

[12] 发明专利申请公开说明书

[21] 申请号 01117873.6

[43]公开日 2001年10月10日

[11]公开号 CN 1316706A

[22]申请日 2001.3.30 [21]申请号 01117873.6

[30]优先权

[32]2000.3.30 [33]EP [31]00106810.5

[71]申请人 曼内斯曼 VDO 股份公司

地址 联邦德国美茵河畔法兰克福

[72]发明人 M·托尼

T·德里豪特

[74]专利代理机构 中国专利代理(香港)有限公司

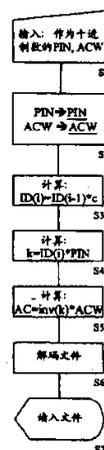
代理人 张志醒

权利要求书 4 页 说明书 8 页 附图页数 5 页

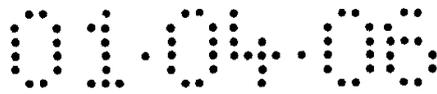
[54]发明名称 具有受保护存储介质的汽车导航系统

[57]摘要

本发明给出了一种导航和多媒体系统,它可检查用户是否有权使用道路交通图数据。所述导航系统具有对所述大容量存储介质中的文件在导航系统中的使用权进行检测的装置。所述文件特别是采用加密方式存储。根据本发明所述方法,为释放文件的使用权,用户首先要向导航系统内输入一个第一密码代码和一个第二密码代码(PIN 和 ACW)。该代码随后被转换成矢量。用导航系统的设备识别号 ID 和第一密码代码 PIN 可先计算出一个密钥 k。用该 k 和第二密码代码 ACW 可计算出一个接入许可识别号 AC,将该号与存储介质内存储的接入许可识别号进行比较。如果两识别号相同,则所属文件被解密,被释放给导航系统以供使用。



ISSN 1008-4274



权 利 要 求 书

1、 作为导航和多媒体系统构成的汽车计算机系统，具有一个包括所属存储器件的中央计算单元 (1)，以及一个输入单元 (2)、一个输出单元 (3) 和一个用于大容量存储介质的读取装置 (5)，它们分别与所述中央计算单元 (1) 相连，本发明的特征是，所述导航或多媒体系统还具有对所述大容量存储介质中的文件在导航或多媒体系统中的使用权进行检测的装置。

2、 如权利要求 1 所述的计算机系统，其特征是，所述大容量存储介质含有加密数据。

3、 如以上权利要求中任何一项所述的计算机系统，其特征是，具有对加密数据进行解密的装置。

4、 如以上权利要求中任何一项所述的计算机系统，其特征是，包括一个文件管理系统，它被设计成可将经所述输入单元输入的接入许可识别号与大容量存储介质中所存数据的接入许可识别号进行比较。

5、 如权利要求 4 所述的计算机系统，其特征是，具有对密码输入的接入许可识别号进行解密的装置。

6、 如以上权利要求中任何一项所述的计算机系统，其特征是，所述接入许可识别号可作为矢量描述。

7、 如权利要求 6 所述的计算机系统，其特征是，该系统涉及一种至少为 m 维的接入许可识别号，其中 m 是大容量存储介质所存文件的数量。

8、 如以上权利要求中任何一项所述的计算机系统，其特征是，具有一个设备识别号 (ID)，它被存储在一个非易失性存储器件内。

9、 如权利要求 8 所述的计算机系统，其特征是，所述设备识别号是可以改变的。

10、 如以上权利要求中任何一项所述的计算机系统，其特征是，具有密钥 (k) 的计算装置，用于对密码输入的第一代码 (PIN) 和存储的设备识别号 (ID) 的加密文件进行解密。

11、 如权利要求 10 所述的计算机系统，其特征是，具有利用密钥 (k) 从第二密码输入的代码 (ACW) 中对接入许可识别号 (AC) 进行计算的装置。

12、 如以上权利要求中任何一项所述的计算机系统，其特征是，所述设



备识别号 (ID) 可作为矢量描述。

13、 如以上权利要求中任何一项所述的计算机系统, 其特征是, 所述设备识别号在每次输入一个新的第一代码后自动改变。

5 14、 如以上权利要求中任何一项所述的计算机系统, 其特征是, 有语音输入装置。

15、 如以上权利要求中任何一项所述的计算机系统, 其特征是, 包括一个光学大容量存储介质的读取设备。

16、 如以上权利要求中任何一项所述的计算机系统, 其特征是, 所述大容量存储介质是 CD-ROM。

10 17、 如以上权利要求中任何一项所述的计算机系统, 其特征是, 所述大容量存储介质是 DVD。

18、 如以上权利要求中任何一项所述的计算机系统, 其特征是, 所述数据是道路交通图数据和/或系统程序和/或应用程序。

15 19、 如以上权利要求中任何一项所述的计算机系统, 其特征是, 该系统与一个通信装置相连, 实现与一个中心站的通信, 所述中心站管理对数据的使用权。

20、 如权利要求 19 所述的计算机系统, 其特征是, 所述导航或多媒体系统与通信装置之间的连接采用短程无线连接实现。

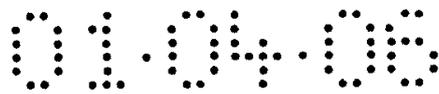
20 21、 如权利要求 19 或 20 所述的计算机系统, 其特征是, 所述与中心站之间的通信采用无线方式。

22、 如权利要求 19 所述的计算机系统, 其特征是, 所述通信经一个移动无线网进行。

23、 如以上权利要求中任何一项所述的计算机系统, 其特征是, 所述系统被设计成可以接收和处理交通信息。

25 24、 释放一种文件供计算机系统使用的方法, 特别是供汽车导航系统或汽车多媒体系统使用, 所述文件与至少另一种文件共同存储在一个存储介质中, 并且具有一个接入许可识别号 (AC), 通过对一个第一和一个第二密码代码 (PIN 和 ACW) 的译码实现所述释放,

30 一用一个存储在计算机系统设备识别号 (ID) 和第一密码代码 (PIN) 计算出一个密钥 (k), 并且



一用所述密钥 (k) 和第二密码代码 (ACW) 确定释放文件所需的识别号 (AC), 以及

一将具有计算出的识别号 (AC) 的文件释放, 用于所述计算机系统。

5 25、 如权利要求 24 所述的方法, 其特征是, 文件的释放通过所述计算机系统的文件管理系统进行。

26、 如以上权利要求中任何一项所述的方法, 其特征是, 用所述密钥 (k) 加密的文件为了用于所述计算机系统的使用, 用所述密钥 (k) 解密。

10 27、 如以上权利要求中任何一项所述的方法, 其特征是, 所述设备识别号 (ID) 随着每次新释放另一个存储介质的文件而改变, 并且将所改变的识别号存储在该计算机系统的一个非易失性固定存储器中。

28、 如以上权利要求中任何一项所述的方法, 其特征是, 所述方法涉及一种分层文件结构。

29、 如以上权利要求中任何一项所述的方法, 其特征是, 所述接入许可识别号作为矢量描述。

15 30、 如权利要求 29 所述的方法, 其特征是, 所述作为矢量描述的接入许可识别号具有二进制分量。

20 31、 如以上权利要求中任何一项所述的方法, 其特征是, 通过所述矢量 $AC(x)=(a(1),a(2),a(3),\dots,a(x-1),a(x),a(x+1),\dots,a(m))$ 的 m 分量 $a(1),a(2),a(3),\dots$ 按照以下方式确定一个文件 $D(x)$ 在所述分层文件结构中的位置, 即所有分配给文件的、而且与文件 $D(x)$ 分层相关的矢量 $AC(x)$ 的分量取一个第一数值, 特别是数值 1, 而所有其他分配给文件的、且不与文件 $D(x)$ 分层相关的分量取一个第二数值, 特别是数值 0。

32、 如以上权利要求中任何一项所述的方法, 其特征是, 所述密钥 (k) 作为矢量描述。

25 33、 如以上权利要求中任何一项所述的方法, 其特征是, 所述设备识别号 (ID) 作为矢量描述。

34、 如权利要求 33 所述的方法, 其特征是, 所述设备识别号的矢量 ID 在每次释放文件后, 通过与一个交变矢量 c 的乘法而改变, 所以一个文件经过 i 次释放后, 有 $ID(i)=ID(i-1)*c$ 。

30 35、 如以上权利要求中任何一项所述的方法, 其特征是, 该方法应用在



汽车导航系统的导航计算机中。

36、 如权利要求 35 所述的方法，其特征是，所述文件中含有道路交通图数据。

5 37、 如以上权利要求中任何一项所述的方法，其特征是，所述文件含有应用程序。

38、 如以上权利要求中任何一项所述的方法，其特征是，所述密码代码之一含有使用权时间限制的信息。

10 39、 如以上权利要求中任何一项所述的汽车计算机系统的存储介质，本发明的特征是，在所述存储介质上以分层文件结构的加密形式存储多个文件，所述加密形式为保证专有授权接入被分配一个可作为矢量描述的认识号。

40、 如权利要求 39 所述的存储介质，其特征是，该介质涉及一种 m 为矢量，其中的 m 等于文件的数量。

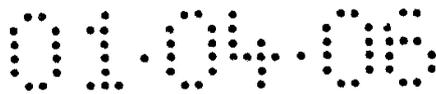
41、 如权利要求 39 或 40 所述的存储介质，其特征是，所述矢量具有二进制分量。

15 42、 如以上权利要求中任何一项所述的存储介质，其特征是，通过所述矢量 $AC(x)=(a(1),a(2),a(3),\dots,a(x-1),a(x),a(x+1),\dots,a(m))$ 的 m 分量 $a(1),a(2),a(3),\dots$ 按照以下方式标定一个文件 $D(x)$ 在所述分层文件结构中的位置，即所有分配给文件的、而且与文件 $D(x)$ 分层相关的矢量 $AC(x)$ 的分量取一个第一数值，特别是数值 1，而所有其他分配给文件的、且不与文件 $D(x)$ 分层相关的分量取一个
20 第二数值，特别是数值 0。

43、 如以上权利要求中任何一项所述的存储介质，其特征是，所述介质是一种光学存储介质。

44、 如以上权利要求中任何一项所述的存储介质，其特征是，所述介质是 CD-ROM。

25 45、 如以上权利要求中任何一项所述的存储介质，其特征是，所述介质是 DVD。



说明书

具有受保护存储介质的汽车导航系统

5 本发明涉及一种作为导航和多媒体系统构成的汽车计算机系统，具有一个包括所属存储器件的中央计算单元，以及一个输入单元、一个输出单元和一个用于大容量存储介质的读取装置，它们分别与所述中央计算单元相连。

此外，本发明还涉及一种所述汽车计算机系统的存储介质和一种释放存储介质内所存文件的方法。

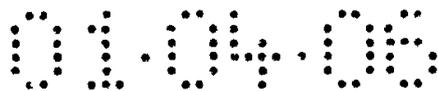
10 长时间以来，汽车导航系统本身已经是公知的，并且越来越多地用于新车或者作为加装设备。用于行驶路线计算的地图与其他文件，如导游手册或饭店指南一同存储在一种存储介质中。作为存储介质通常采用 CD-ROM，其中存储了相应的文件。所述导航系统还包括用于读取文件的所属读取设备。存储介质如 CD-ROM 或者特别是 DVD 具有很大的存储容量，所以可存储很大的数据
15 量，必要时以压缩形式存储。所以这种存储介质有很高的市场价值。借助于合适的设备，例如一种所谓的“CD 烧录机”可以相对简单地制造 CD-ROM 的拷贝。拷贝的 CD-ROM 中有一部分无偿地在相关人员中交换，或者进入非法市场。所以存在一种需要使相应的程序或一般的文件仅能向注册用户开放使用。

20 因为在一个 CD-ROM 或 DVD 上可以存储许多程序或文件，例如存储欧洲的道路交通图数据，所以还存在一种需求是仅向特定的用户释放个别的或特定数量的文件，例如某个国家的道路交通图数据。理想的方式是这种释放也和相应的防拷贝措施相联系，所以文件被释放后也只能由注册以及有权的用户使用。

25 本发明的任务是，提供一种汽车计算机系统，它只允许授权用户使用特定的道路交通图或者程序。

本发明的另一个任务是，提供一种导航或多媒体系统的受保护存储介质。第三个任务是，提供一种释放存储介质内至少与另一个文件共同存储的文件，从而由所述汽车计算机系统使用的方法。

30 以上关于所述汽车计算机系统的第一个任务的解决方案是，所述导航或多



媒体系统还具有对所述大容量存储介质的数据在导航或多媒体系统中的使用权进行检测的装置。通过该方式可检测数据的使用者是否是一个有权的使用者。如果使用者没有使用权，则他将无法进入存储介质的文件。所以含有这些文件的 CD-ROM 或者 DVD 虽然能以任意方式拷贝和散发，但是数据只能在授权的系统中读取。

汽车用多媒体系统和单纯的导航系统的区别是，它具有多种功能。例如它可具有导航功能，包括收音机、CD 或盒带放音机等部分在内的音响功能，电视功能，因特网功能或通信功能。在多媒体系统中各个部分以及输出单元被用于各种不同的功能。其中的光学输出例如用于目标导向指示，电视图象放映以及因特网网页显示在一个光学输出单元上。在随后的实施例中出于概括的原因，主要介绍一种导航系统，但是该系统也可满足具有相同或类似功能的多媒体系统的需要。

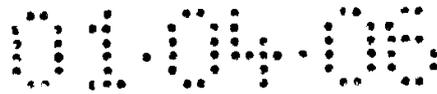
本发明的一个改进特别在于所述大容量存储介质中含有加密的文件。数据的使用只能在授权的导航系统中实现，其中包括相应的对加密文件进行解密的装置。通过该措施可在整体上保证对文件的保护。

为了使各个文件向一个特定的用户开放使用，可以对每个文件用一个不同的密码加密。授权用户只有知道相应的密码才能接入一个特定的文件，而其他文件因为密码是未知的，所以无权进入。但是这种方法需要对不同的文件给出许多密码。

所以在一个优选的实施例中，为释放各个文件设置了一个文件管理系统，它被设计成可将经所述输入单元输入的接入许可识别号与大容量存储介质中所存数据的接入许可识别号进行比较。在这种工作方式中，只需要用一个密码对所有文件进行加密。但是每个文件均有一个自己的存取识别号，它由授权用户一次性输入汽车导航系统中，用于释放相应的文件。文件管理系统将输入的识别号与文件所属的识别号进行比较，后者被存储在存储介质中。只有两个识别号相同时，相应的文件才能释放供导航系统使用。

这种导航系统可在某种程度上提供保护，防止对文件的非法使用。但是识别号在某些情况下可能会与密码一起由一个合法用户转移给一个非法用户，使其对文件解密，所以非法用户也可进入所述文件。

另外一种方案是，所述导航系统具有对密码输入的接入许可识别号进行解



密的装置。通过密码输入所述识别号，可使非法用户的导航系统中没有包含相应的接入许可识别号解密装置时不能使用所述文件。

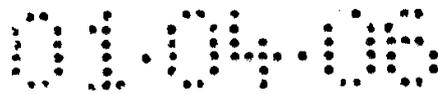
一种特别有利的方案是，所述接入许可识别号可作为矢量描述。通过这种特殊形式的识别号能以简单的方式建立与存储介质中文件目录结构的联系，并且用数学运算进行处理。为此该系统特别涉及一种至少为 m 维的矢量，其中 m 是大容量存储介质所存文件的数量。其中的文件可以是程序、数据库等，特别还包括文件目录，它本身还可含有文件目录和/或文件。

如果所述存储介质具有包括文件目录在内的 m 个文件的结构，则特别是文件的每个矢量具有 m 个分量，例如可用 $a(1), a(2), a(3), \dots, a(m)$ 表示。每个分量 $a(x)$ 均表示一个文件或一个文件目录。如果至特定文件 $D(x)$ 的路径采用分层文件结构，例如经过文件目录 $a(2), a(5), a(9)$ ，则这些分量可用数值 1 标记，而矢量的其他分量则用数值 0 标记。这种矢量与特定文件对应的方式可通过存储在导航系统中的所述文件管理程序完成。

在另一个方案中，所述导航系统具有一个设备识别号 ID ，它被存储在一个非易失性存储器件内。如果该设备识别号 ID 用于检验使用权，则可进一步提高安全性。一个非法用户必须也知道合法用户的设备识别号才能使用存储介质中的文件。再次提高安全性，防止非法使用文件的方案是，设备识别号是可改变的。通过这种方法可防止非法用户知道了一个合法用户的设备识别号后，继续打开合法用户的其他文件用于其本身的用途。

本发明特别包括以下特征，即所述导航系统具有密钥 k 的计算装置，用于对密码输入的第一代码 PIN 和存储的设备识别号 ID 的加密文件进行解密。此外所述导航系统还具有利用密钥 k 从第二密码输入的代码 ACW 中对接入许可识别号 AC 进行计算的装置。一个合法用户使用一个特定的文件，例如一个特定国家的道路交通图数据时，向中心站或销售商支付了相应的费用后可得到两个密码代码，即第一代码 PIN 和第二代码 ACW 。

另一种选择方案是，该导航系统与一个通信装置相连，实现与一个中心站的通信，所述中心站管理对数据的使用权。此时用户可以在任何时间以直接方式释放所需的文件。所述通信装置特别是一种无线电话。该无线电话可以通过一条线路与导航系统相连，或者经短距离无线连接在导航系统和通信装置之间建立无线连接，例如通过公知的蓝牙法建立连接。通过无线电话的无线连接，



还可以让交通信息进入导航系统，从而在行车路线计划中予以考虑。

根据本发明，释放一种存储在存储介质中的文件供计算机系统使用的方法，特别是供汽车导航系统或汽车多媒体系统使用，所述文件与至少另一种文件共同存储在一个存储介质中，并且具有一个接入许可识别号 AC，通过对一个第一和一个第二密码代码（PIN 和 ACW）的译码实现所述释放，其特征是，用
5 一个存储在计算机系统内的计算机系统设备识别号 ID 和第一密码代码 PIN 计算出一个密钥 k，并且用所述密钥 k 和第二密码代码 ACW 确定释放文件所需的识别号 AC，以及将具有计算出的识别号 AC 的文件释放，用于所述计算机系统。此外优选对需释放的文件进行加密。

10 所述存储介质例如是 CD-ROM 或 DVD，其中存储所述文件，并且可以分发，所以该介质虽然能够继续拷贝，但是其中的文件只有在得知了相应的密钥后将文件解码才能使用。为了防止相应的密钥被一个合法用户传递给一个非法用户，可规定密钥只能以加密形式发送给合法用户。加密的代码中含有所述密钥，还含有合法导航系统的设备识别号。这样可保证继续传播含有密钥的加
15 密代码时，该代码在其他具有不同的设备识别号的导航系统中的使用被排除。

为了释放特定供使用的文件，规定了一个第二代码，其中含有需释放文件的数据。该第二代码也必须首先以解密方式进入导航系统，其中同样使只有正确的导航系统设备识别号才可使用。代码在一个非法导航系统中的解密由于其设备识别号不同而会导致其他的解密结果，所以只能得到所述需释放文件的一个
20 错误识别号。为了进一步提高该方法的安全性，规定设备识别号在每次释放一个文件时由中心站进行改变。所述代码 PIN 和 ACW 以及设备识别号 ID、密钥 k 和接入许可识别号 AC 优选作为矢量描述。

在一个特殊的实施例中还规定了交变矢量 c，它在每次重新释放一个文件时与设备识别号 ID 的矢量建立连接，从而生成一个设备识别号的新矢量。

25 本发明的适用于所述导航系统的存储介质内具有多个文件，它们以分层文件结构的加密形式存储，并且根据本发明，为保证专有的授权进入，配给一个可用矢量描述识别号。它特别涉及一种 m 维矢量，其中的 m 表示文件的数量。所述矢量优选具有二进制分量。

下面对照一个实施例和附图对本发明所述导航系统和本发明所述方法作进
30 一步的说明。

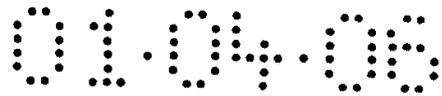


图 1 表示一个导航系统的各组成部分，

图 2 表示用于导航系统的 CD-ROM 的文件目录，

图 3 表示一般形式的分层文件目录，

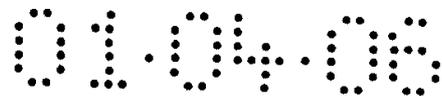
图 4 表示接入许可识别号的各种不同形式，

5 图 5 表示所述方法的流程图。

图 1 中表示的是一个导航系统的各组成部分。该导航系统的中心组成部分是计算单元 1，它与其工作存储器和一个非易失性固定存储器构成导航计算机。和所述中央计算单元 1 相连的是一个人工输入单元 2，经该单元可输入目的地以及加密代码 PIN 和 ACW。作为手动输入单元的选择或附加，可以设置一个语言输入单元。所述导航系统还具有一个光学输出单元 3（选项）以及一个声音输出单元 4，通过该单元可分别输出目的地导航信息。此外所述导航系统还具有一个读取装置 5，它与中央计算单元 1 相连。所述读取装置 5 是为读取 CD-ROM 和/或 DVD 上的文件而设计的。

为了进行位置确定，所述导航系统还具有一个 GPS 接收机 6，它可接收相应的卫星信号，并传递给中央计算单元 1 用于进行定位。为了进行独立于卫星的定位，所述导航系统还具有一个方向传感器 7 和一个路程传感器 8。为了引入交通消息，进行动态导航，所述导航系统还与一个无线电接收机 9 相连，后者用于接收 RDS/TMC 消息。此外所述导航系统还可与一个未画出的无线电话相连。

图 2 表示的是一个具有道路交通图数据和其他文件的 CD-ROM 的分层文件结构的实例。图中表示出“国家”文件目录。此外还可以包含其他文件目录，例如含有专门程序如高速公路枢纽号码与地理数据之间的对应关系程序。文件目录“国家”可具有下一级的文件目录，德国是“DE”，法国是“FR”，“BENELUX”是比荷卢三国。文件目录“DE”还可细分成文件目录“北”和文件目录“南”，它们分别对应于德国相应的地理区域的文件。在文件目录“北”中作为文件包括一个具有道路交通图数据的数据库和另一个具有旅游指南（RF）的数据库。相应的文件也存在于文件目录“南”中。数据目录“FR”中直接包含法国的有关文件，而没有进一步按照地理划分。其中包含道路交通图数据的文件，一个旅游指南和一个饭店指南。文件目录“BENELUX”不仅包括该地区的道路交通图数据文件，而且包括文件目录（RF），其中含有荷兰



(NL)、比利时 (BE) 和卢森堡 (LU) 的旅游指南。

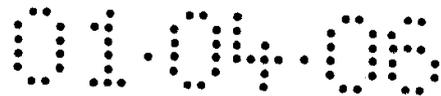
图 3 表示的是对应于图 2 的文件结构的一般形式, 其中的文件采用流水号编号。如上所述, 所述文件不仅可以是文件目录、数据库, 也可以是应用程序。图 3 中表示的每个文件都被分配一个接入许可识别号, 它作为矢量用 18 个分量描述。所述分量的数量等于文件和文件目录的总和。文件目录 D01 用矢量的第一分量表示, 文件目录 D02 用矢量的第二分量表示, 并且一般而言文件目录 m 用矢量的 m 分量表示。一个文件的识别号的所有矢量由通向该文件的路径组成。以上原理见文件 D15 的实例说明, 并且在图 3 中的下部表示出来。通向文件 D15 的路径经过文件或文件目录 D01、D02、D06 和 D15, 从而在属于文件 D15 的矢量中对应的位置 01、02、06 和 15 取数值 1, 而矢量的其他分量则取数值 0。为了对接入许可识别号提供足够的保护, 该识别号不应由过少的分量组成。为了在文件数量较少时也能通过接入许可识别号得到足够的保护, 可以将其扩展, 见图 4 所示。

在图 4a 中表示出来一个具有 10 个分量的接入许可识别号, 文件也应当有同等数量。在图 3b 中表示出该接入许可识别号扩展到 19 个分量, 其中在表示一个文件的分量之间插入随机分量 r, 它可通过导航系统重新消除。

一个导航系统的用户可以购买一张含有许多文件的 CD-ROM, 它首先不必得到最终的使用权。一辆新车的购买者例如可同时与汽车一同购得一个导航系统和一张具有所属数据库的 CD-ROM。因为用户尚未给自己注册, 所以他用其导航系统尚不能进入各个存储在 CD-ROM 中的加密文件。用户首先必须将同样存储在 CD-ROM 中的文件管理系统装载到其计算机系统内。然后用户必须取得使用许可。为此他特别要和一个中心站建立电话联系。用户向该中心站告知其使用某个特定文件的要求, 例如一个特定国家的道路交通图数据以及他的实际设备识别号, 该识别号是它在购买导航系统时得到的, 还要为所用的数据支付使用费。所述中心站首先从现有的设备识别号 $ID(i-1)$ 和一个交变矢量 c 中计算出一个新的设备识别号 $ID(i)$, 例如: $ID(i) = ID(i-1) * c$ 。

然后计算第一密码代码 PIN , 它包含新的设备识别号 $ID(i)$ 和用于 CD-ROM 文件加密所需的密钥 k , 例如按照下式: $PIN = inv[ID(i)] * k$ 。

接着计算第二密码代码 ACW , 它包含密钥 k 和需释放文件的接入许可识别号 AC , 例如按照下式: $ACW = k * AC$ 。



新的设备识别号 $ID(i)$ 以及关于需释放文件的信息和付款模态随后被存储在中心站内。所述密码代码 PIN 和 ACW 被通知给用户。该通知可以采取电话方式或通过信件邮寄。在这两种情况中最好对含有二进制分量的密码代码矢量先作为二进制数字描述，并转换成十进制数字，然后将十进制数字告知用户。用户可以在此情况中将较简单和较短的十进制数字输入其计算机系统，系统再将其转换成二进制数字或具有二进制分量的矢量。用户可以相应地在开始时将设备识别号作为十进制数字通知给中心站，然后在中心站将该十进制设备识别号转换成矢量。在一个选择性实施例中，所述导航系统与一个无线电话相连，其中可设定一种自动化流程。其中用户可以在导航系统中调出一个菜单程序，在菜单中可对存储在 CD-ROM 内的程序和数据库进行选择。用户选择出一个或多个所要求的程序，并且输入关于付款模态的所需数据，例如其信用卡号码。随后用户激活与中心站之间的移动无线连接的发射呼叫。通过该无线连接可将释放要求、付款数据以及当前的设备识别号 $ID(i-1)$ 自动传输出去，所述设备识别号存储在计算机的一个非易失性存储器中。密码代码在中心站内的计算见上所述。

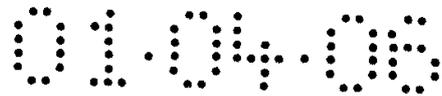
此外的出发点应当是，密码代码已经口头或书面通知给用户。此后的流程见图 5 中所示的流程图。在步骤 S1 中，用户用输入键盘向导航系统内输入作为十进制数字的密码代码 PIN 和 ACW 。在步骤二中，在导航系统内将密码代码转换成具有二进制分量的矢量，其中首先将十进制数字转换成二进制数字，然后用各个二进制数字代表矢量的分量。跟着在导航系统内从现有设备识别号和一个交变矢量中计算出新的设备识别号 $ID(i)$ ，所述现有设备识别号和交变矢量均存储在一个非易失性存储器件内。

在步骤 S4 中，用新的设备识别号 $ID(i)$ 和第一密码代码 PIN 计算出用于文件解密的密钥 k ，计算根据公式： $k = ID(i) * PIN$ 。

随后用密钥 k 或密钥矢量 k 的逆矢量 $inv(k)$ 和第二密码代码 ACW 计算出存取许可识别号 AC ，计算根据公式： $AC = inv(k) * ACW$ 。对于对称式加密算法有： $inv(k) = k$ 。

所述导航系统的文件管理系统此时将释放属于识别号 AC 的文件供使用，并且该文件可用已知的密钥 k 解密，或者显示出来，或者用于进一步处理。

在本发明所述方法中将文件的释放与设备识别号联系在一起，所以释放代



码不能用在其他系统中。由于每次重新释放一个使用许可时，对设备识别号作了改变，所以提高了安全性。存在存储介质中的文件用密钥 k 解密，其中密钥 k 可以从第一密码代码 PIN 中仅在已知设备识别号的情况下生成。该识别号 AC 也可在已知密钥 k 的情况下从第二密码代码中计算出来。所述加密可采用一种公知的方法进行，特别是按照数据加密标准 (DES) 采用 56 位长的密钥进行。

采用本发明所述方法还可以实现有时间期限的文件释放。这种有时间期限的释放在以下情况中例如会需要，即用户仅在一个有限的时间内需要使用一个特定地区的地图数据。这里例如可涉及在某个特定国家中持续几周的一次性国外休假。

这种有期限的文件释放的方法是，所述接入许可识别号中包含表示有时间期限的释放的分量。相应的接入许可识别号例如见图 3c 所示。在该实例中，矢量 AC 的前 10 个分量对于接入许可识别号如前面所述的情况那样与 CD-ROM 中存储的文件建立联系。此外所述矢量还包含分量 t_1 、 t_2 和 t_3 ，它们表示有时间限制的使用。例如用分量 t_1 表示在第一时间段内例如一周内释放所述文件，如果该分量被置于 1。相应地用分量 t_2 表示在第二时间段内例如一个月

15 内释放所述文件，如果该矢量被置于 1。相应地用分量 t_3 表示在第三时间段内例如六个月内释放所述文件。所述时间段从文件被释放时开始。所述导航系统或导航系统的文件管理程序可以识别出是否设置了分量 t_1 至 t_3 中的一个，并且设置一个对应的时标，另外在每次计划的文件的新使用开始时，检查所设定的

20 时间框架是否已经届满。

在所示的实施例，其出发点是文件被存储在一张 CD-ROM 或者类似的介质上，并且该 CD-ROM 已经提供给用户。所述导航系统始终应用该 CD-ROM 上存储的文件。但是也可以在计算单元的存储器，特别是硬盘上存储文件。文件向硬盘的传输可以经 CD-ROM 实现，或者在多媒体系统中例如通过

25 与因特网的移动无线连接实现。

此外所述密码代码也可以在较小存储密度的存储介质中存储，例如存在一种“智能卡”中，并且让用户能够得到。该代码也可通过相应的读取设备直接从该存储介质读到导航系统中。

说明书附图

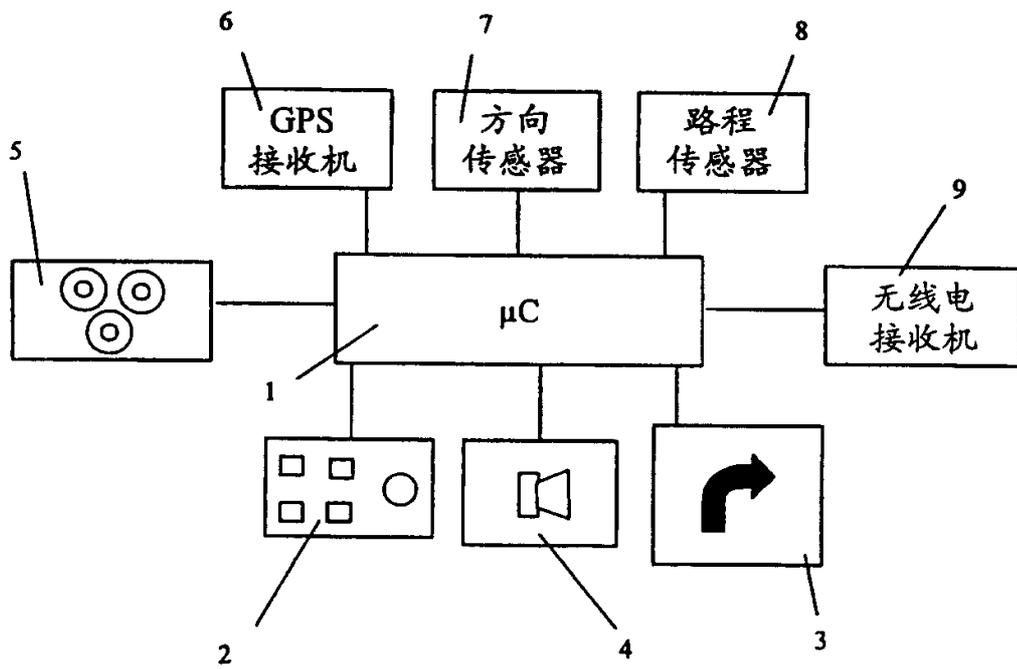


图 1

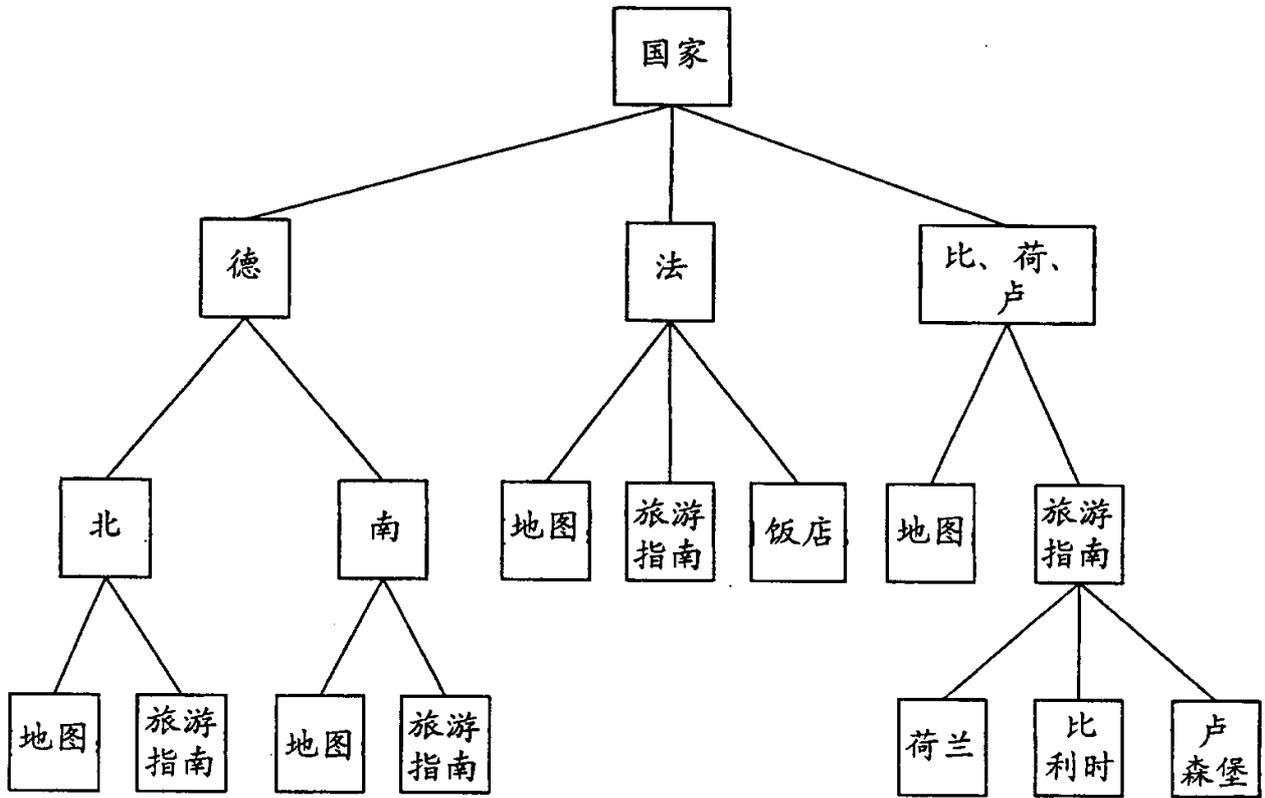
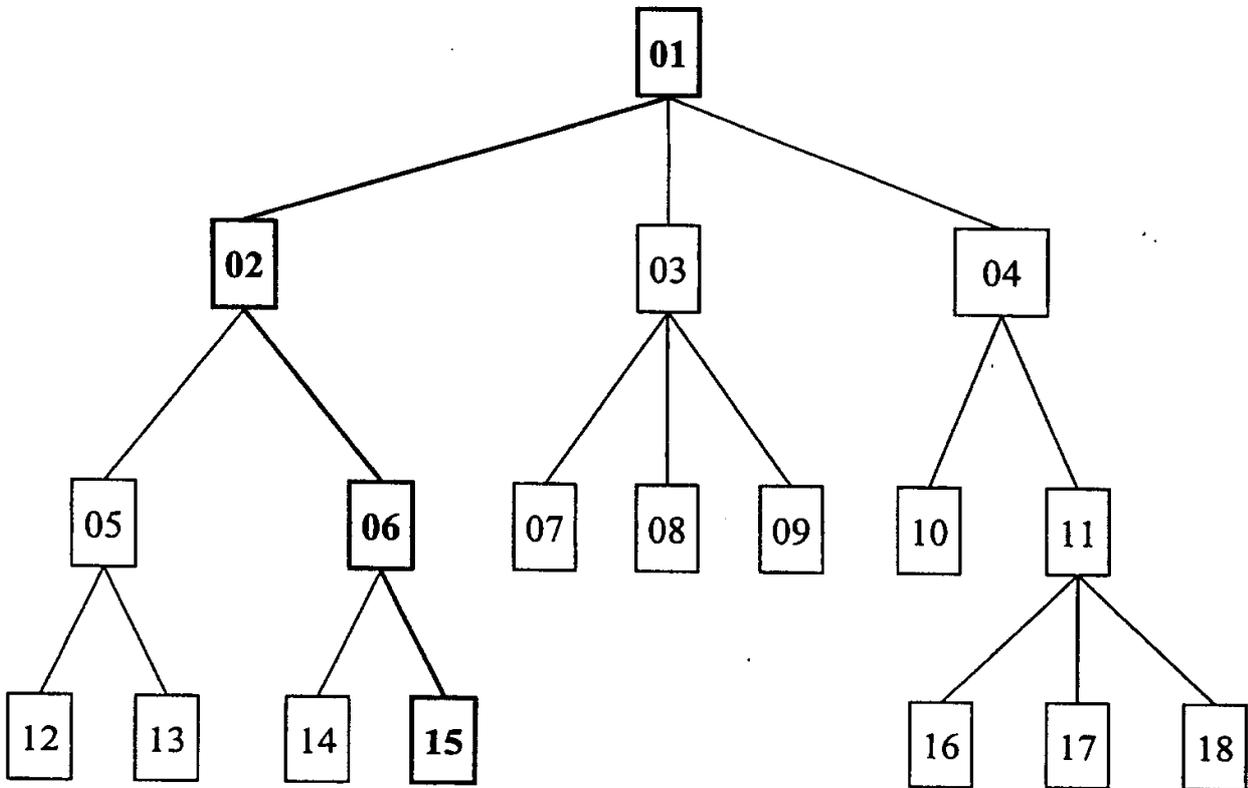


图 2



Nr: **01 02** 03 04 05 **06** 07 08 09 10 11 12 13 14 **15** 16 17 18

AC: **1 1** 0 0 0 **1** 0 0 0 0 0 0 0 0 0 **1** 0 0 0

图 3

Nr: 01 02 03 04 05 06 07 08 09 10

AC: 1 1 0 0 0 1 0 0 0 0

a)

Nr: 01 r 02 r 03 r 04 r 05 r 06 r 07 r 08 r 09 r 10

AC: 1 1 1 0 0 1 0 0 0 1 1 0 0 0 0 1 0 0 0

b)

Nr: 01 02 03 04 05 06 07 08 09 10 t1 t2 t3

AC: 1 1 0 0 0 1 0 0 0 0 0 1 0

c)

图 4

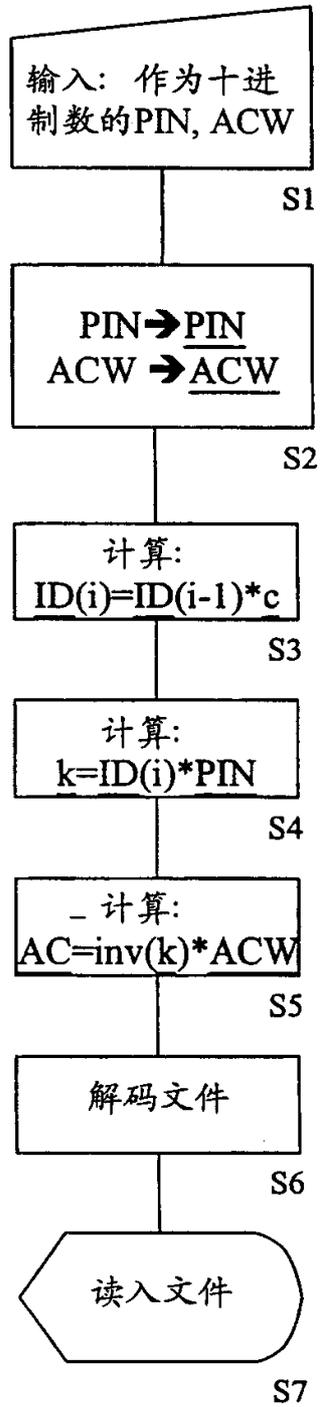


图 5