高，用户在完成一次指纹信息的录入后，在验证过程中包括至少两次判断步骤，也即必须是用户自己的指纹信息，且与预设指纹信息完全匹配时，才能执行第一类进程的指定进程，
5 否则，则需要继续判断是否运行进程或执行相应的报警提示，例如，在获取用户的亲友的指纹或用户自己的指纹后，不需要严格判断即可执行相应的进程，但是，如果既非用户自己的指纹，又非亲友的指纹，无论是第一类进程或第二类进程均主动发出报警提示信息，以保护数据安全。

在上述技术方案中，优选地，还包括：在判定所述指定进程属于所述
10 第二类进程时，验证所述指纹密码信息是否属于所述第一类密码信息或所述第二类密码信息；在验证所述指纹密码信息属于所述第一类密码信息或所述第二类密码信息时，确定所述指纹密码信息验证成功，并运行所述第二类进程的指定进程。

在该技术方案中，通过在运行第二类进程时，若获取第一类密码信息
15 或第二类密码信息，均执行相应的进程，则在保证数据安全的同时，简化了用户的验证步骤，也即对于安全级别较低的进程，用户自己的指纹或亲友的指纹均能实现运行进程的功能，从而提升了用户的使用体验。

在上述技术方案中，优选地，还包括：在判定所述指纹密码信息不属于
20 所述第一类密码信息，或不属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第一类报警提示信息，其中，所述第一类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

在该技术方案中，通过在指纹密码不属于第一类密码信息或第二类密码
25 信息时，发出第一类报警提示信息，实现了指纹验证过程的主动预警功能，也即在检测到非用户本人或亲友要运行第一类进程或第二类进程时，对用户的数据存在极大的安全隐患，此时，发出强烈的报警提示来提示用户数据威胁，例如，终端同时发出振动提示、提示灯闪烁和铃声提示灯信息。

在上述技术方案中，优选地，还包括：在判定所述指定进程属于所述

第一类进程，且所述指纹密码信息属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第二类报警提示信息，其中，所述第二类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

5 在该技术方案中，通过在判定指定进程属于第一类进程，且指纹密码信息属于第二类密码信息时，确定指纹密码信息验证失败，进一步地实现了指纹验证过程的主动预警功能，也即在检测到用户亲友运行第二类进程时，发出缓和且友好的报警提示，例如，终端发出光学提示信号，以提示亲友不具备运行高安全级别的进程的权限，同时，不会对用户造成严重的
10 干扰。

在上述技术方案中，优选地，还包括：在判定所述指定进程属于所述
第一类进程，且所述指纹密码信息属于所述第一类密码信息时，在判定所
述指纹密码信息与所述预设指纹密码信息不匹配时，确定所述指纹密码信
息验证失败，并发出第三类报警提示信息，其中，所述第三类报警提示信
15 息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任
意组合。

在该技术方案中，通过在判定第一类指纹密码信息与预设指纹密码信
息不匹配时，确定验证失败且发出相应的第三类报警提示信息，更进一步
地实现了指纹验证过程的主动预警功能，也即在判定用户本人运行安全级
20 别较高的进程（第一类进程），但是用户输入指纹的顺序或特征不正确时，
提示用户输入错误，其中，还可以在用户输入错误次数大于或等于预设次
数时，锁定指纹密码的验证功能。

图 2 示出了根据本发明的实施例的指纹密码的验证系统的示意框图。

如图 2 所示，根据本发明的实施例的指纹密码的验证系统 200，包括：
25 判断单元 202，用于在获取运行指定进程的指令时，判断所述指定进程是
否属于第一类进程或第二类进程；获取单元 204，用于获取用户针对所述
指定进程输入的指纹密码信息；验证单元 206，用于在判定所述指定进程
属于所述第一类进程时，验证所述指纹密码信息是否属于第一类密码信息
或第二类密码信息；所述判断单元 202 还用于，在验证所述指纹密码信息

属于所述第一类密码信息时，判断所述指纹密码信息是否与预设指纹密码信息匹配；所述指纹密码的验证系统 200 还包括：确定单元 208，用于在判定所述第一类密码信息与所述预设指纹密码信息匹配时，确定所述指纹密码信息验证成功，并运行所述第一类进程的指定进程，其中，所述指纹密码信息包括指纹密码特征和指纹密码录入顺序，所述预设指纹密码信息包括预设指纹密码特征和预设指纹密码录入顺序，所述第一类进程的安全级别高于所述第二类进程的安全级别。

在该技术方案中，通过对于进程类型进行判断，以及对指纹密码信息进行判断，以确定运行进程或进行相应的报警提示，从而在保证数据安全的同时，实现了安全预警的效果。

具体地，在进行指纹验证前，已经预先设定进程的类型，如将网银支付进程、私密数据查看进程和安全操作系统的相关进程设定为第一类进程，同时，如将快速拍照进程、录音进程、屏幕解锁进程、通信人信息查看进程和紧急拨号进程设定为第二类进程。

另外，用户将自己的指纹设定为第一类指纹信息，其中，第一类指纹信息包括用户对第一类进程中的每个进程设定的一组指纹密码（即预设指纹密码信息，包括指纹特征和指纹录入顺序），用户将亲友的指纹设定为第二类指纹信息。

其中，对于第一类进程的安全要求较高，用户在完成一次指纹信息的录入后，在验证过程中包括至少两次判断步骤，也即必须是用户自己的指纹信息，且与预设指纹信息完全匹配时，才能执行第一类进程的指定进程，否则，则需要继续判断是否运行进程或执行相应的报警提示，例如，在获取用户的亲友的指纹或用户自己的指纹后，不需要严格判断即可执行相应的进程，但是，如果既非用户自己的指纹，又非亲友的指纹，无论是第一类进程或第二类进程均主动发出报警提示信息，以保护数据安全。

在上述技术方案中，优选地，所述验证单元 206 还用于：在判定所述指定进程属于所述第二类进程时，验证所述指纹密码信息是否属于所述第一类密码信息或所述第二类密码信息；所述确定单元 208 还用于：在验证所述指纹密码信息属于所述第一类密码信息或所述第二类密码信息时，确

定所述指纹密码信息验证成功，并运行所述第二类进程的指定进程。

在该技术方案中，通过在运行第二类进程时，若获取第一类密码信息或第二类密码信息，均执行相应的进程，则在保证数据安全的同时，简化了用户的验证步骤，也即对于安全级别较低的进程，用户自己的指纹或亲
5 友的指纹均能实现运行进程的功能，从而提升了用户的使用体验。

在上述技术方案中，优选地，所述确定单元 208 还包括：警报提示单元 208A，用于在判定所述指纹密码信息不属于所述第一类密码信息，或不
10 属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第一类报警提示信息，其中，所述第一类报警提示信息包括光学提示信号、
振动提示信号和声音提示信号中的一种或多种的任意组合。

在该技术方案中，通过在指纹密码不属于第一类密码信息或第二类密码信息时，发出第一类报警提示信息，实现了指纹验证过程的主动预警功能，也即在检测到非用户本人或亲友要运行第一类进程或第二类进程时，
15 对用户的数据存在极大的安全隐患，此时，发出强烈的报警提示来提示用户数据威胁，例如，终端同时发出振动提示、提示灯闪烁和铃声提示灯信息。

在上述技术方案中，优选地，所述警报提示单元 208A 还用于：在判定
20 所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第二类报警提示信息，其中，所述第二类报警提示信息包括光学提示信号、振动提示信号和
声音提示信号中的一种或多种的任意组合。

在该技术方案中，通过在判定指定进程属于第一类进程，且指纹密码信息属于第二类密码信息时，确定指纹密码信息验证失败，进一步地实现了
25 指纹验证过程的主动预警功能，也即在检测到用户亲友运行第二类进程时，发出缓和且友好的报警提示，例如，终端发出光学提示信号，以提示亲友不具备运行高安全级别的进程的权限，同时，不会对用户造成严重的
干扰。

在上述技术方案中，优选地，所述警报提示单元 208A 还用于：在判定
所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第一类

密码信息时，在判定所述指纹密码信息与所述预设指纹密码信息不匹配时，确定所述指纹密码信息验证失败，并发出第三类报警提示信息，其中，所述第三类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

- 5 在该技术方案中，通过在判定第一类指纹密码信息与预设指纹密码信息不匹配时，确定验证失败且发出相应的第三类报警提示信息，更进一步地实现了指纹验证过程的主动预警功能，也即在判定用户本人运行安全级别较高的进程（第一类进程），但是用户输入指纹的顺序或特征不正确时，提示用户输入错误，其中，还可以在用户输入错误次数大于或等于预设次数时，锁定指纹密码的验证功能。
- 10

图 3 示出了根据本发明的实施例的终端的示意框图。

如图 3 所示，根据本发明的实施例的终端 300，包括如上述任一项技术方案所述的指纹密码的验证系统 200。

- 图 4 示出了根据本发明的另一个实施例的指纹密码的验证方法的流程图。
- 15

- 如图 4 所示，根据本发明的另一个实施例的指纹密码的验证方法，包括：步骤 402，获取运行指定进程的指令；步骤 404，获取指纹密码信息；步骤 406，判断指定进程是否是第一类进程或第二类进程，若是第一类进程，则执行步骤 408，若是第二类进程，则执行步骤 424；步骤 408，判定指定进程是第一类进程；步骤 410，判断指纹密码信息是否是第一类密码信息，若是，则执行步骤 412，若否，则执行步骤 414；步骤 412，判定指纹密码信息与预设指纹密码是否匹配；步骤 414，判断指纹密码信息是否是第二类密码信息，若是，则执行步骤 420，若否，则执行步骤 422；步骤 416，运行第一类进程；步骤 418，发出第三类报警提示信息；步骤 420，发出第二类报警提示信息；步骤 422，发出第一类报警提示信息；步骤 424，判定指定进程是第二类进程；步骤 426，判断指纹密码信息是否是第一类密码信息或第二类密码信息，若是，则执行步骤 428，若否，则执行步骤 422；步骤 428，运行第二类进程。
- 20
- 25

图 5 示出了根据本发明的另一个实施例的终端的结构示意图。

如图 5 所示, 根据本发明的另一个实施例的终端, 包括: 通信总线 502、输入装置 503、存储器 504 以及处理器 501, 其中:

所述通信总线 502, 用于实现所述输入装置 503、存储器 504 以及处理器 501 之间的连接通信。

5 所述输入装置 503, 用于获取用户针对指定进程输入的指纹密码信息。

所述存储器 504 中存储一组程序代码, 且所述终端调用所述存储器 504 中存储的程序代码, 用于执行以下操作:

所述处理器 501 在获取运行指定进程的指令时, 判断所述指定进程是否属于第一类进程或第二类进程。

10 所述输入装置 503 获取用户针对所述指定进程输入的指纹密码信息。

所述处理器 501 在判定所述指定进程属于所述第一类进程时, 验证所述指纹密码信息是否属于第一类密码信息或第二类密码信息。

所述处理器 501 在验证所述指定密码信息属于所述第一类密码信息时, 判断所述指纹密码信息是否与预设指纹密码信息匹配。

15 所述处理器 501 在判定所述指纹密码信息与所述预设指纹密码信息匹配时, 确定所述指纹密码信息验证成功, 并运行所述第一类进程的指定进程。

其中, 所述指纹密码信息包括指纹密码特征和指纹密码录入顺序, 所述预设指纹密码信息包括预设指纹密码特征和预设指纹密码录入顺序, 所
20 述第一类进程的安全级别高于所述第二类进程的安全级别。

在上述技术方案中, 优选地, 还包括:

所述处理器 501 在判定所述指定进程属于所述第二类进程时, 验证所述指定密码信息是否属于所述第一类密码信息或所述第二类密码信息。

25 所述处理器 501 在验证所述指定密码信息属于所述第一类密码信息或所述第二类密码信息时, 确定所述指纹密码信息验证成功, 并运行所述第二类进程的指定进程。

在上述技术方案中, 优选地, 还包括:

所述处理器 501 在判定所述指纹密码信息不属于所述第一类密码信息, 或不属于所述第二类密码信息时, 确定所述指纹密码信息验证失败,

并发出第一类报警提示信息，

其中，所述第一类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

在上述技术方案中，优选地，还包括：

5 所述处理器 501 在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第二类报警提示信息。

其中，所述第二类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

10 在上述技术方案中，优选地，还包括：

所述处理器 501 在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第一类密码信息时，在判定所述指纹密码信息与所述预设指纹密码信息不匹配时，确定所述指纹密码信息验证失败，并发出第三类报警提示信息。

15 其中，所述第三类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

以上结合附图详细说明了本发明的技术方案，考虑到如何设计一种能够保证数据安全，同时能够安全预警的指纹密码的验证方案的技术问题。因此，本发明提出了一种指纹密码的验证方案和一种终端，通过对于进程
20 类型进行判断，以及对指纹密码信息进行判断，以确定运行进程或进行相应的报警提示，从而在保证数据安全的同时，实现了安全预警的效果。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明
25 的保护范围之内。

权利要求

1. 一种指纹密码的验证方法，其特征在于，包括：

5 在获取运行指定进程的指令时，判断所述指定进程是否属于第一类进程或第二类进程；

获取用户针对所述指定进程输入的指纹密码信息；

在判定所述指定进程属于所述第一类进程时，验证所述指纹密码信息是否属于第一类密码信息或第二类密码信息；

10 在验证所述指定密码信息属于所述第一类密码信息时，判断所述指纹密码信息是否与预设指纹密码信息匹配；

在判定所述指纹密码信息与所述预设指纹密码信息匹配时，确定所述指纹密码信息验证成功，并运行所述第一类进程的指定进程，

15 其中，所述指纹密码信息包括指纹密码特征和指纹密码录入顺序，所述预设指纹密码信息包括预设指纹密码特征和预设指纹密码录入顺序，所述第一类进程的安全级别高于所述第二类进程的安全级别。

2. 根据权利要求 1 所述的指纹密码的验证方法，其特征在于，还包括：

在判定所述指定进程属于所述第二类进程时，验证所述指定密码信息是否属于所述第一类密码信息或所述第二类密码信息；

20 在验证所述指定密码信息属于所述第一类密码信息或所述第二类密码信息时，确定所述指纹密码信息验证成功，并运行所述第二类进程的指定进程。

3. 根据权利要求 1 或 2 所述的指纹密码的验证方法，其特征在于，还包括：

25 在判定所述指纹密码信息不属于所述第一类密码信息，或不属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第一类报警提示信息，

其中，所述第一类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

4. 根据权利要求 1 或 2 所述的指纹密码的验证方法，其特征在于，还

包括:

在判定所述指定进程属于所述第一类进程, 且所述指纹密码信息属于所述第二类密码信息时, 确定所述指纹密码信息验证失败, 并发出第二类报警提示信息,

5 其中, 所述第二类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

5. 根据权利要求 1 或 2 所述的指纹密码的验证方法, 其特征在于, 还包括:

10 在判定所述指定进程属于所述第一类进程, 且所述指纹密码信息属于所述第一类密码信息时, 在判定所述指纹密码信息与所述预设指纹密码信息不匹配时, 确定所述指纹密码信息验证失败, 并发出第三类报警提示信息,

其中, 所述第三类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

15 6. 一种指纹密码的验证系统, 其特征在于, 包括:

判断单元, 用于在获取运行指定进程的指令时, 判断所述指定进程是否属于第一类进程或第二类进程;

获取单元, 用于获取用户针对所述指定进程输入的指纹密码信息;

20 验证单元, 用于在判定所述指定进程属于所述第一类进程时, 验证所述指纹密码信息是否属于第一类密码信息或第二类密码信息;

所述判断单元还用于, 在验证所述指纹密码信息属于所述第一类密码信息时, 判断所述第一类密码信息是否与预设指纹密码信息匹配;

所述指纹密码的验证系统还包括:

25 确定单元, 用于在判定所述指纹密码信息与所述预设指纹密码信息匹配时, 确定所述指纹密码信息验证成功, 并运行所述第一类进程的指定进程,

其中, 所述指纹密码信息包括指纹密码特征和指纹密码录入顺序, 所述预设指纹密码信息包括预设指纹密码特征和预设指纹密码录入顺序, 所述第一类进程的安全级别高于所述第二类进程的安全级别。

7. 根据权利要求 6 所述的指纹密码的验证系统，其特征在于，
所述验证单元还用于：

在判定所述指定进程属于所述第二类进程时，验证所述指定密码信息是否属于所述第一类密码信息或所述第二类密码信息；

5 所述确定单元还用于：

在验证所述指定密码信息属于所述第一类密码信息或所述第二类密码信息时，确定所述指纹密码信息验证成功，并运行所述第二类进程的指定进程。

10 8. 根据权利要求 6 或 7 所述的指纹密码的验证系统，其特征在于，
所述确定单元还包括：

警报提示单元，用于在判定所述指纹密码信息不属于所述第一类密码信息，或不属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第一类报警提示信息，

15 其中，所述第一类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

9. 根据权利要求 6 或 7 所述的指纹密码的验证系统，其特征在于，
所述警报提示单元还用于：

20 在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第二类报警提示信息，

其中，所述第二类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

10. 根据权利要求 6 或 7 所述的指纹密码的验证系统，其特征在于，
所述警报提示单元还用于：

25 在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第一类密码信息时，在判定所述指纹密码信息与所述预设指纹密码信息不匹配时，确定所述指纹密码信息验证失败，并发出第三类报警提示信息，

其中，所述第三类报警提示信息包括光学提示信号、振动提示信号和

声音提示信号中的一种或多种的任意组合。

11. 一种终端，其特征在于，包括通信总线、输入装置、存储器以及处理器，其中：

5 所述通信总线，用于实现所述输入装置、存储器以及处理器之间的连接通信；

所述输入装置，用于获取用户针对指定进程输入的指纹密码信息；

所述存储器中存储一组程序代码，且所述终端调用所述存储器中存储的程序代码，用于执行以下操作：

10 所述处理器在获取运行指定进程的指令时，判断所述指定进程是否属于第一类进程或第二类进程；

所述输入装置获取用户针对所述指定进程输入的指纹密码信息；

所述处理器在判定所述指定进程属于所述第一类进程时，验证所述指纹密码信息是否属于第一类密码信息或第二类密码信息；

15 所述处理器在验证所述指定密码信息属于所述第一类密码信息时，判断所述指纹密码信息是否与预设指纹密码信息匹配；

所述处理器在判定所述指纹密码信息与所述预设指纹密码信息匹配时，确定所述指纹密码信息验证成功，并运行所述第一类进程的指定进程，

20 其中，所述指纹密码信息包括指纹密码特征和指纹密码录入顺序，所述预设指纹密码信息包括预设指纹密码特征和预设指纹密码录入顺序，所述第一类进程的安全级别高于所述第二类进程的安全级别。

12. 根据权利要求 11 所述的终端，其特征在于，还包括：

所述处理器在判定所述指定进程属于所述第二类进程时，验证所述指定密码信息是否属于所述第一类密码信息或所述第二类密码信息；

25 所述处理器在验证所述指定密码信息属于所述第一类密码信息或所述第二类密码信息时，确定所述指纹密码信息验证成功，并运行所述第二类进程的指定进程。

13. 根据权利要求 11 或 12 所述的终端，其特征在于，还包括：

所述处理器在判定所述指纹密码信息不属于所述第一类密码信息，或不属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出

第一类报警提示信息，

其中，所述第一类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

14. 根据权利要求 11 或 12 所述的终端，其特征在于，还包括：

5 所述处理器在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第二类密码信息时，确定所述指纹密码信息验证失败，并发出第二类报警提示信息，

其中，所述第二类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

10 15. 根据权利要求 11 或 12 所述的终端，其特征在于，还包括：

所述处理器在判定所述指定进程属于所述第一类进程，且所述指纹密码信息属于所述第一类密码信息时，在判定所述指纹密码信息与所述预设指纹密码信息不匹配时，确定所述指纹密码信息验证失败，并发出第三类报警提示信息，

15 其中，所述第三类报警提示信息包括光学提示信号、振动提示信号和声音提示信号中的一种或多种的任意组合。

- 1/3 -

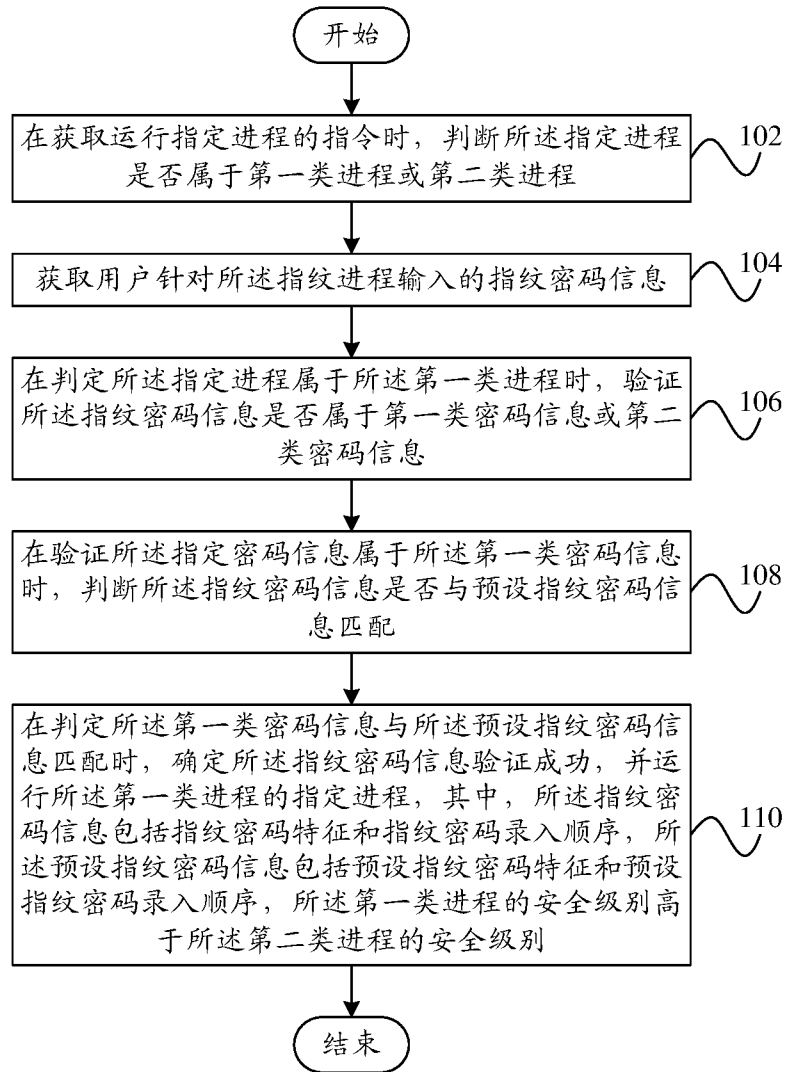


图 1

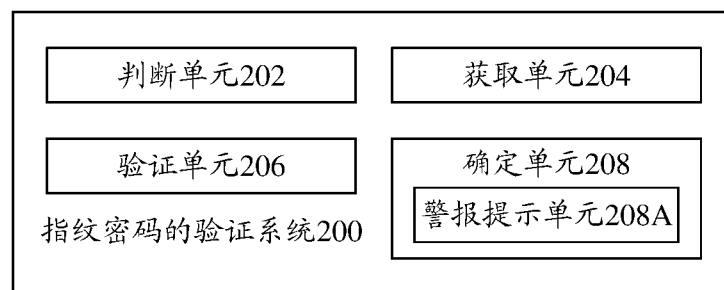


图 2

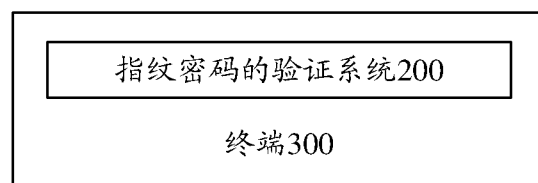


图 3

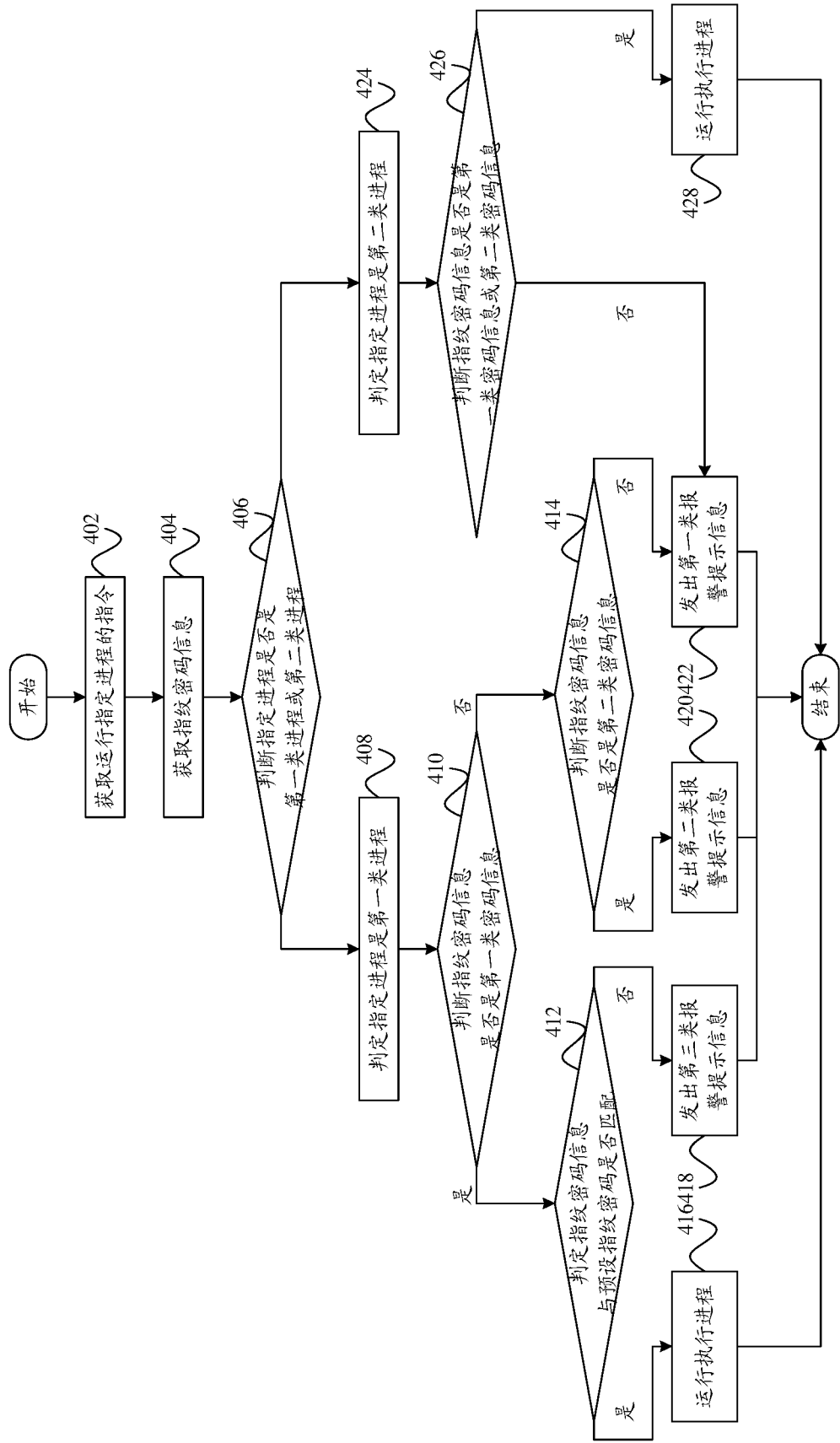


图 4

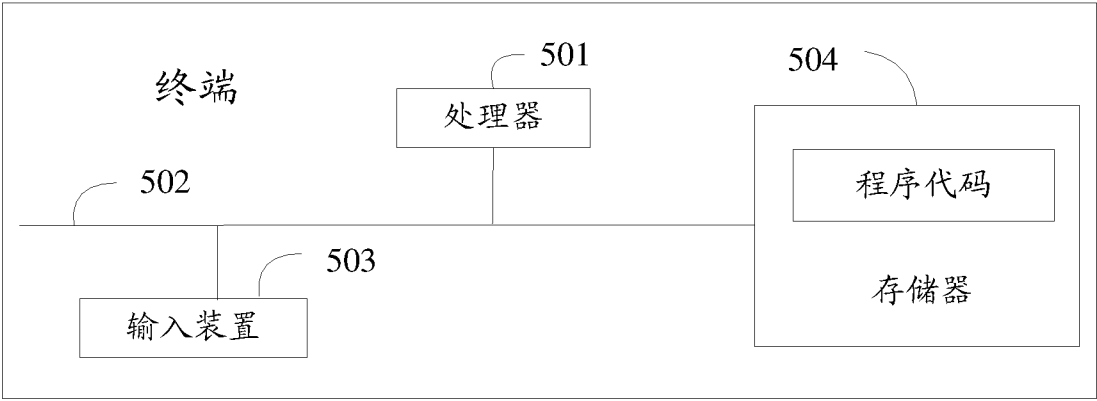


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/085849

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) 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)

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)

WPI, EPODOC, CNPAT, CNKI: first, second, matching, alarm, different, key, security, level, pass, password

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101447051 A (LENOVO (BEIJING) CO., LTD.), 03 June 2009 (03.06.2009), claims 1-6, and description, page 4, paragraph 1 to page 8, paragraph 4	1-15
A	CN 104392166 A (SHENZHEN ZTE MOBILE TELECOM CO., LTD.), 04 March 2015 (04.03.2015), the whole document	1-15
A	CN 104537291 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 22 April 2015 (22.04.2015), the whole document	1-15
A	CN 102314564 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.), 11 January 2012 (11.01.2012), the whole document	1-15
A	US 2013055379 A1 (ADAMS, N.P. et al.), 28 February 2013 (28.02.2013), the whole document	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 15 February 2016 (15.02.2016)	Date of mailing of the international search report 29 February 2016 (29.02.2016)
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 SU, Fei Telephone No.: (86-10) 62413632

International application No.
PCT/CN2015/085849

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2015/085849

A. 主题的分类

H04L 9/32 (2006.01) 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)

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))

WPI, EPDOC, CNPAT, CNKI: 密码, 密钥, 第一, 第二, 匹配, 安全, 级别, 警报, 报警, different, key, security, level, pass, password

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
A	CN 101447051 A (联想北京有限公司) 2009年 6月 3日 (2009 - 06 - 03) 权利要求1-6, 说明书第4第1段-第8页第4段	1-15
A	CN 104392166 A (深圳市中兴移动通信有限公司) 2015年 3月 4日 (2015 - 03 - 04) 全文	1-15
A	CN 104537291 A (宇龙计算机通信科技深圳有限公司) 2015年 4月 22日 (2015 - 04 - 22) 全文	1-15
A	CN 102314564 A (百度在线网络技术北京有限公司) 2012年 1月 11日 (2012 - 01 - 11) 全文	1-15
A	US 2013055379 A1 (ADAMS, NEIL PATRICK 等) 2013年 2月 28日 (2013 - 02 - 28) 全文	1-15

☐ 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

2016年 2月 15日

国际检索报告邮寄日期

2016年 2月 29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

授权官员

苏菲

传真号 (86-10) 62019451

电话号码 (86-10) 62413632

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/085849

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	101447051	A	2009年 6月 3日	无	
CN	104392166	A	2015年 3月 4日	无	
CN	104537291	A	2015年 4月 22日	无	
CN	102314564	A	2012年 1月 11日	无	
US	2013055379	A1	2013年 2月 28日	无	

表 PCT/ISA/210 (同族专利附件) (2009年7月)