



[12] 发明专利申请公开说明书

[21] 申请号 03110640.4

[43] 公开日 2004年1月14日

[11] 公开号 CN1467642A

[22] 申请日 2003.4.18 [21] 申请号 03110640.4

[30] 优先权

[32] 2002.7.9 [33] JP [31] 199437/2002

[71] 申请人 富士通株式会社

地址 日本神奈川

[72] 发明人 梅林祐 田 悦 山中祐介

佐佐木孝興

[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

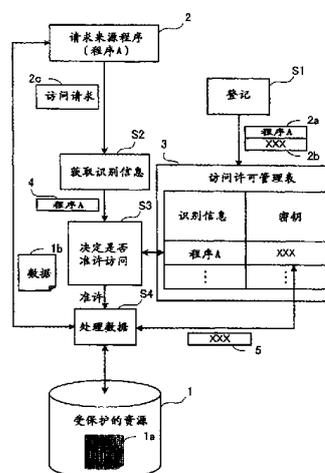
代理人 李 强

权利要求书3页 说明书22页 附图18页

[54] 发明名称 数据保护程序及数据保护方法

[57] 摘要

一种数据保护程序能够有效地限制对于受保护资源的未授权访问，即使在受保护资源处在被一个用户合法访问的状态下也可提供这种保护。关于能够访问受保护资源的程序的识别信息被登记在一张访问许可管理表中。如果后来接收到一个访问请求要求访问受保护资源，就获取关于输出所述访问请求的请求来源程序的识别信息。接着，根据关于该请求来源程序的识别信息是否已被登记在访问许可管理表中，来确定对于受保护资源的访问是否被准许。如果对于受保护资源的访问被准许，就响应访问请求处理受保护资源中的数据。



1. 一种数据保护程序，用于保护存储在受保护资源中的数据，所述的数据保护程序使得一台计算机能够执行一个处理序列，包括：

将关于能够访问所述受保护资源的程序的识别信息登记在一张访问许可管理表中；

如果接收到一个访问请求要求访问所述的受保护资源，就获取关于输出所述访问请求的请求来源程序的识别信息；

根据关于所述请求来源程序的识别信息是否已被登记在所述的访问许可管理表中，来确定对于所述受保护资源的访问是否被准许；以及

如果对于所述受保护资源的访问被准许，就响应所述的访问请求处理所述受保护资源中的数据。

2. 根据权利要求 1 所述的数据保护程序，其中当所述受保护资源中的数据被处理时，如果所述的访问请求是写数据的请求，那么从执行所述请求来源程序的进程传送来的数据就被加密并存入所述的受保护资源，而如果所述的访问请求是读取数据的请求，那么来自所述受保护资源的数据就被解密并传送给执行所述请求来源程序的进程。

3. 根据权利要求 2 所述的数据保护程序，其中所述的处理序列还包括：

将一个与关于程序的识别信息相关的密钥登记在所述的访问许可管理表中；以及

当所述受保护资源中的数据要被加密和解密时，就利用登记在所述访问许可管理表中的与关于请求来源程序的识别信息相关的所述密钥来加密和解密该数据。

4. 根据权利要求 3 所述的数据保护程序，其中一个由用户向所述程序输入的口令唯一确定的值被登记在所述的访问许可管理表中作为所述的密钥。

5. 根据权利要求 3 所述的数据保护程序，其中所述的处理序列

还包括:

当所述受保护资源中的数据要被加密和解密时, 利用一个值加密和解密该数据, 该值通过组合所述的与关于请求来源程序的识别信息相关的密钥与一个预置在所述计算机中的特定值来给出。

6. 根据权利要求 1 所述的数据保护程序, 其中所述的处理序列还包括:

在一张保护资源管理表中登记关于一个包含要保护的数据的文件夹的识别信息; 以及

仅使用登记在所述保护资源管理表中的所述文件夹作为所述的受保护资源。

7. 根据权利要求 1 所述的数据保护程序, 其中所述的处理序列还包括:

登记关于所述程序的识别信息以及可访问资源的资源名的组合; 以及

根据关于所述请求来源程序的识别信息以及由所述访问请求指定的访问目标的资源名的组合是否已经被登记在所述的访问许可管理表中, 来确定对所述受保护资源的访问是否被准许。

8. 一种保护存储在受保护资源中的数据的方法, 所述方法包括: 将关于能够访问所述受保护资源的程序的识别信息登记在一张访问许可管理表中;

如果接收到一个访问请求要求访问所述的受保护资源, 就获取关于输出所述访问请求的请求来源程序的识别信息;

根据关于所述请求来源程序的识别信息是否已被登记在所述的访问许可管理表中, 来确定对于所述受保护资源的访问是否被准许; 以及

如果对于所述受保护资源的访问被准许, 就响应所述的访问请求处理所述受保护资源中的数据。

9. 一种用来保护存储在受保护资源中的数据的装置, 所述装置包括:

识别信息登记装置，用来将关于能够访问所述受保护资源的程序的识别信息登记在一张访问许可管理表中；

识别信息获取装置，如果接收到一个访问请求要求访问所述的受保护资源，就获取关于输出所述访问请求的请求来源程序的识别信息；

访问许可/禁止判定装置，用来根据关于所述请求来源程序的识别信息是否已被登记在所述的访问许可管理表中，确定对于所述受保护资源的访问是否被准许；以及

数据处理装置，如果对于所述受保护资源的访问被准许，就响应所述的访问请求处理所述受保护资源中的数据。

10. 一种计算机可读取的记录媒体，其中存储了用于保护存储在受保护资源中的数据的数据保护程序，所述的数据保护程序可以被一台计算机读取，所述的数据保护程序使得所述的计算机执行一个处理序列，包括：

将关于能够访问所述受保护资源的程序的识别信息登记在一张访问许可管理表中；

如果接收到一个访问请求要求访问所述的受保护资源，就获取关于输出所述访问请求的请求来源程序的识别信息；

根据关于所述请求来源程序的识别信息是否已被登记在所述的访问许可管理表中，来确定对于所述受保护资源的访问是否被准许；以及

如果对于所述受保护资源的访问被准许，就响应所述的访问请求处理所述受保护资源中的数据。

数据保护程序及数据保护方法

技术领域

本发明涉及一种用于保护数据的数据保护程序及数据保护方法，尤其涉及用于限制对被保护资源的访问的数据保护程序及数据保护方法。

背景技术

计算机系统有时要在若干个用户之间共享。当一个计算机系统若干用户间共享时，就有必要限制用户所能使用的资源，以保护某些用户的数据免受疏忽错误及其他用户未授权行为的损害。

常规的计算机系统从一个用户处接收包含了用户名和口令的验证信息，根据接收到的验证信息验证用户，并允许通过验证的用户访问受限资源，这些资源是事先已经授权用户访问的。这样，用户就可以选择访问计算机系统所提供的资源。虽然上述的验证过程基本上是在一个用户接一个用户的基础上进行的，但也可以在一组用户的基础上执行相同的验证过程，以便为各个这样的组提供有选择的访问及信息共享。

迄今为止，对于选择性访问的所有验证操作都必须依照自上而下的过程由系统管理员排序和计划。然而，上述自上而下的选择性访问实现方法的不利之处在于，它在系统工作计划的初始阶段需要消耗大量时间和劳力，这是因为系统管理员必须预先计划要在用户中共享的信息内容，而且各个用户不能根据自己的意愿进行更精细的访问限制设置。

考虑到上述的缺点，已经建议允许系统用户根据自下而上的方法进行更确定的文档保护处理。根据某项提议，用户借助一种文件加密应用对存储在存储设备上的文件进行加密，以避免文件被未经授权的

第三方使用。

根据一种通用的文件加密方法，用户利用诸如文档生成应用—如字处理程序—这样的应用所准备的一个文档文件被直接存储在一个存储设备中，存储在存储设备中的该文档之后再被加密。

当利用这样一种应用生成的文档文件被直接存储在存储设备中时，这些文档文件在存储设备中暂时不受保护。为了减轻所存储文档文件的这种不受保护的状态，已考虑使用一个进程来监视对用户所使用计算机系统存储设备的存取，并自动在文档文件被存储到存储设备时或是之后立即对其进行加密。

根据上述方法，如果文档文件的一个存储目的地（比如一个目录）要被加密，那么文档文件也会用与存储目的地相关的加密密钥被加密，而用户却并未意识到文档的加密。当被加密的文档文件从存储目的地被读出时会被解密。只有当用来监视对存储目的地的存取的机制工作时，文档文件才会被加密和解密。通过仅在某个特定的应用处在激活状态时运行存取监视机制，保护经过加密的文档文件免受未经授权的使用。

然而，如果存取监视机制自动加密和解密文档文件，那么恶意的第三方就可能在存取监视机制工作期间读取加密的文档文件。特别是，当一个激活了存取监视机制的应用 A 在访问存储目的地时，应用 B 也可以访问该存储目的地并读取一个解密的文档文件。

即使应用 A 采取行动限制用户的访问，只要存取监视机制已在应用 A 的控制下被激活，那么就可以通过来自于应用 B 的复制请求等，从存储目的地读取一个经过加密的文档文件。这时，被应用 B 读取的文档文件也会被存取监视机制解密。因此就出现了这样一个问题：第三方可以从存储目的地中取出解密信息。

这就使得欺诈行为成为可能，比如一个拥有访问权的用户通过应用 A 激活存取监视机制，再利用另一个应用 B 读取一个文档文件。举例来说，即使应用 A 受到限制仅允许对数据进行登记，一个被允许使用应用 A 的用户也很容易利用应用 B 通过这样的欺诈操作来读取数

据。

发明内容

本发明的一个目标是要提供一种数据保护程序及数据保护方法，用来有效地防止对受保护资源的未授权访问，即使在所述资源正受到经授权的访问时也要提供这种保护。

为了实现上述目标，提供了一种数据保护程序用于保护存储在受保护资源中的数据。该数据保护程序允许一台计算机执行一个处理序列，包括：在一张访问许可管理表中登记关于能够访问受保护资源的程序的识别信息；如果接收到一个对受保护资源的访问请求，就获取关于输出该访问请求的请求来源程序的识别信息；根据关于该请求来源程序的识别信息是否已经被登记在访问许可管理表中，来决定是否允许对受保护资源进行访问；以及如果对受保护资源的访问被许可，就响应于访问请求处理受保护资源中的数据。

为了实现上述目标，还提供了一种用于保护存储在受保护资源中的数据的方法，该方法包括：在一张访问许可管理表中登记关于能够访问受保护资源的程序的识别信息；如果接收到一个对受保护资源的访问请求，就获取关于输出该访问请求的请求来源程序的识别信息；根据关于该请求来源程序的识别信息是否已经被登记在访问许可管理表中，来决定是否允许对受保护资源进行访问；以及如果对受保护资源的访问被许可，就响应于访问请求处理受保护资源中的数据。

本发明的以上及其他的目标、特性和优点将通过下面结合附图的说明变得明显，各附图以举例形式示出了本发明的优选实施例。

附图说明

图 1 示出了体现本发明原理的方框图；

图 2 示出了本发明一个实施例中所使用的计算机硬件配置的方框图；

图 3 示出了用来提供文件保护功能的一种配置的方框图；

图 4 示出了访问许可管理表的数据结构;

图 5 示出了保护资源管理表的数据结构;

图 6 示意性地示出了当一个客户标识符已被登记时所执行的访问过程;

图 7 示意性地示出了当一个客户标识符未被登记时所执行的访问过程;

图 8 示出了本发明实施例的总工作流程的流程图;

图 9 示出了一张原理图, 表示登记一个待监视的文件夹的过程;

图 10 示出了登记一个待监视文件夹过程的处理序列的流程图;

图 11 示出了一张原理图, 表示登记一个应用的过程;

图 12 示出了登记一个应用过程的处理序列的流程图;

图 13 示出了一张原理图, 表示访问一个文件的过程;

图 14 示出了访问文件过程的处理序列的流程图;

图 15 示出了一张原理图, 表示取消应用登记的过程;

图 16 示出了取消应用登记过程的处理序列的流程图;

图 17 示意性地示出了利用一个特定的硬件/环境值来保护文件的访问过程; 以及

图 18 示出了一张流程图, 表示利用启动器应用的文件保护过程的总工作流程。

具体实施方式

下面, 将参照附图来说明本发明的一个典型实施例。

首先将说明本发明应用于该实施例的概况, 接着再给出该实施例的具体细节。

图 1 以框图形式示出了本发明的原理。如图 1 中所示, 依照本发明的一个数据保护程序是要用来监视对受保护资源 1 的访问, 并保护存储在资源 1 中的数据 1a, 该程序允许计算机执行下面所要描述的一个过程。在图 1 所示的例子中, 假定数据 1a 以加密形式存储在资源 1 中, 以保护自己不受未经授权的访问。

首先，关于能够访问资源 1 的一个程序的识别信息 2a 被登记在一张访问许可管理表 3 中（步骤 S1）。在图 1 所示的例子中，“程序 A”被登记为关于能访问资源 1 的一个程序的识别信息 2a。关于一个程序的识别信息可以是该程序的程序名、执行该程序的进程的进程名、该进程的标识符（进程 ID）、该进程的激活时间，等等。

当登记识别信息 2a 时，一个密钥 2b 与识别信息 2a 一起被登记到访问许可管理表 3 中。密钥 2b 可以是一个值，该值是由请求来源程序 2 被激活时用户所输入的口令唯一确定的。因此就保证了不会产生同样的密钥，除非输入了相同的口令。

此后，当接收到一个要访问资源 1 的访问请求 2c 时，就获取关于输出访问请求 2c 的请求来源程序 2 的识别信息 4（步骤 S2）。

对资源 1 的访问请求 2c 可以通过监视对资源 1 的访问而检测到。例如，监测一个资源的名称（一个驱动器名、一个文件夹名、一个设备名，等等），该资源是访问请求中的一个访问目的地，接着对监测到的名称与资源 1 的名称之间的对应关系进行核对。

然后，根据有关请求来源程序 2 的识别信息 4 是否已经被登记在访问许可管理表 3 中，来决定是否准许对资源 1 的访问（步骤 S3）。在图 1 所示的例子中，由于请求来源程序 2 的识别信息 2a 已经预先登记过，因此对资源 1 的访问就被准许了。如果访问请求是由其识别信息还未被登记在访问许可管理表 3 中的程序发出的，那么它的访问请求就会被拒绝。

如果对资源 1 的访问被准许了，那么就会响应于访问请求 2c 对资源 1 中的数据 1a 进行处理（步骤 S4）。举例来说，如果访问请求 2c 是请求写入由请求来源程序 2 生成的数据 1b，那么就从访问许可管理表 3 中取出与识别信息 4 相关的密钥 5，并用密钥 5 对数据 1b 加密。接着再将加密数据 1a 存储到资源 1 中。如果访问请求 2c 是请求读取数据 1a，那么就从访问许可管理表 3 中取出与识别信息 4 相关的密钥 5，并用密钥 5 对加密数据 1a 进行解密。接着再将解密数据 1b 传送给请求来源程序 2。

在依照上述的数据保护程序在计算机上执行这样的处理期间，仅当发出访问请求 2c 的请求来源程序 2 的识别信息 4 预先被登记在访问许可管理表 3 中时，才允许访问，并且根据访问请求 2c 来访问资源 1 中的数据。

另外，当识别信息被登记在访问许可管理表 3 中时，一个用来加密和解密数据的密钥也连同识别信息一起被登记到访问许可管理表 3 中。因此，即使未经授权的第三方为了操纵目的而将关于它自己程序的识别信息登记到访问许可管理表 3 中，资源 1 中的数据 1a 也不能被解密，除非密钥的一致性被确认。这样，资源 1 中数据 1a 的安全性就得到了保证。

能被登记到访问许可管理表 3 中的密钥可以包括作为参数而来自被允许存取访问许可管理表 3 的程序的输入、预定用户组的组密钥、以及对于运行文件保护系统的本地机独一无二的、被包含在一个密钥生成逻辑中的值（硬盘 ID，硬标记 ID，等等）。

一台安装了上述数据保护程序的计算机的系统管理员给予被允许访问保护数据的用户一种权限，让他能够使用被准许访问资源 1 的程序。可以例如按照以下过程给予用户使用程序的权限：

为了给予用户使用程序的权限，关于受保护资源的信息以及关于被允许访问该资源的应用的信息被彼此关联在一起，并登记在一个表文件或是类似文件中。关于拥有使用应用程序权限的用户的信息被作为各个应用程序的验证信息登记在该表文件或类似文件中。

通过给予用户使用程序的权限，用户就被允许访问一个受保护的资源，该资源可通过这些进行访问，用户可利用这些程序输入和输出数据。举例来说，当依照本发明的一台计算机系统接收到来自一个用户的启动一个应用程序的指令时，该计算机系统就会查看一个表文件，该文件中含有关于受保护资源的登记信息、关于应用程序的登记信息，以及登记的验证信息，该计算机系统再根据表文件中的登记信息确认该用户是否为该应用程序的合法用户以及该应用程序是否能够访问该资源。如果能够访问该资源的应用被合法用户激活，那么计算机系统

就生成一个密钥并将该密钥登记在访问许可管理表 3 中。这样，每个用户就只能访问该用户被授权使用资源。

由某个应用存储在资源 1 中的一个文件或是其他数据被该应用生成一个密钥加密。因此，尝试从一个非正当启动的应用去访问存储在资源 1 中的文件是不能解密该文件的。从而就可以防止和监视根据未被允许访问资源 1 的程序的操作来对信息的未授权处理及泄漏。换句话说，一个被准许访问文件信息的合法用户，会被禁止通过经由系统管理员所不认可的程序的未授权操作来越权控制资源 1。

下面将对本发明的典型实施例进行具体说明。

图 2 以框图形式示出了计算机 100 的硬件配置，该计算机被用于本发明的实施例中。计算机 100 整体由一个 CPU（中央处理单元）101 控制。CPU 101 通过总线 107 与 RAM（随机存取存储器）102、存储设备 103、图形处理器 104、输入接口 105 以及通信接口 106 相连。

RAM 102 临时存储由 CPU 101 执行的 OS（操作系统）程序和应用程序的至少一部分。RAM 102 还存储各种需要由 CPU 101 进行处理的数据。存储设备 103 可能包括例如一个硬盘驱动器（HDD），它存储 OS、各种驱动程序和应用程序。

一台显示器 11 被连接到图形处理器 104 上。图形处理器 104 根据来自 CPU 101 的指令在显示器 11 的屏幕上显示图像。键盘 12 和鼠标 13 连接在输入接口 105 上。输入接口 105 通过总线 107 将从键盘 12 和鼠标 13 上输入的信号传送给 CPU 101。

通信接口 106 连接到网络 10 上。通信接口 106 通过网络 10 向其它计算机传送数据并从其它计算机接收数据。

以上硬件配置能够实现根据本发明实施例的功能。为了实现根据本发明实施例的处理功能，要在计算机 100 中安装一个驱动程序。当计算机 100 执行该驱动程序时实现的处理功能下面将被称为“驱动器”，而当计算机 100 执行应用程序时实现的功能称为“应用”。

下面将说明为了实现根据本发明实施例的文件保护功能而在计算机 100 上构造的处理功能。

图3以框图形式示出了一种用来实现文件保护功能的配置。如图3所示,计算机100包含了一张访问许可管理表210、一张保护资源管理表220、一个应用230和一个驱动器240。根据本发明的实施例,假设被保护资源可以在文件夹(目录)基础上指定。因此,由与存储设备103相关的文件系统定义的若干个文件夹111至114中,任何需要的文件夹都可以被指定为受保护资源。文件夹111中包含多个文件111a、111b……。其他文件夹112至114也包含若干个文件。在图3所示的例子中,文件夹111的识别信息为“文件夹a(folder a)”,文件夹112的识别信息为“文件夹b(folder b)”,文件夹113的识别信息为“文件夹c(folder c)”,而文件夹114的识别信息为“文件夹d(folder d)”。

访问许可管理表210中包含登记信息,该信息被用作判定一个应用是否被准许访问存储设备103的准则。更具体地说,该登记信息包含了应用的识别信息、加密密钥以及用来准许应用访问存储设备103的资源。

保护资源管理表220中包含了关于受保护资源的识别信息。例如,该识别信息可以是作为受保护资源的文件夹的名称。

应用230具有根据用户请求提供服务的功能。例如,应用230可以是包括字处理程序、电子表程序等等在内的多种程序中的任何一种。应用230响应于用户的控制输入生成一个文件。为了将一个生成的文件存储到存储设备103中,应用230输出一个访问请求,以向存储设备103写入生成的文件。要查看存储在存储设备103中的文件,应用230输出一个访问请求,以读取所要查看的文件。

为了保护应用230所生成的文件,应用230接收用户输入的一个口令并进行用户验证。应用230生成一个根据所输入的口令唯一确定的密钥,并通过驱动器240在访问许可管理表210中设置应用230的识别信息、密钥,以及要访问的文件夹的识别信息。

当应用230输出一个写文件的访问请求时,驱动器240就将文件存储到存储设备103中。如果作为文件存储目的地的文件夹被指定为

受保护资源，并且应用 230 对该文件夹的访问是被许可的，那么驱动器 240 就会加密要存到该文件夹中的文件。

当应用 230 输出一个读文件的访问请求时，驱动器 240 就从存储设备 103 获取该文件并将其传送给应用 230。如果存储该文件的文件夹被指定为受保护资源，并且应用 230 对作为存储目的地的该文件夹的访问是被许可的，那么驱动器 240 就会解密所获取的文件。

为了向作为受保护资源的文件夹中写入文件以及从其中取出文件，驱动器 240 具有一个数据表设置单元 241、加密/解密判定单元 242、访问许可/禁止判定单元 243、以及加密/解密处理器 244。

数据表设置单元 241 响应应用 230 的请求，如文件夹监视请求，将数据登记到访问许可管理表 210 和保护资源管理表 220 中或是从其中删除数据。

加密/解密判定单元 242 响应应用 230 的文件访问请求（文件存储请求或是文件查看请求），决定文件是否需要被加密或是解密。更具体地说，加密/解密判定单元 242 要判定文件访问请求中的访问目标（文件存储目的地中的文件夹或是存有待查看文件的文件夹）是否已经在保护资源管理表 220 中被指定为受保护资源。如果访问目标是一个受保护资源，那么加密/解密判定单元 242 就判定该文件需要被加密或解密。

如果加密/解密判定单元 242 判定一个文件需要被加密或解密，那么访问许可/禁止判定单元 243 就要获取关于发出了该文件访问请求的应用 230 的识别信息。该识别信息可以是例如执行应用 230 的进程的标识符（进程 ID）。然后，访问许可/禁止判定单元 243 决定对于受保护资源的文件访问请求是否被准许。更具体地说，如果匹配关于应用的识别信息与访问目标的文件夹结合的信息已经被登记在访问许可管理表 210 中，那么访问许可/禁止判定单元 243 就会允许对文件进行访问。

如果访问许可/禁止判定单元 243 准许了对于受保护资源的文件访问请求，加密/解密处理器 244 就会对文件访问请求所指定的文件进

行加密或解密。更具体地说，如果文件访问请求是一个文件存储请求，那么加密/解密处理器 244 就对文件访问请求所指定的文件进行加密，并将加密文件保存在受保护的指定文件夹中。如果文件访问请求是一个文件查看请求，那么加密/解密处理器 244 就从受保护的文件夹中取出指定的文件，并解密该文件。

下面将说明保存在访问许可管理表 210 及保护资源管理表 220 中数据的具体细节。

图 4 示出了访问许可管理表 210 的一种数据结构的例子。访问许可管理表 210 有一列客户标识符、一列加密密钥和一列允许访问的资源。列与列之间按行并排放置的信息项彼此之间相关联。

客户标识符列包含处理功能的识别信息（客户标识符），处理功能比如作为一个客户被执行的应用 230。客户标识符可以是例如进程 ID 或是执行文件名。在本实施例中，作为客户工作的各进程的 ID 被设置在客户标识符列中。

加密密钥列包含预定数据长度的密钥。每个密钥代表了由一个口令唯一生成的信息，该口令是在允许使用应用 230 时由用户输入的。因此，一个密钥实质上是仅由一个口令生成的。

允许访问的资源列包含关于被允许访问的资源的识别信息，该信息与客户标识符及密钥相关联。在图 4 所示的例子中，允许访问的资源被设为文件夹名。放置在该列中的文件夹名包含了文件系统中到该文件夹的路径。

在图 4 所示的例子中，客户标识符“客户 A”与加密密钥“密钥 α ”及被允许访问的资源“文件夹 a”相关联。

图 5 示出了保护资源管理表 220 的一种数据结构的例子。保护资源管理表 220 含有一列保护资源信息。该列保护资源信息包含受保护资源的识别信息。在本实施例中，受保护资源被设为文件夹名。设置在该列中的文件夹名包含了文件系统中到该文件夹的路径。在图 5 所示的例子中，识别信息被表示为“文件夹 a”的文件夹 111 以及识别信息被表示为“文件夹 b”的文件夹 112 都被设置为受保护资源。

在对登记于保护资源管理表 220 中保护资源（如文件夹）的访问请求中，只有来自于客户标识符已被设置在访问许可管理表 210 中的那些客户的处理请求才会被执行。下面将说明当客户标识符已被登记在访问许可管理表 210 时和当客户标识符未被登记在访问许可管理表 210 时所执行的不同处理过程。

图 6 示意性地示出了当一个客户标识符已被登记时所执行的访问过程。当用户启动应用 230 并输入一个正确的口令作为用户验证信息时，应用 230 就会在步骤 S11 中通过驱动器 240 在访问许可管理表 210 中登记一个客户标识符（进程 ID）、一个密钥和一个资源名（文件夹名）。

例如，假定关于受保护资源的信息以及关于被允许访问那些受保护资源的应用的信息已经被相互关联起来并登记在一个表文件中，还假定被授权使用各个应用程序的用户的信息（包括口令和用户标识符）已被作为验证信息登记在该表文件中。当用户输入一个口令，就会根据该用户口令是否已被登记在验证信息的表文件中来对用户进行验证。如果用户被判定为合法用户，接着就会根据表文件来确定用户被授权使用的应用程序所能访问的受保护资源，该表文件中包含了关于受保护资源的信息以及关于应用程序的信息，它们彼此相关联。执行应用程序的进程的客户端标识符（进程 ID）和取决于口令的密钥与受保护资源的资源名（文件夹名）相关联，并被登记在访问许可管理表 210 中。

随后，应用 230 在步骤 S12 中输出对文件夹 111 中的文件 111a 的访问请求。该访问请求可以是请求生成文件 111a，请求查看文件 111a，请求更新文件 111a，以及请求删除文件 111a。从应用 230 发出的访问请求被传送给驱动器 240。

驱动器 240 响应于应用 230 所发出的访问请求，获取应用 230 的进程 ID。驱动器 240 查看访问许可管理表 210，并从中检索对应于所获取的进程 ID 的客户标识符。然后在步骤 S13 中驱动器 240 获取一个对应于检索出的客户标识符的密钥 α 。

驱动器 240 在步骤 S15 中处理访问请求所指定的文件 111a, 同时用获取的密钥 α 加密或解密文件 111a。举例来说, 如果访问请求是一个生成并保存文件 111a 的请求, 那么驱动器 240 就用密钥 α 加密由应用 230 传送来的数据, 再将加密数据作为文件 111a 保存在文件夹 111 中。

如果访问请求是请求查看已经存储在文件夹 111 中的文件 111a, 那么驱动器 240 就用密钥 α 将文件 111a 解密为明文数据, 再将这些明文数据传送给应用 230。

图 7 示出了当一个客户标识符未被登记时所执行的访问过程。举例来说, 假设这样一种情况, 在步骤 S21 中, 应用 231 发出对文件夹 111 中文件 111a 的访问请求, 而它的客户标识符却并未登记在访问许可管理表 210 中。由于应用 231 的客户标识符并未登记在访问许可管理表 210 中, 因此在步骤 S22 中, 驱动器 240 拒绝响应于访问请求对文件 111a 进行处理。

如上所述, 由于应用 230 的客户标识符 (进程 ID) 以及相应的密钥被事先登记, 基于所登记的客户标识符及密钥而指定的文件夹 111 中文件 111a 就被保护起来免受其它应用 231 的访问。

下面将说明指定一个受保护资源以及处理保护状态下的文件的过程细节。

图 8 是本发明实施例整个工作流程的流程图。当一种处理功能如登记一个客户标识符的功能可以被包含在应用 230 中时, 就能应用图 8 中所示的工作流程。为了将一种处理功能封装到应用 230 中, 需要准备必要的处理功能作为库 (用于多种软件的通用功能及程序), 而且要设定该库在应用 230 工作时被执行。下面将按照连续步骤标号说明图 8 中所示的处理过程。

[步骤 S31] 当用户输入一个口令并使用一个控制输入启动应用 230 时, 应用 230 通过驱动器 240 登记待监视的文件夹并启动一个文件夹监视机制。具体地说, 被设置为受保护资源的文件夹有关的识别信息由应用 230 登记到保护资源管理表中。被设置为受保护设备的文

文件夹可以是用户指定的所需文件夹或用于应用 230 的规定文件夹。这个登记过程仅在一个文件夹最初被指定为受监视对象时才执行一次。响应于该登记过程，驱动器 240 执行一个登记待监视文件夹的过程。

更具体地说，假定关于受保护资源的信息以及关于被允许访问那些受保护资源的应用程序的信息都已经被彼此关联并登记在一个表文件中，还假定被授权使用各个应用程序的用户的信息（包括口令和用户标识符）都已经被作为验证信息登记在表文件中。当用户输入一个口令并使用一个控制输入来启动应用 230，就会根据该用户口令是否已被登记在验证信息表文件中来验证用户。如果该用户被用户验证确认为合法用户，那么就会根据表文件来决定该用户被授权使用的应用程序所能访问的受保护资源，所述的表文件中含有关于受保护资源的信息以及关于应用程序的信息，它们彼此相关联。接着将受保护资源的资源名（文件夹名）登记到保护资源管理表 220 中。

[步骤 S32] 在待监视文件夹被登记且文件夹监视机制被启动之后，应用 230 会激活一种功能（例如字处理程序），该功能是应用用户的控制输入所要执行的。这样的功能会被激活为一个进程。该进程会由 OS（操作系统）分配识别信息（进程 ID）。

[步骤 S33] 应用 230 向驱动器 240 输出一个登记请求，以登记启动进程时所分配到的进程 ID。响应于该登记请求，驱动器 240 会执行一个应用登记进程。

在应用登记进程中，进程 ID 被作为一个客户标识符登记在访问许可管理表 210 中，该表由驱动器 240 管理。这时，应用 230 会生成一个对应于用户所输入口令的密钥。所生成的该密钥与客户标识符被关联登记在访问许可管理表 210 中。在步骤 S31 中被指定为受保护资源的文件夹的识别信息被当作允许访问的资源，与客户标识符关联登记在访问许可管理表 210 中。

[步骤 S34] 应用 230 通过驱动器 240 输出一个对待监视文件夹中某个文件的访问请求，如请求读取一个文件或是请求写入一个文件。响应于该访问请求，驱动器 240 执行一个访问进程。如果要读取文件

中的数据，那么驱动器 240 解密该文件；如果要將数据写入文件，那么驱动器 240 就加密该文件。

[步骤 S35] 应用 230 通知驱动器 240 应用已完成，也就是说，向驱动器 240 发出一个应用登记取消请求。响应于该应用登记取消请求，驱动器 240 执行一个进程以取消对于该应用的登记。更具体地说，驱动器 240 会从访问许可管理表 210 中删除对应于应用 230 的客户标识符，以及与该客户标识符相关的密钥和文件夹识别信息。

[步骤 S36] 应用 230 被终止。下面将说明按图 8 所示顺序当应用 230 发出处理请求时，驱动器 240 所执行处理步骤的细节。

首先将说明步骤 S31 中登记一个待监视文件夹的过程细节。

图 9 概念性地示出了登记一个受保护文件夹的过程。如图 9 所示，在步骤 S41 中应用 230 向驱动器 240 发出一个文件夹监视请求。接着，在步骤 S42 中驱动器 240 将文件夹的识别信息作为受保护资源的信息登记在保护资源管理表 220 中。

图 10 示出了登记一个受保护文件夹过程的处理序列。下面将按照连续的步骤编号说明图 10 中所示的处理序列。

[步骤 S51] 驱动器 240 接收到应用 230 发出的文件夹监视请求。驱动器 240 将接收到的文件夹监视请求传送给数据表设置单元 241。被传送给数据表设置单元 241 的文件夹监视请求中包含关于待监视文件夹的识别信息。

[步骤 S52] 数据表设置单元 241 确定被指定要监视的文件夹是否已经是被监视的目标了。更具体地说，数据表设置单元 241 检索保护资源管理表 220 并确定被文件夹监视请求所指定要监视的文件夹的识别信息是否已经被登记在保护资源管理表 220 中。如果该文件夹的识别信息已经被登记在保护资源管理表 220 中，那么该文件夹就已经是被监视的目标了。如果没有，那么该文件夹还不是被监视的目标。如果被指定要监视的文件夹已经是一个被监视的目标了，那么该处理过程返回应用 230。如果被指定要监视的文件夹还不是一个被监视的目标，那么处理过程将进入步骤 S53。

[步骤 S53] 数据表设置单元 241 将文件夹监视请求所指定文件夹的识别信息登记在保护资源管理表 220 中。随后，处理过程返回应用 230。

下面将说明步骤 S32 中应用激活过程的细节。

图 11 概念性地示出了登记一个应用的过程。在步骤 S61 中，应用 230 发出一个应用登记请求以登记一个应用。在步骤 S62 中，驱动器 240 检索保护资源管理表 220 并确认应用登记请求中所包含的文件夹是否要被监视。如果一个文件夹要被监视，那么在步骤 S63 中，驱动器 240 会将客户标识符、密钥以及文件夹名登记到访问许可管理表 210 中。

图 12 示出了登记一个应用过程的处理序列。下面将按照连续的步骤编号说明图 12 中所示的处理序列。

[步骤 S71] 驱动器 240 接收应用 230 所发出的应用登记请求。驱动器 240 将接收到的应用登记请求传送给数据表设置单元 241。被传送给数据表设置单元 241 的应用登记请求中包含一个客户标识符、一个密钥以及被允许访问的文件夹（访问文件夹）的识别信息。

[步骤 S72] 数据表设置单元 241 确定访问文件夹是否为被监视的目标。更具体地说，数据表设置单元 241 要确定访问文件夹的识别信息是否已经被登记在保护资源管理表 220 中了。如果该访问文件夹的识别信息已经被登记，那么该访问文件夹就是被监视的目标。如果没有，那么该访问文件夹还不是被监视的目标。如果访问文件夹是一个被监视的目标，那么该处理过程进入步骤 S73。如果访问文件夹还不是一个被监视的目标，那么处理过程将返回应用 230。

[步骤 S73] 数据表设置单元 241 确认应用 230 的客户标识符是否已经被登记在访问许可管理表 210 中。如果已经被登记，那么该处理过程返回应用 230。如果没有被登记，那么该处理过程进入步骤 S74。

[步骤 S74] 数据表设置单元 241 将包含在应用登记请求中的客户标识符、密钥以及访问文件夹的组合登记在访问许可管理表 210 中。随后，该处理过程返回应用 230。

下面将详细说明步骤 S34 中的文件访问过程。

图 13 概念性地示出了访问一个文件的过程。应用 230 在步骤 S81 中发出一个文件访问请求。该文件访问请求被驱动器 240 接收。在步骤 S82 中，驱动器 240 检索保护资源管理表 220，并确认应文件访问请求所要访问的文件是否处在受监视的文件夹中。如果所要访问的文件是受监视文件夹中的文件，那么驱动器 240 就在步骤 S83 中检索访问许可管理表 210 并确认输出文件访问请求的应用 230 是否被准许访问该文件。如果应用 230 对该文件的访问被许可，那么驱动器 240 就响应于文件访问请求访问该文件，并在步骤 S84 中向应用 230 返回结果。

图 14 示出了访问文件过程的处理序列。下面将根据连续的步骤编号说明图 14 中所示的处理序列。

[步骤 S91] 驱动器 240 接收应用 230 发出的文件访问请求。接收到的文件访问请求被传送给加密/解密判定单元 242。该文件访问请求所包含的信息代表了文件名、文件位置（关于存储该文件的文件夹的识别信息）、指令语句（表明该文件访问请求是读数据还是写数据的请求）、以及所要写入的数据（如果文件访问请求是写数据请求）。

[步骤 S92] 加密/解密判定单元 242 确定要访问的文件所处的文件夹是否是一个受监视的文件夹。更具体地说，加密/解密判定单元 242 检索保护资源管理表 220 并确定要访问的文件所处文件夹的识别信息是否已经被登记在保护资源管理表 220 中。如果已经登记，那么要访问的文件所处的文件夹是一个受监视的文件夹。如果没有登记，那么要访问的文件所处的文件夹不是一个受监视的文件夹。如果要访问的文件所处的文件夹是一个受监视的文件夹，那么该处理过程进入步骤 S94。如果要访问的文件所处的文件夹不是一个受监视的文件夹，那么该处理过程进入步骤 S93。

[步骤 S93] 驱动器 240 根据文件访问请求，借助于 OS（操作系统）中所包含的文件系统执行一个文件访问进程。

[步骤 S94] 访问许可/禁止判定单元 243 检索访问许可管理表

210, 并确定发出文件访问请求的应用 230 是否被登记为与受监视的该文件夹相关。

更具体地说, 访问许可/禁止判定单元 243 获取发出文件访问请求的应用 230 的进程 ID。该进程 ID 由 OS (操作系统) 管理, 因此访问许可/禁止判定单元 243 可以通过询问 OS 来获取该进程 ID。访问许可/禁止判定单元 243 确定应用 230 的进程 ID 以及要被访问的文件所处文件夹的识别信息的组合是否已经被登记在访问许可管理表 210 中。如果该进程 ID 和文件夹的识别信息的组合已经被登记在访问许可管理表 210 中, 那么访问许可/禁止判定单元 243 就可以判定应用 230 是一个已登记客户。

如果应用 230 是一个已登记客户, 那么该处理过程进入步骤 S96。如果应用 230 不是一个已登记客户, 那么该处理过程进入步骤 S95。

[步骤 S95] 访问许可/禁止判定单元 243 拒绝来自应用 230 的文件访问请求, 并向应用 230 返回结果。随后, 该处理过程返回应用 230。

[步骤 S96] 访问许可/禁止判定单元 243 告知加密/解密处理器 244 该文件访问请求已经被准许。加密/解密处理器 244 从访问许可管理表 210 中获取一个密钥, 该密钥与应用 230 的进程 ID 以及被访问文件所处文件夹的识别信息的组合相关。接着加密/解密处理器 244 执行一个文件访问进程, 其中包括利用所获取的密钥对被访问的文件进行文件加密或解密。

更具体地说, 如果文件访问请求是一个读取文件的请求, 那么加密/解密处理器 244 利用所获取的密钥解密该文件, 并将解密文件传送给应用 230。如果文件访问请求是一个写入文件的请求, 那么加密/解密处理器 244 用获取的密钥加密要写入的数据, 将这些数据形成一个文件, 并将该文件存储在受监视的文件夹中。随后, 该处理过程返回应用 230。

下面将说明步骤 S35 中取消一个应用登记的过程。

图 15 概念性地示出了取消一个应用登记的过程。在步骤 S101 中, 应用 230 发出一个应用登记取消请求。在步骤 S102 中, 驱动器 240 删

除登记在访问许可管理表 210 中的信息。

图 16 是一张流程图，示出了取消一个应用登记的过程的处理序列。下面将按照连续的步骤编号说明图 16 中所示的处理序列。

[步骤 S111] 驱动器 240 获取一个来自应用 230 的应用登记取消请求。驱动器 240 将获取的应用登记取消请求传送给数据表设置单元 241。

[步骤 S112] 数据表设置单元 241 确定应用 230 的进程 ID 是否已经被登记在访问许可管理表 210 中。如果已经登记，那么该处理过程进入步骤 S113。如果没有登记，那么该处理过程返回应用 230。

[步骤 S113] 数据表设置单元 241 从访问许可管理表 210 中删除应用 230 的进程 ID 以及与该进程 ID 相关的数据（密钥以及文件夹识别信息）。

另一方面，可用于加密/解密数据的密钥可以不是作为参数的来自于应用 230 的输入，而可以是分配给用户组的组密钥，以及对于运行文件保护系统的本地机独一无二的值（特定的硬件/环境值），这些值被包含在密钥生成逻辑中。这些特定的硬件/环境值可以是例如硬盘 ID、硬标记 ID 等等。

图 17 示出了利用一个特定的硬件/环境值来保护文件的访问过程。图 17 中所示的访问过程与图 6 中所示的访问过程相似，除了其中加入一个特定的硬件/环境值 250。

当用户启动应用 230 并输入一个正确的口令作为用户验证信息时，应用 230 就会在步骤 S121 中向访问许可管理表 210 登记一个客户标识符、一个密钥和一个资源名。随后，应用 230 在步骤 S122 中发出对文件夹 111 中文件 111a 的访问请求。

驱动器 240a 响应于应用 230 所发出的访问请求，获取应用 230 的进程 ID。在步骤 S123 中，驱动器 240a 检索访问许可管理表 210，并从中获取对应于客户标识符的密钥 α ，所述的客户标识符对应于所获取的进程 ID。在步骤 S124 中，驱动器 240a 还要获取一个特定的硬件/环境值 250。

驱动器 240a 利用所获取的特定硬件/环境值 250 作为用于生成加密密钥或解密密钥的辅助信息（密钥生成辅助信息）。更具体地说，驱动器 240a 将从访问许可管理表 210 中取得的密钥 α 与特定硬件/环境值 250 组合起来，从而生成一个新的密钥。接着在步骤 S125 中，驱动器 240 对访问请求所指定的文件 111a 进行处理，其中包括用生成的新密钥加密或解密数据。

由于加密/解密密钥是用特定的硬件/环境值 250 生成的，因此一个受保护资源只能由一台计算机访问，从而可以针对通过网络进行的未授权访问企图实现增强安全性的保护。

当应用 230 中包含了一种借助库来保护文件的功能时，就可运用图 8 中所示的工作流程。然而，保护文件的功能可以通过一个启动器应用实现。

图 18 示出利用了启动器应用的文件保护过程的工作流程。在图 18 所示的例子中，提供了一个启动器应用 231 和一个子应用 232。启动器应用 231 作为辅助功能，用于响应用户的控制输入来启动各种应用。子应用 232 是由启动器应用 231 启动的一个应用。子应用 232 可以是一个字处理程序、一个电子表格程序，等等。

[步骤 S131] 当用户输入一个口令并使用一个控制输入来请求启动器应用 231 启动子应用 232 时，启动器应用 231 登记一个待监视的文件夹并启动一个文件夹监视机制。更具体地说，启动器应用 231 通过驱动器 240 将要被设置为受保护资源的文件夹的识别信息登记到保护资源管理表 220 中。要被设置为受保护资源的文件夹可以是用户任选指定的文件夹，或者是用于应用 230 的规定文件夹。这个登记过程仅在一个文件夹最初被指定为监视对象时执行一次。

[步骤 S132] 在受监视文件夹被登记且文件夹监视机制被启动后，启动器应用 231 被激活。

[步骤 S133] 启动器应用 231 向 OS 发出一个请求以激活子应用 232，然后子应用 232 被激活。

[步骤 S134] 启动器应用 231 将一个进程 ID 登记在访问许可管理

表 210 中作为客户标识符,该进程 ID 是在子应用 232 被激活时分配的,而表 210 是由驱动器 240 管理的。这时,应用 230 生成一个密钥,该密钥取决于用户所输入的口令。所生成的密钥连同步骤 S134 中登记的客户标识符一起被登记在访问许可管理表 210 中。在步骤 S131 中被指定为受保护资源的文件夹的识别信息作为被允许访问的资源,连同步骤 S134 中登记的客户标识符一起被登记在访问许可管理表 210 中。

[步骤 S135] 子应用 232 通过驱动器 240 访问受监视文件夹中的文件,也就是说,从文件中读取数据或是将数据写入文件。当文件中的数据被读取,驱动器 240 解密数据。当数据被写入文件,驱动器 240 就加密文件。

[步骤 S136] 子应用 232 响应用户的控制输入而被终止。

[步骤 S137] 当子应用 232 被终止时,启动器应用 231 告知驱动器 240 子应用 232 已完成。驱动器 240 从访问许可管理表 210 中删除对应于应用 230 的客户标识符以及与该客户标识符相关的密钥和文件夹识别信息。

[步骤 S138] 结束启动器应用 231。

根据本发明的实施例,如上所述,一个受监视的应用事先被登记,而驱动器 240 选择性地控制并对应用的访问进行判定,以拒绝来自未被登记的应用的访问。因此,可以很容易地限制对于文件的访问。

系统管理员通过允许在被准许访问文件的应用的功能范围内对文件进行处理,并拒绝为其他处理目的而对文件进行的访问,就可以监控信息的未授权泄漏。

即使是一个被允许访问受保护文件的用户,也会被禁止通过无效操作即来自于未被允许访问文件的应用的访问请求来处理文件。

即使驱动器 240 本身被去掉,由一个已登记应用加密的文件在试图用另一个应用解密该文件时也不能被解密。这是因为当一个应用被登记时,就生成了一个仅能被该应用使用的密钥(用作加密密钥或是解密密钥)。

由于分配给各个被允许访问文件的应用的密钥不相同,尝试通过

一个被允许访问该文件但未被登记的应用来解密该文件是不能正确地解密文件的。因此，只有已登记应用的授权用户才能正确地解密文件信息，并能根据应用的功能修正和复制文件信息。

与最近为用于本发明的系统而开发的应用一样，常规程序也可以通过使用一个代理程序（启动器应用）简单地被包含到该系统中，所述的代理程序用于管理那些常规程序的启动、状态和完成。因此，现有的应用不需修改便可用作本实施例的应用。

如果生成密钥的过程根据各个应用来决定，那么就可以比较容易地为各个应用设计并控制关于被保护资源中文件的互操作性及独占性。因此，就可能控制用于所需应用的一组用户之间的信息共享设置。

有了上述的选择性访问控制能力，就可能构建一种系统，用来操作和管理文件信息，它具有自下而上的选择性访问控制及结合自上而下的稳健性与更高安全性的简易计划。

为了实现上述的处理功能，提供了一种数据保护程序，它描述了一台计算机所应具有的各功能的处理细节。当计算机执行该数据保护程序时，上述的处理功能就会在计算机上被执行。描述了处理细节的数据保护程序可以被记录在一种记录媒体上，该媒体可被计算机读取。这种可由计算机读取的记录媒体包括磁记录设备、光盘、磁-光记录媒体、半导体存储器，等等。所述的磁记录设备可以是硬盘驱动器（HDD）、软（磁）盘（FD）、磁带，等等。光盘可以是DVD（数字多功能光盘）、DVD-RAM、CD-ROM（只读光盘）、CD-R（可录）/RW（可重写），等等。磁-光记录媒体可以是MO（磁-光）盘等。

为了发布数据保护程序，存有数据保护程序的便携式记录媒体如DVD、CD-ROM等等可以发售。

另外，数据保护程序也可以被存储在一台服务器计算机的存储设备中，再通过网络从服务器计算机传送给其他计算机。

用来执行数据保护程序的计算机将记录在便携式记录媒体上或是从服务器计算机传送来的数据保护程序装载到例如它自己的存储设备中。接着，该计算机从存储设备中读取数据保护程序，并根据数据

保护程序执行一个处理序列。另外，该计算机也可以直接从便携式记录媒体上读取数据保护程序，并根据服务器程序执行一个处理序列。再另外，该计算机还可以在每次接收到从服务器计算机传送来的一部分数据保护程序时，根据数据保护程序执行一个处理序列。

根据本发明，如上所述，只有当输出了访问请求的请求来源程序的识别信息已经被登记在访问许可管理表中时，基于该访问请求对于受保护资源中数据的访问才能被批准，受保护资源中的数据才能根据访问请求被处理。因此，即使当受保护资源中的数据正处在被一个准许访问该数据的应用访问的状态中，从识别信息未被登记在访问许可管理表中的其他应用访问保护资源中的该数据也是要拒绝的。这样就提高了受保护资源中数据的安全性。

前面所述只是为了说明本发明的基本原理。此外，由于本领域技术人员很容易想出许多修改及变化，因此不希望将本发明限制于本文所示及所说明的确切构造及应用，相应地，所有合适的修改及等价物都可被视为落入附带的权利要求及其等价物所确定的本发明的范围内。

图1

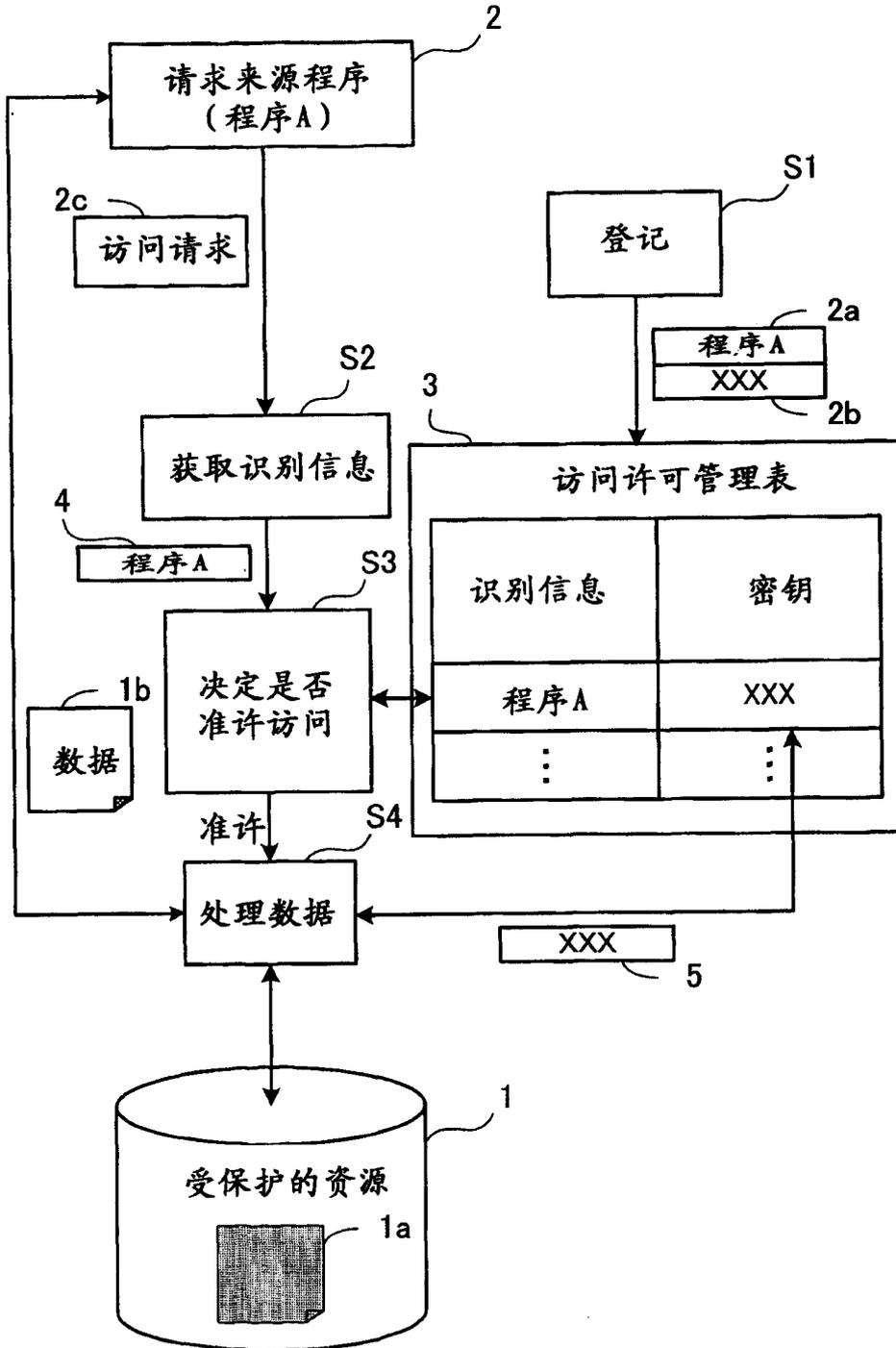


图2

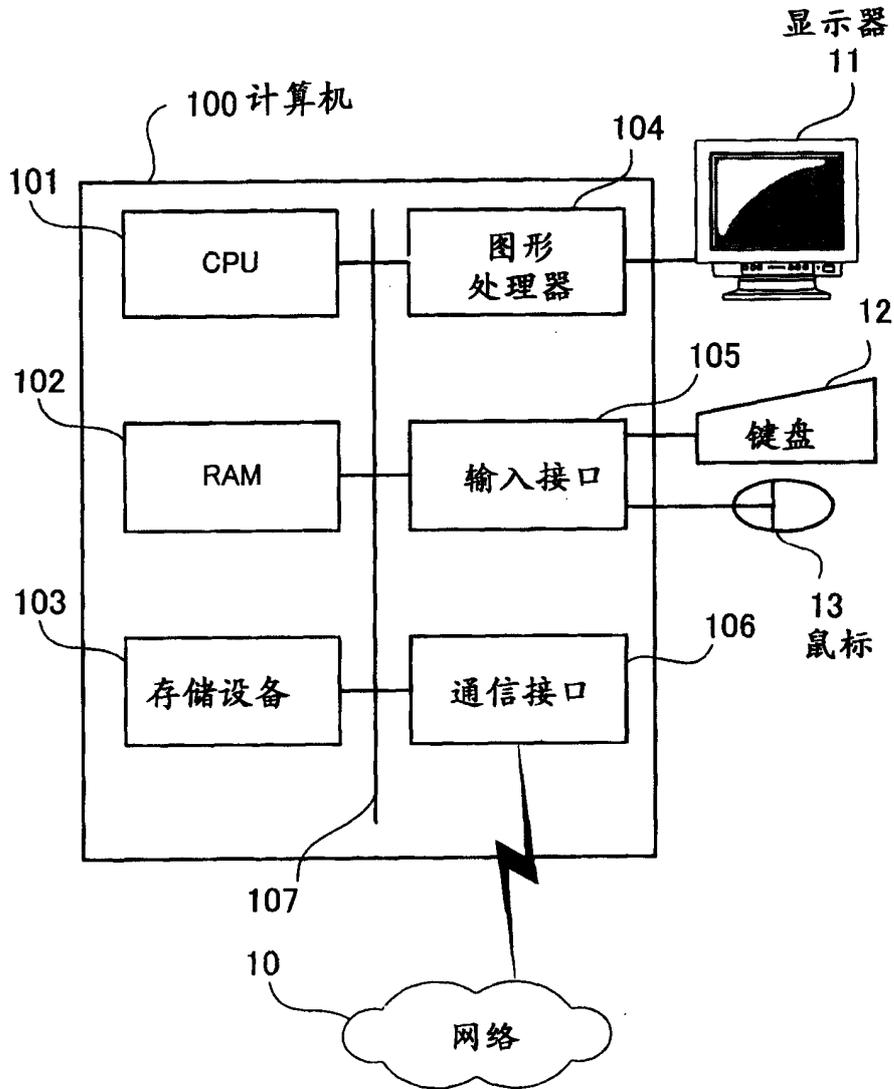


图3

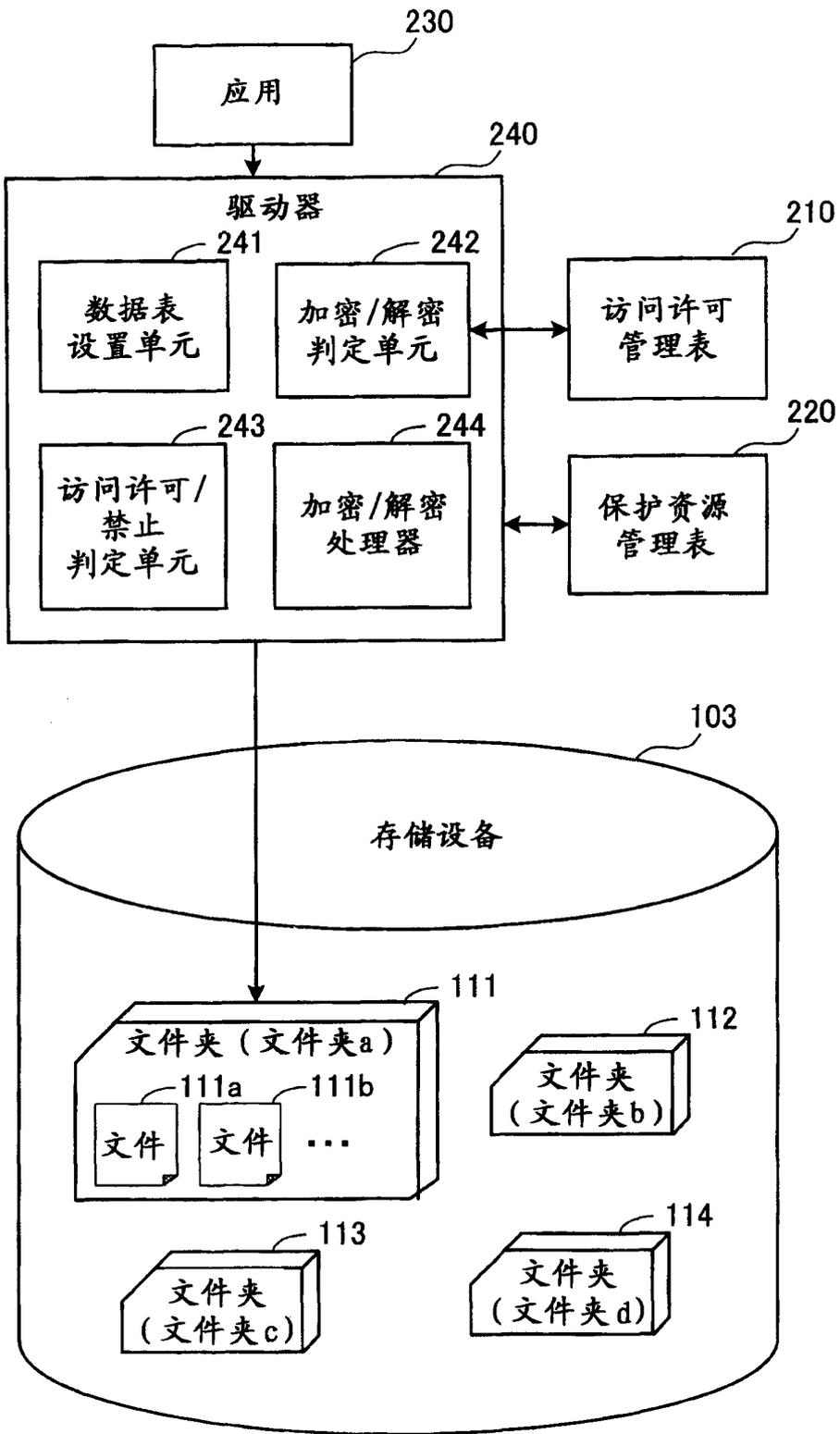


图4

210 访问许可管理表

客户标识符	加密密钥	被允许访问的资源
客户 A 客户 B 客户 C 客户 A · ·	密钥 α 密钥 α 密钥 β 密钥 α · ·	文件夹 a 文件夹 a 文件夹 a 文件夹 b · ·

图5

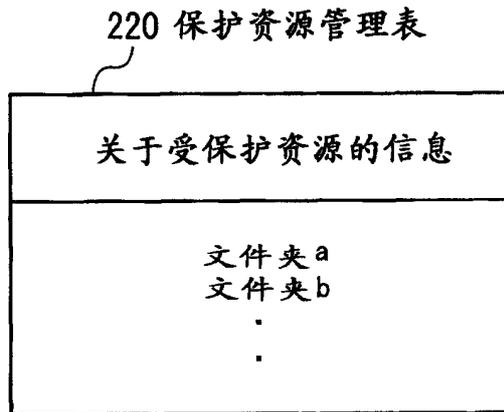
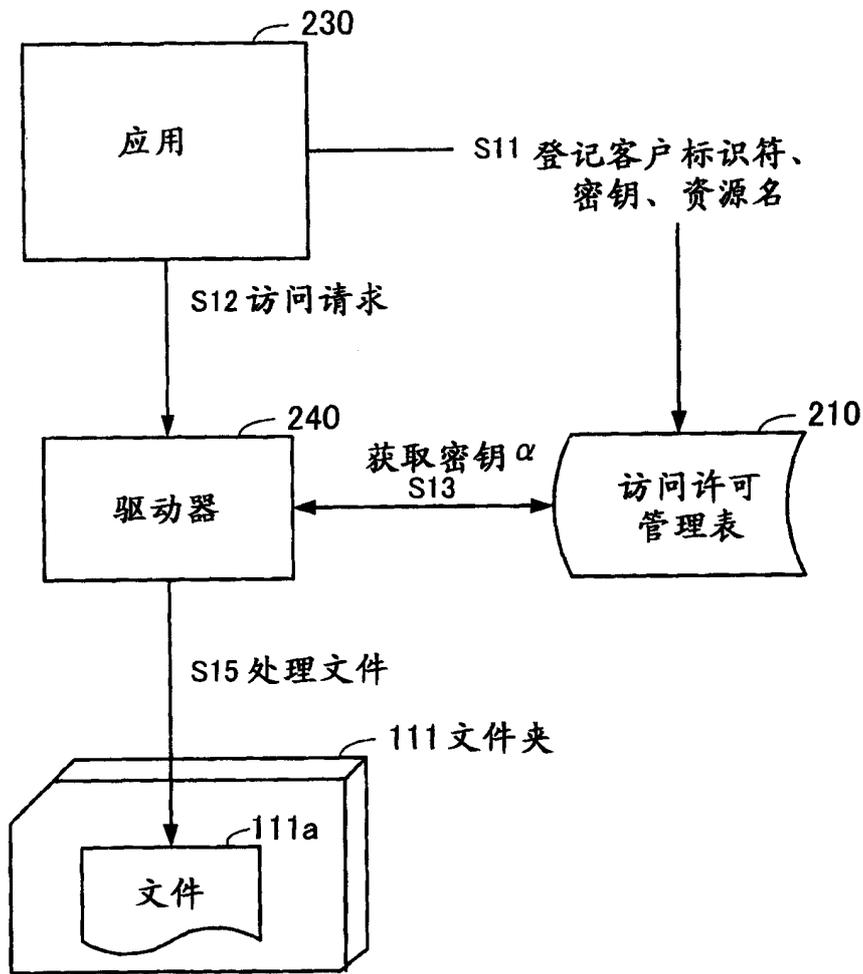
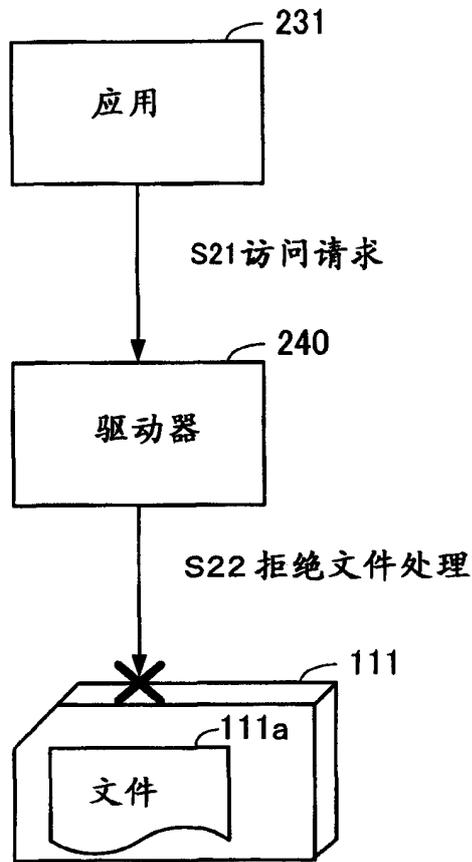


图6



[当客户标识符已被登记时]

图7



受到加密保护

[当客户标识符未被登记时]

图8

<总工作流程（当用作库时）>

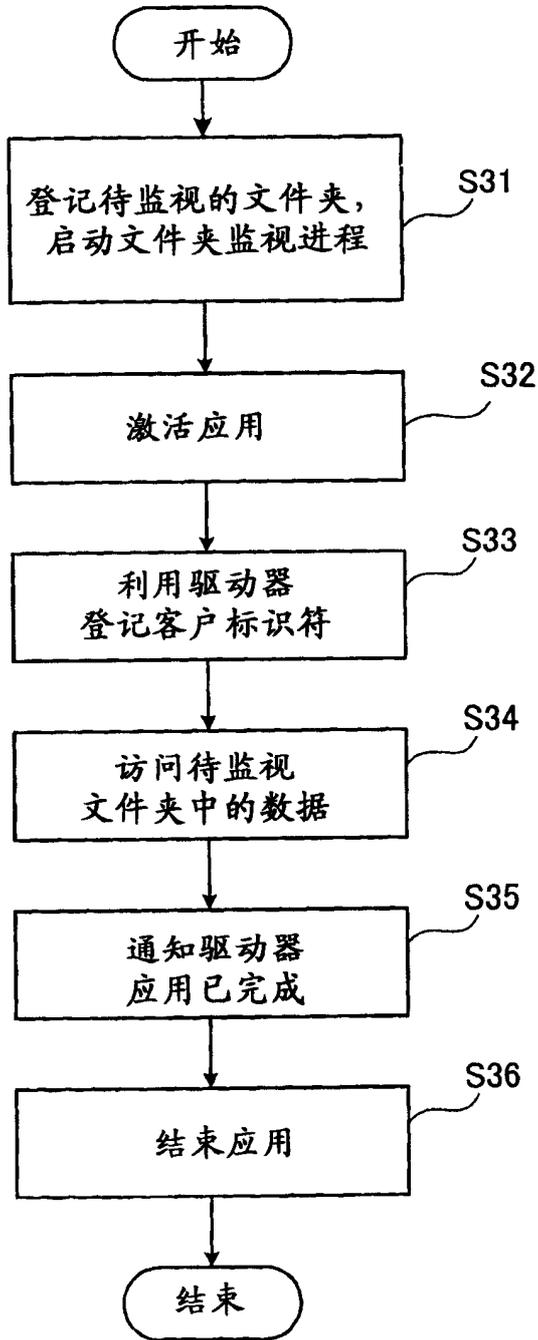
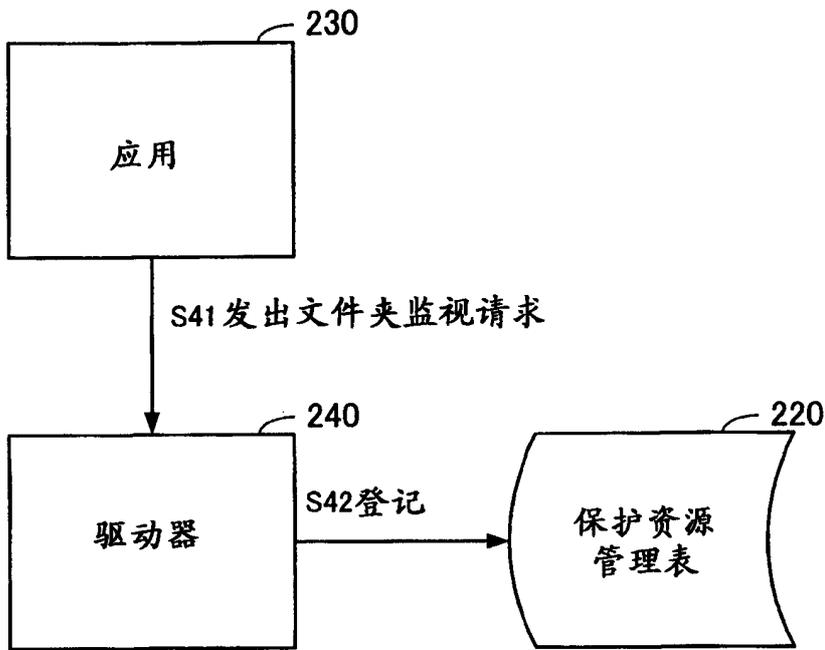


图9



[登记待监视文件夹的过程]

图10

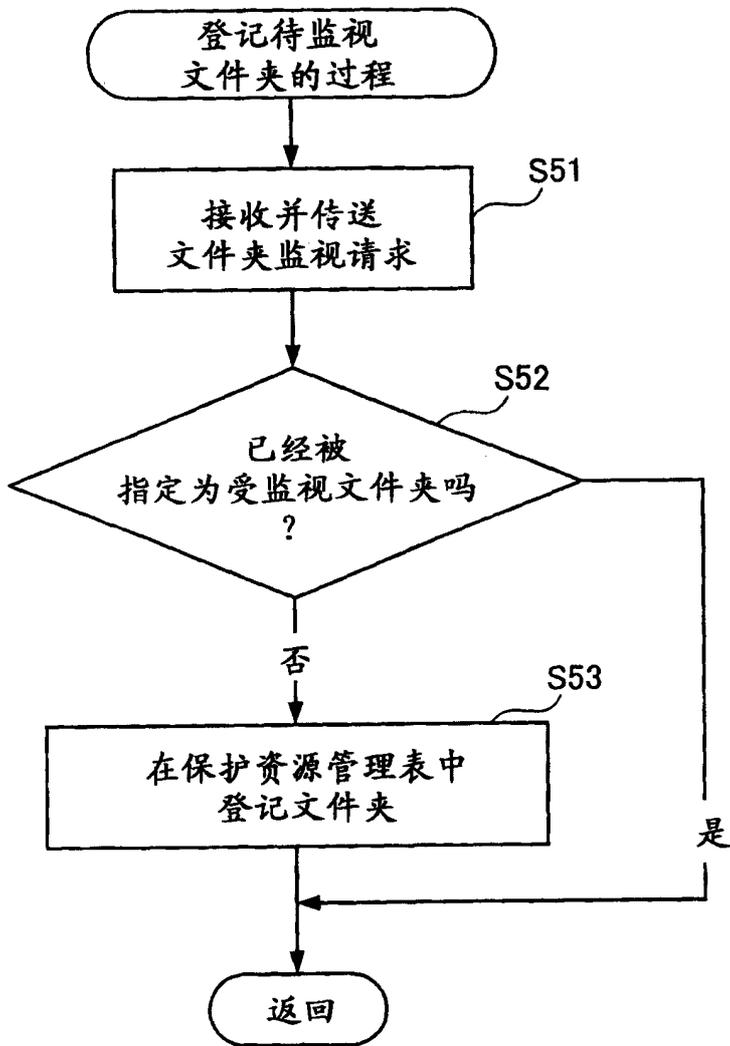
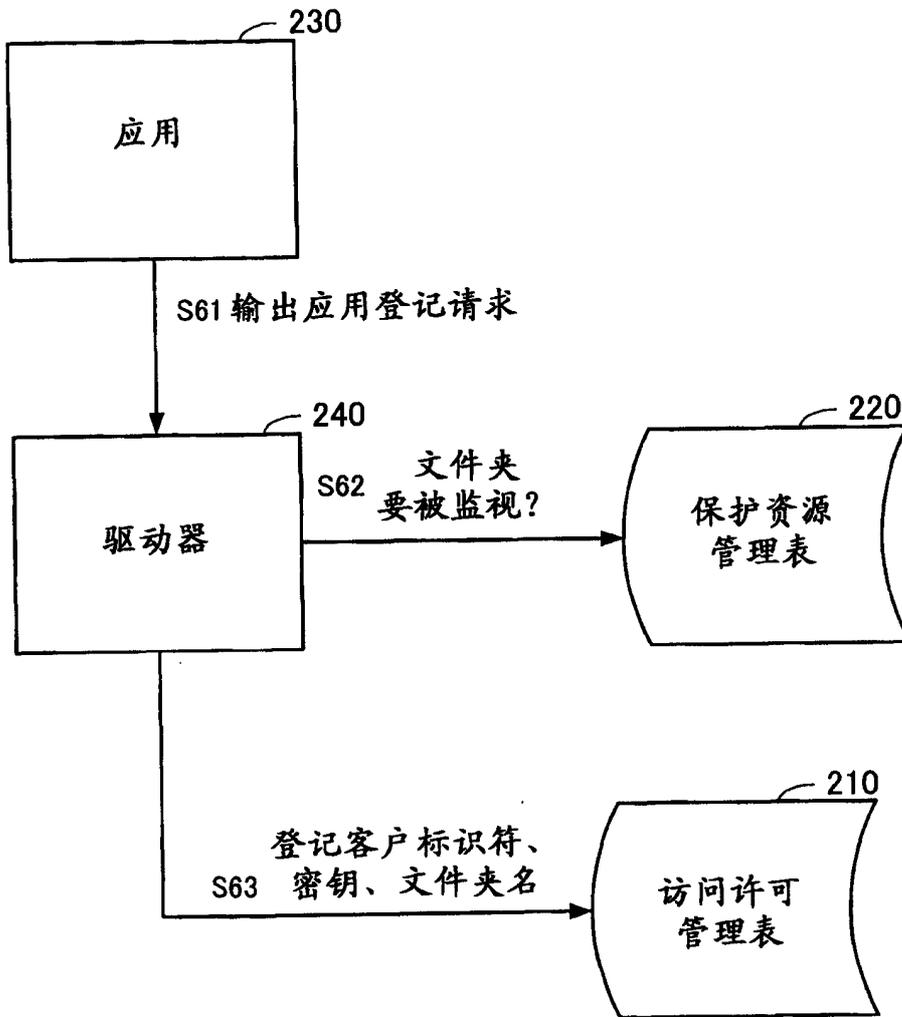
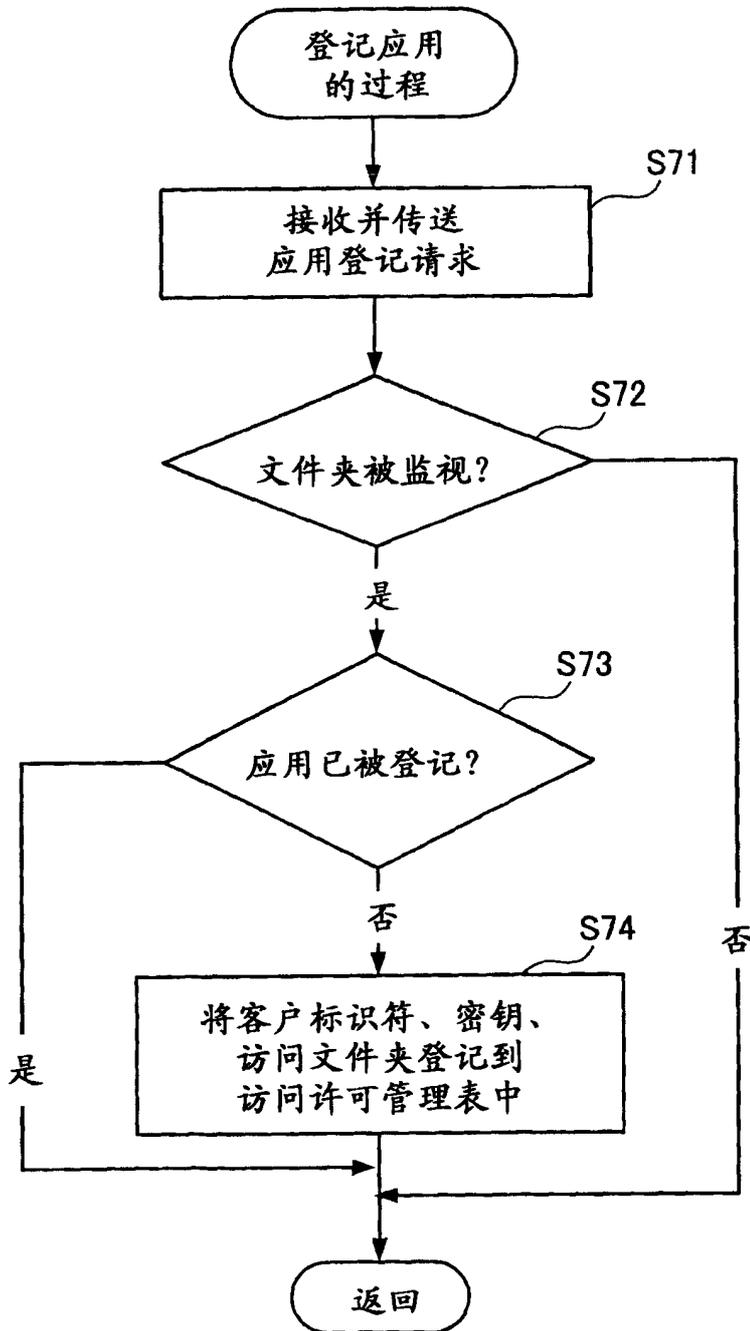


图11



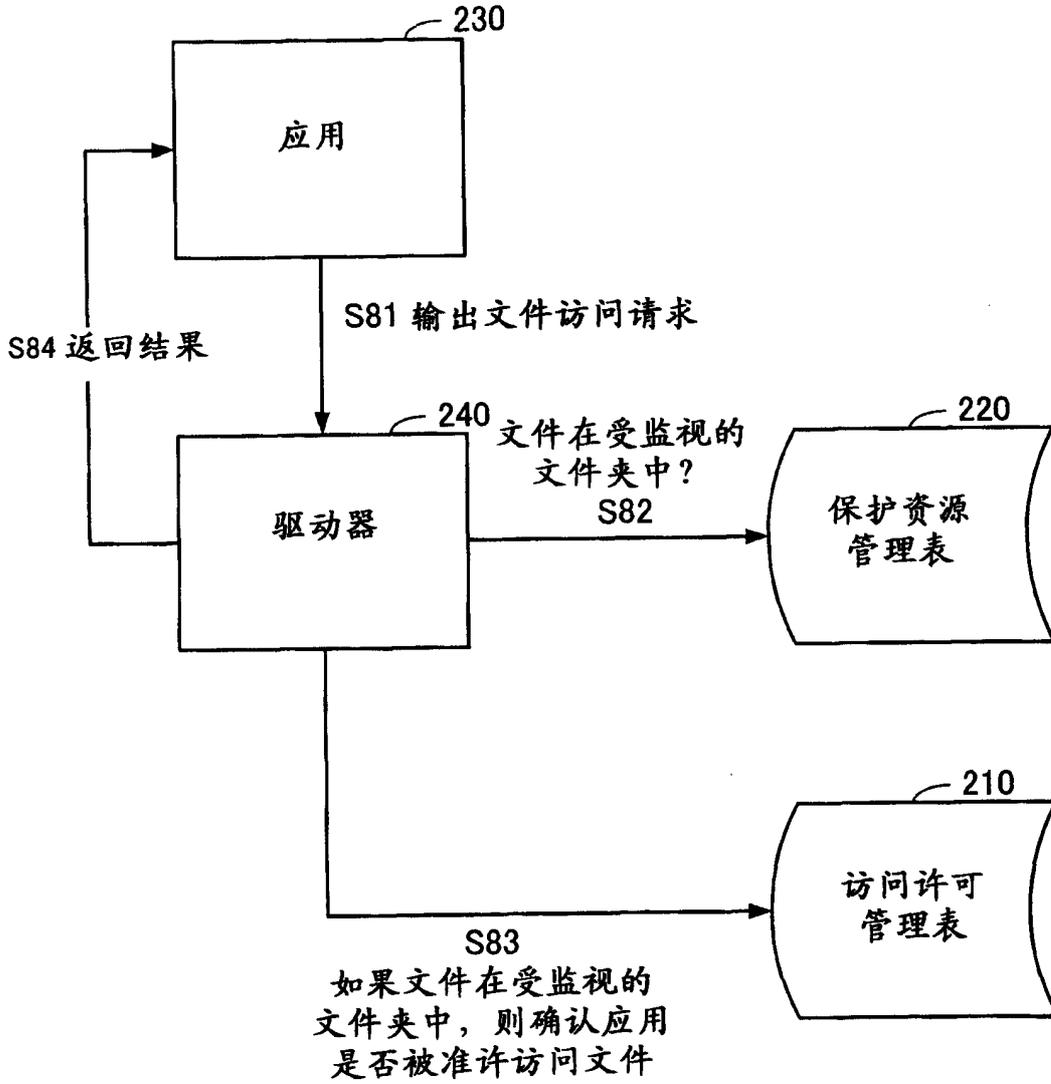
[登记应用的过程]

图12



[登记应用的过程]

图13



[访问文件的过程]

图14

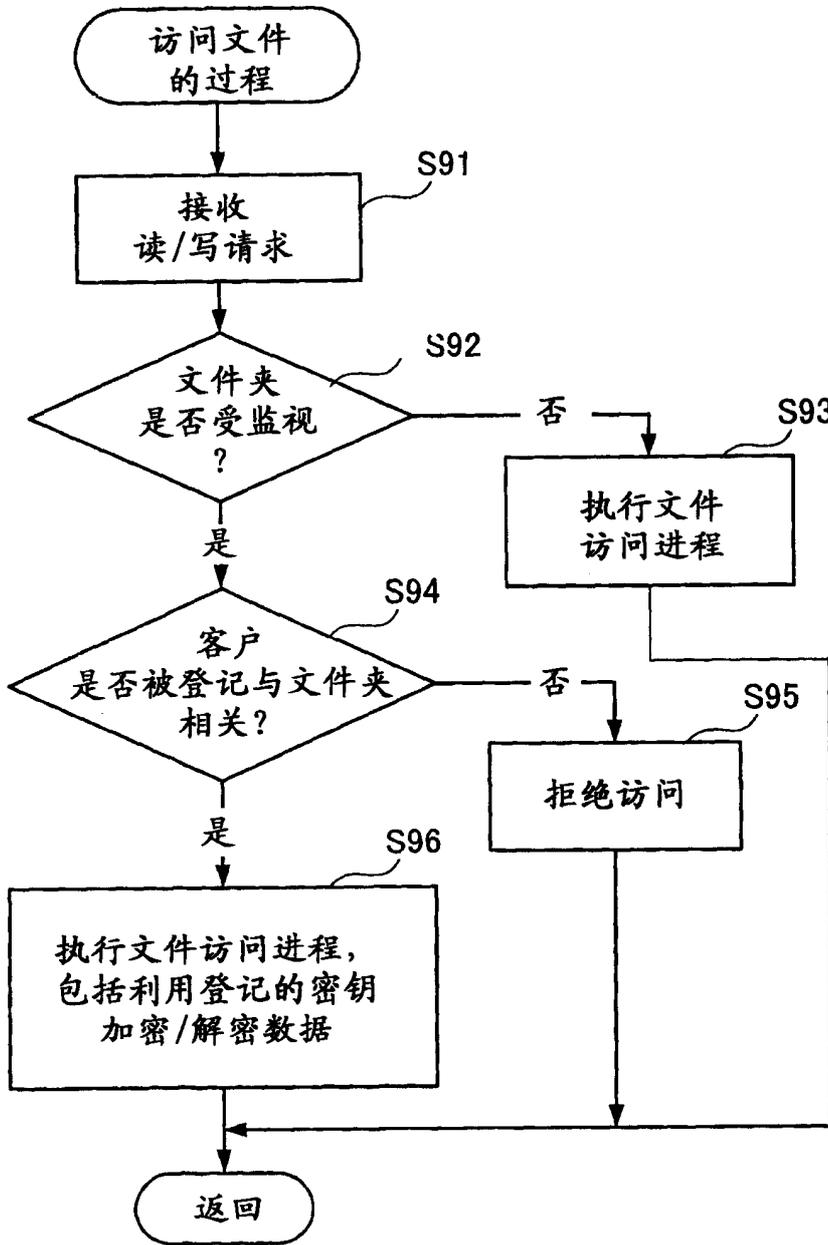
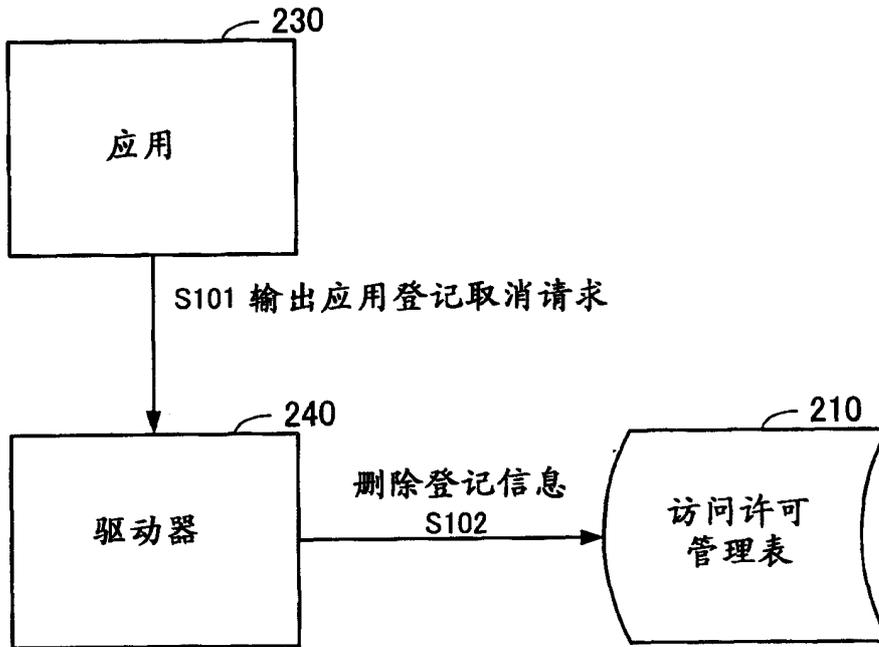


图15



[取消应用登记的过程]

图16

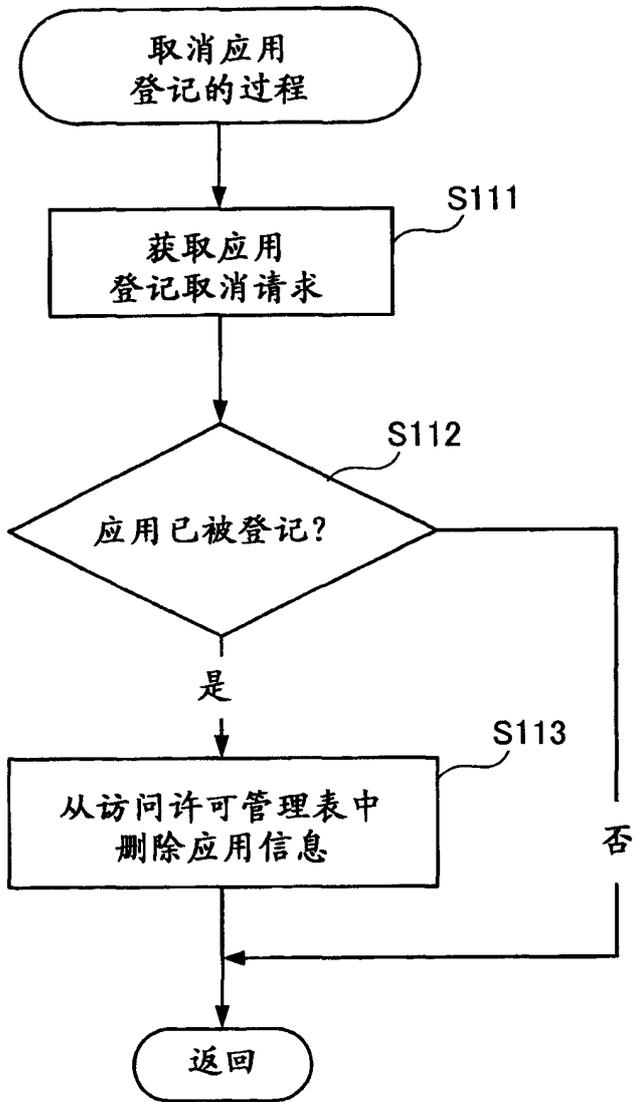


图17

