(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 110312257 A
(43)申请公布日 2019.10.08

(21)申请号 201910512117.0

(22)申请日 2019.06.13

(71)申请人 信利光电股份有限公司
地址 516600 广东省汕尾市区工业大道信利工业城一区第15栋

(72)发明人 吴光斯

(74)专利代理机构 广州粤高专利商标代理有限公司 44102
代理人 李健威

(51)Int.Cl.
H04W 12/12(2009.01)

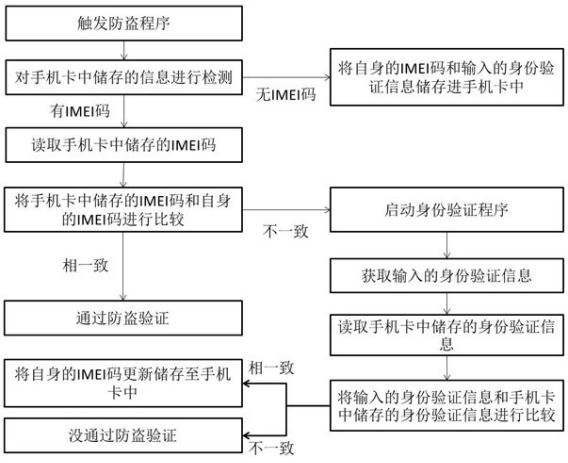
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种手机卡防盗方法、装置及可读存储介质

(57)摘要

本发明公开了一种手机卡防盗方法，包括：触发防盗程序；对手机卡中储存的信息进行检测，若手机卡中储存有IMEI码，则读取手机卡中储存的IMEI码；将手机卡中储存的IMEI码和自身的IMEI码进行比较，若手机卡中储存的IMEI码和自身的IMEI码相一致，则通过防盗验证。该手机卡防盗方法针对手机卡进行防盗处理，可防止通过更换移动通讯设备的方式，使用丢失或被盗的手机卡。本发明公开了一种移动通讯设备和可读存储介质。



CN 110312257 A

1.一种手机卡防盗方法,其特征在于,包括:

触发防盗程序;

对手机卡中储存的信息进行检测,若手机卡中储存有IMEI码,则读取手机卡中储存的IMEI码;

将手机卡中储存的IMEI码和自身的IMEI码进行比较,若手机卡中储存的IMEI码和自身的IMEI码相一致,则通过防盗验证。

2.根据权利要求1的手机卡防盗方法,其特征在于,在对手机卡中储存的信息进行检测时,若手机卡中未储存有IMEI码,则将自身的IMEI码储存进手机卡中。

3.根据权利要求2所述的手机卡防盗方法,其特征在于,在首次将自身的IMEI码储存进手机卡中时,还同时将输入的身份验证信息储存进手机卡中。

4.根据权利要求1的手机卡防盗方法,其特征在于,若手机卡中储存的IMEI码和自身的IMEI码不一致,则启动身份验证程序,以进行身份验证。

5.根据权利要求4的手机卡防盗方法,其特征在于,在进行身份验证时,包括:

获取输入的身份验证信息;

对手机卡中储存的信息进行检测,以读取手机卡中储存的身份验证信息;

将输入的身份验证信息和手机卡中储存的身份验证信息进行比较,若输入的身份验证信息和手机卡中储存的身份验证信息相一致,则将自身的IMEI码更新储存至手机卡中。

6.根据权利要求4所述的手机卡防盗方法,其特征在于,身份验证信息包括密码信息、指纹信息、人脸信息和声纹信息中的至少一项。

7.根据权利要求4所述的手机卡防盗方法,其特征在于,在比较输入的身份验证信息和手机卡中储存的身份验证信息时,若输入的身份验证信息和手机卡中储存的身份验证信息不一致,则没通过防盗验证。

8.根据权利要求1所述的手机卡防盗方法,其特征在于,手机卡内设有可读写的微型存储芯片,微型存储芯片用于储存进行防盗验证的IMEI码和/或进行身份验证的身份验证信息。

9.一种移动通讯设备,包括处理器和与处理器连接的存储器,存储器内储存有供处理器执行的计算机程序;其特征在于,处理器执行该计算机程序时,进行权利要求1-8中任一的手机卡防盗方法。

10.一种可读存储介质,存储有供处理器执行的计算机程序,其特征在于,处理器执行该计算机程序时,进行权利要求1-8中任一的手机卡防盗方法。

一种手机卡防盗方法、装置及可读存储介质

技术领域

[0001] 本发明涉及防盗技术，尤其涉及一种手机卡防盗方法、装置及可读存储介质。

背景技术

[0002] 近几年，随着科技的迅速发展，手机支付逐渐成为日常生活的标配，而手机支付作为当今社会较为流行的支付方式，据统计，2017年中国非金融支付机构综合支付业务的交易规模达到了35.92万亿元人民币，接近36万亿元，环比增长10.2％。而相比于去年同期的刚过20万亿元，同比增幅高达72％。其中，支付宝以39.03％的份额稳坐第一，交易额已经突破14万亿元；腾讯金融(包括微信支付和QQ钱包)则以27.01％尾随其后，交易额9.7万亿元；银联商务以16.98％排第三，三家合计占到了83.02％的市场份额。

[0003] 我们在享受手机支付快捷、便利的同时，也在逐渐提高了安全意识。比如我们在支付软件中设置了复杂的登录密码，也在支付软件的支付界面中设置了相应的支付密码。甚至于，手机本身也具有各式各样的防盗程序，但是现有的防盗方案基本上都是针对手机进行防盗处理的，而没有专门针对手机卡进行防盗处理的，一旦手机出现丢失或者盗窃的情况，盗窃者只需将手机卡更换到新手机中即可开机正常使用，而现有的支付账号和社交账号等，基本上都和手机号进行了绑定，可以通过手机号来登录并修改密码，存在很大安全隐患。

发明内容

[0004] 为了解决上述现有技术的不足，本发明提供一种手机卡防盗方法、移动通讯设备及可读存储介质，针对手机卡进行防盗处理，可防止通过更换移动通讯设备的方式，使用丢失或被盗的手机卡。

[0005] 本发明所要解决的技术问题通过以下技术方案予以实现：

一种手机卡防盗方法，包括：

触发防盗程序；

对手机卡中储存的信息进行检测，若手机卡中储存有IMEI码，则读取手机卡中储存的IMEI码；

将手机卡中储存的IMEI码和自身的IMEI码进行比较，若手机卡中储存的IMEI码和自身的IMEI码相一致，则通过防盗验证。

[0006] 进一步地，在对手机卡中储存的信息进行检测时，若手机卡中未储存有IMEI码，则将自身的IMEI码储存进手机卡中。

[0007] 进一步地，在首次将自身的IMEI码储存进手机卡中时，还同时将输入的身份验证信息储存进手机卡中。

[0008] 进一步地，若手机卡中储存的IMEI码和自身的IMEI码不一致，则启动身份验证程序，以进行身份验证。

[0009] 进一步地，在进行身份验证时，包括：

获取输入的身份验证信息；

对手机卡中储存的信息进行检测，以读取手机卡中储存的身份验证信息；

将输入的身份验证信息和手机卡中储存的身份验证信息进行比较，若输入的身份验证信息和手机卡中储存的身份验证信息相一致，则将自身的IMEI码更新储存至手机卡中。

[0010] 进一步地，身份验证信息包括密码信息、指纹信息、人脸信息和声纹信息中的至少一项。

[0011] 进一步地，在比较输入的身份验证信息和手机卡中储存的身份验证信息时，若输入的身份验证信息和手机卡中储存的身份验证信息不一致，则没通过防盗验证。

[0012] 进一步地，手机卡内设有可读写的微型存储芯片，微型存储芯片用于储存进行防盗验证的IMEI码和/或进行身份验证的身份验证信息。

[0013] 一种移动通讯设备，包括处理器和与处理器连接的存储器，存储器内储存有供处理器执行的计算机程序；处理器执行该计算机程序时，进行上述的手机卡防盗方法。

[0014] 一种可读存储介质，存储有供处理器执行的计算机程序，处理器执行该计算机程序时，进行上述的手机卡防盗方法。

[0015] 本发明具有如下有益效果：该手机卡防盗方法针对手机卡进行防盗处理，在移动通讯设备丢失或被盗后，即使将手机卡更换到新移动通讯设备中，因进行防盗验证的IMEI码和进行身份验证的身份验证信息均储存在手机卡中，只要没通过防盗验证就无法正常使用。

附图说明

[0016] 图1为本发明提供的手机卡防盗方法的步骤框图。

具体实施方式

[0017] 下面结合附图和实施例对本发明进行详细的说明。

[0018] 实施例一

如图1所示，一种手机卡防盗方法，应用于移动通讯设备中，包括：

S101：触发防盗程序。

[0019] 在该步骤S101中，移动通讯设备可以在开机程序中触发防盗程序，或者在第三方软件的登录界面中触发防盗程序，或者在支付软件的支付界面中触发防盗程序，视具体需求而定。

[0020] S102：对手机卡中储存的信息进行检测，若手机卡中储存有IMEI码，则读取手机卡中储存的IMEI码。

[0021] 手机卡内设有可读写的微型存储芯片，微型存储芯片用于储存进行防盗验证的IMEI码和进行身份验证的身份验证信息，通过手机卡里的金属触点与移动通讯设备通讯连接进行数据的读取和写入。

[0022] 移动通讯设备通过手机卡里的金属触点，将储存在手机卡的微型存储芯片里的IMEI码读取出来。

[0023] 在该步骤S102中，在对手机卡中储存的信息进行检测时，若手机卡中未储存有IMEI码，则将自身的IMEI码储存进手机卡中。

[0024] 并且，在首次将自身的IMEI码储存进手机卡中时，还同时将输入的身份验证信息储存进手机卡中。

[0025] 移动通讯设备通过读取自身的硬件信息，以获取自身的IMEI码，以及通过自身的触摸屏、指纹装置、摄像装置、声纹装置等获取用户输入的身份验证信息，然后通过手机卡里的金属触点，将自身的IMEI码和输入的身份验证信息写入到手机卡内的微型存储芯片里。

[0026] S103：将手机卡中储存的IMEI码和自身的IMEI码进行比较，若手机卡中储存的IMEI码和自身的IMEI码相一致，则通过防盗验证；

通过防盗验证后，移动通讯设备就可以正常使用手机卡，比如正常开机、收发短信、拨打接听电话、接入移动网络、登录第三方软件或移动支付等。

[0027] 在该步骤S103中，若手机卡中储存的IMEI码和自身的IMEI码不一致，则启动身份验证程序，以进行身份验证。

[0028] 身份验证程序用于对用户的身份进行识别认证，避免误将用户正常更换移动通讯设备的行为认定为移动通讯设备被盗。

[0029] 该手机卡防盗方法在进行身份验证时，包括：

S104：获取输入的身份验证信息；

移动通讯设备通过自身的触摸屏、指纹装置、摄像装置、声纹装置等获取用户输入的身份验证信息，其中，身份验证信息包括密码信息、指纹信息、人脸信息和声纹信息中的至少一项。

[0030] S105：对手机卡中储存的信息进行检测，以读取手机卡中储存的身份验证信息；

移动通讯设备通过手机卡里的金属触点，将储存在手机卡的微型存储芯片里的身份验证信息读取出来。

[0031] S106：将输入的身份验证信息和手机卡中储存的身份验证信息进行比较，若输入的身份验证信息和手机卡中储存的身份验证信息相一致，则将自身的IMEI码更新储存至手机卡中。

[0032] 在该步骤S106中，在比较输入的身份验证信息和手机卡中储存的身份验证信息时，若输入的身份验证信息和手机卡中储存的身份验证信息不一致，则没通过防盗验证。

[0033] 没通过防盗验证的话，移动通讯设备就无法正常使用手机卡，比如无法开机、无法收发短信、无法拨打接听电话、无法接入移动网络、无法登录第三方软件或无法移动支付等。

[0034] 该手机卡防盗方法针对手机卡进行防盗处理，在移动通讯设备丢失或被盗后，即使将手机卡更换到新移动通讯设备中，因进行防盗验证的IMEI码和进行身份验证的身份验证信息均储存在手机卡中，只要没通过防盗验证就无法正常使用。

[0035] 实施例二

一种移动通讯设备，包括处理器和与处理器连接的存储器，存储器内储存有供处理器执行的计算机程序；处理器执行该计算机程序时，进行实施例一的手机卡防盗方法。

[0036] 实施例三

一种可读存储介质，存储有供处理器执行的计算机程序，处理器执行该计算机程序时，进行实施例一的手机卡防盗方法。

[0037] 以上实施例仅表达了本发明的实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利范围的限制，但凡采用等同替换或等效变换的形式所获得的技术方案，均应落在本发明的保护范围之内。

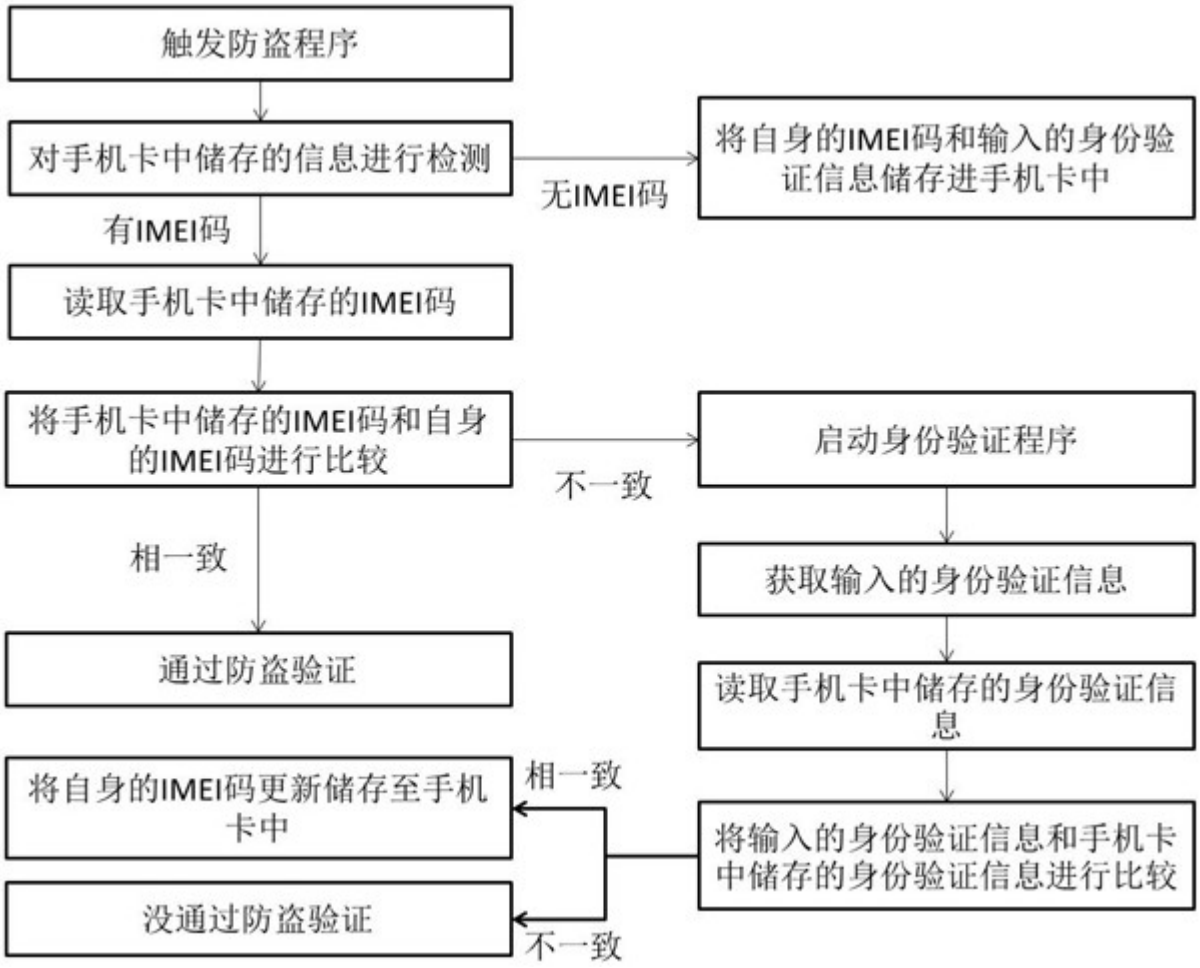

触发防盗程序
对手机卡中储存的信息进行检测
无IMEI码
将自身的IMEI码和输入的身份验证信息储存进手机卡中
有IMEI码
读取手机卡中储存的IMEI码
将手机卡中储存的IMEI码和自身的IMEI码进行比较
不一致
启动身份验证程序
相一致
获取输入的身份验证信息
通过防盗验证
读取手机卡中储存的身份验证信息
将自身的IMEI码更新储存至手机卡中
相一致
将输入的身份验证信息和手机卡中储存的身份验证信息进行比较
没通过防盗验证
不一致

图1