[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/22 (2006.01)
G06F 21/24 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710063102.8

[43] 公开日 2007 年 8 月 1 日

[11] 公开号 CN 101008974A

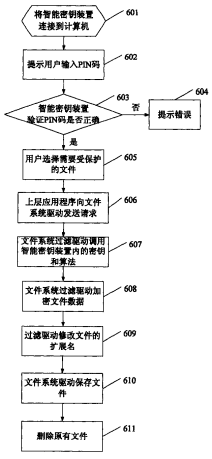
[22] 申请日 2007.1.26
[21] 申请号 200710063102.8
[71] 申请人 北京飞天诚信科技有限公司
地址 100083 北京市海淀区学院路 40 号研 7A 楼 5 层
[72] 发明人 陆 舟 于华章
[74] 专利代理机构 北京中海智圣知识产权代理有限公司
代理人 曾永珠
权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称

一种电子文件保护方法及系统

[57] 摘要

本发明公开了一种利用修改文件名以及结合文件系统过滤驱动和智能密钥装置对电子文件进行加密保护的解决方案，以及实现该方案的文件保护系统。 本发明保证了当用户误操作或非法访问文件时文件不被破坏；并且不需要建立文件列表，避免了列表丢失造成的损失；采用文件系统过滤驱动对文件进行处理，用户在访问和操作文件时不用另外对文件采取保护措施，方便了用户使用；采用智能密钥装置结合文件系统过滤驱动加密文件，使得文件具有更高的安全性。



1. 一种电子文件保护方法，其特征在于：

（1）对文件的保护过程包括：

加密文件；

修改所述加密文件的初始文件名；

存储所述修改过文件名的加密文件；

（2）浏览受保护文件的过程包括：

上层应用程序发送 IRP_MJ_DIRECT_CONTROL 请求；

由文件系统过滤驱动将请求包中的文件名恢复为所述初始文件名，并以所述初始文件名显示受保护文件；

（3）访问受保护文件的过程包括：

上层应用程序发送 IRP_MJ_CREATE 请求；

文件系统过滤驱动将请求包中的文件名以对文件实施保护时修改文件名的方式进行修改；

操作系统建立文件句柄；

上层应用程序利用所述文件句柄发送 IRP_MJ_READ 请求读文件，文件系统过滤驱动进行解密；

或上层应用程序利用所述文件句柄发送 IRP_MJ_WRITE 请求修改文件，文件系统过滤驱动进行加密。

2. 根据权利要求 1 所述的电子文件保护方法，其特征在于：在对文件的保护过程中，加密文件的操作由文件系统过滤驱动完成。

3. 根据权利要求 1 所述的电子文件保护方法，其特征在于：在对文件的保护过程中，加密文件的操作由上层应用程序完成。

4. 根据权利要求 1 所述的电子文件保护方法，其特征在于：在对文件的保护过程中，修改文件名的操作是在初始文件名的扩展名中

加入特征标识串。

5. 根据权利要求 1 所述的电子文件保护方法，其特征在于：在对文件的保护过程中，修改文件名的操作由上层应用程序完成。

6. 根据权利要求 1 所述的电子文件保护方法，其特征在于：在对文件的保护过程中，修改文件名的操作由文件系统过滤驱动完成。

7. 根据权利要求 1 所述的电子文件保护方法，其特征在于：在对文件的保护过程中，完成存储所述修改过文件名的加密文件后将原有文件删除。

8. 根据权利要求 1 所述的电子文件保护方法，其特征在于：智能密钥装置参与所述文件保护、浏览或访问受保护文件的过程。

9. 根据权利要求 8 所述的电子文件保护方法，其特征在于：在进行所述文件保护、浏览或访问受保护文件之前，系统检测智能密钥装置是否存在，如果不存在则不能进行文件保护、浏览或访问受保护文件的操作。

10. 根据权利要求 8 所述的电子文件保护方法，其特征在于：对文件的加密或解密操作由文件系统过滤驱动调用所述智能密钥装置完成。

11. 实现权利要求 1 至 10 之一所述的电子文件保护方法的系统，其特征在于包括：文件保护模块、文件创建模块、文件浏览模块、读文件模块、写文件模块和文件系统过滤驱动模块；

所述文件保护模块对文件进行加密和修改文件名；

所述文件创建模块接收文件创建请求、修改初始文件名并创建文件句柄；

所述文件浏览模块接收文件浏览请求、恢复文件名为初始文件名并以所述初始文件名显示文件；

所述读文件模块接收读文件请求，由文件系统过滤驱动模块根据文件句柄读取文件并解密；

所述写文件模块接收写文件请求，由文件系统过滤驱动模块加密文件并根据文件句柄将文件写入磁盘。

12. 根据权利要求 11 所述的电子文件保护系统，其特征在于：还包括由文件系统过滤驱动模块调用的智能密钥装置，对文件进行加密或解密操作。

13. 根据权利 11 所述的对电子文件的保护系统，其特征在于：包括智能密钥装置监控模块，以监控系统中是否连接有智能密钥装置。

一种电子文件保护方法及系统

技术领域

本发明涉及信息安全技术，尤其涉及一种通过修改文件名并结合文件系统过滤驱动进行电子文件保护的方法及其系统。

背景技术

随着计算机技术和信息技术的快速发展，计算机已成为人们日常生活、办公和学习必不可少的工具，越来越多的数据信息通过电子文件的形式保存在计算机上。这种形式给人们带来便利的同时，也出现了安全性隐患——很多文档信息具有机密性，不能被随意阅读和篡改，因此需要保证敏感信息的安全性。目前人们主要利用加密和密码验证技术来控制非法操作者对敏感信息的访问，例如利用各种密钥机制对文件加密，或利用密码验证来验证操作者的身份，从而防止非法操作者访问文件。

上述将文件加密的文件保护方法虽然可以一定程度的对电子文件起到保护作用，但是如果用户意外访问文件或非法操作者访问文件，由于文件是以密文形式存储的，所以文件会尝试自动恢复，这样文件就会损坏而无法使用。并且此种方法需建立文件列表列出加密保护的文件，文件列表一旦丢失便不能对加密的文件进行解密，导致无法对文件进行操作。而上述利用密码验证保护文件的方法，由于密码容易遗忘和泄漏，也会对文件的安全造成威胁。所以上述两种方法都不能对电子文件起到有效的保护作用。

智能密钥装置是一种带有处理器和存储器的小型硬件装置，它可通过计算机的数据通讯接口与计算机连接。智能密钥装置采用密码验

证用户身份的合法性，在进行身份认证时将智能密钥装置与计算机相连，用户在计算机上输入密码，智能密钥装置会自动校验该密码的正确性，只有当用户输入的密码正确时，才允许用户操作智能密钥装置。智能密钥装置还具有密钥生成功能，并可安全存储密钥和预置加密算法。智能密钥装置与密钥相关的运算完全在装置内部运行，且智能密钥装置具有物理抗攻击的特性，安全性极高。如果可以将这种安全性更高的智能密钥技术应用于文件保护领域，文件的安全性将大大提高。

目前我们使用的 Windows 文件系统的结构是分层的，上层应用程序访问文件系统都需要通过 I/O 请求包（IRP）来记录和管理，每次的 I/O 访问都会促使一个 I/O 请求包被发送到文件系统驱动。在每个 I/O 请求包中，记录了进程打开该文件时得到的文件句柄。通常还会在文件系统驱动的上层加入一层文件系统过滤驱动，它可以对上层应用发送的 I/O 请求包进行过滤，然后再发送到文件系统驱动层。

发明内容

本发明针对现有技术下电子文件存在的安全隐患，提出了利用修改文件名以及结合文件系统过滤驱动和智能密钥装置对电子文件进行加密保护的解决方案。

一种电子文件保护方法，包括对文件的保护，以及对受保护文件的浏览和访问。

（1）对文件的保护过程包括：

加密文件；

修改所述加密文件的初始文件名；

存储所述修改过文件名的加密文件；

（2）浏览受保护文件的过程包括：

上层应用程序发送 IRP_MJ_DIRECT_CONTROL 请求；

由文件系统过滤驱动将请求包中的文件名恢复为所述初始文件名，并以所述初始文件名显示受保护文件；

（3）访问受保护文件的过程包括：

上层应用程序发送 IRP_MJ_CREATE 请求；

文件系统过滤驱动将请求包中的文件名以对文件实施保护时修改文件名的方式进行修改；

操作系统驱动建立文件句柄；

上层应用程序利用所述文件句柄发送 IRP_MJ_READ 请求读文件，文件系统过滤驱动进行解密；

或上层应用程序利用所述文件句柄发送 IRP_MJ_WRITE 请求修改文件，文件系统过滤驱动进行加密。

在上述对文件的保护过程中，加密文件的操作可以由文件系统过滤驱动完成，也可以由上层应用程序完成。

在上述对文件的保护过程中，修改文件名的操作是在初始文件名的扩展名中加入特征标识串。

在上述对文件的保护过程中，修改文件名的操作可以由文件系统过滤驱动完成，也可以由上层应用程序完成。

在上述对文件的保护过程中，当完成存储所述修改过文件名的加密文件后，可以将原有文件删除。

智能密钥装置参与所述文件保护、浏览或访问受保护文件的过程。在进行所述文件保护、浏览或访问受保护文件之前，系统检测智能密钥装置是否存在，如果不存在则不能进行文件保护、浏览或访问受保护文件的操作。

对文件的加密或解密操作由文件系统过滤驱动调用所述智能密

钥装置完成。

应用上述电子文件保护方法的文件保护系统包括：文件保护模块、文件创建模块、文件浏览模块、读文件模块、写文件模块和文件系统过滤驱动模块；

所述文件保护模块对文件进行加密和修改文件名；

所述文件创建模块接收文件创建请求、修改初始文件名并创建文件句柄；

所述文件浏览模块接收文件浏览请求、恢复文件名为初始文件名并以所述初始文件名显示文件；

所述读文件模块接收读文件请求，由文件系统过滤驱动模块根据文件句柄读取文件并解密；

所述写文件模块接收写文件请求，由文件系统过滤驱动模块加密文件并根据文件句柄将文件写入磁盘。

所述电子文件保护系统还包括由文件系统过滤驱动模块调用的智能密钥装置，对文件进行加密或解密操作。

所述电子文件保护系统还包括智能密钥装置监控模块，以监控系统中是否连接有智能密钥装置。

与现有技术相比，本发明的有益效果是：

（1）修改文件名保证了当用户误操作或非法访问文件时，系统不会自动恢复文件，避免文件被破坏；并且本发明不用建立文件列表，避免了列表丢失造成的麻烦；

（2）由于采用文件系统过滤驱动对文件进行处理，用户在访问和操作文件时不用另外对文件采取保护措施，方便了用户使用；

（3）采用智能密钥装置结合文件系统过滤驱动加密文件，使得文件具有更高的安全性。

附图说明

图 1 是用智能密钥装置对文件加密的流程图；

图 2 是用户访问受保护文件的流程图；

图 3 电子文件保护系统的结构示意图。

具体实施方式

现结合附图及实施例对本发明作进一步详细说明。

本发明对文件的保护机制是：利用现有的密钥机制结合文件系统过滤驱动，将受保护的文件加密，再修改文件密文的扩展名（具体实施方式以修改文件的扩展名为例，修改文件名的方法与修改文件扩展名的方法相同），最后通过文件系统驱动将文件写入计算机磁盘；当用户访问受保护的文件时，文件系统过滤驱动自动将文件名还原为初始文件名，再将文件解密，用户即可访问文件。下面对具体的文件保护、浏览、打开、读写过程一一阐述。

系统对文件进行保护的过程是：

步骤 101，用户通过上层应用程序选择想要保护的文件；

步骤 102，上层应用程序将所述文件利用加密算法加密，这里的加密算法可以采用 DES、3DES、AES 等现有加密算法，还可以由文件系统过滤驱动调用智能密钥装置实现对文件的加密；

步骤 103，上层应用程序将加密后的文件的扩展名按照一定规则进行修改，还可以由文件系统过滤驱动完成对所述扩展名的修改；

步骤 104，修改后的文件通过文件系统驱动写入计算机磁盘保存，同时可以将原有文件删除。

用户浏览文件的过程是：

步骤 201，用户在资源管理器中浏览文件列表，上层应用程序向下层发送 IPR_MJ_DIRECT_CONTROL 请求；

步骤 202，文件系统过滤驱动恢复 IRP 请求包中的文件扩展名为初始文件名，使得 Windows 系统在内存中显示的文件名为初始文件名；

步骤 203，用户在资源管理器中看到的文件列表是以初始文件名显示的文件列表。

用户打开受保护文件的过程是：

步骤 301，用户选择要打开的受保护文件；

步骤 302，上层应用程序发送 IRP_MJ_CREATE 请求，此时请求包中的文件名为初始文件名；

步骤 303，文件系统过滤驱动修改请求包中文件名，此修改方式与步骤 103 中的修改方式相同；

步骤 304，建立文件句柄，供修改文件或读取文件时使用。

用户读取文件的过程是：

步骤 401，操作系统根据步骤 304 中生成的文件句柄访问相应文件；

步骤 402，上层应用程序发送 IRP_MJ_READ 请求包，在磁盘上读取文件的密文；

步骤 403，根据步骤 102 中对文件的加密方法，采用相应的解密方法由文件系统过滤驱动调用智能密钥装置解密文件；

步骤 404，系统将解密的文件显示给用户。

用户修改文件的过程是：

步骤 501，文件系统根据步骤 304 中生成的文件句柄访问相应文件；

步骤 502，上层应用程序发送 IRP_MJ_WRITE 请求包，采用相应的加密方法由文件系统过滤驱动调用智能密钥装置对修改后的明文

文件进行加密；

步骤 503，系统将加密后的文件保存到计算机磁盘上。

上述过程中对文件的加密过程采用了文件系统过滤驱动调用智能密钥装置的方法，这样进一步提高了文件的安全性。此时，需要加入智能密钥装置监控程序检测是否有智能密钥装置连接到当前系统，方便文件系统过滤驱动与智能密钥装置的交互以及智能密钥装置与用户的交互。当智能密钥装置连接到计算机时，可以对文件进行加密或解密，当系统没有连接智能密钥装置时，用户将不能访问用智能密钥装置加密或解密的受保护文件。

参考图 1，用智能密钥装置对文件加密的步骤如下：

步骤 601，将智能密钥装置连接到计算机；

步骤 602，监控程序监控到有智能密钥装置插入，提示用户输入 PIN 码；

步骤 603，智能密钥装置验证用户输入的 PIN 码是否正确：如果正确进行步骤 605，否则进行步骤 604；

步骤 604，提示错误；

步骤 605，用户可以通过上层应用程序选择需要受保护的文件；

步骤 606，上层应用程序向文件系统驱动发送请求；

步骤 607，文件系统过滤驱动通过智能密钥装置的驱动程序调用智能密钥装置内部的密钥和算法；

步骤 608，文件系统过滤驱动利用智能密钥装置内置的密钥和算法加密文件；

步骤 609，文件系统过滤驱动修改文件的扩展名，例如 Word 文档的扩展名为.doc，则过滤驱动中规定将需要保护的 Word 文档的扩展名修改为.doc.***；

步骤 610，文件系统过滤驱动将修改过扩展名的密文文件发送至文件系统驱动，由文件系统驱动将其写入计算机磁盘保存；

步骤 611，文件系统过滤驱动程序将原有文件删除。

参考图 2，当满足有智能密钥装置连接到计算机的条件时，用户访问受保护文件的步骤如下：

步骤 701，将智能密钥装置连接到计算机；

步骤 702，监控程序监控到智能密钥装置插入，提示用户输入 PIN 码；

步骤 703，智能密钥装置验证用户输入的 PIN 码是否正确：如果正确进行步骤 705，否则进行步骤 704；

步骤 704，提示错误，用户不能利用智能密钥装置对文件进行解密；；

步骤 705，用户在资源管理器中浏览文件列表，选择需要保护的文件，上层应用程序发送 IRP_MJ_DIRECT_CONTROL 请求包；

步骤 706，文件系统过滤驱动恢复请求包中文件扩展名并在内存显示初始扩展名，用户通过资源管理器看到文件列表中的文件的扩展名与初始文件扩展名相同；

步骤 707，用户在资源管理器中选择要访问的受保护文件，上层应用发送 IRP_MJ_CREATE 请求，请求访问文件；

步骤 708，文件系统驱动读取磁盘上相应的文件并发送至文件系统过滤驱动；

步骤 709，文件系统过滤驱动恢复文件的扩展名；

步骤 710，操作系统建立文件句柄，供修改文件或读取文件时使用；

步骤 711，当用户进行读文件操作时，上层应用程序发送

IRP_READ 请求包，文件系统过滤驱动根据步骤 710 建立的文件句柄通过文件系统驱动程序读取磁盘上的相应文件；

步骤 712，文件系统过滤驱动程序通过智能密钥装置驱动程序调用智能密钥装置内的密钥和算法将文件数据解密，再将明文文件返回上层应用；

步骤 713，当用户进行写文件操作时，上层应用程序发送 IRP_WRITE 请求包，

步骤 714，文件系统过滤驱动通过智能密钥装置的驱动程序调用智能密钥装置内的密钥和算法将文件数据加密，文件系统过滤驱动根据步骤 710 建立的文件句柄将密文保存到计算机磁盘上。

图 3 是电子文件保护系统的结构示意图。参考图 3，其中包括：

文件保护模块 801——用于对首次进行保护操作的文件加密并修改文件名；

文件创建模块 802——用于接收文件系统核心层发送来的文件创建请求，由文件系统过滤驱动模块 806 修改 IRP 请求包中的文件名，并利用修改后的文件名创建文件句柄；

文件浏览模块 803——用于接收文件系统核心层发送来的文件浏览请求，由文件系统过滤驱动模块 806 恢复 IRP 请求包中的内存文件名，并在资源管理器中以初始文件名显示文件；

读文件模块 804——用于接收文件系统核心层发送来的读文件请求，由文件系统过滤驱动模块 806 根据文件句柄读取文件并解密文件；

写文件模块 805——用于接收文件系统核心层发送来的写文件请求，由文件系统过滤驱动模块 806 加密文件并根据文件句柄将文件写入磁盘；

监控模块 808，用于监控智能密钥装置 807 的拔插，以及与文件系统过滤驱动模块 806 进行交互，并提示用户进行相应的操作；

以及文件系统过滤驱动模块 806 和智能密钥装置 807。

其中，加密和解密文件操作由文件系统过滤驱动模块 806 调用智能密钥装置 807 实现；修改文件名的操作由文件系统过滤驱动模块 806 实现。

以上所述实施方式仅为本发明的优选实施例，本发明不限于上述实施例，对于本领域一般技术人员而言，在不背离本发明原理的前提下对它所做的任何显而易见的改动，都属于本发明的构思和所附权利要求的保护范围。

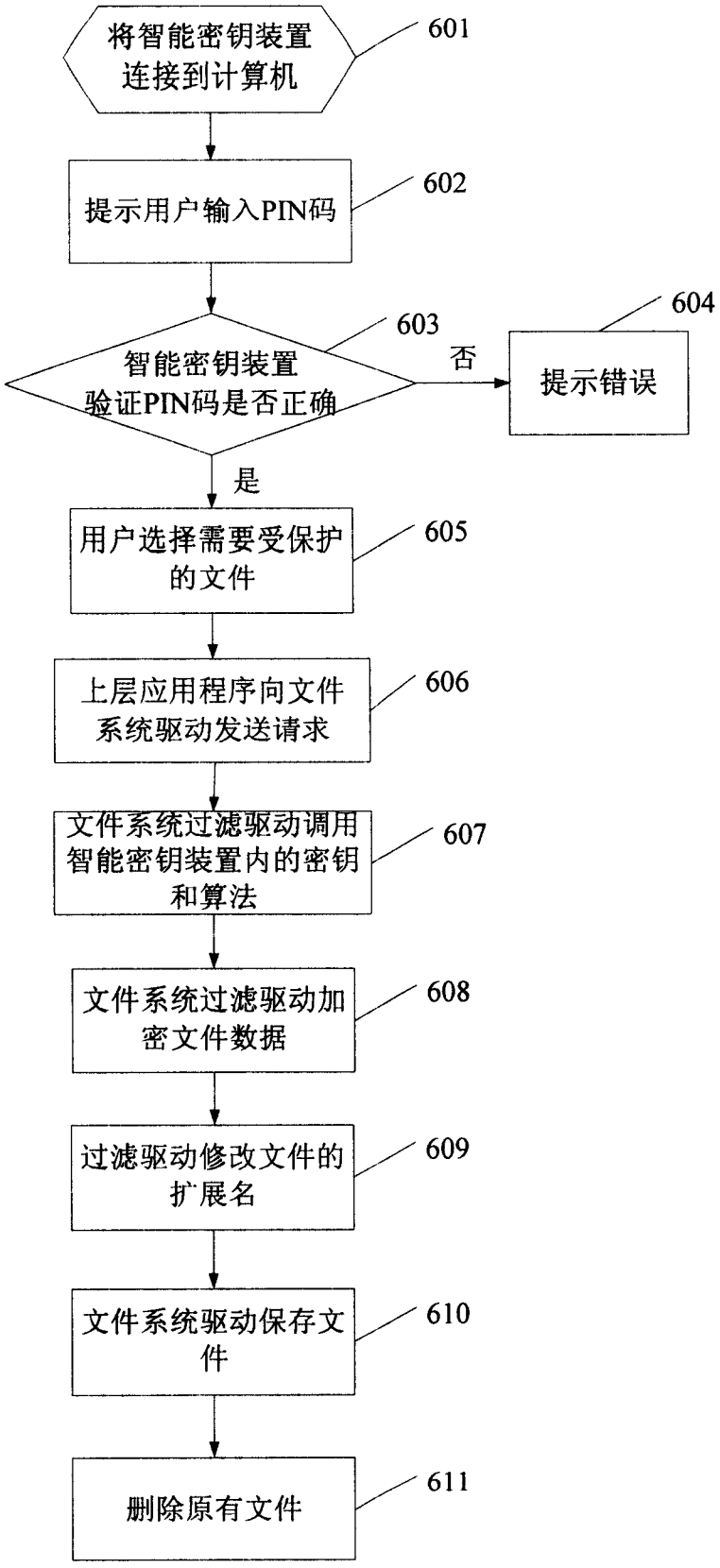

将智能密钥装置连接到计算机
601
提示用户输入PIN码
602
智能密钥装置验证PIN码是否正确
603
否
604
提示错误
是
用户选择需要受保护的文件
605
上层应用程序向文件系统驱动发送请求
606
文件系统过滤驱动调用智能密钥装置内的密钥和算法
607
文件系统过滤驱动加密文件数据
608
过滤驱动修改文件的扩展名
609
文件系统驱动保存文件
610
删除原有文件
611

图 1

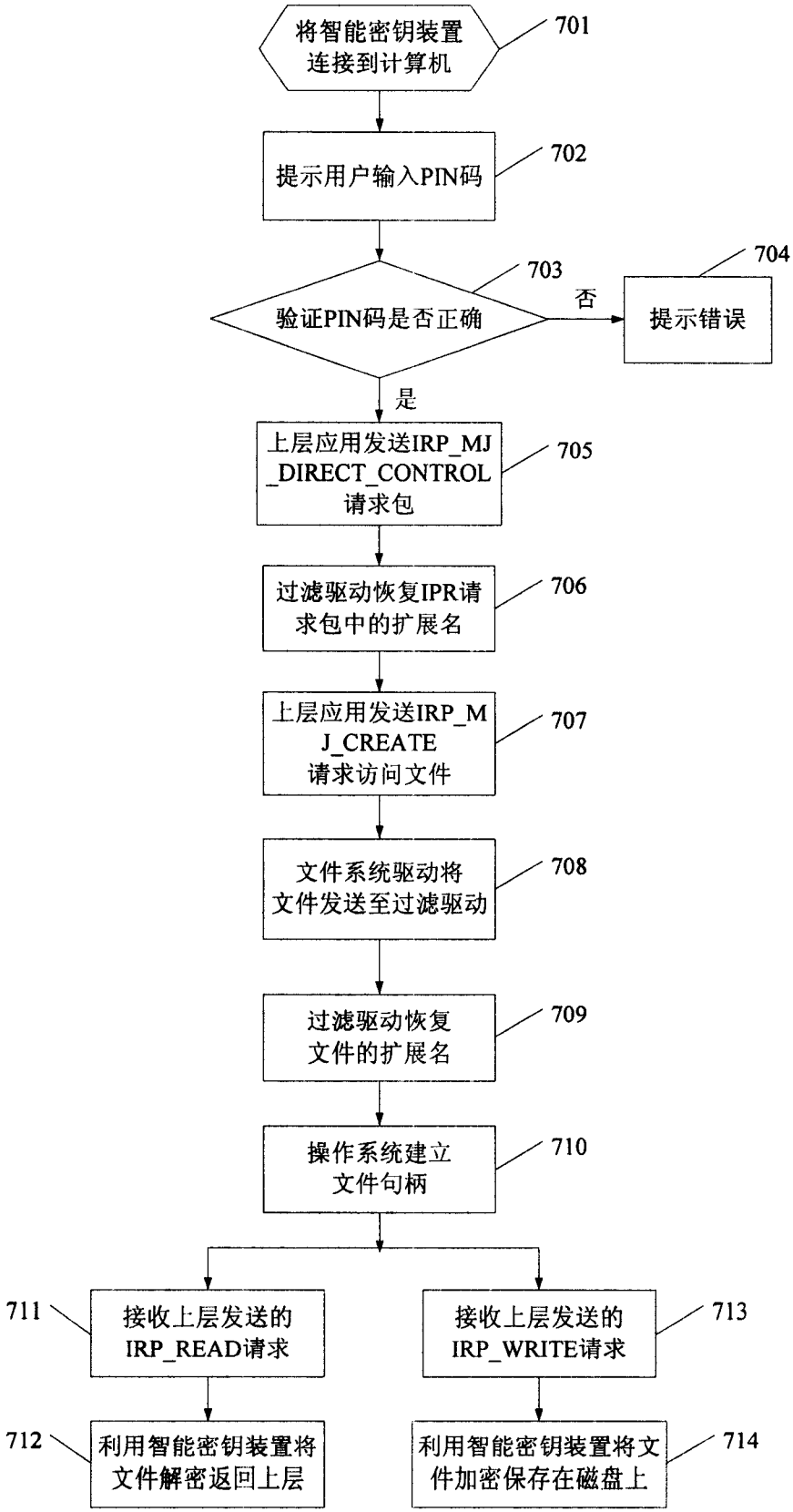

将智能密钥装置连接到计算机
701
提示用户输入PIN码
702
验证PIN码是否正确
703
否
提示错误
704
是
上层应用发送IRP_MJ_DIRECT_CONTROL请求包
705
过滤驱动恢复IPR请求包中的扩展名
706
上层应用发送IRP_MJ_CREATE请求访问文件
707
文件系统驱动将文件发送至过滤驱动
708
过滤驱动恢复文件的扩展名
709
操作系统建立文件句柄
710
接收上层发送的IRP_READ请求
711
利用智能密钥装置将文件解密返回上层
712
接收上层发送的IRP_WRITE请求
713
利用智能密钥装置将文件加密保存在磁盘上
714

图 2

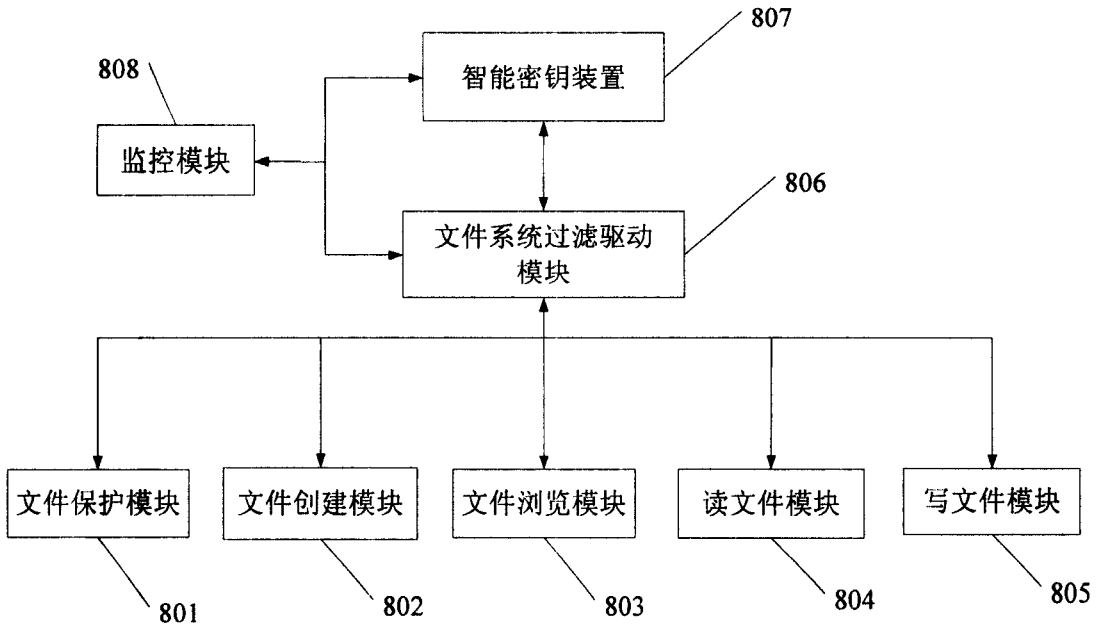

807
智能密钥装置
808
监控模块
806
文件系统过滤驱动模块
文件保护模块
文件创建模块
文件浏览模块
读文件模块
写文件模块
801
802
803
804
805

图 3