

(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
2016 年 12 月 8 日 (08.12.2016)



(10) 国际公布号
WO 2016/192165 A1

(51) 国际专利分类号:
G06F 21/32 (2013.01)

(21) 国际申请号: PCT/CN2015/082991

(22) 国际申请日: 2015 年 6 月 30 日 (30.06.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510289841.3 2015 年 5 月 29 日 (29.05.2015) 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: 吴炽强 (WU, Zhiqiang); 中国广东省深圳
市南山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。 王文林 (WANG, Wenlin); 中国广东省深圳
市南山区科技园北区梦溪道 2 号, Guangdong 518057

(CN)。 张娜 (ZHANG, Na); 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,

[见续页]

(54) Title: DATA ENCRYPTION METHOD AND APPARATUS

(54) 发明名称: 一种数据加密方法及装置

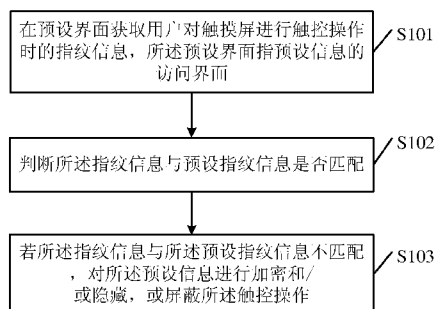


图 1

S101 Acquire fingerprint information on a preset interface when a user performs a touch operation on a touchscreen, the preset interface referring to a visit interface of preset information

S102 Determine whether the fingerprint information matches preset fingerprint information

S103 If the fingerprint information does not match the preset fingerprint information, encrypt and/or hide the preset information, or shield the touch operation

(57) Abstract: Disclosed are a data encryption method and apparatus. The data encryption method comprises: acquiring fingerprint information on a preset interface when a user performs a touch operation on a touchscreen, the preset interface being a visit interface of preset information; determining whether the fingerprint information matches preset fingerprint information; and if the fingerprint information does not match the preset fingerprint information, encrypting and/or hiding the preset information, or shielding the touch operation. When fingerprint information only obtained from a preset interface during a touch operation of a user on a touchscreen does not match preset fingerprint information, only the preset information is encrypted, accordingly the calculation amount is small, overheads of a system are low, and the efficiency is high.

(57) 摘要: 本发明实施例公开了一种数据加密方法及装置, 一种数据加密方法, 包括: 在预设界面获取用户对触摸屏进行触控操作时的指纹信息, 所述预设界面为预设信息的访问界面; 判断所述指纹信息与预设指纹信息是否匹配; 若所述指纹信息与所述预设指纹信息不匹配, 则对所述预设信息进行加密和/或隐藏, 或屏蔽所述触控操作。从而当只在预设界面上获取到的用户对触摸屏进行触控操作时的指纹信息与预设指纹信息不匹配时, 只对预设信息进行加密, 计算量小, 系统开销小, 效率高。



WO 2016/192165 A1



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))。

一种数据加密方法及装置

本申请要求于 2015 年 5 月 29 日提交中国专利局，申请号为 201510289841.3、发明名称为“一种数据加密方法及装置”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

本发明涉及通信技术领域，具体涉及一种数据加密方法及装置。

背景技术

10 随着移动终端的普及，移动终端越来越普遍地进入人们的日常生活，但同时随着通信技术的发展，人们越来越多地利用移动终端来储存敏感性和私密性数据，对数据进行加密成为保证数据安全性的的重要手段。

目前，普遍采用的数据加密方法都是事先对数据进行加密，再通过特定的方式对数据进行解密来完成对数据的读取，从而实现对数据的保护。例如，当
15 用户的相册及短信为私密数据时，那么在用户拍照以及收发短信的时候，即对所有相册的照片以及所有短信进行加密，后续需要查看其中部分照片或者短信时，再通过特定的地方接收指纹或者密码等对需要查看的数据进行解密，从而实现对私密数据的保护。

但是此种对数据进行加密保护的方法中，事先对所有数据进行加密，导致
20 计算量大，系统开销大，效率低。

发明内容

本发明实施例提供了一种数据加密方法及装置。该数据加密方法无需通过对每一个文件或者应用进行加密，利用触摸屏全屏设置指纹传感器等方式获取
25 用户在触摸屏任一位置触控操作时的指纹信息与预设的指纹信息进行比较，当触控操作的指纹与预设指纹匹配时，触控操作有效，可以打开应用或者文件。当触控操作的指纹与预设指纹不匹配时，触控操作失效，或者终端自动对文档进行加密和/或隐藏。本提案提供的数据加密方法无需主人对每个文件进行加密即可实现对隐私的保护，因为无需对每个文件或者应用进行加密从而降低系
30 统开销，提高效率。

本发明实施例第一方面提供一种数据加密方法，包括：

在预设界面获取用户对触摸屏进行触控操作时的指纹信息，所述预设界面为预设信息的访问界面；

判断所述指纹信息与预设指纹信息是否匹配；

- 5 若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

本发明实施例第一方面提供一种数据加密装置，包括：

读取模块，用于在预设界面获取用户对触摸屏进行触控操作时的指纹信息，所述预设界面为预设信息的访问界面；

- 10 判断模块，用于判断所述指纹信息与预设指纹信息是否匹配；

加密模块，用于若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

- 可以看出，本实施例的方案中，在预设界面获取用户对触摸屏进行触控操作时的指纹信息，所述预设界面为预设信息的访问界面；判断所述指纹信息与
15 预设指纹信息是否匹配；若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。从而当只在预设界面上获取到的用户对触摸屏进行触控操作时的指纹信息与预设指纹信息不匹配时，只对预设信息进行加密，计算量小，系统开销小，效率高。

20 附图说明

为了更清楚地说明本发明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简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

- 25 图 1 是本发明实施例提供的一种搜索方法的流程示意图；

图 2 是本发明实施例提供的另一种搜索方法的流程示意图；

图 3 是本发明实施例提供的一种数据加密装置的结构示意图；

图 4 是本发明实施例提供的另一种数据加密装置的结构示意图；

图 5 是本发明实施例提供的又一种数据加密装置的结构示意图。

具体实施方式

本发明实施例提供了一种数据加密方法及装置。该数据加密方法无需通过对每一个文件或者应用进行加密,利用触摸屏全屏设置指纹传感器等方式获取用户在触摸屏任一位置触控操作时的指纹信息与预设的指纹信息进行比对,当触控操作的指纹与预设指纹匹配时,触控操作有效,可以打开应用或者文件。当触控操作的指纹与预设指纹不匹配时,触控操作失效,或者终端自动对文档进行加密和/或隐藏。本提案提供的数据加密方法无需主人对每个文件进行加密即可实现对隐私的保护,因为无需对每个文件或者应用进行加密从而降低系统开销,提高效率。

为了使本技术领域的人员更好地理解本发明方案,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分的实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都应当属于本发明保护的范围。

本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”和“第三”等是用于区别不同对象,而非用于描述特定顺序。此外,术语“包括”以及它们任何变形,意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元,而是可选地还包括没有列出的步骤或单元,或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

本发明实施例的一种数据加密方法的一个实施例,一种数据加密方法包括:在预设界面获取用户对触摸屏进行触控操作时的指纹信息,所述预设界面指预设信息的访问界面;判断所述指纹信息与预设指纹信息是否匹配;若所述指纹信息与所述预设指纹信息不匹配,则对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作,使触控操作暂时失效。。

首先参见图 1,图 1 是本发明的一个实施例提供的一种数据加密方法的流程示意图。其中,如图 1 所示,本发明的一个实施例提供的一种数据加密方法可以包括:

S101、在预设界面获取用户对触摸屏进行触控操作时的指纹信息,所述预

设界面指预设信息的访问界面。

其中，预设信息指存储于终端中特定位置、由终端系统或者用户设定的、需要对其访问进行限制的特定信息，包括特定数据或特定应用等，如可以为手机相册、手机短信、QQ、微信等特定应用，也可以为手机相册应用里面的某一个相册、手机短信应用里面的短信等，还可以为存储在终端中的某一特定文件等；

预设界面是指终端提供给用户访问预设信息的用户界面，如手机相册、手机短信等的访问界面，或手机进入相册后，查看某一指定相册的界面；预设界面还可以为屏幕的解锁界面等。

其中，终端指手机、平板电脑等智能终端，该终端具有能够进行指纹识别的触摸屏，该触摸屏能够感应用户的按压、滑动等操作，并能对与触摸屏接触的指纹进行识别。终端可以在预设界面通过具有指纹识别的触摸屏的任何位置获取用户触控触摸屏时的指纹信息。

可选地，在本发明的一些可能的实施方式中，该预设界面根据用户的需要，将预设信息的访问界面设置为预设界面，从而用户在通过该预设界面进入该应用或者数据时，终端实时通过触摸屏对用户触控触摸屏时的指纹信息进行识别。

举例说明，在本发明的一些可能的实施方式中，若设置手机相册为敏感信息，则将预设界面设置为访问相册的用户界面，那么当用户访问到该用户界面时，终端实时读取用户在该用户界面上触控触摸屏时的指纹信息。

可选地，在预设界面获取用户触控触摸屏时的指纹信息时，可以通过识别用户在预设界面的按压操作。

可选地，在预设界面获取用户触控触摸屏时的指纹信息时，可以通过识别用户在预设界面的滑动操作。

S102、判断所述指纹信息与预设指纹信息是否匹配。

其中，所述指纹信息指用户在预设界面读取到的指纹信息，可通过指纹传感器感应用户在触摸屏上的按压、滑动等操作进行指纹识别。

其中，预设指纹信息指预先存储在终端中的指纹信息，用于与通过触摸屏获取收到的用户触控触摸屏时的指纹信息进行对比。

可选地，在本发明的一些可能的实施方式中，该预设指纹信息可以为一个，

从而所接收到的用户录入的指纹信息只需要与这一个预设指纹信息进行对比，判断用户触控触摸屏时的指纹信息是否与该预设指纹信息匹配。

可选地，在本发明的另一些可能的实施方式中，该预设指纹信息也可以为多个，从而所接收到的用户触控触摸屏时的指纹信息需要与多个预设指纹信息进行对比，用于判断用户触控触摸屏时的指纹信息是否与预设指纹信息匹配。

可选地，在本发明的一些可能的实施方式中，进入不同应用的预设指纹信息可以不一样，也可以一样。

可选地，在本发明的另一些可能的实施方式中，所述预设指纹信息可以由有权限用户进行更改。

10 S103、若所述指纹信息与所述预设指纹信息不匹配，对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

其中，屏蔽所述触控操作指在获取到的用户触控触摸屏时的指纹信息与预设指纹信息不匹配时，暂时使用户在该预设界面的触控操作失效，从而使得在获取到非预设指纹信息时不再在预设界面继续获取用户触控触摸屏的指纹信息，减少系统开销，当下次再进入该预设界面时，触控操作自动重新恢复有效，。

15 可选地，在本发明的一些可能的实施方式中，当预设指纹信息为一个时，判断判断用户触控触摸屏时的指纹信息是否与该一个预设指纹信息是否匹配，若用户触控触摸屏时的指纹信息与该预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

20 可选地，在本发明的另一些可能的实施方式中，当预设指纹信息为多个时，判断用户触控触摸屏时的指纹信息与其中任一个预设指纹信息是否匹配，若用户触控触摸屏时的指纹信息与其中任一个预设指纹信息匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

25 举例说明，在本发明的一些可能的实施方式中，当设置手机相册应用具有访问权限的用户为张三和李四，则可以将预设指纹信息设置为张三和李四的指纹，那么在手机相册的访问界面上接收到指纹信息时，将该指纹信息与预设的张三和李四的指纹进行对比，如果不匹配，则拒绝访问手机相册。

再举例说明，在本发明的另一些可能的实施方式中，当设置手机相册应用里面的某一个特定相册具有访问权限的用户为张三，则将预设指纹信息设置为张三的指纹，那么在该特定相册的访问界面上接收到指纹信息时，将该指纹信

息与预设的张三的指纹进行对比，如果不匹配，则对该特定相册进行加密并隐藏，或屏蔽所述触控操作，使触控操作暂时失效。

可选地，在本发明的一些可能的实施方式中，采用一般的对预设信息设定密码的方式对预设信息进行加密。

5 可以看出，本实施例的方案中，在预设界面获取用户对触摸屏进行触控操作时的指纹信息，所述预设界面指预设信息的访问界面；判断所述指纹信息与预设指纹信息是否匹配；若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作，使触控操作暂时失效。从而当只在预设界面上获取到的用户对触摸屏进行触控操作时的指纹信息与
10 预设指纹信息不匹配时，只对预设信息进行加密，计算量小，系统开销小，效率高。

可选地，在本发明的一些可能的实施方式中，所述预设信息包括特定数据或特定应用，所述对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作，包括：

15 若所述预设信息为特定数据，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作；

若所述预设信息为特定应用，则对所述预设信息进行加密和/或终止访问所述预设信息，或屏蔽所述触控操作。

20 可选地，在本发明的一些可能的实施方式中，对所述特定数据进行加密时，可以用密码对特定数据进行加密。

可选地，在本发明的另一些可能的实施方式中，对所述特定数据进行加密时，也可以利用一定的编码方式对数据进行加密。

25 举例说明，在本发明的一些可能的实施方式中，当预设信息为特定数据时，以存储在手机中的某一私密文件为例，当用户触控触摸屏时的指纹信息与预设指纹信息不匹配时，则可对私密文件进行加密，也可以对私密文件进行隐藏，还可以对私密文件进行加密后并隐藏，或者在此时屏蔽用户对触摸屏进行的触控操作，使触控操作暂时失效，从而实现对私密文件的保护。

再举例说明，在本发明的一些可能的实施方式中，当预设信息为特定应用时，以手机相册应用为例，当用户触控触摸屏时的指纹信息与预设指纹信息不
30 匹配时，则可以对手机相册应用进行加密，此时需要用户输入密码才能进入，

还可以终止用户访问该手机相册,或者在此时屏蔽用户对触摸屏进行的触控操作,使触控操作暂时失效,从而实现对手机相册应用的隐私保护。

可以理解,在预设信息为特定数据时,若触控触摸屏时的指纹信息与预设指纹信息不匹配时,对特定数据进行加密和/或隐藏,或者屏蔽用户对触摸屏进行的触控操作,使触控操作暂时失效,可以阻止用户继续访问特定数据,实现了对特定数据的保护;在预设信息为特定应用时,若触控触摸屏时的指纹信息与预设指纹信息不匹配时,对特定应用进行加密和/或终止用户继续访问该应用,或者屏蔽用户对触摸屏进行的触控操作,使触控操作暂时失效,实现了对特定应用的隐私保护,并且由于只对特定数据或特定应用进行加密,而不是对全部数据进行加密,计算量小。

可选地,在本发明的一些可能的实施方式中,所述在预设界面获取用户对触摸屏进行触控操作时的指纹信息,包括:

若在所述预设界面上获取用户对触摸屏进行的触控操作为按压操作时,则当按压操作发生时,获取指纹信息;

若在所述预设界面上获取用户对触摸屏进行的触控操作为滑动操作时,则在滑动操作起始时刻获取指纹信息。

可选地,在本发明的一些可能的实施方式中,不管用户在预设界面上进行的是何种操作,当接收到用户的对预设界面的触压并且在触压之前或者之后有离开预设界面的操作时,则对指纹信息进行识别。

可选地,在本发明的一些可能的实施方式中,终端通过在屏幕下安装指纹传感器,从而终端可以在用户触摸预设界面屏幕上的任何位置获取用户触控触摸屏时的指纹信息,方便用户操作。

可选地,在本发明的另一些可能的实施方式中,终端也可以在预设界面的特定位置读取用户触控触摸屏时的指纹信息。

可以理解,当用户在预设界面上对触摸屏进行的触控操作可能为按压操作,此时接收按压操作发生时的指纹信息即可正确识别到用户的指纹,当用户在预设界面上对触摸屏进行的触控操作为滑动操作时,选取滑动起始时刻用户接触到预设界面的指纹信息可正确地对用户的指纹进行识别。

可选地,在本发明的一些可能的实施方式中,所述方法还包括:

在所述预设信息的生成过程中,不对所述预设信息做任何加密处理。

举例说明,在本发明的一些可能的实施方式中,在用手机进行拍照后生成照片并将照片存储在手机相册时,此时不对存储于手机相册里面的照片进行任何加密处理,只在后续用户读取手机相册里面的特定照片时,若用户触控触摸屏时的指纹信息与预设指纹信息不匹配时对该特定照片进行加密处理,从而使
5 得计算量小,效率高。

可以理解,若在信息生成的过程中对信息进行加密处理,则需要对所有的信息均进行加密处理,后续在对任一信息进行读取时,相应地都需要进行解密,从而导致计算量大,系统开销大;而在信息生成的过程中不对信息进行加密处理,只在后续读取预设信息时,当用户触控触摸屏时的指纹信息与预设指纹信息不匹配时,只对用户需要访问的预设信息进行加密处理,那么加密的预设信息只是总的信息的一部分,数据量少,从而使得计算量小,系统开销小,效率
10 高。

可选地,在本发明的一些可能的实施方式中,所述方法还包括:

若所述指纹信息与所述预设指纹信息匹配,则显示所述预设信息。

15 可选地,在本发明的一些可能的实施方式中,所述方法还包括:

当所述预设信息为特定数据时,若所述指纹信息与所述预设指纹信息匹配,则显示所述预设信息。

举例说明,在本发明的一些可能的实施方式中,若预设信息为手机相册应用里面的私密相册时,由于在该私密相册里面的照片的生成过程中没有对照片
20 进行加密处理,所以在查看该私密相册,并且用户触控触摸屏时的指纹信息与预设指纹信息匹配时,不需要对该私密相册进行解密则可以直接查看,也即手机直接显示该私密相册给用户。

可选地,在本发明的一些可能的实施方式中,所述方法还包括:

25 当所述预设信息为特定应用时,若所述指纹信息与所述预设指纹信息匹配,则访问所述预设信息。

举例说明,在本发明的一些可能的实施方式中,若预设信息为手机相册应用,由于手机相册应用在初始设置时没有进行加密处理,所以在访问手机相册应用,并且用户触控触摸屏时的指纹信息与预设指纹信息匹配时,可以直接进入手机相册。

30 可以理解,在特定数据生成过程不对特定数据进行加密,以及特定应用初

始设置的时候不对特定应用进行加密,那么在后续有访问权限的用户进行访问时,则不需要对特定数据或者特定应用进行解密即可直接查看特定数据或者访问特定应用,系统开销小,操作方便。

可选地,在本发明的一些可能的实施方式中,所述若所述指纹信息与所述预设指纹信息不匹配,则对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作后,所述方法还包括:

若再获取到所述预设指纹信息,对所述预设信息进行解密和/或显示。

可以理解,由于之前当接收到的用户触控触摸屏时的指令信息不是预设指纹信息时,对该预设信息进行加密或屏蔽该触控操作等操作,从而用户无法查看该预设信息,实现了对预设信息的保护,由于屏蔽该触控操作只时暂时在该预设界面对触控操作进行屏蔽,当再次进入预设界面时,继续获取用户触控触摸屏时的指纹信息,从而当再将获取到预设指纹信息时,将预设信息呈现给有权限用户,实现了有权限用户对预设信息的访问。

可选地,在本发明的另一些可能的实施方式中,当所述预设信息为特定数据时,所述若所述指纹信息与所述预设指纹信息不匹配,则对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作后,所述方法还包括:

若再获取到所述预设指纹,对所述预设信息进行解密和/或显示。可选地,在本发明的一些可能的实施方式中,当之前对特定数据进行加密后,则当再获取到预设指纹信息时,对特定数据进行解密,当之前对特定数据进行隐藏,则当再获取到预设指纹信息时,显示特定数据,当之前加密并隐藏特定数据,则当再获取到预设指纹信息时,显示并解密特定数据。

举例说明,在本发明的一些可能的实施方式中,若由于在访问手机中的某一私密文件时,获取到用户触控触摸屏时的指纹信息不是预设指纹信息时,则对该私密文件进行加密处理,从而用户无法访问该私密文件,当再获取到用户触控触摸屏时的指纹信息为预设指纹信息时,解密该私密文件,从而用户可访问该私密文件。

可选地,在本发明的另一些可能的实施方式中,当所述预设信息为特定应用时,所述若所述指纹信息与所述预设指纹信息不匹配,则对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作后,所述方法还包括:

若再获取到所述预设指纹信息,对所述预设信息进行解密和/或允许访问

所述预设信息。

可选地，在本发明的一些可能的实施方式中，当之前对特定应用进行加密后，则当再获取到的指纹信息与预设指纹信息匹配时，对特定应用进行解密，当之前由于获取到的指纹信息与预设指纹信息不匹配时，终止进入特定应用，
5 则当再获取到的指纹信息与预设指纹信息匹配时，允许进入特定应用。

举例说明，在本发明的一些可能的实施方式中，在对手机相册进行访问时，当无权限用户在访问界面触控触摸屏时的指纹信息不是预设指纹信息时，退出手机相册，当再次由有权限用户在访问界面触控触摸屏时的指纹信息为预设指纹信息时，允许进入手机相册。

10 为了便于更好理解和实施本发明实施例的上述方案，下面结合一些具体的应用场景进行举例说明。

请参见图 2，图 2 是本发明的另一个实施例提供的另一种数据加密方法的流程示意图，其中，如图 2 所示，本发明的另一个实施例提供的另一种数据加密方法可以包括：

15 S201、在预设界面获取用户对触摸屏进行触控操作时的指纹信息，预设界面为预设信息的访问界面。

其中，预设信息指存储于终端中特定位置、由终端系统或者用户设定的、需要对其访问进行限制的特定信息，包括特定数据或特定应用等，如可以为手机相册、手机短信、QQ、微信等特定应用，也可以为手机相册应用里面的某一个相册、手机短信应用里面的短信等，还可以为存储在终端中的某一特定文件等；
20

预设界面是指终端提供给用户访问预设信息的用户界面，如手机相册、手机短信等的访问界面，或手机进入相册后，查看某一指定相册的界面；预设界面还可以为屏幕的解锁界面等。

25 其中，终端指手机、平板电脑等智能终端，该终端具有能够进行指纹识别的触摸屏，该触摸屏能够感应用户的按压、滑动等操作，并能对与触摸屏接触的指纹进行识别。终端可以在预设界面通过具有指纹识别的触摸屏的任何位置获取用户触控触摸屏时的指纹信息。

可选地，在本发明的一些可能的实施方式中，该预设界面根据用户的需要，
30 将预设信息的访问界面设置为预设界面，从而用户在通过该预设界面进入该应

用或者数据时，终端实时通过触摸屏对用户触控触摸屏时的指纹信息进行识别。

举例说明，在本发明的一些可能的实施方式中，若设置手机相册为敏感信息，则将预设界面设置为访问相册的用户界面，那么当用户访问到该用户界面
5 时，终端实时读取用户在该用户界面上触控触摸屏时的指纹信息。

可选地，在预设界面获取用户触控触摸屏时的指纹信息时，可以通过识别用户在预设界面的按压操作。

可选地，在预设界面获取用户触控触摸屏时的指纹信息时，可以通过识别用户在预设界面的滑动操作。

10 可选地，在本发明的一些可能的实施方式中，所述在预设界面获取用户对触摸屏进行触控操作时的指纹信息，包括：

若在所述预设界面上获取用户对触摸屏进行的触控操作为按压操作时，则当按压操作发生时，获取指纹信息；

15 若在所述预设界面上获取用户对触摸屏进行的触控操作为滑动操作时，则在滑动操作起始时刻获取指纹信息。

可选地，在本发明的一些可能的实施方式中，不管用户在预设界面上进行的是何种操作，当接收到用户的对预设界面的触压并且在触压之前或者之后有离开预设界面的操作时，则对指纹信息进行识别。

20 可选地，在本发明的一些可能的实施方式中，终端通过在屏幕下安装指纹传感器，从而终端可以在用户触摸预设界面屏幕上的任何位置读取用户触控触摸屏时的指纹信息，方便用户操作。

可选地，在本发明的另一些可能的实施方式中，终端也可以在预设界面的特定位置读取用户触控触摸屏时的指纹信息。

25 可以理解，当用户在预设界面上对触摸屏进行的触控操作可能为按压操作，此时接收按压操作发生时的指纹信息即可正确识别到用户的指纹，当用户在预设界面上对触摸屏进行的触控操作为滑动操作时，选取滑动起始时刻用户接触到预设界面的指纹信息可正确地对用户的指纹进行识别。

S202、判断该指纹信息与预设指纹信息是否匹配。

30 其中，所述指纹信息指用户在预设界面读取到的指纹信息，可通过指纹传感器感应用户在触摸屏上的按压、滑动等操作进行指纹识别。

其中，预设指纹信息指预先存储在终端中的指纹信息，用于与通过触摸屏获取收到的用户触控触摸屏时的指纹信息进行对比。

可选地，在本发明的一些可能的实施方式中，该预设指纹信息可以为一个，从而所接收到的用户录入的指纹信息只需要与这一个预设指纹信息进行对比，
5 判断用户触控触摸屏时的指纹信息是否与该预设指纹信息匹配。

可选地，在本发明的另一些可能的实施方式中，该预设指纹信息也可以为多个，从而所接收到的用户触控触摸屏时的指纹信息需要与多个预设指纹信息进行对比，用于判断用户触控触摸屏时的指纹信息是否与预设指纹信息匹配。

可选地，在本发明的一些可能的实施方式中，进入不同应用的预设指纹信息可以不一样，也可以一样。
10

可选地，在本发明的另一些可能的实施方式中，所述预设指纹信息可以由有权限用户进行更改。

S203、若该指纹信息与预设指纹信息不匹配，对预设信息进行加密和/或隐藏，或屏蔽触控操作。

15 其中，屏蔽所述触控操作指在获取到的用户触控触摸屏时的指纹信息与预设指纹信息不匹配时，暂时使用户在该预设界面的触控操作失效，从而使得在获取到非预设指纹信息时不再在预设界面继续获取用户触控触摸屏的指纹信息，减少系统开销，当下次再进入该预设界面时，触控操作自动重新恢复有效，。

可选地，在本发明的一些可能的实施方式中，当预设指纹信息为一个时，
20 判断判断用户触控触摸屏时的指纹信息是否与该一个预设指纹信息是否匹配，若用户触控触摸屏时的指纹信息与该预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

可选地，在本发明的另一些可能的实施方式中，当预设指纹信息为多个时，判断用户触控触摸屏时的指纹信息与其中任一个预设指纹信息是否匹配，若
25 用户触控触摸屏时的指纹信息与其中任一个预设指纹信息匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

举例说明，在本发明的一些可能的实施方式中，当设置手机相册应用具有访问权限的用户为张三和李四，则可以将预设指纹信息设置为张三和李四的指纹，那么在手机相册的访问界面上接收到指纹信息时，将该指纹信息与预设的
30 张三和李四的指纹进行对比，如果不匹配，则拒绝访问手机相册。

再举例说明,在本发明的另一些可能的实施方式中,当设置手机相册应用里面的某一个特定相册具有访问权限的用户为张三,则将预设指纹信息设置为张三的指纹,那么在该特定相册的访问界面上接收到指纹信息时,将该指纹信息与预设的张三的指纹进行对比,如果不匹配,则对该特定相册进行加密并隐藏,或屏蔽所述触控操作,使触控操作暂时失效。

可选地,在本发明的一些可能的实施方式中,采用一般的对预设信息设定密码的方式对预设信息进行加密。

可选地,在本发明的一些可能的实施方式中,所述预设信息包括特定数据或特定应用,所述对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作,包括:

若所述预设信息为特定数据,则对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作;

若所述预设信息为特定应用,则对所述预设信息进行加密和/或终止访问所述预设信息,或屏蔽所述触控操作。

可选地,在本发明的一些可能的实施方式中,对所述特定数据进行加密时,可以用密码对特定数据进行加密。

可选地,在本发明的另一些可能的实施方式中,对所述特定数据进行加密时,也可以利用一定的编码方式对数据进行加密。

举例说明,在本发明的一些可能的实施方式中,当预设信息为特定数据时,以存储在手机中的某一私密文件为例,当用户触控触摸屏时的指纹信息与预设指纹信息不匹配时,则可对私密文件进行加密,也可以对私密文件进行隐藏,还可以对私密文件进行加密后并隐藏,或者在此时屏蔽用户对触摸屏进行的触控操作,使触控操作暂时失效,从而实现对私密文件的保护。

再举例说明,在本发明的一些可能的实施方式中,当预设信息为特定应用时,以手机相册应用为例,当用户触控触摸屏时的指纹信息与预设指纹信息不匹配时,则可以对手机相册应用进行加密,此时需要用户输入密码才能进入,还可以终止用户访问该手机相册,或者在此时屏蔽用户对触摸屏进行的触控操作,使触控操作暂时失效,从而实现对手机相册应用的隐私保护。

可以理解,在预设信息为特定数据时,若用户触控触摸屏时的指纹信息与预设指纹信息不匹配时,对特定数据进行加密和/或隐藏,或者屏蔽用户对触

5 触摸屏进行的触控操作,使触控操作暂时失效,可以阻止用户继续访问特定数据,实现了对特定数据的保护;在预设信息为特定应用时,若用户触控触摸屏时的指纹信息与预设指纹信息不匹配时,对特定应用进行加密和/或终止用户继续访问该应用,或者屏蔽用户对触摸屏进行的触控操作,使触控操作暂时失效,实现了对特定应用的隐私保护,并且由于只对特定数据或特定应用进行加密,而不是对全部数据进行加密,计算量小。

可选地,在本发明的一些可能的实施方式中,所述方法还包括:

在所述预设信息的生成过程中,不对所述预设信息做任何加密处理。

10 举例说明,在本发明的一些可能的实施方式中,在用手机进行拍照后生成照片并将照片存储在手机相册时,此时不对存储于手机相册里面的照片进行任何加密处理,只在后续用户读取手机相册里面的特定照片时,若用户触控触摸屏时的指纹信息与预设指纹信息不匹配时对该特定照片进行加密处理,从而使得计算量小,效率高。

15 可以理解,若在信息生成的过程中对信息进行加密处理,则需要对所有的信息均进行加密处理,后续在对任一信息进行读取时,相应地都需要进行解密,从而导致计算量大,系统开销大;而在信息生成的过程中不对信息进行加密处理,只在后续读取预设信息时,当用户触控触摸屏时的指纹信息与预设指纹信息不匹配时,只对用户需要访问的预设信息进行加密处理,那么加密的预设信息只是总的信息的一部分,数据量少,从而使得计算量小,系统开销小,效率高。

20 S204、若再接收到预设指纹信息,则显示预设信息。

可选地,在本发明的一些可能的实施方式中,所述若所述指纹信息与所述预设指纹信息不匹配,则对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作后,所述方法还包括:

25 若再获取到所述预设指纹信息,对所述预设信息进行解密和/或显示。

可以理解,由于之前当接收到的用户触控触摸屏时的指令信息不是预设指纹信息时,对该预设信息进行加密或屏蔽该触控操作等操作,从而用户无法查看该预设信息,实现了对预设信息的保护,由于屏蔽该触控操作只时暂时在该预设界面对触控操作进行屏蔽,当再次进入预设界面时,继续获取用户触控触摸屏时的指纹信息,从而当再将获取到预设指纹信息时,将预设信息呈现给有

权限用户，实现了有权限用户对预设信息的访问。

可选地，在本发明的另一些可能的实施方式中，当所述预设信息为特定数据时，所述若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作后，所述方法还包括：

5 若再获取到所述预设指纹，对所述预设信息进行解密和/或显示。可选地，在本发明的一些可能的实施方式中，当之前对特定数据进行加密后，则当再获取到预设指纹信息时，对特定数据进行解密，当之前对特定数据进行隐藏，则当再获取到预设指纹信息时，显示特定数据，当之前加密并隐藏特定数据，则当再获取到预设指纹信息时，显示并解密特定数据。

10 举例说明，在本发明的一些可能的实施方式中，若由于在访问手机中的某一私密文件时，获取到用户触控触摸屏时的指纹信息不是预设指纹信息时，则对该私密文件进行加密处理，从而用户无法访问该私密文件，当再获取到用户触控触摸屏时的指纹信息为预设指纹信息时，解密该私密文件，从而用户可访问该私密文件。

15 可选地，在本发明的另一些可能的实施方式中，当所述预设信息为特定应用时，所述若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作后，所述方法还包括：

 若再获取到所述预设指纹信息，对所述预设信息进行解密和/或允许访问所述预设信息。

20 可选地，在本发明的一些可能的实施方式中，当之前对特定应用进行加密后，则当再获取到的指纹信息与预设指纹信息匹配时，对特定应用进行解密，当之前由于获取到的指纹信息与预设指纹信息不匹配时，终止进入特定应用，则当再获取到的指纹信息与预设指纹信息匹配时，允许进入特定应用。

25 举例说明，在本发明的一些可能的实施方式中，在对手机相册进行访问时，当无权限用户在访问界面触控触摸屏时的指纹信息不是预设指纹信息时，退出手机相册，当再次由有权限用户在访问界面触控触摸屏时的指纹信息为预设指纹信息时，允许进入手机相册。

 可选地，在本发明的一些可能的实施方式中，所述方法还包括：

 若所述指纹信息与所述预设指纹信息匹配，则显示所述预设信息。

30 可选地，在本发明的一些可能的实施方式中，所述方法还包括：

当所述预设信息为特定数据时，若所述指纹信息与所述预设指纹信息匹配，则显示所述预设信息。

举例说明，在本发明的一些可能的实施方式中，若预设信息为手机相册应用里面的私密相册时，由于在该私密相册里面的照片的生成过程中没有对照片进行加密处理，所以在查看该私密相册，并且用户触控触摸屏时的指纹信息与预设指纹信息匹配时，不需要对该私密相册进行解密则可以直接查看，也即手机直接显示该私密相册给用户。

可选地，在本发明的一些可能的实施方式中，所述方法还包括：

当所述预设信息为特定应用时，若所述指纹信息与所述预设指纹信息匹配，则访问所述预设信息。

举例说明，在本发明的一些可能的实施方式中，若预设信息为手机相册应用，由于手机相册应用在初始设置时没有进行加密处理，所以在访问手机相册应用，并且用户触控触摸屏时的指纹信息与预设指纹信息匹配时，可以直接进入手机相册。

可以理解，在特定数据生成过程不对特定数据进行加密，以及特定应用初始设置的时候不对特定应用进行加密，那么在后续有访问权限的用户进行访问时，则不需要对特定数据或者特定应用进行解密即可直接查看特定数据或者访问特定应用，系统开销小，操作方便。

可以看出，本实施例的方案中，在预设界面获取用户对触摸屏进行触控操作时的指纹信息，所述预设界面指预设信息的访问界面；判断所述指纹信息与预设指纹信息是否匹配；若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作，使触控操作暂时失效。从而当只在预设界面上获取到的用户对触摸屏进行触控操作时的指纹信息与预设指纹信息不匹配时，只对预设信息进行加密，计算量小，系统开销小，效率高。。

下面再举例一个更为具体的应用场景。

例如，在用户进行拍照时不对手机相册进行加密处理，如果要对手机相册进行安全控制，首先需要将手机相册设置为需要通过指纹识别才能进入的一个应用，并且对手机相册设置该手机主人的指纹为预设指纹，则在后续所有使用该手机的所有用户在相册的访问界面访问该相册时，当用户按压到手机屏幕的

任何位置时，指纹传感器将会感应到用户的指纹，对指纹进行识别。首先当手机主人访问手机相册时，可识别到手机主人按压手机屏幕的指纹信息为预设指纹信息，可直接允许手机主人进入手机相册，从而实现手机主人在访问手机相册时不需要对手机相册进行任何加密解密处理即可以访问，操作方便，系统开销小。当其它用户想访问该相册时，再通过识别到该用户按压手机屏幕时的指纹信息不是预设指纹信息，对手机相册进行加密，并终止该用户访问手机相册，同时暂时使该用户在该界面上触控触摸屏的操作失效，下次重新进入该用户界面时才使触控操作恢复有效，从而实现对手机相册的加密保护。

更进一步地，当手机主人再次访问该手机相册时，手机再次识别手机主人按压触摸屏时的指纹信息，判断与预设指纹信息一致，重新对手机相册进行解密，并允许手机主人访问该相册。

请参见图 3，图 3 是本发明的一个实施例提供的一种数据加密装置的结构示意图，其中，如图 3 所示，本发明的一个实施例提供的一种数据加密装置 300 可以包括：

读取模块 310、判断模块 320 和加密模块 330。

其中，读取模块 310，用于在预设界面获取用户对触摸屏进行触控操作时的指纹信息，所述预设界面指预设信息的访问界面。

其中，预设信息指存储于终端中特定位置、由终端系统或者用户设定的、需要对其访问进行限制的特定信息，包括特定数据或特定应用等，如可以为手机相册、手机短信、QQ、微信等特定应用，也可以为手机相册应用里面的某一个相册、手机短信应用里面的短信等，还可以为存储在终端中的某一特定文件等；

预设界面是指终端提供给用户访问预设信息的用户界面，如手机相册、手机短信等的访问界面，或手机进入相册后，查看某一指定相册的界面；预设界面还可以为屏幕的解锁界面等。

其中，终端指手机、平板电脑等智能终端，该终端具有能够进行指纹识别的触摸屏，该触摸屏能够感应用户的按压、滑动等操作，并能对与触摸屏接触的指纹进行识别。终端可以在预设界面通过具有指纹识别的触摸屏的任何位置获取用户触控触摸屏时的指纹信息。

可选地，在本发明的一些可能的实施方式中，该预设界面根据用户的需要，

将预设信息的访问界面设置为预设界面,从而用户在通过该预设界面进入该应用或者数据时,终端实时通过触摸屏对用户触控触摸屏时的指纹信息进行识别。

5 举例说明,在本发明的一些可能的实施方式中,若设置手机相册为敏感信息,则将预设界面设置为访问相册的用户界面,那么当用户访问到该用户界面时,终端实时读取用户在该用户界面上触控触摸屏时的指纹信息。

可选地,在预设界面获取用户触控触摸屏时的指纹信息时,可以通过识别用户在预设界面的按压操作。

10 可选地,在预设界面获取用户触控触摸屏时的指纹信息时,可以通过识别用户在预设界面的滑动操作。

判断模块 320,用于判断所述指纹信息与预设指纹信息是否匹配。

其中,所述指纹信息指用户在预设界面读取到的指纹信息,可通过指纹传感器感应用户在触摸屏上的按压、滑动等操作进行指纹识别。

15 其中,预设指纹信息指预先存储在终端中的指纹信息,用于与通过触摸屏获取收到的用户触控触摸屏时的指纹信息进行对比。

可选地,在本发明的一些可能的实施方式中,该预设指纹信息可以为一个,从而所接收到的用户录入的指纹信息只需要与这一个预设指纹信息进行对比,判断用户触控触摸屏时的指纹信息是否与该预设指纹信息匹配。

20 可选地,在本发明的另一些可能的实施方式中,该预设指纹信息也可以为多个,从而所接收到的用户触控触摸屏时的指纹信息需要与多个预设指纹信息进行对比,用于判断用户触控触摸屏时的指纹信息是否与预设指纹信息匹配。

可选地,在本发明的一些可能的实施方式中,进入不同应用的预设指纹信息可以不一样,也可以一样。

25 可选地,在本发明的另一些可能的实施方式中,所述预设指纹信息可以由有权限用户进行更改。

加密模块 330,用于若所述指纹信息与所述预设指纹信息不匹配,对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作。

30 其中,屏蔽所述触控操作指在获取到的用户触控触摸屏时的指纹信息与预设指纹信息不匹配时,暂时使用户在该预设界面的触控操作失效,从而使得在获取到非预设指纹信息时不再在预设界面继续获取用户触控触摸屏的指纹信

息,减少系统开销,当下次再进入该预设界面时,触控操作自动重新恢复有效,。

可选地,在本发明的一些可能的实施方式中,当预设指纹信息为一个时,判断用户触控触摸屏时的指纹信息是否与该一个预设指纹信息是否匹配,若用户触控触摸屏时的指纹信息与该预设指纹信息不匹配,则对所述预设信息
5 进行加密和/或隐藏,或屏蔽所述触控操作。

可选地,在本发明的另一些可能的实施方式中,当预设指纹信息为多个时,判断用户触控触摸屏时的指纹信息与其中任一个预设指纹信息是否匹配,若用户触控触摸屏时的指纹信息与其中任一个预设指纹信息匹配,则对所述预设信息
10 进行加密和/或隐藏,或屏蔽所述触控操作。

举例说明,在本发明的一些可能的实施方式中,当设置手机相册应用具有访问权限的用户为张三和李四,则可以将预设指纹信息设置为张三和李四的指纹,那么在手机相册的访问界面上接收到指纹信息时,将该指纹信息与预设的张三和李四的指纹进行对比,如果不匹配,则拒绝访问手机相册。

再举例说明,在本发明的另一些可能的实施方式中,当设置手机相册应用
15 里面的某一个特定相册具有访问权限的用户为张三,则将预设指纹信息设置为张三的指纹,那么在该特定相册的访问界面上接收到指纹信息时,将该指纹信息与预设的张三的指纹进行对比,如果不匹配,则对该特定相册进行加密并隐藏,或屏蔽所述触控操作,使触控操作暂时失效。

可选地,在本发明的一些可能的实施方式中,采用一般的对预设信息设定
20 密码的方式对预设信息进行加密。

可以理解的是,本实施例的数据加密装置 300 的各功能模块的功能可根据上述方法实施例中的方法具体实现,其具体实现过程可以参照上述方法实施例的相关描述,此处不再赘述。

可以看出,本实施例的方案中,数据加密装置 300 在预设界面获取用户对
25 触摸屏进行触控操作时的指纹信息,所述预设界面指预设信息的访问界面;数据加密装置 300 判断所述指纹信息与预设指纹信息是否匹配;若所述指纹信息与所述预设指纹信息不匹配,则数据加密装置 300 对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作,使触控操作暂时失效。从而当只在预设界面上获取到的用户对触摸屏进行触控操作时的指纹信息与预设指纹信息不匹配
30 时,只对预设信息进行加密,计算量小,系统开销小,效率高。请参见图 4,

图 4 是本发明的一个实施例提供的一种数据加密装置的结构示意图, 其中, 如图 4 所示, 本发明的一个实施例提供的一种数据加密装置 300 可以包括:

读取模块 410、判断模块 420 和加密模块 430。

其中, 读取模块 410, 用于在预设界面获取用户对触摸屏进行触控操作时的
5 的指纹信息, 所述预设界面指预设信息的访问界面。

其中, 预设信息指存储于终端中特定位置、由终端系统或者用户设定的、
需要对其访问进行限制的特定信息, 包括特定数据或特定应用等, 如可以为手机相册、手机短信、QQ、微信等特定应用, 也可以为手机相册应用里面的某一个相册、手机短信应用里面的短信等, 还可以为存储在终端中的某一特定文件等;
10 件等;

预设界面是指终端提供给用户访问预设信息的用户界面, 如手机相册、手机短信等的访问界面, 或手机进入相册后, 查看某一指定相册的界面; 预设界面还可以为屏幕的解锁界面等。

其中, 终端指手机、平板电脑等智能终端, 该终端具有能够进行指纹识别
15 的触摸屏, 该触摸屏能够感应用户的按压、滑动等操作, 并能对与触摸屏接触的指纹进行识别。终端可以在预设界面通过具有指纹识别的触摸屏的任何位置获取用户触控触摸屏时的指纹信息。

可选地, 在本发明的一些可能的实施方式中, 该预设界面根据用户的需要, 将预设信息的访问界面设置为预设界面, 从而用户在通过该预设界面进入该应用或者数据时, 终端实时通过触摸屏对用户触控触摸屏时的指纹信息进行识别。
20 别。

举例说明, 在本发明的一些可能的实施方式中, 若设置手机相册为敏感信息, 则将预设界面设置为访问相册的用户界面, 那么当用户访问到该用户界面时, 终端实时读取用户在该用户界面上触控触摸屏时的指纹信息。

25 可选地, 在预设界面获取用户触控触摸屏时的指纹信息时, 可以通过识别用户在预设界面的按压操作。

可选地, 在预设界面获取用户触控触摸屏时的指纹信息时, 可以通过识别用户在预设界面的滑动操作。

判断模块 420, 用于判断所述指纹信息与预设指纹信息是否匹配。

30 其中, 所述指纹信息指用户在预设界面读取到的指纹信息, 可通过指纹传

感器感应用户在触摸屏上的按压、滑动等操作进行指纹识别。

其中，预设指纹信息指预先存储在终端中的指纹信息，用于与通过触摸屏获取收到的用户触控触摸屏时的指纹信息进行对比。

5 可选地，在本发明的一些可能的实施方式中，该预设指纹信息可以为一个，从而所接收到的用户录入的指纹信息只需要与这一个预设指纹信息进行对比，判断用户触控触摸屏时的指纹信息是否与该预设指纹信息匹配。

可选地，在本发明的另一些可能的实施方式中，该预设指纹信息也可以为多个，从而所接收到的用户触控触摸屏时的指纹信息需要与多个预设指纹信息进行对比，用于判断用户触控触摸屏时的指纹信息是否与预设指纹信息匹配。

10 可选地，在本发明的一些可能的实施方式中，进入不同应用的预设指纹信息可以不一样，也可以一样。

可选地，在本发明的另一些可能的实施方式中，所述预设指纹信息可以由有权限用户进行更改。

15 加密模块 430，用于若所述指纹信息与所述预设指纹信息不匹配，对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

其中，屏蔽所述触控操作指在获取到的用户触控触摸屏时的指纹信息与预设指纹信息不匹配时，暂时使用户在该预设界面的触控操作失效，从而使得在获取到非预设指纹信息时不再在预设界面继续获取用户触控触摸屏的指纹信息，减少系统开销，当下次再进入该预设界面时，触控操作自动重新恢复有效。

20 可选地，在本发明的一些可能的实施方式中，当预设指纹信息为一个时，判断判断用户触控触摸屏时的指纹信息是否与该一个预设指纹信息是否匹配，若用户触控触摸屏时的指纹信息与该预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

25 可选地，在本发明的另一些可能的实施方式中，当预设指纹信息为多个时，判断用户触控触摸屏时的指纹信息与其中任一个预设指纹信息是否匹配，若用户触控触摸屏时的指纹信息与其中任一个预设指纹信息匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

30 举例说明，在本发明的一些可能的实施方式中，当设置手机相册应用具有访问权限的用户为张三和李四，则可以将预设指纹信息设置为张三和李四的指纹，那么在手机相册的访问界面上接收到指纹信息时，将该指纹信息与预设的

张三和李四的指纹进行对比，如果不匹配，则拒绝访问手机相册。

再举例说明，在本发明的另一些可能的实施方式中，当设置手机相册应用里面的某一个特定相册具有访问权限的用户为张三，则将预设指纹信息设置为张三的指纹，那么在该特定相册的访问界面上接收到指纹信息时，将该指纹信息5 与预设的张三的指纹进行对比，如果不匹配，则对该特定相册进行加密并隐藏，或屏蔽所述触控操作，使触控操作暂时失效。

可选地，在本发明的一些可能的实施方式中，采用一般的对预设信息设定密码的方式对预设信息进行加密。

可选地，在本发明的一些可能的实施方式中，所述预设信息包括特定数据10 或特定应用，所述加密模块包括：

第一加密单元 431，用于若所述预设信息为特定数据，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作；

第二加密单元 432，用于若所述预设信息为特定应用，则对所述预设信息进行加密和/或终止访问所述预设信息，或屏蔽所述触控操作。

15 可选地，在本发明的一些可能的实施方式中，对所述特定数据进行加密时，可以用密码对特定数据进行加密。

可选地，在本发明的另一些可能的实施方式中，对所述特定数据进行加密时，也可以利用一定的编码方式对数据进行加密。

举例说明，在本发明的一些可能的实施方式中，当预设信息为特定数据时，20 以存储在手机中的某一私密文件为例，当用户触控触摸屏时的指纹信息与预设指纹信息不匹配时，则可对私密文件进行加密，也可以对私密文件进行隐藏，还可以对私密文件进行加密后并隐藏，或者在此时屏蔽用户对触摸屏进行的触控操作，使触控操作暂时失效，从而实现对私密文件的保护。

再举例说明，在本发明的一些可能的实施方式中，当预设信息为特定应用25 时，以手机相册应用为例，当用户触控触摸屏时的指纹信息与预设指纹信息不匹配时，则可以对手机相册应用进行加密，此时需要用户输入密码才能进入，还可以终止用户访问该手机相册，或者在此时屏蔽用户对触摸屏进行的触控操作，使触控操作暂时失效，从而实现对手机相册应用的隐私保护。

可以理解，在预设信息为特定数据时，若用户触控触摸屏时的指纹信息与30 预设指纹信息不匹配时，对特定数据进行加密和/或隐藏，或者屏蔽用户对触

5 触摸屏进行的触控操作,使触控操作暂时失效,可以阻止用户继续访问特定数据,实现了对特定数据的保护;在预设信息为特定应用时,若用户触控触摸屏时的指纹信息与预设指纹信息不匹配时,对特定应用进行加密和/或终止用户继续访问该应用,或者屏蔽用户对触摸屏进行的触控操作,使触控操作暂时失效,实现了对特定应用的隐私保护,并且由于只对特定数据或特定应用进行加密,而不是对全部数据进行加密,计算量小。

可选地,在本发明的一些可能的实施方式中,所述读取模块包括:

第一读取单元 411,用于若在上述预设界面上获取用户对触摸屏进行的触控操作为按压操作时,则当按压操作发生时,获取指纹信息;

10 第二读取单元 412,用于若在上述预设界面上获取用户对触摸屏进行的触控操作为滑动操作时,则在滑动操作起始时刻获取指纹信息。

可选地,在本发明的一些可能的实施方式中,不管用户在预设界面上进行的是何种操作,当接收到用户的对预设界面的触压并且在触压之前或者之后有离开预设界面的操作时,则对指纹信息进行识别。

15 可选地,在本发明的一些可能的实施方式中,终端通过在屏幕下安装指纹传感器,从而终端可以在用户触摸预设界面屏幕上的任何位置读取用户触控触摸屏时的指纹信息,方便用户操作。

可选地,在本发明的另一些可能的实施方式中,终端也可以在预设界面的特定位置读取用户触控触摸屏时的指纹信息。

20 可以理解,当用户在预设界面上对触摸屏进行的触控操作可能为按压操作,此时接收按压操作发生时的指纹信息即可正确识别到用户的指纹,当用户在预设界面上对触摸屏进行的触控操作为滑动操作时,选取滑动起始时刻用户接触到预设界面的指纹信息可正确地对用户的指纹进行识别。

25 可选地,在本发明的一些可能的实施方式中,所述数据加密装置 400 还用于:

在上述预设信息的生成过程中,不对所述预设信息做任何加密处理。

举例说明,在本发明的一些可能的实施方式中,在用手机进行拍照后生成照片并将照片存储在手机相册时,此时不对存储于手机相册里面的照片进行任何加密处理,只在后续用户读取手机相册里面的特定照片时,若用户触控触摸屏时的指纹信息与预设指纹信息不匹配时对该特定照片进行加密处理,从而使

30

得计算量小，效率高。

可以理解，若在信息生成的过程中对信息进行加密处理，则需要对所有的信息均进行加密处理，后续在对任一信息进行读取时，相应地都需要进行解密，从而导致计算量大，系统开销大；而在信息生成的过程中不对信息进行加密处理，只在后续读取预设信息时，当用户触控触摸屏时的指纹信息与预设指纹信息不匹配时，只对用户需要访问的预设信息进行加密处理，那么加密的预设信息只是总的信息的一部分，数据量少，从而使得计算量小，系统开销小，效率高。

10 可选地，在本发明的一些可能的实施方式中，所述数据加密装置 400 还包括显示模块 440，用于：

若所述指纹信息与所述预设指纹信息匹配，则显示所述预设信息。

可选地，在本发明的一些可能的实施方式中，所述显示模块 440 用于：

当所述预设信息为特定数据时，若所述指纹信息与所述预设指纹信息匹配，则显示所述预设信息。

15 举例说明，在本发明的一些可能的实施方式中，若预设信息为手机相册应用里面的私密相册时，由于在该私密相册里面的照片的生成过程中没有对照片进行加密处理，所以在查看该私密相册，并且用户触控触摸屏时的指纹信息与预设指纹信息匹配时，不需要对该私密相册进行解密则可以直接查看，也即手机直接显示该私密相册给用户。

20 可选地，在本发明的一些可能的实施方式中，所述显示模块 440 用于：

当所述预设信息为特定应用时，若所述指纹信息与所述预设指纹信息匹配，则访问所述预设信息。

25 举例说明，在本发明的一些可能的实施方式中，若预设信息为手机相册应用，由于手机相册应用在初始设置时没有进行加密处理，所以在访问手机相册应用，并且用户触控触摸屏时的指纹信息与预设指纹信息匹配时，可以直接进入手机相册。

30 可以理解，在特定数据生成过程不对特定数据进行加密，以及特定应用初始设置的时候不对特定应用进行加密，那么在后续有访问权限的用户进行访问时，则不需要对特定数据或者特定应用进行解密即可直接查看特定数据或者访问特定应用，系统开销小，操作方便。

可选地，在本发明的一些可能的实施方式中，在所述加密模块 430 之后，所述装置还包括：

解密模块 450，用于若再接收到所述预设指纹，对所述预设信息进行解密和/或显示。

- 5 可以理解，由于之前当接收到的用户触控触摸屏时的指令信息不是预设指纹信息时，对该预设信息进行加密或屏蔽该触控操作等操作，从而用户无法查看该预设信息，实现了对预设信息的保护，由于屏蔽该触控操作只时暂时在该预设界面对触控操作进行屏蔽，当再次进入预设界面时，继续获取用户触控触摸屏时的指纹信息，从而当再将获取到预设指纹信息时，将预设信息呈现给有
- 10 权限用户，实现了有权限用户对预设信息的访问。

可选地，在本发明的另一些可能的实施方式中，当所述预设信息为特定数据时，所述解密模块 450 用于：

若再获取到所述预设指纹信息，对所述预设信息进行解密和/或显示。

- 15 可选地，在本发明的一些可能的实施方式中，当之前对特定数据进行加密后，则当再获取到预设指纹信息时，对特定数据进行解密，当之前对特定数据进行隐藏，则当再获取到预设指纹信息时，显示特定数据，当之前加密并隐藏特定数据，则当再获取到预设指纹信息时，显示并解密特定数据。

- 20 举例说明，在本发明的一些可能的实施方式中，若由于在访问手机中的某一私密文件时，获取到用户触控触摸屏时的指纹信息不是预设指纹信息时，则对该私密文件进行加密处理，从而用户无法访问该私密文件，当再获取到用户触控触摸屏时的指纹信息为预设指纹信息时，解密该私密文件，从而用户可访问该私密文件。

可选地，在本发明的另一些可能的实施方式中，当所述预设信息为特定应用时，所述解密模块 450 用于：

- 25 若再获取到所述预设指纹信息，对所述预设信息进行解密和/或允许访问所述预设信息。

- 30 可选地，在本发明的一些可能的实施方式中，当之前对特定应用进行加密后，则当再获取到的指纹信息与预设指纹信息匹配时，对特定应用进行解密，当之前由于获取到的指纹信息与预设指纹信息不匹配时，终止进入特定应用，则当再获取到的指纹信息与预设指纹信息匹配时，允许进入特定应用。

举例说明,在本发明的一些可能的实施方式中,在对手机相册进行访问时,当无权限用户在访问界面触控触摸屏时的指纹信息不是预设指纹信息时,退出手机相册,当再次由有权限用户在访问界面触控触摸屏时的指纹信息为预设指纹信息时,允许进入手机相册。

5 可以理解的是,本实施例的数据加密装置 400 的各功能模块的功能可根据上述方法实施例中的方法具体实现,其具体实现过程可以参照上述方法实施例的相关描述,此处不再赘述。

可以看出,本实施例的方案中,数据加密装置 400 在预设界面获取用户对触摸屏进行触控操作时的指纹信息,所述预设界面指预设信息的访问界面;数据加密装置 400 判断所述指纹信息与预设指纹信息是否匹配;若所述指纹信息与所述预设指纹信息不匹配,则数据加密装置 400 对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作,使触控操作暂时失效。从而当只在预设界面上获取到的用户对触摸屏进行触控操作时的指纹信息与预设指纹信息不匹配时,只对预设信息进行加密,计算量小,系统开销小,效率高。参见图 5,图 10
15 5 是本发明的又一个实施例提供的又一种数据加密装置的结构示意图。如图 5 所示,本发明的又一个实施例提供的又一种数据加密装置 500 可以包括:至少一个总线 501、与总线相连的至少一个处理器 502 以及与总线相连的至少一个存储器 503。

其中,处理器 502 通过总线 501,调用存储器 503 中存储的代码以用于在预设界面获取用户对触摸屏进行触控操作时的指纹信息,所述预设界面为预设信息的访问界面;判断所述指纹信息与预设指纹信息是否匹配;若所述指纹信息与所述预设指纹信息不匹配,则对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作。20

其中,预设信息指存储于终端中特定位置、由终端系统或者用户设定的、需要对其访问进行限制的特定信息,包括特定数据或特定应用等,如可以为手机相册、手机短信、QQ、微信等特定应用,也可以为手机相册应用里面的某一个相册、手机短信应用里面的短信等,还可以为存储在终端中的某一特定文件等;25

预设界面是指终端提供给用户访问预设信息的用户界面,如手机相册、手机短信等的访问界面,或手机进入相册后,查看某一指定相册的界面;预设界30

面还可以为屏幕的解锁界面等。

其中，终端指手机、平板电脑等智能终端，该终端具有能够进行指纹识别的触摸屏，该触摸屏能够感应用户的按压、滑动等操作，并能对与触摸屏接触的指纹进行识别。终端可以在预设界面通过具有指纹识别的触摸屏的任何位置

5 获取用户触控触摸屏时的指纹信息。

可选地，在本发明的一些可能的实施方式中，该预设界面根据用户的需要，将预设信息的访问界面设置为预设界面，从而用户在通过该预设界面进入该应用或者数据时，终端实时通过触摸屏对用户触控触摸屏时的指纹信息进行识别。

10 可选地，在预设界面获取用户触控触摸屏时的指纹信息时，可以通过识别用户在预设界面的按压操作。

可选地，在预设界面获取用户触控触摸屏时的指纹信息时，可以通过识别用户在预设界面的滑动操作。

其中，所述指纹信息指用户在预设界面读取到的指纹信息，可通过指纹传

15 感器感应用户在触摸屏上的按压、滑动等操作进行指纹识别。

其中，预设指纹信息指预先存储在终端中的指纹信息，用于与通过触摸屏获取收到的用户触控触摸屏时的指纹信息进行对比。

可选地，在本发明的一些可能的实施方式中，该预设指纹信息可以为一个，从而所接收到的用户录入的指纹信息只需要与这一个预设指纹信息进行对比，

20 判断用户触控触摸屏时的指纹信息是否与该预设指纹信息匹配。

可选地，在本发明的另一些可能的实施方式中，该预设指纹信息也可以为多个，从而所接收到的用户触控触摸屏时的指纹信息需要与多个预设指纹信息进行对比，用于判断用户触控触摸屏时的指纹信息是否与预设指纹信息匹配。

可选地，在本发明的一些可能的实施方式中，进入不同应用的预设指纹信

25 息可以不一样，也可以一样。

可选地，在本发明的另一些可能的实施方式中，所述预设指纹信息可以由有权限用户进行更改。

其中，屏蔽所述触控操作指在获取到的用户触控触摸屏时的指纹信息与预设指纹信息不匹配时，暂时使用户在该预设界面的触控操作失效，从而使得在

30 获取到非预设指纹信息时不再在预设界面继续获取用户触控触摸屏的指纹信

息,减少系统开销,当下次再进入该预设界面时,触控操作自动重新恢复有效,。

可选地,在本发明的一些可能的实施方式中,当预设指纹信息为一个时,判断用户触控触摸屏时的指纹信息是否与该一个预设指纹信息是否匹配,若用户触控触摸屏时的指纹信息与该预设指纹信息不匹配,则对所述预设信息
5 进行加密和/或隐藏,或屏蔽所述触控操作。

可选地,在本发明的另一些可能的实施方式中,当预设指纹信息为多个时,判断用户触控触摸屏时的指纹信息与其中任一个预设指纹信息是否匹配,若用户触控触摸屏时的指纹信息与其中任一个预设指纹信息匹配,则对所述预设信息
10 进行加密和/或隐藏,或屏蔽所述触控操作。

可选地,在本发明的一些可能的实施方式中,采用一般的对预设信息设定密码的方式对预设信息进行加密。

可选地,在本发明的一些可能的实施方式中,所述预设信息包括特定数据或特定应用,处理器 502 用于:

若所述预设信息为特定数据,则对所述预设信息进行加密和/或隐藏,或
15 屏蔽所述触控操作;

若所述预设信息为特定应用,则对所述预设信息进行加密和/或终止访问所述预设信息,或屏蔽所述触控操作。

可选地,在本发明的一些可能的实施方式中,对所述特定数据进行加密时,可以用密码对特定数据进行加密。

可选地,在本发明的另一些可能的实施方式中,对所述特定数据进行加密时,也可以利用一定的编码方式对数据进行加密。

可选地,在本发明的一些可能的实施方式中,处理器 502 所述在预设界面获取用户对触摸屏进行触控操作时的指纹信息,包括:

若在所述预设界面上获取用户对触摸屏进行的触控操作为按压操作时,则
25 当按压操作发生时,获取指纹信息;

若在所述预设界面上获取用户对触摸屏进行的触控操作为滑动操作时,则在滑动操作起始时刻获取指纹信息。

可选地,在本发明的一些可能的实施方式中,不管用户在预设界面上进行的是何种操作,当接收到用户的对预设界面的触压并且在触压之前或者之后有
30 离开预设界面的操作时,则对指纹信息进行识别。

可选地，在本发明的一些可能的实施方式中，终端通过在屏幕下安装指纹传感器，从而终端可以在用户触摸预设界面屏幕上的任何位置读取用户触控触摸屏时的指纹信息，方便用户操作。

5 可选地，在本发明的另一些可能的实施方式中，终端也可以在预设界面的特定位置读取用户触控触摸屏时的指纹信息。

可选地，在本发明的一些可能的实施方式中，处理器 502 还用于：
在所述预设信息的生成过程中，不对所述预设信息做任何加密处理。

可选地，在本发明的一些可能的实施方式中，处理器 502 还用于：
若所述指纹信息与所述预设指纹信息匹配，则显示所述预设信息。

10 可选地，在本发明的一些可能的实施方式中，处理器 502 还用于：
当所述预设信息为特定数据时，若所述指纹信息与所述预设指纹信息匹配，则显示所述预设信息。

可选地，在本发明的一些可能的实施方式中，处理器 502 还用于：
当所述预设信息为特定应用时，若所述指纹信息与所述预设指纹信息匹
15 配，则访问所述预设信息。

可选地，在本发明的一些可能的实施方式中，所述若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作后，处理器 502 还用于：

若再获取到所述预设指纹信息，对所述预设信息进行解密和/或显示。

20 可选地，在本发明的另一些可能的实施方式中，所述若所述预设信息为特定数据时，若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作后，处理器 502 还用于：

若再获取到所述预设指纹，对所述预设信息进行解密和/或显示。可选地，在本发明的另一些可能的实施方式中，当所述预设信息为特定应用时，所述若
25 所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作后，处理器 502 还用于：

若再获取到所述预设指纹信息，对所述预设信息进行解密和/或允许访问所述预设信息。

可选地，在本发明的一些可能的实施方式中，所述方法还包括：
30 在所述预设信息的生成过程中，不对所述预设信息做任何加密处理。

可以理解的是,本实施例的数据加密装置 500 的各功能模块的功能可根据上述方法实施例中的方法具体实现,其具体实现过程可以参照上述方法实施例的相关描述,此处不再赘述。

可以看出,本实施例的方案中,数据加密装置 500 在预设界面获取用户对触摸屏进行触控操作时的指纹信息,所述预设界面指预设信息的访问界面;数据加密装置 500 判断所述指纹信息与预设指纹信息是否匹配;若所述指纹信息与所述预设指纹信息不匹配,则数据加密装置 500 对所述预设信息进行加密和/或隐藏,或屏蔽所述触控操作,使触控操作暂时失效。从而当只在预设界面上获取到的用户对触摸屏进行触控操作时的指纹信息与预设指纹信息不匹配时,只对预设信息进行加密,计算量小,系统开销小,效率高。本发明实施例还提供一种计算机存储介质,其中,该计算机存储介质可存储有程序,该程序执行时包括上述方法实施例中记载的任何音频播放应用的操作方法的部分或全部步骤。

需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明并不受所描述的动作顺序的限制,因为依据本发明,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本发明所必须的。

在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中未详述的部分,可以参见其他实施例的相关描述。

在本申请所提供的几个实施例中,应该理解到,所揭露的装置,可通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部

单元来实现本实施例方案的目的。

另外，在本发明的各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可为个人计算机、服务器或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，以上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

1、一种数据加密方法，其特征在于，所述方法包括：

5 在预设界面获取用户对触摸屏进行触控操作时的指纹信息，所述预设界面为预设信息的访问界面；

判断所述指纹信息与预设指纹信息是否匹配；

若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

2、如权利要求 1 所述的方法，其特征在于，所述预设信息包括特定数据
10 或特定应用，所述对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作，包括：

若所述预设信息为特定数据，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作；

15 若所述预设信息为特定应用，则对所述预设信息进行加密和/或终止访问所述预设信息，或屏蔽所述触控操作。

3、如权利要求 1 所述的方法，其特征在于，所述在预设界面获取用户对触摸屏进行触控操作时的指纹信息，包括：

若在上述预设界面上获取用户对触摸屏进行的触控操作为按压操作时，则当按压操作发生时，获取指纹信息；

20 若在上述预设界面上获取用户对触摸屏进行的触控操作为滑动操作时，则在滑动操作起始时刻获取指纹信息。

4、如权利要求 1 至 3 任一项所述的方法，其特征在于，所述方法还包括：若所述指纹信息与所述预设指纹信息匹配，则显示所述预设信息。

5、如权利要求 1 所述的方法，其特征在于，所述若所述指纹信息与所述
25 预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作后，所述方法还包括：

若再获取到所述预设指纹信息，则对所述预设信息进行解密。

6、一种数据加密装置，其特征在于，所述装置包括：

30 读取模块，用于在预设界面获取用户对触摸屏进行触控操作时的指纹信息，所述预设界面为预设信息的访问界面；

判断模块，用于判断所述指纹信息与预设指纹信息是否匹配；

加密模块，用于若所述指纹信息与所述预设指纹信息不匹配，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作。

7、如权利要求6所述的装置，其特征在于，所述预设信息包括特定数据
5 或特定应用，所述加密模块包括：

第一加密单元，用于若所述预设信息为特定数据，则对所述预设信息进行加密和/或隐藏，或屏蔽所述触控操作；

第二加密单元，用于若所述预设信息为特定应用，则对所述预设信息进行加密和/或终止访问所述预设信息，或屏蔽所述触控操作。

10 8、如权利要求6所述的装置，其特征在于，所述读取模块包括：

第一读取单元，用于若在所述预设界面上获取用户对触摸屏进行的触控操作作为按压操作时，则当按压操作发生时，获取指纹信息；

第二读取单元，用于若在所述预设界面上获取用户对触摸屏进行的触控操作作为滑动操作时，则在滑动操作起始时刻获取指纹信息。

15 9、如权利要求6至8任一项所述的装置，其特征在于，所述装置还包括：

显示模块，用于若所述指纹信息与所述预设指纹信息匹配，则显示所述预设信息。

10、如权利要求6所述的装置，其特征在于，所述装置还包括：

20 解密模块，用于若再获取到所述预设指纹信息，则对所述预设信息进行解密。

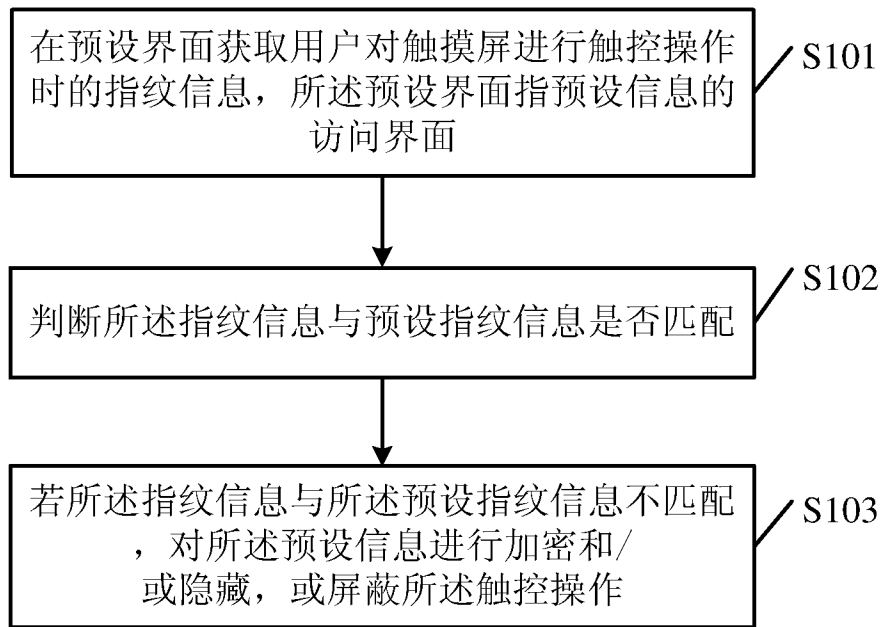


图 1

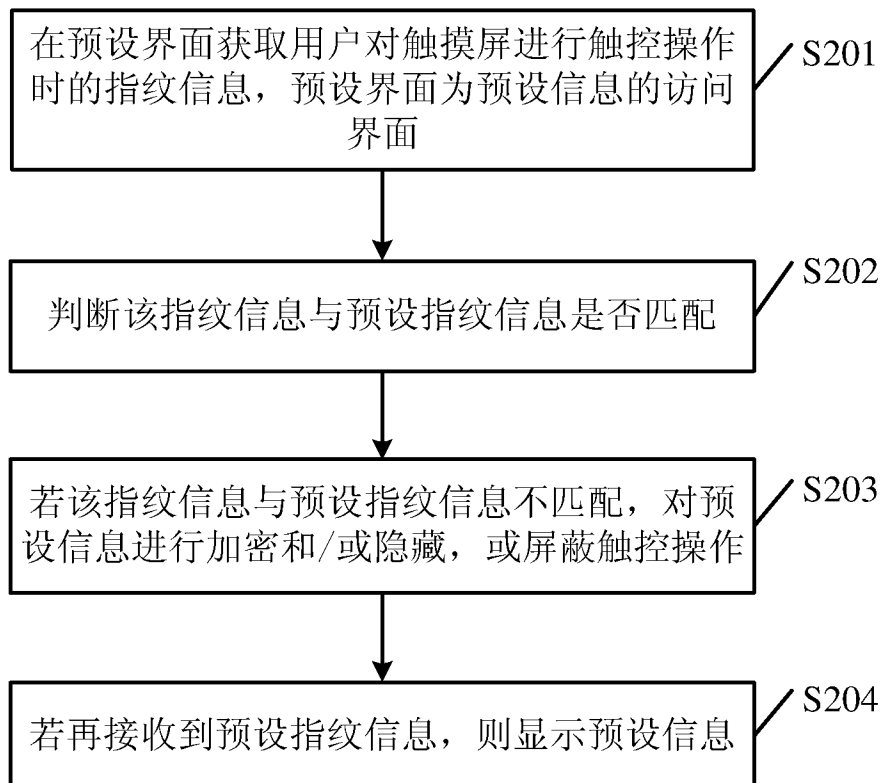


图 2

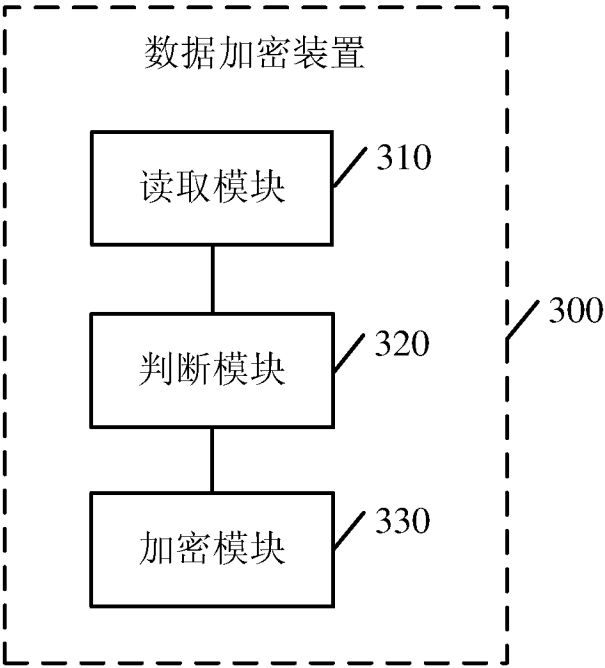


图 3

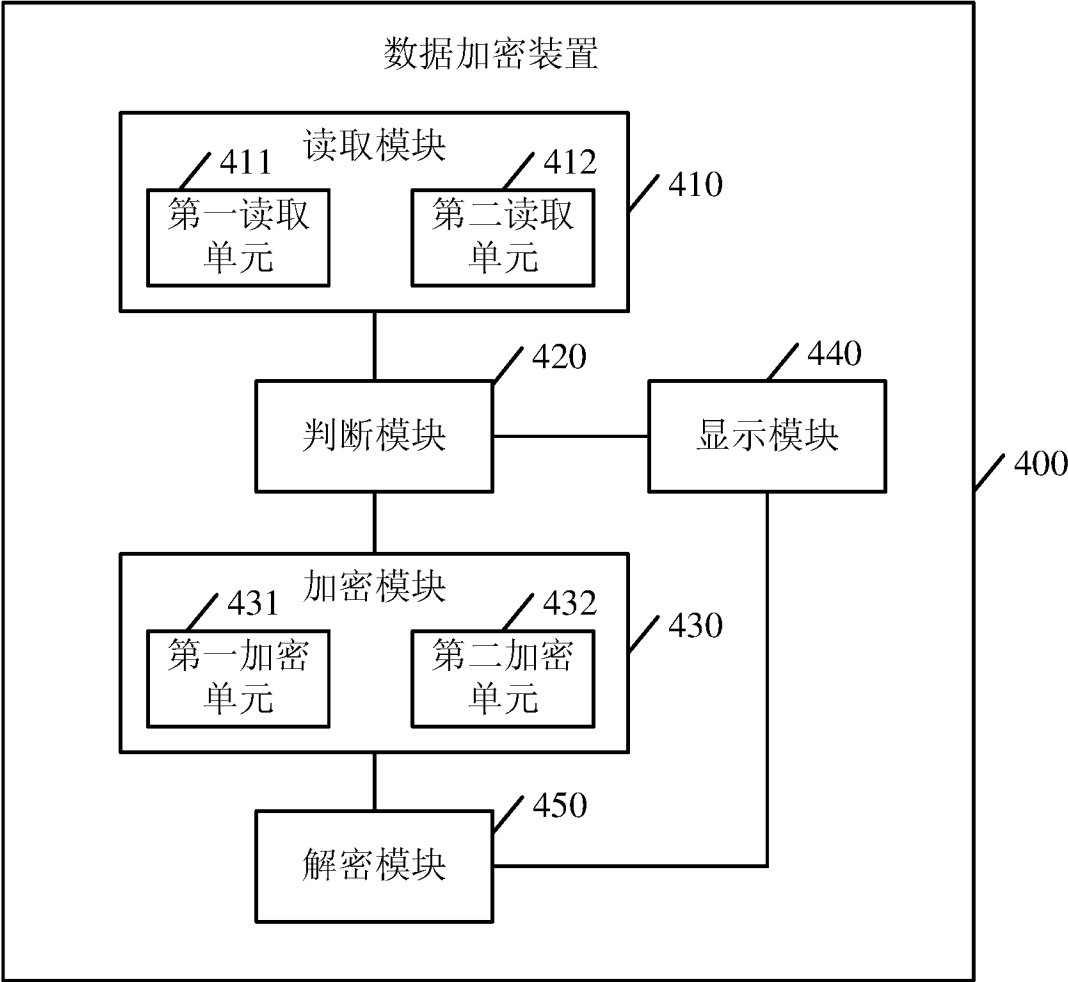


图 4

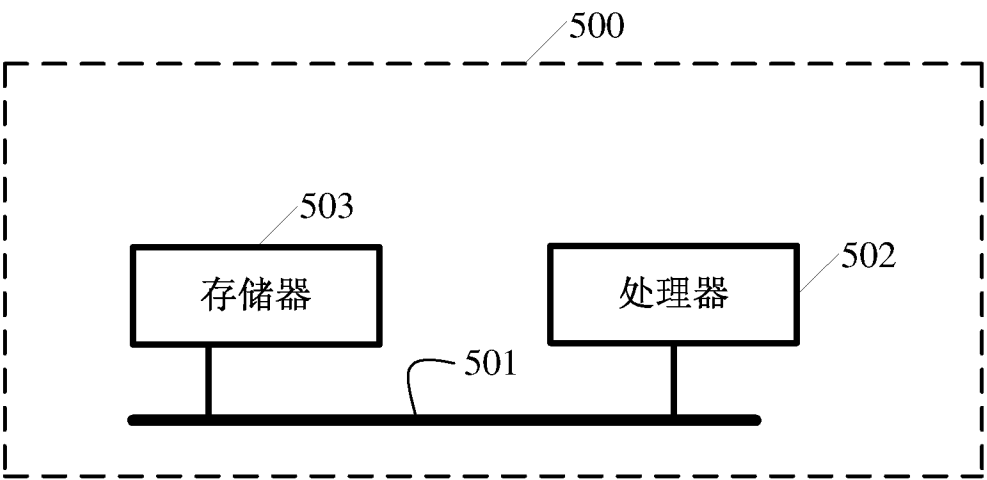


图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/082991

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; H04M; G06K

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

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

CNABS, CPRSABS, CNTXT, DWPI, SIPOABS, CNKI: data, application, software, fingerprint, biometric, face, iris, sound, not match, discrepant+, encrypt+, hid+, shield, forbid+, prohibit, touch+, control+, operat+, access+, manipulat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103294963 A (FUTAIHUA IND SHENZHEN CO., LTD. et al.) 11 September 2013 (11.09.2013) claims 1, 5, 6, and 10	1, 3-6, 8-10
Y	CN 103294963 A (HON HAI PRECISION INDUSTRY CO., LTD. et al.) 11 September 2013 (11.09.2013) claims 1, 5, 6, and 10	2, 7
X	CN 103886239 A (SHENZHEN OPPO COMMUNICAITONS SOFTWARE CORP., LTD.) 25 June 2014 (25.06.2014) description, paragraphs [0020] to [0047] and [0068] to [0084]	1, 3-6, 8-10
Y	CN 103886239 A (SHENZHEN OPPO COMMUNICAITONS SOFTWARE CORP., LTD)	2, 7

☒ 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 14 January 2016	Date of mailing of the international search report 06 February 2016
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimengqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer ZHAO, Chengjuan Telephone No. (86-10) 62411335

INTERNATIONAL SEARCH REPORTInternational application No.
PCT/CN2015/082991

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	25 June 2014 (25.06.2014) description, paragraphs [0020] to [0047] and [0068] to [0084]	
X	JP 2013140440 A (SHARP KK) 18 July 2013 (18.07.2013) claims 1-25	1-10
Y	CN 103366107 A (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD) 23 October 2013 (23.10.2013) claims 1-7	1-10
Y	CN 104573440 A (BAIDU ONLINE NETWORK TECHNOLOGY BEIJING CO., LTD.) 29 April 2015 (29.04.2015) claim 1	1-10
Y	CN 103440446 A (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.) 11 December 2013 (11.12.2013) description, paragraph [0006]	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/082991

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103294963 A	11 September 2013	US 2013223700 A1	29 August 2013
		TW 201335859 A	01 September 2013
CN 103886239 A	25 June 2014	None	
JP 2013140440 A	18 July 2013	None	
CN 103366107 A	23 October 2013	None	
CN 104573440 A	29 April 2015	None	
CN 103440446 A	11 December 2013	None	

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; H04M; G06K 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNABS, CPRSABS, CNTXT, DWPI, SIPOABS, CNKI: 数据, 应用, 程序, 指纹, 生物特征, 脸相, 人脸, 头像, 虹膜, 掌纹, 声音, 不匹配, 加密, 隐藏, 屏蔽, 禁止, 不允许, 终止, 触控, 操作, 访问; data, application, software, fingerprint, biometric, face, iris, sound, not match, discrepant+, encrypt+, hid+, shield, forbid+, prohibit, touch+, control+, operat+, access+, manipul+		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 103294963 A (富泰华工业深圳有限公司等) 2013年 9月 11日 (2013 - 09 - 11) 权利要求1、5、6、10	1、3-6、8-10
Y	CN 103294963 A (富泰华工业深圳有限公司等) 2013年 9月 11日 (2013 - 09 - 11) 权利要求1、5、6、10	2、7
X	CN 103886239 A (深圳市欧珀通信软件有限公司) 2014年 6月 25日 (2014 - 06 - 25) 说明书第[0020]-[0047]、[0068]-[0084]段	1、3-6、8-10
Y	CN 103886239 A (深圳市欧珀通信软件有限公司) 2014年 6月 25日 (2014 - 06 - 25) 说明书第[0020]-[0047]、[0068]-[0084]段	2、7
X	JP 2013140440 A (SHARP KK) 2013年 7月 18日 (2013 - 07 - 18) 权利要求1-25	1-10
Y	CN 103366107 A (广东欧珀移动通信有限公司) 2013年 10月 23日 (2013 - 10 - 23) 权利要求1-7	1-10
☒ 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 1月 14日		国际检索报告邮寄日期 2016年 2月 6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 赵承娟 电话号码 (86-10)62411335

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 104573440 A (百度在线网络技术北京有限公司) 2015年 4月 29日 (2015 - 04 - 29) 权利要求1	1-10
Y	CN 103440446 A (广东欧珀移动通信有限公司) 2013年 12月 11日 (2013 - 12 - 11) 说明书第[0006]段	1-10

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/082991

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	103294963	A	2013年 9月 11日	US	2013223700	A1	2013年 8月 29日
				TW	201335859	A	2013年 9月 1日
CN	103886239	A	2014年 6月 25日	无			
JP	2013140440	A	2013年 7月 18日	无			
CN	103366107	A	2013年 10月 23日	无			
CN	104573440	A	2015年 4月 29日	无			
CN	103440446	A	2013年 12月 11日	无			