(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106599745 A
(43)申请公布日 2017.04.26

(21)申请号 201610967883.2

(22)申请日 2016.11.04

(71)申请人 上海德门信息技术有限公司
地址 201108 上海市闵行区金都路3669号6幢一层A26室

(72)发明人 严清夏

(74)专利代理机构 上海汉声知识产权代理有限公司 31236
代理人 郭国中

(51)Int.Cl.
G06K 7/10(2006.01)
G06K 9/00(2006.01)

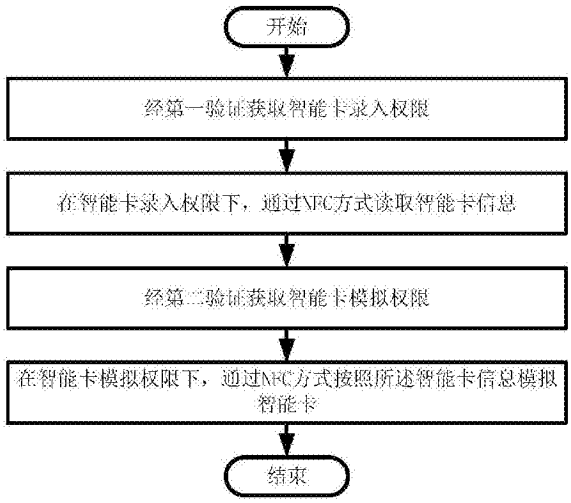
权利要求书2页 说明书7页 附图5页

(54)发明名称

可用于智能卡核验和替代的系统和方法

(57)摘要

本发明提供了一种可用于智能卡核验和替代的方法和系统，尤其是以居民的个人移动通信终端设备作为身份识别的替代方式，无需额外投入设备或系统，利用现有至少具备NFC和指纹识别功能的通信设备即可通过多种方式录入和模拟二代居民身份证信息，部署灵活，使用方便简单，有效推动了居民二代居民身份证系统信息化建设进程，提升了公安、安保系统的调度与反应能力，增强居民日常身份验证需求的便捷性。



CN 106599745 A

1.一种可用于智能卡核验和替代的方法,其特征在于,包括:

录入验证步骤:经第一验证获取智能卡录入权限;

智能卡录入步骤:在智能卡录入权限下,通过NFC方式读取智能卡信息;

模拟验证步骤:经第二验证获取智能卡模拟权限;

智能卡模拟步骤:在智能卡模拟权限下,通过NFC方式按照所述智能卡信息模拟智能卡。

2.根据权利要求1所述的可用于智能卡核验和替代的方法,其特征在于,所述录入验证步骤包括:

智能卡初始验证步骤:通过NFC方式读取智能卡得到智能卡信息、或者从智能卡扫描图像中提取智能卡信息;

指纹初始验证步骤:通过触摸屏提取指纹信息,记为现场指纹信息;

验证对比步骤:通过网络从数据库获取与所述智能卡信息对应的指纹信息,记为已认证指纹信息;将现场指纹信息与已认证指纹信息进行匹配,若匹配,则认为通过第一验证,若不匹配,则认为没有通过第一验证。

3.根据权利要求1所述的可用于智能卡核验和替代的方法,其特征在于,所述智能卡录入步骤包括:

智能卡信息存储步骤:将读取到的智能卡信息存储在本地或者上传服务器。

4.根据权利要求1所述的可用于智能卡核验和替代的方法,其特征在于,所述模拟验证步骤中,采用指纹、人脸、声音、动态安全码中的任一种或任多种方式进行第二验证。

5.根据权利要求1所述的可用于智能卡核验和替代的方法,其特征在于,所述智能卡模拟步骤包括:

智能卡信息调用步骤:调用智能卡信息;

智能卡替代模拟步骤:以与智能卡中线圈相同的谐振频率发射智能卡信息。

6.一种可用于智能卡核验和替代的系统,其特征在于,包括:

录入验证模块:经第一验证获取智能卡录入权限;

智能卡录入模块:在智能卡录入权限下,通过NFC方式读取智能卡信息;

模拟验证模块:经第二验证获取智能卡模拟权限;

智能卡模拟模块:在智能卡模拟权限下,通过NFC方式按照所述智能卡信息模拟智能卡。

7.根据权利要求6所述的可用于智能卡核验和替代的系统,其特征在于,所述录入验证模块包括:

智能卡初始验证模块:通过NFC方式读取智能卡得到智能卡信息、或者从智能卡扫描图像中提取智能卡信息;

指纹初始验证模块:通过触摸屏提取指纹信息,记为现场指纹信息;

验证对比模块:通过网络从数据库获取与所述智能卡信息对应的指纹信息,记为已认证指纹信息;将现场指纹信息与已认证指纹信息进行匹配,若匹配,则认为通过第一验证,若不匹配,则认为没有通过第一验证。

8.根据权利要求6所述的可用于智能卡核验和替代的系统,其特征在于,所述智能卡录入模块包括:

智能卡信息存储模块:将读取到的智能卡信息存储在本地或者上传服务器。

9.根据权利要求6所述的可用于智能卡核验和替代的系统,其特征在于,所述模拟验证模块中,采用指纹、人脸、声音、动态安全码中的任一种或任多种方式进行第二验证。

10.根据权利要求6所述的可用于智能卡核验和替代的系统,其特征在于,所述智能卡模拟模块包括:

智能卡信息调用模块:调用智能卡信息;

智能卡替代模拟模块:以与智能卡中线圈相同的谐振频率发射智能卡信息。

可用于智能卡核验和替代的系统和方法

技术领域

[0001] 本发明涉及信息安全技术领域，具体地，涉及可用于智能卡核验和替代的系统和方法，特别是指一种基于近场通信、指纹识别技术用于二代居民身份证核验或替代的方法和设备。

背景技术

[0002] 近年来，随着人口流动的增加，居民身份信息安全领域变得越来越重要。在二代居民身份证信息化工作的逐步深入下，我国二代居民身份证已经植入居民个人电子数据和指纹信息，以方便于一线警务人员、机场火车站安检人员对居民身份信息的核验工作，具有活动移动性强、突发性强、实时性要求高等特点。在实际操作中，面对的场景多为在移动多变或人流量较大的环境下需要进行警务分析处理以及大量复杂信息进行分析，目前核查人员多采用警务终端或身份证读卡器直接对居民的二代居民身份证进行以上工作。

[0003] 但在正常执法或安检过程中，经常遇到被查验人员没有携带二代居民身份证、或无法正常读取身份证信息的情况，造成执法不便，或被查验人员无法按时乘坐公共交通工具，造成安全隐患和财产的损失；即使大部分公共交通枢纽(机场、火车站)都配备设有办理临时身份证据点，但办理手续繁琐，无法为执法人员以及居民提供实效的便捷与切实的安全。

[0004] 在符合公安部要求的情况下，为了实现实时在线和移动在线的要求，建立基于近场通信NFC技术和指纹识别技术实现利用居民的个人手机调用其电子个人信息作为替代二代居民身份证的虚拟电子身份证，可满足二代居民身份证的核验、指纹信息核验，完成公安系统的警务分析和处理、公共交通系统的身份验证。

发明内容

[0005] 针对现有技术中的缺陷，本发明的目的是提供一种可用于智能卡核验和替代的系统和方法。

[0006] 根据本发明提供的一种可用于智能卡核验和替代的方法，包括：

[0007] 录入验证步骤：经第一验证获取智能卡录入权限；

[0008] 智能卡录入步骤：在智能卡录入权限下，通过NFC方式读取智能卡信息；

[0009] 模拟验证步骤：经第二验证获取智能卡模拟权限；

[0010] 智能卡模拟步骤：在智能卡模拟权限下，通过NFC方式按照所述智能卡信息模拟智能卡。

[0011] 优选地，所述录入验证步骤包括：

[0012] 智能卡初始验证步骤：通过NFC方式读取智能卡得到智能卡信息、或者从智能卡扫描图像中提取智能卡信息；

[0013] 指纹初始验证步骤：通过触摸屏提取指纹信息，记为现场指纹信息；

[0014] 验证对比步骤：通过网络从数据库获取与所述智能卡信息对应的指纹信息，记为

已认证指纹信息;将现场指纹信息与已认证指纹信息进行匹配,若匹配,则认为通过第一验证,若不匹配,则认为没有通过第一验证。

[0015] 优选地,所述智能卡录入步骤包括:

[0016] 智能卡信息存储步骤:将读取到的智能卡信息存储在本地或者上传服务器。

[0017] 优选地,所述模拟验证步骤中,采用指纹、人脸、声音、动态安全码中的任一种或任多种方式进行第二验证。

[0018] 优选地,所述智能卡模拟步骤包括:

[0019] 智能卡信息调用步骤:调用智能卡信息;

[0020] 智能卡替代模拟步骤:以与智能卡中线圈相同的谐振频率发射智能卡信息。

[0021] 根据本发明提供的一种可用于智能卡核验和替代的系统,包括:

[0022] 录入验证模块:经第一验证获取智能卡录入权限;

[0023] 智能卡录入模块:在智能卡录入权限下,通过NFC方式读取智能卡信息;

[0024] 模拟验证模块:经第二验证获取智能卡模拟权限;

[0025] 智能卡模拟模块:在智能卡模拟权限下,通过NFC方式按照所述智能卡信息模拟智能卡。

[0026] 优选地,所述录入验证模块包括:

[0027] 智能卡初始验证模块:通过NFC方式读取智能卡得到智能卡信息、或者从智能卡扫描图像中提取智能卡信息;

[0028] 指纹初始验证模块:通过触摸屏提取指纹信息,记为现场指纹信息;

[0029] 验证对比模块:通过网络从数据库获取与所述智能卡信息对应的指纹信息,记为已认证指纹信息;将现场指纹信息与已认证指纹信息进行匹配,若匹配,则认为通过第一验证,若不匹配,则认为没有通过第一验证。

[0030] 优选地,所述智能卡录入模块包括:

[0031] 智能卡信息存储模块:将读取到的智能卡信息存储在本地或者上传服务器。

[0032] 优选地,所述模拟验证模块中,采用指纹、人脸、声音、动态安全码中的任一种或任多种方式进行第二验证。

[0033] 优选地,所述智能卡模拟模块包括:

[0034] 智能卡信息调用模块:调用智能卡信息;

[0035] 智能卡替代模拟模块:以与智能卡中线圈相同的谐振频率发射智能卡信息。

[0036] 尤其是,所述可用于智能卡核验和替代的系统包括移动通信终端,移动通信终端的控制器包括录入验证模块、身份证录入模块、模拟验证模块、身份证模拟模块;移动通信终端的壳体表面包含NFC读卡区域,NFC读卡区域的内侧设置有NFC天线和连接NFC天线的NFC芯片。NFC读卡区域的内部或者边缘延伸出智能卡定位条,智能卡定位条的一侧面与NFC读卡区域垂直连接;NFC读卡区域平齐或者凹入于壳体正面或背面的表面;智能卡定位条凸出于壳体正面或背面的表面;智能卡为居民身份证,尤其是二代居民身份证。

[0037] 与现有技术相比,本发明具有如下的有益效果:

[0038] 本发明使用居民个人调用其电子个人信息作为替代二代居民身份证的虚拟电子身份证,实现二代居民身份证的录入上传公安专网数据库和调用电子身份信息虚拟卡片,同时调用移动通信终端的指纹识别和摄像头实现指纹和虹膜的保护信息安全的屏障,另外

实现实时动态验证码进行相关操作的验证信息，具有零成本投入，使用方便，安全系数高等特点，可以有效推动了居民二代居民身份证系统信息化建设进程，提升了公安、安保系统的调度与反应能力，增强居民日常身份验证需求的便捷性。

附图说明

[0039] 通过阅读参照以下附图对非限制性实施例所作的详细描述，本发明的其它特征、目的和优点将会变得更明显：

[0040] 图1为基于本发明提供的可用于智能卡核验和替代的系统的移动通信终端设备正面。

[0041] 图2为基于本发明提供的可用于智能卡核验和替代的系统的移动通信终端设备背面

[0042] 图3为利用基于本发明提供的可用于智能卡核验和替代的系统的移动通信终端设备读取二代居民身份证信息的操作示意图。

[0043] 图4为本发明提供的可用于智能卡核验和替代的方法的步骤流程图。

[0044] 图5为本发明提供的可用于智能卡核验和替代的方法中录入验证步骤的子步骤流程图。

[0045] 图中：

[0046] 1-电源键

[0047] 2-前置摄像头

[0048] 3-报警键

[0049] 4-PTT键

[0050] 5-屏幕

[0051] 6-行业功能键

[0052] 7-菜单键

[0053] 8-返回键

[0054] 9-USB接口

[0055] 10-手机键

[0056] 11-拍照键

[0057] 12-音量键

[0058] 13-光敏传感器

[0059] 14-耳机接口

[0060] 15-听筒

[0061] 16-主机锁扣键

[0062] 17-充电接口

[0063] 18-手带孔

[0064] 19-手带支架

[0065] 20-智能卡定位条

[0066] 21-NFC读卡区域

具体实施方式

[0067] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人员进一步理解本发明，但不以任何形式限制本发明。应当指出的是，对本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变化和改进。这些都属于本发明的保护范围。

[0068] 本发明涉及一种可用移动终端设备替代二代居民身份证的方法和系统，其基于近场通信NFC技术和指纹识别技术实现居民个人移动终端设备替代二代居民身份证完成其个人的身份信息的核验的方法和系统。近场通讯NFC技术用于居民二代居民身份证的识读，以及卡模拟替代当前被查验人员的个人的居民身份证件，其技术指标符合《台式居民身份证阅读器通用技术要求》(GA 450-2013)；指纹识别技术用于比对当前被查验人员在公安系统网络的指纹信息，以及提高居民个人移动终端设备的使用安全性，采用光学原理的面阵传感器采集仪，其技术指标符合《居民身份证指纹采集器通用技术要求》(GA/T 1011-2012)。以居民的个人移动通信终端设备作为身份识别的替代方式，无需额外投入设备或系统，利用现有至少具备NFC和指纹识别功能的通信设备即可通过多种方式录入和模拟二代居民身份证信息，部署灵活，使用方便简单，有效推动了居民二代居民身份证系统信息化建设进程，提升了公安、安保系统的调度与反应能力，增强居民日常身份验证需求的便捷性。

[0069] 根据本发明提供的一种可用于智能卡核验和替代的方法，包括：

[0070] 录入验证步骤：经第一验证获取智能卡录入权限；

[0071] 智能卡录入步骤：在智能卡录入权限下，通过NFC方式读取智能卡信息；

[0072] 模拟验证步骤：经第二验证获取智能卡模拟权限；

[0073] 智能卡模拟步骤：在智能卡模拟权限下，通过NFC方式按照所述智能卡信息模拟智能卡。

[0074] 所述录入验证步骤包括：

[0075] 智能卡初始验证步骤：通过NFC方式读取智能卡得到智能卡信息、或者从智能卡扫描图像中提取智能卡信息；

[0076] 指纹初始验证步骤：通过触摸屏提取指纹信息，记为现场指纹信息；

[0077] 验证对比步骤：通过网络从数据库获取与所述智能卡信息对应的指纹信息，记为已认证指纹信息；将现场指纹信息与已认证指纹信息进行匹配，若匹配，则认为通过第一验证，若不匹配，则认为没有通过第一验证。

[0078] 所述智能卡录入步骤包括：

[0079] 智能卡信息存储步骤：将读取到的智能卡信息存储在本地或者上传服务器。

[0080] 所述模拟验证步骤中，采用指纹、人脸、声音、动态安全码中的任一种或任多种方式进行第二验证。

[0081] 所述智能卡模拟步骤包括：

[0082] 智能卡信息调用步骤：调用智能卡信息；

[0083] 智能卡替代模拟步骤：以与智能卡中线圈相同的谐振频率发射智能卡信息。

[0084] 根据本发明提供的一种可用于智能卡核验和替代的系统，包括移动通信终端，移动通信终端的控制器包括录入验证模块、身份证录入模块、模拟验证模块、身份证模拟模

块。

[0085] 录入验证模块:经第一验证获取智能卡录入权限;

[0086] 智能卡录入模块:在智能卡录入权限下,通过NFC方式读取智能卡信息;

[0087] 模拟验证模块:经第二验证获取智能卡模拟权限;

[0088] 智能卡模拟模块:在智能卡模拟权限下,通过NFC方式按照所述智能卡信息模拟智能卡。

[0089] 所述录入验证模块包括:

[0090] 智能卡初始验证模块:通过NFC方式读取智能卡得到智能卡信息、或者从智能卡扫描图像中提取智能卡信息;

[0091] 指纹初始验证模块:通过触摸屏提取指纹信息,记为现场指纹信息;

[0092] 验证对比模块:通过网络从数据库获取与所述智能卡信息对应的指纹信息,记为已认证指纹信息;将现场指纹信息与已认证指纹信息进行匹配,若匹配,则认为通过第一验证,若不匹配,则认为没有通过第一验证。

[0093] 所述智能卡录入模块包括:

[0094] 智能卡信息存储模块:将读取到的智能卡信息存储在本地或者上传服务器。

[0095] 所述模拟验证模块中,采用指纹、人脸、声音、动态安全码中的任一种或任多种方式进行第二验证。

[0096] 所述智能卡模拟模块包括:

[0097] 智能卡信息调用模块:调用智能卡信息;

[0098] 智能卡替代模拟模块:以与智能卡中线圈相同的谐振频率发射智能卡信息。

[0099] 更为具体地,移动通信终端是具备近场通信和指纹识别的移动通信终端设备,包括近场通信NFC模块、指纹识别模块、集成微处理器、无线通信模块、音视频模块、安全验证模块、人机交互模块即触摸屏、以及电源模块。近场通信NFC模块、指纹识别模块、无线通信模块、音视频模块、安全验证模块、人机交互模块即触摸屏,分别与集成微处理器和电源模块连接;安全验证模块与指纹识别、音视频模块、无线通信模块连接;无线通信模块包括WIFI通信模块、4G通信模块、北斗定位模块,音视频模块包括内置摄像头、内置麦克风、内置扬声器,与集成微处理器连接;安全验证模块包括安全码输入装置、安全码验证装置,安全码输入装置与安全码验证装置相连,以实现动态安全码的输入验证;所述移动通信终端还包括开关机开关,开关机开关为硬件开关用于机器的开关机触发,触摸屏开关触发;所述触摸屏,其还包括模数转换器,并配备专用触控笔,方便佩戴手套以及环境恶劣等时使用,可用于显示当前查验信息,包括身份证信息、指纹信息、现场信息、终端接收到的安全信息等,也用于系统操作;通过动态安全码指令与NFC、指纹信息、人脸图像识别相结合的多重身份安全验证,确保二代居民身份证数字信息的安全使用,确认操作者使用权限。

[0100] 进一步地,移动通信终端必须进行安全验证(包括第一验证、第二验证),若没有通过安全验证模块对使用者信息的安全验证,则移动通信终端被锁定无法使用替代或模拟二代居民身份证作为电子身份证使用的功能。安全验证是通过NFC、动态安全码、指纹识别三者相组合的三重验证方式实现,通过安全验证实现对使用者的使用权限限定。

[0101] 移动通信终端的使用权限包括:

[0102] -摄像头使用权,限即拍照和摄像;

[0103] -音频设备使用权，限即录音和播放；

[0104] -身份证识读器使用权，即NFC功能；

[0105] -指纹识别器使用权限；

[0106] -WiFi使用权限；

[0107] -北斗定位开启权限；

[0108] -4G数据连接权限；

[0109] -短消息收发权限；

[0110] -电话拨打权限，即来电、去电；

[0111] -第三方应用安装使用权限，即授权及非授权；

[0112] -与外部设备的USB连接权限，即授权及非授权PC等外部终端的USB连接权限；

[0113] -终端数据操作权限，即授权及非授权备份、删除、上传；

[0114] -终端应用访问无线VPN公安专网的权限。

[0115] 通过安全验证的移动通信终端将根据使用权限使用移动通信终端的相应权限功能，以进行二代居民身份证识读、指纹信息采集和验证。使用时选择身份证识读器使用权对应的身份证识读功能，将二代居民身份证置于NFC读卡区域，移动通信终端读取身份证信息并将身份证信息在触摸屏上显示，将读取出的数据根据使用权限及系统设定进行安全备份以及上传至无线VPN专网操作。将获取的二代居民身份证信息与公安专网数据库进行对比筛选，筛选结果供后台警务人员判断处理；若身份证无法识读，则终端将显示无法识读报警信息。所述的移动通信终端支持单指指纹信息采集，采用指纹采集仪方式采集，指纹识别模块与集成微处理器连接，通过SPI接口与集成微处理器相互通信。

[0116] 使用时选择指纹采集功能，将手指置于采集区域，根据系统提示进行操作，将获取的公民指纹信息与公安专网数据库进行对比筛选，在触摸屏上显示公民身份信息，结果供后台警务人员判断处理，采集所得标准指纹数据将依据权限和系统设定进行安全备份以及上传至无线VPN公安专网操作。

[0117] 使用移动通信终端作为电子身份证信息替代二代居民身份证时，必须通过动态验证码和指纹信息解锁安全模块，由安全模块发出验证指令调用无线VPN公安专网上保存的居民个人的电子身份证信息，并在触摸屏上显示公民身份信息，再由NFC读卡区域模拟出二代居民身份证的卡片状态。

[0118] 所述NFC读卡区域模拟出二代居民身份证的卡片状态，具体为：NFC天线和二代居民身份证内部形式都是线圈，谐振频率都是13.56MHz，从近场通信NFC技术本身而言其具有读写模拟功能(读取二代居民身份证信息)，和卡模拟功能(替代二代居民身份证使用)。

[0119] 所述的移动通信终端触摸屏，通过模数转换器与集成微处理器交互，可用于显示被查验人员身份证信息、指纹信息、图像信息等，显示本机报警信息，显示接收到的报警信息，显示接收到的短消息，显示来电信息、去电信息等。

[0120] 所述的音视频模块通过控制与数据接口与集成微处理器交互，其中配备摄像头两个、扬声器两个、麦克风一个，摄像头为前置摄像头和后置摄像头，前置摄像头主要应用于安全验证的人脸识别功能，后置摄像头主要用于公民身份核验现场拍摄等，在使用时可根据需要切换摄像头，麦克风主要应用于录音功能，扬声器应用于视频播放、语音播报、报警提示等，根据使用环境调节播放音量。

[0121] 所述的无线通信模块与集成微处理器连接，通过控制与数据接口与其通信，无线通信模块支持WiFi数据连接，4G数据连接，支持北斗定位通信。使用时根据当前网络环境切换数据连接方式，在使用时根据北斗获取地理位置信息，在紧急状况下将地理位置信息共享。按照权限分配，无线通信模块将移动通信终端获取的身份信息即包括：身份证信息、指纹信息、人脸图像，同时接收后台公安专网下发的数据信息。

[0122] 所述的移动通信终端采用实名制SIM卡绑定，支持Micro SD卡的绑定，所有的身份权限鉴定依据Micro SD安全卡的安全证书，移动通信终端使用过程中产生的数据加密解密采用Micro SD安全卡的国密SM4算法接口进行数据安全保护，若移动通信终端绑定SIM卡和Micro SD卡，更换后安全验证模块不允许进行操作，移动通信终端被锁定无法使用。

[0123] 所述的移动通信终端可安装经过安全认证授权的第三方应用以完成以上操作，后台可强制销毁安全私密数据，后台可恢复出厂设置。系统设置还包含修改本机信息、查看本机当前安全策略等。

[0124] 本发明针对警务安保的需求，提供一种用移动终端设备替代二代居民身份证的方法和系统，其基于近场通信NFC技术和指纹识别技术实现居民个人移动终端设备替代二代居民身份证完成其个人的身份信息的核验的方法和系统。以居民的个人移动通信终端设备作为身份识别的替代方式，无需额外投入设备或系统，利用现有至少具备NFC和指纹识别功能的通信设备即可通过多种方式录入和模拟二代居民身份证信息，部署灵活，使用方便简单，有效推动了居民二代居民身份证系统信息化建设进程，提升了公安、安保系统的调度与反应能力，增强居民日常身份验证需求的便捷性。

[0125] 本领域技术人员知道，除了以纯计算机可读程序代码方式实现本发明提供的系统及其各个装置、模块、单元以外，完全可以通过将方法步骤进行逻辑编程来使得本发明提供的系统及其各个装置、模块、单元以逻辑门、开关、专用集成电路、可编程逻辑控制器以及嵌入式微控制器等的形式来实现相同功能。所以，本发明提供的系统及其各项装置、模块、单元可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置、模块、单元也可以视为硬件部件内的结构；也可以将用于实现各种功能的装置、模块、单元视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0126] 以上对本发明的具体实施例进行了描述。需要理解的是，本发明并不局限于上述特定实施方式，本领域技术人员可以在权利要求的范围内做出各种变化或修改，这并不影响本发明的实质内容。在不冲突的情况下，本申请的实施例和实施例中的特征可以任意相互组合。

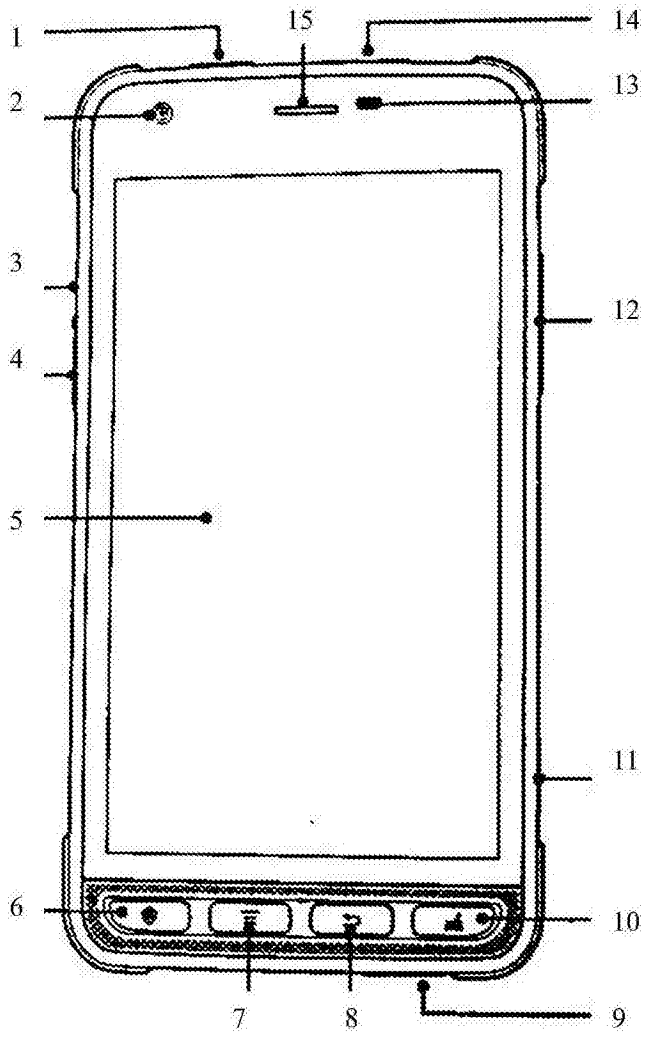


图1

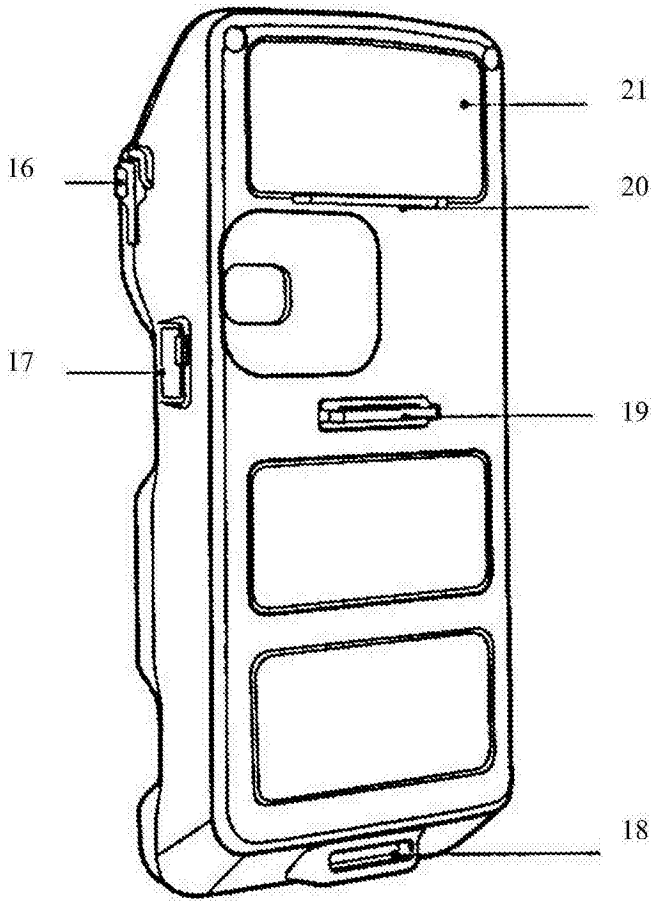


图2

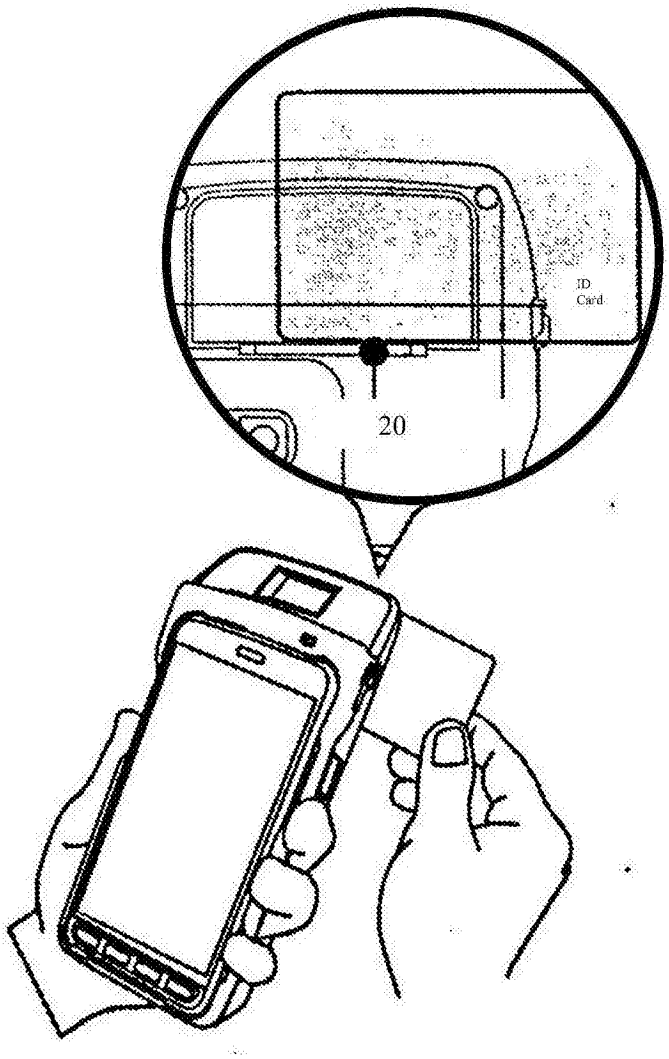


图3

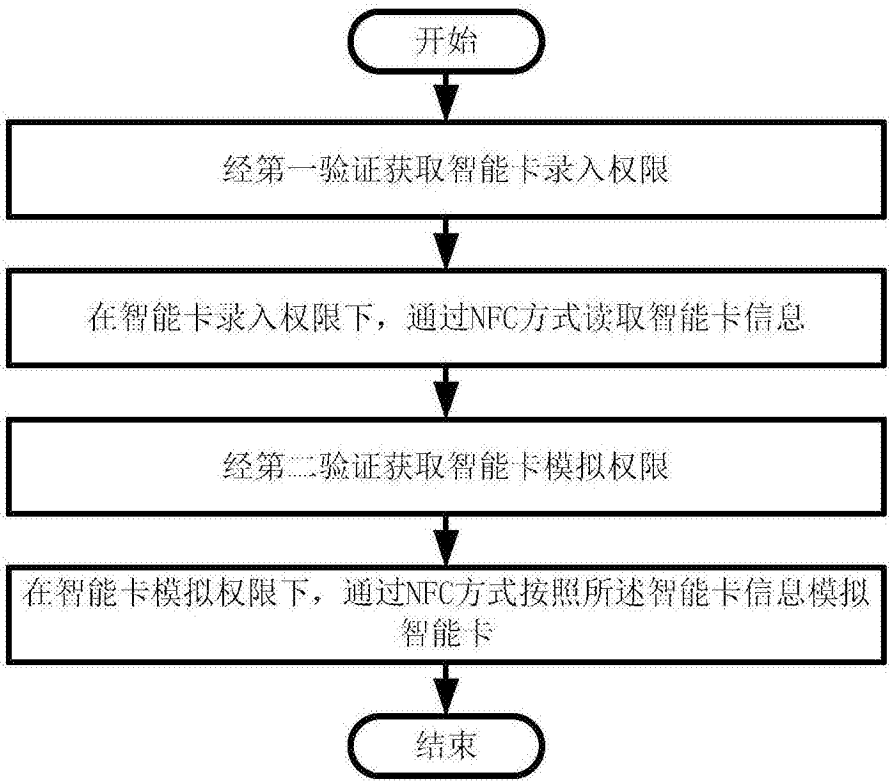

开始
经第一验证获取智能卡录入权限
在智能卡录入权限下，通过NFC方式读取智能卡信息
经第二验证获取智能卡模拟权限
在智能卡模拟权限下，通过NFC方式按照所述智能卡信息模拟智能卡
结束

图4

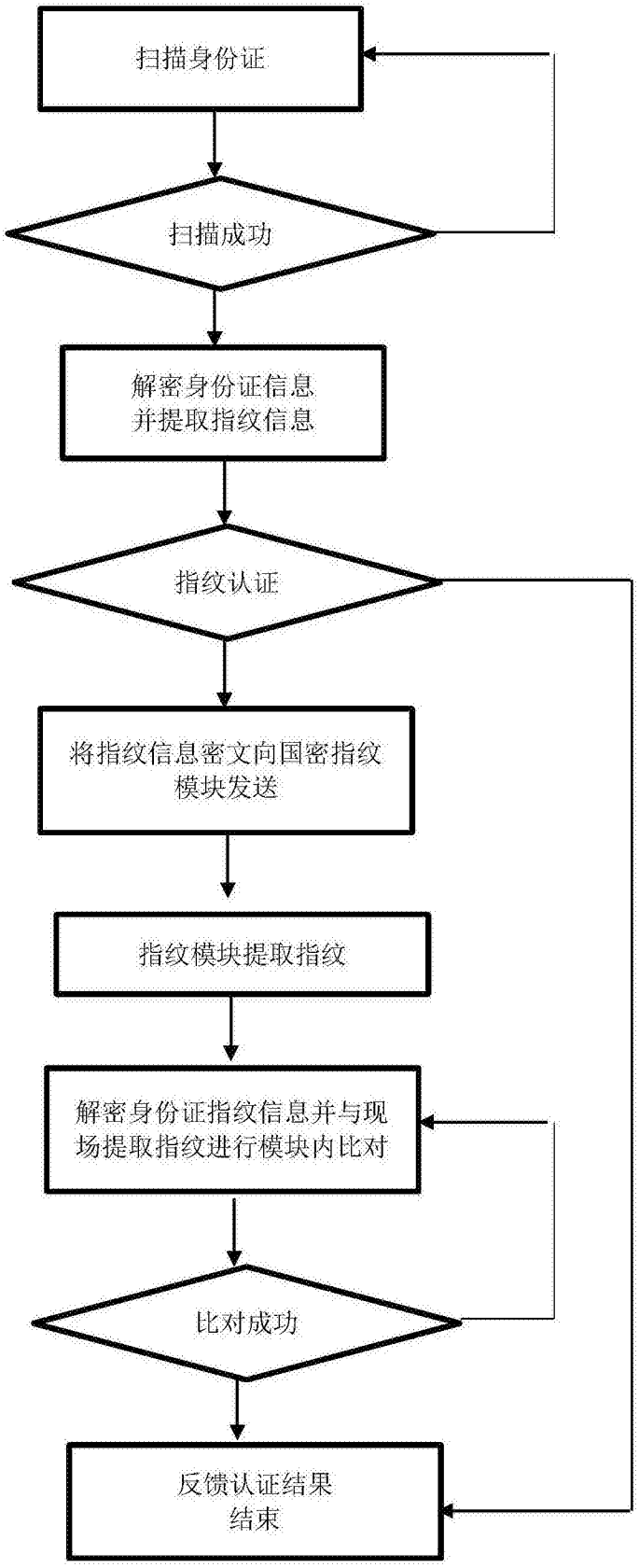

扫描身份证
扫描成功
解密身份证信息
并提取指纹信息
指纹认证
将指纹信息密文向国密指纹
模块发送
指纹模块提取指纹
解密身份证指纹信息并与现
场提取指纹进行模块内比对
比对成功
反馈认证结果
结束

图5