[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 11/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 99816719.3

[45] 授权公告日 2006 年 10 月 4 日

[11] 授权公告号 CN 1278236C

[22] 申请日 1999.6.10 [21] 申请号 99816719.3
[86] 国际申请 PCT/NL1999/000360 1999.6.10
[87] 国际公布 WO2000/077640 英 2000.12.21
[85] 进入国家阶段日期 2001.12.10
[71] 专利权人 贝勒加特投资公司
地址 荷兰海牙
[72] 发明人 爱德华·卡雷尔·德容
尤尔金·诺贝特·埃尔科·博斯
审查员 张桂华

[74] 专利代理机构 北京市中咨律师事务所
代理人 杨晓光 于 静

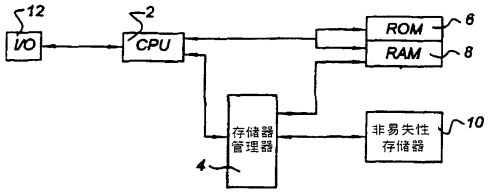
权利要求书 3 页 说明书 9 页 附图 3 页

[54] 发明名称

在分离的存储区域中存储数据组的不同版本的装置和更新存储器中数据组的方法

[57] 摘要

一种用于更新存储器中的数据组的方法，该方法包括：(a)在一第一存储区域中存储所述数据组的一最老版本，其中所述存储器包括至少一个标志，用于识别所述最老版本，和(b)在一分离的第二存储区域中存储所述数据组的最近更新版本，其中，所述存储器包括至少一个标志，用于识别所述最近更新版本。 该方法还包括为每一页面提供其自己的标志，用于识别所述数据组的版本号(gen#)和所述页面的页面号(pg#)。 本发明还涉及一种处理器装置和一种计算机装置，该处理器装置用于实现上述方法，该计算机装置包括该处理器装置。



1.一种用于更新存储器中的数据组的方法，包括以下步骤:

（a）在一第一存储区域中存储所述数据组的一最老版本，其中所述存储器包括至少一个标志，用于识别所述最老版本，和

（b）在一分离的第二存储区域中存储所述数据组的最近更新版本，其中所述存储器包括至少一个标志，用于识别所述最近更新版本;

所述第一存储区域包括第一组一个或多个页面，所述第二存储区域包括第二组一个或多个页面，页面包括连续的存储位置，这些存储位置在例如应用数据存储的分配、更新和解除分配的存储操作期间被用作为一个单元，其特征在于，

所述方法进一步包括为每一页面提供其自己的标志，用于识别所述数据组的版本号和所述页面的页面号。

2.根据权利要求1的方法，其中，每一所述标志包括对所述数据组的标记。

3.根据权利要求1的方法，其中每一页面对应于一条字线。

4.根据权利要求1的方法，包括利用关于标志内容的冗余码写标志，在已从存储装置中读取标志后，由所述冗余码来分析是否已发生写错误。

5.根据权利要求1的方法，包括将所述多个页面中的一个预定页面的预定标志写入所述存储器作为所述更新的最后步骤。

6.根据权利要求1的方法，其中所述标志中的至少一个包括表示所有权和使用权的附加数据，且所述方法包括从这些附加数据识别所有权和使用权。

7.根据权利要求6的方法，其中对于数据组的不同部分，所述使用权不同，且所述方法包括对这些不同部分识别不同的使用权。

8.根据权利要求1的方法，包括分析标志值，并仅允许通过查询所述标志值来访问所述数据组的所述版本。

9.一种计算机装置，包括一处理器和一存储器，该存储器至少具有一

第一存储区域和一分离的第二存储区域，该处理器被配置根据下列操作更新所述存储器：

（a）在所述第一存储区域中存储所述数据组的一最老版本，其中所述存储器包括至少一个标志，用于识别所述最老版本，和

（b）在所述分离的第二存储区域中存储所述数据组的最近更新版本，其中，所述存储器包括至少一个标志，用于识别所述最近更新版本；

所述第一存储区域包括第一组一个或多个页面，所述第二存储区域包括第二组一个或多个页面，页面包括连续的存储位置，这些存储位置在例如应用数据存储的分配、更新和解除分配的存储操作期间被用作为一个单元，

其特征在于，

每一所述页面具有其自己的标志，用于识别所述数据组的版本号和所述页面的页面号。

10.根据权利要求9的处理器装置，其中，每一所述标志包括对所述数据组的标记。

11.根据权利要求9的计算机装置，其中每一页面对应于一条字线。

12.根据权利要求9的计算机装置，其中处理器利用关于标志内容的冗余码写标志，在已从存储器中读取标志后，由所述冗余码来分析是否已发生写错误。

13.根据权利要求9的计算机装置，其中处理器将所述多个页面中的一个预定页面的预定标志写入所述存储器作为所述更新的最后步骤。

14.根据权利要求9的计算机装置，其中所述标志中的至少一个包括表示所有权和使用权的附加数据，其中处理器从这些附加数据识别所有权和使用权。

15.根据权利要求14的计算机装置，其中对于数据组的不同部分，所述使用权不同，其中处理器对这些不同部分识别不同的使用权。

16.根据权利要求9的计算机装置，其中处理器分析标志值，并仅被允许通过查询所述标志值来访问所述数据组的所述版本。

17.根据权利要求9的计算机装置，其中所述处理器包括一中央处理单元（2）和一分离的存储器管理单元（4），且标志值仅为该存储器管理单元（4）所知。

18.根据权利要求17的计算机装置，其中，所述存储器管理单元（4）在将标志写入存储器之前用加密密钥编码标志，所述加密密钥仅为存储器管理单元（4）所知。

19.根据权利要求18的计算机装置，其中所述加密密钥涉及加密单向功能。

20.根据权利要求9的计算机装置，其中该处理器的至少一部分被实现在智能卡的单个芯片中。

在分离的存储区域中存储数据组的不同版本的装置和更新存储器中数据组的方法

技术领域

本发明涉及存储器部件，该部件包括在一存储区域中至少一组数据。该存储器部件可利用易失性 RAM 器件或非易失性硅器件、例如 EEPROM（电可擦可编程只读存储器）、flash-EPROM（闪速电可擦可编程只读存储器）或 ROM（只读存储器）等来实现。通常，这种存储器存储操作系统软件模块、应用程序和应用数据。在根据本发明的这种计算机系统特别可应用的区域中，将某些或所有的操作系统软件模块存储于 ROM 中。

背景技术

在一些应用中，特别是金融交易处理中，必须非常安全地进行存储。在“永久”存储部件中，这种安全存储应用被认为是需要“更新的原子性（Atomicity of Update）“。从现有技术可知使用更新日志，以执行这种安全更新。这种更新日志登记更新期间内需要被改变的数据组的各部分。仅当将数据组及其更新部分一起存储于存储器中时，才可删除该数据组以前版本的所有关联。

发明内容

本发明的目的在于为对于存储于非易失性存储器器件（特别是例如 EEPROM 或闪速 EEPROM 的硅存储器件）中的数据之更新的原子性提供一种机构，以支持应用数据的永久存储。

根据本发明的一个方面，提供了一种用于更新存储器中的数据组的方法，包括以下步骤：（a）在一第一存储区域中存储所述数据组的 -最老版本，其中所述存储器包括至少一个标志，用于识别所述最老版本，和（b）在一分离的第二存储区域中存储所述数据组的最近更新版本，其中，所述存储器包括至少一个标志，用于识别所述最近更新版本；所述第一存储区域包括第一组一个或多个页面，以及所述第二存储区域包括第二组一个或多个页面，页面包括连续的存储位置，这些存储位置在例如应用数据存储的分配、更新和解除分配的存储操作期间被用作为一个整体，其特征在于，所述方法进一步包括为每一页面提供其自己的标志，用于识别所述数据组的版本号（gen#）和所述页面的页面号（pg#）。

根据本发明的另一方面，提供了一种处理器装置，包括一处理器和一存储器，该存储器至少具有一第一存储区域和一分离的第二存储区域，该处理器被配置根据下列操作更新所述存储器：（a）在所述第一存储区域中存储所述数据组的一最老版本，其中所述存储器包括至少一个标志，用于识别所述最老版本，和（b）在所述分离的第二存储区域中存储所述数据组的最近更新版本，其中，所述存储器包括至少一个标志，用于识别所述最近更新版本；所述第一存储区域包括第一组一个或多个页面，以及所述第二存储区域包括第二组一个或多个页面，页面包括连续的存储位置，这些存储位置在例如应用数据存储的分配、更新和解除分配的存储操作期间被用作为一个整体，其特征在于，每一所述页面具有其自己的标志，用于识别所述数据组的版本号（gen#）和所述页面的页面号（pg#）。

根据本发明的又一方面，提供了一种包括所述处理器装置的计算机。

附图说明

下面，参照附图来详细描述本发明，这些附图只是说明本发明，并不限制本发明的范围。

图 1 表示根据本发明的一个实施例的实例；

图 2 表示根据本发明的存储器的可能设置；

图 3 表示根据图 2 设置的可能实施例中的存储器页面的内容；

图 4 说明根据本发明的方法；和

图 5 说明根据本发明的存储器管理单元的可能设置。

具体实施方式

图 1 表示根据本发明的一个可能装置。将中央处理单元 2 连接到输入/输出部件 12 和可包括 ROM 6、RAM 8 和非易失性存储器 10 的存储器上。可在中央处理单元 2 之外或在其中设置存储器管理器 4。所设置的管理器 4 用于执行对应于非易失性存储器 10、最好还有其它存储部 ROM 6 和 RAM 8 的存储功能。图 1 所示实施例涉及所有种类的数据存储器件之管理系统。但是，与硬盘相比，本发明对非易失性硅器件中的数据存储特别有效。其主要应用是在嵌入式计算机系统领域中，和例如智能卡的单片计算机中。

图 2 表示根据本发明的存储器中数据存储的一可能设置。将非易失性数据存储器 10 分成存储单元。其中，将这些存储器存储之单元称为“页面”。为了方便起见，这些页面尺寸相同，例如等于用于实现存储器的硅器件中的“字线”的尺寸。但是，页面也可具有不同的尺寸。存储器管理器 4 一页一页地管理存储器的内容：应用数据存储的分配、更新和解除分配（de-allocation）涉及处理一个或多个页面。

存储器包括一组应用数据元的不同代（或版本）。每一代可被存储在一个或多个页面中。在图 2 中，表示存储器包括一组应用数据元的三个不同代 k、k+1、k+2 的情况。该实例表示代 k 占据三个页

面 1、2 和 3，代 k+1 占据两个页面 i、i+1，代 k+2 占据两个页面 n、n+1。代 k 是该存储器中该组应用数据元的最老版本，而代 k+2 是该组应用数据元的最近更新版本。代 k、k+1、k+2 中的每一个都可以例如涉及软件对象的不同版本。

代 k、k+1、k+2 被显示来形成一“数据组块”（data chunk），其中，该术语在此被用作对单个一组应用数据元的标记（reference）。由未被存储器管理器 4 确定的页面占据的存储器中的任何位置来分配存储所需的页面。图 2 所示数据组块的不同代 k、k+1、k+2 可以存储或可不存储于连续存储器位置中的存储器中。存储器管理器 4 是决定在哪里存储不同代的单元。即使是一代中的页面也不必存储于连续页面中。为了说明这一点，将页面 n 和 n+1 表示为彼此位置相距遥远（其间用点表示）。

实际上，存储器包含多个“数据组块”，即不同数据组的多个代组。

在根据本发明构成和管理的存储器中，存储器管理器 4 执行的管理策略提供更新的原子性。在被存储后，在相同的存储区域中不再变更与该组应用数据元的版本相关的数据。换言之，一旦生成页面就不再对其进行变更。当根据中央处理单元 2 中运行的应用程序需要修改最后更新的一组应用数据元时，存储器管理器 4 分配一新的存储区域，例如一组新的页面。在该新的存储区域中，存储器管理器 4 存储任何已改变的值以及未被改变的该组应用数据元的数据元之值。通过该方法，存储器 10 在任何时间都将保持该数据组块的至少一个一致的、有效的版本。

例如，这种更新动作可与智能卡相关。虽然智能卡中的数据更新仅花费很短的时间（例如约 3 毫秒），在完成与终端的数据事务之前，很少有机会从通信终端中取出智能卡。因此，在完成前更新可能被中断。当这种情况发生时，至少该最后更新版本仍存在于智能

卡的存储器中。

在一个实施例中，在完成数据组的更新后，存储器管理器 4 通过重新分配存储区域来继续存储该数据组的最老版本。例如，存储器管理器 4 可控制一组应用数据元的不多于 10 个版本的存在。在实际实现时，中央处理单元 2 中运行的应用程序将与存储器管理器 4 互相配合来控制其数据的更新过程，例如指示更新的完成。应用程序将提示存储器管理器 4 完成更新，之后，存储器管理器 4 完成对存储器 10 的写操作。在事务处理系统中，这种更新过程信号传输是普遍的。

当存储器中存在该组应用数据元的多个版本时，通过存储器管理器 4 可以分子数据的变更经历。通过为在中央处理单元 2 中运行之应用程序提供部件以检查但不变更在先版本中的数据值，存储器管理器 4 进行上述分析。

图 3 表示根据本发明的一种可能的存储器页面结构。假设将存储器分成页面。图 3 示出两个页面 i、i+1。每个页面 i、i+1 都包含应用程序数据和标志 i、i+1。优选的是，标志值包括三个部分：“组块标识符”chid、代计数 gen#和页面计数 pg#。组块标识符用作对所存储数据的程序编制器单元的唯一标记。代计数器 gen#标识存储数据的版本号码。代计数器 gen#将至少表示两代。页面计数器 pg#表示在页面所属一组程序数据的代中相关页面的页面号码。页面计数器 pg#允许将数据组的一代数据存储为多个页面。

在本发明的一个特定实例中，用特定编码来将标志值存储在存储器中，例如，利用具有设为 1 的限定数目之比特的冗余码。存储器管理器 4 使用该特定编码来检测正确/错误数据写操作。仅当所限定数目之比特被检测为 1（或高）时，存储器管理器 4 才确定该标志值有效。如果该限定数之比特未被设定为 1，则存储器管理器 4 确定该标志值无效。例如，这种情况可以是由于中断对存储器件供电引

起的，例如，当在完成金融交易之前，智能卡用户从终端中取出他的智能卡。

在这一实施例中，在去除数据组的最老代之前，存储器管理器 4 将确定最近更新的代的有效性。可根据使用的硅存储器件的物理特性来确定该特定标志编码方法。应当选择的是，如果存储器件不能全面地写该页面，则很可能导致无效编码。根据存储器芯片设计（即使用的晶体管技术），在将新的数据写入页面前，一些存储器首先将特定页面的所有存储位置值都改为 0 或 1。因此，如上所述，有时较优的是，检查标志中限定数之比特是否是 1，而在其它情况下，检查存在为 0 的限定数之比特可能是更好的。那么，如果发现对标志的检查正确，则问题在于与该标志相关的页面之其余内容是否也被正确写入的已知可能性。

图 4 概述了当按中央处理单元 2 上运行的应用程序的控制来更新存储的应用数据的版本时、本发明一个实施例中的存储器管理器 4 所执行的操作顺序：

a．在存储器 10 中分配新的页面组，步骤 40；

b．定义新的页面组的每个新页面的标志值，步骤 42；

c．将修改形式下的应用程序数据和相应的标志一页一页地写到存储器 10，步骤 44；

d．对每个所写页面检验其结果是正确的，步骤 46；

如上所述，通过检查标志值可以执行这个检验步骤；

e．重新分配保持该组数据之最老代的页面，步骤 48。

用指定的组块标识符 chid、以递增 1 的最近前更新版本的代计数值 gen#和页面计数 pg#来定义每个新页面的标志值。

优选的是，按上述步骤 c 所示一页一页地将页面写入存储器 10。优选的是，对一组数据的页面组的一个预定页面必须是被最后写入，而所有其它页面可以任何顺序来写入。为了方便起见，该预定页面

是该新的页面组的第一页面。实际上，任何页面可被分为若干部分来写。例如，该页面的标志值可与页面中应用程序数据分开来写。但优选的是，在更新动作的最后步骤中写入该预定页面的标志，该预定页面是被写入的最后页面。这清楚地表示了更新动作已完成。直到该预定页面的标志被写入存储器中，还可变更写到任何新页面上的应用程序数据。但是，值得注意的是，对页面数据的部分写入和变更可降低利用本发明可得到的优点，即总的写时间变长。写象EPROM 这样的非易失性存储器 10 花费相当长的时间，如今约为 3 毫秒。因此，最好仅对存储器 20 写一次，即，当整个变更的数据组准备被存储并在连续的时间段内不写入该组数据的变更部分时。另外，如果时间充裕，通常如此，本领域的通常做法是将一组数据的变更部分写入非易失性存储器中。但是，这会导致写操作数量的增加，导致非易失性存储器 10 的不必要的损耗。

因此，根据本发明的一个实施例，优选的是，在将修改的数据组写入非易失性存储器 10 之前，对 RAM 8 中的该组数据的工作副本执行完全修改数据组所需的所有步骤。

作为更新期间中的最后操作，写预定页面的标志值是实现多页面更新的原子性的有利措施。预定页面中有效标志的存在或缺少，其作用是作为“提交”标识：预定页面中的有效标志表示所写页面的有效性和整个更新过程的最后完成。

当通过利用组块标识符 chid 的应用只能物理寻址存储在存储器中的数据时，可以更安全地实现应用程序数据的存储器存储。则存储器 10 变为“按内容编址的存储器”（CAM）。

虽然存储器管理器 4 和中央处理单元 2 可在一个物理处理单元中，但对后一特征而言，特别有利的是，中央处理单元 2 和存储器管理器 4 是两个相互进行通信的物理分离单元。应该明白的是，“物理分离”仍可指单个芯片上制造的单元。则存储器 10 的物理地址空

间不包括在中央处理单元 2 的地址空间中，特别是不包括在存储应用程序或操作系统软件指令的地址空间中。如果存储器管理器 4 也被作成防干预（tamper-resistant）（如智能卡中），将获得免遭“探查”的附加保护。

为了实现这种例如对智能卡的潜在附加保护，存储器管理器 4 可提供附加的接口功能性，例如包含标志尺寸地址寄存器 54 和页面数据尺寸数据寄存器 52（参见图 5）。接口 52、54 与逻辑单元 50 配套，以执行用于扫描和匹配存储于存储器 10 中的标志的逻辑功能。换言之，逻辑单元 50 可从存储器 10 中读取标志，并通过分析标志值来对存储器 10 寻址。

可用硬件实现接口 52、54 和相关的逻辑单元 50。

另外，特定的硬件电路 56、58 将分别作为接口出现在存储器 6、8、10 和逻辑单元 50 之间和中央处理单元 2 和逻辑单元 50 之间。逻辑单元 50 可提供与标志比较逻辑电路相结合的专用地址计数器。另一种硬件电路可包括按内容编址的存储器逻辑电路，按存储器页面实现，至少对于保留的存储比特而言，以包含标志值。

当除特定检测编码外还使用加密技术来编码标志值时，利用根据本发明管理的存储器可获得附加的安全优点。这种加密标志编码往往会隐藏与包含于标志值中的结构信息（象组块标识符 chid、代计数值 gen#和页面计数 pg#）相关的应用数据。可用本领域的技术人员已知的任何编码技术来进行加密编码。一个有利的方法包括利用保密加密单向功能，其中，单向功能步骤涉及仅为存储器管理器 4 所知的保密密钥。通过该方法，存储器管理器 4 通过对前代的编码标志值应用一次或多次单向功能、并接着将所得到的标志值与最近更新代的标志值相比较，可识别前代。这将防止应用程序数据由存储器件内容的恶意强迫“转储”的重构。

如上所述，标志的存储器结构提供多个有利的选项。例如，标

志可包括表示相关应用程序数据的所有权的附加数据。另外，标志值中的这种附加数据可表示对于应用程序数据之不同用户的使用权或使用权组。例如，这种不同的使用权可与对存储器 10 中（应用）程序数据之不同部分的不同访问条件有关。例如，（应用）程序数据的一部分可被定义为只读，而应用程序数据的另一部分被定义为读/写访问。

由于存储器包括以连续代的形式对特定应用数据元的更新经历，本发明有效地提供了存储于存储器中的事项记录（transaction log）。

另外，如上所述，利用所公开的存储器更新/事项记录机构，可减少对根据本发明所管理的存储器件的写操作之数。此外，由本发明提供的写操作的减少数还通过延长硅存储器件的使用寿命而导致该器件的成本降低。特别是提高了存储在防干预单片计算机（象智能卡）上的非易失性存储器中的数据的安全性。采用硬件手段可进一步提高这一安全性，象采用与中央处理单元 2 分离的存储器管理器 4，但不是绝对必要的。

图1

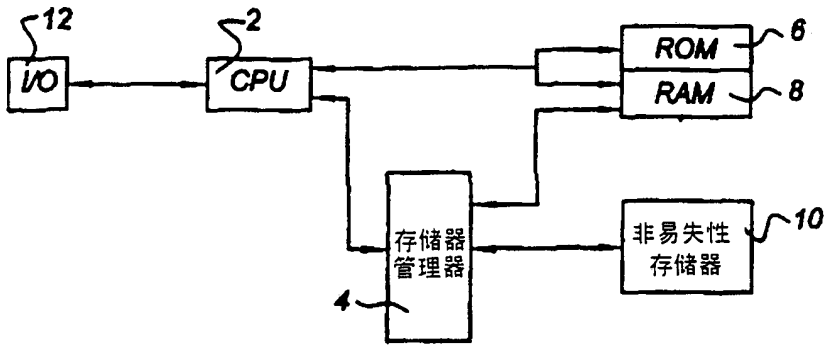

12
I/O
2
CPU
ROM
6
RAM
8
存储器
管理器
4
非易失性
存储器
10

图2

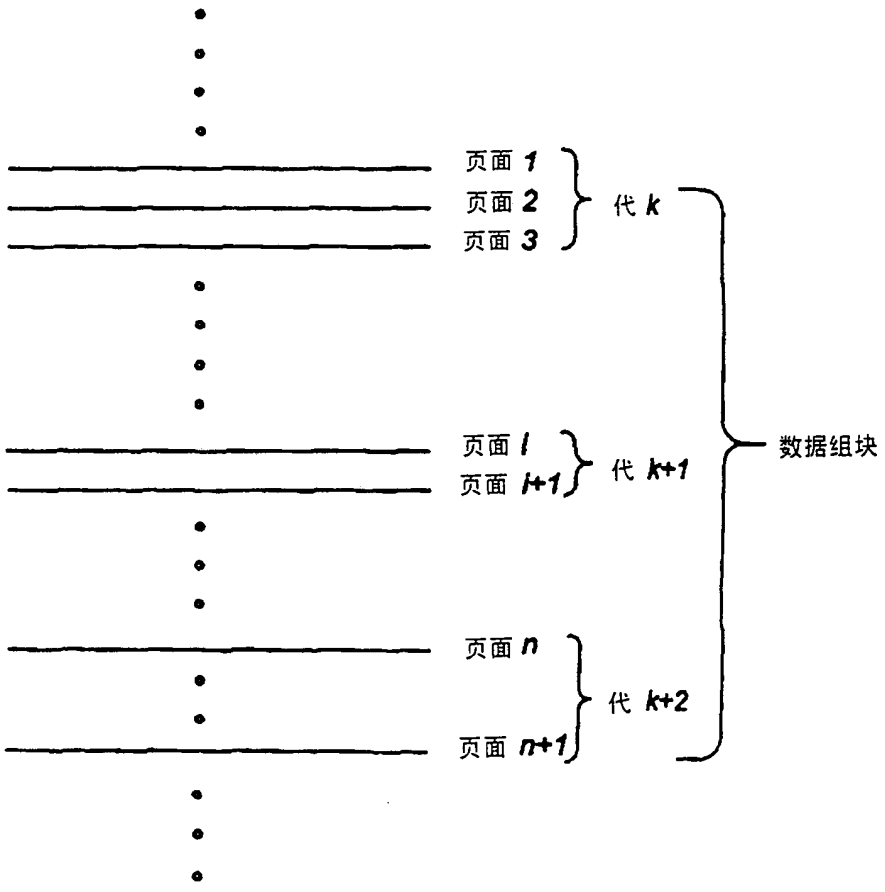

页面 1
页面 2
页面 3
代 k
页面 l
页面 l+1
代 k+1
页面 n
页面 n+1
代 k+2
数据组块

图3

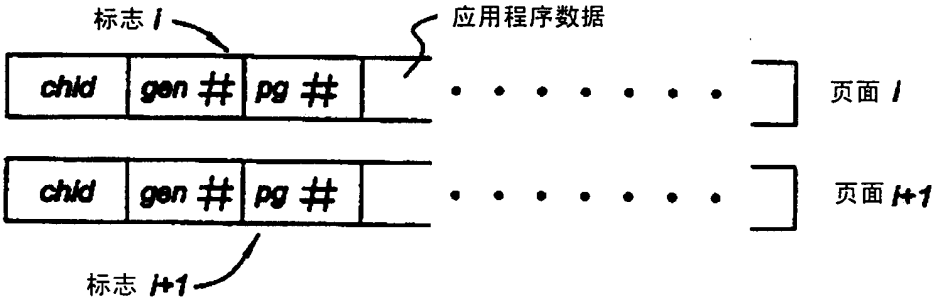

标志 I
应用程序数据
child
gen #
pg #
页面 I
child
gen #
pg #
页面 I+1
标志 I+1

图4

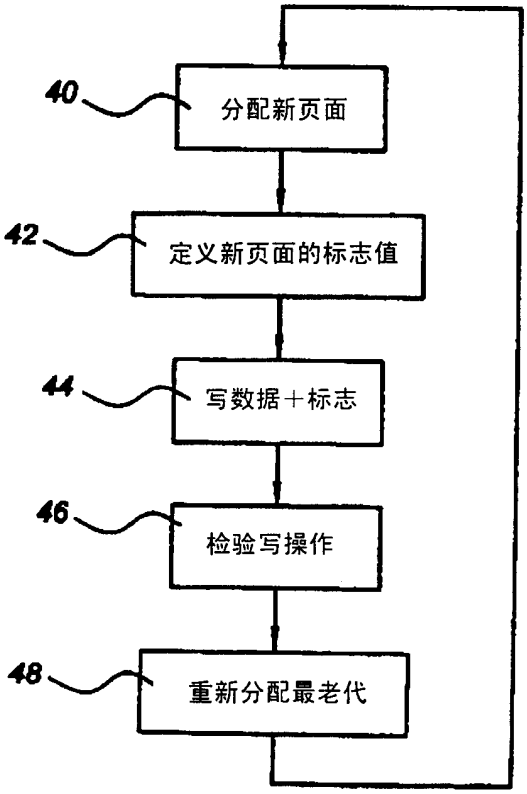
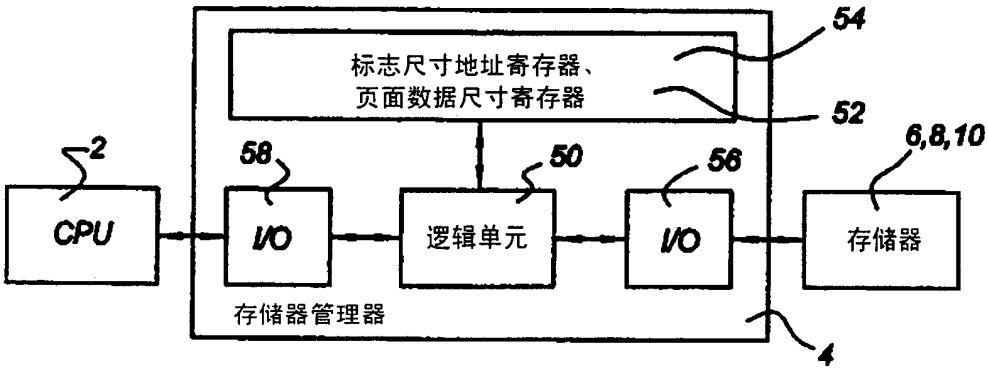

40
分配新页面
42
定义新页面的标志值
44
写数据＋标志
46
检验写操作
48
重新分配最老代

图5


标志尺寸地址寄存器、
页面数据尺寸寄存器
54
52
6,8,10
2
58
50
56
CPU
I/O
逻辑单元
I/O
存储器
存储器管理器
4