(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110555706 B
(45)授权公告日 2024.08.06

(21)申请号 201910812958.3

(22)申请日 2019.08.30

(65)同一申请的已公布的文献号
申请公布号 CN 110555706 A

(43)申请公布日 2019.12.10

(73)专利权人 北京银联金卡科技有限公司
地址 100041 北京市石景山区实兴大街30号院18号楼1层

(72)发明人 杨波 于鸽 尚可 董晶

(74)专利代理机构 北京北新智诚知识产权代理有限公司 11100
专利代理师 满靖

(51)Int.Cl.
G06Q 20/40(2012.01)
G06Q 20/38(2012.01)

(56)对比文件
CN 107679861 A,2018.02.09
CN 109191131 A,2019.01.11
CN 113902446 A,2022.01.07
CN 210691384 U,2020.06.05

审查员 王鑫

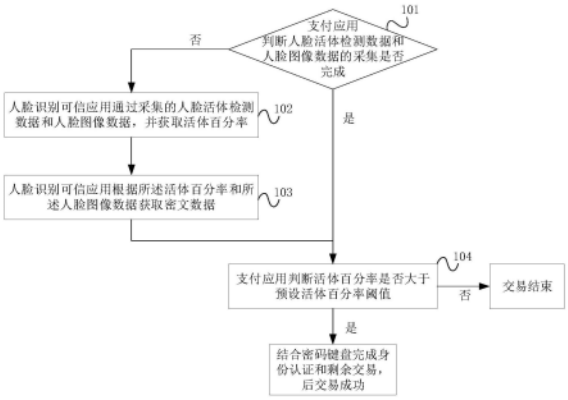
权利要求书2页 说明书10页 附图4页

(54)发明名称

基于安全单元和可信执行环境的人脸支付安全方法及平台

(57)摘要

本发明提供基于安全单元和可信执行环境的人脸支付安全方法及平台,通过人脸识别可信应用和人脸识别摄像头采集的人脸活体检测数据和人脸图像数据,可信执行环境计算获取活体百分率后调用安全单元获取百分率签名结果及密文数据,支付应用判断活体百分率是否大于预设活体百分率阈值,若大于则在富执行环境中结合密码键盘进行用户身份认证和剩余交易。本方案中,安全单元提供安全的密码学算法服务和人脸识别数据保护密钥,可信执行环境保证了人脸活体检测算法的安全执行,并通过与人脸识别摄像头直连保证了人脸支付过程中各数据的完整性、认证性和机密性的保护。



CN 110555706 B

1.基于安全单元和可信执行环境的人脸支付安全方法,其特征在于,包括:

支付应用触发人脸识别支付业务后若未完成人脸识图像抓取和活检,则激活TEE管理器,从而调起可信执行环境中的人脸识别可信应用,人脸识别可信应用激活人脸识别摄像头;

所述人脸识别可信应用根据与TEE直连的人脸识别摄像头采集的人脸活体检测数据l和人脸图像数据p,并将两个数据直接传入TEE中的人脸识别可信应用,人脸识别可信应用计算活体百分率r;

人脸识别可信应用通过TEE调用安全单元的接口,将活体百分率r和人脸图像数据p发送至安全单元,安全单元调用签名算法SIG使用私钥SK_{Face}对活体百分率r和人脸图像数据p进行签名运算,得到签名结果s;

安全单元调用加密算法进行数据处理得到密文数据m;具体的,密文数据m为:签名结果s、活体百分率r和人脸图像数据p三者的加密结果;

人脸识别可信应用接收签名结果s和密文数据m回传至所述人脸识别可信应用;

人脸识别可信应用接收密文数据m和活体百分率r发送至支付应用,此时,支付应用已完成人脸图像的抓取和活体检测,并获得了用于验证消费者身份信息的密文数据m,等待发送至后台认证服务器;

支付应用判断所述活体百分率是否大于预设活体百分率阈值,若大于则进行身份认证,通过后进入支付流程。

2.根据权利要求1所述的基于安全单元和可信执行环境的人脸支付安全方法,其特征在于,所述可信执行环境中的人脸识别可信应用根据采集的人脸活体检测数据和人脸图像数据,包括:

支付应用判断所述人脸活体检测数据和人脸图像数据的采集是否完成;

若未完成,所述支付应用通过可信执行环境调用所述人脸识别可信应用;

所述人脸识别可信应用激活人脸识别摄像头用于抓取人脸数据。

3.根据权利要求2所述的基于安全单元和可信执行环境的人脸支付安全方法,其特征在于,所述支付应用判断所述活体百分率是否大于预设活体百分率阈值,若大于则进行身份认证,包括:

若完成所述人脸活体检测数据和人脸图像数据的采集则直接利用活体百分率和已生成的密文数据执行支付认证流程;

支付应用将所述活体百分率与预设活体百分率阈值进行比对,若大于则密码键盘解锁,所述支付应用获取支付密码;

所述支付应用将已生成的所述密文数据传输至认证服务器,通过所述认证服务器对用户进行身份认证,若通过则进行剩余交易,否则交易结束。

4.一种基于安全单元和可信执行环境的人脸支付安全平台能够实现权利要求1-3任一项所述的方法,其特征在,包括:

支付应用,用于若未完成人脸活体检测数据和人脸图像数据的采集,调起人脸识别可信应用,还用于实现支付流程;

人脸识别可信应用,用于激活所述人脸识别摄像头以及获取活体百分率;

人脸识别摄像头,用于抓取所述人脸活体检测数据和人脸图像数据,并将其发送至可

信执行环境；

可信执行环境，用于调用安全单元中的对称加密算法对所述人脸识别可信应用获取的所述活体百分率和所述人脸识别摄像头采集的所述人脸图像数据进行签名运算，生成签名结果，向安全单元发送加密指令；

安全单元，用于对所述活体百分率、可信执行环境生成的签名结果和人脸识别摄像头采集的人脸图像数据进行加密运算，生成密文数据并回传至所述可信执行环境；

认证服务器，用于根据所述密文数据及支付密码与其存储的生物特征对当前用户进行身份认证；

富执行环境，用于运行支付机构用于人脸识别交易的支付应用，支付应用运行有支付功能模块和人脸识别功能模块，分别处理常规支付流程和人脸识别流程，富执行环境中运行有支付工具以辅助完成支付交易，该支付工具与密码键盘进行数据交互；

密码键盘用于用户向支付应用输入支付密码。

5.根据权利要求4所述的基于安全单元和可信执行环境的人脸支付安全平台，其特征在于，包括：

所述支付应用，还用于，将所述安全单元生成的所述密文数据传输至认证服务器，通过所述认证服务器对用户进行身份认证。

6.跟权利要求5所述的基于安全单元和可信执行环境的人脸支付安全平台，其特征在于，还包括：

可信服务管理平台，用于通过安全通道与所述人脸识别支付平台进行数据交互，用于对安全单元相关密钥及剩余应用进行下发、注册和更新管理，并对交易中人脸图像数据进行保护。

7.根据权利要求6所述的基于安全单元和可信执行环境的人脸支付安全平台，其特征在于，还包括：

可信认证管理平台，用于通过安全通道与所述人脸识别支付平台进行数据交互，用于对可信执行环境的密钥及可信执行环境中的人脸识别可信应用进行下发、注册和更新管理，并对所述可信执行环境的身份进行认证。

基于安全单元和可信执行环境的人脸支付安全方法及平台

技术领域

[0001] 本发明涉及人脸支付领域,尤其涉及一种基于安全单元和可信执行环境的人脸支付安全方法及平台。

背景技术

[0002] 随着人工智能技术的快速发展与衍化,人脸识别技术逐渐被应用于金融支付领域,而人脸识别支付应用的出现向原有支付系统引入了潜在的安全风险。在未有针对性安全保护的情况下,人脸识别相关算法及人脸图像数据在现有支付应用普通操作系统中,容易遭受到外来的恶意攻击,致使用户的支付交易面临严峻的安全威胁。设计一种人脸识别安全支付应用平台,可以有效提高支付应用的防御能力,保证以人脸识别作为用户身份辨别与认证途径从而执行支付流程的安全与稳定。安全支付应用平台以安全单元为基础,以可信执行环境为依托,以防止人脸活体检测结果和用户人脸图像被恶意篡改、窃取和伪造为目的,从而保障终端支付安全。安全单元解决核心密钥存储与密码学算法服务的问题。可信执行环境解决人脸活体检测算法执行、算法结果和人脸图像的完整性、认证性和机密性保护问题。

[0003] 用于支付应用平台的安全单元(Secure Element,SE),多为一颗独立的安全芯片,能够防止外部恶意解析攻击,保护核心敏感数据安全,在芯片中具有密码算法逻辑电路,可以向外部提供安全的密码学算法服务。SE概念在金融领域应用起源于金融IC卡芯片,后来在金融交易终端上逐渐推广具有类似功能的SE芯片,近年来手机终端也开始配备专用的嵌入式SE芯片。SE不仅能防止来自软件层的逻辑攻击,还能抵抗物理攻击,即使其被物理破坏拆解,也能够保护其中存储数据的安全。SE的安全防护能力极高,但其计算和存储资源有限,通常仅用于保护核心敏感的安全密钥数据及提供底层密码学算法服务,不适用于对较大规模数据和较复杂程序逻辑执行的保护。

[0004] 可信执行环境(Trusted Execution Environment,TEE),借鉴于可信计算技术思想,其旨在保护安全敏感的代码执行和相关数据信息免受恶意敌手的攻击和破坏,是建立可信移动终端平台的基础。TEE主要由微内核操作系统组成,隔离于由普通终端操作系统(如安卓和iOS等)组成的富执行环境(Rich Execution Environment,REE)。TEE能够抵御来自软件层的攻击,安全防护能力低于SE,但其实际运行于终端的主控芯片(CPU)上,具有较强的计算能力,能够执行复杂的逻辑程序。国际标准组织(GlobalPlatform,GP)在2011年为TEE制定了标准白皮书,并给出了系统架构设计指南。ARM公司提出了为TEE提供硬件支持的TrustZone隔离技术,通过自底向上的方法可以构建高安全性的隔离环境。近年来,在移动终端设备上构建TEE已经成为手机厂商的标准配置。

[0005] 人脸识别技术已广泛应用于安防、金融和智慧家居等领域,以实现人脸比对与辨别为目的,借助人脸这一生物特征,完成用户个体的身份识别和认证。人脸识别应用于支付领域,是通过人脸特征识别来辨别和确认付款主体的身份,其即可以实现用户(及其对应账户)的辨别(类比于确定银行卡号),又可以作为一种身份认证要素实现身份的确认(类比于

输入密码)。在使用过程中,为了提高安全性,人脸识别往往结合用户密码输入等认证手段一起完成对支付用户的身份认证。人脸识别过程与支付安全相关的算法主要包括活体检测算法和人脸比对算法,前者主要用于确定人脸图像来源于一个真实的活体,防止照片和视频等假体攻击,后者是主要实现在大量用户图像数据中确定当前用户的身份。在支付应用中,一般只集成活体检测算法,而人脸比对算法主要部署在支付机构或认证机构的后台服务器中,结合大量的人脸图像数据库一并使用。

[0006] 为降低支付交易的安全风险,现有支付应用设备在操作系统、物理硬件和密码输入保护方面做了一定的安全设计。然而针对人脸识别算法和相关流程,上述安全设计不足以保护算法的安全执行及结果,且人脸图像数据面临着泄露、篡改和伪造的风险。基于TEE和SE的人脸识别安全支付应用平台,能够有效解决相关安全问题,但在具体的实施和应用中,尚存在以下几点问题:

[0007] 1、现有支付应用没有专为保护人脸活体检测算法进行设计,无法对算法执行及算法结果的完整性、认证性和机密性保护。

[0008] 2、现有支付应用未针对人脸识别流程进行保护。

[0009] 3、人脸图像数据属于用户的隐私数据,一旦泄露将为用户带来长久的安全隐患。现有支付应用在普通操作系统REE中处理人脸图像,由于REE极易被攻破,则人脸图像数据也面临较高的泄露风险。从而,如何为人脸图像数据在终端的产生、处理和传输等各阶段设计安全保护方案,以保障人脸识别支付流程中的图像数据安全性成为亟待解决的问题。

发明内容

[0010] 本发明提供一种基于安全单元和可信执行环境的人脸支付安全方法及平台,用以解决现有技术中人脸支付过程中无法对人脸支付相关算法执行、算法结果、人脸识别流程和人脸图像数据的完整性、认证性和机密性保护的问题。

[0011] 为了实现上述目的,本发明技术方案提供了基于安全单元和可信执行环境的人脸支付安全方法,包括:可信执行环境中的人脸识别可信应用根据采集的人脸活体检测数据和人脸图像数据,生成活体百分率。安全单元中对所述活体百分率和人脸图像数据进行签名和加密后将生成的密文数据回传至所述人脸识别可信应用。支付应用判断所述活体百分率是否大于预设活体百分率阈值,若大于则进行身份认证,通过后进行剩余交易。

[0012] 作为上述技术方案的优选,较佳的,人脸识别可信应用采集人脸活体检测数据和人脸图像数据,包括:支付应用判断所述人脸活体检测数据和人脸图像数据的采集是否完成。若未完成,所述支付应用通过可信执行环境调用所述人脸识别可信应用。所述人脸识别可信应用激活人脸识别摄像头用于抓取人脸数据。

[0013] 作为上述技术方案的优选,较佳的,获取活体百分率,包括:人脸识别摄像头被可信执行环境中的人脸识别可信应用激活后抓取人脸活体检测数据和人脸图像数据。人脸识别可信应用调用活体检测算法根据人脸活体检测数据和人脸图像数据通过计算得到活体百分率。其中,人脸识别摄像头采集的所述人脸图像和所述人脸活体检测数据,仅通过可信执行环境通道传送至可信执行环境中对应的人脸识别工具。

[0014] 作为上述技术方案的优选,较佳的,安全单元对所述活体百分率和人脸图像数据进行签名和加密后将生成的签名结果和密文数据回传至所述人脸识别可信应用,包括:人

脸识别可信应用调用安全单元接口,所述安全单元对所述活体百分率和所述人脸图像数据进行签名运算,生成签名结果。安全单元调用对称加密算法和相应密钥对活体百分率、签名结果和人脸图像数据进行加密运算,生成密文数据并将密文数据回传至人脸识别可信应用。

[0015] 作为上述技术方案的优选,较佳的,支付应用判断活体百分率是否大于预设活体百分率阈值,若大于则进行身份认证,包括:若完成所述人脸活体检测数据和人脸图像数据的采集则直接利用活体百分率和已生成的密文数据执行支付认证流程;支付应用将活体百分率与预设活体百分率阈值进行比对,若大于则密码键盘解锁,支付应用获取支付密码。支付应用将已生成的密文数据传输至认证服务器,通过认证服务器对用户进行身份认证,若通过则进行剩余交易,否则交易结束。

[0016] 为实现上述目的,本发明还提供能够实现上述方法的一种基于安全单元和可信执行环境的人脸支付安全平台,包括:支付应用,用于若未完成人脸活体检测数据和人脸图像数据的采集,调起人脸识别可信应用,还用于实现支付流程。人脸识别可信应用,用于激活所述人脸识别摄像头以及获取活体百分率。人脸识别摄像头,用于抓取人脸活体检测数据和人脸图像数据,并将其发送至可信执行环境。可信执行环境,用于调用安全单元中的对称加密算法对所述人脸识别可信应用获取的活体百分率和所述人脸识别摄像头采集的人脸图像数据进行签名运算,生成签名结果,向安全单元发送加密指令。安全单元,用于对活体百分率、可信执行环境生成的签名结果和人脸识别摄像头采集的人脸图像数据进行加密运算,生成密文数据并回传至所述可信执行环境人脸识别可信应用。认证服务器,用于根据密文数据和支付密码与其存储的生物特征对当前用户进行身份认证。富执行环境,用于运行支付机构用于人脸识别交易的支付应用,支付应用运行有支付功能模块和人脸识别功能模块,分别处理常规支付流程和人脸识别流程,富执行环境中运行有支付工具以辅助完成支付交易,该支付工具与密码键盘进行数据交互。密码键盘用于用户向支付应用输入支付密码。

[0017] 作为上述技术方案的优选,较佳的,支付应用,还用于,将安全单元生成的密文数据传输至认证服务器,通过认证服务器对用户进行身份认证。

[0018] 作为上述技术方案的优选,较佳的,还包括:可信服务管理平台,用于通过安全通道与人脸识别支付平台进行数据交互,用于对安全单元生相关密钥及剩余应用进行下发、注册和更新管理,并对交易中人脸图像数据进行保护。

[0019] 作为上述技术方案的优选,较佳的,还包括:可信认证管理平台,用于通过安全通道与人脸识别支付平台进行数据交互,用于对可信执行环境的密钥及可信执行环境中的人脸识别可信应用进行下发、注册和更新管理,并对可信执行环境的身份进行认证。

[0020] 本发明技术方案提供了人脸支付安全方法及平台,通过人脸识别可信应用通过人脸识别摄像头采集的人脸活体检测数据和人脸图像数据,获取活体百分率后可信执行环境通过安全单元获取密文数据,支付应用判断活体百分率是否大于预设活体百分率阈值,若大于则结合加密密钥进行身份认证,通过后在富执行环境中结合密码键盘进行剩余交易。

[0021] 本发明的优点是:

[0022] 1、本发明基于SE的终端平台可以安全管理与人脸识别过程相关的数据保护密钥,SE能够提供安全的密码学算法服务,TEE保证了人脸活体检测算法的安全执行,TEE与人脸

识别摄像头直连,整体终端平台实现了对人脸活体检测结果和人脸识别图像的数据准确性、完整性、认证性和机密性的保护。

[0023] 2、本发明能够与支付应用原有的支付流程紧密融合,基于终端平台的人脸识别安全支付方法可以有效减少人脸识别过程对传统支付交易引入的安全风险,且能够抵御来自软件层和部分硬件层对终端平台的恶意攻击,从而从整体上提升了人脸识别支付的安全性。

[0024] 3、本发明设计的终端平台和支付方法符合通用的SE与TEE管理机制,配合成熟的TSM(可信服务管理平台)和TAM(可信认证管理平台)机制,能够有效实现所述安全支付应用平台的密钥生命周期管理与认证、TEE与TA的生命周期管理与认证,使平台快速融入现有的可信管理与认证系统环境,从而进一步提升人脸识别支付交易底层的安全管理能力。

附图说明

[0025] 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一简单介绍,显而易见地,下面描述中的附图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。

[0026] 图1为本发明实施例提供的人脸支付安全方法的流程示意图。

[0027] 图2为本发明实施例提供的人脸支付安全方法的具体支付过程的流程图一。

[0028] 图3为本发明实施例提供的人脸支付安全方法的具体支付过程的流程图二。

[0029] 图4为本发明实施例提供的人脸支付安全平台的结构示意图一。

[0030] 图5为本发明实施例提供的人脸支付安全平台的结构示意图二。

具体实施方式

[0031] 为使本发明实施例的目的、技术方案和优点更加清楚,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、完整的描述,显然,所描述的实施例是本发明一部分实施例,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的前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0032] 现具体说明本发明技术方案,图1为本发明实施例提供的流程示意图,如图1所示,包括:

[0033] 步骤101、支付应用判断所述人脸活体检测数据和人脸图像数据的采集是否完成。

[0034] 若未完成,支付应用通过可信执行环境调用所述人脸识别可信应用后,人脸识别可信应用激活人脸识别摄像头用于抓取人脸数据后执行步骤102,若完成执行步骤104。

[0035] 步骤102、人脸识别可信应用通过采集的人脸活体检测数据和人脸图像数据,并获取活体百分率。

[0036] 人脸识别可信应用调用活体检测算法根据所述人脸活体检测数据和人脸图像数据通过计算得到所述活体百分率;

[0037] 其中,人脸识别摄像头采集的所述人脸图像和所述人脸活体检测数据,仅通过可信执行环境通道传送至可信执行环境中对应的人脸识别工具。

[0038] 步骤103、人脸识别可信应用根据所述活体百分率和所述人脸图像数据获取密文

数据。

[0039] 可信执行环境中的人脸识别可信应用调用安全单元接口,所述安全单元对所述活体百分率和所述人脸图像数据进行签名运算,生成签名结果。安全单元调用对称加密算法和相应密钥对活体百分率、签名结果和人脸图像数据进行加密运算,得到密文数据。其中,所述密文数据的加密内容包括人脸图像数据、活体百分率和签名结果。

[0040] 步骤104、支付应用判断活体百分率是否大于预设活体百分率阈值,若大于则将密文数据传输至认证服务器并进行身份认证,通过后,结合密码键盘完成身份认证和剩余交易。若小于,则交易结束。

[0041] 具体的,支付应用将活体百分率与预设活体百分率阈值进行比对,若大于则密码键盘解锁,所述支付应用获取支付密码。同时,支付应用将密文数据传输至认证服务器,通过认证服务器对用户进行身份认证,若通过则进行剩余交易,否则交易结束。其中,支付应用将活体百分率与预设活体百分率阈值进行比对时,述活体百分率以明文形式出现在支付应用的富执行环境中。

[0042] 现用一具体实施例对本发明技术方案进行进一步详细说明:本发明技术方案实施例中涉及的ID与密钥标识下表1所示。

[0043] 表1:ID与密钥标识

[0044]

名称	缩写	形式及功能
SE 身份标识序列号	ID_{SE}	串码，用于唯一标识 SE 芯片
活体识别结果 SE 签名私钥	SK_{Face}	私钥，用于 SE 对人脸活体识别结构结果签名
活体识别结果 SE 验签公钥	PK_{Face}	公钥，用于认证服务器验证 SE 对人脸活体识别结果的签名
人脸图像 SE 加密密钥	*FaceKey*	对称密钥，用于 SE 对人脸图像进行加密及认证服务器进行解密
TEE 身份标识序列号	ID_{TEE}	串码，用于唯一标识 TEEOS 环境
TEE 认证私钥	SK_{TEE}	私钥，用于 TEE 证明身份时对相关消

[0045]

		息进行签名
TEE 认证公钥	PK_{TEE}	公钥，用于 TAM 认证 TEE 时验证其消息的签名
TA 认证私钥	$SK_{TA\_Certify}$	私钥，用于 TAM 下发 TA 时对其进行签名
TA 认证公钥	$PK_{TA\_Certify}$	公钥，用于 TEE 验证合法 TA 时验证其具有的 TAM 签名

[0046] 本发明提供的人脸支付安全方法的具体支付流程如图2所示,具体描述如下:其中,安全单元SE、可信执行环境TEE、富执行环境REE、可信应用TA(Trusted Application)、支付APP即为上述支付应用,支付应用安装在商户或消费者的操作终端中。

[0047] 步骤201、由商户或消费者操作终端平台REE中的支付APP,触发人脸识别支付业务。

[0048] 步骤202、支付APP判断是否完成消费者人脸图像的抓取和活体检测,若完成执行步骤210,否则执行步骤203。

[0049] 步骤203、支付APP激活人脸识别TA。

[0050] 支付APP的人脸识别功能模块通过TEE管理器调用可信执行环境TEE中的人脸识别TA,向TA发送想要的调用指令,人脸识别TA进入活动状态。

[0051] 步骤204、人脸识别摄像头抓取人脸图像。

[0052] 其中,人脸识别TA通过TEE内部的驱动,激活人脸识别摄像头,人脸摄像头根据指令金融活动状态,准备抓取人脸图像。其中人脸识别摄像头通常设于由商户或消费者的操作终端上。

[0053] 步骤205、将人脸活体检测数据l和人脸图像数据p发送至人脸识别TA。

[0054] 具体的,人脸识别摄像头分别抓取消费者人脸活体检测数据l和人脸图像数据p,并将两个数据直接传入TEE中的人脸识别TA。

[0055] 步骤206、人脸识别TA计算活体百分率r。

[0056] 具体的,人脸识别TA调用人脸活体检测SDK相应算法对人脸活体检测数据l进行处理与判别,得出该数据对应的活体百分率r。

[0057] 步骤207、人脸识别TA生成签名结果。

[0058] 其中,人脸识别TA通过TEE调用SE的接口,将活体百分率r和人脸图像数据p发送至SE,SE调用签名算法SIG使用私钥SK_{Face}对活体百分率r和人脸图像数据p进行签名运算,得到签名结果s,方法如下:

[0059] $s=SIG(SK_{Face},r||p)$。

[0060] 步骤208、SE调用加密算法进行数据处理得到密文数据m。

[0061] SE调用对称加密算法ENC使用密钥FaceKey对签名结果s、活体百分率r和人脸图像数据p进行加密运算,得到向后台发送的密文数据m,具体的,m=ENC(FaceKey,s||r||p)。SE完成运算后,将密文数据m和活体百分率r发送至TEE的人脸识别TA中。其中密钥FaceKey为

安全单元SE中的密钥。

[0062] 步骤209、人脸识别TA接收密文数据m和活体百分率r发送至支付APP。

[0063] 此时,支付APP已完成人脸图像的抓取和活体检测,并获得了用于验证消费者身份信息的相关数据,等待发送至后台认证服务器。

[0064] 具体的,密文数据m为:签名结果s、活体百分率r和人脸图像数据p三者的加密结果。

[0065] 步骤210、支付APP根据活体百分率r判断活体检测是否通过,若通过执行步骤211,否则交易结束。

[0066] 支付APP根据r的值做初步判断,若达到所设定的活体百分率阈值,则进行后续人脸支付交易步骤,若未达到阈值要求,则本次交易结束支付失败。

[0067] 此时的活体百分率r出现在REE中,所以它是一个不可信数据,对于其达到活体阈值以上的判断,此处仅为初步判断,相关数据还将在后台认证服务器做最终判断。

[0068] 步骤211、支付APP调用支付功能模块,进入支付流程。

[0069] 步骤212、消费者通过密码键盘输入交易密码。

[0070] 支付设备SDK激活PINPAD密码键盘,消费者通过PINPAD输入专用于人脸识别支付交易的密码,经过安全保护的消费者密码通过支付设备SDK传入支付APP。

[0071] 步骤213、认证服务器对接收的密文数据m和密码对消费者身份进行认证,若认证通过执行步骤214。

[0072] 支付APP将密文数据m和经过安全保护的消费者人脸识别支付交易密码进行组包后,传送至具有生物识别平台的相关机构后台服务器,对消费者的身份进行识别认证,并映射出消费者的交易账户用于后续实际金额的交易操作。

[0073] 步骤214、支付APP判断交易是否完成,若是执行步骤215,否则交易结束。

[0074] 具体的,步骤214中,支付APP单独判断支付密码是否正确,以及人脸是否与消费者本人匹配,若均正确则执行步骤215,否则交易结束。

[0075] 通过人脸数据完成消费者身份认证后,相关服务器与终端平台共同完成原有支付交易流程,通过传统的支付通道,完成相应账户和相应交易金额的实际操作,返回终端平台结果。

[0076] 步骤215、显示交易结果。

[0077] 支付APP判断最终的支付交易是否已成功完成,并通过终端平台屏幕显示最终的交易结果,用于商户和消费者的确认。

[0078] 本发明还提供了一种基于安全单元和可信执行环境的人脸支付安全平台,其结构示意图如图3所示:

[0079] 本发明的硬件层包含PINPAD密码键盘、安全单元SE和人脸摄像头;软件层包含REE和TEE环境。其中,REE中运行有支付APP、支付设备SDK和TEE管理器,支付APP包含支付功能模块和人脸识别功能模块;TEE中运行有人脸识别可信应用TA。

[0080] 支付应用(支付APP)31,用于若未完成人脸活体检测数据和人脸图像数据的采集,调起人脸识别可信应用;还用于,将安全单元生成的密文数据传输至认证服务器,通过所述认证服务器对用户进行身份认证,以及用于进行支付流程。

[0081] 人脸识别可信应用TA32,用于激活人脸识别摄像头以及获取活体百分率,其内含

人脸活体检测算法SDK。

[0082] 人脸识别摄像头33,用于抓取人脸活体检测数据和人脸图像数据,并将其发送至可信执行环境。此摄像头专用于人脸识别过程中捕捉人脸图像数据,并具备活体检测的硬件支持功能,可以是3D结构光、TOF摄像头或红外双目摄像头,由TEE中的对应算法进行驱动。人脸识别摄像头仅与TEE直接连接,不与REE直接连,生成的人脸图像原始数据将仅能直接传入TEE中对应的人脸识别可信应用TA进行处理。

[0083] 可信执行环境TEE34,用于调用安全单元SE中的对称加密算法对所述人脸识别可信应用获取的所述活体百分率和所述人脸识别摄像头采集的所述人脸图像数据进行签名运算,生成签名结果,向安全单元发送加密指令用于指示安全单元生成密文数据m。

[0084] 可信执行环境34基于ARM TrustZone硬件架构实现,是具备与REE隔离的专有环境,这里主要针对TEE OS层进行描述。TEE中安全执行有人脸识别可信应用TA,人脸识别可信应用TA32运行有人脸活体检测算法SDK321,可以对获取的人脸数据执行活体检测等相关算法,TEE存储有TEE身份标识序列号ID_{TEE}、TEE认证私钥SK_{TEE}和TA认证公钥$PK_{TA_Certify}$;TEE与REE通过REE中的TEE管理器进行数据通信,TEE还可以执行其他安全敏感的TA。

[0085] 安全单元SE35,用于对所述活体百分率、可信执行环境34生成的签名结果和人脸识别摄像头采集的人脸图像数据进行加密运算,得到密文数据。

[0086] 具体的,安全单元SE,直接位于平台主板上,用于对人脸活体检测结果进行签名,对人脸图像进行加密,并为上层提供安全的密码学算法,包括签名、对称加密和摘要算法等,SE中具有唯一身份识别序列号ID_{SE}、人脸活体检测结果签名私钥SK_{Face}以及人脸图像对称加密密钥FaceKey。SE直接与平台的TEE相连接,仅接受TEE发送的有效指令,并返回输出结果至TEE中对用的可以应用TA。

[0087] 认证服务器36,用于根据所述密文数据和其存储的生物特征对当前用户进行身份认证,并回传至支付APP31中。

[0088] 富执行环境REE37,用于运行支付机构用于人脸识别交易的支付应用,支付应用运行有支付功能模块和人脸识别功能模块,分别处理常规支付流程和人脸识别流程,富执行环境中运行有支付工具以辅助完成支付交易,该支付工具与密码键盘进行数据交互。其为普通的Android操作系统,执行原有终端的应用程序、组件服务和驱动,运行有支付APP31,实现支付交易功能和人脸识别功能的上层接口和UI,该APP主要由支付机构负责实现。支付APP31的支付功能模块311,主要负责处理支付相关功能的请求、响应和数据组包;人脸识别功能模块312,主要负责处理人脸识别相关功能的请求、响应和数据组包。REE37中还运行有支付设备SDK371,用于处理原有的支付交易算法和协议,这部分内容与支付机构后台规则相关。REE37中运行TEE管理器372,用于实现TEE与REE的数据通信和命令调用功能,在支付APP调用人脸识别可信应用TA时负责发送调用请求,并接收其返回的数据结果。

[0089] PINPAD密码键盘38,用于用户向支付应用输入支付密码。具体的,用于人脸支付时安全输入人脸交易密码,该PINPAD是物理实体键盘,非虚拟键盘。PINPAD需要通过金融行业有关部门的检测认证,内含独立的安全芯片,使用时与支付机构后台对接,直接获取分配给其的加密保护密钥和完整性保护密码,当用户输入人脸交易密码后,将直接在PINPAD内完成加密和完整性保护计算,然后发送至支付机构后台,用户密码不会明文出现在包含支付APP在内的其他环境中。PINPAD与富执行环境REE连接,主要与支付设备SDK交互。

[0090] 本发明提供的基于安全单元和可信执行环境的人脸支付安全平台,可以部署于普通商户,单独面向消费者通过人脸识别完成商品或服务的支付交易,也可以搭配现有支付MIS(管理信息系统)收银机具、自助贩售机具和POS终端,快速改造原有设备使其具备人脸识别支付功能。

[0091] 进一步的,上述人脸识别支付平台分别与认证服务器、TSM(可信服务管理平台)和TAM(可信认证管理平台)进行相关信息数据交互,以支撑和完成人脸识别安全支付流程的进行。

[0092] 可信服务管理平台TSM,用于通过安全通道与人脸识别支付平台进行数据交互,对安全单元生成的密文数据及剩余应用进行下发、注册和更新管理,并对交易中人脸图像数据进行保护。具体的,TSM既可以部署在支付机构后台,也可以由某机构独立运维,主要用于对终端平台的SE进行管理,需要与支付APP后台服务有数据交互。终端平台出厂前,厂商对SE进行密钥预置,则TSM与终端平台之间即可建立安全通道。在终端平台使用过程中,SE运行的Applet应用、功能密钥,均可由TSM通过安全通道下发至SE,同时这些数据的更新升级也通过TSM进行下发完成。TSM负责管理的SE密钥有FaceKey和SK_{Face},当某个终端SE在TSM处完成注册后,TSM将具有SE相对应的ID_{SE}、FaceKey和PK_{Face},TSM将这些数据以某种形式经过某种方式传送至认证服务器,认证服务器在验证终端平台人脸支付交易时会使用到这些数据,以此作为验证的基础。

[0093] 可信认证管理平台,用于通过安全通道与所述人脸识别支付平台进行数据交互,用于对可信执行环境的密钥及可信执行环境中的人脸识别可信应用进行下发、注册和更新管理,并对所述可信执行环境的身份进行认证。

[0094] TAM即可以部署在支付机构后台,也可以由某机构独立运维,主要用于对终端平台的TEE进行管理,需要与支付APP后台服务有数据交互。终端平台出厂前,厂商对TEE进行密钥预置,则TAM与终端平台之间即可建立安全通道。在终端平台使用过程中,TEE OS镜像、TEE运行的TA、功能密钥,均可由TAM通过安全通道下发至终端平台,同时这些数据的更新升级也通过TAM进行下发完成。TAM负责管理的TEE密钥有SK_{TEE}和$PK_{TA_Certify}$,当某个终端TEE在TAM处完成注册后,TAM将具有TEE相对应的ID_{TEE}、PK_{TEE}和$SK_{TA_Certify}$,TAM将ID_{TEE}和PK_{TEE}以某种形式经过某种方式传送至认证服务器,认证服务器在验证终端平台TEE身份时会使用到这两个数据,以此作为验证的基础。

[0095] 认证服务器,主要部署在支付机构后台,用于验证终端平台和消费者的合法身份,是人脸支付交易过程中进行后台人脸识别算法部署的主体,也进行人脸支付交易消费者账户认证的核心组件。人脸识别安全支付流程中,终端平台(支付APP)生成人脸识别组包数据均发送至该认证服务器,认证服务器使用TSM传输的对应密钥数据解包并校验终端平台数据,对活体百分率r进行合格判定后,使用人脸图像数据p和消费者人脸交易密码在自有的人脸图像数据库中进行比对检索,确定对应消费者的具体身份和消费账户,再通过传统路径完成具体金额的支付交易流程,以此完成人脸识别支付交易的核心验证步骤,实现人脸识别安全支付应用平台功能。

[0096] 现结合实际操作过程对本发明技术方案进行说明,

[0097] 消费者启动终端设备中的支付应用31开始支付,支付应用31激活TEE管理器372,从而调起可信执行环境TEE34中的人脸识别可信应用TA32,人脸识别可信应用TA32激活人

脸识别摄像头33采集消费者人脸图像并将此图像回传至人脸识别可信应用TA32,人脸活体检测算法SDK321对人脸图像进行计算得到活体百分率r和人脸像素图像。人脸识别可信应用TA32将活体百分率r和人脸像素图像下发至安全单元SE35进行运算,得到密文数据m。再将密文数据m回传至人脸识别可信应用TA32,经TEE管理器372后回传至支付应用31。支付应用将密文数据m发送至认证服务器36认证后将认证结果回传至支付应用31,若认证通过则密码键盘38输入密码,再经支付设备SDK371计算后将计算结果发至支付应用31,支付应用31中的支付功能模块311执行支付流程。

[0098] 本发明技术方案提供了人脸支付安全方法及平台,通过人脸识别可信应用通过人脸识别摄像头采集的人脸活体检测数据和人脸图像数据,获取活体百分率后可信执行环境通过安全单元获取密文数据,支付应用判断活体百分率是否大于预设活体百分率阈值,若大于则结合加密密钥进行身份认证,通过后在富执行环境中结合密码键盘进行剩余交易。

[0099] 本发明的优点是:

[0100] 1、本发明基于SE的终端平台可以安全管理与人脸识别过程相关的数据保护密钥,SE能够提供安全的密码学算法服务,TEE保证了人脸活体检测算法的安全执行,TEE与人脸识别摄像头直连,整体终端平台实现了对人脸活体检测结果和人脸识别图像的数据准确性、完整性、认证性和机密性的保护。

[0101] 2、本发明能够与支付应用原有的支付流程紧密融合,基于终端平台的人脸识别安全支付方法可以有效减少人脸识别过程对传统支付交易引入的安全风险,且能够抵御来自软件层和部分硬件层对终端平台的恶意攻击,从而从整体上提升了人脸识别支付的安全性。

[0102] 3、本发明设计的终端平台和支付方法符合通用的SE与TEE管理机制,配合成熟的TSM(可信服务管理平台)和TAM(可信认证管理平台)机制,能够有效实现所述安全支付应用平台的密钥生命周期管理与认证、TEE与TA的生命周期管理与认证,使平台快速融入现有的可信管理与认证系统环境,从而进一步提升人脸识别支付交易底层的安全管理能力。

[0103] 最后应说明的是:以上各实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述各实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分或者全部技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

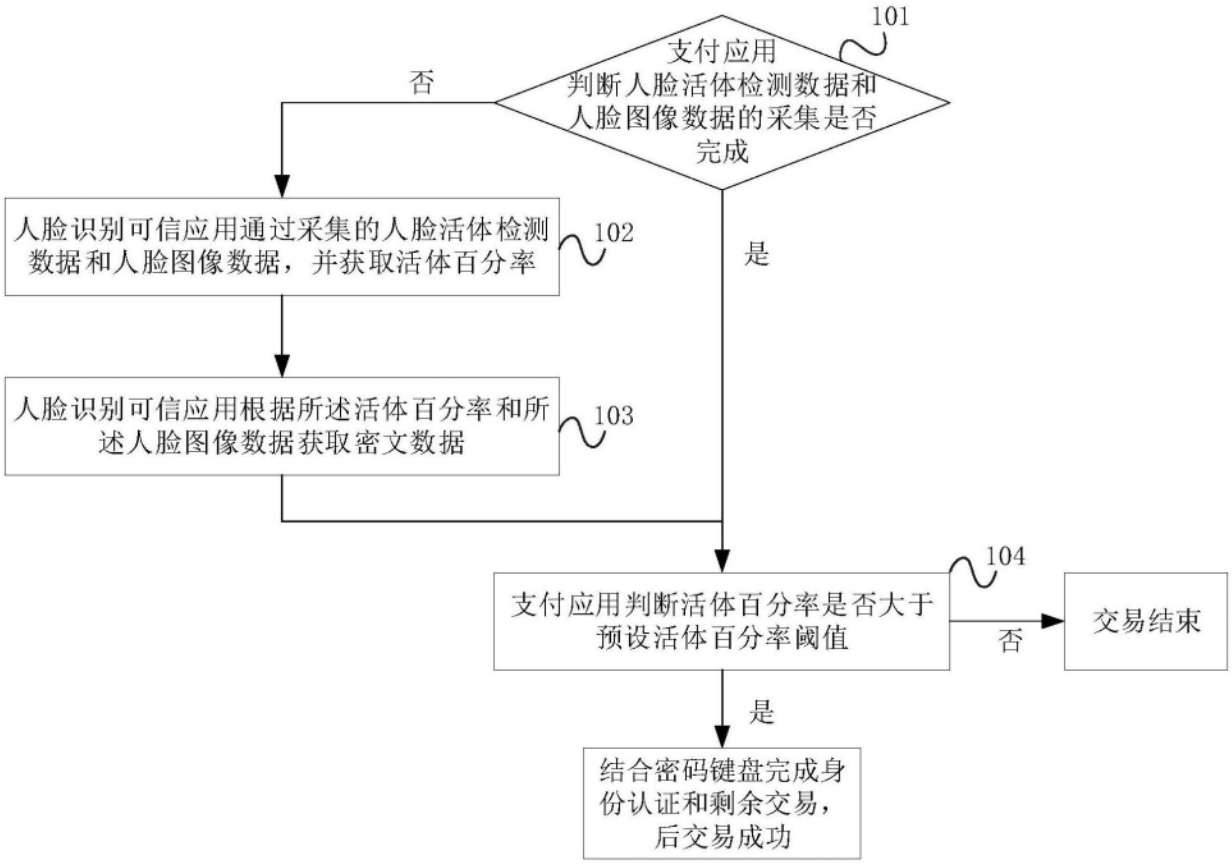

101
支付应用判断人脸活体检测数据和人脸图像数据的采集是否完成
否
是
人脸识别可信应用通过采集的人脸活体检测数据和人脸图像数据，并获取活体百分率
102
人脸识别可信应用根据所述活体百分率和所述人脸图像数据获取密文数据
103
104
支付应用判断活体百分率是否大于预设活体百分率阈值
否
交易结束
是
结合密码键盘完成身份认证和剩余交易，后交易成功

图1

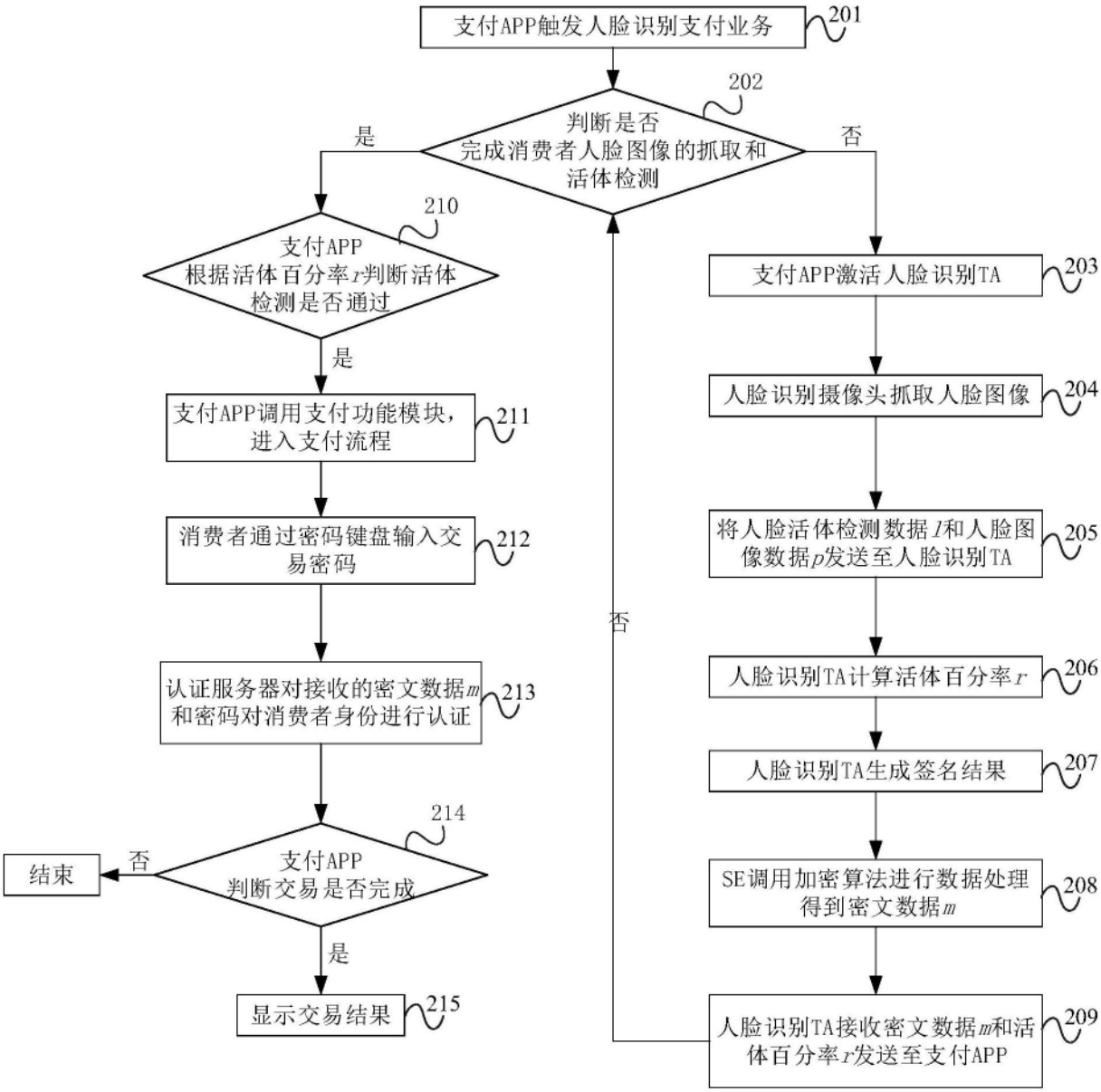

支付APP触发人脸识别支付业务
201
判断是否
完成消费者人脸图像的抓取和
活体检测
202
是
否
支付APP
根据活体百分率r判断活体
检测是否通过
210
是
支付APP调用支付功能模块，
进入支付流程
211
消费者通过密码键盘输入交
易密码
212
认证服务器对接收的密文数据m
和密码对消费者身份进行认证
213
支付APP
判断交易是否完成
214
否
结束
是
显示交易结果
215
支付APP激活人脸识别TA
203
人脸识别摄像头抓取人脸图像
204
将人脸活体检测数据I和人脸图
像数据p发送至人脸识别TA
205
人脸识别TA计算活体百分率r
206
人脸识别TA生成签名结果
207
SE调用加密算法进行数据处理
得到密文数据m
208
人脸识别TA接收密文数据m和活
体百分率r发送至支付APP
209
否

图2

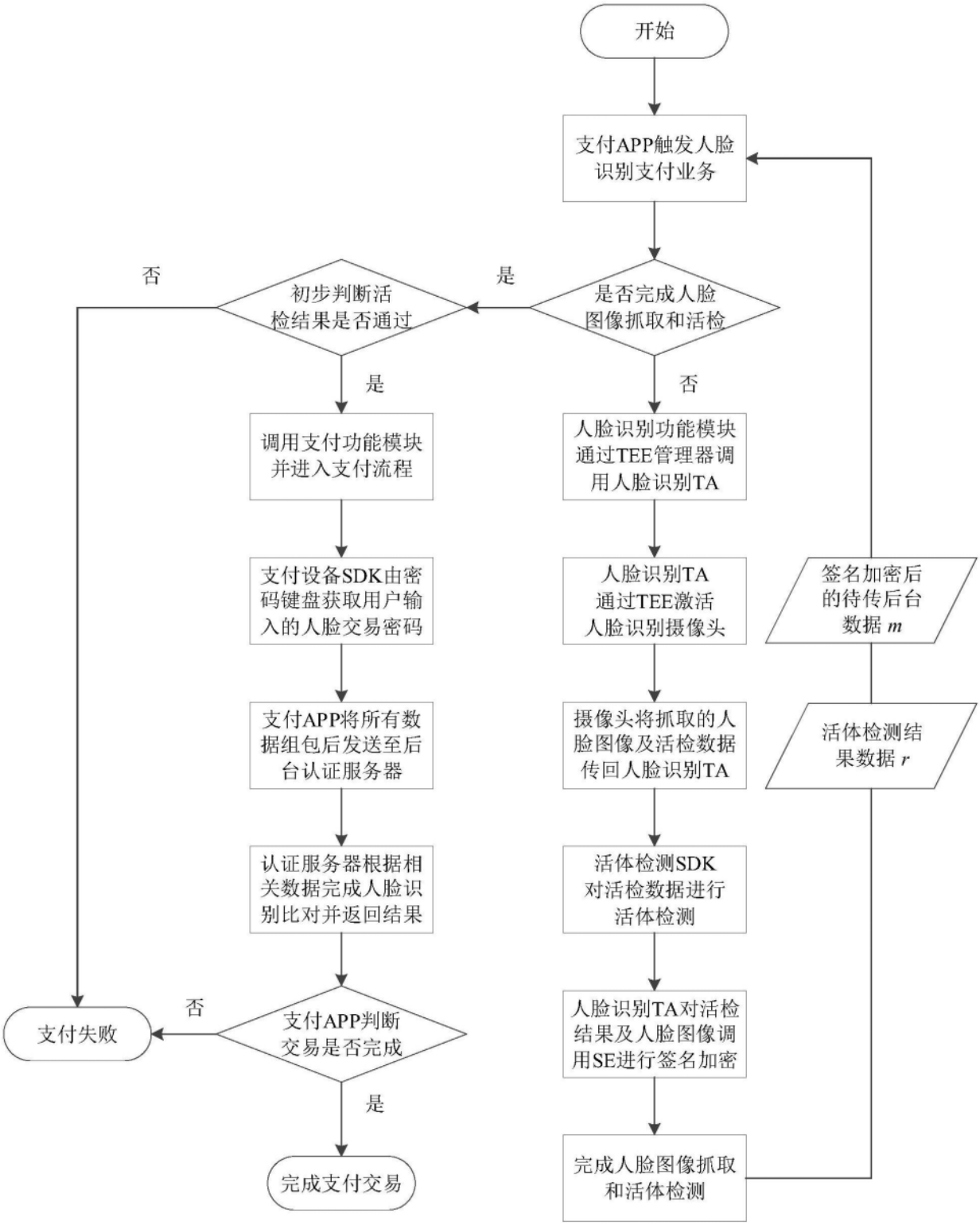

开始
支付APP触发人脸识别支付业务
是否完成人脸图像抓取和活检
是
否
初步判断活检结果是否通过
否
是
支付失败
否
支付APP判断交易是否完成
是
完成支付交易
调用支付功能模块并进入支付流程
支付设备SDK由密码键盘获取用户输入的人脸交易密码
支付APP将所有数据组包后发送至后台认证服务器
认证服务器根据相关数据完成人脸识别比对并返回结果
人脸识别功能模块通过TEE管理器调用人脸识别TA
人脸识别TA通过TEE激活人脸识别摄像头
摄像头将抓取的人脸图像及活检数据传回人脸识别TA
活体检测SDK对活检数据进行活体检测
人脸识别TA对活检结果及人脸图像调用SE进行签名加密
完成人脸图像抓取和活体检测
签名加密后的待传后台数据 m
活体检测结果数据 r

图3

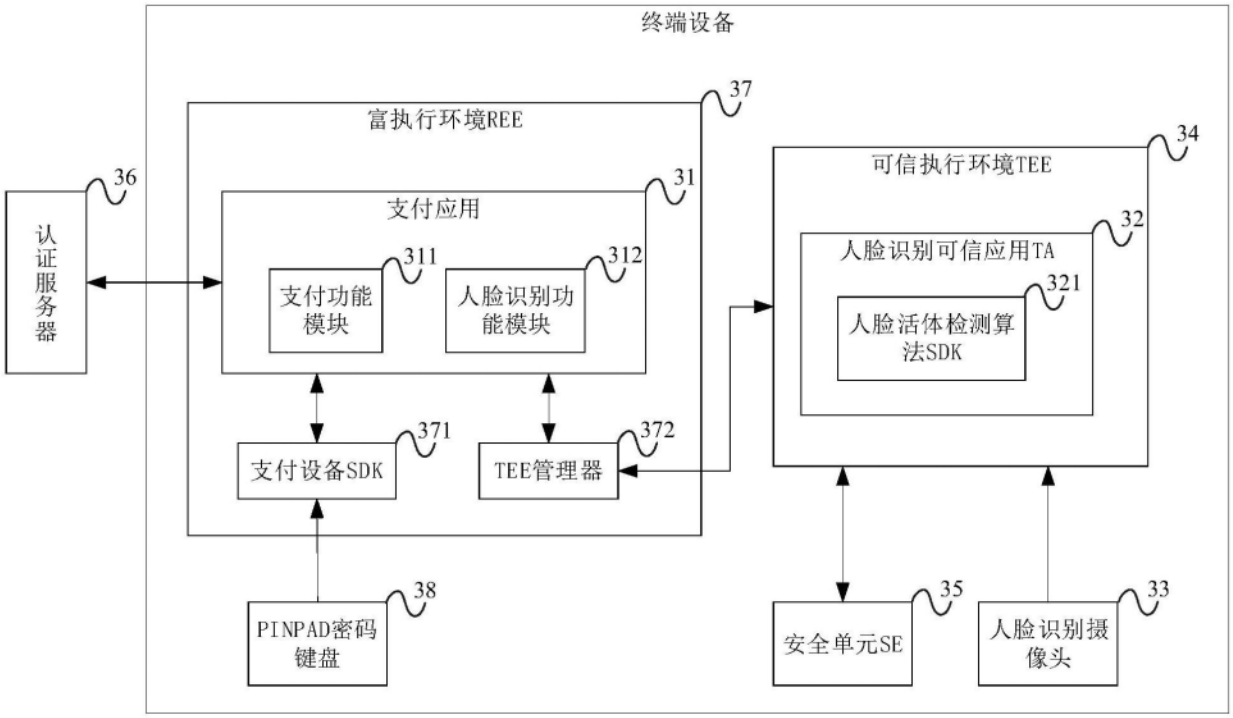

终端设备
富执行环境REE
37
可信执行环境TEE
34
36
认证服务器
支付应用
31
人脸识别可信应用TA
32
311
支付功能模块
312
人脸识别功能模块
321
人脸活体检测算法SDK
371
支付设备SDK
372
TEE管理器
38
PINPAD密码键盘
35
安全单元SE
33
人脸识别摄像头

图4

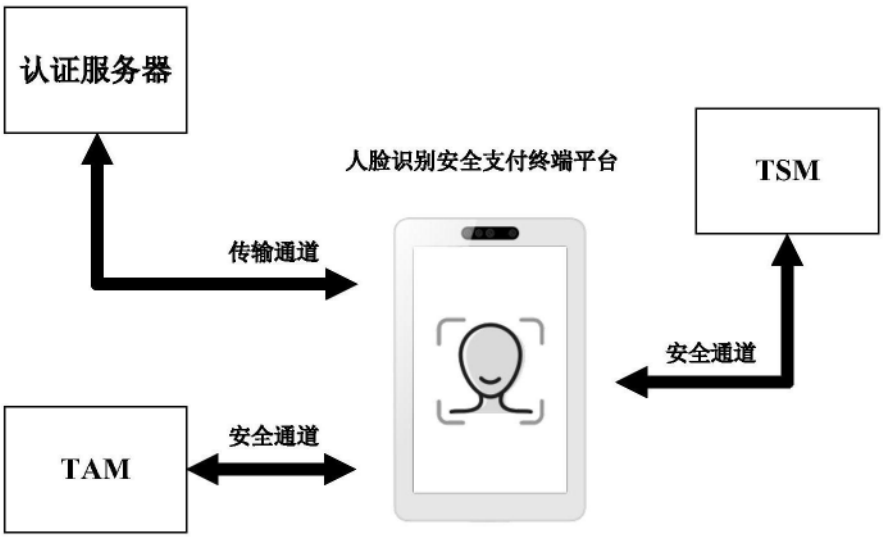

认证服务器
人脸识别安全支付终端平台
TSM
传输通道
安全通道
TAM
安全通道

图5