(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106295290 B
(45)授权公告日 2021.12.21

(21)申请号 201510369312.4

(22)申请日 2015.06.26

(65)同一申请的已公布的文献号
申请公布号 CN 106295290 A

(43)申请公布日 2017.01.04

(73)专利权人 创新先进技术有限公司
地址 英属开曼群岛大开曼岛乔治镇医院路27号开曼企业中心

(72)发明人 皮维

(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315
代理人 朱文杰

(51)Int.Cl.
G06F 21/32(2013.01)

(56)对比文件
CN 102523213 A,2012.06.27
CN 103701977 A,2014.04.02
CN 103886239 A,2014.06.25

审查员 李文浩

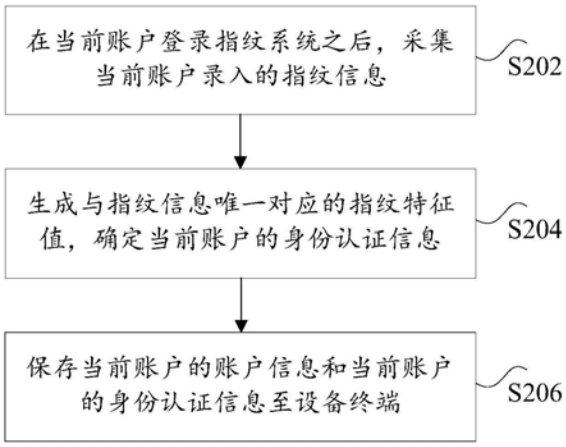
权利要求书3页 说明书21页 附图8页

(54)发明名称

基于指纹信息生成认证信息的方法、装置及系统

(57)摘要

本发明公开了一种基于指纹信息生成认证信息的方法、装置及系统。其中，该方法包括：在当前账户登录指纹系统之后，采集当前账户录入的指纹信息；生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值；保存当前账户的账户信息和当前账户的身份认证信息至设备终端。本发明解决了单独凭借指纹信息与移动设备中存储的指纹信息进行比对的方式来确认用户身份信息，导致的安全性差，指纹信息容易被伪造的技术问题。



CN 106295290 B

1.一种基于指纹信息生成认证信息的方法,其特征在于,包括:

在当前账户登录指纹系统之后,采集所述当前账户录入的多个指纹信息;

生成所述多个指纹信息的扩展信息、以及与所述指纹信息唯一对应的指纹特征值,确定所述当前账户的身份认证信息,其中,所述身份认证信息至少包括:所述指纹信息、所述扩展信息和与所述指纹信息唯一对应的指纹特征值;所述扩展信息包括如下任意一种或多种信息:每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置;

保存所述当前账户的账户信息和所述当前账户的所述身份认证信息至设备终端;

其中,采用如下任意一种指纹特征值生成方式生成与所述指纹信息唯一对应的指纹特征值:

根据所述指纹信息中所包含的指纹模板的图像信息生成所述指纹特征值;

在通过指纹芯片采集所述指纹信息的情况下,根据所述指纹芯片的硬件序列号生成所述指纹特征值;

根据所述指纹信息的采集时间来生成所述指纹特征值;

根据如下任意多个参数的组合来生成所述指纹特征值:所述指纹模板的图像信息、所述指纹芯片的硬件序列号和所述指纹信息的采集时间;

其中,生成所述指纹特征值时,对于多个不同的指纹信息,随机采用所述指纹特征值生成方式;对于相同的指纹信息,采用相同的所述指纹特征值生成方式。

2.根据权利要求1所述的方法,其特征在于,在保存所述当前账户的账户信息和所述当前账户的所述身份认证信息至设备终端之后,所述方法还包括:

采集待验证账户的待验证指纹信息;

采用所述指纹特征值生成方式处理所述待验证指纹信息,生成与所述待验证账户的待验证指纹信息唯一对应的待验证指纹特征值;

将所述待验证指纹信息和所述待验证指纹信息唯一对应的待验证指纹特征值与所述设备终端中已经保存的所述身份认证信息进行比对;

在所述待验证指纹信息与所述身份认证信息中的所述指纹信息相匹配,且所述待验证指纹特征值与所述身份认证信息中的所述指纹特征值也相匹配的情况下,所述待验证账户通过验证。

3.根据权利要求1所述的方法,其特征在于,所述指纹的移动轨迹包括:所述指纹延顺时针方向移动、所述指纹延逆时针方向移动、所述指纹从上至下移动或所述指纹从下至上移动。

4.根据权利要求1至3中任意一项所述的方法,其特征在于,在保存所述当前账户的账户信息和所述当前账户的所述身份认证信息至设备终端之后,所述方法还包括:

将所述当前账户的账户信息和所述当前账户的所述身份认证信息注册至客户端,生成所述当前账户在所述客户端中的注册信息;

在所述客户端验证所述注册信息通过的情况下,将所述注册信息进行加密;

所述客户端保存加密后的所述注册信息。

5.根据权利要求4所述的方法,其特征在于,在所述客户端保存加密后的所述注册信息之后,所述方法还包括:

所述客户端接收到虚拟资源的转移请求指令;

通过所述设备终端上安装的所述指纹系统采集待验证账户的指纹信息；

在根据所述待验证账户的指纹信息生成待验证账户的身份信息之后，将所述待验证账户的账户信息和所述身份信息分别与所述设备终端中已经保存的所述账户信息和所述身份认证信息进行匹配，在匹配成功的情况下，将所述待验证账户的账户信息和所述待验证账户的身份信息发送至所述客户端；

所述客户端根据所述注册信息来验证所述待验证账户的账户信息和所述身份信息，在验证通过的情况下，执行所述虚拟资源的转移请求指令。

6.根据权利要求5所述的方法，其特征在于，执行所述虚拟资源的转移请求指令的步骤包括：

验证所述待验证账户的虚拟资源的转移信息；

在所述转移信息准确的情况下，将所述转移信息和/或所述待验证账户的私钥签名发送至虚拟资源转移服务器，使得所述虚拟资源服务器根据所述虚拟资源的转移信息完成转移功能。

7.一种基于指纹信息生成认证信息的装置，其特征在于，包括：

采集模块，用于在当前账户登录指纹系统之后，采集所述当前账户录入的多个指纹信息；

获取模块，用于生成所述多个指纹信息的扩展信息、以及与所述指纹信息唯一对应的指纹特征值，确定所述当前账户的身份认证信息，其中，所述身份认证信息至少包括：所述指纹信息、所述扩展信息和与所述指纹信息唯一对应的指纹特征值；所述扩展信息包括如下任意一种或多种信息：每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置；

保存模块，用于保存所述当前账户的账户信息和所述当前账户的所述身份认证信息至设备终端；

其中，所述获取模块包括如下任意一种功能模块：

第一生成模块，用于根据所述指纹信息中所包含的指纹模板的图像信息生成所述指纹特征值；

第二生成模块，用于在通过指纹芯片采集所述指纹信息的情况下，根据所述指纹芯片的硬件序列号生成所述指纹特征值；

第三生成模块，用于根据所述指纹信息的采集时间来生成所述指纹特征值；

第四生成模块，用于根据如下任意多个参数的组合来生成所述指纹特征值：所述指纹模板的图像信息、所述指纹芯片的硬件序列号和所述指纹信息的采集时间；

其中，生成所述指纹特征值时，对于多个不同的指纹信息，随机采用所述指纹特征值生成方式；对于相同的指纹信息，采用相同的所述指纹特征值生成方式。

8.根据权利要求7所述的装置，其特征在于，所述指纹的移动轨迹包括：所述指纹延顺时针方向移动、所述指纹延逆时针方向移动、所述指纹从上至下移动或所述指纹从下至上移动。

9.根据权利要求7或8所述的装置，其特征在于，所述装置还包括：

注册模块，用于将所述当前账户的账户信息和所述当前账户的所述身份认证信息注册至客户端，生成所述当前账户在所述客户端中的注册信息。

10.一种基于指纹信息生成认证信息的系统,其特征在于,包括:

指纹芯片,用于在当前账户登录指纹系统之后,采集所述当前账户录入的多个指纹信息;

处理器,与所述指纹芯片连接,用于生成所述多个指纹信息的扩展信息、以及与所述指纹信息唯一对应的指纹特征值,确定所述当前账户的身份认证信息,其中,所述身份认证信息至少包括:所述指纹信息、所述扩展信息和与所述指纹信息唯一对应的指纹特征值;所述扩展信息包括如下任意一种或多种信息:每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置;

存储器,与所述处理器连接,用于保存所述当前账户的账户信息和所述当前账户的所述身份认证信息;

其中,采用如下任意一种指纹特征值生成方式生成与所述指纹信息唯一对应的指纹特征值:

根据所述指纹信息中所包含的指纹模板的图像信息生成所述指纹特征值;

在通过指纹芯片采集所述指纹信息的情况下,根据所述指纹芯片的硬件序列号生成所述指纹特征值;

根据所述指纹信息的采集时间来生成所述指纹特征值;

根据如下任意多个参数的组合来生成所述指纹特征值:所述指纹模板的图像信息、所述指纹芯片的硬件序列号和所述指纹信息的采集时间;

其中,生成所述指纹特征值时,对于多个不同的指纹信息,随机采用所述指纹特征值生成方式;对于相同的指纹信息,采用相同的所述指纹特征值生成方式。

基于指纹信息生成认证信息的方法、装置及系统

技术领域

[0001] 本发明涉及互联网领域，具体而言，涉及一种基于指纹信息生成认证信息的方法、装置及系统。

背景技术

[0002] 随着移动互联网技术的飞速发展，越来越多的移动设备被应用于生活当中，例如：手机，穿戴式设备等。很多硬件厂商都开始计划或者已经在移动移动设备上配备指纹传感器，或者装配整体的指纹识别方案。但是，因为指纹信息涉及到用户的隐私，所以，在对于指纹信息的使用需要做严格的限制。

[0003] 在目前现有的终端设备(例如移动设备)中，通常使用指纹对设备进行解锁操作。在移动设备中配备指纹芯片，并使用相应的技术来保证指纹的安全。其中，指纹解锁技术，主要是用户在终端设备中设置一个普通密码。在输入普通密码后，可以在设备中添加一个或多个指纹信息，设备将指纹信息存储到TEE(安全存储空间)中。当对设备进行解锁时，获取用户的指纹信息，并将指纹信息与设备中存储的一个或多个指纹信息模板进行匹配，当匹配成功后进行解锁操作。

[0004] 进一步的，基于上述基于指纹信息解锁的移动设备，在该移动设备中使用虚拟资源转移(例如支付)客户端完成网上支付的过程中，可以使用指纹来实现支付过程中的身份验证技术，通常是在确认可以通过指纹进行指纹解锁的前提下，才让用户开通指纹支付的功能。具体的，服务端发送开通指令，用户在客户端录入已经在设备中添加过的指纹信息。当指纹校验通过之后，客户端会生成相应的信息返回给服务端。从而使得用户可以开通指纹支付的功能。每当通过指纹进行支付的时候，支付客户端会使用存储在设备TEE(安全存储空间)中的指纹信息，当用户录入的指纹信息与设备存储的指纹信息进行比对成功后，对用户的支付信息进行确认。

[0005] 虽然对于指纹信息的使用普遍都已经作了严格的限制。但是，在将指纹信息用于终端设备的登录以及上述支付的场景中时，通过验证指纹信息确认登录用户的身份，然后进一步完成支付系统中的支付，利用指纹信息的身份认证以及支付仍旧存在一些安全问题。

[0006] 例如，在一台移动设备中，通常允许同时对多个指纹信息进行注册，而现有的支付系统只通过验证指纹信息是否在移动设备中进行过注册，来确定是否进行支付。这就导致当用户在移动终端和/或支付系统中存储、开通了通过验证指纹信息来进行支付时，一旦有第二个用户在该移动设备中注册了自己的指纹信息，那么第二个用户就可以直接通过自己的指纹信息登录该移动终端，然后进入控制支付系统中的支付账户进行支付操作，此时，移动终端和/或支付系统并不知道设备中的指纹信息是谁的。

[0007] 针对上述单独凭借指纹信息与移动设备中存储的指纹信息进行比对的方式来确认用户身份信息，导致的安全性差，指纹信息容易被伪造问题，目前尚未提出有效的解决方案。

发明内容

[0008] 本发明实施例提供了一种基于指纹信息生成认证信息的方法、装置及系统，以至少解决单独凭借指纹信息与移动设备中存储的指纹信息进行比对的方式来确认用户身份信息，导致的安全性差，指纹信息容易被伪造的技术问题。

[0009] 根据本发明实施例的一个方面，提供了一种基于指纹信息生成认证信息的方法，包括：在当前账户登录指纹系统之后，采集当前账户录入的指纹信息；生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值；保存当前账户的账户信息和当前账户的身份认证信息至设备终端。

[0010] 根据本发明实施例的另一方面，还提供了一种基于指纹信息生成认证信息的装置，包括：采集模块，用于在当前账户登录指纹系统之后，采集当前账户录入的指纹信息；获取模块，用于生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值；保存模块，用于保存当前账户的账户信息和当前账户的身份认证信息至设备终端。

[0011] 根据本发明实施例的另一方面，还提供了一种基于指纹信息生成认证信息的系统，包括：指纹芯片，用于在当前账户登录指纹系统之后，采集当前账户录入的指纹信息；处理器，与指纹芯片连接，用于生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值；存储器，与处理器连接，用于保存当前账户的账户信息和当前账户的身份认证信息。

[0012] 在本发明实施例中，采用在当前账户登录指纹系统之后，采集当前账户录入的指纹信息；生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值；保存当前账户的账户信息和当前账户的身份认证信息至设备终端的方式，通过利用指纹信息和与指纹信息唯一对应的指纹特征值确认用户的身份信息，达到了以指纹特征值作为校验条件对指纹信息的真伪进行校验的目的，从而实现了指纹系统和账户信息对指纹信息的双重验证的技术效果，进而解决了单独凭借指纹信息与移动设备中存储的指纹信息进行比对的方式来确认用户身份信息，导致的安全性差，指纹信息容易被伪造的技术问题。

附图说明

[0013] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0014] 图1是本发明实施例的一种基于指纹信息生成认证信息的方法的移动终端的硬件结构框图；

[0015] 图2是根据本发明实施例一的基于指纹信息生成认证信息的方法的流程图；

[0016] 图3是根据本发明实施例的一种用于录入指纹的录入界面示意图；

[0017] 图4是根据本发明实施例一的一种可选的优选的基于指纹信息生成认证信息的方法的流程图；

[0018] 图5是本发明实施例的一种具有指纹芯片的终端设备的硬件结构框图；

[0019] 图6是本发明实施例一的通过基于指纹信息生成认证信息的方法实现安全身份认

证成功注册的实施方式的详细流程图；

[0020] 图7是本发明实施例一的在移动终端中实现支付认证实施方式的详细流程图；

[0021] 图8是根据本发明实施例二的基于指纹信息生成认证信息的装置的示意图；

[0022] 图9是根据本发明实施例二的一种可选的基于指纹信息生成认证信息的装置的获取模块的示意图；

[0023] 图10是根据本发明实施例二的一种可选的基于指纹信息生成认证信息的装置的示意图；以及

[0024] 图11是根据本发明实施例三的一种基于指纹信息生成认证信息的系统的结构框图。

具体实施方式

[0025] 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。

[0026] 需要说明的是，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”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，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、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0027] 实施例1

[0028] 根据本发明实施例，还提供了一种基于指纹信息生成认证信息的方法实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0029] 本申请实施例一所提供的方法实施例可以在移动终端、移动终端或者类似的运算装置中执行。以运行在移动终端上为例，图1是本发明实施例的一种基于指纹信息生成认证信息的方法的移动终端的硬件结构框图。如图1所示，移动终端10可以包括一个或多个(图中仅示出一个)处理器102(处理器102可以包括但不限于微处理器MCU或可编程逻辑器件FPGA等的处理装置)、用于存储数据的存储器104、以及用于通信功能的传输模块106。本领域普通技术人员可以理解，图1所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，移动终端10还可包括比图1中所示更多或者更少的组件，或者具有与图1所示不同的配置。

[0030] 存储器104可用于存储应用软件的软件程序以及模块，如本发明实施例中的基于指纹信息生成认证信息的方法对应的程序指令/模块，处理器102通过运行存储在存储器104内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的应用程序

的漏洞检测方法。存储器104可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器104可进一步包括相对于处理器102远程设置的存储器，这些远程存储器可以通过网络连接至移动终端10。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0031] 传输装置106用于经由一个网络接收或者发送数据。上述的网络具体实例可包括移动终端10的通信供应商提供的无线网络。在一个实例中，传输装置106包括一个网络适配器(Network Interface Controller,NIC)，其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置106可以为射频(Radio Frequency,RF)模块，其用于通过无线方式与互联网进行通讯。

[0032] 在上述运行环境下，本申请提供了如图2所示的基于指纹信息生成认证信息的方法。图2是根据本发明实施例一的基于指纹信息生成认证信息的方法的流程图。

[0033] 步骤S202，在当前账户登录指纹系统之后，采集当前账户录入的指纹信息。

[0034] 本申请上述步骤S202中，用户在以当前账户的账户信息登录指纹系统之后，可以通过安装了该指纹系统的终端设备中内置的指纹信息来采集指纹信息。例如，一台移动设备，用户使用当前账户信息登录移动设备中的指纹系统，并在触摸移动设备提供的指纹芯片之后，通过该指纹系统采集到当前用户的指纹信息。

[0035] 其中，上述指纹信息是包含了用户的指纹细节特征的数字信息，可以通过指纹芯片对指纹进行采集，也可以通过识别包含指纹信息的图片的方式进行采集。

[0036] 步骤S204，生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值。

[0037] 本申请上述步骤S204中，在当前账户登陆指纹系统并采集到对应的指纹信息之后，生成与指纹信息唯一对应的指纹特征值。将指纹信息和与指纹信息唯一对应的指纹特征值进行关联，并利用指纹信息和与指纹信息唯一对应的指纹特征值生成当前账户的一组身份认证信息。

[0038] 此处需要说明的是，指纹特征值用于标识采集到的指纹信息具有唯一性，系统可以采用如下方式来生成该指纹特征值：指纹模板的图像像素值、指纹模板的图像容量大小、指纹芯片的序列号、设备终端的MAC地址等。

[0039] 指纹系统根据系统本身的属性生成指纹特征值。生成指纹特征值时，对于多个不同的指纹信息，采用随机的指纹特征值算法。但是对于相同的指纹信息，在每次生成指纹特征值时，所使用的生成算法是相同的。所以，即使手机被入侵，入侵用户在存储器中添加一个仿制的指纹信息，也无法仿制与指纹信息对应的指纹特征值。并且，指纹特征值时指纹系统根据系统本身的属性随机生成出来的，所以，指纹特征码一旦脱离系统本身用在其他指纹系统中时，因为系统本身的属性不同，所以指纹特征码也就失效了。

[0040] 步骤S206，保存当前账户的账户信息和当前账户的身份认证信息至设备终端。

[0041] 本申请上述步骤S206，将当前登录账户的账户信息和身份认证信息保存在当前的设备终端中，即完成了在设备终端注册安全用户的功能，这种注册了用于验证身份的数据的设备终端具有更高的安全性。

[0042] 由上可知，在设备终端完成上述当前账户的安全性注册之后，设备终端可以通过利用已经保存的指纹信息和与指纹信息唯一对应的指纹特征值来对用户的身份信息进行

匹配，实现了在对用户的指纹信息进行验证的同时，还需要同时验证该指纹信息唯一对应的指纹特征值，来实现对任意一个访问该设备终端的用户进行校验的目的，避免了非法入侵、仿制指纹的用户来非法登录设备终端系统的问题，提高了对账户身份信息进行识别的安全性。

[0043] 在实际应用当中，用户在设备终端上录入指纹信息的过程中，设备终端对生成的指纹信息会被设置一个名称，例如：指纹1或者指纹2。同时，在录入指纹信息时为每个指纹信息生成一个唯一的指纹特征值。指纹特征值可以由时间、芯片等因素构成。可以用4个字节的整数进行表示，例如：指纹1：ID382931932832、指纹2：ID384838282322。

[0044] 由上可知，本申请上述实施例以提供的方案，在当前账户登录指纹系统之后，采集与当前登录账号对应的指纹信息，并同时根据指纹信息，生成与指纹信息唯一对应的指纹特征值。将指纹信息和与指纹信息唯一对应的指纹特征值作为当前登录账号的身份认证信息，通过利用指纹信息和与指纹信息唯一对应的指纹特征值确认用户的身份信息的方法，来验证指纹信息的合法性，达到了以指纹特征值作为校验条件对指纹信息的真伪进行校验的目的，从而实现了指纹系统和账户信息对指纹信息的双重验证的效果，解决了单独凭借指纹信息与移动设备中存储的指纹信息进行比对的方式来确认用户身份信息，导致的安全性差，指纹信息容易被伪造的问题。

[0045] 本申请上述实施例提供的一种优选方案中，上述步骤S204，生成与指纹信息唯一对应的指纹特征值可以包括如下任意一种方式：

[0046] 方式一：根据指纹信息中所包含的指纹模板的图像信息生成指纹特征值。

[0047] 具体的，因为各个移动终端所配置的指纹采集模块的型号不同，以及各个制造移动终端的硬件厂商对于采集得到的指纹信息的处理方式也不同，所以导致采集到的、处理后的包含有指纹模板的图像信息的像素值、纵横比或图片大小也不相同。因此，利用像素值、纵横比和/或图片大小参数作为指纹特征值，可以达到对指纹信息进行唯一标识的作用。

[0048] 方式二：在通过指纹芯片采集指纹信息的情况下，根据指纹芯片的硬件序列号生成指纹特征值。

[0049] 具体的，在芯片制造过程中，制造厂家会对生产的每个硬件分配不同的硬件序列号以便于生产管理。因此，利用可以达到对指纹信息进行唯一标识的作用。

[0050] 方式三：根据指纹信息的采集时间来生成指纹特征值。

[0051] 方式四：根据如下任意多个参数的组合来生成指纹特征值：指纹模板的图像信息、指纹芯片的硬件序列号和指纹信息的采集时间。

[0052] 具体的，可以通过上述四种生成指纹特征值方式中的任意一种对指纹特征值进行你给生成。除此之外，只要能够达到为指纹信息分配一个独一无二的随机数值，并且可以独立标识该指纹的目的的方式，都可以用来生成本方案中指纹特征值，此处不再赘述。

[0053] 此处需要说明的是，在保存当前账户的账户信息和当前账户的身份认证信息至设备终端之后，本申请还可以执行如下验证步骤：

[0054] 首先，采集待验证账户的待验证指纹信息。用于在使用设备终端中设置的指纹芯片账户，该指纹芯片可以采集到当前待验证账户的指纹信息作为待验证的指纹信息。

[0055] 然后，采用指纹特征值生成方式处理待验证指纹信息，生成与待验证账户的待验

证指纹信息唯一对应的待验证指纹特征值。该步骤中使用的指纹特征值生成方式与录入指纹时所采用的指纹特征值生成方式相同，即可以采用上述优选方案中的四种生成方式中的任意一种。

[0056] 接着，将待验证指纹信息和待验证指纹信息唯一对应的待验证指纹特征值与设备终端中已经保存的身份认证信息进行比对，在待验证指纹信息与身份认证信息中的指纹信息相匹配，且待验证指纹特征值与身份认证信息中的指纹特征值也相匹配的情况下，待验证账户通过验证；在待验证指纹信息与身份认证信息中的指纹信息匹配失败，和/或待验证指纹特征值与身份认证信息中的指纹特征值也匹配失败的情况下，待验证账户为非法入侵用户。

[0057] 基于上述方案，即使通过非法的方式在终端设备中注册了合法的指纹信息，仍旧无法来正常登陆设备终端。例如入侵者通过制作纸模等方式仿制手指指纹得到指纹模板，这种盗取到的指纹模板可以骗过指纹芯片，即指纹芯片即便有活体识别能力，但这种仿制的指纹模板也可以使用指套等装置来骗过指纹芯片，完成认证过程。

[0058] 因此，为了更好的解决上述用户指纹信息被窃取导致的用户信息被泄露的问题，本申请上述实施例提供的一种优选方案中，在当前账户录入至少两个指纹的指纹信息的情况下，身份认证信息还可以包括如下任意一种或多种信息：每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置。即可以在采集指纹信息的同时，生成指纹信息的扩展信息，此处的扩展信息可以为上述指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置。优选的，指纹的移动轨迹可以包括如下任意一种移动方式：指纹延顺时针方向移动、指纹延逆时针方向移动、指纹从上至下移动或指纹从下至上移动。

[0059] 由此，设备终端认证当前登录账户时，不仅需要验证指纹信息本身，还需要进一步验证包含了上述扩展信息的身份认证信息。进而，在使用该设备终端进行虚拟资源转移(例如网络支付)的过程中，也可以利用上述扩展信息完成更加安全的支付过程。例如，在用户支付系统中进行指纹注册的时候(不是添加在设备中)，支付系统可以要求用户除了录入指纹以外，增加指纹的扩展信息。例如：[指纹1，录入方向，自上而下]、[指纹2，识别后进行了逆时针旋转]等。

[0060] 由此可知，在实际应用当中，在对指纹信息进行采集时，除了根据指纹信息生成与指纹信息对应的指纹特征值，通过指纹特征值来验证用户身份之外，还可以采用录入多个指纹，并且记录每个指纹的录入顺序作为身份认证信息，或者在有能力记录指纹的识别方向的指纹系统中，记录指纹的录入方向、指纹的旋转方向作为指纹信息的身份认证信息。在开通和\或使用指纹支付功能时，对通过上述方式生成的拓展信息进行验证，从而对用户的身份进行验证。扩展信息的具体采集方式例如：以顺时针旋转自己的指纹的方式进行录入、在擦挂式指纹识别的设备上以由上至下移动手指或者以由下至上移动手指的方式进行录入。

[0061] 通过上述指纹信息的录入方式，采集到的指纹信息不再是唯一的或者静止的信息，指纹信息除了包括静止的指纹模板，还会包含由多种录入方案生成的与指纹信息对应的扩展信息，上述方案下，既有了传统指纹匹配的方便性，又加入了相较于传统密码更强的私有性。解决了目前的指纹技术上的安全性低的问题。

[0062] 如图3所示，以录入多个指纹，并记录每个指纹的录入顺序作为指纹信息的扩展信

息的方式为例。当进行指纹录入的时候，支付系统提示用户录入多个相同或者不同的指纹信息，根据多个指纹信息生成一组身份认证信息。当用户录入了4次手指的指纹信息生成身份认证信息时，记录下用户的身份认证信息为：[user0001,device0001,fingerprint382931932831,fingerprint382931932831fingerprint382931932831,fingerprint384838282322]。从上述身份认证信息中可以得知，前三次用户使用同一只手指进行了指纹的录入，而第四次用户使用了另外一只手指进行指纹的录入。通过上述方法，准确的记录了指纹的录入顺序和录入方式，提高了指纹系统的安全性。

[0063] 进一步的，以录入单个手指的指纹，并记录录入指纹时手指运动方向的方式为例进行说明。手指运动方向以供可以分为四种情况，分别为顺时针旋转、逆时针旋转、自下至上移动、自下至上移动，当进行指纹录入的时候，用户可以在录入指纹信息的同时，同时以上述四种运动方式中的一种进行运动，记录下用户的身份认证信息为[user0001,device0001,[fingerprint382931932831,orentation:04]]。除此之外，还可以在录入指纹信息时，读取设备终端的重力感应器来获取录入指纹时手机所处的状态(屏幕朝下还是朝上)来生成身份认证信息，具体方式此处不再赘述。

[0064] 本申请上述实施例提供的一种优选方案中，如图4所示，在步骤S206保存当前账户的账户信息和当前账户的身份认证信息至设备终端之后，还可以执行如下实施步骤：

[0065] 步骤S207，将当前账户的账户信息和当前账户的身份认证信息注册至客户端，生成当前账户在客户端中的注册信息。

[0066] 本申请上述步骤S207中，用户可以将当前账户信息、指纹信息、与指纹信息对应的指纹特征值注册至客户端中。利用上述账户信息、指纹信息、与指纹信息对应的指纹特征值等信息，在客户端中生成指纹的注册信息。

[0067] 当客户端注册的过程中，在通过读取设备终端已存储的身份认证信息的同时，通过指纹系统获取用户指纹信息。当获取到的指纹信息、根据获取到的指纹信息生成的指纹特征值与已存储的身份认证信息中的信息匹配时，客户端对账户进行注册。

[0068] 以在安装有支付宝客户端(一种可选的客户端)的带有指纹系统的设备终端为例，当支付宝账号成功登陆支付宝之后，支付宝客户端读取设备终端内存储的账户信息身份认证信息，同时将通过指纹系统获取到的指纹信息、根据指纹信息生成的指纹特征值，与读取到的身份认证信息中的指纹信息、与指纹信息对应的指纹特征值进行匹配，在匹配成功时，利用指纹信息、与指纹信息对应的指纹特征值生成一组支付宝客户端用于验证用户身份的注册信息。

[0069] 步骤S208，在客户端验证注册信息通过的情况下，将注册信息进行加密。

[0070] 步骤S209，客户端保存加密后的注册信息。

[0071] 具体的，通过上述步骤S208至步骤S209，将获取到的注册信息进行加密处理，以密文的形式存储至客户端内。当需要对虚拟资源进行转移时，通过将获取到的指纹信息、根据指纹信息生成的指纹特征值与解密后的注册信息进行比对，来完成对用户身份的验证步骤。上述注册信息既可以只存储于设备终端的本地客户端内，也可以同步至与客户端对应的虚拟资源转移服务端当中。

[0072] 本申请上述实施例提供的一种优选方案中，在步骤S209客户端保存加密后的注册信息之后，还可以执行如下实施步骤：

[0073] 步骤S210,客户端接收到虚拟资源的转移请求指令。

[0074] 步骤S211,通过设备终端上安装的指纹系统采集待验证账户的指纹信息。

[0075] 步骤S212,在根据待验证账户的指纹信息生成待验证账户的身份信息之后,将待验证账户的账户信息和身份信息分别与设备终端中已经保存的账户信息和身份认证信息进行匹配,在匹配成功的情况下,将待验证账户的账户信息和待验证账户的身份信息发送至客户端。

[0076] 步骤S213,客户端根据注册信息来验证待验证账户的账户信息和身份信息,在验证通过的情况下,执行虚拟资源的转移请求指令。

[0077] 本申请上述步骤S210至步骤S213,当客户端接收到虚拟资源的转移请求时,需要对指纹信息进行验证。此时通过指纹系统采集用户的指纹信息,并同时根据指纹信息生成一个指纹特征值,将指纹信息、与指纹信息对应的指纹特征值组成一组待验证账户信息。将待验证账户信息与设备终端中已经保存过的账户信息和身份认证信息进行第一次匹配。如果匹配成功,将待验证账户信息与客户端中存储的注册信息进行第二匹配,如果两次都匹配成功,则执行虚拟资源的转移请求指令。

[0078] 本申请上述实施例中的客户端可以是安装在终端设备(例如手机、计算机、IPAD等)上的应用客户端,该应用客户端可以是用于转移虚拟资源的虚拟资源转移客户端,例如,该虚拟资源转移客户端可以是支付终端,转移的虚拟资源可以是用于买卖商品的费用。

[0079] 以支付终端的支付系统为例,首先设备终端通过指纹系统采集待验证的待验证指纹信息,同时生成与指纹信息对应的指纹特征值,将待验证指纹信息和待验证指纹信息对应的指纹特征值作为待验证的待验证账户信息。将待验证账户信息与设备终端中存储的账户信息、身份认证信息进行匹配。如果匹配成功,则说明该待验证指纹在该设备终端的该系统账户中注册过。进而,将待验证账户信息与支付宝客户端中存储的注册信息进行匹配。如果匹配成功,说明该待验证指纹也在支付宝客户端中注册过。上述两次匹配成功后,支付宝客户端执行支付操作。

[0080] 可选的,上述方案进一步可以以使用支付宝客户端进行指纹支付为例进行说明。在上述终端设备上开通指纹支付功能时,需要对账户信息、指纹信息以及与指纹信息唯一对应的指纹特征值同时进行验证。此处的指纹特征值,可以利用指纹芯片的硬件序列号作为指纹特征值作为指纹特征值。支付系统对用户名、设备编号和指纹特征值同时进行校验,当用户名、设备编号和指纹特征值全部校验成功时,则开通指纹支付功能。如果在进行指纹支付操作时,同时也需要对用户名、设备编号和指纹特征值进行校验。

[0081] 这种支付系统利用用户名、设备编号和指纹特征值三个条件来确保开通过程是用户自己完成的方案,可以实现即使手机被入侵,入侵用户在存储器中添加一个仿制的指纹信息的情况下,由于身份认证信息包含了指纹信息及其唯一对应的指纹特征值,而该仿制的指纹信息生成的指纹特征值是与该仿制的指纹唯一对应,因此,非法入侵用户的仿制指纹信息通过了验证,但该仿制指纹的指纹特征值无法与合法的指纹特征值匹配,因此,入侵用户是无法成功通过验证的。

[0082] 本申请上述实施例提供的一种优选方案中,步骤S213执行虚拟资源的转移请求指令的方案可以通过如下实施步骤来实现:

[0083] 步骤S2131,验证待验证账户的虚拟资源的转移信息。

[0084] 步骤S2133，在转移信息准确的情况下，将转移信息和/或待验证账户的私钥签名发送至虚拟资源转移服务器，使得虚拟资源服务器根据虚拟资源的转移信息完成转移功能。

[0085] 本申请上述步骤S2131至步骤S2133中，验证待验证账户并验证通过之后，获取待验证账户对虚拟资源的转移信息，并验证转移信息的有效性。如果确认转移信息为有效时，将虚拟资源的转移信息和/或待验证账户的私钥签名发送至虚拟资源转移服务器端，虚拟资源转移服务器按照转移信息对待验证账户内的虚拟资源进行转移。

[0086] 如图5所示，图5结合上述实施例，本申请的设备终端可以是具有指纹芯片的移动设备，该移动设备安装的支付系统客户端为支付客户端。下面就以在移动终端中实现安全身份认证和支付认证的实施例为例，对本申请上述实施例进行详细说明如下：

[0087] 结合图6所示，支付宝客户端在移动终端中实现安全身份认证成功注册的实施方式可以包括以下步骤：

[0088] 步骤A，登录移动终端的操作系统，通过移动终端的指纹芯片采集用户的指纹信息。

[0089] 步骤B，移动终端生成与指纹信息唯一对应的指纹特征值，得到当前用户的身份认证信息。

[0090] 步骤C，将身份认证信息保存至移动设备的用于存储指纹信息的安全存储空间中。

[0091] 步骤D，登录支付宝客户端，支付宝客户端获取移动终端的安全存储空间中的身份认证信息。

[0092] 步骤E，支付宝客户端根据获取到的身份认证信息生成注册信息。

[0093] 步骤F，支付宝客户端对生成的注册信息进行加密处理。

[0094] 步骤G，将加密后的注册信息保存至支付宝客户端。

[0095] 结合图7所示，在上述图7所示的方案完成身份认证信息注册成功之后，支付宝客户端在移动终端中实现支付认证的过程可以包括以下步骤：

[0096] 步骤a，支付宝客户端接收支付请求。

[0097] 步骤b，支付宝客户端通过移动设备的指纹芯片采集待验证账户的指纹信息。

[0098] 步骤c，移动设备根据待验证账户的指纹信息生成与其对应的指纹特征值，得到待验证账户的身份认证信息。

[0099] 步骤d，移动设备判断待验证账户的身份认证信息和移动终端的安全存储空间中存储的身份认证信息是否匹配。

[0100] 步骤e，当待验证账户的身份认证信息和移动终端的安全存储空间中存储的身份认证信息匹配时，支付宝客户端将待验证账户的身份信息与支付宝客户端中存储的注册信息进行匹配。

[0101] 步骤f，当待验证账户的身份信息与支付宝客户端中存储的注册信息匹配时，支付请求被支付宝客户端接受。

[0102] 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。

[0103] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。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(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，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的方法。

[0104] 实施例2

[0105] 根据本发明实施例，还提供了一种用于实施上述基于指纹信息生成认证信息的方法的基于指纹信息生成认证信息的装置，图8是根据本发明实施例二的基于指纹信息生成认证信息的装置的示意图，如图8所示，该装置包括：采集模块32、获取模块34和保存模块36。

[0106] 其中，采集模块32，用于在当前账户登录指纹系统之后，采集当前账户录入的指纹信息。获取模块34，用于生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值。保存模块36，用于保存当前账户的账户信息和当前账户的身份认证信息至设备终端。

[0107] 由上可知，通过上述采集模块32、获取模块34和保存模块36，在设备终端完成上述当前账户的安全性注册之后，设备终端可以通过利用已经保存的指纹信息和与指纹信息唯一对应的指纹特征值来对用户的身份信息进行匹配，实现了在对用户的指纹信息进行验证的同时，还需要同时验证该指纹信息唯一对应的指纹特征值，来实现对任意一个访问该设备终端的用户进行校验的目的，避免了非法入侵、仿制指纹的用户来非法登录设备终端系统的问题，提高了对账户身份信息进行识别的安全性。

[0108] 在实际应用当中，用户在设备终端上录入指纹信息的过程中，设备终端对生成的指纹信息会被设置一个名称，例如：指纹1或者指纹2。同时，在录入指纹信息时为每个指纹信息生成一个唯一的指纹特征值。指纹特征值可以由时间、芯片等因素构成。可以用4个字节的整数进行表示，例如：指纹1：ID382931932832、指纹2：ID384838282322。

[0109] 以支付终端的支付系统为例，在上述终端设备上开通指纹支付功能时，需要对账户信息、指纹信息以及与指纹信息唯一对应的指纹特征值同时进行验证。此处的指纹特征值，可以利用指纹芯片的硬件序列号作为指纹特征值作为指纹特征值。支付系统对用户名、设备编号和指纹特征值同时进行校验，当用户名、设备编号和指纹特征值全部校验成功时，则开通指纹支付功能。如果在进行指纹支付操作时，同时也需要对用户名、设备编号和指纹特征值进行校验。

[0110] 这种支付系统利用用户名、设备编号和指纹特征值三个条件来确保开通过程是用户自己完成的方案，可以实现即使手机被入侵，入侵用户在存储器中添加一个仿制的指纹信息的情况下，由于身份认证信息包含了指纹信息及其唯一对应的指纹特征值，而该仿制的指纹信息生成的指纹特征值是与该仿制的指纹唯一对应，因此，非法入侵用户的仿制指纹信息通过了验证，但该仿制指纹的指纹特征值无法与合法的指纹特征值匹配，因此，入侵用户是无法成功通过验证的。

[0111] 由上可知，本申请上述实施例以提供的方案，在当前账户登录指纹系统之后，采集

与当前登录账号对应的指纹信息，并同时根据指纹信息，生成与指纹信息唯一对应的指纹特征值。将指纹信息和与指纹信息唯一对应的指纹特征值作为当前登录账号的身份认证信息，通过利用指纹信息和与指纹信息唯一对应的指纹特征值确认用户的身份信息的方法，来验证指纹信息的合法性，达到了以指纹特征值作为校验条件对指纹信息的真伪进行校验的目的，从而实现了指纹系统和账户信息对指纹信息的双重验证的效果，解决了单独凭借指纹信息与移动设备中存储的指纹信息进行比对的方式来确认用户身份信息，导致的安全性差，指纹信息容易被伪造的问题。

[0112] 此处需要说明的是，上述采集模块32、获取模块34和保存模块36对应于实施例一中的步骤S202至步骤S206，三个模块与对应的步骤所实现的示例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的移动终端10中。

[0113] 如图9所示，在本申请提供的一种可选实施例中，上述获取模块34包括如下任意一种功能模块：第一生成模块341、第二生成模块343、第三生成模块345和第四生成模块347。

[0114] 其中，第一生成模块341，用于根据指纹信息中所包含的指纹模板的图像信息生成指纹特征值；第二生成模块343，用于在通过指纹芯片采集指纹信息的情况下，根据指纹芯片的硬件序列号生成指纹特征值；第三生成模块345，用于根据指纹信息的采集时间来生成指纹特征值；第四生成模块347，用于根据如下任意多个参数的组合来生成指纹特征值：指纹模板的图像信息、指纹芯片的硬件序列号和指纹信息的采集时间。

[0115] 具体的，指纹特征值可以通过上述第一生成模块341、第二生成模块343、第三生成模块345和第四生成模块347中任意一个模块生成。除此之外，只要能够达到为指纹信息分配一个独一无二的随机数值，并且可以独立标识该指纹的目的的方式，都可以用来生成本方案中指纹特征值，此处不再赘述。

[0116] 此处需要说明的是，上述第一生成模块341、第二生成模块343、第三生成模块345和第四生成模块347对应于实施例一步骤S204的实现方式一至方式四，四个模块与对应的方案所包含的步骤的四种实现方式所实现的示例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的移动终端10中。

[0117] 此处需要说明的是，在保存模块36完成保存当前账户的账户信息和当前账户的身份认证信息至设备终端之后，本申请还可以包括如下验证功能模块：

[0118] 子采集模块，用于采集待验证账户的待验证指纹信息。用于在使用设备终端中设置的指纹芯片账户，该指纹芯片可以采集到当前待验证账户的指纹信息作为待验证的指纹信息。

[0119] 待验证信息生成模块，采用指纹特征值生成方式处理待验证指纹信息，生成与待验证账户的待验证指纹信息唯一对应的待验证指纹特征值。该功能中使用的指纹特征值生成方式与录入指纹时所采用的指纹特征值生成方式相同，即可以采用上述优选方案中的四种生成方式中的任意一种。

[0120] 用户验证模块，用于将待验证指纹信息和待验证指纹信息唯一对应的待验证指纹特征值与设备终端中已经保存的身份认证信息进行比对，在待验证指纹信息与身份认证信息中的指纹信息相匹配，且待验证指纹特征值与身份认证信息中的指纹特征值也相匹配的

情况下，待验证账户通过验证；在待验证指纹信息与身份认证信息中的指纹信息匹配失败，和/或待验证指纹特征值与身份认证信息中的指纹特征值也匹配失败的情况下，待验证账户为非法入侵用户。

[0121] 在本申请提供的一种可选实施例中，在当前账户录入至少两个指纹的指纹信息的情况下，身份认证信息还包括如下任意一种或多种信息：每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置。

[0122] 基于上述方案，即使通过非法的方式在终端设备中注册了合法的指纹信息，仍旧无法来正常登陆设备终端。例如入侵者通过制作纸模等方式仿制手指指纹得到指纹模板，这种盗取到的指纹模板可以骗过指纹芯片，即指纹芯片即便有活体识别能力，但这种仿制的指纹模板也可以使用指套等装置来骗过指纹芯片，完成认证过程。

[0123] 因此，为了更好的解决上述用户指纹信息被窃取导致的用户信息被泄露的问题，本申请上述实施例提供的一种优选方案中，在当前账户录入至少两个指纹的指纹信息的情况下，身份认证信息还可以包括如下任意一种或多种信息：每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置。即可以在采集指纹信息的同时，生成指纹信息的扩展信息，此处的扩展信息可以为上述指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置。优选的，指纹的移动轨迹可以包括如下任意一种移动方式：指纹延顺时针方向移动、指纹延逆时针方向移动、指纹从上至下移动或指纹从下至上移动。

[0124] 由此，设备终端认证当前登录账户时，不仅需要验证指纹信息本身，还需要进一步验证包含了上述扩展信息的身份认证信息。进而，在使用该设备终端进行虚拟资源转移(例如网络支付)的过程中，也可以利用上述扩展信息完成更加安全的支付过程。例如，在用户支付系统中进行指纹注册的时候(不是添加在设备中)，支付系统可以要求用户除了录入指纹以外，增加指纹的扩展信息。例如：[指纹1，录入方向，自上而下]、[指纹2，识别后进行了逆时针旋转]等。

[0125] 优选的，本申请上述实施例中，指纹的移动轨迹包括：指纹延顺时针方向移动、指纹延逆时针方向移动、指纹从上至下移动或指纹从下至上移动。

[0126] 由此可知，在实际应用当中，在对指纹信息进行采集时，除了根据指纹信息生成与指纹信息对应的指纹特征值，通过指纹特征值来验证用户身份之外，还可以采用录入多个指纹，并且记录每个指纹的录入顺序作为身份认证信息，或者在有能力记录指纹的识别方向的指纹系统中，记录指纹的录入方向、指纹的旋转方向作为指纹信息的身份认证信息。在开通和\或使用指纹支付功能时，对通过上述方式生成的拓展信息进行验证，从而对用户的身份进行验证。扩展信息的具体采集方式例如：以顺时针旋转自己的指纹的方式进行录入、在擦挂式指纹识别的设备上以由上至下移动手指或者以由下至上移动手指的方式进行录入。

[0127] 通过上述指纹信息的录入方式，采集到的指纹信息不再是唯一的或者静止的信息，指纹信息除了包括静止的指纹模板，还会包含由多种录入方案生成的与指纹信息对应的扩展信息，上述方案下，既有了传统指纹匹配的方便性，又加入了相较于传统密码更强的私有性。解决了目前的指纹技术上的安全性低的问题。

[0128] 以录入多个指纹，并记录每个指纹的录入顺序作为指纹信息的扩展信息的方式为例进行说明。当进行指纹录入的时候，用户可以录入多个相同或者不同的指纹信息来生成

一组身份认证信息。当用户录入了4次手指的指纹信息生成身份认证信息时，记录下用户的身份认证信息为：[user0001，device0001，fingerprint382931932831，fingerprint382931932831 fingerprint382931932831,fingerprint384838282322]。从上述身份认证信息中可以得知，前三次用户使用同一只手指进行了指纹的录入，而第四次用户使用了另外一只手指进行指纹的录入。通过上述方法，准确的记录了指纹的录入顺序和录入方式，提高了指纹系统的安全性。

[0129] 进一步的，以录入单个手指的指纹，并记录录入指纹时手指运动方向的方式为例进行说明。手指运动方向以供可以分为四种情况，分别为顺时针旋转、逆时针旋转、自下至上移动、自下至上移动，当进行指纹录入的时候，用户可以在录入指纹信息的同时，同时以上述四种运动方式中的一种进行运动，记录下用户的身份认证信息为[user0001，device0001,[fingerprint382931932831,orentation:04]]。除此之外，还可以在录入指纹信息时，读取设备终端的重力感应器来获取录入指纹时手机所处的状态(屏幕朝下还是朝上)来生成身份认证信息，具体方式此处不再赘述。

[0130] 优选的，如图10所示，本申请上述实施例中，装置还包括：注册模块37，用于将当前账户的账户信息和当前账户的身份认证信息注册至客户端，生成当前账户在客户端中的注册信息。

[0131] 具体的，通过上述注册模块37，用户可以将当前账户信息、指纹信息、与指纹信息对应的指纹特征值注册至客户端中。利用上述账户信息、指纹信息、与指纹信息对应的指纹特征值等信息，在客户端中生成指纹的注册信息。

[0132] 当客户端注册的过程中，在通过读取设备终端已存储的身份认证信息的同时，通过指纹系统获取用户指纹信息。当获取到的指纹信息、根据获取到的指纹信息生成的指纹特征值与已存储的身份认证信息中的信息匹配时，客户端对账户进行注册。

[0133] 以在安装有支付宝客户端(一种可选的客户端)的带有指纹系统的设备终端为例，当支付宝账号成功登陆支付宝之后，支付宝客户端读取设备终端内存储的账户信息身份认证信息，同时将通过指纹系统获取到的指纹信息、根据指纹信息生成的指纹特征值，与读取到的身份认证信息中的指纹信息、与指纹信息对应的指纹特征值进行匹配，在匹配成功时，利用指纹信息、与指纹信息对应的指纹特征值生成一组支付宝客户端用于验证用户身份的注册信息。

[0134] 进一步的，当通过注册模块37客户端中生成指纹的注册信息之后，将获取到的注册信息进行加密处理，以密文的形式存储至客户端内。当需要对虚拟资源进行转移时，通过将获取到的指纹信息、根据指纹信息生成的指纹特征值与解密后的注册信息进行比对，来完成对用户身份的验证步骤。上述注册信息既可以只存储于设备终端的本地客户端内，也可以同步至与客户端对应的虚拟资源转移服务端当中。

[0135] 将获取到的注册信息进行加密处理，以密文的形式存储至客户端内。当需要对虚拟资源进行转移时，通过将获取到的指纹信息、根据指纹信息生成的指纹特征值与解密后的注册信息进行比对，来完成对用户身份的验证步骤。上述注册信息既可以只存储于设备终端的本地客户端内，也可以同步至与客户端对应的虚拟资源转移服务端当中。

[0136] 此处需要说明的是，上述注册模块37对应于实施例一中的步骤S207，注册模块37与对应的方案所包含的步骤S207所实现的示例和应用场景相同，但不限于上述实施例一所

公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的移动终端10中。

[0137] 进一步的，本申请上述实施例提供的一种优选方案中，上述装置还可以执行如下实施步骤：

[0138] 步骤一，客户端接收到虚拟资源的转移请求指令。

[0139] 步骤二，通过设备终端上安装的指纹系统采集待验证账户的指纹信息。

[0140] 步骤三，在根据待验证账户的指纹信息生成待验证账户的身份信息之后，将待验证账户的账户信息和身份信息分别与设备终端中已经保存的账户信息和身份认证信息进行匹配，在匹配成功的情况下，将待验证账户的账户信息和待验证账户的身份信息发送至客户端。

[0141] 步骤四，客户端根据注册信息来验证待验证账户的账户信息和身份信息，在验证通过的情况下，执行虚拟资源的转移请求指令。

[0142] 本申请上述步骤，当客户端接收到虚拟资源的转移请求时，需要对指纹信息进行验证。此时通过指纹系统采集用户的指纹信息，并同时根据指纹信息生成一个指纹特征值，将指纹信息、与指纹信息对应的指纹特征值组成一组待验证账户信息。将待验证账户信息与设备终端中已经保存过的账户信息和身份认证信息进行第一次匹配。如果匹配成功，将待验证账户信息与客户端中存储的注册信息进行第二匹配，如果两次都匹配成功，则执行虚拟资源的转移请求指令。

[0143] 以使用支付宝客户端进行指纹支付为例进行说明。首先设备终端通过指纹系统采集待验证的待验证指纹信息，同时生成与指纹信息对应的指纹特征值，将待验证指纹信息和待验证指纹信息对应的指纹特征值作为待验证的待验证账户信息。将待验证账户信息与设备终端中存储的账户信息、身份认证信息进行匹配。如果匹配成功，则说明该待验证指纹在该设备终端的该系统账户中注册过。进而，将待验证账户信息与支付宝客户端中存储的注册信息进行匹配。如果匹配成功，说明该待验证指纹也在支付宝客户端中注册过。上述两次匹配成功后，支付宝客户端执行支付操作。

[0144] 进一步的，上述步骤四执行虚拟资源的转移请求指令的步骤可以包括：验证待验证账户的虚拟资源的转移信息。并在转移信息准确的情况下，将转移信息和/或待验证账户的私钥签名发送至虚拟资源转移服务器，使得虚拟资源服务器根据虚拟资源的转移信息完成转移功能。

[0145] 通过上述步骤，在验证待验证账户并验证通过之后，获取待验证账户对虚拟资源的转移信息，并验证转移信息的有效性。如果确认转移信息为有效时，将虚拟资源的转移信息和/或待验证账户的私钥签名发送至虚拟资源转移服务器端，虚拟资源转移服务器按照转移信息对待验证账户内的虚拟资源进行转移。

[0146] 实施例3

[0147] 图11是根据本发明实施例三的一种基于指纹信息生成认证信息的系统的结构框图。

[0148] 如图11所示，该基于指纹信息生成认证信息的系统可以包括：指纹芯片112、处理器114、存储器116。

[0149] 其中，指纹芯片112，用于在当前账户登录指纹系统之后，采集当前账户录入的指

纹信息。

[0150] 通过指纹芯片112,用户在以当前账户的账户信息登录指纹系统之后,可以通过安装了该指纹系统的终端设备中内置的指纹信息来采集指纹信息。例如,一台移动设备,用户使用当前账户信息登录移动设备中的指纹系统,并在触摸移动设备提供的指纹芯片之后,通过该指纹系统采集到当前用户的指纹信息。

[0151] 其中,上述指纹信息是包含了用户的指纹细节特征的数字信息,可以通过指纹芯片对指纹进行采集,也可以通过识别包含指纹信息的图片的方式进行采集。

[0152] 处理器114,与指纹芯片连接,用于生成与指纹信息唯一对应的指纹特征值,确定当前账户的身份认证信息,其中,身份认证信息至少包括:指纹信息和与指纹信息唯一对应的指纹特征值。

[0153] 在当前账户登陆指纹系统并通过指纹芯片112采集到对应的指纹信息之后,通过处理器34生成与指纹信息唯一对应的指纹特征值。将指纹信息和与指纹信息唯一对应的指纹特征值进行关联,并利用指纹信息和与指纹信息唯一对应的指纹特征值生成当前账户的一组身份认证信息。

[0154] 此处需要说明的是,指纹特征值用于标识采集到的指纹信息具有唯一性,系统可以采用如下方式来生成该指纹特征值:指纹模板的图像像素值、指纹模板的图像容量大小、指纹芯片的序列号、设备终端的MAC地址等。

[0155] 指纹系统根据系统本身的属性生成指纹特征值。生成指纹特征值时,对于多个不同的指纹信息,采用随机的指纹特征值算法。但是对于相同的指纹信息,在每次生成指纹特征值时,所使用的生成算法是相同的。所以,即使手机被入侵,入侵用户在存储器中添加一个仿制的指纹信息,也无法仿制与指纹信息对应的指纹特征值。并且,指纹特征值时指纹系统根据系统本身的属性随机生成出来的,所以,指纹特征码一旦脱离系统本身用在其他指纹系统中时,因为系统本身的属性不同,所以指纹特征码也就失效了。

[0156] 存储器116,与处理器连接,用于保存当前账户的账户信息和当前账户的身份认证信息。

[0157] 将当前登录账户的账户信息和身份认证信息保存在当前的设备终端的存储器36中,即完成了在设备终端注册安全用户的功能,这种注册了用于验证身份的数据的设备终端具有更高的安全性。

[0158] 由上可知,在设备终端完成上述当前账户的安全性注册之后,设备终端可以通过利用已经保存的指纹信息和与指纹信息唯一对应的指纹特征值来对用户的身份信息进行匹配,实现了在对用户的指纹信息进行验证的同时,还需要同时验证该指纹信息唯一对应的指纹特征值,来实现对任意一个访问该设备终端的用户进行校验的目的,避免了非法入侵、仿制指纹的用户来非法登录设备终端系统的问题,提高了对账户身份信息进行识别的安全性。

[0159] 进一步的,处理器114生成与指纹信息唯一对应的指纹特征值可以包括如下任意一种方式:

[0160] 方式一:根据指纹信息中所包含的指纹模板的图像信息生成指纹特征值。

[0161] 具体的,因为各个移动终端所配置的指纹采集模块的型号不同,以及各个制造移动终端的硬件厂商对于采集得到的指纹信息的处理方式也不同,所以导致采集到的、处理

后的包含有指纹模板的图像信息的像素值、纵横比或图片大小也不相同。因此，利用像素值、纵横比和/或图片大小参数作为指纹特征值，可以达到对指纹信息进行唯一标识的作用。

[0162] 方式二：在通过指纹芯片采集指纹信息的情况下，根据指纹芯片的硬件序列号生成指纹特征值。

[0163] 具体的，在芯片制造过程中，制造厂家会对生产的每个硬件分配不同的硬件序列号以便于生产管理。因此，利用可以达到对指纹信息进行唯一标识的作用。

[0164] 方式三：根据指纹信息的采集时间来生成指纹特征值。

[0165] 方式四：根据如下任意多个参数的组合来生成指纹特征值：指纹模板的图像信息、指纹芯片的硬件序列号和指纹信息的采集时间。

[0166] 具体的，可以通过上述四种生成指纹特征值方式中的任意一种对指纹特征值进行你给生成。除此之外，只要能够达到为指纹信息分配一个独一无二的随机数值，并且可以独立标识该指纹的目的的方式，都可以用来生成本方案中指纹特征值，此处不再赘述。

[0167] 本申请上述实施例提供的一种优选方案中，在当前账户录入至少两个指纹的指纹信息的情况下，身份认证信息还包括如下任意一种或多种信息：每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置。

[0168] 此处需要说明的是，在保存当前账户的账户信息和当前账户的身份认证信息至设备终端之后，本申请还可以执行如下验证步骤：

[0169] 首先，采集待验证账户的待验证指纹信息。用于在使用设备终端中设置的指纹芯片账户，该指纹芯片可以采集到当前待验证账户的指纹信息作为待验证的指纹信息。

[0170] 然后，采用指纹特征值生成方式处理待验证指纹信息，生成与待验证账户的待验证指纹信息唯一对应的待验证指纹特征值。该步骤中使用的指纹特征值生成方式与录入指纹时所采用的指纹特征值生成方式相同，即可以采用上述优选方案中的四种生成方式中的任意一种。

[0171] 接着，将待验证指纹信息和待验证指纹信息唯一对应的待验证指纹特征值与设备终端中已经保存的身份认证信息进行比对，在待验证指纹信息与身份认证信息中的指纹信息相匹配，且待验证指纹特征值与身份认证信息中的指纹特征值也相匹配的情况下，待验证账户通过验证；在待验证指纹信息与身份认证信息中的指纹信息匹配失败，和/或待验证指纹特征值与身份认证信息中的指纹特征值也匹配失败的情况下，待验证账户为非法入侵用户。

[0172] 基于上述方案，即使通过非法的方式在终端设备中注册了合法的指纹信息，仍旧无法来正常登陆设备终端。例如入侵者通过制作纸模等方式仿制手指指纹得到指纹模板，这种盗取到的指纹模板可以骗过指纹芯片，即指纹芯片即便有活体识别能力，但这种仿制的指纹模板也可以使用指套等装置来骗过指纹芯片，完成认证过程。

[0173] 因此，为了更好的解决上述用户指纹信息被窃取导致的用户信息被泄露的问题，本申请上述实施例提供的一种优选方案中，在当前账户录入至少两个指纹的指纹信息的情况下，身份认证信息还可以包括如下任意一种或多种信息：每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置。即可以在采集指纹信息的同时，生成指纹信息的扩展信息，此处的扩展信息可以为上述指纹信息的录入顺序、每个指纹的移动轨迹和每个

指纹的录入位置。优选的，指纹的移动轨迹可以包括如下任意一种移动方式：指纹延顺时针方向移动、指纹延逆时针方向移动、指纹从上至下移动或指纹从下至上移动。

[0174] 由此，设备终端认证当前登录账户时，不仅需要验证指纹信息本身，还需要进一步验证包含了上述扩展信息的身份认证信息。进而，在使用该设备终端进行虚拟资源转移(例如网络支付)的过程中，也可以利用上述扩展信息完成更加安全的支付过程。例如，在用户支付系统中进行指纹注册的时候(不是添加在设备中)，支付系统可以要求用户除了录入指纹以外，增加指纹的扩展信息。例如：[指纹1，录入方向，自上而下]、[指纹2，识别后进行了逆时针旋转]等。

[0175] 优选的，本申请上述实施例中，指纹的移动轨迹包括：指纹延顺时针方向移动、指纹延逆时针方向移动、指纹从上至下移动或指纹从下至上移动。

[0176] 由此可知，在实际应用当中，在对指纹信息进行采集时，除了根据指纹信息生成与指纹信息对应的指纹特征值，通过指纹特征值来验证用户身份之外，还可以采用录入多个指纹，并且记录每个指纹的录入顺序作为身份认证信息，或者在有能力记录指纹的识别方向的指纹系统中，记录指纹的录入方向、指纹的旋转方向作为指纹信息的身份认证信息。在开通和\或使用指纹支付功能时，对通过上述方式生成的拓展信息进行验证，从而对用户的身份进行验证。扩展信息的具体采集方式例如：以顺时针旋转自己的指纹的方式进行录入、在擦挂式指纹识别的设备上以由上至下移动手指或者以由下至上移动手指的方式进行录入。

[0177] 通过上述指纹信息的录入方式，采集到的指纹信息不再是唯一的或者静止的信息，指纹信息除了包括静止的指纹模板，还会包含由多种录入方案生成的与指纹信息对应的扩展信息，上述方案下，既有了传统指纹匹配的方便性，又加入了相较于传统密码更强的私有性。解决了目前的指纹技术上的安全性低的问题。

[0178] 进一步的，当通过存储器116保存当前账户的账户信息和当前账户的身份认证信息至设备终端之后，在上述系统中还可以执行如下实施步骤：

[0179] 步骤一，将当前账户的账户信息和当前账户的身份认证信息注册至客户端，生成当前账户在客户端中的注册信息。

[0180] 步骤二，在客户端验证注册信息通过的情况下，将注册信息进行加密。

[0181] 步骤三，客户端保存加密后的注册信息。

[0182] 具体的，通过上述步骤，将获取到的注册信息进行加密处理，以密文的形式存储至客户端内。当需要对虚拟资源进行转移时，通过将获取到的指纹信息、根据指纹信息生成的指纹特征值与解密后的注册信息进行比对，来完成对用户身份的验证步骤。上述注册信息既可以只存储于设备终端的本地客户端内，也可以同步至与客户端对应的虚拟资源转移服务端当中。

[0183] 进一步的，在客户端保存加密后的注册信息之后，系统还可以执行如下实施：客户端接收到虚拟资源的转移请求指令。通过设备终端上安装的指纹系统采集待验证账户的指纹信息。在根据待验证账户的指纹信息生成待验证账户的身份信息之后，将待验证账户的账户信息和身份信息分别与设备终端中已经保存的账户信息和身份认证信息进行匹配，在匹配成功的情况下，将待验证账户的账户信息和待验证账户的身份信息发送至客户端。客户端根据注册信息来验证待验证账户的账户信息和身份信息，在验证通过的情况下，执行

虚拟资源的转移请求指令。

[0184] 具体的，当客户端接收到虚拟资源的转移请求时，需要对指纹信息进行验证。此时通过指纹系统采集用户的指纹信息，并同时根据指纹信息生成一个指纹特征值，将指纹信息、与指纹信息对应的指纹特征值组成一组待验证账户信息。将待验证账户信息与设备终端中已经保存过的账户信息和身份认证信息进行第一次匹配。如果匹配成功，将待验证账户信息与客户端中存储的注册信息进行第二匹配，如果两次都匹配成功，则执行虚拟资源的转移请求指令。

[0185] 进一步的，执行虚拟资源的转移请求指令的方案可以通过如下实施步骤来实现：验证待验证账户的虚拟资源的转移信息。在转移信息准确的情况下，将转移信息和/或待验证账户的私钥签名发送至虚拟资源转移服务器，使得虚拟资源服务器根据虚拟资源的转移信息完成转移功能。

[0186] 通过本申请上述步骤，在验证待验证账户并验证通过之后，获取待验证账户对虚拟资源的转移信息，并验证转移信息的有效性。如果确认转移信息为有效时，将虚拟资源的转移信息和/或待验证账户的私钥签名发送至虚拟资源转移服务器端，虚拟资源转移服务器按照转移信息对待验证账户内的虚拟资源进行转移。

[0187] 此处需要说明的是，本申请实施例3所涉及到的系统实施例可以包括多个可选的或优选的实施例，可选的或优选的实施例可以与实施例1或实施例2提供的优选或可选实施例相同，但不限于上述实施例1或实施例2提供的优选或可选实施例。

[0188] 实施例4

[0189] 本发明的实施例可以提供一种移动终端，该移动终端可以是移动终端群中的任意一个移动终端设备。可选地，在本实施例中，上述移动终端也可以替换为移动终端等终端设备。

[0190] 可选地，在本实施例中，上述移动终端可以位于计算机网络的多个网络设备中的至少一个网络设备。

[0191] 在本实施例中，上述移动终端可以执行应用程序的漏洞检测方法中以下步骤的程序代码：在当前账户登录指纹系统之后，采集当前账户录入的指纹信息；生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值；保存当前账户的账户信息和当前账户的身份认证信息至设备终端。

[0192] 可选地，该移动终端A可以包括：一个或多个(图中仅示出一个)处理器51、存储器53、以及传输装置55。

[0193] 其中，存储器53可用于存储软件程序以及模块，如本发明实施例中的安全漏洞检测方法和装置对应的程序指令/模块，处理器51通过运行存储在存储器53内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的系统漏洞攻击的检测方法。存储器53可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器53可进一步包括相对于处理器51远程设置的存储器，这些远程存储器可以通过网络连接至终端A。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0194] 上述的传输装置55用于经由一个网络接收或者发送数据。上述的网络具体实例可

包括有线网络及无线网络。在一个实例中，传输装置55包括一个网络适配器(Network Interface Controller,NIC)，其可通过网线与其他网络设备与路由器相连从而可与互联网或局域网进行通讯。在一个实例中，传输装置55为射频(Radio Frequency,RF)模块，其用于通过无线方式与互联网进行通讯。

[0195] 其中，具体地，存储器53用于存储预设动作条件和预设权限用户的信息、以及应用程序。

[0196] 处理器51可以通过传输装置调用存储器53存储的信息及应用程序，以执行下述步骤：在当前账户登录指纹系统之后，采集当前账户录入的指纹信息；生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值；保存当前账户的账户信息和当前账户的身份认证信息至设备终端。

[0197] 可选的，上述处理器51还可以执行如下步骤的程序代码：根据指纹信息中所包含的指纹模板的图像信息生成指纹特征值；在通过指纹芯片采集指纹信息的情况下，根据指纹芯片的硬件序列号生成指纹特征值；根据指纹信息的采集时间来生成指纹特征值；根据如下任意多个参数的组合来生成指纹特征值：指纹模板的图像信息、指纹芯片的硬件序列号和指纹信息的采集时间。

[0198] 可选的，上述处理器51还可以执行如下步骤的程序代码：在当前账户录入至少两个指纹的指纹信息的情况下，身份认证信息还包括如下任意一种或多种信息：每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置。

[0199] 可选的，上述处理器51还可以执行如下步骤的程序代码：将当前账户的账户信息和当前账户的身份认证信息注册至客户端，生成当前账户在客户端中的注册信息；在客户端验证注册信息通过的情况下，将注册信息进行加密；客户端保存加密后的注册信息。

[0200] 可选的，上述处理器51还可以执行如下步骤的程序代码：客户端接收到虚拟资源的转移请求指令；通过设备终端上安装的指纹系统采集待验证账户的指纹信息；在根据待验证账户的指纹信息生成待验证账户的身份信息之后，将待验证账户的账户信息和身份信息分别与设备终端中已经保存的账户信息和身份认证信息进行匹配，在匹配成功的情况下，将待验证账户的账户信息和待验证账户的身份信息发送至客户端；客户端根据注册信息来验证待验证账户的账户信息和身份信息，在验证通过的情况下，执行虚拟资源的转移请求指令。

[0201] 可选的，上述处理器51还可以执行如下步骤的程序代码：验证待验证账户的虚拟资源的转移信息；在转移信息准确的情况下，将转移信息和/或待验证账户的私钥签名发送至虚拟资源转移服务器，使得虚拟资源服务器根据虚拟资源的转移信息完成转移功能。

[0202] 采用本发明实施例，提供了一种基于指纹信息生成认证信息的方案。通过在当前账户登录指纹系统之后，采集当前账户录入的指纹信息；生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值；保存当前账户的账户信息和当前账户的身份认证信息至设备终端，从而达到了以指纹特征值作为校验条件对指纹信息的真伪进行校验的目的，进而解决了单独凭借指纹信息与移动设备中存储的指纹信息进行比对的方式来确认用户身份信息，导致的安全性差，指纹信息容易被伪造的技术问题。

[0203] 本领域普通技术人员可以理解，图1所示的结构仅为示意，移动终端也可以是智能手机(如Android手机、iOS手机等)、平板电脑、掌声电脑以及移动互联网设备(Mobile Internet Devices，MID)、PAD等终端设备。图1其并不对上述电子装置的结构造成限定。例如，移动终端10还可包括比图1中所示更多或者更少的组件(如网络接口、显示装置等)，或者具有与图1所示不同的配置。

[0204] 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终端设备相关的硬件来完成，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。

[0205] 实施例5

[0206] 本发明的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以用于保存上述实施例一所提供的基于指纹信息生成认证信息的方法所执行的程序代码。

[0207] 可选地，在本实施例中，上述存储介质可以位于计算机网络中移动终端群中的任意一个移动终端中，或者位于移动终端群中的任意一个移动终端中。

[0208] 可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：在当前账户登录指纹系统之后，采集当前账户录入的指纹信息；生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息，其中，身份认证信息至少包括：指纹信息和与指纹信息唯一对应的指纹特征值；保存当前账户的账户信息和当前账户的身份认证信息至设备终端。

[0209] 可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：根据指纹信息中所包含的指纹模板的图像信息生成指纹特征值；在通过指纹芯片采集指纹信息的情况下，根据指纹芯片的硬件序列号生成指纹特征值；根据指纹信息的采集时间来生成指纹特征值；根据如下任意多个参数的组合来生成指纹特征值：指纹模板的图像信息、指纹芯片的硬件序列号和指纹信息的采集时间。

[0210] 可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：在当前账户录入至少两个指纹的指纹信息的情况下，身份认证信息还包括如下任意一种或多种信息：每个指纹信息的录入顺序、每个指纹的移动轨迹和每个指纹的录入位置。

[0211] 可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：将当前账户的账户信息和当前账户的身份认证信息注册至客户端，生成当前账户在客户端中的注册信息；在客户端验证注册信息通过的情况下，将注册信息进行加密；客户端保存加密后的注册信息。

[0212] 可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：客户端接收到虚拟资源的转移请求指令；通过设备终端上安装的指纹系统采集待验证账户的指纹信息；在根据待验证账户的指纹信息生成待验证账户的身份信息之后，将待验证账户的账户信息和身份信息分别与设备终端中已经保存的账户信息和身份认证信息进行匹配，在匹配成功的情况下，将待验证账户的账户信息和待验证账户的身份信息发送至客户端；客户端根据注册信息来验证待验证账户的账户信息和身份信息，在验证通过的情况下，执行虚拟资源的转移请求指令。

[0213] 可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：验

证待验证账户的虚拟资源的转移信息;在转移信息准确的情况下,将转移信息和/或待验证账户的私钥签名发送至虚拟资源转移服务器,使得虚拟资源服务器根据虚拟资源的转移信息完成转移功能。

[0214] 此处需要说明的是,上述移动终端群中的任意一个可以与网站服务器和扫描器建立通信关系,扫描器可以扫描移动终端上php执行的web应用程序的值命令。

[0215] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0216] 在本发明的上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其他实施例的相关描述。

[0217] 在本申请所提供的几个实施例中,应该理解到,所揭露的客户端,可通过其它的方式实现。其中,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,单元或模块的间接耦合或通信连接,可以是电性或其它的形式。

[0218] 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。

[0219] 另外,在本发明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。

[0220] 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时,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。

[0221] 以上所述仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

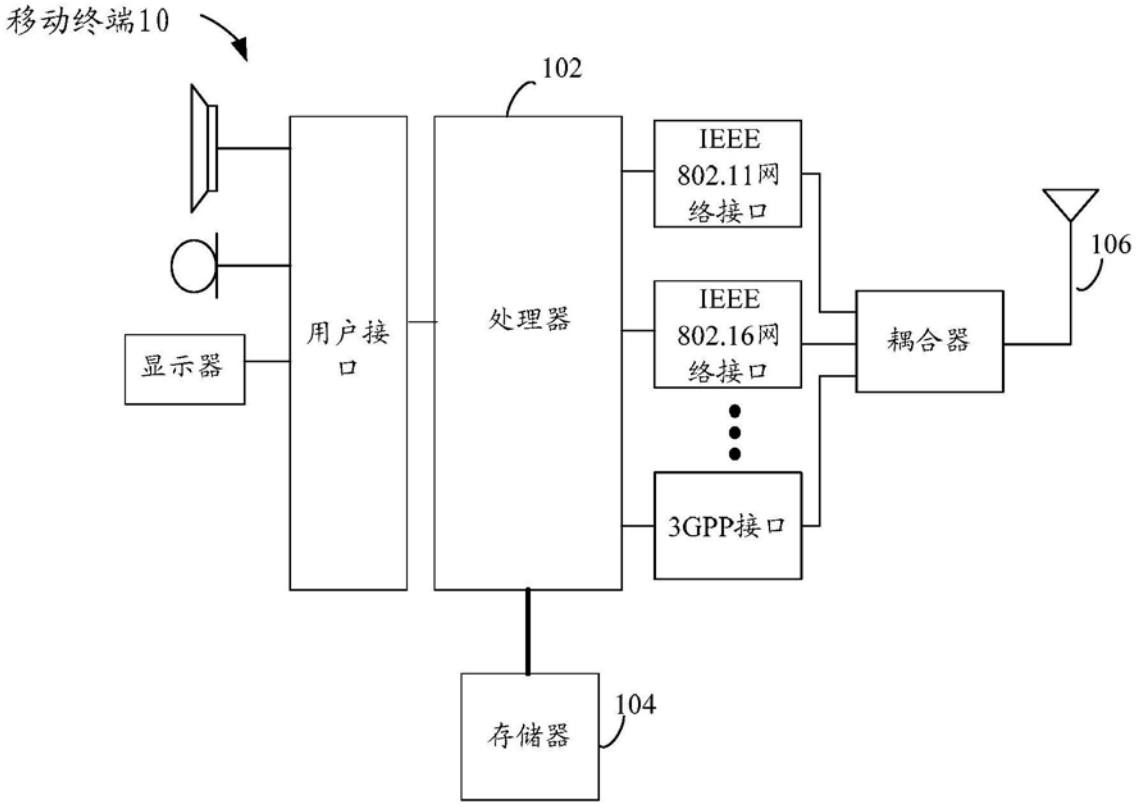

移动终端10
102
IEEE 802.11网络接口
IEEE 802.16网络接口
3GPP接口
106
耦合器
用户接口
处理器
显示器
存储器
104

图1

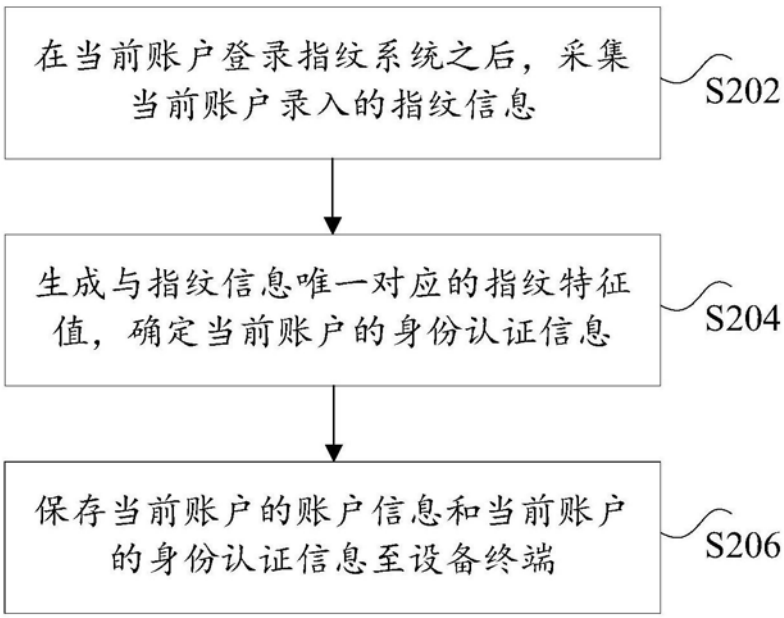

在当前账户登录指纹系统之后，采集当前账户录入的指纹信息
S202
生成与指纹信息唯一对应的指纹特征值，确定当前账户的身份认证信息
S204
保存当前账户的账户信息和当前账户的身份认证信息至设备终端
S206

图2

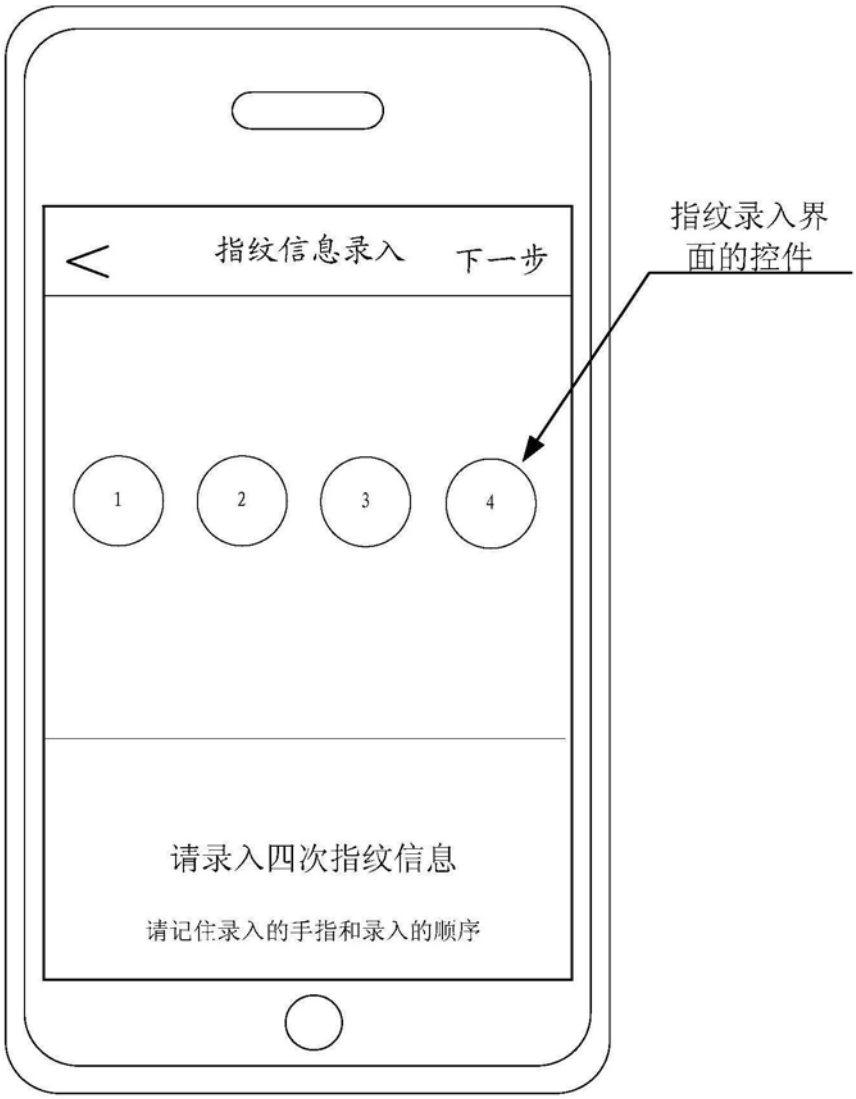


图3

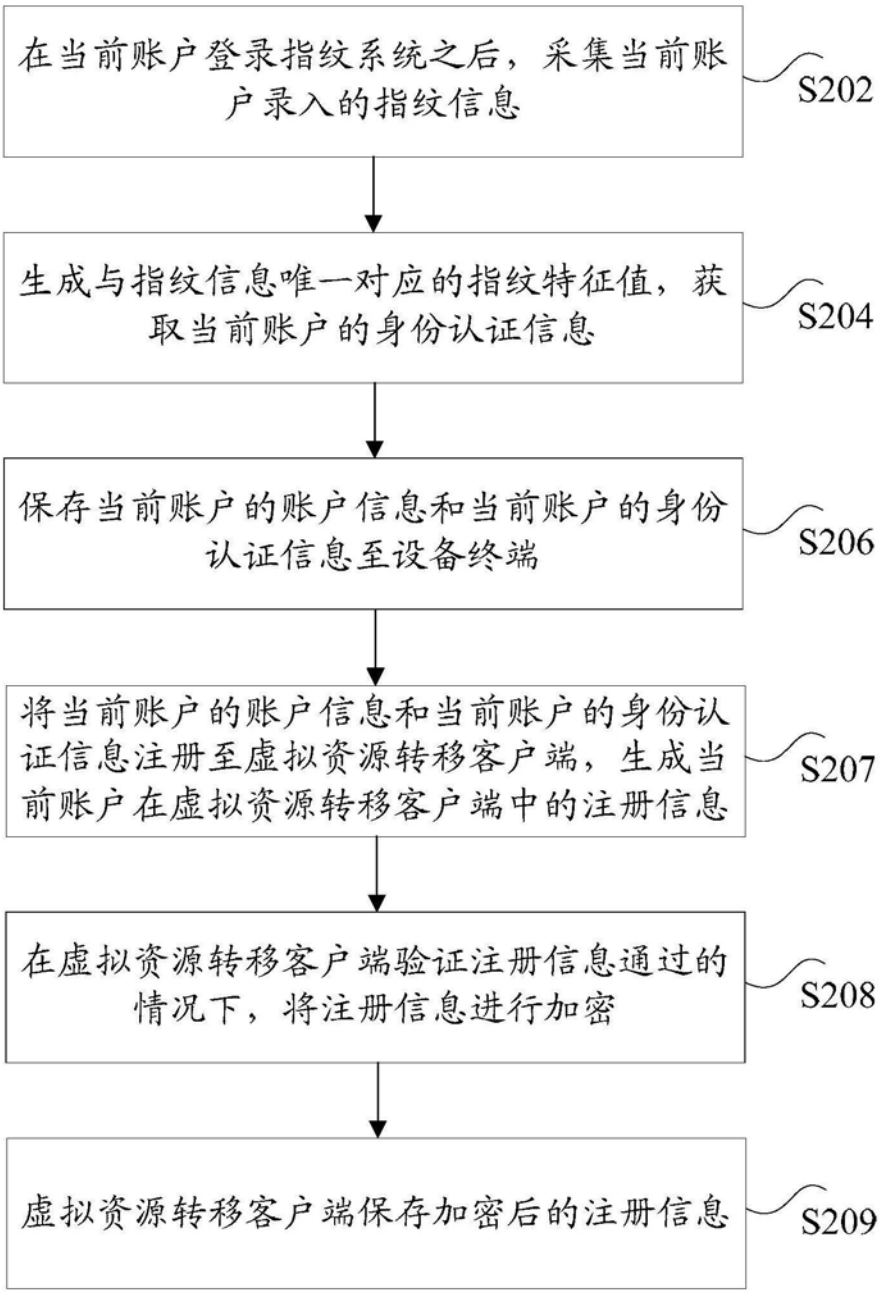

在当前账户登录指纹系统之后，采集当前账户录入的指纹信息
S202
生成与指纹信息唯一对应的指纹特征值，获取当前账户的身份认证信息
S204
保存当前账户的账户信息和当前账户的身份认证信息至设备终端
S206
将当前账户的账户信息和当前账户的身份认证信息注册至虚拟资源转移客户端，生成当前账户在虚拟资源转移客户端中的注册信息
S207
在虚拟资源转移客户端验证注册信息通过的情况下，将注册信息进行加密
S208
虚拟资源转移客户端保存加密后的注册信息
S209

图4

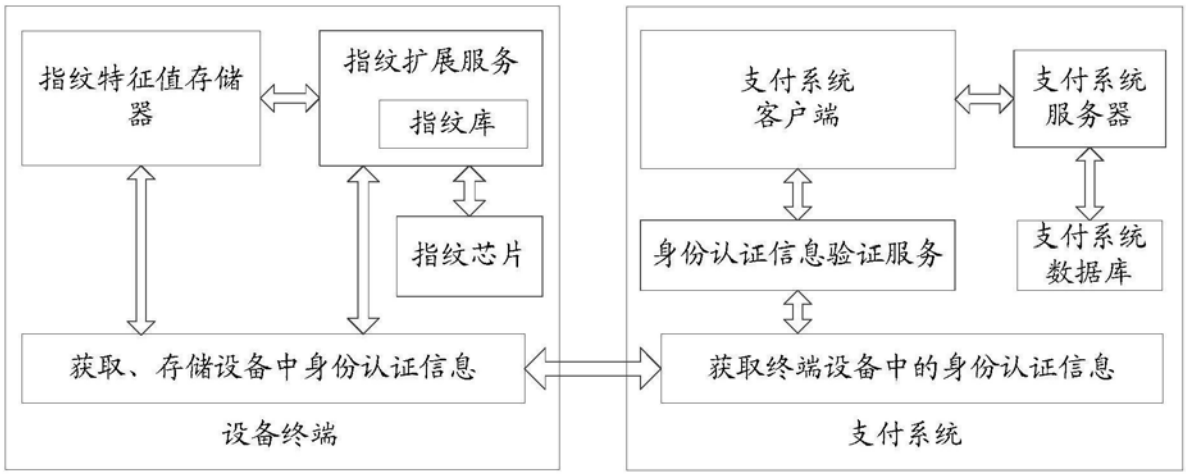

指纹特征值存储器
指纹扩展服务
指纹库
指纹芯片
获取、存储设备中身份认证信息
设备终端
支付系统客户端
支付系统服务器
身份认证信息验证服务
支付系统数据库
获取终端设备中的身份认证信息
支付系统

图5

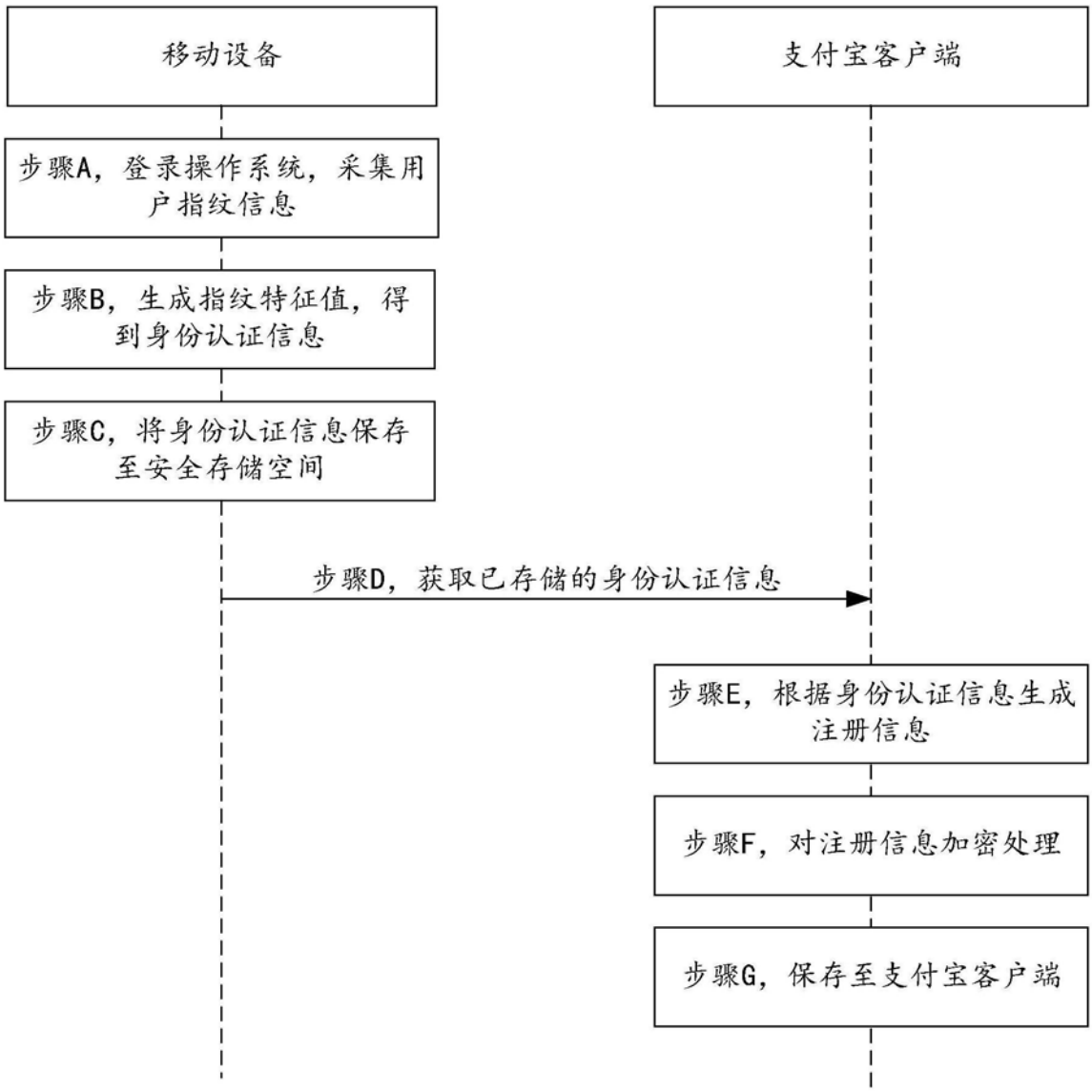

移动设备
支付宝客户端
步骤A，登录操作系统，采集用户指纹信息
步骤B，生成指纹特征值，得到身份认证信息
步骤C，将身份认证信息保存至安全存储空间
步骤D，获取已存储的身份认证信息
步骤E，根据身份认证信息生成注册信息
步骤F，对注册信息加密处理
步骤G，保存至支付宝客户端

图6

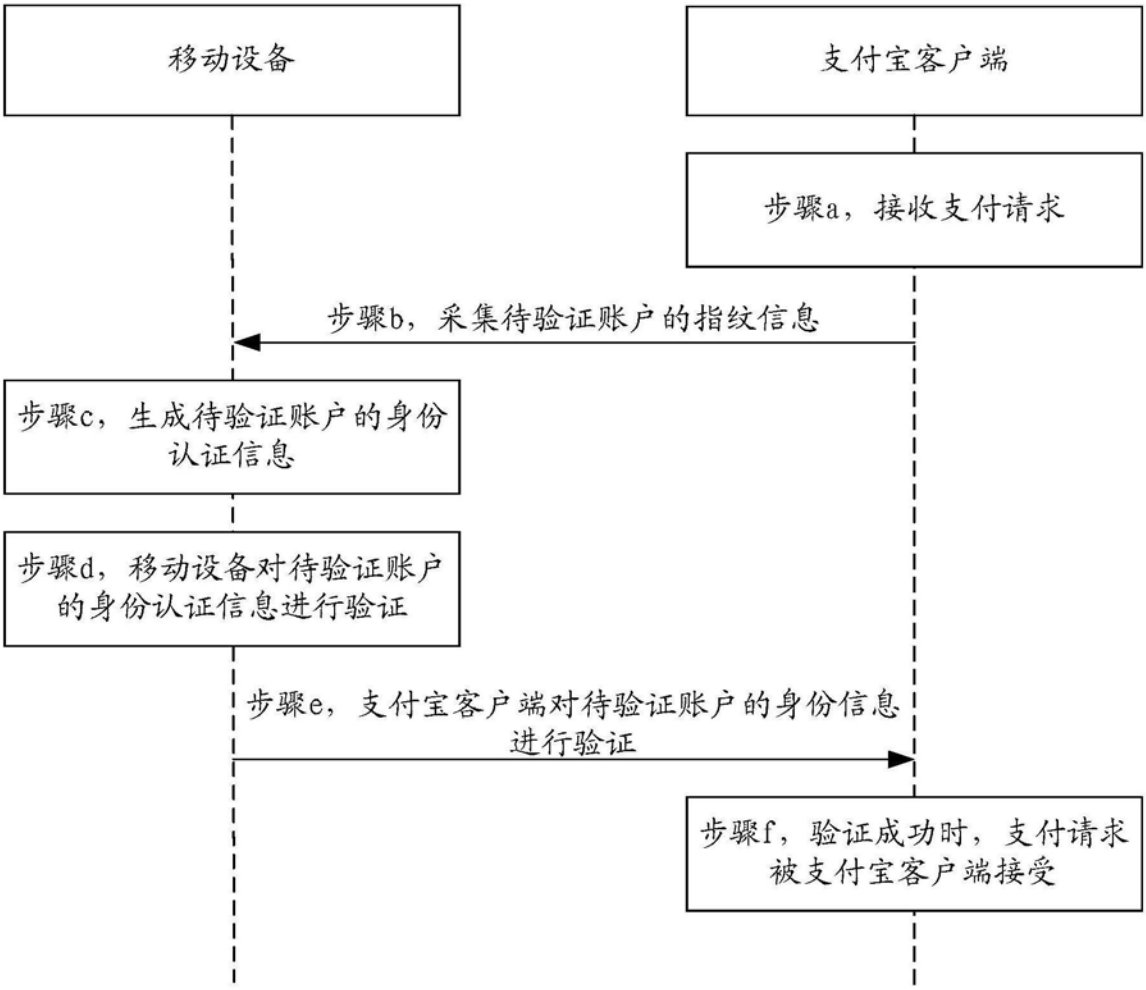

移动设备
支付宝客户端
步骤a，接收支付请求
步骤b，采集待验证账户的指纹信息
步骤c，生成待验证账户的身份认证信息
步骤d，移动设备对待验证账户的身份认证信息进行验证
步骤e，支付宝客户端对待验证账户的身份信息进行验证
步骤f，验证成功时，支付请求被支付宝客户端接受

图7


采集模块 32
获取模块 34
保存模块 36

图8

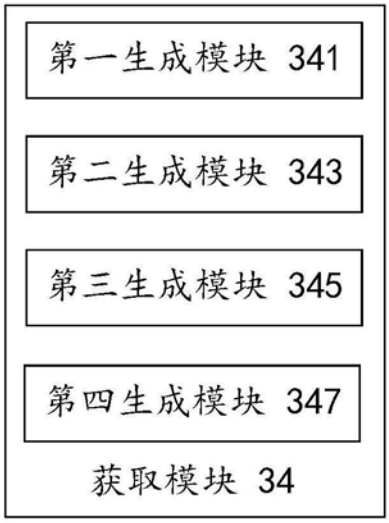

第一生成模块 341
第二生成模块 343
第三生成模块 345
第四生成模块 347
获取模块 34

图9

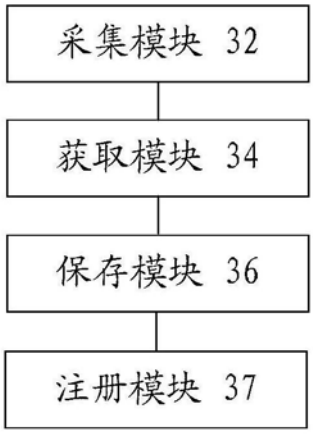

采集模块 32
获取模块 34
保存模块 36
注册模块 37

图10

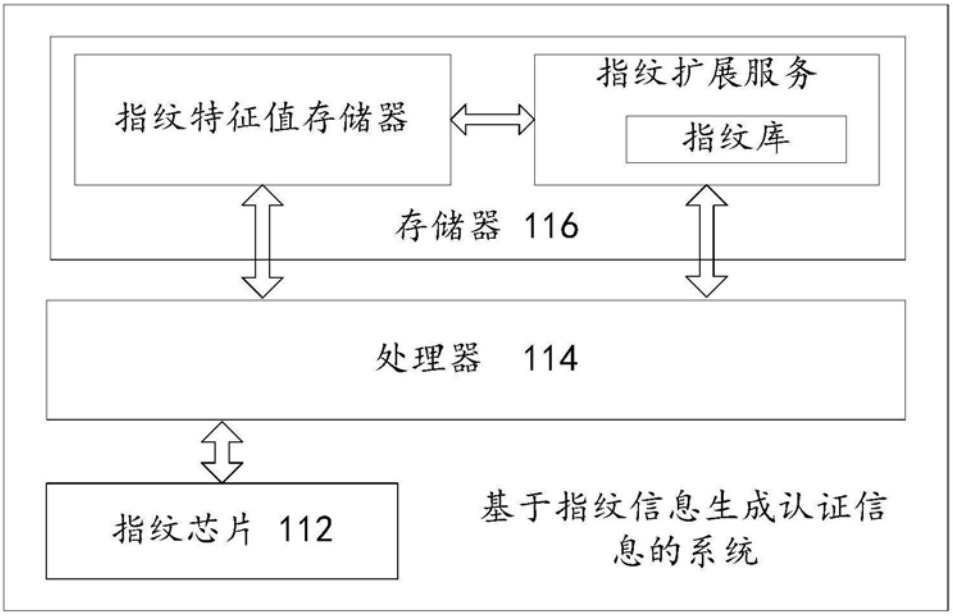

指纹特征值存储器
指纹扩展服务
指纹库
存储器 116
处理器 114
指纹芯片 112
基于指纹信息生成认证信息的系统

图11