

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2013 年 12 月 19 日 (19.12.2013)



WIPO | PCT



(10) 国际公布号
WO 2013/185689 A1

- (51) 国际专利分类号:
G06F 21/00 (2013.01)
- (21) 国际申请号: PCT/CN2013/080070
- (22) 国际申请日: 2013 年 7 月 25 日 (25.07.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210379610.8 2012 年 10 月 9 日 (09.10.2012) CN
- (71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国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, Guangdong 518057 (CN)。
- (72) 发明人: 霍选礼 (HUO, Xuanli); 中国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中兴通讯股份有限公司转交, Guangdong 518057 (CN)。
- (74) 代理人: 北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区学清路 8 号 B 座 1601A, Beijing 100192 (CN)。

- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

- 关于申请人有权申请并被授予专利(细则 4.17(ii))
- 发明人资格(细则 4.17(iv))

[见续页]

(54) Title: AUTHENTICATION METHOD, AUTHENTICATION APPARATUS AND AUTHENTICATION DEVICE

(54) 发明名称: 一种认证方法、认证装置及认证设备

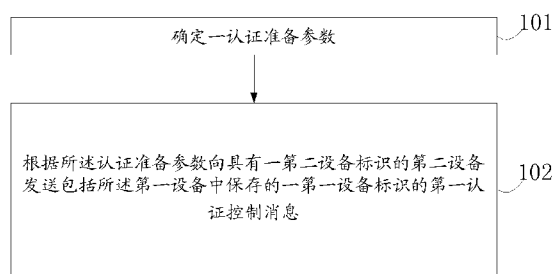


图 1 / Fig. 1

101 DETERMINING AN AUTHENTICATION PREPARATION PARAMETER
102 ACCORDING TO THE AUTHENTICATION PREPARATION PARAMETER, TRANSMITTING TO A SECOND DEVICE WHICH HAS A SECOND DEVICE IDENTIFIER A FIRST AUTHENTICATION CONTROL MESSAGE INCLUDING A FIRST DEVICE IDENTIFIER STORED IN A FIRST DEVICE

(57) Abstract: Provided are an authentication method, an authentication apparatus and an authentication device. The method includes: a first device determining an authentication preparation parameter; and according to the authentication preparation parameter, the first device transmitting to a second device which has a second device identifier a first authentication control message including a first device identifier stored in the first device, controlling the second device to judge whether the first device identifier matches the second device identifier according to the first authentication control message, acquiring the judgment result, and when the judgment result is no, performing a control operation, so as to disable the second device from reading all or some user data from the first device.

(57) 摘要: 本发明实施例提供了一种认证方法、装置和设备, 该方法包括: 第一设备确定认证准备参数; 所述第一设备根据所述认证准备参数向具有第二设备标识的第二设备发送包括所述第一设备中保存的第一设备标识的第一认证控制消息, 控制所述第二设备根据所述第一认证控制消息判断所述第一设备标识和所述第二设备标识是否匹配, 获取判断结果, 当所述判断结果为否时, 进行控制操作, 使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

WO 2013/185689 A1

**本国际公布:**

— 包括国际检索报告(条约第 21 条(3))。

— 在修改权利要求的期限届满之前进行, 在收到该修改后将重新公布(细则 48.2(h))。

— 根据申请人的请求, 在条约第 21 条(2)(a)所规定的期限届满之前进行。

一种认证方法、认证装置及认证设备

技术领域

5 本发明实施例涉及信息技术领域，尤其涉及一种认证方法、认证装置及认证设备。

背景技术

在实际中，一设备可以供其它设备正常使用，出于信息安全方面的考虑，该设备的用户可能不希望该设备被非法设备正常使用。例如，某存储卡的用户可能不希望该存储卡中的全部或者部分用户数据被非法手机读取。但是，
10 目前还没有解决此类问题的有效方法。

发明内容

有鉴于此，本发明实施例提供一种认证方法、认证装置及认证设备，以
15 限制某设备中的全部或部分用户数据被非法设备读取。

为解决上述技术问题，本发明实施例提供方案如下：

本发明实施例提供一种认证方法，包括：

第一设备确定认证准备参数；

20 所述第一设备根据所述认证准备参数向具有第二设备标识的第二设备发送包括所述第一设备中保存的第一设备标识的第一认证控制消息，控制所述第二设备根据所述第一认证控制消息判断所述第一设备标识和所述第二设备标识是否匹配，获取判断结果，当所述判断结果为否时，进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

较佳地，所述第一设备标识为：

25 所述第一设备在未保存所述第一设备标识的情况下连接到具有所述第一设备标识的第三设备时从所述第三设备读取并保存的设备标识；或者，

所述第一设备保存的第三设备标识与具有所述第一设备标识的第四设备的用户通过所述第四设备的输入单元输入的第五设备标识匹配时从所述第四

设备读取并保存的设备标识。

较佳地，所述方法还包括：

当所述判断结果为否时，所述第一设备控制所述第二设备向预设用户通知认证失败相关信息。

5 较佳地，所述控制所述第二设备向预设用户通知认证失败相关信息的步骤包括：

将所述全部或者部分用户数据加密后得到加密数据；

控制所述第二设备将所述加密数据上传到网络存储系统；

其中，所述网络存储系统可基于所述加密数据为所述预设用户提供服务。

10 本发明实施例提供一种认证方法，包括：

第二设备从第一设备接收包括所述第一设备中保存的第一设备标识的第一认证控制消息；

15 在所述第一设备的控制下，所述第二设备根据所述第一认证控制消息判断所述第一设备标识和所述第二设备的第二设备标识是否匹配，获取第一判断结果，当所述第一判断结果为否时，进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

较佳地，所述进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据的步骤包括：

获取用户通过输入单元输入的第六设备标识；

20 判断所述第一设备标识与所述第六设备标识是否匹配，获取第二判断结果；

当所述第二判断结果为否时，进行所述控制操作。

较佳地，所述方法还包括：

25 在所述第一设备的控制下，当所述第一判断结果为否时，所述第二设备向预设用户通知认证失败相关信息。

较佳地，所述向预设用户通知认证失败相关信息的步骤包括：

将来自所述第一设备的加密数据上传到预设的网络存储系统；

其中，所述加密数据由所述第一设备将所述全部或者部分用户数据加密后得到。

本发明实施例还提供一种认证装置，应用于第一设备，所述认证装置包括：

确定模块，其设置为：确定认证准备参数；以及

发送模块，其设置为：根据所述认证准备参数向具有一第二设备标识的第二设备发送包括所述第一设备中保存的一第一设备标识的第一认证控制消息，控制所述第二设备根据所述第一认证控制消息判断所述第一设备标识和所述第二设备标识是否匹配，获取一第一判断结果，当所述第一判断结果为否时，进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

10 较佳地，上述装置还包括：

第一处理模块，其设置为：当所述第一判断结果为否时，控制所述第二设备向预设用户通知认证失败相关信息。

本发明实施例还提供一种认证装置，应用于一第二设备，所述认证装置包括：

15 接收模块，其设置为：从一第一设备接收包括所述第一设备中保存的第一设备标识的第一认证控制消息；以及

第二处理模块，其设置为：在所述第一设备的控制下，根据所述第一认证控制消息判断所述第一设备标识和所述第二设备的第二设备标识是否匹配，获取第一判断结果，当所述第一判断结果为否时，进行控制操作，使所述
20 所述第二设备无法从所述第一设备读取全部或者部分用户数据。

本发明实施例还提供一种认证设备，包括如上所述的认证装置。

本发明实施例还提供另一种认证方法，包括：

存储卡接收具有第二终端识别码的第一终端在所述存储卡内预置的固定程序的控制下生成并发送的认证请求指令；

25 所述存储卡根据所述认证请求指令向所述第一终端发送所述存储卡中保存的第一终端识别码，使所述第一终端在所述固定程序的控制下判断所述第一终端识别码和所述第二终端识别码是否匹配，获取第一判断结果，当所述第一判断结果为否时，所述存储卡删除所述存储卡中保存的用户数据。

较佳地，所述第一终端识别码为：

所述存储卡在未保存所述第一终端识别码的情况下连接到具有所述第一终端识别码的第二终端时，从所述第二终端接收并保存的所述第二终端在所述固定程序的控制下发送的所述第一终端识别码；或者，

5 所述存储卡保存的第三终端识别码与具有所述第一终端识别码的第三终端的用户通过所述第三终端的输入单元输入的第四终端识别码匹配时，所述存储卡从所述第三终端接收并保存的所述第三终端在所述固定程序的控制下发送的所述第一终端识别码。

从以上所述可以看出，本发明实施例至少具有如下有益效果：

10 通过向第二设备发送第一认证控制消息，控制第二设备进行相应的处理，从而使第二设备在第二设备标识与第一设备保存的第一设备标识不匹配时无法从第一设备读取全部或部分用户数据；

15 通过接收第一终端在存储卡内预置的固定程序的控制下发送的认证请求消息，根据认证请求消息向第一终端发送保存的第一终端识别码，使第一终端在在所述固定程序的控制下进行相应的处理，从而使存储卡内保存的终端识别码与第一终端的终端识别码不匹配时，第一终端无法从存储卡读取用户数据。

附图概述

图 1 为本发明实施例提供的一种认证方法的流程图；

20 图 2 为本发明实施例提供的另一种认证方法的流程图；

图 3 为本发明实施例提供的例子的系统结构框图；

图 4 为本发明实施例提供的例子的存储卡识别和终端识别码绑定的流程图；

25 图 5 为本发明实施例提供的例子的存储卡插入其它终端的情况下的流程图；

图 6 为本发明实施例提供的一种认证装置的结构示意图；

图 7 为本发明实施例提供的另一种认证装置的结构示意图。

本发明的较佳实施方式

下面将结合附图及具体实施例对本发明实施例进行详细描述。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。

图 1 为本发明实施例提供的一种认证方法的流程图，参照图 1，所述认证方法包括如下步骤：

步骤 101，第一设备确定认证准备参数；

步骤 102，第一设备根据所述认证准备参数向具有一第二设备标识的第二设备发送包括所述第一设备中保存的一第一设备标识的第一认证控制消息，控制所述第二设备根据所述第一认证控制消息判断所述第一设备标识和所述第二设备标识是否匹配，获取一第一判断结果，当所述第一判断结果为否时，进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

可见，通过向第二设备发送第一认证控制消息，控制第二设备进行相应的处理，从而使第二设备在第二设备标识与第一设备保存的第一设备标识不匹配时无法从第一设备读取全部或部分用户数据。

其中，所述认证准备参数可以为读取所述第一设备中用户数据的读取指令，或者，可以为检测到所述第一设备与所述第二设备连接时生成的参数，或者，可以为所述第二设备在检测到所述第二设备与所述第一设备连接后，因自动运行所述第一设备中预置的固定安装程序而生成的认证请求指令。所述确定一认证准备参数可以为：

从所述第二设备接收到所述读取指令；或者，
检测到所述第一设备与所述第二设备连接时生成所述认证准备参数；或者，

从所述第二设备接收到所述认证请求指令。

所述第二设备在接收所述第一认证控制消息之前可以运行所述第一设备中预置的固定安装程序，并因运行该固定安装程序而会在所述第一认证控制

消息的触发下进行所述判断所述第一设备标识和所述第二设备标识是否匹配，获取一第一判断结果，当所述第一判断结果为否时，进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据的操作。或者，

5 所述第一认证控制消息中可以携带有执行代码，从而使所述第二设备执行该执行代码，并因执行该执行代码而进行所述判断所述第一设备标识和所述第二设备标识是否匹配，获取一第一判断结果，当所述第一判断结果为否时，进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据的操作。

10 判断某两个设备标识（这里为所述第一设备标识和所述第二设备标识）是否匹配，例如：

这两个设备标识是否相同；或者，

这两个设备标识是否属于同一设备标识集合。

所述进行控制操作，例如：

15 拦截所述第二设备为从所述第一设备读取全部或者部分用户数据所需与所述第一设备交互的指令（例如，需要向所述第一设备发送的指令）；或者，

所述第二设备向所述第一设备发送使所述第一设备禁止所述第二设备读取所述全部或者部分用户数据的指令，例如，指示所述第一设备删除所述全部或者部分用户数据的指令，锁定或格式化所述第一设备的指令，等等。则所述认证方法还可以包括：当接收到该指令时，根据该指令禁止所述第二设备读取所述全部或者部分用户数据。

20

所述第一设备标识可以为：

所述第一设备在未保存所述第一设备标识的情况下连接到具有所述第一设备标识的第三设备时从所述第三设备读取并保存的设备标识；或者，

25 所述第一设备保存的一第三设备标识与具有所述第一设备标识的第四设备的用户通过所述第四设备的输入单元输入的一第五设备标识匹配时从所述第四设备读取并保存的设备标识。

其中，所述第三设备与所述第二设备可以相同或不同。所述第四设备与所述第二设备可以相同或不同。所述第五设备标识与所述第三设备标识可以

相同或不同。当某两个设备标识是否匹配为该两个设备标识是否相同时，所述第五设备标识与所述第三设备标识相同。

为了使用户及时获知认证失败相关信息，所述认证方法还可以包括：

当所述第一判断结果为否时，控制所述第二设备向一预设用户通知认证失败相关信息。

具体地，例如，当所述第一判断结果为否时，所述第一设备会收到所述第二设备的认证失败指示，并根据该认证失败指示控制所述第二设备向所述预设用户通知认证失败相关信息。

进一步地，所述控制所述第二设备向一预设用户通知认证失败相关信息可以为控制所述第二设备显式地通知，例如，控制所述第二设备向所述预设用户发送短信来通知所述预设用户认证失败相关信息。

或者，所述控制所述第二设备向一预设用户通知认证失败相关信息可以为控制所述第二设备隐式地通知，例如，所述控制所述第二设备向一预设用户通知认证失败相关信息具体可以为：

15 将所述全部或者部分用户数据加密后得到加密数据；

控制所述第二设备将所述加密数据上传到一网络存储系统；

其中，所述网络存储系统可基于所述加密数据为所述预设用户提供服务。

所述为所述预设用户提供服务，例如，为所述预设用户提供所述加密数据的下载服务，将所述加密数据解密后为所述预设用户提供解密后数据的查询或下载服务，等等。

这样，所述第一设备的原用户既可以知道发生了认证失败，又不会对所述全部或者部分用户数据有太大的使用上的不便。

其中，所述认证失败相关信息例如：认证失败指示，设备被非法使用指示，等等。可选地，所述认证失败相关信息中还可以包括所述第一设备标识和/或所述第二设备标识，这样，所述预设用户就能知道哪个设备被非法使用，或者知道属于自己的设备被哪个设备非法使用。

图 2 为本发明实施例提供的另一种认证方法的流程图，参照图 2，所述认证方法包括如下步骤：

步骤 201, 第二设备从第一设备接收包括所述第一设备中保存的第一设备标识的第一认证控制消息;

步骤 202, 在所述第一设备的控制下, 第二设备根据所述第一认证控制消息判断所述第一设备标识和第二设备的第二设备标识是否匹配, 获取一第一判断结果, 当所述第一判断结果为否时, 进行控制操作, 使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

可见, 第二设备在所述第一设备的控制下进行相应的处理, 从而使第二设备在第二设备标识与第一设备保存的第一设备标识不匹配时无法从第一设备读取全部或部分用户数据。

10 考虑到, 如果所述第一设备属于某用户, 则当该用户通过会判定所述第一判断结果为否的设备来使用所述第一设备时, 该设备就无法从所述第一设备读取全部或者部分用户数据, 从而为该用户造成使用不便。有鉴于此,

所述进行控制操作, 使所述第二设备无法从所述第一设备读取全部或者部分用户数据具体可以为:

15 获取用户通过一输入单元输入的一第六设备标识;

判断所述第一设备标识与所述第六设备标识是否匹配, 获取一第二判断结果;

当所述第二判断结果为否时, 进行所述控制操作。

20 考虑到用户可能输入失误, 则可以允许用户有一次或两次以上出错的机会, 于是有:

所述当所述第二判断结果为否时, 进行所述控制操作可以为:

当所述第二判断结果为否时, 判断所述第六设备标识的输入次数是否达到预设数目, 获取第三判断结果;

当所述第三判断结果为是时, 进行所述控制操作;

25 当所述第三判断结果为否时, 返回所述获取用户通过输入单元输入的第六设备标识的步骤。

其中, 每次输入的所述第六设备标识可以完全相同, 也可以不完全相同。

此外，为了使用户及时获知认证失败相关信息，所述认证方法还可以包括：

在所述第一设备的控制下，当所述第一判断结果为否时，向预设用户通知认证失败相关信息。

5 其中，所述认证失败相关信息例如：认证失败指示，设备被非法使用指示，等等。

其中，所述向一预设用户通知认证失败相关信息可以为向所述预设用户发送包括认证失败相关信息的短信；或者，为了使所述第一设备的原用户不会对所述全部或者部分用户数据有太大的使用上的不便，所述向一预设用户
10 通知认证失败相关信息可以为：

将来自所述第一设备的加密数据上传到一预设的网络存储系统；

其中，所述加密数据由所述第一设备将所述全部或者部分用户数据加密后得到。

所述网络存储系统例如：服务器。

15 本发明实施例还提供一种认证方法，用于一存储卡，所述认证方法包括如下步骤：

步骤 110，存储卡接收具有第二终端识别码的第一终端在所述存储卡内预置的固定程序的控制下生成并发送的认证请求指令；

步骤 111，存储卡根据所述认证请求指令向所述第一终端发送所述存储
20 卡中保存的第一终端识别码，使所述第一终端在所述固定程序的控制下判断所述第一终端识别码和所述第二终端识别码是否匹配，获取第一判断结果，当所述第一判断结果为否时，存储卡删除所保存的用户数据。

可见，通过接收第一终端在存储卡内预置的固定程序的控制下发送的认证请求消息，根据认证请求消息向第一终端发送保存的第一终端识别码，使
25 第一终端在在所述固定程序的控制下进行相应的处理，从而使存储卡内保存的终端识别码与第一终端的终端识别码不匹配时，第一终端无法从存储卡读取用户数据。

其中，所述第一终端识别码可以为：

所述存储卡在未保存所述第一终端识别码的情况下连接到具有所述第一终端识别码的第二终端时，从所述第二终端接收并保存的所述第二终端在所述固定程序的控制下发送的所述第一终端识别码；或者，

5 所述存储卡保存的第三终端识别码与具有所述第一终端识别码的第三终端的用户通过所述第三终端的输入单元输入的第四终端识别码匹配时，所述存储卡从所述第三终端接收并保存的所述第三终端在所述固定程序的控制下发送的所述第一终端识别码。

10 为了将本发明实施例提供的上述三种认证方法阐述明白，下面以所述第一设备为存储卡（例如，T卡），所述第二设备为终端（例如，手机）为例，对上述认证方法进行说明：

15 图3为本发明实施例提供的系统结构框图，参照图3，该系统包括存储了固定程序的存储卡和终端处理器。其中，该固定程序为自动程序。该固定程序是用户不可删除或格式化的，是存储卡存储受保护部分。在终端运行该固定程序的过程中，终端处理器用于判定存储卡内保存的终端识别码和终端的终端识别码是否匹配。

图4为本发明实施例提供的例子的存储卡识别和终端识别码绑定的流程图，参照图4，存储卡初次插入某终端及后来又插入该终端的存储卡识别和终端识别码绑定的步骤如下：

步骤401，存储卡初插入终端；

20 步骤402，终端开机后，检测到有存储卡插入时会自动运行存储卡内预置的固定程序，并按照该固定程序执行步骤403和步骤404；

步骤403，终端保存终端识别码到存储卡；

其中，终端识别码例如，当终端为CDMA制式手机时为MEID，当终端为WCDMA或GSM制式手机时为IMEI，等等。

25 步骤404，存储卡保存该终端识别码后，终端正常使用存储卡；

其中，终端正常使用存储卡，例如：终端从存储卡中读取用户数据。

步骤405，用户拔出存储卡；

步骤406，用户将存储卡重新插入原终端；

步骤 407, 和存储卡内终端识别码对比;

具体地, 终端开机后, 自动运行存储卡内预置的固定程序, 并按照该固定程序执行如下操作: 终端处理器发出指令将终端的终端识别码与存储卡内保存的终端识别码进行对比, 以判定存储卡内保存的终端识别码和终端的终端识别码是否匹配, 如果是, 则执行步骤 408。

步骤 408, 终端正常使用存储卡。

图 5 为本发明实施例提供的例子的存储卡插入其它终端的情况下的流程图, 参照图 5, 此时存储卡内保存了终端识别码且保存的终端识别码为原终端的终端识别码, 则在存储卡插入某其它终端的情况下有如下步骤:

步骤 501, 存储卡插入其它终端;

步骤 502, 输入终端识别码;

具体地, 该其它终端开机后, 自动运行存储卡内固定程序, 并按照该固定程序执行如下操作: 终端处理器发出指令将该其它终端的终端识别码与存储卡内保存的终端识别码进行对比, 以判断存储卡内保存的终端识别码和该其它终端的终端识别码是否匹配, 如果否, 则该其它终端发出指令弹出对话框以提醒输入终端识别码, 并在接收到用户看到对话框后输入的终端识别码时, 判断输入的终端识别码与存储卡内保存的终端识别码是否匹配, 如果是, 则执行步骤 503; 如果否, 执行步骤 508。

步骤 503, 该其它终端判定输入的终端识别码与存储卡内保存的终端识别码匹配, 即该其它终端确认输入正确, 则按照存储卡内固定程序执行步骤 504;

步骤 504, 该其它终端发出指令弹出对话框以提醒是否替换存储卡内保存的终端识别码, 如果是, 则按照存储卡内固定程序执行步骤 505~步骤 507; 如果否, 则按照存储卡内固定程序执行步骤 507。

步骤 505, 该其它终端根据用户的替换指示向存储卡写入该其它终端的终端识别码;

步骤 506, 该其它终端在写入的终端识别码被存储卡保存后, 删除存储卡中保存的原终端识别码;

步骤 507, 该其它终端可正常使用存储卡;

步骤 508, 该其它终端判定输入的终端识别码与存储卡内保存的终端识别码不匹配, 即该其它终端确认输入错误, 则执行步骤 a:

判断当前终端识别码的输入次数是否达到一预设次数 (例如, 3 次),

- 5 如果是, 则向存储卡发送锁定指令以使存储卡锁定, 并按照存储卡内固定程序执行步骤 509~步骤 512; 如果否, 则发出指令弹出对话框以提醒再次输入终端识别码, 判定再次输入的终端识别码与存储卡内保存的终端识别码是否匹配, 如果是, 则按照存储卡内固定程序执行步骤 504~步骤 507; 如果否, 则返回步骤 a。

- 10 步骤 509, 该其它终端向存储卡发送加密指令以使存储卡内数据被存储卡加密后生成加密数据;

步骤 510, 该其它终端将加密数据上传服务器;

其中, 所述服务器例如, 云服务器。

步骤 511, 该其它终端自动发短信通知原终端;

- 15 步骤 512, 该其它终端向存储卡发送格式化指令以使存储卡自动格式化。

本发明实施例还提供一种认证装置, 用于第一设备, 如图 6 所示, 所述认证装置包括:

确定模块, 设置为确定认证准备参数;

- 20 发送模块, 设置为根据所述认证准备参数向具有第二设备标识的第二设备发送包括所述第一设备中保存的第一设备标识的第一认证控制消息, 控制所述第二设备根据所述第一认证控制消息判断所述第一设备标识和所述第二设备标识是否匹配, 获取第一判断结果, 当所述第一判断结果为否时, 进行控制操作, 使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

- 25 可见, 通过向第二设备发送第一认证控制消息, 控制第二设备进行相应的处理, 从而使第二设备在第二设备标识与第一设备保存的第一设备标识不匹配时无法从第一设备读取全部或部分用户数据。

所述认证装置还可以包括:

第一处理模块，设置为当所述第一判断结果为否时，控制所述第二设备向预设用户通知认证失败相关信息。

本发明实施例还提供一种认证装置，用于第二设备，所述第二设备具有第二设备标识，如图7所示，所述认证装置包括：

- 5 接收模块，设置为从一第一设备接收包括所述第一设备中保存的一第一设备标识的第一认证控制消息；

10 第二处理模块，设置为在所述第一设备的控制下，根据所述第一认证控制消息判断所述第一设备标识和所述第二设备标识是否匹配，获取一第一判断结果，当所述第一判断结果为否时，进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

可见，第二设备在所述第一设备的控制下进行相应的处理，从而使第二设备在第二设备标识与第一设备保存的第一设备标识不匹配时无法从第一设备读取全部或部分用户数据。

- 15 本发明实施例还提供一种认证设备，所述认证设备包括以上所述的认证装置。

20 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

以上所述仅是本发明实施例的实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明实施例原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明实施例的保护范围。

25

工业实用性

本发明实施例可以限制某设备中的全部或部分用户数据被非法设备读取。

权 利 要 求 书

1. 一种认证方法，包括：

第一设备确定认证准备参数；

5 所述第一设备根据所述认证准备参数向具有第二设备标识的第二设备发送包括所述第一设备中保存的第一设备标识的第一认证控制消息，控制所述第二设备根据所述第一认证控制消息判断所述第一设备标识和所述第二设备标识是否匹配，获取判断结果，当所述判断结果为否时，进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

2. 如权利要求 1 所述的方法，其中，所述第一设备标识为：

10 所述第一设备在未保存所述第一设备标识的情况下连接到具有所述第一设备标识的第三设备时从所述第三设备读取并保存的设备标识；或者，

所述第一设备保存的第三设备标识与具有所述第一设备标识的第四设备的用户通过所述第四设备的输入单元输入的第五设备标识匹配时从所述第四设备读取并保存的设备标识。

15 3. 如权利要求 1 所述的方法，所述方法还包括：

当所述判断结果为否时，所述第一设备控制所述第二设备向预设用户通知认证失败相关信息。

4. 如权利要求 3 所述的方法，其中，所述控制所述第二设备向预设用户通知认证失败相关信息的步骤包括：

20 将所述全部或者部分用户数据加密后得到加密数据；

控制所述第二设备将所述加密数据上传到网络存储系统；

其中，所述网络存储系统可基于所述加密数据为所述预设用户提供服务。

5. 一种认证方法，包括：

25 第二设备从第一设备接收包括所述第一设备中保存的第一设备标识的第一认证控制消息；

在所述第一设备的控制下，所述第二设备根据所述第一认证控制消息判断所述第一设备标识和所述第二设备的第二设备标识是否匹配，获取第一判断结果，当所述第一判断结果为否时，进行控制操作，使所述第二设备无法

从所述第一设备读取全部或者部分用户数据。

6. 如权利要求 5 所述的方法, 其中, 所述进行控制操作, 使所述第二设备无法从所述第一设备读取全部或者部分用户数据的步骤包括:

获取用户通过输入单元输入的第六设备标识;

5 判断所述第一设备标识与所述第六设备标识是否匹配, 获取第二判断结果;

当所述第二判断结果为否时, 进行所述控制操作。

7. 如权利要求 5 所述的方法, 所述方法还包括:

10 在所述第一设备的控制下, 当所述第一判断结果为否时, 所述第二设备向预设用户通知认证失败相关信息。

8. 如权利要求 7 所述的方法, 其中, 所述向预设用户通知认证失败相关信息的步骤包括:

将来自所述第一设备的加密数据上传到预设的网络存储系统;

15 其中, 所述加密数据由所述第一设备将所述全部或者部分用户数据加密后得到。

9. 一种认证装置, 应用于第一设备, 所述认证装置包括:

确定模块, 其设置为: 确定认证准备参数; 以及

20 发送模块, 其设置为: 根据所述认证准备参数向具有一第二设备标识的第二设备发送包括所述第一设备中保存的一第一设备标识的第一认证控制消息, 控制所述第二设备根据所述第一认证控制消息判断所述第一设备标识和所述第二设备标识是否匹配, 获取一第一判断结果, 当所述第一判断结果为否时, 进行控制操作, 使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

10. 如权利要求 9 所述的装置, 还包括:

25 第一处理模块, 其设置为: 当所述第一判断结果为否时, 控制所述第二设备向预设用户通知认证失败相关信息。

11. 一种认证装置, 应用于一第二设备, 所述认证装置包括:

接收模块, 其设置为: 从一第一设备接收包括所述第一设备中保存的第一设备标识的第一认证控制消息; 以及

第二处理模块，其设置为：在所述第一设备的控制下，根据所述第一认证控制消息判断所述第一设备标识和所述第二设备的第二设备标识是否匹配，获取第一判断结果，当所述第一判断结果为否时，进行控制操作，使所述第二设备无法从所述第一设备读取全部或者部分用户数据。

5 12. 一种认证设备，包括权利要求 9 至 11 中任一项所述的认证装置。

13. 一种认证方法，包括：

存储卡接收具有第二终端识别码的第一终端在所述存储卡内预置的固定程序的控制下生成并发送的认证请求指令；

10 所述存储卡根据所述认证请求指令向所述第一终端发送所述存储卡中保存的第一终端识别码，使所述第一终端在所述固定程序的控制下判断所述第一终端识别码和所述第二终端识别码是否匹配，获取第一判断结果，当所述第一判断结果为否时，所述存储卡删除所述存储卡中保存的用户数据。

14. 如权利要求 13 所述的方法，其中，所述第一终端识别码为：

15 所述存储卡在未保存所述第一终端识别码的情况下连接到具有所述第一终端识别码的第二终端时，从所述第二终端接收并保存的所述第二终端在所述固定程序的控制下发送的所述第一终端识别码；或者，

20 所述存储卡保存的第三终端识别码与具有所述第一终端识别码的第三终端的用户通过所述第三终端的输入单元输入的第四终端识别码匹配时，所述存储卡从所述第三终端接收并保存的所述第三终端在所述固定程序的控制下发送的所述第一终端识别码。

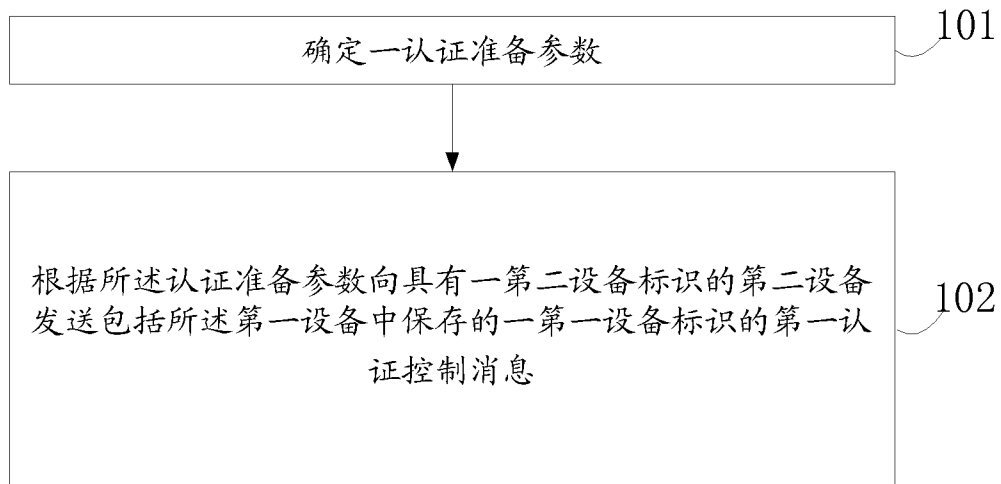


图 1

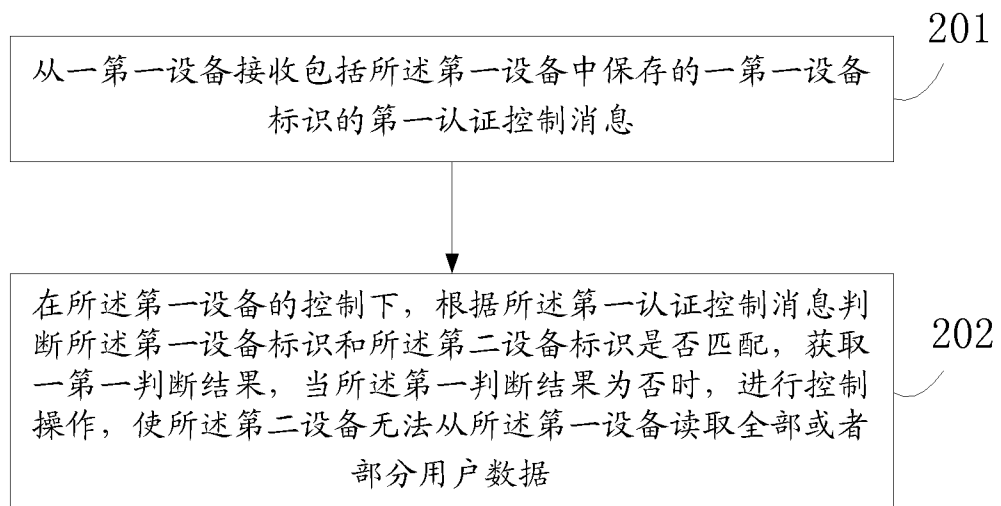


图 2

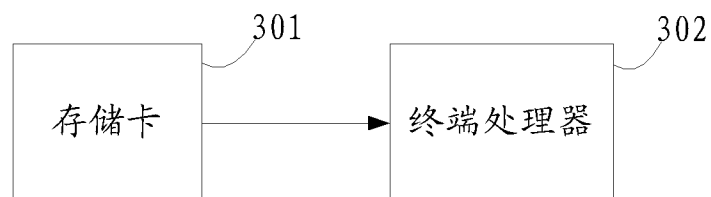


图 3

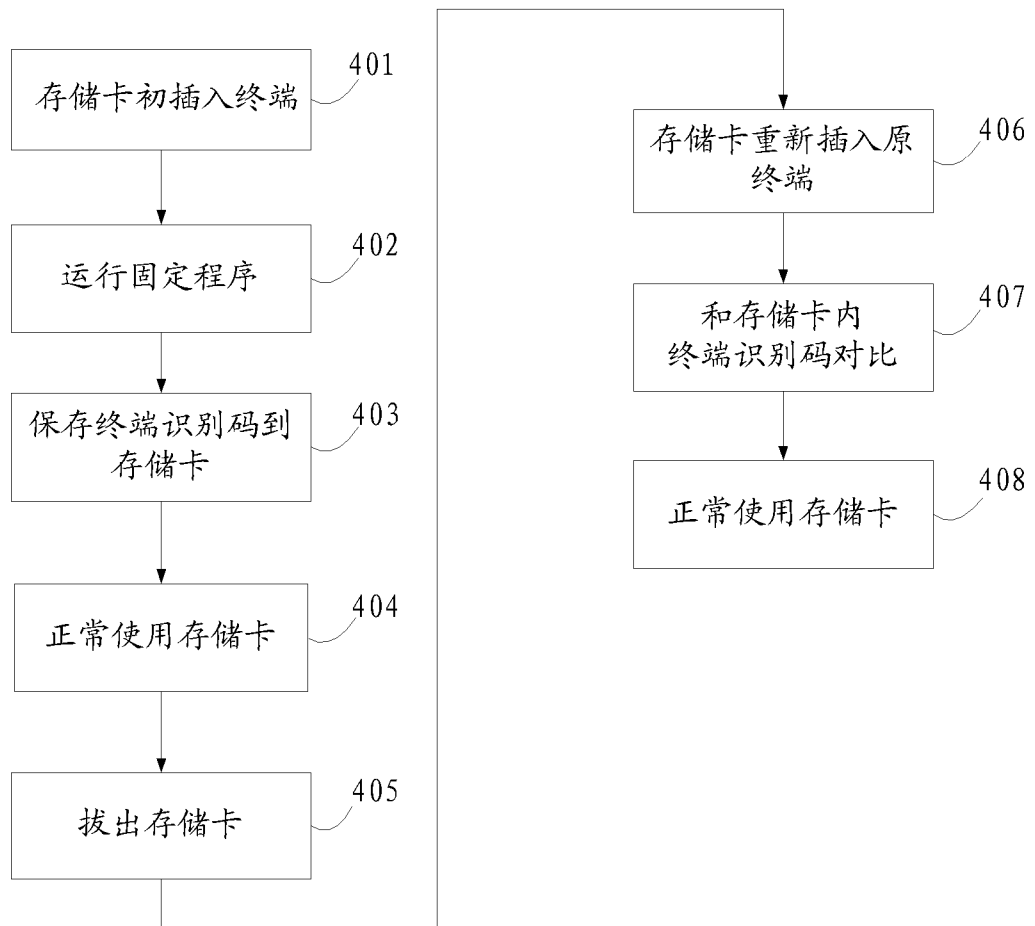


图 4

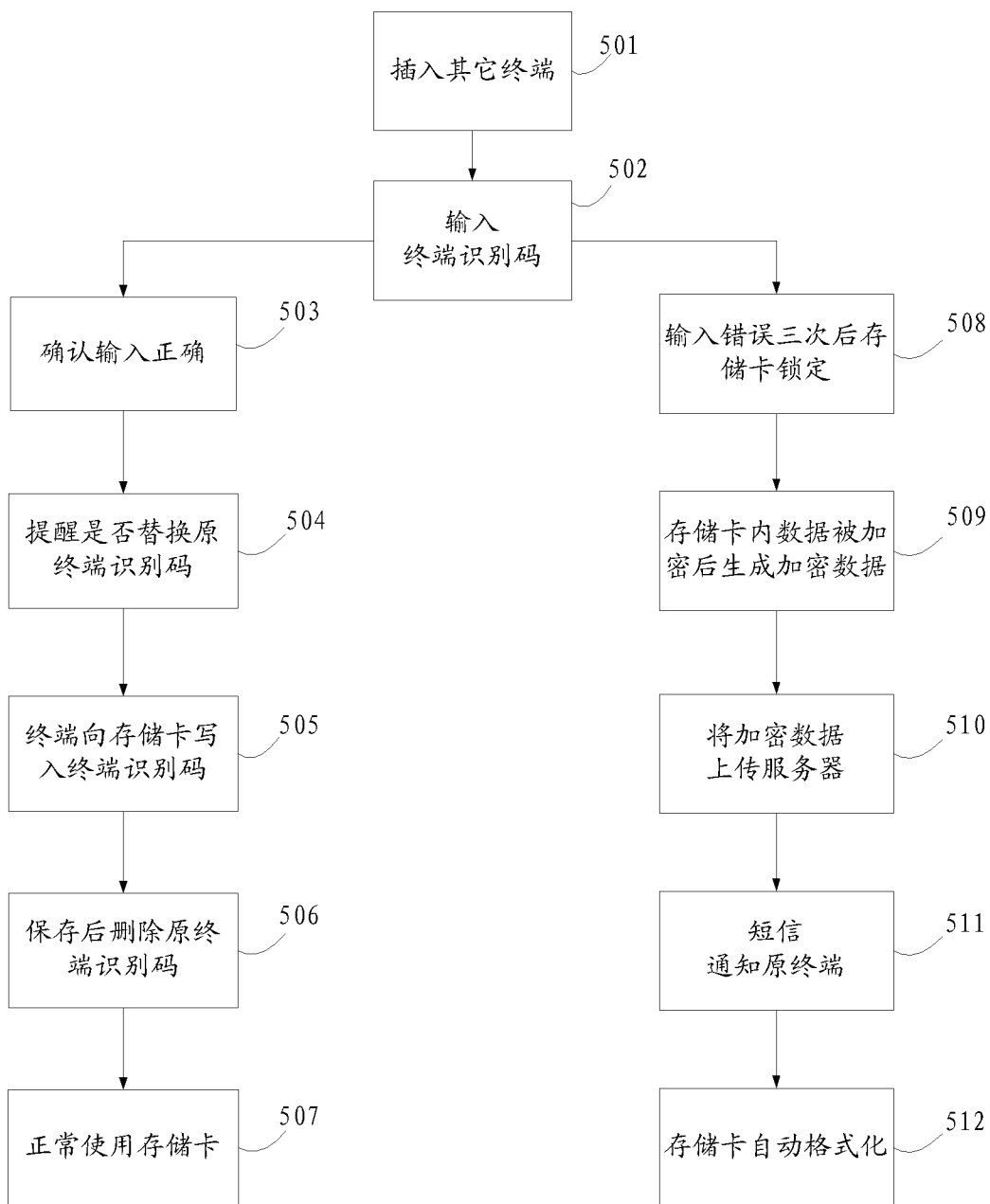


图 5

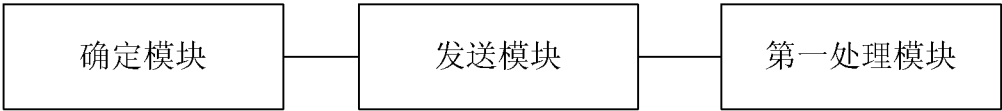


图 6

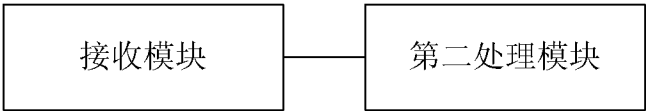


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/080070

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06K/-; H04L/-; G06F/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI; EPODOC; CNKI; IEEE; CNPAT: password; memory w card, memory, storage, terminal, encrypt+, decrypt+, authenticat+, parameter, program, autorun, key, identifier

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101256609 A (PHISON ELECTRONICS CORP.), 03 September 2008 (03.09.2008), description, pages 1, 2, 6 and 7, and figures 1-3	1, 3, 5, 7, 9-13
X	CN 101090316 A (POTEVIO INSTITUTE OF TECHNOLOGY CO., LTD.), 19 December 2007 (19.12.2007), description, pages 5 and 6, and figures 1-2	1, 3, 5, 7, 9-11
X	CN 101276432 A (POTEVIO INSTITUTE OF TECHNOLOGY CO., LTD.), 01 October 2008 (01.10.2008), description, pages 8-10, and figures 1-3	1, 3, 5, 7, 9-11
A	CN 101404577 A (NANJING UNIVERSITY), 08 April 2009 (08.04.2009), see the whole document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 20 October 2013 (20.10.2013)	Date of mailing of the international search report 31 October 2013 (31.10.2013)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LI, Le Telephone No.: (86-10) 62411827

International application No.
PCT/CN2013/080070

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类

G06F 21/00 (2013.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06K /-; H04L/-; G06F /-;

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

WPI;EPODOC;CNKI;IEEE;CNPAT

存储卡, 存储器, 终端, 加密, 解密, 认证, 参数, 程序, 自动运行, 密码, 标识; memory w card, memory, storage, terminal, encrypt+, decrypt+, authenticat+, parameter, program, autorun, key, identifier

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 101256609 A (群联电子股份有限公司) 03.9 月 2008 (03.09.2008) 说明书第 1,2,6,7 页, 图 1-3	1,3,5,7,9-13
X	CN 101090316 A (普天信息技术研究院) 19.12 月 2007 (19.12.2007) 说明书第 5,6 页, 图 1-2	1,3,5,7,9-11
X	CN 101276432 A (普天信息技术研究院有限公司) 01.10 月 2008 (01.10.2008) 说明书第 8-10 页, 图 1-3	1,3,5,7,9-11
A	CN 101404577 A (南京大学) 08.4 月 2009 (08.04.2009) 参见全文	1-14



其余文件在 C 栏的续页中列出。



见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

20.10 月 2013 (20.10.2013)

国际检索报告邮寄日期

31.10 月 2013 (31.10.2013)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

受权官员

李乐

电话号码: (86-10) 62411827

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/080070

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101256609A	03.09.2008	CN101256609B	08.09.2010
CN101090316A	19.12.2007	CN101090316B	20.04.2011
CN101276432A	01.10.2008	CN101276432B	20.07.2011
CN101404577A	08.04.2009	CN101404577B	21.04.2010