

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

G06F 7/00

G06F 11/34

G06F 12/12



[12] 发明专利申请公开说明书

[21] 申请号 200380101643.5

[43] 公开日 2005 年 12 月 7 日

[11] 公开号 CN 1705931A

[22] 申请日 2003.10.14

[21] 申请号 200380101643.5

[30] 优先权

[32] 2002.10.16 [33] FR [31] 0213333

[86] 国际申请 PCT/EP2003/050718 2003.10.14

[87] 国际公布 WO2004/036411 法 2004.4.29

[85] 进入国家阶段日期 2005.4.18

[71] 申请人 汤姆森许可贸易公司

地址 法国布洛里

[72] 发明人 埃里克·迪尔

[74] 专利代理机构 中科专利商标代理有限责任公司

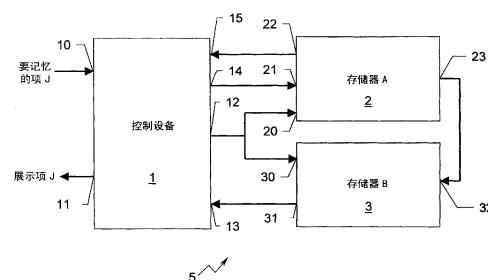
代理人 戎志敏

权利要求书 2 页 说明书 6 页 附图 1 页

[54] 发明名称 存储元素列表的设备和在一个这样的设备中存储元素的方法

[57] 摘要

本发明涉及一种记忆项目列表的设备(5)，用于记忆最后展示给其的任意项(J)。其包括第一存储器(3)、以及当第一存储器已满时且当必须对新项进行记忆时，负责随机地选择记忆在第一存储器中的项以删除该所选项，并记忆所展示的新项的装置。本发明还涉及一种在这样的设备(5)中记忆项(J)的方法。



ISSN 1008-4274

1、一种记忆项目列表的设备(5)，用于记忆最后展示给其的任意项(J)且包括第一存储器(3)，其特征在于：其额外包括当第一存储器已满时且当必须对新项进行记忆时，负责随机地选择记忆在第一存储器中的项以删除该所选项，并记忆所展示的新项的装置。

2、根据权利要求1所述的设备，能够记忆N项，其中N是自然数，其特征在于所述设备还包括第二存储器(2)，设计用于连续地记忆最后展示给所述设备的M项，M是小于N的自然数，所述第一存储器(3)用于记忆N-M个其他项。

3、根据权利要求1或2所述的设备，其特征在于所述设备还适合于提供表示最后展示给其的项(J)是否已经存在于所述设备中的信息。

4、根据权利要求1到3任一项所述的设备，其特征在于所述设备仅包含所记忆的每一项的一个副本。

5、根据前述权利要求任一项所述的设备，其特征在于对于每一项，所述设备还记忆将该项已经展示给其的次数。

6、根据权利要求5所述的设备，其特征在于所述设备适合于提供表示最后展示给其的项是否已经展示给其超过预定数量的次数的信息。

7、一种在根据权利要求2到4任一项所述的设备(5)中记忆项(J)的方法，其特征在于所述方法包括以下步骤：

(a) 接收展示给设备(5)的项(J)；

(b) 验证所述项(J)是否已经存在于所述设备(5)中；以及
-如果所述验证为肯定的，则将所述项(J)指定为最后记忆的项；以及

-如果所述验证为否定的，则将所述项(J)记忆在所述设备中。

8、根据权利要求7所述的设备，其特征在于在步骤(b)中的否定验证的情况下：

- 如果第二存储器(2)未满,则将接收到的项(J)记忆在第二存储器(2)中;以及
- 如果第二存储器(2)已满:
 - i) 将所述第二存储器中所记忆的最早项传送给第一存储器(3);
 - 5 ii) 将接收到的项(J)记忆在所述第二存储器(2)中;以及
 - iii) 如果第一存储器(3)已满,则随机地选择记忆在所述第一存储器中的项以进行删除,从而能够将记忆在所述第二存储器中的最早项传送给所述第一存储器(3)。

存储元素列表的设备和在一个这样的设备中存储元素的方法

5

技术领域

本发明通常涉及需要记忆安全日志的系统中的安全领域。特别地,涉及一种记忆项目列表的设备和在这样的设备中记忆项目的方法。

10 背景技术

为了防止非法尝试访问数据或对数据的欺骗性操作,通常,认为是“安全的”的系统保存事件日志或执行的操作列表。

典型示例涉及一种记录设备,仅授权制作其可以记录的任何内容的一个副本(或有限数量的副本)。这需要数字记录设备在授权针对个人使用的复制的同时,防止非法副本的扩散。对此进行确保的直接方案在于:在记录设备中保持已经由其记录的所有内容的列表(或者,更具体地,所有内容的标识符列表)。每一次当记录设备接收到记录指定内容的命令时,其实现检查该内容是否存在于已经记录的内容列表中。如果该内容(或更具体地,其标识符)包含在该列表中,则记录设备拒绝记录其。

20

在上述示例中所产生的问题在于:记录的内容的潜在数量是无限的。因此,为了使系统的安全得以确保,已经记录的内容列表还必须没有限制,这对于消费电子设备而言是不可能的。在该类型的设备中,通常,使用FIFO(“先入先出”的首字母缩写词)来记忆上述列表。

25

然而,如果该列表的目的是在系统中提供一定的安全性,如同保持列表以防止对内容的非法复制的上述示例,或者针对撤销列表,其包含不再由可信组织看作适合或合法的密码密钥或设备的标识符,则在FIFO存储器中记忆这样的列表的解决方案并不令人满意。事实上,如果存储器的尺寸使其能够记忆 n 项,则所有偷盗者必须做的是向记忆该列表的设备展示 $n+1$ 项,以确保从列表中删除了所记忆的第一项,这

30

明显是对系统安全的折中。

发明内容

本发明的目的是解决上述问题。

5 本发明的主题是一种记忆项目列表的设备，用于记忆最后展示给所述设备的任意项。该设备包括第一存储器，并且根据本发明，还包括：当第一存储器已满时且当必须对新项进行记忆时，负责随机地选择记忆在第一存储器中的项以删除该所选项，并记忆所展示的新项的装置。

10 根据本发明的特定特征，所述设备能够记忆N项，其中N是自然数，并且所述设备还包括第二存储器，设计用于连续地记忆最后展示给所述设备的M项，M是小于N的自然数，所述第一存储器用于记忆N-M个其他项。

15 利用根据本发明的设备，即使将要记忆的多于N个的项展示给其，也不会在最终才知道哪些项无法再在该设备中找到。

 根据另一特征，所述设备还适合于提供表示展示给所述设备的项是否已经存在于所述设备中的信息。

 根据另一特征，所述设备仅包含所记忆的每一项的一个副本。

20 根据本发明的一个特定方面，对于每一项，所述设备还记忆将该项已经展示给其的次数。

 根据本发明的另一方面，所述设备适合于提供表示最后展示给其的项是否已经展示给其超过预定数量的次数的信息。

25 本发明还涉及一种在如上所述的设备中记忆项目的方法。所述方法包括以下步骤：(a) 接收展示给设备的项；(b) 验证所述项是否已经存在于所述设备中；以及

 -如果所述验证为肯定的，则将所述项指定为最后记忆的项；
 以及

 -如果所述验证为否定的，则将所述项记忆在所述设备中。

 根据一个特定实施例，在步骤(b)中的否定验证的情况下：

30 -如果第二存储器未滿，则将接收到的项记忆在第二存储器中；

以及

-如果第二存储器已满:

i) 将所述第二存储器中所记忆的最早项传送给第一存储器; 以

及

5 ii) 将接收到的项记忆在所述第二存储器中; 以及

iii) 如果第一存储器已满, 则随机地选择记忆在所述第一存储器中的项以进行删除, 从而能够将记忆在所述第二存储器中的最早项传送给所述第一存储器。

10 附图说明

通过结合单幅附图所阐明的本发明的非限定性具体实施例的描述, 本发明的其他特征和优点将显而易见, 所述单幅附图示意地示出了根据本发明的记忆设备。

15 具体实施方式

本发明的记忆设备设计为包含最大N项, 例如要记录的内容的标识符。典型地将单幅附图中的参考符号为5的该设备集成到数字记录设备中。

20 该设备5包括两个存储器A和B。参考符号为2的存储器A包含最大M项, 而参考符号为3的存储器B包含最大P项, 从而 $N=M+P$, 其中N、M和P是自然数。

存储器A总是包含在设备中记忆的最后M项。对于存储器B, 其包含在最后M项之前所记忆的项。

25 当将新项J展示给该设备时, 例如当记录设备接收到记录新内容的命令时, 将内容标识符(对应于项J)展示给记忆设备5以验证其是否已经包含在设备5中所记忆的列表中。

30 如果项J已经存在于存储器A中, 则在存储器A中将其标记为所记忆的最后项。如果项J已经存在于存储器B中, 则将其移到存储器A中、所记忆的最后项的位置上。在两个情况下, 因此, 设备5返回项J存在的

如果项J未存在于存储器A或存储器B中，则将J记忆在存储器A中。如果存储器A已经包含M项，则将存储器A中所记忆的最早项传送到存储器B以将其记录在其中。同时从存储器A中删除其以创建针对项J的空间。如果存储器B也已满，即如果其已经包含P项，则随机地选择在存储器B中已记忆的项，删除其并由存储器A中的最早项来替代。然后，设备5根据项J并不存在但是现在被记忆到其中的情况来返回信息。

更具体地，通过参考该单幅图，记忆设备5包括控制设备1和参考符号分别为2和3的两个存储器A和B。

控制设备1具有三个输入10、13和15、以及三个输出11、12和14。
10 输入10接收项J以记忆其，然后将其发送到控制设备的输出12。

输出11是布尔型信号，表示项J是否已经记忆在记忆设备5中。如果已经记忆了项J，则在输出11处的信号是“1”（表示“真”），否则，该信号为“0”（表示“假”）。输入13和15和输出14也是布尔型信号，下面将对其进行描述。

15 存储器A具有两个输入20和21、以及两个输出22和23。输入20接收控制设备的输出12，向其发送要记忆的项J，或者必须确定其存在于存储器A中。与控制设备1的输出14相连的输入21是布尔型信号，表示当其值为“1”（“真”）时，必须将输入20处接收到的项J记忆在存储器A中。

20 存储器A的输出22也是布尔型信号，表示当其值是“1”（“真”）时，在输入20处出现的项J已经存在于存储器A中。该输出22与控制设备1的输入15相关联。

仅当存储器A已满时，且当必须对输入20处出现的新项进行记忆时，使用存储器A的输出23。在这种情况下，该输出23提供存储器A中所记忆的最早项。否则，输出23不提供任何信号。

25 对于存储器B，其具有两个输入30和32和一个输出31。输入30与控制设备1的输出12相关联，且接收必须对其存在于存储器B中进行验证的项J。输出31是布尔型信号，当在输入30处接收到的项J存在于存储器B时，值为1（“真”）；其与控制设备1的输入13相关联。

30 对于存储器B的输入32，当该存储器已满时，其接收来自存储器A

的要记忆的项。出于此目的，输入32与存储器A的输出23相关联。

按照以下方式来操作组件。当控制设备1在其输入10处接收到项J时，其在其输出12处提供该项J。如果该项J存在于存储器A中，则在控制设备1的输入15处接收信号“1”（表示“真”）。如果项J存在于存储器B中，则在控制设备的输入13处接收信号“1”（表示“真”）。

如果在控制设备的输入13和15处接收到的两个布尔型信号具有值“0”（即“假”），表示在输入10处接收到的项J并未存在于存储器A或存储器B中。在这种情况下，控制设备1在其输出11处提供“0”信号（“假”），在其输出14处提供“1”信号，表示必须将项J记录在存储器A中。

如果在输入15处接收到的布尔型信号具有值“1”（“真”），表示项J已经存在于存储器A中，则控制设备1在其输出11处提供“1”信号而在其输出14处提供“0”信号。

如果在输入13处接收到的布尔型信号具有值“1”（“真”），表示项J已经存在于存储器B中，则控制设备1在其输出11处提供“1”信号而在其输出14处提供“1”信号。

当存储器A在其输入20处接收到项J时，其首先验证其是否已经具有该项。如果该项J已经存在于存储器A中，则在输出22处的信号取值“1”（“真”）。然后，将该项J指定为由存储器A最后记忆的项。例如，如果存储器A具有堆栈结构，则将项J放置在堆栈的顶部，否则，对存储器中所存储的项的索引表保持更新。

否则（J并不存在于存储器A中），输出22取值“0”（“假”）。

当在存储器A的输入21处接收到的信号为值“1”（“真”），表示必须在存储器A中记忆输入20处出现的项J，则存在两种可能。或者存储器A包含少于M项，并记忆变为最后记忆的项的新项J。或者，存储器A已经包含M项，在后一种情况下，其将最早的项放在其输出23上，并从其存储器中删除其以将新项J记忆为最近项。

存储器B具有不同于存储器A的行为。当在存储器B的输入30处接收到项J时，该存储器检查其是否已经包含该项J。如果情况如此，则输出31取值“1”，否则（J并不存在于存储器B中），输出31取值“0”。

如果在存储器B的输入32处接收到来自存储器A的项J，则存在两种可能：或者信号31为“真”（值“1”），或者信号31为“假”（值“0”）。

如果信号31为“真”，则存储器B的输入32处接收到的新项替代其数值出现在输入30处的项（其被移到存储器A中）。

- 5 如果信号31为“假”，仍然存在两种可能：或者存储器B包含少于P项，并记忆新项J；或者存储器B已经包含P项，即其已满。在后一种情况下，其随机地选择在存储器B中已存在的项，并删除其以记忆在其输入32处接收到的新项来替代随机选择的项。

- 10 因此，存储器B以随机的方式清空。因此，想要消除记忆设备5中的项的偷盗者必须比在简单FIFO存储类型的情况进行多得多的尝试。事实上，如果存储器的总尺寸为N项，则偷盗者平均必须实现比N多得多的尝试来从存储器中消除项目。

应该注意，在单幅图中分离表示的存储器A和B在实际中可以是相同物理存储器的两个子组件。

- 15 本发明并不局限于以上已经描述的实施例。作为变体，实际上，记忆设备5可以包括空尺寸的存储器A。在另一变体中，用户能够以给定次数向记忆设备展示每一项。例如，如果将该设备集成到记录设备中，并且授权该记录设备对每一个内容制作数量为x的副本，则对于已经由设备记录的每一个内容标识符，该存储器将存储把该内容展示给
20 该设备进行记录的y次。当给定内容展示数量y达到数量x时，则不能再记录该内容，并且记忆设备5将向记录设备返回相应的信息项。

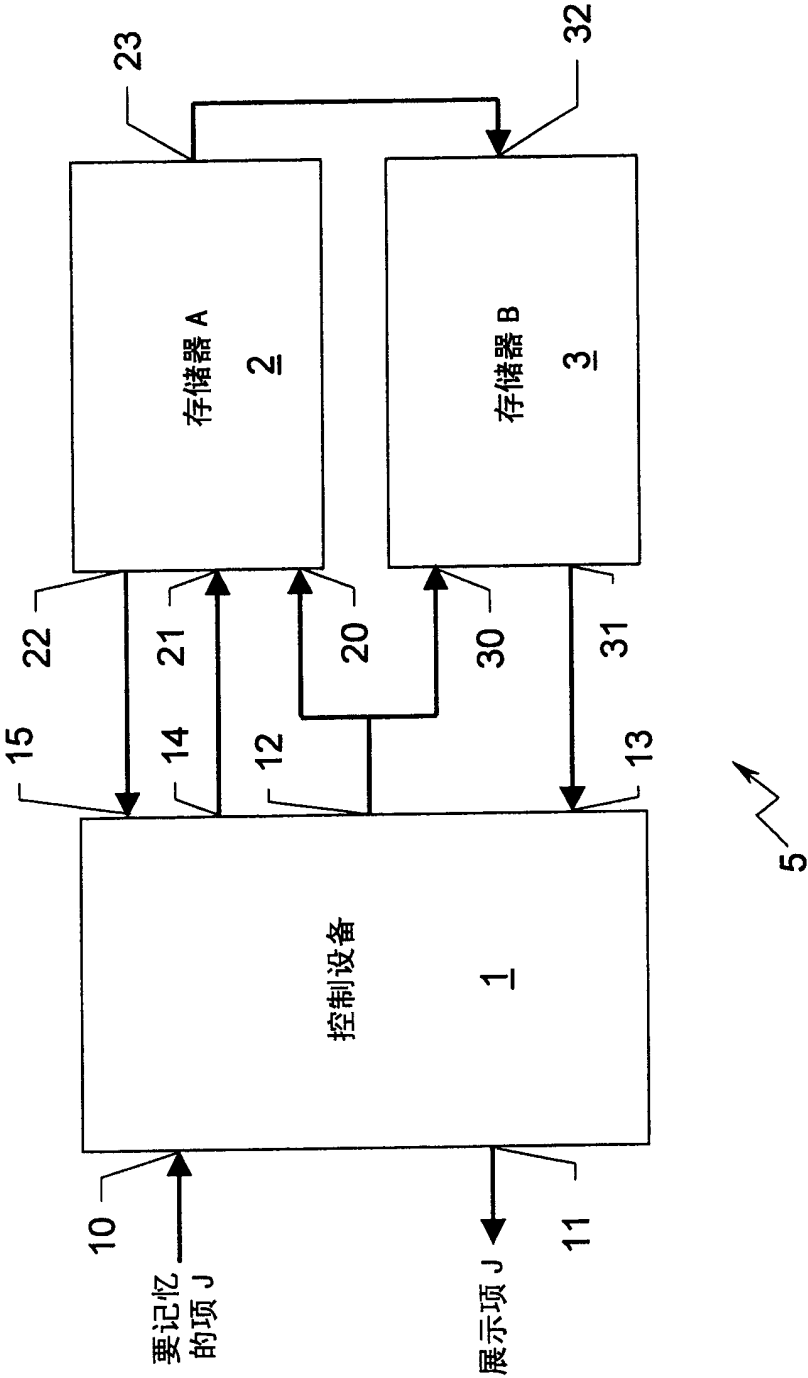


图 1