(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
2022 年 8 月 18 日 (18.08.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/170759 A1

(51) 国际专利分类号:
G06Q 20/40 (2012.01) *G06Q 20/38* (2012.01)

(21) 国际申请号: PCT/CN2021/117232

(22) 国际申请日: 2021 年 9 月 8 日 (08.09.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110179442.7 2021年2月9日 (09.02.2021) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: 李定洲 (LI, Dingzhou); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。 郭伟 (GUO, Wei); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。 祖立军 (ZU, Lijun); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。 钱进 (QIAN, Jin); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。

(74) 代理人: 北京东方亿思知识产权代理有限责任公司 (BEIJING EAST IP LTD.); 中国北京市东城区东长安街1号东方广场东方经贸城东2座1601室, Beijing 100738 (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,

(54) **Title:** INFORMATION PROCESSING METHOD AND APPARATUS, AND ELECTRONIC DEVICE, SERVER AND MEDIUM

(54) 发明名称: 信息处理方法、装置、电子设备、服务器及介质

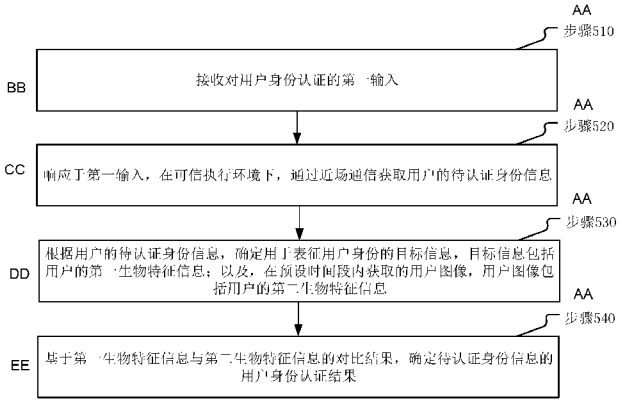


图 5

AA Step
BB Receive a first input for user identity authentication
CC In response to the first input, acquire identity information to be authenticated of a user by means of near field communication in a trusted execution environment
DD Determine, according to the identity information to be authenticated of the user, target information for representing the identity of the user, wherein the target information comprises first biological characteristic information of the user, and acquire a user image within a pre-set time period, wherein the user image comprises second biological characteristic information of the user
EE On the basis of a comparison result between the first biological characteristic information and the second biological characteristic information, determine a user identity authentication result of the identity information to be authenticated

(57) **Abstract:** Disclosed are an information processing method and apparatus, and an electronic device, a server and a medium. The information processing method comprises: firstly, receiving a first input for user identity authentication; next, in response to the first input, acquiring identity information to be authenticated of a user by means of near field communication in a trusted execution environment; then, determining, according to the identity information to be authenticated of the user, target information for representing the identity of the user, wherein the target information comprises first biological characteristic information of the user, and acquiring a

WO 2022/170759 A1

[见续页]

CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))。

user image within a pre-set time period, wherein the user image comprises second biological characteristic information of the user; and then, on the basis of a comparison result between the first biological characteristic information and the second biological characteristic information, determining a user identity authentication result of the identity information to be authenticated. By means of the method, the accuracy of an identity authentication result can be effectively improved, user identity information is prevented from being leaked and tampered with, and network information security is improved.

(57) 摘要：公开了一种信息处理方法、装置、电子设备、服务器及介质。该信息处理方法包括：首先，接收对用户身份认证的第一输入；接着，响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；再者，根据用户的待认证身份信息，确定用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息，以及在预设时间段内获取的用户图像，用户图像包括用户的第二生物特征信息；然后，基于第一生物特征信息与第二生物特征信息的对比结果，确定待认证身份信息的用户身份认证结果。根据该方法，能够有效提高身份认证结果的准确性，防止用户身份信息被泄露和被篡改，提高网络信息安全。

信息处理方法、装置、电子设备、服务器及介质

相关申请的交叉引用

本申请要求享有于 2021 年 02 月 09 日提交的名称为“信息处理方法、装置、电子设备、服务器及介质”的中国专利申请 202110179442.7 的优先权，该申请的全部内容通过引用并入本文中。

技术领域

本公开属于互联网技术领域，尤其涉及一种信息处理方法、装置、电子设备、服务器及介质。

背景技术

随着计算机和互联网的发展，需要用户身份认证的场景也越来越多，如在帐户登录或者网络支付的场景中进行身份认证。

目前，可以通过对比用户身份证件图像和用户图像的方式，或者通过读取用户身份证件内芯片的身份信息的方式进行身份认证。但是，前者的身份认证方式难以识别用户身份证件的真伪，另外，用户身份证件表面信息磨损或者图像拍摄效果不佳，也会降低身份认证结果的准确性。而后者的身份认证方式，也会因为读取用户身份证件的平台自身安全性低，导致用户身份信息被恶意篡改和泄露。

发明内容

本公开实施例提供一种信息处理方法、装置、电子设备、服务器及介质，能够有效提高身份认证结果的准确性，防止用户身份信息被泄露和被篡改，提高网络信息安全。

第一方面，本公开实施例提供了一种信息处理方法，应用于电子设备，包括：

接收对用户身份认证的第一输入；

响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

根据用户的待认证身份信息，确定用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息，以及在预设时间段内获取的用户图像，用户图像包括用户的第二生物特征信息；

基于第一生物特征信息与第二生物特征信息的对比结果，确定待认证身份信息的用户身份认证结果。

第二方面，本公开实施例提供了一种信息处理方法，应用于电子设备，包括：

接收对用户身份认证的第一输入；

响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

向服务器发送用户的待认证身份信息，用户的待认证身份信息用于确定待认证身份信息的用户身份认证结果；

在预设时间段内获取用户图像，并向服务器发送用户图像，用户图像用于与用户的待认证身份进行对比，以确定用户身份认证结果；

接收服务器发送的待认证身份信息的用户身份认证结果。

第三方面，本公开实施例提供了一种信息处理方法，应用于服务器，包括：

接收电子设备发送的用户的待认证身份信息；

在检测到电子设备的设备类型为预设目标设备类型的情况下，获取与用户的待认证身份信息对应的且用于表征用户身份的目标信息，所述目标信息包括用户的第一生物特征信息；

接收电子设备发送的用户图像；

基于第一生物特征信息与用户图像中的第二生物特征信息的对比结果，确定待认证身份信息的用户身份认证结果；

向电子设备发送用户身份认证结果。

第四方面，本公开实施例提供了一种信息处理装置，应用于电子设

备，包括：

接收模块，用于接收对用户身份认证的第一输入；

获取模块，用于响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

处理模块，用于根据用户的待认证身份信息，确定用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息，以及在预设时间段内获取的用户图像，用户图像包括用户的第二生物特征信息；

确定模块，用于基于第一生物特征信息与第二生物特征信息的对比结果，确定待认证身份信息的用户身份认证结果。

第五方面，本公开实施例提供了一种信息处理装置，应用于电子设备，具体可以包括：

接收模块，用于接收对用户身份认证的第一输入；

获取模块，用于响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

发送模块，用于向服务器发送用户的待认证身份信息，用户的待认证身份信息用于确定待认证身份信息的用户身份认证结果；

发送模块还用于，在预设时间段内获取用户图像，并向服务器发送用户图像，用户图像用于与用户的待认证身份进行对比，以确定用户身份认证结果；

接收模块还用于，接收服务器发送的待认证身份信息的用户身份认证结果。

第六方面，本公开实施例提供了一种信息处理装置，应用于服务器，具体可以包括：

接收模块，用于接收电子设备发送的用户的待认证身份信息；

获取模块，用于在检测到电子设备的设备类型为预设目标设备类型的情况下，获取与用户的待认证身份信息对应的且用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息；

接收模块还用于，接收电子设备发送的用户图像；

确定模块，用于基于第一生物特征信息与用户图像中的第二生物特征

信息的对比结果，确定待认证身份信息的用户身份认证结果；

发送模块，用于向电子设备发送用户身份认证结果。

第七方面，本公开实施例提供了一种电子设备，该电子设备包括：处理器和存储有计算机程序指令的存储器；

处理器执行计算机程序指令时实现如第一方面或者第二方面所示的信息处理方法。

第八方面，本公开实施例提供了一种服务器，该服务器包括：处理器和存储有计算机程序指令的存储器；

处理器执行计算机程序指令时实现如第三方面所示的信息处理方法。

第九方面，本公开实施例提供了一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序指令，计算机程序指令被处理器执行时实现如第一方面所示的信息处理方法。

本公开实施例的信息处理方法、装置、设备及介质，通过在可信执行环境 TEE 和近场通信 NFC 获取用户的待认证身份信息的方式，来获取可信任的用于表征用户身份的目标信息如身份证件信息，以避免伪造身份证件的问题，同时也避免了因拍照效果不佳或者拍摄硬件不足造成获取到的目标信息不准确，从而导致用户身份认证结果不正确的问题。

另外，通过在可信执行环境 TEE 中获取目标信息、对比目标信息中的第一生物特征信息和拍摄的用户图像中的第二生物特征信息，有效防止恶意软件截获身份证件信息被替换和篡改的问题，同时，通过可信执行环境 TEE 安全访问电子设备的摄像头，确保用于对比认证的用户图像的准确性，防止注入伪造人脸面部照片或视频的行为。

附图说明

为了更清楚地说明本公开实施例的技术方案，下面将对本公开实施例中所需要使用的附图作简单的介绍，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 是根据本公开第一方面的信息处理方法的实施例的信息处理架构示意图；

图 2 是根据本公开第一方面的信息处理方法的实施例的电子设备和服务器中结构示意图；

图 3 是根据本公开第一方面的信息处理方法的实施例的应用场景的架构示意图；

图 4 是根据本公开第一方面的信息处理方法的实施例的电子设备所属类别对应的 APDU 指令执行位置的示意图；

图 5 是根据本公开第一方面的信息处理方法的实施例的信息处理方法的流程示意图；

图 6 是根据本公开第一方面的信息处理方法的实施例的信息处理界面示意图；

图 7 是根据本公开第一方面的信息处理方法的实施例的原图像直方图的示意图；

图 8 是根据本公开第一方面的信息处理方法的实施例的可信身份认证初始化流程示意图；

图 9 是根据本公开第一方面的信息处理方法的实施例的可信身份认证对比的流程示意图；

图 10 是根据本公开第四方面的信息处理装置的基于电子设备的信息处理装置的实施例结构示意图；

图 11 是根据本公开第五方面的信息处理装置的基于电子设备的信息处理装置的实施例结构示意图；

图 12 是根据本公开第六方面的信息处理装置的基于服务器的信息处理装置的实施例结构示意图；

图 13 是根据本公开第七方面的信息处理设备的实施例的硬件结构示意图。

具体实施方式

下面将详细描述本公开的各个方面的特征和示例性实施例，为了使本公开的目的、技术方案及优点更加清楚明白，以下结合附图及具体实施例，对本公开进行进一步详细描述。应理解，此处所描述的具体实施例仅

被配置为解释本公开，并不被配置为限定本公开。对于本领域技术人员来说，本公开可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本公开的示例来提供对本公开更好的理解。

需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括要素的过程、方法、物品或者设备中还存在另外的相同要素。

目前身份认证方案所处的操作系统大多为安卓系统，这样，身份认证的安全性高度依赖于安卓系统自身的安全性，一旦安卓系统的安全机制失效，那么依赖于安卓系统的安全机制的身份认证方案也会出现漏洞。若身份认证的过程由某个应用程序发起并在安卓环境下执行、且安卓系统环境自身安全性较低时，一旦被攻击者攻击如攻击者获取 root 权限，通过植入木马等手段，窃取并篡改用户的身份认证过程中的信息，伪造与实际不符的身份认证结果，有甚者还会利用伪造的身份信息实施违法活动，造成用户的身份信息的泄露。

现有的身份认证方案，可以通过对比用户身份证件中的用户图像和实时获取用户图像的方式，或者通过读取用户身份证件内芯片的身份信息的方式进行身份认证。但是，前者的身份认证方式难以识别用户身份证件的真伪，以及因用户身份证件表面信息磨损或者电子设备拍摄图像的效果不佳，都会导致身份认证结果不准确。而后者的身份认证方案，通常是授权给应用程序的运营机构进行读取和身份认证，如果运营机构的人员有意泄露授权凭证给非授权机构，或者非授权机构通过反向工程、恶意调试等手段窃取授权凭证，那么非授权机构就存在冒用该凭证取得不当收益的可

能。另外，取用户身份证件内芯片的身份信息的方式中执行人脸比对的身份认证过程在安卓系统内的一个安卓控件内，或者作为安卓应用的一部分来执行，这样，也会因为安卓系统自身安全性低，导致用户的身份信息被恶意篡改和泄露。

由此，本公开实施例提供了一种信息处理方法、装置、设备及存储介质，通过在可信执行环境（trusted execution environment，TEE）和近场通信（near field communication ，NFC）获取用户的待认证身份信息的方式，来获取可信任的用于表征用户身份的目标信息如身份证件信息，以避免伪造身份证件的问题，同时也避免了因拍照效果不佳或者拍摄硬件不足造成获取到的目标信息不准确，从而导致用户身份认证结果不正确的问题。

另外，通过在可信执行环境 TEE 中获取目标信息、对比目标信息中的第一生物特征信息和拍摄的用户图像中的第二生物特征信息，有效防止恶意软件截获身份证件信息被替换和篡改的问题，同时，通过可信执行环境 TEE 安全访问电子设备的摄像头，确保用于对比认证的用户图像的准确性，防止注入伪造人脸面部照片或视频的行为。

为了更好的理解本公开，下面将结合附图 1 至图 11，详细描述根据本公开实施例的信息处理方法、装置、电子设备、服务器及存储介质，应注意，这些实施例并不是用来限制本公开公开的范围。

图 1 是根据本公开第一方面的信息处理方法的实施例的信息处理架构示意图。

如图 1 所示，该信息处理系统包括电子设备 10、服务器 20 和近场通信芯片 30 如身份证件中的芯片、银行卡证件中的芯片、充值卡中的芯片等支持近场通讯的芯片。在电子设备 10 与服务器 20 建立通讯链接的情况下，接收对用户身份认证的第一输入。电子设备 10 响应于第一输入，在可信执行环境下，通过近场通信获取近场通信芯片 30 中用户的待认证身份信息。电子设备 10 根据用户的待认证身份信息，确定用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息，以及在预设时间段内获取的用户图像，用户图像包括用户的第二生物特征信息，以及基于

第一生物特征信息与第二生物特征信息的对比结果，确定待认证身份信息的用户身份认证结果。

这里，在电子设备 10 获取到用户的待认证身份信息之后，也可以将用户的待认证身份信息发送到服务器 20，以使服务器 20 根据用户的待认证身份信息，确定用于表征用户身份的目标信息，并通过电子设备 10 拍摄的用户图像，确定待认证身份信息的用户身份认证结果，然后，将待认证身份信息的用户身份认证结果反馈到电子设备 10，以便电子设备 10 向用户显示用户身份认证结果。

基于上述架构，下面分别对电子设备 10 和服务器 20 进行详细说明。如图 2 所示，本公开实施例中电子设备 10 可以包括电子设备应用程序 101、可信身份认证服务控件 102 和可信身份认证服务 TA103。电子设备应用程序 101 的示例包括可信身份认证服务 SDK1011 即软件开发工具包（software development kit，SDK），可信身份认证服务 TA103 即可信应用程序（trusted application，TA）。

进一步地，电子设备 10 具备可信执行环境 TEE，电子设备 10 通过可信身份认证服务相关的第三方应用程序（Application，APP），由需要开展用户认证服务平台如购物类应用程序或者行业方提供，其通过集成可信身份认证服务 SDK1011 获取可信身份认证服务能力，可信身份认证服务控件 102 作为独立应用程序运行在电子设备上，可信身份认证服务 TA103 运行在可信执行环境 TEE 中。

本公开实施例中的服务器 20，可以运行可信身份服务平台等支撑管理类的平台。该运行可信身份服务平台可以包括权威身份认证模块 201、可信身份认证后台模块 202 和人脸认证对比模块 203。权威身份认证模块 201 用于与身份鉴别平台的身份鉴别服务器进行交互，解析用户的待认证的身份信息的身份信息明文数据。这里，本公开实施例中的可信身份服务平台，用于管理接入和使用可信身份服务平台的第三方应用程序，可结合权威身份认证模块 201 和人脸认证对比模块 203 为可信身份认证服务控件 102 提供业务功能处理流程。

基于上述电子设备 10 和服务器 20 所示的结构，对本公开实施例提供

的信息处理方法进行详细说明，具体如下所示。

基于上述可知，现有的身份证件信息如用户身份证件图像和身份证件号码存在被滥用、盗用、恶意泄露等问题。因此，要想确保身份证件信息安全、合规的使用，首先，要保证用户所使用的身份证件是真实的且就在其身边，这样，通过 NFC 安全读取和解析身份证件信息是本公开实施例的技术基础。而要实现通过 NFC 安全读取和解析身份证有两个前提条件，一是实现从电子设备 10 通过服务器到身份鉴别服务器安全的传输身份证件信息，二是实现 NFC 安全读取身份证件信息。

针对此，本公开实施例基于 TEE 安全保障机制提出从电子设备到服务器的安全信息交互方式。首先，本公开实施例将对接身份鉴别服务器的功能授予权威身份认证模块 201，并预先在服务器中预身份鉴别服务器授予的服务器证书，该服务器证书用于表示该服务器有权限对用户的待认证身份信息进行鉴别。其次，进一步通过与电子设备对应的可信应用管理平台（Trusted Application Management，TAM）将身份鉴别服务器提供的目标信息数据解密授权凭证安全地下载到可信身份认证服务中，实现从电子设备到可信身份服务平台再到身份鉴别平台的安全通讯闭环。

基于此，当电子设备接收到用户对用户身份认证的第一输入时，可通过电子设备中安卓系统和/或 ios 系统中的可信身份认证服务 SDK1011 和可信身份认证服务控件 102 实现对可信身份认证服务 TA103 的调用，以及发起对待认证身份信息的采集和处理，再由其可信地连接到可信身份服务平台与可信身份认证后台模块 202 进行通讯。最后，通过权威身份认证模块 201 完成对待认证身份信息的校验和解析处理。

如此，一方面有效规避了电子设备中 TEE 空间较小能力受限的问题，降低了识读待认证身份信息对电子设备的硬件资源的要求。另一方面，通过可信身份认证服务 TA 基于电子设备数字证书如根信任证书生成一对公私密钥对。其中，公私密钥对中的设备公钥与用户地址（UserId）及电子设备唯一标识会一并记录在可信身份服务平台，当发现某电子设备存在风险时，迅速定位到某台电子设备并终止其继续访问可信身份服务平台，为可信身份服务平台进行电子设备风险防控提供了有效的支持。另外，在确

保了从电子设备到身份鉴别平台的身份认证信息传输的安全后，就已经具备了安全受理待认证身份信息校验和解析的能力，接下来就可以进一步解决 NFC 安全读取身份证件信息和与可信身份服务平台安全对接的过程，具体可以结合图 3 进行详细说明。

图 3 是根据本公开提供的信息处理系统的一个实施例的应用场景的架构示意图。如图 3 所示，近场通讯芯片为包括用户的待认证身份信息的芯片，该芯片支持 NFC 通讯，例如二代身份证件。电子设备 10 包括 NFC 模块和可信身份认证服务 TA103，NFC 模块用于读取和传输二代身份证件中用户的待认证身份信息，可信身份认证服务 TA103 运行在 TEE 可信执行环境中，在二代身份证件与 NFC 进行应用协议数据单元（Application Protocol，APDU）指令通讯时，判断和比对当前物联网电子设备，并确定 NFC 的访问与二代身份证件之间通讯流程。如在一些资源严重受限的物联网电子设备如可穿戴式设备、智能门锁等无法承载计算量较大的设备，还需在 NFC 通讯过程中对其流程做进一步定制，并对 NFC 的访问和与二代身份证件之间的 APDU 指令交互放在设备 TEE 内执行，将二代身份证件访问 APDU 指令的生成、组装和 APDU 响应的处理放在可信身份认证服务后台上进行，具体内容可以具体参照图 4 所示的内容。

服务器 20 运行可信身份服务平台，该运行可信身份服务平台用于基于可信身份认证服务的处理信息方法的支撑管理平台。另外，该运行可信身份服务平台可以包括 APDU 指令操作模块和权威身份认证模块 201，其中，APDU 指令操作模块用于处理二代身份证件访问 APDU 指令的生成、组装和响应，主要与权威身份认证模块 201 进行交互。权威身份认证模块 201 用于与身份鉴别平台进行安全交互确定用户的待认证的身份信息的身份信息明文数据。

基于图 3 所示的系统架构，本公开实施例是通过 TEE 实现对 NFC 信息的安全读取，然后使可信身份认证服务 TA103 全面监听设备外对 NFC 的读取操作。待可信身份认证服务 TA103 收到刷身份证操作请求时，即安全调用电子设备的 NFC 模块，并按照二代身份证件卡规范执行 APDU 指令集，以及将执行指令响应的待认证的身份信息进行回传。接着，可信身

份认证服务 TA103 通过电子设备和服务器之间的安全链接把接收到的待认证的身份信息的密文信息发送到权威身份认证模块 201 中。权威身份认证模块 201 在收到待认证的身份信息的密文信息后即建立与身份鉴别服务器的安全通信，并通过身份鉴别服务器解析和按身份证件属性格式拼接组装成用于表征用户身份的目标信息的原文字符串返回时，由可信身份服务服务平台把目标信息的原文字符串响应回给可信身份认证服务 TA103。此时，可信身份认证服务 TA103 就可以根据事先保存的权威身份鉴别机构的目标信息数据解密授权凭证和目标信息的原文字符串对待认证的身份信息如身份证件号码、身份证件图像和身份证件图像中用户面部图像等进行解密，得到目标信息如身份证件图像中用户面部图像。在上述过程中，可信身份认证服务 TA103 通过 NFC 近场读取到二代身份证件的待认证的身份信息再交由权威身份认证模块 201 服务处理和解析出待认证的身份信息的身份信息明文数据。

另外，需要说明的是，本公开实施例中的信息处理方法可以在电子设备侧执行，也可以在电子设备和服务器上执行。由此，在一些可能的实施例中，如在一些资源严重受限的物联网电子设备如可穿戴式设备、智能门锁等无法承载计算量较大的设备，还需在 NFC 通讯过程中对其流程做进一步定制。具体可以结合图 4 对这些物联网电子设备进行说明。如图 4 所示，针对本公开实施例提供的一些资源严重受限的物联网电子设备（如可穿戴式设备、智能门锁等），还需在 NFC 通讯过程中对其流程做进一步定制，并对 NFC 的访问和与身份证件之间的 APDU 指令交互放在设备 TEE 内执行，将身份证件访问 APDU 指令的生成、组装和 APDU 响应的处理放在可信身份服务平台上进行。即本公开实施例通过 TEE 实现对 NFC 信息的安全读取，然后使可信身份认证服务 TA103 全面监听设备外对 NFC 的读取操作。待可信身份认证服务 TA103 收到刷身份证操作请求时，即安全调用电子设备的 NFC 模块，并按照二代身份证件卡规范执行 APDU 指令集中近场通讯的指令，以及将执行指令响应的待认证的身份信息进行回传，这里，APDU 指令集中的指令由服务器确定。接着，可信身份认证服务 TA103 通过电子设备和服务器之间的安全链接把接收到的待认证的身份

信息的密文信息发送到权威身份认证模块 201 中。权威身份认证模块 201 在收到待认证的身份信息的密文信息后即建立与身份鉴别服务器的安全通信，并通过身份鉴别服务器解析和按身份证件属性格式拼接组装成用于表征用户身份的目标信息的原文字符串返回至权威身份认证模块 201。此时，权威身份认证模块 201 就可以根据事先保存的权威身份鉴别机构的目标信息数据解密授权凭证和目标信息的原文字符串对待认证的身份信息如身份证件号码、身份证件图像和身份证件图像中用户面部图像等的解密，以得到目标信息如份证件图像中用户面部图像。在上述过程中，可信身份认证服务 TA103 通过 NFC 近场读取到二代身份证件的待认证的身份信息再交由权威身份认证模块 201 服务处理和解析出待认证的身份信息的身份信息明文数据。

根据物联网电子设备定制 NFC 的访问与身份证件之间通讯流程时，根据物联网电子设备性能、用途和类型选择合适的处理流程，如智能手机、手提/平板电脑、智能 POS 机具、智能汽车、自助售货机、以及自助闸机使用在 TEE 内调用 NFC 与二代身份证件之间进行 APDU 指令交互的方案；智能手表/手环、智能门锁/门禁使用在设备执行 APDU 指令，在可信身份服务平台进行 APDU 指令的生成、组装和处理。

基于此，当电子设备接收到用户对用户身份认证的第一输入时，响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息，向服务器发送用户的待认证身份信息，用户的待认证身份信息用于确定待认证身份信息的用户身份认证结果。这样，服务器接收电子设备发送的用户的待认证身份信息，在检测到电子设备的设备类型为预设目标设备类型即电子设备的设备类型符合可穿戴式设备、智能门锁等无法承载计算量较大的设备的情况下，获取与用户的待认证身份信息对应的且用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息。再者，电子设备在预设时间段内获取用户图像，并向服务器发送用户图像，用户图像用于与用户的待认证身份进行对比，以确定用户身份认证结果。然后，服务器接收电子设备发送的用户图像，并确定用户图像中的用户的第二生物特征信息，基于第一生物特征信息与第二生物特征信息的对比结果，确

定待认证身份信息的用户身份认证结果，向电子设备发送待认证身份信息的用户身份认证结果。电子设备，接收服务器发送的待认证身份信息的用户身份认证结果，以便向用户提示待认证身份信息的用户身份认证结果。这里，在确定用户的第一生物特征信息时，服务器可以向电子设备发送获取用户图像指令，用户图像指令用于指示电子设备在预设时间段内获取用户图像。电子设备在接收到服务器发送的获取用户图像指令时，获取用户图像。或者，电子设备接收到用户针对获取用户图像指令，也可以使电子设备获取用户图像。

进一步地，电子设备可以在可信执行环境下，通过执行服务器提供的协议数据指令集中近场通讯的指令，获取用户的待认证身份信息。

服务器在目标信息时，可以具体通过如下步骤，即根据待认证身份信息的密文信息，确定按照身份证件属性格式拼接组装成的用于表征用户身份的目标信息的原文字符串，根据预存的目标信息数据解密授权凭证和目标信息的原文字符串，对待认证的身份信息进行解密，得到目标信息。

进一步地，在确定原文字符串的过程中，服务器向身份鉴别服务器发送协议数据指令，协议数据指令用于指示身份鉴别服务器按照身份证件属性格式拼接组装成的用于表征用户身份的目标信息的原文字符串，接收身份鉴别服务器发送的目标信息的原文字符串。

由此，本公开实施例提出一种基于 TEE 和 NFC 的可信身份认证的信息处理方法，可以通过 TEE 安全访问 NFC 进行身份证件的待认证的身份信息识读的方式以获取可靠可信的用于表征用户身份的目标信息，以及在一些实施例中可以在可信执行环境 TEE 中与服务器中运行可信身份服务平台进行交互，以避免伪造身份证的问题，同时也避免了因拍照效果不佳造成获取到的目标信息不准确，提高身份认证的准确性。通过将待认证的身份信息对应的目标信息数据解密授权凭证迁移至 TEE 中，杜绝了待认证的身份信息在电子设备和服务器交互过程中可能被木马病毒窃取的问题。另外，通过从 TEE 内安全访问摄像头，确保用于对比认证的用户图像即实时的用户图像的源头可信，防止注入伪造人脸照片或视频的行为。

另外，针对一些支持 TEE 和 NFC 的物联网电子设备硬件资源严重受

限的问题，本公开实施例利用第四代移动通信技术（the 4th generation mobile communication technology，4G）、第五代移动通信技术（5th generation mobile networks，5G）传输速率更高时延更低的特性，将 NFC 与二代身份证交互的命令进行了拆分，其中，通过近场通信获取用户的待认证身份信息的部分在电子设备实现，主要处理身份证件 APDU 请求响应和交互协议，后端部分移至服务器运行，主要负责身份证件访问 APDU 指令的生成、组装和 APDU 响应的处理。通过上述前后端分离处理的方式，减少了电子设备的 NFC 交互协议的空间占比，对于可穿戴设备等资源比较有限的物联网终端设备，具有更强的适用性。通过电子设备的类别，确定在电子设备和服务器确定对比结果方式，保证了身份证识读和人脸比对功能在电子设备 TEE 空间资源有限的情况下的可用性和适配性。

以上，采用 TEE 安全访问 NFC 识读用户的待认证身份信息的方式确保获取的身份证信息的数据源真实准确，起到防伪身份证效果，同时可信执行环境 TEE 防止恶意软件截获身份证信息数据被替换和篡改。另外，本公开实施例是基于电子设备 TEE 和服务器之间的安全闭环实现的，能够确保信息是密文上送可信身份认证后台解密再以安全 TEE 安全通道传送回来使用的，适用于更多的身份认证场景。

基于上述信息处理架构和应用场景，下面结合图 5 对本公开实施例提供的信息处理方法进行详细说明。

图 5 是根据本公开第一方面的信息处理方法的实施例的信息处理方法的流程示意图。

如图 5 所示，该信息处理方法可以应用于如图 1 所示的电子设备，该信息处理方法具体可以包括如下步骤。

首先，步骤 510，接收对用户身份认证的第一输入。接着，步骤 520，响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息。再者，步骤 530，根据用户的待认证身份信息，确定用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息，以及在预设时间段内获取拍摄的用户图像，用户图像包括用户的第二生物特征信息。然后，步骤 540，基于第一生物特征信息与第二生物特征信息的对

比结果，确定待认证身份信息的用户身份认证结果。

由此，通过在可信执行环境 TEE 和近场通信 NFC 获取用户的待认证身份信息的方式，来获取可信任的用于表征用户身份的目标信息如身份证件信息，以避免伪造身份证件的问题，同时也避免了因拍照效果不佳或者拍摄硬件不足造成获取到的目标信息不准确，从而导致用户身份认证结果不正确的问题。

另外，通过在可信执行环境 TEE 中获取目标信息和对比目标信息中的第一生物特征信息和拍摄的用户图像中的第二生物特征信息，有效防止恶意软件截获身份证件信息被替换和篡改的问题，同时，通过可信执行环境 TEE 安全访问电子设备的摄像头，确保用于对比认证的用户图像的准确性，防止注入伪造人脸面部图像或视频的行为。

基于此，下面对上述步骤进行详细说明，具体如下所示：

首先，涉及步骤 320，本公开实施例提供了以下至少两种方式，获取身份证件的用户的待认证身份信息，具体如下所示。

在一些可能的实施例中，步骤 320 具体可以包括：

响应于第一输入，

在数据交互环境满足预设交互环境、且在可信执行环境下，通过近场通信读取近场通信芯片，获取近场通信芯片的标签内容和用户身份标识；

基于标签内容和用户身份标识，生成用户的待认证身份信息。

进一步地，在通过近场通信读取近场通信芯片，获取近场通信芯片的标签内容和用户身份标识的步骤之前，该信息处理方法还包括：

检测与近场通信芯片的数据交互环境，数据交互环境包括电子设备与近场通信芯片的距离值和在预设距离内电子设备与近场通信芯片的接触时长；

在距离值满足预设距离值和/或接触市场满足预设接触时长时，确定数据交互环境满足预设交互环境。

在另一些可能的实施例中，响应于第一输入，在可信执行环境下，确定目标近场通信芯片，近场通信芯片与电子设备的数据交互环境满足预设近场通讯环境；

通过近场通信芯片与应用协议数据的预设对应关系，获取与目标近场通信芯片对应的目标应用协议数据；

根据目标应用协议数据，获取用户的待认证身份信息。

这里，为了保证用户的信息安全，本公开实施例提供了根据近场通信芯片与应用协议数据的预设对应关系，获取与目标近场通信芯片对应的目标应用协议数据。例如，若近场通信芯片为身份证件，且预设对应关系中表示该电子设备可以访问该身份证件图像中用户面部图像，则电子设备可以获取该身份证件图像中用户面部图像。同理，若预设对应关系中表示该电子设备可以访问身份证件号码、身份证件图像和身份证件用户身份信息，则电子设备可以获取身份证件号码、身份证件图像和身份证件用户身份信息，由此，可以根据用户的前期设定，获取其信息。

另外，本公开实施例中的近场通信芯片与应用协议数据的预设对应关系，可以通过如下步骤确定，即在通过近场通信芯片与应用协议数据的预设对应关系，获取与目标近场通信芯片对应的目标应用协议数据的步骤之前，本公开实施例提供的信息处理方法还包括：

向服务器发送权限请求，权限请求包括电子设备的身份信息，权限请求用于获取近场通信芯片的权限；

接收服务器发送的权限反馈信息，该权限反馈信息包括该电子设备与近场通信芯片进行通讯的权限；

根据权限反馈信息和用户的预先设定，得到近场通信芯片与应用协议数据的预设对应关系。

接着，涉及步骤 330，该步骤可以分为两个部分，即一部分为确定用于表征用户身份的目标信息，另一部分为获取拍摄的用户图像。基于此，分别对两个部分进行说明。

首先，本公开实施例中确定目标信息的过程如下所示，即根据用户的待认证身份信息，确定用于表征用户身份的目标信息，包括：

步骤 3301，根据待认证的身份信息，确定待认证的身份信息的身份信息明文数据。

进一步地，该步骤 3301 具体可以包括：

步骤 33011，向服务器发送身份认证请求，身份认证请求包括待认证的身份信息，身份认证请求用于请求服务器对待认证的身份信息进行解析，以得到待认证的身份信息的身份信息明文数据；

步骤 33012，接收服务器发送的身份认证反馈信息，身份认证反馈信息包括待认证的身份信息的身份信息明文数据。

步骤 3302，根据身份信息明文数据和目标信息数据解密授权凭证，确定第一生物特征信息。

这里，可以根据下述步骤，确定目标信息数据解密授权凭证，具体可以包括步骤 33021-步骤 33023。

步骤 33021，根据电子设备中的数字证书，生成设备公私密钥对。

步骤 33022，通过可信身份认证初始化接口向服务器发送用户身份认证初始化请求，用户身份认证初始化请求包括设备公私密钥对，用户身份认证初始化请求用于与服务器建立安全通信链接，并通过安全通信链接进行密钥交换。

其中，可以基于预存的服务器公钥，获取与服务器对应的可信身份认证初始化接口。

步骤 33023，接收服务器的用户身份认证初始化反馈信息，用户身份认证初始化反馈信息包括目标信息数据解密授权凭证。

需要说明的是，用户身份认证初始化请求还包括应用程序信息，应用程序信息包括下述中的至少一种：应用程序标识、签名证书信息和证书指纹信息，应用程序信息用于确定待认证身份信息的用户身份认证结果的执行环境。

由此，基于上述涉及的可能，本公开实施例中的步骤 3302 具体可以包括：向服务器发送生物特征信息请求，生物特征信息请求包括身份信息明文数据和目标信息数据解密授权凭证，生物特征信息请求用于请求服务器基于身份信息明文数据和目标信息数据解密授权凭证，确定第一生物特征信息；

接收服务器发送的生物特征反馈信息，生物特征反馈信息包括被设备公钥加密的第一生物特征信息。

需要说明的是，本公开实施例中考虑到有一些资源严重受限的物联网电子设备无法进行确定目标信息和对比结果。这样，可以在执行向服务器发送身份认证请求步骤之前，方法还包括：

向服务器发送电子设备的身份标识，电子设备的电子标识用于确定电子设备是否满足身份认证的条件；

接收服务器发送的身份标识反馈信息；

在身份标识反馈信息表征电子设备未满足身份认证的条件下，向服务器发送身份认证请求。

另外，本公开实施例除了上述基于用户的待认证身份信息读取和解析外，还有一个关键就是要将所解析出来的第一生物特征信息如身份证件图像中用户面部图像与身份证持有人的用户图像中的第二生物特征信息进行用户图像比对。在这一过程中，有一个关键问题亟待解决，那就是用户当前的面部信息与原先身份证件采集时的照片存在差异，这其中可能有时间因素也有当初人脸采集设备精度不高甚至是用户面部受过伤害等各种问题。故此，需要对所解析身份证件图像中用户面部图像及持有人的用户图像中的面部信息进下优化。

针对于此，本公开实施例中除了按照图像去模糊对比方法外，还提出了一种对图片清晰度不敏感的特征模型即目标身份证件人像特征模型用于优化人脸对比的错误拒绝率（false reject rate，FRR）。

基于此，涉及该步骤 330 中的另一部分即获取用户图像的过程具体包括步骤 3311-步骤 3303。

步骤 3311，显示固定人像位置区域，固定人像位置区域用于获取用户与固定人像位置区域对应的人体部位图像。

举例说明，如图 6 所示，通过固定人像位置区域获取人体部位图像。这里，传统的人脸识别处理中，会选择较多的人脸特征点进行检测，同时也消耗了较多的性能资源。由于 TEE 资源有限，本公开实施例提出在电子设备人像采集界面使用固定人像位置，在人像采集界面勾画固定人像位置区域以匹配人脸最佳位置，同时舍弃一些人脸旋转对齐的特殊处理，以便快速定位人脸在图像中的位置，提高人脸特征点的定位精度。截取到人脸

区域后，选择人脸特征明显的特征点进行检测，如双眼、鼻子、颧骨、嘴巴、下巴、额头特征点进行检测，以便降低人脸对比的 FRR，使得 TEE 环境能够满足人脸旋转对齐等方面处理的性能消耗。

步骤 3312，在接收到用户拍摄图像的第二输入时，获取待处理的人体部位图像。

进一步地，通过固定位置区域，从人体部位中的多个特征点筛选目标特征点，根据目标特征点，获取与目标特征点对应的人体部位图像。

这样，在人像采集界面勾画固定人像位置区域以匹配人脸最佳位置时，可以舍弃一些人脸旋转的特征点，以便快速定位人脸在图像中的位置，提高人脸特征点的定位精度。

步骤 3313，对待处理的人体部位图像进行灰度归一化处理，得到用户图像。

进一步地，获取待处理的人体部位图像的第一灰度值，第一灰度值与第一灰度级对应，根据第一灰度级通过灰度拉伸，调整待处理的人体部位图像，得到具有第一灰度级的用户图像。

这里，可以对拍摄的用户图像中的人脸照片做灰度归一化处理。灰度归一化处理就是对用户图像进行光照补偿处理，以克服光照变化的影响，本公开实施例中可以利用灰度拉伸的方法将原图像中的灰度分布扩展到具有整个灰度级的图像。例如，采集到的图像是 8 位的灰度图像，应有 256 个灰度级，但往往由于采集时光照等因素的影响，图像的灰度级集中在一个或者几个灰度级区段，这时可以采用灰度拉伸的方法将图像扩展到 256 个灰度级。由此，拍摄到的人脸照片完成光照补偿处理、按色阶映射后，照片变得更加明朗鲜明，更有利于图像对比。

进一步地，在灰度归一化操作时，根据用户图像的 RGB 色彩模式进行灰度归一化处理，按照如下两个公式：

（1）亮度由公式（1）确定：

D=R*0.3086 + G*0.6094 + B*0.0820 （1）

其中，D 为亮度，R 为红色 red 的色彩通道，G 为绿色 green 的色彩通道，B 为蓝色 blue 的色彩通道。

（2）色阶映射由公式（2）确定：

D' = 0 + (D - 255*LOW) / (255*HIGH - 255*LOW) * 255 （2）

其中，D'为色阶，255*LOW 和 255*HIGH 分别是用户图像的原图像直方图中 D 的最低点和 D 的最高点。

如图 7 所示，根据原图像直方图做初步筛选，对像素点的分布明显不正常如主要分布在 x 轴左边、主要分布在 x 轴右边、主要分布在一个很窄的区间的图像，直接视为低质量照片，不做后续处理。图像直方图都是灰度图像，x 轴是灰度值（一般是 0~255），y 轴式图像中每一个灰度级对应的像素点的个数。

然后，涉及步骤 340，基于步骤 330 中获取的用户图像，在一些实施例中，在步骤 340 之前，在第一生物特征信息包括身份证件图像的情况下，通过几何归一化对比身份证件图像和用户图像，得到第一生物特征信息与第二生物特征信息的对比结果。

这样，针对身份证件上的第一生物特征信息如人像图片像素较小识别度不高的问题，本提案通过采用几何归一化处理和灰度归一化变换的方式对采集到的活体照片进行处理，提升了人脸照片与身份证上图像照片比对的识别率，改善了人脸对比的错误拒绝率（False Reject Rate，FRR）。

进一步地，该步骤具体可以包括步骤 3401-步骤 3403。

步骤 3401，识别身份证件图像中的用户面部区域，得到与用户面部区域对应的用户面部图像。

步骤 3402，对用户面部图像或者用户图像中的面部区域进行等比放大或者缩小，并计算用户图像和用户面部图像的特征值。

步骤 3403，根据至少一个特征值，得到第一生物特征信息与第二生物特征信息的对比结果。

举例说明，使用几何归一化算法对比第一生物特征信息与第二生物特征信息。可信身份服务平台中的人脸认证对比模块对身份证件图像通过定位人脸特征模型找到身份证件图像中用户面部区域，按照几何归一化算法确定用户图像中面部位置，比较两者的特征值，在确定用户图像中面部位置的过程中，使用等比放大和缩小活体人脸照片中人脸的几何图形做对

比。进一步地，几何归一化算法就是指根据对比目标定位结果将身份证件图像中用户面部区域中的用户图像中面部位置变化到同一位置和大小。本公开实施例提供的对比步骤包括：

步骤 1，通过人脸模型匹配找出身份证件图像中人物的两眼和鼻子所在的区域；

步骤 2，设定两眼之间的距离为 D，其中心点为 O；

步骤 3，根据人脸面部特点和几何模型确定矩形特征区域，以 O 为中心原点，两眼直线所在为 x 轴，两边各裁剪距离 d，其中 d=D/2，y 轴鼻子方向裁剪 1.5d，另一方向裁剪 0.5d，最后裁剪出一个正方形区域；

步骤 4，通过同样的人脸模型匹配找出用户图像中的两眼和鼻子所在的区域；

步骤 5，设定用户图像中两眼的距离为 D’，其中心点为 O’；

步骤 6，根据人脸面部特点和几何模型确定矩形特征区域，以 O’ 为中心原点，两眼直线所在为 x 轴，两边各裁剪距离 d’，其中 d’=D’/2，y 轴鼻子方向裁剪 1.5d’，另一方向裁剪 0.5d’，最后裁剪出一个正方形区域；

步骤 7，通过等比拉伸或缩放的方式如拉伸比例 V=D’/D，缩放比例 V’=D/D’，使裁剪的身份证件图像和裁剪的用户图像大小一致；

步骤 8，提取两张裁剪区域图片的特征值进行对比，根据两者特征值相等指数，转换成相似度作为第一生物特征信息与第二生物特征信息的对比结果。

需要说明的是，本公开实施例中涉及的对比图像的过程可以如上述步骤 1-步骤 8 所示，这里，可以通过目标身份证件人像特征模型确定两者的对比结果，即进一步地，将至少一个特征值输入到目标身份证件人像特征模型中，得到第一生物特征信息与第二生物特征信息的对比结果。另外，在一些可能的实施例中，可以确定上述涉及的目标身份证件人像特征模型进行确定，具体过程如下所示，由于身份证件图像照片较小、图像分辨率低，为了提高目标身份证件人像特征模型的比对精度，重点选择人脸特征明显的点，舍弃低分辨率下容易误检的特征点，同时辅以大量的身份证图像样本训练，并在每一次人脸比对得到比对结果后，选择相似度超过 N%

（N 为正数，可以根据应用场景进行自定义配置）的身份证人像特征值参与模型迭代训练，进而确定新的目标身份证件人像特征模型。

基于此，本公开实施例中还提供了一种确定目标身份证件人像特征模型的方式，具体如下所示：

根据目标身份证件中用户面部图像的训练特征值，对预设身份证件人像特征模型进行简化，得到目标身份证件人像特征模型。

基于步骤 340 中获取的用户图像，本公开实施例提供了一种确定第一生物特征信息与第二生物特征信息的对比结果的过程，具体如下所示，即在步骤 340 之前，该信息处理方法还包括：

通过对称密钥对第一生物特征信息和第二生物特征信息进行加密，得到加密生物特征信息；

向服务器发送身份认证结果请求，身份认证结果请求包括加密生物特征信息，身份认证结果请求用于请求服务器根据第一生物特征信息和第二生物特征信息，计算第一生物特征信息和第二生物特征信息的生物特征对比结果相似度；

接收服务器发送的身份认证结果反馈信息，身份认证结果反馈信息包括被设备公钥加密的生物特征对比结果相似度；

通过设备私钥加密对生物特征对比结果相似度进行解密，得到生物特征对比结果相似度，生物特征对比结果相似度用于表征第一生物特征信息与第二生物特征信息的对比结果。

基于此，该步骤 340 具体可以包括：在生物特征对比结果相似度满足预设相似度的情况下，确定 待认证身份信息的用户身份认证成功。

需要说明的是，本公开实施例中的目标信息还包括下述中的至少一项：身份证件号码、身份证件图像、身份证件用户身份信息如身份证件中的用户姓名、性别、民族、出生日期、住址。第一生物特征信息包括下述中的至少一项：身份证件图像中用户面部图像、与身份证件对应的用户的虹膜图像。

由此，本公开实施例提出一种基于 TEE 和 NFC 的可信身份认证的信息处理方法，可以通过 TEE 安全访问 NFC 进行身份证件的待认证的身份

信息识读的方式以获取可靠可信的用于表征用户身份的目标信息，以及在一些实施例中可以在可信执行环境 TEE 中与服务器中运行可信身份服务平台进行交互，以避免伪造身份证的问题，同时也避免了因拍照效果不佳造成获取到的目标信息不准确，提高身份认证的准确性。通过将待认证的身份信息对应的目标信息数据解密授权凭证迁移至 TEE 中，杜绝了待认证的身份信息在电子设备和服务器交互过程中可能被木马病毒窃取的问题。另外，通过从 TEE 内安全访问摄像头，确保用于对比认证的用户图像即实时的用户图像的源头可信，防止注入伪造人脸照片或视频的行为。

另外，针对一些支持 TEE 和 NFC 的物联网电子设备硬件资源严重受限的问题，本公开实施例利用第四代移动通信技术（the 4th generation mobile communication technology，4G）、第五代移动通信技术（5th generation mobile networks，5G）传输速率更高时延更低的特性，将 NFC 与二代身份证交互的命令进行了拆分，通过近场通信获取用户的待认证身份信息的部分在电子设备实现，主要处理身份证件 APDU 请求响应和交互协议，后端部分移至服务器运行，主要负责身份证件访问 APDU 指令的生成、组装和 APDU 响应的处理。通过上述前后端分离处理的方式，减少了电子设备的 NFC 交互协议的空间占比，对于可穿戴设备等资源比较有限的物联网终端设备，具有更强的适用性。通过电子设备的类别，确定在电子设备和服务器确定对比结果方式，保证了身份证识读和人脸比对功能在电子设备 TEE 空间资源有限的情况下的可用性和适配性。

以上，采用 TEE 安全访问 NFC 识读用户的待认证身份信息的方式确保获取的身份证信息的数据源真实准确，起到防伪身份证效果，同时可信执行环境 TEE 防止恶意软件截获身份证信息数据被替换和篡改。另外，本公开实施例是基于电子设备 TEE 和服务器之间的安全闭环实现的，能够确保信息是密文上送可信身份认证后台解密再以安全 TEE 安全通道传送回来使用的，适用于更多的身份认证场景。

为了更好的说明上述信息处理方法，本公开实施例结合图 1 和 2 所示的架构对信息处理方法进行详细说明。下述示例可以通过图 8 和图 9 两个过程对信息处理方法进行说明，其中，图 8 为本公开实施例提供的可信身

份认证初始化的过程，图 9 为本公开实施例提供的可信身份认证对比的过程，具体如下所示。

在第三方应用程序如消费类应用程序时，第三方应用程序需事先集成可信身份认证服务 SDK，并在第三方应用程序运行的电子设备上安装可信身份认证服务控件，以及通过该电子设备对应的可信应用管理（TAM）安装可信身份认证服务 TA 到设备 TEE 可信执行环境中。随后，还需在可信身份服务平台录入第三方应用程序的的应用程序标识（AppId）、签名证书信息和证书指纹信息。

如图 8 所示，该资源处理方法中可信身份认证初始化的过程可以包括步骤 801-步骤 813，具体如下所示。

步骤 801，电子设备接收用户针对应用程序 A 发起的可信身份认证初始化的操作。

步骤 802，应用程序 A 向集成的可信身份认证服务 SDK 发起可信身份认证初始化请求，传入交易要素 Context 上下文。这里，交易要素详见表 4。

步骤 803，可信身份认证服务 SDK 通过 Context 上下文，获取到应用程序 A 的 AppId、签名证书信息和证书指纹信息，调用可信身份认证服务控件的可信身份认证初始化接口，传入交易要素应用程序 A 的 AppId、签名证书信息和证书指纹信息。

步骤 804，可信身份认证服务控件调用可信身份认证服务 TA 初始化接口，传入交易要素 AppId、签名证书信息和证书指纹信息。

步骤 805，可信身份认证服务 TA 根据设备根信任证书生成一对设备公私密钥对。

步骤 806，可信身份认证服务 TA 请求可信身份服务平台，传入应用程序 A 的 AppId、签名证书信息和证书指纹信息。

步骤 807，可信身份认证服务 TA 中预置了可信身份服务平台的服务器公钥。可信身份认证服务 TA 通过服务器公钥与可信身份服务平台建立安全链接，使用设备公钥和信身份服务平台的服务器公钥进行会话密钥协商，后续使用协商的会话密钥进行交互。

可信身份认证服务 TA 把应用程序 A 的 AppId、签名证书信息和证书指纹信息使用会话密钥加密，传输到可信身份服务平台。

步骤 808，可信身份服务平台使用会话密钥解密，验证应用程序 A 的 AppId、签名证书信息和证书指纹信息与事先录入在可信身份服务平台中的是否一致，在验证通过时，可以向可信身份认证服务 TA 返回使用设备公钥加密的身份鉴别平台如共公安部下属机构身份认证服务的目标信息数据解密授权凭证的密文。

步骤 809，可信身份认证服务 TA 收到响应后，验证接收到的目标信息数据解密授权凭证的密文所在报文的有效性。在验证有效的情况下，通过设备私钥解密身份鉴别平台的目标信息数据解密授权凭证的密文，保存身份鉴别平台的目标信息数据解密授权凭证到可信身份认证服务 TA 中。

步骤 810，可信身份认证服务 TA 向可信身份认证服务控件返回与可信身份认证初始化的操作对应的操作结果。

步骤 811，可信身份认证服务控件向可信身份认证服务 SDK 返回与可信身份认证初始化的操作对应的操作结果。

步骤 812，可信身份认证服务 SDK 向应用程序 A 返回可信身份认证初始化结果。

步骤 813，应用程序 A 通过电子设备向用户展示可信身份认证初始化结果。

基于上述完成可信身份认证初始化或者注册后，结合图 9，对本公开实施例提供的资源处理方法中可信身份认证对比的过程进行详细说明。

如图 9 所示，该资源处理方法中可信身份认证对比的过程以包括步骤 901-步骤 916，具体如下所示。

步骤 901，电子设备接收用户针对应用程序 A 发起的可信身份认证的对比操作。

步骤 902，应用程序 A 向集成的可信身份认证服务 SDK 发起可信身份认证对比请求，传入交易要素待认证身份信息 UserId 如交易要素详见图 4。

步骤 903，可信身份认证服务 SDK 调用可信身份认证服务控件认证对

比接口，传入交易要素待认证身份信息 UserId。

步骤 904，可信身份认证服务控件调用可信身份认证服务 TA 认证对比接口。

步骤 905，可信身份认证服务 TA 访问设备 NFC 模块，以使电子设备显示刷身份证界面。

步骤 906，电子设备获取近场通信芯片中的待认证身份信息，NFC 模块将待认证身份信息响应给可信身份认证服务 TA，可信身份认证服务 TA 把待认证身份信息发送到权威身份认证模块如公安部下属机构身份认证服务平台。

步骤 907，权威身份认证模块处理接收到的待认证身份信息，把处理后的待认证身份信息明文数据返回给可信身份认证服务 TA。

步骤 908，可信身份认证服务 TA 把权威身份认证模块的目标信息数据解密授权凭证和待认证身份信息的信息明文发送到可信身份服务平台。

步骤 909，可信身份服务平台通过权威身份认证模块得到目标信息，目标信息包括身份证件图像中用户面部图像，使用设备公钥加密后，返回给可信身份认证服务 TA。

步骤 910，可信身份认证服务 TA 安全访问电子设备的摄像头获取用户图像。

步骤 911，可信身份认证服务 TA 将身份证件图像中用户面部图像和使用设备私钥解密的用户图像使用对称密钥加密提交给可信身份服务平台。

步骤 912，可信身份服务平台使用对称密钥解密得到用户图像中的人脸图像，按照用户图像中的人脸图像和身份证件图像中用户面部图像预处理过程对比两张图像，返回使用设备公钥加密的生物特征对比结果相似度。

步骤 913，可信身份认证服务 TA 使用设备私钥解密出生物特征对比结果相似度，返回给可信身份认证服务控件。

步骤 914，可信身份认证服务控件向可信身份认证服务 SDK 返回生物特征对比结果相似度。

步骤 915，可信身份认证服务 SDK 向应用程序 A 返回生物特征对比结果相似度。

步骤 916，应用程序 A 向用户显示与生物特征对比结果相似度对应的待认证身份信息的用户身份认证结果。

需要说明的是，基于可信身份认证服务操作的生命周期可以包括可信身份认证服务初始化功能、可信身份认证服务注册功能、可信身份认证功能、可信身份人证对比功能和可信身份认证服务注销功能，其中，可以先进行可信身份认证服务初始化，初始化验证通过，则可以进行可信身份认证注册、可信身份人证对比和可信身份认证注销操作。

由此，本公开实施例提出一种基于 TEE 和 NFC 的可信身份认证的信息处理方法，可以通过 TEE 安全访问 NFC 进行身份证件的待认证的身份信息识读的方式以获取可靠可信的用于表征用户身份的目标信息，以及在一些实施例中可以在可信执行环境 TEE 中与服务器中运行可信身份服务平台进行交互，以避免伪造身份证的问题，同时也避免了因拍照效果不佳造成获取到的目标信息不准确，提高身份认证的准确性。通过将待认证的身份信息对应的目标信息数据解密授权凭证迁移至 TEE 中，杜绝了待认证的身份信息在电子设备和服务器交互过程中可能被木马病毒窃取的问题。另外，通过从 TEE 内安全访问摄像头，确保用于对比认证的用户图像即实时的用户图像的源头可信，防止注入伪造人脸照片或视频的行为。

另外，针对一些支持 TEE 和 NFC 的物联网电子设备硬件资源严重受限的问题，本公开实施例利用第四代移动通信技术（the 4th generation mobile communication technology，4G）、第五代移动通信技术（5th generation mobile networks，5G）传输速率更高时延更低的特性，将 NFC 与二代身份证交互的命令进行了拆分，其中，通过近场通信获取用户的待认证身份信息的部分在电子设备实现，主要处理身份证件 APDU 请求响应和交互协议，后端部分移至服务器运行，主要负责身份证件访问 APDU 指令的生成、组装和 APDU 响应的处理。通过上述前后端分离处理的方式，减少了电子设备的 NFC 交互协议的空间占比，对于可穿戴设备等资源比较有限的物联网终端设备，具有更强的适用性。通过电子设备的类别，确定

在电子设备和服务器确定对比结果方式，保证了身份证识读和人脸比对功能在电子设备 TEE 空间资源有限的情况下的可用性和适配性。

以上，采用 TEE 安全访问 NFC 识读用户的待认证身份信息的方式确保获取的身份证信息的数据源真实准确，起到防伪身份证效果，同时可信执行环境 TEE 防止恶意软件截获身份证信息数据被替换和篡改。另外，本公开实施例是基于电子设备 TEE 和服务器之间的安全闭环实现的，能够确保信息是密文上送可信身份认证后台解密再以安全 TEE 安全通道传送回来使用的，适用于更多的身份认证场景。

基于相同的发明构思，本公开还提供了一种信息处理装置。具体结合图 10 进行详细说明。

图 10 是根据本公开提供的基于电子设备的信息处理装置的一个实施例结构示意图。

在本公开一些实施例中，图 10 所示装置可以设置于如图 1 所示的电子设备中。

其中，如图 10 所示，该信息处理装置 100 具体可以包括：

接收模块 1001，用于接收对用户身份认证的第一输入；

获取模块 1002，用于响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

处理模块 1003，用于根据用户的待认证身份信息，确定用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息，以及在预设时间段内获取拍摄的用户图像，用户图像包括用户的第二生物特征信息；

确定模块 1004，用于基于第一生物特征信息与第二生物特征信息的对比结果，确定待认证身份信息的用户身份认证结果。

由此，通过在可信执行环境 TEE 和近场通信 NFC 获取用户的待认证身份信息的方式，来获取可信任的用于表征用户身份的目标信息如身份证件信息，以避免伪造身份证件的问题，同时也避免了因拍照效果不佳或者拍摄硬件不足造成获取到的目标信息不准确，从而导致用户身份认证结果不正确的问题。

另外，通过在可信执行环境 TEE 中获取目标信息和对比目标信息中的

第一生物特征信息和拍摄的用户图像中的第二生物特征信息，有效防止恶意软件截获身份证件信息被替换和篡改的问题，同时，通过可信执行环境 TEE 安全访问电子设备的摄像头，确保用于对比认证的用户图像的准确性，防止注入伪造人脸面部照片或视频的行为。

下面分别对本公开实施例中信息处理装置 100 进行详细说明。

在本公开一些实施例中，获取模块 1002 具体可以用于，响应于第一输入，在数据交互环境满足预设交互环境、且在可信执行环境下，通过近场通信读取近场通信芯片，获取近场通信芯片的标签内容和用户身份标识，

基于标签内容和用户身份标识，生成用户的待认证身份信息。

进一步地，信息处理装置 100 还可以包括检测模块，用于检测与近场通信芯片的数据交互环境，数据交互环境包括电子设备与近场通信芯片的距离值和/或在预设距离内电子设备与近场通信芯片的接触时长，在距离值满足预设距离值和/或接触市场满足预设接触时长时，确定数据交互环境满足预设交互环境。

另外，获取模块 1002 具体可以用于，响应于第一输入，在可信执行环境下，确定目标近场通信芯片，近场通信芯片与电子设备的数据交互环境满足预设近场通讯环境，通过近场通信芯片与应用协议数据的预设对应关系，获取与目标近场通信芯片对应的目标应用协议数据，根据目标应用协议数据，获取用户的待认证身份信息。

在本公开一些实施例中，本公开实施例中的处理模块 1003 具体可以用于，根据待认证的身份信息，确定待认证的身份信息的身份信息明文数据，根据身份信息明文数据和目标信息数据解密授权凭证，确定第一生物特征信息。

进一步地，本公开实施例中信息处理装置 100 还可以包括发送模块。基于此，发送模块，用于向服务器发送身份认证请求，身份认证请求包括待认证的身份信息，身份认证请求用于请求服务器对待认证的身份信息进行解析，以得到待认证的身份信息的身份信息明文数据。

本公开实施例中的接收模块 1001，接收服务器发送的身份认证反馈信

息，身份认证反馈信息包括待认证的身份信息的身份信息明文数据。

在一些可能的实施例中，本公开实施例中的发送模块还可以用于，向服务器发送电子设备的身份标识，电子设备的电子标识用于确定电子设备是否满足身份认证的条件。

本公开实施例中的接收模块 1001 还用于，接收服务器发送的身份标识反馈信息。

本公开实施例中的发送模块还可以用于，在身份标识反馈信息表征电子设备未满足身份认证的条件下，向服务器发送身份认证请求。

在一些可能的实施例中，本公开实施例中信息处理装置 100 还可以包括生成模块，用于根据电子设备中的数字证书，生成设备公私密钥对。基于此，本公开实施例中的发送模块还可以用于，通过可信身份认证初始化接口向服务器发送用户身份认证初始化请求，用户身份认证初始化请求包括设备公私密钥对，用户身份认证初始化请求用于与服务器建立安全通信链接，并通过安全通信链接进行密钥交换。本公开实施例中的接收模块 1001 还用于，接收服务器的用户身份认证初始化反馈信息，用户身份认证初始化反馈信息包括目标信息数据解密授权凭证。

在一些可能的实施例中，本公开实施例中的获取模块还可以用于，基于服务器公钥，获取与服务器对应的可信身份认证初始化接口。

本公开实施例中的用户身份认证初始化请求还包括应用程序信息，应用程序信息包括下述中的至少一种：应用程序标识、签名证书信息和证书指纹信息，其中，应用程序信息用于确定待认证身份信息的用户身份认证结果的执行环境。

在一些可能的实施例中，本公开实施例中的处理模块 1003 具体可以用于向服务器发送生物特征信息请求，生物特征信息请求包括身份信息明文数据和目标信息数据解密授权凭证，生物特征信息请求用于请求服务器基于身份信息明文数据和目标信息数据解密授权凭证，确定第一生物特征信息，接收服务器发送的生物特征反馈信息，生物特征反馈信息包括被设备公钥加密的第一生物特征信息。

在一些可能的实施例中，本公开实施例中信息处理装置 100 还可以包

括显示模块，用于显示固定人像位置区域，固定人像位置区域用于获取用户与固定人像位置区域对应的人体部位图像。本公开实施例中的获取模块 1002 具体可以用于，在接收到用户拍摄图像的第二输入时，通过固定位置区域获取待处理的人体部位图像。本公开实施例中的处理模块 1003 具体可以用于，对待处理的人体部位图像进行灰度归一化处理，得到用户图像。

其中，本公开实施例中的获取模块 1002 具体可以用于，通过固定位置区域，从人体部位中的多个特征点筛选目标特征点，根据目标特征点，获取与目标特征点对应的人体部位图像。

本公开实施例中的处理模块 1003 具体可以用于，获取待处理的人体部位图像的第一灰度值，第一灰度值与第一灰度级对应，根据第一灰度级通过灰度拉伸，调整待处理的人体部位图像，得到具有第一灰度级的用户图像。

在一些可能的实施例中，本公开实施例中的确定模块 1004 具体可以用于，在第一生物特征信息包括身份证件图像的情况下，通过几何归一化对比身份证件图像和用户图像，得到第一生物特征信息与第二生物特征信息的对比结果。

其中，本公开实施例中的确定模块 1004 具体可以用于，识别身份证件图像中的用户面部区域，得到与用户面部区域对应的用户面部图像，对用户面部图像或者用户图像中的面部区域进行等比放大或者缩小，并计算用户图像和用户面部图像的特征值，根据至少一个特征值，得到第一生物特征信息与第二生物特征信息的对比结果。

进一步地，本公开实施例中的确定模块 1004 具体可以用于，将至少一个特征值输入到目标身份证件人像特征模型中，得到第一生物特征信息与第二生物特征信息的对比结果。

在一些可能的实施例中，本公开实施例中信息处理装置 100 还可以包括简化模块，用于根据目标身份证件中用户面部图像的训练特征值，对预设身份证件人像特征模型进行简化，得到目标身份证件人像特征模型。本公开实施例中信息处理装置 100 还可以包括加密模块，用于通过对称密钥

对第一生物特征信息和第二生物特征信息进行加密，得到加密生物特征信息。

本公开实施例中的发送模块还用于，向服务器发送身份认证结果请求，身份认证结果请求包括加密生物特征信息，身份认证结果请求用于请求服务器根据第一生物特征信息和第二生物特征信息，计算第一生物特征信息和第二生物特征信息的生物特征对比结果相似度。

本公开实施例中的接收模块 1001 还用于，接收服务器发送的身份认证结果反馈信息，身份认证结果反馈信息包括被设备公钥加密的生物特征对比结果相似度。

本公开实施例中的处理模块 1003 还用于，通过设备私钥加密对生物特征对比结果相似度进行解密，得到生物特征对比结果相似度，生物特征对比结果相似度用于表征第一生物特征信息与第二生物特征信息的对比结果。

在一些可能的实施例中，本公开实施例中的确定模块 1004 具体可以用于，在生物特征对比结果相似度满足预设相似度的情况下，确定 待认证身份信息的用户身份认证成功。

需要说明的是，上述涉及的目标信息还包括下述中的至少一项：身份证件号码、身份证件图像。第一生物特征信息包括下述中的至少一项：身份证件图像中用户面部图像、与身份证件对应的用户的虹膜图像。

由此，通过在可信执行环境 TEE 和近场通信 NFC 获取用户的待认证身份信息的方式，来获取可信任的用于表征用户身份的目标信息如身份证件信息，以避免伪造身份证件的问题，同时也避免了因拍照效果不佳或者拍摄硬件不足造成获取到的目标信息不准确，从而导致用户身份认证结果不正确的问题。

另外，通过在可信执行环境 TEE 中获取目标信息、对比目标信息中的第一生物特征信息和拍摄的用户图像中的第二生物特征信息，有效防止恶意软件截获身份证件信息被替换和篡改的问题，同时，通过可信执行环境 TEE 安全访问电子设备的摄像头，确保用于对比认证的用户图像的准确性，防止注入伪造人脸面部照片或视频的行为。

需要说明的是，图 10 所示的信息处理装置 100 可以执行图 1-图 9 所示的信息处理方法实施例中的各个步骤，并且实现图 1-图 9 所示的方法实施例中的各个过程和效果，在此不做赘述。

基于相同的发明构思，本公开还提供了一种基于电子设备如可穿戴式设备、智能门锁等无法承载计算量较大的信息处理设备。具体结合图 11 进行详细说明。

图 11 是根据本公开提供的基于电子设备的信息处理装置的另一个实施例结构示意图。

在本公开一些实施例中，图 11 所示装置可以设置于可穿戴式设备、智能门锁等无法承载计算量较大的信息处理设备中。

其中，如图 11 所示，该信息处理装置 1100 具体可以包括：

接收模块 1110，用于接收对用户身份认证的第一输入；

获取模块 1120，用于响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

发送模块 1130，用于向服务器发送用户的待认证身份信息，用户的待认证身份信息用于确定待认证身份信息的用户身份认证结果；

发送模块 1130 还用于，在预设时间段内获取用户图像，并向服务器发送用户图像，用户图像用于与用户的待认证身份进行对比，以确定用户身份认证结果；

接收模块 1110 还用于，接收服务器发送的待认证身份信息的用户身份认证结果。

此外，本公开实施例提供的获取模块 1120 具体用于，在可信执行环境下，通过执行协议数据指令集中近场通讯的指令，获取用户的待认证身份信息；其中，近场通讯的指令由服务器确定。

基于相同的发明构思，本公开还提供了一种服务器。具体结合图 12 进行详细说明。

图 12 是根据本公开提供的基于服务器的信息处理装置的一个实施例结构示意图。

在本公开一些实施例中，如图 12 所示，该信息处理装置 1200 具体可

以包括：

接收模块 1210，用于接收电子设备发送的用户的待认证身份信息；

获取模块 1220，用于在检测到用户的待认证身份信息用于确定待认证身份信息的用户身份认证结果时，获取与用户的待认证身份信息对应且用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息；

接收模块 1210 还用于，接收电子设备发送的用户图像；

确定模块 1230，用于基于第一生物特征信息与用户图像中的第二生物特征信息的对比结果，确定待认证身份信息的用户身份认证结果；

发送模块 1240 还用于，向电子设备发送用户身份认证结果。

其中，本公开实施例中的获取模块 1220 具体用于，根据待认证身份信息的密文信息，确定协议数据指令，协议数据指令用于指示按照身份证件属性格式拼接组装成的用于表征用户身份的目标信息的原文字符串，根据预存的目标信息数据解密授权凭证和目标信息的原文字符串，对待认证的身份信息进行解密，得到目标信息。

进一步地，发送模块 1230 还可以用于，向身份鉴别服务器发送协议数据指令，协议数据指令用于指示身份鉴别服务器按照身份证件属性格式拼接组装成的用于表征用户身份的目标信息的原文字符串。基于此，接收模块 1210 还可以用于，接收身份鉴别服务器发送的目标信息的原文字符串。

基于相同的发明构思，本公开还提供了一种信息处理设备。具体结合图 13 进行详细说明。

图 13 示出了本公开实施例提供的信息处理设备的硬件结构示意图。

如图 13 所示，该信息处理 1300 可以包括本公开实施例中涉及的电子设备或者服务器。信息处理 1300 可以包括处理器 1301 和存储有计算机程序指令的存储器 1302。

具体地，上述处理器 1301 可以包括中央处理器（CPU），或者特定集成电路（Application Specific Integrated Circuit，ASIC），或者可以被配置成实施本公开实施例的一个或多个集成电路。

存储器 1302 可以包括用于数据或指令的大容量存储器。举例来说而

非限制，存储器 1302 可包括硬盘驱动器（Hard Disk Drive，HDD）、软盘驱动器、闪存、光盘、磁光盘、磁带或通用串行总线（Universal Serial Bus，USB）驱动器或者两个或更多个以上这些的组合。在合适的情况下，存储器 1302 可包括可移除或不可移除(或固定)的介质。在合适的情况下，存储器 1302 可在综合网关容灾设备的内部或外部。在特定实施例中，存储器 1302 是非易失性固态存储器。在特定实施例中，存储器 1302 包括只读存储器（ROM）。在合适的情况下，该 ROM 可以是掩模编程的 ROM、可编程 ROM（PROM）、可擦除 PROM（EPROM）、电可擦除 PROM（EEPROM）、电可改写 ROM（EAROM）或闪存或者两个或更多个以上这些的组合。

处理器 1301 通过读取并执行存储器 1302 中存储的计算机程序指令，以实现上述实施例中的任意一种信息处理方法。

在一个示例中，数据处理设备还可包括通信接口 1303 和总线 1310。其中，如图 13 所示，处理器 1301、存储器 1302、通信接口 1303 通过总线 1310 连接并完成相互间的通信。

通信接口 1303，主要用于实现本公开实施例中各模块、装置、单元和/或设备之间的通信。

总线 1310 包括硬件、软件或两者，将流量控制设备的部件彼此耦接在一起。举例来说而非限制，总线可包括加速图形端口（AGP）或其他图形总线、增强工业标准架构（EISA）总线、前端总线（FSB）、超传输（HT）互连、工业标准架构（ISA）总线、无限带宽互连、低引脚数（LPC）总线、存储器总线、微信道架构（MCA）总线、外围组件互连（PCI）总线、PCI-Express（PCI-X）总线、串行高级技术附件（SATA）总线、视频电子标准协会局部（VLB）总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线 1310 可包括一个或多个总线。尽管本公开实施例描述和示出了特定的总线，但本公开考虑任何合适的总线或互连。

该数据处理设备可以执行本公开实施例中的信息处理方法，从而实现结合图 1 至图 10 描述的信息处理方法和装置。

另外，结合上述实施例中的信息处理方法，本公开实施例可提供一种计算机可读存储介质来实现。该计算机可读存储介质上存储有计算机程序指令，该计算机程序指令被处理器执行时实现上述实施例中的任意一种信息处理方法。计算机可读存储介质的示例包括非暂态计算机可读存储介质，如只读存储器（Read-Only Memory，简称 ROM）、随机存取存储器（Random Access Memory，简称 RAM）、磁碟或者光盘等。

需要明确的是，本公开并不局限于上文所描述并在图中示出的特定配置和处理。为了简明起见，这里省略了对已知方法的详细描述。在上述实施例中，描述和示出了若干具体的步骤作为示例。但是，本公开的方法过程并不限于所描述和示出的具体步骤，本领域的技术人员可以在领会本公开的精神后，作出各种改变、修改和添加，或者改变步骤之间的顺序。

以上的结构框图中所示的功能块可以实现为硬件、软件、固件或者它们的组合。当以硬件方式实现时，其可以例如是电子电路、专用集成电路（ASIC）、适当的固件、插件、功能卡等等。当以软件方式实现时，本公开的元素是被用于执行所需任务的程序或者代码段。程序或者代码段可以存储在机器可读介质中，或者通过载波中携带的数据信号在传输介质或者通信链路上传送。“机器可读介质”可以包括能够存储或传输信息的任何介质。机器可读介质的例子包括电子电路、半导体存储器设备、ROM、闪存、可擦除 ROM（EROM）、软盘、CD-ROM、光盘、硬盘、光纤介质、射频（RF）链路，等等。代码段可以经由诸如因特网、内联网等的计算机网络被下载。

还需要说明的是，本公开中提及的示例性实施例，基于一系列的步骤或者装置描述一些方法或系统。但是，本公开不局限于上述步骤的顺序，也就是说，可以按照实施例中提及的顺序执行步骤，也可以不同于实施例中的顺序，或者若干步骤同时执行。

以上，仅为本公开的具体实施方式，所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、模块和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。应理解，本公开的保护范围并不局限于此，任何熟悉本技术领域的技术人员在

本公开揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本公开的保护范围之内。

权 利 要 求 书

1.一种信息处理方法，应用于电子设备，包括：

接收对用户身份认证的第一输入；

响应于所述第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

根据所述用户的待认证身份信息，确定用于表征用户身份的目标信息，所述目标信息包括用户的第一生物特征信息，以及在预设时间段内获取的用户图像，所述用户图像包括用户的第二生物特征信息；

基于所述第一生物特征信息与所述第二生物特征信息的对比结果，确定所述待认证身份信息的用户身份认证结果。

2.根据权利要求 1 所述的方法，其中，所述响应于所述第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息，包括：

响应于所述第一输入，

在所述数据交互环境满足预设交互环境、且在可信执行环境下，通过近场通信读取所述近场通信芯片，获取所述近场通信芯片的标签内容和用户身份标识；

基于所述标签内容和用户身份标识，生成所述用户的待认证身份信息。

3.根据权利要求 2 所述的方法，其中，所述通过近场通信读取所述近场通信芯片，获取所述近场通信芯片的标签内容和用户身份标识之前，所述方法还包括：

检测与所述近场通信芯片的数据交互环境，所述数据交互环境包括所述电子设备与所述近场通信芯片的距离值和/或在预设距离内所述电子设备与所述近场通信芯片的接触时长；

在所述距离值满足预设距离值和/或所述接触市场满足预设接触时长时，确定所述数据交互环境满足预设交互环境。

4.根据权利要求 1 所述的方法，其中，所述响应于所述第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息，包括：

响应于所述第一输入，在可信执行环境下，确定目标近场通信芯片，所述近场通信芯片与所述电子设备的数据交互环境满足预设近场通讯环境；

通过近场通信芯片与应用协议数据的预设对应关系，获取与所述目标近场通信芯片对应的目标应用协议数据；

根据所述目标应用协议数据，获取用户的待认证身份信息。

5.根据权利要求 1 所述的方法，其中，所述根据所述用户的待认证身份信息，确定用于表征用户身份的目标信息，包括：

根据所述待认证的身份信息，确定所述待认证的身份信息的身份信息明文数据；

根据所述身份信息明文数据和目标信息数据解密授权凭证，确定所述第一生物特征信息。

6.根据权利要求 5 所述的方法，其中，所述根据所述待认证的身份信息，确定所述待认证的身份信息的身份信息明文数据，包括：

向服务器发送身份认证请求，所述身份认证请求包括所述待认证的身份信息，所述身份认证请求用于请求所述服务器对所述待认证的身份信息进行解析，以得到所述待认证的身份信息的身份信息明文数据；

接收所述服务器发送的身份认证反馈信息，所述身份认证反馈信息包括所述待认证的身份信息的身份信息明文数据。

7.根据权利要求 6 所述的方法，其中，所述向服务器发送身份认证请求之前，所述方法还包括：

向所述服务器发送电子设备的身份标识，所述电子设备的电子标识用于确定所述电子设备是否满足身份认证的条件；

接收所述服务器发送的身份标识反馈信息；

在所述身份标识反馈信息表征所述电子设备未满足身份认证的条件下，向所述服务器发送身份认证请求。

8.根据权利要求 5 所述的方法，其中，所述确定所述第一生物特征信息之前，所述方法还包括：

根据所述电子设备中的数字证书，生成设备公私密钥对；

通过可信身份认证初始化接口向服务器发送用户身份认证初始化请求，所述用户身份认证初始化请求包括所述设备公私密钥对，所述用户身份认证初始化请求用于与所述服务器建立安全通信链接，并通过所述安全通信链接进行密钥交换；

接收所述服务器的用户身份认证初始化反馈信息，所述用户身份认证初始化反馈信息包括所述目标信息数据解密授权凭证。

9.根据权利要求 8 所述的方法，其中，所述通过可信身份认证初始化接口向服务器发送用户身份认证初始化请求之前，所述方法还包括：

基于服务器公钥，获取与所述服务器对应的可信身份认证初始化接口。

10.根据权利要求 9 所述的方法，其中，所述用户身份认证初始化请求还包括应用程序信息，所述应用程序信息包括下述中的至少一种：应用程序标识、签名证书信息和证书指纹信息，其中，所述应用程序信息用于确定所述待认证身份信息的用户身份认证结果的执行环境。

11.根据权利要求 5 或 6 所述的方法，其中，所述根据所述身份信息明文数据和目标信息数据解密授权凭证，确定所述第一生物特征信息，包括：

向所述服务器发送生物特征信息请求，所述生物特征信息请求包括所述身份信息明文数据和目标信息数据解密授权凭证，所述生物特征信息请求用于请求所述服务器基于所述身份信息明文数据和目标信息数据解密授权凭证，确定第一生物特征信息；

接收所述服务器发送的生物特征反馈信息，所述生物特征反馈信息包括被设备公钥加密的第一生物特征信息。

12.根据权利要求 1 所述的方法，其中，所述在预设时间段内获取拍摄的用户图像，包括：

显示固定人像位置区域，所述固定人像位置区域用于获取用户与固定人像位置区域对应的人体部位图像；

在接收到用户拍摄图像的第二输入时，通过所述固定位置区域获取待处理的人体部位图像；

对所述待处理的人体部位图像进行灰度归一化处理，得到所述用户图像。

13.根据权利要求 12 所述的方法，其中，所述通过所述固定位置区域获取待处理的人体部位图像，包括：

通过所述固定位置区域，从人体部位中的多个特征点筛选目标特征点；

根据所述目标特征点，获取与所述目标特征点对应的人体部位图像。

14.根据权利要求 13 所述的方法，其中，所述对所述待处理的人体部位图像进行灰度归一化处理，得到所述用户图像，包括：

获取所述待处理的人体部位图像的第一灰度值，所述第一灰度值与第一灰度级对应；

根据所述第一灰度级通过灰度拉伸，调整所述待处理的人体部位图像，得到具有所述第一灰度级的用户图像。

15.根据权利要求 12 所述的方法，其中，所述第一生物特征信息包括身份证件图像；所述确定所述待认证身份信息的用户身份认证结果之前，所述方法还包括：

通过几何归一化对比所述身份证件图像和所述用户图像，得到所述第一生物特征信息与所述第二生物特征信息的对比结果。

16.根据权利要求 15 所述的方法，其中，所述通过几何归一化对比所述身份证件图像和所述用户图像，得到所述第一生物特征信息与所述第二生物特征信息的对比结果，包括：

识别所述身份证件图像中的用户面部区域，得到与所述用户面部区域对应的用户面部图像；

对所述用户面部图像或者所述用户图像中的面部区域进行等比放大或者缩小，并计算所述用户图像和所述用户面部图像的特征值；

根据所述至少一个特征值，得到所述第一生物特征信息与所述第二生物特征信息的对比结果。

17.根据权利要求 16 所述的方法，其中，所述根据所述至少一个特征值，得到所述第一生物特征信息与所述第二生物特征信息的对比结果，包

括：

将所述至少一个特征值输入到目标身份证件人像特征模型中，得到所述第一生物特征信息与所述第二生物特征信息的对比结果。

18.根据权利要求 17 所述的方法，其中，所述得到所述第一生物特征信息与所述第二生物特征信息的对比结果之前，所述方法还包括：

根据目标身份证件中用户面部图像的训练特征值，对预设身份证件人像特征模型进行简化，得到目标身份证件人像特征模型。

19.根据权利要求 1 所述的方法，其中，所述确定所述待认证身份信息的用户身份认证结果之前，所述方法还包括：

通过对称密钥对所述第一生物特征信息和所述第二生物特征信息进行加密，得到加密生物特征信息；

向服务器发送身份认证结果请求，所述身份认证结果请求包括所述加密生物特征信息，所述身份认证结果请求用于请求所述服务器根据第一生物特征信息和所述第二生物特征信息，计算所述第一生物特征信息和所述第二生物特征信息的生物特征对比结果相似度；

接收所述服务器发送的身份认证结果反馈信息，所述身份认证结果反馈信息包括被设备公钥加密的生物特征对比结果相似度；

通过设备私钥加密对生物特征对比结果相似度进行解密，得到所述生物特征对比结果相似度，所述生物特征对比结果相似度用于表征所述第一生物特征信息与所述第二生物特征信息的对比结果。

20.根据权利要求 19 所述的方法，其中，所述基于所述第一生物特征信息与所述第二生物特征信息的对比结果，确定所述待认证身份信息的用户身份认证结果，包括：

在所述生物特征对比结果相似度满足预设相似度的情况下，确定所述待认证身份信息的用户身份认证成功。

21.根据权利要求 1 所述的方法，其中，所述目标信息还包括下述中的至少一项：身份证件号码、身份证件图像、身份证件用户身份信息；所述第一生物特征信息包括下述中的至少一项：所述身份证件图像中用户面部图像、与所述身份证件对应的用户的虹膜图像。

22.一种信息处理方法，应用于电子设备，包括：

接收对用户身份认证的第一输入；

响应于所述第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

向服务器发送所述用户的待认证身份信息，所述用户的待认证身份信息用于确定所述待认证身份信息的用户身份认证结果；

在预设时间段内获取用户图像，并向所述服务器发送所述用户图像，所述用户图像用于与所述用户的待认证身份进行对比，以确定所述用户身份认证结果；

接收服务器发送的所述待认证身份信息的用户身份认证结果。

23.根据权利要求 22 所述的方法，其中，所述在可信执行环境下，通过近场通信获取用户的待认证身份信息，包括：

在可信执行环境下，通过执行协议数据指令集中近场通讯的指令，获取用户的待认证身份信息；其中，所述近场通讯的指令由服务器确定。

24.一种信息处理方法，应用于服务器，包括：

接收电子设备发送的用户的待认证身份信息；

在检测到所述电子设备的设备类型为预设目标设备类型的情况下，获取与所述用户的待认证身份信息对应的且用于表征用户身份的目标信息，所述目标信息包括用户的第一生物特征信息；

接收所述电子设备发送的用户图像；

基于所述第一生物特征信息与所述用户图像中的第二生物特征信息的对比结果，确定所述待认证身份信息的用户身份认证结果；

向所述电子设备发送所述用户身份认证结果。

25.根据权利要求 24 所述的方法，其中，所述获取与所述用户的待认证身份信息对应的且用于表征用户身份的目标信息，包括：

根据所述待认证身份信息的密文信息，确定协议数据指令，所述协议数据指令用于指示按照身份证件属性格式拼接组装成的用于表征用户身份的目标信息的原文字符串；

根据预存的目标信息数据解密授权凭证和所述目标信息的原文字符

串，对待认证的身份信息进行解密，得到目标信息。

26.根据权利要求 25 所述的方法，其中，所述根据所述待认证身份信息的密文信息，确定协议数据指令，包括：

向身份鉴别服务器发送所述协议数据指令，所述协议数据指令用于指示所述身份鉴别服务器按照身份证件属性格式拼接组装成的用于表征用户身份的目标信息的原文字符串；

接收所述身份鉴别服务器发送的所述目标信息的原文字符串。

27.一种信息处理装置，应用于电子设备，包括：

接收模块，用于接收对用户身份认证的第一输入；

获取模块，用于响应于所述第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

处理模块，用于根据所述用户的待认证身份信息，确定用于表征用户身份的目标信息，所述目标信息包括用户的第一生物特征信息，以及在预设时间段内获取的用户图像，所述用户图像包括用户的第二生物特征信息；

确定模块，用于基于所述第一生物特征信息与所述第二生物特征信息的对比结果，确定所述待认证身份信息的用户身份认证结果。

28.一种信息处理装置，应用于电子设备，包括：

接收模块，用于接收对用户身份认证的第一输入；

获取模块，用于响应于所述第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息；

发送模块，用于向服务器发送所述用户的待认证身份信息，所述用户的待认证身份信息用于确定所述待认证身份信息的用户身份认证结果；

所述发送模块还用于在预设时间段内获取用户图像，并向所述服务器发送所述用户图像，所述用户图像用于与所述用户的待认证身份进行对比，以确定所述用户身份认证结果；

所述接收模块还用于接收服务器发送的所述待认证身份信息的用户身份认证结果。

29.一种信息处理装置，应用于服务器，包括：

接收模块，用于接收电子设备发送的用户的待认证身份信息；

获取模块，用于在检测到所述用户的待认证身份信息用于确定所述待认证身份信息的用户身份认证结果时，获取与所述用户的待认证身份信息对应且用于表征用户身份的目标信息，所述目标信息包括用户的第一生物特征信息；

所述接收模块还用于接收所述电子设备发送的用户图像；

确定模块，用于基于所述第一生物特征信息与所述用户图像中的第二生物特征信息的对比结果，确定所述待认证身份信息的用户身份认证结果；

发送模块，用于向所述电子设备发送所述用户身份认证结果。

30.一种电子设备，所述电子设备包括：处理器和存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 1-21 中任意一项所述信息处理方法或者如权利要求 22-23 中任一项所述信息处理方法。

31.一种服务器，所述服务器包括：处理器和存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 24-26 中任意一项所述信息处理方法。

32.一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现如权利要求 1-21 中任意一项所述信息处理方法，或者实现如权利要求 22-23 中任意一项所述信息处理方法，或者实现如权利要求 24-26 中任意一项所述信息处理方法。

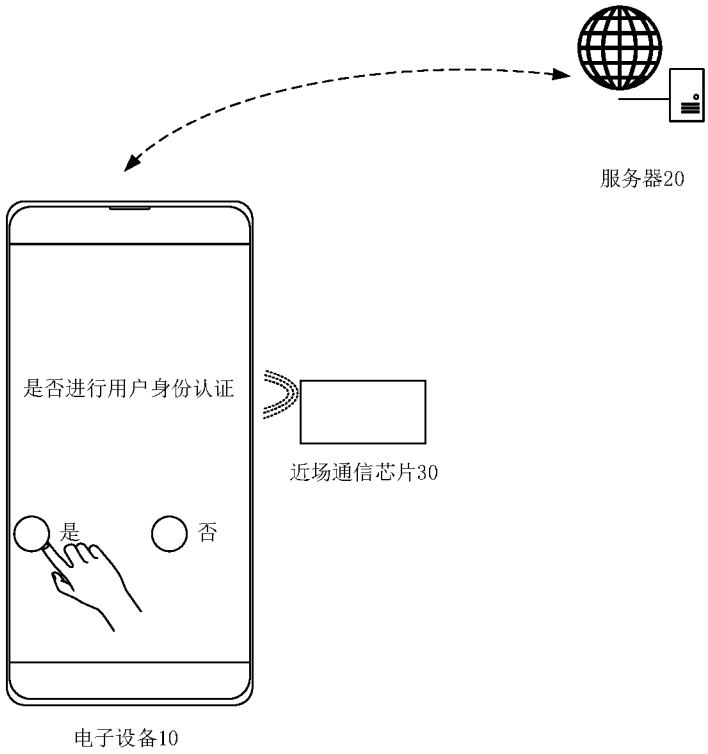

服务器20
是否进行用户身份认证
近场通信芯片30
是
否
电子设备10

图 1

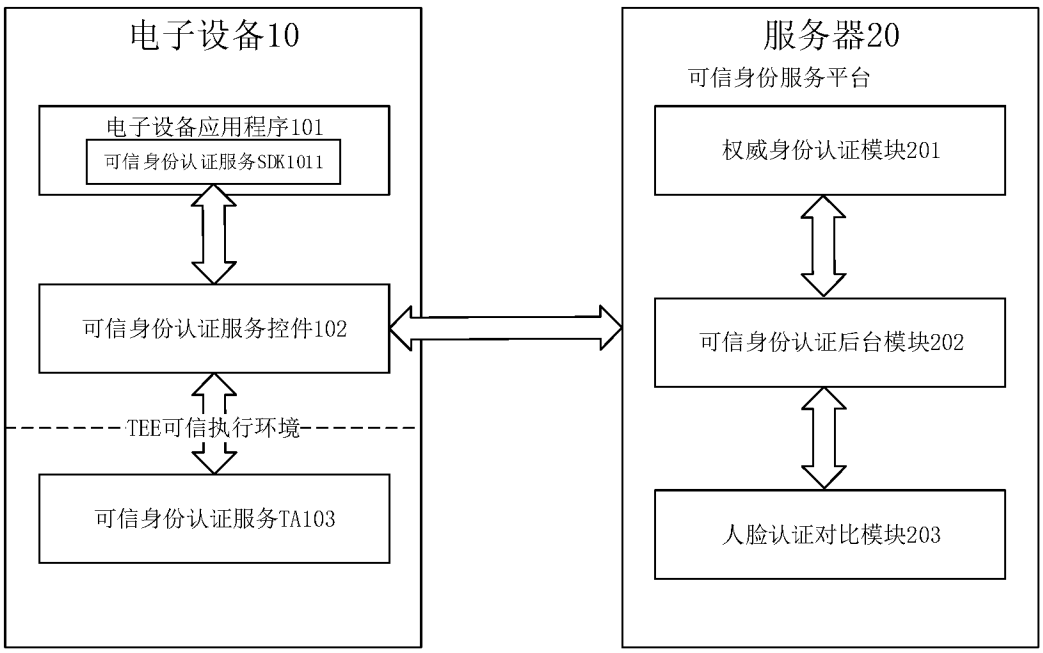

电子设备10
电子设备应用程序101
可信身份认证服务SDK1011
可信身份认证服务控件102
TEE可信执行环境
可信身份认证服务TA103
服务器20
可信身份服务平台
权威身份认证模块201
可信身份认证后台模块202
人脸认证对比模块203

图 2

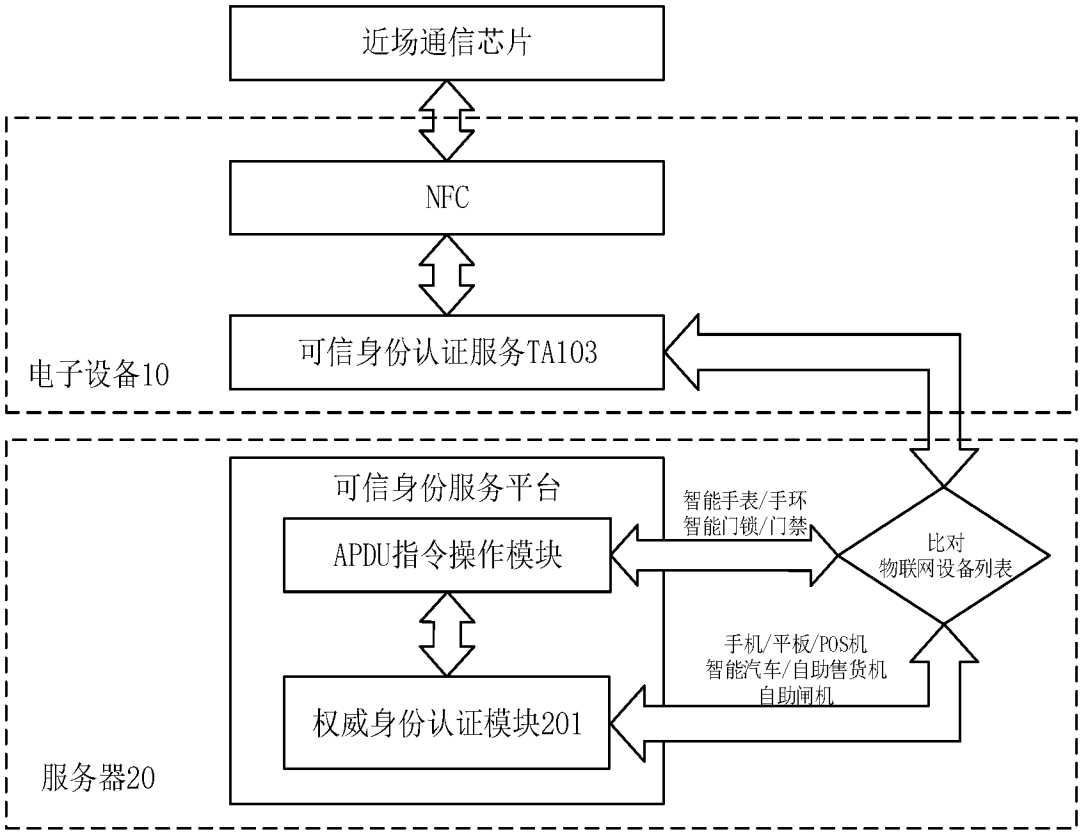


图 3

物联网电子设备	APDU 指令交互适用于 TEE 内执行	APDU 指令的生成、组装和响应处理适用于放在可信身份服务平台
智能手机	√	
手提/平板电脑	√	
智能手表/手环		√
智能门锁/门禁		√
智能 POS 机具	√	
智能汽车	√	
自助售货机	√	
自助闸机	√	

图 4

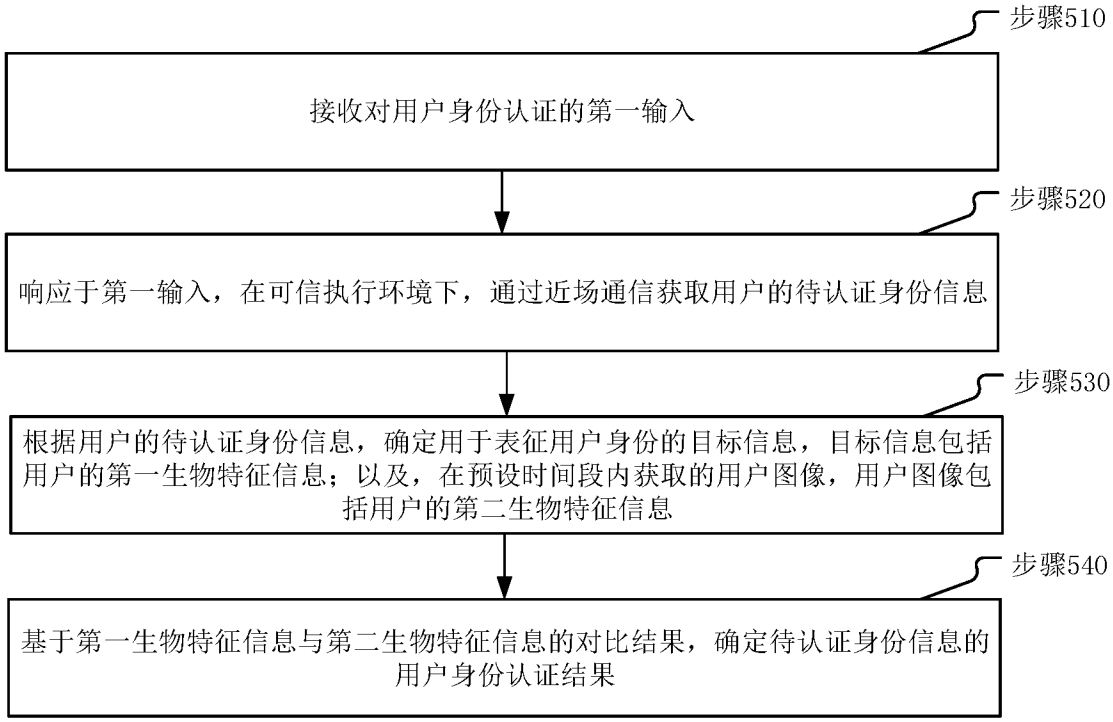
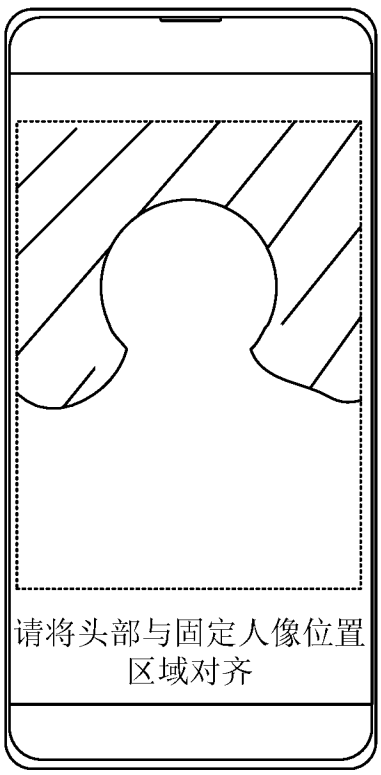
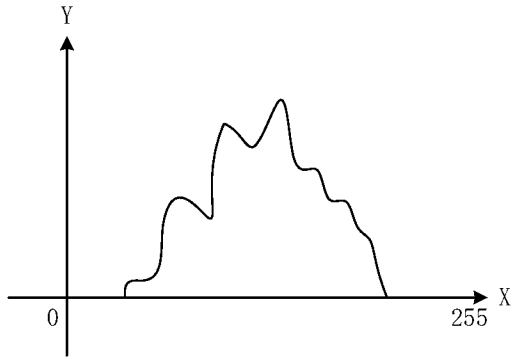

步骤510
接收对用户身份认证的第一输入
步骤520
响应于第一输入，在可信执行环境下，通过近场通信获取用户的待认证身份信息
步骤530
根据用户的待认证身份信息，确定用于表征用户身份的目标信息，目标信息包括用户的第一生物特征信息；以及，在预设时间段内获取的用户图像，用户图像包括用户的第二生物特征信息
步骤540
基于第一生物特征信息与第二生物特征信息的对比结果，确定待认证身份信息的用户身份认证结果

图 5

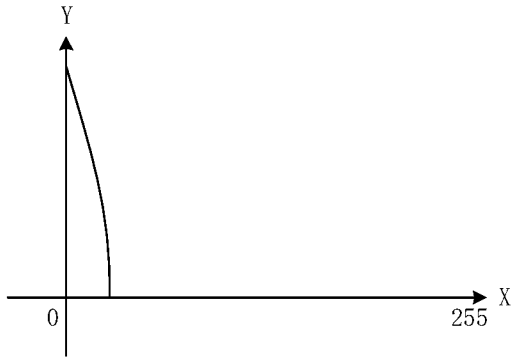

请将头部与固定人像位置区域对齐

电子设备10

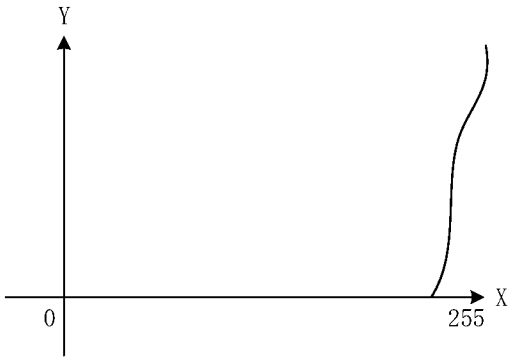
图 6



（1）正常图片



（2）欠曝图片



（3）过曝图片



（4）反差过低图片

图 7

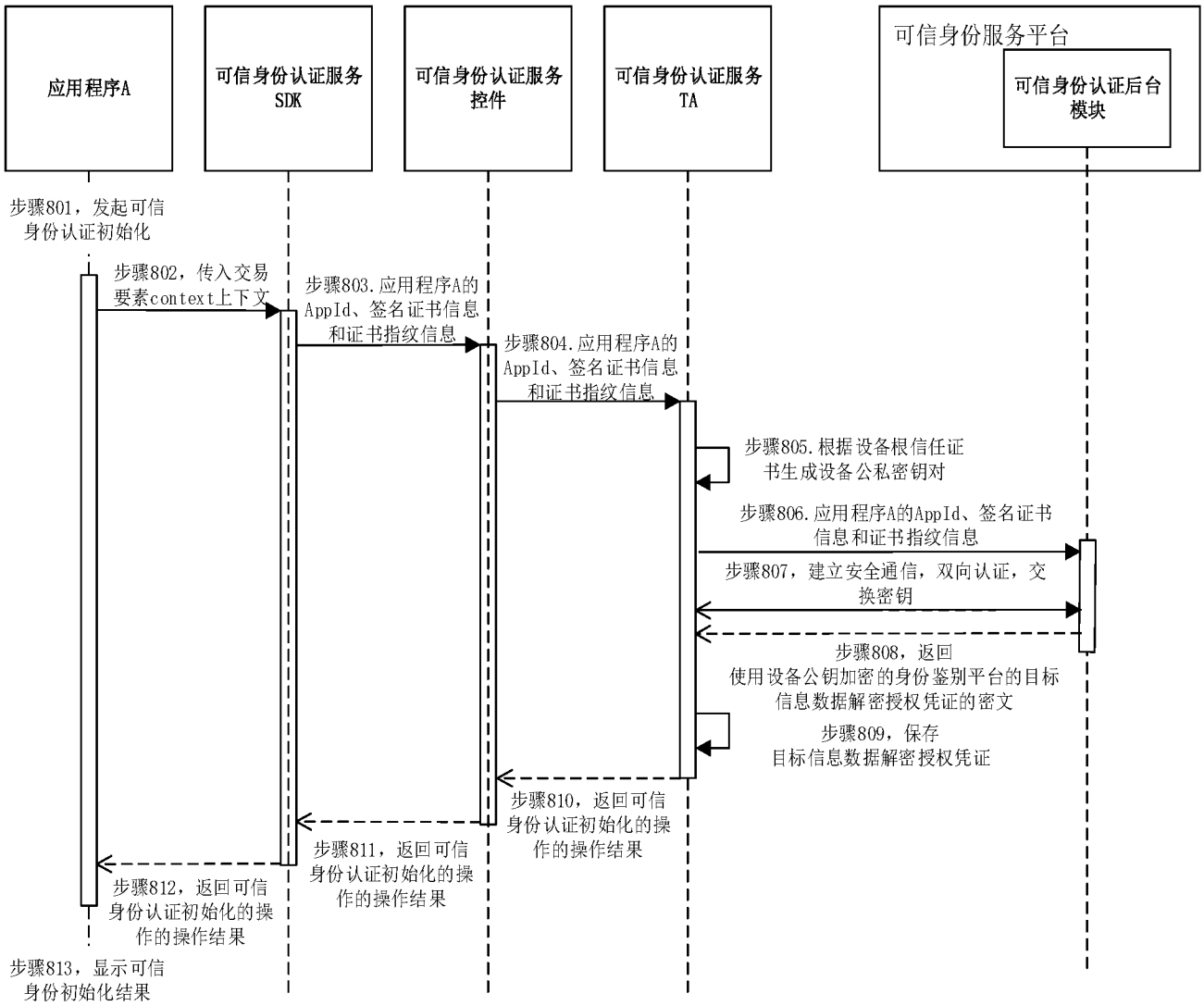

应用程序A
可信身份认证服务SDK
可信身份认证服务控件
可信身份认证服务TA
可信身份服务平台
可信身份认证后台模块
步骤801，发起可信身份认证初始化
步骤802，传入交易要素context上下文
步骤803.应用程序A的AppId、签名证书信息和证书指纹信息
步骤804.应用程序A的AppId、签名证书信息和证书指纹信息
步骤805.根据设备根信任证书生成设备公私密钥对
步骤806.应用程序A的AppId、签名证书信息和证书指纹信息
步骤807，建立安全通信，双向认证，交换密钥
步骤808，返回使用设备公钥加密的身份鉴别平台的目标信息数据解密授权凭证的密文
步骤809，保存目标信息数据解密授权凭证
步骤810，返回可信身份认证初始化的操作的操作结果
步骤811，返回可信身份认证初始化的操作的操作结果
步骤812，返回可信身份认证初始化的操作的操作结果
步骤813，显示可信身份初始化结果

图 8

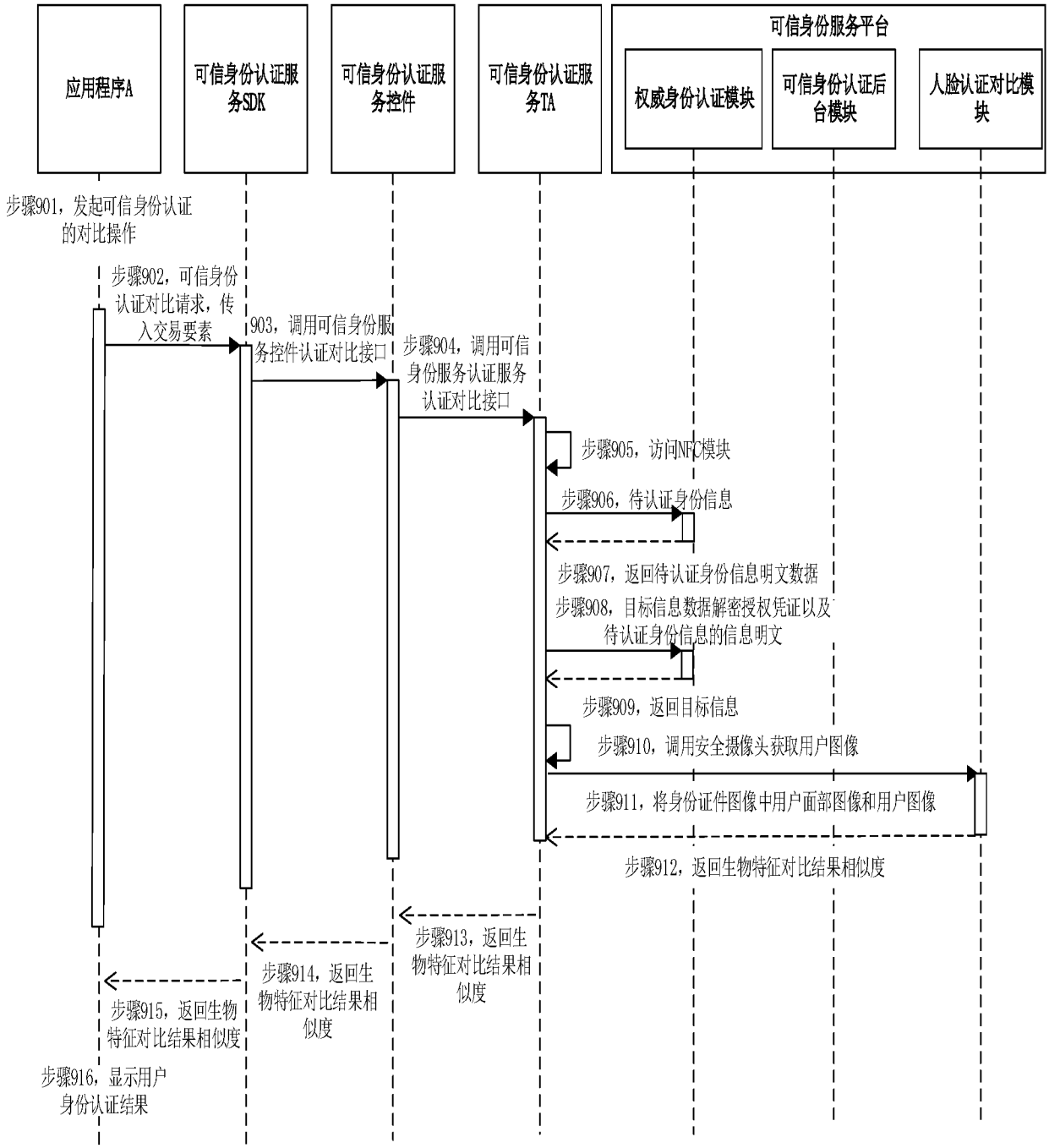

应用程序A
可信身份认证服务SDK
可信身份认证服务控件
可信身份认证服务TA
可信身份服务平台
权威身份认证模块
可信身份认证后台模块
人脸认证对比模块
步骤901，发起可信身份认证的对比操作
步骤902，可信身份认证对比请求，传入交易要素
903，调用可信身份服务控件认证对比接口
步骤904，调用可信身份服务认证服务认证对比接口
步骤905，访问NFC模块
步骤906，待认证身份信息
步骤907，返回待认证身份信息明文数据
步骤908，目标信息数据解密授权凭证以及待认证身份信息的信息明文
步骤909，返回目标信息
步骤910，调用安全摄像头获取用户图像
步骤911，将身份证件图像中用户面部图像和用户图像
步骤912，返回生物特征对比结果相似度
步骤913，返回生物特征对比结果相似度
步骤914，返回生物特征对比结果相似度
步骤915，返回生物特征对比结果相似度
步骤916，显示用户身份认证结果

图 9

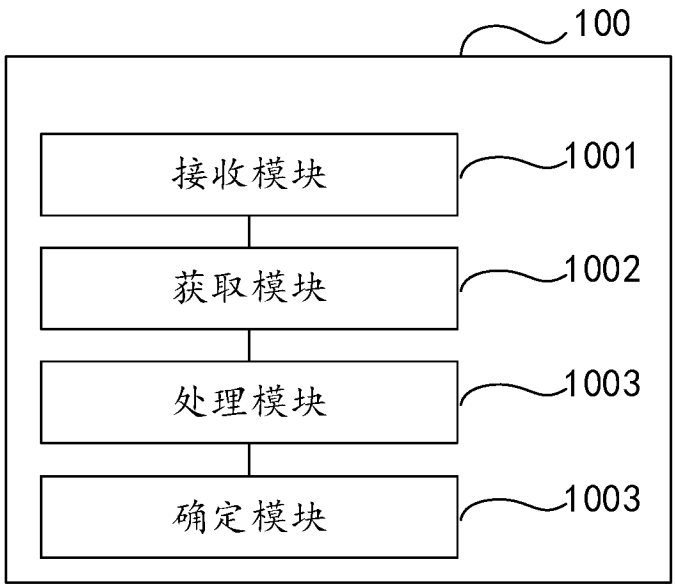

100
接收模块
1001
获取模块
1002
处理模块
1003
确定模块
1003

图 10

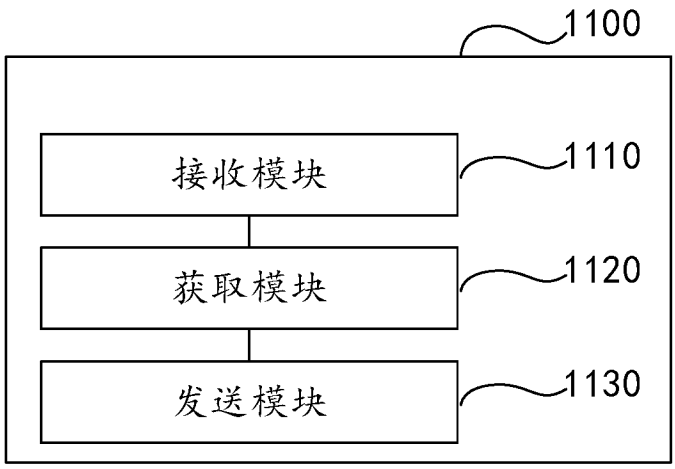

1100
接收模块
1110
获取模块
1120
发送模块
1130

图 11

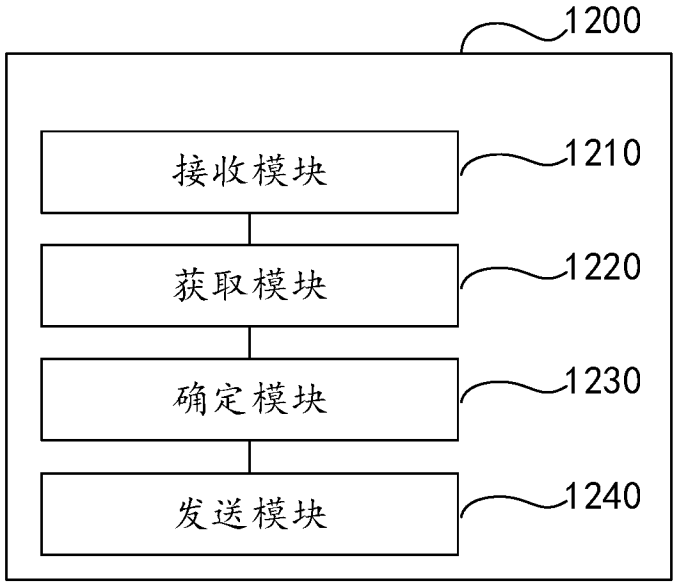

1200
接收模块
1210
获取模块
1220
确定模块
1230
发送模块
1240

图 12

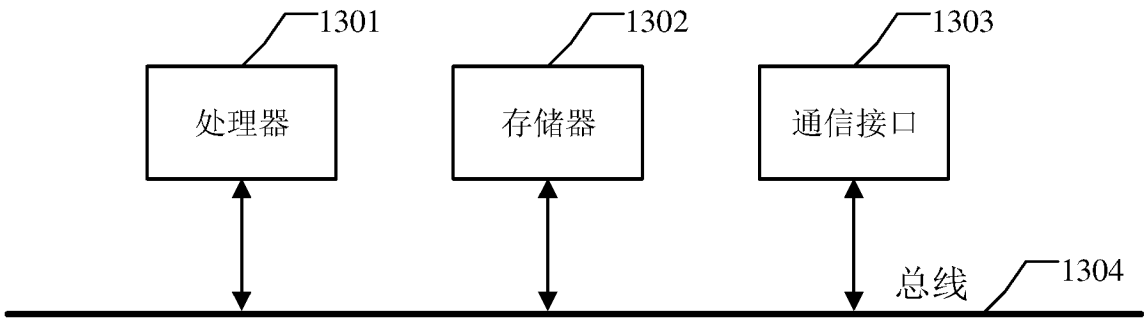

1301
处理器
1302
存储器
1303
通信接口
总线
1304

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/117232

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40(2012.01)i; G06Q 20/38(2012.01)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)

G06Q, 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, CNKI, WPI, EPODOC: 身份, 认证, 近场通信, 生物特征, 图像, 指纹, 人脸, identity, authenticat+, NFC, biological, characteristic, image, fingerprint, face

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112819475 A (CHINA UNIONPAY CO., LTD.) 18 May 2021 (2021-05-18) claims 1-32	1-32
X	CN 111831995 A (HANGZHOU HAIYAN TECHNOLOGY CO., LTD.) 27 October 2020 (2020-10-27) description, paragraphs 23-42	1-32
X	CN 109325332 A (BEIJING KUANGSHI TECHNOLOGY CO., LTD.) 12 February 2019 (2019-02-12) description paragraphs 83-155	1-32
X	CN 107682545 A (SHANXI TEXIN HUANYU INFORMATION TECHNOLOGY CO., LTD.) 09 February 2018 (2018-02-09) description paragraphs 23-86	1-32
A	CN 108462725 A (BEIJING HUADA ZHIBAO ELECTRONIC SYSTEM CO., LTD.) 28 August 2018 (2018-08-28) entire document	1-32
A	CN 105187217 A (CHENGDU 30KAITIAN COMMUNICATION INDUSTRY CO., LTD.) 23 December 2015 (2015-12-23) entire document	1-32

☑ 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
23 November 2021	**08 December 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/117232

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2014082387 A1 (WWTT TECHNOLOGY CHINA) 05 June 2014 (2014-06-05) entire document	1-32

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/117232

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112819475 A	18 May 2021	None	
CN 111831995 A	27 October 2020	None	
CN 109325332 A	12 February 2019	None	
CN 107682545 A	09 February 2018	None	
CN 108462725 A	28 August 2018	None	
CN 105187217 A	23 December 2015	None	
WO 2014082387 A1	05 June 2014	CN 103001773 A	27 March 2013
		HK 1187201 A2	28 March 2014
		JP 2015537476 A	24 December 2015
		DE 112013005682 T5	01 October 2015
		KR 20150090099 A	05 August 2015
		TW 201428529 A	16 July 2014
		US 2016012272 A1	14 January 2016

国际检索报告

国际申请号
PCT/CN2021/117232

A. 主题的分类

G06Q 20/40(2012.01)i; G06Q 20/38(2012.01)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)

G06Q, 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, CNKI, WPI, EPODOC: 身份，认证，近场通信，生物特征，图像，指纹，人脸，identity， authenticat+, NFC, biological, characteristic, image, fingerprint, face

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 112819475 A (中国银联股份有限公司) 2021年5月18日 (2021-05-18) 权利要求1-32	1-32
X	CN 111831995 A (杭州海宴科技有限公司) 2020年10月27日 (2020-10-27) 说明书第23-42段	1-32
X	CN 109325332 A (北京旷视科技有限公司) 2019年2月12日 (2019-02-12) 说明书第83-155段	1-32
X	CN 107682545 A (山西特信环宇信息技术有限公司) 2018年2月9日 (2018-02-09) 说明书第23-86段	1-32
A	CN 108462725 A (北京华大智宝电子系统有限公司) 2018年8月28日 (2018-08-28) 全文	1-32
A	CN 105187217 A (成都三零凯天通信实业有限公司) 2015年12月23日 (2015-12-23) 全文	1-32
A	WO 2014082387 A1 (WWTT TECHNOLOGY CHINA) 2014年6月5日 (2014-06-05) 全文	1-32

☐ 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
2021年11月23日	2021年12月8日
ISA/CN的名称和邮寄地址 中国国家知识产权局(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	受权官员 吴黄飞 电话号码 86-(10)-53961430

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/117232

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	112819475	A	2021年5月18日	无			
CN	111831995	A	2020年10月27日	无			
CN	109325332	A	2019年2月12日	无			
CN	107682545	A	2018年2月9日	无			
CN	108462725	A	2018年8月28日	无			
CN	105187217	A	2015年12月23日	无			
WO	2014082387	A1	2014年6月5日	CN	103001773	A	2013年3月27日
				HK	1187201	A2	2014年3月28日
				JP	2015537476	A	2015年12月24日
				DE	112013005682	T5	2015年10月1日
				KR	20150090099	A	2015年8月5日
				TW	201428529	A	2014年7月16日
				US	2016012272	A1	2016年1月14日