[19] 中华人民共和国国家知识产权局

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

[12] 发明专利说明书

[21] ZL 专利号 00105338.8

[45] 授权公告日 2005 年 1 月 5 日

[11] 授权公告号 CN 1183442C

[22] 申请日 2000.3.31 [21] 申请号 00105338.8

[30] 优先权

[32] 1999.4.30 [33] JP [31] 124182/1999

[71] 专利权人 株式会社东芝

地址 日本神奈川县

[72] 发明人 上林达 田村正文 加藤拓
石桥泰博 山田尚志 东间秀之

审查员 李 菲

[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

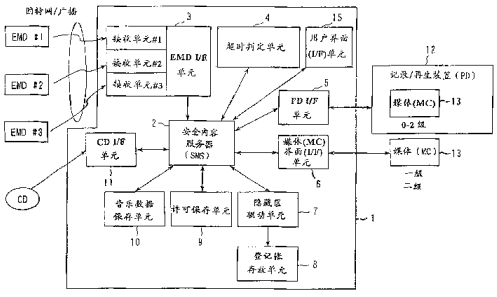
代理人 王永刚

权利要求书 3 页 说明书 22 页 附图 22 页

[54] 发明名称 内容管理方法及内容管理装置

[57] 摘要

规定可在存储媒体上存储的复制内容数的内容管理方法，SMS(2)对上述每个内容赋予预定的可以复制内容数，如接到向存储媒体的复制记录指示，在可以复制内容数还有余数时，就向该存储媒体记录复制内容，每向上述存储媒体记录一个复制内容，就从上述可以复制内容数中减去 1，如接到消去存储媒体的复制内容的指示，就每当从该存储媒体上消去一个复制内容，就将可以复制内容数加 1。



ISSN1008-4274

1.一种用于限制可存储于存储媒体(13)上的复制内容数的内容管理方法，其构成包括:

对所述每个内容赋予一个预定的可以复制的内容数(n);

如接到向所述存储媒体(13)的复制记录指示，在所述可以复制内容数(n)还有余数时，就向该存储媒体(13)记录所述复制内容(S106);

在所述记录之际，每向所述存储媒体(13)记录一个复制内容，就从所述可以复制内容数(n)的余数中减去 1(S110); 并且

如接到消去所述存储媒体(13)的所述复制内容的指示，就每当从该存储媒体(13)上消去一个该复制内容，就将所述可以复制内容数(n)加 1(S209)。

2.如权利要求 1 的方法，其构成还包括:

在设置在所述存储媒体(13)的存储区的可以以隐藏的特定手续访问的隐藏区中记录用于再生所述复制内容的必需信息。

3.如权利要求 1 的方法，其构成还包括:

将每个所述内容的至少所述可以复制内容数(n)记录在可以以隐藏的特定手续访问的隐藏存储区(8)中。

4.如权利要求 1 的方法，其构成还包括:

将每个所述内容的至少所述可以复制内容数(n)和存储复制内容的存储媒体(13)的识别信息(MID)存储在可以以隐藏的特定手续访问的隐藏存储区(8)中; 以及

只有在所述隐藏存储区(8)中存储所述存储媒体(13)的识别信息(MID)时才从该存储媒体(13)消去所述复制内容。

5.如权利要求 1 的方法，其构成还包括:

在将所述复制内容记录于所述存储媒体(13)之际，在设置在该存储媒体(13)的存储区的可以以隐藏的特定手续访问的隐藏区中记录为再生所述复制内容而必需的信息及表示是否可以移动该复制

内容的标志信息(f);以及

参考所述标志信息(f)判断是否可以移动所述复制内容。

6.如权利要求 1 的方法，其构成还包括:

在对所述存储媒体(13)进行数据读出或数据写入处理所需的时间不在预定时间以内时中断以后的处理。

7.如权利要求 1 的方法，其中作为所述存储媒体(13)，在其存储区内，在设置只有以隐藏的特定手续可以访问的隐藏区的同时，也可以包含存储所述存储媒体(13)的识别信息(MID)的第一类存储媒体，和没有所述隐藏区但具有该存储媒体的识别信息(MID)的第二类存储媒体，以及不具有所述隐藏区及该存储媒体的识别信息(MID)的第三类存储媒体。

8.如权利要求 7 的方法，其中在所述存储媒体(13)上记录复制内容之际及从该存储媒体(13)上消去复制内容之际以及再生存储于该存储媒体(13)上的复制内容之际，在判别该存储媒体(13)的类别之后进行与其相应的处理。

9.一种用来规定可存储于存储媒体(13)上的复制内容数的内容管理装置，其构成包括:

存储对所述每个内容赋予的预定的可以复制内容数(n)的存储部；以及

内容管理部(2)，如接到向所述存储媒体(13)的复制记录指示，在所述可以复制内容数(n)还有余数时，就向该存储媒体(13)记录所述复制内容，此际，每向所述存储媒体(13)记录一个复制内容，就从所述可以复制内容数(n)中减去 1，另一方面，如接到消去所述存储媒体(13)的所述复制内容的指示，就每当从该存储媒体(13)上消去一个该复制内容，就将所述可以复制内容数(n)加 1。

10.如权利要求 9 的装置，其中，所述内容管理部(2)，

在设置在所述存储媒体(13)的存储区的可以以隐藏的特定手续访问的隐藏区中，记录用于再生所述复制内容的必需信息。

11.如权利要求 9 的装置，其中，所述内容管理部(2)，

将每个所述内容的至少所述可以复制内容数(n)记录在可以以隐藏的特定手续访问的隐藏存储区(8)中。

12.如权利要求 9 的装置，其中，所述内容管理部(2)，

将每个所述内容的至少所述可以复制内容数(n)和存储复制内容的存储媒体(13)的识别信息(MID)存储在可以以隐藏的特定手续访问的隐藏存储区(8)中;以及

只有在所述隐藏存储区中存储所述存储媒体(13)的识别信息(MID)时才从该存储媒体(13)消去所述复制内容。

13.如权利要求 9 的装置，其中，所述内容管理部(2)，

在设置在该存储媒体(13)的存储区的可以以隐藏的特定手续访问的隐藏区中，记录为再生所述复制内容而必需的信息及表示是否可以移动该复制内容的标志信息(f)；以及

参考所述标志信息(f)判断是否可以移动所述复制内容。

14.如权利要求 9 的装置，其中，所述内容管理部(2)，

在对所述存储媒体(13)进行数据读出或数据写入处理所需的时间不在预定时间以内时，中断后序处理。

15.如权利要求 9 的装置，其中，所述内容管理部(2)，

在所述存储媒体(13)上记录复制内容之际及从该存储媒体(13)上消去复制内容之际以及再生存储于该存储媒体(13)上的复制内容之际，判别所述存储媒体(13)是在其存储区内在设置以隐藏的特定手续可以访问的隐藏区的同时也存储所述存储媒体(13)的识别信息(MID)的第一类存储媒体，和没有所述隐藏区但具有该存储媒体(13)的识别信息(MID)的第二类存储媒体，以及不具有所述隐藏区及该存储媒体(13)的识别信息(MID)的第三类存储媒体之中的哪一种。

16.如权利要求 15 的装置，其中，所述内容管理部(2)，

根据所述判别的该存储媒体(13)的类别进行与其类别相应的处理。

内容管理方法及内容管理装置

技术领域

本发明涉及用来对可存储于存储媒体中的音乐及电影等的拷贝内容数进行规定的内容管理方法及利用该方法的内容管理装置。

背景技术

迄今，内容(著作物等)可进行拷贝管理。通过拷贝世代管理及拷贝数管理取得了著作权保护和利用方便的平衡。

此外，代替拷贝管理，“移动”的概念已经登场。拷贝时不消去原件中的数据，与此相对，移动则是在向不同的场所(媒体)传送数据的同时，消去原始数据。内容数字化和网络的普及就是移动引起的拷贝保护登场的背景。

近年来，由于可以获得通过网络等的原件的忠实拷贝，仅借助拷贝管理很难保护著作权。另外，对于从媒体到媒体的无限制移动，比如以营利为目的的数据(利用移动)分发，就不能进行著作权管理。

这样，对原件的数据(特别是，作为著作权保护对象的内容)的复制进行可靠的管理就很困难。

发明内容

据此，本发明的目的是提供一种通过规定可在存储媒体上复制的内容数来限制内容的复制而可以保护内容的著作权的内容管理方法及利用该方法的内容管理装置。

根据本发明的一个观点，可提供一种用来规定可在存储媒体上存储的复制内容数的内容管理方法，其构成包括：对上述每个内容赋予一个预定的可以复制内容数；如接到向上述存储媒体的复制记录指示，在上述可以复制内容数还有余数时，就向该存储媒体记录上述复制内容；在上述记录之际，每向上述存储媒体记录一个复制内容，就从上述可以复制内容数的余数中减去 1；并且如接到消去上

述存储媒体的上述复制内容的指示，就每当从该存储媒体上消去一个该复制内容，就将上述可以复制内容数加 1。

还有，上述方法也可以包括在设置在上述存储媒体的存储区的可以以隐藏的特定手续访问的隐藏区中记录用于再生上述复制内容的必需信息。

还有，上述方法也可以包括将每个上述内容的至少上述可以复制内容数记录在可以以隐藏的特定手续访问的隐藏存储区中。

还有，上述方法也可以包括将每个上述内容的至少上述可以复制内容数和存储复制内容的存储媒体的识别信息存储在可以以隐藏的特定手续访问的隐藏存储区中，并且只有在上述隐藏存储区中存储上述存储媒体的识别信息时才从该存储媒体消去上述复制内容。

还有，上述方法也可以包括在将上述复制内容记录于上述存储媒体之际，在设置在该存储媒体的存储区的可以以隐藏的特定手续访问的隐藏区中记录为再生上述复制内容而必需的信息及表示是否可以移动该复制内容的标志信息，以及参考上述标志信息判断是否可以移动上述复制内容。

还有，上述方法也可以包括在对上述存储媒体进行数据读出或数据写入处理所需的时间不在预定时间以内时中断后序的处理。

在上述方法中，作为上述存储媒体，在其存储区内，在设置只有以隐藏的特定手续可以访问的隐藏区的同时，也可以包含存储上述存储媒体的识别信息的第一类存储媒体，和没有上述隐藏区但具有该存储媒体的识别信息的第二类存储媒体，以及不具有上述隐藏区及该存储媒体的识别信息的第三类存储媒体。在此场合，在上述存储媒体上记录复制内容之际及从该存储媒体上消去复制内容之际以及再生存储于该存储媒体上的复制内容之际，在判别该存储媒体的类别之后进行与其相应的处理。

根据本发明的另一个观点，可提供一种用来规定可存储于存储媒体上的复制内容数的内容管理装置，其构成包括：对上述每个内容赋予一个预定的可以复制内容数，如接到向上述存储媒体的复制

记录指示，在上述可以复制内容数还有余数时，就向该存储媒体记录上述复制内容，此际，每向上述存储媒体记录一个复制内容，就从上述可以复制内容数中减去 1 的复制内容记录装置；并且如接到消去上述存储媒体的上述复制内容的指示，就每当从该存储媒体上消去一个该复制内容，就将上述可以复制内容数加 1 的复制内容移动装置。

还有，上述装置也可以包括在设置在上述存储媒体的存储区的可以以隐藏的特定手续访问的隐藏区中记录用于再生上述复制内容的必需信息的装置。

还有，上述装置也可以包括将每个上述内容的至少上述可以复制内容数记录在可以以隐藏的特定手续访问的隐藏存储区中的装置。

还有，上述装置也可以包括将每个上述内容的至少上述可以复制内容数和存储复制内容的存储媒体的识别信息存储在可以以隐藏的特定手续访问的隐藏存储区中，并且只有在上述隐藏存储区中存储上述存储媒体的识别信息时才从该存储媒体消去上述复制内容的装置。

还有，上述装置也可以包括在将上述复制内容记录于上述存储媒体之际，在设置在该存储媒体的存储区的可以以隐藏的特定手续访问的隐藏区中记录为再生上述复制内容而必需的信息及表示是否可以移动该复制内容的标志信息的装置，以及参考上述标志信息判断是否可以移动上述复制内容的装置。

还有，上述装置也可以包括在对上述存储媒体进行数据读出或数据写入处理所需的时间不在预定时间以内时中断后序处理的装置。

还有，上述装置，也可以包括在上述存储媒体上记录复制内容之际及从该存储媒体上消去复制内容之际以及再生存储于该存储媒体上的复制内容之际，上述存储媒体具有判别存储媒体是在其存储区内在设置只有以隐藏的特定手续可以访问的隐藏区的同时也包含

存储上述存储媒体的识别信息的第一类存储媒体，和没有上述隐藏区但具有该存储媒体的识别信息的第二类存储媒体，以及不具有上述隐藏区及该存储媒体的识别信息的第三类存储媒体之中的哪一种的判别装置。还有，在此场合，上述装置也可具有在上述判别装置判别该存储媒体的类别之后可进行与上述存储媒体类别相应的处理的装置。

附图简介

图 1 示出的是使用用于规定可在本发明实施形态中的存储媒体上存储的复制内容数的内容管理方法的音乐内容利用管理系统(LCM)的构成例框图。

图 2 为示出存储区的构成例框图。

图 3 为示出记录再生装置(PD)的内部构成例的框图。

图 4A~图 4C 为说明三种存储媒体的特征的框图。

图 5 为示出媒体界面(I/F)单元的内部构成例的框图。

图 6 为说明检入后存储媒体的记录内容用的框图。

图 7A~图 7C 为示出在 LCM 的隐藏区中存放的登记帐的存储例的框图。

图 8A~图 8B 为示出在 LCM 的隐藏区中存放的登记帐的另一存储例的框图。

图 9 示出用于说明检入/检出处理步骤的流程图，包括判别媒体的类别并一直到选择与其类别相应的处理的步骤。

图 10 为说明在存储媒体的类别为二级的场合的检出步骤的框图。

图 11 为说明在存储媒体的类别为二级的场合的检入步骤的框图。

图 12 为说明在存储媒体的类别为二级的场合的再生步骤的框图。

图 13 为说明在存储媒体的类别为一级的场合的检出步骤的框

图。

图 14 为说明在存储媒体的类别为一级的场合的再生步骤的框图。

图 15 为说明在存储媒体的类别为零级的场合的检出步骤的框图。

图 16 为说明在存储媒体的类别为零级的场合的检入步骤的框图。

图 17 为说明在存储媒体的类别为零级的场合的再生步骤的框图。

图 18A~图 18C 为示出在 LCM 的隐藏区中存放的登记帐的又一存储例框图，其中示出包含标志的登记帐。

图 19 为说明利用标志进行检入处理的概略流程图。

图 20 为说明利用公钥加密方式的认证步骤的框图。

图 21 示出通过网络向存储媒体记录复制内容的场合的机器构成例的框图。

图 22 为示出超时判断单元的内部构成例的框图。

图 23 为用于说明超时判断处理一例的流程图。

图 24 为用于说明构成隐藏区用的文件系统的示意图。

图 25 为用于说明隐藏区驱动电路的动作用的流程图。

图 26 为用于说明扇区配置更新时的隐藏区驱动电路的动作用的流程图。

本发明详述

下面参考附图对本发明的实施形态予以说明。

图 1 示出的是使用用于规定可在本发明实施形态中的存储媒体上存储的复制内容数的内容管理方法的音乐内容利用管理系统(以下简称为 LCM)1 的构成例。另外，此处是以音乐作为内容的一个示例，但并不限于此，也可以是电影、游戏软件等。另外，作为媒体使用的是媒体卡(MC)，但并不限于此，也可使用软盘，DVD 等各种

存储媒体。

EMD(电子音乐分发人)是音乐发送服务器或音乐发送广播台。

内容利用管理系统 1，比如，可以是个人计算机(PC)，具有多个与 EMD(此处为 EMD#1~#3)相对应的接收单元#1~#3，EMD 接收所发送的加密内容或其许可(使用条件及加密内容脱密密钥)。接收单元#1~#3 最好是具有再生功能和计费功能。再生功能是用来对发送的音乐内容进行试听。另外，利用计费功能可将中意的内容买下。

LCM1 具有两个安全音乐服务器(以下简称为 SMS)，用户购买的内容经过 EMD 界面(I/F)单元 3 存储于 SMS2 中。需要时音乐内容在 EMD 界面(I/F)单元 3 中实施译码，形式变换及再加密。如 SMS2 接收到加密内容，就存储于音乐数据存放单元 10 中，并将音乐数据脱密密钥存放于许可存放单元 9 之中。SMS2 最好是具有再生功能。利用合适的再生功能，可将 SMS2 管理的音乐内容在 PC 上再生。

SMS2 具有对媒体(以下简称为 MC)13 输出内容数据的功能。MC13 设置于记录再生装置 12(以下简称为 PD(便携器件))内并可再生记录于 MC13 上的内容。

从 SMS2 向 MC13 的记录通过媒体(MC)界面(I/F)单元 6 直接进行，另外可经过 PD12 进行。

MC13 具有该媒体固有的且不能改写的识别信息(MID)，MC13 中存放的内容利用依赖 MC13 的内容脱密密钥加密。

内容脱密密钥利用存放于媒体(MC)界面(I/F)单元 6 及 PD12 中的加密密钥 Kp 加密而记录于 MC13。

MC13 内的内容及内容脱密密钥可以拷贝到另外的任意存储媒体(以下称之为 Mcb)上，但是

1.因为只有正统的 PD12 具有加密密钥 Kp，如表示正统的 PD12 就不能正确地再生存放在 Mcb 上的内容。但是，

2.因为不能拷贝 MC13 的识别信息 MID，而 Mcb 上的识别信息 MID 与拷贝原件的 MC13 的识别信息 MID 不同，结果拷贝到 Mcb 的内容不能正确地再生。即可以防止将 SMS2 记录于 MC13 中的复

制内容接连不断地拷贝到另外的 MC 上使用。

以上是原来考虑的 LCM1 的构成，下面对涉及本发明的方法及构成单元予以说明。

首先，根据图 1 的 LCM1 对检入/检出进行说明。

所谓检出指的是 LMS1 存放作为“父代”的内容而将其复制件作为“子代”内容拷贝到 MC13 上。“子代”内容可在 PD12 上自由地再生，但是从“子代”到“孙代”内容不允许生成。从“父代”内容可生成几个“子代”，由“父代”属性定义。另外，所谓检入指的是，比如，将 MC13 与 LCM1 连接，LCM1 通过将“子代”内容消去(或使其不能使用)而恢复利用 LCM1 内的“父代”内容制作一个“子代”内容的权利。这也称为“父代”内容检入。

如果此检入/检出是单纯地利用原有的 LCM1 实现的，则实际上存在下面这种的“攻击(attack)”。即将存放在 MC13 中的“子代”保存到另外的存储媒体(识别信息 MID 除外)中，将 MC13 的“子代”检入到“父代”。接着，将先保存的“子代”写回到合适的 MC13 中。因为检入已经完成，所以也可以将 LCM1 上的“父代”拷贝到另外的 MC13 上。利用这个方法就可以制作任意个可以使用的“子代”。

在上述的“攻击”中，通过在 MC13 和 LCM1 传送数据之际进行的认证，可能发生对抗。即假定 MC13 不接受从合法的 LCM1 以外发出的数据传送，LCM1 不接受从合法的 MC13 以外发出的数据传送。在此场合，不能将 MC13 内的“子代”保存到另外的记录媒体中。另外，对于 LCM1，通过欺骗也不能检入。所以，上述的“攻击”破产。

然而，实际上，即使以 LCM1 和 MC13 的认证为前提，也不能实现检入/检出。因为存在下面这样的“攻击”之故。即，首先，在 LCM1 上的“父代”不能制作“子代”的状态中，将 LCM1 的数据(特别是许可保存单元 9 的信息)备份到另外的存储媒体。在将“子代”拷贝到 MC13 之后，将备份的 LCM1 的数据返回。因为 LCM1 的“父

代”返回到制作“子代”之前的状态，所以可在另外的 MC13 上制作“子代”。这样一来，就可以制作任意数目的“子代”。

其次，对实现检入/检出方面产生的问题以外的问题进行说明。即经由因特网等规定通信通道向 MC13 上进行记录。利用 EMD 的正规的因特网发送，因为是得到著作权所有者的许诺进行合法的发送，所以没有问题。但是，在图 21 这样的形态中，经过因特网向 MC13 上记录内容是可以的。图 21 中的 PC 上的通信单元 201 只是向 MC13 转发写入协议。LCM1，由于不能区别与该 LCM1 运行的 PC#2 连接的 PD12 和通过通信单元 201 与远方连接的 LCM1 运行的 PC#2 连接的 PD12，就可以通过因特网等网络进行内容的(违法)发送。

下面介绍本发明的要旨。下面按照所示的项目顺序对检入/检出及用来限制通过网络向 MC13 进行记录的装置予以说明。

1.检入/检出

(1-1)检入/检出

(1-2)利用二级的 MC 的复制内容的检入/检出

(1-3)利用登记帐的复制内容的另外的管理方法

(1-4)利用二级的 MC 的复制内容的再生

(1-5)利用一级的 MC 的复制内容的检入/检出，复制内容的再生

(1-6)利用零级的 MC 的复制内容的检入/检出，复制内容的再生

2.用来限制通过网络向 MC 进行记录的复制内容的装置

3.隐藏区

(检入/检出)

为了实现检入/检出，在 MC13 中的存储区中设置以公开的步骤不能读写的区(隐藏区)，在该区中记录对内容进行解码所必需的信息(参考图 2)。另外，在 LCM1 的存储区(比如在 LCM1 是由 PC 构成的场合下的硬盘)上以不公开的步骤设置不能访问的区域(隐藏区)，将下述的登记帐存放于该隐藏区(参考图 2)。此外，在 PD12 的存储

区中也可设置只能以不公开步骤访问的区(隐藏区)并在该区中记录内容解码所必需的信息(参考图 2)。另外，此处将存储区中的隐藏区以外的利用通常的步骤可以访问的区域称为公开区。

如图 1 所示，在 LCM1 中，在隐藏区中设置登记帐存放单元 8，在由 SMS2 执行用来对此登记帐存放单元 8 进行访问的隐藏的特定的手续之后，具有从隐藏区读取数据用的隐藏区驱动单元 7。

如图 4C 所示，MC13 的构成包括不能从存放其识别信息 MID 用的外部改写也不能拷贝的结构形成的识别信息存放单元 13b，隐藏区 13c，公开区 13a，以及每次访问隐藏区 13c 时由认证单元 13d 进行认证对方是合法时才打开入口使得可以对隐藏区 13c 进行访问的的开关(SW)13e。另外，在本实施形态中可以利用的 MC13 有 3 种，如图 4C 所示，将兼备识别信息 MID 和隐藏区两者的 MC13 称为“二级”。不具有隐藏区但具有识别信息 MID 的如图 4B 所示的 MC13 称为“一级”。既不具有隐藏区也不具有识别信息 MID 的如图 4A 所示的 MC13 称为“零级”。这些类别，比如，通过有无识别信息 MID 可判别零级和非零级，并且由识别信息 MID 的构成可判别一级和二级。比如，识别信息是连续数值，超过一定值时是二级。

下面，只要不特意间断，都是以二级 MC13 的场合为例进行说明。

此 MC13，有设置于连接到 LCM1 的 PD12 中场合及直接设置于 LCM1 中的场合。

图 3 为示出记录再生装置(PD)12 的构成例的框图，MC13 与媒体界面(I/F 单元)12f 连接。在 LCM1 通过 PD12 读写 MC13 的场合，通过 PD12 内的隐藏区访问单元访问 MC13 的隐藏区。在媒体界面(I/F 单元)12f 中具有用于访问 MC13 的隐藏区的隐藏区访问单元。PD12 内的隐藏区，也可设置于闪存 12d 中。ROM12c 中写入用于与 MC13 之间进行相互认证的程序以及用于判别 MC13 的类别的程序，依照此程序，在 CPU12a 的控制下，执行与 MC13 之间的相互认证，类别判别等处理。

图 5 为示出 LCM1 的媒体(MC)界面(I/F)单元 6 的构成例的框图，其构成包括用于与 MC13 进行相互认证的认证单元 6c，判别 MC13 的类别的媒体判别单元 6b 以及控制全体这些用的控制单元 6a。认证单元 6c 是用于访问 MC13 的隐藏区的隐藏区访问单元。

其次，对存放在 LCM1 的隐藏区中的登记帐予以说明。

保存在 SMS2 中的所有的音乐内容保持有作为用于识别其每一个的识别信息的内容 ID(TID)，预先确定的可以复制内容数，即子代余数，及检出列表的属性信息。此属性信息称为登记帐。登记帐以图 7 所示的形态存储于设置于隐藏区内的登记帐存放单元 8 中。

在图 7A 中，比如，作为内容 ID“TID1”的子代余数为“2”时，其检出列表为 L1.

检出列表是记录复制内容(子代)的 MC13 的识别信息的列表，比如，在图 7A 中，可以看到对检出列表 L1 中具有“m1”和“m2”这样的识别信息的 2 个 MC13 作为内容 ID“TID1”的内容的子代检出。

(利用二级 MC 的复制内容的检入/检出)

下面，参考图 9~图 11 对利用如图 4C 所示构成的二级 MC13 的检入/检出予以说明。

如 MC13 是设置成与 LCM1 的媒体(MC)界面(I/F)单元 6 或 PD12 连接，则在媒体(MC)界面(I/F)单元 6 和 MC13 之间，或是在 PD12 和 MC13 之间进行相互认证(图 9 步骤 S1)，在双方判断对方合法时(步骤上述 2)，媒体(MC)界面(I/F)单元 6 或 PD12 根据从 MC13 读取的识别信息 MID 判别 MC13 的类别(步骤 3)。此处，因为 MC13 的类别是二级，媒体(MC)界面(I/F)单元 6 或 PD12 就执行与其类别相应的检入/检出处理。

下面参考图 10 对检出的指示通过用户界面(I/F)单元 15，或是通过 PD12，成为 SMS2 的场合予以说明。SMS2 检查有登记帐检出要求的内容(比如设内容 ID 为“TID1”)的子代的余数 n(步骤 S101)，

在 n>0 时，有必要时，进行与 MC13 之间的相互认证(步骤 S102)，如相互确认合法，接着就请求从 MC13 转送其识别信息 MID(比如设 MID=m0)(步骤 S103)。

在 SMS2 中生成随机数 r，利用生成此随机数 r，MC13 的识别信息 m0，及合法的 MC13 和 LCM1 之间的共有的密钥的算法 W 生成加密密钥 w。另外，密钥生成算法 W 取两个变量(此处为 r 和 m0)，实现使加密密钥 w 每次发生变化的作用。此外，在 SMS2 中，将用于使密码化的内容解码的脱密密钥 K(C)利用在 MC13 同 LCM1 之间共有的加密密钥 Kp 以及先前生成的加密密钥 w 进行加密，并将其表示为 w[Kp[k(C)]]。另外，将内容 C 以密钥 K(C)加密，并将其表示为 K(C)[C](步骤 S104)。

SMS2，如在 MC13 的存储区中生成，比如，名称为“TIDI”的文件夹(步骤 S105)，则将加密内容 K(C)[C]和加密内容脱密密钥 w[Kp[k(C)]] 写入该文件夹的公开区内(步骤 S106，步骤 S107)。

其次，SMS2，如应该访问 MC13 的隐藏区 13c，要与 MC13 之间相互认证，确认双方合法而利用开关(SW)13e 打开通到隐藏区 13c 的入口，将随机数 r 写入与隐藏区 13c 内的文件夹“TID1”对应的区域中(步骤 S108~S109)。如到此结束，则利用开关(SW)13e 将可能访问隐藏区 13c 的入口关闭。另外，在步骤 S108 中，对转送随机数 r 到隐藏区 13c 的路径最好也像对对随机数 r 进行加密一样进行转送保护。

最后，SMS2，如图 7B 所示，从具有登记帐的检出要求的内容 ID“TID1”的内容子代的余数 n 减“1”，并在检出列表 L1 中添加该 MC13 的识别信息“m0”(步骤 S110)。

以上处理结束时的 MC13 的存储内容如图 6 所示。

下面对检入的指示通过 LCM1 的用户界面(I/F)单元 15，或通过 PD12 成为 SMS2 的场合参考图 11 予以说明。

SMS2，有必要时，进行与 MC13 之间的相互认证(步骤 S201)，如相互确认合法，接着就请求从 MC13 转送其识别信息 MID(比如设

MID=m0)(步骤 S202)。

SMS2 从有检入要求的内容(比如设内容 ID 为“TID1”)的登记帐，在该检出列表中该 MC13 的识别信息，即，此处登录的“m0”的时候，产生随机数 r1 和随机数 r2(步骤 S203)。于是，将与 MC13 的公开区 13a 的该内容的文件夹(此处为文件夹“TID1”)对应的区域中存储的信息利用随机数 r2 重写而消去(步骤 S204)，另外，SMS2，如应该访问 MC13 的隐藏区 13c，要与 MC13 之间相互认证，确认双方合法而利用开关(SW)13e 打开通到隐藏区 13c 的入口，则通过将随机数 r1 重写于与隐藏区 13c 内的文件夹“TID1”对应的区域中而消去(步骤 S205)。如到此结束，则利用开关(SW)13e 将可能访问隐藏区 13c 的入口关闭。另外，在步骤 S205 中，对转送随机数 r1 到隐藏区 13c 的路径最好也像对对随机数 r1 进行加密一样进行转送保护。

之后，在 SMS2 中，应确认重写消去，要求从 MC13 转送重写后的各区的数值(步骤 S206)，检查该数与 r1、r2 是否一致(步骤 S207)。如确认重写消去，则从 MC13 中消去文件夹“TID1”(步骤 S208)。

最后，如图 7C 所示，将具有登记帐的检入要求的内容 ID“TID1”的内容子代的余数 n 加“1”，并从检出列表 L1 中删除该 MC13 的识别信息“m0”(步骤 S209)。

记录于 MC13 内的隐藏区 13c 中的随机数 r (因为不能确认认证的合法性)不能保存到另外的存储媒体中。因此，在所谓“TID1”的内容检入之后，不能利用返回 MC13 的内容。另外，存储于 LCM1 内的隐藏区中的登记帐(因为不能确认认证的合法性)也不能保存到另外的存储媒体中。因此，在所谓“TID1”的内容检出之后，不能使登记帐返回到检出前的状态。这样，本发明可以提供对前述的攻击的对策。

另外，在检入之际，在 MC13 的隐藏区的内容上以随机数重写这一点在安全上是重要的。可以在 MC13 的隐藏区上重写的是只有

正统的 SMS2，反之，正统的 SMS2 必定可以利用隐藏的手续写入隐藏区。通过以隐藏的手续成功的写入可保证 MC13 的正统性。即可以防止不合法的检入。为增加安全性，SMS2 在隐藏区上以任意的随机数重写之后，应(利用隐藏手续)读出其内容，确认重写的随机数。

(登记帐的复制内容的其他管理方法)

另外，SMS2 也可对在登记帐上没有的标题(内容 ID)的内容进行检入。还有，也可容许从在检出列表上没有的 MC13 检入。在此场合，登记帐不保持对各内容的检出列表。因为检出列表是为防止从“问心无愧”的 MC13 检入的参考之故。在此场合的登记帐的存储内容如图 8A 所示。

如图 8A 所示，在各内容的登记帐中仅仅登录有该内容 ID 和子代的余数。

下面考虑将具有称为 TID7 的内容 ID 的内容从具有识别信息 MID=m0 的 MC13 检入的场合。即在该 MC13 中，现在，以图 6 所示的形态存储有从另外的 SMS2 检出的内容 ID“TID7”的内容。

LCM1，在图 11 所示的手续中，在不参考步骤 S203 的检出列表的情况下将 MC13 内的隐藏区，公开区的存储内容消去的同时，将文件夹“TID7”删除。于是，在登记帐中登录新的内容的登记帐(TID7、1)。

LCM1 通过检入在登记帐中没有的内容可以进行，比如，如下的事情。由自家的 PC 构成的 LCM1 存放的“父代”内容可保持两个“子代”。如从自家的 PC 向 MC13 检出一个“子代”，可向朋友家的 PC 检入。自己购买的“父代”生成“子代”的数目减 1，而将内容赠送给朋友。

这样，假如 LCM1 可以检入在登记帐中没有的内容，“子代”的内容就可以通过 LCM1“移动”。这对于用户是很方便的功能，也可成为半新不旧的市场成立的原因。实际上，下面这种半新不旧的内容的买卖是成立的。即用户此 EMD 购入新生产的内容，在保持

短时期之后，将该内容检入到半新不旧的数据商店的 LCM1 中。此时，该用户接受报酬。半新不旧数据商店可以以比 EMD 的正规价格便宜的价格将数据出售给另外的希望购买的人。

这样，不能控制内容的著作权的“半新不旧市场”的成立对著作权所有人来讲是不希望的。所以，著作权所有人也最好是通过在各内容中保持检出属性标志 f 以便可以控制向不同的 LCM1 的检入。

在此场合的 LCM1 具有的登记帐的形式如图 18A 所示。

如图 18A 所示，在各内容的登记帐中，登录有该内容的 ID，子代的余数，检出列表及检出属性标志 f。

在标志 f 为“1”时，该内容可向其他的 LCM1 检出、检入，而在检出属性标志 f 为“0”时，该内容至少不能向其他的 LCM1 中检入。

比如，考虑内容 ID“TID6”这样一种内容的检出的场合。首先，SMS2 调查登记帐，确认该内容的检出属性标志为“1”。此处，在此值为“0”时，对该 LCM1 该内容不能检出。在标志 f 为“1”时，利用如图 10 所示的步骤，从内容 ID“TID6”的登记帐的子代余数减去“1”而成为“1”(参考图 18B)。顺便指出，检出列表 L6 为空(以ϕ表示)，并且标志 f 为“1”，因为该内容可向设置于其他 PC 上的 LCM1 检入，不需要保持检出列表。另外，标志 f 是在 MC13 的隐藏区中与随机数 r 一起记录。

其次，参考图 19 所示的流程图对于将内容 ID“TID6”这样一种内容向与检出的 LCM1 相同的 LCM1 或另外的 LCM1 检入的场合予以说明。

在图 11 所示的步骤中，MC13 和 LCM1 之间进行相互认证(步骤 S11)，取得 MC13 的识别信息 MID(步骤 S12)。

SMS2，不管有检入要求的内容是否登录在登记帐上，对 MC13 的隐藏区执行前述的隐藏手续(进行与 MC13 之间的相互认证，确认双方的合法性而利用开关(SW)13e 打开通到隐藏区 13c 的入口)，从

隐藏区 13c 读出标志 f (步骤 S13) 。在标志 f 为“1”时(步骤 S14), 执行图 11 的步骤 S204~步骤 S208 (步骤 S15~16) ，在标志 f 为“0”时处理结束。于是，最后，当在登记帐上未登录该内容时，将该内容的子代余数定为“1”的“TID6”登录到新的登记帐上(TID6、1、ϕ 、1)，当将该内容登录到登记帐上时，该内容的子代余数增加“1”(步骤 S17) 。

(利用二级 MC 的复制内容的再生)

下面，参考图 12 对利用如图 4C 所示的存储于构成的二级 MC13 中的复制内容的再生予以说明。

如 MC13 是设置成与 PD12 连接，则 PD12 将请求从 MC13 转送其识别信息 MID(比如设 MID=m0)(步骤 S301)。此时根据识别信息 MID 判别 MC13 的类别，可判别出类别是二级。此时，PD12，在从 MC13 的公开区读出 w[Kp[k(C)]]的同时(步骤 S302)，如应该访问 MC13 的隐藏区 13c，要与 MC13 之间相互认证，确认双方合法而利用开关(SW)13e 打开通到隐藏区 13c 的入口，从与隐藏区 13c 内的文件夹“TID1”对应的区域中将随机数 r 读出(步骤 S303)。如到此结束，则利用开关(SW)13e 将可能访问隐藏区 13c 的入口关闭。

PD12，利用生成随机数 r，MC13 的识别信息 m0，及合法的 MC13 和 PD12 之间的共有的密钥的算法 W 生成加密密钥 w。由加密密钥 w，在 MC13 同 LCM1 之间共有的加密密钥 Kp 以及从 MC13 读出的 w[Kp[k(C)]]对用于内容脱密的脱密密钥 K(C)脱密(步骤 S304) 。

于是，PD12 就可将从 MC13 的公开区的加密内容 K(C)[C] 读出(步骤 S305)，利用脱密单元 12g 对内容 C 脱密，利用解码器 12h 解码，利用 D/A 变换单元将数字信号变换为模拟信号而使音乐再生(步骤 S306)。

(利用一级 MC 的复制内容的检入/检出、复制内容的再生)

下面，参考图 9、图 13 对利用如图 4B 所示的构成的一级 MC13 的检入/检出予以说明。另外，因为一级 MC13 没有隐藏区，所以不能进行检入。

从 MC13 设置成与 LCM1 的媒体(MC)界面(I/F)单元 6 或 PD12 连接直到判别 MC13 的类别与图 9 相同。

此处，因为 MC13 的类别是一级，媒体(MC)界面(I/F)单元 6 或 PD12 就执行与其类别相应的检入/检出处理(步骤 S5) 。

在检入的指示通过 LCM1 的用户界面(I/F)单元 15 或通过 PD12 成为 SMS2 的场合，因为判别 MC13 的类别是一级，对该指示拒绝。

在检出的指示通过 LCM1 的用户界面(I/F)单元 15 或通过 PD12 成为 SMS2 的场合，参考图 13 予以说明。

SMS2 检查有登记帐检出要求的内容(比如设内容 ID 为“TID1”)的子代的余数 n(步骤 S401)，在 n>0 时，有必要时，进行与 MC13 之间的相互认证(步骤 S402)，如相互确认合法，接着就请求从 MC13 转送其识别信息 MID(比如设 MID=m0)(步骤 S103)。

SMS2，与二级的场合相同，生成随机数 r，生成加密密钥 w，利用 w 及 Kp 对内容密钥进行加密而对内容 C 加密(步骤 S404)，在 MC13 的存储区(此处仅为公开区)生成，比如名字为“TID1”的文件夹(步骤 S405) 。于是，将加密内容 K(C)[C]和加密内容脱密密钥 w[Kp[k(C)]] 及随机数 r 写入(步骤 S406~步骤 S408)。

最后，SMS2，如图 7B 所示，从具有登记帐的检出要求的内容 ID“TID1”的内容子代的余数 n 减“1”，并在检出列表 L1 中添加该 MC13 的识别信息“m0”(步骤 S409)。

下面，参考图 14 对利用一级 MC13 中的复制内容的再生予以说明。

如 MC13 是设置成与 PD12 连接，则 PD12 将请求从 MC13 转送其识别信息 MID(比如设 MID=m0)(步骤 S501)。此时根据识别信息 MID 判别 MC13 的类别，可判别出类别是一级。此时，PD12，从该 MC13 的存储区(只是公开区)读出 w[Kp[k(C)]]和随机数 r (步骤

S502~步骤 S503)，利用随机数 r，MC13 的识别信息 m0，及合法的 MC13 和 PD12 之间的共有的密钥的算法 W 生成加密密钥 w。由加密密钥 w，在 MC13 同 LCM1 之间共有的加密密钥 Kp 以及从 MC13 读出的 w[Kp[k(C)]]对用于内容脱密的脱密密钥 K(C)脱密(步骤 S504)。

于是，PD12 就可将从 MC13 的存储区(只是公开区)的加密内容 K(C)[C] 读出(步骤 S505)，利用脱密单元 12g 对内容 C 脱密，利用解码器 12h 解码，利用 D/A 变换单元将数字信号变换为模拟信号而使音乐再生(步骤 S506)。

(利用零级 MC 的复制内容的检入/检出、复制内容的再生)

下面，参考图 9、图 15~图 16 对利用如图 4A 所示的构成的零级 MC13 的检入/检出予以说明。

零级的 MC13 只能利用 PD12 进行检入/检出及再生。另外，由于没有识别信息 MID，所以在检入/检出中使用 PD12 的识别信息 PID 代替。

从 MC13 设置成与 PD12 连接直到判别 MC13 的类别与图 9 相同。此处，因为 MC13 的类别是零级，PD12 就执行与其类别相应的检入/检出处理(步骤 S4)。

在检出的指示通过 PD12 成为 SMS2 的场合，参考图 15 予以说明。

SMS2 检查有登记帐检出要求的内容(比如设内容 ID 为“TID1”)的子代的余数 n(步骤 S601)，在 n>0 时，有必要时，进行与 PD12 之间的相互认证(步骤 S602)，如相互确认合法，接着就请求从 PD12 转送其识别信息 PID(步骤 S603)。

SMS2，与二级的场合相同，生成随机数 r，生成加密密钥 w，利用 w 及 Kp 对内容密钥进行加密而对内容 C 加密(步骤 S604)。不过，此处密钥生成算法 W 所取的 2 个变量是 r 和 PID。

其次，在 MC13 的存储区(此处仅为公开区)生成，比如名字为

“TID1”的文件夹(步骤 S605)。于是，将加密内容 K(C)[C]和加密内容脱密密钥 w[Kp[k(C)]] 及随机数 r 写入(步骤 S606~步骤 S607)。随机数 r 写入 PD12 的隐藏区(步骤 S608)。在步骤 S608 中，对转送随机数 r 到 PD12 的隐藏区的路径最好也像对对随机数 r 进行加密一样进行转送保护。

最后，SMS2，如图 7B 所示，从具有登记帐的检出要求的内容 ID“TID1”的内容子代的余数 n 减“1”，并在检出列表 L1 中添加该 PD12 的识别信息“PID”(步骤 S609)。

下面对检入的指示通过 PD12 成为 SMS2 的场合参考图 16 予以说明。

SMS2，进行与 PD12 之间的相互认证(步骤 S701)，如相互确认合法，接着就请求从 PD12 转送其识别信息 PID (步骤 S702)。

SMS2 从有检入要求的内容(比如设内容 ID 为“TID1”)的登记帐，在该检出列表中该 PD12 的识别信息“PID”登录的时候，产生随机数 r1 和随机数 r2(步骤 S703)。于是，将与 MC13 的公开区 13a 的该内容的文件夹(此处为文件夹“TID1”)对应的区域中存储的信息利用随机数 r2 重写而消去(步骤 S704)，另外，SMS2，如应该访问 PD12 的隐藏区，要与 PD12 之间相互认证，确认双方合法而打开通到隐藏区的入口，则通过将随机数 r1 重写于与隐藏区 13c 内的文件夹“TID1”对应的区域中而消去(步骤 S705)。如到此结束，则将可能访问隐藏区的入口关闭。另外，在步骤 S705 中，对转送随机数 r1 到隐藏区的路径最好也像对对随机数 r1 进行加密一样进行转送保护。

之后，在 SMS2 中，应确认重写消去，要求从 MC13 转送重写后的各区的数值，另外，此 PD12 的隐藏区也执行上述的预定手续，读出该区域重写后的值(步骤 S706)，检查该数与 r1、r2 是否一致(步骤 S707)。如确认重写消去，则从 MC13 中消去文件夹“TID1”(步骤 S708)。

最后，如图 7C 所示，将具有登记帐的检入要求的内容 ID“TID1”

的内容子代的余数 n 加“1”，并从检出列表 L1 中删除该 PD12 的识别信息“PID”(步骤 S709)。

下面，参考图 17 对利用零级 MC13 中存储的复制内容的再生予以说明。如 MC13 是设置成与 PD12 连接，则 PD12 将请求从 MC13 转送其识别信息 MID，因为 MC13 没有识别信息，上移 PD12 可判别出该 MC13 的类别是零级。此时，PD12，从该 MC13 的存储区(只是公开区)读出 w[Kp[k(C)]](步骤 S801)，利用 PD12 本身的识别信息“PID”，存放于其隐藏区中的随机数 r 及密钥的算法 W 生成加密密钥 w。于是，由加密密钥 w，加密密钥 Kp 以及从 MC13 读出的 w[Kp[k(C)]]对内容脱密密钥 K(C)脱密(步骤 S802)。

PD12 就可将从 MC13 的存储区(只是公开区)的加密内容 K(C)[C]读出(步骤 S803)，利用脱密单元 12g 对内容 C 脱密，利用解码器 12h 解码，利用 D/A 变换单元将数字信号变换为模拟信号而使音乐再生(步骤 S804)。

(用来限制通过网络向 MC 进行记录的复制内容的装置)

为了解决本发明的第二个目的的问题，即为了限制经过网络将内容记录到 MC13，在本发明中，如图 1 所示，设置超时判定单元 4。

在超时判定单元 4 中，对 MC13 的读写(任何一方或两方)步骤设定一定的限制时间，如处理在限制时间以内未结束处理就中断。由于通过网络的通信通常比直接连接的机器的通信需要长得多的时间，利用超时功能，可对抗通过网络的非法拷贝。另外，也可以利用频带限制。假定与机器的通信频带在一定以上，可计算出机器在转送某一种大小的数据所需时间的上限。时期的转送时间超过上述时间时则处理中断。

参考图 22 所示的超时判定单元 4 的构成和图 23 所示的流程图再进行稍微具体的叙述。预先设定超时的时间为 t，比如 LCM1 和 PD12 之间的通信频带宽为 b。比如，以与设置成与 PD12 连接的 MC13 之间的检入的场合为例对超时判定单元 4 的处理动作进行说明。

首先，在用于与设置成与 PD12 连接的 MC13 之间的检入的步骤中的某一读写处理动作开始的同时，由 SMS2 通过判定开始信号输入单元 102 输入判定开始信号(步骤 S20)，与此同时由 SMS2 将与 PD12 之间交换的数据包的大小 s 输入到数据大小输入单元 101(步骤 S21)，控制单元 105 通过时刻取得单元 106 从计时器 107 取得现在的时刻 T (步骤 S22)。与此同时，从带宽存放单元 108 取得带宽 b (步骤 S23)，计算出结束预定时刻 T' (步骤 S24)，存放于最终预定时刻存放单元 111(步骤 S25) 。

结束预定时刻 T' 可由带宽 b 和数据大小 s 从 T' =T+s/b 计算而得出。

在与设置成与 PD12 连接的 MC13 之间的读写处理动作结束的同时，由 SMS2 通过判定结束信号输入单元 103 输入判定结束信号(步骤 S26)，再一次取得现在的时刻 T (步骤 S27)，将前面计算出的结束预定时刻 T' 与现在时刻 T 进行比较(步骤 S28)。在该差值超过超时时间之时，判定“NG”并将其通知 SMS2(步骤 S30)。另外，如图 21 所示，假如与 PD12 进行检出的位于 PC#1 中的 LCM1 与通过网络连接的另外一个 PC#2 相连接，则因为得到“NG”的判定结果，所以 PC#1 中的 LCM1 中其以后的检出处理中断。

或是，也可以在即使经过结束预定时刻 T' 该读写动作也未结束时使判定结果为“NG”。

或是，超时判定单元 4 以两种模式动作。一种是在向数据大小输入单元 101 输入数据大小 s 时，超时判定单元 4 计算出结束预定时刻 T' =T+s/b 并存放到最终预定时刻存放单元 111 中。如超时判定单元 4 接收到判定结束信号，就将现在时刻 T 与最终预定时刻存放单元 111 存放的结束预定时刻 T' 进行比较。前者比后者小的场合，超时判定单元 4 将判定结果 OK 通知 SMS2。其他情况下则通知 SMS2 判定结果为“NG”。

另一种模式的动作是在判定开始信号输入到判定开始信号输入单元 102 的场合，超时判定单元 4 将现在时刻 T+超时时间 t 存放于

最终预定时刻存放单元 111 中。超时判定的动作与另一模式的场合相同。

(隐藏区)

在本发明的 LCM1 中，为了存放检入/检出用的登记帐，利用隐藏区。在以 PC 构成 LCM1 的场合，此隐藏区在硬盘(HDD)上生成。

下面对于在 HDD 上生成隐藏区予以说明。

在 HDD 上，通常存在分区。OS 把分区看成为一个驱动器。各分区内存在多个扇区，数据记录在扇区上。扇区内的数据配置称为逻辑格式。文件系统通常具有文件分配表。文件分配表中记录各文件及目录在扇区上的位置。OS 参考文件分配表取得访问对象文件的位置，到达对象文件。扇区的物理配置称为物理格式。各分区可具有不同的物理格式。扇区的位置由磁头的位置识别。各扇区的开始位置利用磁性标记识别。

对 OS 支持的文件系统，OS 保持有驱动器。驱动器认识该文件系统的物理格式计逻辑格式，沿着分区内的扇区可到达文件分配表及各文件对其内容进行读写。

构成本发明的隐藏区的文件系统如图 24 所示。在通常的文件系统中扇区是等距配置，本文件系统则不是。在第一扇区 SC1 的前头有扇区分配表。扇区分配表以下面的形式记录扇区的位置。

磁头位置#2、磁头位置#3、...、磁头位置#n

顺序地示出第二扇区 SC2、第三扇区 SC3、...、第 n 扇区 SCn 的位置。

扇区分配表加密。此加密的脱密密钥依赖系统的固有 ID. 作为系统的固有 ID，比如，可使用 OS 的 ID，BIOS 的 ID 或 CPU 的 ID.

联网，在第二扇区 SC2 的前头存在有文件分配表 FT。其形式如下。

(文件 1、(扇区号、扇区内的位置))、

(文件 2、(扇区号、扇区内的位置))、

...

扇区内的位置是从扇区前头算起的字节数。文件分配表 FT 也加密。其密钥也依赖系统固有的 ID。

本发明的文件系统的访问是利用特别的驱动单元(图 1 的隐藏区驱动单元 7)进行。隐藏区驱动单元 7 的动作如图 25 所示。该驱动单元 7 还具有变更扇区配置的功能。在扇区更新时的隐藏区驱动单元 7 的动作如图 26 所示。

(认证)

在以上的说明中，比如，在设置 LCM1 与 MC13 之际的相互认证及访问隐藏区之际的进行的认证处理举一例进行说明。此例是现在的一直使用的利用公开密钥加密方式的认证，但本发明不限于此。

在图 20 中，说明两台机器(比如 LCM1 和 MC13)之间从 A 向访问 A 的机器的 B 进行认证的场合。

在此场合，机器 A 保有公开密钥 kp，如可访问机器 A，机器 B 保有与公开密钥对应的保密密钥 ks。如机器 B 接收到机器 A 生成的随机数 R，就将其利用保密密钥 ks 加密(以 ks[R]表示)并将 ks[R]返回机器 A。机器 A 利用公开密钥对 ks[R]解码，如解码的结果与先前生成的随机数 R 相等就可判定机器 B 合法。

其后，以与上述相同的方式机器 B 可对机器 A 进行认证而进行相互认证。在此场合，机器 B 保有公开密钥，机器 A 保有保密密钥，机器 A 将机器 B 生成的随机数以保密密钥加密并由机器 B 利用公开密钥解码，确定是否与先前生成的随机数相等而认证。

如以上所详述，根据本发明，可有效地限制复制内容数而保护内容的著作权。

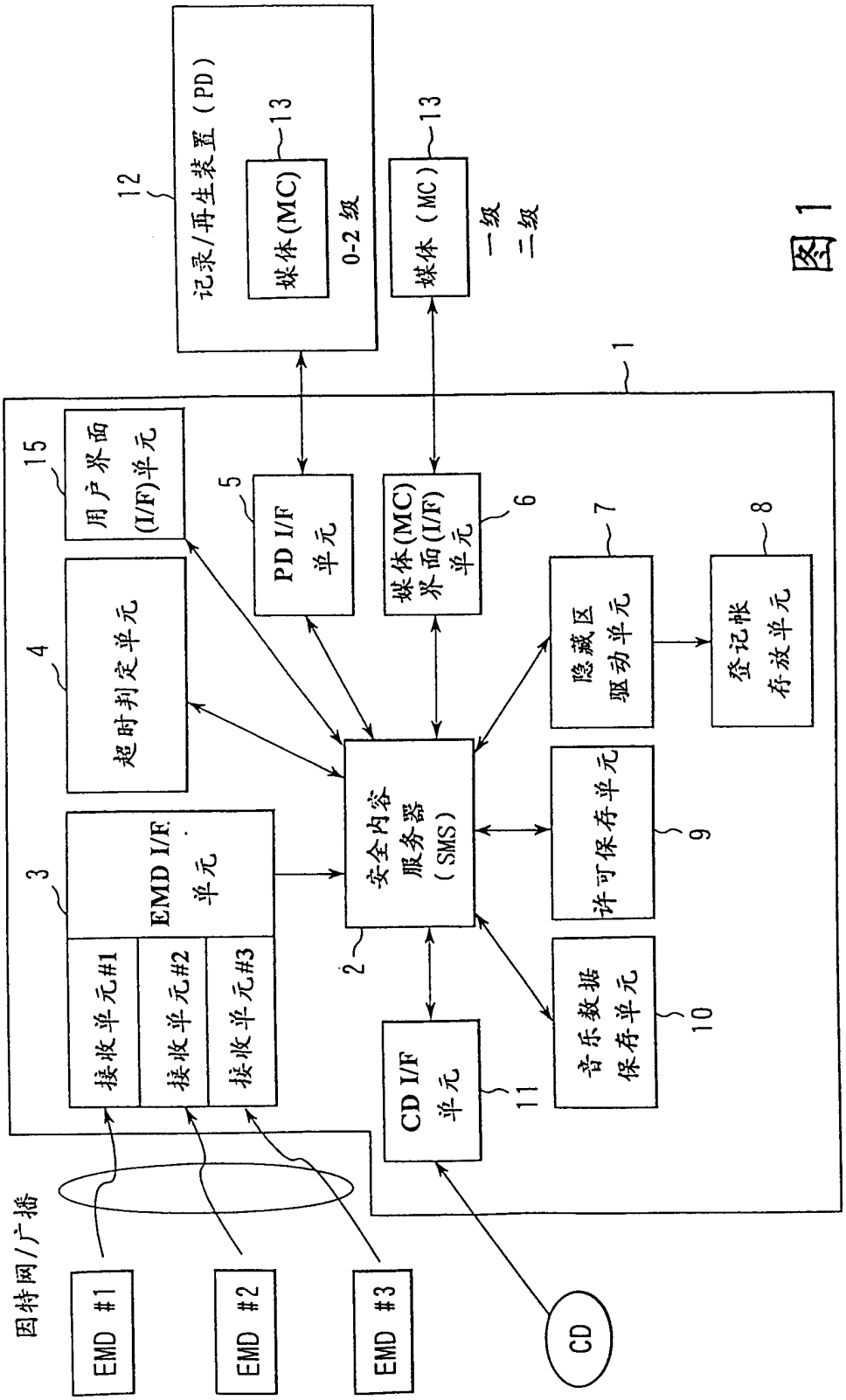

因特网/广播
EMD #1
EMD #2
EMD #3
CD
接收单元#1
接收单元#2
接收单元#3
EMD I/F 单元
3
超时判定单元
4
用户界面 (I/F)单元
15
安全内容服务器 (SMS)
2
PD I/F 单元
5
媒体(MC)界面(I/F)单元
6
隐藏区驱动单元
7
登记帐存放单元
8
许可保存单元
9
音乐数据保存单元
10
CD I/F 单元
11
记录/再生装置 (PD)
12
媒体(MC)
13
0-2 级
媒体 (MC)
13
一级
二级
1

图 1

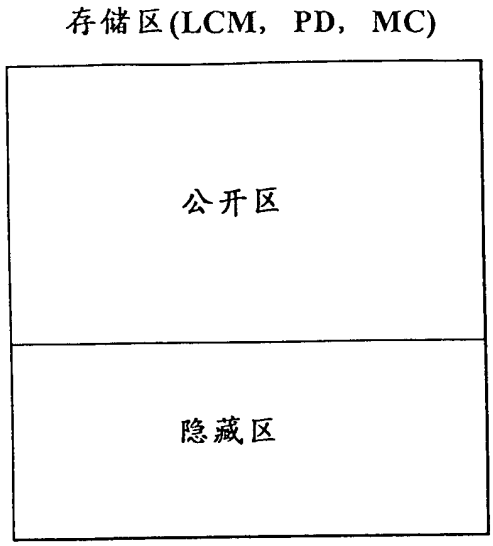

存储区(LCM，PD，MC)
公开区
隐藏区

图 2

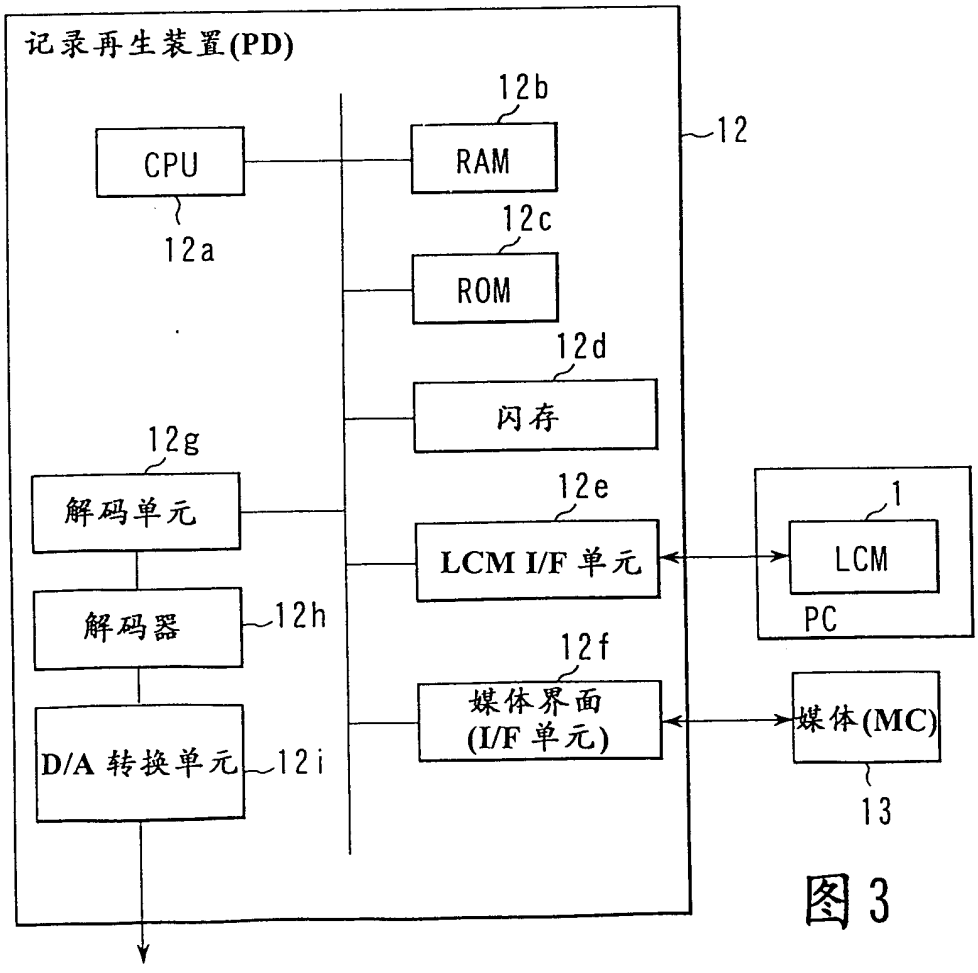

记录再生装置(PD)
12b
12
CPU
RAM
12a
12c
ROM
12d
闪存
12g
解码单元
12e
LCM I/F 单元
1
LCM
PC
解码器
12h
12f
媒体界面
(I/F 单元)
媒体(MC)
D/A 转换单元
12i
13

图 3

图4A

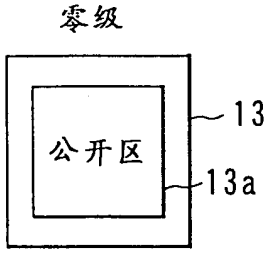

零级
公开区
13
13a

图4B

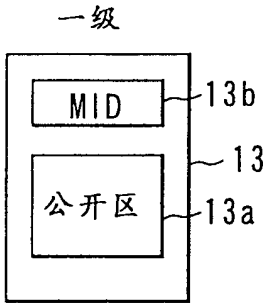
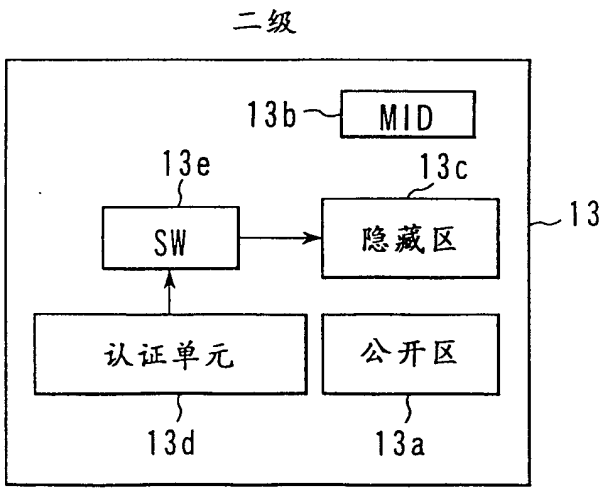

一级
MID
13b
13
公开区
13a

图4C


二级
13b
MID
13e
13c
SW
隐藏区
13
认证单元
公开区
13d
13a

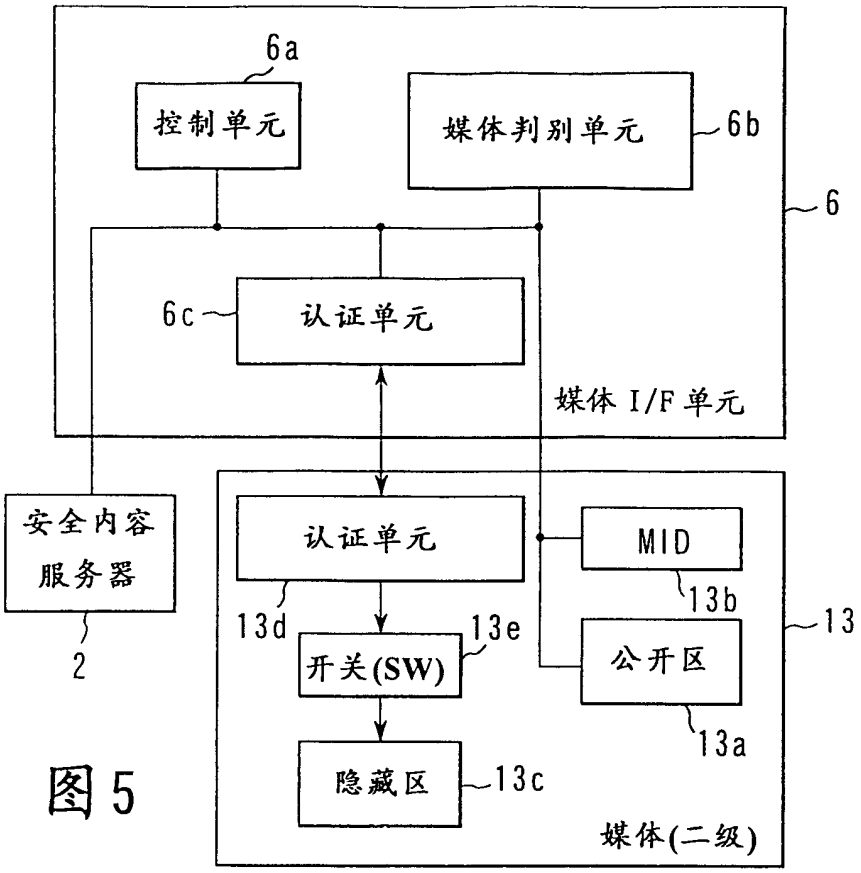

6a
控制单元
媒体判别单元
6b
6
6c
认证单元
媒体 I/F 单元
安全内容
服务器
2
认证单元
MID
13b
13d
13e
开关(SW)
公开区
13
13a
隐藏区
13c
媒体(二级)

图 5

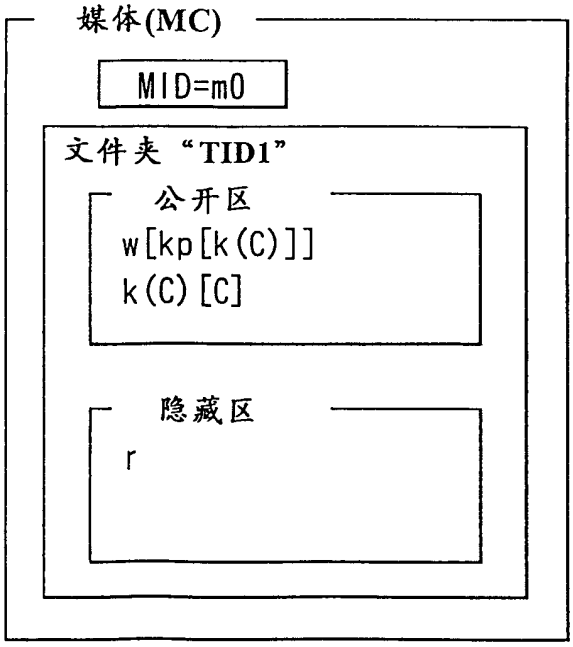

媒体(MC)
MID=m0
文件夹“TID1”
公开区
w[kp[k(C)]]
k(C)[C]
隐藏区
r

图 6

图7A

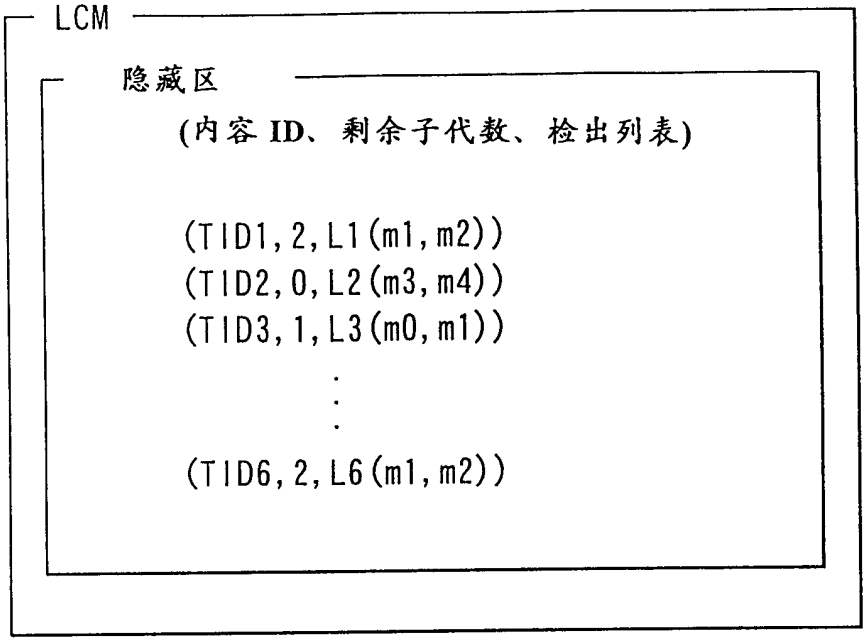

LCM
隐藏区
(内容ID、剩余子代数、检出列表)
(TID1,2,L1(m1,m2))
(TID2,0,L2(m3,m4))
(TID3,1,L3(m0,m1))
(TID6,2,L6(m1,m2))

图7B

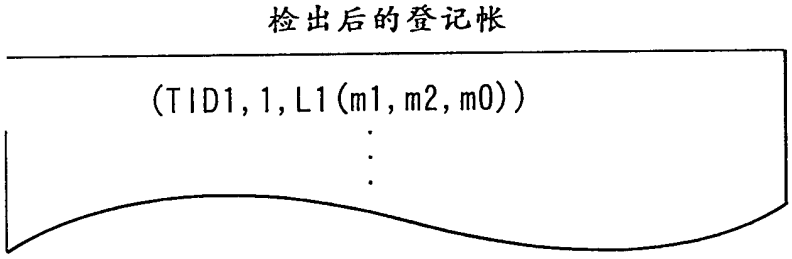

检出后的登记帐
(TID1,1,L1(m1,m2,m0))

图7C

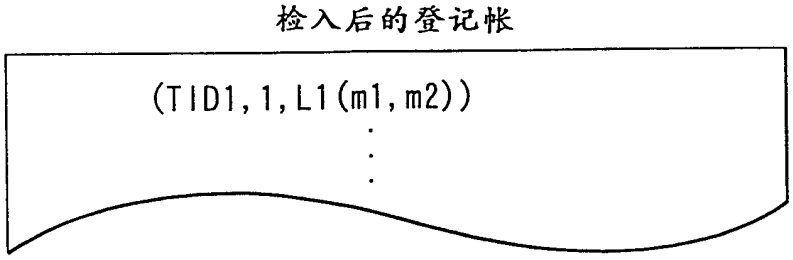

检入后的登记帐
(TID1,1,L1(m1,m2))

图 8A

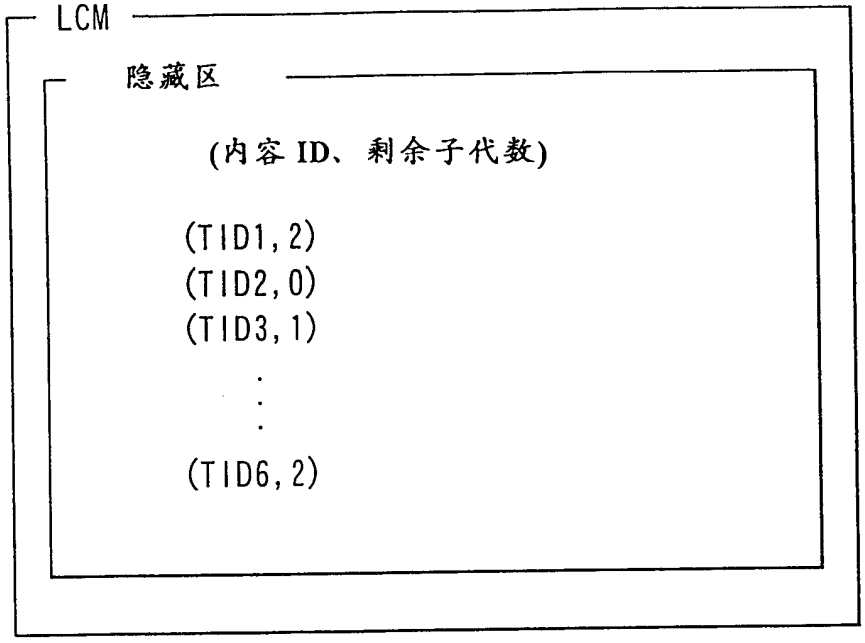
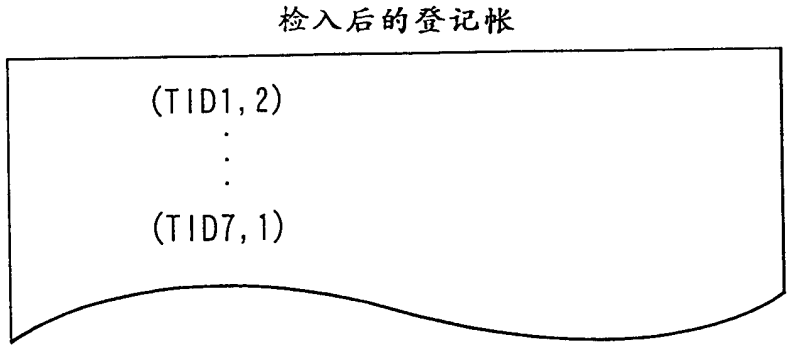

LCM
隐藏区
(内容 ID、剩余子代数)
(TID1,2)
(TID2,0)
(TID3,1)
(TID6,2)

图 8B


检入后的登记帐
(TID1,2)
(TID7,1)

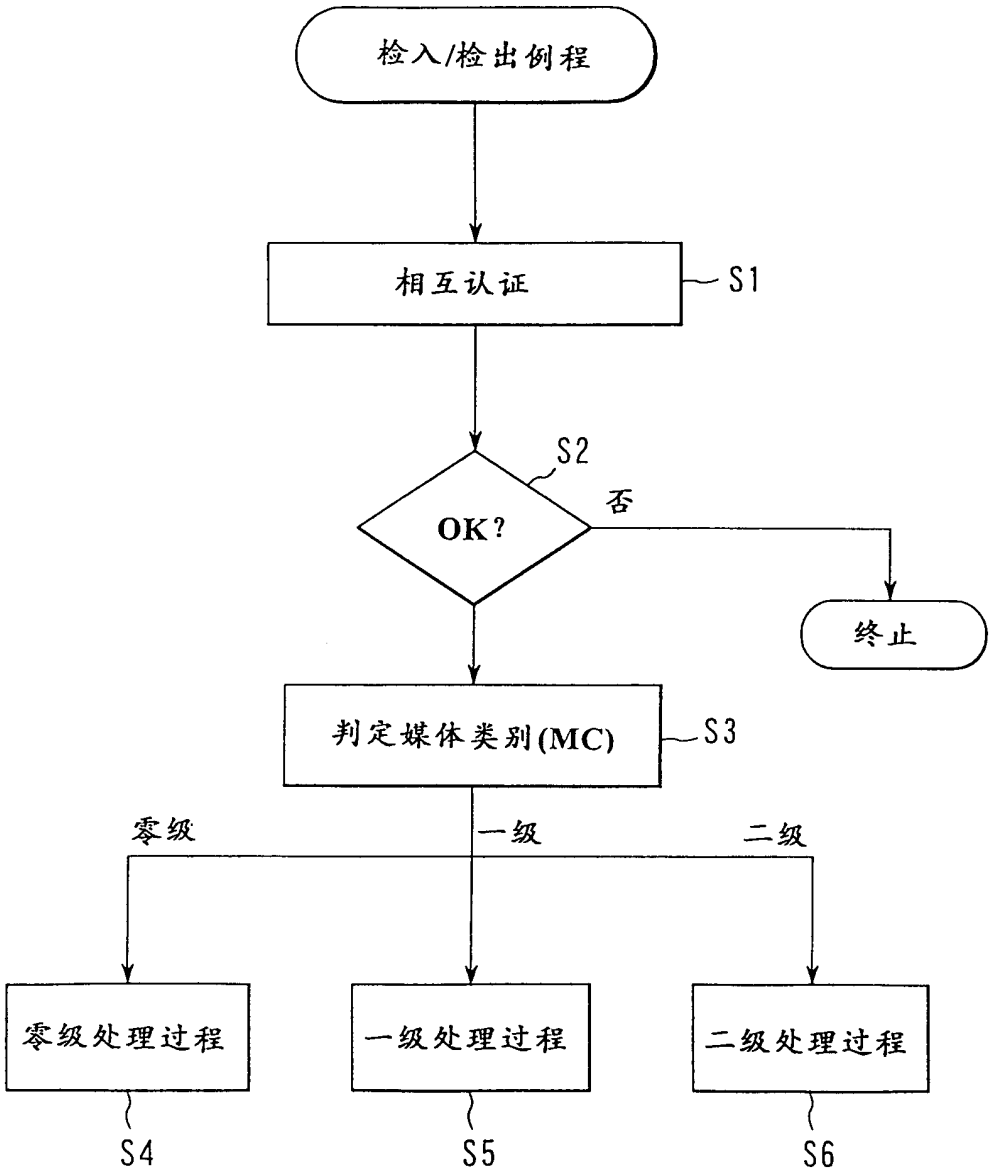

检入/检出例程
相互认证
S1
S2
OK?
否
终止
判定媒体类别(MC)
S3
零级
一级
二级
零级处理过程
一级处理过程
二级处理过程
S4
S5
S6

图 9

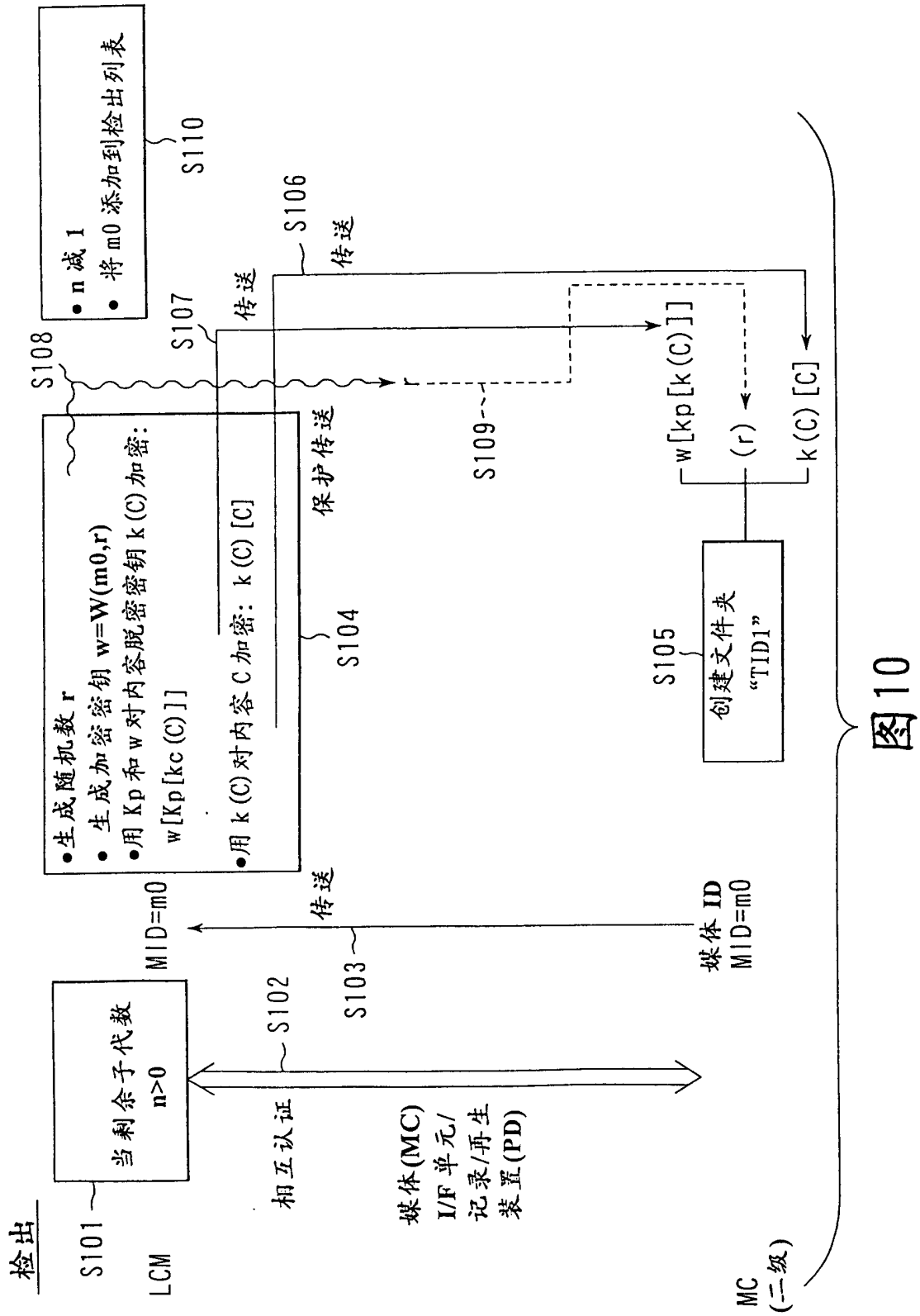

检出
S101
LCM
当剩余子代数 n>0
S102
相互认证
S103
传送
MID=m0
媒体(MC) I/F 单元/ 记录/再生 装置(PD)
媒体 ID MID=m0
S104
•生成随机数 r
• 生成加密密钥 w=W(m0,r)
•用 Kp 和 w 对内容脱密密钥 k(C)加密: w[Kp[kc(C)]]
•用 k(C)对内容 C 加密: k(C)[C]
保护传送
S105
创建文件夹 "TID1"
S106
传送
S107
S108
• n 减 1
• 将 m0 添加到检出列表
S110
S109
r
w[kp[k(C)]]
(r)
k(C)[C]
MC (二级)

图 10

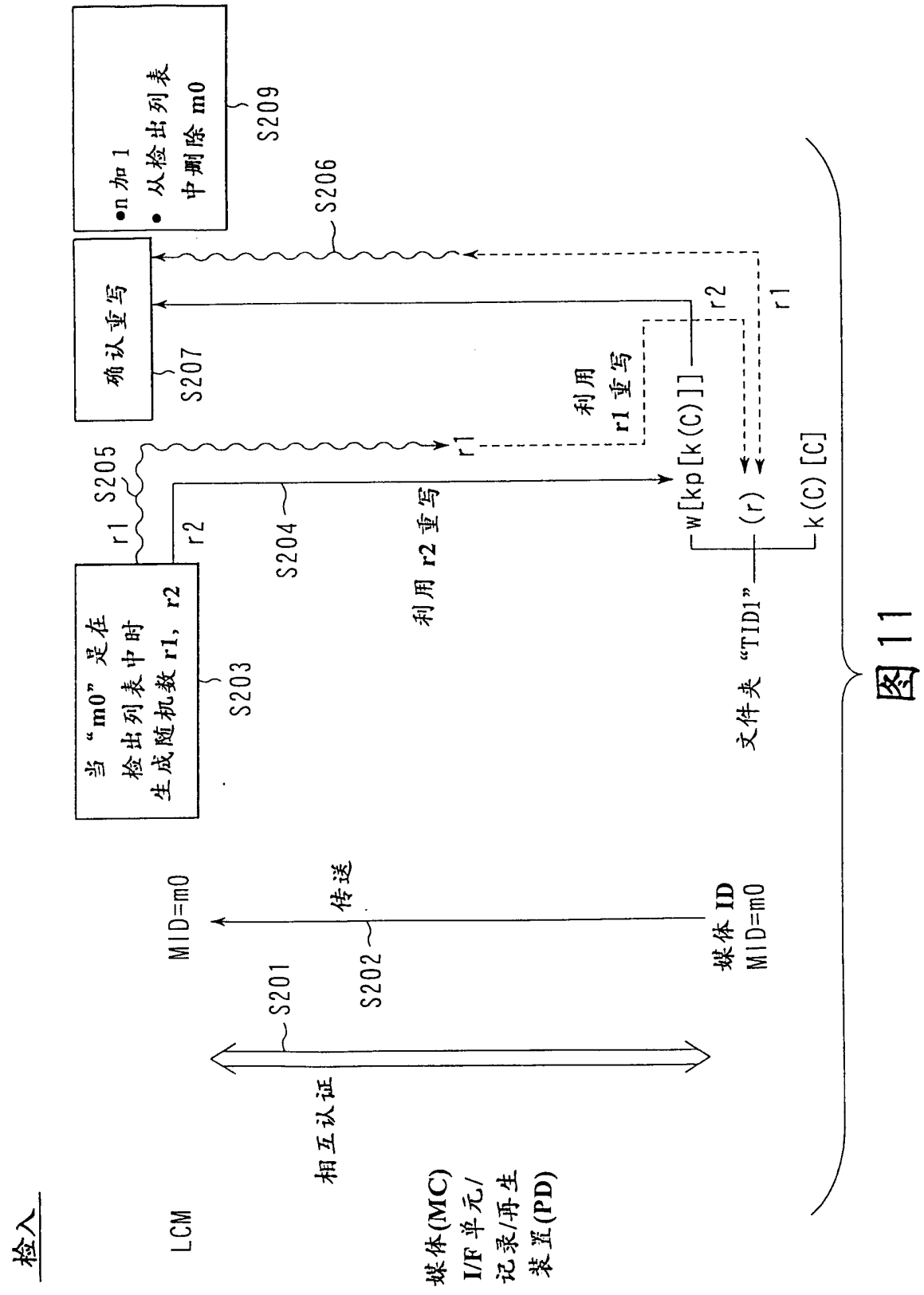

检入
LCM
媒体(MC)
I/F 单元/
记录/再生
装置(PD)
相互认证
S201
MID=m0
传送
S202
媒体 ID
MID=m0
当 "m0" 是在
检出列表中时
生成随机数 r1, r2
S203
r1
S205
r2
S204
利用 r2 重写
r1
S206
确认重写
S207
•n 加 1
• 从检出列表
中删除 m0
S209
利用
r1 重写
w[kp[k(C)]]
r2
r1
(r)
k(C) [C]
文件夹 "TID1"

图 11

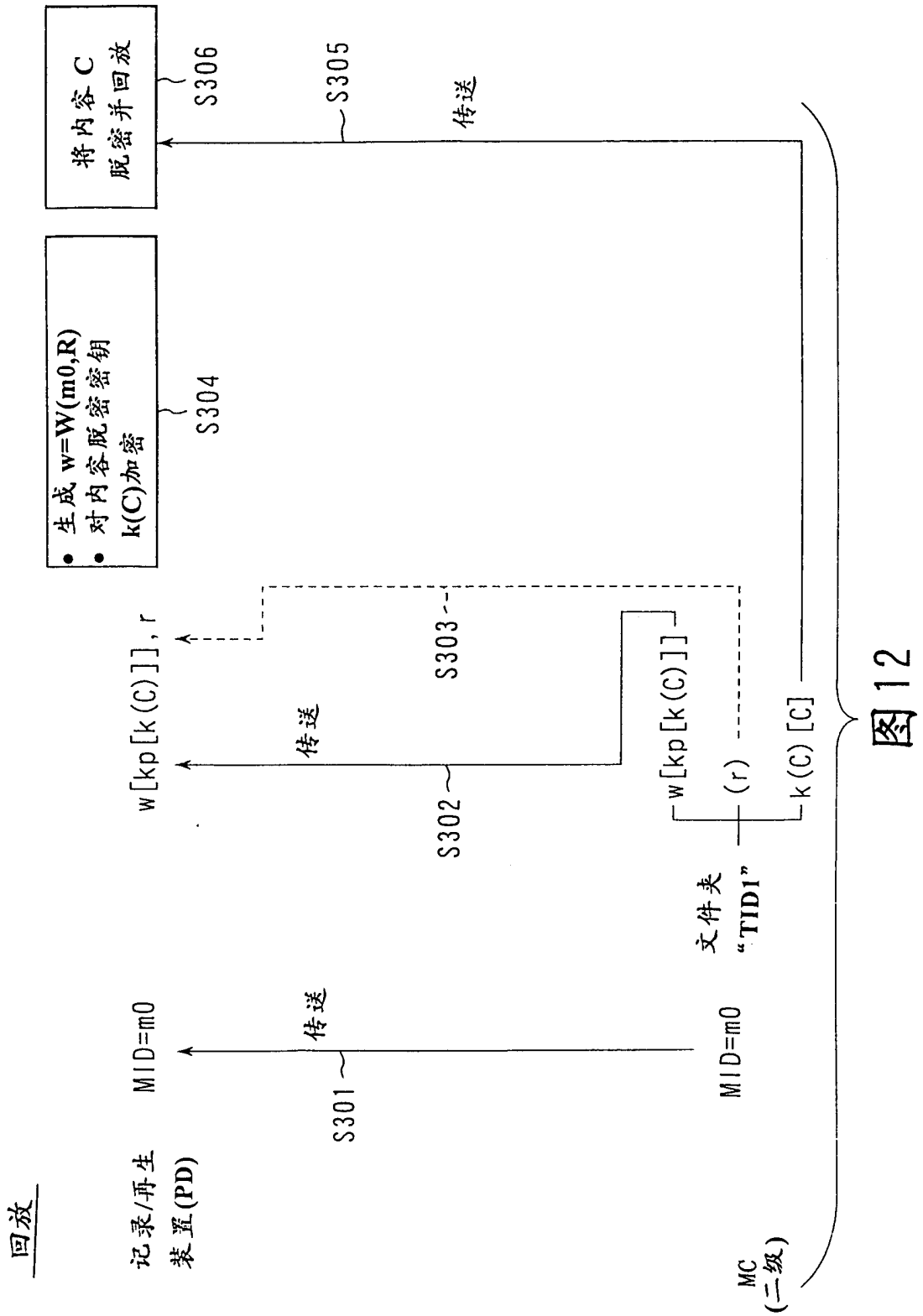

回放
记录/再生装置(PD)
MC(二级)
MID=m0
传送
S301
w[kp[k(C)]],r
传送
S302
S303
文件夹"TID1"
MID=m0
w[kp[k(C)]]
(r)
k(C)[C]
• 生成 w=W(m0,R)
• 对内容加密 k(C)加密
S304
S305
传送
将内容C脱密并回放
S306

图12

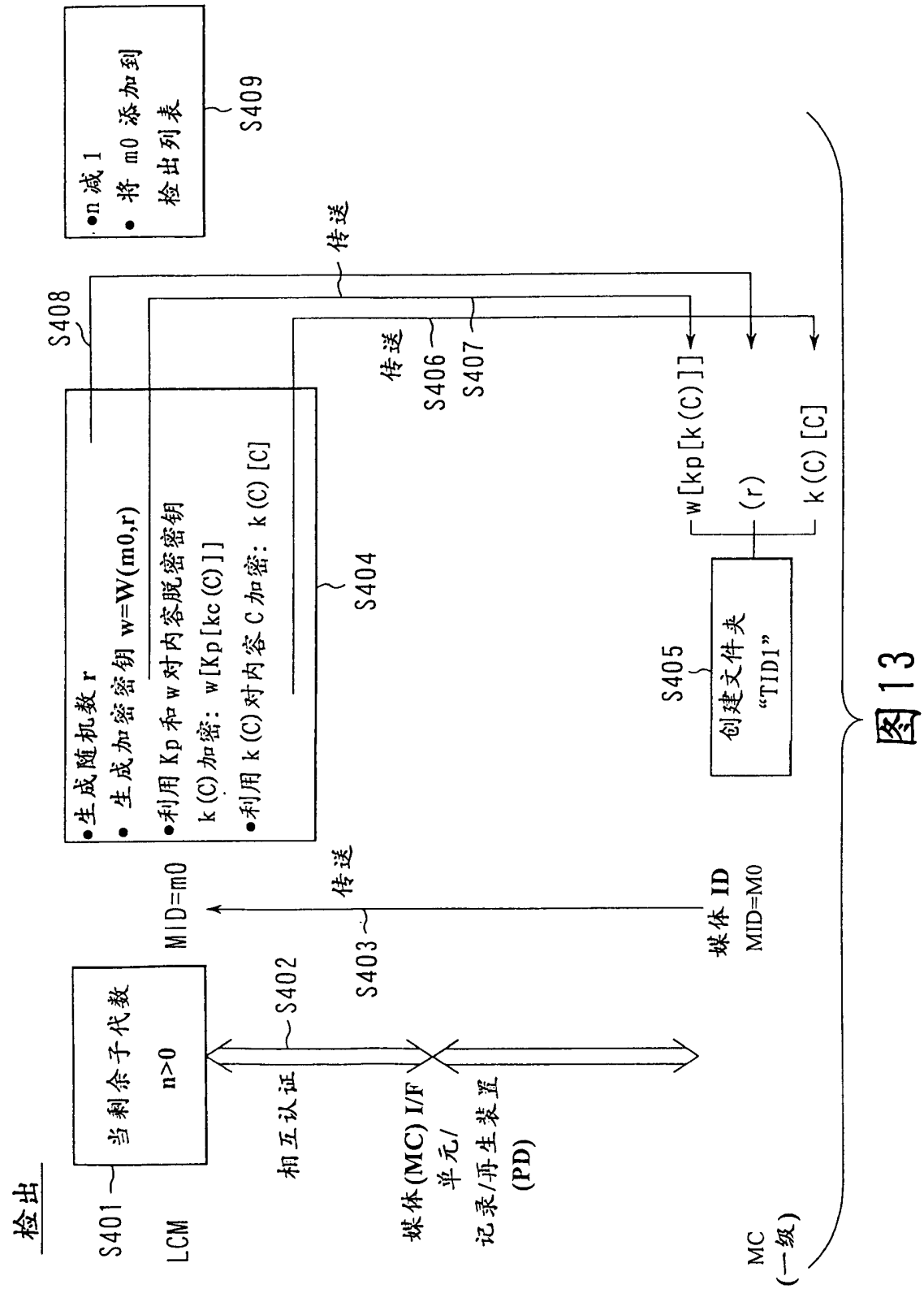

检出
S401
LCM
当剩余子代数
n>0
S402
相互认证
S403
MID=m0
传送
媒体(MC) I/F
单元/
记录/再生装置
(PD)
媒体 ID
MID=M0
MC
(一级)
•生成随机数 r
• 生成加密密钥 w=W(m0,r)
•利用 Kp 和 w 对内容脱密密钥
k(C)加密: w[Kp[kc(C)]]
•利用 k(C)对内容 C 加密: k(C)[C]
S404
传送
S406
S407
S405
创建文件夹
"TID1"
w[kp[k(C)]]
(r)
k(C)[C]
传送
S408
•n 减 1
• 将 m0 添加到
检出列表
S409

图 13

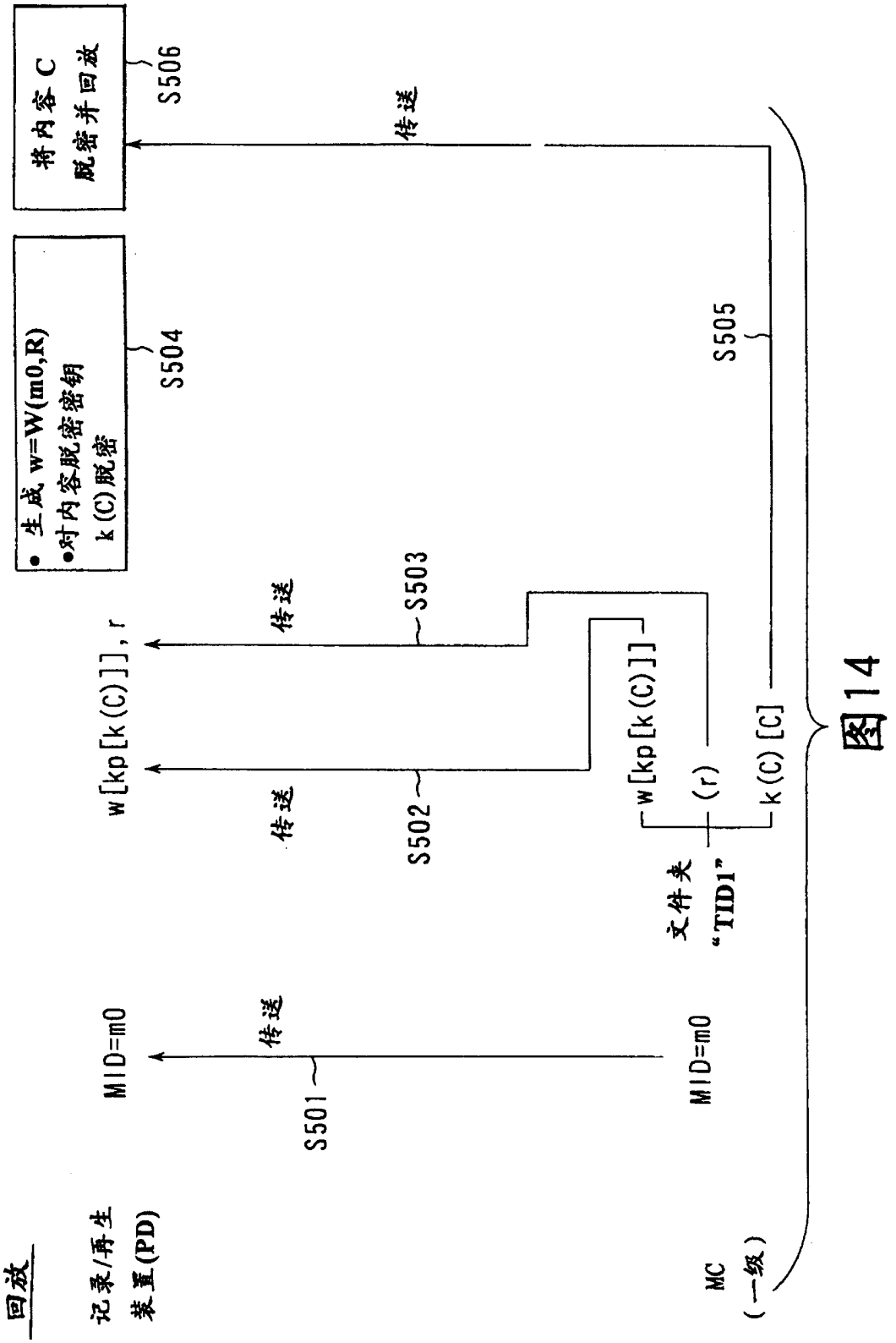

回放
记录/再生装置(PD)
MC（一级）
MID=m0
传送
S501
w[kp[k(C)]],r
传送
S502
S503
w[kp[k(C)]]
(r)
k(C)[C]
文件夹"TID1"
MID=m0
• 生成 w=W(m0,R)
•对内容脱密密钥 k(C)脱密
S504
S505
传送
将内容 C 脱密并回放
S506

图14

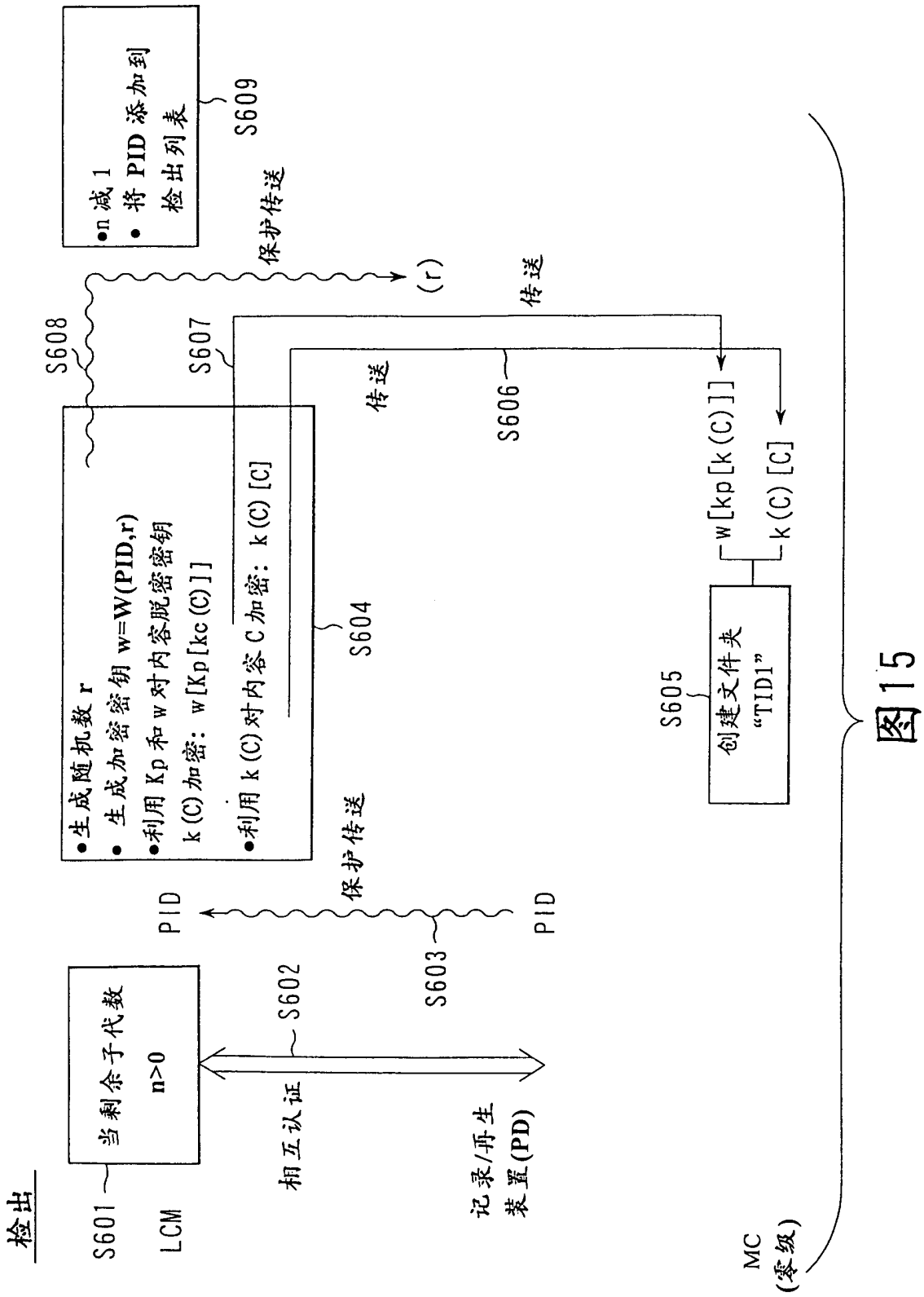

检出
S601
LCM
当剩余子代数
n>0
S602
相互认证
记录/再生
装置(PD)
S603
PID
保护传送
PID
S604
•生成随机数 r
• 生成加密密钥 w=W(PID,r)
•利用 Kp 和 w 对内容脱密密钥
k(C)加密: w[Kp[kc(C)]]
•利用 k(C)对内容 C 加密: k(C)[C]
S605
创建文件夹
"TID1"
w[kp[k(C)]]
k(C)[C]
S606
传送
S607
传送
S608
(r)
保护传送
S609
•n 减 1
• 将 PID 添加到
检出列表
MC
(零级)

图15

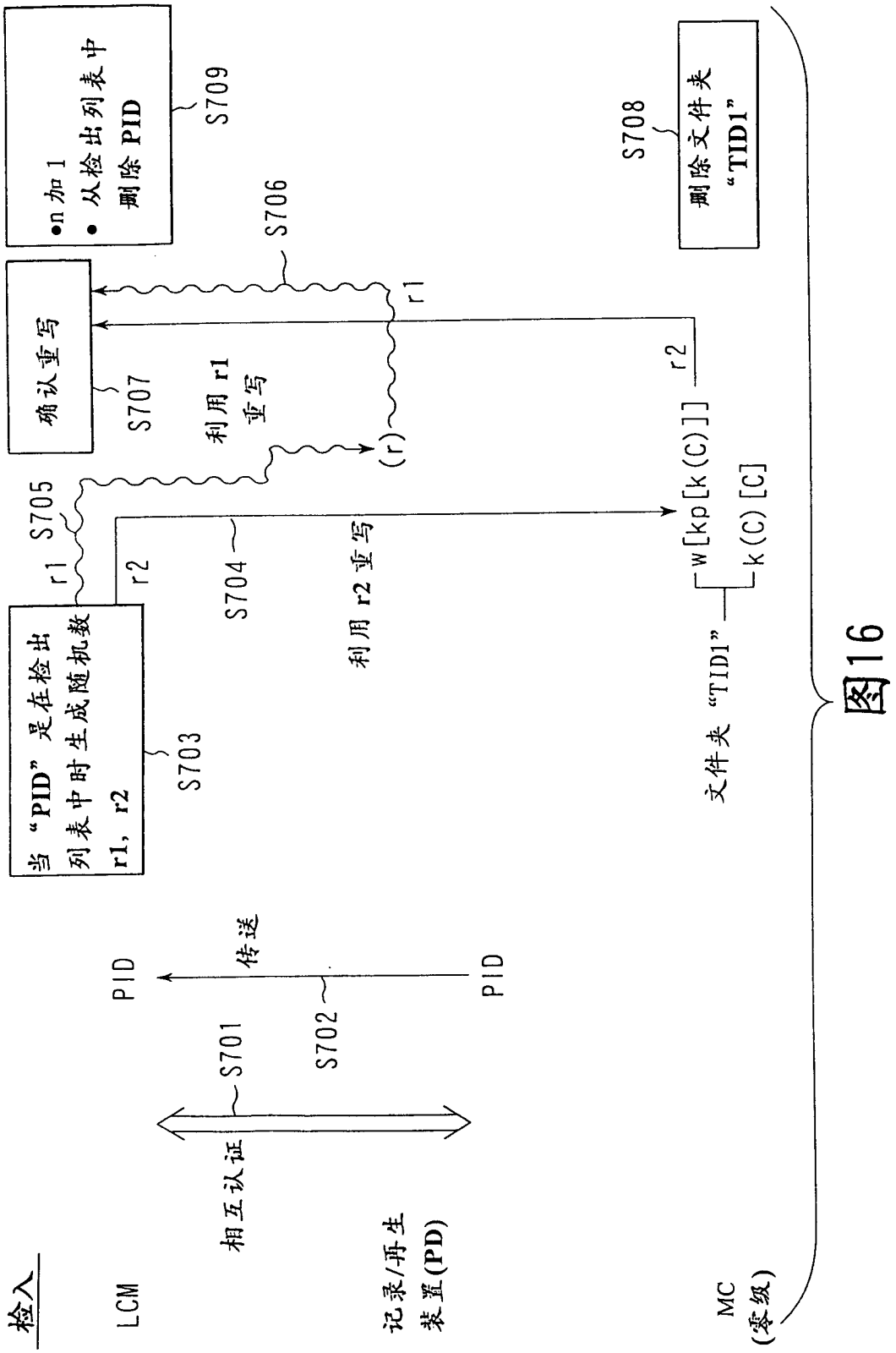

检入
LCM
相互认证
记录/再生
装置(PD)
MC
(零级)
PID
传送
PID
S701
S702
当“PID”是在检出
列表中时生成随机数
r1，r2
S703
r1
r2
S705
S704
利用 r2 重写
文件夹 “TID1”
w[kp[k(C)]]
k(C) [C]
r2
确认重写
S707
利用 r1
重写
(r)
r1
S706
•n 加 1
• 从检出列表中
删除 PID
S709
S708
删除文件夹
“TID1”

图16

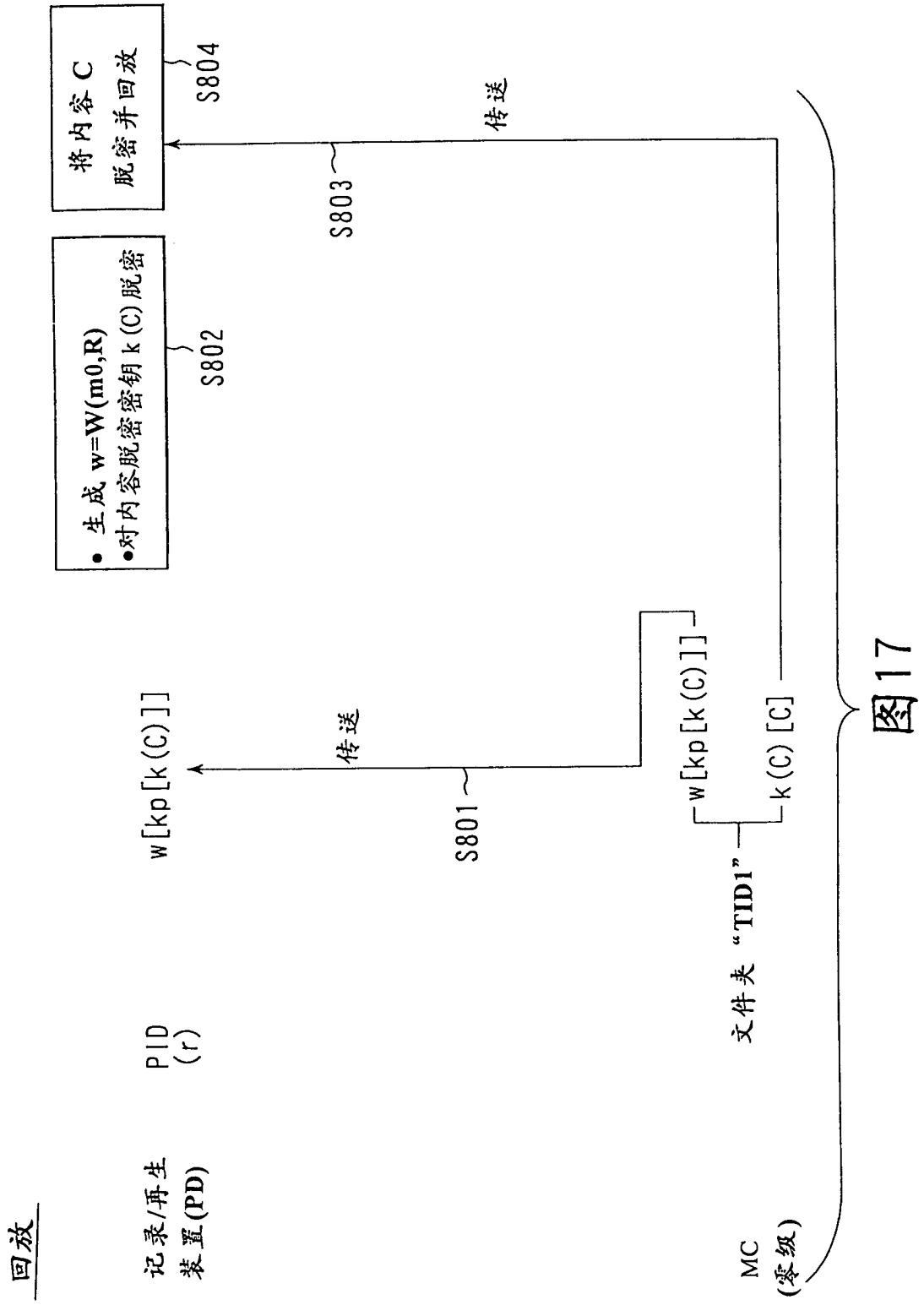

回放
记录/再生装置(PD)
PID (r)
MC (零级)
w[kp[k(C)]]
S801
传送
w[kp[k(C)]]
文件夹 "TID1"
k(C) [C]
传送
S803
• 生成 w=W(m0,R)
•对内容脱密密钥 k(C) 脱密
S802
将内容 C 脱密并回放
S804

图 17

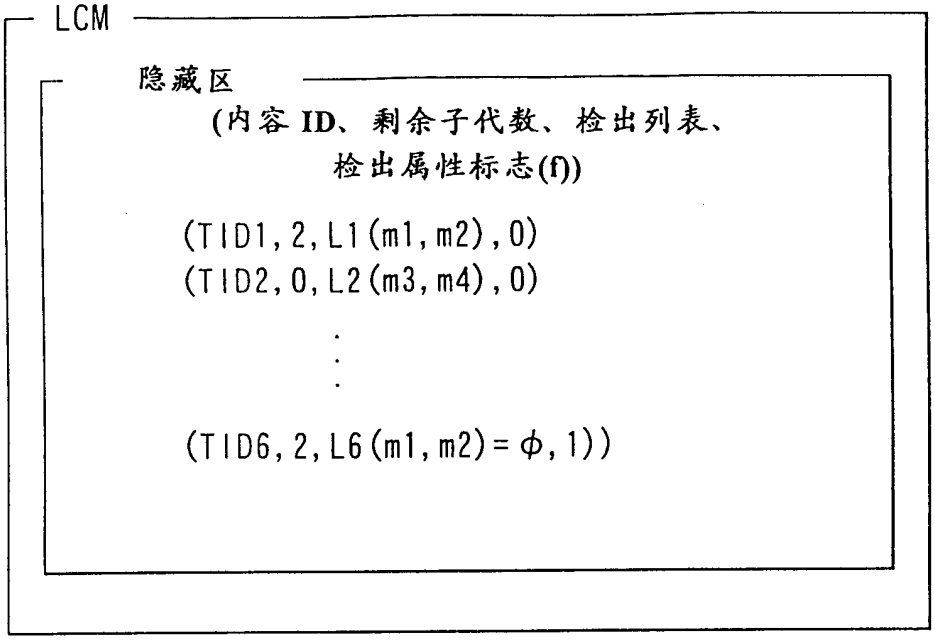


图18A

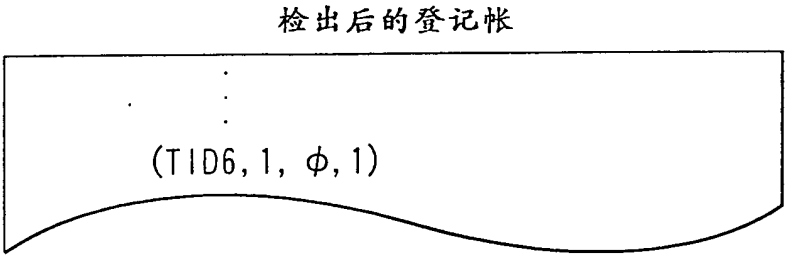


图18B

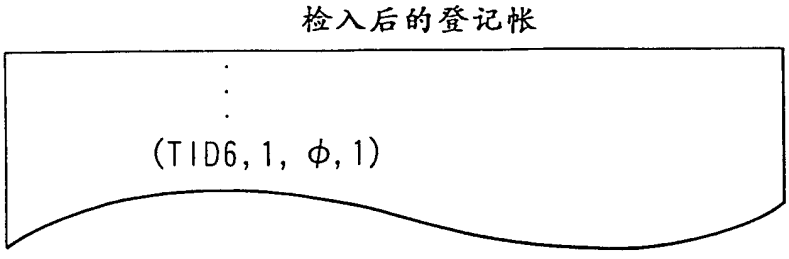


图18C

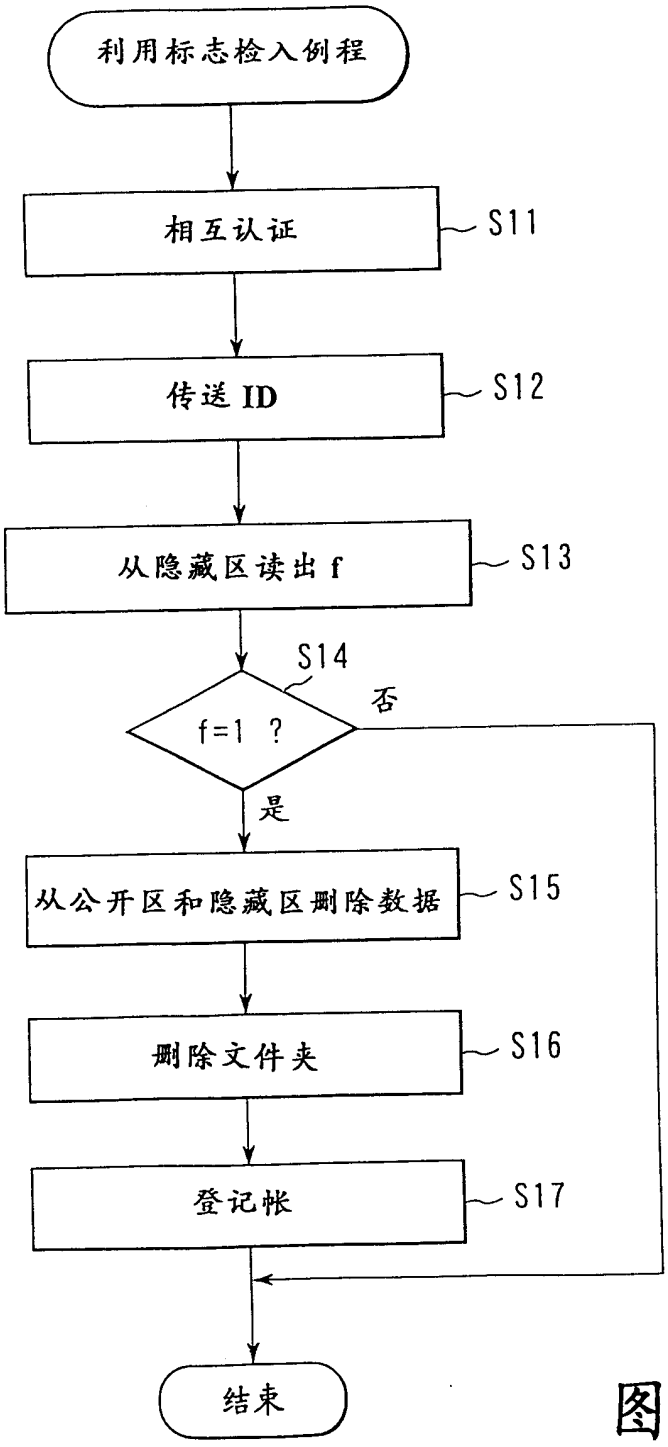

利用标志检入例程
相互认证
S11
传送 ID
S12
从隐藏区读出 f
S13
S14
f=1 ?
否
是
从公开区和隐藏区删除数据
S15
删除文件夹
S16
登记帐
S17
结束

图19

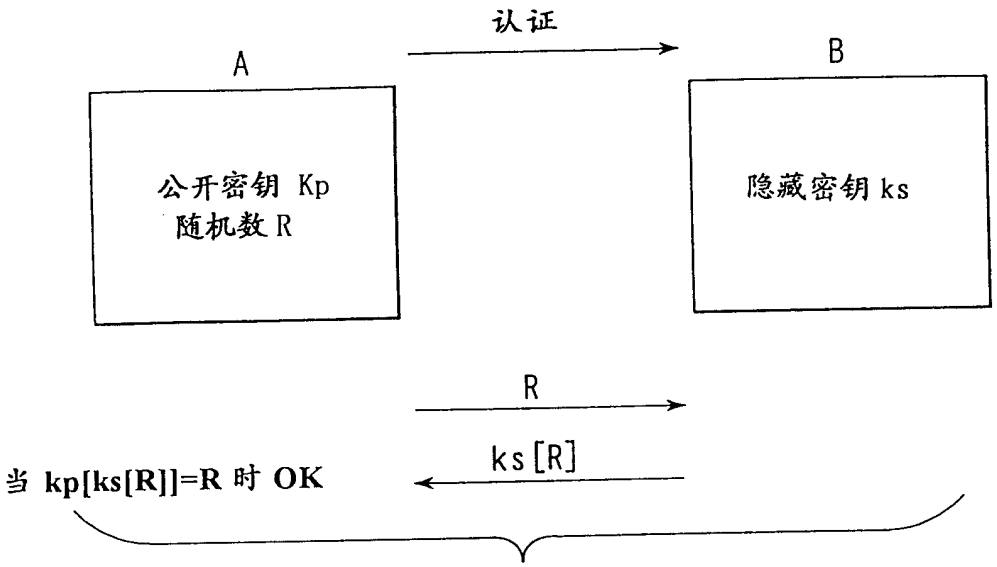

认证
A
B
公开密钥 Kp
随机数 R
隐藏密钥 ks
R
ks[R]
当 kp[ks[R]]=R 时 OK

图 20

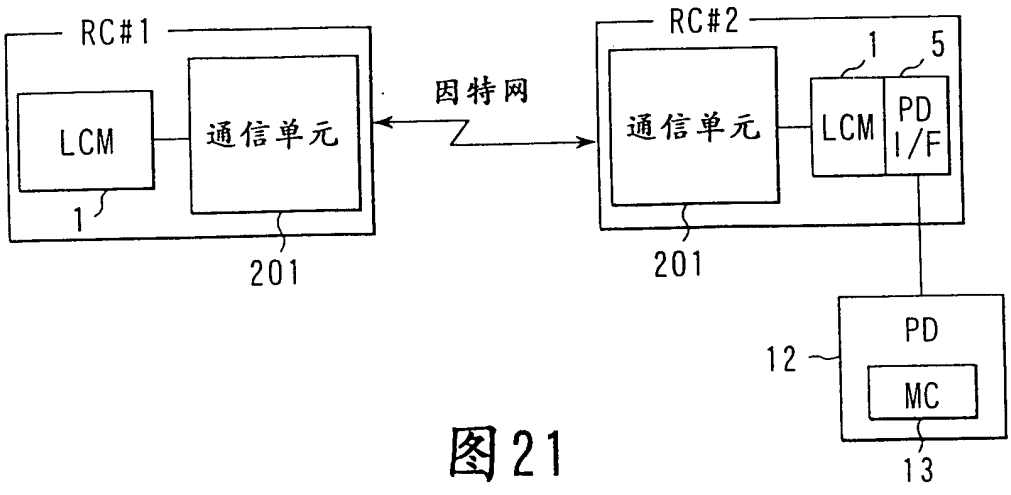

RC#1
LCM
通信单元
1
201
因特网
RC#2
通信单元
LCM
1
5
PD
I/F
201
PD
MC
12
13

图 21

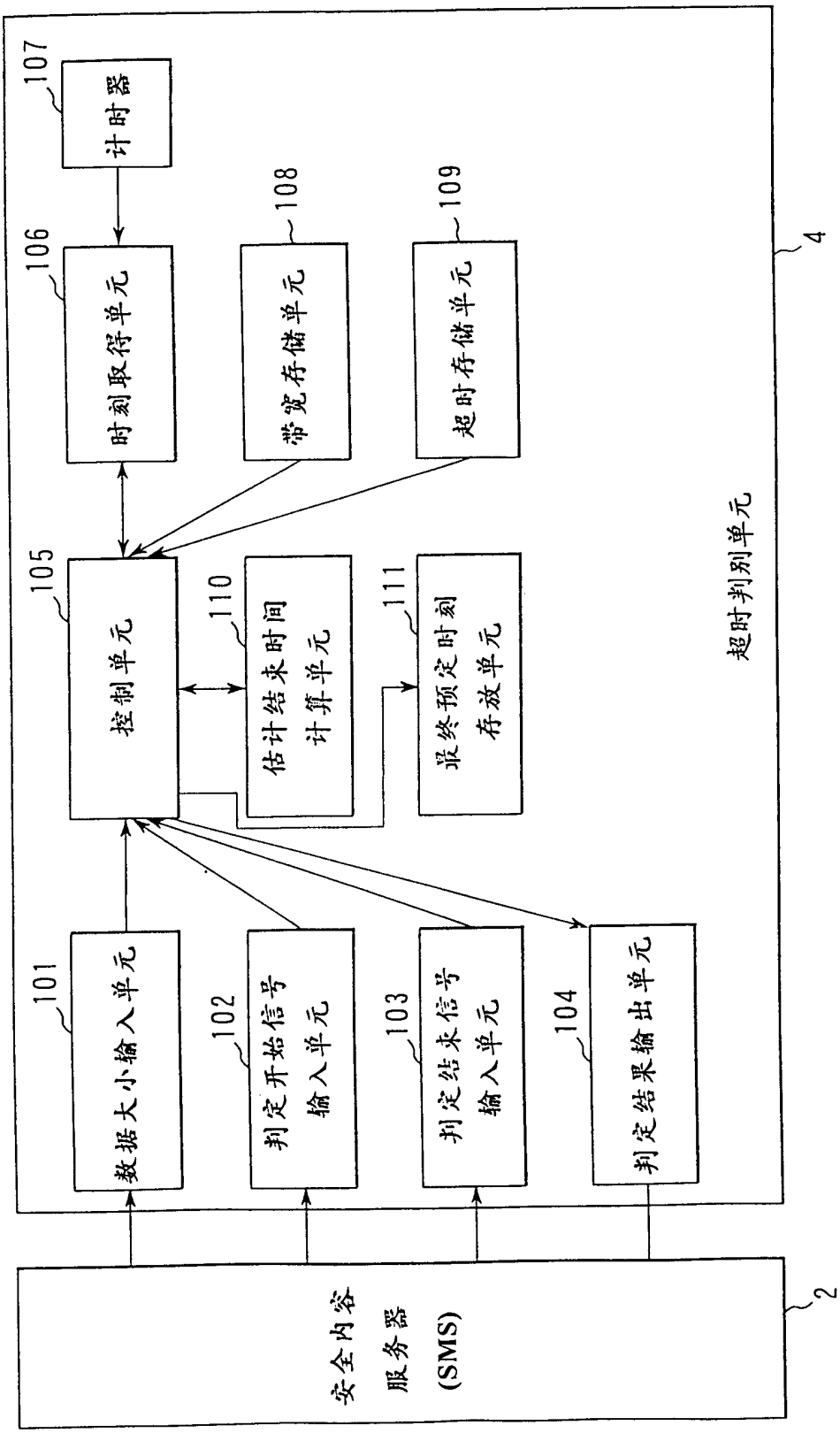

安全内容
服务器
(SMS)
2
数据大小输入单元
101
判定开始信号
输入单元
102
判定结束信号
输入单元
103
判定结果输出单元
104
控制单元
105
时刻取得单元
106
计时器
107
带宽存储单元
108
超时存储单元
109
估计结束时间
计算单元
110
最终预定时刻
存放单元
111
超时判别单元
4

图 22

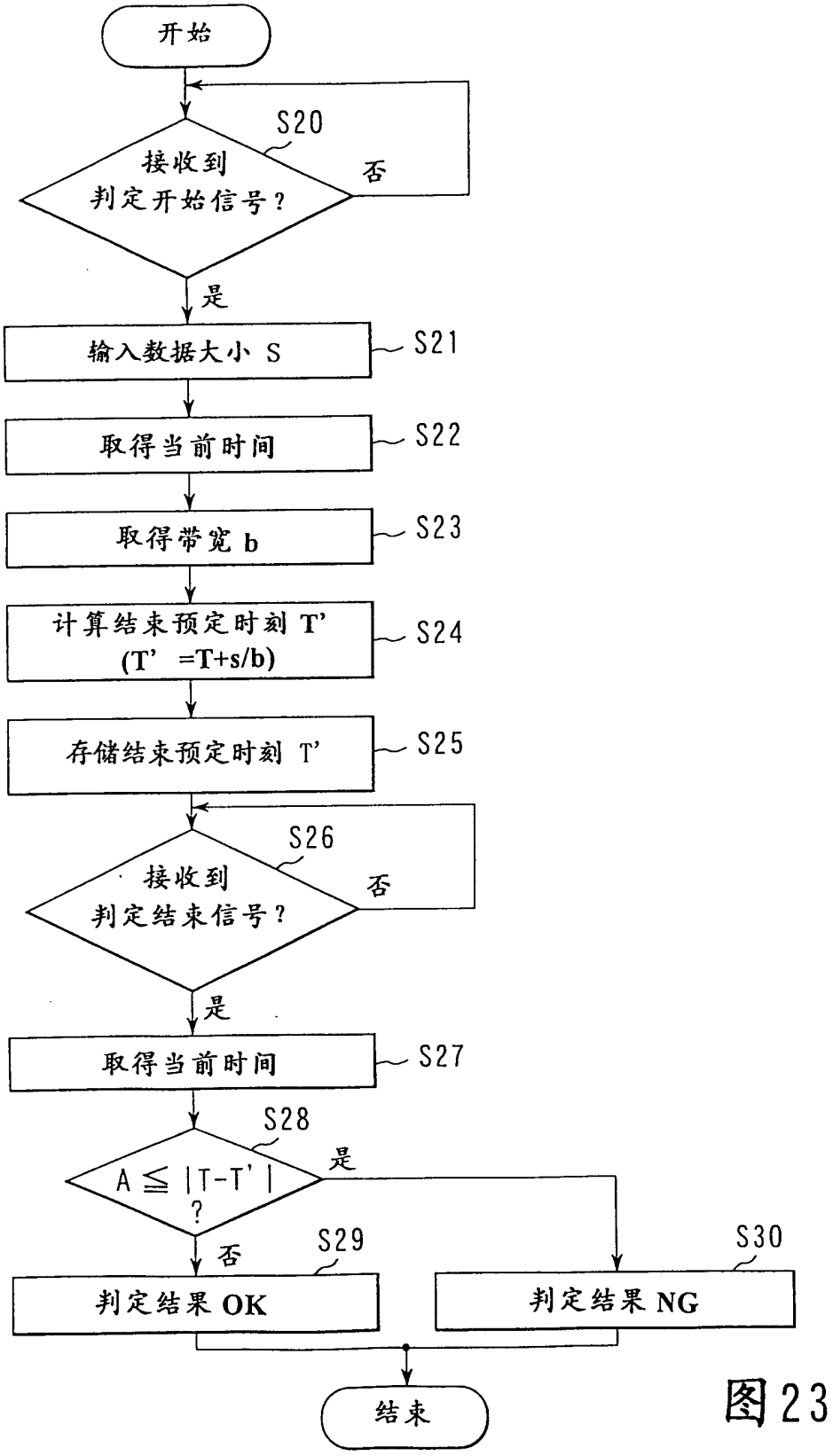

开始
S20
接收到
判定开始信号？
否
是
输入数据大小 S
S21
取得当前时间
S22
取得带宽 b
S23
计算结束预定时刻 T'
(T' =T+s/b)
S24
存储结束预定时刻 T'
S25
S26
接收到
判定结束信号？
否
是
取得当前时间
S27
S28
A ≦ |T-T'|
？
是
否
S29
S30
判定结果 OK
判定结果 NG
结束

图23

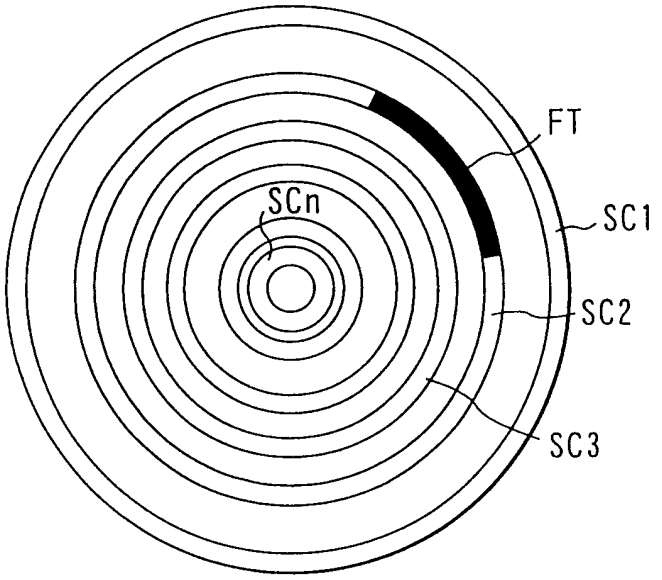

FT
SCn
SC1
SC2
SC3

图24

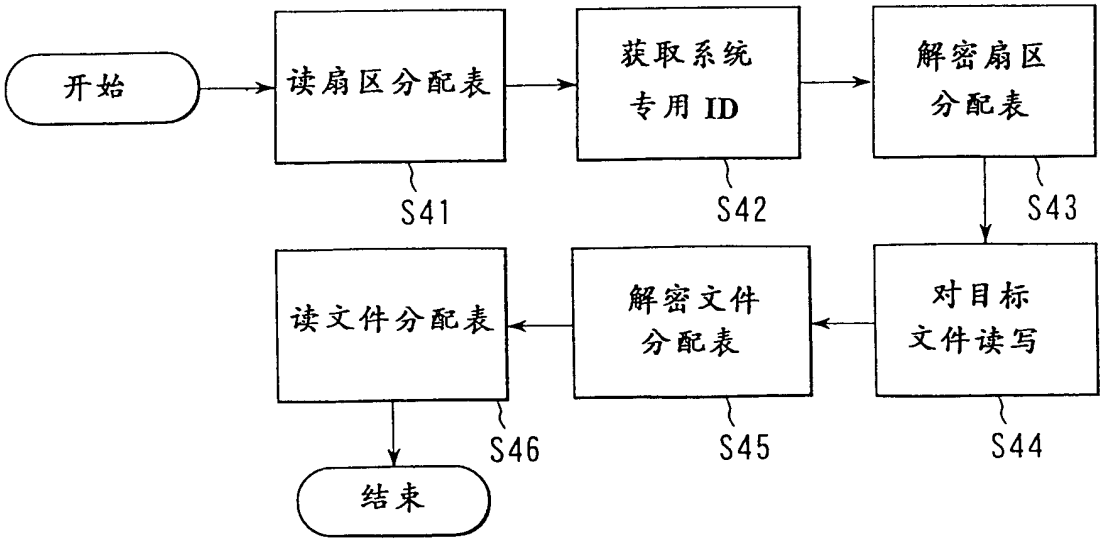

开始
读扇区分配表
获取系统
专用 ID
解密扇区
分配表
S41
S42
S43
读文件分配表
解密文件
分配表
对目标
文件读写
S46
S45
S44
结束

图25

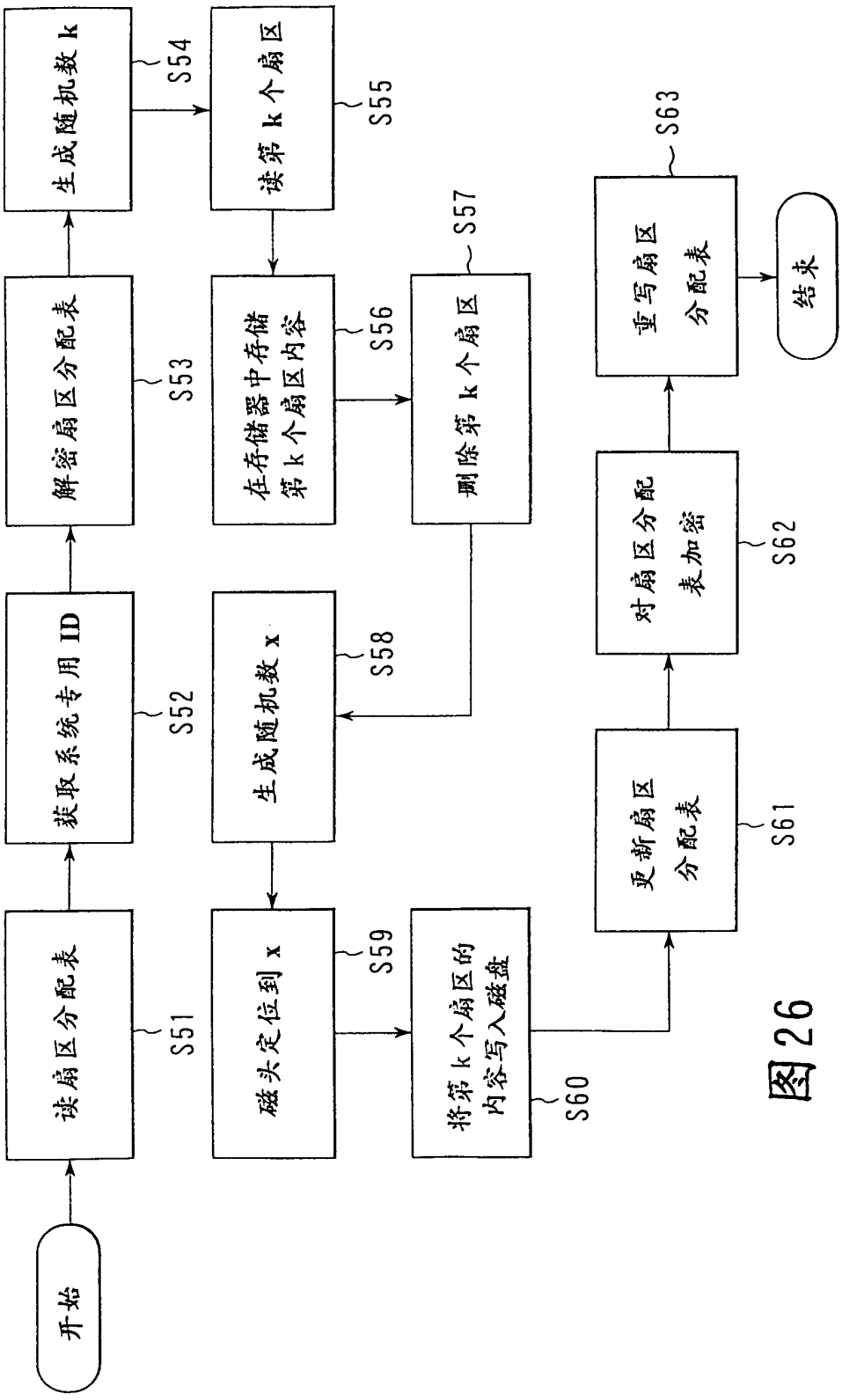

开始
读扇区分配表
S51
获取系统专用 ID
S52
解密扇区分配表
S53
生成随机数 k
S54
读第 k 个扇区
S55
在存储器中存储第 k 个扇区内容
S56
删除第 k 个扇区
S57
生成随机数 x
S58
磁头定位到 x
S59
将第 k 个扇区的内容写入磁盘
S60
更新扇区分配表
S61
对扇区分配表加密
S62
重写扇区分配表
S63
结束

图 26