(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101030427 B
(45)授权公告日 2012.07.18

(21)申请号 200710084484.2
(22)申请日 2007.02.27
(30)优先权数据
2006-051285 2006.02.27 JP
(73)专利权人 株式会社东芝
地址 日本国东京都港区芝浦一丁目1番1号
(72)发明人 磯崎宏 佳藤拓
(74)专利代理机构 上海市华诚律师事务所 31210
代理人 徐申民
(51)Int.Cl.
G11B 20/10(2006.01)
G06F 21/00(2006.01)
(56)对比文件
US 2005/0154608 A1,2005.07.14,
CN 1655131 A,2005.08.17,
US 2005/0038997 A1,2005.02.17,
CN 1396568 A,2003.02.12,
审查员 段瑞玲

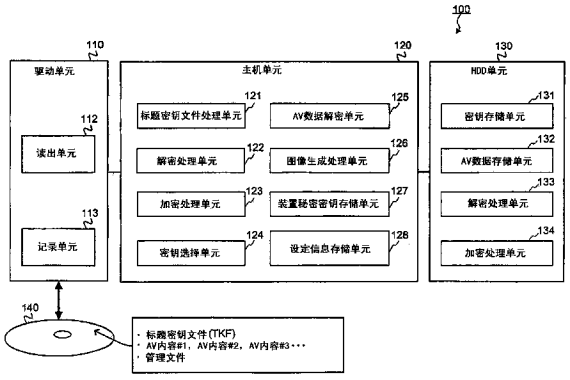
权利要求书 2 页 说明书 16 页 附图 14 页

(54)发明名称

用于记录内容的设备和方法

(57)摘要

内容记录设备包括当用户生成作为从标题内容得到的数据的附属数据时从记录在记录介质上的多种信息选择用于对附属数据进行加密处理的加密密钥的密钥选择单元，其中记录介质在其上记录用于加密作为节目内容的标题内容的标题密钥和包括用标题密钥加密的标题内容的内容数据。内容记录设备也包括用所选择的加密密钥对附属数据进行加密处理的加密处理单元；和在记录介质中记录对其进行加密处理的附属数据和所选择的加密密钥的记录单元。



CN 101030427 B

1. 一种内容记录设备，其特征在于，该内容记录设备包括：

当所述设备生成为从标题内容得到的数据的附属数据时，从记录在记录介质上的信息选择用于对附属数据进行加密处理的加密密钥的密钥选择单元，其中所述记录介质在其上记录用于加密所述标题内容的标题密钥和包括用所述标题密钥加密的所述标题内容的内容数据；

用所选择的加密密钥对所述附属数据进行加密处理的加密处理单元；和

在所述记录介质中记录对其进行加密处理的所述附属数据以及所选择的加密密钥的记录单元；其中

所述内容数据还包括表示存在或不存在对所述标题内容的复制限制的复制控制信息，以及

所述密钥选择单元基于从其得到所述附属数据的所述标题内容的所述复制控制信息选择所述加密密钥。

2. 如权利要求 1 所述的设备，其特征在于，该设备还包括判断由所述标题密钥加密并且包括所述附属数据的所述标题内容的复制控制信息的判断单元，

其中，当所述复制控制信息表示复制禁止时，所述密钥选择单元选择作为对应于包括所述附属数据的所述标题内容的所述标题密钥的加密密钥，

所述加密处理单元用所选择的标题密钥对所述附属数据进行加密处理，以及

所述记录单元在所述记录介质中记录由所述加密处理单元对其进行加密处理的所述附属数据以及所选择的标题密钥。

3. 如权利要求 2 所述的设备，其特征在于，当所述复制控制信息表示“不能复制”或“不能再复制”时，所述密钥选择单元选择作为对应于包括附属数据的标题内容的标题密钥的加密密钥。

4. 如权利要求 2 所述的设备，其特征在于，当所述标题内容基于所述复制控制信息的判断被判断为明码文本时，所述加密处理单元不对附属数据进行加密处理，以及

当所述标题内容基于所述复制控制信息的判断被判断为明码文本时，所述记录单元记录未加密的附属数据。

5. 如权利要求 4 所述的设备，其特征在于，当所述复制控制信息表示“自由复制”时，所述加密处理单元不对附属数据进行加密处理，以及

当所述复制控制信息表示“自由复制”时，所述记录单元记录未加密的附属数据。

6. 如权利要求 2 所述的设备，其特征在于，多个标题内容，寄存分别对应于所述多个标题内容的多个标题密钥的标题密钥文件，和寄存用于加密所述附属数据的标题密钥的附属数据标题密钥文件被进一步记录在记录介质上，以及

所述记录单元通过在所述附属数据标题密钥文件中寄存所选择的标题密钥而更新所述附属数据标题密钥文件。

7. 如权利要求 1 所述的设备，其特征在于，所述密钥选择单元基于包括所述附属数据的所述标题内容的所述复制控制信息新生成用于对所述附属数据进行加密处理的加密密钥，

所述加密处理单元用所述新生成的加密密钥对所述附属数据进行加密处理，以及

所述记录单元在所述记录介质中记录对其进行加密处理的附属数据以及所生成的加

密密钥。

8. 如权利要求 7 所述的设备，其特征在于，当包括所述附属数据的所述标题内容被加密，并且同时所述标题内容的复制控制信息表示复制被允许时，所述密钥选择单元新生成用于对附属数据进行加密处理的加密密钥。

9. 如权利要求 8 所述的设备，其特征在于，当包括所述附属数据的所述标题内容被加密，并且同时所述标题内容的复制控制信息表示“加密无断言”或“复制一次”时，所述密钥选择单元新生成用于对所述附属数据进行加密处理的加密密钥。

10. 如权利要求 8 所述的设备，其特征在于，多个标题内容，以及寄存分别对应于所述多个标题内容的多个标题密钥的标题密钥文件被进一步记录在所述记录介质上，以及

所述记录单元额外地记录新生成的加密密钥，作为所述标题密钥文件中的标题密钥。

11. 如权利要求 8 所述的设备，其特征在于，该设备还包括存储表示用作所述加密密钥的密钥的类型的设定信息的设定信息存储单元，其中

当所述设定信息表示从其得到所述附属数据的所述标题内容的所述标题密钥的使用时，所述密钥选择单元用对应于从其得出所述附属数据的所述标题内容的所述标题密钥加密所述附属数据。

12. 如权利要求 11 所述的设备，其特征在于，当所述设定信息表示从其得出附属数据的标题内容的标题密钥未被使用时，所述密钥选择单元生成新加密密钥，以用新生成的加密密钥对所述附属数据进行加密处理。

13. 如权利要求 8 所述的设备，其特征在于，多个标题内容，寄存分别对应于所述多个标题内容和所述附属数据的所述多个标题密钥的标题密钥文件，以及寄存用于加密所述附属数据的所述多个标题密钥的附属数据标题密钥文件被进一步记录在记录介质上，以及

所述记录单元额外地记录新生成的加密密钥，作为附属数据标题密钥文件中的标题密钥。

14. 如权利要求 1 所述的设备，其特征在于，所述记录单元在所述记录介质中作为单个文件记录由所述加密处理单元对其进行加密处理的所述附属数据和关于所选择的加密密钥的密钥信息。

15. 一种内容记录方法，其特征在于，该方法包括：

当生成为从标题内容得到的数据的附属数据时，从记录在记录介质上的信息选择用于对所述附属数据进行加密处理的加密密钥，其中所述记录介质在其上记录用于加密所述标题内容的标题密钥和包括由所述标题密钥加密的所述标题内容的内容数据；

用所选择的加密密钥对所述附属数据进行加密处理；和

在所述记录介质中记录对其进行加密处理的所述附属数据和所选择的加密密钥；其中

所述内容数据还包括表示存在或不存在对所述标题内容的复制限制的复制控制信息，以及

所述选择包括基于从得到所述附属数据的所述标题内容的所述复制控制信息选择所述加密密钥。

用于记录内容的设备和方法

技术领域

[0001] 本发明涉及用于在记录介质中记录附属数据的内容记录设备和方法。附属数据是作为节目内容的标题内容的一部分的数据。

背景技术

[0002] 常规上，例如，如在高级访问内容系统 (Advanced Access Content System，AACS) 可记录视频书修订版 (Recordable Video Book Revision)0.90 以及用于可记录介质的内容保护 (Content Protection for Recordable Media，CPRM) 的文件中所公开的，为了防止记录在诸如 DVD 的记录介质上的内容的非法复制，已知有一种技术，其中使用对于每一个标题内容都不同的标题密钥在作为程序的视频或音频内容的多个标题内容中的每一个之上进行加密处理，并且经加密的标题内容被记录在 DVD 介质上。

[0003] 在常规技术中，使用在诸如用于及时地记录并播放内容的 DVD 记录器的各种播放设备中给予的装置密钥加密多个标题密钥中的每一个，并且经加密的标题密钥被寄存在标题密钥文件中并记录在 DVD 介质上。当播放标题内容时，使用用于回放的记录和回放设备的装置密钥解密寄存在标题密钥文件中的经加密的标题密钥，并且标题内容被利用经解密的标题密钥解密以便播放标题内容。

[0004] 当一部分标题内容在可再写性 DVD 介质中被删除时，标题密钥文件也被更新。具体地说，标题密钥文件一旦被解密，使用装置密钥再次加密标题密钥文件，在该标题密钥文件中对应于标题内容的标题密钥从 DVD 介质上删除，并且标题密钥文件被记录在 DVD 介质上。所以，对应于被删除的标题内容的标题密钥能被预先复制以防止不法播放利用标题密钥删除的标题内容的攻击。

[0005] 以上常规技术是有效的技术，其中从外界通过广播输入的内容受到保护并且记录在诸如 DVD 介质的记录介质上以防止该内容的非授权使用。

[0006] 然而，常规方法保护由记录和播放设备新生成的内容（以下称“附属数据”）并不充分。附属数据源自 AV 内容，其中包括视频数据和音频数据的内容通过诸如 MPEG2 或 H.264 的编码方法被压缩。

[0007] 例如，附属数据为诸如被用于菜单屏幕的小型图像或音频文件的数据。附属数据的实 例也包括具有用诸如 JPEG 或 GIF 的图像压缩格式压缩的图像数据和用诸如 LPCM 或 MP3 的声频压缩格式数字化的音频数据的数据。附属数据为以不同于 AV 内容的格式记录在 DVD 介质上的图像和音频内容。为了生成附属数据，例如，版权受到保护的 AV 内容用标题密钥加密，一个场景被作为图像文件从 AV 内容提取，图像文件被转换为图像数据以便形成文件，图像数据文件被记录在 DVD 介质上，并且从图像数据文件形成小型图像。所以，表明标题内容目录的菜单屏幕被生。

[0008] 常规上，附属数据的使用限于小型图像等，并且附属数据被作为文件输出，同时附属数据的分辨率被压制成低于成为附属数据生成源的 AV 内容的分辨率。所以，使用受到限制并且对于版权已有一些非常严重的问题。

[0009] 然而，在附属数据被用于菜单屏幕的背景图像的情况下，考虑到当在明码文本中形成时附属数据被记录在DVD介质上。在这种情况下，非授权用户可能将附属数据从DVD介质复制到诸如硬盘的另一个记录介质上，或者非授权用户可能超出美国版权法107节中的公平使用或者日本版权法30节中的私人使用的范围之外通过因特网不法散布附属数据。附属数据是AV内容的一部分，因为附属数据从AV内容生成。结果，虽然AV内容受到保护，但当附属数据被无保护地散布时，AV内容仍未被保护。

[0010] 发明内容

[0011] 根据本发明的一个方面，内容记录设备包括当用户生成为从标题内容得到的数据的附属数据时，从记录在记录介质上的信息选择用于对附属数据进行加密处理的加密密钥的密钥选择单元，其中记录介质在其上记录用于加密作为节目内容的标题内容的标题密钥和包括用标题密钥加密的标题内容的内容数据；用所选择的加密密钥对附属数据进行加密处理的加密处理单元；和在记录介质中记录对其进行加密处理的附属数据以及所选择的加密密钥的记录单元。

[0012] 根据本发明的另一方面，内容记录方法包括当用户生成为从标题内容得到的数据的附属数据时，从记录在记录介质上的信息选择用于对附属数据进行加密处理的加密密钥，其中记录介质在其上记录用于加密作为节目内容的标题内容的标题密钥以及包括由标题密钥加密的标题内容的内容数据；用所选择的加密密钥对附属数据进行加密处理；和在记录介质中记录对其进行加密处理的附属数据和所选择的加密密钥。

[0013] 附图说明

[0014] 图1是显示根据第一实施例的DVD记录器的功能结构的方框图；

[0015] 图2是显示AV内容，标题密钥文件和管理文件的数据结构的示意图；

[0016] 图3是显示根据第一实施例的附属数据生成处理的流程图；

[0017] 图4是显示经压缩的文件的数据结构的示意图；

[0018] 图5是显示标题密钥选择的解释性示意图；

[0019] 图6A是显示根据第一实施例的密钥选择处理的流程图；

[0020] 图6B是显示根据第一实施例的修改例的密钥选择处理的流程图；

[0021] 图7是显示多个密钥号码被设定到AV内容#1的状态的示意图；

[0022] 图8是显示根据第一实施例的标题密钥移动处理的流程图；

[0023] 图9是显示根据第一实施例的附属数据回放处理的流程图；

[0024] 图10是显示根据第一实施例的AV内容回放处理的流程图；

[0025] 图11是显示根据第二实施例的DVD记录器的功能结构的方框图；

[0026] 图12是显示根据第二实施例的密钥选择处理的流程图；以及

[0027] 图13是显示根据第二实施例的修改例的密钥选择处理的流程图。

具体实施方式

[0028] 内容记录设备和内容记录方法的较佳实施例将参照附图详细说明。

[0029] 首先将说明第一实施例。

[0030] 图1是显示根据第一实施例的内容记录和播放设备100的配置的方框图。在可记录的DVD和HD DVD介质（以下称“DVD介质140”）上进行记录和回放的DVD/HD DVD记录

器能被引用为内容记录和播放设备 100 的实例。如图 1 所示，第一实施例的内容记录和播放设备 100（以下称“DVD 记录器 100”）包括驱动单元 110，主机单元 120 和 HDD 单元 130。驱动单元 110 在 DVD 介质 140 中记录数据，以及从 DVD 介质 140 读出数据。主机单元 120 进行标题内容和标题密钥的加密处理和解密处理，并且主机单元 120 还进行从经解密的标题内容生成后面提及的附属数据的处理。标题内容被存储在 HDD 单元 130 中。驱动单元 110 和主机单元 120 以及主机单元 120 和 HDD 单元 130 分别与通用总线或专用总线连接。

[0031] 虽然第一实施例中 DVD 记录器 100 被配置成包括 HDD 单元 130，但 DVD 记录器 100 可以被配置成不包括 HDD 单元 130。

[0032] 如图 1 所示，标题密钥文件 (TKF)，多个 AV 内容 (AV 内容 #1，AV 内容 #2 和 AV 内容 #3)，以及管理文件被作为文件分别记录在 DVD 介质 140 上。在第一实施例中，标题密钥文件能被重写在其中的可再写性介质被用作 DVD 介质 140 的实例。

[0033] 按照 HD DVD 视频记录技术规格的 DVD 介质是用于第一实施例的 DVD 记录器 100 的 DVD 介质 140 的目标格式。然而，DVD 介质 140 并不总是限于按照 HD DVD 视频记录技术规格的 DVD 介质。

[0034] 记录在 DVD 介质 140 上的各种数据将说明如下。图 2 示意性地显示记录在 DVD 介质 140 上的 AV 内容，标题密钥文件和管理文件的数据结构。

[0035] AV 内容是在各个程序中形成的。如图 2 所示，AV 内容由一组包括一组头部和经加密的标题内容的多数据包形成。

[0036] 经加密的标题内容是其中标题内容由标题密钥和后面提及的包括在标题内容内的复制控制信息加密的内容。标题密钥由来自许可组织的被分配在各个 DVD 记录器 100 中的装置密钥加密，并且标题密钥以标题密钥文件的形式被记录。如在本文中使用的，标题内容将意指程序视频或音频内容的单元。例如，一个影片的内容成为一个标题内容。标题内容包括视频数据和音频数据，并且标题内容是通过诸如 MPEG-2 或 H.264 的编码方法压缩的数据。

[0037] 标题密钥是用以对标题内容加密的密钥。在第一实施例中，不同的标题密钥被用于在每个情况下的标题内容。然而，本发明不局限于第一实施例，多个标题内容可以由同一个标题密钥加密。

[0038] 如图 2 所示，头部包括密钥号和复制控制信息。密钥号是表明从经加密的标题密钥的标题密钥文件的头部开始的记录位置的指针。标题密钥被加密以形成经加密的标题密钥，并且当标题内容被加密时使用经加密的标题密钥。例如，在图 2 中，假定 AV 内容 #1 的密钥号是 3，对应于 AV 内容 #1 的标题内容的经加密的标题密钥成为位于从标题密钥文件的头部开始的第三记录的经加密的标题密钥 3。

[0039] 当标题内容是明码文本 (plaintext) 时，明码文本的标题内容被包括在 AV 内容中而不是在经加密的标题内容中。在这种情况下，标题密钥不进行加密，并且密钥号被设定为 0。也就是说，基于 AV 内容的密钥号字段被设定为 0 还是非 0 数，可以判定标题内容是明码文本还是经加密的标题内容。

[0040] 在第一实施例中，当标题内容是明码文本时密钥号被设定为 0。本发明不局限于第一实施例，密钥号可以被设定为不对应于从标题密钥文件的头部开始的记录位置的任意数。

[0041] 复制控制信息是表明对标题内容的复制的限制的信息。“自由复制”(“Copy Free”),“不能复制”(“Copy Never”),“不能再复制”(“No More Copies”),“复制一次”(“Copy One Generation”),“EPN”等被设定在复制控制信息中。

[0042] “自由复制”表明标题内容能无限制地被复制,以及“不能复制”表明不能复制标题内容。“复制一次”表明仅能在一个生成中复制标题内容。“不能再复制”表明因为“复制一次”的标题内容已经被复制一次并且第一生成记录不能被再次复制因此不能在复制控制信息中复制标题内容的状态,也就是,“不能再复制”表明复制被禁止。“EPN”(EncryptionPlus Non-assertion,加密无断言)表明虽然版权通过对标题内容进行加密处理受到保护但在进行复制中复制数和生成不受限制。在“自由复制”情况下标题内容不被加密,并且在除了“自由复制”外的各种状态中标题内容都被加密。复制控制信息被用来加密标题内容,以致复制控制信息的非法变化能被防止。

[0043] 标题密钥文件是其中寄存多个经加密的标题密钥的文件。在经加密的标题密钥中,对应于多个标题内容的各个标题密钥由装置密钥加密。

[0044] 管理文件是管理对应于 AV 内容的经加密的标题内容的标题密钥的文件。如图 2 所示,表明从对应的经加密的标题密钥的标题密钥文件的头部开始的记录位置的密钥号被寄存在每一个 AV 内容中。例如,在图 2 中,因为 AV 内容 #1 的密钥号是 2,对应于 AV 内容 #1 的标题内容的经加密的标题密钥成为位于从标题密钥文件的头部开始的第二记录的经加密的标题密钥 2。

[0045] 类似于头部的密钥号,当标题内容是明码文本时,密钥号在管理文件的对应的 AV 内容中被设定为 0。所以,基于管理文件的密钥号字段是被设定为 0 还是非 0 数,可以判定包括在 AV 内容内的标题内容是明码文本还是经加密的标题内容。

[0046] 在第一实施例中,由管理文件和 AV 内容的头部的密钥号两者指定对应于 AV 内容的经加密的标题内容的经加密的标题密钥。然而,对应于经加密的标题内容的经加密的标题密钥可由管理文件或 AV 内容的头部的密钥号指定。

[0047] 回到图 1,驱动单元 110 包括读出单元 112 和记录单元 113。读出单元 112 直接从 DVD 介质 140 读取数据,并且记录单元 113 直接在 DVD 介质 140 中记录数据。

[0048] 如图 1 所示,主机单元 120 包括标题密钥文件处理单元 121,解密处理单元 122,加密处理单元 123,密钥选择单元 124,AV 数据解码单元 125,图像生成处理单元 126,装置秘密密钥存储单元 127 和设定信息存储单元 128。虽然第一实施例的主机单元 120 包括设定信息存储单元 128,但主机单元 120 可以被配置成不包括设定信息存储单元 128。

[0049] 密钥选择单元 124 从寄存在标题密钥文件中的标题密钥中选择适当的标题密钥,并且密钥选择单元 124 选择用于解密标题内容的标题密钥。密钥选择单元 124 选择在内容记录处理中用于加密附属数据的标题密钥。在内容记录处理中,当关于标题内容的复制控制信息表明能带有类似“复制一次”和“EPN”的限制复制标题内容时,密钥选择单元 124 生成用以加密附属数据的标题密钥。

[0050] 在内容回放处理中,密钥选择单元 124 从寄存在标题密钥文件中的经加密的标题密钥中选择适当的经加密的标题密钥,并且密钥选择单元 124 选择解密经加密的标题内容或附属数据的标题密钥。

[0051] 加密处理单元 123 使用由密钥选择单元 124 选择的标题密钥加密标题内容。加密

处理单元 123 使用由密钥选择单元 124 选择的标题密钥或由密钥选择单元 124 生成的标题密钥加密附属数据。

[0052] 解密处理单元 122 使用由密钥选择单元 124 选择的标题密钥解密经加密的标题内容和经加密的附属数据。

[0053] 标题密钥文件处理单元 121 解密被加密并存储在标题密钥文件中的标题密钥（经加密的标题密钥），并且标题密钥文件处理单元 121 加密标题密钥以在标题密钥文件中寄存标题密钥。

[0054] AV 数据解码单元 125 解码被压缩的标题内容以及附属数据，以便将标题内容和附属数据转换为具有非压缩格式的数据。图像生成处理单元 126 从具有由用户说明或记录器设定的非压缩格式的标题内容中检测图像数据形式中必需的部分，并且图像生成处理单元 126 通过提取图像数据生成附属数据以便将图像数据转换为图像压缩格式。

[0055] 如在本文中使用的，附属数据应该意指通过从标题内容取得数据生成的数据。附属数据的实例包括诸如小型图像和音频文件的从标题内容生成并且用于菜单屏幕的数据。附属数据的实例还包括具有用诸如 JPEG 或 GIF 的图像压缩格式压缩的图像数据和用诸如 LPCM 和 MP3 的音频压缩格式数字化的音频数据的数据。附属数据是能以不同于标题内容的格式记录在 DVD 介质 140 上的内容。在下面的说明中，图像文件通过实例的方式被用作附属数据。然而，即使图像文件以外的其他文件被用作附属数据，本发明也可以被应用。

[0056] 装置秘密密钥存储单元 127 是诸如存储器的记录介质，其中装置密钥被存储并保持机密。装置密钥被用来加密和解密标题密钥，该装置密钥由许可组织分配给 DVD 记录器 100 的制造商。

[0057] 设定信息存储单元 128 是设定信息被存储在其中的诸如存储器的记录介质。设定信息表明用以加密附属数据的密钥的类型。具体地说，设定信息是用于表明附属数据是用与对应于从其得出附属数据的标题内容的标题密钥相同的密钥加密还是用新生成的标题密钥加密的数据。

[0058] 如图 1 所示，HDD 单元 130 包括密钥存储单元 131，AV 数据存储单元 132，解密处理单元 133 和加密处理单元 134。

[0059] 密钥存储单元 131 是诸如硬盘驱动器 (HDD) 或存储器的记录介质，其中存储用于加 密标题内容的标题密钥。AV 数据存储单元 132 是诸如 HDD 的记录介质，其中存储从 DVD 介质 140 复制或移动的经加密的标题内容。

[0060] 解密处理单元 133 使用存储在密钥存储单元 131 中的标题密钥解密经加密的标题内容和附属数据。加密处理单元 134 使用存储在密钥存储单元 131 中的标题密钥加密存储在 AV 数据存储单元 132 中的标题内容和附属数据。

[0061] 第一实施例的 DVD 记录器 100 采用以上配置以生成附属数据。然而，本发明不局限于第一实施例的 DVD 记录器 100，DVD 记录器 100 可以包括具有另一功能的处理单元。

[0062] 然后，将说明由第一实施例的 DVD 记录器 100 进行的附属数据生成处理。图 3 是显示由第一实施例的 DVD 记录器 100 进行的附属数据生成处理的流程图。

[0063] 具体地说，附属数据生成处理是从记录在 DVD 介质 140 上的 AV 内容的标题内容生成用于菜单屏幕的小型图像或背景图像的处理。

[0064] 在这一点上，在 DVD 介质 140 的初始状态中，AV 内容，标题密钥文件和管理文件被

作为文件记录在介质中。有时，包括经加密的标题内容的 AV 内容以及包括未经加密的标题内容的 AV 内容被混合在一个 DVD 介质 140 中。在第一实施例中，假定包括经加密的标题内容的 AV 内容以及包括未经加密的标题内容的 AV 内容也被混合。也就是说，AV 内容 #1 和 AV 内容 #2 由标题密钥加密，而 AV 内容 #3 的标题内容是明码文本。

[0065] 主机单元 120 选择包括作为附属数据提取源的标题内容的 AV 内容（步骤 S301）。

[0066] 然后，密钥选择单元 124 参考记录在 DVD 介质 140 上的管理文件，以检查标题内容是否被加密（步骤 S302）。具体地说，如上所述，判定对应于成为管理文件中的提取源的 AV 内容的密钥号是否为 0。

[0067] 当标题内容为明码文本时（步骤 S302 中为否），AV 数据解码单元 125 解码 AV 内容的标题内容（步骤 S312）。在步骤 S313 中，当由用户说明或装置设定分配所要求的范围时，图像生成处理单元 126 提取静止图像形式的图像数据。在预定的回放时间中从经解码的标题内容生成图像数据。然后，图像生成处理单元 126 将所提取的图像数据转换为图像压缩格式以便生成压缩图像。压缩图像成为附属数据。

[0068] 另一方面，当标题内容被加密时（S302 步骤中为是），标题密钥文件处理单元 121 参考管理文件以便从标题密钥文件获得经加密的标题密钥。

[0069] 接下来，标题密钥文件处理单元 121 使用存储在装置秘密密钥存储单元 127 中的装置密钥解密所获得的经加密的标题密钥（步骤 S304）。

[0070] 然后，解密处理单元 122 使用被加密以变为明码文本的标题密钥和包括在 AV 内容内的复制控制信息解密经加密的标题内容（步骤 S305）。在这一点上，在加密中，使用复制控制信息的一部分（例如，若干位）。

[0071] 解密处理单元 122 可以被配置成，在标题内容解密处理中通过比较在管理文件中分配的经加密的标题密钥与包括在 AV 内容的头部内的密钥号字段的值而作出在管理文件中分配的经加密的标题密钥是否对应于用于加密实际标题内容的密钥的判定。

[0072] AV 数据解码单元 125 解码已经变为明码文本的标题内容（步骤 S306）。在步骤 S307 中，当由用户说明或装置设定分配所要求的范围时，图像生成处理单元 126 提取静止图像形式的图像数据。在预定的回放时间中从经解码的标题内容生成图像数据。然后，图像生成处理单元 126 将所提取的图像数据转换为图像压缩格式以便生成压缩图像。压缩图像成为附属数据。

[0073] 密钥选择单元 124 从记录在 DVD 介质 140 上的标题密钥文件中选择用以加密附属数据的标题密钥，或密钥选择单元 124 进行新生成用以加密附属数据的标题密钥的密钥选择处理（步骤 S308）。详细的密钥选择处理将说明于后。

[0074] 加密处理单元 123 通过使用在步骤 S308 中选择或生成的标题密钥加密作为附属数据的压缩图像（步骤 S309）。

[0075] 记录单元 113 通过将经加密的附属数据与文件 ID，用于加密的标题密钥的密钥号和文件尺寸一起形成在一个单个文件中而封装经加密的压缩图像即经加密的附属数据（步骤 S310），并且记录单元 113 将作为经封装的压缩图像的经加密的附属数据以文件的形式记录在 DVD 介质 140 中（步骤 S311）。

[0076] 图 4 显示第一实施例的经封装的文件的数据结构。经封装的文件包括文件 ID，用于加密的标题密钥的密钥号，文件尺寸和经加密的附属数据。表明该文件具有经加密的附

属数据的预定值被设置在文件 ID 中。密钥号是表明在标题密钥文件中从用于加密的标题密钥的标题密钥文件的头部开始的记录位置的指针。例如，在密钥号字段的值是 5 的情况下，表明使用记录在标题密钥文件中的第五记录位置的标题密钥进行加密处理。在加密处理之前明码文本附属数据（压缩图像）的尺寸被设定在文件尺寸中。除了以上各种信息之外，经封装的文件的数据结构还可以包括复制控制信息。在这种情况下，附属数据可以通过使用标题密钥和复制控制信息加密。

[0077] 在经封装的文件中，在文件扩展名未被封装的明码文本的情况下，文件扩展名可以用不同于表明特定格式的扩展名替换，或者除了带有不同扩展名的文件名之外还可以添加另一扩展名。例如，假定文件名是“file A”，经封装的文件的扩展名是“aaa”，并且明码文本的扩展名是“jpg”，则经封装的文件的名称可被设定为“file A.aaa”并且名称可以被设定为“file A.jpg.aaa”。

[0078] 以下将说明步骤 S308 中的密钥选择处理。在第一实施例的 DVD 记录器 100 中，当对作为附属数据的压缩图像进行加密处理时，用于加密附属数据的标题密钥基于 AV 内容的复制控制信息选择。具体地说，当从其得出附属数据的标题内容的复制控制信息是诸如“不能复制”和“不能再复制”的表明复制禁止的信息时，对应于从其得出附属数据的标题内容（包括附属数据）的标题密钥，即，用于加密标题内容的标题密钥被选为用以对附属数据进行加密处理的标题密钥。

[0079] 图 5 是用于说明用以对附属数据进行加密处理的标题密钥的选择的解释性示意图。

[0080] 假定 AV 内容，标题密钥和管理文件以图 5 所示状态被记录在 DVD 介质 140 上。也就是说，AV 内容 #1，AV 内容 #2 和 AV 内容 #3 被记录，AV 内容 #1 的标题内容由记录在标题密钥文件的第二记录位置上的经加密的标题密钥 2 加密，并且内容的状态被设定为“不能再复制”。假定 AV 内容 #2 由记录在标题密钥文件的第一记录位置上的经加密的标题密钥 1 加密，并且内容的状态被设定为“EPN”。也假定 AV 内容 #3 是明码文本。

[0081] 如图 5 所示，在第一实施例的密钥选择单元 124 中，从其中复制控制信息表明诸如“不能再复制”的复制限制的 AV 内容 #1 的标题内容产生的附属数据由在加密 AV 内容 #1 的标题内容的处理中使用的经加密的标题密钥 2 加密。

[0082] 另一方面，如图 5 所示，在第一实施例的密钥选择单元 124 中，在加密从其中复制控制信息表明诸如“EPN”的没有复制限制或复制控制信息表明复制可以带有限制地进行的 AV 内容 #2 的标题内容生成的附属数据的过程中，对应于密钥号 4 的标题密钥被新生成并且独立于 AV 内容 #2 的标题密钥被寄存在标题密钥文件中，并且附属数据由新生成的标题密钥加密。

[0083] 在图 5 所示的状态中，因为仅三个经加密的标题密钥被寄存在标题密钥文件中，因此在作为标题密钥文件的空记录的第四记录位置中新生成的标题密钥通过利用装置密钥加密标题密钥文件被记录。此外，附属数据由新生成的标题密钥加密，空字段号 (4) 被设定为密钥号字段，并且附属数据被封装在单个文件中并记录在 DVD 介质 140 上。

[0084] 由密钥选择单元 124 进行的特定密钥选择处理将被说明如下。图 6A 是显示由第一实施例的密钥选择单元 124 进行的密钥选择处理的流程图。

[0085] 密钥选择单元 124 检查关于包括作为附属数据提取源的标题内容的 AV 内容的复

制控制信息的状态（步骤 S601）。当复制控制信息表明诸如“不能再复制”或“不能复制”的复制限制时，密钥选择单元 124 从标题密钥文件选择对应于作为附属数据提取源的标题内容的标题密钥（经加密的标题密钥）（步骤 S602）。在这一点上，如图 5 所示，在选择标题密钥的过程中参考对应于包括寄存在 DVD 介质 140 的管理文件中的标题内容的 AV 内 容的密钥号。当复制控制信息表明“自由复制”时，附属数据被记录在 DVD 介质 140 上同时不通过图 3 中的步骤 S302（否），S312，S313，S310 和 S311 的处理进行加密。即使在密钥选择处理的步骤 S601 中判定复制控制信息表明“自由复制”，标题密钥也未被选择，并且密钥选择处理在不加密附属数据的情况下结束。所以，附属数据通过图 3 中的步骤 S309，S310 和 S311 的处理被记录在 DVD 介质 140 上，同时保留在明码文本中。

[0086] 另一方面，在步骤 S601 中，当复制控制信息表明诸如“EPN”或“复制一次”的没有复制限制，或当复制控制信息表明复制可带有限制地进行时，密钥选择单元 124 参考存储在设定信息存储单元 128 中的设定信息（步骤 S603），并且密钥选择单元 124 判定与对应于作为附属数据提取源的标题内容的标题密钥相同的密钥是否被用作用于加密附属数据的密钥（步骤 S604）。

[0087] 当在设定信息中设定与对应于作为附属数据提取源的标题内容的标题密钥相同的密钥被用作用于加密附属数据的密钥时（步骤 S604 中为是），密钥选择单元 124 选择对应于作为附属数据提取源的标题内容的标题密钥（经加密的标题密钥）。

[0088] 另一方面，在步骤 S604 中，当在设定信息中设定与对应于作为附属数据提取源的标题内容的标题密钥相同的密钥未被用作用于加密附属数据的密钥时（步骤 S604 中为否），密钥选择单元 124 新生成标题密钥（步骤 S605）。标题密钥文件处理单元 121 搜索 DVD 介质 140 的标题密钥文件的空记录（步骤 S606）。然后，标题密钥文件处理单元 121 使用装置密钥加密新生成的标题密钥，并且记录单元 113 将经加密的新生成的标题密钥记录在标题密钥文件的空记录中，更新标题密钥文件（步骤 S607）。

[0089] 虽然第一实施例的主机单元 120 被配置成包括设定信息存储单元 128，但主机单元 120 可以被配置成不包括设定信息存储单元 128。在这种情况下，在步骤 S601 中，即使复制控制信息表明诸如“EPN”或“复制一次”的没有复制限制，或者即使复制控制信息表明复制可以带有限制地进行，与对应于作为附属数据提取源的标题内容的标题密钥相同的密钥也可以用作用于加密附属数据的密钥，象在“不能再复制”或“不能复制”的场合下一样。也就是说，当标题内容被加密时，不考虑复制控制信息，与对应于作为附属数据提取源的标题内容的标题密钥相同的密钥被用作用于加密附属数据的密钥。在这种情况下，不必进行步骤 S601 的判断复制控制信息的处理。

[0090] 或者，复制控制信息被判断，并且当复制控制信息表明诸如“EPN”或“复制一次”的没有复制限制或当复制控制信息表明复制可以带有限制地进行时可以新生成标题密钥以便加密附属数据。

[0091] 图 6B 是显示作为第一实施例的修改例的密钥选择处理的流程图。图 6B 显示当设定信 息存储单元不存在并且同时当进行对复制控制信息状态的判定时由密钥选择单元 124 进行的密钥选择处理。

[0092] 首先，密钥选择单元 124 检查关于包括附属数据提取源的标题内容的 AV 内容的复制控制信息的状态（步骤 S601）。当复制控制信息表明诸如“不能再复制”或“不能复制”的

复制限制时，进行与在图 6A 中说明的相同的处理（步骤 S602）。当复制控制信息表明“自由复制”时，附属数据被记录在 DVD 介质 140 上同时保留在明码文本中并且不通过图 3 中的步骤 S302（否），S312，S313，S310 和 S311 的处理加密。即使在密钥选择处理的步骤 S601 中判定复制控制信息表明“自由复制”，类似于图 6A 中的处理，标题密钥未被选择，密钥选择处理在不加密附属数据的情况下结束，并且附属数据被记录在 DVD 介质 140 上同时保留在明码文本中。

[0093] 另一方面，在步骤 S601 中，当复制控制信息表明诸如“EPN”或“复制一次”的没有复制限制，或当复制控制信息表明复制可以带有限制地进行时，密钥选择单元 124 新生成标题密钥（步骤 S608）。标题密钥文件处理单元 121 搜索 DVD 介质 140 的标题密钥文件的空记录（步骤 S609），并且由标题密钥文件处理单元 121 新生成的标题密钥由装置密钥加密。然后，记录单元 113 将经加密的新标题密钥记录在标题密钥文件的空记录中以便更新标题密钥文件（步骤 S610）。

[0094] 这样，在步骤 S309 中，附属数据（压缩图像）由以上述方式选择或生成的标题密钥加密，并且经加密的附属数据被记录在 DVD 介质 140 上。

[0095] 当在步骤 S602 中选择用于加密标题内容的标题密钥时参考对应于包括寄存在 DVD 介质 140 的管理文件中的标题内容的 AV 内容的密钥号。然而，本发明不局限于上述技术。也就是说，密钥选择单元 124 可以配置成通过参考在 AV 内容的头部的密钥号字段中设定的密钥号选择标题密钥。

[0096] 例如，作为编辑标题内容的结果，有时相关于 AV 内容 #1 设定多个密钥号码并且在图 7 中显示多个标题密钥。在图 7 中，因为在 AV 内容 #1 中数据包 #1 至数据包 #N 的密钥号码被设定为 2，AV 内容 #1 的代表性标题密钥是记录在标题密钥文件的第二记录上的经加密的标题密钥。然而，因为在 AV 内容 #1 中最后的数据包 #(N+1) 的密钥号被设定为 1，数据包 #(N+1) 由记录在标题密钥文件的第一记录上的标题密钥加密。所以，在从数据包 #(N+1) 提取附属数据的情况下，必要的是附属数据由记录在标题密钥文件的第一记录上的标题密钥加密。

[0097] 然而，因为在管理文件的各个 AV 内容中密钥号被单独地设置，加密利用不是数据包 #(N+1) 的附属数据的标题密钥的标题密钥进行，并且附属数据不能被保护。在这种情况下，通过利用在 AV 内容的头部设定的密钥号选择标题密钥以便加密附属数据，这样就使附属数据的内容得到适当保护。

[0098] 包括在记录在 DVD 介质 140 上的标题密钥文件内的标题密钥能被移到另一个记录介质。例如，在包括如同第一实施例的 DVD 记录器 100 的内置 HDD 单元的情况下，存储在 HDD 单元的 AV 数据存储单元 132 中的经加密的标题内容能通过将记录在 DVD 介质 140 上的标题密钥移动至 HDD 单元 130 而被播放。

[0099] 即使不同于第一实施例的 DVD 记录器 100，在 DVD 记录器 100 不包括 HDD 单元 130 的情况下，记录在 DVD 介质 140 上的标题密钥仍能被移到另一个 DVD 介质。

[0100] 记录在 DVD 介质 140 上的标题密钥向另一个记录介质的移动将被说明如下。由第一实施例的 DVD 记录器 100 进行的从 DVD 介质 140 向 HDD 单元 130 移动标题密钥文件中的标题密钥的处理将通过实例的方法说明。图 8 是显示由第一实施例的 DVD 记录器 100 进行的标题密钥移动处理的流程图。

[0101] 读出单元 112 从 DVD 介质 140 读取标题密钥文件（步骤 S801）。标题密钥文件处理单元 121 使用装置密钥解密所读取的标题密钥文件中的全部经加密的标题密钥（步骤 S802），并且标题密钥文件处理单元 121 在易失性存储器（未显示）的机密区域中记录全部经解密的标题密钥（步骤 S803）。存储在机密区域中的数据不能被从 DVD 记录器 100 外部读取。

[0102] 然后，标题密钥文件处理单元 121 将作为移动目标的标题密钥移动至不同于易失性存储器的机密区域的区域中（步骤 S804）。

[0103] 然后，标题密钥文件处理单元 121 使用装置密钥加密移动目标以外的剩余的标题密钥，并且标题密钥文件处理单元 121 从易失性存储器删除标题密钥（步骤 S805）。

[0104] 记录单元 113 在 DVD 介质 140 中记录包括经加密的标题密钥的标题密钥文件（步骤 S806）。所以，包括除了移动目标之外的全部标题密钥的经加密的标题密钥的标题密钥文件被记录在 DVD 介质 140 上。

[0105] 然后，标题密钥文件处理单元 121 将移动目标的标题密钥从易失性存储器的机密区域移动到 HDD 单元 130 的密钥存储单元 131，并且加密处理单元 134 加密所移动的标题密钥（步骤 S807），并且经加密的标题密钥被存储在密钥存储单元 131 中（步骤 S808）。在用于标题密钥移动处理的密钥的计算中，更可取的是唯一值被包括在 DVD 记录器 100 中。

[0106] 读出单元 112 从 DVD 介质 140 读取经加密的标题内容以便在 HDD 单元 130 的 AV 数据存储单元 132 中复制经加密的标题内容（步骤 S809）。在这一点上，经加密的标题内容未被解密，经加密的标题内容的复制在加密的状态中进行。

[0107] 在 DVD 介质中包括经加密的标题内容的 AV 内容可以被删除，或者 AV 内容可以被保留在 DVD 介质 140 中。

[0108] 标题密钥和由标题密钥加密的标题内容通过上述标题密钥移动处理被存储在结合到 DVD 记录器 100 中的 HDD 中，以致由移动目标的标题密钥加密的标题内容能没有 DVD 介质地被播放。当通过上述标题密钥移动处理从 DVD 介质 140 向 HDD 单元 130 移动标题密钥时经加密的标题内容被复制到 HDD 单元 130，以致被复制（移动）到 HDD 单元 130 的经加密的标题内容也能通过利用移动到 HDD 单元 130 的标题密钥解密经加密的标题内容而被播放，即使 DVD 介质 140 不存在也一样。

[0109] 为说明攻击情况，考虑从其中复制控制信息表明“不能再复制”的标题内容生成附属数据并且附属数据由不同于用于加密标题内容的标题密钥的标题密钥加密，与第一实施例的 DVD 记录器 100 不同。

[0110] 在初始状态中，如图 2 所示，在 DVD 介质 140 中不存在附属数据，在 DVD 介质 140 中存在包括标题内容的 AV 内容，并且经加密的标题密钥 1，经加密的标题密钥 2 和经加密的标题密钥 3 被寄存在标题密钥文件中。

[0111] 在这种情况下，诸如背景图像的附属数据从 AV 内容 #1 生成，标题密钥被新生成，并且新生成的标题密钥 4 被记录在标题密钥文件上。在这一点上，DVD 介质中的标题密钥文件具有已经寄存的经加密的标题密钥 1 至 3 以及新生成的经加密的标题密钥 4。

[0112] 接下来，考虑经加密的标题密钥 4 通过上面提及的标题密钥移动处理被移到 HDD 单元 130。在这种情况下，经加密的标题密钥 1，经加密的标题密钥 2 和经加密的标题密钥 3 被寄存在 DVD 介质 140 的标题密钥文件中。

[0113] 然后，附属数据从 AV 内容 #1 再次被生成，经加密的标题密钥 5 被新生成，并且经加密的标题密钥 5 被存储在标题密钥文件的第四记录中。在这一点上，DVD 介质 140 中的标题密钥文件具有经加密的标题密钥 1，经加密的标题密钥 2，经加密的标题密钥 3 和经加密的标题密钥 5 的四个标题密钥。

[0114] 当附属数据从其中复制控制信息表明“不能再复制”的 AV 内容 #1 被生成时，附属数据能利用新标题密钥 4 和标题密钥 5 复制。也就是说，当附属数据与新加密的标题密钥一起被存储在另一个记录介质中时，附属数据能利用在另一个记录介质中的新标题密钥 4 和 5 播放，同时也能利用对应于 DVD 介质的 AV 内容 #1 的标题密钥 1 播放。这意味着虽然作为附属数据提取源的 AV 内容 #1 的复制控制信息表明“不能再复制”，但一部分 AV 内容 #1 能被作为附属数据多次复制。所以，AV 内容以及附属数据的版权不能被保护。

[0115] 因为许多附属数据通过以上处理被复制，AV 内容的大部分能作为附属数据被复制。 在这种情况下，由“不能再复制”的复制控制信息保护的 AV 内容大体上被排除。

[0116] 在第一实施例的 DVD 记录器 100 中，当 AV 内容的复制控制信息表明诸如“不能复制”或“不能再复制”的复制限制时，附属数据由与对应于 AV 内容的标题内容的标题密钥相同的标题密钥加密。所以，附属数据的非法使用和非法复制被防止，并且标题内容的版权保护方面的实质性下降被防止。

[0117] 当附属数据由与对应于 AV 内容的标题内容的标题密钥相同的标题密钥加密时，必要的是作为提取源的标题内容的标题密钥被移到另一个记录介质上，以便向另一个记录介质复制和从该记录介质回放附属数据。在这一点上，因为在 DVD 介质上不存在对应于作为提取源的标题内容的标题密钥，作为 DVD 介质中的提取源的标题内容不能被播放。所以，即使附属数据被复制到另一个记录介质，由“不能复制”或“不能再复制”的复制控制信息保护的作为提取源的标题内容能受到保护。

[0118] 另一方面，即使仅附属数据不用任何标题密钥被复制到另一个记录介质，附属数据也不能被播放，因为用以加密附属数据的标题密钥与作为提取源的标题内容一起被记录在 DVD 介质上。

[0119] 这样，附属数据的非法使用和非法复制被防止，并且标题内容的版权保护方面实质性的下降被防止。

[0120] 在第一实施例中，其中标题密钥文件能被重写的可再写性介质用实例的方法被作为 DVD 介质 140 进行说明。另一方面，在其中数据能被一次写入的一次写介质中，标题密钥文件不能被更新。所以，因为新标题密钥不能被生成，附属数据能由独立于标题内容的复制控制信息存在于标题密钥文件中的任何标题密钥加密。显然，附属数据可以由与用于加密标题内容的标题密钥相同的标题密钥加密。

[0121] 在第一实施例中，作为附属数据的图像文件从 AV 内容生成。然而，附属数据不局限于图像文件。例如，第一实施例的相同的处理还可以在能从 AV 内容提取的诸如音频文件和文本文件的数据被作为附属数据提取的情况下进行。

[0122] 接下来，播放由以上处理记录在 DVD 介质 140 上的附属数据的处理将说明如下。图 9 是显示由第一实施例的 DVD 记录器 100 进行的附属数据播放处理的流程图。附属数据回放处理对应于输出处理的一部分，例如标题内容的菜单屏幕。

[0123] 首先，主机单元 120 从 DVD 介质 140 选择作为输出目标的附属数据（步骤 S901）。

密钥选择处理单元 124 检查所选择的附属数据是否被加密（步骤 S902）。在图 4 中说明的经封装的文件的扩展名被用于判定附属数据是明码文本还是经加密的数据的技术。

[0124] 当附属数据是明码文本时（步骤 S902 中为否），AV 数据解密单元 125 解码附属数据（步骤 S906），并且 AV 数据解密单元 125 将附属数据输出至显示装置（步骤 S907）。

[0125] 当附属数据在步骤 S902 中被加密时（步骤 S902 中为是），标题密钥文件处理单元 121 参考经封装的文件的密钥号字段以从标题密钥文件获得对应于密钥号的经加密的标题密钥（步骤 S903）。然后，标题密钥文件处理单元 121 使用装置密钥解密所获得的经加密的标题密钥（步骤 S904）。

[0126] 解密处理单元 122 使用经解密的标题密钥解密经加密的附属数据（步骤 S905）。AV 数据解密单元 125 解密附属数据（步骤 S906），并且 AV 数据解密单元 125 将附属数据输出至显示装置（步骤 S907）。

[0127] 接下来，回放记录在 DVD 介质 140 上的 AV 内容的处理将说明如下。图 10 是显示由第一实施例的 DVD 记录器 100 进行的 AV 内容回放处理的流程图。

[0128] 首先，主机单元 120 从 DVD 介质 140 选择用于作为输出目标的 AV 内容的经加密的内容（步骤 S1001）。密钥选择处理单元 124 使用 DVD 介质 140 中的管理文件以便检查所选择的标题内容是否被加密（步骤 S1002）。

[0129] 当标题内容是明码文本时（步骤 S1002 中为否），AV 数据解码单元 125 解码标题内容（步骤 S1006），并且 AV 数据解码单元 125 将标题内容输出至显示装置（步骤 S1007）。

[0130] 当标题内容在步骤 S1002 中被加密时（步骤 S1002 中为是），标题密钥文件处理单元 121 参考管理文件的密钥号以便从标题密钥文件获得对应于密钥号的经加密的标题密钥（步骤 S1003）。然后，标题密钥文件处理单元 121 使用装置密钥解密所获得的经加密的标题密钥（步骤 S1004）。

[0131] 解密处理单元 122 使用经解密的标题密钥解密经加密的标题内容（步骤 S1005）。AV 数据解码单元 125 解码标题内容（步骤 S1006），并且 AV 数据解码单元 125 将标题内容输出至显示装置（步骤 S1007）。

[0132] 这样，记录在 DVD 介质 140 上的附属数据和标题内容被播放。

[0133] 如上所述，在第一实施例的 DVD 记录器 100 中，当 AV 内容的复制控制信息表明诸如“不能复制”或“不能再复制”的复制限制时，附属数据由与对应于 AV 内容的标题内容的标题密钥相同的标题密钥加密。所以，附属数据的非法使用和非法复制被防止，并且标题内容的版权保护被加强。

[0134] 第二实施例将说明如下。

[0135] 在第一实施例的 DVD 记录器 100 中，用以加密附属数据的标题密钥在标题密钥文件中被管理。另一方面，在第二实施例的 DVD 记录器 100 中，新生成的用以加密附属数据的标题密钥在不同于标题密钥文件的文件中被管理。

[0136] 图 11 是显示根据第二实施例的 DVD 记录器 1100 的配置的方框图。如图 11 所示，第二实施例的 DVD 记录器 1100 包括驱动单元 110，主机单元 1120 和 HDD 单元 130。驱动单元 110 在 DVD 介质 140 中记录数据，并且驱动单元 110 从 DVD 介质 140 读取数据。主机单元 1120 进行标题内容或标题密钥的加密处理和解密处理，并且主机单元 1120 进行从经解密的标题内容生成附属数据的处理。标题内容被存储在 HDD 单元 130 中。类似于第一实施

例，驱动单元 110 和主机单元 1120 以及主机单元 1120 和 HDD 单元 130 与通用总线或专用总线连接。

[0137] 类似于第一实施例，DVD 记录器 1100 可以被配置成不包括 HDD 单元 130。

[0138] 类似于第一实施例，标题密钥文件 (TKF)，多个 AV 内容 (AV 内容 #1，AV 内容 #2 和 AV 内容 #3) 和管理文件在 DVD 介质 140 中以文件的形式被记录。第二实施例与第一实施例的区别在于管理附属数据的附属数据标题密钥文件被存储在 DVD 介质 140 中。

[0139] 附属数据标题密钥文件具有与图 2 所示的标题密钥文件相同的结构，并且附属数据标题密钥文件具有其中多个经加密的标题密钥被寄存的结构。经加密的标题密钥是其中标题密钥在加密附属数据中被加密的经加密的标题密钥。

[0140] 在第二实施例的 DVD 记录器 1100 中，驱动单元 110 和 HDD 单元 130 具有与第一实施例相同的配置。第二实施例的 DVD 记录器 1100 与第一实施例的 DVD 记录器 100 的区别在于主机单元 1120 包括附属数据标题密钥文件处理单元 1121 和密钥选择单元 1124，同时主机单元 1120 不包括密钥选择单元 124 和设定信息存储单元 128 的功能。然而，类似于第一实施例，主机单元 1120 包括标题密钥文件处理单元 121，解密处理单元 122，加密处理单元 123，AV 数据解码单元 125，图像生成处理单元 126，和装置秘密密钥存储单元 127。

[0141] 附属数据标题密钥文件处理单元 1121 在附属数据标题密钥文件中加密并存储标题密钥。附属数据标题密钥文件处理单元 1121 解密寄存在 DVD 介质 140 的附属数据标题密钥文件中的经加密的标题密钥，并且使用标题密钥加密附属数据。密钥选择单元 1124 与第一实施例的密钥选择单元 124 的区别在于标题密钥在新生成时不考虑包括作为附属数据提取源的标题内容的 AV 内容的复制控制信息的状态。

[0142] 由第二实施例的 DVD 记录器 1100 进行的附属数据生成处理类似于图 3 中说明的第一实施例的附属数据生成处理。第二实施例在密钥选择处理方面不同于第一实施例。

[0143] 由 DVD 记录器 1100 进行的步骤 S308 中的密钥选择处理将说明如下。图 12 是显示由第二实施例的 DVD 记录器 1100 在步骤 S308 中进行的密钥选择处理的过程的流程图。密钥选择单元 124 新生成标题密钥时不考虑包括作为附属数据提取源的标题内容的 AV 内容 的复制控制信息的状态（步骤 S1201）。附属数据标题密钥文件处理单元 1121 检查 DVD 介质 140 中是否存在附属数据标题密钥文件（步骤 S1202）。当附属数据标题密钥文件不存在时（步骤 S1202 中为否），附属数据标题密钥文件被新生成（步骤 S1203）。当附属数据标题密钥文件存在时（步骤 S1202 中为是），附属数据标题密钥文件不生成。

[0144] 接下来，附属数据标题密钥文件处理单元 1121 在 DVD 介质 140 中搜索附属数据标题密钥文件的空记录（步骤 S1204）。附属数据标题密钥文件处理单元 1121 使用装置密钥加密新生成的标题密钥，记录单元 113 通过在标题密钥文件的空记录中记录新加密的标题密钥更新附属数据标题密钥文件（步骤 S1205）。

[0145] 这样，类似于第一实施例，附属数据（压缩图像）用所生成的标题密钥加密并且记录在 DVD 介质 140 上。

[0146] 第二实施例的 DVD 记录器 1100 的标题密钥文件处理单元 121 禁止存储在附属数据标题密钥文件中的标题密钥被移到诸如 HDD 单元 130 的另一个记录介质中。具体地说，即使进行寄存在附属数据标题密钥文件中的标题密钥被移到另一个记录介质的操作，标题密钥文件处理单元 121 也拒绝移动操作。或者，在图 8 所示的标题密钥移动处理中，对寄存

在附属数据标题密钥文件中的标题密钥不进行从易失性存储器的机密区域向另一个区域移动作为步骤 S804 中的移动目标的标题密钥的处理。所以，通过将用以加密附属数据的标题密钥移向另一个记录介质才能实现的附属数据复制能被防止。

[0147] 除了标题密钥从附属数据标题密钥文件获得之外，在第二实施例中的附属数据回放处理以与第一实施例中图 9 的附属数据回放处理相同的方式进行。

[0148] 在第二实施例中的标题内容回放处理以与第一实施例中图 10 的标题内容回放处理相同的方式进行。

[0149] 这样，在第二实施例的 DVD 记录器 1100 中，用以加密附属数据的标题密钥在不同于标题密钥文件的附属数据标题密钥文件中进行管理，并且寄存在附属数据标题密钥文件中的标题密钥被禁止移到另一个记录介质。所以，附属数据的标题密钥容易管理，附属数据的非法使用和非法复制被防止，并且标题内容的版权保护被加强。

[0150] 在第二实施例中，用以加密附属数据的标题密钥被存储在附属数据标题密钥文件中时不考虑标题内容的复制控制信息。或者，复制控制信息被判断，并且用以加密附属数据的标题密钥可以取决于复制控制信息而被存储在附属数据标题密钥文件中。图 13 是显示作为第二实施例的修改例的密钥选择处理的流程图。图 13 显示当用于加密附属数据的标题密钥取决于复制控制信息被存储在附属数据标题密钥文件中时的密钥选择处理。在图 13 的修改例中，类似于第一实施例，假定主机单元 120 包括设定信息存储单元 128。然而，本发明不局限于其中主机单元 120 包括设定信息存储单元 128 的配置。

[0151] 密钥选择单元 1124 检查关于包括作为附属数据提取源的标题内容的 AV 内容的复制控制信息的状态（步骤 S1301）。当复制控制信息表明诸如“不能再复制”或“不能复制”的复制限制时，类似于第一实施例，密钥选择单元 124 从标题密钥文件中选择对应于作为附属数据提取源的标题内容的标题密钥（经加密的标题密钥）（步骤 S1302）。当复制控制信息表明“自由复制”时，通过图 3 的步骤 S302（否），S312，S313，S310 和 S311 的处理，附属数据被记录在 DVD 介质 140 上，同时被保留在明码文本中。即使在密钥选择处理的步骤 S1301 中复制控制信息表明“自由复制”，密钥选择处理也在标题密钥未被选择以加密附属数据的同时结束。所以，通过图 3 中的步骤 S309，S310 和 S311 的处理，附属数据被记录在 DVD 介质上，同时保留在明码文本中。

[0152] 在步骤 S1301 中，当复制控制信息表明如同“EPN”或“复制一次”的复制可无限制地或有限制地进行时，密钥选择单元 1124 参考存储在设定信息存储单元 128 中的设定信息（步骤 S1303）以判定与对应于作为附属数据提取源的标题内容的标题密钥相同的密钥是否被用作用以加密附属数据的密钥（步骤 S1304）。

[0153] 当在设定信息中设定与对应于作为附属数据提取源的标题内容的标题密钥相同的密钥被用作用于加密附属数据的密钥时（步骤 S1304 中为是），密钥选择单元 1124 选择对应于作为附属数据提取源的标题内容的标题密钥（经加密的标题密钥）（步骤 S1302）。

[0154] 另一方面，在步骤 S1304 中，当在设定信息中设定与对应于作为附属数据提取源的标题内容的标题密钥相同的密钥未被用作用于加密附属数据的密钥（步骤 S1304 中为否）时，密钥选择单元 124 新生成标题密钥（步骤 S1305）。

[0155] 然后，附属数据标题密钥文件处理单元 1121 检查 DVD 介质 140 中是否存在附属数据标题密钥文件（步骤 S1306）。当附属数据标题密钥文件不存在时（步骤 S1306 中为否），

附属数据标题密钥文件处理单元 1121 新生成附属数据标题密钥文件（步骤 S1307）。当附属数据标题密钥文件存在时（步骤 S1306 中为是），附属数据标题密钥文件处理单元 1121 不生成附属数据标题密钥文件。

[0156] 然后，附属数据标题密钥文件处理单元 1121 在 DVD 介质 140 中搜索附属数据标题密钥文件的空记录（步骤 S1308）。附属数据标题密钥文件处理单元 1121 使用装置密钥加密新生成的标题密钥，并且记录单元 113 通过在标题密钥文件的空记录中记录新加密的标题密钥更新附属数据标题密钥文件（步骤 S1309）。

[0157] 在密钥选择处理的修改例中，类似于第一实施例，主机单元 120 包括设定信息存储单元 128。然而，也可以采用不设置设定信息存储单元 128 而判断复制控制信息的配置。在 这种情况下，如图 6B 所示，当复制控制信息表明像“EPN”或“复制一次”的复制可以无限制地或有限制地进行时，主机单元 120 可以被配置成使新标题密钥被生成时不进行设定信息的判定（即，不进行步骤 S1303 和 S1304 的处理）。

[0158] 虽然在第二实施例中多个标题密钥被存储在附属数据标题密钥文件中，但本发明不局限于该第二实施例。或者，例如，能被寄存在附属数据标题密钥中的标题密钥数目限于一个，所有的多个图像附属数据由相同的标题密钥加密，并且标题密钥可以被配置成不被移动。

[0159] 虽然在第二实施例中用于加密标题内容的附属数据标题密钥和标题密钥文件被逐一地形成，本发明不局限于该第二实施例。例如，附属数据标题密钥被寄存在存储用于加密标题内容的标题密钥的标题密钥文件中，同时与标题密钥分离，并且所进行的管理可以仅使附属数据标题密钥不能被移动。在这种情况下，附属数据向另一个记录介质的移动或附属数据的复制能被防止，以实现与第一实施例相同的效果。

[0160] 在第一和第二实施例中，当附属数据从其中复制控制信息表明“复制一次”或“EPN”的标题内容生成时，用以加密附属数据的标题密钥被新生成。在这些情况下，附属数据可以由对应于提取源的标题内容的标题密钥，即，用以加密提取源的标题内容的标题密钥加密。

[0161] 用于加密从其中复制控制信息表明“复制一次”的标题内容生成的附属数据的标题密钥和用于加密从其中复制控制信息表明“EPN”的标题内容生成的附属数据的标题密钥两者之一可以被设定为新生成的标题密钥，而另一个标题密钥被设定为对应于提取源的标题内容的标题密钥。

[0162] 由第一和第二实施例的 DVD 记录器执行的内容记录程序在先被存入 ROM 等装置后再被提供。

[0163] 由第一和第二实施例的 DVD 记录器执行的内容记录程序可以被配置成以可安装格式或可执行格式的内容记录程序被记录在诸如 CD-ROM，软磁盘 (FD)，CD-R 或 DVD 的计算机可读的记录介质上的状态提供。

[0164] 由第一和第二实施例的 DVD 记录器执行的内容记录程序可以被配置成存储在连接到诸如因特网的网络的计算机中和通过网络下载。由第一和第二实施例的 DVD 记录器执行的内容记录程序可以被配置成通过诸如因特网的网络提供或分配。

[0165] 由第一和第二实施例的 DVD 记录器执行的内容记录程序以包括主机单元 120，驱动单元 110 和 HDD 单元 130 的模块结构形成。在实际的硬件中，CPU（处理器）从 ROM 读取

内容记录程序以执行内容记录程序，其通过在主存储装置上装载各个单元而在主存储装置上生成各个单元。

[0166] 本领域的熟练技术人员易于实现其他的优点和修改。因此，本发明在其更广泛的各个方面不限于在本文展示和说明的具体细节和代表性实施例。据此，可以进行各种各样的修改而不背离由附后的权利要求及其等价内容所定义的总体发明构思的精神或范围。

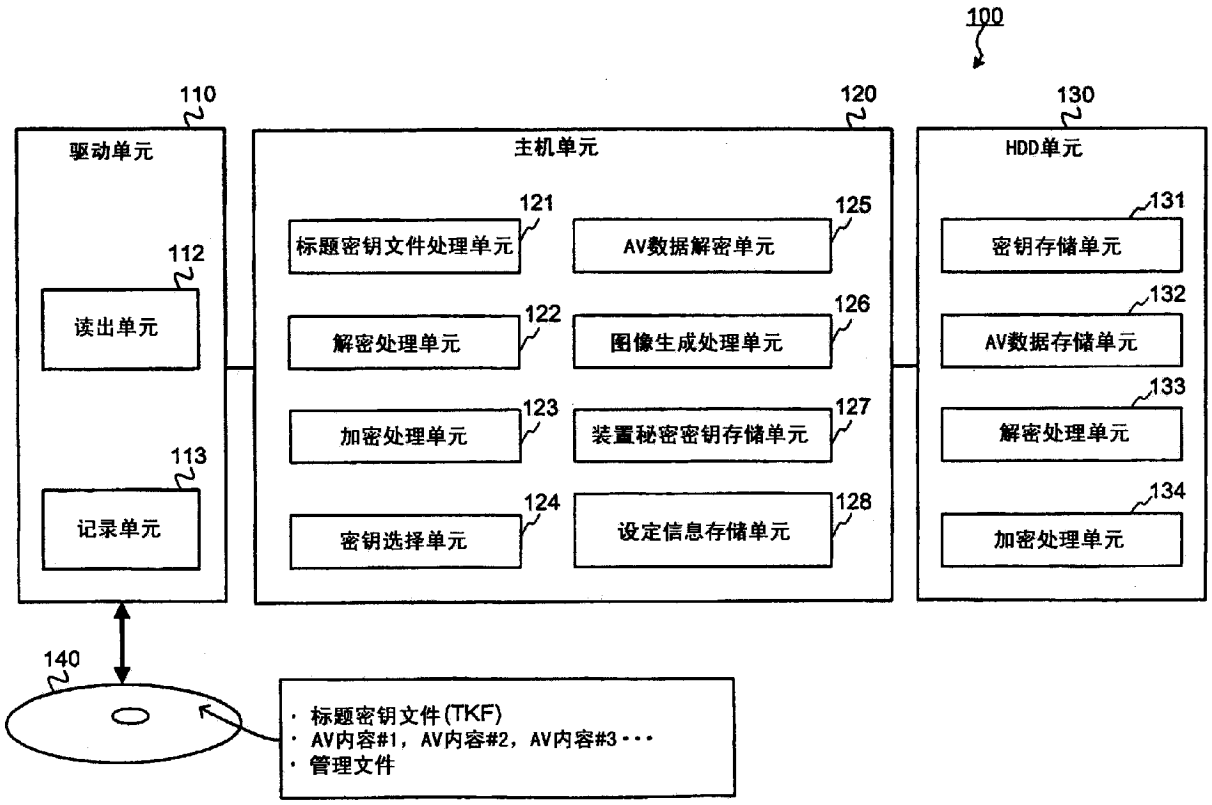
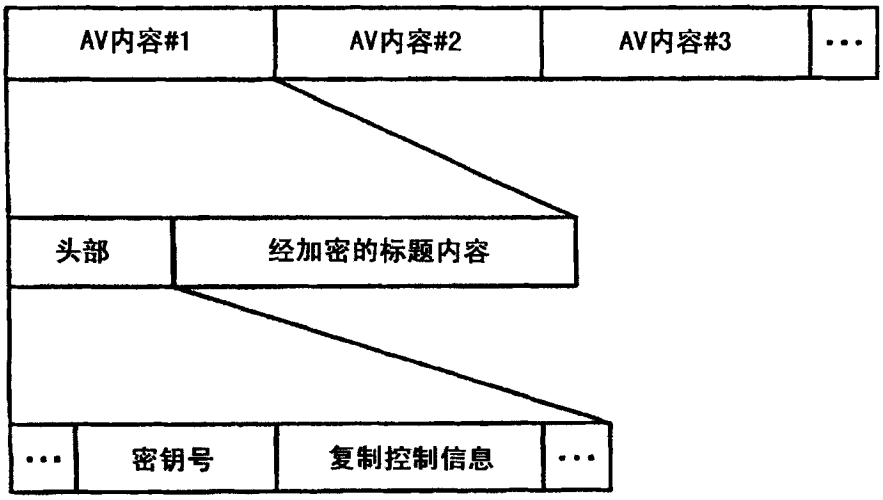

100
110
驱动单元
112
读出单元
113
记录单元
120
主机单元
121
标题密钥文件处理单元
122
解密处理单元
123
加密处理单元
124
密钥选择单元
125
AV数据解密单元
126
图像生成处理单元
127
装置秘密密钥存储单元
128
设定信息存储单元
130
HDD单元
131
密钥存储单元
132
AV数据存储单元
133
解密处理单元
134
加密处理单元
140
· 标题密钥文件(TKF)
· AV内容#1，AV内容#2，AV内容#3···
· 管理文件

图 1


AV内容#1
AV内容#2
AV内容#3
...
头部
经加密的标题内容
...
密钥号
复制控制信息
...

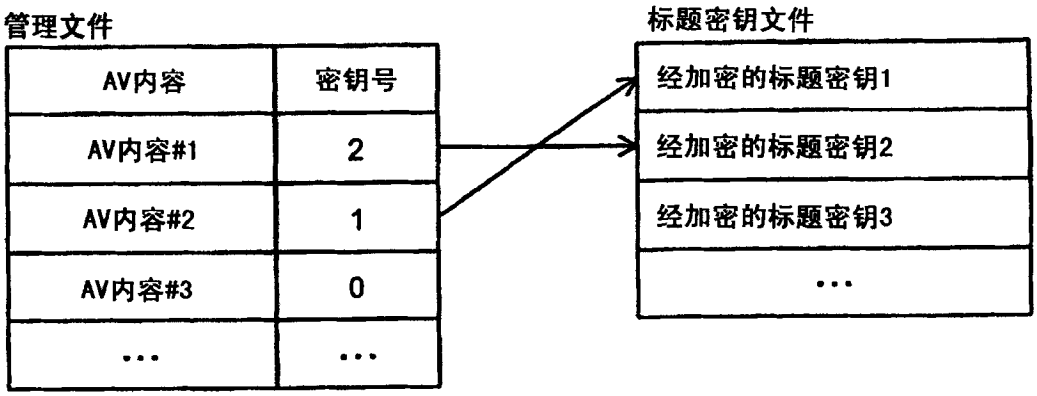

管理文件
AV内容
密钥号
AV内容#1
2
AV内容#2
1
AV内容#3
0
...
...
标题密钥文件
经加密的标题密钥1
经加密的标题密钥2
经加密的标题密钥3
...

图 2

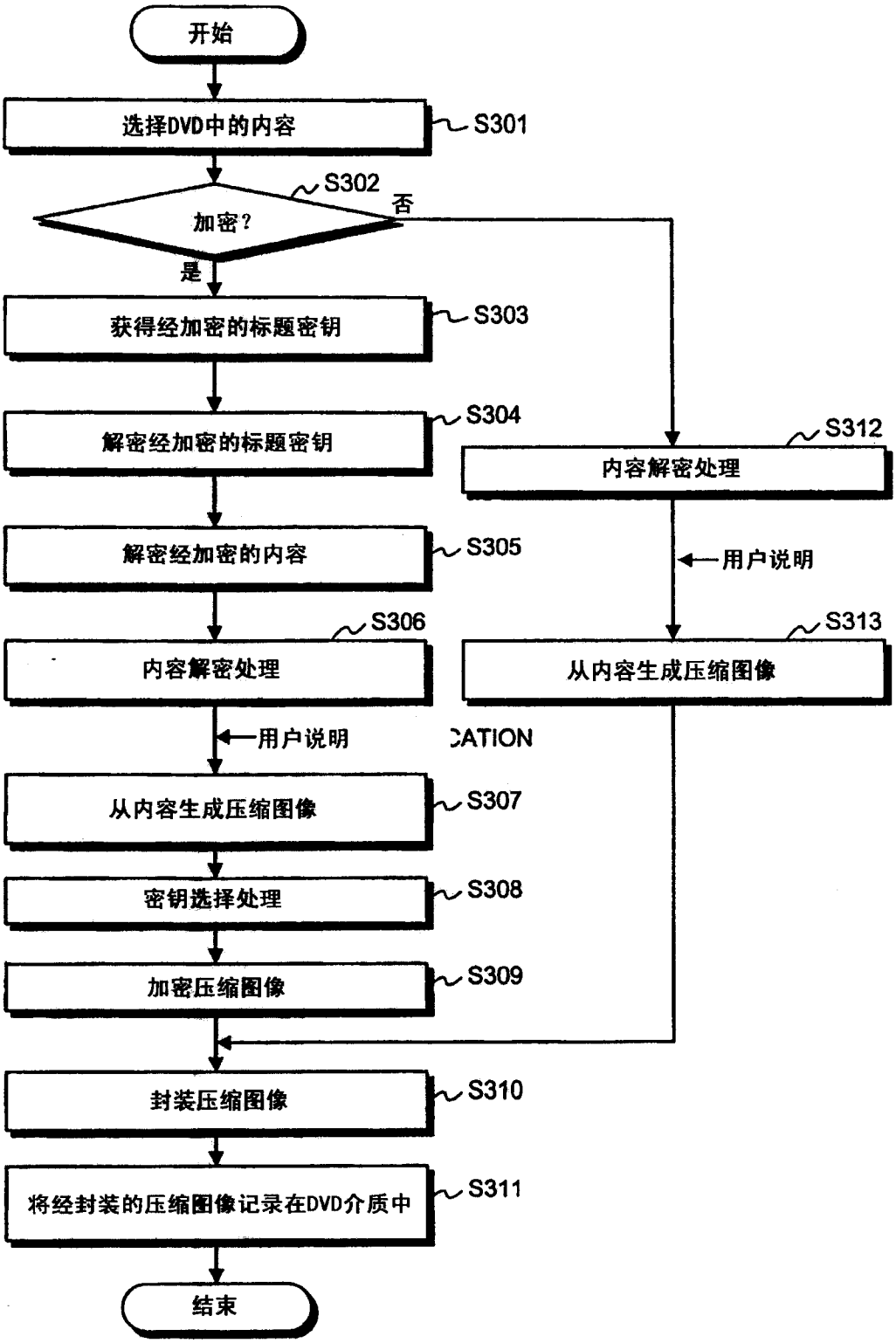

开始
选择DVD中的内容
S301
S302
加密？
否
是
获得经加密的标题密钥
S303
解密经加密的标题密钥
S304
解密经加密的内容
S305
内容解密处理
S306
用户说明
CATION
从内容生成压缩图像
S307
密钥选择处理
S308
加密压缩图像
S309
封装压缩图像
S310
将经封装的压缩图像记录在DVD介质中
S311
结束
S312
内容解密处理
用户说明
S313
从内容生成压缩图像

图 3

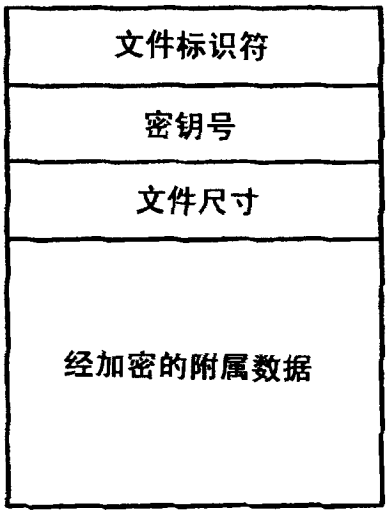


图 4

管理文件

AV内容	密钥号
AV内容#1	2
AV内容#2	1
AV内容#3	0
...	...

标题密钥文件

经加密的标题密钥1
经加密的标题密钥2
经加密的标题密钥3
...

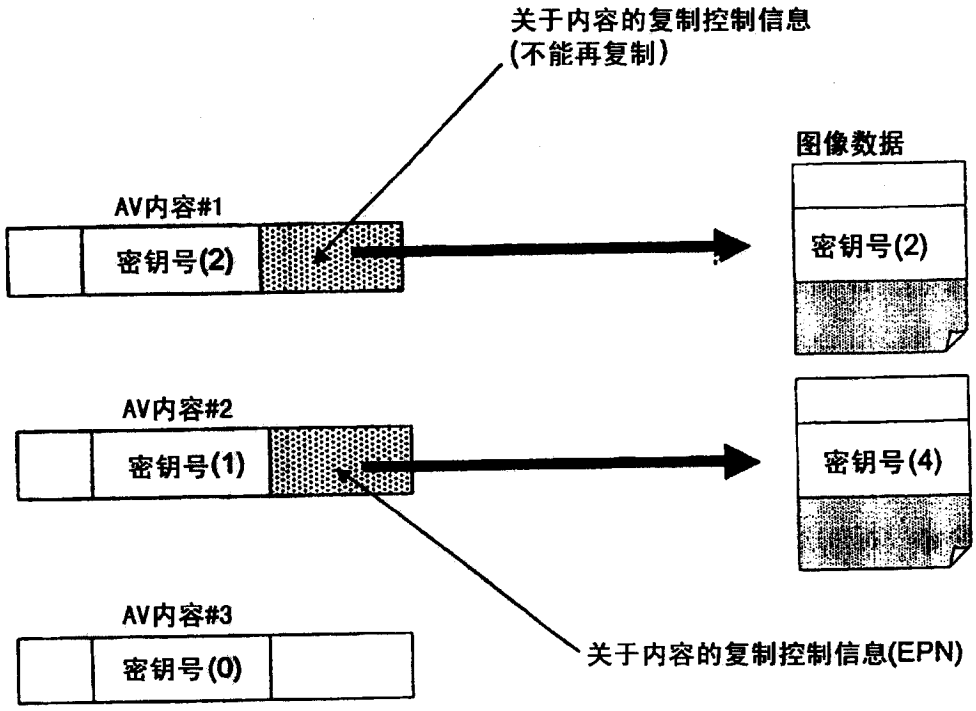


图 5

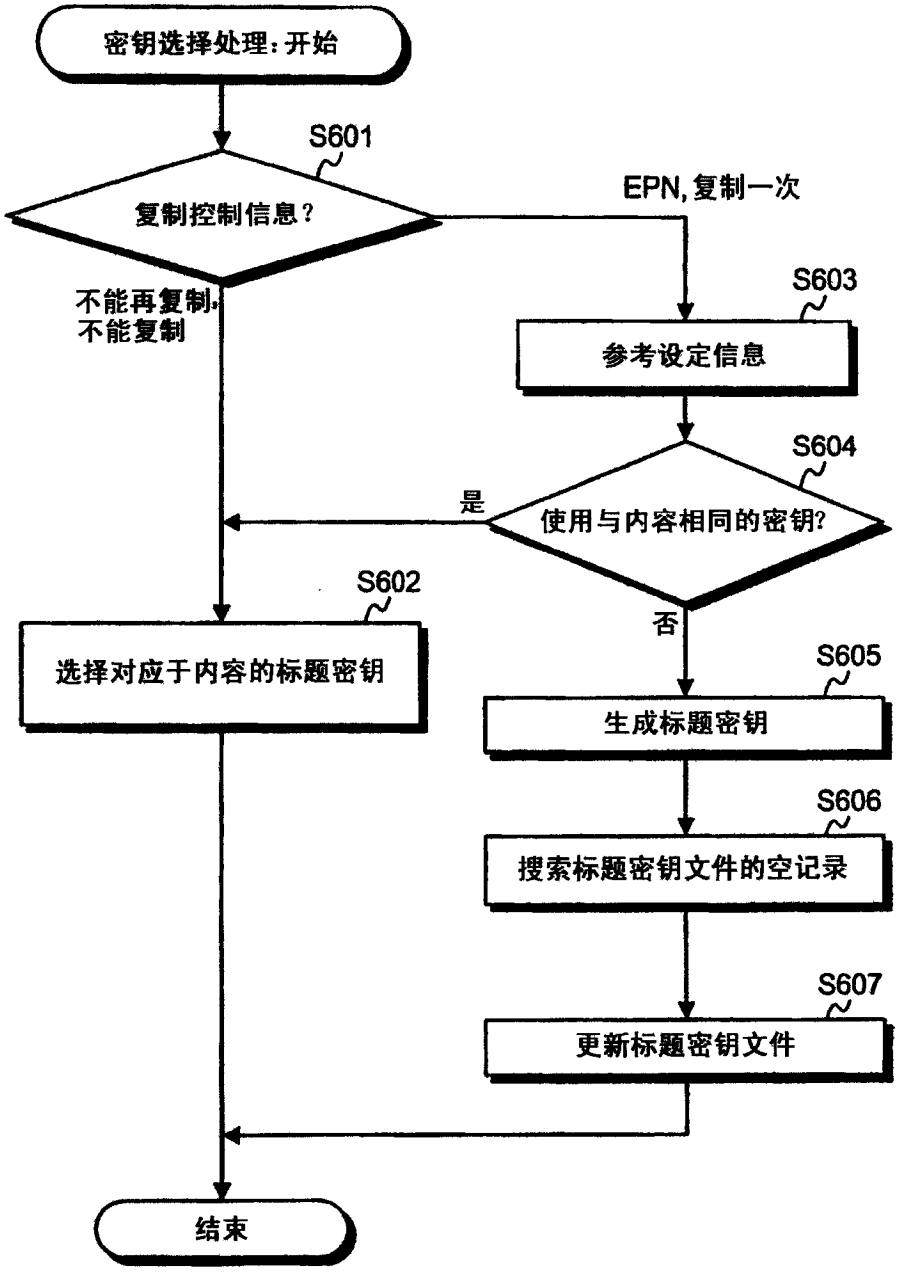

密钥选择处理：开始
S601
复制控制信息？
EPN，复制一次
不能再复制，
不能复制
S603
参考设定信息
S604
是
使用与内容相同的密钥?
否
S602
选择对应于内容的标题密钥
S605
生成标题密钥
S606
搜索标题密钥文件的空记录
S607
更新标题密钥文件
结束

图 6A

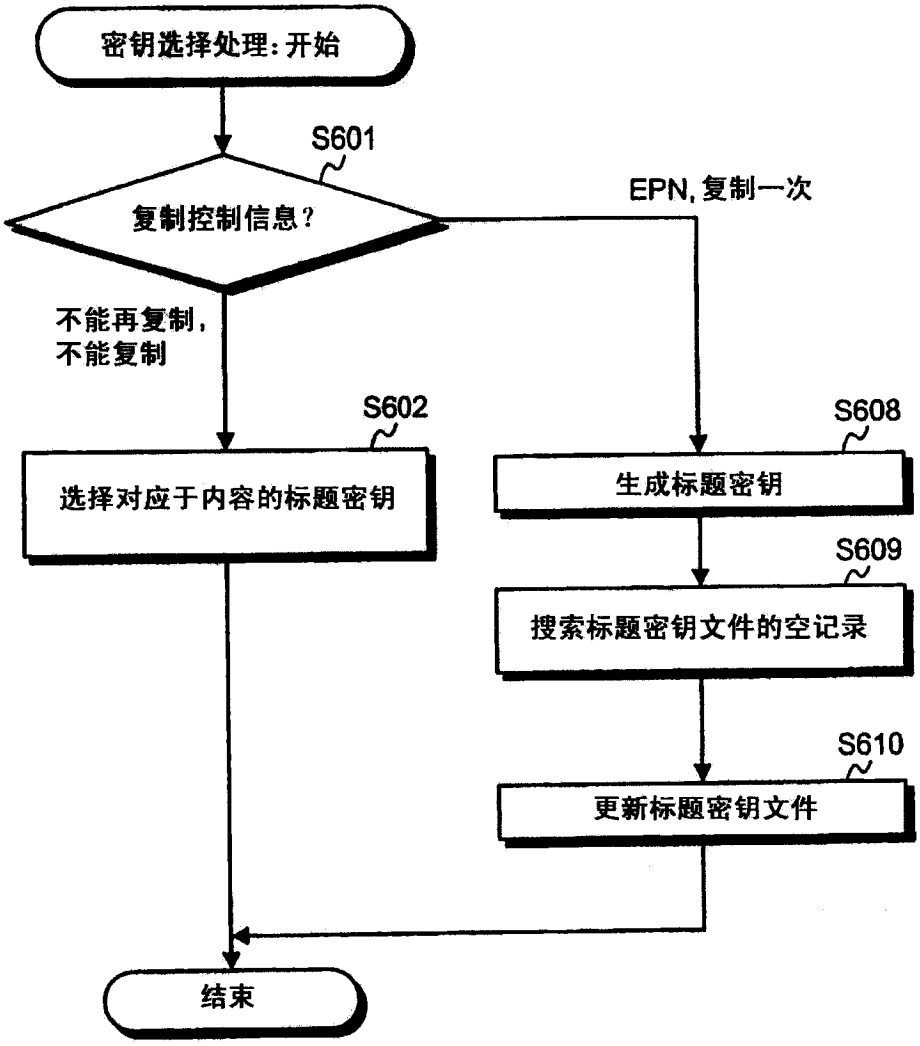

密钥选择处理：开始
S601
复制控制信息？
EPN，复制一次
不能再复制，
不能复制
S602
选择对应于内容的标题密钥
S608
生成标题密钥
S609
搜索标题密钥文件的空记录
S610
更新标题密钥文件
结束

图 6B

管理文件

AV内容	密钥号
AV内容#1	2
AV内容#2	1
AV内容#3	0
...	...

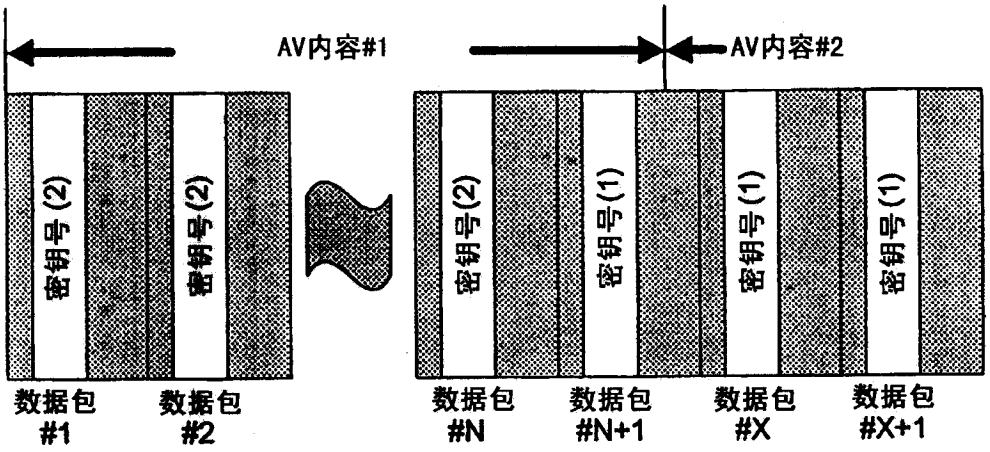


图 7

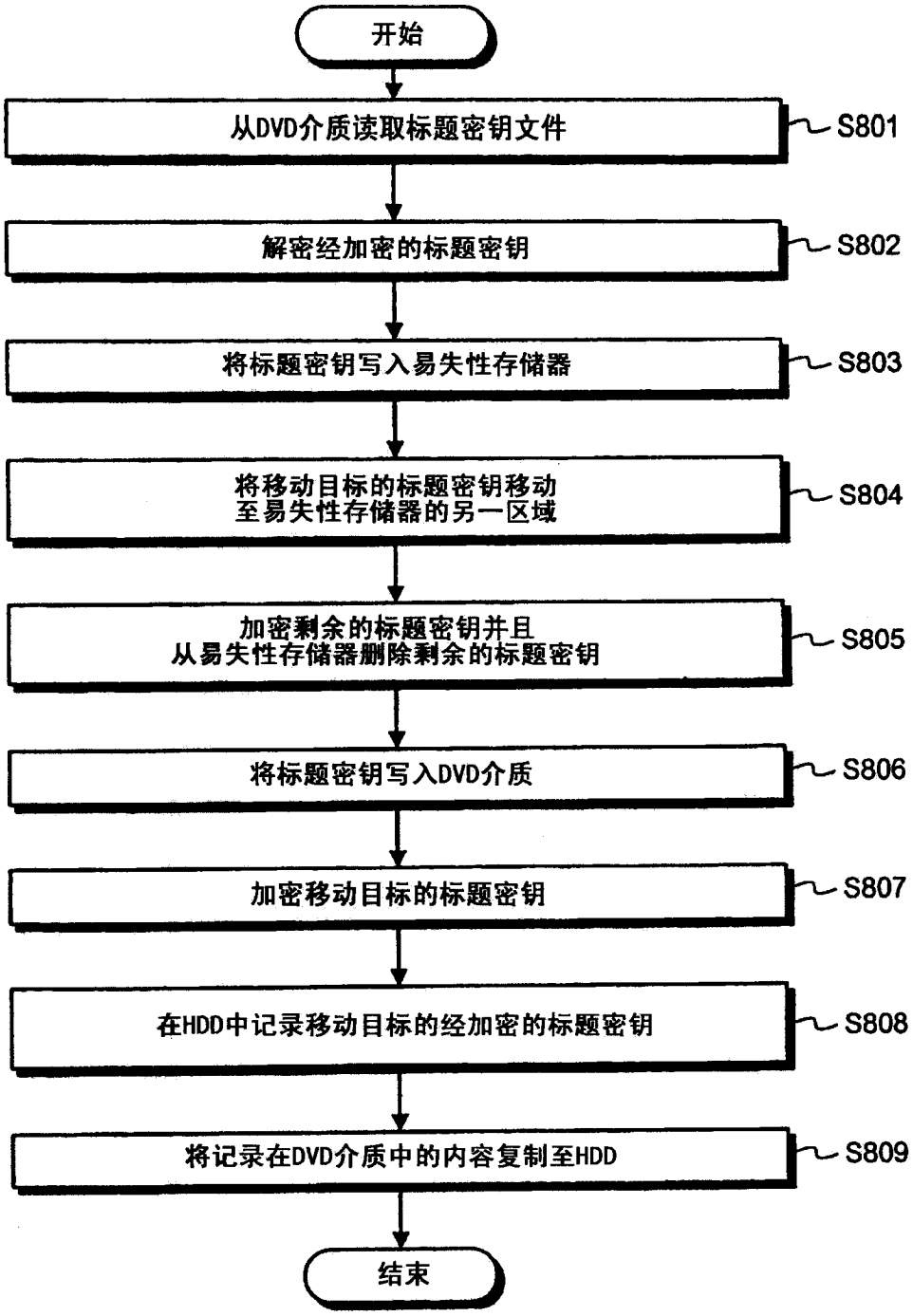

开始
从DVD介质读取标题密钥文件
S801
解密经加密的标题密钥
S802
将标题密钥写入易失性存储器
S803
将移动目标的标题密钥移动
至易失性存储器的另一区域
S804
加密剩余的标题密钥并且
从易失性存储器删除剩余的标题密钥
S805
将标题密钥写入DVD介质
S806
加密移动目标的标题密钥
S807
在HDD中记录移动目标的经加密的标题密钥
S808
将记录在DVD介质中的内容复制至HDD
S809
结束

图 8

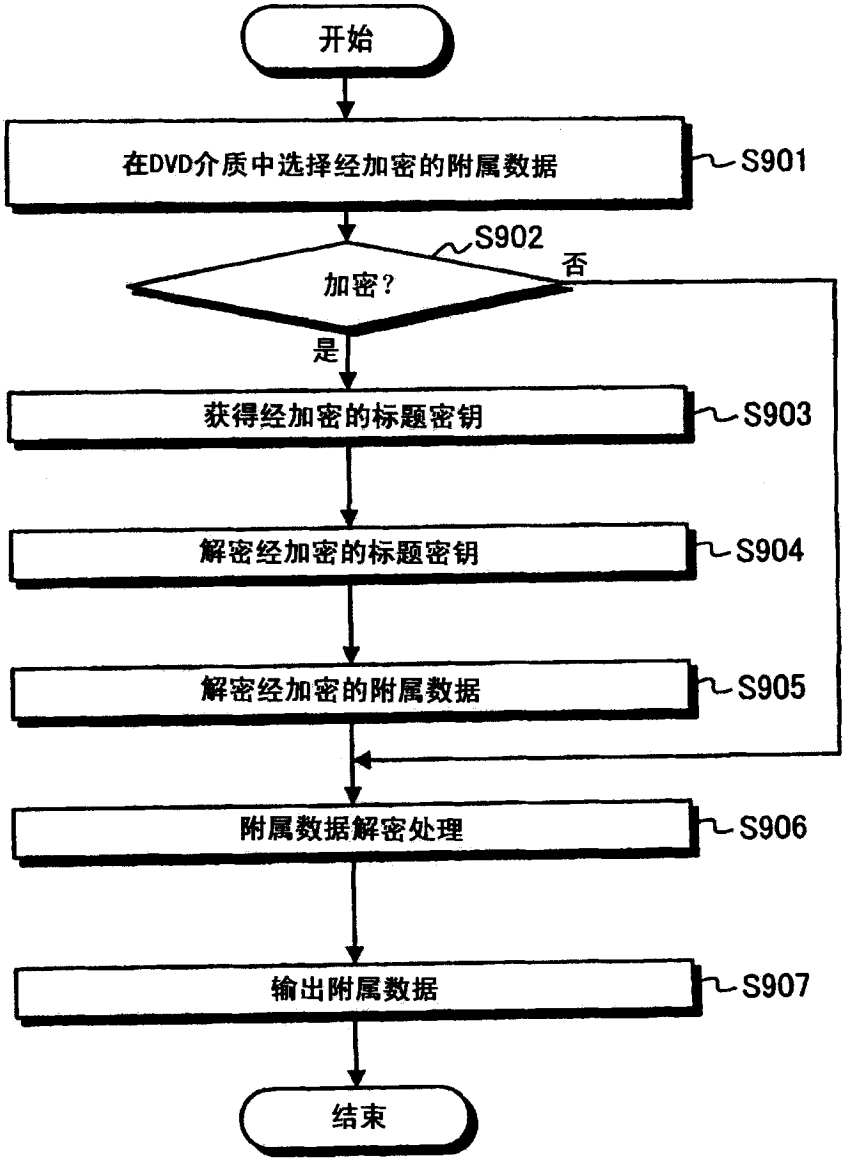

开始
在DVD介质中选择经加密的附属数据
S901
S902
加密？
否
是
获得经加密的标题密钥
S903
解密经加密的标题密钥
S904
解密经加密的附属数据
S905
附属数据解密处理
S906
输出附属数据
S907
结束

图 9

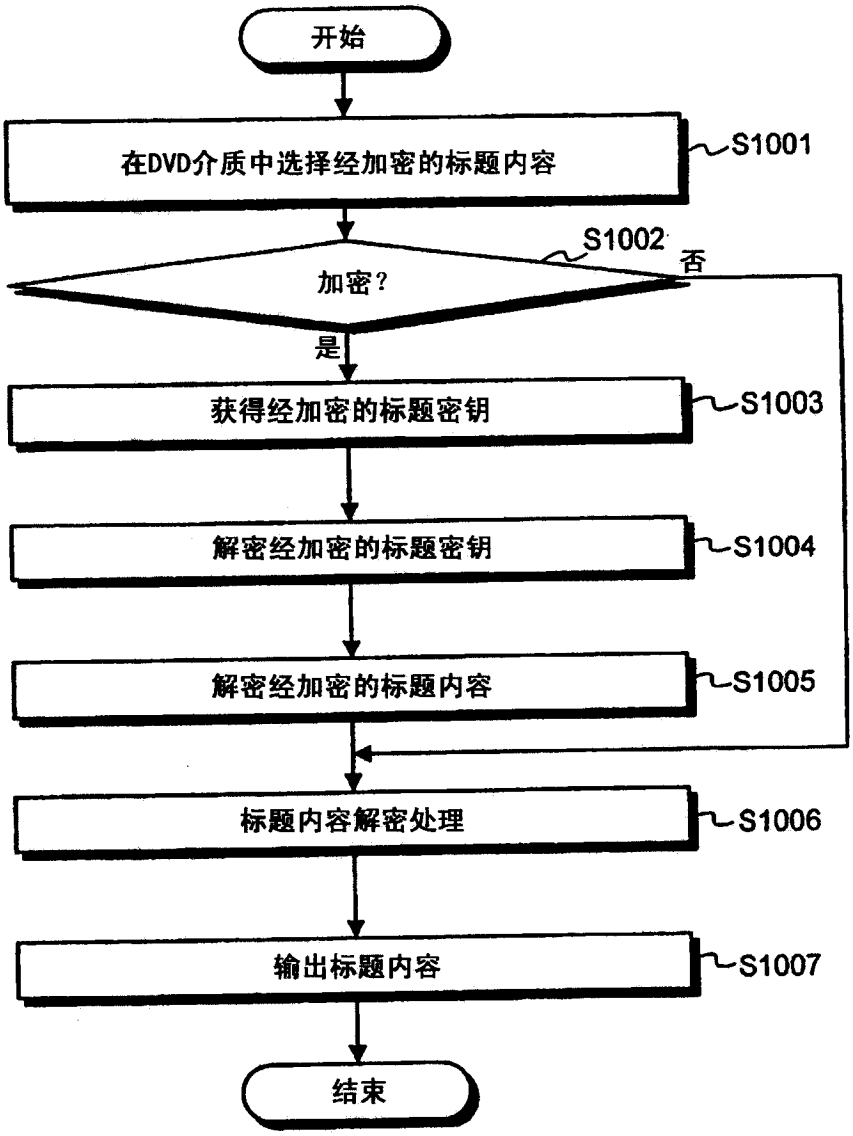

开始
在DVD介质中选择经加密的标题内容
S1001
S1002
加密？
否
是
获得经加密的标题密钥
S1003
解密经加密的标题密钥
S1004
解密经加密的标题内容
S1005
标题内容解密处理
S1006
输出标题内容
S1007
结束

图 10

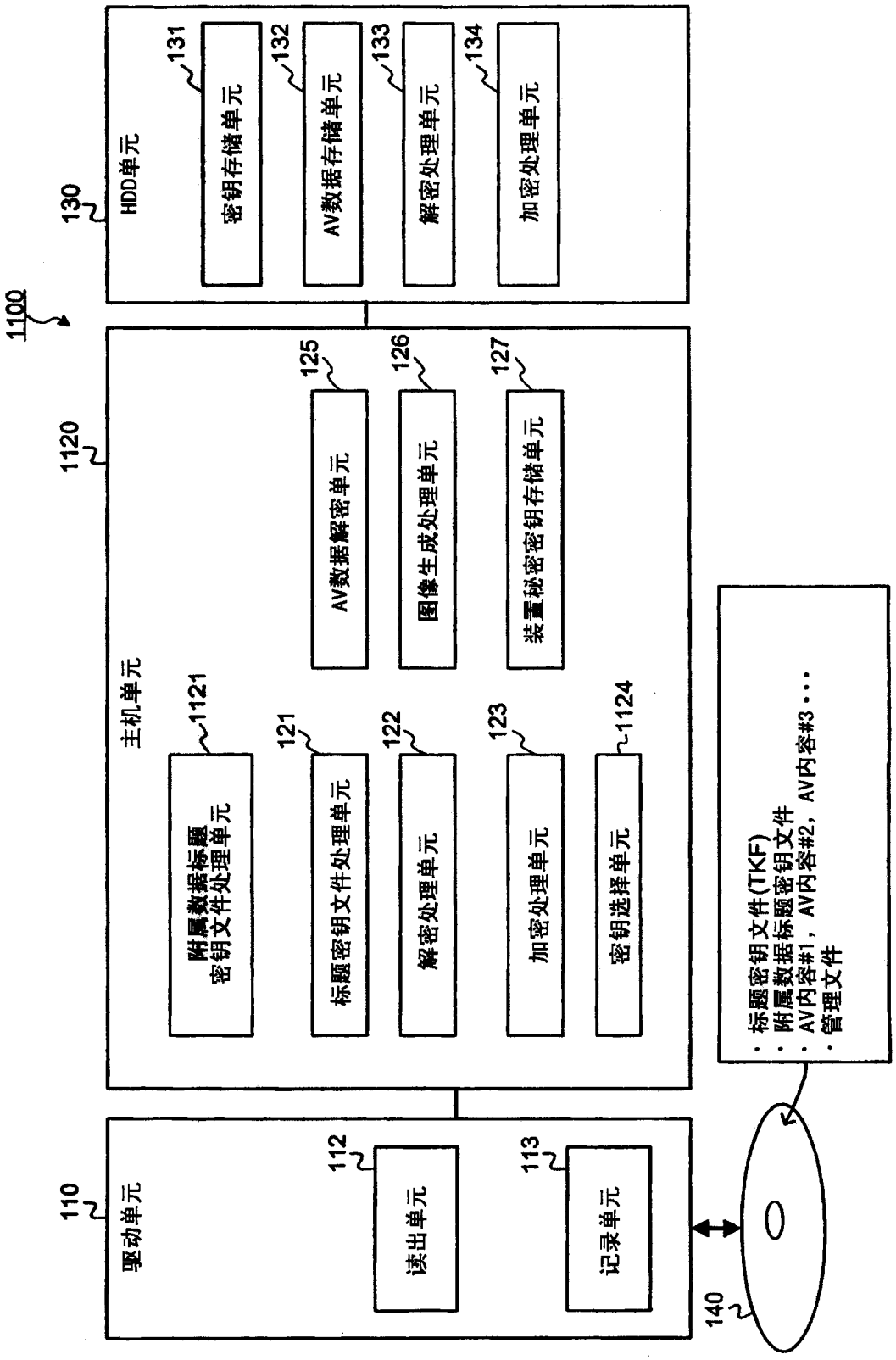

1100
HDD单元
130
密钥存储单元
131
AV数据存储单元
132
解密处理单元
133
加密处理单元
134
主机单元
1120
AV数据解密单元
125
图像生成处理单元
126
装置秘密密钥存储单元
127
附属数据标题
密钥文件处理单元
1121
标题密钥文件处理单元
121
解密处理单元
122
加密处理单元
123
密钥选择单元
1124
驱动单元
110
读出单元
112
记录单元
113
140
· 标题密钥文件(TKF)
· 附属数据标题密钥文件
· AV内容#1，AV内容#2，AV内容#3 ···
· 管理文件

图 11

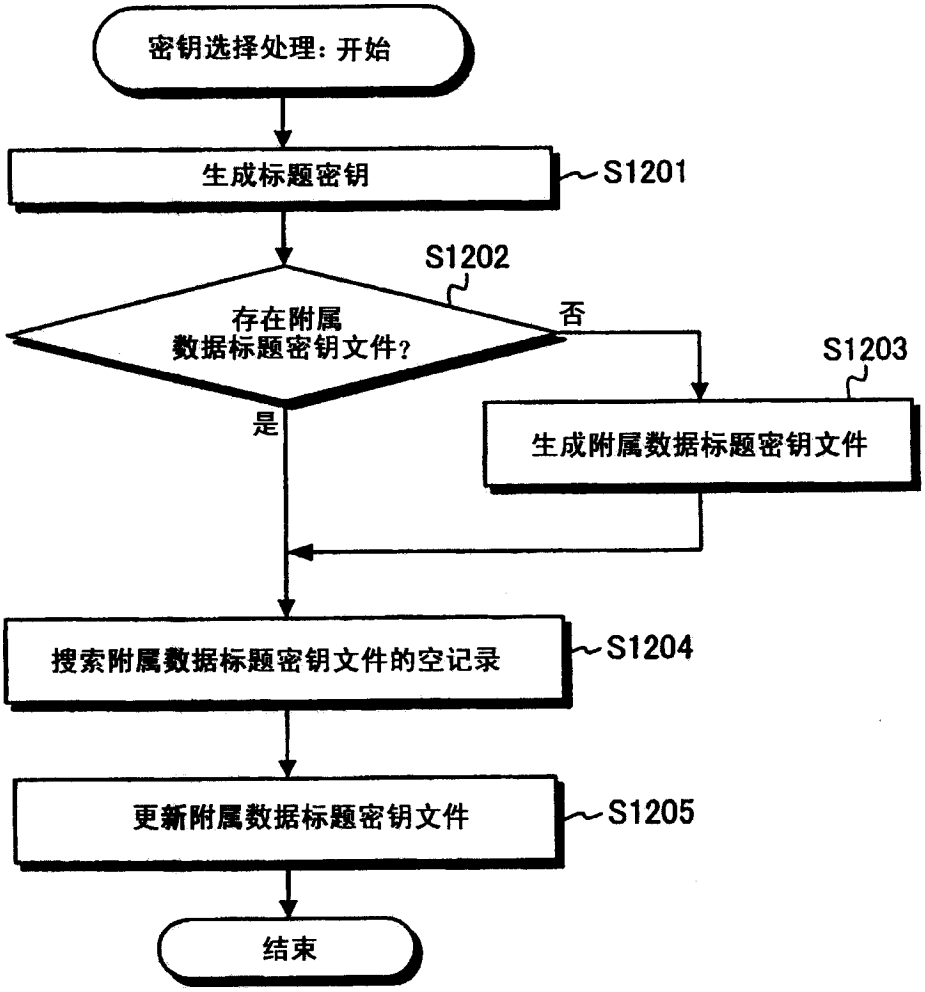

密钥选择处理：开始
生成标题密钥
S1201
S1202
存在附属
数据标题密钥文件？
否
是
S1203
生成附属数据标题密钥文件
搜索附属数据标题密钥文件的空记录
S1204
更新附属数据标题密钥文件
S1205
结束

图 12

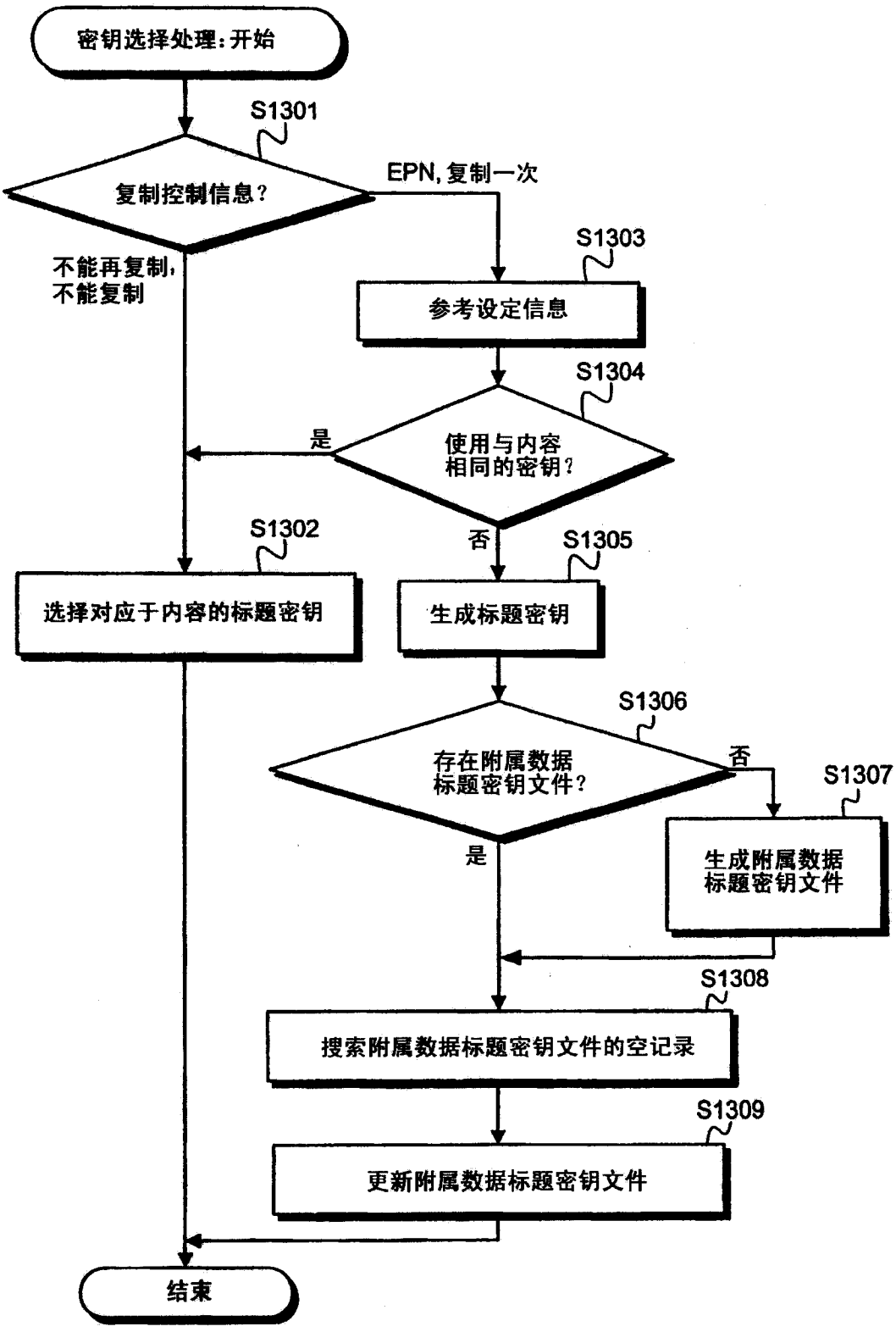

密钥选择处理：开始
S1301
复制控制信息？
EPN，复制一次
不能再复制，
不能复制
S1303
参考设定信息
S1304
使用与内容
相同的密钥？
是
否
S1302
选择对应于内容的标题密钥
S1305
生成标题密钥
S1306
存在附属数据
标题密钥文件？
否
S1307
生成附属数据
标题密钥文件
是
S1308
搜索附属数据标题密钥文件的空记录
S1309
更新附属数据标题密钥文件
结束

图 13