

[12] 发明专利申请公开说明书

[21] 申请号 00111656.8

[43] 公开日 2001 年 8 月 8 日

[11] 公开号 CN 1307283A

[22] 申请日 2000.2.3 [21] 申请号 00111656.8
 [71] 申请人 英业达集团(上海)电子技术有限公司
 地址 200233 上海市桂菁路 7 号
 [72] 发明人 邱全成 陈乃东

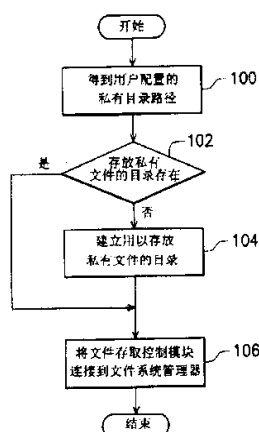
[74] 专利代理机构 上海专利商标事务所
 代理人 陈 亮

权利要求书 5 页 说明书 9 页 附图页数 5 页

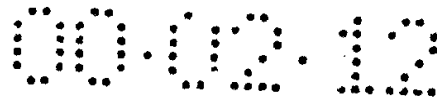
[54] 发明名称 多用户的安全性操作文件系统与方法

[57] 摘要

本发明提供一种多用户的安全性操作文件系统与方法。本多用户的安全性操作文件系统包括：文件系统管理器，用以管理系统内部的文件；及安全操作模块，使得上述多用户的安全性操作文件系统可以执行系统初始化模块、用户登入模块及文件存取控制模块，根据用户登入的用户名，产生私有文件目录路径，或存取其私有文件目录内的私有文件。如此，每个登录的用户可以拥有自己的私有文件，这些文件在其他用户看来是不存在的，以提供私有文件的安全性。

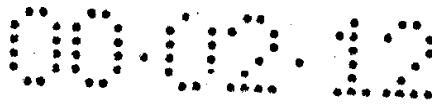


ISSN 1008-4274



权 利 要 求 书

1. 一种多用户的安全性操作文件系统，包括：
文件系统管理器，设置于电脑的操作系统中，用以管理系统内部的文件；及安全操作模块，嵌入至上述文件系统管理器中，使得上述多用户的安全性操作文件系统可以产生私有文件目录路径，或使该用户可以存取其私有文件目录内的私有文件。
2. 如权利要求 1 所述的安全性操作文件系统，其特征在于，上述安全操作模块存在于电脑的虚拟设备中。
3. 如权利要求 1 所述的安全性操作文件系统，其特征在于，上述安全操作模块还包括系统初始化模块，该系统初始化模块的执行系包括下列步骤：
得到用户配置的私有目录路径；
检查存放私有文件的目录；
建立用以存放和有文件的目录；及
将文件存取控制模块连接到文件系统管理器。
4. 如权利要求 1 所述的安全性操作文件系统，其特征在于，上述安全操作模块还包括用户登入模块，该用户登入模块的执行系包括下列步骤：
当用户进行登录时，系统会得到并且分析文件的存取请求；
接着判断传入的路径是否位于私有目录；
系统获取当前的用户名；
在路径中增加用户名后，做为系统文件系统视图的路径，然后进行至步骤；
直接使用传入的路径做为系统文件系统视图的路径；及
使用改变后的文件请求调用后续处理模块。
5. 如权利要求 1 所述的安全性操作文件系统，其特征在于，上述安全操作模块还包括文件存取控制模块，该文件存取控制模块的执行包括下列步骤：
首先，在用户登入时，得到登入的用户名；
接着判断用户对应的私有目录是否存在；及
为用户建立一私有目录，且目录名与用户名相同，然后结束。
6. 如权利要求 1 所述的安全性操作文件系统，其特征在于，上述安全操作模块是经由上述文件系统管理器的一介面嵌入至上述文件系统管理器中，以监视所有的文件操作。
7. 如权利要求 1 所述的安全性操作文件系统，其特征在于，上述和有文件目



录的路径系由私有目录路径及用户名合并而成。

8. 如权利要求 6 所述的安全性操作文件系统，其特征在于，上述介面用以使具体的文件系统可将本身的模块地址提供给上述文件系统管理器。

9. 一种多用户的安全性操作文件方法，包含下列步骤：

执行一文件系统管理器，该文件系统管理器是设置于电脑的操作系统中，用以管理系统内部的文件；及

执行一安全操作模块，该安全操作模块是嵌入至上述文件系统管理器中，使得上述多用户的安全性操作文件系统可以产生私有文件目录路径，或使该用户可以存取其私有文件目录内的私有文件。

10. 如权利要求 9 所述的安全性操作文件方法，其特征在于，上述安全操作模块存在于电脑的虚拟设备中。

11. 如权利要求 9 所述的安全性操作文件方法，其特征在于，上述安全操作模块还包括系统初始化模块，该系统初始化模块的执行包括下列步骤：

首先得到用户配置的私有目录路径；

检查存放私有文件的目录；

建立用以存放私有文件的目录；及

将文件存取控制模块连接到文件系统管理器。

12. 如权利要求 9 所述的安全性操作文件方法，其特征在于，上述安全操作模块还包括用户登入模块，该用户登入模块的执行包括下列步骤：

当用户进行登录时，系统会得到并且分析文件的存取请求；

接着判断传入的路径是否位于私有目录；

系统获取当前的用户名；

在路径中增加用户名后，做为系统文件系统视图的路径；

直接使用传入的路径做为系统文件系统视图的路径；及

使用改变后的文件请求调用后续处理模块。

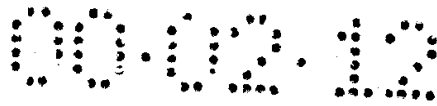
13. 如权利要求 9 所述的安全性操作文件方法，其特征在于，上述安全操作模块还包括文件存取控制模块，该文件存取控制模块的执行包括下列步骤：

首先，在用户登入时，得到登入的用户名；

接着判断用户对应的私有目录是否存在；及

为用户建立一私有目录，且目录名与用户名相同，然后结束。

14. 如权利要求 9 所述的安全性操作文件方法，其特征在于，上述安全操作模



块经由上述文件系统管理器的一介面嵌入至上述文件系统管理器中，以监视所有的文件操作。

15. 如权利要求 9 所述的安全性操作文件方法，其特征在于，上述私有文件目录的路径是由私有目录路径及用户名合并而成。

16. 如权利要求 14 所述的安全性操作文件方法，其特征在于，上述介面用以使具体的文件系统可将本身的模块地址提供给上述文件系统管理器。

17. 一种多用户的安全性操作文件系统，包括：

文件系统管理器，设置于电脑的操作系统中，用以管理系统内部的文件；及安全操作模块，嵌入至上述文件系统管理器中，使得上述多用户的安全性操作文件系统可以依序执行系统初始化模块、用户登入模块及文件存取控制模块，籍以根据用户登入的用户名，产生私有文件目录路径，或使该用户可以存取其私有文件目录内的私有文件。

18. 如权利要求 17 所述的安全性操作文件系统，其特征在于，上述安全操作模块存在于电脑的虚拟设备中。

19. 如权利要求 17 所述的安全性操作文件系统，其特征在于，上述系统初始化模块的执行包括下列步骤：

得到用户配置的私有目录路径；

检查存放私有文件的目录；

建立用以存放私有文件的目录；及

将文件存取控制模块连接到文件系统管理器。

20. 如权利要求 17 所述的安全性操作文件系统，其特征在于，上述用户登入模块的执行包括下列步骤：

当用户进行登录时，系统会得到并且分析文件的存取请求；

接着判断传入的路径是否位于私有目录；

系统获取当前的用户名；

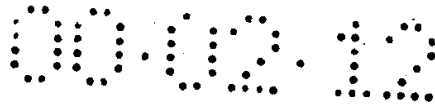
在路径中增加用户名后，做为系统文件系统视图的路径，然后进行至步骤；

直接使用传入的路径做为系统文件系统视图的路径；及

使用改变后的文件请求调用后续处理模块。

21. 如权利要求 17 所述的安全性操作文件系统，其特征在于，上述文件存取控制模块的执行包括下列步骤：

首先，在用户登入时，得到登入的用户名；



接着判断用户对应的私有目录是否存在：及

为用户建立一私有目录，且目录名与用户名相同，然后结束。

22. 如权利要求 17 所述的安全性操作文件系统，其特征在于，上述安全操作模块是经由上述文件系统管理器的一介面嵌入至上述文件系统管理器中，以监视所有的文件操作。

23. 如权利要求 17 所述的安全性操作文件系统，其特征在于，上述私有文件目录的路径系由私有目录路径及用户名合并而成。

24. 如权利要求 22 所述的安全性操作文件系统，其特征在于，上述介面用以使具体的文件系统可将本身的模块地址提供给上述文件系统管理器。

25. 一种多用户的安全性操作文件方法，包含下列步骤：

执行一文件系统管理器，该文件系统管理器是设置于电脑的操作系统中，用以管理系统内部的文件；及

执行一安全操作模块，该安全操作模块是嵌入至上述文件系统管理器中，使得上述多用户的安全性操作文件系统可以依序执行系统初始化模块、用户登入模块及文件存取控制模块，藉以根据用户登入的用户名，产生私有文件目录路径，或使该用户可以存取其私有文件目录内的私有文件。

26. 如权利要求 25 所述的安全性操作文件方法，其特征在于，上述安全操作模块存在于电脑的虚拟设备中。

27. 如权利要求 25 所述的安全性操作文件方法，其特征在于，上述系统初始化模块的执行包括下列步骤：

首先得到用户配置的私有目录路径；

检查存放私有文件的目录；

建立用以存放私有文件的目录；及

将文件存取控制模块连接到文件系统管理器。

28. 如权利要求 25 所述的安全性操作文件方法，其特征在于，上述用户登入模块的执行包括下列步骤：

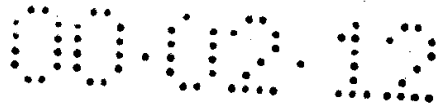
当用户进行登录时，系统会得到并且分析文件的存取请求；

接着判断传入的路径是否位于私有目录；

系统获取当前的用户名；

在路径中增加用户名后，做为系统文件系统视图的路径；

直接使用传入的路径做为系统文件系统视图的路径；及



使用改变后的文件请求调用后续处理模块。

29. 如权利要求 25 所述的安全性操作文件方法，其特征在于，上述文件存取控制模块的执行包括下列步骤：

首先，在用户登入时，得到登入的用户名；

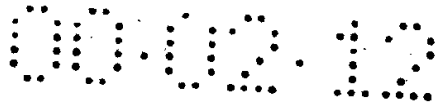
接着判断用户对应的私有目录：及

为用户建立一私有目录，且目录名与用户名相同，然后结束。

30. 如权利要求 25 所述的安全性操作文件方法，其特征在于，上述安全操作模块是经由上述文件系统管理器的一介面嵌入至上述文件系统管理器中，以监视所有的文件操作。

31. 如权利要求 25 所述的安全性操作文件方法，其特征在于，上述和有文件目录的路径是由私有目录路径及用户名合并而成。

32. 如权利要求 32 所述的安全性操作文件方法，其特征在于，上述介面用以使具体的文件系统可将本身的模块地址提供给上述文件系统管理器。



说明书

多用户的安全性操作文件系统与方法

本发明涉及一种多用户的安全性操作文件系统与方法。

由于 Windows 操作系统的单用户设计，系统中所有的文件都是共享的，不同的用户登录到系统中，可以存取本地硬盘上的所有文件。请参阅图 1，由于应用程序 20 可直接存取整个文件系统管理器 10，所以任何使用者通过应用程序，均可存取文件系统管理器 10 中的所有文件。然而，在多人使用一台电脑的情况下，完全共享的文件系统，由于所有文件均可被各使用者自由存取，反而会给使用者带来不便。目前，多个用户同时使用一台电脑的装置已经逐渐成熟，在这样的系统对文件安全性操作的要求相当高，不过单靠 Windows 系统本身并无法解决这个问题。

本发明针对 Windows 系统的上述缺点，提出一种多用户的安全性操作文件系统及方法，通过对 Windows 文件系统的增强，提供了基本的文件安全性操作功能。不同的用户可以利用 Windows 的登录机制建立用户名称等信息。每个登录的用户可以有自己的私有文件，这些文件在其他用户看来是不存在的，籍以提供私有文件的安全性。

为了进一步说明本发明的结构、方法及特点，兹配合附图说明实施例如下，其中：

图 1 示出了已知 Windows 中的文件系统的结构图；

图 2 示出了具有多用户安全性操作文件系统的文件系统结构图；

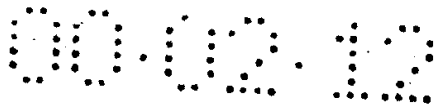
图 3 示出了本发明的多用户安全性操作文件系统及执行方法的初始化流程图；

图 4 示出了本发明的多用户安全性操作文件系统及执行方法的文件存取控制流程图；

图 5 示出了本发明的多用户安全性操作文件系统及执行方法的用户登录流程图；

图 6 示出了本发明的统文件系统视图与用户文件系统视图间的转换示意图。

请参阅图 2，与前述已知的 Windows 的文件系统不同的，本发明主要是在原有的结构中嵌入带有多用户的安全性操作文件系统的文件系统管理器安全操作模块 35，使用者通过应用程序 40 欲存取文件系统管理器 30 内的文件时，必须先经由上述文件系统管理器安全操作模块 35，决定其可存取的路径，然后系统再将该路径显



示给使用者。至于该使用者不可存取的路径，系统并不会显示给该使用者。

本发明的核心部分存在于一个虚拟设备中，虚拟设备是一种 Windows 的系统模块，开发人员可以利用 32 位的 C 语言或组合语言的编译程序，直接完成所需的虚拟设备，当然也可以利用硬件或者硬件与软件的组合来实现这种虚拟设备。在 Windows 系统启动的过程中，VMM(虚拟机管理器)会把所有用到的虚拟设备装入内存，并调用其初始化过程。在所有的虚拟设备初始化完成前，系统不会调用任何用户程序，所以用户不可能利用本系统装入前的时间进行非法存取。当本虚拟设备载入至系统后，将一直存在于系统中，直到系统结束。在本系统的虚拟设备的初始化过程中，会通过文件系统管理器(IFSMGR, Installable File System Manager)的一个介面，将多用户安全文件系统嵌入到整个文件系统中，从而形成一个新的带有安全功能的文件系统。这个介面具体由文件系统管理器(IFSMGR)提供，介面的名称是“IFSMgr_Install File System Api Hook”。这个介面本身是供给具体的文件系统设备，使具体的文件系统能够将自己的模块地址提供给文件管理器。在本发明中利用这个介面将多用户文件系统的文件系统管理器安全操作模块提供给文件管理器，从而达到嵌入到文件系统管理器中并实现监视所有的文件操作的目的。多用户的安全性操作文件系统就是利用这个安全操作模块对系统中的文件操作进行监控，实现对系统中的文件操作进行管理，使每个用户只能存取到属于自己的文件及目录。

上述介面“IFSMgr_Install File System API Hook”定义如下：

```
IFSMgr_Install File System Api Hook(pIFS File Hook Func Hook Func);
```

其中，HookFunc 是功能回调函数，其定义为：

```
tyPedef int(*pIFS File Hook Func)(pIFSFunc pfn, int, fn, int Drive,  
int ResType, int CodePage, pirq pir);
```

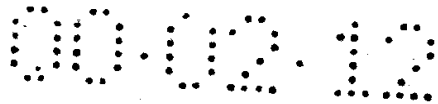
上述 pfn 是回调链的下一个连接，fn 是功能号，Driver 是逻辑盘符，ResType 是所操作的资源类型，CodePage 是代码页，pir 是功能参数。

在本系统中，要对功能参数中的路径进行修改，然后用修改后的 pir 功能参数调用回调链中的下一个函数。

实施例 1

本发明的多用户安全性操作文件系统包括有系统初始化、用户登入及文件存取等三个模块。

首先说明上述多用户安全性操作文件系统的虚拟设备初始化模块，此一部分是



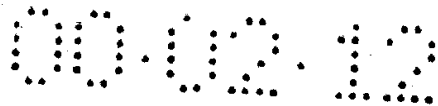
在 Windows 9x 系统引导时运作，其主要是用以判断系统私有目录环境是否完整，若发现有不完整的地方，就要进行对应的恢复工作。只有在首次安装或用户重新安装时，系统私有目录环境不会不完整。当系统检测到私有目录不存在的时候，就必须加以重新建立。重新建立私有目录不会影响到系统的安全性，因为这种情况只有在系统安装时才会发生，而在系统安装时所有用户都还没有建立私有文件，所以也不至于影响到私有文件的安全性。

请参阅图 3，本发明的多用户的安全性操作文件系统的虚拟设备初始化流程系包括下列步骤：(i) 步骤 100，首先得到用户配置的私有目录路径；(ii) 步骤 102，接着检查存放私有文件的目录是否存在，若不存在则进行下一步骤，否则进行至步骤 106；(iii) 步骤 104，建立用以存放私有文件的目录，然后进行下一步骤；(iv) 步骤 106，将文件存取控制模块连接到文件系统管理器。

在上述流程中，存放私有文件的目录的名称与位置是在系统安装时，由安装者指定的，等系统启动后，这个目录会成为不可见，也就是说，非该目录的使用者将完全无法看到该目录的存在。

在使用前述的方法监视系统中文件的存取操作后，对所有系统中的文件进行存取时，都要经过这个模块。这个模块首先检查用户存取的文件是否存在于私有目录中。因为所有用户的私有文件都存放在指定的位置，所以只要判断被存取的文件的路径，就可以检测出用户所存取的文件是否私有文件。若用户使用的不是私有文件，则本系统只需直接进行文件操作。若用户操作的是私有文件，则必须把用户指定的文件路径转变成实际文件操作所需要的路径，其方法是将用户名加到用户指定的路径上，也就是将用户名加入到私有文件目录和其他子目录间。例如，私有文件目录为“C: \Personal”，用户 John 传入的文件路径为“C: \Personal \Sub1 \P101.bmp”，转换时就要将用户名“John”加到“C: \Personal”与“Sub1 \Pic1.bmp”之间，而形成“C: \Personal \John \Sub1 \Pic. bmp”。

请参阅图 4，本发明的多用户的安全性操作文件系统的文件存取控制流程包括下列步骤：(i) 首先，步骤 200，当用户进行登录时，系统会得到并且分析文件的存取请求；(ii) 接着，在步骤 202 中，判断传入的路径是否位于私有目录，若是则进行下一步骤，否则进行步骤 208；(iii) 步骤 204，系统获取当前的用户名，进行下一步骤；(iv) 步骤 206，在路径中增加用户名后，做为系统文件系统视图的路径，然后进行至步骤 210；(v) 步骤 208，直接使用传入的路径做为系统文件系统视图的路径；(vi) 步骤 210，使用改变后的文件请求调用后续处理模块，然后结束。



多用户的安全性操作文件系统的用户登入部分，主要实现对新用户首次登入时的文件系统环境的建立。要判断一个用户是否新用户，只需查询该用户的私有目录是否已经建立。若还没有建立，就表示该用户为首次登入。此时必须为该用户建立私有文件目录，而这个私有文件目录的路径就是私有目录路径加上用户名。若经查询，私有文件目录已经存在，则这个部分就可以不做任何操作，直接退出。

请参阅图 5，本发明的多用户的安全性操作文件系统的用户登录流程系包括下列步骤：(i)首先，在步骤 300 中，当用户登入时，得到登入的用户名；(ii)步骤 302，判断用户对应的私有目录是否存在，若是则结束，否则进行下一步骤；(iii)步骤 304，为用户建立一私有目录，且目录名与用户名相同，然后结束。

多用户文件系统利用了 Windows 的用户登录的特性来确定用户名。所有使用 Windows 系统的人都要进行系统登录，以确定用户名。因为在普通的 Windows 系统中用户名并没有任何特殊的意义，所以一般情况下，每个使用系统的用户都使用同一个用户名登入系统。但在多用户安全操作文件系统中，用户名涉及到用户可以存取的文件，这使得用户名成为一个关键，所以当使用多用户安全操作文件系统时，不同用户必须以不同的用户名登入系统。

本系统为每个用户提供了本地存取的安全性，只要用户以不同的用户名登入系统，就可以安全地在系统中存放自己的私有文件，而不必担心其他用户会查看或毁坏私有的文件。用户所要做的就是将私有文件存放到指定的私有文件目录中。在上述实施例中是使用“C: \Personal”来表示私有文件目录，用户不但可以在该目录中存放文件，还可以在其下建立子目录。本系统通过文件系统映射的方法，使每个用户只能见到私有文件目录中自己的文件。经由此种方法，用户私有文件的安全性可以得到保障，与传统设定文件存取权限的方法不同，此种方法直接映射文件系统视图。对于一般的用户来说，设定文件存取权限的操作，不但复杂且容易出错。而使用本发明所描述的文件系统视图法，不但使用简便，且安全性更佳。用户只须知道私有文件目录的位置，就可以把需要保护的文件存于其中。

多用户文件系统是根据当前(current)用户名来识别不同的用户。当前用户名可以直接从系统中得到。所有的用户的私有文件都保存在一个公用的私有目录内，预设的目录为 C: \PERSONAL。每个用户都可以操作这个目录。但是不同的用户所看到的目录中的内容是不同的。每个登录用户都只能在 PERSONAL 目录中看到属于自己的文件在多用户的安全性操作文件系统中使用了文件系统视图的概念，所谓文件系统视图就是从某个角度看到的文件系统结构，包括用户的文件系统视图和系统

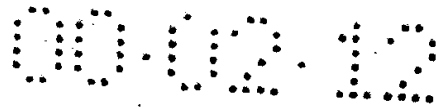


的文件系统视图。用户的文件系统视图就是这个用户所看到的本地的文件系统及网络映射过来的文件系统，也就是这个用户所有可以存取到的文件和目录(文件夹)。在普通的 Windows 系统中，使用不同用户名登入系统的用户有不同的文件系统视图。文件系统视图就是从操作系统本身的角度去看文件系统，这包括了所有从用户角度可看到的文件和不可见的文件、用户的文件和系统的文件等所有的文件。

在 Windows 中，文件系统管理器 IFSMGR 管理系统级的文件系统，即 IFSMGR 对系统文件系统视图进行操作。在普通的 Windows 中，所有用户的文件系统视图和系统的文件系统视图是相同的。在带有多用户的安全性操作文件系统的 Windows 中，由于多用户的安全性操作文件系统的作用，用户的文件系统视图不再和系统的文件系统视图相同，并且不同用户的文件系统视图也不相同。如此，用户的私有文件就可以得到保护。本发明的多用户安全性操作文件系统的功用就是把系统的文件系统视图转变为用户的文件系统视图。

请参阅图 6，其示出了多用户的安全性操作文件系统的系统文件系统视图和用户文件系统视图间转变的示意图。以图 6 的示意图为例，可以发现用户 Jack 和用户 John 在 C: \PERSONAL 中所看到文件是不同的，而在系统文件系统视图 50 中包括了所有用户的文件，例如用户 Jack 的文件系统视图 60 和用户 John 的文件系统视图 70，每个用户的文件存放在不同的目录中。因此，不同的用户即使有相同文件名的私有文件，其内容也可以是不同的。在用户的文件系统视图中只有相对应的属于该用户的文件。

在把用户文件系统视图转换到系统文件系统视图的过程就是在私有目录名和其他路径间加上用户名。例如，用户 Jack 要存取 C: \PERSONAL \text1。将用户名“Jack”插入到私有文件目录名“C: \PERSONAL”和其他路径“\text1”之间。经多用户的安全性操作文件系统处理后，传给系统的路径变为“C: \PERSONAL \ Jack \text1”。所以，用户对 C: \PERSONAL \text1 的操作，实际上被转移到了系统文件系统视图的 C: \PERSONAL \ Jack \text1 上进行操作。需要注意的是用户 John 的私有目录文件操作都是在私有文件目录后加上 John，形成 C: \PERSONAL \ John \ …，而根本无法形成 C: \PERSONAL \ Jack \ … 的路径，从而无法存取 Jack 的私有文件。对于非私有目录下的文件，多用户的安全性操作文件系统直接把路径传递到文件系统管理器，所以所有用户都可以存取到。由此可见在多用户的安全性操作文件系统中所有位于私有目录中的目录和文件都无法被其他用户存取到。即使两个用户具有相同名称的文件或子目录，其文件或子目录内容也会随着当前用户的



不同而不同。

本发明目前可应用在 Windows 多用户系统中，Windows 的多用户系统允许两个或两个以上的用户同时使用一台电脑，如此当两个用户使用不同的用户名登录到系统中时，其均仅能存取自己的私有文件，但相互间不能看到对方的私有文件。本发明的系统在单机运行的 Windows 系统中也可以使用，以提供用户存取私有文件的空间。

实施例 2

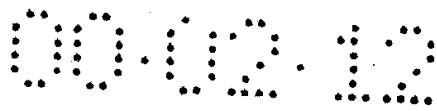
本发明的多用户安全性操作文件方法包括有执行系统初始化、执行用户登入及执行文件存取等三个模块。

首先说明上述多用户安全性操作文件方法的执行虚拟设备初始化模块，此一部分是在 Windows 9x 系统引导时运作，其主要是用以判断系统私有目录环境是否完整，若发现有不完整的地方，就要进行对应的恢复工作。只有在首次安装或用户重新安装时，系统私有目录环境不会不完整。当系统检测到私有目录不存在的时候，就必须加以重新建立。重新建立私有目录不会影响到系统的安全性，因为这种情况只有在系统安装时才会发生，而在系统安装时所有用户都还没有建立私有文件，所以也不至于影响到私有文件的安全性。

请参阅图 3，本发明的多用户的安全性操作文件方法的执行虚拟设备初始化流程包括下列步骤：(i) 步骤 100，首先得到用户配置的私有目录路径；(ii) 步骤 102，接着检查存放私有文件的目录是否存在，若不存在则进行下一步骤，否则进行至步骤 106；(iii) 步骤 104，建立用以存放私有文件的目录，然后进行下一步骤；(iv) 步骤 106，将文件存取控制模块连接到文件系统管理器。

在上述流程中，存放私有文件的目录的名称与位置是在系统安装时，由安装者指定的，等系统启动后，这个目录会成为不可见，也就是说，非该目录的使用者将完全无法看到该目录的存在。

在使用前述的方法监视系统中文件的存取操作后，对所有系统中的文件进行存取时，都要经过这个模块。这个模块首先检查用户存取的文件是否存在于私有目录中。因为所有用户的私有文件都存放在指定的位置，所以只要判断被存取的文件的路径，就可以检测出用户所存取的文件是否是私有文件。若用户使用的不是私有文件，则本系统只需直接进行文件操作。若用户操作的是私有文件，则必须把用户指定的文件路径转变成实际文件操作所需要的路径，其方法是将用户名加到用户指定的路径上，也就是将用户名加入到私有文件目录和其他子目录间。例如，私有文件



目录为“C: \Personal”，用户 John 传入的文件路径为“C: \Personal \Sub1 \Pic1. bmp”，转换时就要将用户名“John”加到“C: \Personal”与“Sub1 \Pic1. bmp”之间，而形成“C: \Personal \John \Sub1 \Pic1. bmp”。

请参阅图 4，本发明的多用户的安全性操作文件方法的文件存取控制流程包括下列步骤：(i) 首先，步骤 200，当用户进行登录时，系统会得到并且分析文件的存取请求；(ii) 接着，在步骤 202 中，判断传入的路径是否位于私有目录，若是则进行下一步骤，否则进行步骤 208；(iii) 步骤 204，系统获取当前的用户名，进行下一步骤；(iv) 步骤 206，在路径中增加用户名后，做为系统文件系统视图的路径，然后进行至步骤 210；(v) 步骤 208，直接使用传入的路径做为系统文件系统视图的路径；(vi) 步骤 210，使用改变后的文件请求调用后续处理模块，然后结束。

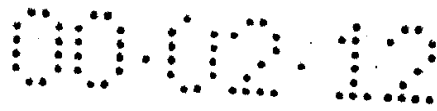
多用户的安全性操作文件方法的执行用户登入部分，主要实现对新用户首次登入时的文件系统环境的建立。要判断一个用户是否新用户，只需查询该用户的私有目录是否已经建立。若还没有建立，就表示该用户为首次登入。

此时必须为该用户建立私有文件目录，而这个私有文件目录的路径就是私有目录路径加上用户名。若经查询和有文件目录已经存在，则这个部分就可以不做任何操作，直接退出。

请参阅图 5，本发明的的多用户的安全性操作文件方法的执行用户登录流程系包括下列步骤：(i) 首先，在步骤 300 中，当用户登入时，得到登入的用户名；(ii) 步骤 302，判断用户对应的私有目录是否存在，若是则结束，否则进行下一步骤；(iii) 步骤 304，为用户建立一私有目录，且目录名与用户名相同，然后结束。

多用户文件系统利用了 Windows 的用户登录的特性来确定用户名。所有使用 Windows 系统的人都要进行系统登录，以确定用户名。因为在普通的 Windows 系统中用户名并没有任何特殊的意义，所以一般情况下，每个使用系统的用户都使用同一个用户名登入系统。但在多用户安全操作文件系统中，用户名涉及到用户可以存取的文件，这使得用户名成为一个关键，所以当使用多用户安全操作文件系统时，不同用户必须以不同的用户名登入系统。

本方法为每个用户提供了本地存取的安全性，只要用户以不同的用户名登入系统，就可以安全地在系统中存放自己的私有文件，而不必担心其他用户会查看或毁坏和有的文件。用户所要做的就是将私有文件存放到指定的私有文件目录中。在上述实施例中系使用“C: \Personal”来表示私有文件目录，用户不但可以在该目录中存放文件，还可以在其下建立子目录。本方法通过文件系统映射的方法，使每



个用户只能见到私有文件目录中自己的文件。经由此种方法，用户私有文件的安全性可以得到保障，与传统设定文件存取权限的方法不同，此种方法直接映射文件系统视图。对于一般的用户来说，设定文件存取权限的操作，不但复杂且容易出错。而使用本发明所描述的文件系统视图法，不但使用简便，且安全性更佳。用户只须知道私有文件目录的位置，就可以把需要保护的文件存于其中。

多用户文件系统是根据当前的(current)用户名来识别不同的用户。当前用户名可以直接从系统中得到。所有的用户的私有文件都保存在一个公用的私有目录内，预设的目录为 C: \PERSONAL。每个用户都可以操作这个目录，但是不同的用户所看到的目录中的内容是不同的。每个登录用户都只能在 PERSONAL 目录中看到属于自己的文件在多用户的安全性操作文件方法中使用了文件系统视图的概念，所谓文件系统视图就是从某个角度看到的文件系统结构，包括用户的文件系统视图和系统的文件系统视图。用户的文件系统视图就是这个用户所看到的本地的文件系统及网路映射过来的文件系统，也就是这个用户所有可以存取到的文件和目录(文件夹)。在普通的 Windows 系统中，使用不同用户名登入系统的用户有不同的文件系统视图。文件系统视图就是从操作系统本身的角度去看文件系统，这包括了所有从用户角度可看到的文件和不可见的文件、用户的文件和系统的文件等所有的文件。

在 Windows 中，文件系统管理器 IFMGR 管理系统级的文件系统，即 IFMGR 对系统文件系统视图进行操作。在普通的 Windows 中，所有用户的文件系统视图和系统的文件系统视图是相同的。在带有多用户的安全性操作文件系统的 Windows 中，由于多用户的安全性操作文件方法的作用，用户的文件系统视图不再和系统的文件系统视图相同，并且不同用户的文件系统视图也不相同。如此，用户的私有文件就可以得到保护。本发明的多用户安全性操作文件系统的功用就是把系统的文件系统视图转变为用户的文件系统视图。

请参阅图 6，其示出了多用户的安全性操作文件方法的系统文件系统视图和用户文件系统视图间转变的示意图。以图 6 的示意图为例，可以发现用户 Jack 和用户 John 在 C: \PERSONAL 中所看到文件是不同的，而在系统文件系统视图 50 中包括了所有用户的文件，例如用户 Jack 的文件系统视图 60 和用户 John 的文件系统视图 70，每个用户的文件存放在不同的目录中。因此，不同的用户即使有相同文件名的私有文件，其内容也可以是不同的。在用户的文件系统视图中只有相对应的属于该用户的文件在把用户文件系统视图转换到系统文件系统视图的过程就是在私有目录名和其他路径间加上用户名。例如，用户 Jack 要存取 C: \PERSONAL \

text1。将用户名“Jack”插入到私有文件目录名“C: \PERSONAL”和其他路径“\text1”之间。经多用户的安全性操作文件方法处理后，传给系统的路径变为“C: \PERSONAL\Jack\text1”。所以，用户对 C: \PERSONAL\text1 的操作，实际上被转移到了系统文件系统视图的 C: \PERSONAL\Jack\text1 上进行操作。需要注意的是用户 John 的私有目录文件操作都是在私有文件目录后加上 John，形成 C: \PERSONAL\John\…，而根本无法形成 C: \PERSONAL\Jack\…的路径，从而无法存取 Jack 的私有文件。对于非私有目录下的文件，多用户的安全性操作文件系统直接把路径传递到文件系统管理器，所以所有用户都可以存取到。由此可见在多用户的安全性操作文件方法中所有位于私有目录中的目录和文件都无法被其他用户存取到。即使两个用户具有相同名称的文件或子目录，其文件或子目录内容也会随着当前用户的不同而不同。

本发明目前可应用在 Windows 多用户系统中，Windows 的多用户系统允许两个或两个以上的用户同时使用一台电脑，如此当两个用户使用不同的用户名登录到系统中时其均仅能存取自己的私有文件，但相互间不能看到对方的私有文件。本发明的系统在单机运行的 Windows 系统中也可以使用，以提供用户存取私有文件的空间。

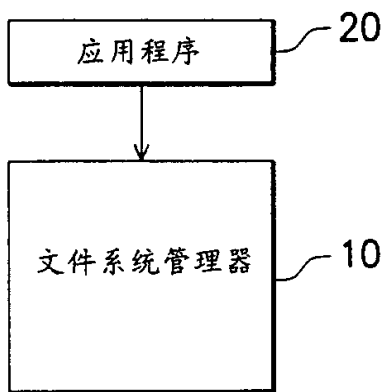


图 1

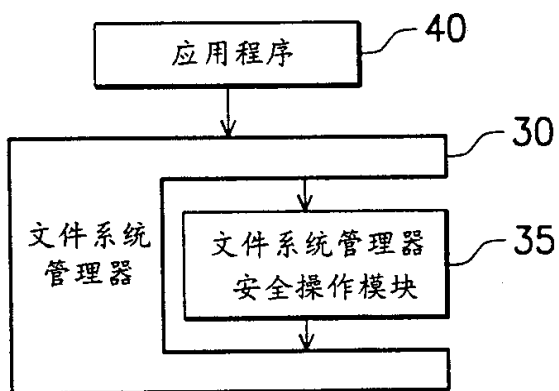


图 2

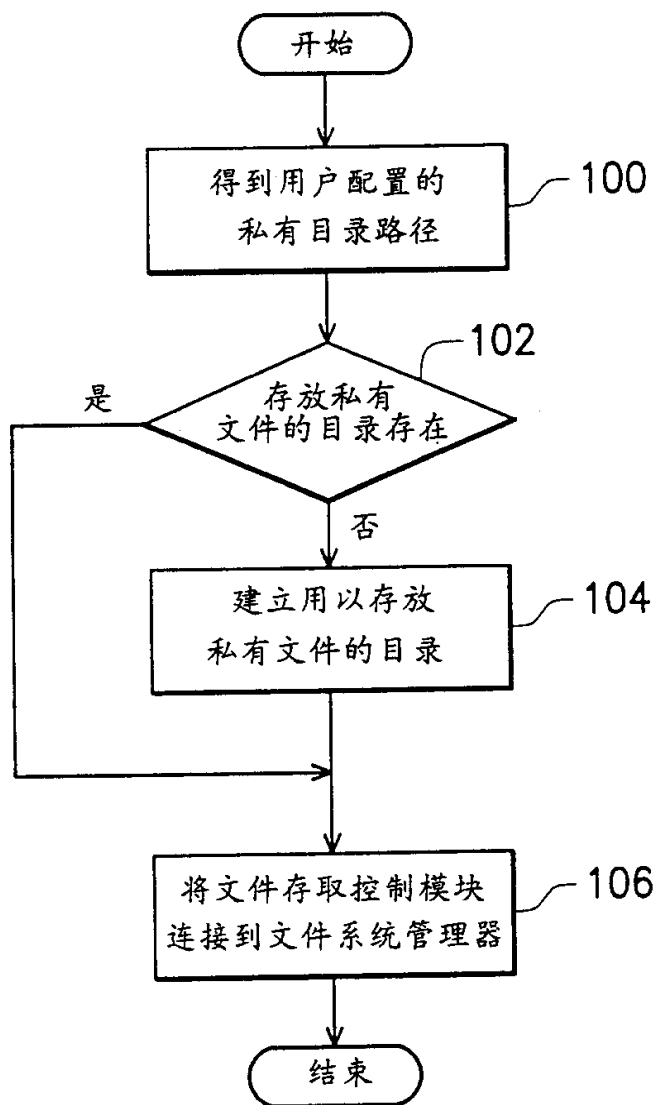


图 3

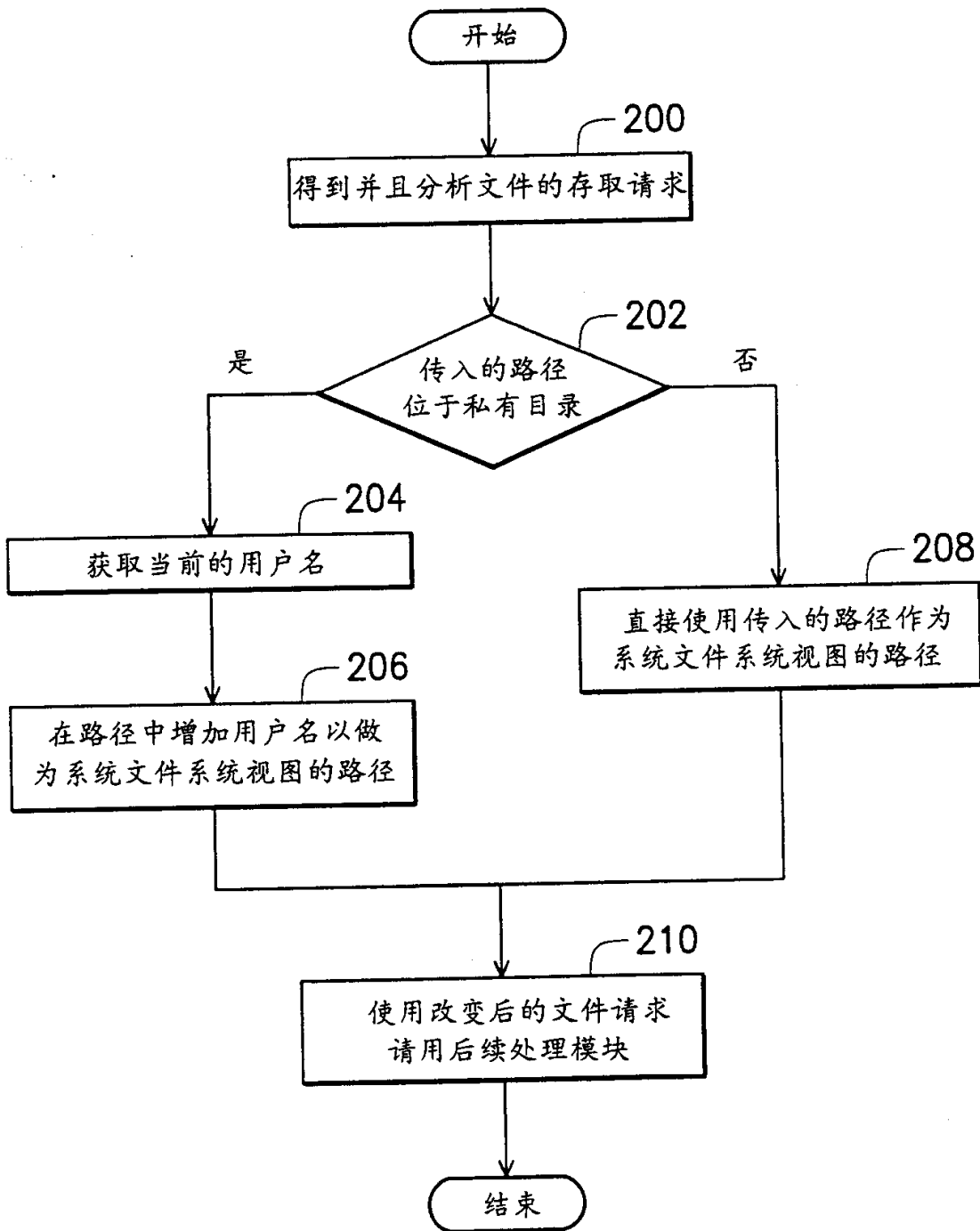


图 4

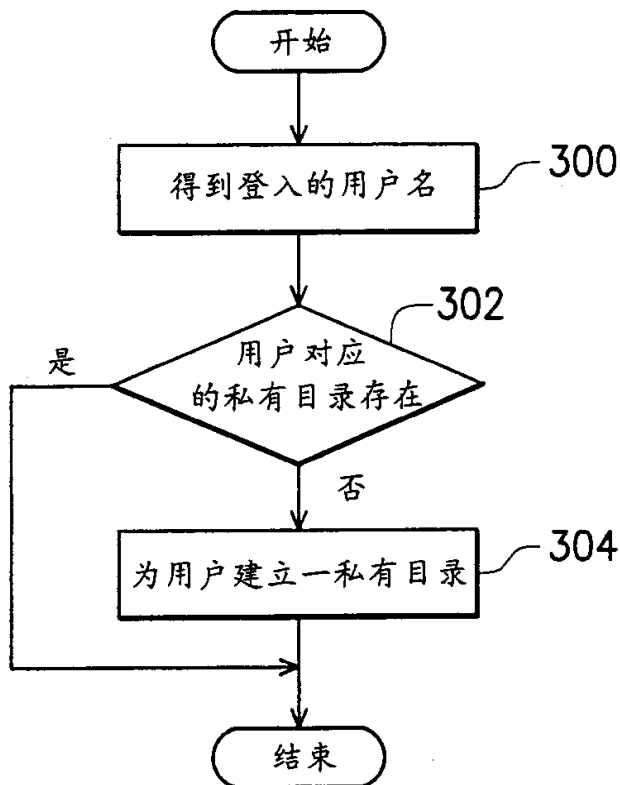


图 5

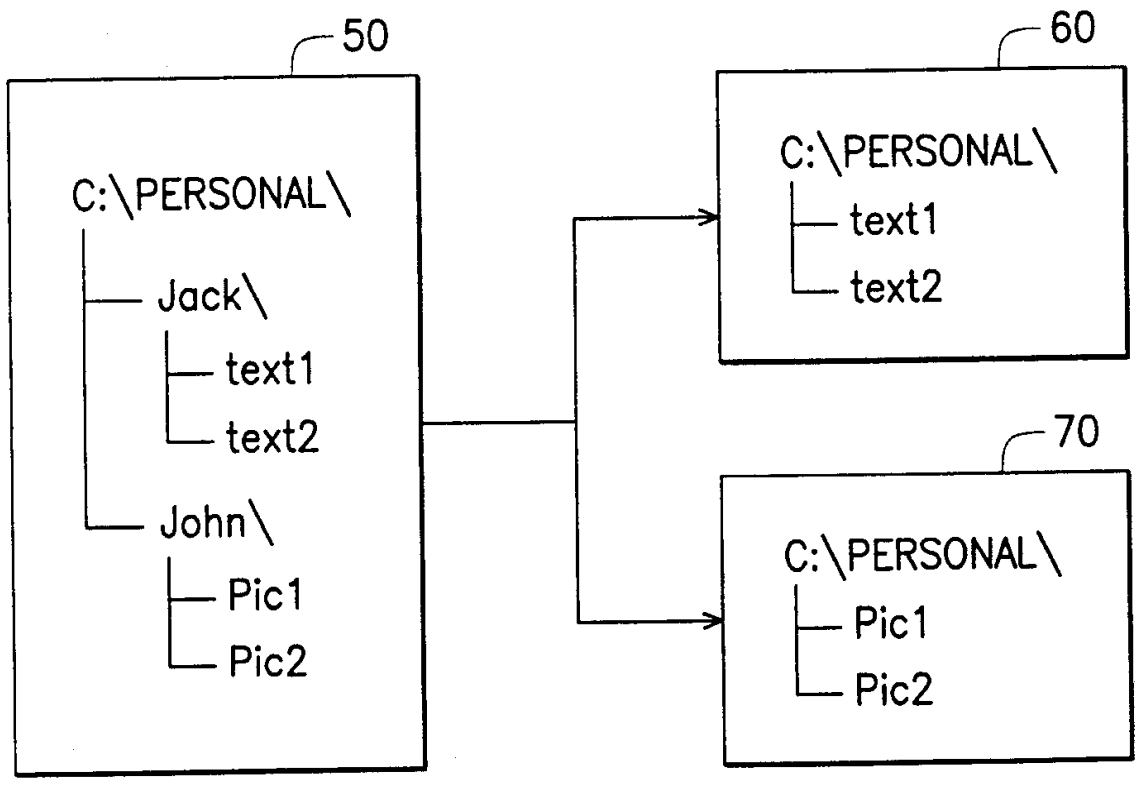


图 6