(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 105530641 A
(43)申请公布日 2016.04.27

(21)申请号 201410525026.8

(22)申请日 2014.09.30

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 杨飞

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 张建秀 李丹

(51)Int.Cl.
H04W 12/06(2009.01)

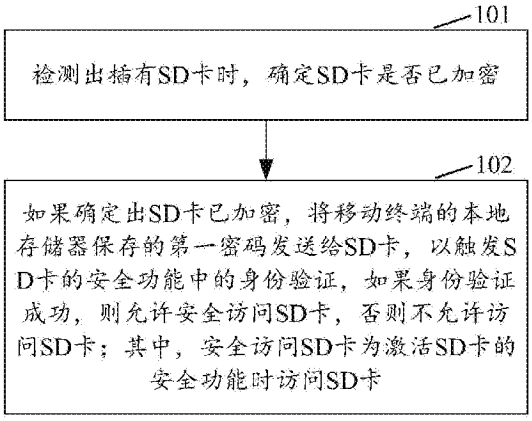
权利要求书2页 说明书7页 附图1页

(54)发明名称

一种移动终端中实现SD卡安全管理的方法和装置

(57)摘要

本发明公开了一种移动终端中实现安全数字存储卡(SD卡)安全管理的方法和装置,包括检测出插有SD卡时,确定SD卡是否已加密;如果确定出SD卡已加密,将移动终端的本地存储器保存的第一密码发送给SD卡,以触发SD卡的安全功能中的身份验证,如果身份验证成功,则允许安全访问SD卡,否则不允许访问SD卡;其中,安全访问SD卡为激活SD卡的安全功能时访问SD卡。通过本发明提供的技术方案,充分利用了SD卡的安全功能,有效提高了SD卡中数据的安全性。



CN 105530641 A

1. 一种移动终端中实现安全数字存储卡 SD 卡安全管理的方法，其特征在于，包括：

检测出插有 SD 卡时，确定 SD 卡是否已加密；

如果确定出 SD 卡已加密，将移动终端的本地存储器保存的第一密码发送给 SD 卡，以触发 SD 卡的安全功能中的身份验证，如果身份验证成功，则允许安全访问 SD 卡，否则不允许访问 SD 卡；其中，安全访问 SD 卡为激活 SD 卡的安全功能时访问 SD 卡。

2. 根据权利要求 1 所述的方法，其特征在于，所述第一密码是根据移动设备国际身份码 IMEI 码获取、保存在所述本地存储器中。

3. 根据权利要求 1 所述的方法，其特征在于，所述确定 SD 卡是否已加密之后，该方法还包括：如果确定出所述 SD 卡未加密，根据预先设置的加密策略确定是否需要加密 SD 卡；

其中，加密策略包括：

如果用于配置是否加密所述 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡；或者，

如果用于配置所述移动终端是否启用安全功能的安全配置项为选中，且用于配置是否加密所述 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡。

4. 根据权利要求 3 所述的方法，其特征在于，所述安全配置项为选中包括：用于配置是否启用图形密码的图案密码配置项、用于配置是否启用数字密码的数字密码配置项、以及用于配置是否启用个人识别密码 PIN 的 PIN 配置项中的至少一个配置项为选中。

5. 根据权利要求 3 所述的方法，其特征在于，所述根据预先设置的加密策略确定是否需要加密 SD 卡之后，该方法还包括：如果确定出需要加密 SD 卡，将所述第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

6. 根据权利要求 3 所述的方法，其特征在于，所述根据预先设置的加密策略确定是否需要加密 SD 卡之后，该方法还包括：如果确定出不需要加密 SD 卡，允许普通访问 SD 卡；其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

7. 根据权利要求 6 所述的方法，其特征在于，所述允许普通访问 SD 卡之后，该方法还包括：如果用于配置是否加密所述 SD 卡的加密 SD 卡配置项改变为选中，则确定出需要加密 SD 卡，将所述第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

8. 根据权利要求 1 或 5 或 7 所述的方法，其特征在于，所述允许安全访问 SD 卡之后，该方法还包括：如果用于配置是否加密所述 SD 卡的加密 SD 卡配置项改变为未选中，则删除所述 SD 卡中保存的第二密码，以关闭所述安全功能，并允许普通访问 SD 卡；其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

9. 一种移动终端中实现安全数字存储卡 SD 卡安全管理的装置，其特征在于，包括安全检测单元和安全访问单元，其中，

安全检测单元，用于检测出插有 SD 卡时，确定 SD 卡是否已加密，当确定出 SD 卡已加密时，发送第一消息；

安全访问单元，用于接收到来自安全检测单元的第一消息时，将移动终端的本地存储器保存的第一密码发送给 SD 卡，以触发 SD 卡的安全功能中的身份验证，如果身份验证成功，则允许安全访问 SD 卡，否则不允许访问 SD 卡；其中，安全访问 SD 卡为激活 SD 卡的安全功能时访问 SD 卡。

10. 根据权利要求 9 所述的装置，其特征在于，所述第一密码是根据移动设备国际身份

码 IMEI 码获取、保存在所述本地存储器中。

11. 根据权利要求 9 所述的装置，其特征在于，所述安全检测单元还用于：当确定出 SD 卡未加密时，根据预先设置的加密策略确定是否需要加密 SD 卡，当确定出需要加密 SD 卡时，发送第二消息，当确定出不需要加密 SD 卡时，发送第三消息；

其中，加密策略包括：

如果用于配置是否加密所述 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡；或者，

如果用于配置所述移动终端是否启用安全功能的安全配置项为选中，且用于配置是否加密所述 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡。

12. 根据权利要求 11 所述的装置，其特征在于，所述安全配置项为选中包括：用于配置是否启用图形密码的图案密码配置项、用于配置是否启用数字密码的数字密码配置项、以及用于配置是否启用个人识别密码 PIN 的 PIN 配置项中的至少一个配置项为选中。

13. 根据权利要求 11 所述的装置，其特征在于，所述安全访问单元还用于：当接收到来自所述安全检测单元的第二消息时，将所述第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

14. 根据权利要求 11 所述的装置，其特征在于，所述安全访问单元还用于：当接收到来自所述安全检测单元的第三消息时，允许普通访问 SD 卡；其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

15. 根据权利要求 14 所述的装置，其特征在于，所述检测单元还用于：当允许普通访问 SD 卡，且检测出用于配置是否加密所述 SD 卡的加密 SD 卡配置项改变为选中时，发送所述第二消息；

所述安全访问单元还用于：当接收到来自所述安全检测单元的第二消息时，将所述第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

16. 根据权利要求 9 或 13 或 15 所述的装置，其特征在于，所述检测单元还用于：当允许安全访问 SD 卡，且用于配置是否加密所述 SD 卡的加密 SD 卡配置项改变为未选中时，发送第四消息；

所述安全访问单元还用于，当接收到来自所述安全检测单元的第四消息时，删除所述 SD 卡中保存的第二密码，以关闭所述安全功能，并允许普通访问 SD 卡；其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

一种移动终端中实现SD卡安全管理的方法和装置

技术领域

[0001] 本发明涉及移动终端应用技术，尤指一种移动终端中实现安全数字存储卡（SD卡）安全管理的方法和装置。

背景技术

[0002] 随着移动互联网技术的迅猛发展，移动终端如智能手机和平板电脑得到了高速发展和广泛应用。人们逐渐习惯了使用移动终端完成很多重要的操作，例如移动终端支付等。这样，需要在移动终端中保存越来越多的重要用户信息，例如个人支付账号、邮箱、密码、文件和相片等。因此人们对移动终端的安全性的要求也越来越高。

[0003] 目前，在例如安卓操作系统（ANDROID）、苹果手机操作系统（IOS）和微软视窗手机操作系统（WINDOWS PHONE）等主流操作系统中，均提供了多种可选择的用于增强移动终端安全性的安全配置项，例如图案密码配置项、数字密码配置项和个人识别密码PIN配置等。通过选中这些配置项中的至少一个配置项，可以较好地增加移动终端的安全性。然而，上述安全配置项只能对移动终端中的内置存储器起到较好的安全性保护的作用，对于移动终端中外置的安全数字存储卡（SD，Secure Digital Memory Card）没有起到安全性保护的作用。一旦手机丢失或者SD卡被盗取并通过其他设备读取数据，SD卡中保存的重要用户数据就会泄露。

[0004] 为此，有些移动终端的用户通过使用加密软件，将要保存到SD卡中的重要用户数据加密，然后再保存到SD卡中。这种方法，虽然可以提高SD卡中的数据的安全性，但是仍然存在几个方面缺陷。第一，一旦SD卡被盗取并通过其他设备读取到加密后的密文数据，有可能破解密文数据得到解密后的数据即明文数据；第二，即使在上述情况下无法破解密文数据，也可以以格式化或全部删除数据的方式恶意破坏密文数据；第三，如果用户因长期不使用SD卡中密文数据而忘记密码，则其自身也无法从密文数据中提读取明文数据。上述缺陷，降低了这种方法保护SD卡中数据的安全性，从而阻碍了其得到广泛的应用。

发明内容

[0005] 为了解决上述技术问题，本发明提供了一种移动终端中实现SD卡安全管理的方法和装置，充分利用SD卡的安全功能，能够有效提高SD卡中数据的安全性。

[0006] 为了达到本发明目的，本发明公开了一种移动终端中实现安全数字存储卡SD卡安全管理的方法，包括：

[0007] 检测出插有SD卡时，确定SD卡是否已加密；

[0008] 如果确定出SD卡已加密，将移动终端的本地存储器保存的第一密码发送给SD卡，以触发SD卡的安全功能中的身份验证，如果身份验证成功，则允许安全访问SD卡，否则不允许访问SD卡；其中，安全访问SD卡为激活SD卡的安全功能时访问SD卡。

[0009] 其中，所述第一密码是根据移动设备国际身份码IMEI码获取、保存在所述本地存储器中。

[0010] 进一步地，所述确定 SD 卡是否已加密之后，该方法还包括：如果确定出所述 SD 卡未加密，根据预先设置的加密策略确定是否需要加密 SD 卡；

[0011] 其中，加密策略包括：

[0012] 如果用于配置是否加密所述 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡；或者，

[0013] 如果用于配置所述移动终端是否启用安全功能的安全配置项为选中，且用于配置是否加密所述 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡。

[0014] 其中，所述安全配置项为选中包括：用于配置是否启用图形密码的图案密码配置项、用于配置是否启用数字密码的数字密码配置项、以及用于配置是否启用个人识别密码 PIN 的 PIN 配置项中的至少一个配置项为选中。

[0015] 进一步地，所述根据预先设置的加密策略确定是否需要加密 SD 卡之后，该方法还包括：如果确定出需要加密 SD 卡，将所述第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

[0016] 进一步地，所述根据预先设置的加密策略确定是否需要加密 SD 卡之后，该方法还包括：如果确定出不需要加密 SD 卡，允许普通访问 SD 卡；其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

[0017] 进一步地，所述允许普通访问 SD 卡之后，该方法还包括：如果用于配置是否加密所述 SD 卡的加密 SD 卡配置项改变为选中，则确定出需要加密 SD 卡，将所述第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

[0018] 进一步地，所述允许安全访问 SD 卡之后，该方法还包括：如果用于配置是否加密所述 SD 卡的加密 SD 卡配置项改变为未选中，则删除所述 SD 卡中保存的第二密码，以关闭所述安全功能，并允许普通访问 SD 卡；其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

[0019] 本发明还包括了一种移动终端中实现安全数字存储卡 SD 卡安全管理的装置，包括安全检测单元和安全访问单元，其中，

[0020] 安全检测单元，用于检测出插有 SD 卡时，确定 SD 卡是否已加密，当确定出 SD 卡已加密时，发送第一消息；

[0021] 安全访问单元，用于接收到来自安全检测单元的第一消息时，将移动终端的本地存储器保存的第一密码发送给 SD 卡，以触发 SD 卡的安全功能中的身份验证，如果身份验证成功，则允许安全访问 SD 卡，否则不允许访问 SD 卡；其中，安全访问 SD 卡为激活 SD 卡的安全功能时访问 SD 卡。

[0022] 其中，所述第一密码是根据移动设备国际身份码 IMEI 码获取、保存在所述本地存储器中。

[0023] 进一步地，所述安全检测单元还用于：当确定出 SD 卡未加密时，根据预先设置的加密策略确定是否需要加密 SD 卡，当确定出需要加密 SD 卡时，发送第二消息，当确定出不需要加密 SD 卡时，发送第三消息；

[0024] 其中，加密策略包括：

[0025] 如果用于配置是否加密所述 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡；或者，

[0026] 如果用于配置所述移动终端是否启用安全功能的安全配置项为选中，且用于配置是否加密所述 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡。

[0027] 其中，所述安全配置项为选中包括：用于配置是否启用图形密码的图案密码配置项、用于配置是否启用数字密码的数字密码配置项、以及用于配置是否启用个人识别密码 PIN 的 PIN 配置项中的至少一个配置项为选中。

[0028] 进一步地，所述安全访问单元还用于：当接收到来自所述安全检测单元的第二消息时，将所述第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

[0029] 进一步地，所述安全访问单元还用于：当接收到来自所述安全检测单元的第三消息时，允许普通访问 SD 卡；其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

[0030] 进一步地，所述检测单元还用于：当允许普通访问 SD 卡，且检测出用于配置是否加密所述 SD 卡的加密 SD 卡配置项改变为选中时，发送所述第二消息；

[0031] 相应地，所述安全访问单元还用于：当接收到来自所述安全检测单元的第二消息时，将所述第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

[0032] 进一步地，所述检测单元还用于：当允许安全访问 SD 卡，且用于配置是否加密所述 SD 卡的加密 SD 卡配置项改变为未选中时，发送第四消息；

[0033] 相应地，所述安全访问单元还用于，当接收到来自所述安全检测单元的第四消息时，删除所述 SD 卡中保存的第二密码，以关闭所述安全功能，并允许普通访问 SD 卡；其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

[0034] 与现有技术相比，本发明技术方案包括：检测出插有 SD 卡时，确定 SD 卡是否已加密；如果确定出 SD 卡已加密，将移动终端的本地存储器保存的第一密码发送给 SD 卡，以触发 SD 卡的安全功能中的身份验证，如果身份验证成功，则允许安全访问 SD 卡，否则不允许访问 SD 卡；其中，安全访问 SD 卡为激活 SD 卡的安全功能时访问 SD 卡。通过本发明技术方案，一方面，当出现已加密的 SD 卡被盗取的情况时，由于盗取者无法获取第一密码并通过 SD 卡的安全功能中的身份验证，这样有效避免了通过其他设备读取 SD 卡中数据，有效降低了 SD 卡中数据破解的可能性；另一方面，当出现上述情况时，已加密的 SD 卡的安全功能保证了除非以物理方式破坏 SD 卡，不能以格式化或全部删除数据的方式恶意破坏 SD 卡中数据，进一步降低了恶意破坏 SD 卡中数据的可能性。从上述两方面的有益效果，不难看出本发明技术方案有效提高了 SD 卡中数据的安全性，较好提高了移动终端的安全功能的用户体验。

[0035] 另外，由于本发明技术方案是通过 IMEI 码经过预先设置的加密算法计算用于激活 SD 卡的安全功能的第一密码和将第一密码保存为用于加密 SD 卡的第二密码，因此避免了用户通过加密软件加密数据时忘记加密密码造成加密后的数据的不可解密和使用的可能性，增加了本发明技术方案的易用性。

[0036] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0037] 附图用来提供对本发明技术方案的进一步理解，并且构成说明书的一部分，与本申请的实施例一起用于解释本发明的技术方案，并不构成对本发明技术方案的限制。

[0038] 图 1 为本发明移动终端中实现 SD 卡安全管理的方法的流程图；

[0039] 图 2 为本发明移动终端中实现 SD 卡安全管理的装置的组成结构示意图。

具体实施方式

[0040] 为使本发明的目的、技术方案和优点更加清楚明白，下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0041] 在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行。并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0042] 图 1 为本发明移动终端中实现 SD 卡安全管理的方法的流程图，如图 1 所示，包括：

[0043] 步骤 101：检测出插有 SD 卡时，确定 SD 卡是否已加密。

[0044] 其中，检测出插有 SD 卡可以包括移动终端启动时检测出插有 SD 卡，或者检测出插入 SD 卡。检测测移动终端中是否插有 SD 卡、以及移动终端中是否插入 SD 卡的具体实现，为本领域技术人员的公知技术手段，此处不再赘述。

[0045] 本步骤中确定 SD 卡是否为已加密或未加密的具体实现，属于本领域技术人员的惯用技术手段，此处不再赘述。

[0046] 步骤 102：如果确定出 SD 卡已加密，将移动终端的本地存储器保存的第一密码发送给 SD 卡，以触发 SD 卡的安全功能中的身份验证，如果身份验证成功，则允许安全访问 SD 卡，否则不允许访问 SD 卡。

[0047] 其中，安全访问 SD 卡为激活 SD 卡的安全功能时访问 SD 卡。

[0048] 本步骤中，将移动终端的本地存储器保存的第一密码发送给 SD 卡，以触发 SD 卡的安全功能中的身份验证可以包括：本步骤通过请求身份验证相应的第一安全命令向 SD 卡发送第一密码，其中，第一安全命令中包括第一密码；第一安全命令触发 SD 卡比较第一密码和第二密码是否一致，SD 卡通过响应身份验证相应的第二安全命令返回是否一致的身份验证结果；第二安全命令触发本步骤确定是否身份验证成功。

[0049] 本步骤中，如果确定出身份验证失败，则不允许访问 SD 卡，同时还可以以人机交互的方式如在移动终端的显示屏上以提示框的方式提示：SD 卡加密不能访问。

[0050] 本步骤中第一密码是根据移动设备国际身份码（IMEI 码）获取、保存在本地存储器中。

[0051] 可以在步骤 101 之前根据 IMEI 码经过预先设置的密码算法，计算第一密码，并将第一密码保存在本地存储器中。其中，密码算法的输入为 IMEI 码，输出为第一密码。通过密码算法保证 IMEI 码与第一密码一一对应。本领域技术人员可以通过多种方法设计密码算法，例如，多种数学运算结合的密码算法。

[0052] 进一步地，

[0053] 步骤 101 中确定 SD 是否已加密之后，本发明方法还可以包括：确定出 SD 卡未加

密，根据预先设置的加密策略确定是否需要加密 SD 卡。

[0054] 在一个实施例中，本步骤中的加密策略可以包括：

[0055] 如果用于配置是否加密 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡。

[0056] 在另一个实施例中，本步骤中的加密策略可以包括：

[0057] 如果用于配置移动终端是否启用安全功能的安全配置项为选中，且加密 SD 卡配置项为选中，则需要加密 SD 卡。

[0058] 其中，移动终端的安全配置项为选中包括：用于配置是否启用图形密码的图案密码配置项、用于配置是否启用数字密码的数字密码配置项、以及用于配置是否启用个人识别密码 (PIN) 的 PIN 配置项中的至少一个配置项为选中。本领域技术人员应该清楚的是，在移动终端的某些操作系统中，可以支持同时选中上述三个配置项中的两项或者三项。

[0059] 需要说明的是，在上面的实施例中，当移动终端的安全配置项为未选中时，加密 SD 卡配置项可以设置为灰色，也就是说，此时 SD 卡配置项不可选中。

[0060] 进一步地，

[0061] 根据预先设置的加密策略确定是否需要加密 SD 卡之后，本发明方法还可以包括：如果确定出需要加密 SD 卡，将第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

[0062] 具体来讲，向 SD 卡发送与激活安全功能相应的第三安全命令，触发 SD 卡将第一密码保存为 SD 卡中的第二密码，从而触发 SD 卡激活安全功能，并允许安全访问 SD 卡；其中，第三安全命令中包括第一密码。

[0063] 需要说明的是，当 SD 卡的安全功能激活，或者身份验证成功之后，对于写入的访问请求，SD 卡会基于第二密码对接收到的数据进行加密并保存下来，对于读取的访问请求，SD 卡会基于第二密码对要读出的数据进行解密并发送出去。其中，SD 卡的安全功能的更详细内容可以参考 SD 卡协议，此处不再赘述。

[0064] 通过上述说明不难看出，当通过本步骤激活 SD 卡的安全功能时，SD 中保存的第二密码与 SD 卡插入的移动终端的 IMEI 码一一对应，由于 IMEI 码与移动终端一一对应，因此通过本步骤将移动终端和插入其中的 SD 卡绑定。

[0065] 进一步地，

[0066] 根据预先设置的加密策略确定是否需要加密 SD 卡之后，本发明方法还可以包括：如果确定出不需要加密 SD 卡，允许普通访问 SD 卡。其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

[0067] 相应地，

[0068] 允许普通访问 SD 卡之后，该方法还可以包括：

[0069] 如果用于配置是否加密 SD 卡的加密 SD 卡配置项改变为选中，则确定出需要加密 SD 卡，将第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

[0070] 相应地，

[0071] 允许安全访问 SD 卡之后，本发明方法还可以包括：

[0072] 如果用于配置是否加密 SD 卡的加密 SD 卡配置项改变为未选中，则删除 SD 卡中保存的第二密码，以关闭安全功能，并允许普通访问 SD 卡。

[0073] 本步骤中，删除 SD 卡中保存的第二密码，以关闭安全功能可以包括：向 SD 卡发送与关闭安全功能相应的第四安全，触发 SD 卡删除 SD 卡中保存的第二密码；其中，第四安全命令中包括用于身份验证的密码。本领域技术人员清楚的是，SD 卡在根据第四命令删除第二密码之前首先根据第四命令携带的密码进行身份验证，如果该密码为第一密码，则通过身份验证，并关闭安全功能。

[0074] 综上所述，在 SD 卡的安全功能激活时，只有激活该 SD 卡的移动终端能够关闭该 SD 卡的安全功能。

[0075] 需要说明的是，本发明方法基于 SD 卡协议规定的串行外围设备接口（SPI 接口）实现与 SD 卡通过安全命令进行通信。具体实现属于本领域技术人员的惯用技术手段，并不用于限定本发明的保护范围，这里不再赘述。

[0076] 综上所述，安全命令至少包括第一安全命令、第二安全命令、第三安全命令和第四安全命令，安全命令的具体格式可以参考 SD 卡的相关协议，此处不再赘述。

[0077] 图 2 为本发明移动终端中实现 SD 卡安全管理的装置的组成结构示意图，如图 2 所示，包括安全检测单元和安全访问管理单元，其中，

[0078] 安全检测单元，用于检测出插有 SD 卡时，确定 SD 卡是否已加密，当确定出 SD 卡已加密时，发送第一消息。

[0079] 安全访问单元，用于接收到来自安全检测单元的第一消息时，将移动终端的本地存储器保存的第一密码发送给 SD 卡，以触发 SD 卡的安全功能中的身份验证，如果身份验证成功，则允许安全访问 SD 卡，否则不允许访问 SD 卡。

[0080] 其中，安全访问 SD 卡为激活 SD 卡的安全功能时访问 SD 卡。

[0081] 其中，第一密码是根据移动设备国际身份码 IMEI 码获取、保存在本地存储器中。

[0082] 进一步地，

[0083] 安全检测单元还用于：当确定出 SD 卡未加密时，根据预先设置的加密策略确定是否需要加密 SD 卡，当确定出需要加密 SD 卡时，发送第二消息，当确定出不需要加密 SD 卡时，发送第三消息。

[0084] 其中，加密策略包括：

[0085] 如果用于配置是否加密 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡；或者，

[0086] 如果用于配置移动终端是否启用安全功能的安全配置项为选中，且用于配置是否加密 SD 卡的加密 SD 卡配置项为选中，则需要加密 SD 卡。

[0087] 其中，安全配置项为选中包括：用于配置是否启用图形密码的图案密码配置项、用于配置是否启用数字密码的数字密码配置项、以及用于配置是否启用个人识别密码（PIN）的 PIN 配置项中的至少一个配置项为选中。

[0088] 进一步地，

[0089] 安全访问单元还用于：当接收到来自安全检测单元的第二消息时，将第一密码发送给 SD 卡并保存为 SD 中的第二密码，以激活 SD 卡的安全功能，并允许安全访问 SD 卡。

[0090] 进一步地，

[0091] 安全访问单元还用于：当接收到来自安全检测单元的第三消息时，允许普通访问 SD 卡；其中，普通访问 SD 卡为关闭 SD 卡的安全功能时访问 SD 卡。

[0092] 进一步地，

[0093] 安全检测单元还用于：当允许普通访问SD卡，且检测出用于配置是否加密SD卡的加密SD卡配置项改变为选中时，发送第二消息。

[0094] 进一步地，

[0095] 检测单元还用于：当允许安全访问SD卡，且用于配置是否加密SD卡的加密SD卡配置项改变为未选中时，发送第四消息。

[0096] 相应地，

[0097] 安全访问单元还用于，当接收到来自安全检测单元的第四消息时，删除SD卡中保存的第二密码，以关闭安全功能，并允许普通访问SD卡；其中，普通访问SD卡为关闭SD卡的安全功能时访问SD卡。

[0098] 虽然本发明所揭露的实施方式如上所述，但所述的内容仅为便于理解本发明而采用的实施方式，并非用以限定本发明。任何本发明所属领域内的技术人员，在不脱离本发明所揭露的精神和范围的前提下，可以在实施的形式及细节上进行任何的修改与变化，但本发明的专利保护范围，仍须以所附的权利要求书所界定的范围为准。

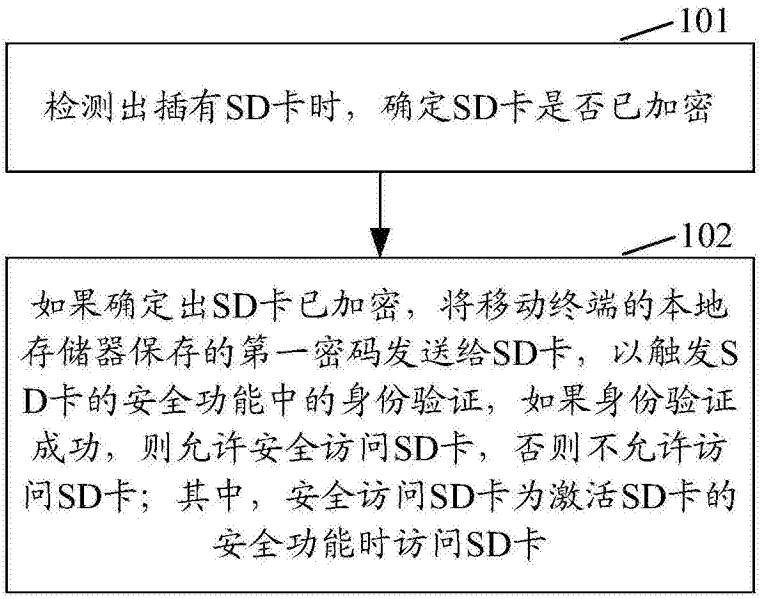

101
检测出插有SD卡时，确定SD卡是否已加密
102
如果确定出SD卡已加密，将移动终端的本地存储器保存的第一密码发送给SD卡，以触发SD卡的安全功能中的身份验证，如果身份验证成功，则允许安全访问SD卡，否则不允许访问SD卡；其中，安全访问SD卡为激活SD卡的安全功能时访问SD卡

图 1

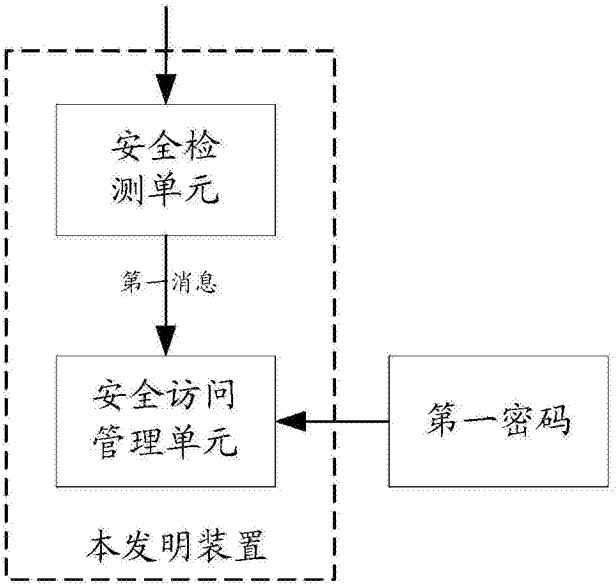

安全检测单元
第一消息
安全访问管理单元
第一密码
本发明装置

图 2