(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 9 日 (09.02.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/020437 A1

(51) 国际专利分类号:
G06F 21/32 (2013.01)

(21) 国际申请号: PCT/CN2015/093526

(22) 国际申请日: 2015 年 10 月 31 日 (31.10.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510466838.4 2015 年 7 月 31 日 (31.07.2015) 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: **白波 (BAI, Bo)**; 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） (YOULINK 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) Title: INFORMATION ENCRYPTION METHOD AND TERMINAL DEVICE

(54) 发明名称 : 一种信息加密方法及终端设备

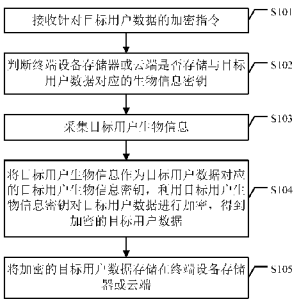

图 1

S101 Receive an encryption command for target user data

S102 Determine whether a biometrics information key corresponding to the target user data is stored on a terminal device storage or on a cloud terminal

S103 Acquire target user biometrics information

S104 Take said biometrics information as the target user biometrics information key corresponding to the target user data, and encrypt the target user data with the biometrics target user information key to obtain the encrypted target user data

S105 Store the encrypted target user data on the terminal device storage or on the cloud terminal

(57) **Abstract**: Disclosed in embodiments of the present invention are an information encryption method and a terminal device, the method comprising: receiving an encryption command for target user data (S101); determining whether a biometrics information key corresponding to the target user data is stored on a terminal device storage or on a cloud terminal (S102); if not, acquiring target user biometrics information (S103); taking said biometrics information as the target user biometrics information key corresponding to the target user data, and encrypting the target user data with the target user biometrics information key to obtain encrypted target user data (S104); and storing the encrypted target user data on the terminal device storage or on the cloud terminal (S105). By implementing the embodiments of the present invention, the security of the user data can be improved.

(57) **摘要**: 本发明实施例公开了一种信息加密方法及终端设备，该方法包括：接收针对目标用户数据的加密指令（S101）；判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥（S102）；若否，采集目标用户生物信息（S103）；将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据（S104）；将加密的目标用户数据存储在终端设备存储器或云端（S105）。实施本发明实施例，可以提高用户数据的安全性。

WO 2017/020437 A1

说 明 书

一种信息加密方法及终端设备

技术领域

本发明涉及通信技术领域，具体涉及一种信息加密方法及终端设备。

背景技术

随着通信技术的快速发展，终端设备中用户数据的安全性引起了广泛关注，当前普遍采用的方法是通过设置字符密码对用户数据进行加密。由于终端设备中的用户数据繁多，使用字符密码对用户数据进行加密时，用户为了使用方便，一般会对所有的用户数据均设置同一个密码，会导致用户数据的安全性较低。

发明内容

本发明实施例提供一种信息加密方法及终端设备，可以提高用户数据的安全性。

本发明实施例第一方面，提供了一种信息加密方法，包括:

接收针对目标用户数据的加密指令;

判断终端设备存储器或云端是否存储与所述目标用户数据对应的生物信息密钥;

若否，采集目标用户生物信息;

将所述目标用户生物信息作为所述目标用户数据对应的目标用户生物信息密钥，利用所述目标用户生物信息密钥对所述目标用户数据进行加密，得到加密的目标用户数据;

将所述加密的目标用户数据存储在所述终端设备存储器或所述云端。

在本发明实施例第一方面的第一种可能的实现方式中，所述将所述加密的目标用户数据存储在所述终端设备存储器或所述云端之后，所述方法还包括:

接收针对所述加密的目标用户数据的访问指令;

输出提示信息，所述提示信息用于提示输入解密密钥;

当所述解密密钥输入后，判断所述解密密钥与所述目标用户数据对应的所述目标用户生物信息密钥是否匹配;

若匹配，解密所述加密的目标用户数据，获取所述目标用户数据。

结合本发明实施例第一方面，在本发明实施例第一方面的第二种可能的实现方式中，所述采集目标用户生物信息包括:

采集至少两个用户生物信息;

当所述至少两个用户生物信息相互匹配时，确认目标用户生物信息采集成功。

结合本发明实施例第一方面的第二种可能的实现方式，在本发明实施例第一方面的第三种可能的实现方式中，所述确认目标用户生物信息采集成功，包括:

将所述至少两个用户生物信息进行合成，得到目标用户生物信息。

结合本发明实施例第一方面的第二种可能的实现方式，在本发明实施例第一方面的第四种可能的实现方式中，所述确认目标用户生物信息采集成功，包括:

从所述至少两个用户生物信息中选择任一个作为目标用户生物信息。

本发明实施例第二方面，提供了一种终端设备，包括:

第一接收单元，用于接收针对目标用户数据的加密指令;

第一判断单元，用于判断终端设备存储器或云端是否存储与所述目标用户数据对应的生物信息密钥;

采集单元，用于当所述第一判断单元判断结果为否时，采集目标用户生物信息;

加密单元，用于将所述目标用户生物信息作为所述目标用户数据对应的目标用户生物信息密钥，利用所述目标用户生物信息密钥对所述目标用户数据进行加密，得到加密的目标用户数据;

存储单元，用于将所述加密的目标用户数据存储在所述终端设备存储器或所述云端。

在本发明实施例第二方面的第一种可能的实现方式中，所述终端设备还包括:

第二接收单元，用于接收针对所述加密的目标用户数据的访问指令;

输出单元，用于输出提示信息，所述提示信息用于提示输入解密密钥;

第二判断单元，用于当所述解密密钥输入后，判断所述解密密钥与所述目

标用户数据对应的所述目标用户生物信息密钥是否匹配;

解密单元，用于当所述第二判断单元判断结果为是时，解密所述加密的目标用户数据，获取所述目标用户数据。

结合本发明实施例第二方面，在本发明实施例第二方面的第二种可能的实现方式中，所述采集单元包括:

采集子单元，用于采集至少两个用户生物信息;

确认子单元，用于当所述至少两个用户生物信息相互匹配时，确认目标用户生物信息采集成功。

结合本发明实施例第二方面的第二种可能的实现方式，在本发明实施例第二方面的第三种可能的实现方式中，所述确认子单元确认目标用户生物信息采集成功的方式具体为:

所述确认单元将所述至少两个用户生物信息进行合成，得到目标用户生物信息。

结合本发明实施例第二方面的第二种可能的实现方式，在本发明实施例第二方面的第四种可能的实现方式中，所述确认子单元确认目标用户生物信息采集成功的方式具体为:

所述确认单元从所述至少两个用户生物信息中选择任一个作为目标用户生物信息。

本发明实施例中，终端设备接收针对目标用户数据的加密指令；判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥；若否，采集目标用户生物信息；将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据；将加密的目标用户数据存储在终端设备存储器或云端。与现有技术中使用字符密码相比，本发明实施例中采用生物信息密钥对用户数据进行加密，由于生物信息的唯一性与不可复制性，用户数据的安全性较高，与现有技术相比，提高了用户数据的安全性。

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。

图1是本发明实施例公开的一种信息加密方法的流程图；

图2是本发明实施例公开的另一种信息加密方法的流程图；

图3是本发明实施例公开的另一种信息加密方法的流程图；

图4是本发明实施例公开的一种终端设备的结构示意图；

图5是本发明实施例公开的另一种终端设备的结构示意图；

图6是本发明实施例公开的另一种终端设备的结构示意图。

具体实施方式

下面将结合本发明实施方式中的附图，对本发明实施方式中的技术方案进行清楚、完整地描述。显然，所描述的实施方式是本发明的一部分实施方式，而不是全部实施方式。基于本发明中的实施方式，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施方式，都应属于本发明保护的范围。

本发明实施例提供一种信息加密方法及终端设备，可以提高用户数据的安全性。以下分别进行详细说明。

本发明实施例中描述的终端设备可包括：手机、平板电脑或者随身听等，上述终端设备仅是举例，而非穷举，包含但不限于上述终端设备。

请参阅图1，图1是本发明实施例公开的一种信息加密方法的流程图。如图1所示，本实施例中所描述的信息加密方法，包括步骤：

S101，接收针对目标用户数据的加密指令。

本发明实施例中，当需要对目标用户数据进行加密时，用户针对目标用户数据输入加密指令，终端设备接收用户输入的针对目标用户数据的加密指令。目标用户数据可以为图片、录音、文档、视频、音乐等用户私密数据。

在步骤S101之前，还可以包括如下步骤：

当用户数据生成时，判断信息加密功能是否开启；

若信息加密功能未开启，输出第一提示信息，第一提示信息用于提示是否开启信息加密功能；

当接收到开启信息加密功能指令后，开启信息加密功能。

本发明实施例中，用户数据可以由终端设备中的应用生成，例如，用户数据为图片时，用户数据由拍摄应用生成；用户数据为录音时，用户数据由录音应用生成。信息加密功能是使用生物信息对用户数据进行加密的功能，当信息加密功能开启时，可以利用生物信息对用户数据进行加密，生物信息包括但不限于：指纹、虹膜、声纹、人脸、视网膜等信息。

S102，判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥。

本发明实施例中，若目标用户数据已进行信息加密，则目标用户数据有一个与之对应的生物信息密钥，判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥是为了判断目标用户数据是否加密。若终端设备存储器或云端存储与目标用户数据对应的生物信息密钥，则表明目标用户数据已加密，终端设备会输出通知消息，该通知消息用于通知用户该目标用户数据已加密，是否重新加密，若用户选择重新加密，则先输入目标用户数据对应的原始生物信息密钥，再输入目标用户数据的新生物信息密钥，若用户选择不重新加密，则结束；若终端设备存储器或云端未存储与目标用户数据对应的生物信息密钥，则执行步骤S103。

S103，采集目标用户生物信息。

本发明实施例中，若终端设备存储器或云端未存储与目标用户数据对应的生物信息密钥，则采集目标用户生物信息，终端设备可以采集用户在终端设备上输入的目标用户生物信息，举例来说，若目标用户生物信息为目标用户指纹信息，则开启指纹识别功能，在终端设备上的指纹识别区域采集目标用户的指纹信息；若目标用户生物信息为目标用户虹膜信息，则开启终端设备的摄像头，获取目标用户的眼部图像信息；若目标用户生物信息为目标用户声纹信息，则开启终端设备的麦克风，采集目标用户的声音信息。

S104，将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据。

本发明实施例中，用户生物信息密钥与传统的字符串密钥不同，用户生物信息密钥为目标用户生物信息，例如指纹信息、虹膜信息、人脸图像信息等。采集目标用户生物信息后，将目标用户生物信息作为目标用户数据对应的目标

用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据。

S105，将加密的目标用户数据存储在终端设备存储器或云端。

本发明实施例中，当目标用户数据加密成功后，加密的目标用户数据可以存储在终端设备存储器或云端，由于采用目标用户生物信息对目标用户数据进行加密，只有目标用户本人输入目标用户生物信息才能对加密的目标用户数据进行解密，大大的提供了目标用户数据的安全性。

本发明实施例中，终端设备接收针对目标用户数据的加密指令；判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥；若否，采集目标用户生物信息；将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据；将加密的目标用户数据存储在终端设备存储器或云端。与现有技术中使用字符密码相比，本发明实施例中采用生物信息密钥对用户数据进行加密，由于生物信息的唯一性与不可复制性，用户数据的安全性较高，与现有技术相比，提高了用户数据的安全性。

请参阅图2，图2是本发明实施例公开的另一种信息加密方法的流程图。如图2所示，本实施例中所描述的信息加密方法，包括步骤：

S201，接收针对目标用户数据的加密指令。

S202，判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥。

S203，采集目标用户生物信息。

S204，将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据。

S205，将加密的目标用户数据存储在终端设备存储器或云端。

S206，接收针对加密的目标用户数据的访问指令。

本发明实施例中，当目标用户数据加密后，若需要对加密的目标用户数据进行解密，则用户针对加密的目标用户数据输入访问指令，终端设备接收用户输入的针对加密的目标用户数据的访问指令。加密的目标用户数据可以为加密的图片、录音、文档、视频、音乐等目标用户数据。

S207，输出提示信息，提示信息用于提示输入解密密钥。

本发明实施例中，当接收针对加密的目标用户数据的访问指令之后，输出用于提示输入解密密钥的提示信息，输出用于提示输入解密密钥的提示信息可以是输出用于提示用户输入解密密钥的提示信息。解密密钥为与目标用户数据对应的目标用户生物信息，根据目标用户生物信息的类别，输入解密密钥的方式有区别，例如，当目标用户生物信息为指纹信息时，目标用户可以在终端设备上的指纹识别区域输入目标用户的指纹信息；当目标用户生物信息为目标用户虹膜信息时，则终端设备开启终端设备的摄像头，目标用户将目标用户的眼部区域对准终端设备的摄像头，以使终端设备的摄像头获取目标用户的眼部图像信息；当目标用户生物信息为目标用户声纹信息时，则终端设备开启终端设备的麦克风，目标用户通过终端设备的麦克风输入目标用户的声音信息。

S208，当解密密钥输入后，判断解密密钥与目标用户数据对应的目标用户生物信息密钥是否匹配。

本发明实施例中，当用户输入解密密钥后，判断解密密钥与目标用户数据对应的目标用户生物信息密钥是否匹配。举例来说，若解密密钥为指纹信息，当指纹信息输入后，判断输入的指纹信息与目标用户数据对应的目标用户指纹信息是否匹配，具体而言，可以通过判断输入的指纹图像与目标用户数据对应的目标用户指纹图像是否匹配，也可以通过判断输入的指纹信息中的指纹特征与目标用户数据对应的目标用户指纹特征是否匹配，目标用户指纹特征可以包括指纹的纹路特征、指纹的核心点位置、指纹的三角点位置等；若解密密钥为虹膜信息，当虹膜信息输入后，判断输入的虹膜信息与目标用户数据对应的目标用户虹膜信息是否匹配，具体而言，可以通过判断输入的虹膜图像与目标用户数据对应的目标用户虹膜图像是否匹配；若解密密钥为声纹信息，当声纹信息输入后，判断输入的声纹信息与目标用户数据对应的目标用户声纹信息是否匹配，具体而言，可以通过判断输入的声纹特征与目标用户数据对应的目标用户声纹特征是否匹配，目标用户声纹特征可以包括共振峰的频率值、共振峰的走向、声纹波形等。

S209，若匹配，解密加密的目标用户数据，获取目标用户数据。

本发明实施例中，若解密密钥与目标用户数据对应的目标用户生物信息密钥匹配，则解密加密的目标用户数据，获取目标用户数据。例如，若解密密钥

为指纹信息，当输入的指纹信息与目标用户数据对应的目标用户指纹信息匹配时，则解密加密的目标用户数据，获取目标用户数据，具体而言，当输入的指纹图像与目标用户数据对应的目标用户指纹图像匹配时，或者输入的指纹信息中的指纹特征与目标用户数据对应的目标用户指纹特征匹配时，解密加密的目标用户数据，获取目标用户数据；若解密密钥为虹膜信息，当输入的虹膜信息与目标用户数据对应的目标用户虹膜信息匹配时，则解密加密的目标用户数据，获取目标用户数据，具体而言，当输入的虹膜图像与目标用户数据对应的目标用户虹膜图像匹配时，解密加密的目标用户数据，获取目标用户数据；若解密密钥为声纹信息，当输入的声纹信息与目标用户数据对应的目标用户声纹信息匹配时，则解密加密的目标用户数据，获取目标用户数据，具体而言，当输入的声纹特征与目标用户数据对应的目标用户声纹特征匹配时，则解密加密的目标用户数据，获取目标用户数据。

本发明实施例中的步骤S201~步骤S205可以参阅图1所示的步骤S101~步骤S105，本发明实施例不再赘述。

本发明实施例中，终端设备接收针对目标用户数据的加密指令；判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥；若否，采集目标用户生物信息；将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据；将加密的目标用户数据存储在终端设备存储器或云端；接收针对加密的目标用户数据的访问指令；输出提示信息，提示信息用于提示输入解密密钥；当解密密钥输入后，判断解密密钥与目标用户数据对应的目标用户生物信息密钥是否匹配；若匹配，解密加密的目标用户数据，获取目标用户数据。实施本发明实施例，可以提高用户数据的安全性。

请参阅图3，图3是本发明实施例公开的另一种信息加密方法的流程图。如图3所示，本实施例中所描述的信息加密方法，包括步骤：

S301，接收针对目标用户数据的加密指令。

S302，判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥。

S303，采集至少两个用户生物信息。

本发明实施例中，为了提高采集的用户生物信息的准确性，防止由于用户

误操作采集的用户生物信息，在采集目标用户生物信息时，首先采集至少两个用户生物信息。

S304，当至少两个用户生物信息相互匹配时，确认目标用户生物信息采集成功。

本发明实施例中，当采集的至少两个用户生物信息相互匹配时，则表明采集的用户生物信息为有效信息，则确认目标用户生物信息采集成功。

在一些可行的实施方式中，步骤S304中确认目标用户生物信息采集成功可以包括:

将至少两个用户生物信息进行合成，得到目标用户生物信息。

本发明实施例中，当采集的至少两个用户生物信息相互匹配时，将至少两个用户生物信息进行合成，得到目标用户生物信息，例如，若用户生物信息为用户指纹信息，可以将至少两个用户指纹信息进行合成，得到目标用户指纹信息。

在一些可行的实施方式中，步骤S304中确认目标用户生物信息采集成功可以包括:

从至少两个用户生物信息中选择任一个作为目标用户生物信息。

本发明实施例中，当采集的至少两个用户生物信息相互匹配时，从至少两个用户生物信息中选择任一个作为目标用户生物信息，例如，若用户生物信息为用户指纹信息，可以从至少两个用户指纹信息中选择任一个作为目标用户指纹信息。

S305，将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据。

S306，将加密的目标用户数据存储在终端设备存储器或云端。

本发明实施例中的步骤S301~步骤S302可以参阅图1所示的步骤S101~步骤S102，步骤S305~步骤S306可以参阅图1所示的步骤S104~步骤S105，本发明实施例不再赘述。

本发明实施例中，接收针对目标用户数据的加密指令；判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥；采集至少两个用户生物信息；当至少两个用户生物信息相互匹配时，确认目标用户生物信息采集成

功；将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据；将加密的目标用户数据存储在终端设备存储器或云端。实施本发明实施例，可以提高采集的用户生物信息的准确性，提高用户数据的安全性。

请参阅图4，图4是本发明实施例公开的一种终端设备的结构示意图，如图4所示，本发明实施例所描述的终端设备，包括：第一接收单元401、第一判断单元402、采集单元403、加密单元404和存储单元405，其中：

第一接收单元401，用于接收针对目标用户数据的加密指令。

本发明实施例中，当需要对目标用户数据进行加密时，用户针对目标用户数据输入加密指令，第一接收单元401接收用户输入的针对目标用户数据的加密指令。目标用户数据可以为图片、录音、文档、视频、音乐等用户私密数据。

第一判断单元402，用于判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥。

本发明实施例中，若目标用户数据已进行信息加密，则目标用户数据有一个与之对应的生物信息密钥，第一判断单元402判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥是为了判断目标用户数据是否加密。若终端设备存储器或云端存储与目标用户数据对应的生物信息密钥，则表明目标用户数据已加密，终端设备会输出通知消息，该通知消息用于通知用户该目标用户数据已加密，是否重新加密，若用户选择重新加密，则先输入目标用户数据对应的原始生物信息密钥，再输入目标用户数据的新生物信息密钥，若用户选择不重新加密，则结束；若终端设备存储器或云端未存储与目标用户数据对应的生物信息密钥，则触发采集单元403采集目标用户生物信息。

采集单元403，用于当第一判断单元402判断结果为否时，采集目标用户生物信息。

本发明实施例中，若终端设备存储器或云端未存储与目标用户数据对应的生物信息密钥，采集单元403则采集目标用户生物信息，采集单元403可以采集用户在终端设备上输入的目标用户生物信息，举例来说，若目标用户生物信息为目标用户指纹信息，则开启指纹识别功能，采集单元403在终端设备上的指纹识别区域采集目标用户的指纹信息；若目标用户生物信息为目标用户虹膜信息，则开启终端设备的摄像头，采集单元403采集目标用户的眼部图像信息；若目标

用户生物信息为目标用户声纹信息，则开启终端设备的麦克风，采集单元403采集目标用户的声音信息。

可选的，如图5所示，图5是本发明实施例公开的另一种终端设备的结构示意图，图5中的采集单元403包括采集子单元4031和确认子单元4032，其中：

采集子单元4031，用于采集至少两个用户生物信息。

本发明实施例中，为了提高采集的用户生物信息的准确性，防止由于用户误操作采集的用户生物信息，采集子单元4031在采集目标用户生物信息时，首先采集至少两个用户生物信息。

确认子单元4032，用于当至少两个用户生物信息相互匹配时，确认目标用户生物信息采集成功。

本发明实施例中，当采集的至少两个用户生物信息相互匹配时，则表明采集的用户生物信息为有效信息，确认子单元4032则确认目标用户生物信息采集成功。

可选的，确认子单元4032确认目标用户生物信息采集成功的方式具体为：

确认子单元4032将至少两个用户生物信息进行合成，得到目标用户生物信息。

本发明实施例中，当采集的至少两个用户生物信息相互匹配时，确认子单元4032将至少两个用户生物信息进行合成，得到目标用户生物信息，例如，若用户生物信息为用户指纹信息，可以将至少两个用户指纹信息进行合成，得到目标用户指纹信息。

可选的，确认子单元4032确认目标用户生物信息采集成功的方式具体为：

确认子单元4032从至少两个用户生物信息中选择任一个作为目标用户生物信息。

本发明实施例中，当采集的至少两个用户生物信息相互匹配时，确认子单元4032从至少两个用户生物信息中选择任一个作为目标用户生物信息，例如，若用户生物信息为用户指纹信息，可以从至少两个用户指纹信息中选择任一个作为目标用户指纹信息。

加密单元404，用于将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据。

本发明实施例中，用户生物信息密钥与传统的字符串密钥不同，用户生物信息密钥为目标用户生物信息，例如指纹信息、虹膜信息、人脸图像信息等。采集单元403采集目标用户生物信息后，加密单元404将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据。

存储单元405，用于将加密的目标用户数据存储在终端设备存储器或云端。

本发明实施例中，当目标用户数据加密成功后，存储单元405可以将加密的目标用户数据存储在终端设备存储器或云端，由于采用目标用户生物信息对目标用户数据进行加密，只有目标用户本人输入目标用户生物信息才能对加密的目标用户数据进行解密，大大的提供了目标用户数据的安全性。

本发明实施例中，第一接收单元401接收针对目标用户数据的加密指令；第一判断单元402判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥；若否，采集单元403采集目标用户生物信息；加密单元404将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，加密单元404利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据；存储单元405将加密的目标用户数据存储在终端设备存储器或云端。与现有技术中使用字符密码相比，本发明实施例中采用生物信息密钥对用户数据进行加密，由于生物信息的唯一性与不可复制性，用户数据的安全性较高，与现有技术相比，提高了用户数据的安全性。

请参阅图6，图6是本发明实施例公开的另一种终端设备的结构示意图，如图6所示，图6所描述的终端设备，除了包括图4所示的第一接收单元401、第一判断单元402、采集单元403、加密单元404和存储单元405之外，还包括：

第二接收单元406，用于接收针对加密的目标用户数据的访问指令。

本发明实施例中，当目标用户数据加密后，若需要对加密的目标用户数据进行解密，则用户针对加密的目标用户数据输入访问指令，第二接收单元406接收用户输入的针对加密的目标用户数据的访问指令。加密的目标用户数据可以为加密的图片、录音、文档、视频、音乐等目标用户数据。

输出单元407，用于输出提示信息，提示信息用于提示输入解密密钥。

本发明实施例中，当第二接收单元406接收针对加密的目标用户数据的访问指令之后，输出单元407输出用于提示输入解密密钥的提示信息，输出用于提示

输入解密密钥的提示信息可以是输出用于提示用户输入解密密钥的提示信息。解密密钥为与目标用户数据对应的目标用户生物信息，根据目标用户生物信息的类别，输入解密密钥的方式有区别，例如，当目标用户生物信息为指纹信息时，目标用户可以在终端设备上的指纹识别区域输入目标用户的指纹信息；当目标用户生物信息为目标用户虹膜信息时，则终端设备开启终端设备的摄像头，目标用户将目标用户的眼部区域对准终端设备的摄像头，以使终端设备的摄像头获取目标用户的眼部图像信息；当目标用户生物信息为目标用户声纹信息时，则终端设备开启终端设备的麦克风，目标用户通过终端设备的麦克风输入目标用户的声音信息。

第二判断单元408，用于当解密密钥输入后，判断解密密钥与目标用户数据对应的目标用户生物信息密钥是否匹配。

本发明实施例中，当用户输入解密密钥后，判断解密密钥与目标用户数据对应的目标用户生物信息密钥是否匹配。举例来说，若解密密钥为指纹信息，当指纹信息输入后，第二判断单元408判断输入的指纹信息与目标用户数据对应的目标用户指纹信息是否匹配，具体而言，可以通过判断输入的指纹图像与目标用户数据对应的目标用户指纹图像是否匹配，也可以通过判断输入的指纹信息中的指纹特征与目标用户数据对应的目标用户指纹特征是否匹配，目标用户指纹特征可以包括指纹的纹路特征、指纹的核心点位置、指纹的三角点位置等；若解密密钥为虹膜信息，当虹膜信息输入后，第二判断单元408判断输入的虹膜信息与目标用户数据对应的目标用户虹膜信息是否匹配，具体而言，可以通过判断输入的虹膜图像与目标用户数据对应的目标用户虹膜图像是否匹配；若解密密钥为声纹信息，当声纹信息输入后，第二判断单元408判断输入的声纹信息与目标用户数据对应的目标用户声纹信息是否匹配，具体而言，可以通过判断输入的声纹特征与目标用户数据对应的目标用户声纹特征是否匹配，目标用户声纹特征可以包括共振峰的频率值、共振峰的走向、声纹波形等。

解密单元409，用于当第二判断单元408判断结果为是时，解密加密的目标用户数据，获取目标用户数据。

本发明实施例中，若解密密钥与目标用户数据对应的目标用户生物信息密钥匹配，解密单元409则解密加密的目标用户数据，获取目标用户数据。例如，若解密密钥为指纹信息，当输入的指纹信息与目标用户数据对应的目标用户指

纹信息匹配时，解密单元409则解密加密的目标用户数据，获取目标用户数据，具体而言，当输入的指纹图像与目标用户数据对应的目标用户指纹图像匹配时，或者输入的指纹信息中的指纹特征与目标用户数据对应的目标用户指纹特征匹配时，解密单元409解密加密的目标用户数据，获取目标用户数据；若解密密钥为虹膜信息，当输入的虹膜信息与目标用户数据对应的目标用户虹膜信息匹配时，解密单元409则解密加密的目标用户数据，获取目标用户数据，具体而言，当输入的虹膜图像与目标用户数据对应的目标用户虹膜图像匹配时，解密单元409解密加密的目标用户数据，获取目标用户数据；若解密密钥为声纹信息，当输入的声纹信息与目标用户数据对应的目标用户声纹信息匹配时，解密单元409则解密加密的目标用户数据，获取目标用户数据，具体而言，当输入的声纹特征与目标用户数据对应的目标用户声纹特征匹配时，解密单元409则解密加密的目标用户数据，获取目标用户数据。

本发明实施例中，第一接收单元401接收针对目标用户数据的加密指令；第一判断单元402判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥；若否，采集单元403采集目标用户生物信息；加密单元404将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据；存储单元405将加密的目标用户数据存储在终端设备存储器或云端；第二接收单元406接收针对加密的目标用户数据的访问指令；输出单元407输出提示信息，提示信息用于提示输入解密密钥；当解密密钥输入后，第二判断单元408判断解密密钥与目标用户数据对应的目标用户生物信息密钥是否匹配；若匹配，解密单元409解密加密的目标用户数据，获取目标用户数据。实施本发明实施例，可以提高用户数据的安全性。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器（Read-Only Memory ，ROM）、随机存取器（Random Access Memory，RAM）、磁盘或光盘等。

以上对本发明实施例所提供的一种信息加密方法及终端设备进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的

一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

权 利 要 求 书

1、一种信息加密方法，其特征在于，包括:

接收针对目标用户数据的加密指令;

判断终端设备存储器或云端是否存储与所述目标用户数据对应的生物信息密钥;

若否，采集目标用户生物信息;

将所述目标用户生物信息作为所述目标用户数据对应的目标用户生物信息密钥，利用所述目标用户生物信息密钥对所述目标用户数据进行加密，得到加密的目标用户数据;

将所述加密的目标用户数据存储在所述终端设备存储器或所述云端。

2、根据权利要求1所述的方法，其特征在于，所述将所述加密的目标用户数据存储在所述终端设备存储器或所述云端之后，所述方法还包括:

接收针对所述加密的目标用户数据的访问指令;

输出提示信息，所述提示信息用于提示输入解密密钥;

当所述解密密钥输入后，判断所述解密密钥与所述目标用户数据对应的所述目标用户生物信息密钥是否匹配;

若匹配，解密所述加密的目标用户数据，获取所述目标用户数据。

3、根据权利要求1所述的方法，其特征在于，所述采集目标用户生物信息包括:

采集至少两个用户生物信息;

当所述至少两个用户生物信息相互匹配时，确认目标用户生物信息采集成功。

4、根据权利要求3所述的方法，其特征在于，所述确认目标用户生物信息采集成功，包括:

将所述至少两个用户生物信息进行合成，得到目标用户生物信息。

5、根据权利要求3所述的方法，其特征在于，所述确认目标用户生物信息

采集成功，包括:

从所述至少两个用户生物信息中选择任一个作为目标用户生物信息。

6、一种终端设备，其特征在于，包括:

第一接收单元，用于接收针对目标用户数据的加密指令;

第一判断单元，用于判断终端设备存储器或云端是否存储与所述目标用户数据对应的生物信息密钥;

采集单元，用于当所述第一判断单元判断结果为否时，采集目标用户生物信息;

加密单元，用于将所述目标用户生物信息作为所述目标用户数据对应的目标用户生物信息密钥，利用所述目标用户生物信息密钥对所述目标用户数据进行加密，得到加密的目标用户数据;

存储单元，用于将所述加密的目标用户数据存储在所述终端设备存储器或所述云端。

7、根据权利要求6所述的终端设备，其特征在于，所述终端设备还包括:

第二接收单元，用于接收针对所述加密的目标用户数据的访问指令;

输出单元，用于输出提示信息，所述提示信息用于提示输入解密密钥;

第二判断单元，用于当所述解密密钥输入后，判断所述解密密钥与所述目标用户数据对应的所述目标用户生物信息密钥是否匹配;

解密单元，用于当所述第二判断单元判断结果为是时，解密所述加密的目标用户数据，获取所述目标用户数据。

8、根据权利要求6所述的终端设备，其特征在于，所述采集单元包括:

采集子单元，用于采集至少两个用户生物信息;

确认子单元，用于当所述至少两个用户生物信息相互匹配时，确认目标用户生物信息采集成功。

9、根据权利要求8所述的终端设备，其特征在于，所述确认子单元确认目标用户生物信息采集成功的方式具体为:

所述确认单元将所述至少两个用户生物信息进行合成，得到目标用户生物信息。

10、根据权利要求8所述的终端设备，其特征在于，所述确认子单元确认目标用户生物信息采集成功的方式具体为：

所述确认单元从所述至少两个用户生物信息中选择任一个作为目标用户生物信息。

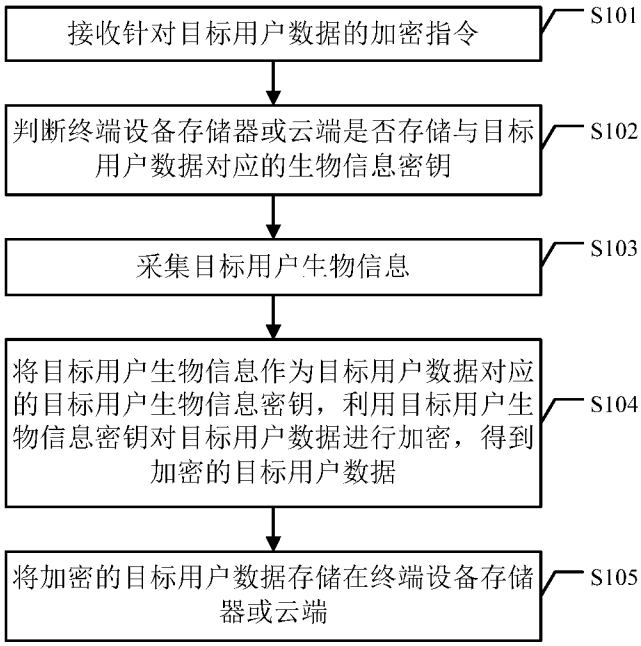
接收针对目标用户数据的加密指令
S101
判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥
S102
采集目标用户生物信息
S103
将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据
S104
将加密的目标用户数据存储在终端设备存储器或云端
S105

图 1

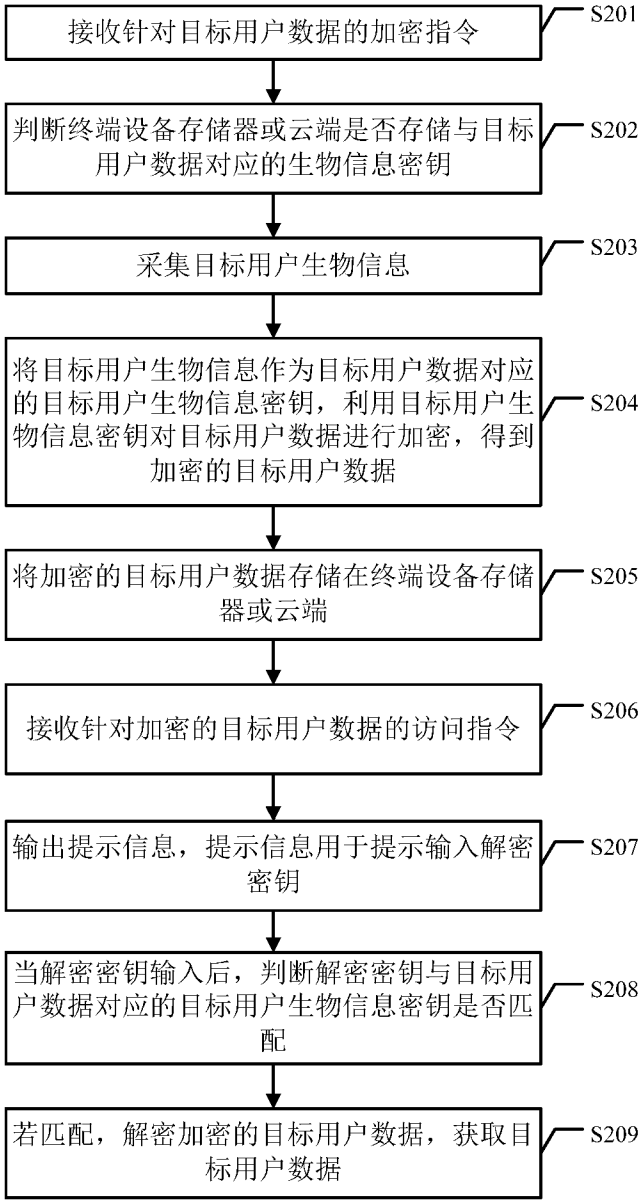
接收针对目标用户数据的加密指令
S201
判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥
S202
采集目标用户生物信息
S203
将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据
S204
将加密的目标用户数据存储在终端设备存储器或云端
S205
接收针对加密的目标用户数据的访问指令
S206
输出提示信息，提示信息用于提示输入解密密钥
S207
当解密密钥输入后，判断解密密钥与目标用户数据对应的目标用户生物信息密钥是否匹配
S208
若匹配，解密加密的目标用户数据，获取目标用户数据
S209

图 2

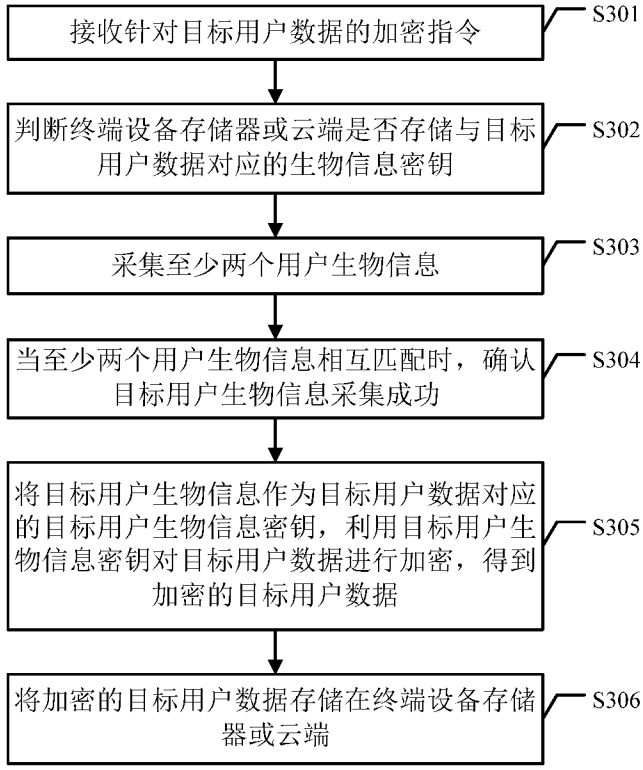
接收针对目标用户数据的加密指令
S301
判断终端设备存储器或云端是否存储与目标用户数据对应的生物信息密钥
S302
采集至少两个用户生物信息
S303
当至少两个用户生物信息相互匹配时，确认目标用户生物信息采集成功
S304
将目标用户生物信息作为目标用户数据对应的目标用户生物信息密钥，利用目标用户生物信息密钥对目标用户数据进行加密，得到加密的目标用户数据
S305
将加密的目标用户数据存储在终端设备存储器或云端
S306

图 3

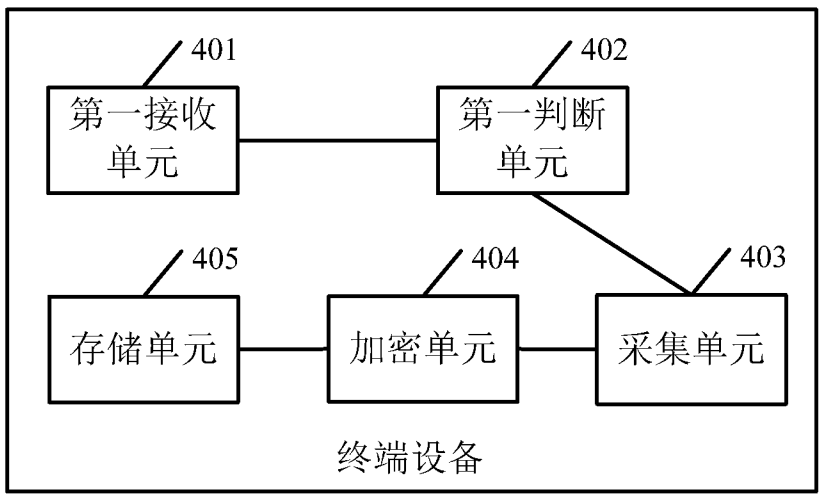
401
第一接收单元
402
第一判断单元
405
存储单元
404
加密单元
403
采集单元
终端设备

图 4

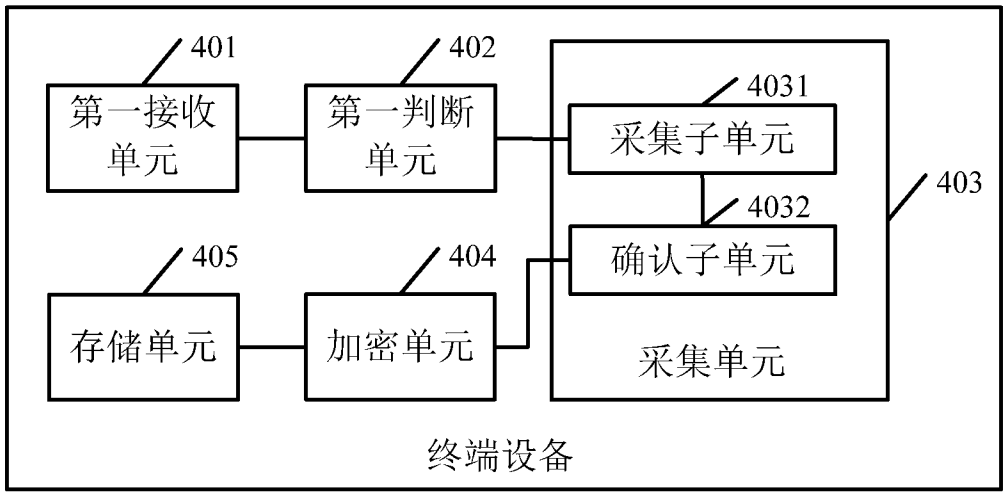
401
第一接收单元
402
第一判断单元
4031
采集子单元
403
4032
确认子单元
405
存储单元
404
加密单元
采集单元
终端设备

图 5

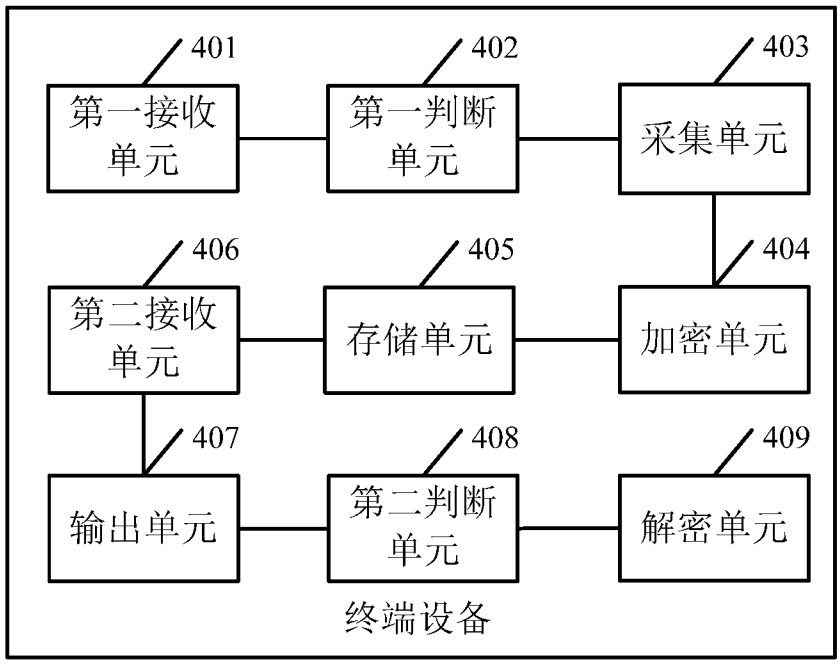
401
第一接收单元
402
第一判断单元
403
采集单元
406
第二接收单元
405
存储单元
404
加密单元
407
输出单元
408
第二判断单元
409
解密单元
终端设备

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/093526

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; H04W; H04Q; H04L

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

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

CNTXT; CNABS; DWPI; TWTXT; SIPOABS; CNKI: double, judge, store, need or not, acquire; cloud, biological, encrypt, determine

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104239768 A (SHENZHEN HOFAN ELECTRONIC COMMERCE CO., LTD.), 24 December 2014 (24.12.2014), description, paragraphs [0038]-[0049], and figures 1-3	1-10
X	CN 102316452 A (LIAONING GOETHINK TECHNOLOGY CO., LTD.), 11 January 2012 (11.01.2012), description, paragraphs [0034]-[0078], and figures 1-2	1-10
A	WO 2015028824 A1 (SIM & PIN LTD.), 05 March 2015 (05.03.2015), the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 April 2016 (12.04.2016)	**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 **LI, Bing** Telephone No.: (86-10) **62411327**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/093526

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104239768 A	24 December 2014	WO 2016033835 A1	10 March 2016
CN 102316452 A	11 January 2012	None	
WO 2015028824 A1	05 March 2015	GB 201315420 D0	16 October 2013
		GB 2517732 A	04 March 2015

国际检索报告

国际申请号
PCT/CN2015/093526

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; H04W; H04Q; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNTXT;CNABS;DWPI;TWTXT;SIPOABS;CNKI:加密，双重，判断，生物，存储，云，是否需要，采集;cloud,biological, enctypt,determine

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 104239768 A (深圳市浩方电子商务有限公司) 2014年 12月 24日 (2014-12-24) 说明书第[0038]-[0049]段，图1-3	1-10
X	CN 102316452 A (辽宁国兴科技有限公司) 2012年 1月 11日 (2012-01-11) 说明书第[0034]-[0078]段，图1-2	1-10
A	WO 2015028824 A1 (SIM & PIN LTD) 2015年 3月 5日 (2015-03-05) 全文	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	国际检索报告邮寄日期
2016年 4月 12日	2016年 4月 29日

ISA/CN的名称和邮寄地址	受权官员
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	李冰
传真号 (86-10)62019451	电话号码 (86-10)62411327

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/093526

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	104239768	A	2014年 12月 24日	WO	2016033835	A1	2016年 3月 10日
CN	102316452	A	2012年 1月 11日		无		
WO	2015028824	A1	2015年 3月 5日	GB	201315420	D0	2013年 10月 16日
				GB	2517732	A	2015年 3月 4日