[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G11B 20/00 (2006.01)
G11B 20/10 (2006.01)
H04L 9/08 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510119200.X

[43] 公开日 2006 年 8 月 2 日

[11] 公开号 CN 1811954A

[22] 申请日 2005.9.29
[21] 申请号 200510119200.X
[30] 优先权
[32] 2004.9.30 [33] JP [31] 2004-288469
[71] 申请人 株式会社东芝
地址 日本东京都
[72] 发明人 小岛正

[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 李春晖

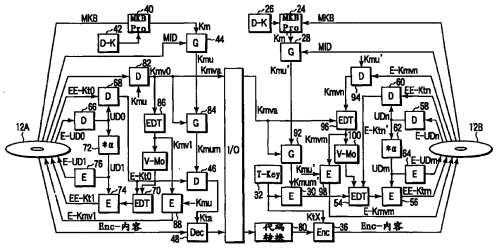
权利要求书 4 页 说明书 28 页 附图 17 页

[54] 发明名称

内容管理方法和记录媒体

[57] 摘要

本发明涉及内容管理方法和记录媒体。在该方法中，将内容数据从第一记录媒体移动到第二记录媒体上，第一记录媒体记录了加密内容(Enc-content)(密钥是第一密钥(Kt))、第一已加密密钥(E-Kt)(密钥是第四密钥(Kmum)，该第四密钥从第二密钥(Kmv)和第三密钥(Kmu)产生)以及第二已加密密钥(E-Kmv)(密钥是所述第三密钥(Kmu))。该方法包括：将从所述第一记录媒体中读取的所述加密内容(Enc-content)和所述第二已加密密钥(E-Kmv)解密，以获得所述明文内容和所述第二密钥；将所述明文内容和所述第二密钥传送给所述第二记录媒体；以及从所述第一记录媒体中删除所述第二已加密密钥(E-Kmv)。



1、一种内容管理方法，用于将内容数据从第一存储媒体移动到第二存储媒体，

其中所述第一存储媒体记录：

加密内容，该加密内容是用第一密钥加密明文内容获得的，

第一已加密密钥，该第一已加密密钥是用第四密钥加密第一密钥而获得的，该第四密钥从第二密钥和第三密钥产生，以及

第二已加密密钥，该第二已加密密钥是用所述第三密钥加密所述第二密钥而获得的，

所述方法的特征在于包括：

将从所述第一记录媒体中读取的所述加密内容和所述第二已加密密钥解密，以获得所述明文内容和所述第二密钥；

将所述明文内容和所述第二密钥传送给所述第二记录媒体；以及

从所述第一记录媒体中删除所述第二已加密密钥，

由此使所述加密内容和所述第一已加密密钥保持记录在所述第一记录媒体上，但禁止所述加密内容被解密。

2、一种内容管理方法，用于将内容数据从第一记录媒体移动到第二记录媒体，

其中所述第一记录媒体记录：

加密内容，该加密内容是用第一密钥加密明文内容获得的，

第一已加密密钥，该第一已加密密钥是用第四密钥和第五密钥加密第一密钥而获得的，该第四密钥从第二密钥和第三密钥产生，

第二已加密密钥，该第二已加密密钥是用所述第三密钥加密所述第二密钥获得的，以及

第五已加密密钥，该第五已加密密钥是用预定密钥加密所述第五密钥而获得的，

所述方法的特征在于包括：

从所述第一记录媒体中读取所述第一已加密密钥、所述第二已加密密钥和所述第五已加密密钥；

用所述第三密钥解密所述第二已加密密钥，以获得所述第二密钥;

用所述预定密钥解密所述第五已加密密钥，以获得所述第五密钥;

用所述第四密钥和所述第五密钥解密所述第一已加密密钥以获得所述第一密钥，所述第四密钥从所述第二密钥和所述第三密钥产生;

用所述第一密钥解密所述加密内容，以获得所述明文内容;

将所述明文内容和所述第二密钥传送给所述第二记录媒体;

从所述第一记录媒体中删除所述第二已加密密钥;

更新所述第五密钥;

用所述更新后的第五密钥加密被所述第四密钥加密的所述第一密钥以更新所述第一密钥，

用所述预定密钥加密所述更新后的第五密钥，以改变所述更新后的第五密钥，

由此使所述加密内容和所述第一已加密密钥保持记录在所述第一记录媒体中，但禁止所述加密内容被解密。

3、根据权利要求 2 所述的方法，其特征在于还包括:

省去记录传送到所述第二就媒体的所述明文内容的步骤;

用所述第三密钥将传送到所述第二记录媒体的所述第二密钥加密；以及

在传送到所述第二记录媒体的内容数据已经记录在所述第二记录媒体中的情况下，在所述第二记录媒体中记录所述已加密的第二密钥。

4、根据权利要求 2 所述的方法，其特征在于，所述第三密钥包括媒体专有密钥。

5、根据权利要求 2 所述的方法，其特征在于，所述第五密钥基于保密信息记录和再现系统，在该保密信息记录和再现系统中仅仅在所述记录媒体的驱动器中允许执行记录、再现和数据更新。

6、根据权利要求 2 所述的方法，其特征在于，

所述内容数据包括多个内容，

为所述多个内容提供多个第一密钥和第二密钥，

从所述多个第二密钥计算所述校验数据;

所述校验数据被插入到已加密文件密钥的文件中;

用所述第三密钥将插入后的已加密第一密钥的文件加密，以获得包括双重

加密的第一密钥的加密数据文件，并且将已加密校验数据记录在所述第一记录媒体中。

7、根据权利要求 6 所述的方法，其特征在于，

所述已加密第一密钥的文件包括每个所述第一密钥的附加信息和标志，所述第一密钥的附加信息包括每个所述第一密钥的标识，所述标志指示所述已加密第二密钥是被存储在所述第一记录媒体中还是被从所述第一记录媒体中删除；并且

所述已加密第二密钥的文件包括每个所述第二密钥和被删除的第二密钥的附加信息和标志，所述第二密钥和被删除的第二密钥的附加信息包括每个所述内容的标识，所述标志指示所述已加密第一密钥是否被存储在所述第一记录媒体中。

8、根据权利要求 2 所述的方法，其特征在于，

所述内容数据包括多个内容，

为所述多个内容提供多个第一密钥和第二密钥，

用所述第四密钥将所述多个第一密钥加密，以获得已加密第一密钥的文件；

用所述第三密钥件所述多个第二密钥加密，以获得已加密第二密钥的文件；

用更新后的第三密钥将已加密第一密钥的文件和已加密第二密钥的文件加密，以获得双重加密的第一密钥和双重加密的第二密钥；以及

将所述双重加密的第一密钥和所述双重加密的第二密钥记录在所述第一记录媒体中。

9、根据权利要求 8 所述的方法，其特征在于，

所述已加密第一密钥的文件包括每个所述第一密钥的附加信息和标志，所述第一密钥的附加信息包括每个所述第一密钥的标识，所述标志指示所述已加密第二密钥是被存储在所述第一记录媒体中还是被从所述第一记录媒体中删除；并且

所述已加密第二密钥的文件包括每个所述第二密钥和被删除的第二密钥的附加信息和标志，所述第二密钥和被删除的第二密钥的附加信息包括每个所述内容的标识，所述标志指示所述已加密第一密钥是否被存储在所述第一记录媒体中。

10、一种记录媒体，其特征在于，记录了加密内容、第一已加密密钥以及

一个第二已加密密钥，所述加密内容是通过用第一密钥加密明文内容而获得的，所述第一已加密密钥是通过用第四密钥加密第一密钥而获得的，而该第四密钥是根据第二密钥和第三密钥产生的，所述第二已加密密钥是通过用所述第三密钥加密所述第二密钥而获得的。

11、一种记录媒体，其特征在于，记录了加密内容、第一已加密密钥、第二已加密密钥以及第五已加密密钥，所述加密内容是通过用第一密钥加密一明文内容获得的，所述第一已加密密钥是通过用第四密钥和第五密钥加密第一密钥而获得的，而该第四密钥是从第二密钥和第三密钥产生的，所述第二已加密密钥是用所述第三密钥加密所述第二密钥获得的，所述第五已加密密钥是用预定密钥加密所述第五密钥而获得的。

内容管理方法和记录媒体

技术领域

本发明涉及一种用于管理内容数据的内容管理方法以及一种记录媒体。

背景技术

目前已知的记录数字化信息（文本、音频、视频、程序等等）的数字记录媒体包括高密度盘(compact disc，CD）和数字通用盘（digital versatile disc，DVD）。

在这样的数字记录媒体中，由于记录了数字数据，该记录的数字数据可以很容易地复制到其它数字记录媒体上，而不会损失音频或视频的质量。但此性能具有一个相矛盾的问题，即，可以产生大量的复制品，非法传播复制光盘，从而侵犯版权。

因此，现在已经尝试利用下述方法防止非法复制，该方法通过利用一个密钥加密一个版权内容（数字化信息），为了隐藏该加密密钥利用另一个密钥加密该内容加密密钥，并在记录媒体上将该加密的加密密钥与该加密内容一起记录。但在最近，非法用户又试图在另一个数字记录媒体上将该数字记录媒体上所有的数据一起复制，包括加密的内容和加密的加密密钥。

此外，正如数字电视广播所显示的，现在还有另一种仅仅允许在一个记录媒体存储内容（一次性复制）的版权保护方法。此方法仅仅允许在一个记录媒体中存储该内容，并且因此在删除或者禁止再现原始记录媒体中内容的先决条件下，此方法允许移动内容，即，允许原始记录媒体中的内容复制到另一个记录媒体上。在这种情况下，由于删除原始记录媒体上的内容要花费很长的时间，所以，通过删除加密钥，就不能解密内容，从而不能再在现该内容，并且因此认为该内容实际上被删除。

但是，在此方法中，由于加密内容仍然保留在记录媒体中，如果通过某种方法恢复了已经删除的加密密钥，就可能解密并再现该加密内容。结果，可复写的内容就可以保存在多个媒体上，包括移动到其它记录媒体上的内容。因此，

如何防止这种所有数据的非法拷贝的加密密钥恢复（批量复制）就很重要了。

允许移动内容的版权保护方法包括文献1(公开号为2003-132625的日本专利申请)、文献2（公开号为2003-109302的日本专利申请）以及文献3（公开号为2003-122637的日本专利申请)。这些公开揭示了作为内容非法复制预防技术的非法复制情况下的加密密钥废除系统或者具有媒体绑定功能从而禁止在其它数字记录媒体上的非法复制的方法。例如，内容加密密钥由另一个密钥加密，并与加密内容一起记录在同一个记录媒体上，在通过授权的方法将该内容在记录媒体间移动后，防止非法复制恢复已经从原始记录媒体上删除了的加密过的加密密钥。

这些现有技术是用于防止批量复制的方法，这些方法包括了一种用于记录和再现一记录媒体中数据的保密信息记录和再现系统，该系统运行在驱动器中，还采用了不允许从驱动器外面看到保密信息的结构。由于此保密信息是与密钥管理系统为一体的密钥的一部分，所以即使批量复制了该驱动器中输出的所有数据，也不能解密加密了的内容。

但是，这些现有技术是不能应用在不具有保密信息记录和再现功能的传统DVD驱动器上的，而可应用在传统DVD驱动器的技术在文献4（公开号为2004-186825的日本专利申请）中公开。这里，仅仅当第一次下载数字内容时，作为一个用于加密内容的密钥，产生并记录两种类型，即，“加密的密钥文件”和“多重加密的密钥文件”，该“加密的密钥文件”由传统DVD记录驱动器使用的方法（CPRM:可记录媒体的内容保护）加密，而“多重加密的密钥文件”是通过用加密密钥加密该已加密的加密密钥文件而获得的，其中该加密密钥是在保密信息记录和再现方法中的保密信息，并且当将该内容从首次下载的记录媒体移动到另一个记录媒体上时，仅仅将加密的内容和多重加密的加密密钥文件记录在另一个记录媒体上，这就是允许仅仅移动可以记录和再现保密内容的驱动器的版权管理方法。

依据这样的系统，记录了下载内容的最初的记录媒体就可以由CPRM驱动器再现。进一步地，如果不是特别需要进行移动，此系统在首次下载时记录可应用于CPRM的加密内容和加密的加密密钥是足够的。这样，如果限制了功能，即使驱动器不具有新的保密信息记录和再现功能，也可以进行记录和再现。

此方法的一个优点是，即使内容被移动过程移动到另一个记录媒体上，首

次记录媒体也总是可以被再现，此外本方法的优点还在于，即使由于重编码移动使压缩比率改变而造成质量降低，由于原始内容记录在最初的记录媒体中，重编码移动也是安全的。

但是，一次性复制是数字 TV 广播的基本准则，由于本方法中内容存在于两个位置上，所以本方法不能用于数字 TV 广播，就需要适用于这种情况的技术。

在传统的版权保护系统中，内容是加密的，加密中使用的加密密钥也是加密的并且记录在同一个记录媒体中。在这种情况下，为了防止非法复制，在一个加密管理系统中，建立了加密密钥的一部分的废除功能或者媒体绑定功能，从而提高了保护性能。在此系统中，当在记录媒体间移动内容时，在移动了内容后通过仅仅从原始记录媒体中删除加密密钥，也可以认为与删除内容是相同的。

但是，在可移动并且开放的记录媒体中，例如光盘中，通过在记录加密密钥的区域读出数据以及在存储单元中存储该读取数据，在内容的合法移动过程后，有可能进行非法复制，该非法复制复原先前从原始媒体中删除的加密密钥，而该加密密钥来源于存储器单元中的加密密钥记录区域中的数据。

在当前 DVD 记录器的版权保护系统中，可能在 HDD（硬盘驱动器）中首次记录内容，并且将此内容从 HDD 移动到 DVD 中。但是，一旦记录在 DVD 中的内容不允许被移动到其它 DVD 上或者再次被移动到 HDD 中。原因如下，在将内容从原始媒体移动到新记录媒体中后，根据提前保存的加密的加密密钥数据，可能恢复其中已经由删除过程删除了加密密钥的原始记录媒体。在这样的方法中，即使加密设备是很高级的，仅仅通过原样复制一部分加密数据，仍然可以生成非法复本。

发明内容

本发明致力于提供一种内容管理方法和一种记录媒体，其消除了由于相关技术的限制或缺陷而产生的一个或多个问题。

根据本发明，在可移动媒体间移动内容是可能的，例如，在 DVD 与 DVD 间，或者从例如 DVD 的可移动媒体到例如 HDD 的固定媒体。

根据本发明的一个实施例，提供了一种内容管理方法，该内容管理方法用

于将内容数据从第一存储媒体移动到第二存储媒体，其中所述第一存储媒体记录了：

加密内容（Enc-content），该加密内容是用第一密钥（Kt）加密明文内容而获得的，

第一已加密密钥(E-Kt)，该第一已加密密钥(E-Kt)是用第四密钥(Kmum)加密第一密钥而获得的，该第四密钥从第二密钥（Kmv）和第三密钥（Kmu）产生，以及

第二已加密密钥（E-Kmv），该第二已加密密钥（E-Kmv）是用所述第三密钥（Kmu）加密所述第二密钥（Kmv）而获得的，所述方法包括：

解密从所述第一记录媒体中读取的所述加密内容（Enc-content）以及所述第二已加密密钥（E-Kmv），以获得所述明文内容和所述第二密钥；

将所述明文内容和所述第二密钥传送给所述第二记录媒体；以及

从所述第一记录媒体中删除所述第二已加密密钥（E-Kmv），

由此使所述加密内容（Enc-content）和所述第一已加密密钥保持记录在所述第一记录媒体上，但禁止所述加密内容（Enc-content）被解密。

依据本发明的另一个实施例，提供了一种内容管理方法，其用于将内容数据从第一记录媒体移动到第二记录媒体上，其中所述第一记录媒体记录了：

加密内容（Enc-content），该加密内容（Enc-content）是用第一密钥（Kt）加密明文内容获得的，

第一已加密密钥（EE-Kt），该第一已加密密钥（EE-Kt）是用第四密钥（Kmum）和第五密钥（UDm）加密第一密钥而获得的，该第四密钥（Kmum）从第二密钥（Kmv）和第三密钥（Kmu）产生，

第二已加密密钥（E-Kmv），该第二已加密密钥（E-Kmv）是用所述第三密钥（Kmu）加密所述第二密钥（Kmv）获得的，以及

第五已加密密钥（E-UDm），该第五已加密密钥（E-UDm）是用预定密钥加密所述第五密钥而获得的，

所述方法包括：

从所述第一记录媒体中读取所述第一已加密密钥（EE-Kt）、所述第二已加密密钥（E-Kmv）和所述第五已加密密钥（E-UDm）；

用所述第三密钥（Kmu）解密所述第二已加密密钥（E-Kmv），以获得所

述第二密钥（Kmv）;

用所述预定密钥解密所述第五已加密密钥（E-UDm），以获得所述第五密钥（UDm）;

用所述第四密钥（Kmum）和所述第五密钥（UDm）解密所述第一已加密密钥（EE-Kt）以获得所述第一密钥（Kt），所述第四密钥（Kmum）从所述第二密钥（Kmv）和所述第三密钥（Kmu）产生;

用所述第一密钥（Kt）解密所述加密内容（Enc-content），以获得所述明文内容;

将所述明文内容和所述第二密钥传送给所述第二记录媒体;

从所述第一记录媒体中删除所述第二已加密密钥（E-Kmv）;

更新所述第五密钥（UDm）;

用所述更新后的第五密钥（UDm）加密被所述第四密钥（Kmum）加密的所述第一密钥（E-Kt）以更新所述第一密钥（E-Kt），

用所述预定密钥加密所述更新后的第五密钥（Um），以改变所述更新后的第五密钥，

由此使所述加密内容（Enc-content）和所述第一已加密密钥保持记录在所述第一记录媒体上，但禁止所述加密内容（Enc-content）被解密。

依据本发明的另一个实施例，一种记录媒体记录了加密内容（Enc-content）、第一已加密密钥（E-Kt）以及第二已加密密钥（E-Kmv），所述加密内容（Enc-content）是用第一密钥（Kt）加密一明文内容而获得的，所述第一已加密密钥（E-Kt）是用第四密钥（Kmum）加密第一密钥而获得的，而该第四密钥从第二密钥（Kmv）和第三密钥（Kmu）产生，所述第二已加密密钥（E-Kmv）是用所述第三密钥（Kmu）加密所述第二密钥（Kmv）而获得的。

根据本发明的另一个实施例，一种记录媒体记录了加密内容（Enc-content）、第一已加密密钥（EE-Kt）、第二已加密密钥（E-Kmv）以及第五已加密密钥（E-UDm），所述加密内容（Enc-content）是用第一密钥（Kt）加密一明文内容获得的，所述第一已加密密钥（EE-Kt）是用第四密钥（Kmum）和第五密钥（UDm）加密第一密钥而获得的，而该第四密钥（Kmum）从第二密钥（Kmv）和第三密钥（Kmu）产生，所述第二已加密密钥（E-Kmv）是用

所述第三密钥（Kmu）加密所述第二密钥（Kmv）获得的，所述第五已加密密钥（E-UDm）是用预定密钥加密所述第五密钥而获得的。

本发明的其它目的和优点将在如下的说明书中阐明，并且在某种程度上在说明书中将变得清楚，或者可以通过实施本发明而获知。

通过特别是下面所指出的实施和组合，将实现并获得本发明的目的和优点。

附图说明

与说明书相结合并组成说明书一部分的附图图解了本发明的实施例，并且这些附图与如上所述的总体描述以及如下所述的实施例详细描述一起解释了本发明的原理，其中：

图 1 是表示了使用 CPRM 方法的版权保护系统的基本配置的处理系统图；

图 2 是表示了移动内容时记录媒体的状态转变的图；

图 3 是表示了可以利用保密信息记录和再现技术而移动的版权保护方法的处理系统图；

图 4 是表示了在改变（降低）分辨率的重编码处理后，利用图 3 所示的系统进行内容移动处理的配置的系统图；

图 5 是表示了图 4 所示的内容移动处理中记录媒体的状态转变的图；

图 6 是本发明第一实施例的一个可以进行依据重编码移动处理的加密管理系统图；

图 7 是在图 6 的系统中使用的“标题密钥文件”和“移动-密钥文件”的配置图，其中“标题密钥文件”由多个多重加密的标题密钥组成，“移动-密钥文件”由多个已加密的移动-密钥组成；

图 8 是当在多个记录媒体间移动内容时每个记录媒体的状态转换图；

图 9 是加密管理系统（图 6）的详细图，其使得能够进行依据本发明第一实施例的重编码移动处理；

图 10 是图 9 中数据读取方解密处理和记录方加密处理的详细图，其中包括了记录在记录媒体中的数据文件的关系；

图 11 是图 9 中数据读取方解密处理和记录方加密处理的详细图，其中包括了记录在记录媒体中的数据文件的关系；

图 12 是记录媒体的数据排列图，其中包括根据本发明记录的加密内容和已

加密的加密密钥;

图 13 是用于解释本发明的保密信息嵌入方法的图;

图 14 是由目前 DVD 系统的 16 组记录扇区组成的 ECC 方框图;

图 15 是表示了嵌入了保密信息的物理扇区的细节的图;

图 16 是依据本发明第二实施例的加密管理系统;

图 17 是在图 16 的系统中使用的"标题密钥文件"和"移动密钥文件"的配置图，其中"标题密钥文件"由多个多重加密的标题密钥组成，"移动密钥文件"由多个已加密的移动密钥组成; 以及

图 18 是标题密钥的加密管理系统。

具体实施方式

现在将参照附图描述依据本发明的内容管理方法、记录及再现装置以及记录媒体的实施例。

图 1 是表示了 CPRM 方法的基本配置的处理系统图，该 CPRM 方法就是依据本发明的版权保护系统。

如图 1 所示，在可以是 DVD-RAM 和 DVD-RW 盘的记录媒体 12 中，记录了一个已加密的加密密钥块（MKB: 媒体密钥块）和一个盘专有 ID（MID: 媒体 ID），该已加密的加密密钥预先用多个设备密钥加密。

（在数字记录媒体中记录内容）

驱动器 16 和 A/V 板 14 间的进行验证 22 之后，驱动器 16 读出记录媒体 12 中的 MKB 和 MID，并将其发送到 A/V 板 14。

在 A/V 板 14 中，利用被输入到 MKB 处理单元（MKB-pro）24 的 MKB 和设备密钥 26 中提取出媒体密钥（Km）。

提取出的媒体密钥（Km）和从记录媒体 12 中读出的 MID 被输入到诸如散列函数设备的信号处理单元[G]28 中，并且产生一个媒体专有密钥（Kmu）。

标题密钥（Kt: T-key）32 被输入到加密单元（E）30 中，并且被媒体专有密钥（Kmu）加密，然后作为已加密的标题密钥（E-Kt）被记录在记录媒体 12 中。

另一方面，标题密钥（Kt）32 也被输入到加密单元（Enc）36 中，然后加密内容（新内容）34。加密内容（Enc-content）被记录在记录媒体 12 中。

（从数字记录媒体中再现内容）

在驱动器 18 和 A/V 板 20 之间的进行验证后，驱动器 18 读出记录在记录媒体 12 中的 MKB 和 MID，并将它们发送到 A/V 板 20。

在 A/V 板 20 中，利用被输入到 MKB 处理单元（MKB-pro）40 的 MKB 和 A/V 板 20 拥有的设备密钥 42 中提取出媒体密钥（Km）。

提取出的媒体密钥（Km）和从盘 12 中读出的 MID 被输入到诸如散列函数设备的信号处理单元[G]44 中，并且产生一个媒体专有密钥（Kmu）。

从记录媒体 12 中读出的已加密的标题密钥（E-Kt）被输入到解密单元（D）46 中，并且利用媒体专有密钥（Kmu）解密，以产生一个标题密钥（Kt）。

加密内容（Enc-content）从记录媒体 12 中被输入到解密单元（Dec）48 中，并且由标题密钥（Kt）解密，从而产生明文内容（Content）50。

图 2 是解释将内容从记录媒体 A 移动到记录媒体 B 的移动处理的图。将记录在记录媒体 A 中的加密内容解密，并将其发送到记录媒体 B 侧的记录驱动器中。记录媒体 B 的记录驱动器在将发送内容加密，并在记录媒体 B 中记录该加密内容，并且进一步将此时加密内容用的标题密钥用媒体 B 的媒体专有密钥加密，并记录在记录媒体 B 中。

当向记录媒体 B 侧的驱动器的内容传输结束时，记录媒体 A 侧的驱动器停止再现操作，改变到记录模式，同时删除在记录媒体 A 中用于加密内容的标题密钥（图 2 中的-标记）。在这种情况下，如果在记录媒体 A 中存在多个内容文件，将特定内容文件发送到记录媒体 B，而仅仅删除已传输内容的内容加密标题密钥。通过这种操作，结束了移动处理。

根据图 1 和 2 中所示的 CPRM 系统的基本配置，在将内容从记录媒体 A 移动到记录媒体 B 之前，通过读出并保存记录在记录媒体 A 中的已加密标题密钥，并且在内容移动处理终止后将保存的已加密标题密钥文件原样放回到记录媒体 A 中，以恢复从记录媒体 A 中删除的已加密的标题密钥，这样仍然可能恢复要再现的加密内容。这样的行为违背了基于一次复制管理的内容约定。

图 3 是表示了利用保密信息记录和再现技术可以进行移动处理的版权保护方法的图。通过利用保密信息记录和再现技术，就有可能防止读取、保存已加密标题密钥文件以及存回到记录媒体中的非法复制。与图 1 相同的设备用相同的附图标记表示，并且将省略其详细说明。在图 3 中，省略了驱动器和 A/V 板

之间的验证。

（在数字记录媒体中存储内容）

在驱动器 16 和 A/V 板 14 之间的进行印证之后，驱动器 16 读出记录媒体 12 中记录的 MKB 和 MID，并将它们发送到 A/V 板 14。

在 A/V 板 14 中，利用输入到 MKB 处理单元 24 的 MKB 和设备密钥 26，提取出媒体密钥（Km）。

提取出的媒体密钥（Km）和从记录媒体 12 中读出的 MID 被输入到信号处理单元[G]28 中，该信号处理单元[G]28 诸如是散列函数设备，随后产生媒体专有密钥（Kmu）。

标题密钥（Kt1'：T-key）32 被输入到加密单元（E）30 中，通过利用媒体专有密钥（Kmu）产生一个已加密的标题密钥（E-Kt1'）。

该已加密标题密钥（E-Kt1'）被发送到编辑器（EDT）54 中，该编辑器（EDT）54 将已加密标题密钥（E-Kt1'）添加到从记录媒体 12 中读出的已加密标题密钥（E-Kt0）上。将编辑器 54 的输出提供给驱动器 16，并且该输出被加密单元（E）56 中的保密信息信号（UD：updat）进一步加密，并且作为多重已加密内容加密密钥（EE-Kt1）保存在记录媒体 12 中。

另一方面，标题密钥（Kt1'：T-key）32 被输入到加密单元（Ecn）36 中，并将一个内容（新内容 New content）34 加密。将加密内容（Enc-content）保存在记录媒体 12 中。

位于图 3 中心的记录媒体 12 的左侧方框表示了在记录媒体 12 中另外记录一个新加密的内容 34 的系统的配置，而该记录媒体 12 已经存储了多个加密内容。

多个多重已加密标题密钥（EE-Kt）也作为加密内容存储在记录媒体 12 中。要预先（在移动处理之前）读出记录在记录媒体 12 中的多重已加密标题密钥（EE-Kt）和已加密保密信息（E-UD0）。在解密单元（D）58 中将已加密保密信息（E-UD0）解密为保密信息（UD0），并且利用此保密信息（UD0），在解密单元（D）60 中将多重加密标题密钥（EE-Kt0）解密为已加密标题密钥（E-Kt0）。将此已加密密钥（E-Kt0）发送给内容加密侧的 A/V 板 14，并且将其添加到编辑器（EDT）54 中的已加密标题密钥（E-Kt'）上，然后将添加结果发送给驱动器 16。

在驱动器 16 侧，保密信息（UD0）被更新为更新单元（*α）62 中的保密信息（UD1）。例如，更新单元（*α）62 将保密信息（UD0）加上整数（n），通过或者将保密信息（UD0）递增整数（n）。可选择地，更新单元（*α）62 可以利用随机信号产生器更新保密信息（UD0）。利用更新后的保密信息（UD1），在加密单元（E）56 中加密由驱动器 16 发送的编辑后的已加密标题密钥，并且将其作为多重已加密标题密钥（EE-Kt1）记录在记录媒体 12 中。

利用预定的保密密钥或者在驱动器中提取出的媒体专有密钥（Kmu），在加密单元（E）64 中加密更新后的保密信息（UD1）。将已加密的更新保密信息（UD1 作为已加密的保密信息（E-UD1）记录在记录媒体 12 中。

在多重已加密标题密钥的每次重写操作中都更新此处理，并且更新多重已加密标题密钥。

图 3 的右侧方框表示了当移动加密内容时加密内容的解密。

（从数字记录媒体再现内容）

在驱动器 18 和 A/V 板 20 间的进行验证后，驱动器 18 读取记录在记录媒体 12 中的 MKB 和 MID，并将它们发送给 A/V 板 20。

在 A/V 板 20 中，利用输入到 MKB 处理单元 40 的 MKB 以及 A/V 板 20 的设备密钥 42 提取媒体密钥（Km）。

提取的媒体密钥（Km）和从记录媒体 12 中读出的 MID 被输入到信号处理单元[G]44 中，该信号处理单元[G]44 诸如是散列函数设备，然后产生媒体专有密钥（Kmu）。

从记录媒体 12 中读出已加密的保密信息（E-UD1），并在解密单元（D）66 中将其解密成保密信息（UD1）。从记录媒体 12 中读出多重已加密标题密钥（EE-Kt1），并将其输入到解密单元（D）66，然后利用此保密信息将其解密，以产生一个已加密标题密钥（E-Kt1）。

已加密标题密钥（E-Kt1）被输入到解密单元（D）66，并且利用根据 MKB 和 MID 产生的媒体专有密钥（Kmu）解密。此时，产生了多个标题密钥，但要选择要移动的内容的特定标题密钥（Kt1'）。

将从记录媒体 12 中读出的加密内容（Enc-content）输入到解密单元（D）48，然后将其用标题密钥（Kt1'）解密，从而再现了明文内容（Content）50。

利用此处理，编辑器（EDT）70 将特定标题密钥（Kt1'） 从移动后内容

的已加密标题密钥（E-Kt1）中删除，并且产生（更新）已加密标题密钥（E-Kt2）。在更新单元（*α）72 中更新在解密单元（D）66 中解密出的保密信息，并产生更新后的保密信息（UD2）。

内容回放包括仅回放和用于移动的回放。用于移动的回放需要编辑器 70、更新单元（*α）72、加密单元（E）74 和解密单元（E）76。但是，仅回放就不需要这些单元。在用于移动的回放期间，编辑器 70 从已加密标题密钥（E-Kt1）中删除用于移动的内容的已加密标题密钥，并输出剩余的已加密标题密钥（E-Kt2）。

利用加密单元（E）74 中更新的保密信息（UD2），将编辑器 7 中编辑的（更新后的）已加密标题密钥（E-Kt2）解密，并将其作为多重已加密标题密钥（EE-Kt2）记录在记录媒体 12 中。

在加密单元（E）76 中将更新后的保密信息（UD2）加密，并将其作为已加密的保密信息（E-UD2）记录在记录媒体 12 中。

利用此处理，在记录媒体 12 中，将移动的内容的标题密钥（Kt1'）删除，该加密内容是不能被解密的，因此实际上被删除了。

根据图 3 的系统，由附加的记录和移动处理更新并改变标题密钥的加密密钥。因此，即使预先保存了已加密的标题密钥，并试图依据备份的已加密标题密钥恢复该标题密钥，由于用于加密标题密钥的保密信息（UD）已经被更新了，所以也不能恢复标题密钥，并且避免了由于加密密钥的恢复而引起的非法复制。所以图 3 的版权保护系统支持了移动功能。

但是，在图 3 中的具有移动功能的版权保护系统中，如果移动时改变了内容的分辨率（压缩率）并且内容被移动并记录在一个具有较小记录容量的记录媒体中，也不可能高质量地复原原始内容。

图 4 是表示了在利用图 3 所示的系统重编码处理后进行内容移动和记录的配置的系统图。

在图 4 中，利用图 4 左侧（相应于图 3 的右侧）的驱动器 18A 和 A/V 板 20A，从记录媒体 12A 中读出内容，并利用图 4 右侧（相应于图 3 的左侧）的驱动器 16B 和 A/V 板 14B 将其再次加密，之后将加密内容记录在记录媒体 12B 中。

利用图 3 所解释的读取处理，通过 I/O 将从记录媒体 12A 中读出的内容发

送到记录媒体 12B 的记录驱动器 16B 中，并且为了降低分辨率首次输入到代码转换器 80 中，并且被再次加密。

进一步地，利用图 3 所解释的写处理，将代码转换器 80 中产生的明文内容加密，并将其记录在记录媒体 12B 中。

图 5 是表示了图 4 所示的内容移动处理的图。这里，假设记录媒体中记录的加密内容是一个文件。记录媒体 A 记录了一个高速率压缩的加密内容。读取的内容（加密内容）被再次加密为低速率压缩的加密内容，并将其记录在记录媒体 B 中。这样，内容就通过重编码从记录媒体 A 移动到记录媒体 B 上了。

如图 5 所示，在内容被复制后，将记录媒体 A 的加密标题密钥删除，实质上是从文件管理器的角度上删除了内容。由于删除了用于解密的标题密钥，加密内容不能被再次存储，并且当保护版权的时候，内容可以在记录媒体间移动，并且可以在用户期望的或优选的状态中使用。

虽然移动处理是一个重要的功能，但如果为了减小数据大小以将内容用在便携设备中而执行重编码，就不能再现高质量的原始内容。新的版权保护系统可以防止非法复制，其中该非法复制是通过对记录媒体进行非法处理恢复标题密钥的方法从而复原已删除的加密内容，其中该记录媒体在授权的移动处理后已经删除了标题密钥，这样该新的版权保护系统就可以提供移动功能了。但是如果在高质量内容的移动处理中进行内容的重编码或者相似处理，那么就无法再次存储高质量的内容。换句话说，购买高质量内容的授权用户不允许根据使用模式暂时降低内容的分辨率，这意味着降低了用户便利性。

在这种情况的启示下，下面将解释将“内容移动”功能改变为“内容再现权利的移动”功能的实例。

图 6 是本发明的加密管理系统的实例。在图 6 中，省略了驱动器和 A/V 板部分。与图 4 相比，新增了移动-密钥（Kmv），而其它的都相同。利用媒体专有密钥（Kmum）加密标题密钥（T-key）32，其中该媒体专有密钥（Kmum）是根据媒体密钥（Kmu）和移动-密钥（Kmv）产生的。这样，移动-密钥（Kmv）就用于加密或解密标题密钥，而该标题密钥是用于在加密单元（E）30 或解密单元（D）46 中加密或解密内容的，与先前的技术不同，移动内容时，并不删除标题密钥，但删除移动-密钥，这样也不能再现（解密）内容。移动-密钥（Kmv）与内容形成对，所述对在记录媒体间移动，同时在移动目的地的记录媒体中，

移动-密钥（Kmv）被加密单元（E）98 利用移动目的记录媒体的媒体专有密钥加密并被存储。但是在本发明中，由于允许重编码移动，移动目的地的记录媒体中可能已经记录了仅仅分辨率不同的相同内容。因此，如果目的地站已经记录了不同分辨率的相同内容，那么就不移动该内容，而仅仅移动该移动-密钥。也就是说，在试图将内容移回原始记录媒体的情况下，如果处于不允许解密状态的加密内容已经记录在原始记录媒体中，仅仅移动该移动-密钥就能解密该加密内容。此处理的详细操作如下。

在驱动器和 A/V 板（未示出）之间进行验证后，驱动器读出记录在记录媒体 12A 中的 MKB 和 MID，并将它们发送到 A/V 板。

在 A/V 板中，利用输入到 MKB 处理单元 40 中的 MKB 和设备的设备密钥（D-K）42 提取出媒体密钥（Km）。

将提取的媒体密钥（Km）以及从记录媒体 12 中读出的 MID 输入到信号处理单元[G]44 中，该信号处理单元[G]44 诸如是散列函数设备，然后产生媒体专有密钥（Kmu）。

读出记录在记录媒体 12A 中的已加密的移动-密钥（E-Kmv0），并将其输入到解密单元（D）82，之后利用媒体专有密钥（Kmu）解密，然后产生移动-密钥文件（Kmv0）。

根据此移动-密钥文件（Kmv0），提取出相应于要移动的内容的移动-密钥（Kmva），并且将其与信号处理单元[G]44 产生的媒体专有密钥（Kmu）一起输入到信号处理单元[G]84 中，随后产生一个媒体专有移动-密钥（Kmum）。

从记录媒体 12A 中读出已加密的保密信息（E-UD0），并在解密单元（D）66 中将其解密为保密信息（UD0）。另一方面，从记录媒体 12A 中读出多重加密的标题密钥文件（EE-Kt0），并将其输入到解密单元（D）68 中，之后利用保密信息（UD0）解密，以产生已加密的标题密钥文件（E-Kt0）。

这个已加密的标题密钥文件（E-Kt0）被输入到解密单元（D）46 中，并利用媒体专有移动-密钥（Emum）解密，从而产生相应于要移动的内容的标题密钥（Kta）。

从记录媒体 12A 中读出的加密内容（Enc-content）被输入到解密单元（Dec）48，并利用标题密钥（Kta）将其解密。这样就产生了明文内容（Content）。此时，通过接口（I/O）将相应于内容的移动-密钥（Kmva）与明文内容一起发送

到记录媒体 12B 侧的驱动器中，之后将移动-密钥（Kmva）重新加密并记录在记录媒体 12B 中。

与本发明的范围无关，通过 I/O 输出的内容数据和移动-密钥数据是以其它数字接口标准加密和解密的，自然防止了设备间数据传输中的违法复制。

当将内容和移动-密钥（Kmva）发送到记录媒体 12B 侧时，在记录媒体 12A 侧，首先，将移动-密钥文件（Kmv0）输入到编辑器（EDT）86 中，将相应于该被移动内容的移动-密钥（Kmua）从密钥文件中删除，并产生一个新的移动-密钥文件（Kmv1）。将这个新的移动-密钥文件（Kmv1）输入到加密单元（E）88 中，利用媒体专有密钥（Kmu）将其加密，并将其作为已加密的移动-密钥（E-Kmv1）记录在记录媒体 12A 中。

与此同时，将移动-密钥文件（Kmv1）输入到移动-密钥校验数据处理单元（V-Mo）90 中，并产生移动-密钥校验数据（V-Mo1）。将移动-密钥校验数据（V-Mo1）和已加密的标题密钥（E-Kt0）数据输入到编辑器（EDT）70 中，随后产生已加密的标题密钥（E-Kt1）。但是在此，并不删除相应于被移动内容的标题密钥（Kta）。

另一方面，在更新单元（*α）72 中更新在解密单元（D）66 中解密的保密信息（UD0），从而产生更新后的保密信息（UD1）。

在编辑器（EDT）70 中编辑的已加密标题密钥被输入到加密单元（E）74 中，并且将其用从更新单元（*α）72 输出的更新后的保密信息加密，并将其作为多重加密的标题密钥（EE-Kt1）记录在记录媒体 12A 中。

在加密单元（E）76 中将更新后的保密信息（UD1）加密，并将其作为已加密的保密信息（E-UD1）记录在记录媒体 12A 中。

这样，在移动处理中就没有删除用于解密该加密内容的标题密钥，而将其以加密状态保留在原始记录媒体中。另一方面，从原始记录媒体中删除解密此已加密的标题密钥所需的移动-密钥（Kva）。因此，即使将在记录媒体中可被加密的密钥合并，由于不存在移动-密钥，也不能将用于解密该加密内容的标题文件解密。

在这样的方式中，如果试图通过将内容从内容保存媒体中移动到原始媒体，而将该内容从内容存储媒体返回到原始媒体中，仅仅通过返回该移动-密钥，就可以将保留的加密状态的内容复原到可解密状态。例如在首次移动中，当通过

下变换将内容移动为较低的信息质量时，这样的处理可以通过复原到原始记录媒体而将信息质量返回到原始质量。换句话说，曾经通过下变换而使图片质量恶化的图像可以返回到原始的水平。

下面将解释在记录媒体 12B 中记录内容的操作。

在记录媒体 12B 侧的驱动器中，将通过接口（I/O）传送的明文内容数据和移动-密钥（Kmva）加密。

将经过代码转换器 80 重编码过的内容输入到加密单元（Enc）36 中，通过利用由随机数字产生器等新产生的标题密钥（Ktx）32，将该内容加密，并将其作为加密内容（Enc-content）记录在记录媒体 12B 中。

从记录媒体 12B 中读出 MKB，将其输入到 MKB 处理单元 24 中，利用分别提供在设备中的盘密钥（D-K）26 提取出设备密钥（Km'）。然后，从记录媒体 12B 中读出 MID，将该 MID 与设备密钥（Km'）一起输入到信号处理单元[G]28 中，该信号处理单元[G]28 例如是散列函数设备，并且产生媒体专有密钥（Kmu'）。

通过接口（I/O）从记录媒体 12A 传输的移动-密钥（Kmva）与媒体专有密钥（Kmu'）一起被输入到信号处理单元[G]92 中，该信号处理单元[G]92 例如是散列函数设备，并且产生媒体专有移动-密钥（Kmum'）。

在随机数字产生器等中产生的标题密钥（Ktx）32 被输入到加密单元（E）30 中，并利用媒体专有移动-密钥（Kmum）将其加密，从而产生已加密的标题密钥（E-Ktx）。

读出记录在记录媒体 12B 中的移动-密钥文件（E-Kmvn），并将其输入到解密单元（D）94 中，随后利用记录媒体 12B 的专有密钥（Kmu'）将其解密，并且产生移动-密钥文件（Kmvn）。将此移动-密钥文件（Kmvn）和移动-密钥（Kmva）输入到编辑器（EDT）96 中，产生要将移动-密钥（Kmva）添加到其中的移动-密钥文件（Kmvm）。

将移动-密钥文件（Kmvm）输入到加密单元（E）98 中，并将其利用媒体专有密钥（Kmu'）加密，产生已加密的移动-密钥文件（E-Kmvm）并将其记录在记录媒体 12B 中。

从记录媒体 12B 中读出已加密的保密信息（E-UDn），并且在解密单元（D）58 中将其解密为保密信息（UDn）。另一方面，从记录媒体 12B 中读出多重加

密的标题密钥文件（EE-Ktn），并将其输入到解密单元（D）60 中，利用保密信息（UDn）解密该已加密的标题密钥文件（E-Ktn）。

将移动-密钥文件（Kmvm）输入到移动-密钥校验数据处理单元（V-Mo）100 中，产生移动-密钥校验数据（V-Mon）。将此移动-密钥校验数据（V-Mon）和已加密的标题密钥（E-Ktx）输入到编辑器（EDT）54 中，产生已加密的标题密钥（E-Ktm）。这里，已加密的标题密钥（Ktx）和移动-密钥文件（Kmvm）的校验数据（V-Mo）被合并为一组，产生已加密的标题密钥（E-Ktm）。

在另一方面，在更新单元（*α）62 中将在解密单元（D）58 中解密的保密信息（UDn）更新，从而产生更新后的保密信息（UDm）。

由编辑器（EDT）54 编辑的已加密的标题密钥（E-Ktm）被输入到加密单元（E）56 中，被更新后的保密信息（UDm）加密，并作为多重加密的标题密钥（EE-Ktm）记录在记录媒体 12B 中。

在加密单元（E）64 中加密更新后的保密信息（UDm），并将其作为已加密的保密信息（E-UDm）记录在记录媒体 12B 中。

图 7 是在本发明中使用的“标题密钥文件”和“移动密钥文件”的配置图，其中“标题密钥文件”由多个多重加密的标题密钥组成，“移动-密钥文件”由多个已加密的移动-密钥组成。

在每个标题密钥中，内容号码（内容标识 ID）、记录了对象内容的地址数据、多重加密的标题密钥（Enc2-Ktn: 与 EE-Ktn 相同）以及表示记录媒体中存在或不存在标题-密钥和移动-密钥的信息组成了一组标题密钥信息，并且该标题密钥信息被组合为多个组。表示存在或不存在的信息包括“11”（标题-密钥和移动-密钥都存在）、“10”（存在标题-密钥但不存在移动-密钥）、“00”（标题-密钥和移动-密钥都不存在）。该文件还包括已被保密信息（UD）加密的移动-密钥的验证数据的数据。已加密标题密钥的文件标识代码指示了该文件是已加密的标题密钥文件。

在每个移动-密钥中，内容号码（内容标识 ID）、记录了对象内容的地址数据、已加密的移动-密钥（E-Kmv）以及表示记录媒体中存在或不存在标题密钥和移动-密钥的信息组成了一组移动-密钥信息。表示存在或不存在的信息包括“11”（标题-密钥和移动-密钥都存在）、“01”（不存在移动-密钥但存在标题-密钥）、“00”（标题-密钥和移动-密钥都不存在）。

当移动内容时，将加密内容保留在移动的源的原始媒体中，从移动-密钥文件删除相应于该被移动内容的内容移动-密钥（E-Kmv）（移动-密钥文件都变为“0”）。标题密钥文件中的存在或不存在信息变为“10”，而移动密钥文件中的该信息变为“01”。移动-密钥文件被改正（或更新）为新的移动-密钥文件。不从已加密的标题密钥文件中删除被移动内容的标题密钥。但是要根据新的移动-密钥文件将移动-密钥的校验数据（V-Mo）更新，并用保密信息更新数据（UD）加密，并且被记录为更新后的已加密移动-密钥文件（Enc V-Mo）。

这样，从第一媒体移动到另一个媒体的内容的标题密钥就被保留（加密）在第一媒体中，但是已加密标题密钥的解密是非常困难的，除非提供了已经从第一媒体中删除了的移动-密钥。另一方面，如果通过在移动之前复制该已加密的移动-密钥而保存了该移动-密钥，并且在移动处理后从复制的已加密移动-密钥文件中恢复该移动-密钥，那么该移动-密钥是与包含在标题-密钥文件中的移动-密钥校验数据（Enc V-Mo）不匹配的，所有可用的标题密钥不能被解密，防止了这样的非法处理。如果删除了用于解密内容的移动密钥，就不能解密该被删除的已加密标题密钥。相应于保留的移动密钥的保留的已加密标题密钥可以被解密。但是，如果将其中删除了某些移动密钥的移动密钥文件复原到未删除任何移动密钥的原始移动密钥文件，就不能校验该校验数据，这样所有的标题密钥就都不能使用了。这防止了移动密钥文件的非法备份和复原。

通过组成这样的已加密标题密钥文件和已加密移动密钥文件，当重复进行移动过程时，如果相同内容号码的内容被再次移动到某一记录媒体中，通过选择使用不能被再现和解密但记录在某一媒体中的加密内容，或者由加密该新传输的被移动内容来记录，就可能重编码移动再现降低了数据质量的高质量原始数据。

图 8 是当在多个记录媒体间移动内容时每个记录媒体的状态转换图。

记录在记录媒体 A 中的高质量内容被重新编码，并被移动到记录媒体 B 中。在记录媒体 B 中，记录了低压缩比的加密内容、多重加密的标题文件和已加密的移动-密钥文件。通过这个移动处理，从记录媒体 A 中删除对象内容的已加密移动-密钥。由普通移动处理，将一内容从记录媒体 B 移动到记录媒体 C 中。此时，将此内容的移动-密钥从记录媒体 B 中删除。

当将内容从记录媒体 C 移到原始记录媒体 A 时，通过确认其内容号码是相

同的，不能被解密并且已经记录在记录媒体 A 中的加密内容就被保持记录在记录媒体 A 中，并且记录媒体 C 中的该内容不移动，而仅仅将移动-密钥移到记录媒体 A 中。

通过这个过程，解密该标题密钥的条件就就绪了，该标题密钥用于为了解密一个记录在记录媒体 A 中的并且当前很难被解密的加密内容，该加密内容可以被解密，结果，记录原始高质量内容的记录媒体 A 就被复原了。

图 9 是可以进行重编码移动内容的版权保护系统的配置图。

基本操作与图 6 是相同的。也就是，图 6 表示了移动处理中内容提供侧驱动器和内容接收侧驱动器之间的关系，而图 9 表示了新内容的记录和加密处理以及特定内容的移动处理中的读取和解密处理。

尽管在图 6 中未经区分而一起表示，通过在图 9 中划分为用于内容编码处理的 A/V 板和用于记录及再现处理的驱动器，也表示了每个加密处理的排列关系。

加密单元 36 用 A/V 板 14 产生的标题密钥（Kt1'）32 将新内容 34 加密，并将其发送到驱动器 16。加密单元 30 用媒体专有密钥（Kmu）和媒体专有移动-密钥（Kmum）将标题密钥（Kt1'）加密，其中该媒体专有密钥通过预先从信号处理单元[G]28 中利用从记录媒体 12 中读出的 MKB 和 MID 产生，媒体专有移动-密钥（Kmum）是从信号处理单元[G]92 中利用新的移动-密钥（Kmv1'）104 产生，从而产生已加密的标题密钥（E-Kt1'）。相似的，解密单元（D）94 利用该媒体专有密钥（Kmu）将用于已记录媒体的移动-密钥文件（E-Kmv0）解密，以产生移动-密钥（Kmv0），其中该已记录的加密内容预先从记录媒体 12 中读出。编辑器（EDT）96 将移动-密钥（Kmv0）和上述新的移动-密钥（Kmv1'）104 合并，产生移动-密钥（Kmv1）。此移动-密钥（Kmv1）被加密单元（E）98 利用媒体专有密钥（Kmu）加密，并作为已加密媒体专有密钥（E-Kmv1）发送到驱动器 16。从记录媒体 12 中，读出记录的加密内容的多重加密标题密钥文件（E2-Kt0），该多重加密标题密钥（E2-Kt0）被驱动器 16 中的解密单元（D）60 利用记录在相同记录媒体 12 中的保密信息（UD0）解密，然后作为已加密的标题密钥文件（E-Kt0）从驱动器 16 发送到 A/V 板 14。

进一步地，移动-密钥校验数据处理单元（V-Mo）100 检测到上述移动-密钥（Kmv1）的校验数据（V-Mo1），数据编辑器（EDT）54 将该校验数据（V-Mo1）

与已加密标题密钥文件（E-Kt0）和已加密标题密钥文件（E-Kt1'）合并。从数据编辑器（EDT）中生成已加密标题密钥文件（E-Kt1），并将其发送到驱动器16。

向移动-密钥校验数据产生器(V-Mo)100提供已加密标题密钥文件(E-Kt0)中的移动-密钥校验数据（V-Mo0）和移动-密钥（Kmv1），其中，已加密标题密钥文件（E-Kt0）最初记录在记录媒体12中，并通过解密单元60获得，该移动-密钥（Kmv1）是编辑器96将新移动-密钥（Kmv1'）加到移动-密钥（Kmv0）上获得的，而该移动密钥(Kmv0)是通过解密读取的已加密移动-密钥(E-Kmv0)获得的。移动-密钥校验数据产生器（V-Mo）100 获得基于移动-密钥文件数据（Kmv0）的校验数据，该移动-密钥文件数据（Kmv0）中已经删除了该新的移动-密钥（Kmv1'），并且移动-密钥校验数据产生器（V-Mo）100检查该校验数据与已加密标题密钥文件（E-Kt0）中的校验数据是否一致并且检查在记录的加密内容中是否存在违法记录。校验数据产生的例子包括计算标题密钥的函数，并使计算结果为预定的幂数。例如，将移动-密钥1乘以函数α，其结果加上移动-密钥2，将结果乘以函数α^2，其结果加上0，再将结果乘以函数α^3，等等。校验数据的产生并不局限于上述方法。进一步地，计算并产生移动-密钥(Kmv1)的新校验数据，编辑器（EDT）54将其加到已加密标题密钥文件（E-Kt1）中。这样，就将A/V板发送的加密内容（Enc-content）直接记录在记录媒体12中了，并且将更新后的已加密移动-密钥文件（E-Kmv1）重写在更新前的已加密移动-密钥文件（E-Kmv0）上。

驱动器16中的加密单元56利用更新保密信息（UD1）将已加密标题密钥文件（E-Kt1）加密，其中，该更新保密信息（UD1）是通过更新先前读出的保密信息（UD0）而获得的，将多重加密标题密钥文件（E2-Kt1）记录在记录媒体12中。同样地，保密信息（UD1）被加密单元64利用媒体专有密钥（Kmu）加密，并且利用图13、14和15中所示的特殊记录方法将其作为已加密的保密信息（E-UD1）记录在记录媒体12中。特殊记录方法意味着记录的数据不能被普通再现方法再现。如果将纠错码加到主数据上，并且加上保密信息（例如，用异或操作），该保密信息就是主数据的差错。因此，当对主数据进行纠错操作时，保密数据就从主数据中消失了。由于纠错处理是在驱动器中执行的，所以可以防止驱动器外部执行的非法复制操作。

在A/V板和驱动器的关系中，在驱动器和A/V板之间的数据传输中非法复制的可能性就很高，其中该驱动器是PC（个人电脑）外围设备，而该A/V板是装配在个人电脑侧。

因此目前，要在驱动器和A/V板之间进行验证，并且在数据的传输中，利用只有在验证成功时才有效的时限加密/解密（总线-密钥）将数据加密和传输。也就是说，验证后，当相互确定了对方没有非法行为时，数据传输侧发送用总线-密钥加密的传输数据，而接收侧通过用总线-密钥解密来接收已加密的传输数据。

此过程在图9中的验证块和驱动器和A/V板之间的每条传输线的粗线部分之间进行。

图9中特定内容移动处理中的读取和解密处理机制与图6中所示的相同。作为记录侧的加密处理，移动-密钥校验数据处理单元（V-Mo）90 包括以下功能：根据记录在记录媒体 12 中记录的移动-密钥和包含在已加密标题密钥文件（E-Kt）中包括的移动-密钥校验数据（Enc V-Mo），检查在加密密钥中是否进行了非法记录，并且如果确定发现了非法记录，就拒绝再现。

图10和11表示了具体图9中数据读取侧的解密处理和记录侧的加密处理，其中包括了记录在记录媒体中的数据文件的关系。

在图10中，解释了记录媒体12中记录的数据文件和加密管理系统之间的关系。在下面的说明中，为了理清将加密的密钥和用在加密中使用的加密密钥之间的关系，加密数据被部分地表示为“E（加密密钥、要加密的数据）”。

预先记录的MKB文件114是已加密的密钥块，从该密钥块中提取出加密和解密处理中使用的媒体密钥（Km）。

MID 116是记录媒体12的特定标识信息，该信息记录在记录媒体12的最内部外围的BCA（burst cutting area）中，该信息用于当前DVD-RAM标准等等中。通过将此标识信息合并到加密管理系统中，加密就如同记录媒体上的媒体绑定功能那样运行。处理的结果是，从MKB 114和MID 116中提取出的媒体密钥（Km）在函数产生器[G]44中被合成，从而产生了媒体专有密钥（Kmu）。由于此媒体密钥（Kmu）的功能与对象媒体的特定加密密钥相同，所以如果将数据整体地复制到另一个记录媒体上，用此密钥加密的数据就不能被解密，其原因是此媒体的媒体专有密钥是不同的。

E（Kmu，UD）118是用特殊记录和再现方法记录的保密信息数据，该特殊记录和再现方法用媒体专有密钥（Kmu）加密保密信息（UD）。每次为移动处理单元读出内容以及每次记录新内容的时候，更新并记录保密信息。在仅仅内容读取和再现处理中，保密信息保持相同的记录状态。

E（Kmu，Kmv_i）120 是移动密钥文件。它是用媒体专有密钥（Kmu）加密的一组多个移动-密钥。在再现操作中，用媒体专有密钥（Kmu）将读出的已加密的移动-密钥（E-Kmv）解密，并从指定的内容标识信息中检测内容的移动-密钥（Kmv），函数产生器84将移动-密钥（Kmv）与媒体专有密钥（Kmu）结合，产生媒体专有移动-密钥（Kmum）。在移动处理的再现中，媒体专有移动-密钥（Kmum）与移动-密钥一起传输到外部，其中该移动密钥与被移动内容相关并与被移动内容相配对，已加密标题密钥的解密处理之后，从移动-密钥文件中删除该移动-密钥。用媒体专有密钥（Kmu）加密该移动-密钥文件，并将其重写为一个新的移动-密钥文件。此时，根据用媒体专有密钥（Kmu）加密之前的新的移动-密钥文件，计算并产生移动-密钥的新校验数据。将该新的校验数据发送到用于合并新标题密钥文件数据的块中，并将其结合到标题密钥文件中。

E（UD，E（Kmum，Kt_i））122是多重加密的标题密钥文件。这是由仅在驱动器中记录和再现的保密信息（UD）多重加密一组多个已加密标题密钥和移动-密钥校验数据组成的文件。在再现操作中，E（UD，E（Kmum，Kt_i））122被在驱动器中解调的保密信息(UD)解密，产生已加密标题密钥文件(E-Kt)。用媒体专有移动-密钥（Kmum）将已加密标题密钥文件（E-Kt）解密，并产生标题密钥文件（Kt）。将一对象内容的标题密钥文件（Kt）提供给内容解密单元48。在移动处理再现操作中，将根据移动-密钥文件计算的移动-密钥校验数据与先前的校验数据替换，其中该移动-密钥文件中已经删除了相应于被移动内容的移动-密钥，而该先前的校验数据是附加到已加密标题密钥文件（E-Kt）的，并且产生了新的已加密标题密钥文件（E-Kt）。将此新的已加密标题密钥文件（E-Kt）发送到驱动器，并由更新后的新UD数据加密，并将其记录在记录媒体中。也就是说，在移动处理中，涉及被移动内容的的已加密标题密钥并没有被删除，并且被保留了，并且存在被移动内容的数据文件，但是已加密标题文件被改变成标识代码作为指示该标题密钥不能解密的信息。当然，当给出内容删除命令时，就删除了该对象内容的已加密标题密钥，并且其它信息也被删除

了，这样就不存在已删除的内容了。

E（Kt，content_1）124是被加密密钥（Kt）加密的内容文件。

图11表示了一个加密管理处理，其中包括记录在记录媒体中的数据文件与记录新内容时的新文件之间的关系。在记录过程中，假设有三种类型，即，“记录新来自某一其它数据源的内容（产生新移动-密钥）”、“记录与移动-密钥成对形成的新内容”的移动处理记录以及“基于包含在移动-密钥数据中的内容号码（内容标识信息）确定”加密内容是否出现在记录媒体中，在该记录媒体中，相同标识号码的移动-密钥被删除。构成记录侧加密管理处理以对所有这些要求可用。

在如上述所说明的模式中使用一预先记录的MKB文件114。

MID 116也与上述说明相同。

如图10所示，当每次重写移动-密钥文件或标题密钥文件时，都将E(Kmu，UD）文件118更新为新数据，并且由加密单元64用媒体专有密钥（Kmu）将其加密和重写。

E（Kmu，Kmv_i）文件120是移动-密钥文件，在移动记录的情况下或者当记录新内容时，就添加新移动-密钥，并且由加密单元98利用媒体专有密钥（Kmu）将新文件加密和重写。这就是一个自我管理的内容文件，并且在完整的新内容中，产生内容管理号码（标识ID）和新的移动-密钥，将这些产生的密钥添加到记录在记录媒体中的移动-密钥文件中，并且在记录媒体中产生、加密并记录新的移动-密钥文件。当输入的内容伴随有移动-密钥时，确定记录媒体中是否存储了标识号码与输入内容的标识号码一致的内容。如果标识号码相互一致并且记录媒体不能进行重编码移动处理，就不记录内容数据，而仅仅将移动-密钥添加到移动-密钥文件的特定位置上，并将其重写。如果标识号码相互不一致，与记录新内容相同，在记录媒体上记录移动-密钥文件和内容文件。在这种情况下，移动-密钥被记录为记录内容的移动-密钥。

E（UD，E（Kmum，Kt_i））文件122是一个标题密钥文件。当记录新内容时，由随机号码产生器等新产生一个标题密钥32，并由编辑器54将其与记录在记录媒体中的另一内容的标题密钥合并，并将其与新移动-密钥校验数据一起被编辑为新的标题密钥文件，并被加密单元56利用保密信息（UD）多重加密，其中该保密信息被驱动器中的更新单元62更新。在移动处理中，将与内容成对

发送的移动-密钥信息中的内容号码（标识 ID）与已经在记录媒体中记录的内容号码信息相比较，以确定是否已经记录了相同的内容，当已经记录了相同的内容时，不发布新的标题密钥，而仅重写新移动-密钥文件的校验数据，并且生成新的已加密标题密钥文件，将该新的已加密标题密钥文件被更新后的 UD 多重加密，并被记录在记录媒体中。如果没有记录相同内容，那么发布新的标题密钥，并将其用在输入内容的加密中，同时，用媒体专有移动-密钥（Kmum）将新的标题密钥加密，其中该媒体专有移动-密钥（Kmum）由媒体专有密钥（Kmu）和移动-密钥（Kmv）产生，该媒体专有密钥（Kmu）是从驱动器中的记录媒体中记录的 MKB 和 MID 提取的，该移动-密钥（Kmv）是与内容成对发送的。将新标题密钥添加到记录的已加密标题密钥文件中，而组成新的标题密钥文件，并用更新后的 UD 将该新的标题密钥文件多重加密，并记录在记录媒体中。

E（Kt，content_i）124 意味着由标题密钥（Kt）加密的多个内容文件。当移动中已经记录了相同内容时，可以选择是否记录该加密内容。当已经将其记录时，在记录了高质量数据的情况下，就不记录被移动的内容数据了。在记录了高质量数据的情况下，就不记录被移动的内容数据了。在没有记录高质量数据的情况下，例如，已记录数据的质量是相同或较低的，就需要用户来决定了。

图 12 是根据本发明的记录媒体的数据构成图，其中该数据媒体具有记录的加密内容和已加密的加密密钥。媒体 ID（MID）是提前在引导区域内侧提供的 BCA 中写入的信息数据。在记录和再现媒体中，由于 ID 号码是单独记录的，通过在加密管理系统中引入 ID 号码，加密密钥就成为每个媒体中的专有密钥，并且预期具有绑定在记录加密内容的记录媒体的效果。MKB 是预先记录在引导区域的一串密钥，可以由分别分布在记录和再现装置中的设备密钥（D－K）提取出同一媒体密钥（Km）。在数据区域的内围侧，记录了本发明的移动-密钥文件和双重加密的标题文件，在外围，记录了加密内容文件。

图 13 是用于解释本发明的保密信息 UD 的嵌入处理方法的图。M-数据选择 R01 选择用于加密的 MKB（媒体密钥块）、加密内容以及要记录到盘 AD1 的用于加密/解密的加密密钥。IED 产生用于产生被称为扇区的物理数据块的 ID（标识数据）的 IED（ID 错误检测代码）。ID 包括扇区号码和扇区信息。

首先，将需要记录的数据与 2K 字节的数据帧单元中的扇区 ID 和其它信息合并，并通过错误检测代码（EDC）产生器 R02 将其输入到扰码处理单元 R03

中。这里，为了伺服系统的稳定性，进行扰码处理是以防止连续出现相同的数据。扰码处理单元R03的输出数据被输入到16数据帧处理单元D031中，将16组数据帧合并。数据被输入PO/PI产生器R051，产生错误检测和校正码（PO/PI）。

接着，数据（PO/PI）被输入到PO交织处理单元R06，PO被交织处理以及分散和安排，组成了16组ECC块的记录扇区。PO交织处理单元R06的输出数据被输入到同步叠加和调制处理单元R07，在每个特定数据长度中都叠加和调制同步信号。处理单元R07的输出被输入到UD替换单元R14，产生16组物理扇区。

另一方面，在UD-Pa（UD奇偶性）处理单元R11和调制-2单元R13中，UD信号R10被特殊调制器R13调制，在UD替换单元R14中用处理单元R07的输出部分地替换调制后的UD。然后通过记录媒体写入单元R08将其记录在记录媒体AD1中。

通过这样的处理，被UD调制信号替换的部分被看作是主数据块中的错误，但是当错误量级很小时，就将被替换的部分作为普通错误的部分处理，并且由错误校正处理改正。另一方面，由仅仅安装在驱动器中的特殊解调器解调特殊调制的UD，利用UD专用纠错码将解调后的UD进行纠错处理。

利用这样的处理，仅仅在驱动器中才能记录或再现以及使用该UD数据，并且不能在外部操作该UD数据，因此UD数据可以被用作保密信息，并且当将其运用在加密密钥的更新后数据时，就可以有效阻止将预先保存的已加密的加密密钥复原为删除的已加密加密密钥的非法复制。

图14是由DVD系统的由16组记录扇区组成的ECC方框图。

图15是表示了嵌入保密信息的一个物理扇区的关系的图。在多个物理扇区中将保密信息（UD）分散和配置，并且不需要明显损坏主信息的纠错能力，就能提高主信息的复原。

图16和17表示本发明的第二实施例。

在图6和7所示的第一实施例中，通过利用与移动-密钥和标题密钥联系的更新信息（UD），防止了从保存的备份数据复原标题数据文件的非法复制。通过将移动-密钥的校验数据汇编到标题密钥文件中，防止了利用保存的备份数据将移动-密钥文件非法重复原。在图16和17的第二实施例中，不使用移动-密钥

校验数据，并且利用更新信息（UD）将移动-密钥文件和标题密钥文件多重加密，当进行记录或移动时要经常用更新信息（UD）更新加密密钥文件，这样就能禁止通过保存备份数据的非法复原。其它数据处理与图 6 和图 7 的处理相同。

图 18 是标题密钥的加密处理修改实例。

在图 6 到图 16 中，函数产生器（G）通过将媒体专有密钥（Kmu）和移动-密钥（Kmv）合成而组成了标题密钥（Kt），并且产生了媒体专有移动-密钥（Kmum），通过利用该媒体专有移动-密钥（Kmum），将标题密钥（Kt）加密。这就是图 18 中的方法 A。

在其它的处理中，在利用媒体专有密钥（Kmu）将标题密钥（Kt）加密后，进一步将其利用移动-密钥（Kmv）进行多重加密，并且进一步利用移动-密钥将其三重加密，这就是方法 B。在此方法中，不产生媒体专有移动-密钥（Kmum）。即，标题密钥被加密三次。

虽然上述说明涉及了本发明的特定实施例，但是应当理解在不背离其精神的条件下可以对其进行多种修改。所附的权利要求书就试图覆盖这些落入本发明的实际范围和精神的修改。因此从各种方面来说，这些实施例中的记录媒体 12 都被认为是例证性的，而并不是限制性的，本发明的范围将由所附的权利要求所指示，而不是前面的说明书所指示的内容，并且本发明包含了落入本权利要求的等同物的含义和范围的所有改变。

根据本发明的一个实施例，提供了一种记录和再现装置，该装置用于将内容数据从第一记录媒体移动到第二记录媒体，其中，所述第一记录媒体记录了加密内容（Enc-content）、第一已加密密钥（E-Kt）以及第二已加密密钥（E-Kmv），所述加密内容（Enc-content）是通过用第一密钥（Kt）加密明文内容获得的，所述第一已加密密钥（E-Kt）是通过用第四密钥（Kmum）加密第一密钥而获得的，而该第四密钥从第二密钥（Kmv）和第三密钥（Kmu）产生，所述第二已加密密钥（E-Kmv）是用所述第三密钥（Kmu）加密所述第二密钥（Kmv）而获得的，所述装置包括:

解密单元，其将从所述第一记录媒体中读取的所述加密内容（Enc-content）以及所述第二已加密密钥（E-Kmv）解密，以获得所述明文内容和所述第二密钥;

传送单元，其将所述明文内容和所述第二密钥传送给所述第二记录媒体;

以及

删除单元，其从所述第一记录媒体中删除所述第二已加密密钥（E-Kmv），

由此使所述加密内容（Enc-content）和所述第一已加密密钥保持记录在所述第一记录媒体上，但禁止所述加密内容（Enc-content）被解密。

根据本发明另一实施例，提供了一种记录和再现装置，该装置用于将内容数据从第一记录媒体移动到第二记录媒体上，其中，所述第一记录媒体记录了加密内容（Enc-content）、第一已加密密钥（EE-Kt）、第二已加密密钥（E-Kmv）以及第五已加密密钥（E-UDm），所述加密内容（Enc-content）是通过用第一密钥（Kt）加密明文内容获得的，所述第一已加密密钥（EE-Kt）是用第四密钥（Kmum）和第五密钥（UDm）加密第一密钥而获得的，该第四密钥（Kmum）从第二密钥（Kmv）和第三密钥（Kmu）产生，所述第二已加密密钥（E-Kmv）是用所述第三密钥（Kmu）加密所述第二密钥（Kmv）而获得的，所述第五已加密密钥（E-UDm）是用预定密钥加密所述第五密钥（UDM）而获得的，所述装置包括:

读取单元，其从所述第一记录媒体中读取所述第一已加密密钥（EE-Kt）、所述第二已加密密钥（E-Kmv）和所述第五已加密密钥（E-UDm）;

解密单元，其用所述第三密钥（Kmu）解密所述第二已加密密钥（E-Kmv），以获得所述第二密钥（Kmv）;

解密单元，其用所述预定密钥解密所述第五已加密密钥（E-UDm），以获得所述第五密钥（UDm）;

解密单元，其用所述第四密钥（Kmum）和所述第五密钥（UDm）解密所述第一已加密密钥（EE-Kt）以获得所述第一密钥（Kt），所述第四密钥（Kmum）从所述第二密钥（Kmv）和所述第三密钥（Kmu）产生;

解密单元，其用所述第一密钥（Kt）解密所述加密内容（Enc-content），以获得所述明文内容;

传送单元，其将所述明文内容和所述第二密钥传送给所述第二记录媒体;

删除单元，其从所述第一记录媒体中删除所述第二已加密密钥（E-Kmv）;

更新单元，其更新所述第五密钥（UDm）;

加密单元，其用所述更新后的第五密钥（UDm）加密被所述第四密钥（Kmum）加密的所述第一密钥（E-Kt）以更新所述第一密钥（E-Kt），

加密单元，其用所述预定密钥加密所述更新后的第五密钥（Um），以改变所述更新后的第五密钥，

由此使所述加密内容（Enc-content）和所述第一已加密密钥保持记录在所述第一记录媒体上，但禁止所述加密内容（Enc-content）被解密。

所述装置还包括:

省略单元，该省略单元省略记录传送到所述第二记录媒体的明文内容，用所述第三密钥将传送到所述第二记录媒体的所述第二密钥加密，并且在传送到所述第二记录媒体的内容数据已经记录在所述第二记录媒体中的情况下，在所述第二记录媒体中记录所述已加密的第二密钥。

在所述装置中，所述第三密钥（Kmu）包括媒体专有密钥。

在所述装置中，所述第五密钥（UDm）是基于保密信息记录和再现系统的，其中，在所述保密信息记录和再现系统中仅仅在记录媒体的驱动器中允许执行记录、再现和密钥更新。

在所述装置中，所述内容数据包括多个内容，为所述多个内容提供多个第一密钥（Kt）和第二密钥（Kmv），从所述多个第二密钥（Kmv）计算校验数据（V-Mo），将所述校验数据（V-Mo）插入已加密的第一密钥（Kt）的文件中，用所述第三密钥（UDm）将插入后的已加密第一密钥（Kt）的文件加密以获得包括双重加密的第一密钥（EE-Kt）的已加密数据文件，并且将已加密的校验数据（Enc-V-Mo）记录在所述第一记录媒体中。

在所述装置中，所述已加密第一密钥的文件包括每个第一密钥的附加信息和标志，所述附加信息包括每个第一密钥的标识，所述标志指示了所述已加密第二密钥是被存储在所述第一记录媒体中还是被从所述第一记录媒体中删除；所述已加密第二密钥的文件包括每个第二密钥和被删除的第二密钥的附加信息和标志，所述附加信息包括每个所述内容的标识，所述标志指示所述已加密第一密钥是否被存储在所述第一记录媒体中。

在所述装置中，所述内容数据包括多个内容，为所述多个内容提供多个第一密钥（Kt）和第二密钥（Kmv）；用所述第四密钥加密所述多个第一密钥（Kt），以获得已加密第一密钥的文件；用所述第三密钥加密所述多个第二密钥（Kmum），以获得已加密第二密钥的文件；用更新后的第三密钥（UD）加密已加密第一密钥的文件和已加密第二密钥的文件，以获得双重加密的第一密钥

和双重加密的第二密钥；将双重加密的第一密钥和双重加密的第二密钥记录在所述第一记录媒体中。

在所述装置中，所述已加密第一密钥的文件包括每个第一密钥的附加信息和标志，所述附加信息包括每个第一密钥的标识，所述标志指示所述已加密第二密钥是被存储在所述第一记录媒体中还是被从所述第一记录媒体中删除；并且所述已加密第二密钥的文件包括每个第二密钥和被删除的第二密钥的附加信息和标志，所第二密钥和被删除的第二密钥的附加信息包括每个所述内容的标识，所述标志指示所述已加密第一密钥是否被存储在所述第一记录媒体中。

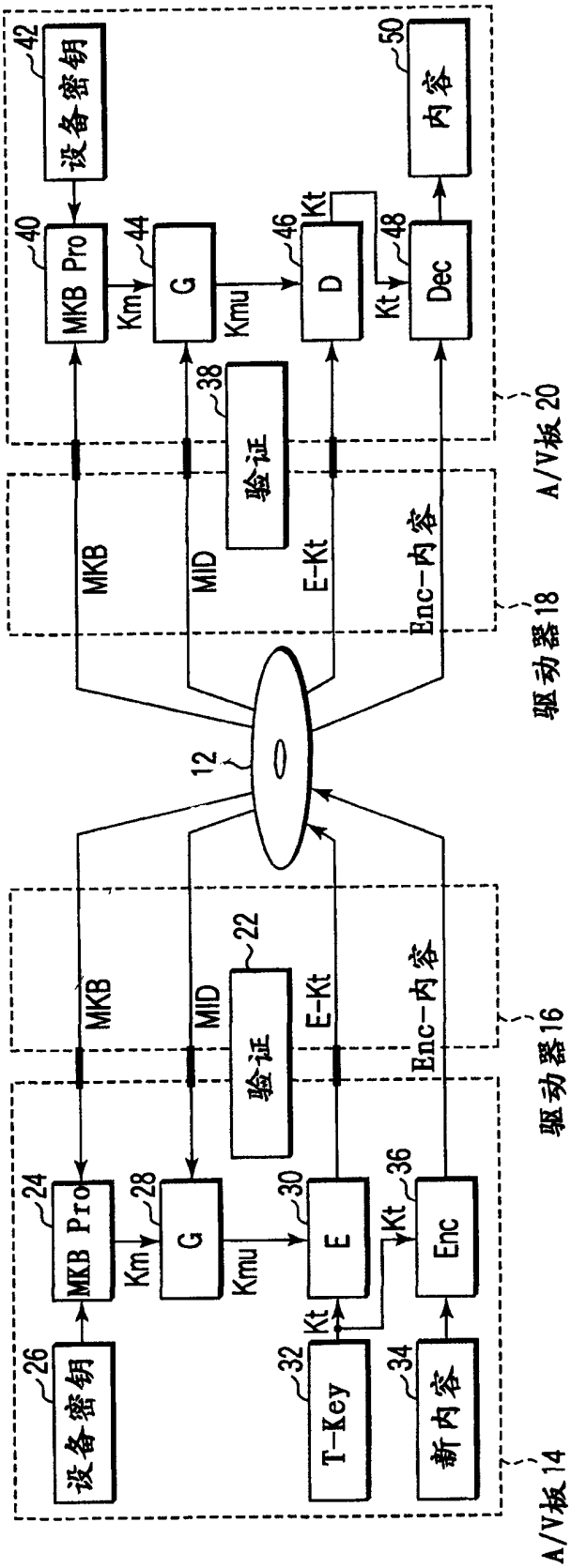

A/V板14
设备密钥 26
MKB Pro 24
Km
G 28
Kmu
E 30
Kt
T-Key 32
Kt
Enc 36
新内容 34
驱动器16
MKB
MID
验证 22
E-Kt
Enc-内容
12
驱动器18
MKB
MID
验证 38
E-Kt
Enc-内容
A/V板20
设备密钥 42
MKB Pro 40
Km
G 44
Kmu
D 46
Kt
Kt
Dec 48
内容 50

图 1

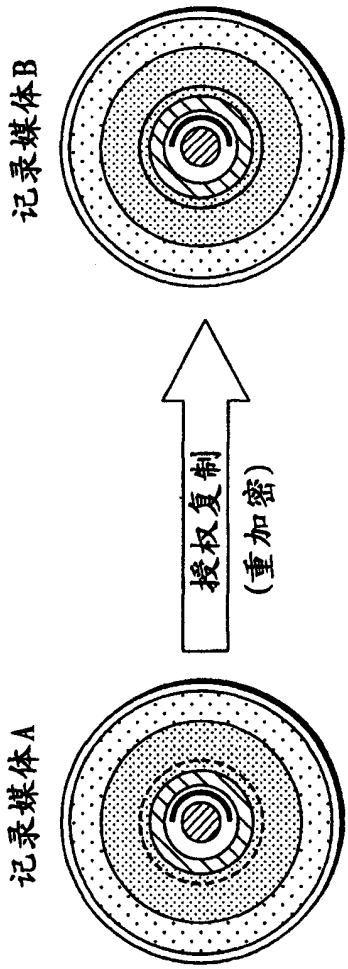

记录媒体A
授权复制
(重加密)
记录媒体B

图 2

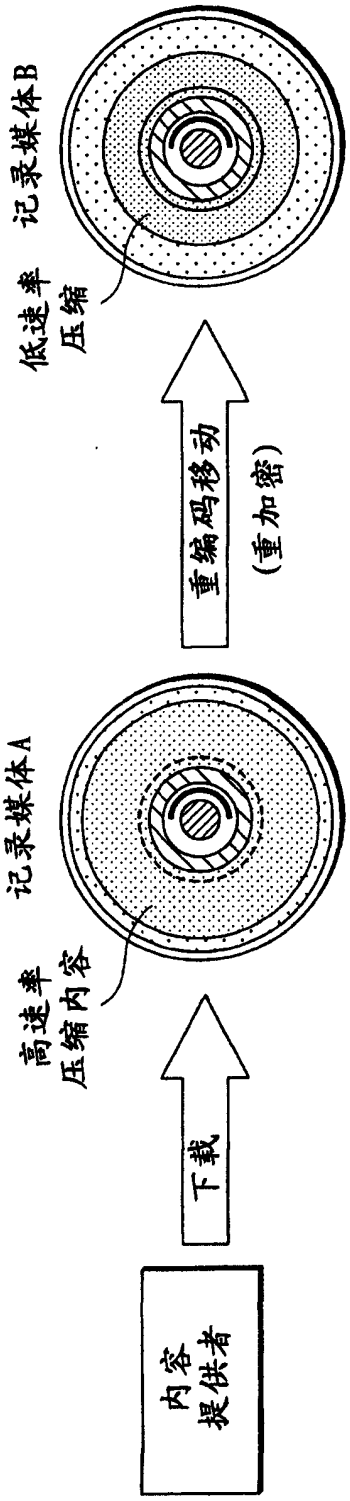

内容
提供者
下载
记录媒体A
高速率
压缩内容
重编码移动
(重加密)
记录媒体B
低速率
压缩

图 5

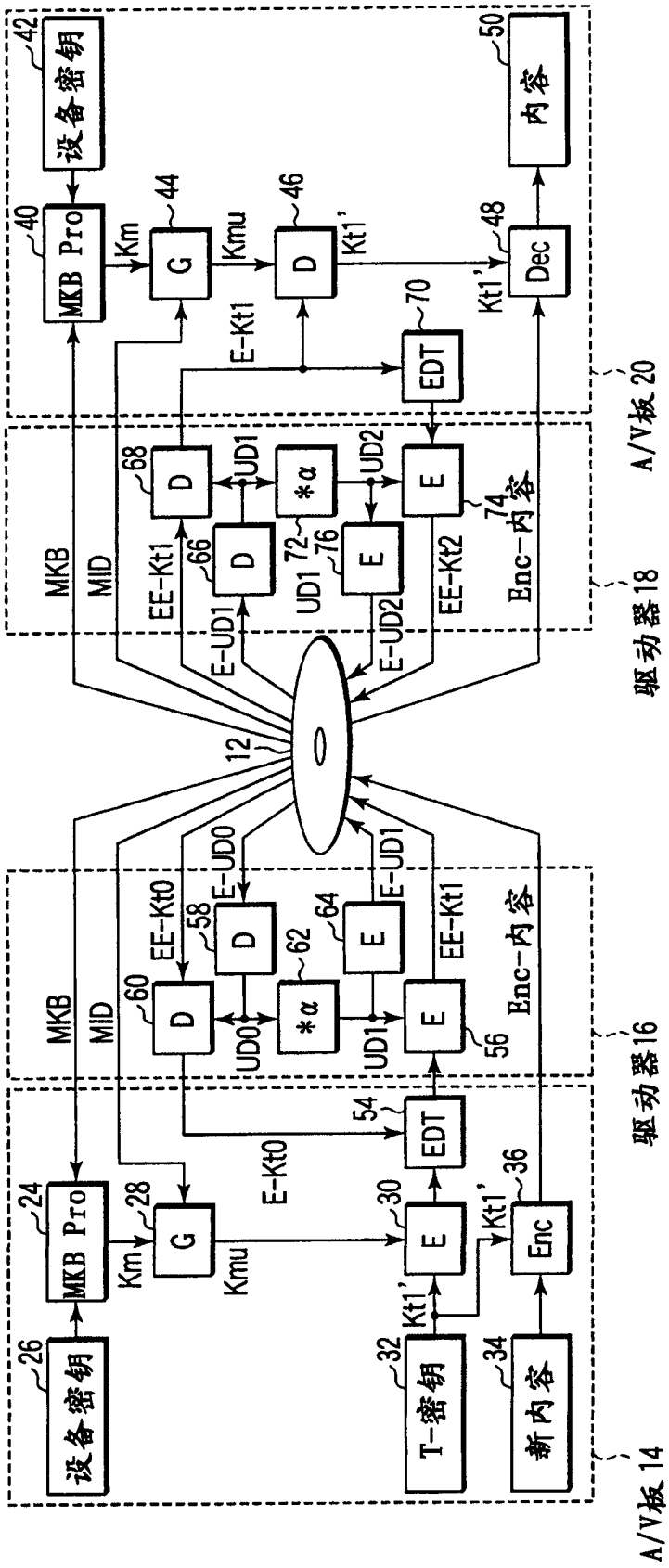

A/V板 14
驱动器16
驱动器18
A/V板 20
设备密钥
MKB Pro
G
D
Dec
内容
EDT
E
Enc
新内容
T-密钥
*α
MKB
MID
Km
Kmu
Kt1'
E-Kt0
E-Kt1
EE-Kt0
EE-Kt1
E-UD0
E-UD1
E-UD2
EE-UD1
EE-UD2
UD0
UD1
UD2
Enc-内容
12
24
26
28
30
32
34
36
40
42
44
46
48
50
54
56
58
60
62
64
66
68
70
72
74
76

图 3

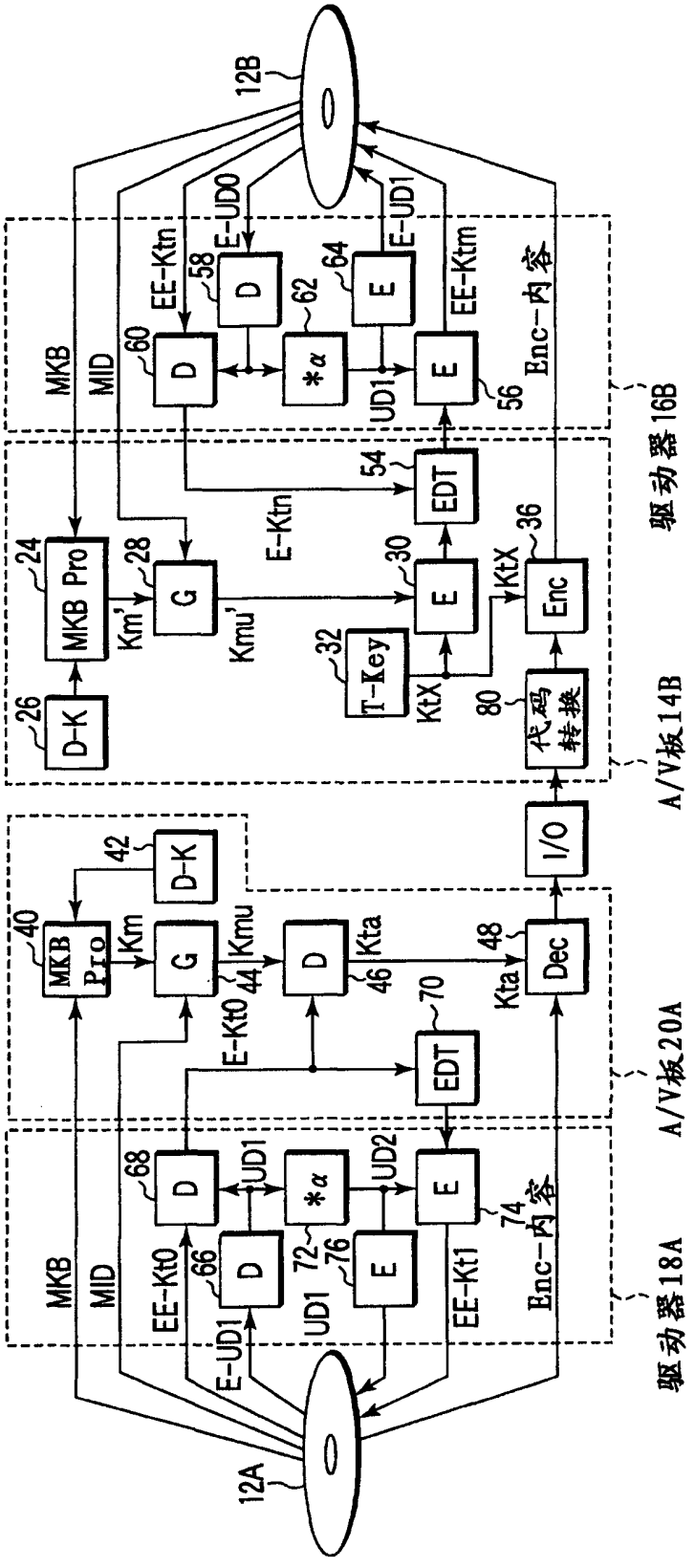

12B
MKB
MID
EE-Ktn
58
D
E-UD0
62
*α
64
E
E-UD1
EE-Ktm
60
D
UD1
E
56
Enc-内容
驱动器16B
54
EDT
E-Ktn
24
MKB Pro
Km'
28
G
Kmu'
30
E
KtX
36
Enc
26
D-K
32
T-Key
KtX
80
代码转换
A/V板14B
I/O
42
D-K
40
MKB Pro
Km
G
Kmu
44
D
Kta
46
48
Dec
Kta
E-Kt0
70
EDT
A/V板20A
68
D
UD1
*α
UD2
E
74
Enc-内容
MKB
MID
EE-Kt0
66
D
72
UD1
76
E
EE-Kt1
E-UD1
驱动器18A
12A

图 4

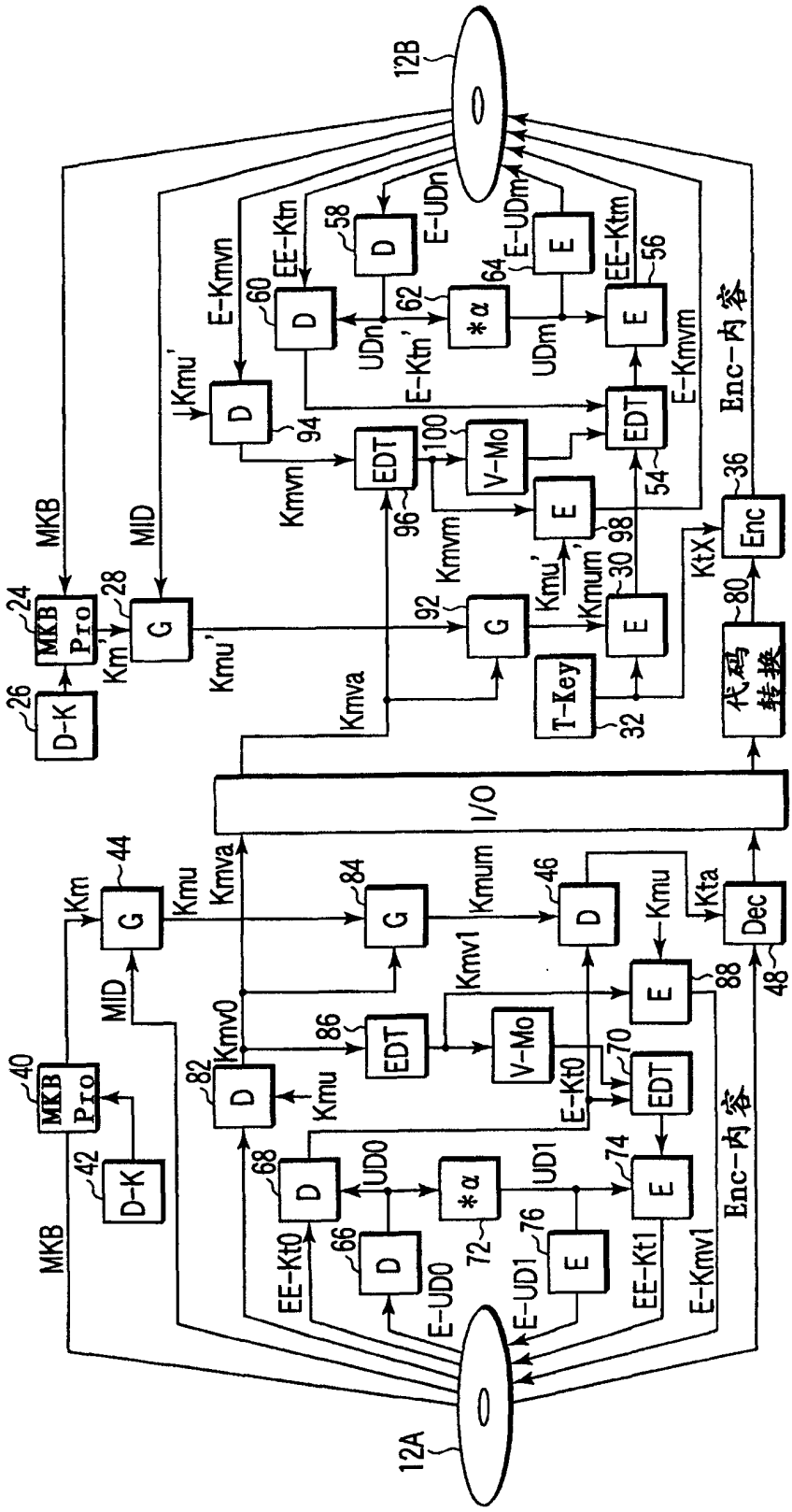

12B
12A
I/O
MKB
MID
D-K
MKB Pro
G
D
E
EDT
V-Mo
*α
T-Key
Enc
Dec
代码转换
Enc-内容
Km
Kmu
Kmva
Kmum
Kmv1
Kmv0
Kmvn
Kmvm
Kmu'
Km'
Kmum'
KtX
Kta
UDn
UDm
UD0
UD1
E-Ktm
E-Ktn'
E-Kt0
E-Kt1
E-Kmvn
E-Kmvm
E-Kmv1
E-UDn
E-UDm
E-UD0
E-UD1
EE-Ktm
EE-Kt0
EE-Kt1
24
26
28
30
32
36
40
42
44
46
48
54
56
58
60
62
64
66
68
70
72
74
76
80
82
84
86
88
92
94
96
98
100

图 6

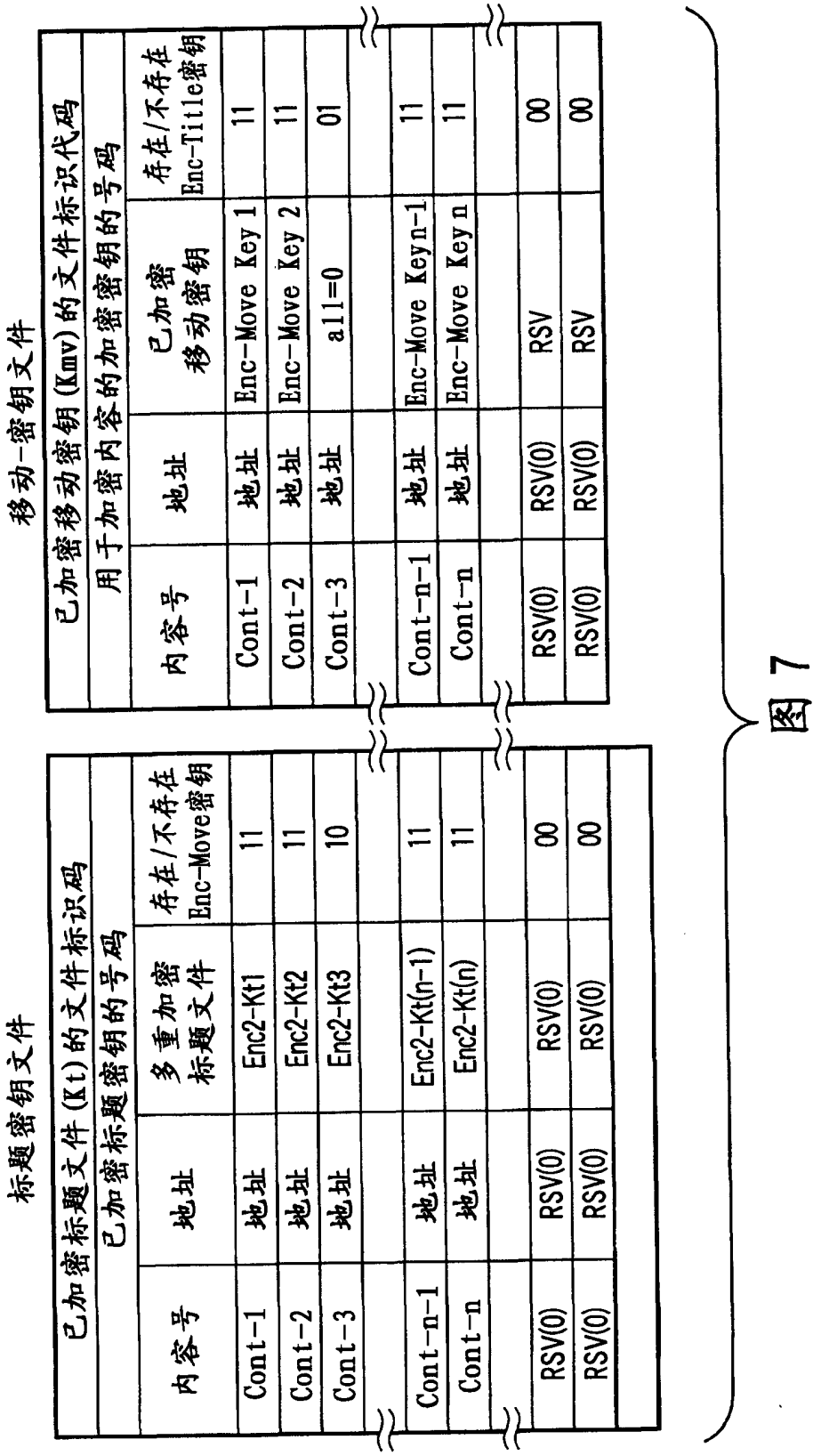

标题密钥文件
已加密标题文件(Kt)的文件标识码
已加密标题密钥的号码
内容号
地址
多重加密标题文件
存在/不存在Enc-Move密钥
Cont-1
地址
Enc2-Kt1
11
Cont-2
地址
Enc2-Kt2
11
Cont-3
地址
Enc2-Kt3
10
Cont-n-1
地址
Enc2-Kt(n-1)
11
Cont-n
地址
Enc2-Kt(n)
11
RSV(0)
RSV(0)
00
RSV(0)
RSV(0)
00
移动-密钥文件
已加密移动密钥(Kmv)的文件标识代码
用于加密内容的加密密钥的号码
内容号
地址
已加密移动密钥
存在/不存在Enc-Title密钥
Cont-1
地址
Enc-Move Key 1
11
Cont-2
地址
Enc-Move Key 2
11
Cont-3
地址
all=0
01
Cont-n-1
地址
Enc-Move Keyn-1
11
Cont-n
地址
Enc-Move Key n
11
RSV(0)
RSV(0)
RSV
00
RSV(0)
RSV(0)
RSV
00

图 7

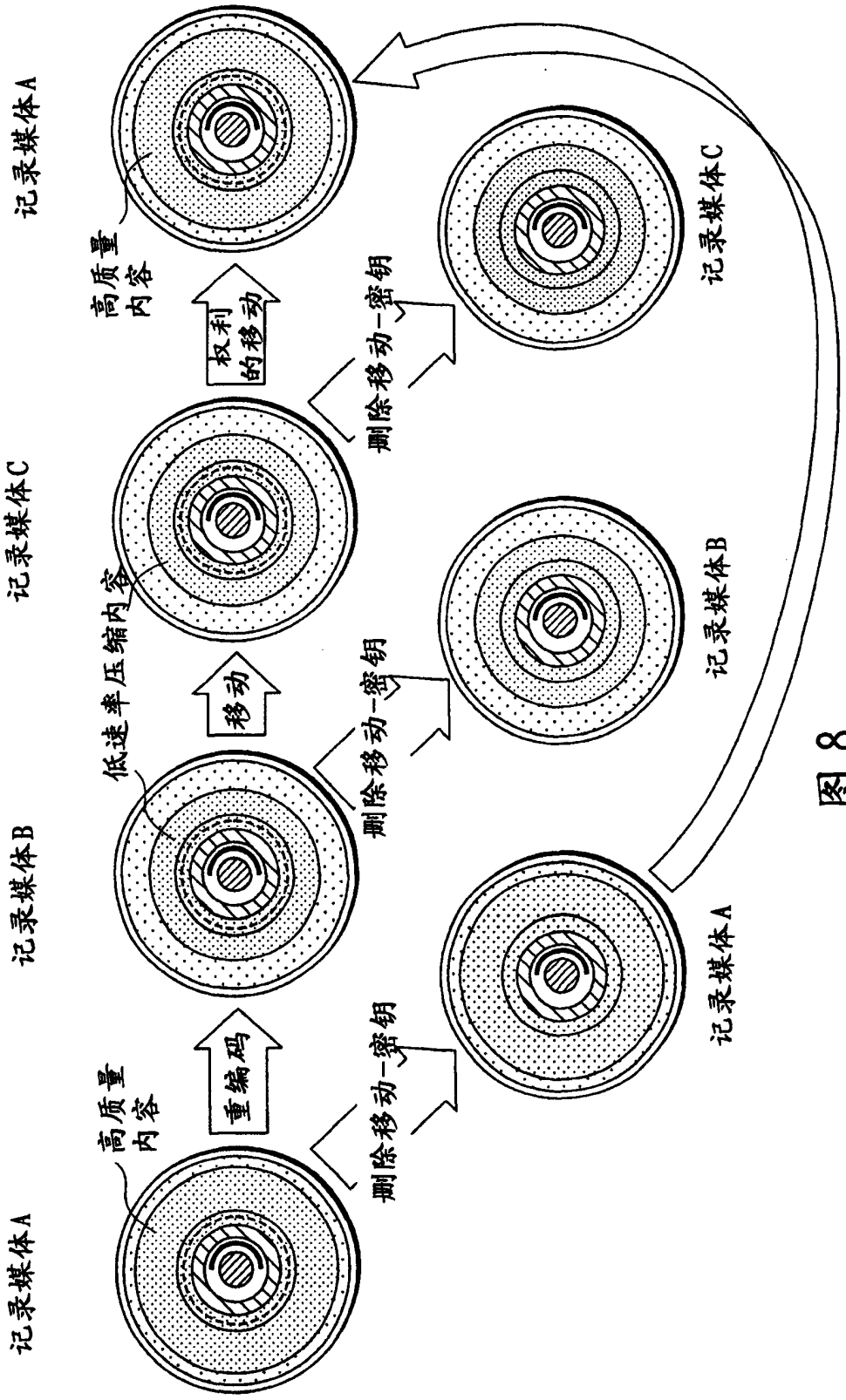

记录媒体A
记录媒体B
记录媒体C
高质量内容
重编码
低速率压缩内容
移动
权利的移动
删除移动-密钥
删除移动-密钥
删除移动-密钥
记录媒体A
记录媒体B
记录媒体C
高质量内容

图 8

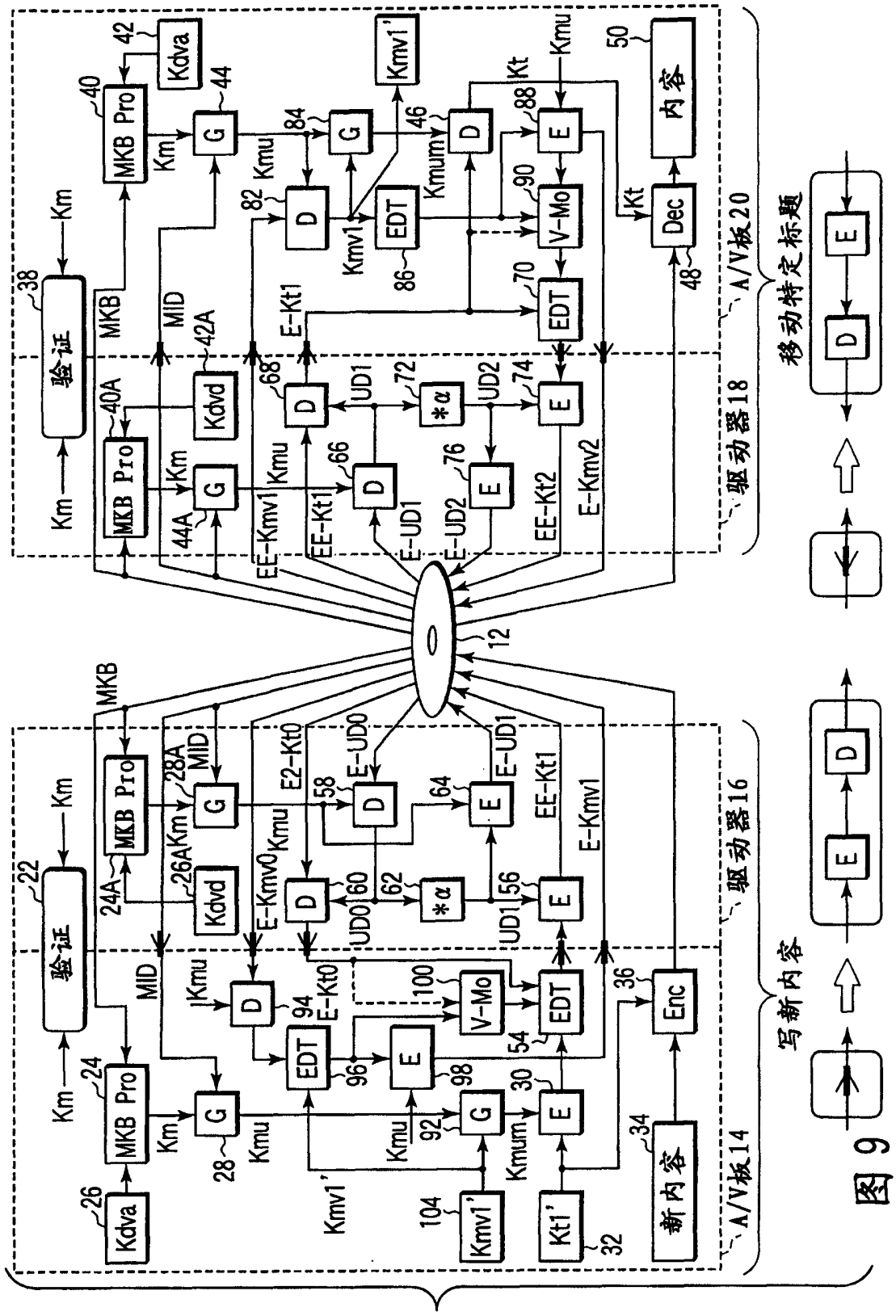

A/V板14
驱动器16
A/V板20
驱动器18
写新内容
移动特定标题
验证
MKB Pro
Kdva
Kdvd
MKB
MID
Km
Kmu
Kmv1
Kmv1'
Kmum
Kt
Kt1'
E-Kmv0
E-Kmv1
E-Kmv2
E-Kt0
E-Kt1
E-Kt2
E2-Kt0
EE-Kmv1
EE-Kt1
EE-Kt2
E-UD0
E-UD1
E-UD2
UD0
UD1
UD2
*α
EDT
V-Mo
Enc
Dec
新内容
内容
12
22
24
24A
26
26A
28
28A
30
32
34
36
38
40
40A
42
42A
44
44A
46
48
50
54
56
58
60
62
64
66
68
70
72
74
76
82
84
86
88
90
92
94
96
98
100
104

图 9

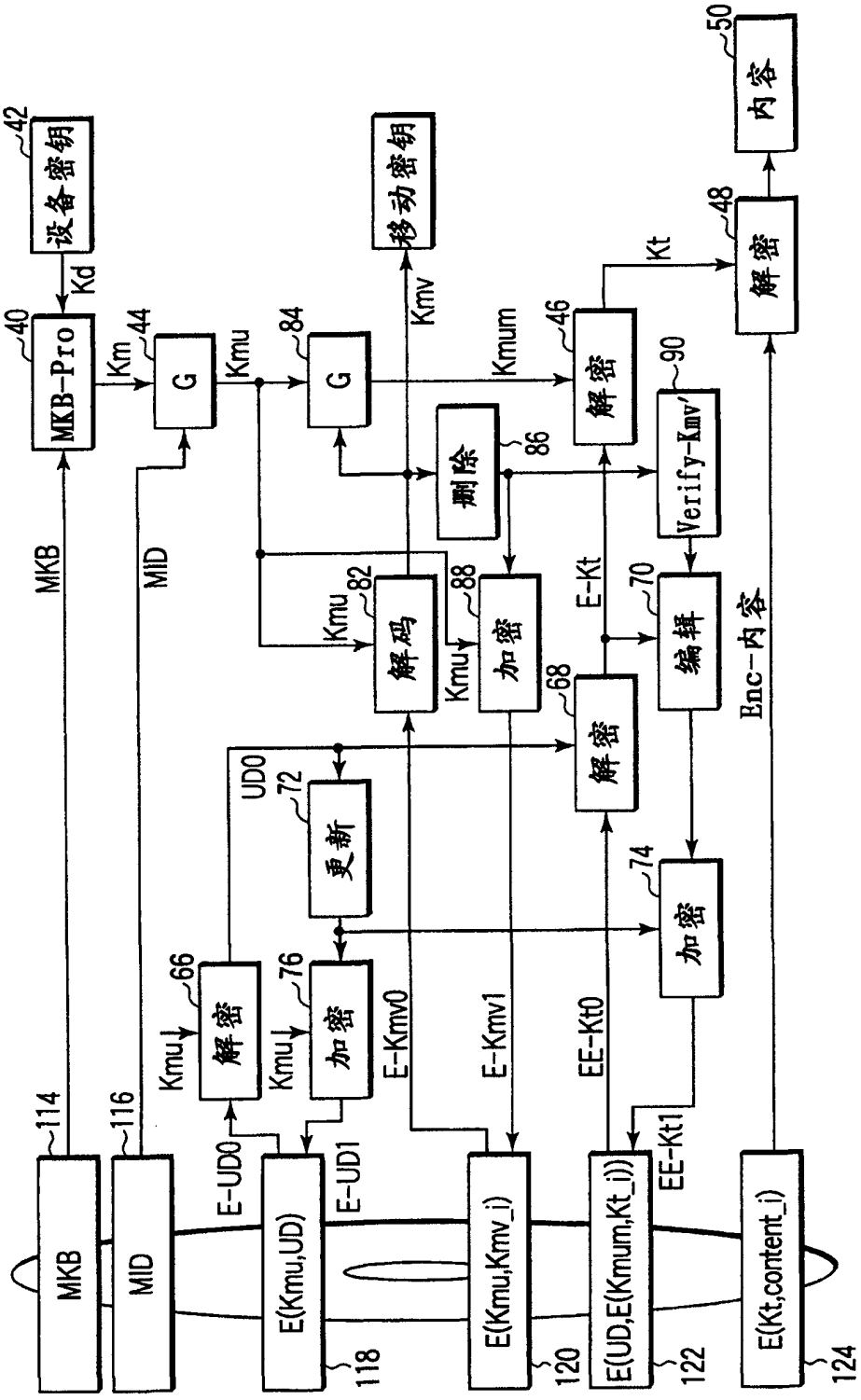

MKB
MID
E(Kmu,UD)
E(Kmu,Kmv_i)
E(UD,E(Kmum,Kt_i))
E(Kt,content_i)
114
116
118
120
122
124
E-UD0
E-UD1
E-Kmv0
E-Kmv1
EE-Kt0
EE-Kt1
Enc-内容
MKB-Pro
设备密钥
移动密钥
内容
G
G
解密
解密
解密
解密
加密
加密
加密
解码
更新
删除
编辑
Verify-Kmv'
Km
Kd
Kmu
Kmv
Kmum
Kt
E-Kt
UD0
40
42
44
46
48
50
66
68
70
72
74
76
82
84
86
88
90

图 10

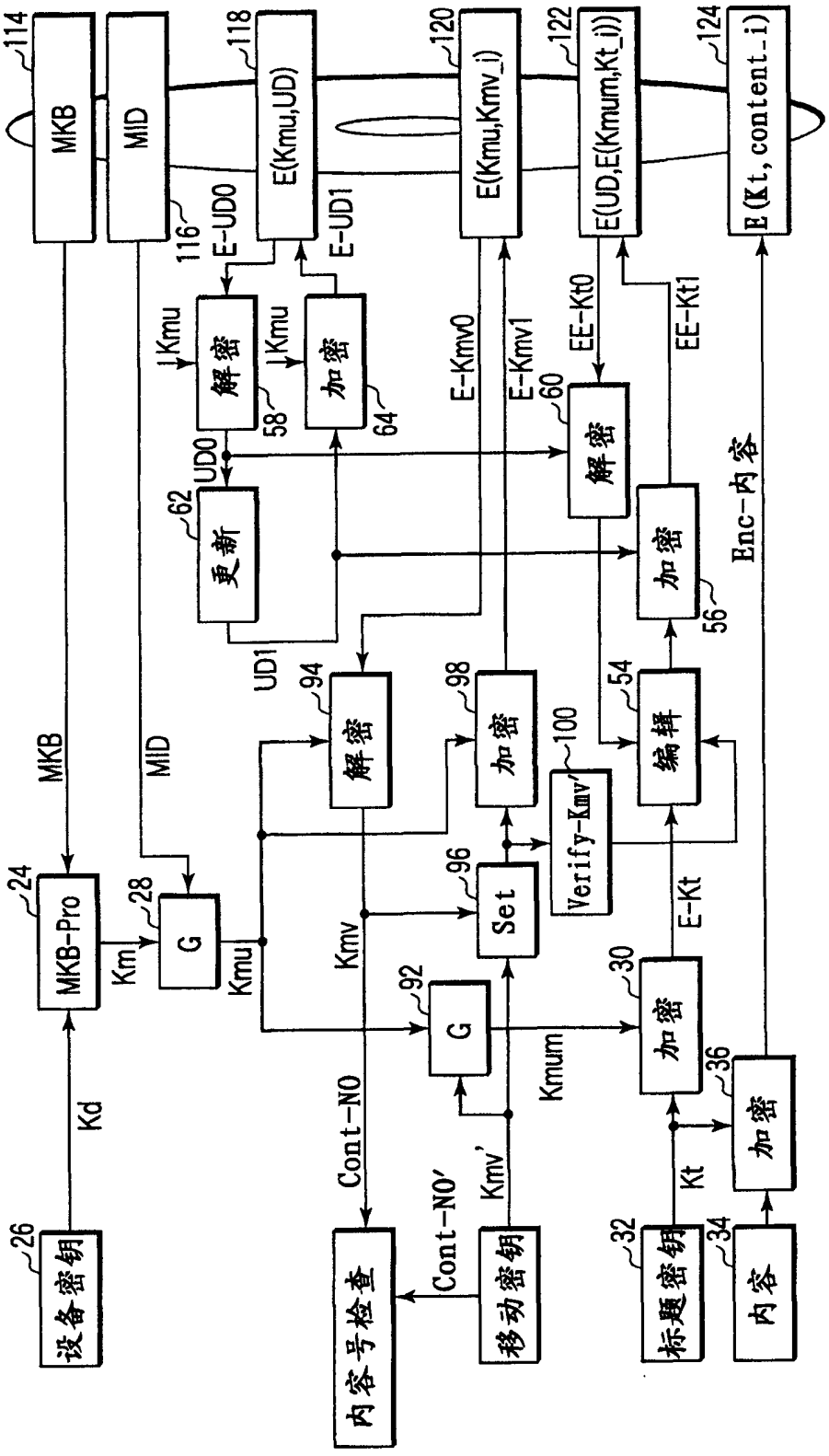

114
MKB
MID
118
E(Kmu,UD)
120
E(Kmu,Kmv_i)
122
E(UD,E(Kmum,Kt_i))
124
E(Kt,content_i)
116
E-UD0
E-UD1
Kmu
Kmu
解密
加密
58
64
E-Kmv0
E-Kmv1
EE-Kt0
EE-Kt1
60
解密
UD0
62
更新
加密
56
Enc-内容
UD1
94
解密
98
加密
100
Verify-Kmv
54
编辑
MKB
MID
24
MKB-Pro
28
G
Km
Kmu
Kmv
96
Set
92
G
30
加密
E-Kt
Kmum
36
加密
Kd
Cont-NO
Cont-NO'
Kmv'
Kt
26
设备密钥
内容号检查
移动密钥
32
标题密钥
34
内容

图 11

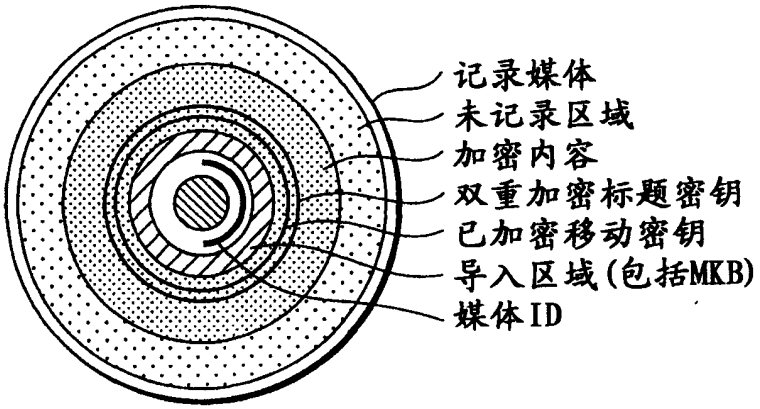


图 12

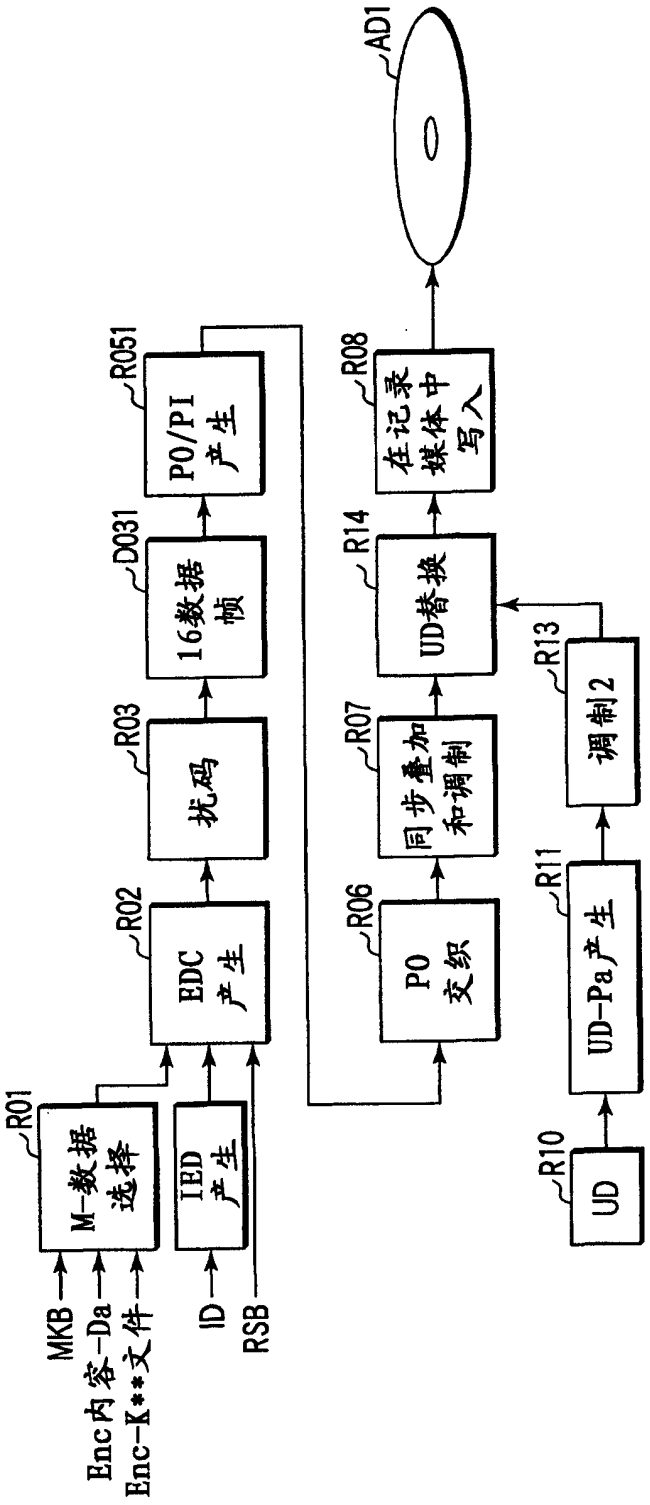

AD1
R051
PO/PI 产生
R08
在记录媒体中写入
D031
16数据帧
R14
UD替换
R03
扰码
R07
同步叠加和调制
R02
EDC 产生
R06
PO 交织
R01
M-数据选择
IED 产生
R13
调制2
R11
UD-Pa产生
R10
UD
MKB
Enc内容-Da
Enc-K**文件
ID
RSB

图 13

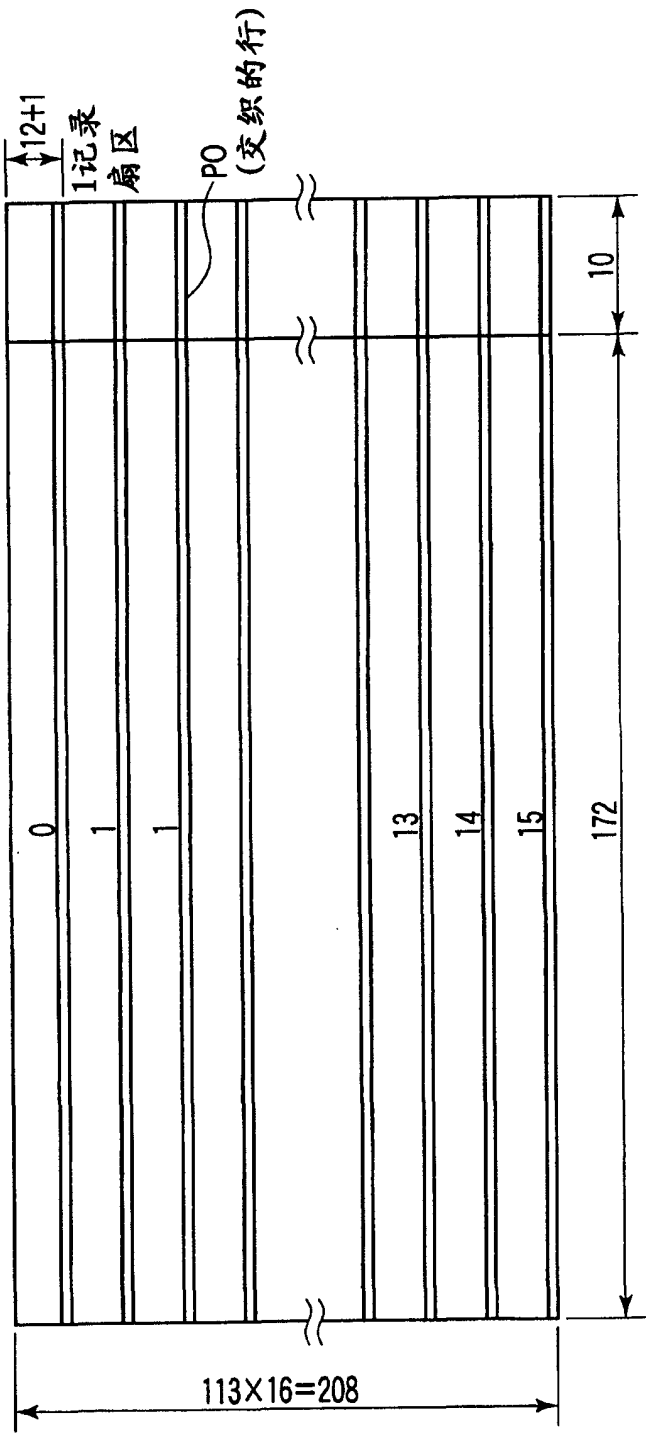


图 14

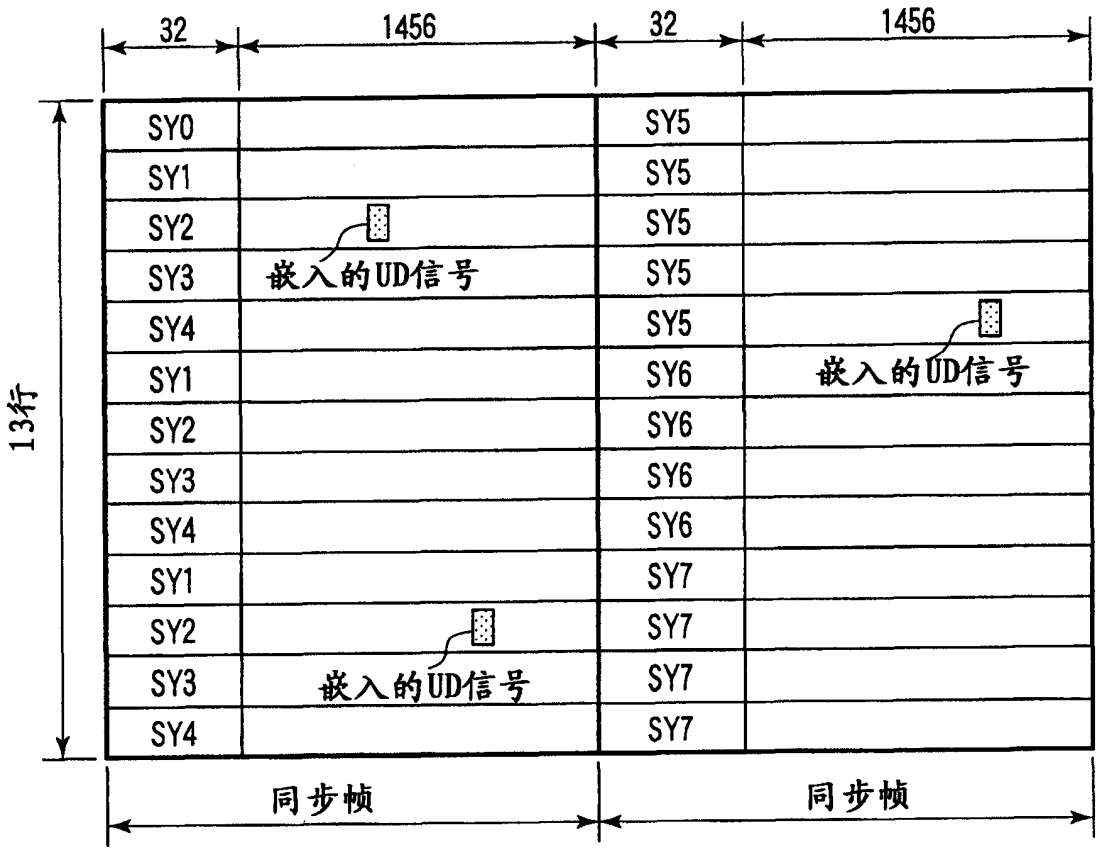

32
1456
32
1456
13行
SY0
SY1
SY2
SY3
SY4
SY1
SY2
SY3
SY4
SY1
SY2
SY3
SY4
SY5
SY5
SY5
SY5
SY5
SY6
SY6
SY6
SY6
SY7
SY7
SY7
SY7
嵌入的UD信号
嵌入的UD信号
嵌入的UD信号
同步帧
同步帧

图15

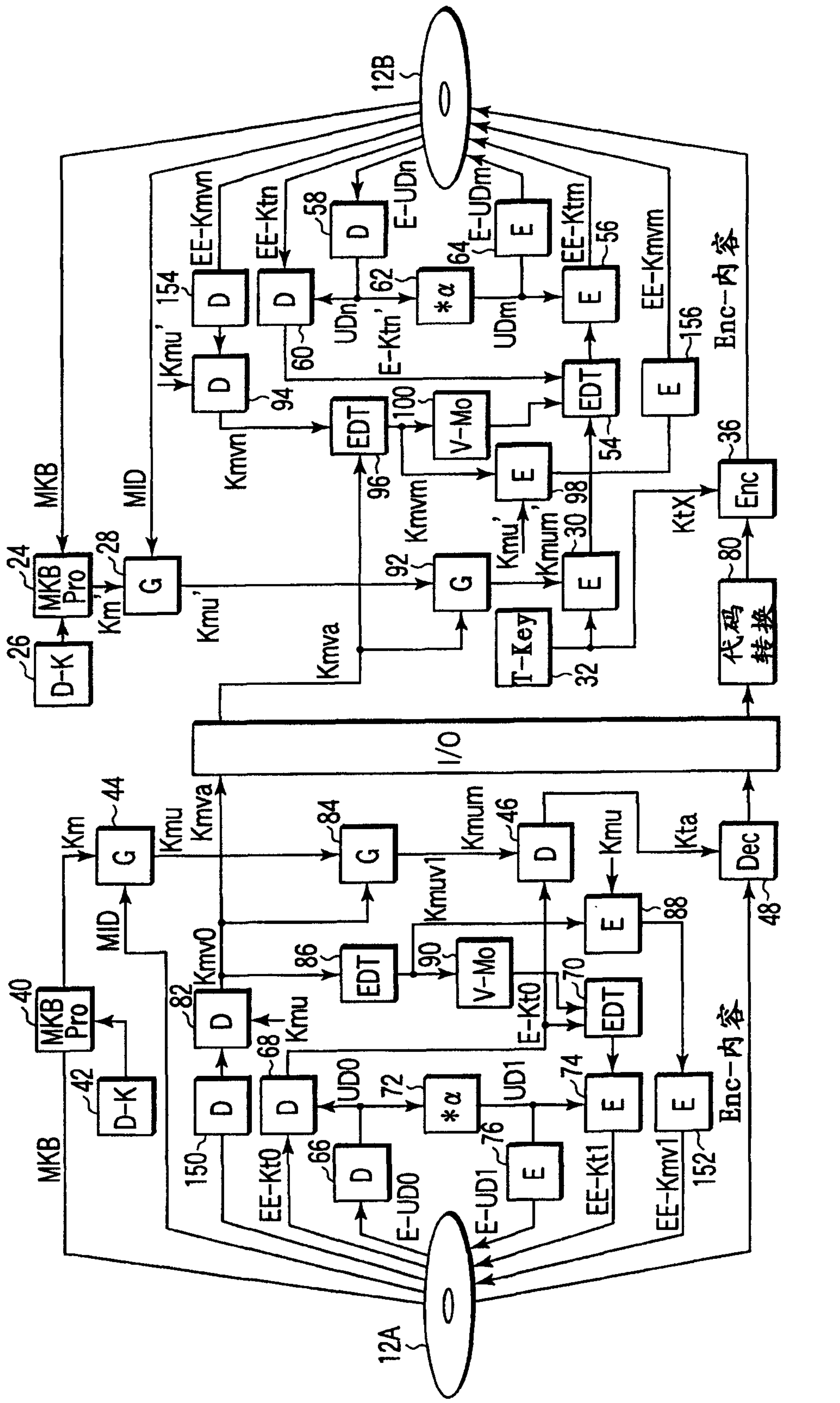

12A
12B
MKB
MID
D-K
MKB Pro
G
Km
Kmu
Kmva
Kmv0
Kmvn
Kmvm
Kmum
Kmuv1
Kmu'
Km'
EDT
V-Mo
I/O
T-Key
KtX
Kta
Enc
Dec
代码转换
Enc-内容
EE-Kmvn
EE-Ktn
E-UDn
E-UDm
EE-Ktm
EE-Kmvm
UDn
UDm
E-Ktn'
E-Kt0
UD0
UD1
EE-Kt0
E-UD0
E-UD1
EE-Kt1
EE-Kmv1
*α

图 16

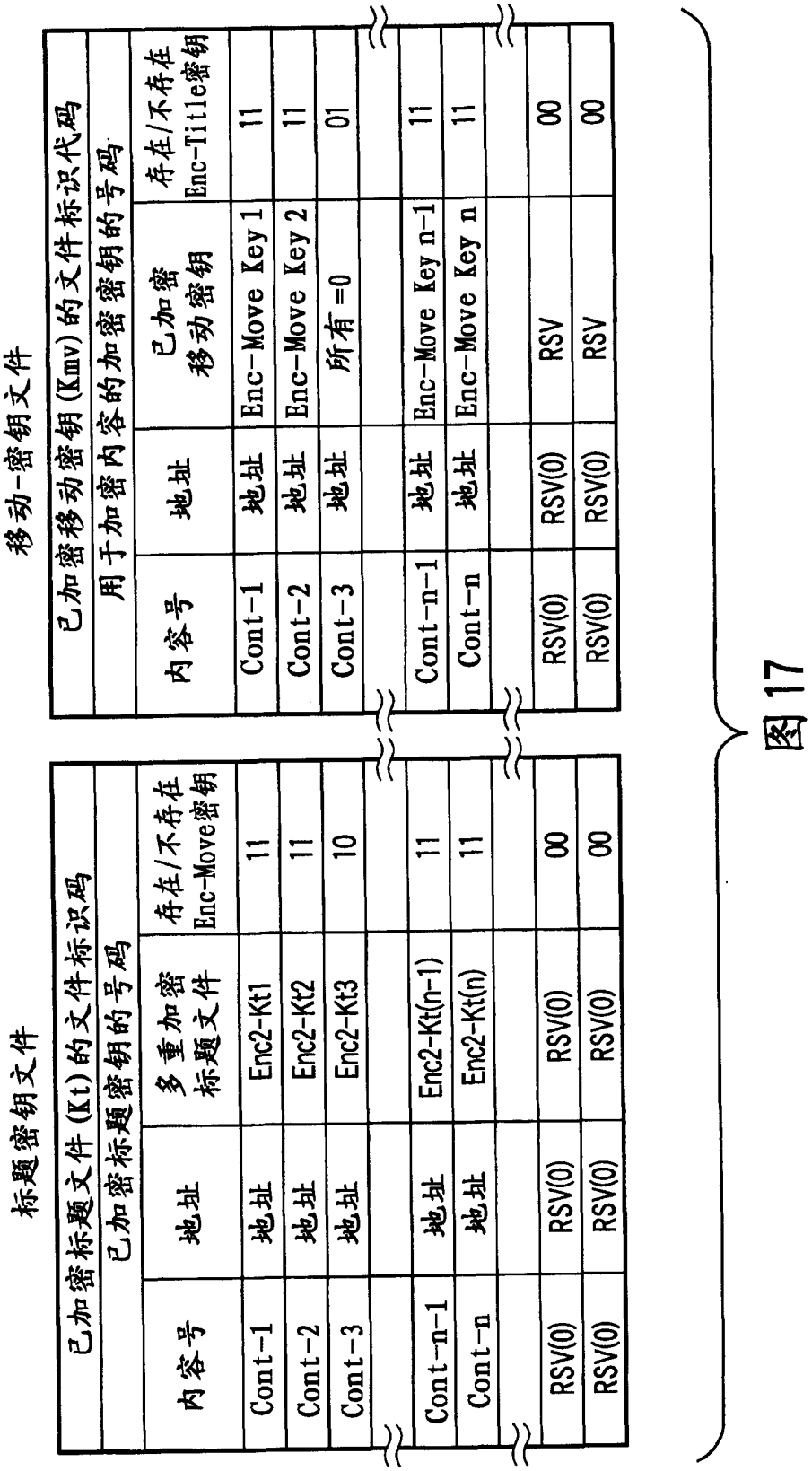

标题密钥文件
已加密标题文件(Kt)的文件标识码
已加密标题密钥的号码
内容号
地址
多重加密标题文件
存在/不存在Enc-Move密钥
Cont-1
地址
Enc2-Kt1
11
Cont-2
地址
Enc2-Kt2
11
Cont-3
地址
Enc2-Kt3
10
Cont-n-1
地址
Enc2-Kt(n-1)
11
Cont-n
地址
Enc2-Kt(n)
11
RSV(0)
RSV(0)
00
RSV(0)
RSV(0)
00
移动-密钥文件
已加密移动密钥(Kmv)的文件标识代码
用于加密内容的加密密钥的号码
内容号
地址
已加密移动密钥
存在/不存在Enc-Title密钥
Cont-1
地址
Enc-Move Key 1
11
Cont-2
地址
Enc-Move Key 2
11
Cont-3
地址
所有=0
01
Cont-n-1
地址
Enc-Move Key n-1
11
Cont-n
地址
Enc-Move Key n
11
RSV(0)
RSV(0)
RSV
00
RSV(0)
RSV(0)
RSV
00

图17

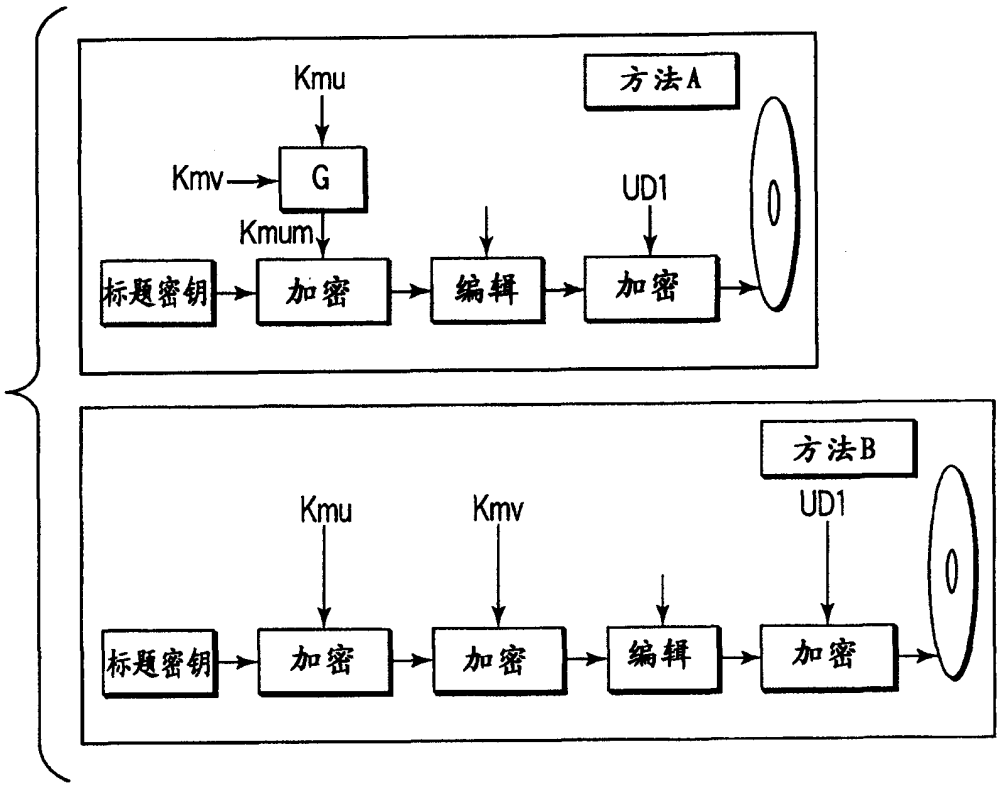

方法A
Kmu
Kmv
G
Kmum
UD1
标题密钥
加密
编辑
加密
方法B
Kmu
Kmv
UD1
标题密钥
加密
加密
编辑
加密

图 18