



(12) 发明专利

(10) 授权公告号 CN 101158587 B

(45) 授权公告日 2011.06.22

(21) 申请号 200710185099.7

G06F 21/24 (2006.01)

(22) 申请日 2002.10.23

(56) 对比文件

(30) 优先权数据

325267/2001 2001.10.23 JP

US 5999622 A, 1999.12.07, 全文.

(62) 分案原申请数据

02148052.4 2002.10.23

JP 特开 2000-146619 A, 2000.05.26, 全文.

(73) 专利权人 丰田自动车株式会社

US 5787170 A, 1998.07.28, 全文.

地址 日本爱知县

US 5065429 A, 1991.11.12, 全文.

(72) 发明人 多田昭人

EP 1189409 A2, 2002.03.20, 全文.

(74) 专利代理机构 永新专利商标代理有限公司

审查员 胡小伟

72002

代理人 钟胜光

(51) Int. Cl.

G01C 21/32 (2006.01)

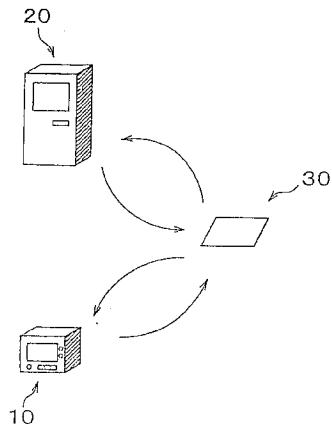
权利要求书 1 页 说明书 7 页 附图 7 页

(54) 发明名称

地图数据处理装置

(57) 摘要

本发明涉及一种地图数据处理装置，用于处理保存在便携式存储介质中的其一部分被加密的地图数据，其特征在于包括：保持部件，用于可分离地保持所述存储介质；解密装置，用于从由所述保持部件保持的所述存储介质中读取存储在所述存储介质上的所述地图数据，以及使用由所述保持部件保持的所述存储介质的特定代码来解密所述读取的地图数据；扩展地图数据创建装置，用于创建将与所述解密的地图数据不同的地图数据增加到所述解密的地图数据中的扩展地图数据；加密装置，用于使用由所述保持部件保持的所述存储介质的特定代码来仅加密所述扩展地图数据的一部分；以及，地图数据存储装置，用于在由所述保持部件保持的所述存储介质上存储仅其一部分已被加密的所述地图数据。该装置能够使对该存储介质的地图数据之非法复制减至最低程度，同时保持地图数据的处理时间短。



1. 一种地图数据处理装置,用于处理保存在便携式存储介质(30)中的其一部分被加密的地图数据,其特征在于包括:

保持部件(22a),用于可分离地保持所述存储介质(30);

解密装置(11),用于从由所述保持部件(22a)保持的所述存储介质(30)中读取存储在所述存储介质(30)上的所述地图数据,以及使用由所述保持部件(22a)保持的所述存储介质(30)的特定代码来解密所述读取的地图数据;

微型计算机(21),用于通过将新购买的地图数据加入到所述解密的地图数据来创建扩充地图数据;

加密装置(21),用于使用由所述保持部件(22a)保持的所述存储介质(30)的特定代码来仅加密所述扩充地图数据的一部分;以及

地图数据存储装置(21),用于在由所述保持部件(22a)保持的所述存储介质(30)上存储仅其一部分已被加密的所述扩充地图数据。

## 地图数据处理装置

[0001] 本申请是申请号为 02148052.4、申请日为 2002 年 10 月 23 日和题目为“地图数据处理方法、地图数据处理装置、存储介质和交通工具上的地图数据处理装置”的中国专利申请的一个分案申请。

### 技术领域

[0002] 本发明涉及一种地图数据处理方法,用于处理保存在便携式可读 / 可写存储介质(诸如存储卡)上的地图数据,还涉及一种地图数据处理装置、可与其一起使用的存储介质和交通工具上的地图数据处理装置。

### 背景技术

[0003] 目前已出现一种系统,其中最新的地图数据从位于加油站或便利店等地点的地图数据销售机(下文中称为“公共信息站终端”)通过付费而保存在称为存储卡的存储介质(例如智能介质)上。该存储介质接着用在一个交通工具上的导航系统或类似系统中,并且保存在存储介质中的地图数据被用作路线导向。这种系统的一个例子在日本专利公开出版号 2000-146619 中公开。根据该系统,利用最新地图数据用于路线导向,能够提供精确的路线导向。

[0004] 但是根据该系统,保存在存储介质中的地图数据能够被复制到同样类型的另一个存储介质上,并且复制的地图数据也能够由导航系统所使用。也就是说,使用该系统,有可能非法复制地图数据,这将给地图的销售带来不利的影响。相反,在地图数据已经由公共信息站终端加密之后在存储介质上保存地图数据是希望得到的。在该加密的地图数据已经由导航系统解密后,该数据再被使用。结果,地图数据的非法复制能够被最小化。

[0005] 但是,当所有的地图数据被加密时,要花时间来对它解密。因此该方法不适用于要求进行快速数据处理的装置,比如导航系统。

### 发明内容

[0007] 因此,本发明的目的是提供一种地图数据处理装置,其能够使对该存储介质的地图数据之非法复制减至最低程度,同时保持地图数据的处理时间短。

[0008] 为了实现本发明的目的,按照本发明的一种地图数据处理装置,用于处理保存在便携式存储介质(30)中的其一部分被加密的地图数据,其特征在于包括:

[0009] 保持部件(22a),用于可分离地保持所述存储介质(30);

[0010] 解密装置(11),用于从由所述保持部件(22a)保持的所述存储介质(30)中读取存储在所述存储介质(30)上的所述地图数据,以及使用由所述保持部件(22a)保持的所述存储介质(30)的特定代码来解密所述读取的地图数据;

[0011] 微型计算机(21),用于通过将新购买的地图数据加入到所述解密的地图数据来创建扩充地图数据;

[0012] 加密装置(21),用于使用由所述保持部件(22a)保持的所述存储介质(30)的特定代码来仅加密所述扩充地图数据的一部分;以及

[0013] 地图数据存储装置 (21), 用于在由所述保持部件 (22a) 保持的所述存储介质 (30) 上存储仅其一部分已被加密的所述地图数据。

[0014] 附图说明

[0015] 通过结合附图阅读以下本发明优选实施例的详细说明, 本发明的上述和其他目的、特征、优点、技术和工业上的意义将被更好地理解, 其中:

[0016] 图 1 是根据本发明的一个示例的实施例的地图数据分配系统的总的结构图;

[0017] 图 2 是图 1 所示的导航系统的框图;

[0018] 图 3 是图 1 所示的公共信息站终端的框图;

[0019] 图 4 是表示由图 3 所示的公共信息站终端 (kiosk terminal) 的 CPU 执行的程序的流程图;

[0020] 图 5A 是在帧格式中具有道路密集之部分的地图的示图;

[0021] 图 5B 是在帧格式中具有设施密集之部分的地图的示图;

[0022] 图 6 是表示由图 2 所示的导航系统的 CPU 执行的程序的流程图; 和

[0023] 图 7 是表示地图数据的结构的例子的示图。

[0024] 实现发明的具体方式

[0025] 在接下来的说明和附图中, 本发明根据示例的实施例被更详细地说明。

[0026] 图 1 示出了一种地图数据分配系统的总的结构。该系统包括作为安装在相应车辆上的车载终端的导航系统 (导航终端) 10、公共信息站终端 (地面终端, 地图数据销售机) 20 和存储卡 30, 存储卡 30 是一种半导体存储介质 (例如智能介质), 公共信息站终端最好位于诸如车站、便利店或加油站这样的位置。该存储卡 30 是便携式的、对于包括地图数据的数据可读 / 可写的存储介质。对每个存储卡 30 特定的序列号是以只读代码 (即卡识别代码) 写入到卡上作为数据。

[0027] 参照图 2, 导航系统 10 包括作为它的主要部件的微型计算机 11。该微型计算机 11 包括 CPU (中央处理单元) 11a、ROM (只读存储器) 11b、RAM (随机存取存储器) 11c、和输入 / 输出接口 11d, 它们全部由总线连接。CPU 11a 使用 RAM 11c 的数据存储功能来执行一个将被随后说明的程序 (例行程序), 它被保存在 ROM 11b 中。

[0028] 而且, 导航系统 10 还包括 GPS 系统 (全球定位系统) 12、地面波发送装置 13、显示装置 14、声音装置 15、操作开关部分 16 和读 / 写装置 17, 它们每一个都连接到输入 / 输出接口 11d, 从而使信号能够在它们之间传送。

[0029] GPS 系统 12 连接到天线 12a, 它从 GPS 卫星 (未示出) 接收 GPS 信号。接着, 利用以预定的时间间隔 (例如 1 秒) 通过天线 12a 接收的 GPS 信号, GPS 系统 12 识别其所在之车辆的位置 (下文称为“车辆位置”), 并将表示识别的车辆位置的数据发送到微型计算机 11。

[0030] 地面波发送装置 13 连接到地面波天线 13a, 并从中央计算机 40 接收无线信号 (见图 3)。显示装置 14 包括显示器 (未示出), 并根据来自微型计算机 11 的命令信号显示信息 (比如需要的地图)。声音装置 15 连接到扬声器 15a 并根据来自微型计算机 11 的命令信号产生需要的声音。操作开关部分 16 包括多个开关, 当它们由用户操作时, 能够使得诸如预定信息 (如目的地) 被输入到微型计算机 11。

[0031] 读 / 写装置 17 包括卡保持装置 17a, 用于以可分离 (可拆卸) 的方式保持存储卡

30。读 / 写装置 17 根据来自微型计算机 11 的命令, 读出在插入的存储卡 30 上的数据并在存储卡 30 上写入必要的数据。

[0032] 前述结构的导航系统 10 接着根据由 GPS 系统 12 获得的车辆位置和用操作开关部分 16 输入的目的地等信息, 从插入到卡保持装置 17a 中的存储卡 30 读出地图数据。接着, 如以下所述, 解密读出的地图数据后, 导航系统 10 接着在显示装置 14 上显示作为地图的地图数据。

[0033] 现在参照图 3, 公共信息站终端 20 包括微型计算机 21。该微型计算机 21 包括 CPU 21a, ROM 21b, RAM 21c 和输入 / 输出接口 21d, 它们都通过总线连接在一起。CPU 21a 执行被保存在 ROM 21b 中的 程序 (例行程序), 其使用 RAM 21c 的数据保存功能, 以下将做说明。

[0034] 而且, 公共信息站终端 20 还包括读 / 写装置 22, 外部存储器 23 和传输电路 24。读 / 写装置 22 包括可分离 (可拆卸) 地保持存储卡 30 的保持部分 (保持装置) 22a, 由用户操作的操作开关部分 22b, 和读 / 写部分 22d。该读 / 写部分 22d 从插入的存储卡 30 中读出地图数据以及存储卡 30 的序列号等。读 / 写部分 22d 也在存储卡 30 上写入地图数据等。在这些装置和进一步包括在公共信息站终端 20 中的其他装置中, 操作开关部分 22b 和读 / 写部分 22d 连接到输入 / 输出接口 21d, 使得信号能够在操作开关部分 22b 和读 / 写部分 22d 与微型计算机 21 之间传输。

[0035] 外部存储器 23 可以是硬盘、MO(磁光盘)或其他类似存储装置, 它连接到输入 / 输出接口 21d 以便数据能够与微型计算机 21 交换。外部存储器 23 提供给微型计算机 21 以必要的信息, 比如地图数据和程序, 并且根据来自 CPU 21a 的命令保存必要的信息。因此, 外部存储器 23 起着地图数据库的功能。保存在外部存储器 23 中的地图数据是没有经过任何类型的加密处理的数据。

[0036] 传输电路 24 连接到微型计算机 21 的输入 / 输出接口 21d, 并通过预定的网络连接到位于远地的中央计算机 40。传输电路 24 从中央计算机 40 获得各种数据, 比如最新的地图数据和与地图数据的费用相关的数据等, 并提供该数据到微型计算机 21。

[0037] 接着将说明上述地图数据处理系统的操作。当用户将存储卡 30 插入到读 / 写装置 22 时, 公共信息站终端 20 的 CPU 21a 执行图 4 所示的程序, 使用操作开关部分 22b 识别用户希望购买的地图数据, 并将为地图数据支付的费用插入到现金插入口 22c。

[0038] 更具体地说, CPU 21a 从步骤 S400 开始该过程, 并前进到步骤 S405。在步骤 S405, 保存在存储卡 30 中的序列号被读出。接着在步骤 S410, 由用户识别的地图数据 (即购买的地图数据) 从外部存储器 (即地图数据库) 23 读出。接着, 程序前进到步骤 S415, 在该步骤中, CPU 21a 用在步骤 S405 读出的存储卡 30 的序列号作为密钥 (secret key) 加密地图数据的一部分。或者, 可以根据序列号和预定函数产生一个适当的密钥, 利用该密钥、而不是只利用该序列号作为密钥, 可以进行加密。

[0039] 这里, 将参照图 5A 和 5B 详细说明该加密。地图数据是覆盖特定区域的地图信息, 如图 5A 和 5B 所示, 它已被译为数据格式。在图 5A 中的例子示出的地图 MAP1 中, 区域 C1 道路密集。与道路不密集的区域比较, 这些区域提供更重要的地图数据。这里, 公共信息站终端 20 只对该道路密集区域 C1 加密。而且, 当没有道路密集的区域 C1 时, 如图 5B 中的地图 MAP2 所示, 只有设施密集的区域 C2 被示出。以这种方式, 公共信息站终端 20 选择相对

重要的部分作为地图数据，并且只加密选择的部分。作为地图信息，该相对重要的部分可以是一个或多个主要道路（例如，高速公路，国道），或一个或多个大型设施（例如，地方官办公场所，市政厅，体育馆，棒球场）。

[0040] 再参照图 4，程序前进到步骤 S420，在该步骤中，CPU 21a 在存储卡 30 中写入（保存）地图数据，该数据中只有前述部分已经被加密，其数据格式中包含表示存储卡 30 的序列号的数据。然后该程序转到步骤 S495，该程序在此结束。根据该程序，其中一部分已经被加密的所购买之地图数据，和能够表示存储卡 30 的序列号的数据（即，其中序列号可被识别的数据）被保存在存储卡 30 中。

[0041] 接着将描述该装置的操作，在用户插入合法的存储卡 30 时的情况下，在该存储卡 30 上，前述的地图数据已经被保存在导航系统 10 的读 / 写装置 17 中，用户利用存储卡 30 上的数据信息用于路线导向或类似作用。

[0042] 在这种情况下，导航系统 10 的 CPU 11a 启动图 6 所示的程序，它以步骤 S600 开始。接着在步骤 S605，CPU 11a 读出已经插入到读 / 写装置 17 中的存储卡 30 的序列号。程序接着前进到步骤 S610，在该步骤中，CPU 11a 从存储卡 30 中读出地图数据。接着在步骤 S615 中，CPU 11a 根据表示序列号的数据重放序列号，该数据被包括在读出的地图数据中。CPU 11a 接着确定该序列号是否在步骤 S605 中读出的存储卡 30 的序列号匹配。

[0043] 因此，在这时，因为合法的存储卡 30 被插入到读 / 写装置 17 中，根据包含在地图数据中的数据重放的序列号与插入到读 / 写装置 17 中的存储卡 30 的序列号相匹配。因此，在步骤 S615 中由 CPU 11a 做出的判断为“是”，并且程序前进到步骤 S620。在步骤 S620 中，CPU 11a 使用在步骤 S605 中读出的序列号作为密钥、解密在步骤 S610 中读出的地图数据的加密部分，并建立没有加密部分的正常地图数据。当使用根据存储卡 30 的序列号产生的密钥和预定的函数对公共信息站终端 20 中的地图数据加密时，导航系统 10 根据插入到读 / 写装置 17 中的存储卡 30 的序列号和预定函数产生密钥，并用该密钥解密该加密的地图数据。

[0044] 接着，程序前进到步骤 S625，在该步骤中，CPU 11a 使用在步骤 S625 中被解密的地图数据，来执行路线导向处理。在该路线导向中，基于被建立的地图数据的地图被显示在显示装置 14 中。接着，当微型计算机 11 在步骤 S625 中完成路线导向处理时，程序前进到步骤 S695，在此结束。

[0045] 如上所述，当合法的存储卡 30 被使用时，导航系统 10 正常地根据存储卡 30 的序列号解密保存在存储卡 30 中的地图数据的加密部分。结果，正常的（即，未加密的）地图数据被获得，导航系统 10 接着使用它来进行路线导向等。

[0046] 接着将被说明的情况是，其中地图数据已经被非法复制到存储卡 30 上并且存储卡 30 已经被插入到导航系统 10 的读 / 写装置 17 中。例如，通过把合法的存储卡 30 插入到典型的个人计算机中，用个人计算机解密该加密的地图数据，建立其中没有加密部分的地图数据，并将其保存在另一个存储卡 30 中，可以完成这种非法复制。

[0047] 当非法的存储卡 30 被插入到读 / 写装置 17 中时，CPU 11a 在步骤 S605 中从插入的存储卡 30 读出序列号，并且在步骤 S610 中从存储卡 30 中读出地图数据，在该步骤后程序前进到步骤 S615。在这时，根据与包含在地图数据中的序列号相关的数据回放的序列号与在步骤 S605 中读出的存储卡 30 的序列号不匹配。因此，在步骤 S615 由 CPU 11a 做出的

判断是“否”，并且程序前进到步骤 S630。在步骤 S630，表示存储卡 30 不能被使用的显示内容被显示在显示装置 14 中，并且程序直接到步骤 S695，在此立即结束。

[0048] 因此，地图数据已经被非法复制于其上的存储卡 30 不能由导航系统 10 使用，因为它具有与保存在地图数据中的数据的序列号不同的序列号。

[0049] 接着将说明数据的非法复制和伪造。在这种情况下，合法购买（保存）到存储卡 30 上的地图数据被非法复制到同样类型的另一个存储卡 30 上。而且，关于包含在已经进行非法复制的存储卡 30 上的地图数据中的序列号的数据已经被伪造，从而使得该序列号与具有非法复制的存储卡 30 的序列号相同。在这种情况下，在 CPU 11a 已经执行从步骤 S600 到 S610 的处理后，程序前进到步骤 S615，其中由 CPU 11a 做出的判断是“是”。程序接着前进到步骤 S620，在该步骤中，利用具有非法复制的存储卡 30 的序列号，数据的加密部分被解密。

[0050] 因为该地图数据的一部分是用合法存储卡 30 的序列号加密，但是，在步骤 S620 被解密的地图数据变得恶化（即，正常数据不能被解密），并且地图数据不能在步骤 S625 中被正常使用。即，这种类型的恶化（corruption）呈现出存储卡 30 具有不能使用的非法拷贝。

[0051] 如上所述，根据该示例性实施例的地图数据处理系统，地图数据从公共信息站终端 20 被购买，并且购买的地图数据被保存在已经插入公共信息站终端 20 的读 / 写装置 22 中的存储卡 30 上。此时，公共信息站终端 20 用对所插入的存储卡 30 特定的、并保存在该卡上的代码（即，序列号），来加密地图数据的重要部分作为地图信息，并且在存储卡 30 上保存加密的地图数据。接着，当存储卡 30 被插入到读 / 写装置 17 中时，导航系统 10 利用对插入的存储卡 30 为特定的代码、解密保存在存储卡 30 上的地图数据的加密部分，并且建立未被加密的合法地图数据。而且，如果对插入到读 / 写装置 17 中的存储卡 30 为特定的代码（即，序列号）与根据写到地图数据中的数据重放的特定代码（即，序列号）不匹配，则可以确定的是，存储卡 30 正在进行地图数据的非法复制，并且导航系统 10 呈现存储卡 30 上的地图数据不能使用（即，禁止使用存储卡 30 上的地图数据）。

[0052] 因此，当保存在合法存储卡 30 中的加密的地图数据已经被非法复制到另一个存储卡 30 时，地图数据没有被正确解密，或者具有非法拷贝的存储卡 30 被呈现出不能使用。因此可以使地图数据非法复制到另一个存储卡 30 上的情况降低到最小程度。

[0053] 应当注意的是，本发明不限于前述的示例性实施例，而可以用本发明之范围内的进一步改变和修改实现。例如，在前述的示例性实施例中，地图数据被公共信息站终端 20 加密，并由导航系统 10 解密。然而另一方式是，同样由导航系统 10 加密的地图数据可以被保存在存储卡 30 上，并且保存在存储卡 30 上的该地图数据可以由公共信息站终端 20 解密。

[0054] 而且，优选的是，公共信息站终端 20 被构造以便能够保存新购买的一个特定区域的地图数据在存储卡 30 上，在该卡上，另一个特定区域的地图数据已经被合法保存，或者将这个特定区域的地图数据存储在不同的存储卡 30 上。更具体地说，公共信息站终端 20 从插入的存储卡 30 中读出保存在存储卡 30 上的地图数据，并用存储卡 30 的序列号解密该地图数据。公共信息站终端 20 接着将不同的新购买的地图数据加入到解密的地图数据中，并建立将被保存的扩充的地图数据。当存储卡 30 具有更大的容量时，公共信息站终端 20

接着用插入的存储卡 30 的序列号、或用那一张存储卡 30 的序列号来加密所建立的扩展地图数据的一部分，并在插入的存储卡 30 上保存该扩展地图数据。通过以这种方式（即，通过给公共信息站终端 20 一个解密函数）构建公共信息站终端 20，在开始有可能的是，已经在小容量存储卡 30 上保存了有限区域的地图数据的用户再保存更多的地图数据，包括该有限区域的地图数据，或者再在单个大容量存储卡 30 上再保存该有限区域的地图数据与不同的地图数据。

[0055] 而且，根据前面的示例性实施例，地图数据的加密部分可以是地图数据或其中一部分中的完全索引区域。也就是说，如图 7 所示，地图数据被分成一个实际数据区域和一个索引区域。在实际数据区域保存了多个位置数据，它们用经度 x 和纬度 y 表示道路交点和设施等的位置。在索引区域保存了索引数据，用于识别以下数据的顶端地址：i) 表示每条道路（的交点）或每个设施的名字（通过分类）的数据，用于识别每条道路交点和每个设施之目的，以及 ii) 表示那个道路或设施的位置数据。索引数据也识别该顶端地址的数据长度。当地图数据用这种方法被分成实际数据区域和索引区域时，该索引区域的所有数据或一部分数据可以被加密。而且，该示例性实施例的存储卡 30 也可以是另一种记录介质，比如 CD-ROM，只要它也是便携式的、并能读和写（即保存）数据。

[0056] 而且，在前述的示例性实施例中，公共信息站终端 20 被用作向存储卡 30 提供地图数据（即信息）的装置（设备）。然而另一方式是，一个提供地图数据的中心站（即地图数据分配服务器）和一台个人计算机也可以被用作向存储卡 30 提供地图数据的装置。本发明也可以被应用到这种情况。

[0057] 更具体地说，地图数据通过传输从保存地图数据的中心站被提供 给个人计算机。而且，一种专用的应用程序被安装在个人计算机上，用于在存储卡 30 上保存地图数据。接着，使用该专用软件，个人计算机加密由中心站提供（即从中心站发送的）的地图数据（或地图数据的一部分），并且在存储卡 30 上保存该加密的地图数据。这一加密是利用保存地图数据的存储卡 30 的序列号实现的，这与前述的示例性实施例相同。因此，通过个人计算机保存在存储卡 30 中的地图数据由导航系统 10 解密，正如通过公共信息站终端 20 保存在存储卡 30 上的地图数据，然后该地图数据被用作路线导向等。

[0058] 在这种情况下，由中心站提供（即发送）到个人计算机的地图数据暂时不加密地保存在个人计算机中。但是，一旦在该数据已经保存在存储卡 30 中后，如上所述，该专用的应用程序立即从个人计算机中擦去该数据，从而将地图数据非法复制到存储卡 30 上的情况降低到最小程度。

[0059] 而且，在将地图数据从中心站传输到个人计算机期间，优选的是，地图数据在由中心站用普通的加密被加密后、被发送到个人计算机，从而防止地图数据由第三方非法截取（即复制）。在这种情况下，个人计算机在从中心站接收地图数据后进行解密，并在由专用应用程序用特殊加密手段来加密它后，将其存储在存储卡 30 上。

[0060] 另外，根据前述的示例性实施例，加密和解密是利用存储卡 30 的序列号来实现的。但是，该序列号本身也可以如上所述被加密并解密。即，在生产存储卡 30 时，序列号能够用预定的方法被加密，并且然后该加密的序列号能够保存在存储卡 30 上。接着公共信息站终端 20 首先对已经插入到公共信息站终端 20 的存储卡 30 上的加密序列号进行解密，并获得该正常序列号。使用该正常序列号，公共信息站终端 20 加密地图数据的一部分，它接

着保存在存储卡 30 上。同时，导航系统 10 对已经插入到导航系统 10 中的存储卡 30 上的加密序列号进行解密，并获得该正常序列号。使用该正常序列号，导航系统 10 解密存储卡 30 上的地图数据的加密部分，并使用该解密的地图数据来作路线导向等。因此，因为序列号和地图数据都需要以这种方式被加密和解密，防止地图数据之非法复制的效果更加得以改善。

[0061] 当存储卡 30 被用户插入到公共信息站终端 20 并且给出一个命令要求购买的特定地图数据时，公共信息站终端 20 在存储卡 30 上保存该地图数据。此时，公共信息站终端 20 用一个序列号作为密钥来加密地图数据的一部分，该序列号是一个对存储卡 30 为特定的代码。接着，当存储卡 30 被插入到导航系统 10 中时，导航系统 10 读出存储卡 30 上保存的地图数据，并利用存储卡 30 的序列号作为密钥、来解密该加密部分，其中包括读出的地图数据。结果，可以将地图数据非法复制到另一个存储介质的情况降低到最小程度。

[0062] 尽管本发明已经参照其优选实施例被说明，应该理解的是，本发明不限于这些优选的实施例和结构。相反，本发明旨在覆盖各种修改和等效的装置。另外，尽管这些优选实施例的各种组件是以各种组合和结构示出，它们是示例性的，其他的组合和结构（包括更多、更少和只有单个部件）都在本发明的宗旨和范围内。

图 1

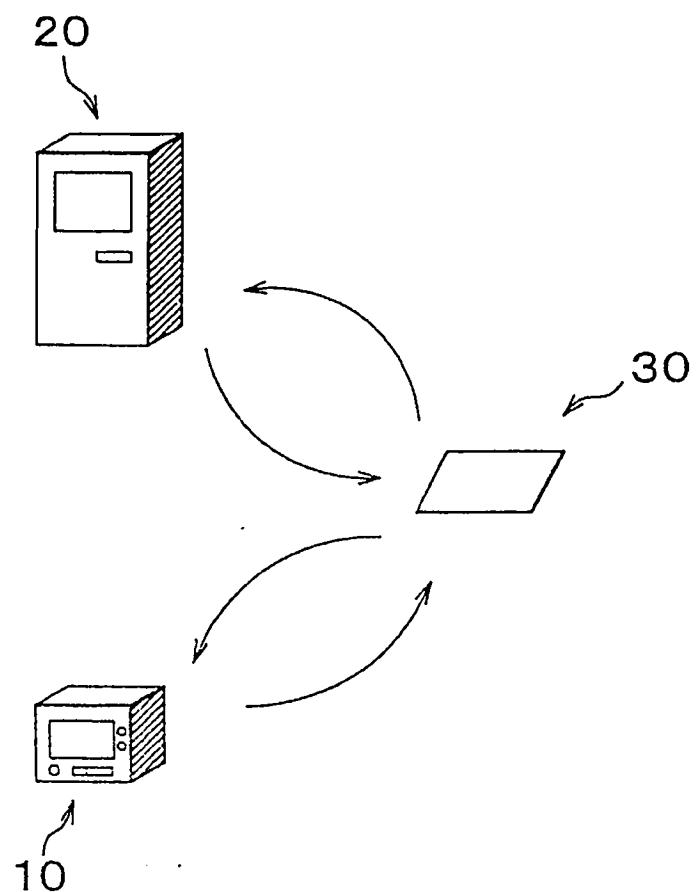


图2

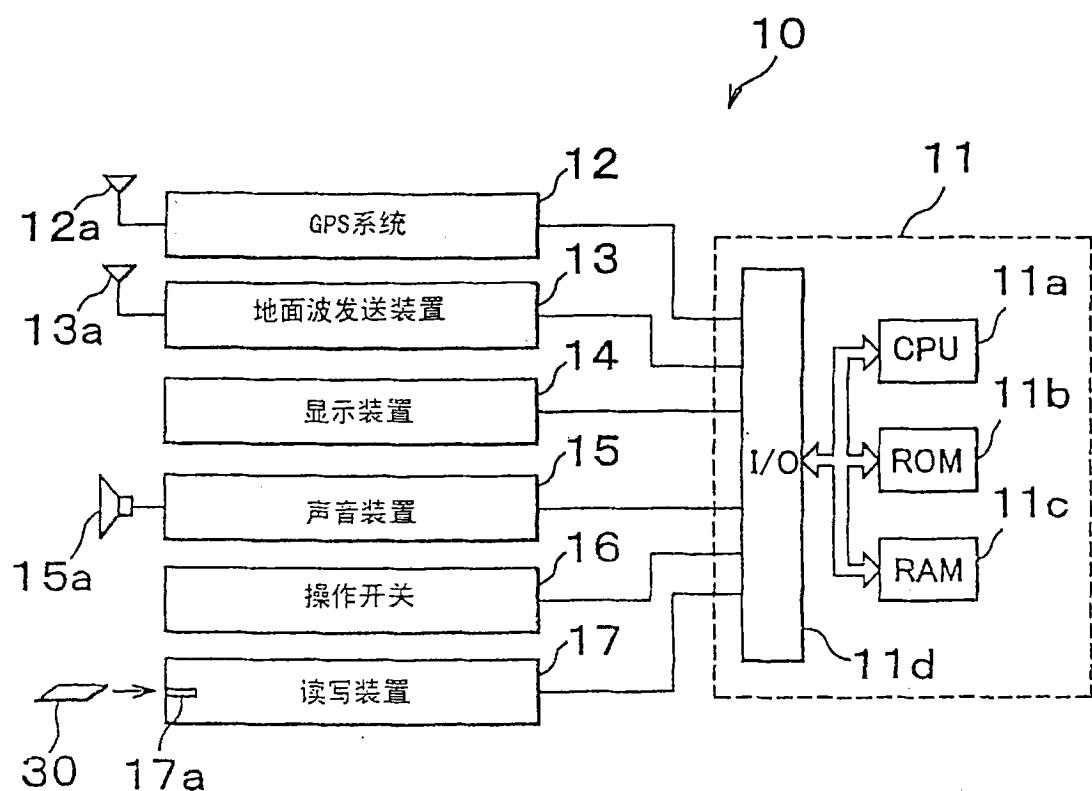


图3

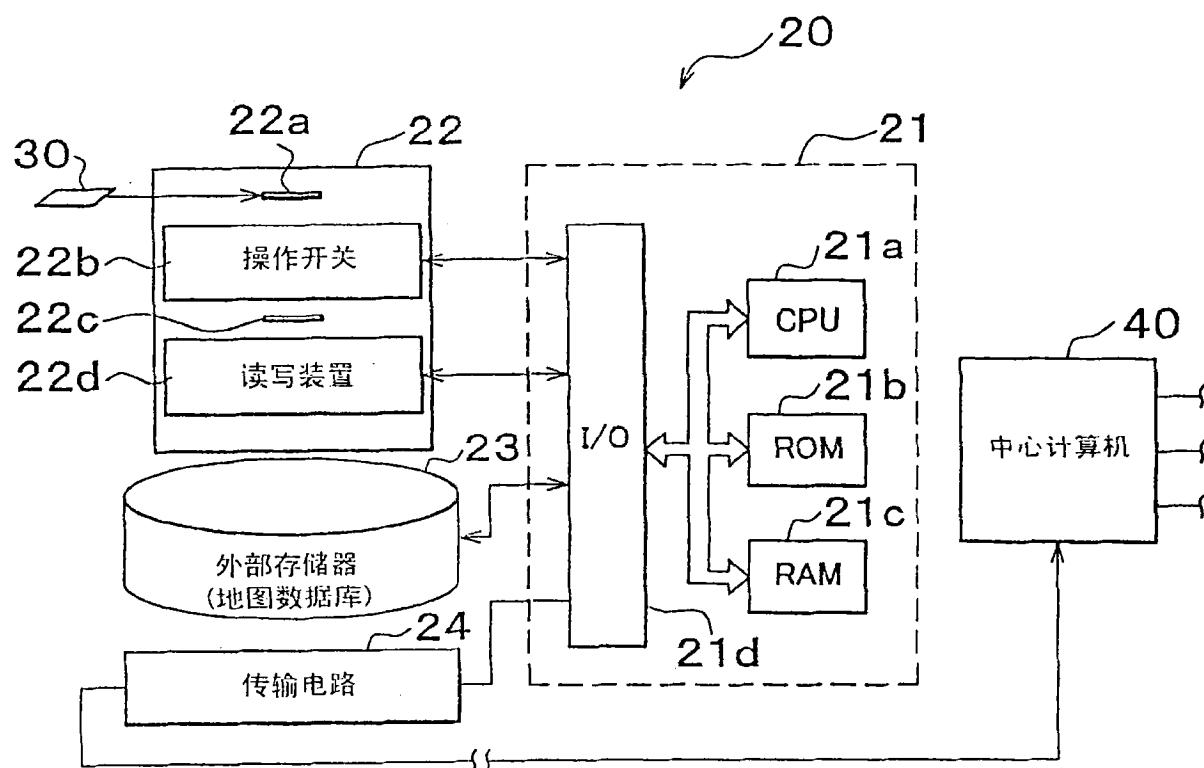


图 4

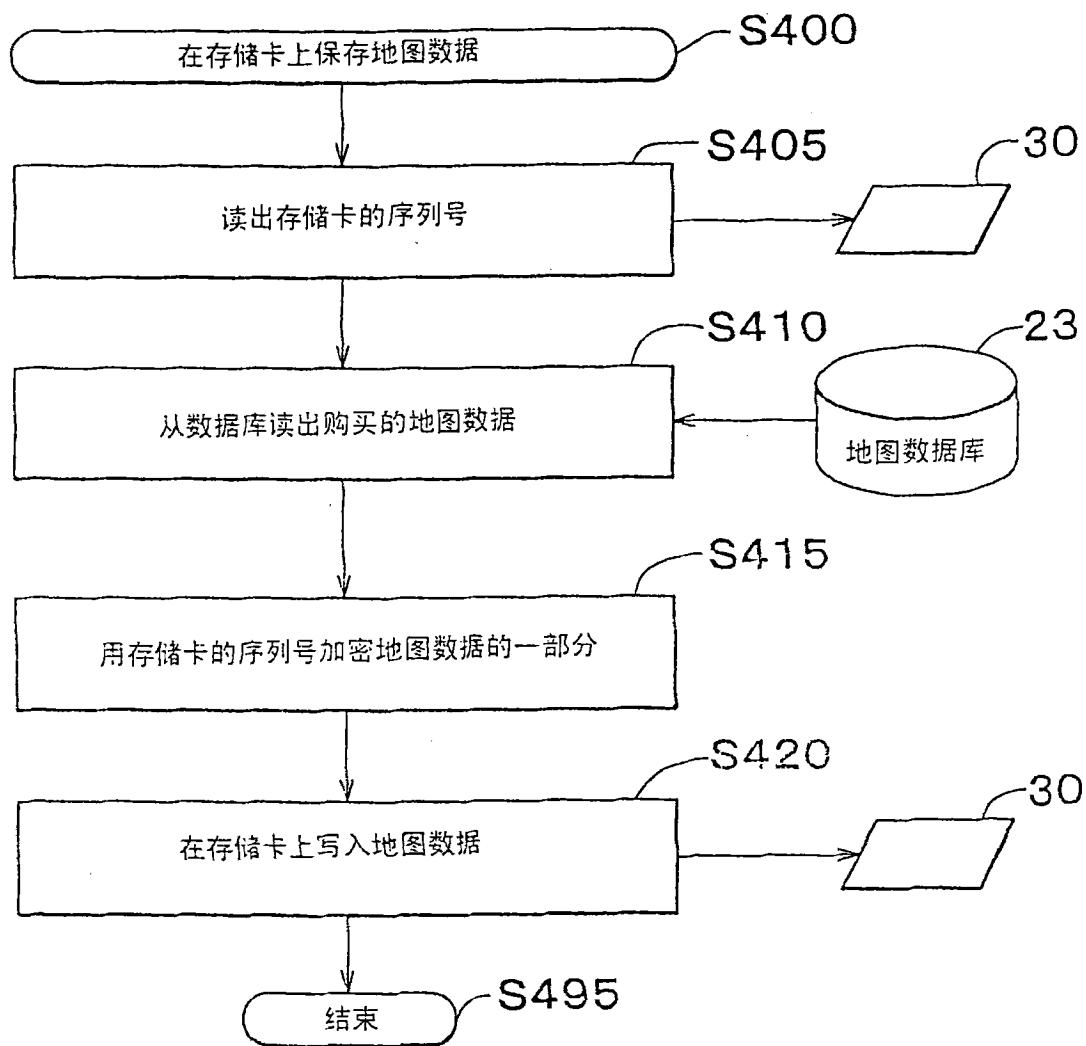


图 5A

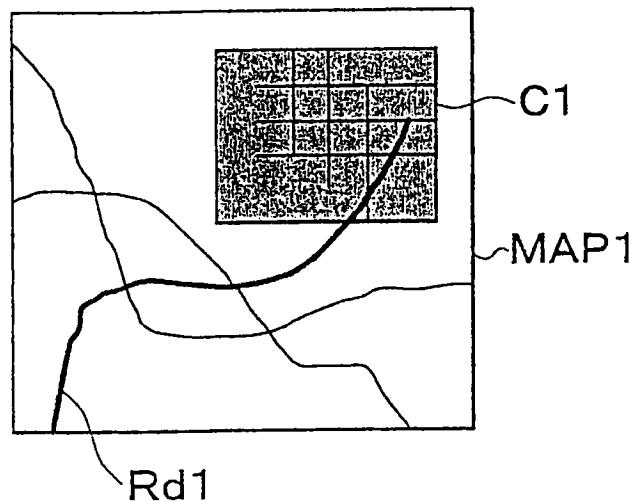


图 5B

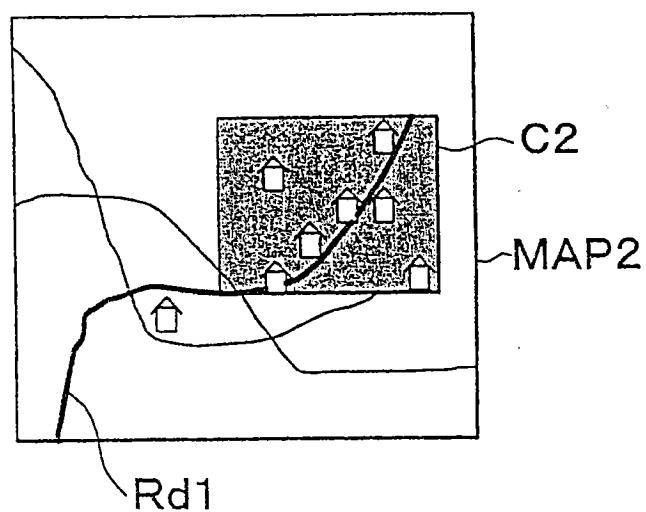
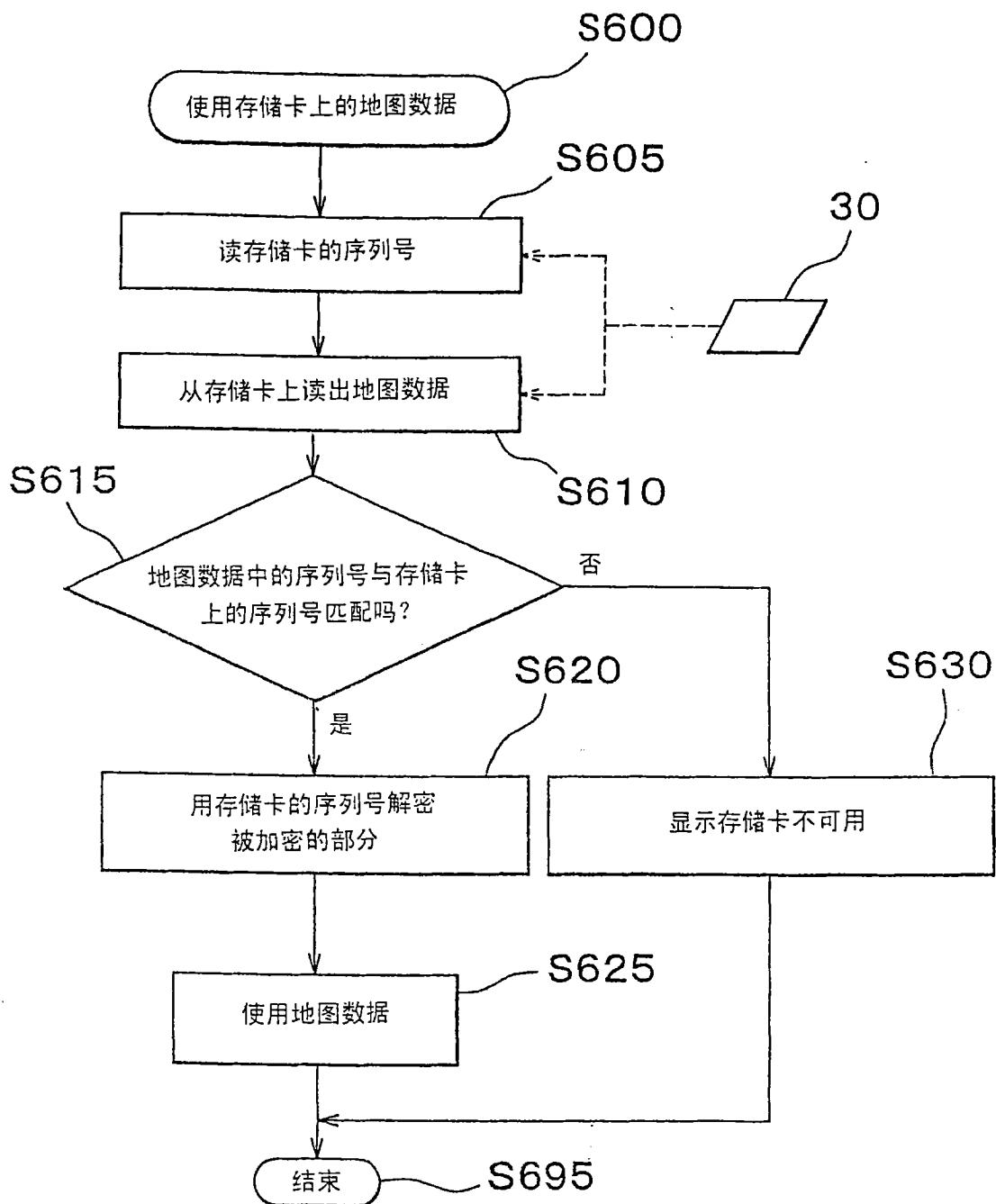


图 6



## 图 7

