(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1667608 B
(45)授权公告日 2010.04.28

(21)申请号 200410092577.6
(22)申请日 2004.11.15
(30)优先权数据
10/737,581 2003.12.15 US
(73)专利权人 联想(新加坡)私人有限公司
地址 新加坡彰宜
(72)发明人 本杰明·C·里德 马克·A·斯密斯
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李颖
(51)Int.Cl.
G06F 17/30(2006.01)
(56)对比文件
US 5675725 A,1997.10.07, 全文.
US 2002120791 A1,2002.08.29, 全文.

审查员 郝晓丽

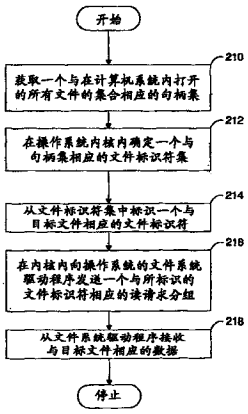
权利要求书 4 页 说明书 5 页 附图 10 页

(54)发明名称

在计算机系统内访问至少一个目标文件的方法和系统

(57)摘要

本发明提供了一种在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的方法和系统。在一个典型实施例中,这种方法和系统包括:(1)获取一个与在计算机系统内打开的所有文件的集合相应的句柄集;(2)在操作系统的内核内确定一个与句柄集相应的文件标识符集;(3)从文件标识符集中标识一个与目标文件相应的文件标识符;(4)在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组;以及(5)从文件系统驱动程序接收与目标文件相应的数据。



CN 1667608 B

1. 一种在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的方法，所述方法包括下列步骤：

通过向内核发布“Nt 查询系统信息”，以及从内核获取对于句柄集内每个句柄的一个“系统句柄信息”数组，来获取一个与在计算机系统内打开的所有文件的集合相应的句柄集；

在操作系统的内核内确定一个与句柄集相应的文件标识符集；

从文件标识符集中标识一个与目标文件相应的文件标识符，以标识与所标识的与目标文件相应的文件标识符相应的文件对象；

通过将所标识的文件对象传送给内核，以及通过读请求分组向内核请求从与所标识的文件对象相应的目标文件读取数据，来在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组；以及

通过在内核内从文件系统驱动程序接收来自与所标识的文件对象相应的目标文件的数据，以及从内核获取来自与所标识的文件对象相应的目标文件的数据，来从文件系统驱动程序接收与目标文件相应的数据，

其中所述“Nt 查询系统信息”请求有关句柄集内每个句柄的所有信息，所述“系统句柄信息”包括一个指向一个文件对象的指针，其中所述文件对象包括文件标识符信息。

2. 权利要求 1 的方法，其中所述确定步骤包括：

对于句柄集内每个句柄，向内核传送一个指向与所述每个句柄相应的文件对象的指针。

3. 权利要求 2 的方法，其中所述确定步骤还包括：

对于句柄集内每个句柄，从内核内输出一个与所传送的文件对象相应的文件标识符。

4. 权利要求 3 的方法，其中所述标识步骤包括：

标识与所标识的文件标识符相应的文件对象，所述所标识的文件标识符与目标文件相应。

5. 权利要求 4 的方法，其中所述读请求分组包括一个中断请求分组。

6. 权利要求 1 的方法，其中所述通过读请求分组向内核请求从与所标识的文件对象相应的目标文件读取数据包括：

在内核内以一定的偏置量和一定的长度产生一个与所标识的文件对象相应的中断请求分组；以及

向操作系统的文件系统驱动程序传送中断请求分组。

7. 一种在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的系统，所述系统包括：

一个配置成获取一个与在计算机系统内打开的所有文件的集合相应的句柄集的获取模块，进一步包括一个配置成向内核发布“Nt 查询系统信息”的发布模块，以及一个配置成从内核获取对于句柄集内每个句柄的一个“系统句柄信息”数组的获取模块；

一个配置成在操作系统的内核内确定一个与句柄集相应的文件标识符集的确定模块；

一个配置成从文件标识符集中标识一个与目标文件相应的文件标识符，以标识与所标识的与目标文件相应的文件标识符相应的文件对象的标识模块；

一个配置成在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组的发送模块，进一步包括一个配置成向内核传送所标识的文件对象的传送模块，以及一个配置成通过读请求分组向内核请求从与所标识的文件对象相应的目标文件读取数据的请求模块；以及

一个配置成从文件系统驱动程序接收与目标文件相应的数据的接收模块，进一步包括一个配置成在内核内从文件系统驱动程序接收来自与所标识的文件对象相应的目标文件的数据的接收模块，以及一个配置成从内核获取来自与所标识的文件对象相应的目标文件的数据的获取模块，

其中所述“Nt 查询系统信息”请求有关句柄集内每个句柄的所有信息，所述“系统句柄信息”包括一个指向一个文件对象的指针，其中所述文件对象包括文件标识符信息。

8. 权利要求 7 的系统，其中所述确定模块包括：

一个配置成对于句柄集内每个句柄，向内核传送一个指向与所述每个句柄相应的文件对象的指针的传送模块。

9. 权利要求 8 的系统，其中所述确定模块还包括：

一个配置成对于句柄集内每个句柄从内核内输出一个与所传送的文件对象相应的文件标识符的输出模块。

10. 权利要求 9 的系统，其中所述标识模块包括：

一个配置成标识与所标识的文件标识符相应的文件对象的标识模块，所述所标识的文件标识符与目标文件相应。

11. 权利要求 10 的系统，其中所述读请求分组包括一个中断请求分组。

12. 权利要求 7 的系统，其中所述请求模块包括：

一个配置成在内核内以一定的偏置量和一定长度产生一个与所标识的文件对象相应的中断请求分组的产生模块；以及

一个配置成向操作系统的文件系统驱动程序传送中断请求分组的传送模块。

13. 一种在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的方法，所述方法包括下列步骤：

通过向内核发布“Nt 查询系统信息”，以及从内核获取对于句柄集内每个句柄的一个“系统句柄信息”数组，来获取一个与在计算机系统内打开的所有文件的集合相应的句柄集；

在操作系统的内核内确定一个与句柄集相应的文件标识符集；

从文件标识符集中标识一个与目标文件相应的文件标识符，以标识与所标识的与目标文件相应的文件标识符相应的文件对象；以及

通过向内核传送所标识的文件对象，以及通过读请求分组向内核请求从与所标识的文件对象相应的目标文件读取数据，来在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组，

其中所述“Nt 查询系统信息”请求有关句柄集内每个句柄的所有信息，其中所述“系统句柄信息”包括一个指向一个文件对象的指针，其中所述文件对象包括文件标识符信息。

14. 权利要求 13 的方法，其中所述确定步骤包括：

对于句柄集内每个句柄，向内核传送一个指向与所述每个句柄相应的文件对象的指

针。

15. 权利要求 14 的方法，其中所述确定步骤还包括：

对于句柄集内每个句柄，从内核内输出一个与所传送的文件对象相应的文件标识符。

16. 权利要求 15 的方法，其中所述标识步骤包括：

标识与所标识的文件标识符相应的文件对象，所述所标识的文件标识符与目标文件相应。

17. 权利要求 16 的方法，其中所述读请求分组包括一个中断请求分组。

18. 权利要求 13 的方法，其中所述通过读请求分组向内核请求从与所标识的文件对象相应的目标文件读取数据包括：

在内核内以一定的偏置量和一定长度产生一个与所标识的文件对象相应的中断请求分组；以及

向操作系统的文件系统驱动程序传送中断请求分组。

19. 一种在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的系统，所述系统包括：

一个配置成获取一个与在计算机系统内打开的所有文件的集合相应的句柄集的获取模块，进一步包括一个配置成向内核发布“Nt 查询系统信息”的发布模块，以及一个配置成从内核获取对于句柄集内每个句柄的一个“系统句柄信息”数组的获取模块；

一个配置成在操作系统的内核内确定一个与句柄集相应的文件标识符集的确定模块；

一个配置成从标识文件标识符集中标识一个与目标文件相应的文件标识符，以标识与所标识的与目标文件相应的文件标识符相应的文件对象的标识模块；以及

一个配置成在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组的发送模块，进一步包括一个配置成向内核传送所标识的文件对象的传送模块，以及一个配置成通过读请求分组向内核请求从与所标识的文件对象相应的目标文件读取数据的请求模块，

其中所述“Nt 查询系统信息”请求有关在句柄集内每个句柄的所有信息，所述“系统句柄信息”包括一个指向一个文件对象的指针，其中所述文件对象包括文件标识符信息。

20. 权利要求 19 的系统，其中所述确定模块包括：

一个配置成对于句柄集内每个句柄，向内核传送一个指向与所述每个句柄相应的文件对象的指针的传送模块。

21. 权利要求 20 的系统，其中所述确定模块还包括：

一个配置成对于句柄集内每个句柄从内核内输出一个与所传送的文件对象相应的文件标识符的输出模块。

22. 权利要求 21 的系统，其中所述标识模块包括：

一个配置成标识与所标识的文件标识符相应的文件对象的标识模块，所述所标识的文件标识符与目标文件相应。

23. 权利要求 22 的系统，其中所述读请求分组包括一个中断请求分组。

24. 权利要求 19 的系统，其中所述请求模块包括：

一个配置成在内核内以一定的偏置量和一定长度产生一个与所标识的文件对象相应

的中断请求分组的产生模块；以及

一个配置成向操作系统的文件系统驱动程序传送中断请求分组的传送模块。

在计算机系统内访问至少一个目标文件的方法和系统

[0001] 相关申请

[0002] 本申请涉及 2003 年 12 月 15 日递交的共同待审、共同拥有、共同转让的美国专利申请 No.（序号未定），代理人案号为 No.ARC9-2003-0089。

技术领域

[0003] 本发明与操作系统有关，特别是涉及在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的方法和系统。

背景技术

[0004] Microsoft Windows（以下简称为“Windows”）内核和 Windows 程序具有防止文件被其他过程打开和读取的能力。这是通过打开一个文件和不给其他过程特有权限（诸如读取之类）来实现的。只要这个过程保持将文件打开，其他过程就服从这个过程所允许的权限。其他过程要打开这样的文件的尝试将导致 Windows“共享违例 (sharingviolation)”，而不能读取这个文件内的数据。

[0005] 访问打开的文件的需要

[0006] 然而，在这些文件内的数据可能对于许多应用，特别是备份应用，是极为重要的。例如，对于备份应用 (backup application) 来说重要的是能读取和备份一个计算机内的每个文件。此外，这些受保护文件中有一些是含有 Windows 注册表信息的文件，因此是正确操作一个所恢复的备份映像所必需的。

[0007] 现有技术系统

[0008] 当前，备份应用采取两个途径中的一个途径来规避这个问题。

[0009] 扇区式拷贝 (sector-wise copy)

[0010] 在第一现有技术途径中，如现有技术的图 1A 所示，应用将 :(1) 对驱动器 (drive) 上的数据进行扇区式拷贝，如步骤 112 所示 ;然后 (2) 产生盘的整个映像 (image)，如步骤 114 所示。不幸的是，这种方法产生驱动器的一个巨大拷贝。此外，这种技术产生一个盘映像，很难对一个文件的扇区定位。这使从此映像进行“单个文件恢复”非常困难。

[0011] 关机和预引导

[0012] 应用使用的第二个现有技术途径，如现有技术的图 1B 所示，是 :(1) 使计算机关机，如步骤 122 所示，然后 (2) 将计算机引入一个“预引导 (preboot)”环境，如步骤 124 所示，(3) 在预引导环境内执行文件拷贝，如步骤 126 所示。计算机或者重新引导，或者完成对 Windows 的引导。这种方法由于需要重新引导才能拷贝这些文件，因此并不好。此外，在计算机正在运行的同时进行备份是不可能的。

[0013] 因此，需要有一种方法和系统，其能够在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件。

发明内容

[0014] 本发明提供了一种在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的方法和系统。在一个典型实施例中，这种方法和系统包括：(1) 获取一个与在计算机系统内打开的所有文件的集合相应的句柄集；(2) 在操作系统的内核内确定一个与句柄集相应的文件标识集；(3) 从文件标识符集中标识一个与目标文件相应的文件标识符；(4) 在内核内向操作系统的文件系统驱动程序 (file system driver) 发送一个与所标识的文件标识符相应的读请求分组；以及 (5) 从文件系统驱动程序接收与目标文件相应的数据。

[0015] 在一个典型实施例中，获取句柄集包括：(a) 向内核发布一个 NtQuerySystemInformation(Nt 查询系统信息)，其中所述 NtQuerySystemInforrnation 请求有关句柄集内每个句柄的所有信息；以及 (b) 从内核获取对于在句柄集内每个句柄的一个 SYSTEM_HANDLE_INFORMATION(系统句柄信息) 数组，其中所述 SYSTEM_HANDLE_INFORMATION 包括一个 FILE_OBJECT(文件对象)，其中所述 FILE_OBJECT 包括文件标识符信息。

[0016] 在一个典型实施例中，确定与句柄集相应的文件标识符集包括对于句柄集内每个句柄向内核传送一个指向与这个句柄相应的 FILE_OBJECT 的指针。在一个进一步的实施例中，确定包括对于句柄集内每个句柄从内核内输出一个与所传送的 FILE_OBJECT 相应的文件标识符。

[0017] 在一个典型实施例中，标识与目标文件相应的文件标识符包括标识与所标识的与目标文件相应的文件标识符相应的 FILE_OBJECT。

[0018] 在一个典型实施例中，发送读请求分组包括：(a) 向内核传送所标识的 FILE_OBJECT；以及 (b) 通过读请求分组向内核请求从与所标识的 FILE_OBJECT 相应的目标文件读取数据，其中所述读请求分组包括一个中断请求分组 (IRP)。在一个进一步的实施例中，请求读取数据包括：(i) 在内核内以一定的偏置量和一定长度产生一个与所标识的 FILE_OBJECT 相应的 IRP；以及 (ii) 向操作系统的文件系统驱动程序传送 IRP。

[0019] 在一个典型实施例中，接收与目标文件相应的数据包括：(a) 在内核内从文件系统驱动程序接收来自与所标识的 FILE_OBJECT 相应的目标文件的数据；以及 (b) 从内核获取来自与所标识的 FILE_OBJECT 相应的目标文件的数据。

[0020] 在一个典型实施例中，这种方法和系统包括：(1) 获取一个与在计算机系统内打开的所有文件的集合相应的句柄集；(2) 在操作系统的内核内确定一个与句柄集相应的文件标识符集；(3) 从文件标识符集中标识一个与目标文件相应的文件标识符；以及 (4) 在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组。

[0021] 在一个典型实施例中，获取句柄集包括：(a) 向内核发布一个 NtQuerySystemInformation(Nt 查询系统信息)，其中所述 NtQuerySystemInforrnation 请求有关句柄集内每个句柄的所有信息；以及 (b) 从内核获取对于在句柄集内每个句柄的一个 SYSTEM_HANDLE_INFORMATION(系统句柄信息) 数组，其中所述 SYSTEM_HANDLE_INFORMATION 包括一个 FILE_OBJECT(文件对象)，其中所述 FILE_OBJECT 包括文件标识符信息。

[0022] 在一个典型实施例中，标识与目标文件相应的文件标识符包括标识与所标识的与

目标文件相应的文件标识符相应的 FILE_OBJECT。

[0023] 在一个典型实施例中，发送读请求分组包括：(a) 向内核传送所标识的 FILE_OBJECT；以及 (b) 通过读请求分组向内核请求从与所标识的 FILE_OBJECT 相应的目标文件读取数据。

[0024] 本发明还提供了一种用于可编程计算机的计算机程序产品，具有体现在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的可读程序代码。在一个典型实施例中，这种计算机程序产品包括：(1) 获取一个与在计算机系统内打开的所有文件的集合相应的句柄集的计算机可读代码；(2) 在操作系统的内核内确定一个与句柄集相应的文件标识符集的计算机可读代码；(3) 从文件标识符集中标识一个与目标文件相应的文件标识符的计算机可读代码；(4) 在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组的计算机可读代码；以及 (5) 从文件系统驱动程序接收与目标文件相应的数据的计算机可读代码。

[0025] 在一个典型实施例中，这种计算机程序产品包括：(1) 获取一个与在计算机系统内打开的所有文件的集合相应的句柄集的计算机可读代码；(2) 在操作系统的内核内确定一个与句柄集相应的文件标识符集的计算机可读代码；(3) 从文件标识符集中标识一个与目标文件相应的文件标识符的计算机可读代码；以及 (4) 在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组的计算机可读代码。

附图说明

[0026] 图 1A 为一种现有技术的流程图。

[0027] 图 1B 为另一种现有技术的流程图。

[0028] 图 2 为按照本发明的一个典型实施例设计的流程图。

[0029] 图 3 为按照本发明的一个典型实施例设计的获取步骤的流程图。

[0030] 图 4A 为按照本发明的一个典型实施例设计的确定步骤的流程图。

[0031] 图 4B 为按照本发明的另一个典型实施例设计的确定步骤的流程图。

[0032] 图 5 为按照本发明的一个典型实施例设计的标识步骤的流程图。

[0033] 图 6A 为按照本发明的一个典型实施例设计的发送步骤的流程图。

[0034] 图 6B 为按照本发明的另一个典型实施例设计的发送步骤的流程图。

[0035] 图 7 为按照本发明的一个典型实施例设计的接收步骤的流程图。

具体实施方式

[0036] 本发明提供了一种在一个具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的方法和系统。在一个典型实施例中，本发明提供了一种在 Windows 保持运行的同时读取受保护的 Windows 文件的内容的方法和系统。本发明提供了一种在具有在文件打开时实现文件锁定的操作系统的计算机系统内访问至少一个目标文件的方法和系统。在一个典型实施例中，这种方法和系统包括：(1) 获取一个与在计算机系统内打开的所有文件的集合相应的句柄集；(2) 在操作系统的内核内确定一个与句柄集相应的文件标识符集；(3) 从文件标识符集中标识一个与目标文件相应的文件标识符；(4) 在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分

组；以及 (5) 从文件系统驱动程序接收与目标文件相应的数据。

[0037] 参见图 2，在一个典型实施例中，本发明包括：(1) 获取一个与在计算机系统内打开的所有文件的集合相应的句柄集的步骤 210；(2) 在操作系统的内核内确定一个与句柄集相应的文件标识符集的步骤 212；从文件标识符集中标识一个与目标文件相应的文件标识符的步骤 214；在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组的步骤 216；以及从文件系统驱动程序接收与目标文件相应的数据的步骤 218。

[0038] 概述

[0039] 本发明通过两个相互配合工作在它们之间来回发送数据的程序来读取受保护的 Windows 文件。在高层，这两个程序中的一个程序 (例如 wam.sys) 在内核内运行，完成实际读取，而另一个程序 (例如 bam.exe) 在用户空间内运行，推导出有关文件的信息，将这信息传送给内核程序，以便给内核程序足够的信息，使它知道从哪里进行读取。然后，内核程序将读出数据返回给用户级程序。

[0040] 获取句柄集

[0041] 具体地说，用户级程序向内核发布一个 NtQuerySystemInformation，请求有关打开的文件句柄的所有信息。内核返回在内核内每个打开的句柄的 SYSTEM_HANDLE_INFORMATION 的数组 (array)。

[0042] 参见图 3，在一个典型实施例中，获取步骤 210 包括：向内核发布一个 NtQuerySystemInformation 的步骤 310，其中所述 NtQuerySystemInformation 请求有关在句柄集内每个句柄的所有信息；以及 (b) 从内核获取对于句柄集内每个句柄的一个 SYSTEM_HANDLE_INFORMATION 数组的步骤 312，其中所述 SYSTEM_HANDLE_INFORMATION 包括一个指向一个 FILE_OBJECT 的指针，其中所述 FILE_OBJECT 包括文件标识符信息。

[0043] 确定与句柄集相应的文件标识符集

[0044] 然而，仍然需要各文件句柄与名之间的对应关系。仍然需要找出哪个句柄是目标文件的句柄。在 SYSTEM_HANDLE_INFORMATION 内的一段信息是一个指向一个 FILE_OBJECT 的指针。FILE_OBJECT 含有文件名信息。然而，存储 FILE_OBJECT 的存储器只能在内核内使用。

[0045] 因此，用户级程序将一个指向这个存储器的指针传入内核级程序。然后，内核级程序传回这个 FILE_OBJECT 描述的文件名。

[0046] 参见图 4A，在一个典型实施例中，确定步骤 212 包括对于句柄集内每个句柄向内核传送一个指向与所述每个句柄相应的 FILE_OBJECT 的指针的步骤 412。在一个进一步的实施例中，如图 4B 所示，确定步骤 212 还包括对于句柄集内每个句柄从内核内输出一个与所传送的 FILE_OBJECT 相应的文件标识符的步骤 422。

[0047] 标识与目标文件相应的文件标识符

[0048] 用户级程序继续这样执行，直到从内核返回了它所寻找的文件名。它现在就有一个指向希望读取的受保护文件，即目标文件，的句柄。实质上，已经执行了文件打开。

[0049] 参见图 5，在一个典型实施例中，标识步骤 214 包括标识与所标识的与目标文件相应的文件标识符相应的 FILE_OBJECT 的步骤 512。

[0050] 发送读请求分组

[0051] 在用户空间内用句柄应该能直接进行读取。然而，这句柄仍然受原来保护过程所加的权限的限制，因此尝试读取这个句柄会产生共享违例。

[0052] 因此，内核级程序将这个 FILE_OBJECT 传回给内核程序，请求它以一定的偏置量 (offset) 和 PAGE_SIZE（通常为 4096 个字节）长度从由 FILE_OBJECT 描述的文件读取数据。简单地从内核发布 ZwReadFile 也会由于上述原因出现共享违例而失败。

[0053] 在内核内通过产生一个中断请求分组 (IRP) 从这个文件提取数据，将它一直传送到这个 FILE_OBJECT 驻留的基层文件系统 (NTFS，FAT32 等）。

[0054] 参见图 6A，在一个典型实施例中，发送步骤 216 包括向内核传送所标识的 FILE_OBJECT 的步骤 612 和通过读请求分组向内核请求从与所标识的 FILE_OBJECT 相应的目标文件读取数据的步骤 614，其中所述读请求分组包括一个中断请求分组 (IRP)。在一个进一步的实施例中，如图 6B 所示，请求步骤 614 包括在内核内以一定的偏置量和一定的长度产生一个与所标识的 FILE_OBJECT 相应的 IRP 的步骤 622 和向操作系统的文件系统驱动程序传送 IRP 的步骤 624。

[0055] 接收与目标文件相应的数据

[0056] 文件系统用所请求的数据进行响应，内核程序将这数据传回到用户空间。这样，对一个受保护文件执行了一次读取。以不同的偏置量重复这些读取，直到到达这个文件的末尾，从而得到盘上这个文件的数据的一个理想拷贝。

[0057] 参见图 7，在一个典型实施例中，接收步骤 218 包括在内核内从文件系统驱动程序接收来自与所标识的 FILE_OBJECT 相应的目标文件的数据的步骤 712 和从内核获取来自与所标识的 FILE_OBJECT 相应的目标文件的数据的步骤 714。

[0058] 总结

[0059] 从以上对本发明的一个优选实施例和各个备选方案的充分说明中熟悉该技术领域的人员可以看到，按照在这里给出的原理，存在不背离本发明的许多备选方案和等效方案。因此，本发明的专利保护范围不是由以上说明而是由所附权利要求书给出。

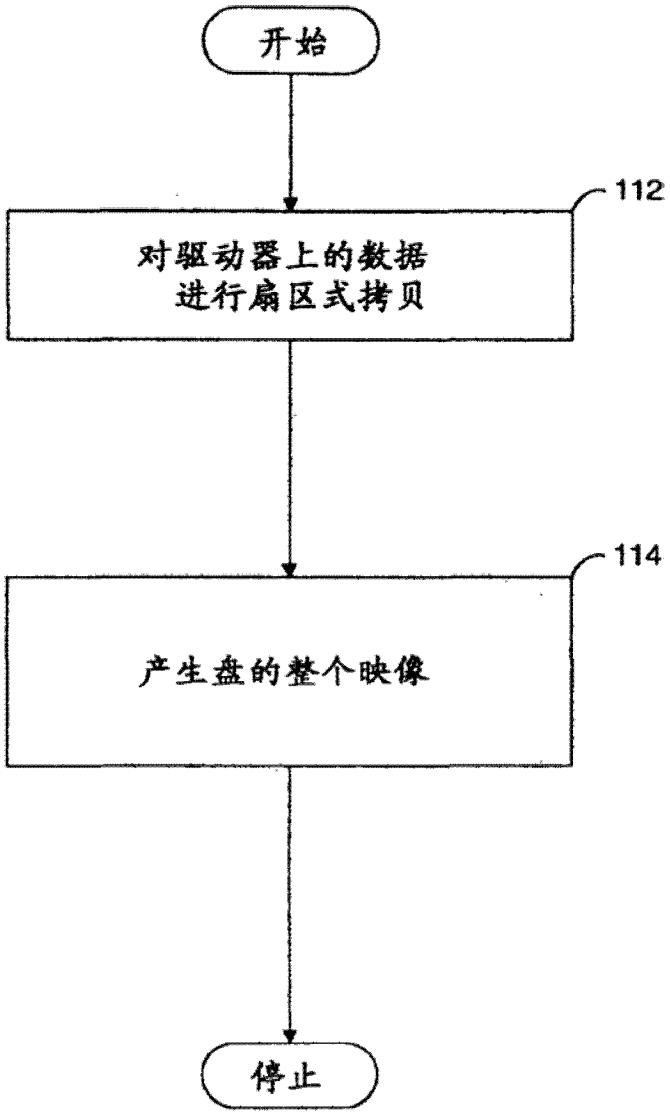


图 1A（现有技术）

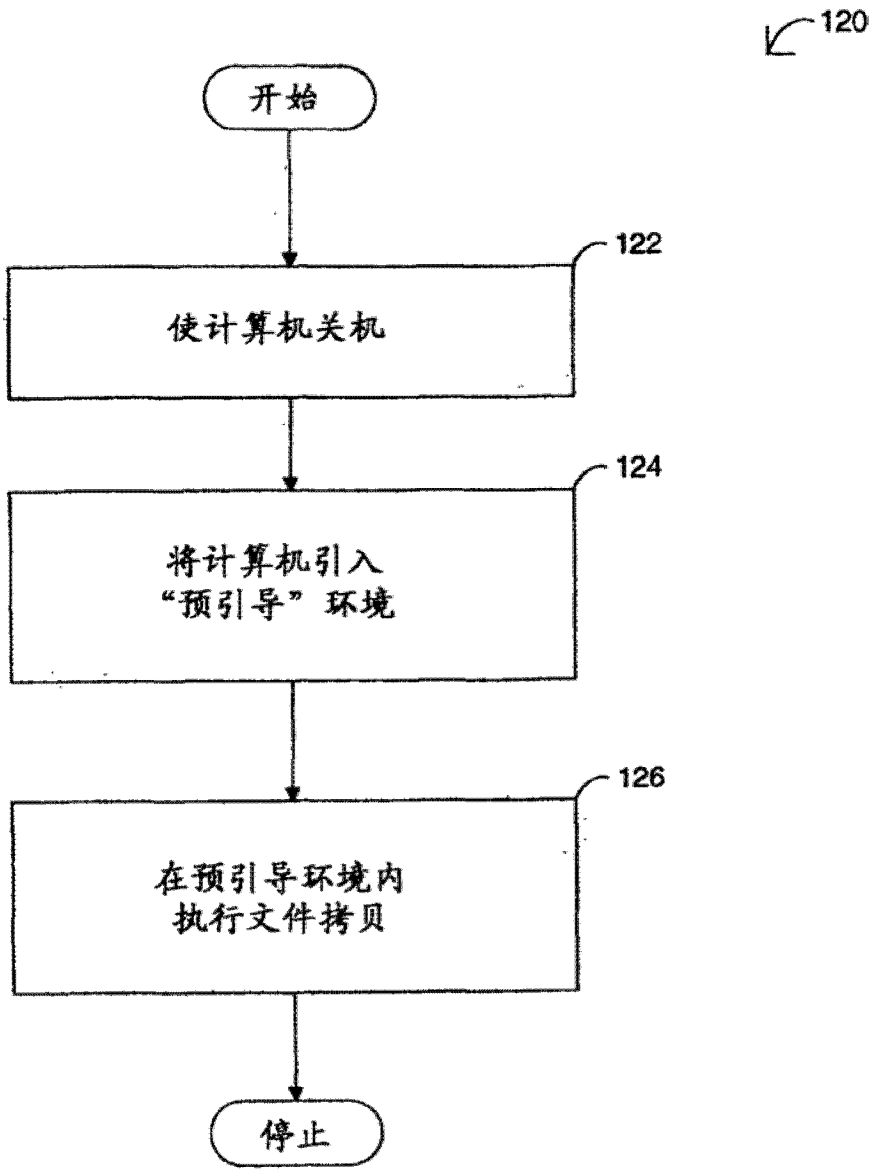


图 1B（现有技术）

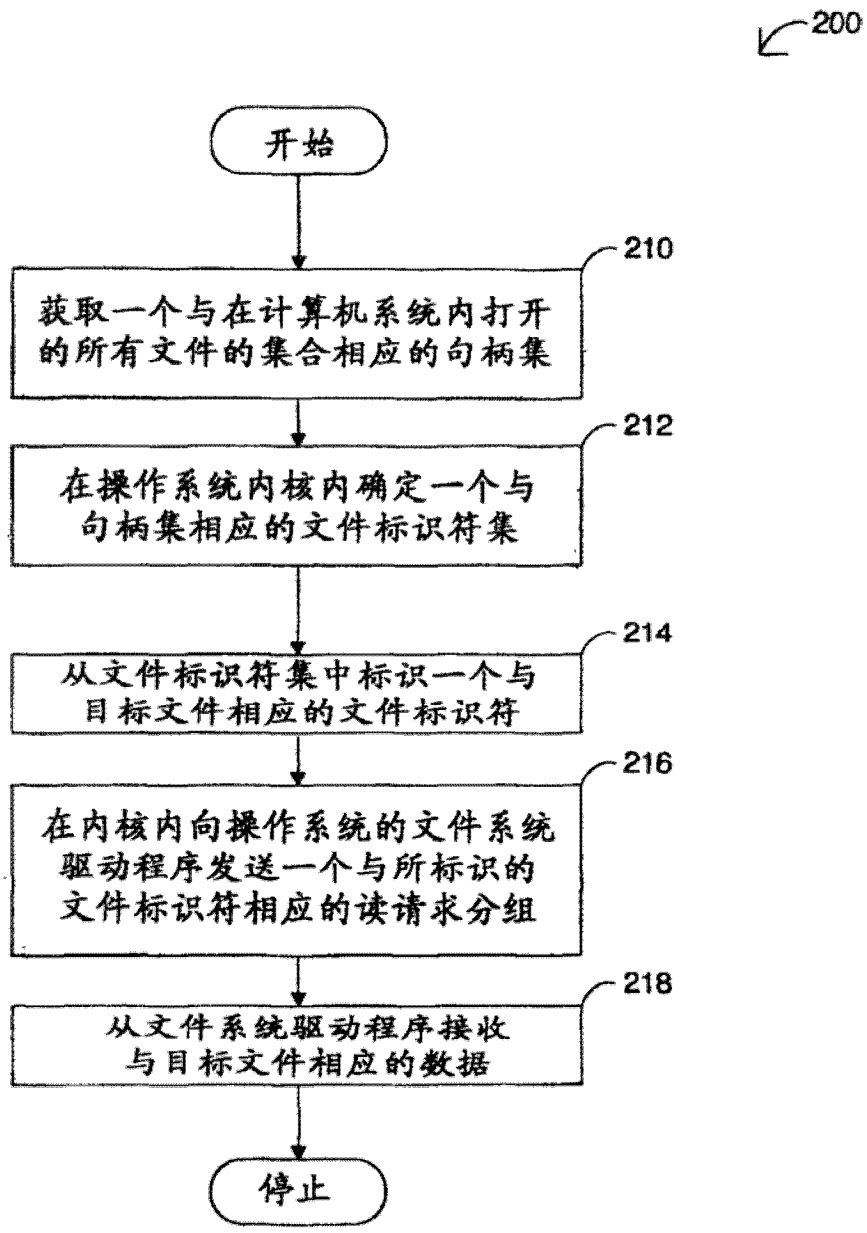

200
开始
210
获取一个与在计算机系统内打开的所有文件的集合相应的句柄集
212
在操作系统内核内确定一个与句柄集相应的文件标识符集
214
从文件标识符集中标识一个与目标文件相应的文件标识符
216
在内核内向操作系统的文件系统驱动程序发送一个与所标识的文件标识符相应的读请求分组
218
从文件系统驱动程序接收与目标文件相应的数据
停止

图 2

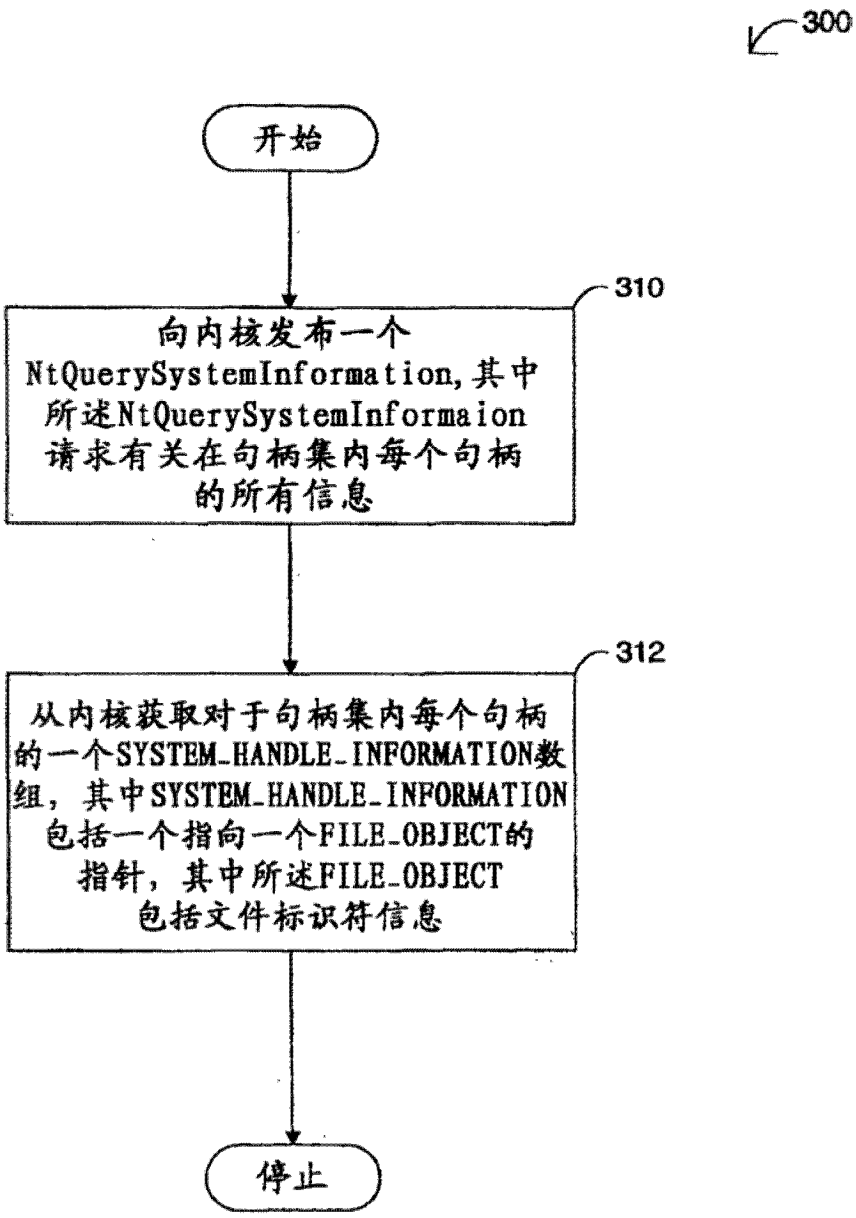

300
开始
310
向内核发布一个NtQuerySystemInformation,其中所述NtQuerySystemInformaion请求有关在句柄集内每个句柄的所有信息
312
从内核获取对于句柄集内每个句柄的一个SYSTEM_HANDLE_INFORMATION数组，其中SYSTEM_HANDLE_INFORMATION包括一个指向一个FILE_OBJECT的指针，其中所述FILE_OBJECT包括文件标识符信息
停止

图 3

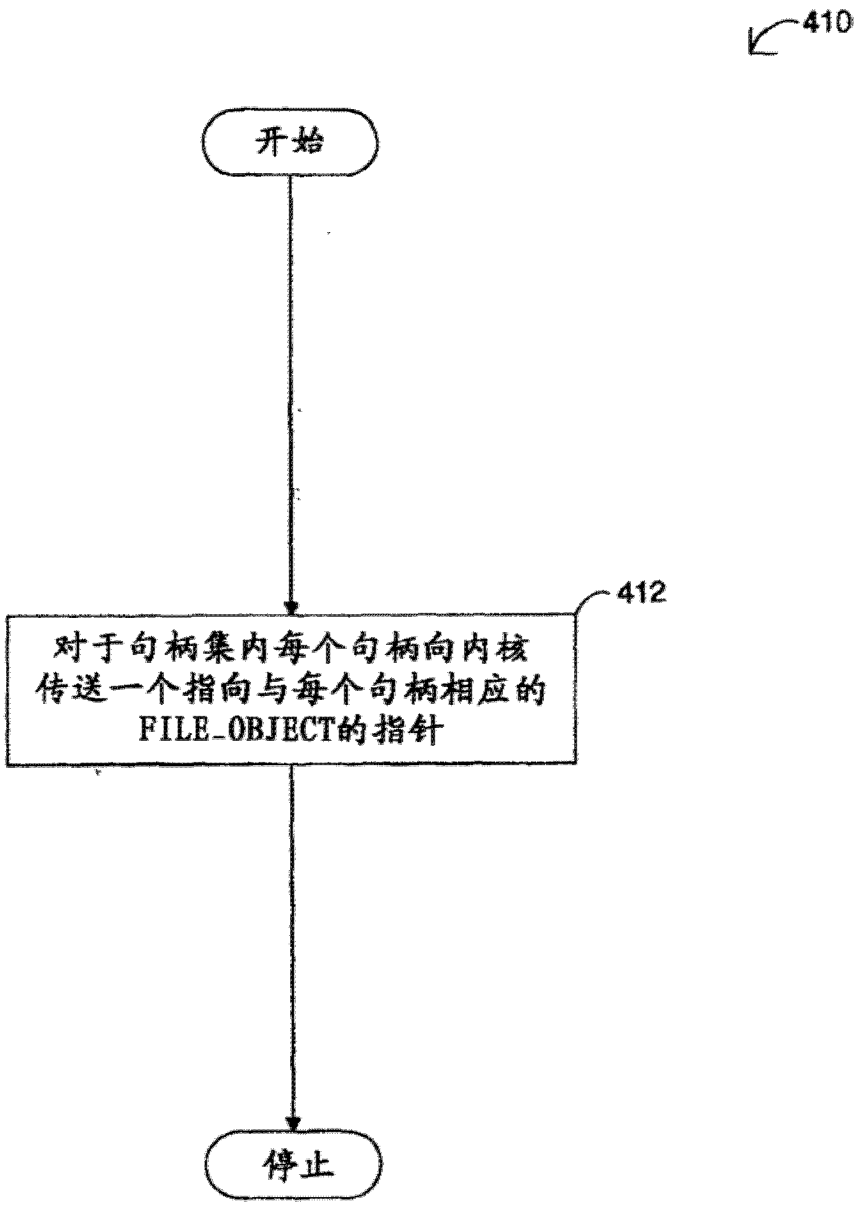

410
开始
412
对于句柄集内每个句柄向内核传送一个指向与每个句柄相应的FILE_OBJECT的指针
停止

图 4A

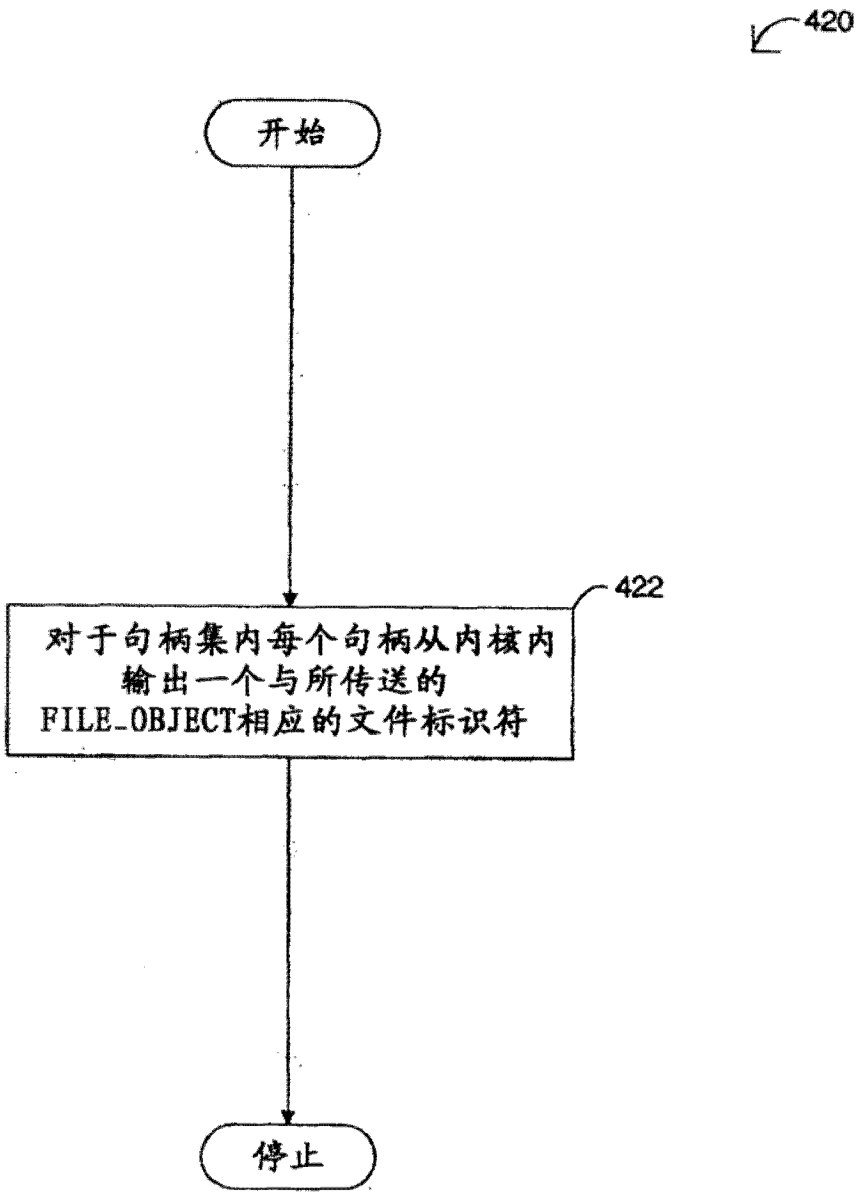

420
开始
422
对于句柄集内每个句柄从内核内
输出一个与所传送的
FILE_OBJECT相应的文件标识符
停止

图 4B

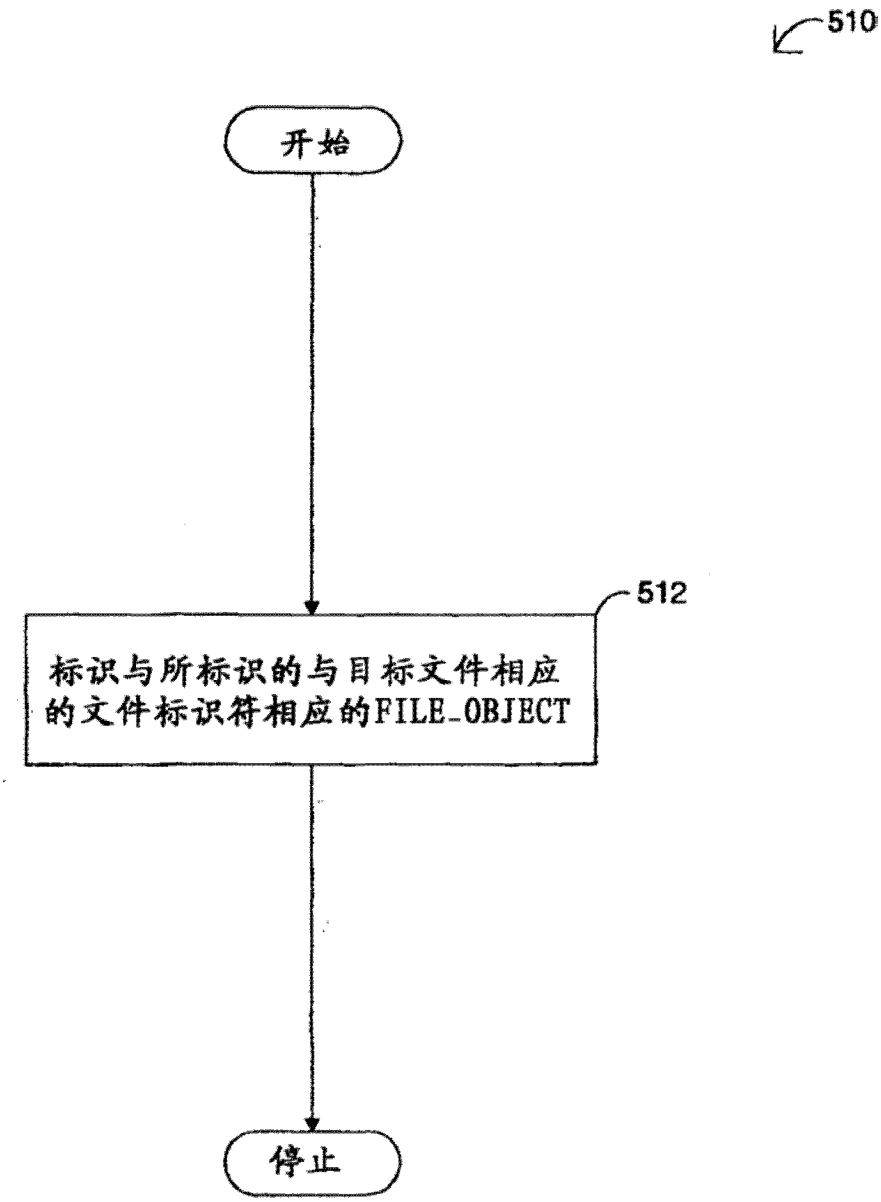


图 5

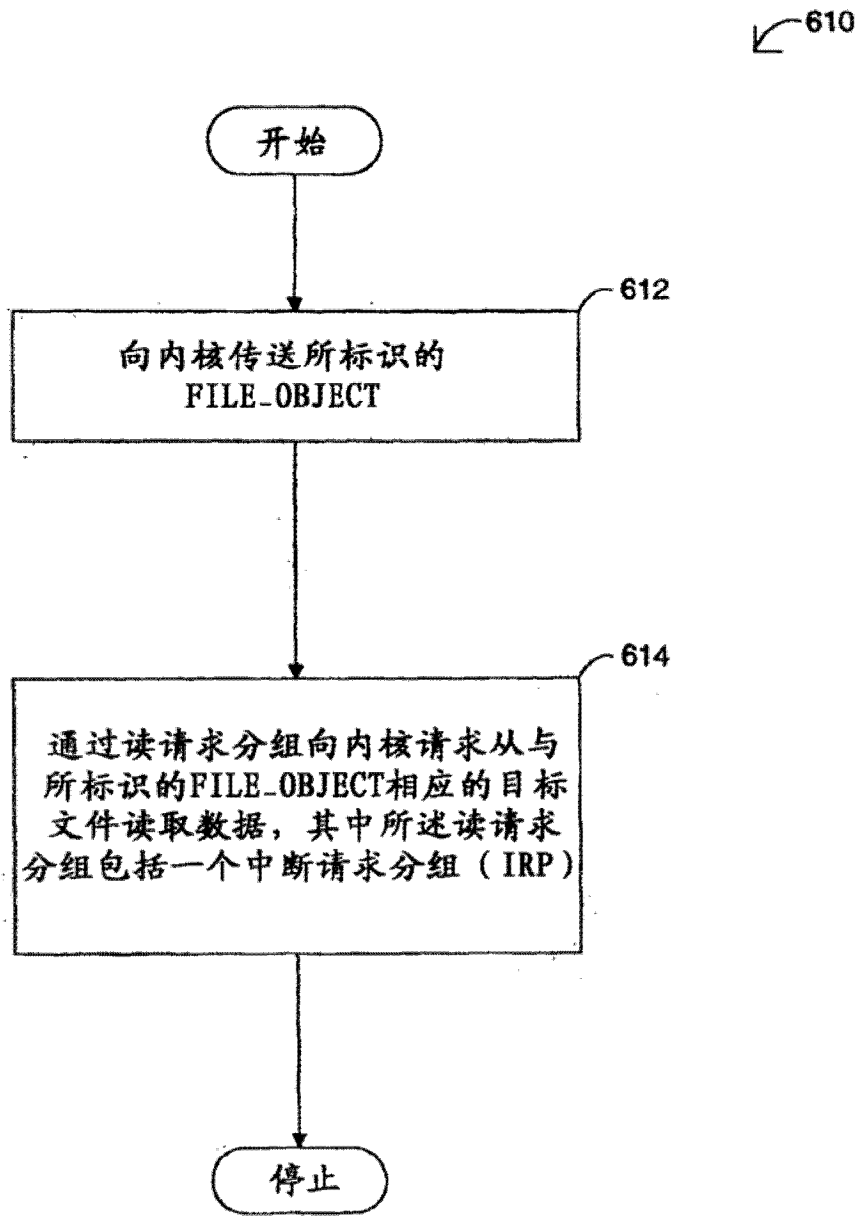

610
开始
612
向内核传送所标识的
FILE_OBJECT
614
通过读请求分组向内核请求从与所标识的FILE_OBJECT相应的目标文件读取数据，其中所述读请求分组包括一个中断请求分组（IRP）
停止

图 6A

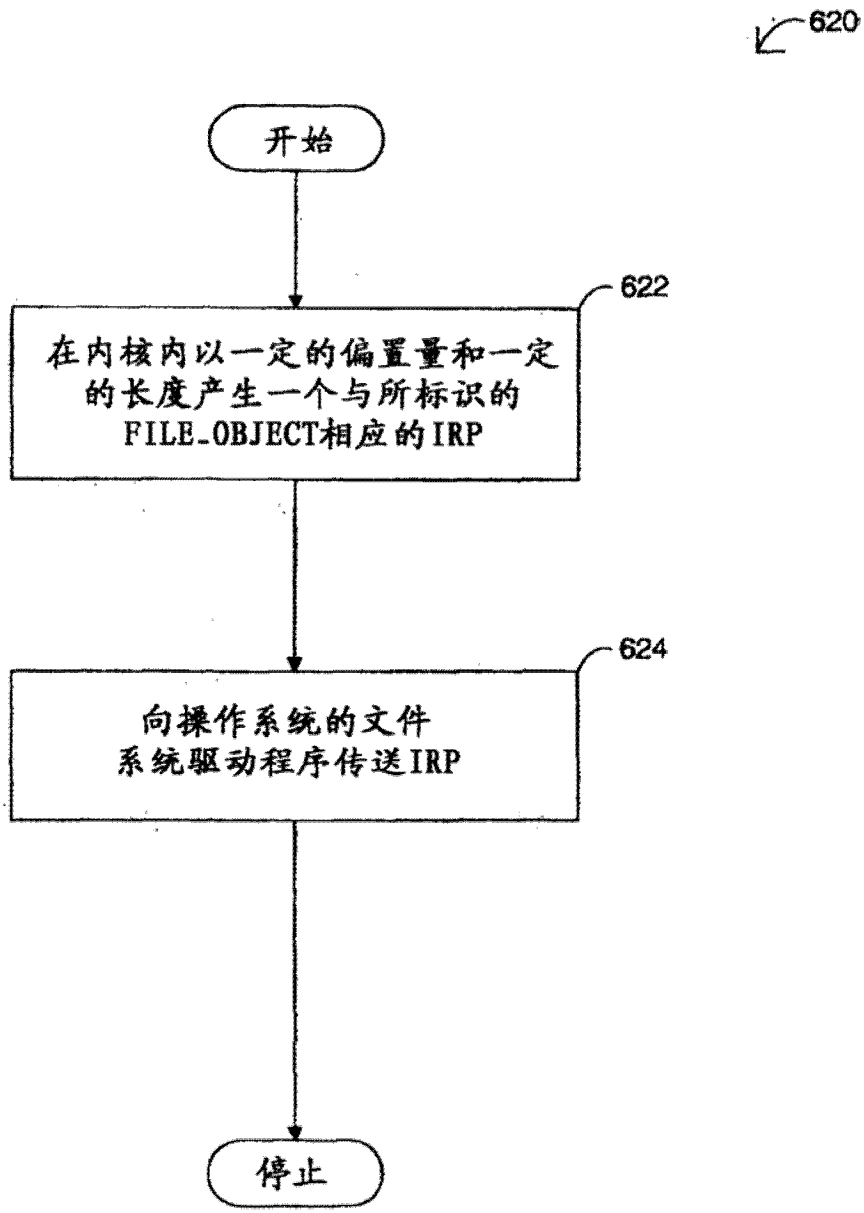

620
开始
622
在内核内以一定的偏置量和一定的长度产生一个与所标识的FILE_OBJECT相应的IRP
624
向操作系统的文件系统驱动程序传送IRP
停止

图 6B

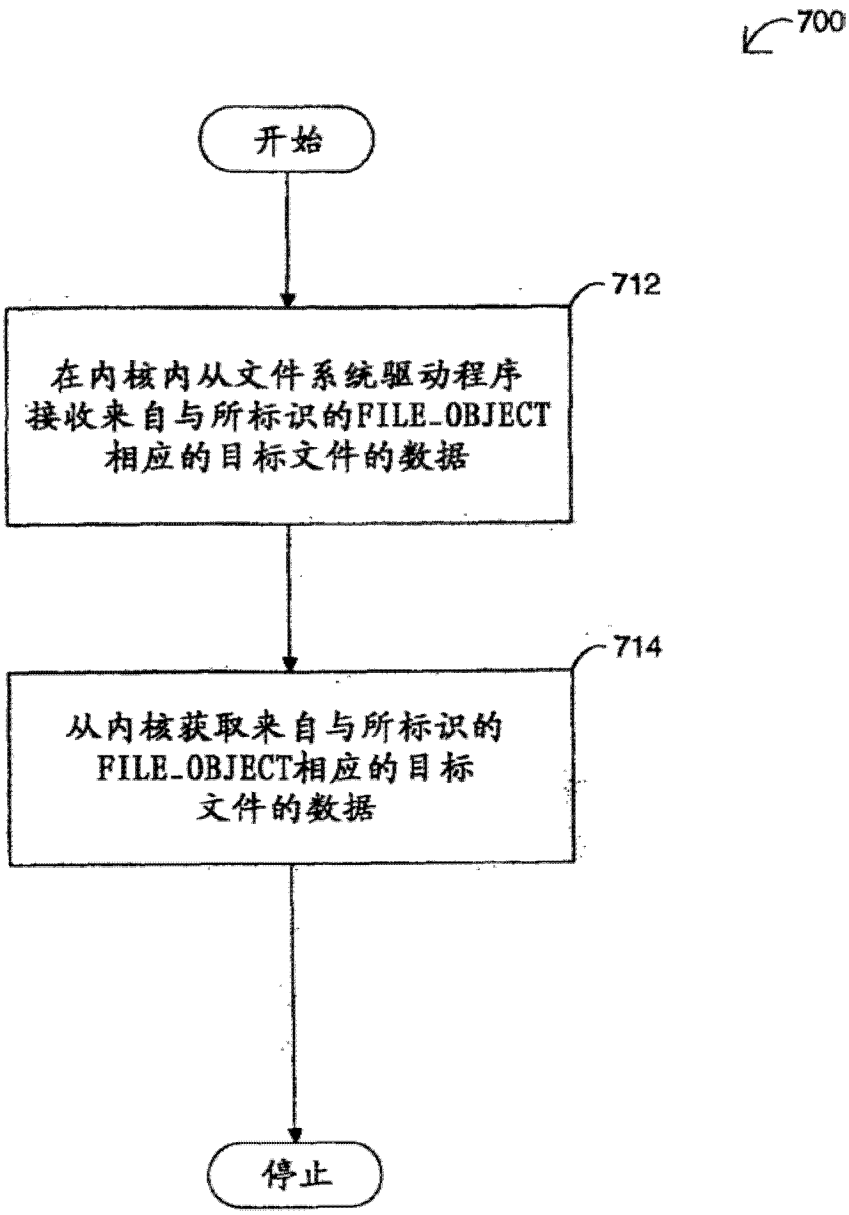

700
开始
712
在内核内从文件系统驱动程序接收来自与所标识的FILE_OBJECT相应的目标文件的数据
714
从内核获取来自与所标识的FILE_OBJECT相应的目标文件的数据
停止

图 7