(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1655133 B
(45)授权公告日 2010.09.15

(21)申请号 200510008273.1

(22)申请日 2005.02.07

(30)优先权数据
04100546.3 2004.02.12 EP

(73)专利权人 耶德托存取公司
地址 荷兰霍夫多普

(72)发明人 杰拉德·J.·德克尔
艾尔伯特-简·波斯恰
安托尼尔斯·J.·P·.M·. 范德文

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李德山

(51)Int.Cl.
G06F 13/00(2006.01)
G06F 12/00(2006.01)

(56)对比文件
CN 1197234 A,1998.10.28, 全文.
US 5757919 A,1998.05.26, 全文.
US 5251304 A,1993.10.05, 全文.
EP 0330404 A2,1989.08.30, 说明书第3栏第43行至第14栏第35行,附图3-24A.
CN 1195827 A,1998.10.14, 全文.
CN 1282933 A,2001.02.07, 全文.

审查员 徐飞兵

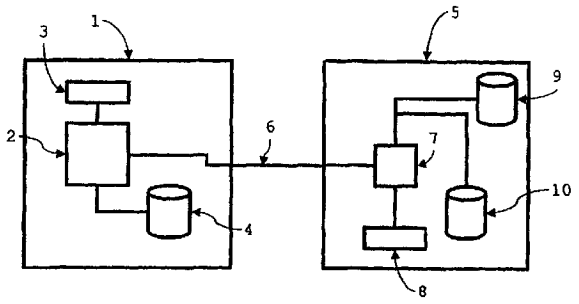
权利要求书 2 页 说明书 17 页 附图 4 页

(54)发明名称

用于外部数据存储的方法与系统

(57)摘要

一种用于系统中的外部数据存储的方法,该系统包括:初级处理装置(1;72),其具有一个处理器(2;74)和一个初级数据存储单元(4;77),适于在处理器(2;74)中运行应用程序,以便处理有效记录,并且被配置用于将属于有效记录的数据存储在初级数据存储单元(4;77)之中;以及次级数据存储系统(5;57;69),其可以访问初级处理装置(1;72),该方法包括步骤:将属于一个有效记录的数据装载到初级数据存储单元(4;77)之中,以及通过将属于该记录的至少一个数据片(34)传送到次级数据存储系统(5;57;69)以供存储,来使该记录外在化。外在化记录的步骤包括由使用属于该记录的数据的一个应用程序,向一个被安排向次级数据存储系统(5;57;69)传送数据片(34)的接口(6-8;60,61,62,66,70,78)来发起一次调用。



CN 1655133 B

1. 一种用于系统中的外部数据存储的方法，该系统包括：

初级处理装置 (1 ;72)，其具有一个处理器 (2 ;74) 和一个初级数据存储单元 (4 ;77)，适于运行应用程序以在处理器 (2 ;74) 中处理有效记录，并且配置用于将属于有效记录的数据存储在初级数据存储单元 (4 ;77) 之中 ;以及

次级数据存储系统 (5 ;57 ;69)，其可以访问初级处理装置 (1 ;72)，该方法包括步骤：

将属于一个有效记录的数据装载到初级数据存储单元 (4 ;77) 之中 ;以及

通过将属于该记录的至少一个数据片 (34) 传送到次级数据存储系统 (5 ;57 ;69) 以供存储，来使该记录外在化，

其中，所述使该记录外在化的步骤包括，通过使用属于该记录的数据的一个应用程序，向一个被安排向次级数据存储系统 (5 ;57 ;69) 传送数据片 (34) 的接口 (6-8 ;60,61,62,66,70,78) 发起一次调用，

其特征在于，所述方法还包括传送一个数据段 (48 ;52 ;56)，该数据段包括属于一个记录的仅有一个数据片 (34) 的至少一个相关部分 (35-37) 所对应的数据 (41-43)，以及

为该数据片 (34) 的每一部分 (35-37) 计算一个认证值 (45 ;49 ;54)，以及，将反映该认证值 (45 ;49 ;54) 的数据纳入到包含有对应于该部分 (35-37) 的数据 (41-43) 的数据段 (48 ;52 ;56) 中。

2. 根据权利要求 1 所述的方法，其中，该数据片 (34) 被划分为多个部分 (35-37)，并且其中，多个数据段 (48 ;52 ;56) 被传送到次级数据存储系统 (5 ;57 ;69)，以供存储，上述数据段中的每一个都包括对应于所述多个部分 (35-37) 中的一个相关部分的数据 (41-43)。

3. 根据权利要求 1 所述的方法，其中，通过对该数据片 (34) 的一个相关部分 (35-37) 至少部分地加密，来产生对应于该相关部分 (35-37) 的数据 (41-43)。

4. 根据权利要求 1 所述的方法，包括使用从另一部分 (35,36) 导出的信息作为输入，为所述数据片 (34) 的至少一部分 (36-37) 计算认证值。

5. 根据权利要求 1 所述的方法，包括：在初级处理装置 (1) 的初级数据存储单元 (4) 中，为每一个外在化记录存储一个参考数据对象 (11)，每一个外在化记录包含一个唯一的标识符，其中，反映该唯一的标识符的数据被纳入到每一个数据段 (48 ;52 ;56) 之中，上述数据段包括与属于该记录的数据片 (34) 的一个部分 (35-37) 相对应的数据 (41-43)。

6. 根据权利要求 1 所述的方法，包括：为所述外在化记录存储反映版本计数的信息，并且在对该记录外在化之前，令版本计数加 1。

7. 一种用于在系统中对记录内在化的方法，该系统包括：

初级处理装置 (1 ;72)，其具有一个处理器 (2 ;74) 和一个初级数据存储单元 (4 ;77)，适于在处理器 (2 ;74) 中处理有效记录，并且被配置用于将属于有效记录的数据存储在初级数据存储单元 (4 ;77) 之中 ;以及

次级数据存储系统 (5 ;57 ;69)，其可以访问初级处理装置 (1 ;72)，并且被安排存储借助于根据权利要求 1-6 中任何一项所述方法传送的数据片 (34)，该方法包括步骤：

将属于该记录的数据装载到初级数据存储单元 (4 ;77) 之中 ;其中

该系统包括一个接口 (6-8 ;60,61,62,66,70,78)，用于从次级数据存储系统 (5 ;57 ;69) 中检索属于该记录的数据片 (34)，该方法还包括如下步骤：

通过一个应用程序使用属于该记录的数据，确定该记录将被内在化并且至少调用该接

口 (6-8 ;60,61,62,66,70,78) 一次,

其特征在于,所述方法还包括 :从次级存储系统 (5,57 ;69) 接收至少一个数据段 (48,52,56),该数据段包括与一个数据片 (34) 的至少一个相关部分 (35-37) 对应的数据 (41-43),以及

接收至少一个含有认证值 (45,49 ;54) 的数据段 (48,52,56),检索被存储在初级处理装置 (1) 中的一个加密的信息片 (46),使用所述加密的信息片 (46),根据对应于所述数据片 (34) 的至少一个相关部分 (35-37) 的至少一部分数据 (41-43),为每一个数据段 (48,52,56) 计算一个核对认证值,以及,将该核对认证值跟针对每一个数据段 (48,52,56) 的认证值 (45,49 ;54) 进行比较。

8. 根据权利要求 7 所述的方法,包括 :从存储在初级处理装置 (1) 的初级数据存储单元 (4) 中的一个参考对象 (11) 中,检索该记录的一个唯一的标识符,其中,该数据段 (48,52,56) 被存储在次级数据存储系统 (5,57 ;69) 之中,具有反映该唯一的标识符的信息,并且,响应于含有反映该唯一的标识符的信息的内在化消息而被接收。

9. 根据权利要求 7 所述的方法,其中,该数据片 (34) 包括多个部分 (35-37),该方法包括接收多个数据段 (48,52,56),每一个数据段包括对应于所述多个部分 (35-37) 中的一个相关部分的数据 (41-43)。

10. 根据权利要求 8 所述的方法,包括 :从参考对象 (11) 中检索反映各部分 (35-37) 的数目的信息,以及响应于相应数目的内在化消息的其中之一,接收每一个数据段 (48,52,56)。

11. 根据权利要求 7 所述的方法,包括 :接收一个数据段 (48,52,56) 的序列,每一个数据段都包括一个认证值 (45,49,54),其中,利用从一个数据段 (48,52,56) 导出的信息 (45,49) 作为输入,为至少另一个数据段 (48,52,56) 计算核对认证值。

12. 根据权利要求 7 所述的方法,包括 :检索被存储在初级处理装置 (1) 之中的一个加密密钥 (40),并对一个接收的数据段 (48,52,56) 的至少一部分 (41-43) 进行解密。

13. 根据权利要求 7 所述的方法,包括 :接收一个数据段 (48,52,56),该数据段包括反映用于外在化记录的版本计数的信息,并将该版本计数跟一个参考版本计数进行比较。

用于外部数据存储的方法与系统

技术领域

[0001] 本发明一般地涉及从外部存储由一个处理装置处理的数据的方法。特别是，本发明涉及外部存储数据的各种方法，内在化 (internalization) 数据的各种方法，以及实现外部数据存储和数据内在化的方法。本发明还涉及将这样的方法应用于多媒体系统，以及用于执行这样的方法的系统和计算机程序。

背景技术

[0002] 实现外部数据存储的方法的实例以及适于执行这样一种方法的外部数据存储的方法和系统的实例可以从，例如，US5757919 中获知。此份公报公开了一种用于保持从一个物理安全环境按页发送到一个外部存储单元的页面的完整性和保密性的方法与系统。这种物理安全环境包括一个安全的处理器，该处理器通过总线被连接到一个随机存取存储器。一个完整性检查引擎在安全环境和不安全环境（特别是一个外部存储单元）之间执行数据翻页的单向散列 (hash)。在一个实施例中，安全处理器被构成为使用一个 1K 的页面。在不安全环境中的一个主处理器将存储在外部存储器中的安全处理器的页面视为 1K 数据块。若一个页面被确定为需要，则就该页面是否存在于安全存储器之中作出判断。若该页面存在，则出现页面命中，并且不需要采取进一步的动作。若该页面不存在，则出现页面故障。当出现页面故障时，就要对在安全存储器中是否还有需要的页面能被映射到的可用空间作出判断。若没有可用空间，则选择一个页面将它翻出。可以使用不同的选择标准，诸如把最近用得最少的翻出。

[0003] 已知的方法和系统存在这样的缺点，即，难以选择有待于传送到次级数据存储系统的数据片。由于页面的翻入和翻出通常涉及等待时间 (latency)，并且在出现页面故障时，安全服务会使等待时间延长，这就使有效 (active) 记录的处理变慢。

[0004] 在法国专利 FR-A-2803471 中，公开了一种外部数据存储方法、内在化数据方法、处理多媒体系统中的记录的方法、以及适于执行这些方法的系统的另一个实例。此份公报公开了在电视接收机中的存储器管理方法。该电视系统包括电视机，植入电视机中的本地存储装置，以及跟电视机相关联的外部存储装置，诸如存储卡或盘驱动器。该系统包括一段计算机程序，其中包括多个可执行模块。第一模块接收并分析每一项存储信息的请求。若存储装置的特性不允许存储新信息，则第一模块触发第二模块。第二模块在遵守已存储信息的使用标准的同时，释放存储器空间。第一和第二模块使用一系列的简单的程序来优化信息的存储。这些步骤实现，例如，将数据从第一存储装置移动到第二存储装置。

[0005] 这种已知系统和方法的一个问题就是，一旦记录已经被外在化 (externalised)，它们就不允许对记录的一部分或全部进行处理。若发生此种情况，并且该数据片 (piece of data) 将在一个稍后阶段返送到该电视机，则属于该记录的数据的全集将不同于在外在化 (externalisation) 之前由该项应用对电视机最后处理的数据的全集。

发明内容

[0006] 本发明提供一种实现外部数据存储的方法，一种外部数据存储的方法，一种内在化记录的方法，一种实现记录的内在化的方法，一种在向 / 从次级存储系统传送数据的数目方面更加有效的初级处理装置和计算机程序装置。

[0007] 这是通过提供一种用于在系统中实现外部数据存储的方法实现的，该系统包括 ：

[0008] 初级处理装置，其具有一个处理器以及一个初级数据存储单元，适于在处理器中处理有效记录，并且被配置用于将属于有效记录的数据存储在初级数据存储单元之中 ；以及

[0009] 次级数据存储系统，可以访问初级处理装置，该方法包括 ：

[0010] 属于一个有效记录的数据被存储在初级数据存储单元之中，以及

[0011] 通过将属于该有效记录的至少一个数据片传送到次级数据存储系统以供存储，来使该记录外在化，其中

[0012] 外在化记录的步骤包括接收由使用属于该记录的数据的应用程序，通过一个被安排向次级数据存储系统发送数据片的应用程序接口，来启动的至少一次调用。

[0013] 这样一来，由于所传送的数据片属于一个记录，所以该方法较好地考虑到这样一个事实，即，相比那种基于该处理器运行的过程可用的存储器地址的方案，初级处理装置的处理器将更加需要去访问属于该记录的数据。由于外在化是由实际上使用属于该记录的数据的应用程序来启动的，所以，要预测哪一个记录、从而哪一个数据片，在不久的将来在初级处理装置中可能被需要，是比较容易的。

[0014] 本发明具有附加的优点，即，在使虚拟存储器地址与物理地址相联系时，不一定需要页面表 (page table)。

[0015] 一个优选的实施例包括接收至少一个外在化消息，该消息包括标识一个数据段的信息，该数据段又包括对应于仅有的一个数据片的至少一个相关部分的数据，并且，响应于该外在化消息传送至少所述标识的数据段。

[0016] 这样一来，被传送到次级存储系统以供存储的每一个数据段都包括对应于仅有的一个数据片的一个相关部分的数据。在有一个以上的记录将被外在化的情况下，这排除了存储具有跟属于一个记录的数据相对应的子段以及跟属于一个未来的记录的数据相对应的子段的数据段。换句话说，属于一个记录的数据所对应的数据通常被存储在，与属于另一个记录的数据所对应的数据相分离的一个独立数据段之中。本实施例具有消除向，特别是从，次级存储系统进行不必要的数据传送的优点。

[0017] 一个优选的实施例包括，将数据片划分为多个部分，接收多条外在化消息，其中每一条外在化消息都标识一个数据段，该数据段包括对应于所述多个部分中的一个相关部分的数据，并且响应于每一条外在化消息传送至少所述标识的数据段。

[0018] 本实施例具有这样的优点 :它适应于初级存储装置可用的主存储器的大小和 / 或通往次级存储系统的接口的特性，诸如数据管线 (pipeline) 的宽度。

[0019] 在一个优选的实施例中，通过至少部分地对该数据片的相关部分进行加密，来产生对应于一个相关部分的数据。

[0020] 由于被传送到次级存储系统以供存储的各数据段至少部分地被加密，所以，只有初级数据存储单元以及初级数据处理装置的处理器需要装入一个安全环境中，以便保持数据的绝对的整体安全性。由于初级处理装置仅需要有一个具有有限存储容量的初级存储单

元，由于有了从外部存储数据的可能性，所以提供这样一个安全环境是较为廉价和容易的。

[0021] 一个优选的实施例包括：将数据片划分为连续各部分的一个序列，接收一系列的外在化消息，其中每一条外在化消息都包括标识该记录的信息，以及借助于该对应部分在该序列中的位置来标识一个数据段的信息，以及，在传送到次级存储系统之前，在该数据段中纳入对应于标识一个数据段的信息的数据。

[0022] 这个实施例具有这样的优点：描述各数据段被再次读出的顺序的信息被存储在次级存储系统之中。因此，在一个具有十分有限的容量的初级处理装置中，特别是具有有限易失性的主存储器中，将被装回到初级存储单元的数据片的各部分可以进行串行处理，而不需要缓冲各组成部分，或者这些部分所关联的数据段。

[0023] 最好是，该方法包括，为该数据片的每一部分计算一个认证值，并且将反映认证值的数据包含在含有与该部分对应的数据的数据段中。

[0024] 因此，在一个稍后的阶段，有可能确定该数据段中的数据，特别是对应于与该数据段相关的数据片的一部分的数据，是否已经被篡改。

[0025] 根据本发明的另一方面，提供了一种用于系统中的外部数据存储的方法，该系统包括：

[0026] 初级处理装置，其具有一个处理器和一个初级数据存储单元，适于运行应用程序，以便在处理器中处理有效记录，并且被配置用于将属于有效记录的数据存储在初级数据存储单元之中；以及

[0027] 次级数据存储系统，其可以访问初级处理装置，该方法包括步骤：

[0028] 把属于一个有效记录的数据装载到初级数据存储单元之中；以及

[0029] 通过将属于该记录的至少一个数据片传送到次级数据存储系统以供存储，来使该记录外在化，其中，

[0030] 外在化记录的步骤包括由使用属于该记录的数据的应用程序，向一个被安排向次级数据存储系统传送数据片的接口发起一次调用。

[0031] 当应用本方法时，对属于记录的数据的外部存储的控制被转移到实际上使用该数据的应用程序。调用可以施加于一个应用程序接口，它适于执行根据本发明的实现外部数据存储的方法。可供替代地，也可以由运行于初级处理装置之中的应用程序直接地执行本方法。因此，它具有这样的优点：允许应用程序确定一个记录是否已被外在化。这样一来，应用程序就能避免把属于一个它在不久的将来要处理的记录的一个数据片传送到次级存储装置。由于跟外在化记录以及随后在要再次进行修改时，从次级存储系统中检索该数据片相关联的等待时间被避免，所以，应用程序的执行被加速。

[0032] 最好是，本方法包括传送一个数据段，该数据段包括跟属于一个记录的仅有一个数据片的至少一个相关部分对应的数据。

[0033] 这样一来，被传送到次级存储系统以供存储的每一个数据段都包括对应于仅有一个数据片的一个相关部分的数据。在有一个以上记录将被外在化的情况下，这排除了存储具有跟属于一个记录的数据对应的子段以及跟属于一个未来的记录的数据对应的子段的数据段。换句话说，属于一个记录的数据所对应的数据通常被存储在，与属于另一个记录的数据所对应的数据相分离的独立的数据段之中。本实施例具有消除向，特别是从，次级存储系统进行不必要的数据传送的优点。

[0034] 在一个优选的实施例中，该数据片被划分为多个部分，并且其中多个数据段（其中每一个都包括对应于多个部分中的一个相关部分的数据）被传送到次级数据存储系统以供存储。

[0035] 本实施例具有这样的优点：允许外在化适应于初级处理装置可用的主存储器的大小和/或通往次级存储系统的接口的特性，诸如数据管线的宽度。

[0036] 在一个优选的实施例中，通过至少部分地对该数据片的相关部分进行加密，来产生对应于一个相关部分的数据。

[0037] 由于被传送到次级存储系统以供存储的各数据段至少部分地被加密，所以，只有初级数据存储单元以及初级数据处理装置的处理器需要装入一个安全环境中，以便保持数据的绝对的整体安全性。由于初级处理装置仅需要有一个具有有限存储容量的初级存储单元，由于有从外部存储数据的可能性，所以提供这样一个安全环境是较为廉价和容易的。

[0038] 最好是，本方法包括，为数据片的每一部分计算一个认证值，并使反映该认证值的数据包括在含有与该部分相对应的数据的数据段中。

[0039] 这样一来，从外部存储数据的完整性得以证实。

[0040] 这个实施例的一个优选的变形形式包括：使用从另一部分导出的信息作为输入，为该数据片的至少一部分计算认证值。

[0041] 因此，在数据片被划分为各部分，并且从外部被存储在独立的数据段的场合，数据段的全集的完整性得以证实。

[0042] 最好是，本方法包括：在初级装置的数据存储单元中，为每一个已外在化的记录存储一个参考数据对象，包括一个唯一的标识符，其中，反映该唯一的标识符的数据被纳入到每一个数据段之中，上述数据段包括与属于该记录的数据片的一部分相对应的数据。

[0043] 这样一来，含有与外部存储的数据片相对应的数据的不同数据段的检索将变得更方便。

[0044] 最好是，本发明的方法包括：为已外在化的记录存储反映版本计数的信息，并且在对该记录外在化之前，令版本计数加 1。

[0045] 因此，就有可能对该记录已经被外在化的次数保持跟踪。同时也允许在属于被存储在初级存储单元中的记录的数据与外部存储的数据片之间实现同步。

[0046] 根据本发明的另一方面，提供了一种用于在系统中内在化记录的方法，该系统包括：

[0047] 初级处理装置，其具有一个处理器和一个初级数据存储单元，适于在处理器中处理有效记录，并且被配置用于将属于有效记录的数据存储在初级数据存储单元之中；以及

[0048] 次级数据存储系统，其可以访问初级处理装置，并且被安排存储借助于根据本发明的外部数据存储方法而传送的数据片，该方法包括步骤：

[0049] 将属于该记录的数据装载到初级数据存储单元之中，其中

[0050] 该系统包括一个接口，用于从次级数据存储系统检索属于该记录的数据片，该方法还包括：

[0051] 一段应用程序的各步骤，该应用程序被配置用于使用属于该记录的数据，确定该记录将被内在化，并且至少调用该接口一次。

[0052] 因此，被配置使用属于一个记录的数据的应用程序确定属于一个记录的数据片是

否从次级存储系统传送到初级处理装置。初级处理装置可以相同于在向次级存储系统传送数据片时所涉及的初级处理装置，或者它可以是一个不同的装置。因此，本方法具有这样的优点：即，它允许属于一个记录的数据共享。

[0053] 本发明的一个优选实施例包括：从次级存储系统接收至少一个数据段，该数据段包括对应于一个数据片的至少一个相关部分的数据。

[0054] 因此，该数据段包括与属于一个记录的一个数据片的一个相关部分相对应的数据。不需要将属于一个记录的数据跟属于另一个记录的数据分离开，也不需要与在应用程序已经确定需要的属于一个记录的数据一起，对属于另一个记录的数据进行不必要的传送。

[0055] 最好是，该方法包括：从被存储在初级处理装置的一个数据存储单元的一个参考对象中，检索该记录的唯一的标识符，其中，各数据段被存储在次级数据存储系统之中，具有反映该唯一的标识符的信息，并且，响应于含有反映该唯一的标识符的信息的内在化消息而被接收。

[0056] 因此，初级处理装置能知道该记录的存在，并且，即使在该数据没有被存储在初级数据存储单元之中时，它仍然具有一种访问属于它的数据的机制。

[0057] 在本发明的一个优选实施例中，该数据片包括多个部分，该方法包括接收多个数据段，每一个数据段都包括对应于所述多个部分中的一个相关部分的数据。

[0058] 这样一来，由于属于被内在化的记录的数据片的该部分可以在初级数据存储单元中进行处理并且顺序地装入，这样就可以在一个具有有限处理能力（例如有限的主存储器）的初级处理装置中执行本方法的这个实施例。本实施例也适于考虑通往次级数据存储系统的接口在能力方面的任何限制。

[0059] 一个优选实施例包括：接收含有一个认证值的至少一个数据段，检索被存储在初级处理装置之中的一个秘密的信息片，使用该秘密的信息片，从对应于该数据片的至少一个相关部分的数据的至少一部分中，为每一个数据段计算一个核对认证值，并将该核对认证值跟针对每一个数据段的认证值进行比较。

[0060] 这样一来，就能确定在接收的各数据段中所包含的数据是否可信。由于该核对认证值已经被计算，所以就不需要把它存储在初级处理装置（特别是在初级数据存储单元）之中。

[0061] 最好是，本方法包括：接收一个数据段，该数据段包括反映该外在化记录的版本计数的信息，并将该版本计数跟一个参考版本计数进行比较。

[0062] 这使得初级处理装置能验证所检索的数据是否为属于所期望的记录的一个版本的数据。若其他初级处理装置已经访问了外部存储的数据片，则尤其有用。

[0063] 根据本发明的另一方面，提供了一种在系统中实现记录的内在化的方法，包括：

[0064] 初级处理装置，其具有一个处理器和一个初级数据存储单元，适于在处理器中处理有效记录，并且被配置用于将属于一个有效记录的数据存储在初级数据存储单元之中；以及

[0065] 次级数据存储系统，其可以访问初级处理装置，并且被安排存储借助于如上面所定义的、根据本发明的外部数据存储方法而传送的数据片，该方法包括步骤：

[0066] 属于一个有效记录的数据被装载到初级数据存储单元之中，以及

[0067] 通过从次级数据存储系统中检索属于该记录的至少一个数据片，来使该记录内在化，其中，

[0068] 内在化记录的步骤包括接收由使用属于该记录的数据的应用程序，通过一个被安排从次级数据存储系统检索该数据片的应用程序接口，来启动的至少一次调用。

[0069] 该方法由应用程序接口来执行，使得根据本发明的内在化记录的方法的一个实施例得以执行。特别是，它把执行本方法所需的某些功能转移到一个可访问多种应用程序的应用程序接口。因此，此项功能不需要被纳入到应用程序之中。应用程序仍然控制着哪一个记录被内在化，以及何时进行内在化，由此避免了与不必要地经常重复的内在化和外在化有关的大部分等待时间。这个实施例特别适用于具有多任务能力的初级处理装置。

[0070] 本发明还提供了一种外部数据存储的方法，内在化数据的方法，处理多媒体系统中的记录的方法，允许初级处理装置验证属于一个记录的数据的完整性的系统与计算机程序。

[0071] 通过提供一种用于系统中的外部数据存储的方法就能做到这一步，该系统包括：

[0072] 初级处理装置，其具有一个处理器和一个初级数据存储单元，适于在处理器中处理有效记录，并且被配置用于将属于有效记录的数据存储在初级数据存储单元之中；以及

[0073] 次级数据存储系统，其可以访问初级处理装置，该方法包括：

[0074] 将属于一个有效记录的数据装载到初级数据存储单元之中，以及

[0075] 通过将属于该有效记录的至少一个数据片传送到次级数据存储单元以供存储，来使该记录外在化，其中，

[0076] 该方法包括存储反映该外在化记录的版本计数的信息，并且在外在化该记录之前，令版本计数加 1。

[0077] 因此，若在外在化之后，属于该记录的数据的任何部分（例如，已外在化的数据片或者被保留在初级数据存储单元之中的任何数据）被修改，则可以跟被存储的版本计数进行比较，以确定各部分是否仍然同步。

[0078] 本发明具有附加的优点，即，由于保存了反映该记录已经被外在化的次数的一个计数，所以获得了对该初级装置使用该记录的一个量度，允许对这种使用设置一种限制。进一步的效果是，有可能对哪一个记录被外在化得最频繁保持跟踪，因此，这个记录可以被保存在初级存储单元之中，也可以改为另一个已外在化的记录。

[0079] 最好是，该方法包括：在初级处理装置的数据存储单元中为每一个外在化的记录存储一个参考数据对象，包括一个唯一的标识符，以及反映版本计数的信息的一份拷贝。

[0080] 因此，初级处理装置能访问该信息的一份拷贝，该信息不能由次级存储系统可以访问的任何其他处理装置改变。

[0081] 本优选实施例还包括：向次级数据存储系统传送至少一个数据段，该数据段包括对应于该数据片的至少一个相关部分的数据，以及对应于反映版本计数的信息的数据。

[0082] 因此，在一个数据段中，对该数据片的这一部分有效的一个版本计数，连同每一个数据段，被存储在次级存储系统之中。本实施例具有这样的优点，它允许将该数据片切分为多个部分，这些部分以这样一种方式从外部被存储，使得可以证实这些部分属于该记录所属的数据的全集的同一版本。特别是，各数据段可以被存储在次级数据存储系统内的不同存储单元之中，并且再次被组合成为属于该记录的数据的一个有效集合。

[0083] 一个优选的实施例包括：确定在属于一个有效记录的任何数据装载到初级数据存储单元之后是否已经被更改，并且仅在确定属于该有效记录的某些数据已经被更改之后，才令版本计数加 1。

[0084] 这限制了版本计数值的取值范围。当反映版本计数的信息的一个拷贝被存储在初级存储单元时尤其有利，因为需要保留用于存储这份拷贝的存储器空间较小。

[0085] 根据本发明的另一方面，提供了一种用于在系统中内在化记录的方法，该系统包括：

[0086] 初级处理装置，其具有一个处理器和一个初级数据存储单元，适于在处理器中处理有效记录，并且被配置用于将属于一个有效记录的数据存储在初级数据存储单元之中；以及

[0087] 次级数据存储系统，其可以访问初级处理装置，并且被安排存储借助于根据本发明的最后陈述的外部数据存储方法而传送的数据片，该方法包括：

[0088] 从次级数据存储系统检索出含有对应于该数据片的至少一个相关部分的数据的至少一个数据段，其中

[0089] 含有反映已外在化记录的版本计数的信息的一个数据段被接收，并且该版本计数跟一个参考版本计数进行比较。

[0090] 该方法具有这样的优点，允许对从次级数据存储系统中检索出来的数据进行检查。这在允许不同的初级处理装置对记录进行外在化和内在化的环境中特别有用。若该记录已经被一个第一初级处理装置外在化，并且随后被一个第二初级处理装置内在化和外在化，则第一初级处理装置能以最小的处理努力来确定它最后处理的记录的版本不再可用于内在化。因此，它知道，将需要提供给它关于在次级存储系统中的现在的最新版本的信息。

[0091] 本方法的一个实施例包括：从一个可信的第三方系统中接收参考版本计数。

[0092] 这在初级处理装置中启动一次“交换”。第一初级处理装置可以外在化该记录。然后，第二初级处理装置执行本方法的这个实施例，以便能内在化该记录，并且继续对它进行处理。在需要考虑安全问题的环境中，这尤其有用。可信的第三方控制对已外在化的记录的访问。即，若第二初级处理装置再次外在化该记录，则版本计数再次被加 1。若第一初级处理装置从可新的第三方系统中接收一个已更新的版本计数，则它随后只能内在化该记录。

[0093] 在处理多媒体系统中的记录的方法中，通过应用上述各种方法中的任何一种，都能受益，上述多媒体系统适于对形成一个事件的数字内容中的至少一个连续片段提供访问，并且包括一个条件访问子系统，该子系统被安排按照包含在至少一个记录之中的信息，来控制对该事件的访问，其中，该多媒体系统包括一个安全的初级处理装置，其具有一个处理器和一个初级数据存储单元，适于在一个事件正在被访问时，在处理器中运行至少一个应用程序以处理有效记录，并且被配置用于将属于一个有效记录的数据存储在初级数据存储单元之中，以及

[0094] 一个次级数据存储系统，其可以访问初级处理装置。

[0095] 在本发明的语境中，名词“安全”指的是，初级处理装置备有对它所存储和 / 或处理的数据的入侵性和非入侵性攻击能抵御的装置，该装置可以用硬件或软件来实现，或者通过二者的组合来实现。由于在使初级处理装置抗篡改方面所涉及的成本和努力随着其能力的增加而增加，所以，优选限制其大小，特别是初级数据存储单元的大小。由于属于记录

的数据的部分或全部都能以一种有利的方式从外部存储在次级存储系统之中，所以本发明允许在这样做的同时，保留存取大量不同记录的能力。

[0096] 根据本发明的另一方面，提供了一个初级处理装置，其具有一个处理器和一个初级数据存储单元，适于在处理器中处理有效记录，配置用于将属于一个有效记录的数据存储在初级数据存储单元之中，并且适于执行根据本发明的上述各种方法中的任何一种。

[0097] 根据本发明的又一方面，提供了计算机程序装置，当它被具有一个处理器和一个初级数据存储单元的初级处理装置运行时，使得该初级处理装置能执行根据本发明的上述各种方法中的任何一种。

附图说明

[0098] 现在，将参照诸附图，对本发明进行更详细的说明，在诸附图中：

[0099] 图 1 是本发明所针对的一种系统的十分简略的总览图。

[0100] 图 2 是在本发明的一种变形中，初级处理装置所保持的一个数据库的一意图。

[0101] 图 3 是在图 2 的变形中，在次级存储系统中所存储的一个数据库的示意图。

[0102] 图 4 是表示一个记录的生成的流程图。

[0103] 图 5 是表示由初级处理装置对记录的修改的流程图。

[0104] 图 6 是表示在记录的外在化过程中的几个步骤的流程图。

[0105] 图 7 表示其中已经实施本发明的一个多媒体系统的实例。

[0106] 图 8 表示图 1 所示的初级处理装置的基本结构的一个实例。

具体实施方式

[0107] 为了说明根据本发明的外部数据存储方法的一般原理，图 1 表示可以在其中应用本发明的一个系统的简化实例。更专门的实例将在下文中参照图 7 和 8 加以说明。

[0108] 在图 1 中，第一处理装置 1 包括一个中央处理单元 (CPU)2，主存储器 3 以及一个初级海量存储装置 4。第一处理装置 1 可以，例如，被实现为一个服务器（例如，一个数据库服务器），一部个人计算机，个人数字助理，嵌入式处理装置，移动电话，等等。简而言之，凡是具有一个处理器、数据存储单元和用于访问一个次级数据存储单元的装置的任何数据处理装置都适于实施本发明。根据实施方式，主存储器 3 可以跟 CPU 2 集成在一块单独的芯片之上。

[0109] 在本文所描述的实例中，通过暂时地从初级海量存储装置 4 向次级存储系统传送数据，根据本发明的方法能被用来最大限度地利用初级海量存储装置 4 的有限的容量。然而，本方法也可以同样地被用来较好地利用主存储器 3 或 CPU2 中的高速缓冲存储器（未示出）的容量。因此，本文所使用的名词“初级数据存储单元”可以指易失性和非易失性数据存储装置二者，包括光学的、磁性的和固态存储装置。

[0110] 在图 1 中，第一处理装置 1 被连接到由第二处理装置 5 形成的一个次级数据存储系统。此种连接借助于数据链路 6 来实现。第二处理装置 5 还包括一个具有主存储器 8 的中央处理单元 (CPU)7，第一和第二次级海量存储装置 9 和 10。在本发明的基本实施例中，若次级存储系统被实现为诸如第二处理装置 5 那样的外部装置，则虽然存在某种微处理器，用以将数据导入到次级海量存储装置，但是第二处理装置包括 CPU7 并不是一项必需的要

求。在最简单的实施例中，本发明通过暂时地将数据传送到在第一处理装置 1 内部的第二海量存储装置，就能简单地和最大限度地利用初级海量存储装置 5 的有限的容量。

[0111] 然而，在优选实施例中，由于本发明的方法被实施于这样一个系统之中，即，初级处理装置跟次级处理装置相比，在对付黑客攻击方面要采取更严密的防范措施，所以要利用一个外部装置。在这样的系统中，根据本发明的方法特别有用之处在于，它提供了一种能够使初级处理装置的容量和 / 或尺寸保持很小的机制，使得防范措施变得更容易和更廉价。

[0112] 数据链路 6 可以是一种网络链路，例如，以太网，IEEE 1394（火线）链路，或者它可能是一种数据总线链路，例如使用 USB，SCSI，RS-232，蓝牙或相似类型的链路。根据所使用的链路的类型以及为处理属于该协议的消息所需的处理能力，可以用一个较简单的控制器来取代第二处理装置的 CPU7。

[0113] 第一处理装置 1 适于运行一种或多种应用程序，这些程序是由 CPU2 执行的。至少一种应用程序被配置用于处理各种记录。为此目的，一个记录被理解为被安排由应用程序处理的许多数据项的集合。数据的安排由对它进行处理的应用程序来规定。本发明包括固定长度和可变长度的记录二者。根据本发明，准备由在 CPU2 上执行的应用程序处理的记录成为有效的记录。有效记录，即，至少在这些记录有效的期间，属于由在任何一个时刻在第一处理装置 1 上运行的应用程序变为有效的记录的所有数据，都被存储在初级海量存储装置 4 之中。这并不排除数据的部分或全部的拷贝（可能不再是当前的）也被存储在别处，例如在次级海量存储装置 9、10 其中之一。

[0114] 根据本发明的应用程序被配置成能自主地决定是否将数据的部分或全部从外部存储，即，到初级海量存储装置 4 以外的一个不同的存储装置之中。据此作出这样的决定的规则可以改变。例如，数据的部分或全部可以建立备份。然而，本发明最好是被用来使记录外在化，使得属于该记录的数据的大部分可以从初级海量存储装置 4 移出，以便释放空间。这个部分，或者使其能恢复的数据，即，对应于这一部分的数据，被传送到次级海量存储装置 9、10 其中之一，以供存储，并且在以后借助于在本文中被分别称为外在化和内在化的处理过程来进行检索。

[0115] 在决定要外在化记录时，应用程序调用一个接口，该接口被安排用于将属于该记录的一个数据片传送到第二处理装置 5。在本文中，一个接口被定义为支持到次级存储系统的连接的物理和逻辑安排。最好是，在第一处理装置 1 中安装另一个应用程序或操作系统，第一处理装置 1 支持一个应用程序接口，处理待外在化的记录的应用程序可以调用该应用程序接口。因此，第一处理装置 1 的应用程序的开发者不需要精确地考虑用于外在化记录的机制。尽管如此，在本发明的范围内，仍然不能排除在应用程序中包括这样的实施例，在该实施例中包括用于外在化记录的部分或全部逻辑。在这样的实施例中，所指的接口大部分都是物理接口，即，通过数据链路 6 向第二处理装置 5 传送数据的机制。

[0116] 要注意的是，在本发明中，在第一处理装置 1 上运行的并且对记录进行处理的应用程序调用该接口，以便使记录外在化。然而，使用属于该项记录的数据（由在第一处理装置上处理该项记录的应用来提供）的另一项应用，也可以作出调用，并且可以由运行于第一处理装置 1 之上的应用程序来结束对该项记录的处理。这另一项应用甚至可以在被连接到第一处理装置 1 的一个独立的处理装置（包括在第二处理装置 5）上运行。

[0117] 为了允许对该记录的随后内在化，在初级处理装置 1 的一个初级数据存储单元中存储着一个初级数据库（图 2）。这最好是初级海量存储装置 4，但也可以是另一数据存储单元，例如主存储器 3，或者某些其他的易失性或非易失性存储器单元。要注意的是，第一处理装置 1 在其中存储了初级数据库的初级数据存储单元也可以是一个外围装置，但是为了更快地访问初级数据库，它最好是一个内部装置。在任何情况下，它最好是被纳入到与第一处理装置 1 共享的一个安全环境之中。

[0118] 图 2 表示在初级数据库中的初级数据库表格 11 的构成。要注意的是，该表格是本发明的一种实施方式的一个实例。只要对每一项已经被外在化的记录都有至少一个参考数据对象，确切的数据结构对本发明来说是不重要的。在这个实例中，针对每一外在化记录都有一个初级数据库记录 12a-12e，它们对应于在初级数据库表格 11 中的一行。每一个初级数据库记录 12 在索引列 13 中都包括一个字段，其中含有一个唯一的密钥或索引号，用以访问初级数据库记录 12。对每一外在化记录来说，在索引列 13 中的值是唯一的。在初级数据库列表 11 的版本号列 14 中，为每一外在化记录存储一个版本号。版本号可以是一个简单的计数器，或者它也可以是能反映相关的外在化记录的版本计数的任何其他类型的信息。例如，在一项记录含有多个字段、而每一个字段又有有限数目的值的场合，在版本号列 14 中的信息可能是唯一地标识在外在化记录的字段中的值的有限数目的可能排列的其中之一。反映版本计数的其他类型的信息也是可以设想的。

[0119] 在本实例中，第二处理装置 5 在被存储在次级海量存储装置 9，10 的每一个上的数据库中保存一个扩展记录表格 15（图 3）。所示的每一行都对应于一项扩展记录 16a-16e。每一项扩展记录 16 都跟一个外在化的记录相关。在索引列 17 中的各条目都含有反映相关的外在记录的唯一的标识符的信息。扩展记录表格 15 还包括第一、第二和第三数据块列 18-21。这样一来，在本实例的次级海量存储装置 9，10 中的每一项扩展记录都可以包括 3 个数据块。在针对一项外在化记录的一项扩展记录 16 中的每一个数据块都包括属于该外在化记录的一个数据片的至少一个相关部分所对应的数据。通过对应，意味着可以从外在化记录中的数据，完全地恢复该数据片的相关部分。因此，在数据块中的数据可以是属于该外在化记录的数据片的相关部分的一个已加密的、已编码的或已压缩的版本。最好是，每一个数据块都跟一个认证字符串存储在一起。该扩展记录表格还包括一个版本号列 21，在其中存储着反映外在化记录的版本计数的信息。上面结合在初级数据库表格 11（图 2）的版本号列 14 中的各条目已经叙述的内容对图 3 所示的版本号列 21 中的各条目也成立。在一种可供替代的实施方式中，在第一、第二和第三数据段列 18-20 其中之一的每一个数据块都可以包括反映一个仅对该数据块来说有效的版本计数的独立信息，或者跟这个信息存储在一起。

[0120] 当运行于第一处理装置 1 之上并且使用本发明的应用程序产生一项记录时，第一处理装置 1 就遍历图 4 所示的各步骤。在第一步骤 22 中，一个版本计数器被初始化。例如，当使用顺序号时，版本计数器被设置为数值 0，即，从 -1 增加到 0。然后应用程序使该记录有效，并对它进行正常处理。在处理时，属于该记录（它已被应用程序修改过）的数据被存储在初级海量存储装置 4 之中。在某些点上，应用程序可以决定对该项记录不进行任何进一步的处理，或者确定存在令该项记录外在化的另一理由。这样，通过调用一个接口，就能启动该记录的外在化。如上所述，这可以是作为第一处理装置 1 的操作系统的一部分而提

供的，或者是由另一个应用程序来提供的一个应用程序接口。

[0121] 假定至少 CPU2、主存储器 3，以及初级海量存储装置 4 是一个安全环境的组成部分，同时假定属于该记录的数据有待于保护。这样一来，在第二步骤 23 中，属于该记录的数据被加密，并且为该数据计算至少一个认证字符串。在下一个步骤 24 中，一项初级记录被写入到初级海量存储装置 4 内的初级数据库表格 11 中。这将导致把反映正在被外在化的记录的一个唯一的标识符的信息输入到索引列 13 的一个相应的条目之中。而且，版本计数被写入到版本号列 14 中的一个条目之中。因此，针对外在化记录的一个参考数据对象就被存储在初级海量存储装置 4 之中，该参考数据对象包括一个唯一的标识符以及反映版本计数的信息的一份拷贝。

[0122] 然后，在步骤 25 中，属于该记录的已加密的数据片，连同一个认证字符串以及反映版本计数的信息一起，被传送到第二处理装置 5。第二处理装置 5 将已传送的数据段的内容存储在扩展记录表格 15 之中。

[0123] 根据本发明，使用已外在化的记录的应用程序也可以自主地决定再次内在化该记录。内在化处理的一个实施例示于图 5。因此，在某一点上，使用（即，被配置去使用）属于该记录的数据的应用程序确定该项记录将被内在化。该应用程序调用通往次级存储系统的一个接口。软件，例如一个应用程序接口（它是通往次级存储系统的接口的一部分）保证向第二处理装置 5 发送一条消息，请求包括属于一项外在化记录的数据所对应的数据的数据段。该消息至少包括反映该外在化记录的唯一的标识符的信息。此项信息从初级数据库表格 11 的索引列 13 中的相关条目被检索出来。在步骤 26 中，该接口保证，能检索到至少一个数据段，该数据段包括对应于外部存储的数据片的至少一个相关部分的数据。被检索的数据段包括反映版本计数的信息。此项信息是从扩展记录表格 15 的版本号列 21 的相关条目中获得的。在步骤 27 中，第一处理装置 1 使用一个保密的加密密钥，对已检索的数据段中的数据片的加密部分进行解密。然后，它从已解密的数据中，计算出一个核对认证字符串。在步骤 28 中，该核对认证字符串跟在已检索的数据段中所含有的一个认证字符串进行比较。若二者匹配，则从被包含在已检索的数据段的信息中导出一个版本计数，并且将其跟从初级数据库表格 11 的版本号列 14 中所导出的一个版本计数进行比较。若二者匹配，则已解密的数据片被用来组合新的内在化记录。该内在化记录被存储在初级海量存储装置 4，以备应用程序使用。

[0124] 假定运行于第一处理装置 1 之上的应用程序实际上修改了属于该项记录的数据（步骤 29）。在修改之后，它可以再次决定该项记录要被外在化。在那种情况下，在步骤 30 中，版本计数被更新，即被加 1。在步骤 31 中，属于该项记录的一个数据片被加密，同时为它计算一个认证字符串。然后，在初级数据库表格 11 中的初级记录被重写，即，反映已加 1 的版本计数的信息被写入到版本号列 14 的对应条目之中。一个数据段，包括已加密的数据片，认证字符串，以及反映已更新的版本计数的信息的一份拷贝被传送到第二处理装置 5，在那里，在扩展记录表格 15 中的相应的扩展记录 16 被更新，或者，若它已被删除，则被重写。

[0125] 要注意的是，本发明的一个实施例考虑到 CPU2 和 / 或主存储器 3 和 / 或数据链路 6 的特性。这些方面示于图 6。当属于一个记录的一个数据片 34 的一部分被处理，以纳入一个准备传送的数据段，或者从一个已检索的数据段中取出时，它被保存在主存储器 3 之中。

因此，CPU2 或主存储器 3 的容量可以为该部分的大小设置一个范围，超出这个范围时，内在化和外在化处理将使第一处理装置 1 的速度降低到不能接受的地步。对数据片的该部分的大小的另一种限制就是所得到的数据段的大小，该数据段包括加密部分、认证字符串、版本计数以及索引信息。在第一步骤 38 中，考虑到上述各项约束条件的最大限制，第一处理装置 1 将属于一个有待于外在化的记录的数据片 34 划分为多个部分 35-37。在这种情况下，分为第一、第二和第三部分 35-37。划分为多个部分 35-37 的操作可以由处理该项记录的应用程序来实现，或者通过执行属于由该应用程序调用的应用程序接口的模块来实现。在一个随后的步骤 39 中，使用一个保密的加密密钥 40 对部分 35-37 中的每一部分进行单独的加密，并将其存储到初级海量存储装置 4、CPU2 和主存储器 3 所共享的安全环境之中。第一数据块 41 跟属于正在进行外在化的数据片 34 的第一部分 35 相对应，第二数据块 42 跟第二部分 36 相对应，第三数据块 43 跟第三部分 37 相对应。

[0126] 在下一个步骤 44 中，使用第一数据块 41 作为输入，为数据片 34 的第一部分 35 计算一个第一认证字符串 45，以及一个保密的认证密钥 46。保密的认证密钥 46 也被存储在初级海量存储装置 4、CPU2 和主存储器 3 所共享的安全环境之中。在随后的步骤 47 中，生成一个第一数据段 48。第一数据段 48 包括第一数据块 41、第一认证字符串 45、对应于被存储在针对外在化记录的初级数据库表格 11 的索引列 13 的条目之中的索引值的信息，以及反映第一数据段 48 跟在构成数据片 34 的各部分 35-37 的序列中的第一部分 35 相关这样一个事实的信息。然后，第一数据段 48 被传送到第二处理装置 5 以供存储。

[0127] 与此同时，在步骤 50 中对第二认证字符串 49 进行计算。第二认证字符串 49 是从第二数据块 42 以及第一认证字符串 45 计算出来的。这可以这样来完成，例如，首先，将第二数据块 42 跟第一认证字符串 45 串接在一起，然后使用如同在步骤 44 中所使用的认证密钥 46，用相同的认证算法对前一步的串接结果进行计算。

[0128] 在步骤 51 中生成第二数据段 52。步骤 51 对应于步骤 50。因此，第二数据段 52 包括第二数据块 42，第二认证字符串 49，反映已外在化记录的唯一的标识符的信息，以及反映第二数据段 52 跟从数据片 34 形成的各部分 35-37 的序列中的第二部分 36 相关这样一个事实的信息。

[0129] 在步骤 53 中，使用第二认证字符串 49 作为输入，还有认证密钥 46 以及第三数据块 43，来计算第三认证字符串 54。步骤 53 基本上对应于步骤 50。

[0130] 在步骤 55 中，生成第三数据段 56，并且被传送到第二处理装置 5。类似于第一和第二数据段 48、52，第三数据段 56 包括第三数据块 43，第三认证字符串 54，反映已外在化记录的唯一的标识符的信息，以及反映第三数据段 56 跟从数据片 34 形成的各部分 35-37 的序列中的第三部分 37 相关这样一个事实的信息。

[0131] 要注意的是，本发明的方法可以同时应用于属于数据片 34 所属的记录以外的记录的各数据片。然而，跟属于一个记录的数据片 34 的各部分 35-37 相关的各数据段 48、52、56 不包括跟属于另一个记录的一个数据片的各部分相关的各数据块。这就保证了第一、第二和第三数据段 48、52、56 保留着适合于数据链路 6 的大小。它还能保证由第二处理装置 5 进行有效的处理。特别是，当该记录被再次内在化时，第一、第二和第三数据段 48、52、56 的确切的拷贝被检索。为了避免不必要的数据传送，把为一项记录生成的各数据段跟为另一项记录生成的那些数据段分隔开来是有利的。

[0132] 图 7 表示一个在其中进行记录处理的、适于应用本发明的系统的一个特例。所图解的系统是一个多媒体系统，它适于访问至少一个连续的数字内容片，同时包括一个条件访问子系统，用以控制对数字内容的访问。具体地说，图 7 表示一个用于记录和回放内容数据的个人视频记录器 57，上述内容数据是以广播的形式接收的，或者是从内容分销商那里下载的。

[0133] 个人视频记录器包括一个调谐器 58，用以调谐到一个特定的载频。它还包括一个解调器 59，用以取出一个传输流，其中包括一个或多个载有数字内容的单元流。这些可以是，例如，MPEG-2 单元流或者 MPEG-4 访问单元的流。由多媒体处理器 60 对各单元流进行处理，为此目的，该处理器 60 必须访问主存储器 61。多媒体处理器 60 被连接到例如 I^2C 总线那样的系统总线 62。多媒体处理器 60 还被连接到一个视频编码器 63 以及一个音频数字 - 模拟转换器 (DAC)64。这样一来，个人视频记录器就能通过适当的输出，给出一个回放装置（例如一部电视机）可用的模拟视频和音频信号。当然，在一个可供替代的实施例中，个人视频记录器还可以包括一个编码器，用以给出采取（未经保护的）MPEG-2 编码流形式的输出，后者可以例如在以太网上传送，或者从 IEEE 1394 家庭网络向一个或多个家庭网络终端设备传送。

[0134] 一个接口控制器 65 也被连接到系统总线 62。接口控制器 65 把各项命令从用户那里转发到控制个人视频记录器 57 的运行的多媒体处理器 60，还可以可选地向用户提供反馈信息。例如，接口控制器可以控制一个红外口，以便从一个遥控单元（未示出）接受各项命令，或者它可以控制个人视频记录器 57 的一个前面板接口。

[0135] 个人视频记录器 57 还包括一个盘控制器 66，它被连接到系统总线 62，还被连接到光盘驱动器 67 以及硬盘驱动器 68。光盘驱动器 67 以及硬盘驱动器 68 仅被认为是在根据本发明的方法中所使用的一个次级数据存储系统中所包含的海量存储单元的代表。

[0136] 条件访问子系统包括一个条件访问模块 (CAM)70，后者又包括一个处理器 71，用以跟条件访问模块 70 进行双向的直接通信。CAM 70 附带地包括一个加密协处理器 72，一个专用的数字信号处理器，用以实行加密和 / 或解密运算。从数字视频广播 (DVB) 的各种实施方式中就可以获知这样的 CAM 70 的各种实例，在其中，CAM 70 通过一个公共接口 (CI) 跟一个集成的接收机解码器进行通信，个人视频记录器 57 就是集成的接收机解码器的一个特例。在这些已知的实施方式中，条件访问模块 70 采取 PCMCIA 卡的形式。

[0137] 条件访问子系统还包括一块智能卡 72。其上载有智能卡集成电路 (IC)73。智能卡 72 最好是符合于 ISO 7816-2 标准。智能卡 72 通过物理互连系统跟 CAM 70 建立接口关系，并且通过它跟个人视频记录器 57 建立接口关系，上述物理互连系统包括在智能卡上的接触片（未示出）以及在 CAM 70 中的接触引脚（未示出），以及用以实现一种通信协议的一个或多个软件模块。

[0138] 图 8 表示智能卡 IC 73 包括一个中央处理单元 (CPU)74。它还包括 3 种类型的存储器模块，即，一个掩模只读存储器 (mask ROM)75，随机存取存储器 (RAM)76 以及电擦除可编程只读存储器 (EEPROM)77。当然，智能卡 IC 73 还包括一个输入 / 输出 (I/O) 口 78，作为通往 CAM 70 的接口的一部分。智能卡 IC 73 的可供替代的实施例可以包括一个铁电随机存取存储器，用以取代 EEPROM 77。

[0139] 掩模 ROM 75 是一种非易失性存储器。智能卡 72 的操作系统被存储在掩模 ROM 75

之中。适宜的操作系统的实例为 MULTOS，Java 卡和 Windows 卡。此外，一种或多种加密密钥可以存储在掩模 ROM75 之中。RAM 76 形成存储器工作空间。RAM 76 是易失性存储器，并且当智能卡 IC 72 的电源被关断之后，所有数据将丢失。EEPROM77 表示非易失性存储器，用于存储动态应用数据。

[0140] 在智能卡 IC 73 中所包含的 3 种类型的存储器当中，RAM 76 通常是最昂贵的，其后依次为 EEPROM 77 以及掩模 ROM 75。令存储器的数量，尤其是较昂贵类型的存储器的数量保持有限，终归是有利的。通过对存储在智能卡 72（即，EEPROM 77）的初级数据存储单元中的动态应用数据中所包含的各项记录进行内在化和外在化，智能卡 72 就能用有限容量的 EEPROM 77 进行工作。作为根据本发明的方法的一部分，通过将属于已内在化或已外在化的记录的数据片划分为各部分，智能卡 IC 73 就能用有限大小的 RAM 76 以及有限容量的 I/O 78 进行管理。

[0141] 典型地使用一个在其中含有图 7 所示的多媒体系统的广播系统包括一个用户管理系统 (SMS)，在那里保存着所有用户的细节。诸如该用户可以收看的频道和事件，他的支付状态，他的智能卡 72 是否有效，以及其他信息都被保存在 SMS 之上。一个事件被定义为数字内容的一个连续的片段，例如 DVB MPEG-2 服务中的一个片段，它既处于条件访问的管理之下，同时具有相关的事件信息。用一个或多个控制字作为通往加扰算法的密钥对一个事件进行加扰。用户进行预订的付款发票从 SMS 被送出。SMS 经由一个条件访问 (CA) 系统，通过向用户发送各项命令来控制分配到各用户之中的智能卡 72。CA 系统为智能卡 72 将这些命令转换为正确的格式，并将各项命令插入到传输流中去。CA 系统的另一项功能就是对各控制字进行加密，当向用户广播一个事件时，就用上述控制字对该事件进行加扰。这些已加密的控制字，连同形成该事件的内容一起，作为资格控制信息 (ECMs) 而被发送。

[0142] 提供的内容以及在广播中出现的每一个事件由一个调度系统进行调度。由各内容服务器对内容进行编码 / 压缩。来自各内容服务器和 CA 系统的格式化数据以多路复用方式进入一个传输流，然后，该传输流经过调制进入适当的广播网络（即，卫星、电缆、地面、因特网，等等）。

[0143] 个人视频记录器 57 使用调谐器 58 和解调器 59 来恢复传输流。由多媒体处理器 60 将已加扰的传输流路由到条件访问模块 70。条件访问子系统使用一个密钥分级对传输流进行解扰。被存储在智能卡 72（例如掩模 ROM 75）之中的是智能卡 72 唯一的密钥，称为 X 密钥。在某些可供替代的系统中，可能有很多级别的 X 密钥，其中较高等级的被称为组密钥，并且被分配给各用户组。为了简单起见，本说明书假定只有一个等级。

[0144] 多媒体系统包括一个或多个软件模块，其中的至少某一些被安装在智能卡 72（其他的可以安装在个人视频记录器 57 或 CAM 70）之上，它们实现了一个事件管理系统 (EMS)。事件管理系统包括一段运行于智能卡 72 之上的应用程序，智能卡 72 处理含有用以控制对事件的访问的信息的记录。这些记录包括会晤记录和事件记录。当事件记录以及会晤记录被处理时，它们是有效的，并且被存储在 EEPROM77 之中。通过把属于该记录的至少一个数据片传送到一个次级存储系统中的一个存储装置（例如，在个人视频记录器 57 里面的硬盘驱动器 58）之中，就能使事件记录和会晤记录二者外在化。

[0145] 在一个示范性的实施例中，事件记录包括下列字段：有效标志，更改标志，版本号，记录标识符，回放计数以及拷贝次数计数。每次事件记录有效时，有效标志就被置位。至少

当一个事件被记录、拷贝或回放时，该事件记录才有效。当一个事件记录有效时，由智能卡的 CPU 74 对它进行处理。同时属于该记录的数据被存储在 EEPROM 77 之中。在处理事件记录的过程中，若对属于该事件记录的任何数据作出更改，则更改标志被置位。具有一个更改标志的优点是可以避免不必要的外在化。在优选实施例中，当接收到一道要求外在化该事件记录的命令时，首先对更改标志进行检查。若它没有被置位，则外在化是不必要的，因为被存储在个人视频记录器 57 里面的拷贝仍然是精确的。在对事件记录进行每一次外在化之前，版本号被加 1。在调用智能卡 72 上的应用程序接口时，以及由智能卡 72 上的应用程序接口作出调用时，记录标识符允许该事件记录被识别。回放计数以及拷贝次数计数是反映回放计数的两种类型的信息，每次事件记录变为有效以便访问相关事件时，回放计数就被加 1。当需要访问该事件（例如制作该事件的一份拷贝、对该事件进行解扰和解码、把它记录到被插入到光盘驱动器 67 的光盘或硬盘驱动器 68 等）时，就会出现这种情况。

[0146] 会晤记录包括资格信息以及节目密钥 (P 密钥)。P 密钥被用来对在已接收的 ECM 中所包含的已加密的各控制字进行解密，同时可以作为已加扰的传输流的一部分，由个人视频记录器 57 进行记录。通过为该事件付费来获得针对一个事件的 P 密钥和资格信息，于是，广播公司的 CA 系统发出一项或多项资格管理信息 (EMMs)，其中包括用智能卡 72 的 X 密钥进行加密的资格信息和 P 密钥。智能卡 72 从 EMMs 中取出 P 密钥和资格信息，并将它们添加到会晤记录中去。有一个针对每一次记录的会晤的会晤记录，即，每一个连续的时间段，在该时间段中，内容数据被记录在硬盘驱动器 68 或者光盘驱动器 67 中的一张光盘之上。每一个会晤记录都被链接到一个或多个事件记录，并且由此跟各事件建立关联，而这些事件又跟各事件记录建立关联。在一次观测会晤的过程中提供对一个事件的访问，在此段时间内，该会晤记录是有效的，即，属于该会晤记录的数据存在于 EEPROM 77 之中。在回放该事件时，该事件记录也是有效的。

[0147] 为了实现事件和会晤记录的外在化以及随后的内在化，智能卡 72 包括一个应用程序接口，它被安排去接收和处理来自一项正在实现 EMS 的应用的信息，并由此使用该事件和会晤记录。假定在一次会晤期间一个事件已经被记录，同时假定为访问该事件所需的 P 密钥已经被存储在一个相关的会晤记录之中，当记录已经完成，并且不需要立即回放时，控制着记录过程、并因此使用该事件和会晤记录的该项应用就向实现记录的外在化的智能卡应用程序接口 (API) 发出一项外在化调用。下面的说明将集中在事件记录的外在化，应当理解，会晤记录的外在化也以类似方式进行。

[0148] 在一个实施例中，API 将属于该记录（该记录可以包括属于该记录或者它的一个子集的所有数据）的一个数据片划分为一系列的连续的各部分。每一部分的大小视介于 EEPROM 77 以及个人视频记录器 57 的硬盘驱动器 68 之间的接口的最大处理能力而定。最大处理能力取决于 RAM 76、中央处理单元 74、I/O 口 78、处理器 70、介于 CAM69 以及个人视频记录器 57 之间的 PCMCIA 接口的大小，或者系统总线 62 的大小，而这又取决于特定的实施方式。

[0149] 随后，API 接收到针对每一部分的外在化消息，每一项外在化消息都代表着一项传送一个数据段的请求，上述数据段包括对应于待传送的数据片的至少一个相关部分的数据。API 使用结合图 6 所列出的方法来产生该数据段。这就是说，属于该事件记录的数据片的每一部分都被加密，同时为它计算一个认证值。为该数据片的每一部分生成一个独立的

数据段，包括已计算的认证值、该数据片的加密部分、以及该部分在通过将该数据片划分为连续的部分而产生的各部分的序列中的位置。此外，该数据段还包括反映版本号的信息。

[0150] API 为每一个数据段接收一个独立的外在化消息。使用图 6 所示方法产生的数据段被一个接一个地返回，每一个都响应于一项相关的外在化消息。这些外在化消息包括对应于事件记录标识符的信息，以及借助于数据片的相关部分在各部分的序列中的位置来识别该数据段的信息。可选地，响应于第一次收到的调用，API 可以返回表示在序列中有多少个部分的信息。

[0151] 在最后一个数据段已经被传送之后，该应用发送一项确认请求。若正确的外在化得到确认，则保存在 EEPROM 77 中的属于该记录的数据拷贝中的更改标志被复位。只有在这以后，该记录才能被去激活，并且被传送用于外部存储的属于该记录的数据片才可以从 EEPROM77 中被删除。然而，在 EEPROM 77 中，为每一个外在化的记录都保存了一个参考数据对象。该参考数据对象包括记录标识以及版本号。

[0152] 当该事件记录被再次内在化（例如，启动相关事件的回放）时，智能卡 API 从使用属于该事件记录的数据的一项应用中接收到一次调用。然后，该 API 检索被存储在硬盘驱动器 68 之中的各数据段。再次地，各数据段被独立地检索和处理。在这里，每一个数据段都包括跟属于该记录的数据片的一部分所对应的数据，它在序列中有一个规定好的位置，各数据段被依次地检索出来。因此，含有对应于序列中的第一部分的数据的数据段首先被检索。这对于在不必首先对所有的数据段进行缓冲存储的前提下，能为每一个数据段计算一个参考认证值来说是必需的。只有用于第一数据段的参考认证值才可以在不使用为一个或多个其他数据段而计算的参考认证值的条件下计算出来。要注意的是，使用已计算的参考认证值就能排除对存储参考认证值的需求。仅需存储一个认证密钥。认证密钥可以存储在掩模 ROM 75 之中，后者的价格比 EEPROM 77 便宜。可供替代地，它也可以被存储在 EEPROM 77 之中，以便在智能卡 72 的试用期限内允许对认证密钥进行一次更改。

[0153] 使用被存储在智能卡 72 之中的加密密钥对该数据段进行解密（假定使用对称算法）。然后，将被包含在数据段之中的版本号跟已计算的参考认证值进行比较，同时将该事件记录的版本号跟被存储在 EEPROM 77 的参考数据对象中的版本号进行比较。若二者均为正确，则对每一个后继的数据段重复这一处理过程，并且属于该事件记录的数据片在 EEPROM 77 中被重新组合。此后，该事件记录被激活，并从中检索数据，以便允许条件访问子系统去控制被存储在硬盘驱动器 68 的一个事件的回放、拷贝或其他用途。

[0154] 由于属于该事件记录的数据以加密的形式被存储于外部，所以对黑客来说，要想向下修改回放计数，以得到比根据在会晤记录中的资格信息所允许的收看次数更多的收看次数是很困难的。即使黑客推断出加密密钥，然后需要认证密钥去为含有对应于被向下修改的回放计数的信息的一个数据段去计算一个新的认证值。由于使用链接，所以还需要针对所有的与该事件记录有关的其他各数据段的认证值。不可能简单地制作一份早先的数据段的拷贝，因为它的版本号跟被存储在智能卡 72 的 EEPROM 77 之中的参考数据对象的版本号不匹配，所以早先的各数据段不能导致事件记录的成功的内在化。

[0155] 将版本号纳入到保存在智能卡 72 的 EEPROM 77 的参考数据对象之中以及纳入到被传送到硬盘驱动器 68 的数据段之中，使得用第二智能卡来取代第一智能卡的处理过程得以实现。最好是从一个可信的第三方，例如向个人视频记录器 57 广播数据的 CA 系统，向

第二智能卡提供跟在第一智能卡的参考数据对象中的数据相对应的数据。然后，第二智能卡就能使用所提供的数据对该记录进行内在化。当它随后再次对该记录进行外在化时，其版本号被加 1。因此，第一智能卡将不再对该记录进行内在化，因为它正在为该记录存储一个具有先前的版本号的参考数据对象。当然，应当向第二智能卡提供加密和认证密钥，以及参考数据对象。

[0156] 本发明并不局限于上述各实施例，而是可以在所附权利要求书的范围内发生改变。例如，含有个人视频记录器 57 以及具有插入的智能卡 72 的条件访问模块 69 的系统就是类似地适用本发明的类似的多媒体系统的代表。这包括这样的系统，它含有一个机顶盒，用以取代个人视频记录器，一部具有相关外围硬件的个人计算机，用以接收由条件访问方法保护的数字内容，或者一部个人视频记录器，它被安排去接收模拟信号。

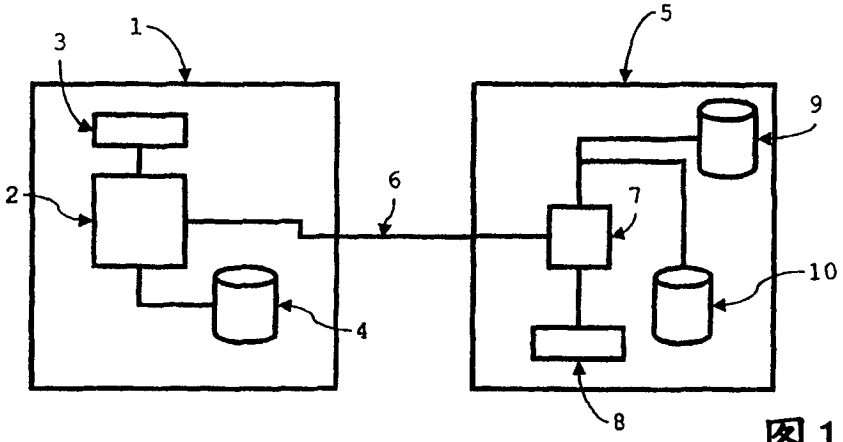

1
2
3
4
5
6
7
8
9
10

图 1

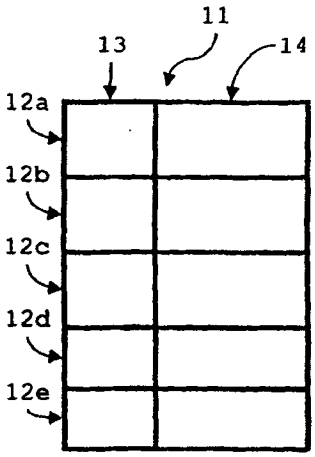

11
13
14
12a
12b
12c
12d
12e

图 2

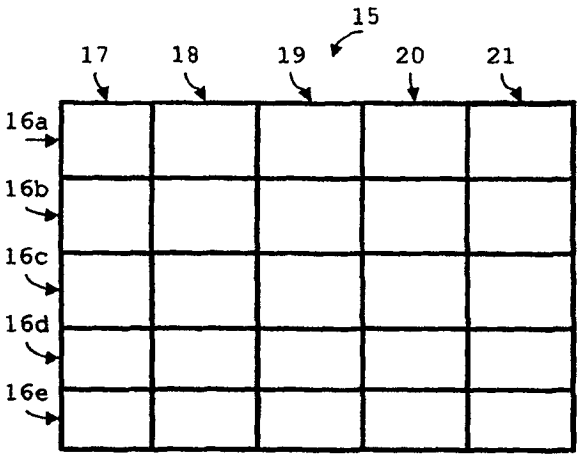

15
17
18
19
20
21
16a
16b
16c
16d
16e

图 3

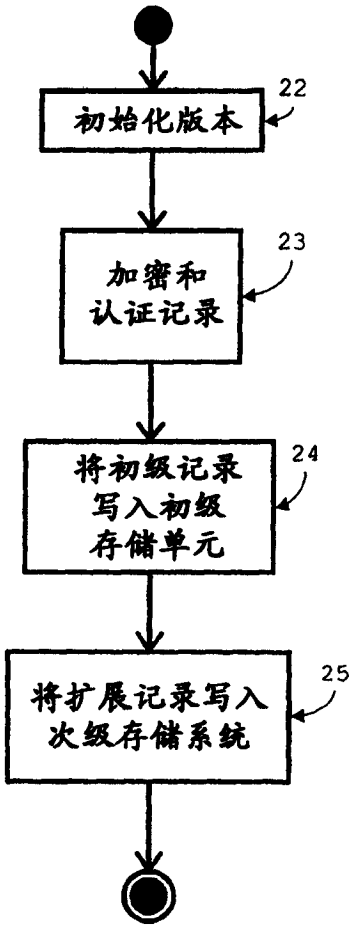

初始化版本
22
加密和
认证记录
23
将初级记录
写入初级
存储单元
24
将扩展记录写入
次级存储系统
25

图 4

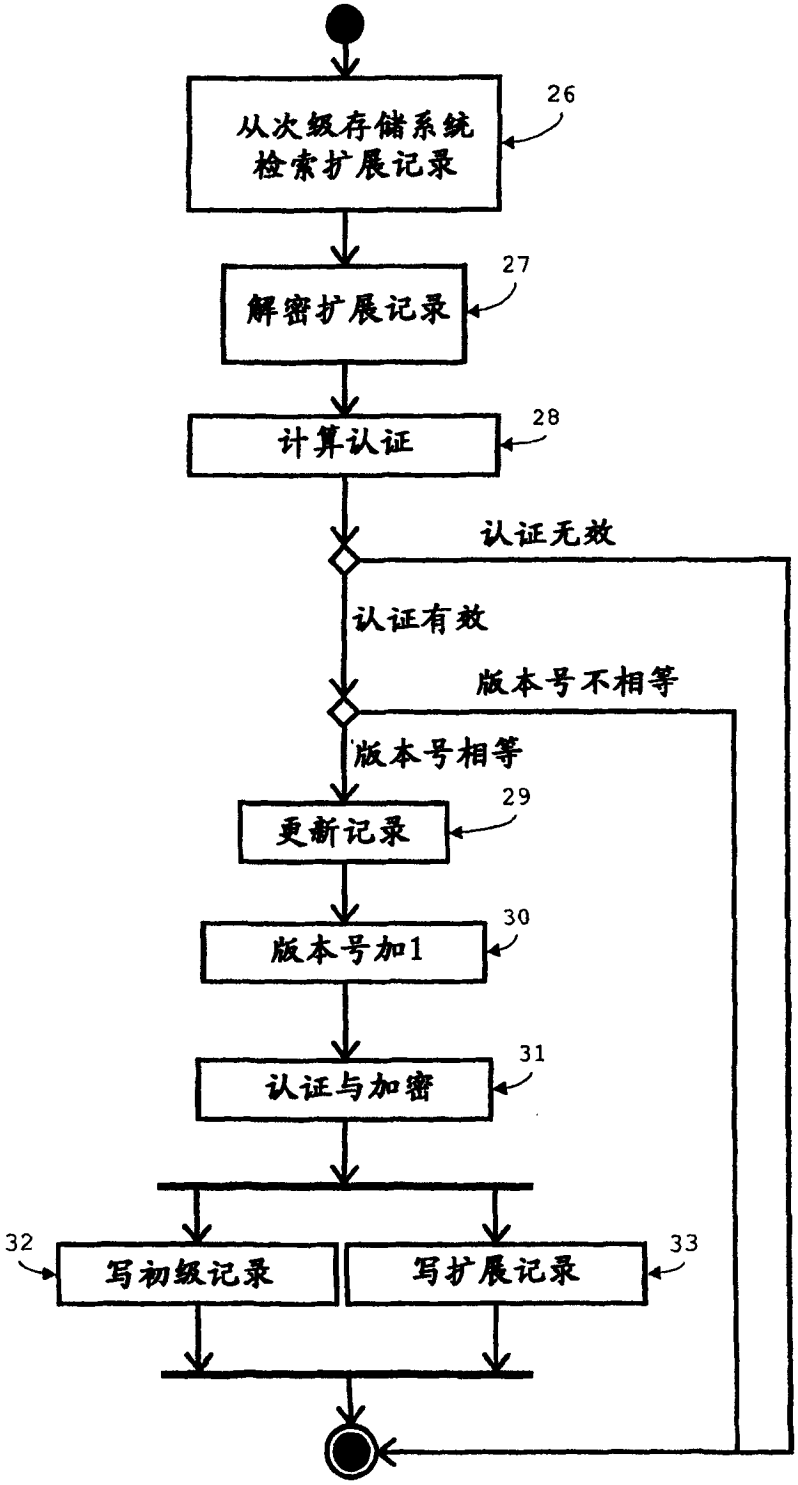

从次级存储系统
检索扩展记录
26
解密扩展记录
27
计算认证
28
认证无效
认证有效
版本号不相等
版本号相等
更新记录
29
版本号加1
30
认证与加密
31
写初级记录
32
写扩展记录
33

图 5

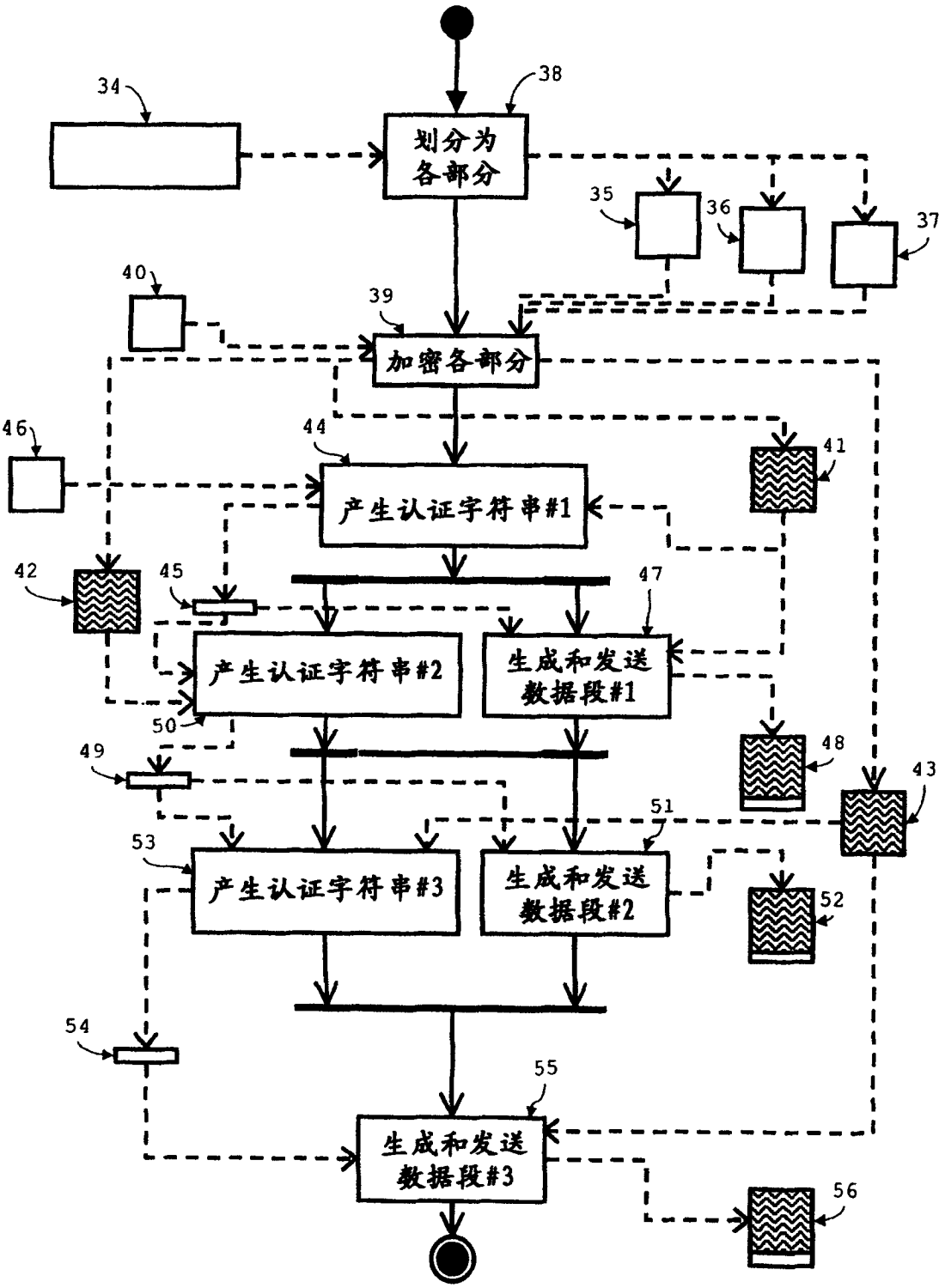

34
38
划分为
各部分
35
36
37
40
39
加密各部分
46
44
41
产生认证字符串#1
42
45
47
产生认证字符串#2
生成和发送
数据段#1
50
49
48
43
51
53
产生认证字符串#3
生成和发送
数据段#2
52
54
55
生成和发送
数据段#3
56

图 6

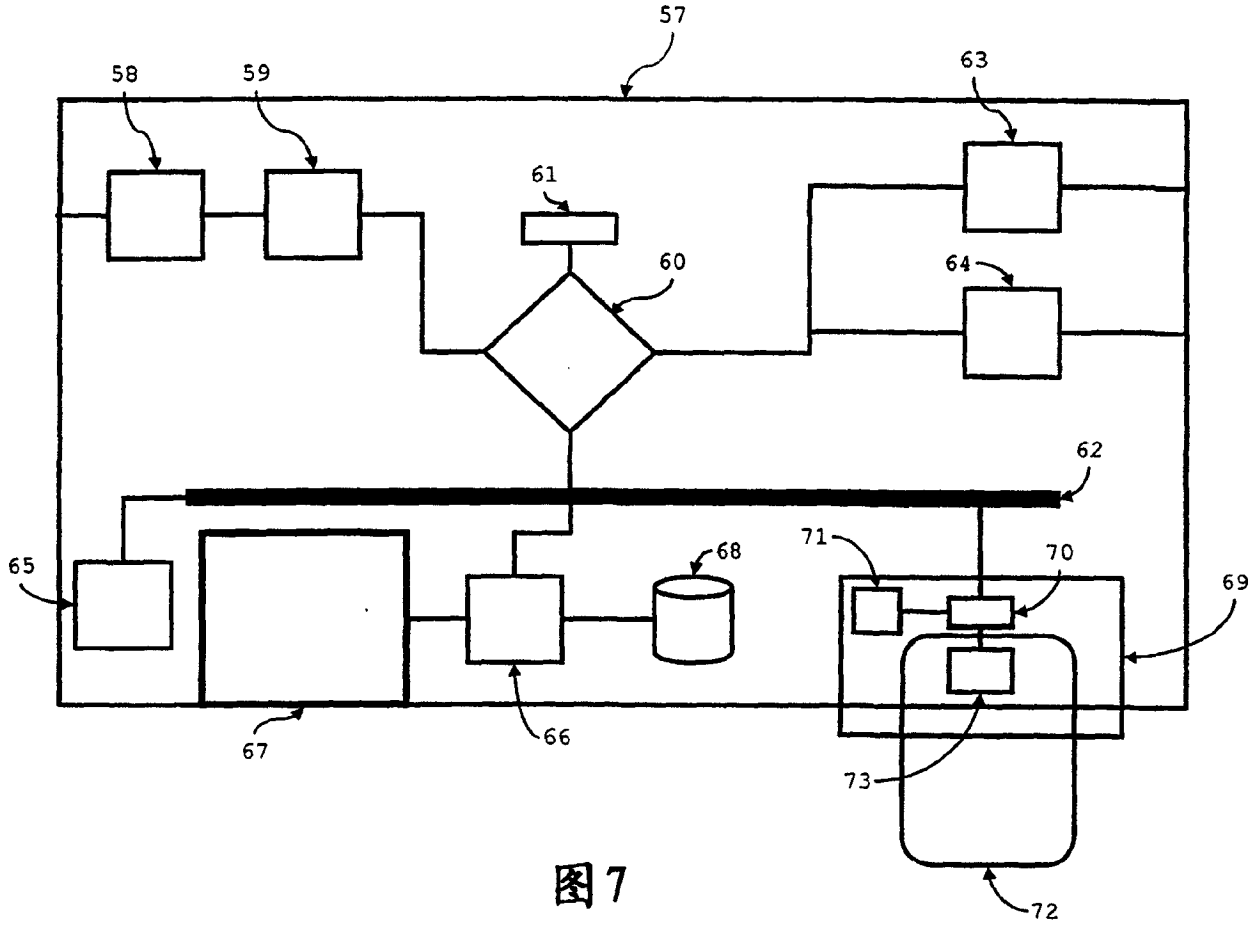


图7

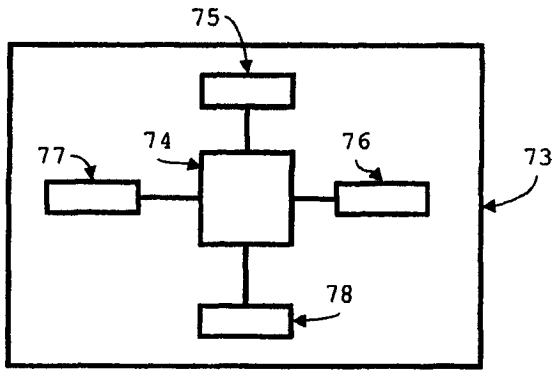


图8