(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102117394 A
(43)申请公布日 2011.07.06

(21)申请号 201010623060.0

(22)申请日 2010.12.31

(30)优先权数据
10305005.0 2010.01.04 EP

(71)申请人 汤姆森许可贸易公司
地址 法国伊西莱穆利诺

(72)发明人 奥利维耶·库尔泰

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王波波

(51)Int.Cl.
G06F 21/22(2006.01)

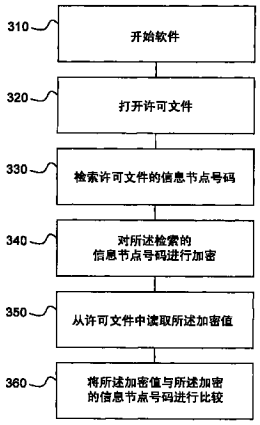
权利要求书 2 页 说明书 4 页 附图 3 页

(54)发明名称

检测是否已经复制了计算机文件的方法和装置以及能够进行这种检测的方法和装置

(57)摘要

本发明涉及一种检测是否已经复制了计算机文件的方法，所述计算机文件具有信息节点号码。获取所述计算机文件的信息节点号码(330)。从计算机文件中读取所存储的信息节点号码(350)，所存储的信息节点号码是不应该从中复制计算机文件的文件系统的信息节点号码。将所获取的信息节点号码与所读取的信息节点号码进行比较(360)，并且如果所获取的信息节点号码与所读取的信息节点号码不匹配，则确定已经复制了所述计算机文件。还提出了一种是能够进行计算机文件复制检测的方法、一种与所述方法相对应的装置(420)和软件程序产品(430)。



CN 102117394 A

1. 一种检测是否已经复制了计算机文件的方法，所述计算机文件包括软件程序并且具有信息节点号码，在执行所述软件程序的装置 (410) 处，所述方法包括以下步骤 :

- 获取 (330) 所述计算机文件的信息节点号码 ;

- 读取 (350) 存储的信息节点号码，所述存储的信息节点号码是不应该从中复制所述计算机文件的文件系统的信息节点号码 ;

- 将所获取的信息节点号码与所读取的信息节点号码进行比较 (360) ;以及

- 如果所获取的信息节点号码与所读取的信息节点号码不匹配，则确定已经复制了所述计算机文件。

2. 根据权利要求 1 所述的方法，其中从所述计算机文件中读取所述存储的信息节点号码。

3. 根据权利要求 1 所述的方法，其中使用加密密钥对所读取的信息节点号码进行加密，并且所述方法还包括步骤 :使用所述加密密钥对所获取的信息节点号码进行加密 (340)，以便能够进行所述比较。

4. 根据权利要求 1 所述的方法，其中使用加密密钥对所读取的信息节点号码进行加密，并且所述方法还包括步骤 :使用相应的解密密钥对所获取的信息节点号码进行解密，以便能够进行所述比较。

5. 根据权利要求 1 所述的方法，其中所述计算机文件是软件应用程序的许可文件，并且在所述装置执行所述软件应用程序期间执行所述方法，所述方法还包括步骤 :当确定已经复制了所述许可文件时停止所述软件应用程序的执行。

6. 一种能够通过计算机文件中包括的软件程序来检测计算机文件的复制的方法，所述方法包括装置 (410) 处执行的以下步骤 :

- 创建 (230) 所述计算机文件，从而将所述计算机文件与信息节点号码相关联 ;

- 获取 (240) 所创建的计算机文件的信息节点号码 ;以及

- 存储 (260) 所获取的信息节点号码。

7. 根据权利要求 6 所述的方法，其中将所获取的信息节点号码存储在所述计算机文件中。

8. 一种用于检测是否已经复制了计算机文件的装置 (410)，所述计算机文件包括软件程序并且具有信息节点号码，所述装置 (410) 包括处理器 (420)，当执行所述软件应用程序时，所述处理器 (420) 用于 :

- 获取所述计算机文件的信息节点号码 ;

- 读取存储的信息节点号码，所述存储的信息节点号码是不应该从中复制所述计算机文件的文件系统的信息节点号码 ;

- 将所获取的信息节点号码与所读取的信息节点号码进行比较 ;以及

- 如果所获取的信息节点号码与所读取的信息节点号码不匹配，则确定已经复制了所述计算机文件。

9. 根据权利要求 8 所述的装置，其中所述处理器还用于执行软件应用程序，并且用于在确定已经复制了所述计算机文件时停止执行所述软件应用程序。

10. 一种能够通过计算机文件中包括的软件程序检测计算机文件的复制的装置 (410)，所述装置 (410) 包括处理器 (420)，所述处理器用于 :

- 创建所述计算机文件；

- 获取所创建的计算机文件的信息节点号码；以及

- 存储所获取的信息节点号码。

11. 一种其上存储了指令的软件程序产品 (430)，当处理器 (420) 执行所述指令时执行根据权利要求 1 至 5 中任一项所述的方法。

12. 一种其上存储了指令的软件程序产品 (430)，当处理器 (420) 执行所述指令时执行根据权利要求 6 和 7 中任一项所述的方法。

检测是否已经复制了计算机文件的方法和装置以及能够进行这种检测的方法和装置

技术领域

[0001] 本发明通常涉及复制保护，具体地涉及软件复制保护。

背景技术

[0002] 这一部分意欲向读者介绍现有技术的各个方面，可能涉及下面将要描述并且要求权利的本发明的各个方面。相信这种讨论有助于向读者提供背景信息来更好的理解本发明的各个方面。因此，应该理解的是这些陈述应该照此阅读，而不是对现有技术的承认。

[0003] 毫无疑问地是软件发行人面临着一定程度的盗版行为，一些人们使用软件应用程序的未授权副本而没有付钱。这在计算机游戏领域尤为如此。游戏提供商和发行人因此使用了保护机制并且试图打击盗版。这些保护机制包括：

[0004] • SecuROM。

[0005] • 安全媒介。

[0006] • 改变软盘上的地址标记和其他标记或者同步信息组。

[0007] • 在不能写到 CD-R 上的地方使用 CD-ROM 上的数据。

[0008] • 软件要求付费的证据以便正确工作。因此也可以使用注册码和序列号。

[0009] • 软件狗。

[0010] • 总线加密。

[0011] • 密钥文件必须存储在与软件执行文件相同的目录下。

[0012] • 经由电话或因特网产生进行产品激活。

[0013] 通常通过计算机的唯一标识符将软件与特定的计算机绑定在一起，例如硬件序列号或者 MAC 地址，但是因为在标准 PC 上几乎没有标识符可以容易地使用，这对于标准 PC 是困难的。另外，如果将所述标识符设置 在文件中（例如密钥文件），可以将所述文件本身复制到另一台计算机，并且可以在调制解调器的以太网卡上改变 MAC 地址，从而越过复制保护。

[0014] 除了上述问题之外，黑客通常通过开发至少部分地击败这些保护机制的工具对此做出反应。

[0015] Banikazemi 等人在“Storage-base File System IntegrityChecker”中介绍了指令检测系统 (IDS)。这种系统能够检测对于数据的修改，并且也允许退回未修改的数据。IDS 包括在集中的盘中存储数据的多台主机以及独特的存储区网络卷标控制器 (SVC)。其中，SVC 通过读取诸如文件的超级块和信息节点表之类的元数据来产生验证数据。然后将所述验证数据存储在主机不可访问的位置中，以便确定它们不会篡改所述验证数据。然后，SVC 例如使用信息节点号码来检验指令是否已经修改了文件。尽管所述系统可以很好地适用于指令检测，它并没有防止文件的复制。

[0016] 因此应该理解的是需要另外的复制保护方案，特别是适用于标准 PC 的复制保护方案。本发明提出了这种解决方案。

发明内容

[0017] 在第一方面，本发明涉及一种检测是否已经复制了计算机文件的方法，所述计算机文件包括软件程序并且具有信息节点号码。由执行软件程序的处理器获取所述计算机文件的信息节点号码；读取所存储的信息节点号码，所存储的信息节点号码是不应该从中复制计算机文件的文件系统的信息节点号码；将所获取的信息节点号码与所读取的信息节点号码进行比较；以及如果所获取的信息节点号码与所读取的信息节点号码不匹配，则确定已经复制了所述计算机文件。

[0018] 在第一优选实施例中，从所述计算机文件中读取所述存储的信息节点号码。

[0019] 在第二优选实施例中，使用加密密钥对所读取的信息节点号码进行加密，并且使用所述加密密钥对所获取的信息节点号码进行加密，以便能够进行所述比较。

[0020] 在第三优选实施例中，使用加密密钥对所读取的信息节点号码进行 加密，并且使用相应的解密密钥对所获取的信息节点号码进行解密，以便能够进行所述比较。

[0021] 在第四优选实施例中，所述计算机文件是软件应用程序的许可文件，并且在装置执行所述软件应用程序期间执行所述方法。当确定已经复制了所述许可文件时停止所述软件应用程序的执行。

[0022] 在第二方面，本发明涉及一种能够进行检测的方法，使得能够由计算机文件中包括的软件程序检测计算机文件的复制。创建所述计算机文件，从而将所述计算机文件与所获取和存储的信息节点号码相关联。

[0023] 在第一优选实施例中，所述信息节点号码存储在所述计算机文件中。

[0024] 在第三方面，本发明涉及一种检测装置，用于检测是否已经复制了包括软件程序并且具有信息节点号码的计算机文件。所述装置包括处理器，当执行所述软件应用程序时，所述处理器用于：获取所述计算机文件的信息节点号码；读取存储的信息节点号码，所述存储的信息节点号码是不应该从中复制计算机文件的文件系统的信息节点号码；将所获取的信息节点号码与所读取的信息节点号码进行比较；以及如果所获取的信息节点号码与所读取的信息节点号码不匹配，则确定已经复制了所述计算机文件。

[0025] 在第一优选实施例中，所述处理器还用于执行软件应用程序，并且用于在确定已经复制了所述计算机文件时停止执行所述软件应用程序。

[0026] 在第四方面，本发明涉及一种能够进行检测的装置，使得能够由计算机文件中包括的软件程序检测计算机文件的复制。所述装置包括处理器，所述处理器用于：创建所述计算机文件；获取所创建的计算机文件的信息节点号码；以及将所获取的信息节点号码存储在所创建的计算机文件中。

[0027] 在第五方面，本发明涉及一种其上存储了指令的软件程序产品，当处理器执行所述指令时，所述软件程序产品执行根据第一方面的方法。

[0028] 在第六方面，本发明涉及一种其上存储了指令的软件程序产品，当处理器执行所述指令时，所述软件程序产品执行根据第二方面的方法。

附图说明

[0029] 现在将作为非限制示例，参考附图描述本发明的优选特征，其中：

[0030] 图 1 示出了使用树形结构的现有技术文件系统；

[0031] 图 2 示出了根据本发明优选实施例的软件安装方法；

[0032] 图 3 示出了根据本发明优选实施例的复制控制方法；以及

[0033] 图 4 示出了适用于实现根据本发明的方法的系统。

具体实施方式

[0034] 本发明的主要发明思想是使用文件系统来实现复制控制，这也就是为什么将文件系统的简短描述用来促进对本发明的理解。

[0035] 文件系统可以说是促进数据的组织和访问的系统。磁盘文件系统是用于诸如磁盘之类的存储器件上的一种文件系统。存在多种磁盘文件系统，例如但是只是作为示例的 FAT、NTFS、HFS 和 UFS。在这些磁盘系统文件中，因为 FAT 和 NTFS 由微软视窗操作系统使用，FAT 和某种程度上的 NTFS 特别广泛使用。

[0036] 对于大多数磁盘文件系统的共同特征是使用树形结构，图 1 中示出了一个示例。所述文件系统 100 包括：多个目录 110、120、130 和多个文件 140、141。根目录 110 位于所述树形结构的顶部。根目录 110 包括三个子目录 120。所述子目录 120 的子目录 2 和子目录 3 包括多个文件 140，而所述子目录 120 的子目录 1 包括另外的子目录 130。所述另外的子目录 130，即子目录 4 包括文件 141。本领域普通技术人员应该理解，这只是一个示例，并且例如这对目录层次的个数没有限制。

[0037] 所述文件系统 100 中的每一个实体，即目录、子目录和文件可以看作是节点，称作信息节点 142（只对于一个文件 141 示出了信息节点）。每一个信息节点与元数据相关联，例如与所有权、访问权利和类型有关的信息，并且所述信息节点是由信息节点号码来标识，所述信息节点号码在文件系统中是唯一的，并且在其寿命期间对于所述实体保持相同。换句话说，所述信息节点号码对于每一个实体是恒定的。

[0038] 因此，本发明的主要发明思想是使用所述信息节点号码来执行复制 控制。

[0039] 图 2 示出了根据本发明优选实施例的软件安装方法。假设用户有权利安装所述软件；任意授权检查超过了本发明的范围。在步骤 210 中，用户开始对于软件的应用程序安装，称作安装向导。所述安装向导将软件文件复制 (220) 到文件系统中，通常复制到硬盘上，并且执行安装所需要的其他现有技术任务，尽管这些任务超过了本发明的范围。

[0040] 所述安装向导也在文件系统中创建 (230) 称作许可文件的文件，优选地在与至少一些已复制（已安装）软件文件相同的目录中，尽管可以在其他位置创建该文件，只要其位置对于所述软件应用程序是已知的。然后，所述安装向导然后获取 (240) 所述创建的许可文件的信息节点号码，并且使用所述安装的软件程序已知的秘密密钥对所述信息节点号码加密 (250)。所述安装向导最后将所述加密的信息节点号码存储 (260) 在许可文件中。然后安装所述软件。

[0041] 应该注意的是所述许可文件不必只是具有（并且可能地存储）信息节点值；例如，所述许可文件也可以包括计算机代码和 / 或其他数据。

[0042] 图 3 示出了根据本发明优选实施例的复制控制方法。在步骤 310 中，开始所述软件。所述软件然后打开 (320) 所述许可文件，获取 (330 信息节点号码，并且用所述秘密密钥对所述信息节点号码加密 (340)。所述软件然后读取 (350) 在所述许可文件中存储的加

密值，并且将所述加密信息节点号码与所读取的加密值进行比较 (360)。在这些值不同的情况下，中断所述软件的执行；相反如果这些值相同，所述软件执行继续。同样地，如果在文件系统中不存在许可文件，所述方法可能在 320 处已经停止。

[0043] 本领域普通技术人员应该理解的是在不影响所述方法运转的情况下，可以略微更改图 2 和图 3 中所示方法的步骤。例如，可以在将软件文件复制到目录 X（步骤 220）之前产生（步骤 230）许可文件；实际上，可以在开始安装向导（步骤 210）之前的任意时刻执行所述复制步骤 (220)。另外在图 3 中，可以在开始所述软件 (310) 和比较所述值（步骤 360）之间的任意点执行所读取步骤 (350)。

[0044] 还应该理解的是图 3 的复制控制方法具有至少一个替代实施例。这种替代实施例使用解密来代替加密，但是总体思想是相同的。在所述替代实施例中，如同在优选实施例中那样执行步骤 310-330，接着执行步骤 350，即从许可文件读取加密值。然而，对所述加密值进行解密，结果是将原始的信息节点号码与所述许可文件的所获取的信息节点号码进行比较。自然地在该替代实施例中，所述软件访问与安装向导的加密密钥相对应的解密密钥。在另外的变体中，将许可文件的已加密信息节点号码存储在另一个位置，即在除了许可文件之外的另外文件中。

[0045] 图 4 示出了适用于实现根据本发明方法的系统。所述系统 400 包括计算机 410 和所述计算机 410 内部的存储装置 424。所述计算机 410 有利地包括处理器 420、存储器 422、网络接口 428 以及用于从数据载体读取数据的读取器 426，所述数据载体例如是存储（卸载）软件应用程序和安装向导的 DAD 430。

[0046] 在软件安装期间，即在图 3 所示的方法中，读取器 426 从所述载体 430 读取安装向导，所述处理器 420 执行所述方法的步骤，必要的指令其他部分（存储器 422、存储装置 424）执行特定的任务。

[0047] 在复制控制期间，即在图 4 所示的方法中，所述处理器 420 执行所述方法的步骤，必要的指令其他部件（具体地是存储装置 424）执行特定的任务。

[0048] 还应该理解的是，优选地通过任意合适的现有技术软件保护技术来保护所述软件的加密密钥（或者在替代实施例中保护解密密钥），例如代码模糊，使得攻击者难以恢复所述加密密钥。然而，这些技术超出了本发明的范围。

[0049] 因为特定文件未必与两个不同文件系统中的相同信息节点号码相关联，本发明可以提供一种复制保护，具有成功检测未授权复制的较高可能性。

[0050] 应该理解的是本发明的方法可以只使用标准操作来实现，读取和写入，这意味着不存在攻击者可以截取的特定系统调用。

[0051] 因此应该理解的是本发明可以提供一种方法和装置，用于软件应用 程序的复制保护。

[0052] 描述、（适当的）权利要求和附图中公开的每一个特征可以独立地或者按照任意适当的组合来提供。按照硬件形式实现描述的特征也可以按照软件实现，反之亦然。在权利要求中出现的参考数字只是用于说明而不具有限制本发明范围的效果。

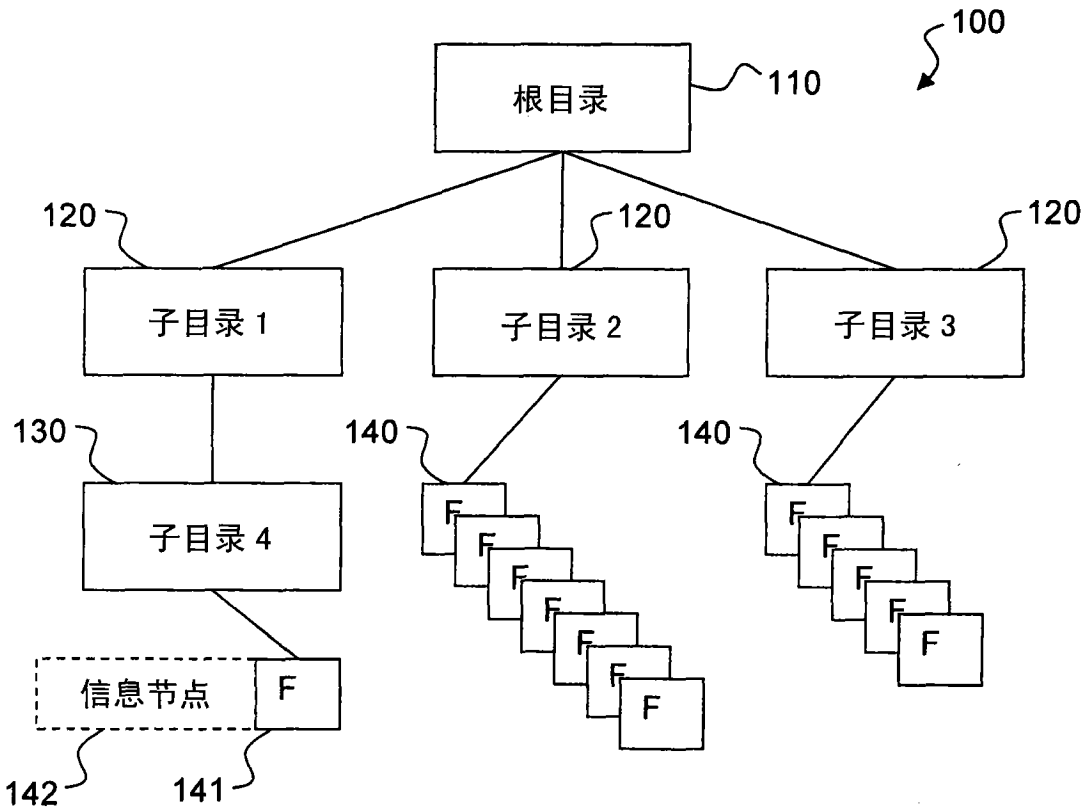

100
根目录
110
120
120
120
子目录 1
子目录 2
子目录 3
130
140
140
子目录 4
F
信息节点
F
142
141
（现有技术）

图 1

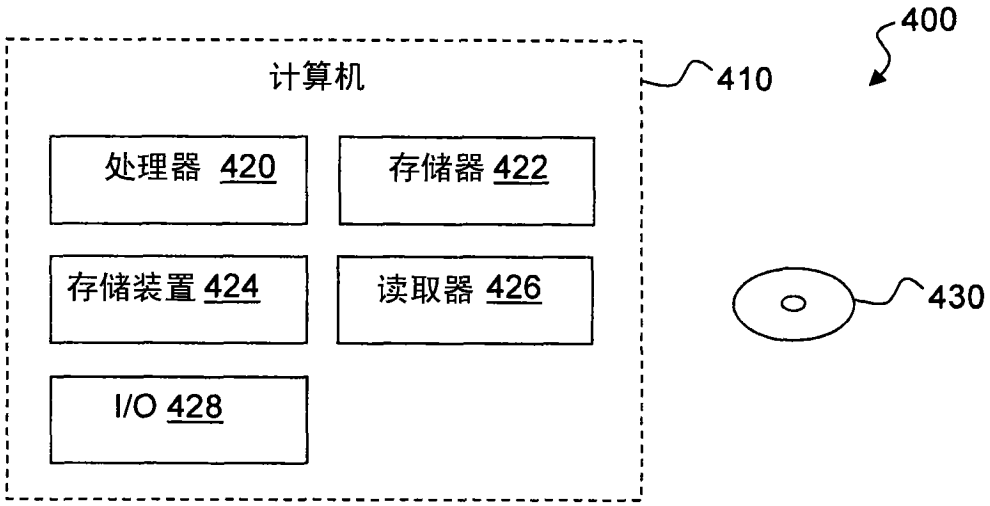

400
计算机
410
处理器 420
存储器 422
存储装置 424
读取器 426
I/O 428
430

图 4

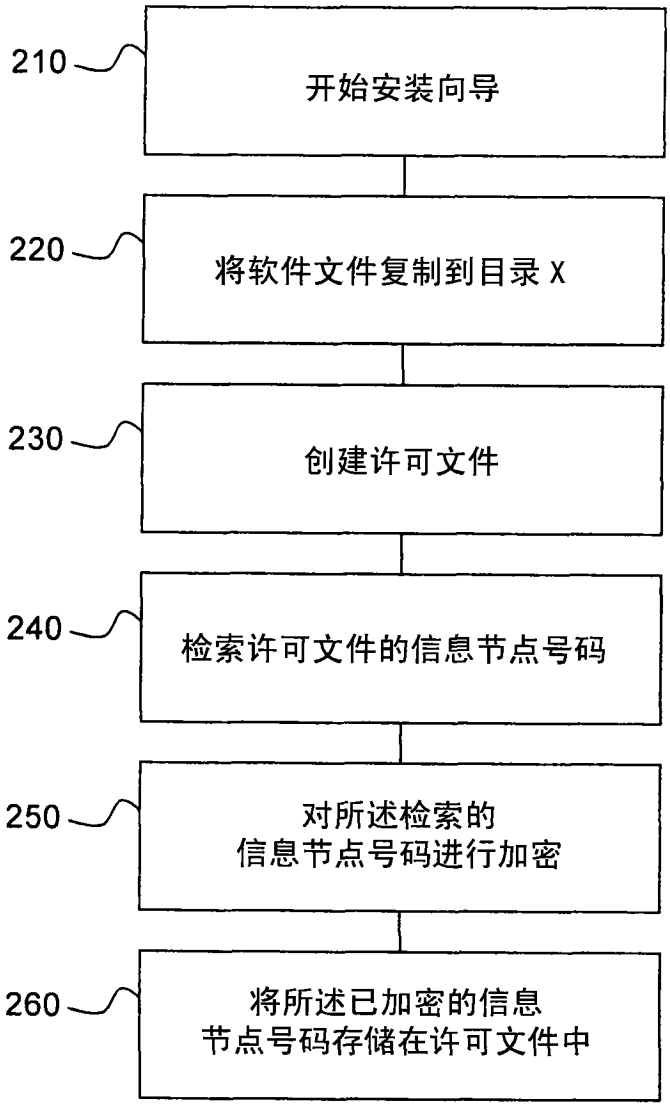

210
开始安装向导
220
将软件文件复制到目录 X
230
创建许可文件
240
检索许可文件的信息节点号码
250
对所述检索的
信息节点号码进行加密
260
将所述已加密的信息
节点号码存储在许可文件中

图 2

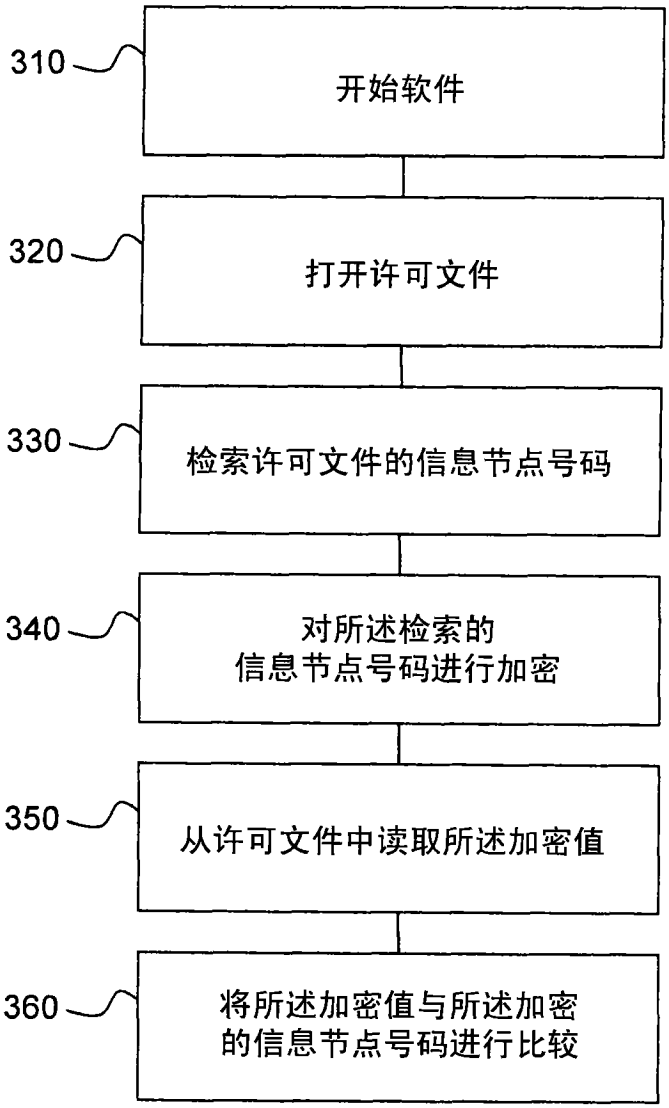

310
开始软件
320
打开许可文件
330
检索许可文件的信息节点号码
340
对所述检索的
信息节点号码进行加密
350
从许可文件中读取所述加密值
360
将所述加密值与所述加密
的信息节点号码进行比较

图 3