

(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 2 月 2 日 (02.02.2017)



(10) 国际公布号
WO 2017/016033 A1

- (51) 国际专利分类号:
G06F 21/32 (2013.01)
- (21) 国际申请号:
PCT/CN2015/088492
- (22) 国际申请日:
2015 年 8 月 30 日 (30.08.2015)
- (25) 申请语言:
中文
- (26) 公布语言:
中文
- (30) 优先权:
201510460556.3 2015 年 7 月 30 日 (30.07.2015) 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)。 郭建军 (GUO, Jianjun); 中国广东省深圳市
南山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。 吴殿清 (WU, Dianqing); 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

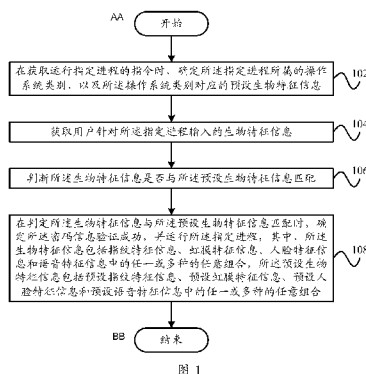
市南山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。

- (74) 代理人: 北京友联知识产权代理事务所(普通合
伙) (YOU LINK INTELLECTUAL PROPERTY
LAW FIRM); 中国北京市海淀区学清路 8 号科技财
富中心 A 座 506 室尚志峰, Beijing 100192 (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, HU, IE,
IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,

[见续页]

(54) Title: PASSWORD INFORMATION AUTHENTICATION METHOD, PASSWORD INFORMATION AUTHENTICATION
SYSTEM, AND TERMINAL

(54) 发明名称: 密码信息的验证方法、密码信息的验证系统和终端



102 UPON OBTAINING INSTRUCTION TO RUN DESIGNATED PROCESS, THE
TYPE OF OPERATING SYSTEM TO WHICH DESIGNATED PROCESS BELONGS
AND PRESET BIOMETRIC FEATURE INFORMATION CORRESPONDING TO
OPERATING SYSTEM TYPE ARE DETERMINED
104 BIOMETRIC FEATURE INFORMATION INPUTTED BY USER IN
CONNECTION WITH DESIGNATED PROCESS IS OBTAINED
106 IT IS DETERMINED WHETHER BIOMETRIC FEATURE INFORMATION
MATCHES PRESET BIOMETRIC FEATURE INFORMATION
108 IF IT IS DETERMINED THAT BIOMETRIC FEATURE INFORMATION
MATCHES PRESET BIOMETRIC FEATURE INFORMATION, THEN PASSWORD
INFORMATION AUTHENTICATION IS DETERMINED TO BE SUCCESSFUL AND
DESIGNATED PROCESS IS RUN; BIOMETRIC FEATURE INFORMATION
COMPRISES ANY COMBINATION OF ANY ONE OR SEVERAL OF FINGERPRINT
FEATURE INFORMATION, IRIS FEATURE INFORMATION, FACIAL FEATURE
INFORMATION, AND VOICE FEATURE INFORMATION; SAID PRESET
BIOMETRIC FEATURE INFORMATION COMPRISES ANY COMBINATION OF
ANY ONE OR SEVERAL OF PRESET FINGERPRINT FEATURE INFORMATION,
PRESET IRIS FEATURE INFORMATION, PRESET FACIAL FEATURE
INFORMATION, AND PRESET VOICE FEATURE INFORMATION
AA START
BB END

图 1

(57) Abstract: Provided are a password information authentication method, a password information authentication system, and a terminal, said password information authentication method comprising: upon obtaining an instruction to run a designated process, determining the type of operating system to which the designated process belongs, and preset biometric feature information corresponding to the operating system type (102); obtaining biometric feature information inputted by a user in connection with the designated process (104); determining whether the biometric feature information matches the preset biometric feature information (106); if it is determined that the biometric feature information matches the preset biometric feature information, then determining the password information authentication to be successful and running the designated process, said biometric feature information comprising any combination of any one or several of fingerprint feature information, iris feature information, facial feature information, and voice feature information (108). The method improves data security in terminals having multiple operating systems; at the same time, the steps of encryption and decryption are simplified, improving user experience.

(57) 摘要:

[见续页]



WO 2017/016033 A1

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)。

一种密码信息的验证方法、密码信息的验证系统和终端，其中，所述密码信息的验证方法，包括：在获取运行指定进程的指令时，确定指定进程所属的操作系统类别，以及操作系统类别对应的预设生物特征信息（102）；获取用户针对指定进程输入的生物特征信息（104）；判断生物特征信息是否与预设生物特征信息匹配（106）；在判定生物特征信息与预设生物特征信息匹配时，确定密码信息验证成功，并运行指定进程，其中，所述生物特征信息包括指纹特征信息、虹膜特征信息、人脸特征信息和语音特征信息中的任一或多种的任意组合（108）。该方法提高了多操作系统终端的数据安全，同时简化了加密步骤和解密步骤，提升了用户的使用体验。

密码信息的验证方法、密码信息的验证系统和终端

5 技术领域

本发明涉及密码验证技术领域，具体而言，涉及一种密码信息的验证方法，一种密码信息的验证系统和一种终端。

背景技术

10 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，而对于多操作系
15 统的终端而言，进程所在的操作系统决定了该进程的安全等级，如果根据相关技术对于每个进程进行指纹加密和指纹解密，明显会增加终端的功耗和运算量，另外，也会增加用户的操作步骤和记忆的难度。

因此，如何设计一种能够保证数据安全和操作便捷的密码信息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，提出了一种新的密码信息的验证方案，通过针对指定进程所述的操作系统进行生物特征信息的匹配，实现了对任一操作系统内的进程进行统一验证方式，在保证进程的数据安
25 全的同时，简化了用户的验证步骤，提升了用户的使用体验。

实现上述目的，根据本发明的第一方面的实施例，提供了一种密码信息的验证方法，包括：在获取运行指定进程的指令时，确定所述指定进程所属的操作系统类别，以及所述操作系统类别对应的预设生物特征信息；获取用户针对所述指定进程输入的生物特征信息；判断所述生物特征信息

是否与所述预设生物特征信息匹配；在判定所述生物特征信息与所述预设生物特征信息匹配时，确定所述密码信息验证成功，并运行所述指定进程，其中，所述生物特征信息包括指纹特征信息、虹膜特征信息、人脸特征信息和语音特征信息中的任一或多种的任意组合，所述预设生物特征信息包括预设指纹特征信息、预设虹膜特征信息、预设人脸特征信息和预设语音特征信息中的任一或多种的任意组合。

在该技术方案中，通过针对指定进程所述的操作系统进行生物特征信息的匹配，实现了对任一操作系统内的进程进行统一验证方式，在保证进程的数据安全的同时，简化了用户的验证步骤，提升了用户的使用体验。

具体地，对于多个操作系统的终端而言，终端用户根据个人需求和使用习惯将应用进程划分于相应的操作系统中，终端中已预先设置了每个操作系统的验证制式，例如，终端中的操作系统 A 和操作系统 B 分别对应于高级和低级两种安全等级，在用户的生物特征信息与预设生物特征信息完全匹配时（包括生物特征信息的个数、输入顺序和特征信息等），才能完成对操作系统 A 中的应用进程的验证过程，对于操作系统 B 而言，在输入的生物特征信息为用户本人或用户亲属指纹时，上述生物特征信息中的任一个均属于预设生物特征信息，则完成对操作系统 B 的验证过程。

在上述技术方案中，优选地，在获取运行指定进程的指令时，确定所述指定进程所属的操作系统，以及所述操作系统对应的预设生物特征信息，具体包括以下步骤：在确定所述指定进程属于第一类操作系统时，确定所述第一类操作系统对应的所述预设生物特征信息中的第一预设生物特征信息，其中，所述第一预设生物特征信息包括一个预设生物特征或多个预设生物特征、预设顺序和预设数量。

在该技术方案中，通过在确定第一类操作系统时，确定相应的第一预设生物特征信息，实现了对第一类操作系统的验证模式的确定，确保了第一类操作系统的数据安全，其中，第一类操作系统中可以设定为包括安全级别较高的应用程序，例如社交软件数据、网银数据、支付密钥数据和照片私密数据等。

在上述技术方案中，优选地，在获取运行指定进程的指令时，确定所述指定进程所属的操作系统，以及所述操作系统对应的预设生物特征信

息，具体还包括以下步骤：在确定所述指定进程属于第二类操作系统时，确定所述第二类操作系统对应的所述预设生物特征信息中的第二预设生物特征信息，其中，所述第二预设生物特征信息包括第一预设生物特征信息中的预设生物特征、预设顺序和预设数量，和不属于所述第一预设生物特征信息的至少一个生物特征或多个预设生物特征的组合、预设顺序和预设数量，所述第一类操作系统的安全级别高于所述第二类操作系统的安全级别。

在该技术方案中，通过在确定指定进程（例如浏览器）属于第二类操作系统时，确定第二类操作系统对应的预设生物特征信息中的第二预设生物特征信息，确定了第二类操作系统的验证模式，其中，第二预设生物特征信息除包括所有的第一预设生物特征信息外，还包括其他生物特征信息（如用户亲属的生物特征信息等），也即对于第二类操作系统的验证过程，可以在验证生物特征与预设生物特征匹配时确认验证成功，第二类操作系统包括本地游戏数据、网络游戏缓存数据和网页浏览数据等。

在上述技术方案中，优选地，判断所述生物特征信息是否与所述预设生物特征信息匹配，具体包括以下步骤：判断所述生物特征信息中的生物特征是否与所述预设生物特征匹配，所述生物特征信息中的输入顺序是否与预设顺序匹配，以及所述生物特征信息中的数量是否与预设数量匹配。

在该技术方案中，通过进一步对生物特征的输入顺序进行匹配判断，提升了第一类操作系统的验证过程的可靠性，也即只有在生物特征与预设生物特征匹配，且输入顺序与预设顺序匹配时，确认第一类操作系统的验证成功，提升了第一类操作系统中的指定进程的安全程度。

在上述技术方案中，优选地，还包括：在获取用户对所述终端的指定操作系统的密码预设指令后，生成密码预设界面；提示用户输入预设生物特征信息，并判断是否在指定时间内获取所述预设生物特征信息；在判定在所述指定时间内获取所述预设生物特征信息后，判断所述预设生物特征信息是否与预存储的生物特征信息匹配，所述预存储的生物特征信息中包括预存储的生物特征及预存储的生物特征名称；在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征匹配时，将所述预存储的生物特征信息作为所述指定操作系统的加密信息；在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征不匹配时，预存储所述

预设生物特性信息，并将所述预存储的生物特征信息作为所述指定操作系统的加密信息；根据用户指令创建所述预设生物特征信息与所述指定操作系统的映射关系，并将所述预存储的生物特征名称推送至密码预设界面。

在该技术方案中，通过生成密码预设界面，提示用户输入预设生物特征信息，并在指定时间内获取预设生物特征信息，判断预设生物特征信息是否与预存储的生物特征信息匹配，限定获取预设生物特征信息的输入时间，使得更进一步地提升了密码预设过程的安全性，同时直观地提示了用户预设生物特征信息，另外，在预设生物特征的持续时间过长时，强制结束密码验证过程，从而避免预设生物特征信息的泄漏。

根据本发明的第二方面，还提出了一种密码信息的验证系统，包括：确定单元，用于在获取运行指定进程的指令时，确定所述指定进程所属的操作系统类别，以及所述操作系统类别对应的预设生物特征信息；获取单元，用于获取用户针对所述指定进程输入的生物特征信息；判断单元，用于判断所述生物特征信息是否与所述预设生物特征信息匹配；所述确定单元还用于：在判定所述生物特征信息与所述预设生物特征信息匹配时，确定所述密码信息验证成功，并运行所述指定进程，其中，所述生物特征信息包括指纹特征信息、虹膜特征信息、人脸特征信息和语音特征信息中的任一或多种的任意组合，所述预设生物特征信息包括预设指纹特征信息、预设虹膜特征信息、预设人脸特征信息和预设语音特征信息中的任一或多种的任意组合。

在该技术方案中，通过针对指定进程所述的操作系统进行生物特征信息的匹配，实现了对任一操作系统内的进程进行统一验证方式，在保证进程的数据安全的同时，简化了用户的验证步骤，提升了用户的使用体验。

具体地，对于多个操作系统的终端而言，终端用户根据个人需求和使用习惯将应用进程划分于相应的操作系统中，终端中已预先设置了每个操作系统的验证制式，例如，终端中的操作系统 A 和操作系统 B 分别对应于高级和低级两种安全等级，在用户的生物特征信息与预设生物特征信息完全匹配时（包括生物特征信息的个数、输入顺序和特征信息等），才能完成对操作系统 A 中的应用进程的验证过程，对于操作系统 B 而言，在输入的生物特征信息为用户本人或用户亲属指纹时，上述生物特征信息中的任一个均属于预设生物特征信息，则完成对操作系统 B 的验证过程。

在上述技术方案中，优选地，所述确定单元还用于：在确定所述指定进程属于第一类操作系统时，确定所述第一类操作系统对应的所述预设生物特征信息中的第一预设生物特征信息，其中，所述第一预设生物特征信息包括一个预设生物特征或多个预设生物特征、预设顺序和预设数量。

5 在该技术方案中，通过在确定第一类操作系统时，确定相应的第一预设生物特征信息，实现了对第一类操作系统的验证模式的确定，确保了第一类操作系统的数据安全，其中，第一类操作系统中可以设定为包括安全级别较高的应用程序，例如社交软件数据、网银数据、支付密钥数据和照片私密数据等。

10 在上述技术方案中，优选地，所述确定单元还用于：在确定所述指定进程属于第二类操作系统时，确定所述第二类操作系统对应的所述预设生物特征信息中的第二预设生物特征信息，其中，所述第二预设生物特征信息包括第一预设生物特征信息中的预设生物特征、预设顺序和预设数量，和不属于所述第一预设生物特征信息的至少一个生物特征或多个预设生物特征的组合、预设顺序和预设数量，所述第一类操作系统的安全级别高于
15 所述第二类操作系统的安全级别。

在该技术方案中，通过在确定指定进程（例如浏览器）属于第二类操作系统时，确定第二类操作系统对应的预设生物特征信息中的第二预设生物特征信息，确定了第二类操作系统的验证模式，其中，第二预设生物特征信息除包括所有的第一预设生物特征信息外，还包括其他生物特征信息
20 （如用户亲属的生物特征信息等），也即对于第二类操作系统的验证过程，可以在验证生物特征与预设生物特征匹配时确认验证成功，第二类操作系统包括本地游戏数据、网络游戏缓存数据和网页浏览数据等。

在上述技术方案中，优选地，所述判断单元还用于：判断所述生物特征信息中的生物特征是否与所述预设生物特征匹配，所述生物特征信息中的输入顺序是否与预设顺序匹配，以及所述生物特征信息中的数量是否与预设数量匹配。
25

在该技术方案中，通过进一步对生物特征的输入顺序进行匹配判断，提升了第一类操作系统的验证过程的可靠性，也即只有在生物特征与预设生物特征匹配，且输入顺序与预设顺序匹配时，确认第一类操作系统的验证成功，提升了第一类操作系统中的指定进程的安全程度。
30

在上述技术方案中，优选地，还包括：生成单元，用于在获取用户对所述终端的指定操作系统的密码预设指令后，生成密码预设界面；提示单元，用于提示用户输入预设生物特征信息，并判断是否在指定时间内获取所述预设生物特征信息；所述判断单元还用于：在判定在所述指定时间内获取所述预设生物特征信息后，判断所述预设生物特征信息是否与预存储的生物特征信息匹配，所述预存储的生物特征信息中包括预存储的生物特征及预存储的生物特征名称；所述密码信息的验证系统还包括：密码确定单元，用于在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征匹配时，将所述预存储的生物特征信息作为所述指定操作系统的加密信息；所述密码确定单元还用于：在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征不匹配时，预存储所述预设生物特征信息，并将所述预存储的生物特征信息作为所述指定操作系统的加密信息；所述密码信息的验证系统还包括：推送单元，用于根据用户指令创建所述预设生物特征信息与所述指定操作系统的映射关系，并将所述预存储的生物特征名称推送至密码预设界面。

在该技术方案中，通过生成密码预设界面，提示用户输入预设生物特征信息，并在指定时间内获取预设生物特征信息，判断预设生物特征信息是否与预存储的生物特征信息匹配，限定获取预设生物特征信息的输入时间，使得更进一步地提升了密码预设过程的安全性，同时直观地提示了用户预设生物特征信息，另外，在预设生物特征的持续时间过长时，强制结束密码验证过程，从而避免预设生物特征信息的泄漏。

根据本发明的第三方面，还提出了一种终端，包括：如上述任一项技术方案所述的密码信息的验证系统。

通过以上技术方案，通过针对指定进程所述的操作系统进行生物特征信息的匹配，实现了对任一操作系统内的进程进行统一验证方式，在保证进程的数据安全的同时，简化了用户的验证步骤，提升了用户的使用体验。

附图说明

图 1 示出了根据本发明的实施例的密码信息的验证方法的示意流程

图；

图 2 示出了根据本发明的实施例的密码信息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 4A 至 4C 示出了根据本发明的一个实施例的终端的验证方案的界面示意图；

图 5A 至 5C 示出了根据本发明的另一个实施例的终端的验证方案的界面示意图；

图 6A 至 6C 示出了根据本发明的再一个实施例的终端的验证方案的界面示意图。

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其他方式来实施，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实施例的在线播放流媒体文件时降低终端功耗的方法的示意图。

如图 1 所示，根据本发明的第一方面的实施例的多媒体文件的群组播放方法，包括：步骤 102，在获取运行指定进程的指令时，确定所述指定进程所属的操作系统类别，以及所述操作系统类别对应的预设生物特征信息；步骤 104，获取用户针对所述指定进程输入的生物特征信息；步骤 106，判断所述生物特征信息是否与所述预设生物特征信息匹配；步骤 108，在判定所述生物特征信息与所述预设生物特征信息匹配时，确定所述密码信息验证成功，并运行所述指定进程，其中，所述生物特征信息包括指纹特征信息、虹膜特征信息、人脸特征信息和语音特征信息中的任一或多种的任意组合，所述预设生物特征信息包括预设指纹特征信息、预设

虹膜特征信息、预设人脸特征信息和预设语音特征信息中的任一或多种的任意组合。

在该技术方案中，通过针对指定进程所述的操作系统进行生物特征信息的匹配，实现了对任一操作系统内的进程进行统一验证方式，在保证进
5 程的数据安全的同时，简化了用户的验证步骤，提升了用户的使用体验。

具体地，对于多个操作系统的终端而言，终端用户根据个人需求和使用习惯将应用进程划分于相应的操作系统中，终端中已预先设置了每个操作系统的验证制式，例如，终端中的操作系统 A 和操作系统 B 分别对应于高级和低级两种安全等级，在用户的生物特征信息与预设生物特征信息
10 完全匹配时（包括生物特征信息的个数、输入顺序和特征信息等），才能完成对操作系统 A 中的应用进程的验证过程，对于操作系统 B 而言，在输入的生物特征信息为用户本人或用户亲属指纹时，上述生物特征信息中的任一个均属于预设生物特征信息，则完成对操作系统 B 的验证过程。

在上述技术方案中，优选地，在获取运行指定进程的指令时，确定所述指定进程所属的操作系统，以及所述操作系统对应的预设生物特征信息，具体包括以下步骤：在确定所述指定进程属于第一类操作系统时，确定所述第一类操作系统对应的所述预设生物特征信息中的第一预设生物特征信息，其中，所述第一预设生物特征信息包括一个预设生物特征或多个
15 预设生物特征、预设顺序和预设数量。

在该技术方案中，通过在确定第一类操作系统时，确定相应的第一预设生物特征信息，实现了对第一类操作系统的验证模式的确定，确保了第一类操作系统的数据安全，其中，第一类操作系统中可以设定为包括安全
20 级别较高的应用程序，例如社交软件数据、网银数据、支付密钥数据和照片私密数据等。

在上述技术方案中，优选地，在获取运行指定进程的指令时，确定所述指定进程所属的操作系统，以及所述操作系统对应的预设生物特征信息，具体还包括以下步骤：在确定所述指定进程属于第二类操作系统时，确定所述第二类操作系统对应的所述预设生物特征信息中的第二预设生物特征信息，其中，所述第二预设生物特征信息包括第一预设生物特征信息
25 中的预设生物特征、预设顺序和预设数量，和不属于所述第一预设生物特征信息的至少一个生物特征或多个预设生物特征的组合、预设顺序和预设

数量，所述第一类操作系统的安全级别高于所述第二类操作系统的安全级别。

在该技术方案中，通过在确定指定进程（例如浏览器）属于第二类操作系统时，确定第二类操作系统对应的预设生物特征信息中的第二预设生物特征信息，确定了第二类操作系统的验证模式，其中，第二预设生物特征信息除包括所有的第一预设生物特征信息外，还包括其他生物特征信息（如用户亲属的生物特征信息等），也即对于第二类操作系统的验证过程，可以在验证生物特征与预设生物特征匹配时确认验证成功，第二类操作系统包括本地游戏数据、网络游戏缓存数据和网页浏览数据等。

在上述技术方案中，优选地，判断所述生物特征信息是否与所述预设生物特征信息匹配，具体包括以下步骤：判断所述生物特征信息中的生物特征是否与所述预设生物特征匹配，所述生物特征信息中的输入顺序是否与预设顺序匹配，以及所述生物特征信息中的数量是否与预设数量匹配。

在该技术方案中，通过进一步对生物特征的输入顺序进行匹配判断，提升了第一类操作系统的验证过程的可靠性，也即只有在生物特征与预设生物特征匹配，且输入顺序与预设顺序匹配时，确认第一类操作系统的验证成功，提升了第一类操作系统中的指定进程的安全程度。

在上述技术方案中，优选地，还包括：在获取用户对所述终端的指定操作系统的密码预设指令后，生成密码预设界面；提示用户输入预设生物特征信息，并判断是否在指定时间内获取所述预设生物特征信息；在判定在所述指定时间内获取所述预设生物特征信息后，判断所述预设生物特征信息是否与预存储的生物特征信息匹配，所述预存储的生物特征信息中包括预存储的生物特征及预存储的生物特征名称；在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征匹配时，将所述预存储的生物特征信息作为所述指定操作系统的加密信息；在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征不匹配时，预存储所述预设生物特性信息，并将所述预存储的生物特征信息作为所述指定操作系统的加密信息；根据用户指令创建所述预设生物特征信息与所述指定操作系统的映射关系，并将所述预存储的生物特征名称推送至密码预设界面。

在该技术方案中，通过生成密码预设界面，提示用户输入预设生物特征信息，并在指定时间内获取预设生物特征信息，判断预设生物特征信息

是否与预存储的生物特征信息匹配，限定获取预设生物特征信息的输入时间，使得更进一步地提升了密码预设过程的安全性，同时直观地提示了用户预设生物特征信息，另外，在预设生物特征的持续时间过长时，强制结束密码验证过程，从而避免预设生物特征信息的泄漏。

5 参看图 2，根据本发明的第二方面的实施例的密码信息的验证系统 200，包括：确定单元 202，用于在获取运行指定进程的指令时，确定所述指定进程所属的操作系统类别，以及所述操作系统类别对应的预设生物特征信息；获取单元 204，用于获取用户针对所述指定进程输入的生物特征信息；判断单元 206，用于判断所述生物特征信息是否与所述预设生物特征信息匹配；所述确定单元 202 还用于：在判定所述生物特征信息与所述预设生物特征信息匹配时，确定所述密码信息验证成功，并运行所述指定进程，其中，所述生物特征信息包括指纹特征信息、虹膜特征信息、人脸特征信息和语音特征信息中的任一或多种的任意组合，所述预设生物特征信息包括预设指纹特征信息、预设虹膜特征信息、预设人脸特征信息和
10 预设语音特征信息中的任一或多种的任意组合。

在该技术方案中，通过针对指定进程所述的操作系统进行生物特征信息的匹配，实现了对任一操作系统内的进程进行统一验证方式，在保证进程的数据安全的同时，简化了用户的验证步骤，提升了用户的使用体验。

具体地，对于多个操作系统的终端而言，终端用户根据个人需求和使
20 用习惯将应用进程划分于相应的操作系统中，终端中已预先设置了每个操作系统的验证制式，例如，终端中的操作系统 A 和操作系统 B 分别对应于高级和低级两种安全等级，在用户的生物特征信息与预设生物特征信息完全匹配时（包括生物特征信息的个数、输入顺序和特征信息等），才能完成对操作系统 A 中的应用进程的验证过程，对于操作系统 B 而言，在
25 输入的生物特征信息为用户本人或用户亲属指纹时，上述生物特征信息中的任一个均属于预设生物特征信息，则完成对操作系统 B 的验证过程。

在上述技术方案中，优选地，所述确定单元 202 还用于：在确定所述指定进程属于第一类操作系统时，确定所述第一类操作系统对应的所述预设生物特征信息中的第一预设生物特征信息，其中，所述第一预设生物特征信息包括一个预设生物特征或多个预设生物特征、预设顺序和预设数量。
30

在该技术方案中，通过在确定第一类操作系统时，确定相应的第一预设生物特征信息，实现了对第一类操作系统的验证模式的确定，确保了第一类操作系统的数据安全，其中，第一类操作系统中可以设定为包括安全级别较高的应用程序，例如社交软件数据、网银数据、支付密钥数据和照片私密数据等。

在上述技术方案中，优选地，所述确定单元 202 还用于：在确定所述指定进程属于第二类操作系统时，确定所述第二类操作系统对应的所述预设生物特征信息中的第二预设生物特征信息，其中，所述第二预设生物特征信息包括第一预设生物特征信息中的预设生物特征、预设顺序和预设数量，和不属于所述第一预设生物特征信息的至少一个生物特征或多个预设生物特征的组合、预设顺序和预设数量，所述第一类操作系统的安全级别高于所述第二类操作系统的安全级别。

在该技术方案中，通过在确定指定进程（例如浏览器）属于第二类操作系统时，确定第二类操作系统对应的预设生物特征信息中的第二预设生物特征信息，确定了第二类操作系统的验证模式，其中，第二预设生物特征信息除包括所有的第一预设生物特征信息外，还包括其他生物特征信息（如用户亲属的生物特征信息等），也即对于第二类操作系统的验证过程，可以在验证生物特征与预设生物特征匹配时确认验证成功，第二类操作系统包括本地游戏数据、网络游戏缓存数据和网页浏览数据等。

在上述技术方案中，优选地，所述判断单元 206 还用于：判断所述生物特征信息中的生物特征是否与所述预设生物特征匹配，所述生物特征信息中的输入顺序是否与预设顺序匹配，以及所述生物特征信息中的数量是否与预设数量匹配。

在该技术方案中，通过进一步对生物特征的输入顺序进行匹配判断，提升了第一类操作系统的验证过程的可靠性，也即只有在生物特征与预设生物特征匹配，且输入顺序与预设顺序匹配时，确认第一类操作系统的验证成功，提升了第一类操作系统中的指定进程的安全程度。

在上述技术方案中，优选地，还包括：生成单元 208，用于在获取用户对所述终端的指定操作系统的密码预设指令后，生成密码预设界面；提示单元 210，用于提示用户输入预设生物特征信息，并判断是否在指定时间内获取所述预设生物特征信息；所述判断单元 206 还用于：在判定在所

述指定时间内获取所述预设生物特征信息后，判断所述预设生物特征信息是否与预存储的生物特征信息匹配，所述预存储的生物特征信息中包括预存储的生物特征及预存储的生物特征名称；所述密码信息的验证系统 200 还包括：密码确定单元 212，用于在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征匹配时，将所述预存储的生物特征信息作为所述指定操作系统的加密信息；所述密码确定单元 212 还用于：在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征不匹配时，预存储所述预设生物特性信息，并将所述预存储的生物特征信息作为所述指定操作系统的加密信息；所述密码信息的验证系统 200 还包括：推送单元 214，用于根据用户指令创建所述预设生物特征信息与所述指定操作系统的映射关系，并将所述预存储的生物特征名称推送至密码预设界面。

在该技术方案中，通过生成密码预设界面，提示用户输入预设生物特征信息，并在指定时间内获取预设生物特征信息，判断预设生物特征信息是否与预存储的生物特征信息匹配，限定获取预设生物特征信息的输入时间，使得更进一步地提升了密码预设过程的安全性，同时直观地提示了用户预设生物特征信息，另外，在预设生物特征的持续时间过长时，强制结束密码验证过程，从而避免预设生物特征信息的泄漏。

参看图 3，根据本发明的第三方面，还提出了一种终端 300，包括：如上述任一项技术方案所述的密码信息的验证系统 200。

下面结合图 4A 至图 4C、图 5A 至图 5C 至图 6A 至图 6C 说明根据本发明的实施例的密码信息验证方案：

实施例一：

如图 4A 至图 4C 所示，对于终端的操作系统 1 的指定进程进行验证之前，包括：指纹录入，获取用户（或用户亲属）输入的指纹信息，其中，指纹信息包括指纹特征、指纹特征的个数和输入顺序；系统 1 功能定义，也即将上述指纹录入的过程的指纹特征映射于待加密的操作系统，或者映射于操作系统中的指定进程（如图 4C 中所示的“VPN 联网”、“打开系统 1 微信应用”和“打开系统 1 短信应用”等），并获取用户输入的指纹录入名称（如图 4B 中所示的“中指”），并在用户确认后，完成指纹密码的预设过程。

实施例二：

如图 5A 至图 5C 所示，对于终端的操作系统 2 的指定进程进行验证之前，包括：指纹录入，获取用户（或用户亲属）输入的指纹信息，其中，指纹信息包括指纹特征、指纹特征的个数和输入顺序；系统 2 功能定义，也即将上述指纹录入的过程的指纹特征映射于待加密的操作系统，或者映射于操作系统中的指定进程（如图 5C 中所示的“进入操作系统 2”、“运行本体游戏”和“运行联网游戏”等），并获取用户输入的指纹录入名称（如图 5B 中所示的“食指”），并在用户确认后，完成指纹密码的预设过程。

实施例三：

如图 6A 至图 6C 所示，对于终端的操作系统 3 的指定进程进行验证之前，包括：指纹录入，获取用户（或用户亲属）输入的指纹信息，其中，指纹信息包括指纹特征、指纹特征的个数和输入顺序；系统 3 功能定义，也即将上述指纹录入的过程的指纹特征映射于待加密的操作系统，或者映射于操作系统中的指定进程（如图 6C 中所示的“打开操作系统 3”、“打开系统 3 录音应用”和“打开系统 3 拍照应用”等），并获取用户输入的指纹录入名称（如图 6B 中所示的“拇指”），并在用户确认后，完成指纹密码的预设过程。

表 1

用户	用户级别	多系统	指纹信息	功能操作
用户 A	高级用户	系统 1	左中指	打开系统 1 中的私密短信
		系统 2	系统 1	打开系统 2 中的本地游戏
		系统 3	系统 1	解锁系统 3
用户 B	中级用户	系统 2	右中指	打开系统 2 中的拍照应用
		系统 3	左大拇指	打开系统 3 的录音机应用
用户 C	普通用户	系统 3	右大拇指	解锁屏幕

表 1 示出了根据本发明的实施例的指纹信息与功能操作之间的映射关系。

通过以上技术方案，考虑到相关技术中提出的如何设计一种能够保证数据安全和操作便捷的密码信息的验证方案的技术问题，本申请提出了一种新的密码信息的验证方案，通过针对指定进程所述的操作系统进行生物

特征信息的匹配，实现了对任一操作系统内的进程进行统一验证方式，在保证进程的数据安全的同时，简化了用户的验证步骤，提升了用户的使用体验。

- 5 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，均应包含在本发明的保护范围之内。

权利要求书

1. 一种密码信息的验证方法，适用于运行有多个操作系统的终端，其特征在于，包括：

- 5 在获取运行指定进程的指令时，确定所述指定进程所属的操作系统类别，以及所述操作系统类别对应的预设生物特征信息；
 获取用户针对所述指定进程输入的生物特征信息；
 判断所述生物特征信息是否与所述预设生物特征信息匹配；
 在判定所述生物特征信息与所述预设生物特征信息匹配时，确定所述
10 密码信息验证成功，并运行所述指定进程，

 其中，所述生物特征信息包括指纹特征信息、虹膜特征信息、人脸特征信息和语音特征信息中的任一或多种的任意组合，所述预设生物特征信息包括预设指纹特征信息、预设虹膜特征信息、预设人脸特征信息和预设语音特征信息中的任一或多种的任意组合。

- 15 2. 根据权利要求 1 所述的密码信息的验证方法，其特征在于，在获取运行指定进程的指令时，确定所述指定进程所属的操作系统，以及所述操作系统对应的预设生物特征信息，具体包括以下步骤：

 在确定所述指定进程属于第一类操作系统时，确定所述第一类操作系统对应的所述预设生物特征信息中的第一预设生物特征信息，

- 20 其中，所述第一预设生物特征信息包括一个预设生物特征或多个预设生物特征、预设顺序和预设数量。

 3. 根据权利要求 1 所述的密码信息的验证方法，其特征在于，在获取运行指定进程的指令时，确定所述指定进程所属的操作系统，以及所述操作系统对应的预设生物特征信息，具体还包括以下步骤：

- 25 在确定所述指定进程属于第二类操作系统时，确定所述第二类操作系统对应的所述预设生物特征信息中的第二预设生物特征信息，

 其中，所述第二预设生物特征信息包括第一预设生物特征信息中的预设生物特征、预设顺序和预设数量，和不属于所述第一预设生物特征信息的至少一个生物特征或多个预设生物特征的组合、预设顺序和预设数量，

- 30 所述第一类操作系统的安全级别高于所述第二类操作系统的安全级别。

4. 根据权利要求 2 所述的密码信息的验证方法, 其特征在于, 判断所述生物特征信息是否与所述预设生物特征信息匹配, 具体包括以下步骤:

判断所述生物特征信息中的生物特征是否与所述预设生物特征匹配,
5 所述生物特征信息中的输入顺序是否与预设顺气匹配, 以及所述生物特征信息中的数量是否与预设数量匹配。

5. 根据权利要求 3 或 4 所述的密码信息的验证方法, 其特征在于, 还包括:

在获取用户对所述终端的指定操作系统的密码预设指令后, 生成密码
10 预设界面;

提示用户输入预设生物特征信息, 并判断是否在指定时间内获取所述预设生物特征信息;

在判定在所述指定时间内获取所述预设生物特征信息后, 判断所述预设生物特征信息是否与预存储的生物特征信息匹配, 所述预存储的生物特征信息中包括预存储的生物特征及预存储的生物特征名称;
15

在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征匹配时, 将所述预存储的生物特征信息作为所述指定操作系统的加密信息;

在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征不匹配时, 预存储所述预设生物特性信息, 并将所述预存储的生物特征信息作为所述指定操作系统的加密信息;
20

根据用户指令创建所述预设生物特征信息与所述指定操作系统的映射关系, 并将所述预存储的生物特征名称推送至密码预设界面。

6. 一种密码信息的验证系统, 适用于运行有多个操作系统的终端, 其特征在于, 包括:
25

确定单元, 用于在获取运行指定进程的指令时, 确定所述指定进程所属的操作系统类别, 以及所述操作系统类别对应的预设生物特征信息;

获取单元, 用于获取用户针对所述指定进程输入的生物特征信息;

判断单元, 用于判断所述生物特征信息是否与所述预设生物特征信息
30 匹配;

所述确定单元还用于: 在判定所述生物特征信息与所述预设生物特征

信息匹配时，确定所述密码信息验证成功，并运行所述指定进程，

其中，所述生物特征信息包括指纹特征信息、虹膜特征信息、人脸特征信息和语音特征信息中的任一或多种的任意组合，所述预设生物特征信息包括预设指纹特征信息、预设虹膜特征信息、预设人脸特征信息和预设语音特征信息中的任一或多种的任意组合。

7. 根据权利要求 6 所述的密码信息的验证系统，其特征在于，所述确定单元还用于：

在确定所述指定进程属于第一类操作系统时，确定所述第一类操作系统对应的所述预设生物特征信息中的第一预设生物特征信息，

其中，所述第一预设生物特征信息包括一个预设生物特征或多个预设生物特征、预设顺序和预设数量。

8. 根据权利要求 6 所述的密码信息的验证系统，其特征在于，所述确定单元还用于：

在确定所述指定进程属于第二类操作系统时，确定所述第二类操作系统对应的所述预设生物特征信息中的第二预设生物特征信息，

其中，所述第二预设生物特征信息包括第一预设生物特征信息中的预设生物特征、预设顺序和预设数量，和不属于所述第一预设生物特征信息的至少一个生物特征或多个预设生物特征的组合、预设顺序和预设数量，所述第一类操作系统的安全级别高于所述第二类操作系统的安全级别。

9. 根据权利要求 7 或 8 所述的密码信息的验证系统，其特征在于，所述判断单元还用于：

判断所述生物特征信息中的生物特征是否与所述预设生物特征匹配，所述生物特征信息中的输入顺序是否与预设顺序匹配，以及所述生物特征信息中的数量是否与预设数量匹配。

10. 根据权利要求 9 所述的密码信息的验证系统，其特征在于，还包括：

生成单元，用于在获取用户对所述终端的指定操作系统的密码预设指令后，生成密码预设界面；

提示单元，用于提示用户输入预设生物特征信息，并判断是否在指定时间内获取所述预设生物特征信息；

所述判断单元还用于：在判定在所述指定时间内获取所述预设生物特

征信息后，判断所述预设生物特征信息是否与预存储的生物特征信息匹配，所述预存储的生物特征信息中包括预存储的生物特征及预存储的生物特征名称；

所述密码信息的验证系统还包括：

- 5 密码确定单元，用于在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征匹配时，将所述预存储的生物特征信息作为所述指定操作系统的加密信息；

- 10 所述密码确定单元还用于：在判定所述预设生物特征信息中的预设生物特征与所述预存储的生物特征不匹配时，预存储所述预设生物特性信息，并将所述预存储的生物特征信息作为所述指定操作系统的加密信息；

所述密码信息的验证系统还包括：

推送单元，用于根据用户指令创建所述预设生物特征信息与所述指定操作系统的映射关系，并将所述预存储的生物特征名称推送至密码预设界面。

- 15 11. 一种终端，其特征在于，包括：如权利要求 6 至 10 中任一项所述的密码信息的验证系统。

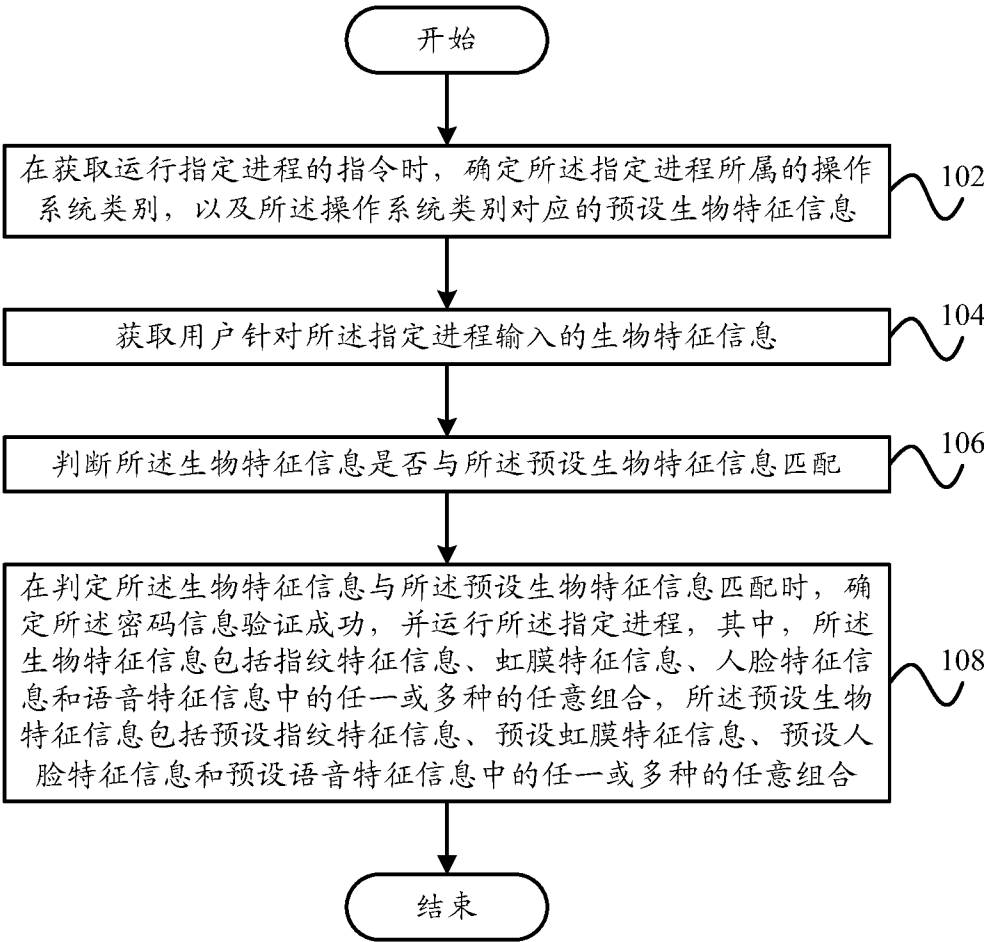


图 1

5

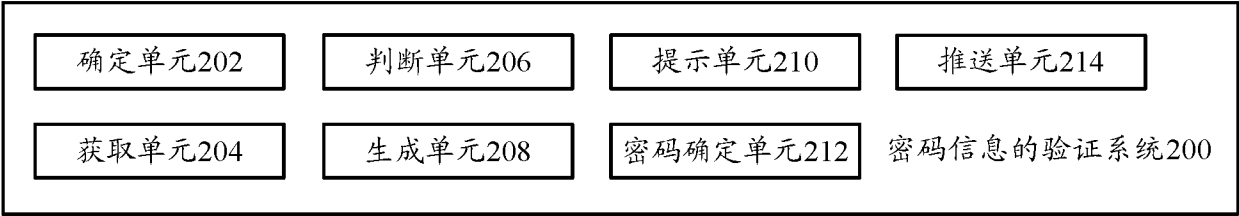


图 2

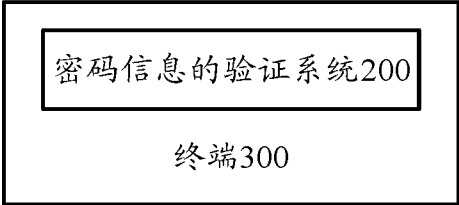


图 3

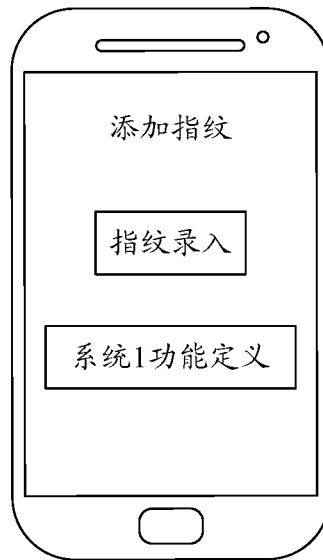


图 4A

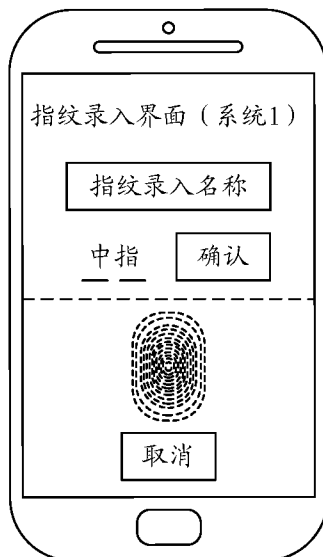


图 4B

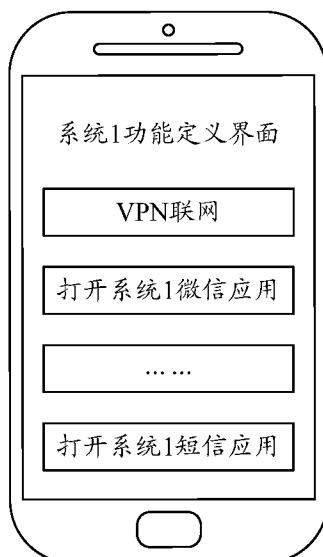


图 4C

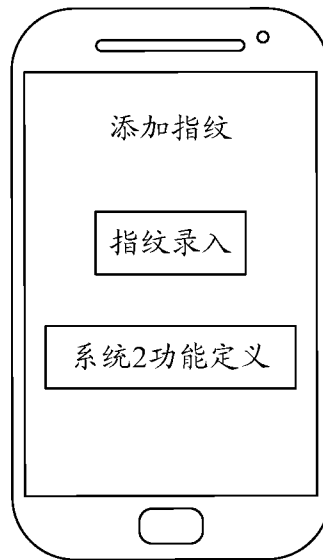


图 5A

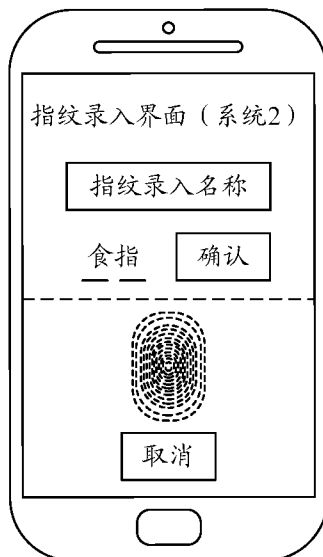


图 5B

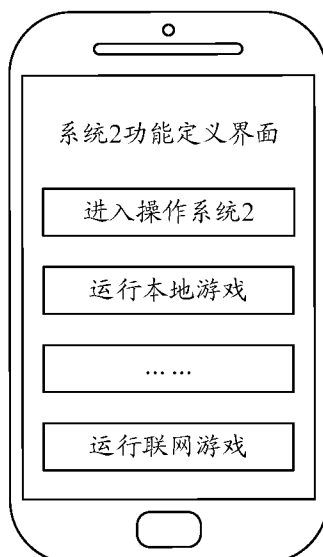


图 5C

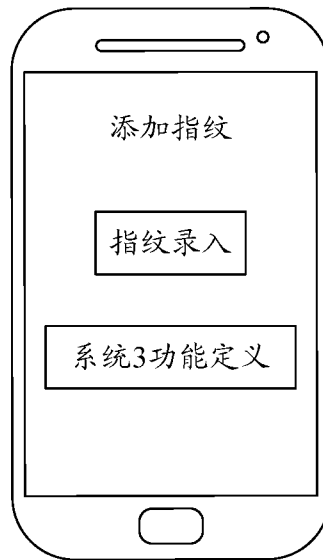


图 6A

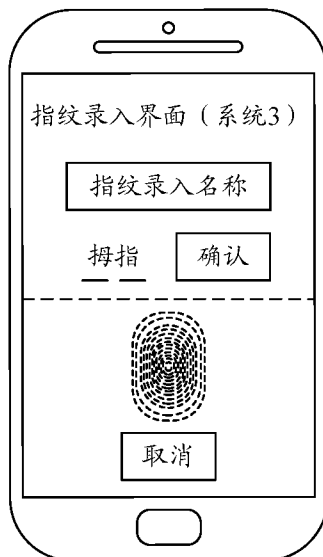


图 6B

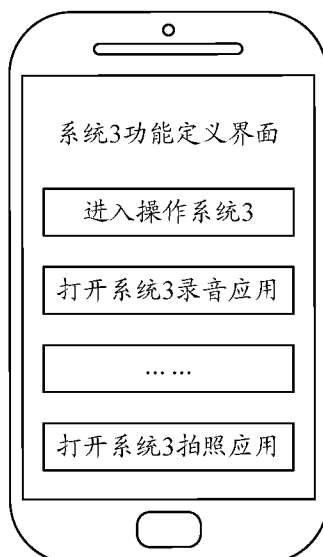


图 6C

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/088492

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)

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)

CNPAT, WPI, EPODOC, CNKI, GOOGLE: multi ? operating system, local, local host, process, fingerprint, application, low level, security level, network, verify, high level, authentication, biological feature, code, extranet, multilevel, automatic, system, change, mapped, corresponding, switch, multi, security, mapping, correspond, grade, level, OS, software, program, operating system

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104077516 A (HUAWEI TECHNOLOGIES CO., LTD.), 01 October 2014 (01.10.2014), description, paragraphs [0086]-[0108], and figure 1	1-11
A	CN 104462935 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 25 March 2015 (25.03.2015), the whole document	1-11
A	CN 104077576 A (NANCHANG O-FILM BIO-IDENTIFICATION TECHNOLOGY CO., LTD. et al.), 01 October 2014 (01.10.2014), the whole document	1-11
A	WO 2015073413 A1 (MOTOROLA MOBILITY LLC), 21 May 2015 (21.05.2015), the whole document	1-11
A	CN 104615927 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 13 May 2015 (13.05.2015), the whole document	1-11

☒ 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 07 April 2016 (07.04.2016)	Date of mailing of the international search report 29 April 2016 (29.04.2016)
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 FAN, Yuxia Telephone No.: (86-10) 82245727

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/088492

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104156657 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 19 November 2014 (19.11.2014), the whole document	1-11

International application No.
PCT/CN2015/088492

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

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) 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)) CNPAT, WPI, EPODOC, CNKI, GOOGLE: 多?操作系统, 本地, 本机, 进程, 指纹, 应用, 低级, 层次, 安全级别, 网络, 操作系统, 级别, 验证, 对应, 切换, 高级, 鉴权, 生物特征, 映射, 软件, 密码, 外网, 等级, 多级, 自动, 安全, system, change, mapped, corresponding, switch, multi, security, mapping, correspond, grade, level, OS, software, program, operating system																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>CN 104077516 A (华为技术有限公司) 2014年 10月 1日 (2014 - 10 - 01) 说明书第[0086]-[0108]段, 图1</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>CN 104462935 A (宇龙计算机通信科技深圳有限公司) 2015年 3月 25日 (2015 - 03 - 25) 全文</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>CN 104077576 A (南昌欧菲生物识别技术有限公司 等) 2014年 10月 1日 (2014 - 10 - 01) 全文</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>WO 2015073413 A1 (MOTOROLA MOBILITY LLC) 2015年 5月 21日 (2015 - 05 - 21) 全文</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>CN 104615927 A (宇龙计算机通信科技深圳有限公司) 2015年 5月 13日 (2015 - 05 - 13) 全文</td> <td>1-11</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	A	CN 104077516 A (华为技术有限公司) 2014年 10月 1日 (2014 - 10 - 01) 说明书第[0086]-[0108]段, 图1	1-11	A	CN 104462935 A (宇龙计算机通信科技深圳有限公司) 2015年 3月 25日 (2015 - 03 - 25) 全文	1-11	A	CN 104077576 A (南昌欧菲生物识别技术有限公司 等) 2014年 10月 1日 (2014 - 10 - 01) 全文	1-11	A	WO 2015073413 A1 (MOTOROLA MOBILITY LLC) 2015年 5月 21日 (2015 - 05 - 21) 全文	1-11	A	CN 104615927 A (宇龙计算机通信科技深圳有限公司) 2015年 5月 13日 (2015 - 05 - 13) 全文	1-11
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
A	CN 104077516 A (华为技术有限公司) 2014年 10月 1日 (2014 - 10 - 01) 说明书第[0086]-[0108]段, 图1	1-11																		
A	CN 104462935 A (宇龙计算机通信科技深圳有限公司) 2015年 3月 25日 (2015 - 03 - 25) 全文	1-11																		
A	CN 104077576 A (南昌欧菲生物识别技术有限公司 等) 2014年 10月 1日 (2014 - 10 - 01) 全文	1-11																		
A	WO 2015073413 A1 (MOTOROLA MOBILITY LLC) 2015年 5月 21日 (2015 - 05 - 21) 全文	1-11																		
A	CN 104615927 A (宇龙计算机通信科技深圳有限公司) 2015年 5月 13日 (2015 - 05 - 13) 全文	1-11																		
☒ 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 4月 7日		国际检索报告邮寄日期 2016年 4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 传真号 (86-10)62019451		授权官员 范玉霞 电话号码 (86-10)82245727																		

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 104156657 A (字龙计算机通信科技深圳有限公司) 2014年 11月 19日 (2014 - 11 - 19) 全文	1-11

国际申请号
PCT/CN2015/088492

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	104077516	A	2014年 10月 1日	WO	2015197008	A1	2015年 12月 30日
CN	104462935	A	2015年 3月 25日	无			
CN	104077576	A	2014年 10月 1日	无			
WO	2015073413	A1	2015年 5月 21日	US	2015137938	A1	2015年 5月 21日
CN	104615927	A	2015年 5月 13日	无			
CN	104156657	A	2014年 11月 19日	无			