[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 17/00

[12] 发明专利说明书

[21] ZL 专利号 95115532.6

[43] 授权公告日 2003 年 6 月 18 日

[11] 授权公告号 CN 1111809C

[22] 申请日 1995.8.10 [21] 申请号 95115532.6

[30] 优先权

[32] 1994. 8.10 [33] JP [31] 219372/1994

[32] 1994. 9.20 [33] JP [31] 225228/1994

[71] 专利权人 富士通株式会社

地址 日本神奈川

[72] 发明人 秋山良太 吉冈诚

审查员 韩 燕

[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

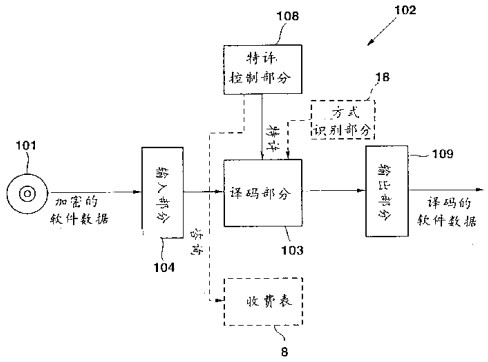
代理人 杜日新

权利要求书 3 页 说明书 19 页 附图 23 页

[54] 发明名称 数据管理模块、数据复制管理装置以及数据复制管理系统

[57] 摘要

一种数据管理模块，与数据复制装置一起使用，用于选择并复制加密数据，包括：输入装置；用于许可所述加密数据被译码的特许控制装置；译码装置，用于对由所述特许控制装置许可的加密数据进行译码；用数据存储装置；以及输出装置，特许控制装置根据译码装置所译码的加密数据的特征，减少剩余差额值，将差额值与预定的截止值比较，并根据比较结果许可译码另外的加密数据。 还有数据复制管理系统。



ISSN1008-4274

1. 一种数据管理模块（102），与数据复制装置（105）一起使用，用于选择并复制加密数据，其特征在于包括:

用于输入所述加密数据的输入装置（104）;

用于许可所述加密数据被译码的特许控制装置（108）;

译码装置（103），用于对由所述特许控制装置许可的加密数据进行译码;

用数据存储装置，用于存储余额差值；以及

用于输出由所述译码装置译码的译码数据的输出装置(109),

所述特许控制装置（108）根据所述译码装置（103）所译码的所述加密数据的特征，减少剩余差额值，将差额值与预定的截止值比较，并根据比较结果许可译码另外的加密数据。

2. 如权利要求 1 的数据管理模块，还包括费用数据存储装置，其中所述的特许控制装置借助于参照费用数据存储装置，许可对数据存储介质中的特定数据进行译码。

3. 如权利要求 1 的数据管理模块，还包括加密装置，并且其中所述特许控制装置当把由译码处理产生或处理的用户数据向外输出时，借助于加密装置对用户数据进行加密。

4. 如权利要求 3 的数据管理模块，其中所述用户数据是费用数据。

5. 如权利要求 1 的数据管理模块，其中所述译码装置具有方式识别装置，它能够根据所述加密数据的特征改变用于译码的加密利用方式。

6. 如权利要求 1 的数据管理模块，其中所述译码装置包括:

位于输入侧的输入缓冲器;

译码执行装置，用来通过特定逻辑执行加密或对输入数据进

行译码;

置于所述译码执行装置前面的中间寄存器;

位于所述输入寄存器和所述中间寄存器之间的选择器，用来向所述中间寄存器选择地输出来自所述输入寄存器或来自所述译码执行装置的输出；以及

位于所述译码执行装置下一级的输出缓冲器，用来顺序地输出译码的数据。

7. 如权利要求 6 的数据管理模块，其中所述输入缓冲器或输出缓冲器是移位寄存器。

8. 一种数据复制装置，包括:

驱动装置，用于从存储加密的专用数据的存储介质中读取加密数据;

解调装置，用于从所述存储介质中读取加密数据并解调所述加密数据;

数据管理模块，包括用来输入所述加密数据的输入装置，用来对特定加密数据许可解调的特许控制装置，用来对由所述输入装置输入的并由所述特许控制装置允许译码的加密数据进行译码的装置，以及用来输出由所述译码装置的译码数据的输出装置;以及

用来输出所述管理模块的译码数据输出的输出装置。

9. 如权利要求 8 的数据复制装置，还包括卡驱动装置，所述含有数据管理模块的卡可以连续在所述驱动装置上。

10. 一种数据复制管理系统，包括控制中心以及数据复制装置，其中:

所述控制中心具有特许指令发出装置，用来对来自所述数据复制装置的利用请求发出作为特许指令的键数据；以及

所述数据复制装置具有译码装置，根据所述键数据对所述数据进行译码。

11. 如权利要求 10 的数据复制管理系统，其中所述控制中心具有费用数据存储装置，用来存储用户的费用数据，并且所述数据复制装置具有加密装置，当所述费用数据被报告给控制中心时，对所述数据进行加密。

12. 如权利要求 10 的数据复制管理系统，其中所述控制中心具有数据安全检查装置，用来检查加密的或非加密的数据的可靠性。

13. 如权利要求 10 的数据复制管理系统，其中:

所述控制中心具有发送侧检验和发生装置，用来由加密的或非加密的数据产生检验和；以及

所述数据复制装置具有接收侧检验和发生装置，用来接收来自控制中心的所述数据以及检验和，并由所述数据产生一个检验和，以及比较装置，用来比较由接收侧检验和产生装置产生的检验和和从所述控制中心收到的检验和。

14. 如权利要求 13 的数据复制管理系统，其中所述的控制中心具有加密装置，用来加密所述数据，所述发送侧检验和产生装置对于由所述加密装置加密之前的数据或对加密之后的数据产生检验和。

15. 如权利要求 13 的数据复制管理系统，其中如权利要求 1 所述的数据管理模块具有显示装置，用来显示按照权利要求 13 由比较装置进行的比较结果。

16. 如权利要求 13 的数据复制管理系统，其中所述比较装置只有当所述两个检验和相等时，才执行关于费用数据存储装置的按量收费。

数据管理模块、数据复制管理装置以及数据复制管理系统

随着大容量存储介质如*CD—ROM*之类以及高速通信技术如*B—ISDN*等的发展，人们试图使用这些以数字数据的形式分布静止的/运动的图象数据以及计算机程序数据。

尤其是视频介质作品等等，它们已经普遍地作为录象磁带供应，现在也已经以*CD—ROM*的形式出售，并且使用*CD—ROM*的交互性能（双向特性）的游戏软件现在也正出现在市场上。

卫星通信和有线/无线/光通信线路也已付诸商业应用。现在可以通过这些线路，把视频介质作品等传输给用户。

因为这类数字数据可以非常容易地被复制到其它介质上，并且不会象在重复复制模似信号那样降低数据质量；便可以极容易地复制数据而不降低质量。然而，另一方面，作者和数据程序员的利益将由此受到损害。换句话说，只要能提供大容量的光盘和磁盘，就容易用很少的指令知识复制通过*CD—ROM*或通信线路接收到的内容。

通常禁止这类数字数据介质的租借，其理由是因为得不到充分地保护。

此外，例如软件、包括电影、程序等等都是很贵的。通常，只有当用户认为这些的确是他们需要的并且可以在他们自己的硬件上运行时才下决心买它们。

为了应付这种情况，已经实现了一种新的数据分布系统，其中存储着若干附加的功能限制数据的*CD—ROM*被便宜地出售，并且把用来解除这些限制的代码告诉用户，如果他们为其所需的数据付费的话。

然而，已经发现，这种数据分布系统不能充分地反应数据特征。

更具体地说，在发送解除功能限制的代码的系统中，因为用户必须付以费用的总额，所付的费用是非常高的。因而，例如当用户希望一周只看一场电影或只用查表计算软件时，就难于根据利用的量管理费用。

为了解决这种问题，在已公布的被审查的专利申请*No.* 6—19707中披露了一种系统，其中当因使用费用而需要付费时，使用费被预先存储在*IC*卡中。*IC*卡的使用费用被记录在系统中，当软件被使用时，则从使用费余额中由系统减去本次使用的费用。

此外，在本发明的申请人的专利申请*No.* 6—96871中披露了一种系统，它借助于在这种存储介质如*CR—ROM*之类提供一个可重写区，从而进行数据利用时间的管理。

本发明涉及一种可应用于视频作品的数据分布系统的技术，尤其是数字化数据和计算机程序数据。本发明提供一种数据管理系统，它使得具有较好的可靠性，并根据数据利用量更有效地进行费用管理，而又不使数据存储介质复杂化。

本发明的数据管理模块用来选择地复制特定的加密数据(*encrypted data*)，包括字符、图表、图象或声音(加密软件数据)。

这种数据管理模块包括用来输入加密数据的输入部分，特许控制部分，用来对特定的加密数据给以译码特许，译码部分，用来根据

特许控制部分给出的特许，对由输入部分输入的加密数据进行译码，以及输出部分，用来输出经过译码部分译码的数据。

按照本发明，被提供给输入部分的加密数据可以是来自如 *CR—ROM*，*MO* 或类似的存储介质的数据，或通过卫星线路以及地面一般的通信线路收到的数据。关于这类数据，可以用于例如字符、图表、图象和声音以及程序。

译码部分包括所谓的 *DES* 电路（数据加密标准（(*Data Encryption Standard*），并由包括 *CPU* 之类的特许控制部分控制。

译码部分可以配备有方式识别部分，从而可以按照数据特征采用最佳的译码方式。

特许控制部分可以制成使得只有当在费用数据存储部分存在差额时，才使译码部分进行译码。在这种情况下，根据数据复制情况，对于费用数据存储部分执行按量付费。这就是说，特许控制部分执行费用数据存储部分的计数值的减法操作。

因而，按照本发明，不用使数据存储介质复杂化，便能够更好地进行保护管理以及更有效的收费管理。

图 1 是说明本发明原理的方块图。

图 2 是本发明的数据复制装置的功能方块图。

图 3 是表示本实施例的 *DES* 的内部功能的方块图。

图 4 表示各种 *DES* 方式。

图 5 是 *DES* 执行部分的硬件结构方块图。

图 6 是 *DES* 执行部分的处理顺序图。

图 7 是本发明的整个数据分布系统的略图。

图 8 是本实施例的按照费用数据存储部分的差额确定输出的

硬件结构图。

图 9 是本实施例中用于证实要被复制的数据的安全保证的机构方块图。

图 10 是本实施例中用于证实要被复制的数据的安全保证的数据结构方块图。

图 11 是本实施例中的检验和发生部分的功能方块图。

图 12 是表示本发明的按用户需要规则及其技术概念的图。

图 13 是在控制中心和数据复制装置之间加密或检验和共享的一种方块图。

图 14 是在控制中心和数据复制装置这间加密或检验和装共享的一种方块图。

图 15 是在控制中心和数据复制装置之间加密或检验和共享的一种方块图。

图 16 是在控制中心和数据复制装置之间加密或检验和共享的一种方块图。

图 17 是在控制中心和数据复制装置之产加密或检验和共享的一种方块图。

图 18 是在控制中心和数据复制装置之间加密或检验和共享的一种方块图。

图 19 是在控制中心和数据复制装置之间加密或检验和共享的一种方块图。

图 20 是在控制中心和数据复制装置之间加密或检验和共享的一种方块图。

图 21 是在控制中心和数据复制装置之间加密或检验和共享的

一种方块图。

图 22 是在控制中心和数据复制装置之间加密或检验和共享的一种方块图。

图 23 是表示本发明的费用数据存储部分概念的图。

图 24 是以卡的形式制成的数据管理系统的外观图。

在详述最佳实施例之前，首先说明本发明的要点。

图 1 示出了本发明的原理，按照本发明，数据管理模块用来选择性地复制特定的加密数据（加密软件数据），例如字符、图象、声音等等，并根据复制的数据项目、数据数量或复制的时间长短收费。

图 24 所示为管理模块 102 的外形。如图所示，数据管理模块 102 遵从 *PCMCIA* 作成卡的形状。虽然图中没画出，但在其一个端面上有一连接端子，它连接于数据复制装置的槽内。在另一端面上有一电池壳体部分 114 和显示部分 113。

如图 1 所示，被加到输入部分 104 的加密数据可以是来自数据存储介质如 *CD—ROM*101 的数据或通过卫星或一般通信线路接收的数据。关于数据类型，可以使用例如字符、图表、图象之类，当还有程序。

紧接输入部分 104 的一级是译码部分 103，用来对加密数据进行译码。译码部分 103 包括所谓的 *DES* 电路（数据加密标准），并由具有 *CPU* 的特许控制部分 108 所控制。

译码部分 103 可以具有方式识别部分（见图 3），从而根据数据特征在各种译码方式中选择最佳的一种方式。

同时，特许控制部分 108 只有当费用数据存储部分 8 仍然具有剩余的差额时才在译码部分 103 给出特许，以便进行译码。在这种

情况下，按照数据复制情况，费用数据存储部分 8 就执行按量收费。就是说，特许控制部分108 执行费用数据存储部分 8 的计数值的减法操作。

费用数据存储部分 8 的结构示于图 23。如图所示，费用数据存储部分 8 能够以表的形式记录软件 *ID* 和差额。软件 *ID* 是一种指示数据内容的 *ID*；更具体地说，电影之类的名称以代码形式记录在其中。

在特许控制部分 108 中，根据要被译码的量从软件 *ID* 记录的差额中减去相当于译码数据的费用。

当差额为零时，就向输出部分 109 报告说差额已不存在。在输出部分 109，当图象数据被包括在要被输出的译码数据中时，可以在屏幕上迭加上指示没有剩余额差存在的信息。此外，当被译码的数据是音频数据时，可以作为音频信息迭加在要被复制的数据上，报告差额的减少或不足。

此外，当关于软件 *ID* 具有不足的差额时，可以借助于用户预定设定的指令把记录在其它软件 *ID* 中的差额转移到本软件 *ID* 的差额中来。

按照这种方法，按照本发明，特许控制部分 108 和译码部分 103 被置于和数 据复制装置相连的模块 102 内，从而允许非常安全的数据收费。

此外，当费用数据存储部分 8 也被放在模块 102 中时，并关于这费用（用户数据）被输出到外部设备时，借助于提供加密部分进行加密，以改善安全性。译码部分 103 可以起这种加密部分的作用。

此外，借助于对译码部分 103 提供输入输出缓冲器，便可以并

行地执行数据的输入输出，从而实现高速译码。

下面说明最佳实施例。

图 12 表示在由本发明提出的超分布系统中按用户（卖主：控制中心，端点用户：数据复制装置、分布通道）要求的规则以及技术概念。

如图所示，对卖主而言，关于复制保护例如检验码插入、加密技术等是重要的，而对于端点用户而言，通过采用检验和代码而保证数据完整，以及由高速加密技术进行的文件传递和管理是重要的。在另一方面，在分布通道上，数据出售管理功能将起重要作用。本实施例将根据这些要点进行说明。

图 2 是本实施例使用的数据复制装置的功能结构框图。

为了说明方便，假定在本实施例中要被输入的加密数据存储在 *CR—ROM*，*MO* 或类似的介质中。然而，可以使用通过广播卫星线路、地面一般线路通信或光学以及金属的通信线路提供作为通信数据复制的线路。

（数据复制装置的结构）

如图 2 所示，由虚线包围的部分（*SD* 电路 3）表示数据管理模块 102。它可以位于图 24 所示的 *PCMCIA* 卡中，或以板或卡的形式固定在数据复制装置上。

在图中，1 表示解调电路/控制电路，其功能是对存储在 *CD—ROM* 中的 *MPEG* 标准的图象/音频数据进行解调，并把解调过的数据输给译码器 2。

译码器 2 用来执行误差校正和位重排，并以高达 *2MB/sec.*（平均/*MB/sec.*）的速度传递图象/音频数据（加密数据）到 *SD* 电路 3。

在数据管理模块102中，即SD电路3中，通过I/O(5：输入部分104)接收的图象/音频数据(加密数据)被作为译码部分103的DES(数据加密标准)7译码，并通过I/O(6：输出部分109)送到SD电路3外部的解多路复用器13。在解多路复用器13中，音频数据和图象数据被分开，并被送到MPEG处理部分(MPEG—2)。MPEG处理部分(MPEG—2)的功能是扩展被压缩的MPEG标准图象/音频数据，并且当音频和视频被分开并被输出时，借助于同步控制部分(VRC)调节图象数据和音频数据使其同步。

在数据被D/A转换之后，输出给TV监视器或扬声器。

另一方面，当数据输出给计算机(PC)时，MPEG数据可以作为数字数据被输出。当这些数据是程序时，它们可以通过SCST接口输出，这在图中没有示出。

此外，这些数据的传送和接收被数据复制装置内的作为特许控制部分的控制CPU10和SD电路3内的控制CPU4所分担。不过，控制CPU10只能起SD电路3内的CPU4的作用。

对于本实施例中的DES7，使用由？？FIP' SPUB？？制成的？？："46DATA EN CRYPRION STANDARD NIST"?? 而对于MPEG处理部分，则使用ISO/IEC CD13818'1—3"。

(SD电路内部的功能)

在SD电路3中，控制CPU作为特许控制部分108，并识别在DES7中关于由CD—ROM101读出的加密数据是否被允许译码。

当进行这一识别时，控制CPU4首先从CD—ROM101中读出要被复制的软件的ID，然后询问费用数据存储部分8。这时它将进行检查，以便证实它是在费用数据存储部分8中登记的同一个软件

ID。

然 后，只有当在软件 *ID* 的登记区域内还有剩余差额 时，才执行 *DES7* 中的译码。

费用数据存储部分 8 的结构如图 23 所示。如图所示，在费用数据存储部分 8 中可以用表的形式记录软件 *ID* 和差额。软件 *ID* 是指示数据内容的 *ID*；更具体地说就是电影之类的名称，以代码的形式记录在其中。

在特许控制部分108 中，根据要被译码的量从要被译码的软件的 *ID* 中记录的差额中减去相应的量。

然后，在译码期间差额成为零时，就通知输出部分 109，使其进行下面的处理。

例如，当图象数据包括在要被输出的译码数据中时，指示没有剩余差额的信息就被迭加在屏幕上。此外，如果要被译码的数据是音频数据，它们就被迭加在被复制的数据上，并以为音频信息报告差额的减少或不足。

此外，当具有关于软件 *ID* 的不足的差额时，记录在其它软件 *ID* 中的差额可以借助于用户事先设置的指令被转移到当前软件 *ID* 的差额中去。

如图 7 所示，当愿意更新这一差额时，作为卡提供的数据管理模块 102 被带到商店，通过付费使费用数据存储部分 8 中的差额增加。

另外，通过由线路传输接收在财政单位 32 或在控制中心 31 给出的具有电子标记的代码数据表示的费用状态数据，或用电话口头通知，可以增加差额，这些也可以由用户通过键盘 9 输入。借助于电

子标记，使用户 接收到的付费状态数据确保安全。从而不允许用户改变它们。这就是说，控制*CPU*4 证实输入的费用状态数据的电子标记，当其不一致时，它将拒绝在费用数据存储部分 8 中的额外的记录。

此外，根据本发明，费用数据存储部分 8 并不是基本的，收费值数据可被输出到软盘或类似的介质中。不过，当关于费用值数据之类的用户数据被输出到外部时；控制 *CPU*4 将在 *OES*7 中对费用值数据加密，并作为加密数据输出。

这意味着当费用值数据向外部输出时，*DES*7 将作为加密部分。

费用值数据的输出不限于软盘，如图 7 所示，也可以通过通信线输出给控制中心 31。

(*DES* 的详细说明)

图 3 是 *DES*7 的详图。如图所示，*DES*7 包括 *DES* 执行部分 15 (由控制 *CPU*4 执行)，并且由键数据 16 对输入数据(*IN*)译码，并作为输出数据(*OUT*)输出。

在本实施例中，*DES* 执行部分 15 包括方式识别部分 18，它具有从几种 *DES* 方式中选择最佳方式的功能，并将其传递给 *DES* 执行部分 15。

(*DES* 方式的说明)

在 DES 方式中典型的逻辑操作说明如下。

图 4(*a*)表示基本的 *ECB* 方式，其中在 *DES* 执行部分 15 中，借助于 64 位的键数据 16 将 64 位的输入数据串加密(或编码)，并将其作为 64 位的输出数据串。

图 4(*b*)表示 *CBC* 方式，其中在 *DES* 执行部分 15 由 764 位的键

数据 16 对 64 位的输入数据串加密之后，它将被返回并再次被输入到 *DES* 执行部分 15。这是一种借助于反馈来输出最后所得结果的系统，直到所有数据都被输入并适合于文件的数据处理为止。

图 4(*c*)表示 *OFB* 方式，它适用于通信数据，在通信数据中容易产生误差，其中的音频数据的误差对其它具有大的影响。

图 4(*d*)表示 *CFB* 方式，它适用于自同步型数据。

方式识别部分 18借助于分析数据形式等等从存储在方式表 20 中的方式当中读出最佳的方式，并将其送入 *DES* 执行部分 15。在 *DES* 执行部分 15，根据选择的方式进行加密/编码。

(*DES* 执行部分高速的算术处理)

图 5 是 *DES* 执行部分 15 的硬件结构框图。

图中，在输入侧设置有 64 位的作为输入缓冲器的位移寄存器(输入寄存器 21：*REG*1)，它是 64 位的，具有 8 个 8 位的相连的寄存器，与其相邻设置有选择器 *se*1。选择器 *se*1 选择来自 *DES* 处理主电路 25(下文说明)的输出或选择来自位移寄存器 21 的输出作为它的输入。

和选择器 *se*1 相邻设置的是 8 位的寄存器 23(*REG*2)，与其相邻的部分是 *DES* 处理主电路 25。*DES* 处理主电路作为 *DES* 执行部分 15。这就是说，在 *DES* 处理主电路 15 中，上面参照图 4 所述的各种 *DES* 方式作为 *ROM*(只读存储器)被记录，借助于来自控制 *CPU*4 的指令，选择最佳 *DES* 逻辑，并进行译码。

D ES 处理主电路 25 的输出被分支到选择器 *se*1 和作为输出缓冲器的输出寄存器 24(*REG*3)。然后，输出寄存器 24(*REG*3)和输出被用作最后的加密的或译码数据。

这一处理的顺序如图 6 所示。

在图 6 中，对输入寄存器 21 的输出，在来自寄存器 23 输出的下一周期第一个时钟定时进行 *DES* 处理。然后，在下一个时钟定时，它被从寄存器 24 中输出。在输出寄存器 24 输出的时刻，在输入侧，下一周期的加密数据将从输入寄存器 21 中取出。

用这种方式，按照本实施例，借助于提供输入寄存器 21 作为输入缓冲器以及提供输出寄存器 24 作为输出缓冲器，便能独立地且连续地进行加密数据的输入和译码数据的输出。这样，它可以用比常规情况下高的速度进行加密和编码，在常规情况下，输入和输出是在 *DES* 周期地进行转换的。

（本发明的数据分布状况的完整图）

图 7 所示为本发明所要实现的数据分布状况的完整图的一个例子。

在本实施例中，数据从运送中心(这里为了方便，假设控制中心也可以起运送中心的作用）以存储在 *CD—ROM* 中的加密数据的形式被运送到分布通道。

端点用户到商店 27 购买（可能邮寄）作为数据存储介质 101 的 *CD—ROM*。与此同时，端点用户购买以卡的形式制成的作为 *SD* 卡的数据管理模块 102。

若干加密的软件数据存储在 *CD—ROM* 中。更具体地说，按照本发明存储在 *CD—ROM* 中的数据都是加密的，当对其进行译码和复制时，基本的是使用作为数据管理模块 102 的 *SD* 卡以确保安全。此外，*SD* 卡配置有根据要被使用的数据量的费用收集系统。这样在其它介质上复制存储在 *CD—ROM* 内的加密数据本身是没有意义

的，当采用 *CD—ROM* 租借系统时，如果根据要被使用的量提供费用收集系统，便不会减少数据提供者的利益。

当用户愿意用自己的数据复制装置 15 复制存在 *CD—ROM* 中的数据时，他必须首先在卡驱动装置 28 中插入 *SD* 卡(102)并在数据复制装置 105 上装上 *CD—ROM*(101)。

然后借助于起动装在数据复制装置 105 中的通信功能(这功能可作为一种操作功能提供)，端点用户将通过家用电话 30 从装在数据复制装置 105 中的调制器中向控制中心 31 发出请求，要求使用所需的软件数据。接着，控制中心 31 向用户的数据复制装置 105 发出由加密特许指令(键数据)构成的数据。

已经收到特许指令的数据复制装置 105 读 *CD—ROM*101，并通过 *SD* 步的译码部分 103 对所需数据按顺序译码。

与此同时，控制 *CPU* 将对译码的数据量进行计数，或对译码用的时间进行计数，并从费用数据管理存储部分 8 中减去相应于软件 *ID* 的值。然后，除非到其差额为“0”时，将一直连续地进行加密数据的译码。

当费用管理存储部分的差额值为“ 0” 时，则终止译码数据的输出。实现这一终止的硬件结构示于图 8。

在图 8 中，当在费用数据存储部分中的差额为“0”，并检测到这一情况时，一直监视着费用数据管理部分 8 的控制 *CPU*3，将把这数据报告给数据复制装置 105 中的控制 *CPU*10。根据这个报告，控制 *CPU*10 改变保持在寄存器 81 中的值，并关闭 *TV* 监视器和计算机(*PC*)输出级的 *AND* 电路(*AND*83)和模拟开关(*SW*82)。这样，即使图象数据被包括在该数据中，任何转换成模拟数据的音频数据也

将被送到输出装置中。

此外，图象数据的输出可被转换到其它的图象数据。另外，另一种图象数据可被迭加到原先的图象上。

在至此所作的说明中，根据的是差额由 *SD* 电路 3 中的费用数据存储部分 8 管理的情况。不过，这收费值差额可由控制中心 31 管理。在这种情况下，当费用值差额数据被输出到数据复制装置 105 的外部时，控制 *CPU* 将使用 *DES7* 对费用值差额数据进行加密，从而增加安全性，并通过电话线作为加密数据通知控制中心 31。

控 制中心 31 将根据接收到的来自数据复制装置 105 费用值差额数据，在财政单位 32 从端点用户的帐号中接受相应于使用量的费用，并将其送到数据提供者的帐号上。

这样，按照本发明，因为不仅存储在 *CR—ROM* 中的数据，而且由操作该数据产生的用户数据被加密之后向外输出，就能够防止借助于改变用户数据进行的数据非法使用。

（运送数据的安全保证）

因为在数据分布通道中，数据有可能混有病毒，使端点用户可能复制带有病毒的数据，从而使他已经存储的数据或硬件被破坏，甚至使其为因有病毒而不能操作的数据付费。

图 9 表示能够检测数据复制装置 105 的分布通道中病毒侵入的结构。

具体地说，控制中心 31 具有检验和发生部分 111*a*。它具有由要被运送的数据产生检验和（*CS*）的功能，即产生检验数据安全性的代码。在本实施例中，通过散列（*hash*）函数使功能代码作为检验和（*CS*）输出。

这种检验和发生部分111*a*的逻辑发图11所示。即，在通过*DES*加密执行操作的情况下，将基本上采用*CBC*方式(图4(*b*))，程序或数据将被1块单位(1 *block units*)划分，曾经由*CBC*方式(块返回)输出的数据将被返回，并被当作输入，并用下一个输入块执行异或控制(*EOR*)。其结果再次被输入*DES*加密，并把其输出返回到输入端，和上述的情况类似。然后，当输入最后块时，被转换并加密的输出将被用作检验和(*CS*)。

图10是一种步骤图。其中当源程序通过编辑变成目标程序之后被压缩，并把压缩的句子目标程序输入给散列函数*h*(在检验和发生部分111*a*处理过的)，得到检验和(*CS*)，并使其和压缩的句子目标程序结合。

当这种加密程序通过分布通道混入计算机病毒时，借助于下面说明的数据复制装置105中的机构可以容易地证实病毒的侵入。

更具体地说，数据复制装置105具有和111*a*类似的检验和发生部分111*b*，用和上述相同的方法从数据中产生检验和(*CS'*)。然后在比较部分112，附加在数据上的检验和(*CS*)和在检验和发生部分111*b*所产生的检验和(*CS'*)进行比较。

此时，当病毒混入通过分布通道的数据中并且因此数据被改变时，在检验和发生部分111*b*发生的检验和(*CS'*)自然和原来的检验和*CS*)不同。

因而，当比较部分112检测出异常结果时，在显示部分113上就显示出指示异常情况的红色。这显示可以通过在数据管理模块102(见图24)的一端提供显示灯113来容易地实现，数据管理模块102例如可以以卡的形式构成，借助于开关装置(*SW*)可以改变显示状

态。在处理检验和发生部分 111*b* 的期间内，则显示表明目前正进行处理的黄色，当比较结果基本正常时，则显示兰色。

然后，只有当在比较部分 112 的比较处理正常结果时，才从费用数据存储部分 8 中执行按量收费。更具体地说，特许控制部分 108（在图 9 中未示出）将进行从费用数据存储部分 8 中减去相应的费用。

检验和发生和参照图 9、10 所说明的加密之间的关系如图 13 至 22 所示。在这些图中，假设数据存储在 *CD—ROM* 中，并且由数据提供者（控制中心）供给端点用户（数据复制装置）。

在图 13 中，用 131*a*、131*b* 和 131*c* 表示的是在装置中（*RAM* 或硬盘）形成的逻辑介质。相对地，用 132 表示的是物理介质，包括 *CD—ROM*、*MO*、*Write—once DVD* 或 *IC* 卡等。

通过使用键数据（K1）由句子的数据（存储在 *RAM* 或硬盘中的）产生检验和，并被存储在 *CD—ROM* 的特定区域中。然后，使用键数据（K2）对句子数据加密，并被存储在 *CD—ROM* 上的不同于存储检验和（*CS*）的区域中，并被提供给端点用户。端点用户用键数据（K2）对加密的数据译码，同时执行标题分析，并把其暂时存储在存储器或其它存储装置中。然后，使用键数据（K1）从被译码的句子数据中产生检验和，并把其和从 *CD—ROM* 中读出的检验和进行比较。然后，只有当它们一致时，才执行收费处理。

图 14 表示在图 13 的例子中在数据提供者处（控制中心）不进行加密处理的情况。

在图 14 中，由标号 141 指示的是在装置（*RAM* 或硬盘之类）中形成的逻辑介质，与此相对，标号 142 表示物理介质，其中包括 *CD*

—*ROM*,*MO*,*Write—onc* *DVD* 或 *IC* 卡等。

在图 15 中，标号 151*a*、151*b* 指示的是在装置(*RAM* 或硬盘等)中形成的逻辑介质。与此相对，标号 152 表示物理介质，其中包括 *CD—ROM*、*MO*、*Write—once* *DVD* 或 *IC* 卡等。

如图 15 所示，由加密数据产生检验和。就是说，句子数据首先由键数据(K2)加密，并被存储在 *CD—ROM* 中。然后由加密的数据产生检验和，并把其存储在特定的区域中供给端点用户。

在端点用户例，在执行标题分析时，从加密数据直接地产生检验和，并把它和存储在 *CD—ROM* 中的检验和进行比较。

在图 16 中，标号 161*a*、161*b* 和 161*c* 是在装置(*RAM* 或硬盘)中形成的逻辑介质。与此相对，标号 162 是物理介质，包括 *CD—ROM*,*MO*,*Write—once* *DVD* 或 *IC* 卡等。

虽然在数据提供者(控制中心)一侧的处理和图 13 所示的相似，但在端点用户侧(数据复制装置侧)的费用处理是不同的。即费用处理通过标题分析开始，并且当比较检验和的结果表明它们不一致时，费用处理就被无效(旧状态返回重写)。

在图 17 中，标号 171*a* 表示在装置(*RAM* 或硬盘等)中形成的逻辑介质。与此相对，标号 172 表示物理介质，其中包括 *CD—ROM*,*MO*,*Write—once* *DVD* 或 *IC* 卡等。

虽然在数据提供侧(控制中心)的处理和图 14 所示的相似，但在端点用户侧(数据复制侧)的费用处理是不同的。即费用处理通过标题分析开始，并且如果比较检验和的结果表明它们不一致时，费用处理就被取消(旧状态返回重写)。

在图 18 中，标号 181*a* 和 181*b* 表示在装置(*RAM* 或硬盘)中形

成的逻辑介质。与此相对，标号 182 表示物理介质，其中包括 *CD—ROM，MO，Write—once DVD* 或 *IC* 卡等。

虽然在数据提供者一侧(控制中心)的处理和图 15 中的类似，但在端点用户侧(数据复制装置侧)的费用处理是不同的。即根据比较的结果执行费用处理，并由此起动费用处理译码。

在图 19 中，标号 191*a* 和 191*b* 是在装置(*RAM* 或硬盘等)中形成的逻辑介质。与此相对，标号 192 是物理介质，其中包括 *CD—ROM，MO，Write—once DVD* 或 *IC* 卡等。

虽然在数据提供者侧(控制中心)的处理和图 16 所示的相似，但在端点用户侧(数据复制装置侧)的费用处理是不同的。即，费用处理根据标题分析的结果开始，并且当比较检验和的结果表明它们不一致时，费用处理将被无效(旧状态返回重写)。

在图 20 中，标号 201*a* 代表装置(*RAM* 或硬盘等)中形成的逻辑介质。与此相对，标号 202 是物理介质，其中包括 *CD—ROM，MO，Write—once DVD* 或 *IC* 卡等。

虽然在数据提供侧(控制中心)的处理和图 15 表示的相似，但是在端点用户侧(数据复制装置侧)的费用处理是不同的。即费用处理由标题分析开始，并且当比较检验和的结果表明它们不一致时，费用处理将被无效(旧状态返回重写)。

在图 21 和 22 中，标号 210、220 是物理介质，其中包括 *CD—ROM，MO，Write—once DVD* 或 *IC* 卡等。

费用处理在标题分析的同时开始，如果比较结果表明它们不一致，费用处理将被无效(旧状态返回重写)。

如上所述，在图 9 到 22 所示的例子中，因为容易证实数据的可

靠性，所以能够防止破坏硬件或数据以及由复制混有病毒的数据引起的不公平的收费。

（控制中心进行的数据租借时间管理）；下面说明由控制中心31操作的数据利用时间管理的情况。

控制中心31对数据复制装置105发出特许指令，根据软件，对利用开始时间（时间标记）进行加密，并通过通信线（或通过调制解调器）把它送到数据复制装置105。

在数据复制装置105中，当收到这个时间标记时，由它自己的*SD*电路3进行译码，并写进费用数据存储部分8中。此时，如图23所示，如果费用数据差额值对每个软件都被设定，则对应于该软件*ID*写入时间标记。

用这种方式，通过管理时间标记，就可以管理端点用户的数据利用时间。

此外，加密的时间标记可以在控制中心31由操作员口头传递给端点用户，端点用户可把它通过键盘输入到自己的数据复制装置105中。此时，如果用户非法地改变时间标记，则会由*SD*电路3的控制*CPU*检测到，使软件的译码被拒绝。

这样，因为时间标记被加密，并且只作为无意义的数字串呈现于用户；对它的分析是困难的，因而保证了收费的可靠性。

此外，在上述的实施例中，无须说明，要被提供给数据复制装置105的数据不仅包括存储在有形的介质如*CD—ROM*之类中的数据，而且也包括通过高速通信系统从计算机获得的通信数据。

图. 1

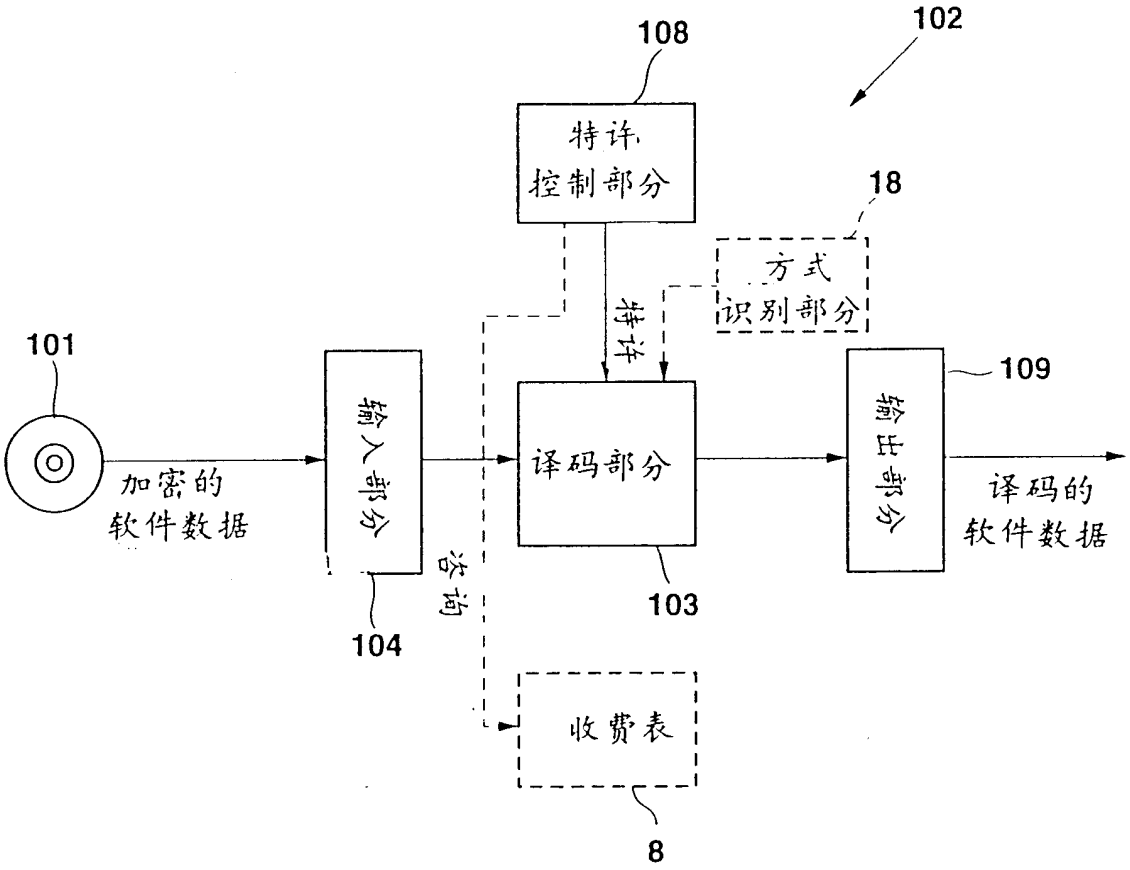

102
108
特许
控制部分
18
方式
识别部分
特许
101
输入部分
译码部分
109
输出部分
加密的
软件数据
译码的
软件数据
咨询
103
104
收费表
8

图. 2

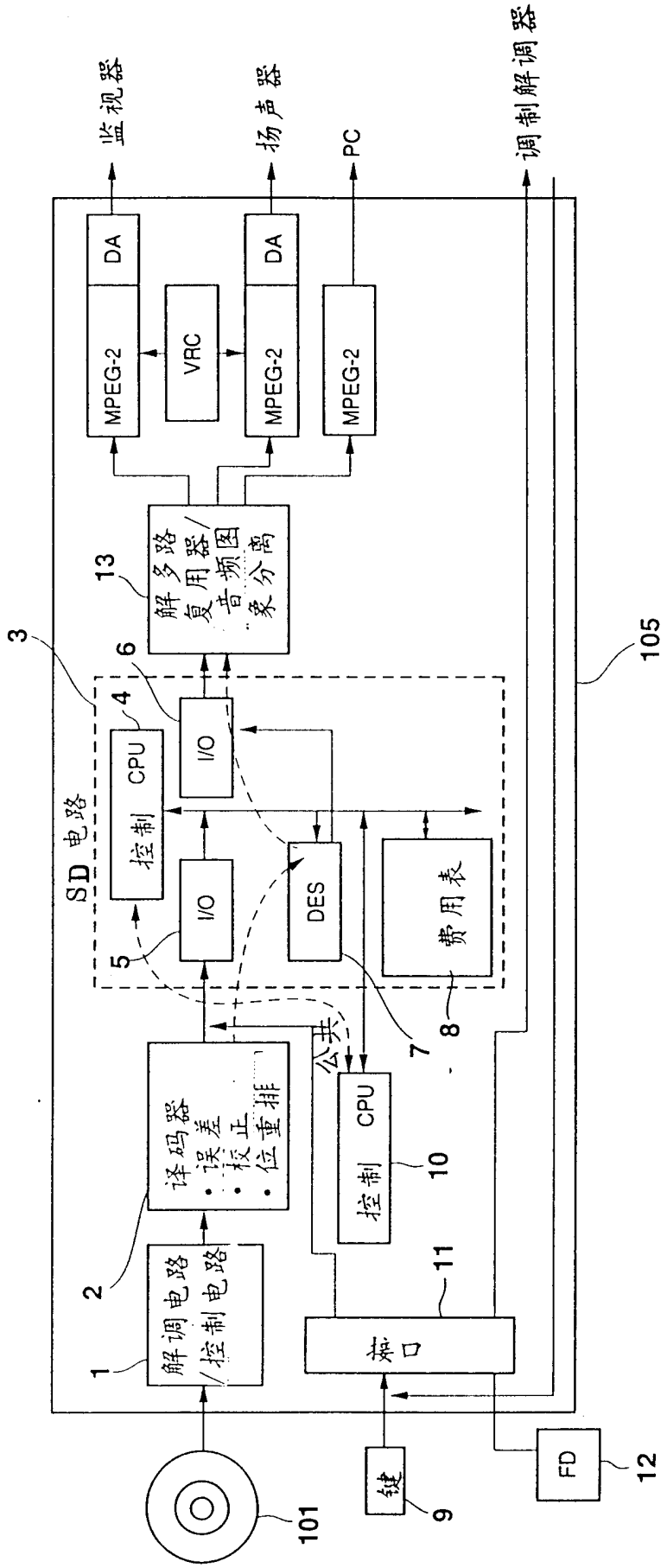

监视器
扬声器
PC
调制解调器
DA
DA
MPEG-2
VRC
MPEG-2
MPEG-2
解多路复用器/音频图象分离
13
3
6
4
SD 电路
控制 CPU
I/O
I/O
DES
费用表
5
7
8
公共
105
译码器
• 误差
• 校正
• 位重排
2
解调电路/控制电路
1
控制 CPU
10
11
端口
键
9
FD
12
101

图. 3

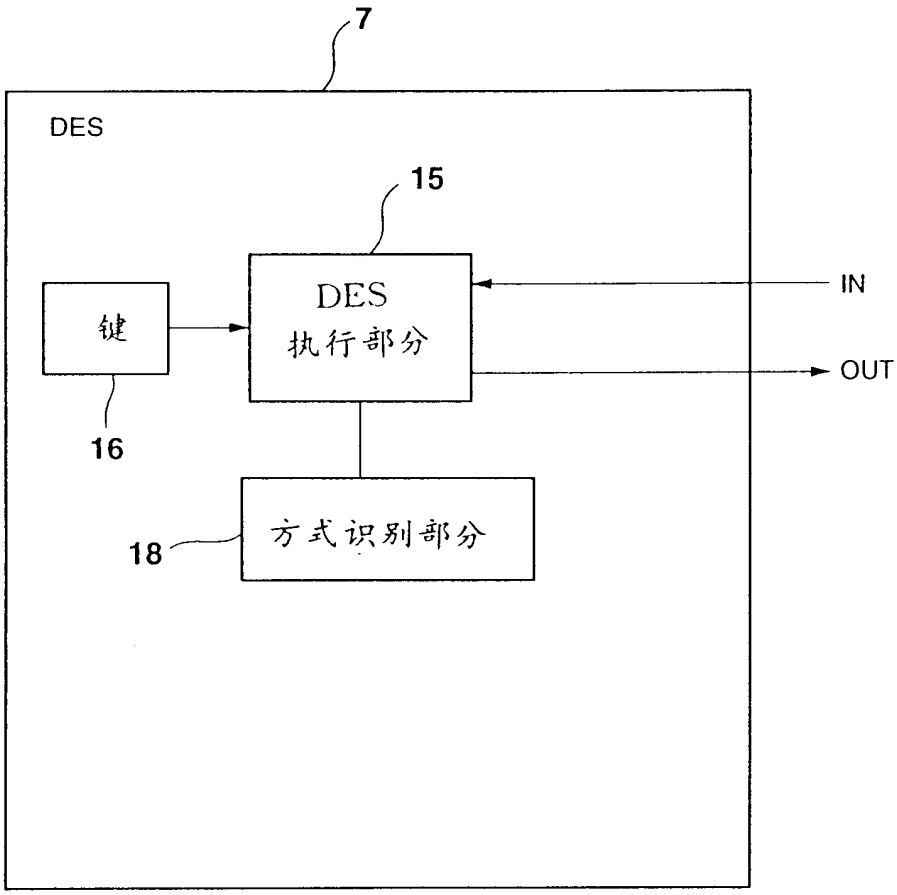


图. 4 A

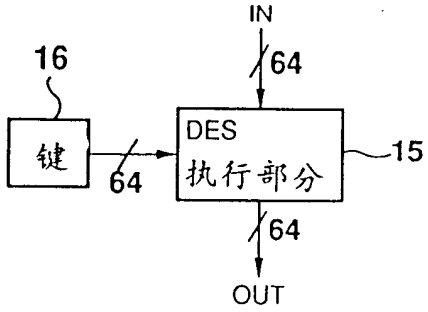


图. 4 B

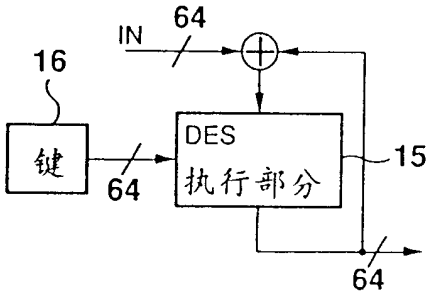


图. 4 C

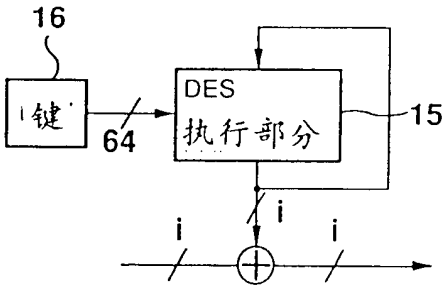


图. 4 D

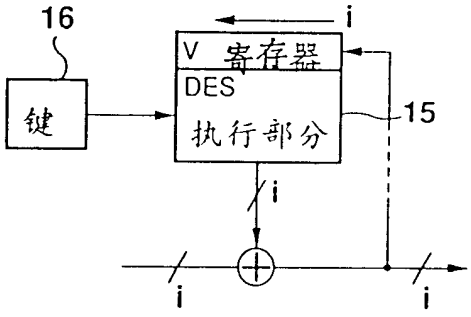


图. 5

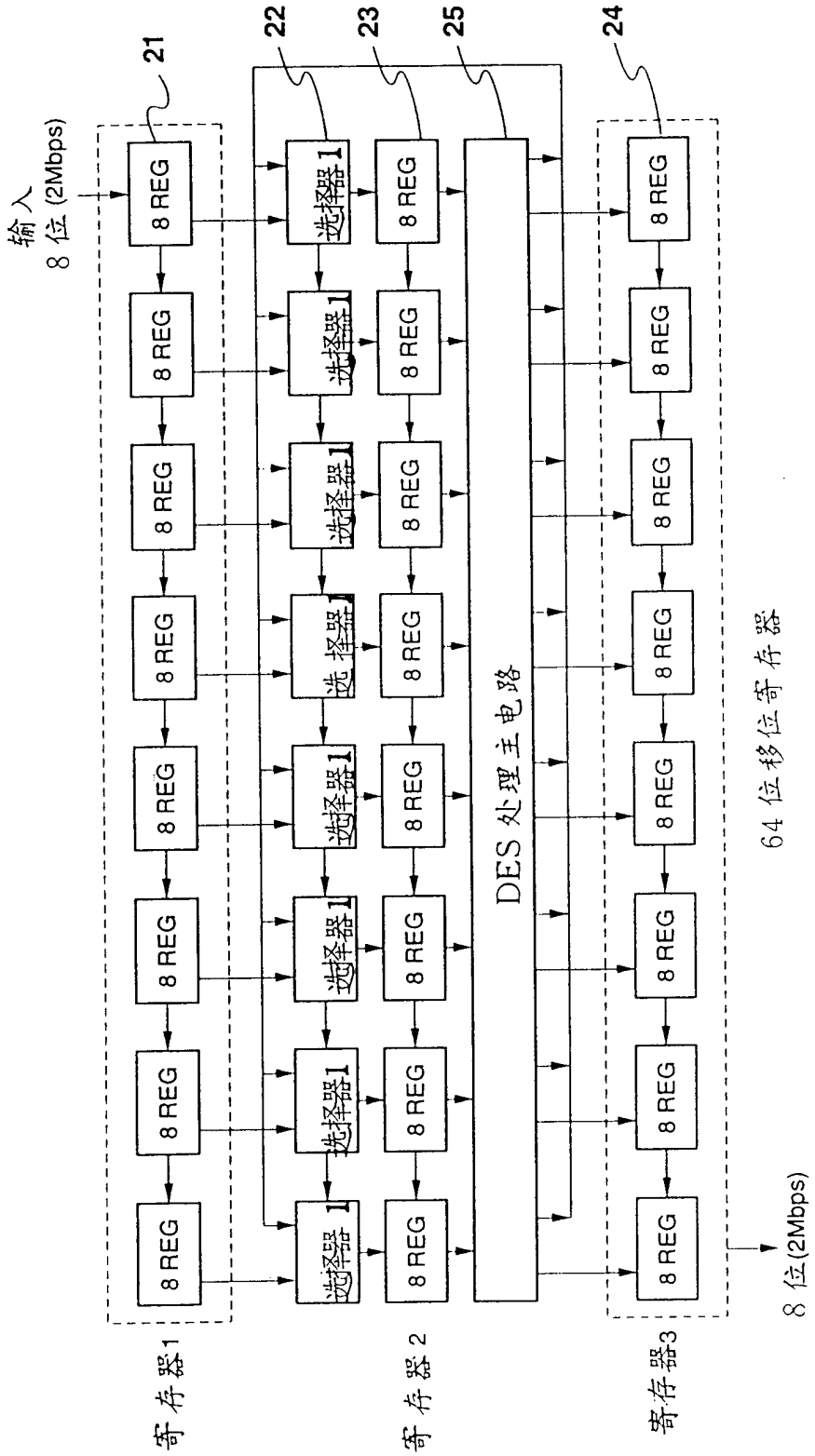

输入
8 位 (2Mbps)
21
22
23
25
24
8 REG
选择器 1
DES 处理主电路
64 位移位寄存器
8 位(2Mbps)
寄存器1
寄存器 2
寄存器3

图. 6

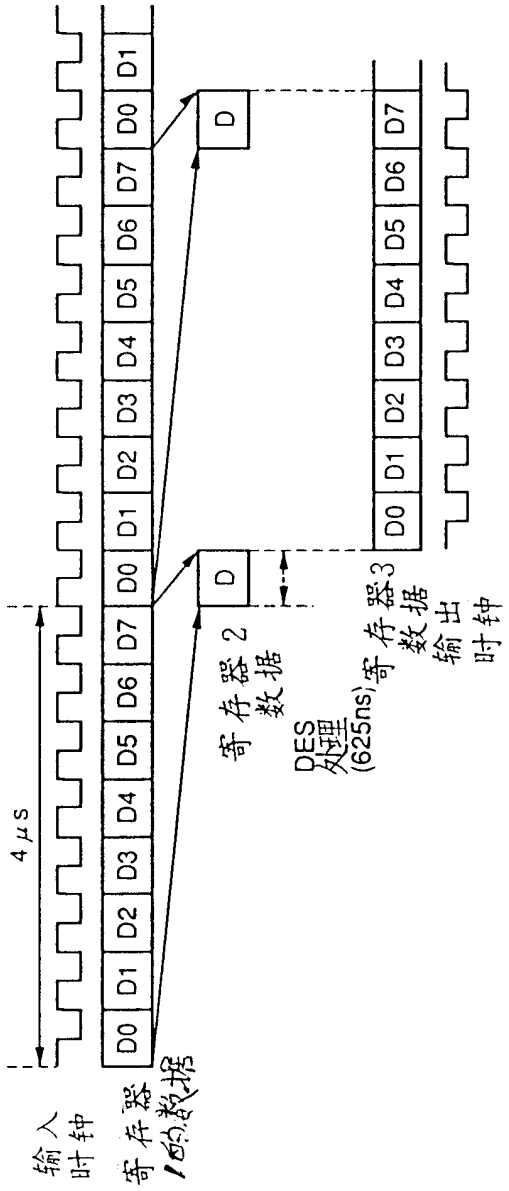

4 μs
输入时钟
寄存器1的数据
D0 D1 D2 D3 D4 D5 D6 D7
D
寄存器2数据
DES处理(625ns)
寄存器3数据输出时钟
D0 D1 D2 D3 D4 D5 D6 D7

图. 7

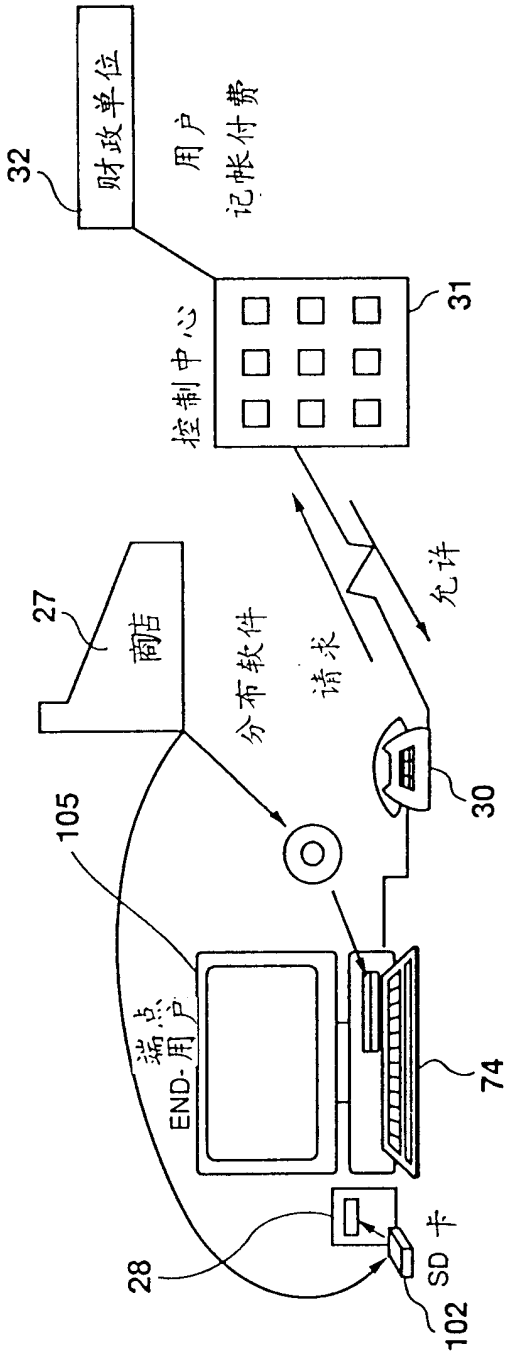

32
财政单位
用户
记帐付费
控制中心
31
27
商店
分布软件
请求
允许
105
30
端点
END-用户
74
28
SD 卡
102

图. 8

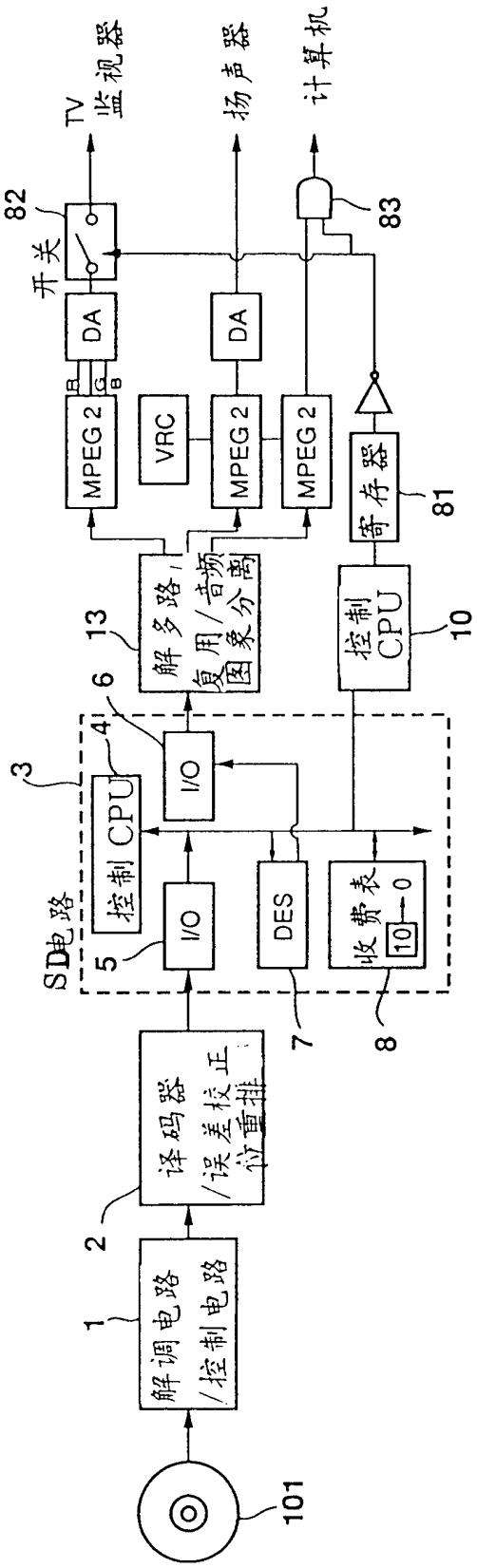

101
解调电路/控制电路
1
译码器/误差校正/分重排
2
SD电路
3
控制 CPU
4
I/O
6
5
I/O
DES
7
收费表
10
8
解多路/音频/图象分离
13
控制 CPU
10
寄存器
81
MPEG 2
VRC
MPEG 2
MPEG 2
DA
DA
开关
82
83
TV 监视器
扬声器
计算机

图. 9

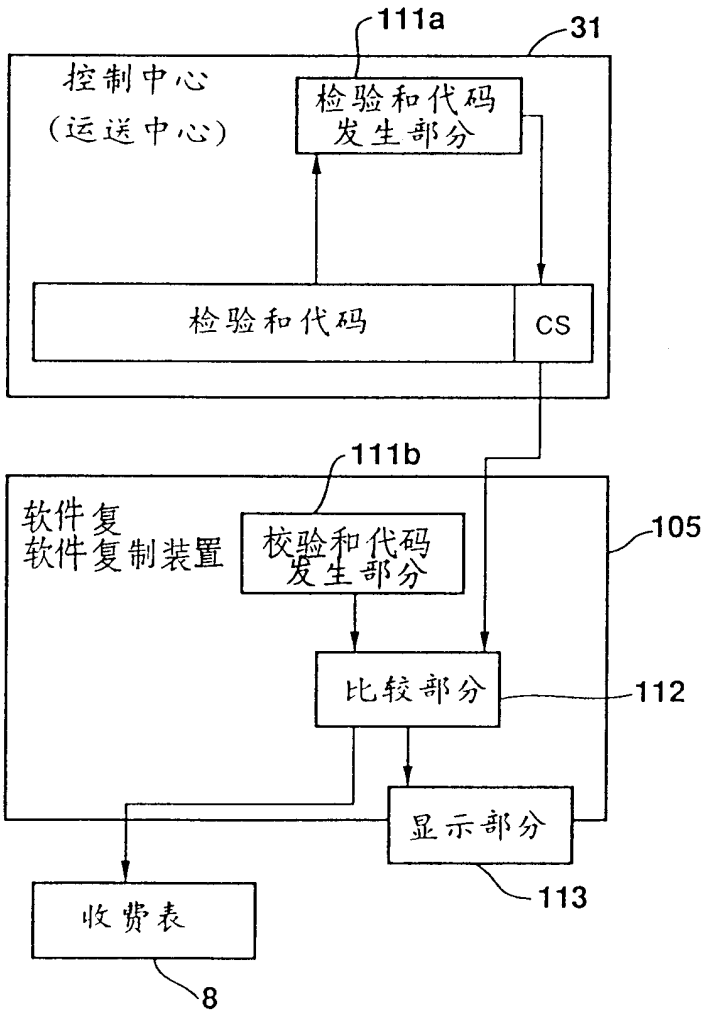

111a
31
控制中心
(运送中心)
检验和代码
发生部分
检验和代码
CS
111b
软件复
软件复制装置
校验和代码
发生部分
105
比较部分
112
显示部分
113
收费表
8

图. 10

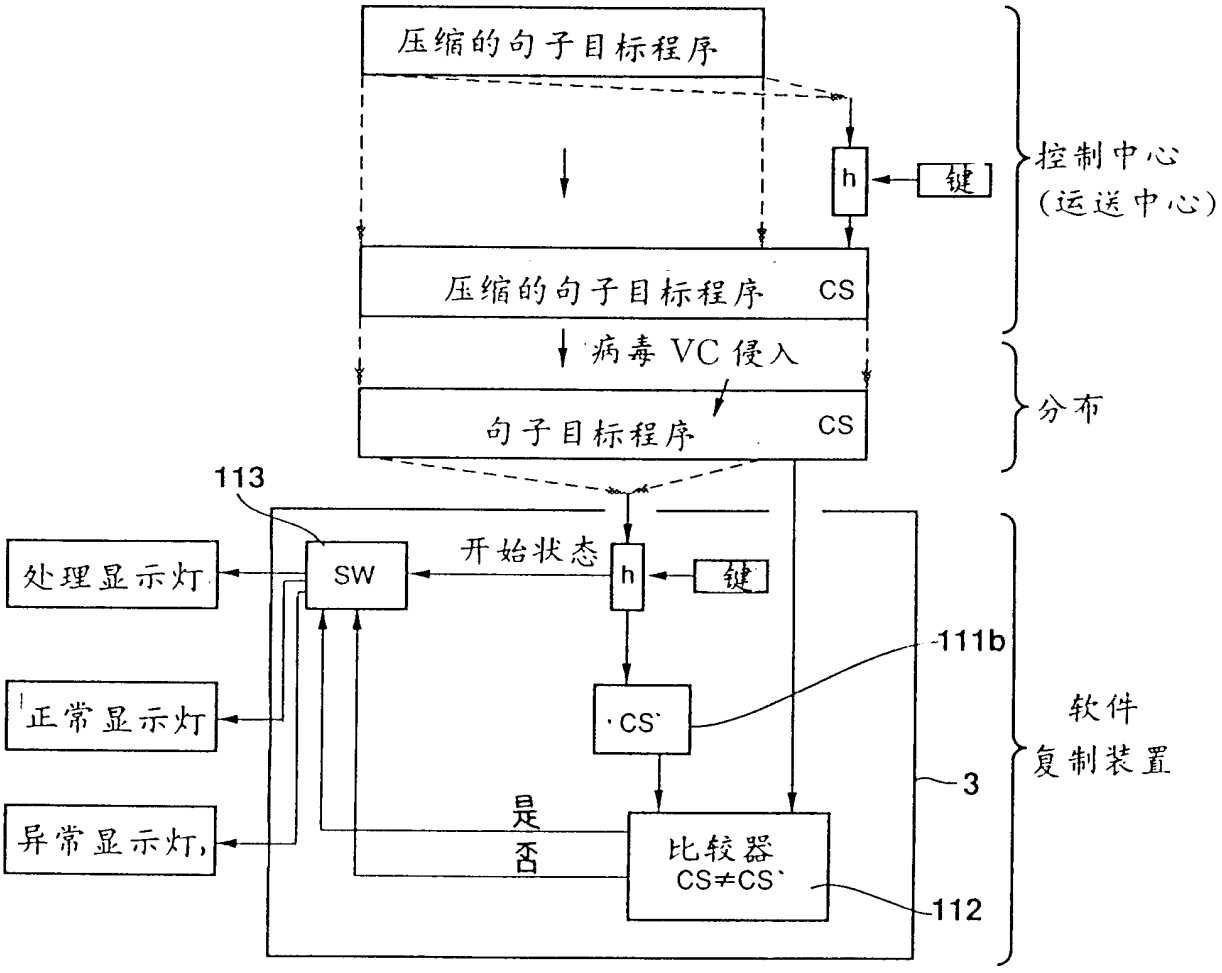

压缩的句子目标程序
h
键
控制中心
(运送中心)
压缩的句子目标程序 CS
病毒 VC 侵入
句子目标程序 CS
分布
113
处理显示灯
SW
开始状态
h
键
正常显示灯
CS`
111b
软件
复制装置
3
异常显示灯
是
否
比较器
CS≠CS`
112

图. 11

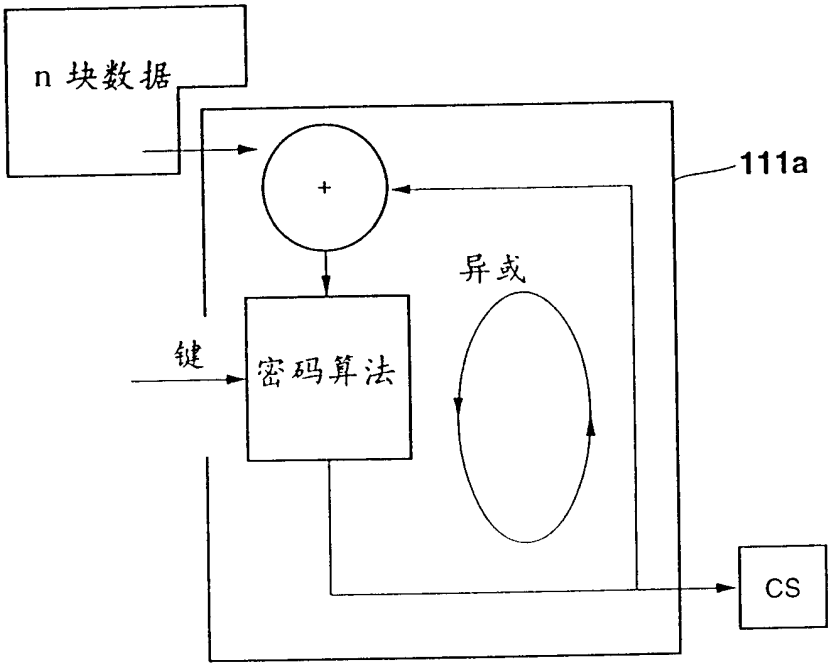

n 块数据
+
111a
异或
键
密码算法
CS

图12

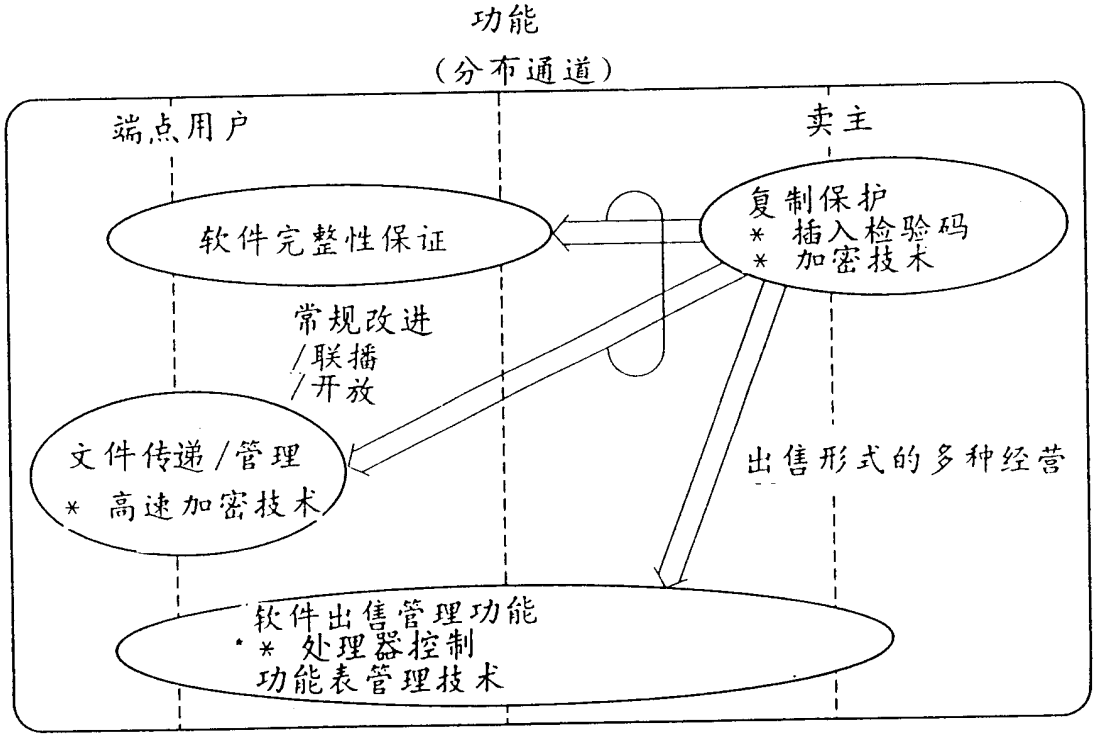

功能
(分布通道)
端点用户
卖主
软件完整性保证
复制保护
* 插入检验码
* 加密技术
常规改进
/联播
/开放
文件传递/管理
* 高速加密技术
出售形式的多种经营
软件出售管理功能
* 处理器控制
功能表管理技术

图. 13

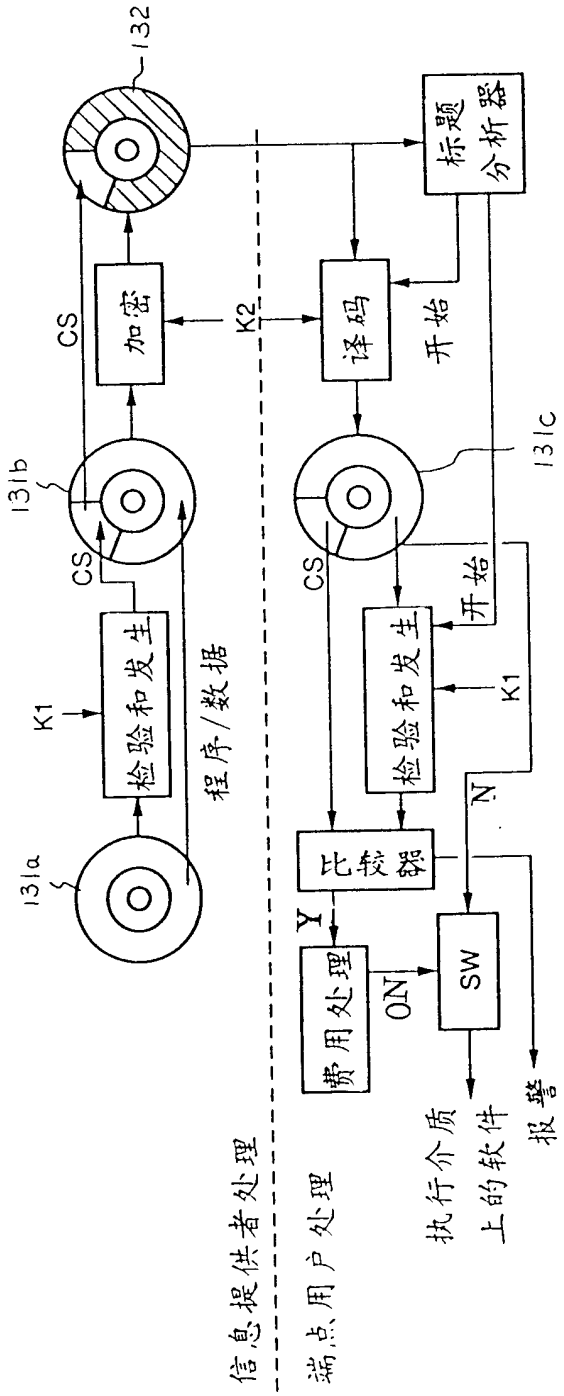

132
CS
加密
K2
译码
标题
分析器
开始
131b
CS
131c
CS
K1
检验和发生
程序/数据
检验和发生
开始
K1
131a
比较器
N
Y
费用处理
ON
SW
执行介质
上的软件
报警
信息提供者处理
端点用户处理

图. 14

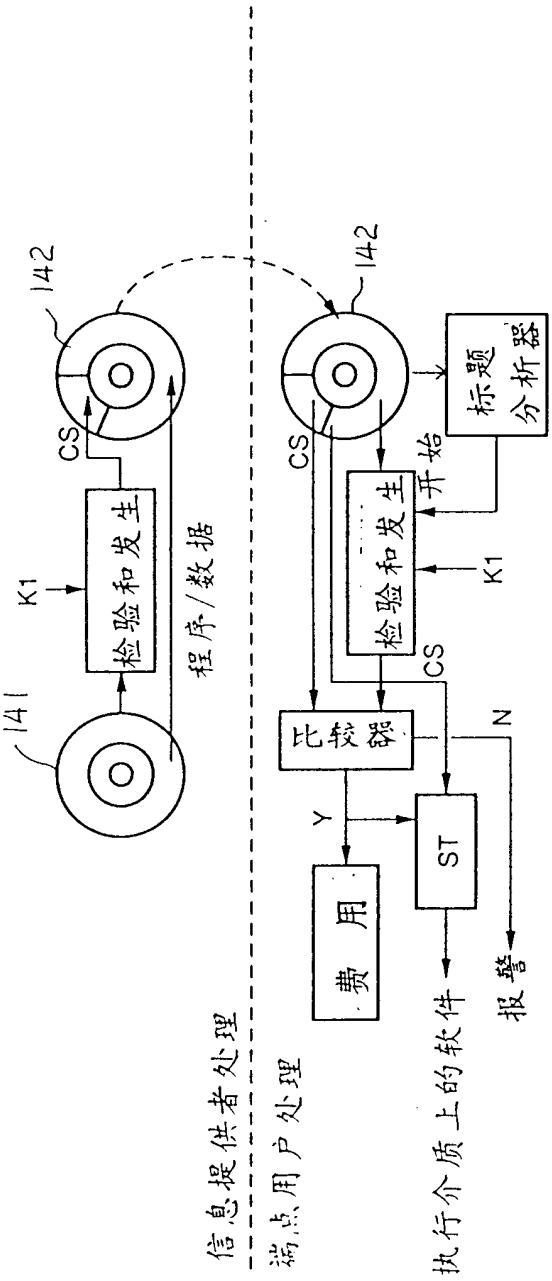

141
142
K1
检验和发生
CS
程序/数据
信息提供者处理
端点用户处理
142
CS
标题分析器
开始
检验和发生
K1
CS
比较器
N
Y
费用
ST
执行介质上的软件
报警

图. 15

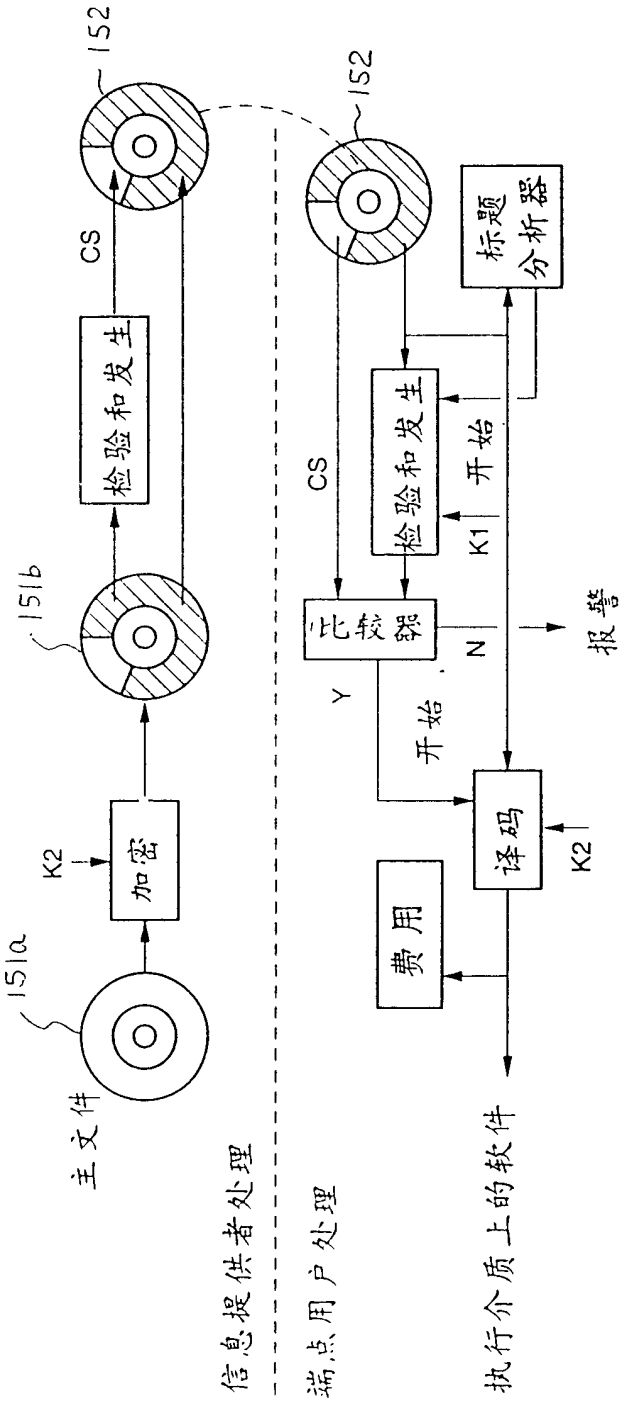

主文件
1510
加密
K2
1516
检验和发生
CS
152
信息提供者处理
端点用户处理
152
CS
检验和发生
K1
开始
比较器
N
Y
报警
开始
费用
译码
K2
标题分析器
执行介质上的软件

图. 16

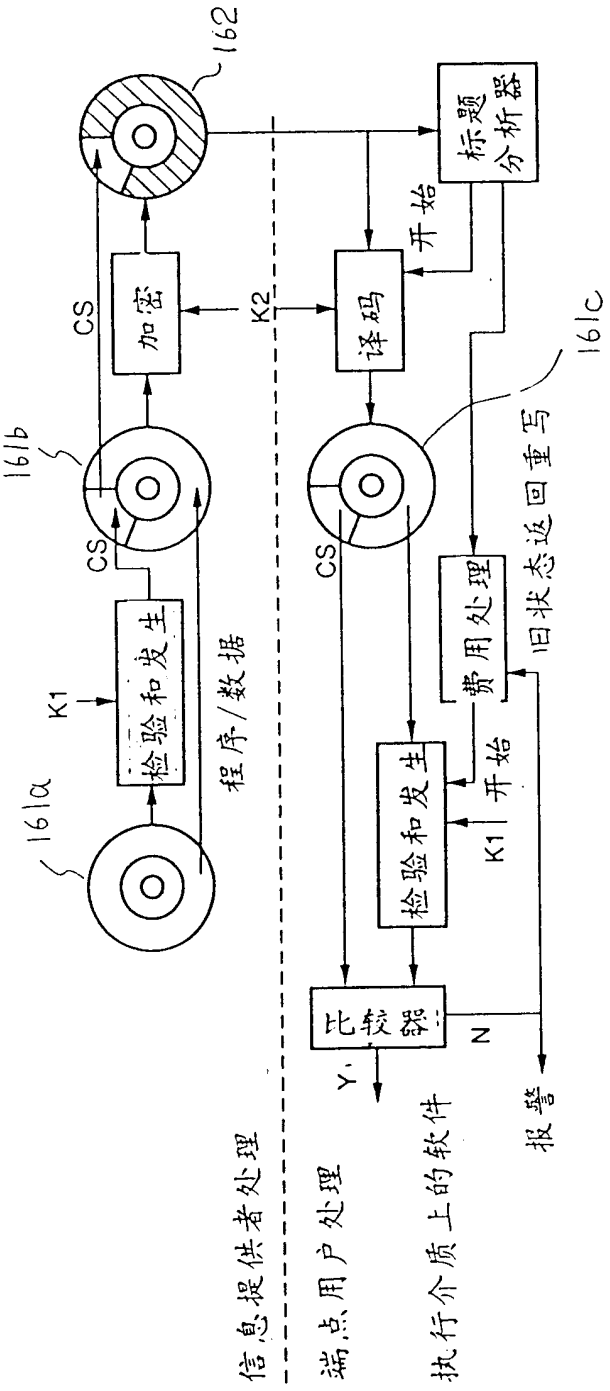

信息提供者处理
端点用户处理
执行介质上的软件
程序/数据
161a
161b
161c
162
K1
K2
CS
检验和发生
加密
译码
标题分析器
开始
费用处理
旧状态返回重写
比较器
Y
N
报警

图. 17

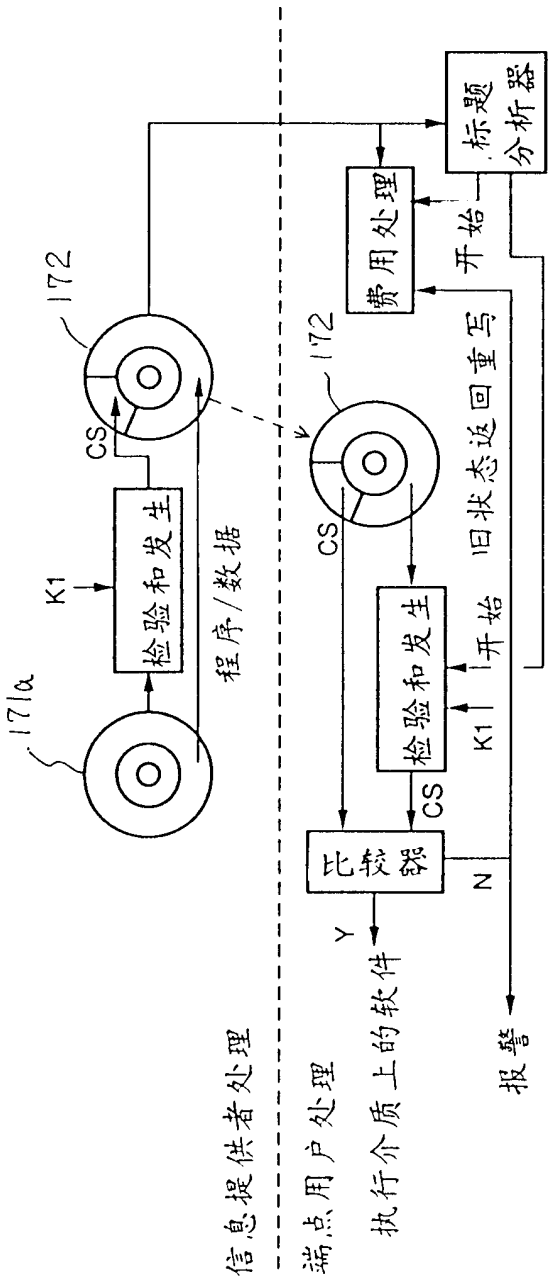

信息提供者处理
端点用户处理
171a
172
CS
K1
检验和发生
程序/数据
172
CS
费用处理
标题
分析器
开始
旧状态返回重写
检验和发生
K1
开始
CS
比较
N
Y
执行介质上的软件
报警

图. 18

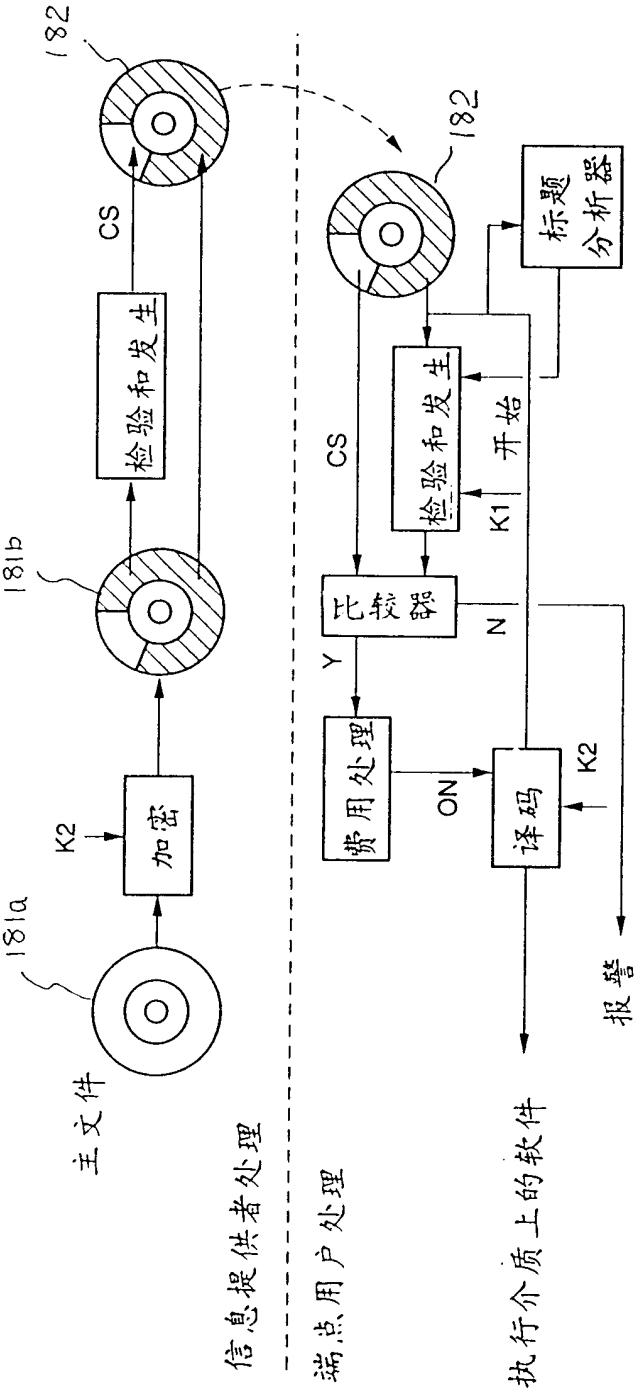

主文件
181a
K2
加密
181b
检验和发生
CS
182
信息提供者处理
端点用户处理
执行介质上的软件
CS
182
检验和发生
K1
开始
比较器
Y
N
费用处理
ON
译码
K2
报警
标题分析器

图. 19

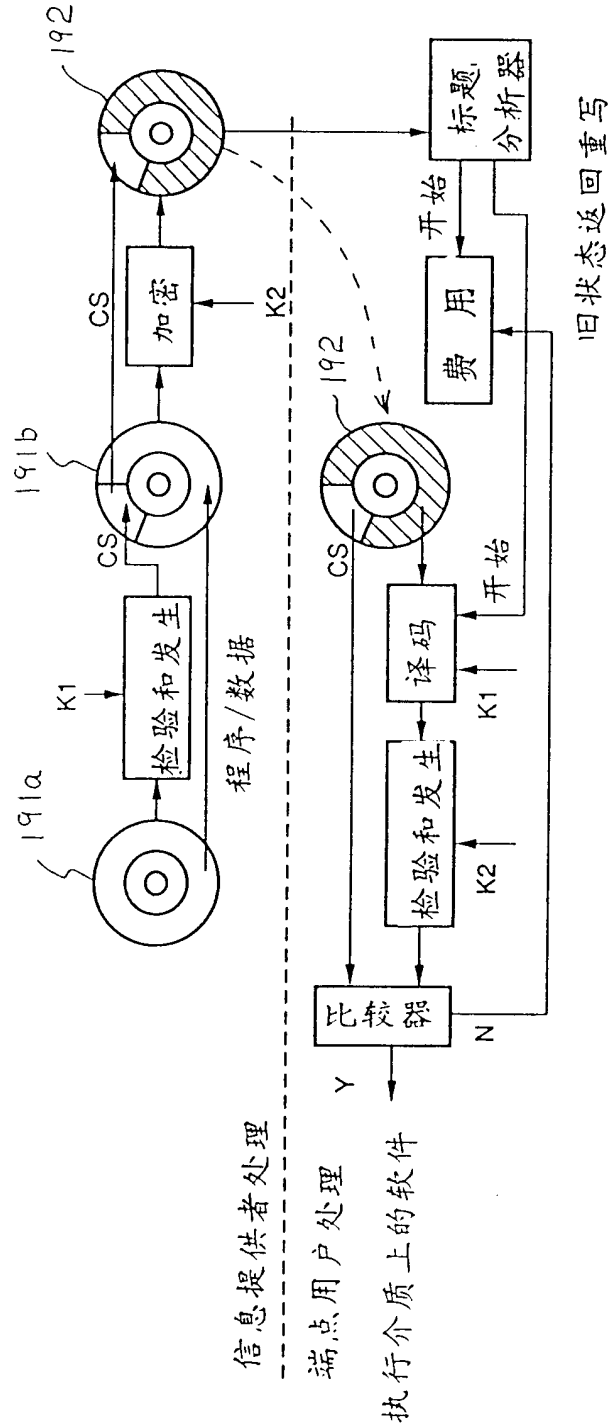

192
标题分析器
开始
费用
K2
加密
CS
191b
K1
检验和发生
191a
程序/数据
192
CS
开始
译码
K1
检验和发生
K2
比较器
N
Y
信息提供者处理
端点用户处理
执行介质上的软件
旧状态返回重写

图. 20

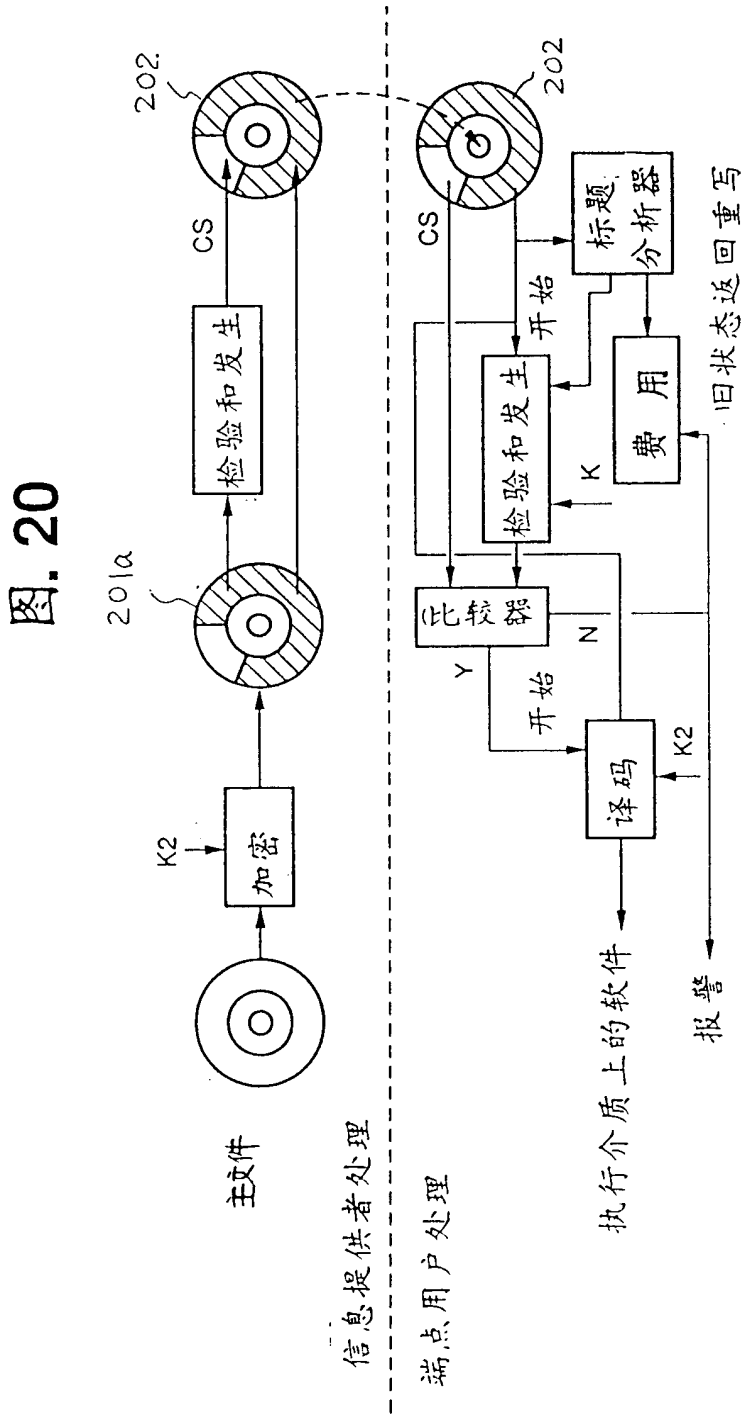

202
CS
检验和发生
201a
K2
加密
主文件
信息提供者处理
端点用户处理
202
CS
标题分析器
开始
检验和发生
K
费用
旧状态返回重写
比较键
N
Y
开始
译码
K2
执行介质上的软件
报警

图. 21

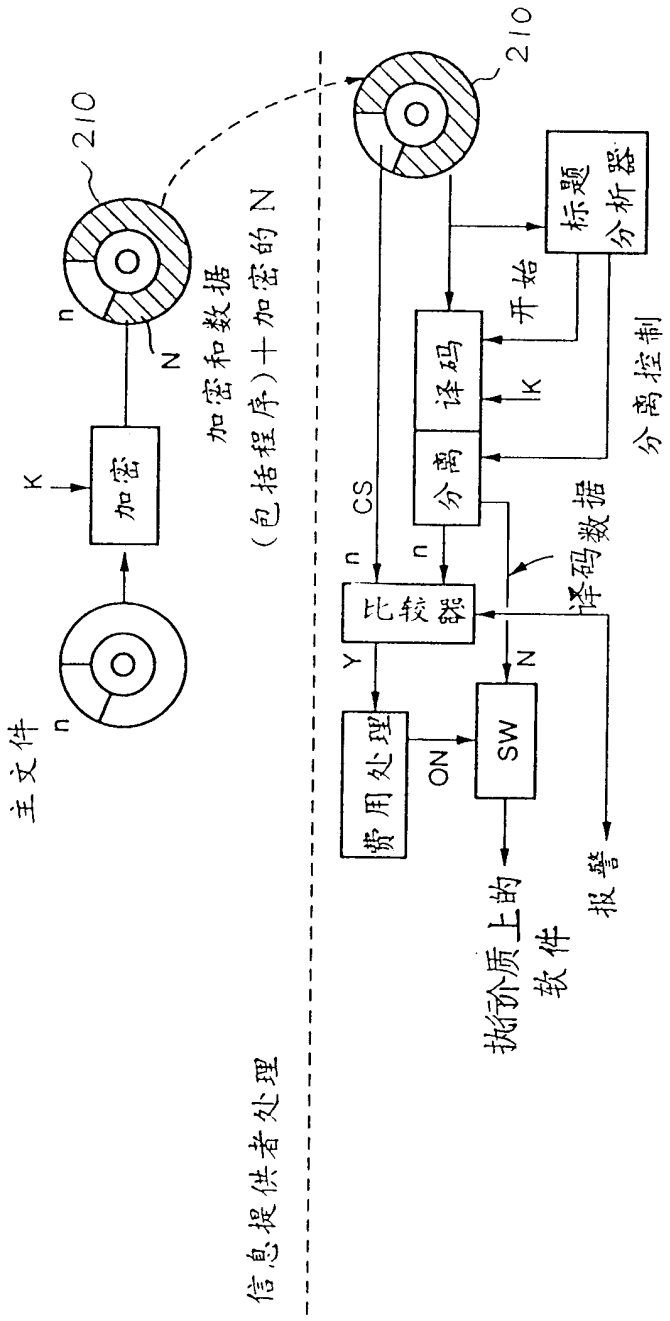

主文件
n
K
加密
n
N
210
加密和数据
(包括程序)+加密的 N
信息提供者处理
210
CS
n
比较器
Y
费用处理
ON
SW
N
执行质上的
软件
报警
n
分离
译码
K
开始
译码数据
标题
分析器
分离控制

图. 22

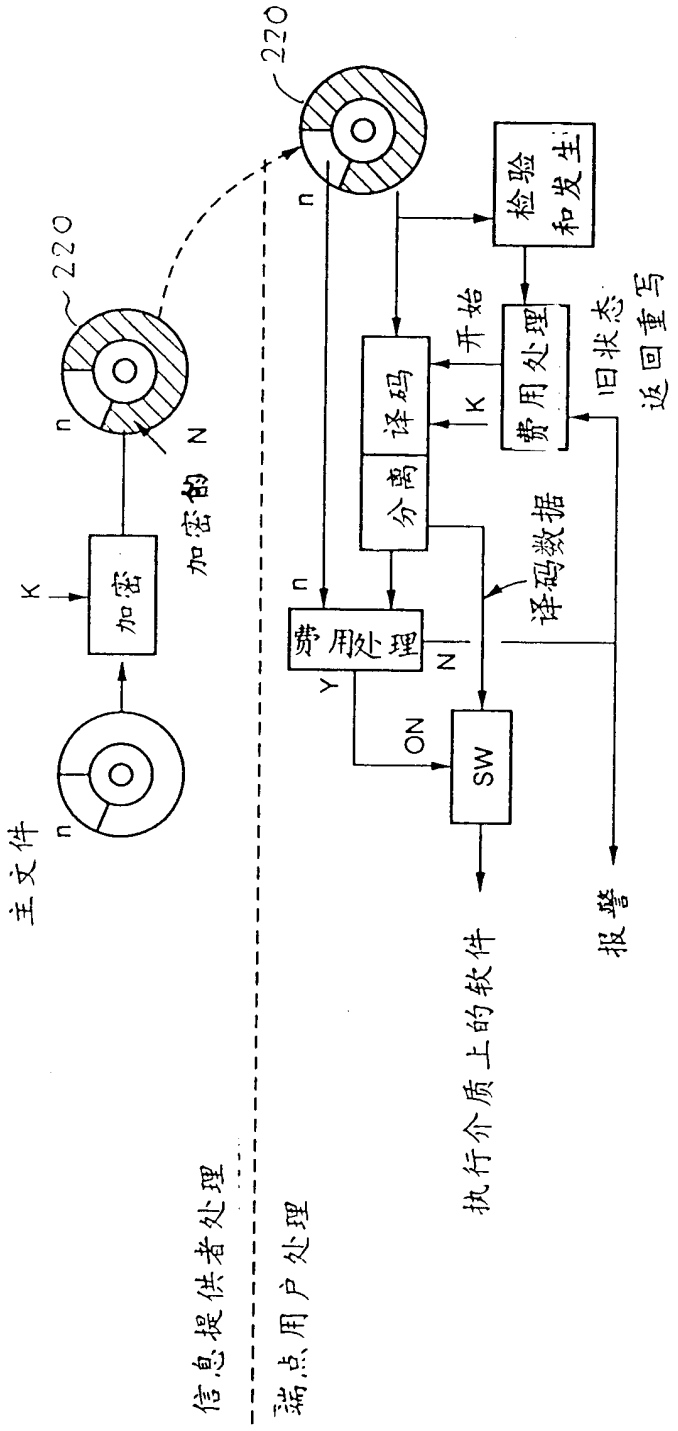

主文件
n
K
加密
220
n
加密的 N
信息提供者处理
端点用户处理
220
n
检验和发生
费用处理
开始
K
旧状态
返回重写
译码
分离
译码数据
n
费用处理
N
Y
ON
SW
执行介质上的软件
报警

图. 23

8

软件 ID	费用差额	时间标记
ABC 001	36000	654321
DEF 030	5000	871592
GHI 330	150	110542
⋮	⋮	⋮
VSY 245	650	33251
XYZ 003	2103	29875

图. 24