



(12) 发明专利

(10) 授权公告号 CN 103456092 B

(45) 授权公告日 2016. 01. 20

(21) 申请号 201310422178. 0

CN 101551926 A, 2009. 10. 07,

(22) 申请日 2013. 09. 16

CN 101751727 A, 2010. 06. 23,

(73) 专利权人 广州广电运通金融电子股份有限公司

CN 1809848 A, 2006. 07. 26,

CN 102194276 A, 2011. 09. 21,

地址 510663 广东省广州市科学城科林路9号

审查员 姚连芳

(72) 发明人 肖大海 欧阳小明 王庆华
董学文 雍容 黄婉琦

(74) 专利代理机构 广州新诺专利商标事务有限公司 44100

代理人 华辉 林玉芳

(51) Int. Cl.

G07F 7/08(2006. 01)

G07F 19/00(2006. 01)

(56) 对比文件

CN 101645183 A, 2010. 02. 10,

CN 202196470 U, 2012. 04. 18,

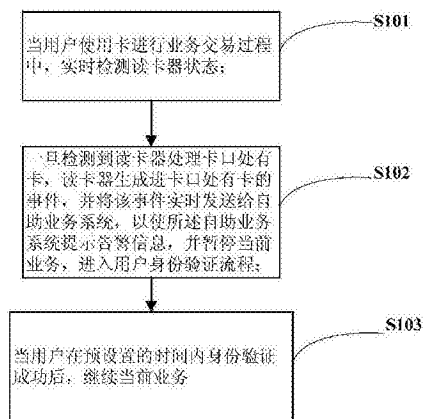
权利要求书2页 说明书7页 附图3页

(54) 发明名称

读卡器处理卡方法、装置

(57) 摘要

本发明提供了一种读卡器处理卡方法、装置及自助设备,在检测到读卡器中有卡时,仍然不断的检测读卡器处理卡口是否存在卡,一旦检测到处理卡口有卡,则向用户提示告警当心卡被调包,同时暂停当前正在进行的业务,要求用户进行身份验证,自助服务界面切换到等待用户输入密码界面,只有当用户在规定的时间内正确输入了密码,才会继续当前业务的处理。该方案能有效避免以下情况:用户进行自助业务过程中,不法分子在读卡器上插入一张伪卡冒充用户的卡,从引诱用户交出业务操作权让用户蒙受经济损失,提高了自助业务的安全性。



1. 一种读卡器处理卡方法,其特征在于,包括:

当用户使用卡进行业务交易过程中,实时检测读卡器状态;

一旦检测到读卡器处理卡口处有卡,读卡器生成进卡口处有卡的事件,并将该事件实时发送给自助业务系统,以使所述自助业务系统提示告警信息,并暂停当前业务,进入用户身份验证流程;

当用户在预设置的时间内身份验证成功后,继续当前业务。

2. 根据权利要求 1 所述的方法,其特征在于,所述实时检测读卡器状态,包括:

利用读卡器判卡进卡或判磁进卡的硬件提供的处理卡功能,对读卡器进卡口处是否有卡进行检测。

3. 根据权利要求 1 所述的方法,其特征在于,所述实时检测读卡器状态,包括:

利用读卡器异物检测功能,对读卡器进卡口处是否有卡进行检测。

4. 根据权利要求 3 所述的方法,其特征在于,所述利用读卡器异物检测功能,对读卡器进卡口处是否有卡进行检测,包括:

在没有业务操作期间,读卡器异物检测装置处于正常工作模式,当读卡器异物检测装置在预设置的时间内一直检测到有异物遮挡,停止业务处理,并发出报警通知;

在开始进行业务操作时,切换所述读卡器异物检测装置由正常工作模式进入紧急工作模式,只要读卡器异物检测装置一检测到异物遮挡,就会立即报警。

5. 根据权利要求 1—4 任一项所述的方法,其特征在于,所述方法还包括:

如果当前业务的操作结果并不会导致用户帐户资金或用户密码发生变化,则在完成本次业务之后或者本次业务超时之后,才进入用户身份验证流程;

对于本次业务的操作结果会导致用户帐户资金或用户密码发生变化,则立即暂停当前业务,进入用户身份验证流程。

6. 根据权利要求 1 所述的方法,其特征在于,所述方法还包括:

若当用户在预设置的时间内身份验证失败,终止当前业务,进行退卡或吞卡处理。

7. 一种读卡器处理卡装置,其特征在于,所述装置包括:

第一检测模块和第二检测模块,分别用于检测读卡器内部和进卡口是否有卡,并将检测结果发送给判断分析模块;

所述判断分析模块,用于接收所述第一检测模块和第二检测模块的监测结果,当所述第一检测模块与所述第二检测模块均检测到有卡,且自助业务系统正在进行业务处理时,所述判断分析模块向自助业务系统和告警提示模块分别发送告警信息;

所述告警提示模块,用于向用户通过屏幕显示或者声音提示的方式传达告警信息;

所述自助业务系统,用于接收告警信息,中止当前业务的进行,并调用用户身份验证模块进行用户身份验证;

所述用户身份验证模块,用于完成身份验证流程,若成功完成身份验证,则发送信息给所述自助业务系统,以使自助业务系统继续当前业务;如果身份验证模块在预设置的时间里进行用户身份验证失败,则自助业务系统终止当前业务,最后进行退卡或者吞卡处理。

8. 根据权利要求 7 所述的装置,其特征在于,所述第二检测模块,采用读卡器判卡进卡或判磁进卡的硬件提供的处理卡功能模块,或采用读卡器异物检测功能模块。

9. 根据权利要求 7 或 8 所述的装置,其特征在于,所述的用户身份验证模块,采用用户

再次输入帐户密码进行身份验证的功能模块。

读卡器处理卡方法、装置

技术领域

[0001] 本发明涉及金融自助终端技术领域，尤其涉及一种读卡器处理卡方法、装置以及其自助设备。

背景技术

[0002] 日常生活中常见的一种金融自助设备是 ATM(Automated Teller machine, ATM)，自助设备进行大部分自助服务，要使用银行卡，如有卡存款、有卡取款、查询、改密、转账等。在自助服务过程中，用户要确保银行卡信息和密码信息至少有一没有泄密，如当用户在自助服务过程中正确输入密码后，到银行卡退卡的过程中，要保证操作权不能被其他人掌握。目前的自助设备并没有很好的解决这个问题，仍存在以下问题：

[0003] 当用户在自助服务过程中，把卡插入读卡器内，输入密码，正在界面操作进行交易过程中，犯罪分子在读卡器处理卡口插上一张伪卡冒充用户的真卡，然后不法分子诱骗用户说其服务完成卡已退出，用户看到读卡器处理卡口确实有卡，往往误以为是自己的卡被退出来了，就拿着伪卡主动或被迫离开自助设备。实际上用户的卡仍然还在读卡器内，由于用户已经输入了正确的密码，这时犯罪分子就可以继续进行交易，取走了用户卡内的现金。这就是目前不法分子利用自助设备读卡器中有卡时，还在读卡器处理卡口插卡，自助设备对此情况在技术上没有任何提示和处理的特点，在用户业务操作过程中对银行卡进行调包，盗取用户银行卡内的现金，导致自助设备存在安全隐患。

[0004] 因此，有必要对自助设备现有技术进行改进，来有效防止用户银行卡被调包，防止在自助业务过程中操作权落入到不法分子手中，给用户卡内资金安全带来危险。

发明内容

[0005] 本发明的目的是提供一种读卡器处理卡方法、装置及自助设备，以使自助设备在为用户进行业务处理过程中，防止在用户进行业务过程中，业务操作权落入他人手中，让用户及时识破银行卡调包骗局，从而提高自助设备的安全性和智能性，保障用户财产安全。

[0006] 为实现上述目的，本发明提供了如下技术方案：

[0007] 一种读卡器处理卡方法，应用于自助设备，包括：

[0008] 当用户使用卡进行业务交易过程中，实时检测读卡器状态；

[0009] 一旦检测到读卡器处理卡口处有卡，读卡器生成进卡口处有卡的事件，并将该事件实时发送给自助业务系统，以使所述自助业务系统提示告警信息，并暂停当前业务，进入用户身份验证流程；

[0010] 当用户在预设置的时间内身份验证成功后，继续当前业务。

[0011] 其中，所述的读卡器第二检测模块，其对处理卡口处的卡的检测功能，可以由读卡器检测装置提供的判磁模块或判卡模块实现，也可以由读卡器处理卡口异物检测装置实现。

[0012] 所述的告警指令的生成既可以是读卡器装置本身根据其两个检测模块的结果产

生；也可以由自助业务系统根据读卡器传送来的两个检测模块的检测结果产生。

[0013] 其中，所述用户进行身份验证，可以是要求用户再次输入密码，或者指纹等生物信息，或者自助业务系统提供的其他可以验证用户身份的公知技术手段，如手机验证，U盾验证等方式。

[0014] 一种读卡器处理卡装置，应用于自助设备，包括：

[0015] 第一检测模块和第二检测模块，分别用于检测读卡器内部和进卡口是否有卡，并将检测结果发送给判断分析模块；

[0016] 所述判断分析模块，用于接收所述第一检测模块和第二检测模块的监测结果，当所述第一检测模块与所述第二检测模块均检测到有卡，且自助业务系统正在进行业务处理时，所述判断分析模块向自助业务系统和告警提示模块分别发送告警信息；

[0017] 所述告警提示模块，用于向用户通过屏幕显示或者声音提示的方式传达告警信息；

[0018] 所述自助业务系统，用于接收告警信息，中止当前业务的进行，并调用用户身份验证模块进行用户身份验证；

[0019] 所述用户身份验证模块，用于完成身份验证流程，若成功完成身份验证，则发送信息给所述自助业务系统，以使自助业务系统继续当前业务；如果身份验证模块在预设置的时间里进行用户身份验证失败，则自助业务系统终止当前业务，最后进行退卡或者吞卡处理。

[0020] 通过以上方案可知，本发明提供一种读卡器处理卡方法、装置及自助设备，在检测到读卡器中有卡时，仍然不断的检测读卡器处理卡口是否存在卡，一旦检测到处理卡口有卡，则向用户提示告警当心卡被调包，同时暂停当前正在进行的业务，要求用户进行身份验证，自助服务界面切换到等待用户输入密码界面，只有当用户在规定的时间内正确输入了密码，才会继续当前业务的处理。该方案能有效避免以下情况：用户进行自助业务过程中，不法分子在读卡器上插入一张伪卡冒充用户的卡，从引诱用户交出业务操作权让用户蒙受经济损失。本方案提高了自助业务的安全性。

附图说明

[0021] 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简单地介绍，显而易见地，下面描述中的附图仅仅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。

[0022] 图1是本发明实施例中一种读卡器处理卡方法的流程图；

[0023] 图2是本发明实施例中一种读卡器处理卡装置的结构示意图；

[0024] 图3是本发明实施例中读卡器异物检测装置的两种工作模式切换流程图；

[0025] 图4是本发明实施例中一种读卡器异物检测切换控制方法流程图。

具体实施方式

[0026] 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作出创造性劳动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。

[0027] 请参阅图 1,图 1 为本申请实施例提供的一种读卡器处理卡方法的流程图,包括:

[0028] 步骤 S101:当用户使用卡进行业务交易过程中,实时检测读卡器状态;

[0029] 用户在使用卡进行自助业务操作时,读卡器中有卡,自助设备处于正常服务状态。当读卡器由于出现故障导致里面有卡不能退出或者吞卡的情况,也就是自助设备并不是在服务状态时,不是本方案考虑范围之内。

[0030] 按照现有技术,自助设备正在服务状态,读卡器中有卡,当读卡器处理卡口检测到卡或者异物时候,读卡器不会将处理卡口有卡或异物的事件发送给自助业务系统,对该事件并不做任何处理。因而,当用户在业务操作过程中,不法分子在读卡器处理卡口插上一张假卡,引诱用户交出业务操作权,自助设备在现有技术下不会告警用户,并不会采取安全措施保障用户帐户资金安全。

[0031] 优选的,检测到读卡器进卡口处是否有卡,可采用的检测手段是利用读卡器判卡进卡或判磁进卡的硬件提供的处理卡功能,读卡器可以把检测到进卡口处有卡的事件立即发送给自助业务系统。

[0032] 另外,检测到读卡器进卡口处是否有卡,还可采用的检测手段是读卡器异物检测功能,对现有技术的改进之处是在业务过程之中读卡器只要一检测到异物,立即将检测到异物事件发送给自助业务系统,而不是现有技术的在较长时间(如大于 5 分钟)才能检测到异物操作处理,现有技术只有在较长时间(如大于 5 分钟)检测到异物是为了防止插卡等临时性异物干扰,而安装在读卡器进卡口的异物检测装置的目的是发现读卡器进卡口是否存在有盗取卡信息的盗卡装置。

[0033] 步骤 S102:一旦检测到读卡器处理卡口处有卡,读卡器生成进卡口处有卡的事件,并将该事件实时发送给自助业务系统,以使所述自助业务系统提示告警信息,并暂停当前业务,进入用户身份验证流程;

[0034] 为有效防止不法分子在用户进行业务操作过程之中,在读卡器进卡口插一张卡以假乱真诱骗用户而获取业务操作权,在用户业务操作过程中一旦检测到读卡器进卡口有卡,读卡器会将该事件及时发送给自助业务系统处理,自助业务系统及时提醒用户注意防止卡被调包。

[0035] 所述的提示告警信息,包括用户当心卡调包等,可以采用语音提示告警信息方式,或者采用在屏幕上显示告警信息的方式。

[0036] 所述的自助业务系统暂停当前业务,进入用户身份验证流程,如果当前业务的操作结果并不会导致用户帐户资金或用户密码发生变化,如查询业务,可以在完成本次业务之后或者本次业务超时之后,才进入用户身份验证流程;对于本次业务的操作结果会导致用户帐户资金或用户密码,二者只要其一会发生变化,如改密业务或转账业务,则立即暂停当前业务,进入用户身份验证流程。

[0037] 步骤 S103:当用户在规定的时间内身份验证成功后,继续当前业务。

[0038] 需要说明的是,若用户身份验证不成功,自助业务系统终止当前业务,吞卡或者退卡结束本次业务操作。

[0039] 其中,所述的 用户身份验证,如果在一定时限内,用户没有输入密码,或者输入密

码三次出错,则终止本次业务,并作退卡或者吞卡处理。

[0040] 其中,所述的终止本次业务,对于取款业务已经扣帐成功但是还没有成功出钞的,在终止本次业务之前,应该发起取款冲正流程进行平账处理。对于存款业务还没有点钞完毕的,钞票做回收处理,钞票不再传送到出钞口。

[0041] 与方法实例对应的,本申请实施例提供的一种读卡器处理卡装置的结构示意图如图 2 所示,包括:

[0042] 第一检测模块 201,第二检测模块 202,判断分析模块 203,自助业务系统 204,告警提示模块 205,身份验证模块 206,其中

[0043] 第一检测模块 201 与第二检测模块 202 分别用于检测读卡器里面和进卡口是否有卡,并把检测结果传送给判断分析模块 203,当判断分析模块 203 同时发现接受到的第一检测模块 201 与第二检测模块 202 均检测到有卡,且自助业务系统正在进行业务处理时,判断分析模块 203 向自助业务系统 204 和告警提示模块 205 发送一告警信息,告警提示模块 205 向用户通过屏幕显示或者声音提示的方式传达告警信息,自助业务系统 204 以接收到告警信息,中止当前业务的进行,并调用用户身份验证模块 206,要求用户进行身份验证,用户通过身份验证模块 206 输入身份信息,身份验证模块 206 成功完成身份验证后,发送信息给自助业务系统 204,自助业务系统 204 继续当前业务,如果身份验证模块 206 在规定的时间内进行用户身份验证失败,自助业务系统 204 终止当前业务,最后进行退卡或者吞卡处理。

[0044] 所述的第二检测模块 202,可采用读卡器判卡进卡或判磁进卡的硬件提供的处理卡功能模块,也可采用读卡器异物检测功能模块。

[0045] 优选的,所述的身份验证模块 206,可采用用户再次输入帐户密码进行身份验证的功能模块。

[0046] 图 3 和图 4 是本发明实施例提供的一种读卡器异物检测装置处理卡方法,包括:

[0047] 现有的读卡器异物检测装置,是为了防止不法分子在读卡器上加装读卡器等装置非法获取用户卡信息而研发的产品。读卡器异物检测装置只有在相当长的一段时间(如半个小时,最好要大于一笔业务的时间)里一直检测到有异物存在,才会报警,判断出读卡器有异物遮挡,如果在较短的一段时间里一直检测到有异物存在,不会报警,如用户退卡,卡在取卡口,直到吞卡,有 2-3 分钟的取卡超时时间,这段时间读卡器异物检测装置肯定会检测到取卡口有异物存在,但实际上是正常情况的进出卡,是不能发送报警信息,向自助业务服务系统发送读卡器有异常的信号。

[0048] 本实施例,在用户进行业务过程中,当用户卡还在读卡器中,如果读卡器的异物检测装置检测到有异物,会进行警报提示,读卡器中的卡随后要进行取款和转账交易时,强制用户重新输入密码。这样,警报提示会提高用户警惕,震慑犯罪;随后的现金交易强制重新输入密码,会保护用户资金安全,即使用户上当,也不会造成损失。即只要读卡器中有卡,外界往异型嘴插入另一张卡,读卡器中的卡进行现金交易就需要重新输入密码了,即使卡掉包成功,用户资金安全仍然得到了保障。

[0049] 本实例的一种利用读卡器异物检测功能处理卡的方法,分为以下几个步骤:

[0050] 1)读卡器异物检测装置检测到异物,如果读卡器中有卡,转步骤 2);否则不做任何处理,流程结束

[0051] 2)如果正在进行业务为取款或转账业务,暂停本次业务处理,进入输入密码界面,

等待用户输入密码,用户在规定时间内输入密码正确,本次业务继续进行,流程结束;否则转步骤3)。

[0052] 3) 如果正在进行业务为非取款和非转账业务,本次业务继续进行,当用户在后续业务操作过程中,继续使用读卡器中的卡进行取款或转账业务时,要求用户重新输入密码,用户在规定时间内输入密码正确,业务继续进行,流程结束。

[0053] 较佳地,在业务过程中异物检测装置由没有检测到异物状态,切换到检测有异物状态,则本方案安全控制系统才起作用。

[0054] 本实例将读卡器异物检测装置工作状态分为两种:

[0055] 正常工作模式:该状态是指目前技术下的对读卡器装置上的异物进行检测工作状态,异物检测装置工作与这种状态下,一旦检测到读卡器有异物,并不会立即向监控系统和自助服务系统发送一信号,报告读卡器存在异物,只有在较长一段时间内,如持续检测到异物的时间积累超过 20 分钟,甚至更长,这时自助终端监控系统可以断定读卡器上加装了一个异物,一旦某个时候异物消失,那么这个时间积累就要清零,重新计数。从而把诸如以下正常情况检测到异物加以有效区分:用户进行业务操作时诸如插卡、处理卡、退卡和取卡导致的由于银行卡暂时经过读卡器进/出卡口,导致异物检测系统检测到异物。

[0056] 紧急工作模式:本方案新增加的一种工作状态,读卡器异物检测装置工作与该种状态下,只要检测到读卡器有异物,立即向自助服务系统发送一信号,报告读卡器存在异物,自助业务系统会立即中断现有正常业务的进行,进入紧急处理模式。

[0057] 读卡器异物检测装置处于该种工作状态的前提条件是读卡器中已经有一张银行卡正在进行业务处理,当用户正确输入密码后,读卡器异物检测装置开始启动该种工作状态,直到用户操作完业务退卡成功为止。

[0058] 本实例中读卡器异物检测装置的两种工作模式切换流程如下:

[0059] 1) 判断读卡器中是否有卡?

[0060] 2) 如有,则读卡器异物检测装置进入紧急工作状态,当异物检测装置一旦检测到有异物存在,立即中断现在正在进行的业务处理,自助业务系统切换到密码输入界面。只有当用户密码输入正确才会继续进行当前正在处理的业务,否则会中止业务进行,并吞卡。

[0061] 3) 如没有,则读卡器异物检测装置进入正常工作状态,只有当异物检测装置在较长时间(如 20 分钟以上)一直检测到有异物存在,才会暂停业务系统工作,并通知维护人员排除读卡器异物。

[0062] 本实例的一种读卡器异物检测切换控制方法流程如下:

[0063] 1) 自助设备在空闲时,没有业务操作期间,读卡器异物检测装置处于正常工作模式,在此模式下,只有当读卡器异物检测装置连续较长时间(如 20 分钟以上,可根据实际情况需要进行设置)一直检测到有异物遮挡,才会停止业务处理,并报警通知维护人员介入排除异物。

[0064] 连续较长时间一直检测到异物才会报警,而不是一检测到异物就马上报警,这是考虑用户正常的插卡,取卡等业务操作需要,这些时候读卡器也会检测到异物,但是是正常的。

[0065] 读卡器异物检测装置在工作模式下,其报警是通知维护人员,因为此种情况下的报警,是因为读卡器上可能被不法分子安装了盗取用户卡信息的盗卡装置而导致异物检测

装置报警,需要维护人员介入排除异物。

[0066] 2) 用户开始进行业务操作,插卡,读卡器处理卡,切换读卡器异物检测装置由正常工作模式进入紧急工作模式,该模式下,只要读卡器异物检测装置一检测到异物遮挡,就会立即报警,提醒用户注意,继续当前业务就需要用户在此输入密码。

[0067] 读卡器异物检测装置在紧急工作模式下,其报警并不通知维护人员,而是提醒正在进行业务操作的用户,这是因为此种情况并不认为是安装了盗取用户卡信息的盗卡装置而导致异物检测装置报警,而是可能有人干扰用户业务操作故意在读卡器处理卡口上插上诸如假卡等异物来诱骗用户。

[0068] 3) 业务系统在处理用户业务过程中,一旦接收到有异物信号,马上响应中断,中断目前业务的继续进行,切换到密码输入界面,等待用户输入密码。

[0069] 读卡器异物检测装置在紧急工作模式下,如果要继续进行当前的业务,要求用户必须重新输入密码,这样可以防止用户被人诱骗离开了自助设备,后续的人也无法继续用该用户的卡进行业务操作,保证了该用户的资金安全。

[0070] 4) 如果密码输入错误三次以上或者密码输入超时,中止现有业务的进行,吞卡;如果用户正确输入密码则继续当前业务的进行。

[0071] 5) 用户完成业务操作,读卡器退卡成功,切换读卡器异物检测装置由紧急工作模式进入正常工作模式,流程结束。

[0072] 本领域普通技术人员可以理解:附图只是一个实施例的示意图,附图中的单元或流程并不一定是实施本发明所必须的。

[0073] 在本申请所提供的几个实施例中,应该理解到,所揭露的系统,设备和方法,可以通过其它的方式实现。例如,以上所描述的设备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,设备或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0074] 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。

[0075] 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,也可以采用硬件加软件功能单元的形式实现。

[0076] 上述以软件功能单元的形式实现的集成的单元,可以存储在一个计算机可读存储介质中。上述软件功能单元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(可以是个人计算机,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部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(Read-Only Memory,简称ROM)、随机存取存储器(Random Access Memory,简称RAM)、磁碟或者光盘等各种可以存储程序代码的介质。最后应说明的是:以上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精神和范围。

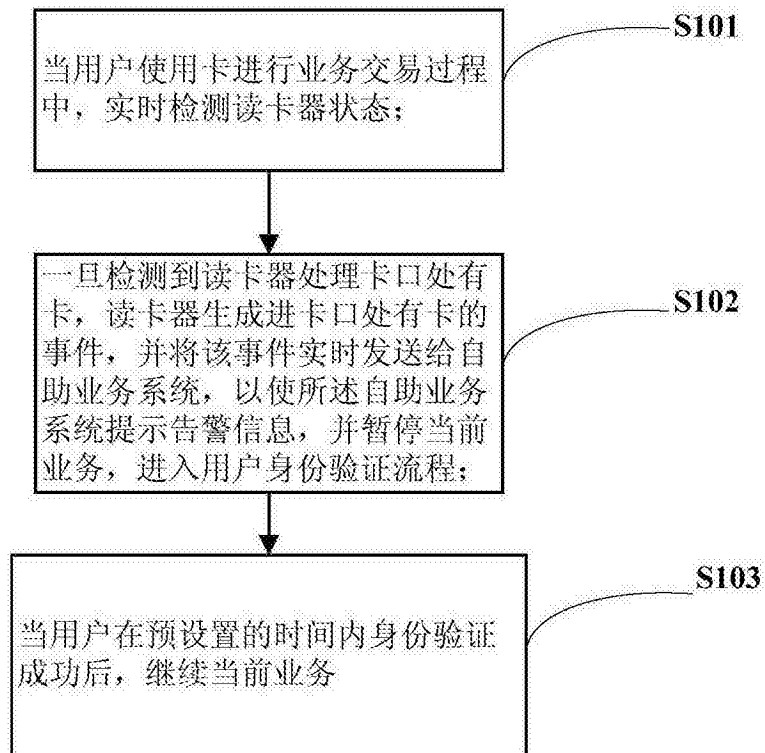


图 1

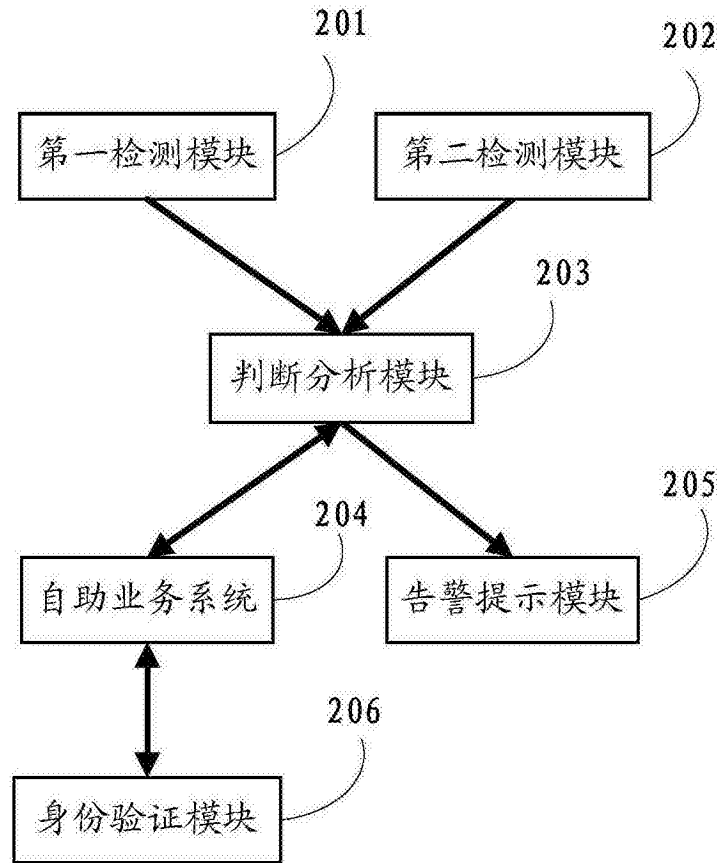


图 2

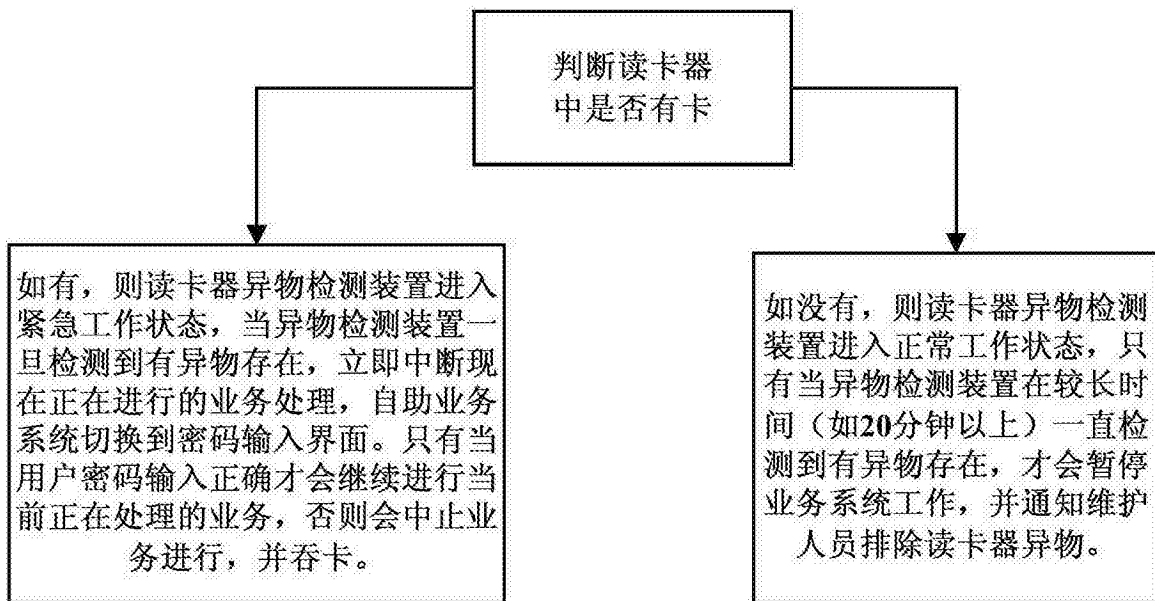


图 3

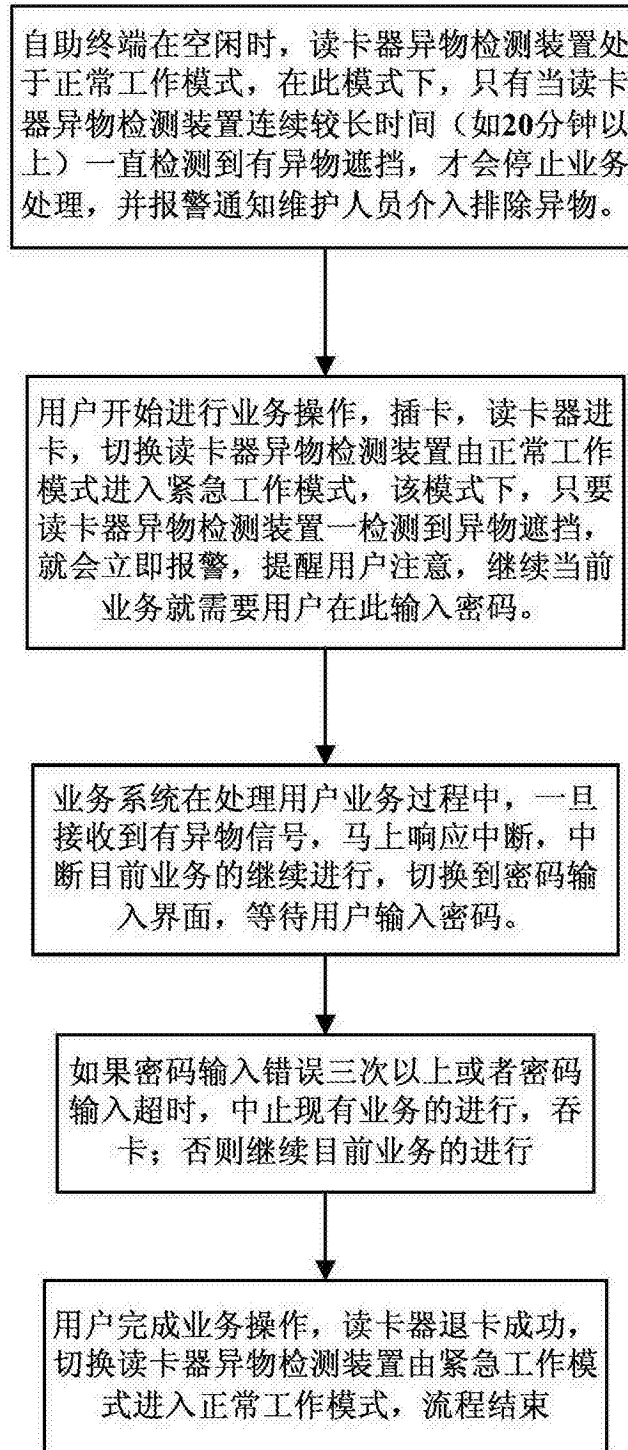


图 4