(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 105208011 B
(45)授权公告日 2019.07.30

(21)申请号 201510543545.1

(22)申请日 2015.08.31

(65)同一申请的已公布的文献号
申请公布号 CN 105208011 A

(43)申请公布日 2015.12.30

(73)专利权人 努比亚技术有限公司
地址 518000 广东省深圳市南山区高新区北环大道9018号大族创新大厦A区6-8层、10-11层、B区6层、C区6-10层

(72)发明人 刘睿

(74)专利代理机构 深圳协成知识产权代理事务所(普通合伙) 44458
代理人 章小燕

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 104580117 A,2015.04.29,
CN 101753305 A,2010.06.23,
CN 103607400 A,2014.02.26,
CN 102685090 A,2012.09.19,
CN 103763101 A,2014.04.30,

审查员 马旗超

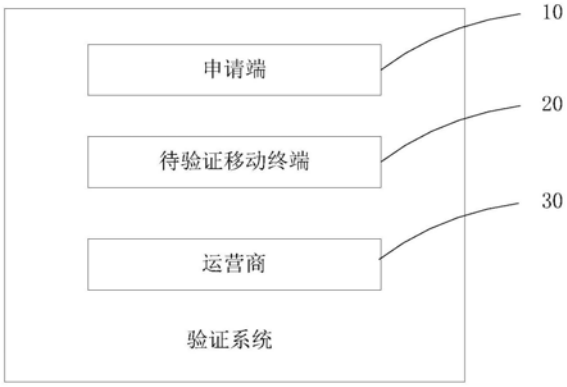
权利要求书2页 说明书11页 附图7页

(54)发明名称

一种验证系统及方法

(57)摘要

本发明公开了一种验证系统及方法，属于通信技术领域。该系统包括：申请端、待验证移动终端和运营商，其中，申请端，用于输入待验证手机号码，并向运营商发送包含待验证手机号码及申请端信息的验证请求，运营商将申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端；待验证移动终端，用于接收运营商发来的申请端信息及验证码，并将待验证手机号码及待验证移动终端物理地址与申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示，本发明通过对申请验证的移动终端及待验证的移动终端的信息匹配，来判断验证码的是否存在安全风险，并根据判断结果自动提供不同的风险提示，提高了验证码的安全性，提供了更好的用户体验。



CN 105208011 B

1.一种验证系统,其特征在于,包括:申请端、待验证移动终端和运营商,其中,

所述申请端,用于输入待验证手机号码,并向运营商发送包含所述待验证手机号码及申请端信息的验证请求,所述申请端信息包括:申请端手机号码及申请端物理地址;

所述运营商,用于接收所述申请端发来的验证请求,并将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端;

所述待验证移动终端,用于接收运营商发来的申请端信息及验证码,并将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示;

所述待验证移动终端包括:第一判断单元和第二判断单元,其中,

所述第一判断单元,用于判断所述申请端手机号码与所述待验证手机号码是否相同;若所述申请端手机号码与所述待验证手机号码不同,则验证码存在安全风险,并在所述待验证移动终端上显示第一风险提示信息;

所述第二判断单元,用于当所述申请端手机号码与所述待验证手机号码相同时,判断所述申请端物理地址与所述待验证移动终端物理地址是否相同;若所述申请端物理地址与所述待验证移动终端物理地址不同,则验证码存在安全风险,并在所述待验证移动终端上显示第二风险提示信息;若所述申请端物理地址与所述待验证移动终端物理地址相同,则验证码安全。

2.根据权利要求1所述的一种验证系统,其特征在于,所述申请端物理地址为:申请端蓝牙地址和/或申请端WLAN MAC地址;所述待验证移动终端物理地址为:待验证移动终端蓝牙地址和/或待验证移动终端WLAN MAC地址。

3.根据权利要求1所述的一种验证系统,其特征在于,所述申请端包括:

输入单元,用于在申请端的APP验证码获取界面输入待验证手机号码,触发“点击获取”按钮;

加密发送单元,用于获取申请端信息,将所述申请端信息加密并与所述待验证手机号码一同发送至运营商,其中,所述申请端信息包括:申请端手机号码及申请端物理地址;

相应地,所述运营商包括:

接收反馈单元,用于接收加密后的申请端信息及验证码,并将所述加密后的申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端。

4.根据权利要求3所述的一种验证系统,其特征在于,所述待验证移动终端内还设置有系统框架,所述系统框架用于接收加密后的申请端信息,并进行解密,得到申请端手机号码和申请端物理地址。

5.一种验证方法,其特征在于,包括:

申请端输入待验证手机号码,并向运营商发送包含所述待验证手机号码及申请端信息的验证请求,所述申请端信息包括:申请端手机号码及申请端物理地址;

运营商将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端;

将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示;

所述将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示具体为:

判断所述申请端手机号码与所述待验证手机号码是否相同；

若所述申请端手机号码与所述待验证手机号码不同，则验证码存在安全风险，并在所述待验证移动终端上显示第一风险提示信息；

若所述申请端手机号码与所述待验证手机号码相同，判断所述申请端物理地址与所述待验证移动终端物理地址是否相同；

若所述申请端物理地址与所述待验证移动终端物理地址不同，则验证码存在安全风险，并在所述待验证移动终端上显示第二风险提示信息；

若所述申请端物理地址与所述待验证移动终端物理地址相同，则验证码安全。

6.根据权利要求5所述的一种验证方法，其特征在于，所述申请端物理地址为：申请端蓝牙地址和/或申请端WLAN MAC地址；所述待验证移动终端物理地址为：待验证移动终端蓝牙地址和/或待验证移动终端WLAN MAC地址。

7.根据权利要求5所述的一种验证方法，其特征在于，所述申请端输入待验证手机号码，并向运营商发送包含所述待验证手机号码及申请端信息的验证请求具体为：

在申请端的APP验证码获取界面输入待验证手机号码，触发“点击获取”按钮；

获取申请端信息，将所述申请端信息加密并与所述待验证手机号码一同发送至运营商，其中，所述申请端信息包括：申请端手机号码及申请端物理地址；

相应地，所述运营商将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端具体为：

所述运营商将加密后的申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端。

8.根据权利要求7所述的一种验证方法，其特征在于，所述待验证移动终端内设置有系统框架，所述系统框架用于接收加密后的申请端信息，并进行解密，得到申请端手机号码和申请端物理地址。

一种验证系统及方法

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种验证系统及方法。

背景技术

[0002] 随着微信、QQ等社交工具越来越普及，短信的使用场景变得越来越少，而随着用户使用第三方软件越来越多，第三方软件对于用户的身份验证的频率越来越高，一减一增之间，验证码在日常收到的短信中占据了越来越大的比例。

[0003] 由此也催生了很多骗术，其中最常见的就是骗子发送验证码到你的手机上，然后他向你索要验证码，如果你给了他验证码，则相当于他验证成功了你的身份，然后他便可以查看你的信息，盗走你的账户甚至转走你的财产。

[0004] 在现有技术中，提供验证码的短信上会写着提示“泄露验证码有资金被盗风险”，但往往用户会忽略，此外，现在的短信验证码更多是直接以一个弹窗出现，一般只显示验证码和复制按钮，用户如果不进入短信应用连这句提示都看不到，降低了账户或财产的安全性。

发明内容

[0005] 本发明的主要目的在于提出一种验证系统及方法，通过对申请验证的移动终端及待验证的移动终端的信息匹配，来判断验证码的是否存在安全风险，并根据判断结果自动提供不同的风险提示，提高了验证码的安全性，提供了更好的用户体验。

[0006] 本发明解决上述技术问题的技术方案如下：

[0007] 根据本发明的一个方面，提供的一种验证系统，包括：申请端、待验证移动终端和运营商，其中，

[0008] 所述申请端，用于输入待验证手机号码，并向运营商发送包含所述待验证手机号码及申请端信息的验证请求，所述申请端信息包括：申请端手机号码及申请端物理地址；

[0009] 所述运营商，用于接收所述申请端发来的验证请求，并将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端；

[0010] 所述待验证移动终端，用于接收运营商发来的申请端信息及验证码，并将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示。

[0011] 优选地，所述待验证移动终端包括：第一判断单元和第二判断单元，其中

[0012] 所述第一判断单元，用于判断所述申请端手机号码与所述待验证手机号码是否相同；若所述申请端手机号码与所述待验证手机号码不同，则验证码存在安全风险，并在所述待验证移动终端上显示第一风险提示信息；

[0013] 所述第二判断单元，用于当所述申请端手机号码与所述待验证手机号码相同时，判断所述申请端物理地址与所述待验证移动终端物理地址是否相同；若所述申请端物理地址与所述待验证移动终端物理地址不同，则验证码存在安全风险，并在所述待验证移动终

端上显示第二风险提示信息;若所述申请端物理地址与所述待验证移动终端物理地址相同,则验证码安全。

[0014] 优选地,所述申请端物理地址为:申请端蓝牙地址和/或申请端WLAN MAC地址;所述待验证移动终端物理地址为:待验证移动终端蓝牙地址和/或待验证移动终端WLAN MAC地址。

[0015] 优选地,所述申请端包括:

[0016] 输入单元,用于在申请端的APP验证码获取界面输入待验证手机号码,触发“点击获取”按钮;

[0017] 加密发送单元,用于获取申请端信息,将所述申请端信息加密并与所述待验证手机号码一同发送至运营商,其中,所述申请端信息包括:申请端手机号码及申请端物理地址;

[0018] 相应地,所述运营商包括:

[0019] 接收反馈单元,用于接收加密后的申请端信息及验证码,并将所述加密后的申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端。

[0020] 优选地,所述待验证移动终端内还设置有系统框架,所述系统框架用于接收加密后的申请端信息,并进行解密,得到申请端手机号码和申请端物理地址。

[0021] 根据本发明的另外一个方面,提供的一种验证方法,包括:

[0022] 申请端输入待验证手机号码,并向运营商发送包含所述待验证手机号码及申请端信息的验证请求,所述申请端信息包括:申请端手机号码及申请端物理地址;

[0023] 运营商将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端;

[0024] 将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示。

[0025] 优选地,所述将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示具体为:

[0026] 判断所述申请端手机号码与所述待验证手机号码是否相同;

[0027] 若所述申请端手机号码与所述待验证手机号码不同,则验证码存在安全风险,并在所述待验证移动终端上显示第一风险提示信息;

[0028] 若所述申请端手机号码与所述待验证手机号码相同,判断所述申请端物理地址与所述待验证移动终端物理地址是否相同;

[0029] 若所述申请端物理地址与所述待验证移动终端物理地址不同,则验证码存在安全风险,并在所述待验证移动终端上显示第二风险提示信息;

[0030] 若所述申请端物理地址与所述待验证移动终端物理地址相同,则验证码安全。

[0031] 优选地,所述申请端物理地址为:申请端蓝牙地址和/或申请端WLAN MAC地址;所述待验证移动终端物理地址为:待验证移动终端蓝牙地址和/或待验证移动终端WLAN MAC地址。

[0032] 优选地,所述申请端输入待验证手机号码,并向运营商发送包含所述待验证手机号码及申请端信息的验证请求具体为:

[0033] 在申请端的APP验证码获取界面输入待验证手机号码,触发“点击获取”按钮;

[0034] 获取申请端信息，将所述申请端信息加密并与所述待验证手机号码一同发送至运营商，其中，所述申请端信息包括：申请端手机号码及申请端物理地址；

[0035] 相应地，所述运营商将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端具体为：

[0036] 所述运营商将加密后的申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端。

[0037] 优选地，所述待验证移动终端内设置有系统框架，所述系统框架用于接收加密后的申请端信息，并进行解密，得到申请端手机号码和申请端物理地址。

[0038] 本发明提供了一种验证系统及方法，该系统包括：申请端、待验证移动终端和运营商，其中，所述申请端，用于输入待验证手机号码，并向运营商发送包含所述待验证手机号码及申请端信息的验证请求，所述申请端信息包括：申请端手机号码及申请端物理地址；所述运营商，用于接收所述申请端发来的验证请求，并将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端；所述待验证移动终端，用于接收运营商发来的申请端信息及验证码，并将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示，本发明通过对申请验证的移动终端及待验证的移动终端的信息匹配，来判断验证码的是否存在安全风险，并根据判断结果自动提供不同的风险提示，提高了验证码的安全性，提供了更好的用户体验。

附图说明

[0039] 图1为实现本发明各个实施例的移动终端的硬件结构示意图；

[0040] 图2为如图1所示的移动终端的无线通信系统示意图；

[0041] 图3为本发明的实施例一的一种验证系统的示范性结构框图；

[0042] 图4为本发明的实施例一的一种第三方应用程序APP验证码获取界面；

[0043] 图5为本发明的实施例一的第一风险提示信息界面；

[0044] 图6为本发明的实施例一的第二风险提示信息界面；

[0045] 图7为本发明的实施例二的待验证移动终端的示范性结构框图；

[0046] 图8为本发明的实施例三的申请端的示范性结构框图；

[0047] 图9为本发明的实施例三的运营商的示范性结构框图；

[0048] 图10为本发明的实施例四的一种验证方法的流程图；

[0049] 图11为本发明的实施例五的一种验证方法的流程图；

[0050] 图12为本发明的实施例六的一种验证方法的流程图。

具体实施方式

[0051] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。移动终端可以以各种形式来实施。例如，本发明中描述的终端可以包括诸如移动电话、智能电话、笔记本电脑、数字广播接收器、PDA(个人数字助理)、PAD(平板电脑)、PMP(便携式多媒体播放器)、导航装置等等的移动终端以及诸如数字TV、台式计算机等等的固定终端。下面，假设终端是移动终端。然而，本领域技术人员将理解的是，除了特别用于移动目的的元件之外，根据本发明的实施方式的构造也能够应用于固定类型的终端。

[0052] 图1为实现本发明各个实施例的移动终端的硬件结构示意。

[0053] 移动终端100可以包括无线通信单元110、A/V(音频/视频)输入单元120、用户输入单元130、感测单元140、输出单元150、存储器160、接口单元170、控制器180和电源单元190等等。图1示出了具有各种组件的移动终端,但是应理解的是,并不要求实施所有示出的组件。可以替代地实施更多或更少的组件。将在下面详细描述移动终端的元件。

[0054] 无线通信单元110通常包括一个或多个组件,其允许移动终端100与无线通信系统或网络之间的无线电通信。例如,无线通信单元可以包括广播接收模块111、移动通信模块112、无线互联网模块113、短程通信模块114和位置信息模块115中的至少一个。

[0055] 广播接收模块111经由广播信道从外部广播管理服务器接收广播信号和/或广播相关信息。广播信道可以包括卫星信道和/或地面信道。广播管理服务器可以是生成并发送广播信号和/或广播相关信息的服务器或者接收之前生成的广播信号和/或广播相关信息并且将其发送给终端的服务器。广播信号可以包括TV广播信号、无线电广播信号、数据广播信号等等。而且,广播信号可以进一步包括与TV或无线电广播信号组合的广播信号。广播相关信息也可以经由移动通信网络提供,并且在该情况下,广播相关信息可以由移动通信模块112来接收。广播信号可以以各种形式存在,例如,其可以以数字多媒体广播(DMB)的电子节目指南(EPG)、数字视频广播手持(DVB-H)的电子服务指南(ESG)等等的形式而存在。广播接收模块111可以通过使用各种类型的广播系统接收信号广播。特别地,广播接收模块111可以通过使用诸如多媒体广播-地面(DMB-T)、数字多媒体广播-卫星(DMB-S)、数字视频广播-手持(DVB-H),前向链路媒体(MediaFLO®)的数据广播系统、地面数字广播综合服务(ISDB-T)等等的数字广播系统接收数字广播。广播接收模块111可以被构造为适合提供广播信号的各种广播系统以及上述数字广播系统。经由广播接收模块111接收的广播信号和/或广播相关信息可以存储在存储器160(或者其它类型的存储介质)中。

[0056] 移动通信模块112将无线电信号发送到基站(例如,接入点、节点B等等)、外部终端以及服务器中的至少一个和/或从其接收无线电信号。这样的无线电信号可以包括语音通话信号、视频通话信号、或者根据文本和/或多媒体消息发送和/或接收的各种类型的数据。

[0057] 无线互联网模块113支持移动终端的无线互联网接入。该模块可以内部或外部地耦接到终端。该模块所涉及的无线互联网接入技术可以包括WLAN(无线LAN)(Wi-Fi)、Wibro(无线宽带)、Wimax(全球微波互联接入)、HSDPA(高速下行链路分组接入)等等。

[0058] 短程通信模块114是用于支持短程通信的模块。短程通信技术的一些示例包括蓝牙™、射频识别(RFID)、红外数据协会(IrDA)、超宽带(UWB)、紫蜂™等等。

[0059] 位置信息模块115是用于检查或获取移动终端的位置信息的模块。位置信息模块的典型示例是GPS(全球定位系统)。根据当前的技术,GPS模块115计算来自三个或更多卫星的距离信息和准确的时间信息并且对于计算的信息应用三角测量法,从而根据经度、纬度和高度准确地计算三维当前位置信息。当前,用于计算位置和时间信息的方法使用三颗卫星并且通过使用另外的一颗卫星校正计算出的位置和时间信息的误差。此外,GPS模块115能够通过实时地连续计算当前位置信息来计算速度信息。

[0060] A/V输入单元120用于接收音频或视频信号。A/V输入单元120可以包括相机121和麦克风1220,相机121对在视频捕获模式或图像捕获模式中由图像捕获装置获得的静态图片或视频的图像数据进行处理。处理后的图像帧可以显示在显示模块151上。经相机121处

理后的图像帧可以存储在存储器160(或其它存储介质)中或者经由无线通信单元110进行发送,可以根据移动终端的构造提供两个或更多相机1210。麦克风122可以在电话通话模式、记录模式、语音识别模式等等运行模式中经由麦克风接收声音(音频数据),并且能够将这样的声音处理为音频数据。处理后的音频(语音)数据可以在电话通话模式的情况下转换为可经由移动通信模块112发送到移动通信基站的格式输出。麦克风122可以实施各种类型的噪声消除(或抑制)算法以消除(或抑制)在接收和发送音频信号的过程中产生的噪声或者干扰。

[0061] 用户输入单元130可以根据用户输入的命令生成键输入数据以控制移动终端的各种操作。用户输入单元130允许用户输入各种类型的信息,并且可以包括键盘、锅仔片、触摸板(例如,检测由于被接触而导致的电阻、压力、电容等等的变化的触敏组件)、滚轮、摇杆等等。特别地,当触摸板以层的形式叠加在显示模块151上时,可以形成触摸屏。

[0062] 感测单元140检测移动终端100的当前状态,(例如,移动终端100的打开或关闭状态)、移动终端100的位置、用户对于移动终端100的接触(即,触摸输入)的有无、移动终端100的取向、移动终端100的加速或减速移动和方向等等,并且生成用于控制移动终端100的操作的命令或信号。例如,当移动终端100实施为滑动型移动电话时,感测单元140可以感测该滑动型电话是打开还是关闭。另外,感测单元140能够检测电源单元190是否提供电力或者接口单元170是否与外部装置耦接。感测单元140可以包括接近传感器1410将在下面结合触摸屏来对此进行描述。

[0063] 接口单元170用作至少一个外部装置与移动终端100连接可以通过的接口。例如,外部装置可以包括有线或无线头戴式耳机端口、外部电源(或电池充电器)端口、有线或无线数据端口、存储卡端口、用于连接具有识别模块的装置的端口、音频输入/输出(I/O)端口、视频I/O端口、耳机端口等等。识别模块可以是存储用于验证用户使用移动终端100的各种信息并且可以包括用户识别模块(UIM)、客户识别模块(SIM)、通用客户识别模块(USIM)等等。另外,具有识别模块的装置(下面称为"识别装置")可以采取智能卡的形式,因此,识别装置可以经由端口或其它连接装置与移动终端100连接。接口单元170可以用于接收来自外部装置的输入(例如,数据信息、电力等等)并且将接收到的输入传输到移动终端100内的一个或多个元件或者可以用于在移动终端和外部装置之间传输数据。

[0064] 另外,当移动终端100与外部底座连接时,接口单元170可以用作允许通过其将电力从底座提供到移动终端100的路径或者可以用作允许从底座输入的各种命令信号通过其传输到移动终端的路径。从底座输入的各种命令信号或电力可以用作用于识别移动终端是否准确地安装在底座上的信号。输出单元150被构造为以视觉、音频和/或触觉方式提供输出信号(例如,音频信号、视频信号、警报信号、振动信号等等)。输出单元150可以包括显示模块151、音频输出模块152、警报模块153等等。

[0065] 显示模块151可以显示在移动终端100中处理的信息。例如,当移动终端100处于电话通话模式时,显示模块151可以显示与通话或其它通信(例如,文本消息收发、多媒体文件下载等等)相关的用户界面(UI)或图形用户界面(GUI)。当移动终端100处于视频通话模式或者图像捕获模式时,显示模块151可以显示捕获的图像和/或接收的图像、示出视频或图像以及相关功能的UI或GUI等等。

[0066] 同时,当显示模块151和触摸板以层的形式彼此叠加以形成触摸屏时,显示模块

151可以用作输入装置和输出装置。显示模块151可以包括液晶显示器(LCD)、薄膜晶体管LCD(TFT-LCD)、有机发光二极管(OLED)显示器、柔性显示器、三维(3D)显示器等等中的至少一种。这些显示器中的一些可以被构造为透明状以允许用户从外部观看，这可以称为透明显示器，典型的透明显示器可以例如为TOLED(透明有机发光二极管)显示器等等。根据特定想要的实施方式，移动终端100可以包括两个或更多显示模块(或其它显示装置)，例如，移动终端可以包括外部显示模块(未示出)和内部显示模块(未示出)。触摸屏可用于检测触摸输入压力以及触摸输入位置和触摸输入面积。

[0067] 音频输出模块152可以在移动终端处于呼叫信号接收模式、通话模式、记录模式、语音识别模式、广播接收模式等等模式下时，将无线通信单元110接收的或者在存储器160中存储的音频数据转换音频信号并且输出为声音。而且，音频输出模块152可以提供与移动终端100执行的特定功能相关的音频输出(例如，呼叫信号接收声音、消息接收声音等等)。音频输出模块152可以包括扬声器、蜂鸣器等等。

[0068] 警报模块153可以提供输出以将事件的发生通知给移动终端100。典型的事件可以包括呼叫接收、消息接收、键信号输入、触摸输入等等。除了音频或视频输出之外，警报模块153可以以不同的方式提供输出以通知事件的发生。例如，警报模块153可以以振动的形式提供输出，当接收到呼叫、消息或一些其它进入通信(incomingcommunication)时，警报模块153可以提供触觉输出(即，振动)以将其通知给用户。通过提供这样的触觉输出，即使在用户的移动电话处于用户的口袋中时，用户也能够识别出各种事件的发生。警报模块153也可以经由显示模块151或音频输出模块152提供通知事件的发生的输出。

[0069] 存储器160可以存储由控制器180执行的处理和控制操作的软件程序等等，或者可以暂时地存储已经输出或将要输出的数据(例如，电话簿、消息、静态图像、视频等等)。而且，存储器160可以存储关于当触摸施加到触摸屏时输出的各种方式的振动和音频信号的数据。

[0070] 存储器160可以包括至少一种类型的存储介质，所述存储介质包括闪存、硬盘、多媒体卡、卡型存储器(例如，SD或DX存储器等等)、随机访问存储器(RAM)、静态随机访问存储器(SRAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、可编程只读存储器(PROM)、磁性存储器、磁盘、光盘等等。而且，移动终端100可以与通过网络连接执行存储器160的存储功能的网络存储装置协作。

[0071] 控制器180通常控制移动终端的总体操作。例如，控制器180执行与语音通话、数据通信、视频通话等等相关的控制和处理。另外，控制器180可以包括用于再现(或回放)多媒体数据的多媒体模块1810，多媒体模块1810可以构造在控制器180内，或者可以构造为与控制器180分离。控制器180可以执行模式识别处理，以将在触摸屏上执行的手写输入或者图片绘制输入识别为字符或图像。

[0072] 电源单元190在控制器180的控制下接收外部电力或内部电力并且提供操作各元件和组件所需的适当的电力。

[0073] 这里描述的各种实施方式可以以使用例如计算机软件、硬件或其任何组合的计算机可读介质来实施。对于硬件实施，这里描述的实施方式可以通过使用特定用途集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理装置(DSPD)、可编程逻辑装置(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器、被设计为执行这里描述的功能的

电子单元中的至少一种来实施，在一些情况下，这样的实施方式可以在控制器180中实施。对于软件实施，诸如过程或功能的实施方式可以与允许执行至少一种功能或操作的单独的软件模块来实施。软件代码可以由以任何适当的编程语言编写的软件应用程序(或程序)来实施，软件代码可以存储在存储器160中并且由控制器180执行。

[0074] 至此，已经按照其功能描述了移动终端。下面，为了简要起见，将描述诸如折叠型、直板型、摆动型、滑动型移动终端等等的各种类型的移动终端中的滑动型移动终端作为示例。因此，本发明能够应用于任何类型的移动终端，并且不限于滑动型移动终端。

[0075] 如图1中所示的移动终端100可以被构造为利用经由帧或分组发送数据的诸如有线和无线通信系统以及基于卫星的通信系统来操作。

[0076] 现在将参考图2描述其中根据本发明的移动终端能够操作的通信系统。

[0077] 这样的通信系统可以使用不同的空中接口和/或物理层。例如，由通信系统使用的空中接口包括例如频分多址(FDMA)、时分多址(TDMA)、码分多址(CDMA)和通用移动通信系统(UMTS)(特别地，长期演进(LTE))、全球移动通信系统(GSM)等等。作为非限制性示例，下面的描述涉及CDMA通信系统，但是这样的教导同样适用于其它类型的系统。

[0078] 参考图2，CDMA无线通信系统可以包括多个移动终端100、多个基站(BS)270、基站控制器(BSC)275和移动交换中心(MSC)280。MSC280被构造为与公共电话交换网络(PSTN)290形成接口。MSC280还被构造为与可以经由回程线路耦接到基站270的BSC275形成接口。回程线路可以根据若干已知的接口中的任一种来构造，所述接口包括例如E1/T1、ATM，IP、PPP、帧中继、HDSL、ADSL或xDSL。将理解的是，如图2中所示的系统可以包括多个BSC2750。

[0079] 每个BS270可以服务一个或多个分区(或区域)，由多向天线或指向特定方向的天线覆盖的每个分区放射状地远离BS270。或者，每个分区可以由用于分集接收的两个或更多天线覆盖。每个BS270可以被构造为支持多个频率分配，并且每个频率分配具有特定频谱(例如，1.25MHz，5MHz等等)。

[0080] 分区与频率分配的交叉可以被称为CDMA信道。BS270也可以被称为基站收发器子系统(BTS)或者其它等效术语。在这样的情况下，术语"基站"可以用于笼统地表示单个BSC275和至少一个BS270。基站也可以被称为"蜂窝站"。或者，特定BS270的各分区可以被称为多个蜂窝站。

[0081] 如图2中所示，广播发射器(BT)295将广播信号发送给在系统内操作的移动终端100。如图1中所示的广播接收模块111被设置在移动终端100处以接收由BT295发送的广播信号。在图2中，示出了几个全球定位系统(GPS)卫星300。卫星300帮助定位多个移动终端100中的至少一个。

[0082] 在图2中，描绘了多个卫星300，但是理解的是，可以利用任何数目的卫星获得有用的定位信息。如图1中所示的GPS模块115通常被构造为与卫星300配合以获得想要的定位信息。替代GPS跟踪技术或者在GPS跟踪技术之外，可以使用可以跟踪移动终端的位置的其它技术。另外，至少一个GPS卫星300可以选择性地或者额外地处理卫星DMB传输。

[0083] 作为无线通信系统的一个典型操作，BS270接收来自各种移动终端100的反向链路信号。移动终端100通常参与通话、消息收发和其它类型的通信。特定基站270接收的每个反向链路信号被在特定BS270内进行处理。获得的数据被转发给相关的BSC275。BSC提供通话资源分配和包括BS270之间的软切换过程的协调的移动管理功能。BSC275还将接收到的数

据路由到MSC280，其提供用于与PSTN290形成接口的额外的路由服务。类似地，PSTN290与MSC280形成接口，MSC与BSC275形成接口，并且BSC275相应地控制BS270以将正向链路信号发送到移动终端100。

[0084] 基于上述移动终端硬件结构以及通信系统，提出本发明方法各个实施例。

[0085] 实施例一

[0086] 图3为本实施例的一种验证系统的示范性结构框图，下面结合图3来描述本实施例的一种验证系统，如图3所示，一种验证系统，包括：

[0087] 申请端10、待验证移动终端20和运营商30，其中，

[0088] 所述申请端10，用于输入待验证手机号码，并向运营商30发送包含所述待验证手机号码及申请端信息的验证请求，所述申请端信息包括：申请端手机号码及申请端物理地址；

[0089] 所述运营商30，用于接收所述申请端10发来的验证请求，并将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端20；

[0090] 所述待验证移动终端20，用于接收运营商30发来的申请端信息及验证码，并将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示。

[0091] 在本实施例中，通过对申请验证的移动终端及待验证的移动终端的信息匹配，来判断验证码的是否存在安全风险，并根据判断结果自动提供不同的风险提示，提高了验证码的安全性，提供了更好的用户体验。

[0092] 在本实施例中，申请端也即申请验证的移动终端为具备通信功能的终端，比如为手机。

[0093] 在本实施例中，当移动终端上安装有某一第三方应用程序APP时，比如：中国移动10086的登陆APP或支付宝等，需要进行身份验证时，需要用户通过手机等移动终端向运营商发送绑定的手机号码进行验证，验证成功后会以短信的形式发送一验证码至绑定手机号码。

[0094] 在本实施例中，当移动终端首次安装第三方应用程序APP时，会自动获取移动终端的手机号码、物理地址，之后，移动终端每次接收到所述第三方应用程序APP的验证消息时，都会在向运营商发送验证请求的同时，将其对应的手机号码、物理地址与待验证的手机号码(也即该第三方应用程序账号绑定的手机号码)一同发送给运营商，运营商在想所述待验证的手机号码发送验证码的同时，也将其接收到的所述申请端对应的手机号码、物理地址与待验证的手机号码一同发送给待验证手机号码对应的待验证移动终端，由于待验证移动终端获取自身的手机号码、物理地址与所述申请端的进行比对，若匹配成功，则表示申请端与待验证移动终端为同一个移动终端，所述申请验证码的用户为注册用户，当申请端手机号码与待验证手机号码不同时，说明申请验证的用户不是注册用户，有可能时骗子，此时则发出第一风险提示信息“骗子正打算骗你，不要把验证码告知他”；如果申请端手机号码与待验证手机号码相同时，但物理地址不同，也有可能存在风险，则发出第二风险提示信息“系统检测到蓝牙地址和手机WLAN MAC地址变动，如果您没有换手机，极有可能是骗子在骗取你的验证码，盗取你的个人信息和财产!”；只有当手机号码和物理地址全相同时，才不做提示，此时用户可放心使用验证码。

[0095] 在本实施例中，图4为一种第三方应用程序APP验证码获取界面，当用户在申请端的验证码获取界面输入待验证手机号码，点击获取按钮后，在向运营商发送验证请求的报文中加入获取到的申请端信息，所述申请端信息只是几个字段，并不会导致任何效率变差，其中，申请端信息会通过系统进行加密生成密文，运营商只能知道自己拿到的内容是用户的手机信息，但无法解析，这样能有效避免运营商偷窥用户个人信息；运营商获取到验证请求后，将所述密文和生成的验证码打包一起放进一个新的报文，并发送至用户输入的待验证手机号码所对应的待验证移动终端；待验证移动终端收到新的报文后，将所述报文发送至系统框架，所述用于接收加密后的申请端信息，并进行解密，得到申请端手机号码和申请端物理地址，随后进行对比以获得验证结果并提供与验证结果对应的风险提示。

[0096] 在本实施例中，所述申请端物理地址为：申请端蓝牙地址和/或申请端WLAN MAC地址；所述待验证移动终端物理地址为：待验证移动终端蓝牙地址和/或待验证移动终端WLAN MAC地址，由于所述蓝牙地址及移动终端WLAN MAC地址都是与移动终端唯一对应的身份地址，所以两者可以分开来用，当然，为了更高的安全性，这两也可以一起用，也即当申请端和待验证移动终端的手机号码、蓝牙地址及移动终端WLAN MAC三者全部匹配时，才认定为安全，否则，第一风险提示信息就如图5所示，相应的，第二风险提示信息就如图6所示。

[0097] 实施例二

[0098] 如图7所示，在本实施例中，所述待验证移动终端20包括：第一判断单元21和第二判断单元22，其中

[0099] 所述第一判断单元21，用于判断所述申请端手机号码与所述待验证手机号码是否相同；若所述申请端手机号码与所述待验证手机号码不同，则验证码存在安全风险，并在所述待验证移动终端20上显示第一风险提示信息；

[0100] 所述第二判断单元22，用于当所述申请端手机号码与所述待验证手机号码相同时，判断所述申请端物理地址与所述待验证移动终端物理地址是否相同；若所述申请端物理地址与所述待验证移动终端物理地址不同，则验证码存在安全风险，并在所述待验证移动终端20上显示第二风险提示信息；若所述申请端物理地址与所述待验证移动终端物理地址相同，则验证码安全。

[0101] 实施例三

[0102] 如图8所示，在本实施例中，所述申请端10包括：

[0103] 输入单元11，用于在申请端10的APP验证码获取界面输入待验证手机号码，触发“点击获取”按钮；

[0104] 加密发送单元12，用于获取申请端信息，将所述申请端信息加密并与所述待验证手机号码一同发送至运营商，其中，所述申请端信息包括：申请端手机号码及申请端物理地址；

[0105] 相应地，如图9所示，所述运营商30包括：

[0106] 接收反馈单元，用于接收加密后的申请端信息及验证码，并将所述加密后的申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端。

[0107] 实施例四

[0108] 图10为本实施例的一种验证方法的流程图，下面结合图10来描述本实施例的一种验证方法，如图10所示，一种验证方法，包括：

[0109] S10、申请端输入待验证手机号码，并向运营商发送包含所述待验证手机号码及申请端信息的验证请求，所述申请端信息包括：申请端手机号码及申请端物理地址；

[0110] S20、运营商将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端；

[0111] S30、将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示。

[0112] 在本实施例中，所述申请端物理地址为：申请端蓝牙地址和/或申请端WLAN MAC地址；所述待验证移动终端物理地址为：待验证移动终端蓝牙地址和/或待验证移动终端WLAN MAC地址。

[0113] 实施例五

[0114] 如图11所示，在本实施例中，所述S30包括：

[0115] S31、判断所述申请端手机号码与所述待验证手机号码是否相同；

[0116] S32、若所述申请端手机号码与所述待验证手机号码不同，则验证码存在安全风险，并在所述待验证移动终端上显示第一风险提示信息；

[0117] S33、若所述申请端手机号码与所述待验证手机号码相同，判断所述申请端物理地址与所述待验证移动终端物理地址是否相同；

[0118] S34、若所述申请端物理地址与所述待验证移动终端物理地址不同，则验证码存在安全风险，并在所述待验证移动终端上显示第二风险提示信息；

[0119] S35、若所述申请端物理地址与所述待验证移动终端物理地址相同，则验证码安全。

[0120] 实施例六

[0121] 如图12所示，在本实施例中，所述步骤S10包括：

[0122] S11、在申请端的APP验证码获取界面输入待验证手机号码，触发“点击获取”按钮；

[0123] S12、获取申请端信息，将所述申请端信息加密并与所述待验证手机号码一同发送至运营商，其中，所述申请端信息包括：申请端手机号码及申请端物理地址；

[0124] 相应地，所述S20具体为：

[0125] S21、所述运营商将加密后的申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端。

[0126] 需要说明的是，在本文中，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、物品或者装置不仅包括那些要素，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、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0127] 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。

[0128] 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上述实施例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,空调器,或者网络设备等)执行本发明各个实施例所述的方法。

[0129] 以上仅为本发明的优选实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本发明的专利保护范围内。

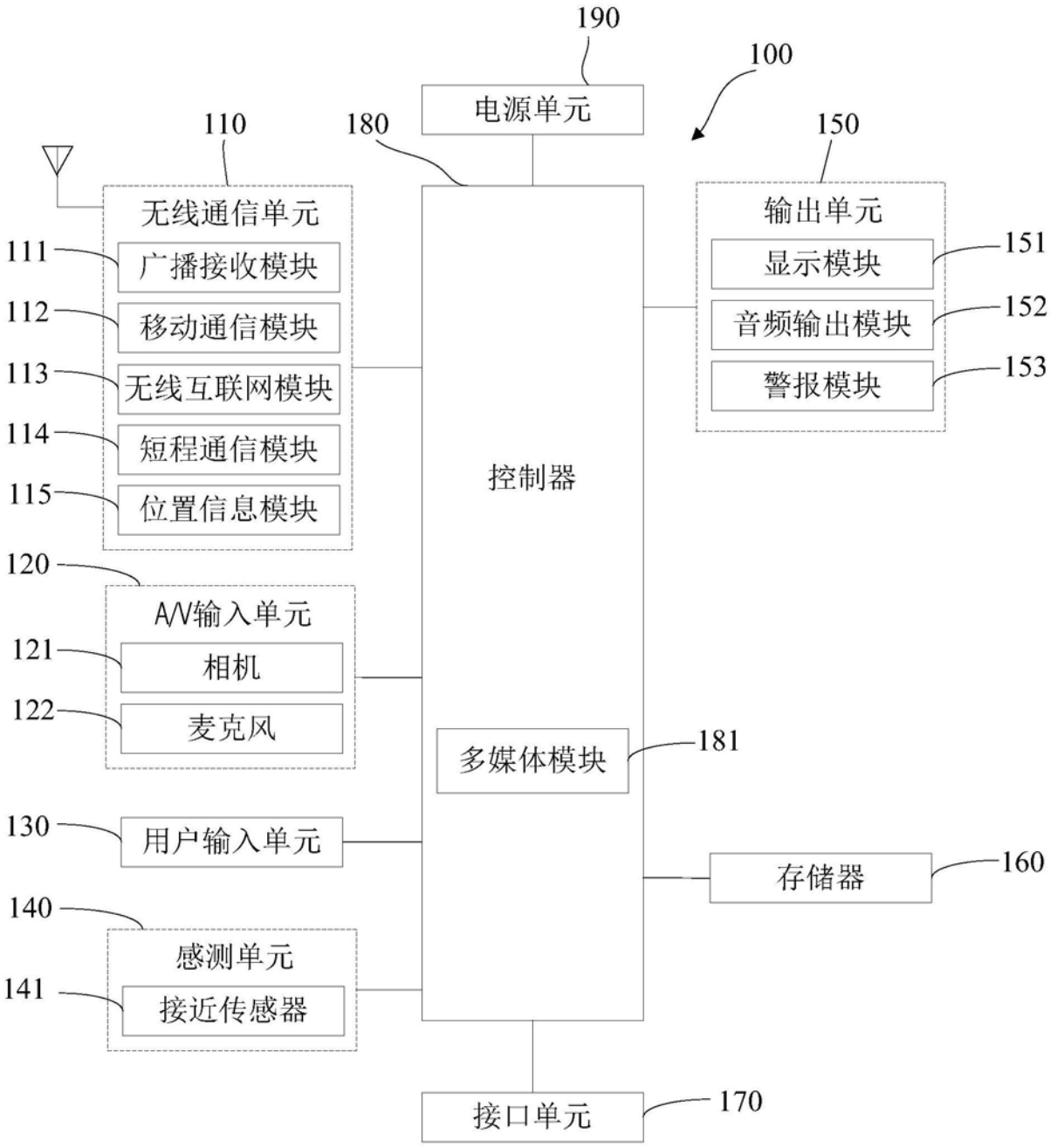

190
100
电源单元
110
180
150
无线通信单元
输出单元
111
广播接收模块
显示模块
151
112
移动通信模块
音频输出模块
152
113
无线互联网模块
警报模块
153
114
短程通信模块
控制器
115
位置信息模块
120
A/V输入单元
121
相机
122
麦克风
多媒体模块
181
130
用户输入单元
存储器
160
140
感测单元
141
接近传感器
接口单元
170

图1

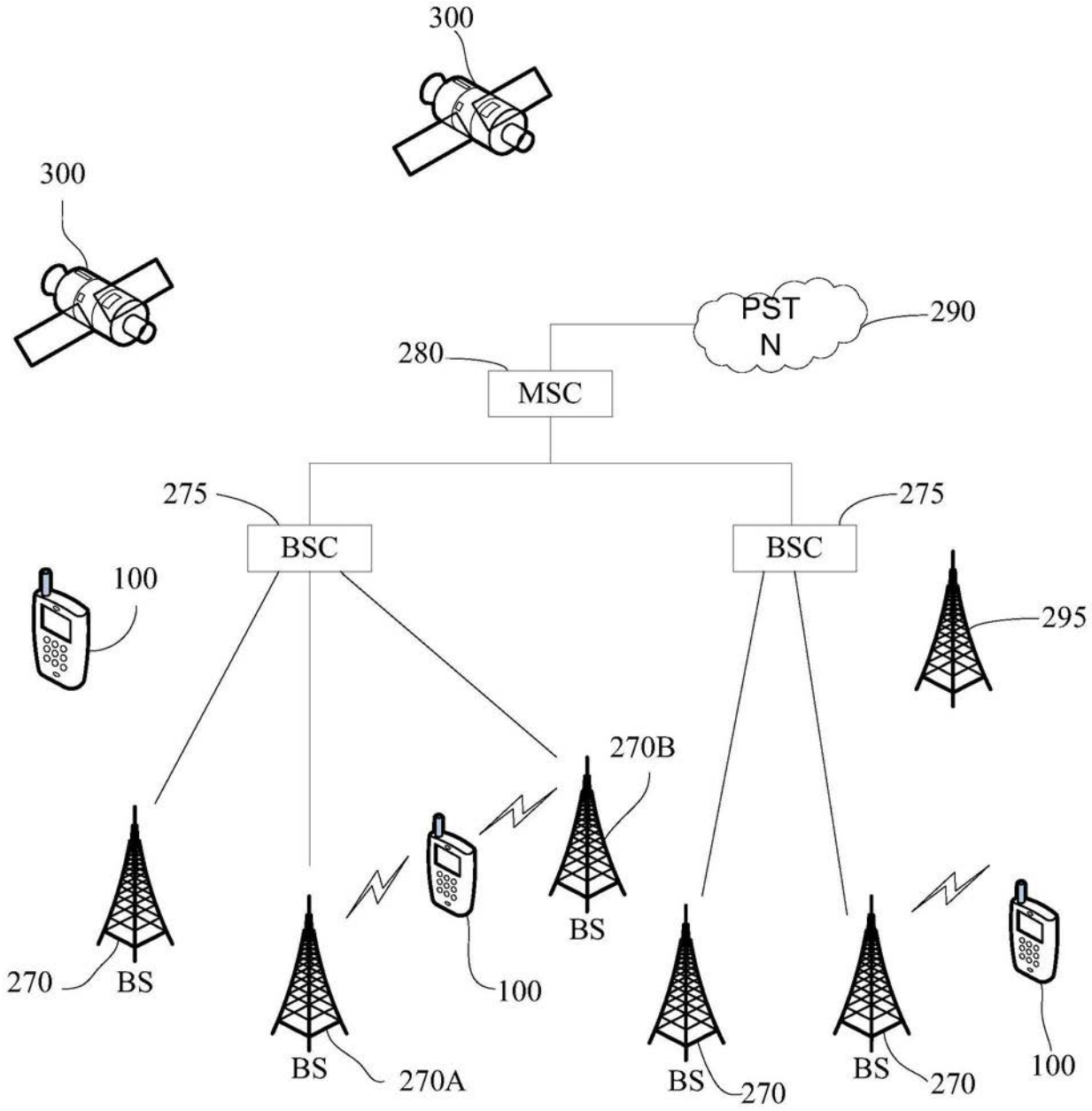

300
300
PST
N
290
280
MSC
275
BSC
275
BSC
100
295
270B
BS
270
BS
100
BS
270A
BS
270
BS
270
100

图2

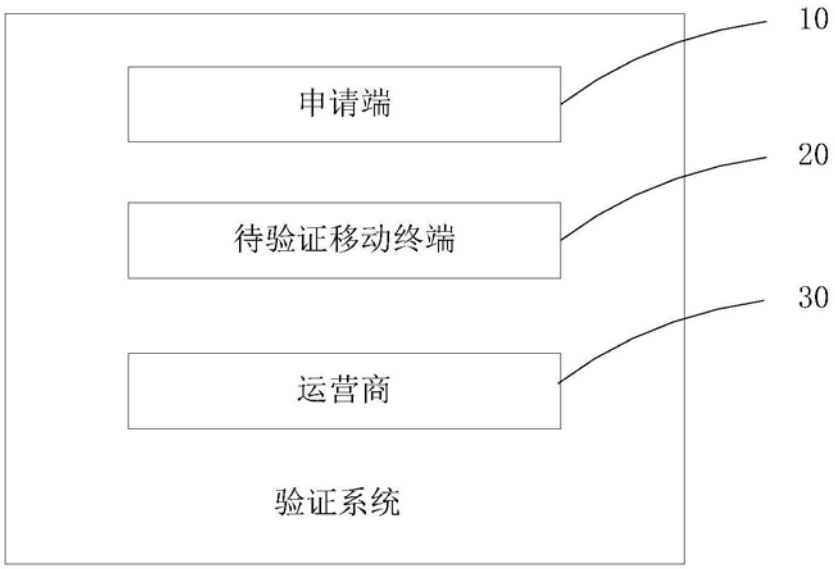

10
申请端
20
待验证移动终端
30
运营商
验证系统

图3


返回
登录
136[redacted]3935
服务密码
动态密码
短信验证码
点击获取
登录
同意《登录协议》

图4


警告
骗子正打算骗你，不要把验证码告知他！
我知道了

图5


警告
系统检测到蓝牙地址和手机WLAN MAC地址变动，如果您没有换手机，极有可能是骗子在骗取你的验证码，盗取你的个人信息和财产！
我知道了

图6

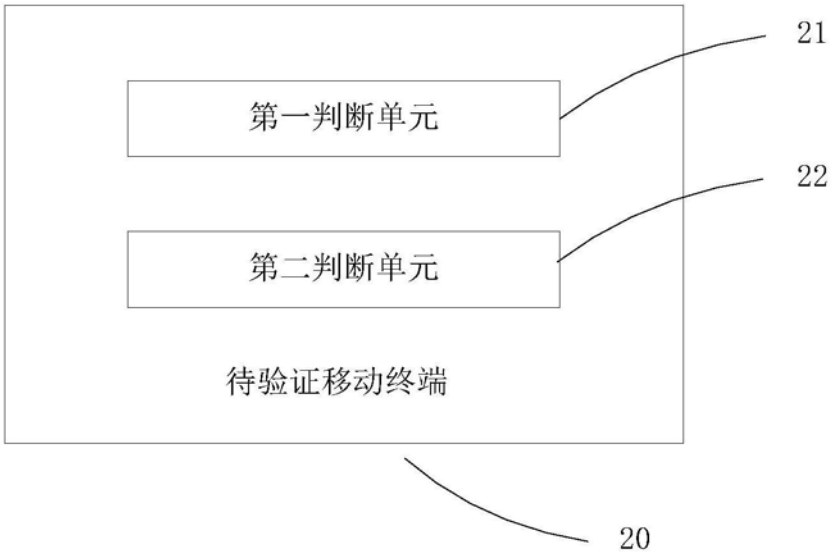


图7

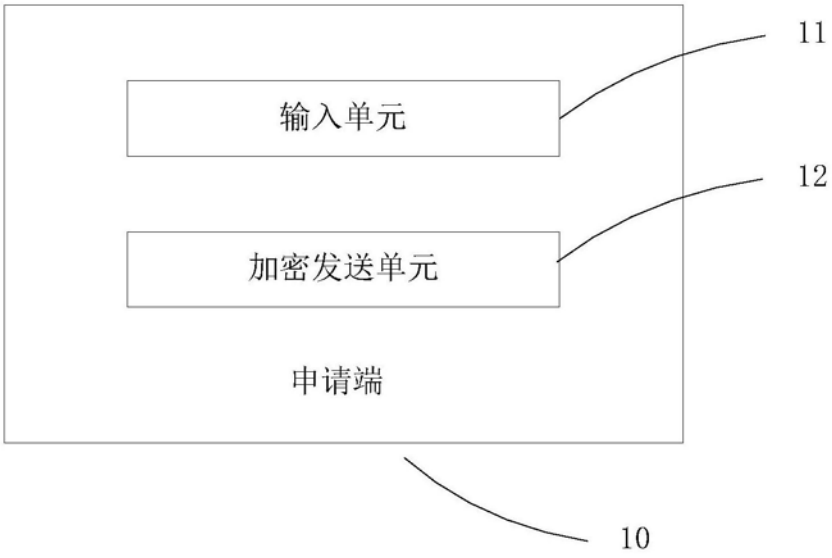


图8

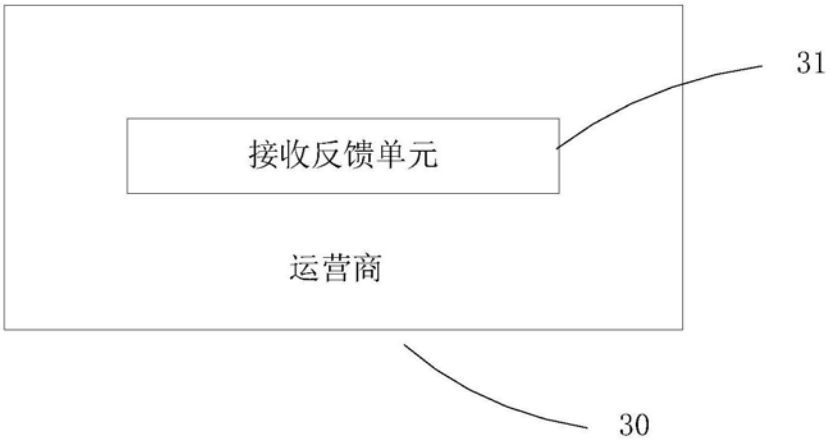

31
接收反馈单元
运营商
30

图9

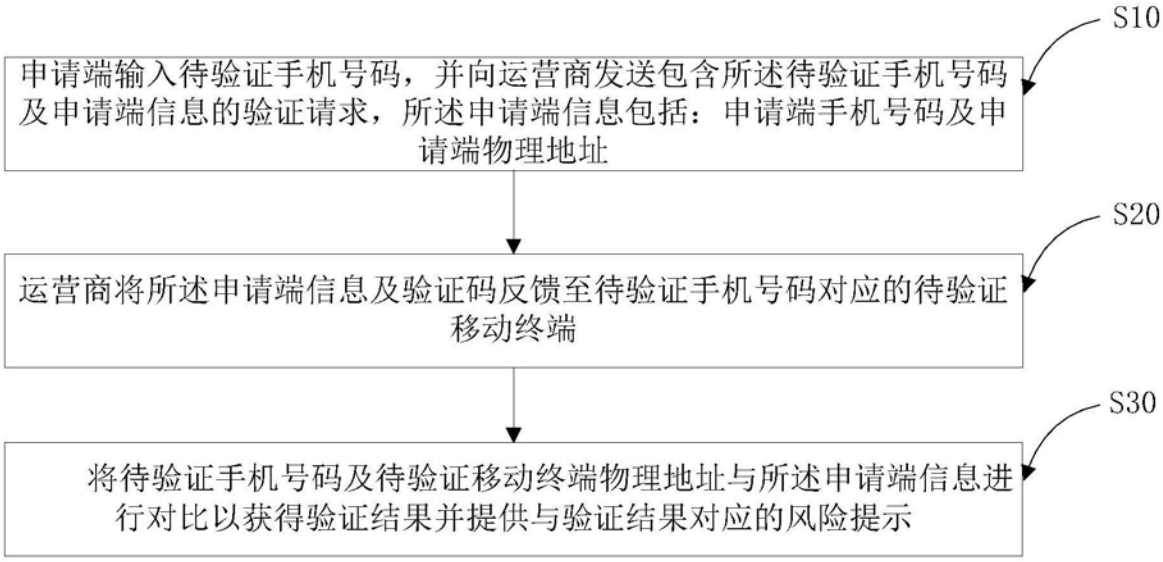

S10
申请端输入待验证手机号码，并向运营商发送包含所述待验证手机号码及申请端信息的验证请求，所述申请端信息包括：申请端手机号码及申请端物理地址
S20
运营商将所述申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端
S30
将待验证手机号码及待验证移动终端物理地址与所述申请端信息进行对比以获得验证结果并提供与验证结果对应的风险提示

图10

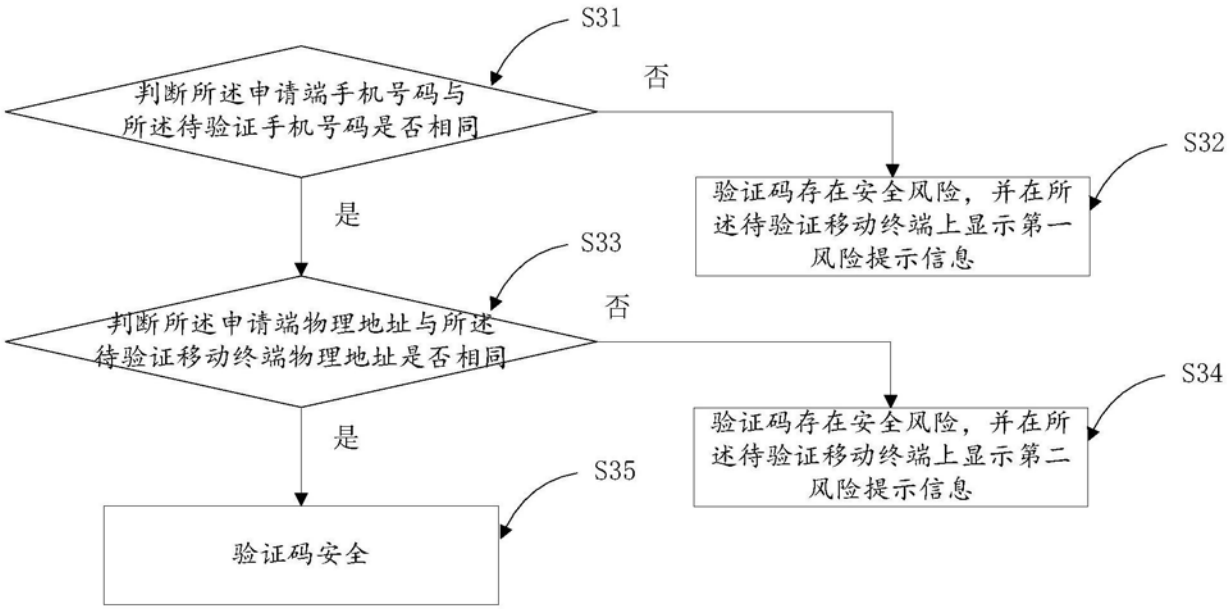

S31
判断所述申请端手机号码与所述待验证手机号码是否相同
否
是
S32
验证码存在安全风险，并在所述待验证移动终端上显示第一风险提示信息
S33
判断所述申请端物理地址与所述待验证移动终端物理地址是否相同
否
是
S34
验证码存在安全风险，并在所述待验证移动终端上显示第二风险提示信息
S35
验证码安全

图11

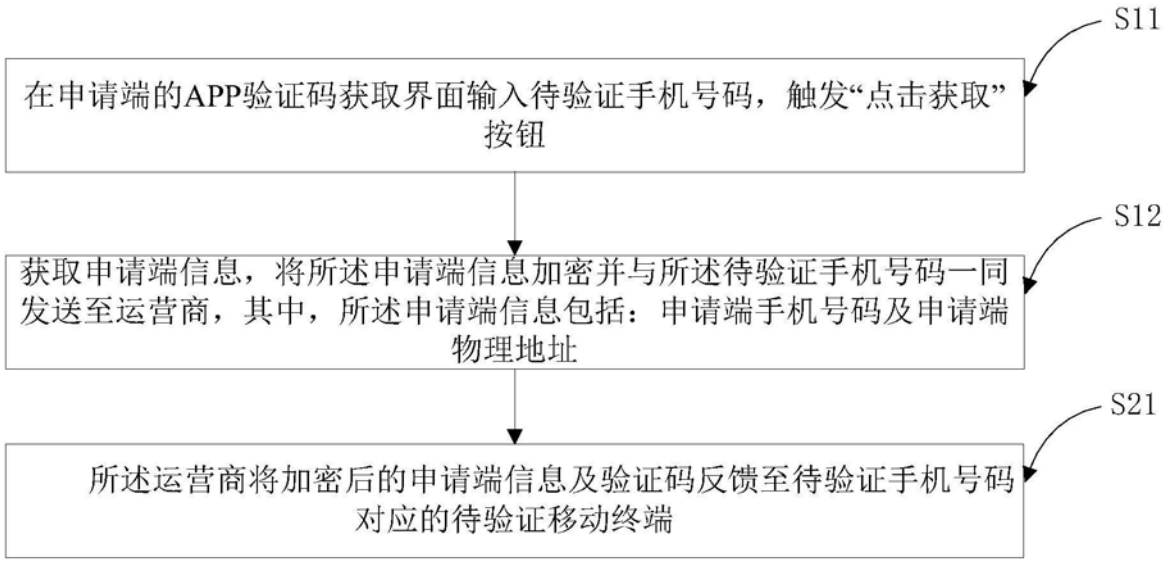

S11
在申请端的APP验证码获取界面输入待验证手机号码，触发“点击获取”按钮
S12
获取申请端信息，将所述申请端信息加密并与所述待验证手机号码一同发送至运营商，其中，所述申请端信息包括：申请端手机号码及申请端物理地址
S21
所述运营商将加密后的申请端信息及验证码反馈至待验证手机号码对应的待验证移动终端

图12