(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 101329714 B
(45)授权公告日 2015.06.17

(21)申请号 200810131150.0

(22)申请日 2005.03.24

(30)优先权数据
2004-110069 2004.04.02 JP
2004-146963 2004.05.17 JP
2004-151621 2004.05.21 JP
2004-163734 2004.06.01 JP
2004-196531 2004.07.02 JP
2004-201009 2004.07.07 JP
2004-206335 2004.07.13 JP

(62)分案原申请数据
200580017845.0 2005.03.24

(73)专利权人 松下电器产业株式会社
地址 日本大阪府

(72)发明人 野仲真佐男 布田裕一 中野稔久
横田薰 大森基司 宫崎雅也
山本雅哉 村濑薰 小野田仙一

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 林锦辉 王英

(51)Int.Cl.
G06F 21/10(2013.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)
H04L 9/32(2006.01)

(56)对比文件
US 2003023856 A1,2003.01.30,
CN 1422034 A,2003.06.04,
CN 1155799 A,1997.07.30,

审查员 陈安安

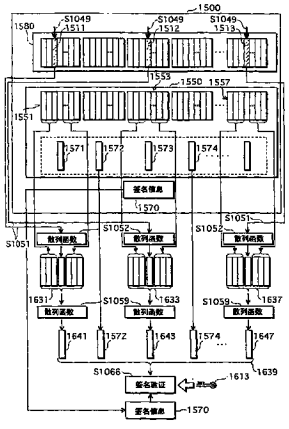
权利要求书6页 说明书62页 附图71页

(54)发明名称

未授权内容检测系统

(57)摘要

在回放内容的时候，执行装置进行回放处理的负荷很大，因为执行装置要在内容回放的同时验证内容的有效性，因此必须为执行装置配备高效处理器。本发明通过为验证只使用预定数量的已加密单元，能够减少验证处理负荷，其中的已加密单元是从构成DVD上记录的已加密内容的多个已加密单元中随机选择出来的。另外，通过每次进行验证的时候随机地选择预定数量的已加密单元，本发明能够将检测未授权内容的准确度提高到某种程度。



CN 101329714 B

1.一种数据处理装置，用于使用记录介质上记录的数字作品，该记录介质还在上面记录了（i）基于构成所述数字作品的多个数据块组而产生的多个记录摘要值以及（ii）基于所述多个记录摘要值的一些或者全部而产生的记录签名数据，该数据处理装置包括：

使用部件，用于使用所述数字作品；

选择部件，用于在每次回放所述数字作品时从所述多个数据块组中随机地选择预定数量的数据块组，所述预定数量小于所有所述多个数据块组的数量；

计算部件，用于基于被选数据块组来计算一个或多个计算摘要值；

读取部件，用于从所述多个记录摘要值中读取不包括与所计算出的计算摘要值对应的记录摘要值的多个剩余记录摘要值；

签名验证部件，用于通过利用所述记录签名数据、所述多个计算摘要值以及所述多个剩余记录摘要值，验证所述数字作品是否有效；以及

使用控制部件，用于当所述签名验证部件判定所述数字作品无效的时候，停止所述使用部件使用所述数字作品；其中

所述记录介质在其上记录多个主记录摘要值，所述多个主记录摘要值中的每个是对应多个数据块中之一而产生的，

在所述记录介质上记录的所述多个记录摘要值中的每个是根据（i）预定数目的主记录摘要值和（ii）预定数目的数据块标识符而二次产生的摘要值，所述预定数目的主记录摘要值是相对于包括预定数目的数据块的每个数据块组而产生的，以及

所述计算部件根据多个被选数据块中的每个计算主计算摘要值，并且通过对所计算出的主计算摘要值、与在包括所述多个被选数据块的同一数据块组中所包括的不同数据块对应的主记录摘要值、和对应于每一个摘要值的所述预定数目的数据块标识符执行操作来二次计算所述计算摘要值。

2.如权利要求1所述的数据处理装置，其中

所述数字作品包括多个文件，所述多个文件中的每一个都由所述多个数据块中的两个或者更多个构成，并且与所述多个记录摘要值中之一对应，

所述多个记录摘要值中的每一个都是通过使用多个主记录摘要值产生的，所述多个主记录摘要值与构成与所述记录摘要值相对应的文件的所述多个数据块中的两个或者多个数据块一一对应，

所述计算部件包括：

计算子部件，用于读取与所述文件中包括的多个未被选中数据块对应的多个主记录摘要值，并且相对于包括所述多个被选数据块中至少之一的每个文件，使用所读取的多个主记录摘要值和所计算出的主计算摘要值来计算所述计算摘要值；

读取子部件，用于相对于不包括所述多个被选数据块的每个文件，读取与该文件对应的多个剩余记录摘要值；

所述签名验证部件

a）通过对所述多个计算摘要值、所读取的多个剩余记录摘要值和所述记录签名数据执行签名验证算法来执行签名验证处理；以及

b）当所述签名验证处理成功时判定所述数字作品是有效的，以及当所述签名验证处理失败时判定所述数字作品是无效的。

3. 如权利要求 2 所述的数据处理装置，其中

所述多个记录摘要值是多个散列值，每一个散列值都是利用散列函数产生的，以及

所述计算子部件计算出的次计算摘要值是通过将所述散列函数应用于与所述多个未被选中的多个数据块相对应的所述多个主记录摘要值以及所述主计算摘要值而计算出的散列值。

4. 如权利要求 2 所述的数据处理装置，其中

所述数字作品是数字内容，并且所述使用部件通过回放所述数字内容来使用所述数字内容。

5. 如权利要求 2 所述的数据处理装置，其中

所述数字作品是计算机程序，并且所述使用部件通过对构成所述计算机程序的指令代码进行解码，并按照已解码代码进行操作来使用所述计算机程序。

6. 如权利要求 2 所述的数据处理装置，代替所述使用控制部件，包括：

警告显示部件，用于当判定所述数字作品为无效的时候，显示所述数字作品无效的通知。

7. 如权利要求 1 所述的数据处理装置，其中所述记录介质已经另外记录了 (i) 表明所述记录介质上允许外部装置访问的访问允许区域的区域信息以及 (ii) 基于所述数字作品和所述区域信息的部分或者全部而产生的签名数据，所述数据处理装置进一步包括：

访问禁止部件，用于基于所述区域信息禁止对所述访问允许区域以外的区域的访问；以及

验证部件，用于通过使用所述数字作品、所述区域信息和所述签名数据验证所述数字作品和所述区域信息是否有效，以及

所述使用控制部件，用于当所述验证部件判定所述数字作品和所述区域信息中的至少一个无效的时候，停止所述使用部件使用所述数字作品。

8. 如权利要求 1 所述的数据处理装置，其中

所述选择部件、所述计算部件、所述读取部件以及所述签名验证部件是在单个大规模集成电路上一起组装的。

9. 如权利要求 1 所述的数据处理装置，其中

所述读取部件还从所述记录介质读取与所述被选数据块组对应的多个记录摘要值，以及

所述数据处理装置还包括：

摘要值验证部件，用于对记录在所述记录介质上的所述多个记录摘要值和所述多个计算摘要值进行验证；以及

第二使用控制部件，用于当根据所述摘要值验证部件的验证结果判定所述数字作品为无效时，停止所述使用部件使用所述数字作品。

10. 一种数据处理方法，用于使用记录介质上记录的数字作品，该记录介质上还记录了 (i) 基于构成所述数字作品的多个数据块组而产生的多个记录摘要值以及 (ii) 基于所述多个记录摘要值的一些或者全部而产生的记录签名数据，包括以下步骤：

(a) 使用所述数字作品；

(b) 在每次回放所述数字作品时从所述多个数据块组随机地选择预定数量的数据块

组，所述预定数量小于所有所述多个数据块组的数量；

(c) 基于被选数据块组计算一个或多个计算摘要值；

(d) 从所述多个记录摘要值中读取不包括与所计算出的计算摘要值对应的记录摘要值的多个剩余记录摘要值；

(e) 通过使用所述记录签名数据、所述多个计算摘要值和所述多个剩余记录摘要值来验证所述数字作品是否有效；以及

(f) 在步骤 (e) 中判定所述数字作品无效的时候，停止所述步骤 (a)；其中

所述记录介质在其上记录多个主记录摘要值，所述多个主记录摘要值中的每个是对应多个数据块中之一而产生的，

在所述记录介质上记录的所述多个记录摘要值中的每个是根据 (i) 预定数目的主记录摘要值和 (ii) 预定数目的数据块标识符而二次产生的摘要值，所述预定数目的主记录摘要值是相对于包括预定数目的数据块的每个数据块组而产生的，以及

所述计算部件根据多个被选数据块中的每个计算主计算摘要值，并且通过对所计算出的主计算摘要值、与在包括所述多个被选数据块的同一数据块组中所包括的不同数据块对应的主记录摘要值、和对应于每一个摘要值的所述预定数目的数据块标识符执行操作来二次计算所述计算摘要值。

11. 一种数据处理装置，用于使用记录介质上记录的数字作品，该记录介质还在上面记录了 (i) 基于构成所述数字作品的多个数据块组而产生的多个记录摘要值以及 (ii) 基于所述多个记录摘要值的一些或者全部而产生的记录签名数据，该数据处理装置包括：

使用部件，用于使用所述数字作品；

选择部件，用于在每次回放所述数字作品时从所述多个数据块组中随机地选择预定数量的数据块组，所述预定数量小于所有所述多个数据块组的数量；

计算部件，用于基于被选数据块组来计算一个或多个计算摘要值；

读取部件，用于从所述多个记录摘要值中读取不包括与所计算出的计算摘要值对应的记录摘要值的多个剩余记录摘要值；

签名验证部件，用于通过利用所述记录签名数据、所述多个计算摘要值以及所述多个剩余记录摘要值，验证所述数字作品是否有效；

查询部件，用于当所述签名验证部件所执行的验证失败时，查询是否允许使用所述数字作品；以及

使用控制部件，用于当响应于所述查询部件进行的查询而接收到指示禁止使用所述数字作品的使用禁止信息时，停止所述使用部件使用所述数字作品；其中

所述记录介质在其上记录多个主记录摘要值，所述多个主记录摘要值中的每个是对应多个数据块中之一而产生的，

在所述记录介质上记录的所述多个记录摘要值中的每个是根据 (i) 预定数目的主记录摘要值和 (ii) 预定数目的数据块标识符而二次产生的摘要值，所述预定数目的主记录摘要值是相对于包括预定数目的数据块的每个数据块组而产生的，以及

所述计算部件根据多个被选数据块中的每个计算主计算摘要值，并且通过对所计算出的主计算摘要值、与在包括所述多个被选数据块的同一数据块组中所包括的不同数据块对应的主记录摘要值、和对应于每一个摘要值的所述预定数目的数据块标识符执行操作来二

次计算所述计算摘要值。

12. 如权利要求 11 所述的数据处理装置，其中

所述数据处理装置经由通信信道与分发装置相连，

当所述签名验证部件所执行的验证失败时，所述数据处理装置向所述分发装置发送用于识别所述数字作品的标识符，以及

所述使用控制部件从所述分发装置接收所述使用禁止信息。

13. 如权利要求 11 所述的数据处理装置，其中

当所述数字作品是新内容时，所述使用控制部件接收到所述使用禁止信息。

14. 如权利要求 11 所述的数据处理装置，其中

当所述数字作品是在过去的预定时间段内创建时，所述使用控制部件接收到所述使用禁止信息。

15. 一种在数据处理装置中使用的数据处理方法，该数据处理装置用于使用记录介质上记录的数字作品，该记录介质还在上面记录了 (i) 基于构成所述数字作品的多个数据块组而产生的多个记录摘要值以及 (ii) 基于所述多个记录摘要值的一些或者全部而产生的记录签名数据，该数据处理方法包括 ：

(a) 使用所述数字作品 ；

(b) 在每次回放所述数字作品时从所述多个数据块组中随机地选择预定数量的数据块组，所述预定数量小于所有所述多个数据块组的数量 ；

(c) 基于被选数据块组来计算一个或多个计算摘要值 ；

(d) 从所述多个记录摘要值中读取不包括与所计算出的计算摘要值对应的记录摘要值的多个剩余记录摘要值 ；

(e) 通过利用所述记录签名数据、所述多个计算摘要值以及所述多个剩余记录摘要值，验证所述数字作品是否有效 ；

(f) 当步骤 (e) 中所执行的验证失败时，查询是否允许使用所述数字作品 ；以及

(g) 当响应于步骤 (f) 中进行的查询而接收到指示禁止使用所述数字作品的使用禁止信息时，停止步骤 (a) 使用所述数字作品 ；其中

所述记录介质在其上记录多个主记录摘要值，所述多个主记录摘要值中的每个是对应多个数据块中之一而产生的，

在所述记录介质上记录的所述多个记录摘要值中的每个是根据 (i) 预定数目的主记录摘要值和 (ii) 预定数目的数据块标识符而二次产生的摘要值，所述预定数目的主记录摘要值是相对于包括预定数目的数据块的每个数据块组而产生的，以及

所述计算部件根据多个被选数据块中的每个计算主计算摘要值，并且通过对所计算出的主计算摘要值、与在包括所述多个被选数据块的同一数据块组中所包括的不同数据块对应的主记录摘要值、和对应于每一个摘要值的所述预定数目的数据块标识符执行操作来二次计算所述计算摘要值。

16. 一种数据处理装置，用于使用记录介质上记录的数字作品，该记录介质还在上面记录了 (i) 基于构成所述数字作品的多个数据块组而产生的多个记录摘要值以及 (ii) 基于所述多个记录摘要值的一些或者全部而产生的记录签名数据，该数据处理装置包括 ：

使用部件，用于使用所述数字作品 ；

检测部件，用于检测引起对所述数字作品的验证的执行的触发；

选择部件，用于在所述检测部件检测到所述触发时，在每次回放所述数字作品时从所述多个数据块组中随机地选择预定数量的数据块组，所述预定数量小于所有所述多个数据块组的数量；

计算部件，用于基于被选数据块组来计算一个或多个计算摘要值；

读取部件，用于从所述多个记录摘要值中读取不包括与所计算出的计算摘要值对应的记录摘要值的多个剩余记录摘要值；

签名验证部件，用于通过利用所述记录签名数据、所述多个计算摘要值以及所述多个剩余记录摘要值，验证所述数字作品是否有效；以及

使用控制部件，用于当所述签名验证部件判定所述数字作品无效时，停止所述使用部件使用所述数字作品；其中

所述记录介质在其上记录多个主记录摘要值，所述多个主记录摘要值中的每个是对应多个数据块中之一而产生的，

在所述记录介质上记录的所述多个记录摘要值中的每个是根据 (i) 预定数目的主记录摘要值和 (ii) 预定数目的数据块标识符而二次产生的摘要值，所述预定数目的主记录摘要值是相对于包括预定数目的数据块的每个数据块组而产生的，以及

所述计算部件根据多个被选数据块中的每个计算主计算摘要值，并且通过对所计算出的主计算摘要值、与在包括所述多个被选数据块的同一数据块组中所包括的不同数据块对应的主记录摘要值、和对应于每一个摘要值的所述预定数目的数据块标识符执行操作来二次计算所述计算摘要值。

17. 如权利要求 16 所述的数据处理装置，其中

所述检测部件具有用于测量自所述记录介质被加载后的经过时间的功能，以及

当所述经过时间满足预定条件时，所述检测部件判定执行对所述数字作品的验证。

18. 一种数据处理装置中使用的数据处理方法，该数据处理装置用于使用记录介质上记录的数字作品，该记录介质还在上面记录了 (i) 基于构成所述数字作品的多个数据块组而产生的多个记录摘要值以及 (ii) 基于所述多个记录摘要值的一些或者全部而产生的记录签名数据，该数据处理方法包括：

(a) 使用所述数字作品；

(b) 检测引起对所述数字作品的验证的执行的触发；

(c) 在检测步骤 (b) 中检测到所述触发时，在每次回放所述数字作品时从所述多个数据块组中随机地选择预定数量的数据块组，所述预定数量小于所有所述多个数据块组的数量；

(d) 基于被选数据块组来计算一个或多个计算摘要值；

(e) 从所述多个记录摘要值中读取不包括与所计算出的计算摘要值对应的记录摘要值的多个剩余记录摘要值；

(f) 通过利用所述记录签名数据、所述多个计算摘要值以及所述多个剩余记录摘要值，验证所述数字作品是否有效；以及

(g) 当步骤 (f) 中判定所述数字作品无效时，停止步骤 (a) 使用所述数字作品；其中

所述记录介质在其上记录多个主记录摘要值，所述多个主记录摘要值中的每个是对应

多个数据块中之一而产生的，

在所述记录介质上记录的所述多个记录摘要值中的每个是根据 (i) 预定数目的主记录摘要值和 (ii) 预定数目的数据块标识符而二次产生的摘要值，所述预定数目的主记录摘要值是相对于包括预定数目的数据块的每个数据块组而产生的，以及

所述计算部件根据多个被选数据块中的每个计算主计算摘要值，并且通过对所计算出的主计算摘要值、与在包括所述多个被选数据块的同一数据块组中所包括的不同数据块对应的主记录摘要值、和对应于每一个摘要值的所述预定数目的数据块标识符执行操作来二次计算所述计算摘要值。

19. 一种数据处理装置，用于使用记录介质上记录的数字作品，该记录介质还在上面记录了 (i) 基于构成所述数字作品的多个数据块组而产生的多个记录摘要值以及 (ii) 基于所述多个记录摘要值的一些或者全部而产生的记录签名数据，该数据处理装置包括：

使用部件，用于使用所述数字作品；

选择部件，用于在每次回放所述数字作品时从所述记录介质被加载时开始，按照固定的时间间隔从所述多个数据块组中随机地选择预定数量的数据块组，所述预定数量小于所有所述多个数据块组的数量；

计算部件，用于基于被选数据块组来计算一个或多个计算摘要值；

读取部件，用于从所述多个记录摘要值中读取不包括与所计算出的计算摘要值对应的记录摘要值的多个剩余记录摘要值；

签名验证部件，用于通过利用所述记录签名数据、所述多个计算摘要值以及所述多个剩余记录摘要值，验证所述数字作品是否有效；以及

使用控制部件，用于当所述签名验证部件判定所述数字作品无效时，停止所述使用部件使用所述数字作品；其中

所述记录介质在其上记录多个主记录摘要值，所述多个主记录摘要值中的每个是对应多个数据块中之一而产生的，

在所述记录介质上记录的所述多个记录摘要值中的每个是根据 (i) 预定数目的主记录摘要值和 (ii) 预定数目的数据块标识符而二次产生的摘要值，所述预定数目的主记录摘要值是相对于包括预定数目的数据块的每个数据块组而产生的，以及

所述计算部件根据多个被选数据块中的每个计算主计算摘要值，并且通过对所计算出的主计算摘要值、与在包括所述多个被选数据块的同一数据块组中所包括的不同数据块对应的主记录摘要值、和对应于每一个摘要值的所述预定数目的数据块标识符执行操作来二次计算所述计算摘要值。

未授权内容检测系统

[0001] 本申请是 2005 年 3 月 24 日提交的、申请号为 200580017845.0、名称为“未授权内容检测系统”的申请的分案申请。

技术领域

[0002] 本发明涉及验证内容有效性的技术，特别涉及减小这种验证中牵涉到的处理负荷的技术。

背景技术

[0003] 防止涉及内容的非法复制、伪造和替换的欺骗状况的手段包括：应用签名信息，表明内容是由合法权利持有人颁发的；以及与内容一起分发验证信息，用于验证内容中是否包括其中已经进行了伪造之类的未授权内容。

[0004] 作为这种手段的一个实例，专利文献 1 公开了通过在网络上分发签名信息、验证信息和内容，验证内容有效性的一种技术。根据这种技术，在内容的发送之前将鉴别信息发送给执行装置，其中的鉴别信息包括发送源的签名信息和验证信息，这里的验证信息用于检查构成内容的各个部分内容的一致性。接收鉴别信息的时候，执行装置验证其中包括的签名信息。如果签名信息的验证成功，执行装置就接收和播放内容。与这一回放并行，执行装置利用验证信息重复各个部分内容的一致性的验证，当验证失败的时候，停止回放。

[0005] 即使执行装置已经收到了包括未授权内容的内容，这种技术也允许执行装置不开始回放这些内容，或者在回放过程中停止回放。

[0006] [专利文献 1] 美国专利出版物第 6480961 号；

[0007] [专利文献 2] 日本专利申请公开出版物第 2002-281013 号；

[0008] [非专利文献 1]http://positron.jfet.org/dvdvideo.html(2004 年 5 月 17 日访问的)；

[0009] [非专利文献 2]http://www.pioneer.co.jp/crdl/tech/mpeg/1.html(2004 年 5 月 17 日访问的)

[0010] [非专利文献 3]“The Art of Computer Programming Vol.2Seminumerical Algorithms”，Donald E.Knuth 著，ISBN：0-201-03822-6；以及

[0011] [非专利文献 4]“Joho Security(Information Security)”，AtsukoMiyaji 和 Hiroaki Kikuchi 编著，日本信息处理协会汇编。

发明内容

[0012] [本发明要解决的问题]

[0013] 但是，根据上面描述的传统技术，执行装置必须与回放并行地连续验证验证信息，因此存在执行装置的处理负荷在内容回放期间变高的问题。

[0014] 此外，从安全性的角度看，常常是分发编码内容而不是内容。在这种情况下，执行装置也必须并行地进行解密处理，因此处理负荷增加得更多。

[0015] 因此，处理装置必须配备用于并行地进行这些处理的高性能处理器。

[0016] 通过减少处理装置在内容回放期间的处理负荷，本发明能够解决这些问题，并且本发明的目的在于提供实现无障碍内容回放的一种数据处理装置、一种数据处理方法、一种数据处理程序和一种记录介质，即使配备的处理器性能不高。

[0017] [解决问题的手段]

[0018] 为了实现上述目的，本发明的数据处理装置使用记录介质上记录的数字作品，该记录介质还在上面记录了(i)从构成所述数字作品的多个数据块产生的多个记录摘要值以及(ii)在所述多个记录摘要值的一些或者全部的基础之上产生的记录签名数据，该数据处理装置包括：使用部件，用于使用所述数字作品；

[0019] 选择部件，用于从所述多个数据块随机地选择预定数量的数据块；计算部件，用于关于所述多个被选数据块的每一个计算计算摘要值；读取部件，用于从所述多个记录摘要值读取多个剩余的记录摘要值，这些剩余的记录摘要值的每一个都与所述多个未被选数据块之一对应；签名验证部件，通过利用所述记录签名数据、所述多个计算摘要值以及所述多个剩余的记录摘要值，用于验证所述数字作品是否有效；以及使用控制部件，当所述签名验证部件判定所述数字作品无效的时候，用于停止所述使用部件使用所述数字作品。

[0020] [本发明的有益效果]

[0021] 按照以上结构，本发明的数据处理装置的选择部件从所述多个数据块选择预定数量的数据块。计算部件从所述多个被选数据块计算多个计算摘要值，同时签名验证部件通过利用计算出来的所述多个计算摘要值，从所述记录介质读出的记录签名数据和所述剩余的记录签名数据，验证所述数字作品的有效性。因此，通过将要新计算的计算摘要值限制为预定数量，能够减少记录签名数据的验证中涉及到的处理负荷。

[0022] 另外，选择单元进行的选择是随机的。因此，每次进行验证的时候，不同的数据块会成为验证目标，所以能够在某种程度上弥补将用于验证的数据块的数量限制为预定数所引起的验证准确度的下降。更进一步，第三方很难预测将选择哪些数据块，这样就能够防止只是伪造或者替换验证未授权信息不使用的数字作品一部分的欺骗行为。

[0023] 在本发明的数据处理装置中，所述多个记录摘要值可以包括多个主记录摘要值，这些主记录摘要值中的每一个都是为所述多个数据块之一产生的，还包括从所述多个主记录摘要值中的两个或者更多个产生的多个次记录摘要值，并且所述记录签名数据可以通过对所述多个次记录摘要值进行数字签名来产生。所述读取部件可以从所述多个主记录摘要值读取所述多个剩余的记录摘要值。所述签名验证部件通过在所述多个计算摘要值和所述多个剩余的记录摘要值的基础之上计算一个或者更多个次计算摘要值，并且利用所述记录签名数据、所述多个次记录摘要值和所述多个次计算摘要值进行数字签名验证，来验 证所述数字作品的有效性。

[0024] 按照上述结构，所述多个记录摘要值包括多个第一记录摘要值和多个第二记录摘要值。所述签名验证部件在所述多个计算摘要值和所述多个剩余的记录摘要值的基础之上计算一个或者更多个第二计算摘要值。因此，所述读取单元只读取计算所述第二计算摘要值所需要的多个第一记录摘要值，以及不与多个被选数据块对应的多个第二摘要值。这样，有可能减少从记录介质读取的记录摘要值的总数。

[0025] 在本发明的数据处理装置里，所述数字作品可以包括多个文件，所述多个文件中

的每一个都与所述多个次记录摘要值之一相对应，并且由所述多个数据块中的两个或者更多个构成。所述多个次记录摘要值中的每一个都可以通过使用多个主记录摘要值产生，所述多个主记录摘要值与构成一个文件的所述多个数据块中的两个或者更多个一一对应，该文件与所述次记录摘要值相对应。所述签名验证部件包括：主读取子部件，用于从所述记录介质读取所述记录签名数据；计算子部件，用于关于包括所述多个被选数据块中至少一个的每一个文件，通过利用所述文件中包括的所述多个未被选中的数据块相对应的多个主记录摘要值，以及与所述多个被选数据块相对应的所述多个计算摘要值，计算次计算摘要值；次读取子部件，用于关于不包括所述多个被选数据块中任何一个的每个文件，读取与所述文件相对应的次记录摘要值；签名子部件，通过利用所述多个计算出来的次计算摘要值和所述读取的多个次记录摘要值进行所述数字签名，用于产生计算签名数据；以及比较子部件，用于将所述计算签名数据与所述记录签名数据进行比较。当所述计算签名数据和所述记录签名数据互相一致的时候，所述签名验证部件可以验证所述数字作品是有效的，当所述计算签名数据和所述记录签名数据不一致的时候，判定所述数字作品无效。

[0026] 按照上述结构，所述读取部件关于包括所述多个被选数据块的至少一个的每个文件，读取与所述文件中包括的所述多个未被选数据块相对应的多个第一记录摘要值。另一方面，所述签名验证部件中的第二读取子部件关于不包括所述多个被选数据块中任何一个的每个文 件，从所述记录介质读取与所述文件相对应的第二记录摘要值。因此，能够减少从所述记录介质读取的记录摘要值的总数。更进一步，通过在所述多个第二记录摘要值和所述多个第二计算摘要值的基础之上产生计算签名数据，并且将所产生的计算签名数据与所述记录签名数据进行比较，能够轻松地验证数字作品的有效性。

[0027] 在本发明的所述的数据处理装置中，所述多个记录摘要值可以是多个散列值，每一个散列值都是由一个散列函数产生的。所述计算部件产生的所述多个计算摘要值可以是通过将所述散列函数应用于所述多个被选数据块中的每一个计算出来的多个散列值。所述计算子部件计算出来的所述多个次计算摘要值可以是通过将所述散列函数应用于与所述多个未被选中的多个数据块相对应的所述多个主记录摘要值和所述多个计算摘要值计算出来的散列值。

[0028] 按照上述结构，所述多个记录摘要值是由所述散列函数产生的。所述计算部件和所述计算子部件利用所属散列函数来计算所述多个计算摘要值和所述多个第二计算摘要值。

[0029] 由于所述散列函数是一种单向函数，如果用于计算与所述多个被选数据块对应的所述多个第一记录摘要值的所述多个数据块甚至部分地不同于所述多个被选数据块，所述多个第一记录摘要值和所述多个第一计算摘要值互不相同。因此，伪造所述多个被选数据块的时候，所述多个计算摘要值和所述多个第二计算摘要值与所述记录介质上记录的对应的多个第一摘要值和多个第二摘要值一致。因而能够准确地检测所述多个被选数据块的伪造。

[0030] 在本发明的数据处理装置中，所述数字作品可以是多项数字内容，并且所述使用部件通过回放所述多项数字内容来使用所述多项数字内容。

[0031] 按照以上结构，所述使用控制部件停止回放已经被伪造的数字内容。因此能够减少伪造内容的循环。

[0032] 在本发明的数据处理装置中，所述数字作品可以是计算机程序，并且所述使用部件通过对构成所述计算机程序的指令代码进行解码，并按照已解码代码运行来使用所述计算机程序。

[0033] 按照以上结构，所述使用控制部件停止执行已经被伪造的计算机程序。因此，能够防止执行未授权程序产生的负面影响，比如用户数据的破坏和不应该使用的数据的应用。

[0034] 本发明的数据处理装置，代替所述使用控制部件，可以包括警告显示部件，判定所述数字作品为无效的时候，用于显示所述数字作品无效的一个通知。

[0035] 按照上述结构，当所述数字作品被验证为无效的时候，所述警告显示部件据此显示，因此，所述数据处理装置能够通知用户所述记录介质上记录的数字作品是未授权的。因此，用户会清楚记录介质上记录的数字作品是未授权的，并且采取保护措施，比如不将记录介质载入数据处理装置。因此，能够避免使用所述数字作品带来的负面影响。

[0036] 在本发明的所述数据处理装置中，所述记录介质已经另外记录了 (i) 具有已调整数据大小，从而使所述记录介质上的自由空间的容量成为一预定值或者更小的值的多项填充内容以及 (ii) 在所述数字作品的部分或者全部以及所述填充内容的基础之上产生的签名数据。所述数据处理装置进一步包括 :验证部件，用于通过使用所述数字作品、所述多项填充内容和所述签名数据来验证所述数字作品和所述多项填充内容是不是有效。所述使用控制部件用于在所述验证部件判定所述数字作品和所述多项填充内容中的至少一样无效的时候，停止所述使用部件使用所述数字作品。

[0037] 按照以上结构，所述多项填充内容记录在所述记录介质上。如果所述自由空间的容量是预定值，它足够小，或者甚至比所述预定值还小，未授权第三人不能添加未授权信息到所述记录介质上。更进一步，所述数据处理装置不仅验证所述数字作品的有效性，还验证填充内容的有效性。因此，即使伪造了所述多项填充内容的一部分或者全部，所述数据处理装置也会停止所述数字作品的使用。所以，即使按照这种方式分发未授权信息，也能够防止未授权信息的使用。

[0038] 在本发明的数据处理装置中，所述记录介质已经另外记录了 (i) 表明所述记录介质上允许外部装置访问的访问允许区域的区域信息以及 (ii) 在所述数字作品和所述区域信息的一部分或者全部的基础 之上产生的签名数据。所述数据处理装置可以进一步包括 :访问禁止部件，用于基于所述区域信息禁止对所述访问允许区域以外的区域的访问 ;以及验证部件，用于通过使用所述数字作品、所述区域信息和所述签名数据验证所述数字作品和所述区域信息是否有效。所述使用控制部件用于当所述验证部件判定所述数字作品和所述区域信息中的至少一样无效的时候，停止所述使用部件使用所述数字作品。

[0039] 总之，在记录介质中，除了数字作品以外，有时会包括说明使用数字作品的程序的程序文件。按照以上结构，数据处理装置不访问区域信息表明的访问允许区域以外的区域。

[0040] 因此，即使未授权第三人将未授权信息添加到记录介质上的自由空间，并且进一步伪造所述程序文件，从而使用未授权信息，数据处理装置也不会读取未授权信息。

[0041] 另外，由于所述签名数据是在数字作品和区域信息的基础之上产生的，因此使用控制单元能够停止使用部件使用所述数字作品，即使未授权人员伪造了区域信息。这样就能够防止使用未授权信息。

[0042] 在这里，权利要求中的数据处理装置是以下实施例中的一种执行装置。权利要求

中的数据块与第一、第五和第六实施例中的已加密单元相对应，也与第二到第四实施例中的部分内容相对应。

附图说明

[0043] 图 1 是说明第一实施例中未授权内容检测系统结构的结构示意图；

[0044] 图 2 是说明第一实施例的分发装置 1100 的结构的框图；

[0045] 图 3 说明要输入分发装置 1100 的内容 1120 的结构；

[0046] 图 4 说明执行装置信息存储部件 1104 储存的装置标识表 1130 的结构；

[0047] 图 5 说明密钥块生成部件 1103 产生的密钥块 1150 的细节；

[0048] 图 6 说明单元生成部件 (unit generating unit)1105 进行的分裂内容 (split contents) 的产生程序的总的概要；

[0049] 图 7 说明单元生成部件 1105 产生的单元拾取信息 1200 的结构；

[0050] 图 8 说明加密处理部件 1106 进行的加密处理的一部分；

[0051] 图 9 说明加密处理部件 1106 产生的已加密内容 1330 的结构；

[0052] 图 10 说明报头信息生成部件 1107 执行的报头信息 1260 产生程序的总的概要；

[0053] 图 11 说明报头信息生成部件 1107 执行的第一散列表的产生程序；

[0054] 图 12 说明报头信息生成部件 1107 产生的第二散列表的细节；

[0055] 图 13 说明签名信息生成部件 1111 进行的处理；

[0056] 图 14 说明第一实施例的 DVD 1500 储存的信息；

[0057] 图 15 是说明第一实施例的执行装置 1600 的结构的框图；

[0058] 图 16 说明签名信息验证部件 1611 进行的签名信息的验证处理的总的概要；

[0059] 图 17 说明签名信息验证部件 1611 进行的处理的一部分；

[0060] 图 18 说明签名信息验证部件 1611 执行的被替换第一散列表的产生程序；

[0061] 图 19 说明签名信息验证部件 1611 执行的被替换第二散列表的产生程序；

[0062] 图 20 说明签名信息验证部件 1611 进行的签名信息验证；

[0063] 图 21 是说明分发装置 1100 工作状况的流程图；

[0064] 图 22 是说明分发装置 1100 工作状况的流程图（图 21 的继续）；

[0065] 图 23 说明执行装置 1600 执行的签名信息的验证程序；

[0066] 图 24 是说明执行装置 1600 的工作状况的流程图；

[0067] 图 25 是说明执行装置 1600 的工作状况的流程图（图 24 的继续）；

[0068] 图 26 是说明第一实施例的变型中执行装置 1100b 的结构的框图；

[0069] 图 27 是说明第二实施例中分发装置 2100 的结构的框图；

[0070] 图 28 说明要输入分发装置 2100 的内容 2120 和多则标识信息；

[0071] 图 29 说明选择部件 2105 所作处理的总的概要；

[0072] 图 30 说明报头信息生成部件 2107 产生的被选位置信息 2160 的结构；

[0073] 图 31 说明报头信息生成部件 2107 产生的报头信息 2200 的结构；

[0074] 图 32 说明加密处理部件 2109 产生的已加密内容的结构；

[0075] 图 33 说明第二实施例的 DVD 2500 上记录的信息；

[0076] 图 34 是说明第二实施例的执行装置 2600 的结构的框图；

[0077] 图 35 是说明分发装置 2100 的工作状况的流程图；

[0078] 图 36 是说明执行装置 2600 的工作状况的流程图；

[0079] 图 37 是说明第三实施例的分发装置 3100 的结构的框图；

[0080] 图 38 说明报头信息生成部件 3107 产生的报头选择信息 3130 的结构；

[0081] 图 39 说明第三实施例的 DVD 3500 上记录的信息；

[0082] 图 40 是说明第三实施例的执行装置 3600 的结构的框图；

[0083] 图 41 是说明第四实施例的分发装置 4100 的结构的框图；

[0084] 图 42 说明部分内容产生部件 4105 产生的分裂内容和多则标识信息；

[0085] 图 43 说明报头信息生成部件 4107 产生的内容位置信息 4140 的结构；

[0086] 图 44 说明报头信息生成部件 4107 产生的报头信息 4160 的结构；

[0087] 图 45 说明第四实施例的 DVD 4500 上记录的信息；

[0088] 图 46 是说明第四实施例的执行装置 4600 的结构的框图；

[0089] 图 47 说明选择部件 4611 执行的被选位置信息 4620 的产生程序的总的概要；

[0090] 图 48 说明选择部件 4611 执行的被选报头信息 4630 的产生程序的总的概要；

[0091] 图 49 说明部分内容解密部件 4616 执行的解密处理的总的概要；

[0092] 图 50 是说明分发装置 4100 的工作状况的流程图；

[0093] 图 51 说明分发装置 4100 执行的签名信息 4170 的产生程序；

[0094] 图 52 是说明执行装置 4600 的工作状况的流程图；

[0095] 图 53 是说明执行装置 4600 的工作状况的流程图（图 52 的继续）；

[0096] 图 54 说明执行装置 4600 执行的签名信息和报头信息的验证程序；

[0097] 图 55 是说明第五实施例的分发装置 5100 的结构的框图；

[0098] 图 56 说明填充内容生成部件 5108 产生的分裂填充内容 5120 的结构；

[0099] 图 57 说明填充内容生成部件 5108 输出的单元拾取信息 5140 的结构；

[0100] 图 58 说明报头信息生成部件 5107 执行的报头信息 5109 产生程序的总的概要；

[0101] 图 59 说明报头信息生成部件 5107 产生的第二散列表 5180 的结构；

[0102] 图 60 说明第五实施例的 DVD 5500 上记录的信息；

[0103] 图 61 是说明第五实施例的执行装置 5600 的结构的框图；

[0104] 图 62 是说明分发装置 5100 的工作状况的流程图；

[0105] 图 63 是说明分发装置 5100 的工作状况的流程图（图 62 的继续）；

[0106] 图 64 是说明执行装置 5600 的工作状况的流程图；

[0107] 图 65 说明预想的未授权 DVD 5500b；

[0108] 图 66 说明预想的未授权 DVD 5500c；

[0109] 图 67 是说明第六实施例的分发装置 6100 的结构的框图；

[0110] 图 68 说明分配产生部件 6108 产生的写入分配信息 6120；

[0111] 图 69 说明第六实施例的 DVD 6500 上记录的信息；

[0112] 图 70 是说明第六实施例的执行装置 6600 的结构的框图；以及

[0113] 图 71 说明 DVD 1500 的配置和获取部件 1601 的结构。

具体实施方式

[0114] 1. 第一实施例

[0115] 下面将在附图的帮助下描述未授权内容检测系统 1，作为本发明的实施例的一个实例。

[0116] 1.1 未授权内容检测系统 1

[0117] 如图 1 所示，未授权内容检测系统 1 包括分发装置 1100、执行装置 1600 和监视器 1620。

[0118] 分发装置 1100 是一个例如内容的合法版权持有人拥有的包括视频和音频的装置。根据操作员执行的操作，分发装置 1100 获取内容，并且通过对获取的内容加密产生已加密内容。另外，分发装置 1100 利用这些内容产生各种信息。分发装置 1100 产生的信息包括例如执行装置 1600 用于验证内容中是否包括未授权内容的时候使用的报头信息。此外，分发装置 1100 利用专用于它自己的签名密钥产生签名信息，并且将产生的已加密内容、签名信息、报头信息之类写在 DVD（数字多功能盘）1500 上。

[0119] 通过分发渠道将 DVD 1500 销售或者分发给用户。

[0120] 装载了 DVD 1500 的时候，执行装置 1600 从装载的 DVD 1500 读取签名信息、报头信息之类，并且基于从 DVD 1500 读取的信息，进行读取的签名信息的验证以及是否包括未授权内容的验证。

[0121] 只有当签名信息的验证成功的时候，执行装置 1600 才开始回放这些内容。

[0122] 下面详细介绍组成未授权内容检测系统 1 和 DVD 1500 的各个装置。

[0123] 1.2 分发装置 1100

[0124] 如图 2 所示，分发装置 1100 包括输入部件 1101、内容密钥生成部件 1102、密钥块生成部件 1103、执行装置信息存储部件 1104、单元生成部件 1105、加密处理部件 1106、报头信息生成部件 1107、签名信息生成部件 1111、签名密钥存储部件 1112 和记录部件 1114。

[0125] 1.2.1 输入部件 1101

[0126] 输入部件 1101 根据操作员的操作从外部装置或者外部记录介质接收内容。在这里利用图 3 介绍输入部件 1101 接收的内容的结构。

[0127] 如图 3 所示，输入部件 1101 收到的内容 1120 包括 c 个文件（c 是 1 或更大的整数）CNT1 1121、CNT2 1122、CNT3 1123、……、CNTc 1124。在这里，输入部件 1101 获得的内容 1120 是对于执行装置 1600 来说可播放格式的（如同后面将详细介绍的一样），DVD 视频格式和 MPEG-2（运动图像专家组 2）格式都是这种可播放格式的实例。描述本实施例的时候假设内容 1120 是 DVD 视频格式的，所述 文件中的每一个都是 VOB（视频对象）文件。

[0128] 获得内容 1120 的时候，输入部件 1101 指令内容密钥生成部件 1102 产生内容密钥，并且将获得的内容 1120 输出给单元生成部件 1105。

[0129] 1.2.2 内容密钥生成部件 1102

[0130] 由输入部件 1101 指令内容密钥生成部件 1102 产生内容密钥。响应这一指令，内容密钥生成部件 1102 产生一个伪随机数，然后利用产生的这个伪随机数产生 128 比特长度的内容密钥 CK。替换伪随机数，利用例如信号上的噪声可以产生真随机数。非专利文献 3 提供产生随机数的方法细节。另外，可以将不同的方法用来产生内容密钥。

[0131] 随后，内容密钥生成部件 1102 将产生的内容密钥 CK 输出给密钥块生成部件 1103 和加密处理部件 1106。

[0132] 1.2.3 密钥块生成部件 1103 和执行装置信息存储部件 1104

[0133] 执行装置信息存储部件 1104 包括例如 ROM 或者 EEPROM，并且储存如图 4 所示的装置标识表 1130。

[0134] 装置标识表 1130 由 n 个装置标识符和 n 个装置密钥（n 是一个自然数）组成。装置标识符是多则标识信息，每一则标识信息都是专用于允许在 DVD 1500 上读取分发装置 1100 写入的信息并且播放所读取的信息的装置的。与装置标识符一一对应的装置密钥是多则密钥信息，这多则密钥信息分别专用于对应装置标识符表明的各个装置。例如，装置标识符 AID_1 1131 对应于装置密钥 DK_1 1136。

[0135] 密钥块生成部件 1103 从内容密钥生成部件 1102 接收内容密钥 CK，并且产生密钥块。

[0136] 图 5 说明在这一点上产生的密钥块 1150 的一个结构实例。密钥块 1150 由 n 个装置标识符和 n 个已加密内容密钥组成。装置标识符与装置标识表 1130 中包括的装置标识符相同。装置标识符与已加密内容密钥一一对应，并且已加密内容密钥是通过利用对应的装置密钥对内容密钥 CK 应用加密算法 E1 而产生的。例如，装置标识符 AID_11141 与装置标识表 1130 中包括的装置标识符 AID_1 1131 相同，并且对应于已加密内容密钥 Enc(DK_1, CK)1142。已加密内容密钥 Enc(DK_1,CK)1142 是通过利用装置标识表 1130 里包括的装置密钥 DK_1 1136 对内容密钥 CK 进行加密产生的。在以后的说明中，将利用密钥 A 加密明文 B 产生的已加密文本表示为 Enc(A, B)。

[0137] 下面描述产生密钥块 1150 的程序。

[0138] 接收内容密钥 CK 的时候，密钥块生成部件 1103 从执行装置信息存储部件 1104 的装置标识表 1130 读取第一行中的装置标识符 AID_1 1131 和装置密钥 DK_1 1136。密钥块生成部件 1103 通过利用读取的装置密钥 DK_1 1136 对内容密钥 CK 应用加密算法 E1 来产生已加密内容密钥 Enc(DK_1, CK)。在这里，作为一个实例，加密算法 E1 采用了 AES（先进加密标准）。非专利文献 4 提供了 AES 的细节。注意，这里使用的加密系统不限于 AES，而是可以采用不同的系统。

[0139] 密钥块生成部件 1103 储存读取的装置标识符 AID_1 1131 和产生的已加密内容密钥 Enc(DK_1, CK)，并且将这两者互相联系起来。

[0140] 密钥块生成部件 1103 为 n 对装置标识符和装置密钥重复同一种处理，产生 n 对装置标识符和已加密内容密钥，并且将这些对放在一起形成密钥块 1150。

[0141] 接下来，密钥块生成部件 1103 将产生的密钥块 1150 输出给记录部件 1114。

[0142] 在这里，作为最简单的实例，描述了将专用密钥赋予用于播放写入 DVD 1500 的信息的每个装置这种情况。但是专利文献 2 公开的技术包括减少已加密内容密钥的数量和防止专用装置播放这些内容的那一些技术。

[0143] 1.2.4 单元生成部件 1105

[0144] 单元生成部件 1105 从输入部件 1102 接收内容 1120。接收内容 1120 的时候，单元生成部件 1105 在下面描述的程序里产生分裂内容和单元拾取信息。

[0145] 下面描述的是：分裂内容产生 (a)；和单元拾取信息产生 (b)。

[0146] (a) 分裂内容的产生

[0147] 如图 6 所示，单元生成部件 1105 从内容 1120 产生分裂内容 1160。下面在图 6 的

帮助下描述用于产生分裂内容 1160 的程序。

[0148] 接收内容 1120 的时候，单元生成部件 1105 产生与收到的内容 1120 中包括的文件 CNT1 1121 对应的一个文件标识符 FID1 1161 和一则文件标识信息 AD1。文件标识符 FID1 1161 是唯一地表明文件 CNT1 1121 的标识信息，并且是例如表明内容 1120 中文件 CNT 1121 顺序的自然数或者文件的名称。这一则文件标识信息 AD1 是用于标识文件 CNT1 1121 的信息，并且是例如从内容 1120 的首部开始算起的偏移、扇区号或者地址。

[0149] 下一步，单元生成部件 1105 关于每个 VOBU（视频对象单元）分裂文件 CNT1 1121，产生 m 个单元 U1_1、U1_2、……、U1_m(m 是一个任意自然数）。然后，单元生成部件 1105 产生单元数 N1，它表明产生的单元的数量（在这里 N1 ＝ m)。

[0150] 下一步，单元生成部件 1105 产生由文件标识符 FID1 1161、文件标识信息 AD1 和单元数 N1 组成的文件信息，并且将产生的文件信息储存起来。

[0151] 然后，单元生成部件 1105 为各个单元产生单元标识符。这些单元标识符是多则标识信息，每一则信息都唯一地标识 m 个单元中的一个，并且可以是例如从首部单元开始的序数，象 1、2、3、……、m，或者可以是从首部单元开始的累计比特数。在本实施例中，假设单元标识符是从首部单元开始的序数。在以下说明中，将一对对应的单元标识符和单元叫做一则单元信息，而将 m 则单元信息统一叫做分裂文件 (split file)。这样，从文件 CNT1 1121 产生的分裂文件 splCNT1 1171 由图 6 所示的 m 则单元信息 1191、1192、1193、……、1194 组成。每一则单元信息都由对应的单元标识符和单元组成。例如，一则单元信息 1191 包括单元标识符 UID1_1 1181 和单元 U1_11186。

[0152] 下一步，单元生成部件 1105 产生包括文件标识符 FID1 1161 和分裂文件 splCNT1 1171 的分裂文件信息 1176。

[0153] 单元生成部件 1105 针对所有文件重复同一种处理，以产生 c 则文件信息和 c 则分裂文件信息 1176、1177、1178、……、1179。在这里，产生的 c 则分裂文件信息一起叫做分裂内容 1160。注意，对于不 同的文件，产生的单元的数量 m 可能不同。

[0154] 下一步，单元生成部件 1105 将产生的分裂内容 1160 输出给加密处理部件 1106。

[0155] 注意，这里的单元生成部件 1105 产生文件标识符和文件标识信息，但是，这些东西可以和内容 1120 一起从外部输入。

[0156] 另外，各个文件是关于每个 VOBU 分裂的，但是，分裂单元不限于此。例如，可以将每个文件每 64kB 分裂一次，或者将对应于一秒钟回放时间的每一部分分裂一次。也可以设计成让操作员输入表明分裂单位 (split unit) 的信息。

[0157] (b) 单元拾取信息的产生

[0158] 在完成了分裂内容 1160 的输出以后，单元生成部件 1105 产生由 c 则文件信息组成的单元拾取信息。图 7 说明在这一点产生的单元拾取信息 1200 的结构。

[0159] 单元拾取信息 1200 由 c 则文件信息 1201、1202、……、1204 组成。每一则文件信息都由文件标识符、一则文件标识信息和单元数组成。

[0160] 作为一个实例，一则文件信息 1201 包括文件标识符 FID1 1211、一则文件标识信息 AD1 1216 和单元数 N1 1221。

[0161] 单元生成部件 1105 将产生出来的单元拾取信息 1200 输出给签名信息生成部件 1111 和记录部件 1114。

[0162] 1.2.5 加密处理部件 1106

[0163] 加密处理部件 1106 从内容密钥生成部件 1102 接收内容密钥 CK，并且从单元生成部件 1105 接收分裂内容 1160。

[0164] 图 8 说明加密处理部件 1106 进行的处理的一部分。下面在图 8 的帮助下描述加密处理部件 1106 进行的处理。

[0165] 接收分裂内容 1160 的时候，加密处理部件 1106 选择由收到的分裂内容 1160 组成的分裂文件信息 1176 中包括的分裂文件 splCNT11171。加密处理部件 1106 从选中的分裂文件 splCNT1 1171 的单元信息 1191 的首部则 (head piece) 提取单元 U1_1 1186，并且通过利用内容密钥 CK 将加密算法 E1 应用于提取出来的 U1_1 1186 来产生已 加密单元 EU1_1 1231。在这里，EU1_1 = Enc(CK, U1_1)。

[0166] 加密处理部件 1106 产生由单元信息 1191 中包括的产生出来的已加密单元 EU1_1 1231 和单元标识符 UID1_1 1181 组成的已加密单元信息 1241。在以下说明中，一对对应单元标识符和已加密单元指的是一则已加密单元信息。

[0167] 加密处理部件 1106 为单元信息 1192、1193、……、1194 的其余部分重复相同样的处理，产生对应则已加密单元信息 1242、1243、……、1244。在这里，将从一个分裂文件产生的 m 则已加密单元信息统称为已加密分裂文件。

[0168] 如图 8 所示，在上述程序中从分裂文件 splCNT1 1171 产生的已加密分裂文件 EsplCNT1 1251 由 m 则已加密单元信息 1241、1242、1243、 ……、1244 组成。每一则已加密单元信息都是在分裂文件 1171 组成的一则单元信息的基础之上产生的，并且包括单元标识符和已加密单元。例如，已加密单元信息 1241 是在单元信息 1191 的基础之上产生的，并且包括单元标识符 UID1_1 1181 和已加密单元 EU1_11231。

[0169] 下一步，加密处理部件 1106 从产生的已加密分裂文件 EsplCNT11251 组成的每一则已加密单元信息提取已加密单元。在这里，将 m 个已提取的已加密单元统称为已加密文件 ECNT1。

[0170] 然后，加密处理部件 1106 通过利用产生出来的已加密分裂文件 EsplCNT1 1251 替换分裂文件信息 1176 中包括的分裂文件 splCNT11171，产生已加密分裂文件信息。

[0171] 加密处理部件 1106 对这些则分裂文件信息 1177、1178、……、1179 进行同样的处理，产生已加密分裂文件信息和已加密文件。

[0172] 将在这一点产生的 c 则已加密分裂文件信息统称为已加密分裂内容。然后，加密处理部件 1106 将产生的已加密分裂内容输出给报头信息生成部件 1107。图 10 说明这里输出的已加密分裂内容 1210 的结构。

[0173] 下一步，加密处理部件 1106 将 c 个已加密文件作为已加密内容输出给记录部件 1114。图 9 说明这里产生的已加密内容 1330 的结构。 已加密内容 1330 由 c 个已加密文件 ECNT1 1331、ECNT2 1332、ECNT3 1333、……、ECNTc 1334 组成。这些已加密文件中的每一个都是在已加密分裂内容中包括的已加密分裂文件的基础之上产生的，并且包括多个已加密单元。作为一个实例，已加密文件 ECNT1 1331 包括已加密单元 EU1_1、EU1_2、……

[0174] 1.2.6 报头信息生成部件 1107

[0175] 报头信息生成部件 1107 从加密处理部件 1106 接收已加密分裂内容 1210。接收已加密分裂内容 1210 的时候，报头信息生成部件 1107 利用收到的如图 10 所示的已加密分裂

内容产生报头信息 1260。

[0176] 图 10 说明报头信息生成部件 1107 执行的报头信息 1260 的产生程序的概要。报头信息生成部件 1107 收到的已加密分裂内容 1210 由 c 则已加密分裂文件信息 1246、1247、1248、……、1249 组成。每一则已加密分裂文件信息都包括文件标识符和已加密分裂文件。例如，一则已加密分裂文件信息 1246 包括文件标识符 FID1 1161 和已加密分裂文件 EsplCNT1 1251。

[0177] 报头信息生成部件 1107 在已加密分裂文件信息 1246 中包括的每一分裂文件的基础之上产生第一散列表。例如，报头信息生成部件 1107 在已加密分裂文件 EsplCNT1 1251 的基础之上产生第一散列表 HA1TBL1 1261。报头信息生成部件 1107 从产生出来的 c 个第一散列表产生第二散列表 HA2TBL 1269。

[0178] 下面详细描述第一和第二散列表的上述产生程序。

[0179] 1.2.6.1 第一散列表的产生

[0180] 图 11 说明报头信息生成部件 1107 执行的第一散列表 HA1TBL11261 的产生程序的概要。

[0181] 下面在图 11 的帮助下描述第一散列表 HA1TBL1 1261 的产生程序。所有第一散列表 HA1TBL2、HA1TBL3、……、HA1TBLc 的产生程序都与第一散列表 HA1TBL1 1261 的相同。

[0182] 首先，报头信息生成部件 1107 从已加密分裂文件 Esp1CNT1 1251 组成的首部已加密单元信息 1241 提取已加密单元 EU1_1 1231，并且通过将提取出来的已加密单元 EU1_1 1231 赋予散列函数来产生单元 散列值 UHA1_1 1271。

[0183] 在这里，将利用块密码 (block cipher) 的 SHA-1(安全散列算法 -1) 或者 CBC-MAC(密码块链接消息鉴别码，Cipher BlockChaining-Message Authentication Code) 应用于上述散列函数。

[0184] 在这里，报头信息生成部件 1107 通过利用产生出来的单元散列值 UHA1_1 1271 替换已加密单元信息 1241 的已加密单元 EU1_1 1231 来产生单元散列信息 1281。

[0185] 报头信息生成部件 1107 为已加密单元信息 1242、1243、……、1244 的其余部分重复同样的处理来产生对应则单元散列信息 1282、1283、……、1284。将这一点产生的 m 则单元散列信息统称为第一散列表 HA1TBL1 1261。图 11 说明这一点产生的第一散列表 HA1TBL1 1261 的结构。

[0186] 1.2.6.2 第二散列表的产生

[0187] 报头信息生成部件 1107 重复以上程序。在完成了从已加密分裂内容 1210 产生上述 c 个第一散列表以后，报头信息生成部件 1107 从产生出来的 c 个第一散列表产生图 12 所示的第二散列表 1269。第二散列表 HA2TBL 1269 由 c 则文件散列信息 1301、1302、1303、……、1304 组成，每一则文件散列信息都包括文件标识符和文件散列值。作为一个实例，一则文件散列信息 1301 包括文件标识符 FID1 1161 和文件散列值 FHA1 1291。

[0188] 下面描述第二散列表 1269 的产生程序。

[0189] 报头信息生成部件 1107 通过将组成所产生的第一散列表 HA1TBL1 1261 的全部单元标识符和单元散列值组合起来形成的组合结果赋予散列函数来产生文件散列值 FHA1 1291。

[0190] 接下来，报头信息生成部件 1107 从对应于第一散列表 HA1TBL11261 的已加密分裂

文件信息 1246 提取文件标识符 FID1 1161，并且产生提取的文件标识符 FID1 1161 和产生的文件散列值 FHA1 1291 组成的文件散列信息 1301。

[0191] 报头信息生成部件 1107 为第一散列表 1262、1263、……、1264 重复同样的处理，分别产生所述则文件散列信息 1302、1303、……、1304。

[0192] 下一步，报头信息生成部件 1107 将产生出来的这些 c 则第一散列信息放到一起形成第二散列表 HA2TBL 1269。

[0193] 这样就完成了对第一散列表 (1.2.6.1) 和第二散列表 (1.2.6.2) 的产生程序的描述。报头信息生成部件 1107 产生包括在上述程序中产生的 c 个第一散列表和单个第二散列表 HA2TBL 1269 的报头信息 1260，并且将产生出来的报头信息 1260 输出给记录部件 1114。

[0194] 更进一步，报头信息生成部件 1107 将产生出来的第二散列表 HA2TBL 1269 输出给签名信息生成部件 1111。

[0195] 1.2.7 签名信息生成部件 1111 和签名密钥存储部件 1112

[0196] 由 ROM 组成的签名密钥存储部件 1112 储存分发装置 1100 专用的签名密钥 1113。

[0197] 图 13 说明签名信息生成部件 1111 的工作情况的概要。下面在图 13 的帮助下描述签名信息生成部件 1111 进行的签名信息的产生。

[0198] 从报头信息生成部件 1107 接收第二散列表 HA2TBL 1269 的时候，签名信息生成部件 1111 从单元生成部件 1105 接收单元拾取信息 1200。接收单元拾取信息 1200 和第二散列表 1269 的时候，签名信息生成部件 1111 从签名密钥存储部件 1112 读取签名密钥 1113。

[0199] 接下来，签名信息生成部件 1111 利用读取出来的签名密钥 1113 从收到的单元拾取信息 1200 和第二散列表 1269 产生签名信息 1310。更加具体地说，签名信息生成部件 1111 利用读取出来的签名密钥 1113，将签名生成算法 S 应用于组合收到的第二散列表 1269 中包括的 c 个文件散列值和单元拾取信息 1200 中包括的 c 个文件信息得到的组合起来的结果。

[0200] 作为一个实例，为签名生成算法 S 使用 DSA（数字签名算法）。

[0201] 然后，签名信息生成部件 1111 将产生出来的签名信息 1310 输出给记录部件 1114。

[0202] 1.2.8 记录部件 1114

[0203] 用记录部件 1114 装载 DVD 1500。

[0204] 记录部件 1114 接收：来自密钥块生成部件 1103 的密钥块 1150；来自单元生成部件 1105 的单元拾取信息 1200；来自加密处理部件 1106 的已加密内容 1330；来自报头信息生成部件 1107 的报头信息 1260；以及来自签名信息生成部件 1111 的签名信息 1310。

[0205] 接收上述信息的时候，记录部件 1114 向 DVD 1500 写入收到的密钥块 1150、单元拾取信息 1200、报头信息 1260、签名信息 1310 和已加密内容 1330。

[0206] 1.3DVD 1500

[0207] DVD 1500 是载入执行装置 1600 的可移动光盘介质。

[0208] 如图 14 所示，DVD 1500 储存密钥块 1510、单元拾取信息 1530、报头信息 1550、签名信息 1570 和已加密内容 1580。这些已经被分发装置 1100 写入，并且分别与分发装置 1100 产生的密钥块 1150、单元拾取信息 1200、报头信息 1260、签名信息 1310 和已加密内容 1330 相同。因此，为这些项提供一些简短描述。

[0209] 1.3.1 密钥块 1510

[0210] 密钥块 1510 由 n 个装置标识符 AID_1、AID_2、AID_3、……、AID_n 和分别对应于这 n 个装置标识符的 n 个已加密内容密钥 Enc(DK_1,CK)、Enc(DK_2,CK)、Enc(DK_3,CK)、……、Enc(DK_n,CK) 组成。

[0211] 1.3.2 单元拾取信息 1530

[0212] 单元拾取信息 1530 由 c 则文件信息 1541、1542、……等等组成，每一则文件信息都包括文件标识符、文件标识信息和单元数。各则文件信息都对应于已加密内容 1580 中包括的已加密文件。另外，每一文件都对应于报头信息 1550 中包括的第一散列表。

[0213] 1.3.3 已加密内容 1580

[0214] 已加密内容 1580 由 c 个已加密文件 1581、1582、1583、……、1587 组成。每一个已加密文件都包括多个已加密单元。

[0215] 1.3.4 报头信息 1550

[0216] 报头信息由 c 个第一散列表 1551、1552、……、1557 和第二散列表 1556 组成。

[0217] 每一个第一散列表都由多则单元散列信息组成，每一则单元散列 信息都包括单元标识符和单元散列值。

[0218] 第二散列表 1556 由 c 则文件散列信息 1561、1562、1563、……、1567 组成，每一则文件散列信息都包括文件标识符和文件散列值。

[0219] 1.3.5 签名信息 1570

[0220] 通过将签名生成算法 S 应用于通过组合第二散列表 1556 中包括的 c 个文件散列值和单元拾取信息 1530 中包括的 c 则文件信息形成的组合结果来产生签名信息 1570。

[0221] 1.4 执行装置 1600

[0222] 如图 15 所示，执行装置 1600 由获取部件 1601、内容密钥获取部件 1602、装置密钥存储部件 1604、执行部件 1606、签名信息验证部件 1611 和验证密钥存储部件 1612 组成。

[0223] 1.4.1 获取部件 1601

[0224] 给获取部件 1601 装载 DVD 1500。检测装载在其上的 DVD 1500 的时候，获取部件 1601 从 DVD 1500 读取密钥块 1510、单元拾取信息 1530 和签名信息 1510，并且在输出读取的单元拾取信息 1530 和签名信息 1570 给签名信息验证部件 1611 的时候，输出读取的密钥块 1510 给内容密钥获取部件 1602。

[0225] 另外，获取部件 1601 根据来自执行部件 1606 和签名信息验证部件 1611 的指令从 DVD 1500 读取报头信息 1550 和已加密内容 1580 的全部或部分。

[0226] 1.4.2 内容密钥获取部件 1602 和装置密钥存储部件 1604

[0227] 由 ROM 组成的装置密钥存储部件 1604 储存如图 15 所示的装置标识符 AID_p 1608 和装置密钥 DK_p 1609(p 是等于或小于 n 的一个自然数)。

[0228] 装置标识符 AID_p 1608 是独一无二地表明执行装置 1600 的标识信息，而装置密钥 DK_p 1609 则是专用于执行装置 1600 的密钥信息。

[0229] 内容密钥获取部件 1602 从获取部件 1601 接收密钥块 1510。接收密钥块 1510 的时候，内容密钥获取部件 1602 从装置密钥存储部件 1604 读取装置标识符 AID_p 1608。然后，内容密钥获取部件 1602 检测对应于从收到的密钥块 1510 读取的装置标识符 AID_p 1608 的装置 标识符，并且提取对应于被检测装置标识符的已加密内容密钥。

[0230] 随后，内容密钥获取部件 1602 从装置密钥存储部件 1604 读取装置密钥 DK_p

1609。内容密钥获取部件 1602 通过利用读取的装置密钥 DK_p 1609 将解密算法 D1 应用于被提取的已加密内容密钥来产生内容密钥 CK，然后将产生的内容密钥 CK 输出给执行部件 1606。

[0231] 在这里，解密算法 D1 是用于对加密算法 E1 产生的已加密文本进行解密所使用的算法。

[0232] 1.4.3 签名信息验证部件 1611 和验证密钥存储部件 1612

[0233] 由 ROM 组成的验证密钥存储部件 1612 储存验证密钥 1613。验证密钥 1613 是与分发装置 1100 储存的签名密钥 1113 对应的密钥信息。

[0234] 签名信息验证部件 1611 从获取部件 1601 接收单元拾取信息 1530 和签名信息 1570。

[0235] 图 16 说明签名信息验证部件 1611 执行的签名信息验证操作的概要。接收单元拾取信息 1530 和签名信息 1570 的时候，签名信息验证部件 1611 从收到的单元拾取信息 1530 选择文件标识符的 i 个 (i 是等于或小于 c 的一个自然数)，如图 16 所示。在这里，在假设签名信息验证部件 1611 已经选择了文件标识符 FID1 1531、FID3 1533、……的情况下，提供以下描述。

[0236] 签名信息验证部件 1611 在与被选文件标识符 FID1 1531 对应的第一散列表 HA1TBL1 1551 和已加密文件 ECNT1 1581 的基础之上产生一个被替换第一散列表 REPHA1TBL1 1631。签名信息验证部件 1611 针对其它被选文件标识符 FID3、……、等等进行同样的处理，以产生被替换第一散列表 1633、……、等等。签名信息验证部件 1611 在产生的被替换第一散列表 1631、1633、……、等等和 DVD 1500 中储存的第二散列表 HA2TBL 1556 的基础之上产生被替换第二散列表 REPHA2TBL 1639，并且利用产生的被替换第二散列表 REPHA2TBL 1639 验证签名信息 1570。

[0237] 这就结束了图 16 中所说明的概要。下面在附图的帮助下详细描述：被替换第一散列表的产生 (1.4.3.1)；被替换第二散列表的产生 (1.4.3.2)；以及签名信息的验证程序 (1.4.3.3)。

[0238] 1.4.3.1 被替换第一散列表的产生

[0239] 在图 17 和 18 的帮助下介绍产生被替换第一散列表的程序。

[0240] 如图 17 所示，签名信息验证部件 1611 从收到的单元拾取信息 1530 中包括的 c 则文件信息中选择 i 则 (i 是等于或小于 c 的一个自然数)。选择 i 则的方法是例如产生 i 个伪随机数 (r1、r2、……、ri)，其中的每一个都大于或等于 1，并且小于或等于 c。并且选择第 r1、r2、……、ri 个文件标识符。选择方法不限于这种方法，可以使用任何方法只要很难预测将选中哪些文件标识符。例如，可以使用温度、湿度和电子信号上的噪声等等。

[0241] 在本实施例中，在假设 i ＝ 7，并且选择 7 则文件信息 1541、1543、……、等等的情况下进行以下描述。

[0242] 随后，签名信息验证部件 1611 选择与被选择文件信息 1541 里包括的文件标识符 FID1 相对应的已加密文件 ECNT1 1581 中的已加密单元中的任意一个，并且从 DVD 1500 读取被选已加密单元，如图 18 所示。更加具体地说，签名信息验证部件 1611 读取被选文件信息 1541 里包括的单元数 N1，并且产生伪随机数 t(在这里 t ＝ 3)，它是 N1 或更小。然后，签名信息验证部件 1611 在被选文件信息 1541 中包括的文件标识信息 AD1 的基础之上，通

过获取部件 1601 从 DVD1500 读取已加密单元 EU1_3，它是已加密文件 ENCT1 1581 中的第三已加密单元。

[0243] 下一步，签名信息验证部件 1611 通过将读取的已加密单元 EU1_3 赋予一个散列函数来产生替换单元散列值 H3。在这里，签名信息验证部件 1611 使用与分发装置 1100 的报头信息生成部件 1107 使用的相同的散列函数。

[0244] 下一步，签名信息验证部件 1611 通过获取部件 1601 读取报头信息 1550 中包括的第一散列表 HA1TBL1 1551。

[0245] 然后，签名信息验证部件 1611 利用计算出来的替换单元散列值 H3 替换组成读取的第一散列表 HA1TBL1 1551 的 m 则单元散列信息中，对应于与 t = 3 一致的单元标识符 UID1_3 的单元散列值 UHA1_3。 结果是被替换的第一散列表 REPHA1TBL1 1631。

[0246] 签名信息验证部件 1611 为其它被选则文件信息 1542、……、等等重复同样的处理，以分别产生被替换第一散列表 REPHATBL31633 等等。

[0247] 1.4.3.2 被替换第二散列表的产生

[0248] 下面在图 19 的帮助下描述产生被替换第二散列表的程序。

[0249] 在基于选择的 7 则文件信息完成被替换第一散列表的产生以后，签名信息验证部件 1611 组合组成所产生的被替换第一散列表 REPHA1TBL1 1631 的所有单元标识符、所有单元散列值和被替换散列值，并且通过将组合结果赋予散列函数产生替换文件散列值 fha1。以类似的方式，签名信息验证部件 1611 分别基于被替换第一散列表 1633 REPHA1TBL3、……、等等产生替换文件散列值 fha3、……、等等。

[0250] 下一步，签名信息验证部件 1611 从 DVD 1500 读取报头信息 1550 中包括的第二散列表 HA2TBL 1556。从读取出来的第二散列表 HA2TBL 1556 中包括的 c 则文件散列信息，签名信息验证部件 1611 分别利用产生出来的替换文件散列值 fha1、fha3、……、等等替换包括文件标识符 FID1、FID3、……、等等的文件散列信息的文件散列值，这些文件标识符 FID1、FID3、……、等等包括在被选七则文件信息中。对其进行了这一替换的第二散列表 HA2TBL 1556 是被替换第二散列表 REPHA2TBL 1639。

[0251] 1.4.3.3 签名信息验证

[0252] 下面在图 20 的帮助下描述签名信息验证。

[0253] 在产生了被替换第二散列表 REPHA2TBL 1639 以后，签名信息验证部件 1611 从验证密钥存储部件 1612 读取验证密钥 1613。

[0254] 随后，签名信息验证部件 1611 产生通过将被替换第二散列表 REPHA2TBL 1639 中包括的全部文件散列值和替换文件散列值以及单元拾取信息 1530 中包括的 c 则文件信息组合起来，形成的组合结果，并且通过利用验证密钥 1613 将签名验证算法 V 应用于所产生的组合结果来产生签名验证信息。然后，签名信息验证部件 1611 将产 生的签名验证信息和从获取部件 1601 收到的签名信息 1570 进行比较。当这两者不一致时，签名信息验证部件 1611 判定签名验证不成功，并且输出回放禁止信息给执行部件 1606 表明禁止内容回放。在这里，签名验证算法 V 是用于验证通过利用签名生成算法 S 产生的签名的一个算法。

[0255] 当这两者一致时，签名信息验证部件 1611 结束这一验证处理。

[0256] 1.4.4 执行部件 1606

[0257] 执行部件 1606 从内容密钥获取部件 1602 接收内容密钥 CK。

[0258] 另外，执行部件 1606 还可以从签名信息验证部件 1611 接收回放禁止信息。

[0259] 接收内容密钥 CK 的时候，执行部件 1606 通过获取部件 1601 从 DVD 1500 读取组成已加密内容 1580 的已加密文件 ECNT1。执行部件 1606 利用收到的内容密钥 CK 将解密算法 D1 顺序地应用于组成读取的已加密文件 1581 的已加密单元 EU1_1、EU1_2、……、等等，以产生由单元 U1_1、U1_2、……、等等组成的文件 CNT1。

[0260] 接下来，执行部件 1606 扩展所产生的文件 CNT1 来产生视频和音频数据。执行部件 1606 基于所产生的视频和音频数据产生视频和音频信号，并且将所产生的视频和音频信号输出给监视器 1620。

[0261] 关于已加密文件 ECNT2、……、和 ECNTc，执行部件 1606 用相似的方式重复读出、解密和扩展，以及输出视频和音频信号。

[0262] 如果在重复期间从签名信息验证部件 1611 接收回放禁止信息，执行部件 1606 就退出重复，并通过例如点亮指示灯或者让监视器 1620 显示通知出错的画面来通知用户装载了的 DVD 的不能回放。

[0263] 1.4.5 监视器 1620

[0264] 监视器 1620 有用电缆与执行装置 1600 连接的内置扬声器。

[0265] 监视器 1620 从执行装置 1600 的执行部件 1606 接收视频和音频信号，从收到的图像信号产生画面，并且显示这些画面。另外，监视器 1620 从音频信号产生声音，从扬声器输出产生的声音。

[0266] 1.5 工作状况

[0267] 下面描述分发装置 1100 和执行装置 1600 的工作状况。

[0268] 1.5.1 分发装置 1100 的工作状况

[0269] 下面在图 21 和 22 所示的流程图的帮助下描述分发装置 1100 的工作状况。

[0270] 输入部件 1101 根据操作员进行的操作获得由 c 个文件组成的内容 1120（步骤 S1011），并且指令内容密钥生成部件 1102 产生内容密钥。

[0271] 内容密钥生成部件 1102 用随机数产生内容密钥 CK，将产生出来的内容密钥 CK 输出给密钥块生成部件 1103（步骤 S1012）。

[0272] 密钥块生成部件 1103 接收内容密钥 CK，从执行装置信息存储部件 1104 读取装置标识表 1130（步骤 S1013）。密钥块生成部件 1103 利用收到的内容密钥 CK 和读取的装置标识表 1130 产生密钥块 1150（步骤 S1016）。

[0273] 在步骤 S1017 到 S1023 里，分发装置 1100 的单元生成部件 1105 关于组成内容 1120 的每个文件重复步骤 S1018 到 S1022 的处理。

[0274] 单元生成部件 1105 产生对应于文件的文件标识符和文件标识信息（步骤 S1018）。接下来，单元生成部件 1105 通过分裂文件产生 m 个单元（步骤 S1019），产生表明所产生单元的数量的单元数，并且产生所产生的文件标识符、文件标识信息和单元数组成的文件信息（步骤 S1020）。

[0275] 下一步，单元生成部件 1105 产生与所产生的单元一一对应的单元标识符（步骤 S1021）。接下来，单元生成部件 1105 产生 m 则单元信息，这些信息中的每一则都包括对应的单元标识符和单元，并且将这些则单元信息放在一起形成分裂文件。然后，单元生成部件 1105 产生由分裂文件和文件标识符组成的分裂文件信息（步骤 S1022）。

[0276] 为所有文件以及 c 则分裂文件信息和文件信息的产生重复步骤 S1017 到 S1023 以后，单元生成部件 105 产生由 c 则文件信息组成的单元拾取信息 1200（步骤 S1024），并且将产生的单元拾取信息 1200 输出给签名信息生成部件 1111 和记录部件 1114。另外，单元生成部件 1105 将 c 则分裂文件信息组成的分裂内容 1160 输出给加密处理部件 1106。

[0277] 加密处理部件 1106 从单元生成部件 1105 接收分裂内容 1160，通过利用内容密钥 CK 对组成收到的分裂内容 1160 的各个分裂文件的每一个单元进行加密，来产生已加密分裂内容 1210（步骤 S1026）。

[0278] 下一步，加密处理部件 1106 通过从每一个已加密分裂文件提取已加密单元来产生 c 个已加密文件，并且将这些已加密文件放在一起形成已加密内容 1330（步骤 S1027）。下一步，加密处理部件 1106 在将已加密内容 1330 输出给记录部件 1114 的同时，将已加密分裂内容 1210 输出给报头信息生成部件 1107。

[0279] 报头信息生成部件 1107 从加密处理部件 1106 接收已加密分裂内容 1210。报头信息生成部件 1107 将组成已加密分裂内容 1210 的每一个已加密分裂文件中包括的已加密单元赋予散列函数来计算单元散列值，并且产生 c 个第一散列表（步骤 S1028）。

[0280] 下一步，报头信息生成部件 1107 关于每一个第一散列表基于第一散列表计算文件散列值，并且产生包括 c 个计算出来的文件散列值在内的第二散列表 1269（步骤 S1029）。

[0281] 下一步，报头信息生成部件 1107 产生报头信息 1260，这些报头信息 1260 包括所产生的第二散列表 1269 和 c 个第一散列表（步骤 S1031）。

[0282] 签名信息生成部件 1111 从签名密钥存储部件 1112 读取签名密钥 1113（步骤 S1032），并且通过利用读取的签名密钥 1113，将签名生成算法应用于第二散列表 1269 和单元拾取信息，来产生签名信息（步骤 S1033）。

[0283] 记录部件 1114 将密钥块 1150、单元信息 1200、报头信息 1260、签名信息 1310 和已加密内容 1330 写入 DVD 1500（步骤 S1034）。

[0284] 1.5.2 执行装置 1600 的工作状况

[0285] 图 23 说明签名信息的验证过程中涉及的信息制造处理。为了描述方便，考虑到报头信息 1550，在图中只画出了第一散列表中包括的单元散列值和第二散列表中包括的文件散列值。图 24 和 25 是说明执行装置 1600 工作状况的流程图。注意，图 23 到 25 中相同的步骤编号表示相同的处理。

[0286] 下面在图 23 到 25 的帮助下说明执行装置 1600 的工作状况。

[0287] 装载了 DVD 1500 的时候，获取部件 1601 从 DVD 1500 读取密钥块 1510、单元拾取信息 1530 和签名信息 1570，并且将密钥块 1510 输出给内容密钥获取部件 1602，同时将单元拾取信息 1530 和签名信息 1570 输出给签名信息验证部件 1611（步骤 S1041）。

[0288] 签名信息验证部件 1611 接收单元拾取信息 1530 和签名信息 1570，利用随机数选择单元拾取信息 1530 中包括的 c 个文件标识符中的 i 个（步骤 S1046）。

[0289] 在步骤 S1047 到 S1057 里，签名信息验证部件 1611 关于被选 i 个文件标识符中的每一个重复步骤 S1048 到 S1056 的处理，产生 i 个被替换第一散列表。

[0290] 签名信息验证部件 1611 从单元信息提取与被选文件标识符中的一个对应的单元数（步骤 S1048）。接下来，签名信息验证部件 1611 产生随机数 t，它是 1 或者更大，小于或等于读取的单元数（步骤 S1049）。签名信息验证部件 1611 从单元信息提取与被选文件标

识符对应的一则文件标识信息，并且基于提取的单元标识信息，从 DVD1500 读取与被选文件标识符对应的已加密文件中的第 t 个已加密单元（步骤 S1051）。在图 23 中，每次重复以上处理的时候，签名信息验证部件 1161 都顺序读取：已加密文件 1581 中包括的已加密单元 1511；已加密文件 1583 中包括的已加密单元 1512；……；以及已加密文件 1587 中包括的已加密单元 1513。

[0291] 签名信息验证部件 1611 通过将读取的已加密单元赋予散列函数来计算替换单元散列值（步骤 S1052）。

[0292] 下一步，签名信息验证部件 1611 从 DVD 1500 读取对应于被选文件标识符的第一散列表（步骤 S1054），并且通过利用计算出来的替换单元散列值替换与计算出来的替换单元散列值相对应的单元散列值来产生被替换第一散列表（步骤 S1056）。在图 32 中，每次重复上述处理的时候，签名信息验证部件 1611：从已加密单元 1511 和第一散列表 1551 产生被替换第一散列表 1631；从已加密单元 1512 和第一散列表 1553 产生被替换第一散列表 1633；……；并且从已加密 单元 1513 和第一散列表 1557 产生被替换第一散列表 1637。

[0293] 为所有 i 个文件标识符完成了步骤 S1047 到 S1057 的重复以后，签名信息验证部件 1611 通过一个一个地将被替换第一散列表赋予散列函数来计算 i 个替换文件散列值（步骤 S1059）。

[0294] 下一步，签名信息验证部件 1611 从 DVD 1500 读取第二散列表 1556（步骤 S1061），并且通过利用计算出来的 i 个文件散列值替换与被选 i 个文件标识符相对应的文件散列值来产生被替换第二散列表 1639（步骤 S1063）。在图 23 中，所产生的被替换第二散列表 1639 包括：从被替换第一散列表 1631 计算出来的替换文件散列值 1641；从 DVD 1500 读取的文件散列值 1572；从被替换第一散列表 1633 计算出来的替换文件散列值 1643；……；以及从被替换第一散列表 1637 计算出来的替换文件散列值 1647。

[0295] 下一步，签名信息验证部件 1611 从验证密钥存储部件 1612 读取验证密钥 1613（步骤 S1064），并且利用单元拾取信息 1530、所产生的被替换第二散列表以及读取的验证密钥 1613 来验证签名信息 1570（步骤 S1066）。

[0296] 当签名信息的验证成功的时候（步骤 S1067：是），签名信息验证部件 1611 结束签名信息 1570 的验证。

[0297] 如果签名验证不成功（步骤 S1067：否），签名信息验证部件 1611 就将回放禁止信息输出给执行部件 1606（步骤 S1073）。

[0298] 内容密钥获取部件 1602 接收密钥块 1510，从装置密钥存储部件 1604 读取装置标识符 1608 和装置密钥 1609（步骤 S1071）。然后，内容密钥获取部件 1602 从读取的装置标识符 1608、装置密钥 1609 和密钥块 1510 产生内容密钥 CK，并且将产生出来的内容密钥 CK 输出给执行部件 1606（步骤 1072）。

[0299] 执行部件 1606 接收内容密钥 CK。在这里，如果已经从签名信息验证部件 1611 收到回放禁止信息（步骤 S1074：是），执行部件 1606 就通知用户 DVD 1500 上储存的内容的回放实际上不可能（步骤 S1076），并且结束回放。

[0300] 如果还没有收到回放禁止信息（步骤 S1074：否），执行部件 1606 就从 DVD 1500 读取组成已加密内容 1580 的已加密文件（步骤 S1077）。执行部件 1606 首先通过利用内容密钥 CK 对读取的已加密文件进行解密来产生文件（步骤 S1079），然后通过扩展所产生的文

件来产生视频和音频数据（步骤S1081）。然后，执行部件1606分别从所产生的视频和音频数据产生视频和音频信号，将这些信号输出给监视器1400，并且让监视器1400播放这些视频和音频（步骤S1082）。已经完成全部已加密文件的读取，或者通过用户进行的操作得到指令结束回放的时候（步骤S1084：是），执行部件1606结束回放。

[0301] 如果仍然有已加密文件还没有被读取，并且执行部件1606还没有从用户收到结束回放的指令，执行部件1606就返回步骤S1074，并且重复步骤1074到S1084的处理。

[0302] 1.6 综述和有益效果

[0303] 如同已经描述的一样，在本实施例中，DVD 1500储存：包括c个已加密文件的已加密内容，已加密文件中的每一个已加密文件都包括多个已加密单元；包括在多个已加密单元基础之上产生的c个第一散列表和第二散列表的报头信息；以及基于第二散列表产生的签名信息。

[0304] 在开始已加密内容的读出、解密、回放的同时，执行装置1600利用随机数随机地选择i个已加密单元，并且在所选择的i个已加密单元的基础之上计算替换单元散列值和替换文件散列值。

[0305] 下一步，执行装置1600从DVD读取第二散列表，并且通过从读取的第二散列表中包括的文件散列值中利用计算出来的替换文件散列值替换与计算出来的替换文件散列值相对应的文件散列值，产生被替换的第二散列表。然后，执行装置1600利用被替换第二散列表验证签名信息。如果验证不成功，执行装置1600就退出内容的回放。

[0306] 于是，通过将为了验证签名信息而新计算出来的单元散列值的数量限制到i个，就能够减少签名信息验证中涉及的计算量，这会降低内容回放过程中的处理负荷。

[0307] 此外，通过利用第一和第二散列表组成的两层结构对签名信息进行验证，执行装置1600能够减少从DVD 1500读出的信息的量。更 加具体地说，在本发明的第一实施例中，根本不需要读取与没被选中的文件信息相对应的第一散列表。因此，能够缩短读取信息所需要的时间。

[0308] 另外，在第一实施例中读取对应于被选文件信息的第一散列表。但是，从构成与被选文件信息相对应的第一散列表的组件中，只能读取与计算出来的替换单元散列值相对应的单元散列值以外的组件。对于第二散列表的读取也是这样。在这里，可以进一步减少从DVD 1500读取的信息的量。

[0309] 通过利用从已加密单元产生的被替换散列值对签名信息进行验证，可以一次完成是否包括未授权内容的验证和是否利用合法权利持有人拥有的签名密钥产生签名信息的验证。

[0310] 在验证处理中，如果将DVD 1500的全部或部分已加密内容替换成未授权内容，那么第一实施例很有可能检测出未授权内容，因为只是随机地选择了i个已加密单元用于使用。

[0311] 在这里，具体的说明是在已加密内容的一半已经被重新写入未授权内容这一假设的基础之上提供的。所选单个已加密单元是分发装置1100产生的有效已加密单元的概率是1/2。例如，在选择七个已加密单元并且进行所述验证的时候，所有被选的七个已加密单元是有效的已加密单元的概率是$(1/2)^7 = 1/128$。也就是说，在这种情况下，不能检测到未授权内容的概率小于1％。在这里，第一实施例充当一个威慑力量（acts as a deterrent）

来防止用未授权内容替换合法权利持有人分发的内容的一部分并且分发这一内容的欺骗行为。

[0312] 1.7 第一实施例的变型

[0313] 在第一实施例中，分发装置 1100 将组成获得的内容的每一个文件分裂成一些单元，然后对每个单元加密。但是，分发装置 1100 可以针对每个文件进行加密以产生已加密文件，并且通过分裂每一个已产生的已加密文件来产生已加密单元。在这种情况下，执行装置 1600 的执行部件 1606 从 DVD 1500 读取已加密内容，针对每一个已加密文件对读取的已加密内容进行解密，并且播放已解密内容。

[0314] 下面在图 26 的帮助下描述本变型的分发装置 1100b。

[0315] 分发装置 1100b 由以下部件组成：输入部件 1101b、内容密钥生成部件 1102、密钥块生成部件 1103、执行装置信息存储部件 1104、单元生成部件 1105b、加密处理部件 1106b、报头信息生成部件 1107、签名信息生成部件 1111、签名密钥存储部件 1112 和记录部件 1114。

[0316] 由于内容密钥生成部件 1102、密钥块生成部件 1103 和执行装置信息存储部件 1104、报头信息生成部件 1107、签名信息生成部件 1111、签名密钥存储部件 1112 和记录部件 1114 与第一实施例中的一样，因此省去了对这些组件的描述。

[0317] 另外，由于输入部件 1101b 与第一实施例的输入部件 1101 相同，只有是输出内容给加密处理部件而不是输出给单元生成部件除外，因此也省去了对它的描述。

[0318] 1.7.1 加密处理部件 1106b

[0319] 加密处理部件 1106b 从内容密钥生成部件 1102 接收内容密钥 CK。

[0320] 加密处理部件 1106 从输入部件 1101b 接收内容。在这里，内容由文件 CNT1、CNT2、……、CNTc 组成，如同图 3 所示的内容 1120 那种情形一样。

[0321] 接收内容的时候，加密处理部件 1106 通过利用内容密钥 CK 对收到的内容中包括的文件 CNT1 应用加密算法 E1 来产生已加密文件 ECT1。

[0322] 加密处理部件 1106 对文件 CNT2 到 CNTc 进行同样的处理，产生已加密文件 ECNT2 到 ECNTc。

[0323] 下一步，加密处理部件 1106 将所产生的已加密文件 ECNT1、ECNT2、ECNT3、……、ECNTc 组成的已加密内容输出给单元生成部件 1105b 和记录部件 1114b。

[0324] 1.7.2 单元生成部件 1105b

[0325] 单元生成部件 1105b 从加密处理部件 1106b 接收已加密内容。接收已加密内容的时候，单元生成部件 1105b 产生与收到的已加密内容中包括的已加密文件 ECNT1 相对应的文件标识符 FID1 和所述则文件标识信息 AD1。

[0326] 下一步，单元生成部件 1105b 将已加密文件 ECNT1 分裂成每一个都是 64kB 的来产生 m 个已加密单元。在这一点上，如果最后的已加密单元小于 64kB，就用“000……000”这样的数据补充已加密单元。

[0327] 下一步，单元生成部件 1105b 产生表明所产生的已加密单元数量的一个数 N1，然后产生由所产生的文件标识符 FID1、一则文件标识信息 AD1 和单元数 N1 组成的文件信息。

[0328] 下一步，单元生成部件 1105b 产生分别与所产生的 m 个已加密单元 EU1_1、EU1_2、EU1_3、……、EU1_m 相对应的单元标识符 UID1_1、UID1_2、UID1_3、……、UID1_m。接下来，

单元生成部件 1105b 通过将对应的已加密单元与单元标识符配对来形成 m 则已加密单元信息。

[0329] 下一步，单元生成部件 1105b 将 m 则已加密单元信息放在一起来形成已加密分裂文件 SplECNT1。

[0330] 单元生成部件 1105b 针对已加密内容中包括的已加密文件 ECNT2、ECNT3、……、ECNTc 的剩余部分以及其余则文件信息重复同样的处理，来产生已加密分裂文件 Spl1ECNT2、Spl1ECNT3、……、Spl1ECNTc。然后，单元生成部件 1105b 将所产生的 c 个已加密分裂文件 SplECNT1、SplECNT2、……、SplECNTc 输出给报头信息生成部件 1107b 作为已加密分裂内容。

[0331] 另外，单元生成部件 1105b 产生由 c 则文件信息组成的单元拾取信息，并且将所产生的单元拾取信息输出给记录部件 1114 和签名信息生成部件 1111b。

[0332] 2. 第二实施例

[0333] 下面在附图的帮助下描述本发明的第二实施例。

[0334] 2.1 未授权内容检测系统

[0335] 第二实施例的未授权内容检测系统由分发装置、执行装置和监视器组成，如同在第一实施例的未授权内容检测系统 1 中一样。

[0336] 分发装置根据操作员进行的操作获取内容，并且通过加密所获得的内容来产生已加密内容。另外，分发装置提取这些内容的一部分， 并且基于提取的这一部分内容（以后叫做代表性的部分内容）产生信息，例如用于检测内容中是否包括未授权内容的报头信息，用于证明内容是由合法权利持有人发布 (issued) 的的签名信息，等等。分发装置将产生的已加密内容、签名信息等等写入 DVD。

[0337] DVD 将通过分发渠道出售或者分发给用户。

[0338] 装载有 DVD 的时候，执行装置从装载的 DVD 中储存的已加密内容产生代表性的部分内容，并且基于所产生的代表性的部分内容来验证签名信息和报头信息。如果验证成功，执行装置就开始回放这些内容。当验证不成功的时候，执行装置禁止内容回放。

[0339] 下面将详细描述组成本实施例的未授权内容检测系统的各个装置以及 DVD。

[0340] 2.2 分发装置 2100

[0341] 图 27 说明构成本实施例的未授权内容检测系统中分发装置的结构。如图 27 所示，分发装置 2100 由输入部件 2101、内容密钥生成部件 2102、密钥块生成部件 2103、执行装置信息存储部件 1104、选择部件 2105、报头信息生成部件 2107、签名信息生成部件 2108、签名密钥存储部件 1112、加密处理部件 2109 和记录部件 2114 组成。

[0342] 下面详细描述组成分发装置 2100 的各个组件。注意，由于执行装置信息存储部件 1104 和签名密钥存储部件 1112 与第一实施例中的相同，因此省去了对这些组件的描述。

[0343] 2.2.1 输入部件 2101

[0344] 输入部件 2101 根据操作员的操作从外部装置或者外部记录介质获取内容和多则识别信息。

[0345] 图 28 说明输入部件 2101 获得的内容和标识信息的结构实例。内容 2120 由 c 项部分内容 CNT1 2121、CNT2 2122、CNT3 2123、……、CNTc 2127 组成。在这里，输入部件 2101 获得的内容 2120 是用于执行装置 2600 的可播放格式的（如同下面将详细描述的一样），并

且 DVD 视频格式和 MPEG-2 格式是这种可播放格式的实例。

[0346] 每一则标识信息是独一无二地表明构成内容 2120 的部分内容之一的信息，并且是例如来自内容的首部、扇区号的部分内容的对应项 的偏移，或者是通过引用内容首部指定的部分内容的所述项的回放起始点。例如，一则标识信息 AD1 2131 与部分内容 CNT1 2121 相对应，部分内容 CNT1 2121 的首部位于来自内容 2120 的首部的 AD1。

[0347] 输入部件 2101 将获得的内容 2120 和 c 则标识信息输出给内容密钥生成部件 2102。

[0348] 2.2.2 内容密钥生成部件 2102

[0349] 内容密钥生成部件 2102 从输入部件 2101 接收内容 2120 和 c 则标识信息。接收内容 2120 和 c 则标识信息的时候，内容密钥生成部件 2102 产生伪随机数，并且利用产生的伪随机数产生 128 比特长度的内容密钥 CK。替换伪随机数，也可以利用例如信号上的噪声产生真实的随机数。

[0350] 下一步，内容密钥生成部件 2102 将所产生的内容密钥 CK、收到的内容 2120 和 c 则标识信息输出给密钥块生成部件 2103 和加密处理部件 2109。

[0351] 2.2.3 密钥块生成部件 2103

[0352] 密钥块生成部件 2103 从内容密钥生成部件 2102 接收内容密钥 CK、内容 2120 和 c 则标识信息。接收内容密钥 CK 的时候，密钥块生成部件 2103 通过利用执行装置信息存储部件 1104 中储存的装置标识表 1130 和收到的内容密钥 CK 产生密钥块。由于产生密钥块的程序与第一实施例中的一样，因此省去了对它的描述。另外，在这里产生的密钥块具有与图 5 所示的密钥块 1150 一样的结构。

[0353] 下一步，密钥块生成部件 2103 向选择部件 2105 输出所产生的密钥块以及收到的内容密钥 CK、内容 2120 和 c 则标识信息。

[0354] 2.2.4 选择部件 2105

[0355] 图 29 说明选择部件 2105 进行的处理的概要。下面在图 29 的帮助下描述选择部件 2105。

[0356] 选择部件 2105 从密钥块生成部件 2103 接收密钥块、内容密钥 CK、内容 2120 和 c 则标识信息。接收这些组信息的时候，选择部件 2105 从收到的 c 则标识信息中选择 k 则。在这里的描述中假设 k = 3。

[0357] 关于选择方法，可以选择 k 则，例如通过利用随机数，或者从日 期、温度等等。也可以设计成从操作员接受选择。如果内容 2120 是 MPEG 格式的，那么可以选择表明图像内 (intra pictures) 的多则标识信息。另外，选择部件 2105 可以预存标识要选择的 k 则的信息，或者可以响应来自操作员的指令进行选择。

[0358] 如图 29 所示，这里的选择部件 2105 选择多则标识信息 AD32133、AD72134 和 ADc 2137。

[0359] 下一步，选择部件 2105 提取与选自收到的内容 2120 的所述则标识信息 AD3 2133 相对应的一项部分内容 CNT 3，并且产生由所选择的一则标识信息 AD3 2133 和所提取的一项部分内容 CNT3 组成的一则代表性的信息 2141。在这里，所选择的一项部分内容叫做“一项代表性的部分内容”。

[0360] 选择部件 2105 为多则标识信息 AD7 2134 和 ADc 2137 重复同一种处理，以产生多

则代表性的信息 2142 和 2143。

[0361] 下一步，选择部件 2105 向报头信息生成部件 2107 输出：所产生的三则代表性的信息 2141、2142 和 2143；收到密钥块、内容密钥 CK 和内容 2120。

[0362] 2.2.5 报头信息生成部件 2107

[0363] 报头信息生成部件 2107 从选择部件 2105 接收三则代表性的信息 2141、2142 和 2143，密钥块、内容密钥 CK 和内容 2120。

[0364] 接收这些内容的时候，报头信息生成部件 2107 产生独一无二地标识收到的所述则代表性的信息 2141 的标识信息标识符 ADID1。产生标识信息标识符的方法包括例如顺序赋予自然数和利用随机数的随机赋予。

[0365] 下一步，报头信息生成部件 2107 从收到的所述则代表性的信息 2141 提取所述则标识信息 AD3，并且产生由所产生的标识信息标识符 ADID1 和所述则标识信息 AD3 组成的一则代表性的检测信息。

[0366] 随后，报头信息生成部件 2107 从收到的所述则代表性的信息 2141 提取所述则代表性的部分内容 CNT3，并且通过将提取出来的代表性的部分内容 CNT3 赋予散列函数来产生部分散列值 HA3。报头信息生成部件 2107 产生由所产生的标识信息标识符 ADID1 和部分散 列值 HA3 组成的一则代表性的散列信息。

[0367] 报头信息生成部件 2107 为所述则代表性信息 2142 和 2143 重复同样的处理，并且产生多则代表性的检测信息和代表性的散列信息。报头信息生成部件 2107 产生由所产生的三则代表性的检测信息组成的被选位置信息。

[0368] 图 30 说明在这一点产生的被选位置信息的结构。被选位置信息 2160 由多则代表性的检测信息 2161、2162 和 2163 组成，这些信息分别对应于所述则代表性的信息 2141、4142 和 2143。每一则代表性的检测信息都由标识信息标识符和一则标识信息组成。作为一个实例，所述则代表性的检测信息 2161 对应于所述则代表性的信息 2141，并且包括标识信息标识符 AID1 2171 和一则标识信息 AD3 2176。

[0369] 另外，报头信息生成部件 2107 产生由所产生的三则代表性的散列信息组成的报头信息。

[0370] 图 31 说明在这一点产生的报头信息的结构。如图 31 所示，报头信息 2200 由多则代表性的散列信息 2201、2202 和 2203 组成，这些信息分别与所述则代表性的检测信息 2161、2162 和 2163 相对应。

[0371] 每一则代表性的散列信息包括标识信息标识符和部分散列值。例如，所述则代表性的散列信息 2201 是基于所述则代表性的信息 2141 产生的，并且包括标识信息标识符 ADID1 2211 和部分散列值 HA3。

[0372] 下一步，报头信息生成部件 2107 向签名信息生成部件 2108 输出所产生的被选位置信息 2160、报头信息 2200 和收到的密钥块、内容密钥 CK 和内容 2120。

[0373] 2.2.6 签名信息生成部件 2108

[0374] 签名信息生成部件 2108 从报头信息生成部件 2107 接收被选位置信息 2160、报头信息 2200、密钥块、内容密钥 CK 和内容 2120。接收这些组信息的时候，签名信息生成部件 2108 提取收到的报头信息 2200 中包括的部分散列值 HA3、HA5 和 HAc。

[0375] 下一步，签名信息生成部件 2108 从签名密钥存储部件 1112 读取签名密钥 1113。

通过将签名生成算法S赋予利用签名密钥1113的读取将提取的部分散列值HA3、HA5和HAc组合起来形成的组合结果，签名信息生成部件2108产生签名信息。

[0376] 下一步，签名信息生成部件2108将产生的签名信息和收到的被选位置信息2160、报头信息2200、密钥块、内容密钥CK和内容2120输出给加密处理部件2109。

[0377] 2.2.7加密处理部件2109

[0378] 加密处理部件2109从签名信息生成部件2108接收签名信息、被选位置信息2160、报头信息2200、密钥块、内容密钥CK和内容2120。

[0379] 接收这些组信息的时候，通过将加密算法E1分别应用于构成收到的内容2120的所述项部分内容CNT1、CNT2、CNT3、……、CNTc，加密处理部件2109利用收到的内容密钥CK产生多项已加密部分内容ECNT1、ECNT2、ECNT3、……、ECNTc。所产生的多项已加密部分内容ECNT1、ECNT2、ECNT3、……、ECNTc统称为已加密内容。在这里，可以将加密内容表示为ECNTb = Enc(CK,CNTb)，其中b是c或者更小的自然数。图32说明在这一点产生的已加密内容2220的结构。

[0380] 随后，加密处理部件2109通过将加密算法E1应用于收到的被选位置信息，利用收到的内容密钥CK来产生已加密被选位置信息。

[0381] 下一步，加密处理部件2109将所产生的已加密内容2220和已加密被选位置信息以及收到的签名信息、报头信息2200和密钥块输出给记录部件2114。

[0382] 2.2.8记录部件2114

[0383] 记录部件2114能够装载DVD。

[0384] 记录部件2114从加密处理部件2109接收已加密内容2220、已加密被选位置信息、签名信息、报头信息2200和密钥块，并且将收到的已加密内容2220、已加密被选位置信息、签名信息、报头信息2200和密钥块写入DVD。

[0385] 2.3DVD 2500

[0386] 如图33所示，DVD 2500储存密钥块2510、已加密被选位置信息2530、报头信息2550、签名信息2570和已加密内容2580。

[0387] 密钥块2510、已加密被选位置信息2530、报头信息2550、签名 信息2570和已加密内容2580已经由分发装置2100写入，这些组件的结构如同上面所述的一样。

[0388] 2.4执行装置2600

[0389] 如图34所示，执行装置2600由以下部件组成：获取部件2601、内容密钥获取部件2602、装置密钥存储部件1604、位置信息解密部件2606、签名信息验证部件2611、验证密钥存储部件1612、代表性的部分内容解密部件2616、报头信息验证部件2617和执行部件2618。

[0390] 下面详细描述构成执行装置2600的各个组件。注意，由于装置密钥存储部件1604和验证密钥存储部件1612与构成第一实施例的执行装置1600的那些一样，因此省去了对这些组件的描述。

[0391] 2.4.1获取部件2601

[0392] 获取部件2601装载DVD 2500。检测到DVD 2500被装载到它上面的时候，获取部件从DVD 2500读取密钥块2510、已加密被选位置信息2530、报头信息2550、签名信息2570和已加密内容2580。获取部件2601将读取的密钥块2510、已加密被选位置信息2530、报头

信息 2550、签名信息 2570 和已加密内容 2580 输出给内容密钥获取部件 2602。

[0393] 2.4.2 内容密钥获取部件 2602

[0394] 内容密钥获取部件 2602 从获取部件 2601 接收密钥块 2510、已加密被选位置信息 2530、报头信息 2550、签名信息 2570 和已加密内容 2580。

[0395] 收到这些组信息的时候，内容密钥获取部件 2602 利用装置标识符 AID_p 和装置密钥存储部件 1604 储存的装置密钥 DK_p 以及收到的密钥块产生内容密钥 CK。产生内容密钥 CK 的程序与构成第一实施例的执行装置 1600 的内容密钥获取部件 1602 所执行的内容密钥 CK 的产生程序一样，因此省去了对它的描述。

[0396] 下面，内容密钥获取部件 2602 将所产生的内容密钥 CK，以及收到的已加密被选位置信息 2530、报头信息 2550、签名信息 2570 和已加密内容 2580 输出给位置信息解密部件 2606。

[0397] 2.4.3 位置信息解密部件 2606

[0398] 位置信息解密部件 2606 从内容密钥获取部件 2602 接收内容密钥 CK、已加密被选位置信息 2530、报头信息 2550、签名信息 2570 和已加密内容 2580。

[0399] 接收这些组信息的时候，位置信息解密部件 2606 通过将解密算法 D1 应用于收到的已加密被选位置信息 2530，利用收到的内容密钥 CK 产生被选位置信息。在这一点产生的被选位置信息与图 30 所示被选位置信息 2160 一样具有相同的结构。

[0400] 下一步，位置信息解密部件 2606 将所产生的被选位置信息以及收到的内容密钥 CK、报头信息 2550、签名信息 2570 和已加密内容 2580 输出给签名信息验证部件 2611。

[0401] 2.4.4 签名信息验证部件 2611

[0402] 签名信息验证部件 2611 从位置信息解密部件 2606 接收被选位置信息、内容密钥 CK、报头信息 2550、签名信息 2570 和已加密内容 2580。

[0403] 接收这些组信息的时候，签名信息验证部件 2611 从验证密钥存储部件 1612 读取验证密钥。接下来，签名信息验证部件 2611 分别从构成收到的报头信息 2550 的三则代表性的散列信息提取部分散列值 HA3、HA7 和 HAc，并且通过利用读取的验证密钥将签名验证算法 V 应用于将所提取的部分散列值 HA3、HA7 和 HAc 组合起来形成的组合结果产生签名验证信息。签名信息验证部件 2611 将所产生的签名验证信息和收到的签名信息进行比较。当这两者不一致的时候，签名信息验证部件 2611 判定签名验证不成功，并退出后面的处理。

[0404] 当这两者一致的时候，签名信息验证部件 2611 判定签名验证成功，并且将收到的被选位置信息、内容密钥 CK、报头信息 2550 和已加密内容 2580 输出给代表性的部分内容解密部件 2616。

[0405] 2.4.5 代表性的部分内容解密部件 2616

[0406] 代表性的部分内容解密部件 2616 从签名信息验证部件 2611 接收被选位置信息、内容密钥 CK、报头信息 2550 和已加密内容 2580。

[0407] 接收这些组信息的时候，代表性的部分内容解密部件 2616 提取构成收到的被选位置信息的第一代表性检测信息中包括的标识信息 标识符 ADID1 和对应则标识信息 AD3，并且进一步基于提取出来的所述则标识信息 AD3 从收到的已加密内容 2580 提取一项已加密部分内容 ECNT3。下一步，代表性的部分内容解密部件 2616 通过将解密算法 D1 应用于提取出来的已加密部分内容 ECNT3，利用收到的内容密钥 CK 产生所述项代表性的部分内容

CNT3。在这里，将所产生的所述项代表性的部分内容 CNT3 和所提取的所述则标识信息标识符 ADID1 这一对叫做“一则验证代表性信息”。

[0408] 下一步，代表性的部分内容解密部件 2616 为其余则代表性的检测信息重复同一种处理，以产生由标识信息标识符 ADID2 和所述项代表性的部分内容 CNT7 组成的一则代表性信息以及由标识信息标识符 ADID3 和所述项代表性部分内容 CNTc 组成的一则验证代表性信息。

[0409] 下一步，代表性的部分内容解密部件 2616 将所产生的三则验证代表性信息和收到的内容密钥 CK、报头信息 2550 和已加密内容 2580 输出给报头信息验证部件 2617。

[0410] 2.4.6 报头信息验证部件 2617

[0411] 报头信息验证部件 2617 从代表性的部分内容解密部件 2616 接收三则验证代表性的信息、内容密钥 CK、报头信息 2550 和已加密内容 2580。

[0412] 接收这些组信息的时候，报头信息验证部件 2617 通过分别将收到的三则验证代表性的信息里包括的所述项代表性的部分内容 CNT3、CNT7 和 CNTc 赋予所述散列函数，产生验证散列值 H3、H7 和 Hc。这里使用的散列函数与分发装置 2100 的报头信息生成部件 2107 里使用的一样。

[0413] 下一步，报头信息验证部件 2617 在报头信息 2550 中搜索与对应则验证代表性的信息里包括的标识信息标识符 ADID1 一致的标识信息标识符，并且提取与检测到的标识信息标识符相对应的部分散列值 HA3。然后，报头信息验证部件 2617 比较所提取的部分散列值 HA3 和所产生的验证散列值 H3。

[0414] 另外，报头信息验证部件 2617 基于对应则验证代表性的信息里 包括的标识信息标识符 ADID2，从报头信息 2550 提取部分散列值 HA7，并且比较所提取的部分散列值 HA7 和所产生的验证散列值 H7。

[0415] 报头信息验证部件 2617 基于对应则验证代表性的信息中包括的标识信息标识符 ADIDc，从报头信息 2550 提取部分散列值 HAc，并且比较所提取的部分值 HAc 和所产生的验证散列值 Hc。

[0416] 比较这三对中的每一对，并且有一对互相不同的时候，报头信息验证部件 2617 就退出后面的处理。

[0417] 当上面三对的比较中所有三对都相符的时候，报头信息验证部件 2617 就判定报头信息 2550 的验证是成功的，并且将收到的内容密钥 CK 和已加密内容 2580 输出给执行部件 2618。

[0418] 2.4.7 执行部件 2618

[0419] 执行部件 2618 从报头信息验证部件 2617 接收内容密钥 CK 和已加密内容 2580。

[0420] 接收这些组信息的时候，执行部件 2618 通过将解密算法 D1 应用于组成收到的已加密内容 2580 的已加密的一些项部分内容 ECNT1、ECNT2、ECNT3、……、ECNTc 中的每一项，利用收到的内容密钥 CK 产生由一些项部分内容 CNT1、CNT2、CNT3、……、CNTc 组成的内容。

[0421] 下一步，执行部件 2618 扩展所产生的内容来产生视频和音频数据，并且从所产生的视频和音频数据产生视频和音频信号。执行部件 2618 将所产生的视频和音频信号输出给监视器。

[0422] 2.5 分发装置 2100 和执行装置 2600 的工作状况

[0423] 下面描述分发装置 2100 和执行装置 2600 的工作状况。

[0424] 2.5.1 分发装置 2100 的工作状况

[0425] 下面在图 35 所示流程图的帮助下描述分发装置 2100 的工作状况。

[0426] 输入部件 2101 接收由 c 项部分内容和 c 则标识信息组成的内容 2120(步骤 S2011),并且将收到的内容 2120 和标识信息输出给内容密钥生成部件 2102。

[0427] 内容密钥生成部件 2102 接收内容 2120 和 c 则标识信息,并且产 生内容密钥(步骤 S2012)。

[0428] 密钥块生成部件 2103 从内容密钥生成部件 2102 接收内容密钥、内容 2120 和 c 则标识信息,并且从执行装置信息存储部件 1104 读取装置标识符和装置密钥(步骤 S2013)。密钥块生成部件 2103 通过利用读取的装置标识符和装置密钥来产生密钥块(步骤 S2014),并且将所产生的密钥块、收到的内容密钥、内容 2120 和 c 则标识信息输出给选择部件 2105。

[0429] 选择部件 2105 接收密钥块、内容密钥、内容 2120 和标识信息,并且通过从收到的内容 2120 选择 k 项代表性的部分内容产生 k 则代表性的信息(步骤 S2016)。然后,选择部件 2105 将所产生的 k 则代表性的信息和收到的内容密钥和内容 2120 输出给报头信息生成部件 2107。

[0430] 报头信息生成部件 2107 从选择部件 2105 接收 k 则代表性的信息、内容密钥和内容 2120,并且从收到的 k 则代表性的信息产生被选位置信息 2160 和报头信息 2200(步骤 S2018)。下一步,报头信息生成部件 2107 将所产生的被选位置信息 2160 和报头信息 2200 以及收到的密钥块、内容密钥和内容 2120 输出给签名信息生成部件 2108。

[0431] 接下来,签名信息生成部件 2108 从报头信息生成部件 2107 接收被选位置信息 2160、报头信息 2200、密钥块、内容密钥和内容 2120。接收这些组信息的时候,签名信息生成部件 2108 从签名密钥存储部件 1112 读取签名密钥 1113(步骤 S2019),并且从读取的签名密钥 1113 和报头信息 2200 产生签名信息(步骤 S2021)。下一步,签名信息生成部件 2108 将所产生的签名信息和收到的密钥块、被选位置信息 2160、报头信息 2200、内容密钥和内容 2120 输出给加密处理部件 2109。

[0432] 加密处理部件 2109 从签名信息生成部件 2108 接收签名信息、密钥块、被选位置信息 2160、报头信息 2200、内容密钥和内容 2120,并且通过利用收到的内容密钥对被选位置信息 2160 进行加密来产生已加密被选位置信息(步骤 S2022)。接下来,加密处理部件 2109 通过利用内容密钥加密内容 2120 来产生已加密内容(步骤 S2023),然 后将所产生的已加密被选位置信息和已加密内容以及收到的密钥块、签名信息和报头信息 2200 输出给记录部件 2114。

[0433] 记录部件 2114 将从加密处理部件 2109 收到的密钥块、已加密被选位置信息、报头信息 2200、签名信息和已加密内容写入 DVD 2500(步骤 S2024)。

[0434] 2.5.2 执行装置 2600 的工作状况

[0435] 下面在图 36 所示流程图的帮助下描述执行装置 2600 的工作状况。

[0436] 装载了 DVD 2500 的时候,获取部件 2601 从 DVD 2500 读取密钥块 2510、已加密被选位置信息 2530、报头信息 2550、签名信息 2570 和已加密内容 2580(步骤 S2041)。然后,获取部件 2601 将读取的密钥块 2510、已加密被选位置信息 2530、报头信息 2550、签名信息 2570 和已加密内容 2580 输出给内容密钥获取部件 2602。

[0437] 从获取部件 2601 接收密钥块 2510、已加密被选位置信息 2530、报头信息 2550、签名信息 2570 和已加密内容 2580 的时候，内容密钥获取部件 2602 从装置密钥存储部件 1604 读取装置标识符和装置密钥（步骤 S2042）。内容密钥获取部件 2602 从读取的装置标识符和装置密钥以及收到的密钥块 2510 产生内容密钥（步骤 S2043）。内容密钥获取部件 2602 将所产生的内容密钥和收到的已加密被选位置信息 2530、报头信息 2550、签名信息 2570 和已加密内容 2580 输出给位置信息解密部件 2606。

[0438] 位置信息解密部件 2606 从内容密钥获取部件 2602 接收内容密钥、已加密被选位置信息 2530、报头信息 2550、签名信息 2570 和已加密内容 2580，并且通过利用收到的内容密钥对已加密被选位置信息 2530 进行解密来产生被选位置信息（步骤 S2044）。下一步，位置信息解密部件 2606 将所产生的被选位置信息和收到的内容密钥、报头信息 2550、签名信息 2570 和已加密内容 2580 输出给签名信息验证部件 2611。

[0439] 签名信息验证部件 2611 从位置信息解密部件 2606 接收被选位置信息、内容密钥、报头信息 2550、签名信息信息 2570 和已加密内容 2580，并且从验证密钥存储部件 1612 读取验证密钥（步骤 S2046）。然后，签名信息验证部件 2611 通过利用读取的验证密钥和收到的报头信息 2550 验证签名信息 2570（步骤 S2048）。签名信息 2570 的验证不成功的时候（步骤 S2049 :否），签名信息验证部件 2611 退出执行装置 2600 中的随后处理。

[0440] 当签名信息 2570 的验证成功的时候（步骤 S2049 :是），签名信息验证部件 2611 将收到的被选位置信息、内容密钥、报头信息 2550 和已加密内容 2580 输出给代表性的部分内容解密部件 2616。

[0441] 代表性的部分内容解密部件 2616 从签名信息验证部件 2611 接收被选位置信息、内容密钥、报头信息 2550 和已加密内容 2580，并且基于收到的被选位置信息、已加密内容 2580 和内容密钥产生 k 则代表性的部分内容（步骤 S2051）。然后，代表性的部分内容解密部件 2616 产生由对应项代表性部分内容和标识信息标识符组成的 k 则验证代表性的信息（步骤 S2052），并且将所产生的 k 则验证代表性的信息和收到的内容密钥、报头信息 2550 和已加密内容 2580 输出给报头信息验证部件 2617。

[0442] 报头信息验证部件 2617 从代表性的部分内容解密部件 2616 接收 k 则验证代表性的信息、内容密钥、报头信息 2550 和已加密内容 2580，并且通过利用收到的 k 则验证代表性的信息验证报头信息 2550（步骤 S2054）。如果验证不成功（步骤 S2056 :否），报头信息验证部件 2617 就退出后面的处理。

[0443] 当所述验证成功的时候（步骤 S2056 :是），报头信息验证部件 2617 就将收到的内容密钥和已加密内容 2580 输出给执行部件 2618。

[0444] 从报头信息验证部件 2617 接收内容密钥和已加密内容 2580 的时候，执行部件 2618 通过利用收到的内容密钥对已加密内容 2580 进行解密来产生内容（步骤 S2057），扩展所产生的内容（步骤 S2058），并且让监视器播放这些内容（步骤 S2059）。

[0445] 2.6 综述和有益结果

[0446] 如同已经描述的一样，在第二实施例中，分发装置 2100 只利用来自组成所述内容的 c 项部分内容的 k 项代表性的部分内容产生报头 信息，并且进一步通过将签名生成算法应用于所述报头信息来产生签名信息。

[0447] 执行装置 2600 通过基于被选位置信息产生 k 项代表性的部分内容，并且利用所产

生的 k 项代表性的部分内容验证报头信息，来验证是否包括未授权内容。当验证成功的时候，判定没有包括任何未授权内容，执行装置 2600 开始内容回放。

[0448] 因此，只利用组成内容的 c 项部分内容中的 k 则来验证报头信息能够减少执行装置 2600 进行验证的处理负荷。

[0449] 更进一步，还可能减少分发装置 2100 中报头信息的产生中所涉及的处理负荷。

[0450] 3. 第三实施例

[0451] 下面描述本发明第三实施例中的未授权内容检测系统。

[0452] 3.1 未授权内容检测系统

[0453] 第三实施例中的未授权内容检测系统由分发装置、执行装置和监视器组成，如同第一实施例中的未授权内容检测系统中一样。

[0454] 分发装置根据操作员的操作获取内容，并且通过对获取的内容加密来产生已加密内容。

[0455] 另外，分发装置提取内容的一部分，并且基于提取的内容的一部分（以后将它叫做“一项代表性的部分内容”）产生信息，比如用于检测内容中是否包括未授权内容的报头信息，用于证明内容是由合法权利持有人颁布的的签名信息，等等。分发装置重复一项代表性的部分内容的提取，一则报头信息的产生，以及一则签名信息的产生，来产生多则报头信息和签名信息，并且将所产生的已加密内容和多则报头信息和签名信息写入 DVD。

[0456] 通过分发渠道将 DVD 售出，分发给用户。

[0457] 执行装置从 DVD 上记录的多则签名信息和多则报头信息选择一则，并且验证被选的多则签名和报头信息。

[0458] 下面详细描述组成本实施例的未授权内容检测系统的各个装置和 DVD。

[0459] 3.2 分发装置 3100

[0460] 图 37 说明本实施例中分发装置的结构。如图 37 所示，分发装置 3100 由输入部件 2101、内容密钥生成部件 2102、密钥块生成部件 2103、执行装置信息存储部件 1104、选择部件 3105、报头信息生成部件 3107、签名信息生成部件 3108、签名密钥存储部件 1112、加密处理部件 3109 和记录部件 3114 组成。输入部件 2101、内容密钥生成部件 2102、密钥块生成部件 2103、执行装置信息存储部件 1104 和签名密钥存储部件 1112 与第二实施例中的一样，因此在这里省去了对这些组件的描述。

[0461] 3.2.1 选择部件 3105

[0462] 选择部件 3105 预存迭代次数 x（x 是一个大于或等于 2 的整数）。

[0463] 选择部件 3105 从密钥块生成部件 2103 接收密钥块、内容密钥 CK、内容和 c 则标识信息。接收密钥块、内容密钥 CK、内容和 c 则标识信息的时候，选择部件 3105 按照与第二实施例中选择部件 2105 一样的方式产生 k 则代表性的信息。

[0464] 选择部件 3105 重复同一种处理 x 次来产生 x 组 k 则代表性信息。在这里，将第一组代表性的信息叫做第一代表性的组，而第二组、……、第 x 组代表性的信息则分别叫做第二代表性的组和第 x 代表性的组。这里的一个具体实例是所有第一到第 x 个代表性的组都分别由 k 则代表性的信息组成，但是，组与组之间代表性的信息的则数可以不同。

[0465] 下一步，选择部件 3105 将所产生的第一、第二、……、第 x 个代表性的组以及收到的密钥块、内容密钥 CK 和内容输出给报头信息生成部件 3107。

[0466] 3.2.2 报头信息生成部件 3105

[0467] 报头信息生成部件 3107 从选择部件 3105 接收第一、第二和第 x 个代表性的组，密钥块、内容密钥 CK 和内容。

[0468] 接收这些组信息的时候，报头信息生成部件 3107 基于收到的第一代表性的组中包括的 k 则代表性的信息和内容，产生被选位置信息 POS1 和报头信息 HEAD1。产生被选位置信息和报头信息的具体程序与第二实施例的报头信息生成部件 2107 执行的被选位置信息 2160 和 报头信息 2200 的产生程序相同，因此，省去了对它的描述。被选位置信息 POS1 与图 30 所示的被选位置信息 2160 一样具有相同结构，而报头信息 HEAD1 则与图 31 所示的报头信息 2200 一样具有相同结构。

[0469] 下一步，报头信息生成部件 3107 产生专用于产生的被选位置信息 POS 1 和报头信息 HEAD1 这一对的一个报头标识符 HEADID1。在这里，将所产生的报头标识符 HEADID1、一则被选位置信息 POS1 和一则报头信息 HEAD1 一起叫做第一报头组。

[0470] 报头信息生成部件 3107 针对第二、第三、……、第 x 个代表性的组重复同样的处理，以产生第二、第三、……、第 x 个报头组。

[0471] 下一步，报头信息生成部件 3107 从第一到第 x 报头组提取报头标识符，并且产生由所提取的 x 则报头标识符组成的报头选择信息。

[0472] 图 38 给出在这一点产生的报头选择信息的结构的一个实例。报头选择信息 3130 由 x 个报头标识符组成，并且这些报头标识符分别对应于第一到第 x 个报头组。

[0473] 下一步，报头信息生成部件 3107 将所产生的报头选择信息 3130 和第一、第二、……、第 x 个报头组，以及收到的密钥块、内容密钥 CK 和内容输出给签名信息生成部件 3108。

[0474] 3.2.3 签名信息生成部件 3108

[0475] 签名信息生成部件 3108 从报头信息生成部件 3107 接收报头选择信息 3130 和第一、第二、……、第 x 个报头组，以及密钥块、内容密钥 CK 和内容。

[0476] 接收这些组信息的时候，签名信息生成部件 3108 从签名密钥存储部件 1112 读取签名密钥 1113。

[0477] 下一步，签名信息生成部件 3108 利用第一报头组中包括的报头信息 HEAD1 和读取的签名密钥 1113 产生一则签名信息 Sign1。产生所述则签名信息的具体程序与签名信息生成部件 2108 执行的一样。

[0478] 在这里，将术语“第一报头组”重新赋予将所产生的一则签名信息 Sign1 加到报头标识符 HEADID1、一则被选位置信息 POS1 和一则报头信息 HEAD1 上去形成的结果。

[0479] 签名信息生成部件 3108 针对第二到第 x 个报头组重复同样的处理来产生多则签名信息，并且通过将所产生的多则签名信息分别加到对应的报头标识符、多则被选位置信息和多则报头信息上去，新形成第二到第 x 个报头组。

[0480] 下一步，签名信息生成部件 3108 将第一、第二、……、第 x 个报头组，以及收到的报头选择信息 3130、密钥块、内容密钥 CK 以及内容输出给加密处理部件 3109。

[0481] 3.2.4 加密处理部件 3109

[0482] 加密处理部件 3109 从签名信息生成部件 3108 接收第一、第二、……、第 x 个报头组，报头选择信息 3130、密钥块、内容密钥 CK 以及内容。

[0483] 加密处理部件 3109 通过将加密算法 E1 应用于构成收到的内容的各项部分内容利用收到的内容密钥 CK 来产生 c 项已加密部分内容，并且将所产生的 c 项已加密部分内容放在一起来形成已加密内容。在这一点产生的已加密内容与图 32 中已加密内容 2220 一样具有相同的结构。

[0484] 下一步，加密处理部件 3109 从第一报头组提取所述则被选位置信息 POS1，并且通过将加密算法 E1 应用于所提取的所述则被选位置信息 POS1 利用内容密钥 CK 来产生一则已加密被选位置信息 EPOS1。接下来，加密处理部件 3109 用产生的所述则已加密被选位置信息 EPOS1 替换第一报头信息组中包括的所述则被选位置信息 POS1。在这里，EPOS1 = Enc(CK，POS1)。

[0485] 加密处理部件 3109 针对第二到第 x 个报头组进行同样的处理来产生多则已加密被选位置信息，并且用所述多则已加密被选位置信息替换对应的多则被选位置信息。

[0486] 下一步，加密处理部件 3109 将第一、第二、……、第 x 个报头组、所产生的已加密内容以及收到的报头选择信息 3130 和密钥块输出给记录部件 3114。

[0487] 3.2.5 记录部件 3114

[0488] 记录部件 3114 从加密处理部件 3109 接收第一、第二、……、第 x 个报头组、已加密内容、报头选择信息 3130 和密钥块，并且将收到的第一、第二、……、第 x 个报头组、已加密内容、报头选择信息 3130 和密钥块写入 DVD。

[0489] 3.3DVD 3500

[0490] 图 39 说明本实施例的 DVD 记录的信息。

[0491] 如图 39 所示，DVD 3500 储存密钥块 3510、报头选择信息 3520、第一报头组 3530、第二报头组 3540、……、第 x 报头组 3560，以及已加密内容 3580。

[0492] 第一报头组 3530、第二报头组 3540、……、第 x 报头组 3560 中的每一个都由报头标识符、一则已加密被选位置信息、一则报头信息和一则签名信息组成。

[0493] 例如，第一报头组 3530 由报头标识符 HEAD13531、一则已加密被选位置信息 EPOS13532、一则报头信息 HEAD1 和一则签名信息 Sign1 3534 组成。

[0494] 已经由分发装置 3100 将这些组信息写入 DVD 3500。每一组信息的结构都和前面提到过的一样，因此这里省去了对它们的描述。

[0495] 3.4 执行装置 3600

[0496] 如图 40 所示，执行装置 3600 由获取部件 3601、内容密钥获取部件 2602、装置密钥存储部件 1604、位置信息解密部件 2606、签名信息验证部件 2611、验证密钥存储部件 1612、代表性的部分内容解密部件 2616、报头信息验证部件 2617 和执行部件 2618 组成。

[0497] 除了获取部件 3601 以外的组件与构成第二实施例中执行装置 2600 的内容密钥获取部件 2602、装置密钥存储部件 1604、位置信息解密部件 2606、签名信息验证部件 2611、验证密钥存储部件 1612、代表性的部分内容解密部件 2616、报头信息验证部件 2617 和执行部件 2618 一样具有同样的结构和工作状况。因此，这里仅仅描述获取部件 3601。

[0498] 3.4.1 获取部件 3601

[0499] 检测到上面装载了 DVD 3500 的时候，获取部件 3601 从 DVD3500 读取报头选择信息 3520。然后，获取部件 3601 利用一个随机数 选择读取的报头信息 3520 中包括的报头标识符 HEADID1、HEADID2、HEADID3、……、HEADIDx 中的一个。选择方法不限于这种方法，可

以采用任何方法，只要第三方很难预测选择的是哪一个标识符就行。

[0500] 下一步，获取部件 3601 从 DVD 3500 上记录的第一、第二、……、第 x 个报头组中提取包括被选报头标识符的报头组，并且从这个报头组读取一则已加密被选位置信息、一则报头信息以及一则签名信息。

[0501] 接下来，获取部件 3601 从 DVD 3500 读取密钥块 3510 和已加密内容 3580，并且将读取的密钥块 3510、已加密内容、已加密被选位置信息、报头信息和签名信息输出给内容密钥获取部件 2602。

[0502] 3.5 综述和有益效果

[0503] 如上所述，第三实施例的分发装置 3100 产生 x 组，每一组都由一则已加密被选位置信息、一则报头信息和一则签名信息组成，执行装置选择 x 组中的一组，并且通过利用被选组的一则已加密被选位置信息、一则报头信息和一则签名信息来验证是否包括未授权内容。

[0504] 所以，通过增加验证所使用的代表性的部分内容的则数，能够提高检测未授权内容的准确度。更进一步，很难预测执行装置 3600 里从第一到第 x 个报头组选择了哪一个报头组，因此能够防止利用未授权内容仅仅专门替换不用于验证的多则部分内容这种欺骗性行为。

[0505] 4. 第四实施例

[0506] 下面描述本发明第四实施例的未授权内容检测系统。

[0507] 4.1 未授权内容检测系统

[0508] 如同在第一实施例中一样，第四实施例的未授权内容检测系统由分发装置、执行装置和监视器组成。

[0509] 分发装置按照操作员的操作来获取内容，并且通过对获得的内容进行加密来产生已加密内容。

[0510] 另外，分发装置将内容分裂成多项部分内容，并且基于所有项部分内容，产生用于验证内容中是否包括未授权内容的报头信息以及用于证明内容是由合法权利持有人颁发的的签名信息。分发装置将所产生的已加密内容、签名信息等等写入 DVD。

[0511] 将通过分发渠道将 DVD 销售或者分发给用户。

[0512] 装载了 DVD 的时候，执行装置从构成内容的多项部分内容中选择一些项，并且只利用所选项部分内容来验证报头信息。

[0513] 下面将详细描述组成本实施例的未授权内容检测系统的各个装置和 DVD。

[0514] 4.2 分发装置 4100

[0515] 图 41 说明第四实施例的分发装置的结构。如图 41 所示，分发装置 4100 由输入部件 4101、内容密钥生成部件 4102、密钥块生成部件 4103、执行装置信息存储部件 1104、部分内容生成部件 4105、报头信息生成部件 4107、签名信息生成部件 4108、签名密钥存储部件 1112、加密处理部件 4109 和记录部件 4114 组成。

[0516] 下面描述构成分发装置 4100 的各个组件。注意，由于执行装置信息存储部件 1104 和签名密钥存储部件 1112 与第一实施例中的一样，因此这里省去了对这些组件的描述。

[0517] 4.2.1 输入部件 4101

[0518] 输入部件 4101 根据分发装置 4100 的操作员的操作，从外部装置或者外部记录介

质获取内容。在这里获得的内容是执行装置 4600 能够播放的格式（如同后面将详细描述的一样），DVD 视频格式和 MPEG-2 格式都是这种可播放格式的实例。

[0519] 输入部件 4101 将获得的内容输出给内容密钥生成部件 4102。

[0520] 4.2.2 内容密钥生成部件 4102

[0521] 内容密钥生成部件 4102 从输入部件 4101 接收内容。接收这些内容的时候，内容密钥生成部件 4102 产生伪随机数，并且利用所产生的伪随机数产生 128 比特长的内容密钥 CK。替代伪随机数，也可以利用例如信号上的噪声来产生真随机数。

[0522] 下一步，内容密钥生成部件 4102 将所产生的内容密钥 CK 和收到的内容输出给密钥块生成部件 4103。

[0523] 4.2.3 密钥块生成部件 4103

[0524] 密钥块生成部件 4103 从内容密钥生成部件 4102 接收内容密钥 CK 和内容。接收内容密钥 CK 和内容的时候，密钥块生成部件 4103 利用收到的内容密钥 CK 和执行装置信息存储部件 1104 中储存的装置标识表来产生密钥块。产生密钥块的具体程序和第一实施例的密钥块生成部件 1103 执行的相同，因此省去了对它的描述。

[0525] 下一步，密钥块生成部件 4103 将所产生的密钥块、收到的内容密钥 CK 和内容输出给部分内容生成部件 4105。

[0526] 4.2.4 部分内容生成部件 4105

[0527] 部分内容生成部件 4105 从密钥块生成部件 4103 接收密钥块、内容密钥 CK 和内容。

[0528] 接收这些组信息的时候，部分内容生成部件 4105 将收到的内容分裂成 c 项部分内容 CNT1、CNT2、CNT3、……、CNTc。例如，当内容的格式是 DVD 视频格式的时候，可以将 VOB 或者 VOBU 用作分裂单元。另一方面，当内容的格式是 MPEG-2 格式的时候，可以将 GOP（图片组）、字段、帧或者内部图片用作分裂单元。不考虑内容格式，也可以将内容分裂成每个都是 64 千字节的，或者每一部分对应于回放时间的一秒钟。在这一点产生的 c 项部分内容一起叫做分裂内容。

[0529] 下一步，部分内容生成部件 4105 产生多则标识信息 AD1、AD2、AD3、……、ADc，它们分别对应于所产生的 n 项部分内容。每一则标识信息都是独一无二地标识对应项部分内容的信息，并且是例如通过引用内容的首部，或者是从内容的首部算起的一个偏移指定的所述项部分内容的回放起始点。

[0530] 图 42 说明在这一点产生的分裂内容和标识信息。分裂内容 4120 由 c 项部分内容 CNT1 4121、CNT2 4122、CNT3 4123、……、CNTc4127 组成。每一项部分内容对应于一则标识信息。例如，一则标识信息 AD1 4131 是用于标识所述项部分内容 CNT1 4121 的信息。

[0531] 下一步，部分内容生成部件 4105 将产生的 c 则标识信息和分裂内容 4120，以及收到的密钥块和内容密钥 CK 输出给报头信息生成部件 4107。

[0532] 4.2.5 报头信息生成部件 4107

[0533] 报头信息生成部件 4107 从部分内容生成部件 4105 接收 c 则标识 信息 AD1、AD2、AD3、……、ADc，以及分裂内容 4120、密钥块和内容密钥 CK。

[0534] 接收这些组信息的时候，报头信息生成部件 4107 利用随机数产生独一无二地标识所述则标识信息 AD1 的标识信息标识符 ADID1。

[0535] 在这里，产生的标识信息标识符 ADID1 和收到的所述则标识信息 AD1 构成的一对叫作“一则内容检测信息”。

[0536] 下一步，报头信息生成部件 4107 基于收到的多则标识信息 AD1 从分裂内容 4120 提取部分内容 CNT1 4121，并且通过将提取出来的所述项部分内容 CNT1 4121 赋予散列函数来计算部分散列值 HA1。在这里，所产生的标识信息标识符 ADID1 和计算出来的散列值 HA1 所构成的一对叫作“一则部分散列信息”。

[0537] 报头信息生成部件 4107 针对其余则标识信息 AD2、AD3、……、ADc 重复同一种处理，以产生多则内容检测信息和多则部分散列信息。

[0538] 下一步，报头信息生成部件 4107 产生由 c 则内容检测信息组成的内容位置信息。图 43 说明在这一点产生的内容位置信息的结构。内容位置信息 4140 由 c 则内容检测信息 4141、4142、4143、……、4146 组成。每一则内容检测信息都包括标识信息标识符和一则标识信息。作为一个实例，所述则内容检测信息 4141 包括标识信息标识符 ADID1 4151 和所述则标识信息 AD1 4131。

[0539] 接下来，报头信息生成部件 4107 产生由所产生的 c 则部分散列信息组成的报头信息。图 44 说明在这一点产生的报头信息的结构。报头信息 4160 由 c 则部分散列信息 4161、4162、4163、……、4166 组成。每一则部分散列信息都包括标识信息标识符和部分散列值，并且对应于构成所述内容位置信息 4140 的一则内容检测信息。例如，所述则部分散列信息 4161 包括标识信息标识符 ADID 4171 和部分散列值 HA1 4172。

[0540] 下一步，报头信息生成部件 4107 将产生的内容位置信息 4140 和报头信息 4160，以及收到的分裂内容 4120、密钥块和内容密钥 CK 输出给签名信息生成部件 4108。

[0541] 4.2.6 签名信息生成部件 4108

[0542] 签名信息生成部件 4108 从报头信息生成部件 4107 接收内容位置信息 4140、报头信息 4160、分裂内容 4120、密钥块和内容密钥 CK。

[0543] 接收这些组信息的时候，签名信息生成部件 4108 提取构成收到的报头信息 4160 的各则部分散列信息中包括的散列值。签名信息生成部件 4108 通过将组合提取出来的 c 个部分散列值 HA1、HA2、HA3、……、HAc 形成的组合结果赋予散列函数来产生组合后的散列值。

[0544] 下一步，签名信息生成部件 4108 从签名密钥存储部件 1112 读取签名密钥 1113，并且通过将签名生成算法 S 应用于所产生的组合后散列值，利用读取的签名密钥 1113 来产生签名信息。

[0545] 已经产生了签名信息的时候，签名信息生成部件 4108 将产生的签名信息以及收到的内容位置信息 4140、报头信息 4160、分裂内容 4120、密钥块和内容密钥 CK 输出给加密处理部件 4109。

[0546] 4.2.7 加密处理部件 4109

[0547] 加密处理部件 4109 从签名信息生成部件 4108 接收签名信息、内容位置信息 4140、报头信息 4160、分裂内容 4120、密钥块和内容密钥 CK。

[0548] 接收这些组信息的时候，加密处理部件 4109 通过将加密算法应用于构成收到的分裂内容 4120 的所述项部分内容 CNT1 4121 来产生一项已加密部分内容 ECNT1。加密处理部件 4109 针对多项部分内容 CNT2 4122、CNT3 4123、……、CNTc 4127 重复同一种处理，以

产生多项已加密部分内容 ECNT2、ECNT3、……、ECNTc。

[0549] 下一步，加密处理部件 4109 产生由所产生的 c 项已加密部分内容 ECNT1、ECNT2、ECNT3、……、ECNTc 组成的已加密内容。在这一点产生的已加密内容与第二实施例的已加密内容 2220（图 32）一样具有同样的结构。

[0550] 下一步，加密处理部件 4109 将所产生的已加密内容以及收到的签名信息、内容位置信息 4140、报头信息 4160 和密钥块输出给记录部件 4114。

[0551] 4.2.8 记录部件 4114

[0552] 给记录部件 4114 装载 DVD。

[0553] 记录部件 4114 从加密处理部件 4109 接收已加密内容、签名信息、内容位置信息 4140、报头信息 4160 和密钥块。

[0554] 接收这些组信息的时候，记录部件 4114 将收到的已加密内容、签名信息、内容位置信息 4140、报头信息 4160 和密钥写入 DVD。

[0555] 4.3DVD 4500

[0556] 图 45 说明第四实施例的 DVD 里储存的信息。如图 45 所示，DVD4500 储存密钥块 4510、内容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580。

[0557] 这些组信息已经由分发装置 4100 写入。各组信息的结构已经在上面说明过，因此省去了对它们的描述。

[0558] 4.4 执行装置 4600

[0559] 图 46 说明第四实施例的执行装置的结构。如图 46 所示，执行装置 4600 由获取部件 4601、内容密钥获取部件 4602、装置密钥存储部件 1604、签名信息、验证部件 4606、验证密钥存储部件 1612、选择部件 4611、部分内容解密部件 4616、报头信息验证部件 4617 和执行部件 2618 组成。

[0560] 下面详细描述构成执行装置 4600 的各个组件。注意，由于装置密钥存储部件 1604 和验证密钥存储部件 1612 与第一实施例中的一样，而执行部件 2618 又与第二实施例中的一样，因此省去了对这些组件的描述。

[0561] 4.4.1 获取部件 4601

[0562] 将 DVD 4500 装载进获取部件 4601。检测到上面装载了 DVD4500 的时候，获取部件 4601 读取密钥块 4510、内容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580，并且将读取的密钥块 4510、内容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580 输出给内容密钥获取部件 4602。

[0563] 4.4.2 内容密钥获取部件 4602

[0564] 内容密钥获取部件 4602 从获取部件 4601 接收密钥块 4510、内 容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580。

[0565] 接收这些组信息的时候，内容密钥获取部件 4602 通过使用收到的密钥块 4510、装置标识符 AID p 和装置密钥存储部件 1604 储存的装置密钥 DK p 来产生内容密钥 CK。产生内容密钥 CK 的程序与构成第一实施例的执行装置 1600 的内容密钥获取部件 1602 执行的程序一样，因此省去了对它的描述。

[0566] 下一步，内容密钥获取部件 4602 将所产生的内容密钥 CK 和收到的内容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580 输出给签名信息验证部件 4606。

[0567] 4.4.3 签名信息验证部件 4606

[0568] 签名信息验证部件 4606 从内容密钥获取部件 4602 接收内容密钥 CK、内容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580。

[0569] 接收这些组信息的时候，签名信息验证部件 4606 在以下程序中验证签名信息 4570。

[0570] 首先，签名信息验证部件 4606 从构成收到的报头信息的各则部分散列信息提取部分散列值，并且通过将组合所提取的部分散列值 HA1、HA2、HA3、……、HAc 组合起来形成的组合结果赋予散列函数来计算签名验证组合后散列值。

[0571] 下一步，签名信息验证部件 4606 从验证密钥存储部件 1612 读取验证密钥 1613，并且通过将签名验证算法 V 应用于计算出来的签名验证组合后散列值来产生签名验证信息。然后，签名信息验证部件 4606 比较所产生的签名验证信息和收到的签名信息。当这两者不一致的时候，签名信息验证部件 4606 判定签名信息 4570 的验证不成功，并且退出执行装置 4600 中的后续处理。

[0572] 当这两者一致的时候，签名信息验证部件 4606 判定签名信息 4570 的验证成功，并且将收到的内容密钥 CK、内容位置信息 4530、报头信息 4550 和已加密内容 4580 输出给选择部件 4611。

[0573] 4.4.4 选择部件 4611

[0574] 选择部件 4611 从签名信息验证部件 4606 接收内容密钥 CK、内 容位置信息 4530、报头信息 4550 和已加密内容 4580。

[0575] 接收这些组信息的时候，选择部件 4611 在下面将描述的程序里从收到的内容位置信息 4530 产生被选位置信息。图 47 说明选择部件 4611 执行的被选位置信息的产生程序的概要，以及在这一点产生的被选位置信息的结构。下面在图 47 的帮助之下描述被选位置信息的产生程序。

[0576] 选择部件 4611 利用随机数从构成收到的内容位置信息 4530 的 c 则内容检测信息 4531、4532、4533、……、4536 中选择出 k 则。选择方法不限于这种方法，可以使用任何方法，只要第三方很难预测选中了哪些则就行。

[0577] 图 47 说明选择了包括多则内容检测信息 4531、4533 和 4536 的 k 则的情形。

[0578] 下一步，选择部件 4611 产生由被选 k 则内容检测信息 4531、4533、……、4536 组成的被选位置信息 4620。

[0579] 下一步，选择部件 4611 在以下程序中基于收到的报头信息 4550 产生选择报头信息。图 48 说明产生选择报头信息的程序的概要和选择报头信息的结构。下面在图 48 的帮助下，给出选择报头信息的产生程序的理由。

[0580] 首先，选择部件 4611 从构成所产生的被选位置信息 4620 的多则内容检测信息 4531、4532、……、4536 中的每一则提取标识信息标识符，并且进一步提取包括与提取的标识信息标识符 ADID1、ADID3、……、ADIDc 相同的多则部分散列信息 4551、4553、……、4556。

[0581] 下一步，选择部件 4611 产生由提取出来的多则部分散列信息 4551、4553、……、4556 组成的选择报头信息 4630。

[0582] 下一步，选择部件 4611 将所产生的被选位置信息 4620、选择报头信息 4630 和收到的内容密钥 CK 以及已加密内容 4580 输出给部分内容解密部件 4616。

[0583] 4.4.5 部分内容解密部件 4616

[0584] 部分内容解密部件 4616 从选择部件 4611 接收被选位置信息 4620、选择报头信息 4630、内容密钥 CK 和已加密内容 4580。

[0585] 接收这些组信息的时候，部分内容解密部件 4616 在下面描述的程序里产生验证内容。图 49 说明产生验证内容的程序的概要和在这一点产生的验证内容 4650 的结构。下面在图 49 的帮助之下描述产生验证内容的程序。

[0586] 首先，部分内容解密部件 4616 从构成收到的被选位置信息 4620 的内容检测信息 4531 提取所述则标识信息 AD1，并且进一步基于提取的所述则标识信息 AD1 从收到的已加密内容 4580 提取所述则已加密部分内容 ECNT1。

[0587] 部分内容解密部件 4616 通过将所述解密算法 D1 应用于所述项提取出来的部分内容 ECNT1 来产生所述项部分内容 CNT1。随后，部分内容解密部件 4616 产生由所述则内容检测信息 4531 中包括的标识信息标识符 ADID1 和所产生的所述项部分内容 CNT1 组成的一则验证部分内容信息 4651。

[0588] 部分内容解密部件 4616 针对其余多则内容检测信息 4532、……、4536 重复同样的处理来产生多则验证部分内容信息 4652、……、4656。下一步，部分内容解密部件 4616 产生由所产生的 k 则验证部分内容信息组成的验证内容 4650。

[0589] 已经产生了验证内容 4650 的时候，部分内容解密部件 4616 将所产生的验证内容 4650 和收到的选择报头信息 4630、内容密钥 CK 以及已加密内容 4580 输出给报头信息验证部件 4617。

[0590] 4.4.6 报头信息验证部件 4617

[0591] 报头信息验证部件 4617 从部分内容解密部件 4616 接收验证内容 4650、选择报头信息 4630、内容密钥 CK 和已加密内容 4580。

[0592] 接收这些组信息的时候，报头信息验证部件 4617 通过将构成收到的验证内容 4650 的第一则验证部分内容信息 4651 中包括的一项部分内容 CNT1 4624 赋予散列函数来产生验证散列值 H1。

[0593] 下一步，报头信息验证部件 4617 提取所述则验证部分内容信息 4651 中包括的标识信息标识符 ADID1 4621。然后，报头信息验证部件 4617 检测包括与从收到的选择报头信息 4630 提取的标识信息标识 符 ADID1 4621 一样的标识信息的一则部分散列信息 4551，并且提取检测到的部分散列信息 4551 中包括的部分散列值 HA1。下一步，报头信息验证部件 4617 比较提取出来的部分散列值 HA1 4632 和计算出来的验证散列值 H1。

[0594] 报头信息验证部件 4617 针对其余则验证部分内容信息 4652、……、4656 重复同样的处理，并且将部分散列值与验证散列值进行 k 次比较。

[0595] 在这 k 次比较中，一旦部分散列值和验证散列值互相不同，报头信息验证部件 4617 就退出执行装置 4600 中的后续处理。

[0596] 在 k 次比较中，当所有部分散列值和验证散列值对都相同的时候，报头信息验证部件 4617 将收到的内容密钥 CK 和已加密内容 4580 输出给执行部件 4618。

[0597] 4.5 工作状况

[0598] 下面描述分发装置 4100 和执行装置 4600 的工作状况。

[0599] 4.5.1 分发装置 4100 的工作状况

[0600] 图 50 是一个流程图，它说明分发装置 4100 的工作状况，而图 51 则说明分发装置 4100 的工作状况中处理内容的流。

[0601] 下面在图 50 和 51 的帮助之下描述分发装置 4100 的工作状况。

[0602] 输入部件 4101 获取内容（步骤 S4012），并且将获取的内容输出给内容密钥生成部件 4102。

[0603] 内容密钥生成部件 4102 接收这些内容，利用随机数产生内容密钥（步骤 S4013），并且将产生的内容密钥和收到的内容输出给密钥块生成部件 4103。

[0604] 接收内容密钥和内容的时候，密钥块生成部件 4103 产生密钥块，并且将所产生的密钥块以及收到的内容密钥和内容输出给部分内容生成部件 4105（步骤 S4014）。

[0605] 部分内容生成部件 4105 从密钥块生成部件 4103 接收密钥块、内容密钥、内容。下一步，部分内容生成部件 4105 将收到的内容 4119 分裂，如图 51 所示，以产生 c 项部分内容（步骤 S4016），并且将所产生的 c 项部分内容放在一起来形成分裂内容 4120。下一步，部分内容生成部件 4105 产生分别对应于所产生的 c 项部分内容的多则标识信息（步骤 S4018），并且将所产生的分裂内容 4120 和 c 则标识信息，以及收到的密钥块、内容密钥和内容输出给报头信息生成部件 4107。

[0606] 报头信息生成部件 4107 从部分内容生成部件 4105 接收分裂内容、c 则标识信息、密钥块以及内容密钥，产生分别对应于收到的所述多则标识信息的标识信息标识符，并且进一步产生包括所产生的标识信息标识符和多则标识信息的内容位置信息 4140。更进一步，如图 51 所示，报头信息生成部件 4107 通过将构成收到的分裂内容 4120 的 c 项部分内容分别赋予散列函数来计算 c 个部分散列值，并且产生包括计算出来的 c 个部分散列值的报头信息 4160（步骤 S4019）。下一步，报头信息生成部件 4107 将所产生的内容位置信息 4140 和报头信息 4160 以及收到的密钥块和内容密钥输出给签名信息生成部件 4108。

[0607] 签名信息生成部件 4108 从报头信息生成部件 4107 接收内容位置信息 4140、报头信息 4160、密钥块和内容密钥。如图 51 所示，签名信息生成部件 4108 提取收到的报头信息中包括的 c 个部分散列值，将提取出来的 c 个部分散列值组合起来，并且通过将组合出来的结果赋予散列函数来计算组合后散列值（步骤 S4021）。

[0608] 下一步，签名信息生成部件 4108 从签名密钥存储部件 1112 读取签名密钥 1113（步骤 S4022）。如图 51 所示，签名信息生成部件 4108 通过将签名生成算法应用于所产生的组合后散列值，利用读取的签名密钥 1113 来产生签名信息 4170（步骤 S4023）。

[0609] 下一步，签名信息生成部件 4108 将所产生的签名信息、收到的内容位置信息 4140、报头信息 4160、分裂内容 4120 和内容密钥输出给加密处理部件 4109。

[0610] 加密处理部件 4109 接收签名信息、内容位置信息 4140、报头信息 4160、分裂内容 4120 和内容密钥，并且通过利用收到的内容密钥加密构成分裂内容 4120 的各项部分内容来产生已加密内容（步骤 S4024）。加密处理部件 4109 将所产生的已加密内容以及收到的签名 信息、内容位置信息 4140、报头信息 4160 和密钥块输出给记录部件 4114。

[0611] 记录部件 4114 接收已加密内容、签名信息、内容位置信息 4140、报头信息 4160 和密钥块，并且将收到的密钥块、内容位置信息 4140、报头信息 4160、签名信息、已加密内容写入 DVD 4500（步骤 S4026）。

[0612] 4.5.2 执行装置 4600 的工作状况

[0613] 图 52 和 53 是说明执行装置 4600 的工作状况的流程图。图 54 从原理上说明构成执行装置 4600 的各个组件处理的信息。注意，图 52 到 54 中同样的步骤号表示同样的处理。

[0614] 下面在图 52 到 54 的帮助下描述执行装置 4600 的工作状况。

[0615] 装载了 DVD 4500 的时候，获取部件 4601 从 DVD 4500 读取密钥块 4510、内容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580（步骤 S4041），并且将读取的这些组信息输出给内容密钥获取部件 4602。

[0616] 内容密钥获取部件 4602 接收密钥块 4510、内容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580，并且通过利用收到的密钥块 4510、装置标识符和装置密钥存储部件 1604 储存的装置密钥来产生内容密钥（步骤 S4042）。下一步，内容密钥获取部件 4602 将所产生的内容密钥以及收到的内容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580 输出给签名信息验证部件 4606。

[0617] 签名信息验证部件 4606 接收内容密钥、内容位置信息 4530、报头信息 4550、签名信息 4570 和已加密内容 4580，组合收到的报头信息 4550 中包括的 c 个部分散列值，并且通过将组合后结果赋予散列函数来产生签名验证组合后散列值（步骤 S4043）。下一步，签名信息验证部件 4606 从验证密钥存储部件 1612 读取验证密钥 1613（步骤 S4044），并且利用读取的验证密钥 1613 和所产生的签名验证组合后散列值来验证收到的签名信息 4570（步骤 S4046）。

[0618] 如果签名信息 4570 的验证不成功（步骤 S4048 :否），签名信息验证部件 4606 就退出执行装置 4600 中的后续处理。

[0619] 如果签名信息 4570 的验证成功（步骤 S4048 :是），签名信息验 证部件 4606 就将收到的内容密钥、内容位置信息 4530、报头信息 4550 和已加密内容 4580 输出给选择部件 4611。

[0620] 接收内容密钥、内容位置信息 4530、报头信息 4550 和已加密内容 4580 的时候，选择部件 4611 选择内容位置信息 4530 中包括的 c 则内容检测信息里选择 k 则（步骤 S4049）。下一步，选择部件 4611 产生由被选多则内容检测信息组成的被选位置信息 4620（步骤 S4051）。然后，选择部件 4611 在构成所产生的被选位置信息 4620 的 k 则内容检测信息里包括的标识信息标识符的基础之上，从收到的报头信息 4550 选择 k 则部分散列信息（步骤 S4053），并且产生由被选 k 则部分散列信息组成的选择报头信息 4630（步骤 S4056）。下一步，选择部件 4611 将所产生的被选位置信息 4620 和选择报头信息 4630 以及收到的内容密钥和已加密内容 4580 输出给部分内容解密部件 4616。

[0621] 部分内容解密部件 4616 接收被选位置信息 4620、选择报头信息 4630、内容密钥和已加密内容 4580，并且在如图 54 所示收到的被选位置信息 4620 中包括的多则标识信息的基础之上，从已加密内容 4580 提取 k 项已加密部分内容 4581、4582、4583、……、4586（步骤 S4057）。下一步，部分内容解密部件 4616 通过对提取的 k 项已加密部分内容 4581、4582、4583、……、4586 进行解密来产生多项部分内容（步骤 S4059）。下一步，部分内容解密部件 4616 产生包括收到的被选位置信息 4620 中包括的 k 个标识信息标识符，和产生的 k 项部分内容的验证内容 4650（步骤 S4061）。部分内容解密部件 4616 将所产生的验证内容 4650 以及收到的选择报头信息 4630、内容密钥和已加密内容 4650 输出给报头信息验证部件 4617。

[0622] 报头信息验证部件 4617 接收验证内容 4650、选择报头信息 4530、内容密钥和已加

密内容 4580。接收这些组信息的时候，报头信息验证部件 4617 通过分别将收到的验证内容 4650 中包括的 k 项部分内容 4591、4592、4593、……、4596 赋予散列函数来产生 k 个验证散列值（步骤 S4062），并且分别比较收到的报头信息中包括的 k 个部分散列值和对应的产生的验证散列值（步骤 S4064 ：是）。

[0623] 在 k 对的比较中，每一对由验证散列值和对应的部分散列值组成，当任意一对不一致的时候（步骤 S4066 ：否），报头信息验证部件 4617 退出执行装置 4600 中的后续处理。

[0624] 在 k 对的比较中，当所有 k 对都一致的时候（步骤 S4066 ：是），报头信息验证部件 4617 将收到的内容密钥和已加密内容 4580 输出给执行部件 2618。

[0625] 执行部件 2618 从报头信息验证部件 4617 接收内容密钥和已加密内容 4580，通过利用收到的内容密钥对构成收到的已加密内容 4580 的各个已加密部分内容进行解密来产生由 c 项部分内容组成的内容（步骤 S4067），扩展所产生的内容（步骤 S4068），并且让监视器显示扩展后的内容（步骤 S4071）。

[0626] 4.6 综述和有益效果

[0627] 如同已经描述过的一样，第四实施例的未授权内容检测系统由分发装置 4100 和执行装置 4600 组成，并且分发装置 4100 通过分裂内容来产生 c 项部分内容，并且进一步利用所有产生的 c 项部分内容来产生报头信息和验证信息。

[0628] 执行装置 4600 从构成已加密内容的 c 项已加密部分内容选择 k 项，并且从报头信息中包括的 c 个部分散列值提取与被选 k 项部分内容相对应的 k 个部分散列值。执行装置 4600 利用提取出来的 k 个部分散列值，只验证被选 k 项已加密部分内容。只有当验证成功的时候，执行装置 4600 才通过对已加密内容解密来产生内容，并且播放已解密内容。

[0629] 因此，通过将用于验证是否包括未授权内容的已加密部分内容的项数限制为 k 项，能够降低验证中涉及的处理负荷。

[0630] 每次执行装置 4600 进行验证的时候，通过利用随机数选择不同的一项已加密部分内容，能够弥补因为将用于验证的已加密部分内容的项数限制为 k 项而引起的检测未授权内容的准确度的下降。

[0631] 另外，很难预测会将哪些项已加密部分内容用于验证，因此能够防止利用未授权内容只是专门替换构成已加密内容的多项已加密部分内容中不用于验证的多项已加密部分内容这样的欺骗行为。

[0632] 5. 第五实施例

[0633] 下面描述本发明第五实施例的未授权内容检测系统。

[0634] 5.1 未授权内容检测系统

[0635] 第五实施例的未授权内容检测系统由分发装置、执行装置和监视器组成，如同第一实施例中一样。

[0636] 分发装置根据操作员的操作获取内容，并且通过对获取的内容进行加密来产生已加密内容。另外，分发装置产生单元拾取信息、报头信息和执行装置验证内容有效性的签名信息。

[0637] 分发装置获取 DVD 上可写区域的存储容量，以及所产生的可变信息的数据大小。

[0638] 分发装置计算填充容量，这个填充容量是通过从获取的存储容量中减去获取的各种信息的数据大小的总和来得到的，并且产生数据大小对应于计算出来的填充容量的填充

内容，并且将产生的填充内容与各种信息一起写入 DVD。

[0639] 5.2 分发装置 5100

[0640] 图 55 说明第五实施例的分发装置的结构。如图 55 所示，分发装置 5100 由输入部件 1101、内容密钥生成部件 1102、密钥块生成部件 1103、执行装置信息存储部件 1104、单元生成部件 5105、加密处理部件 5106、报头信息生成部件 5107、填充内容生成部件 5108、签名信息生成部件 5111、签名密钥存储部件 1112 和记录部件 5114 组成。

[0641] 下面描述构成分发装置 5100 的各个组件。注意，由于输入部件 1101、内容密钥生成部件 1102、密钥块生成部件 110、执行装置信息存储部件 1104 和签名密钥存储部件 1112 都与第一实施例的分发装置 1100 中的一样，因此省去了对这些组件的描述。

[0642] 5.2.1 单元生成部件 5105

[0643] 作为第一实施例中描述的单元生成部件 1105，单元生成部件 5105 从输入部件 1101 接收由 c 个文件 CNT1、CNT2、CNT3、……等等组成的内容，并且利用收到的内容产生单元拾取信息和分裂内容。产生单元拾取信息和分裂内容的程序与第一实施例的单元生成部件 1105 所执行的那些一样，并且这里产生的单元拾取信息和分裂内 容的结构分别在图 6 和 7 中说明，因此省去了对它们的说明。

[0644] 下一步，单元生成部件 5105 将所产生的分裂内容输出给加密处理部件 5106，同时将所产生的单元拾取信息输出给填充内容生成部件 5108。

[0645] 5.2.2 加密处理部件 5106

[0646] 加密处理部件 5106 从单元生成部件 5105 接收分裂内容，并且在收到的分裂内容的基础之上产生已加密分裂内容和已加密内容。产生这些已加密分裂内容和已加密内容的程序与第一实施例的加密处理部件 1106 执行的那些相同，所产生的已加密内容和已加密分裂内容的结构分别在图 9 和 10 中说明，因此省去了对它们的描述。

[0647] 下一步，加密处理部件 5106 将所产生的已加密分裂内容输出给报头信息生成部件 5107，同时将所产生的已加密内容输出给记录部件 5114 和填充内容生成部件 5108。

[0648] 5.2.3 填充内容生成部件 5108

[0649] 填充内容生成部件 5108 预存密钥块大小 KBSIZE、文件信息大小 FISIZE、单元散列大小 USIZE、文件散列大小 FSIZE、比率 RT 和分裂数 j。

[0650] 单元散列大小 USIZE 说明构成报头信息生成部件 5107 产生的第一散列表的多则单元散列信息的数据大小。具体而言，这里的单元散列信息与第一实施例的报头信息生成部件 1107 产生的单元散列信息相同。

[0651] 文件散列大小 FSIZE 说明构成报头信息生成部件 5107 产生的第二散列表的多则文件散列信息的位长度。具体而言，这里的文件散列信息与第一实施例的报头信息生成部件 1107 产生的文件散列信息一样。

[0652] 比率 RT 说明签名信息生成部件 5111 通过将签名生成算法 S 应用于信息 A 产生签名 SignA 的情况下，信息 A 和签名 SignA 之间的比特长度比。

[0653] 分裂数 j 是填充内容生成部件 5108 分裂填充内容所产生的单元的数量（后面将详细描述）。

[0654] 另外，填充内容生成部件 5108 预存 56 比特长度的不能回放信息 DAMY，表明不能播放填充内容。

[0655] 填充内容生成部件 5108 从单元生成部件 5105 接收单元拾取信息，同时从加密处理部件 5106 接收已加密内容。

[0656] 接收单元拾取信息和已加密内容的时候，填充内容生成部件 5108 利用收到的单元拾取信息和已加密内容，按照以下程序计算填充容量，并且基于计算出来的填充容量产生填充内容，更新单元拾取信息。

[0657] 下面详细描述上面提到的填充容量的计算 (a)，填充内容的产生 (b) 和单元拾取信息的更新 (c)。

[0658] (a) 填充容量计算

[0659] 填充容量表明将密钥块、单元拾取信息、报头信息、签名信息和已加密内容写上去以后，DVD 上的自由空间。下面描述产生填充容量的程序。

[0660] 首先，填充内容生成部件 5108 通过记录部件 5114 测量装载在记录部件 5114 上的 DVD 上可写区域的存储容量，并且产生表明将信息写入其中能够使用的最大存储容量 MSIZE。在这里，不是通过记录部件 5114 测量可写区域的存储容量，而是可以通过从操作员的输入来获得最大存储容量 MSIZE。

[0661] 下一步，填充内容生成部件 5108 测量收到的已加密内容的数据大小，并且产生内容大小 CNSIZE。

[0662] 下一步，填充内容生成部件 5108 对收到的内容拾取信息中包括的文件信息的则数 c 进行计数，并且利用以下公式计算更新以后单元拾取信息的数据大小 UCSIZE（在 (c) 中对单元拾取信息更新的以下描述中将描述细节）：

[0663] UCSIZE = FISIZE×(c+1)。

[0664] 下一步，填充内容生成部件 5108 提取收到的单元拾取信息中包括的 c 个单元数 N1、N2、N3、……、Nc，并且利用提取的单元数 N1、N2、N3、……、Nc 和储存的分裂数 j，通过利用以下公式计算报头信息生成部件 5107 产生的第一散列表（后面将详细描述）的 (c+1) 个的数据大小的总和 HA1SIZE：

[0665] HA1SIZE = [N1+N2+N3+…+Nc+j]×USIZE。

[0666] 随后，填充内容生成部件 5108 利用以下公式产生由报头信息生成部件 5107 产生的第二散列表（后面将详细描述）的数据大小 HA2SIZE：

[0667] HA2SIZE = FSIZE×(c+1)，

[0668] 并且利用以下公式，从所产生的第一散列表的数据大小 HA1SIZE 和第二散列表的数据大小 HA2SIZE 的总和，计算报头信息生成部件 5107 产生的报头信息的数据大小 HEADSIZE：

[0669] HEADSIZE = HA1SIZE+HA2SIZE。

[0670] 下一步，填充内容生成部件 5108 利用以下公式计算 SigSIZE，它表明签名信息生成部件 5111 产生的签名信息的的数据大小：

[0671] SigSIZE = (UCSIZE+HA2SIZE)×RT。

[0672] 下一步，填充内容生成部件 5108 利用以下公式计算填充内容 FilSIZE：

[0673] FilSIZE = MSIZE-[KBSIZE+UCSIZE+HEADSIZE+SigSIZE]。

[0674] (b) 填充内容的产生

[0675] 已经计算了填充容量 FilSIZE 的时候，填充内容生成部件 5108 产生一个随机数，

并且将所产生的随机数与不能回放信息 DAMY 组合起来产生数据大小是 FilSIZE 的填充内容。

[0676] 下一步，填充内容生成部件 5108 产生用于专门表明所产生的填充内容的文件标识符 FIDf，以及用于标识所产生的填充内容的文件标识信息 ADf。下一步，填充内容生成部件 5108 基于储存的分裂数 j，将所产生的分裂内容分裂成 j 个单元 Uf_1、Uf_2、Uf_3、……、Uf_j，并且产生单元标识符 UIDf_1、UIDf_2、UIDf_3、……、UIDf_j，每一个都对应于单元之一。在这里，在这以后将单元和对应的单元标识符构成的一对叫做“（一则）单元信息”。另外，填充内容生成部件 5108 产生由 j 则单元信息组成的分裂填充内容。图 56 说明在这一点产生的分裂填充内容的结构。如图 56 所示，分裂填充内容 5120 由多则单元信息 5121、5122、5123、……、5126 组成，每一则单元信息 都包括一个单元标识符和一个单元。例如，所述则单元信息 5121 包括单元标识符 UIDf_1 5131 和单元 Uf_1 5132。从填充内容产生分裂填充内容的程序与从文件产生分裂文件的程序相同，因此这里只对其进行简单描述。

[0677] 在这里，将所产生的文件标识符 FIDf 和分裂填充内容 5120 所构成的一对叫作填充文件信息。

[0678] (c) 单元拾取信息更新

[0679] 已经产生了填充内容和分裂填充内容 5120 的时候，填充内容生成部件 5108 产生由所产生的文件标识符 FIDf、所产生的所述则文件标识信息 ADf 和表明所产生的单元数目的单元数 Nf 组成的一则文件信息，并且将所产生的这一则文件信息添加到收到的单元拾取信息中去。图 57 说明将产生的所述则文件信息加到上面去以后的单元拾取信息 5140。所述单元拾取信息 5140 由 (c+1) 则文件信息 5141、5142、5143、……、5146 和 5147 组成，每一则文件信息都包括文件标识符、一则文件标识信息和单元数。多则文件信息 5141、5124、5143、……、5146 是由单元生成部件 5105 基于所述内容产生的，并且与构成图 7 所示的单元拾取信息 1200 的多则文件信息 1201、1202、1203、……、1204 相同。所述则文件信息 5147 是由填充内容生成部件 5108 基于填充内容产生的，并且包括与填充内容、一则文件标识信息 AD1 5152 和单元数 Nf 5153 相对应的文件标识符 FIDf 5151。

[0680] 下一步，填充内容生成部件 5108 将所产生的填充内容和单元拾取信息 5140 输出给记录部件 5114；将所产生的填充文件信息输出给报头信息生成部件 5107；将单元拾取信息 5140 输出给签名信息生成部件 5111。

[0681] 5.2.4 报头信息生成部件 5107

[0682] 报头信息生成部件 5107 从加密处理单元 5106 接收已加密分裂内容，同时从填充内容生成部件 5108 接收包括文件标识符 FIDf 和一则分裂填充内容 5120 的填充文件信息 5156。

[0683] 接收填充文件信息 5156 和已加密分裂内容 5160 的时候，报头信息生成部件 5107 从收到的多组信息产生报头信息 5190，如图 58 所 示。图 58 说明，报头信息生成部件 5107 执行的报头信息 5190 的产生程序的的概要。下面在图 58 的帮助下描述报头信息 5190 的产生程序。

[0684] 报头信息生成部件 5107 从收到的已加密分裂内容 5160 产生第一散列表 HA1TBL1 5171、HA1TBL2 5172、HA1TBL3 5173、……、HA1TBLc 5176。在这里产生的第一散列表 HA1TBL1 5171、HA1TBL25172、HA1TBL3 5173、……、HA1TBLc 5176 与第一散列表

HA1TBL11261、HA1TBL2 1262、HA1TBL3 1263、……、HA1TBLc 1264 相同，并且产生程序也相同。因此省去了对这些第一散列表的描述。

[0685] 下一步，报头信息生成部件 5107 基于收到的填充文件信息 5156 中包括的填充内容，产生第一散列表 HA1TBLf5177。产生程序与从已加密分裂文件产生第一散列表的程序相同，因此省去了对它的描述。

[0686] 下一步，报头信息生成部件 5107 分别基于 (c+1) 个第一散列表计算文件散列值，产生多则文件散列信息，每一则都包括计算出来的 (c+1) 个文件散列值中的一个，以及对应于文件散列值的文件标识符，并且进一步产生由所产生的 (c+1) 则文件信息组成的第二散列表 HA2TBL 5180。产生第二散列表的具体程序与第一实施例中第二散列表 1269 的产生程序相同，除了使用从填充内容生成部件 5108 接收的文件标识符 FIDf 5157 和分裂填充内容 5120 不同以外，因此省去了对它的描述。

[0687] 图 59 说明在这一点产生的第二散列表 HA2TBL 5180 的结构。第二散列表 HA2TBL 5180 由 (c+1) 则文件散列信息 5181、5182、5183、……、5186 和 5187 组成。每一则文件散列信息都包括文件标识符和文件散列值。从已加密分裂内容 5160 产生多则文件散列信息 5181 到 5186，并且它们与构成第一实施例中描述的第二散列表 HA2TBL 1269 的多则文件散列信息 1301 到 1304 相同。所述则文件散列信息 5187 是在填充文件信息 5156 的基础之上产生的。

[0688] 报头信息生成部件 5107 将所产生的第二散列表 5180 输出给签名信息生成部件 5111，同时将包括所产生的 (c+1) 个第一散列表和第二 散列表 HA2TBL 5180 的报头信息 5190 输出给记录部件 5114。

[0689] 5.2.5 签名信息生成部件 5111

[0690] 签名信息生成部件 5111 从填充内容生成部件 5108 接收单元拾取信息 5140，同时从报头信息生成部件 5107 接收第二散列表 HA2TBL5180。

[0691] 接收单元拾取信息 5140 和第二散列表 HA2TBL 5180 的时候，签名信息生成部件 5111 读取签名密钥存储部件 1112 记录的签名密钥 1113。

[0692] 下一步，签名信息生成部件 5111 通过将签名生成算法 S 应用于组合结果利用读取的签名密钥 1113 来产生签名信息，其中的组合结果是通过将构成收到的第二散列表 HA2TBL 5180 的 (c+1) 个文件散列值与构成收到的单元拾取信息 5140 的 (c+1) 则文件信息组合起来形成的。

[0693] 下一步，签名信息生成部件 5111 将所产生的签名信息输出给记录部件 5114。

[0694] 5.2.6 记录部件 5114

[0695] 在记录部件 5114 中装载 DVD。

[0696] 记录部件 5114 响应填充内容生成部件 5108 的指令，测量装载的 DVD 上可写区域的存储容量。

[0697] 记录部件 5114 从密钥块生成部件 1103 接收密钥块；从加密处理部件 5106 接收已加密内容；并且从填充内容生成部件 5108 接收填充内容和单元拾取信息 5140。另外，记录部件 5114 从报头信息生成部件 5107 接收报头信息 5190，同时从签名信息生成部件 5111 接收签名信息。

[0698] 接收这些组信息的时候，记录部件 5114 将收到的密钥块、已加密内容、填充内容、

单元拾取信息 5140、报头信息 5190 和签名信息写入 DVD。

[0699] 5.3DVD 5500

[0700] 图 60 说明第五实施例的 DVD 中存储的信息。如图 60 所示，DVD5500 储存密钥块 5510、单元拾取信息 5530、报头信息 5550、已加密 内容 5580 和填充内容 5590。

[0701] 这些组信息已经由分发装置 5100 写入。各组信息的结构和上面描述的一样，因此省去了对它们的描述。

[0702] 5.4 执行装置 5600

[0703] 如图 61 所示，执行装置 5600 由获取部件 1601、内容密钥获取部件 1602、装置密钥存储部件 1604、执行部件 5606、签名信息验证部件 5611 和验证密钥存储部件 1612 组成。

[0704] 下面描述构成执行装置 5600 的各个组件。注意，由于获取部件 1601、内容密钥获取部件 1602 和验证密钥存储部件 1612 与第一实施例中的一样，因此，省去了对这些组件的描述。

[0705] 5.4.1 签名信息验证部件 5611

[0706] 签名信息验证部件 5611 从获取部件 1601 接收单元拾取信息 5530 和签名信息 5570。

[0707] 接收这些组信息的时候，签名信息验证部件 5611 利用收到的单元拾取信息 5530 和 DVD 5500 中储存的报头信息 5550、已加密内容 5580 和填充内容 5590 验证收到的签名信息 5570。省去了验证的具体程序，因为它与构成第一实施例的执行装置 1600 的签名信息验证部件 1611 所进行的签名信息的验证相同，只有在已加密内容 5580 以外使用了填充内容 5590 不同除外。

[0708] 5.4.2 执行部件 5606

[0709] 执行部件 5606 预存 56 比特长度的不能回放信息 DAMY。

[0710] 执行部件 5606 从内容密钥获取部件 1602 接收内容密钥 CK。另外，执行部件 5606 还可以从签名信息验证部件 5611 接收回放禁止信息。

[0711] 接收内容密钥 CK 的时候，执行部件 5606 通过获取部件 1601 一个一个地读取构成已加密内容 5580 的已加密文件 ECNT1、ECNT2、ECNT3、……、ECNTc 或者填充内容 5590。

[0712] 执行部件 5606 将读取的已加密文件的前 56 比特或者读取的填充内容的前 56 比特与储存的不能回放信息 DAMY 进行比较。当两者互不相同的时候，读取的信息是已加密文件并且是可播放的，因此执行 部件 5606 通过利用收到的内容密钥 CK 针对每个单元对读取的已加密文件进行解密来产生文件。下一步，执行部件 5606 扩展产生的文件来产生视频和音频数据，从产生的视频和音频数据产生视频和音频信号，并且通过将产生的视频和音频信号输出给监视器来播放内容。

[0713] 当前 56 比特与储存的播放不能回放信息 DAMY 相同的时候，读取的信息是填充内容，不能播放，因此执行部件 5606 退出上述解密、扩展和回放过程，开始处理下一个已加密文件。

[0714] 直到已经完成了所有已加密文件和填充内容的读取，执行部件 5606 在类似程序中重复读出、与不能回放信息 DAMY 的比较、解密、扩展和回放。

[0715] 如果在上述重复期间从签名信息验证部件 5611 接收回放禁止信息，执行部件 5606 退出重复。

[0716] 5.5 工作状况

[0717] 下面描述第五实施例的分发装置 5100 和执行装置 5600 的工作状况。

[0718] 5.5.1 分发装置 5100 的工作状况

[0719] 下面在图 62 和 63 所示的流程图的帮助下描述分发装置 5100 的工作状况。

[0720] 分发装置 5100 的输入部件 5101 接收内容的输入（步骤 S5011），将接收的内容输出给单元生成部件 5105，并且指令内容密钥生成部件 1102 产生内容密钥。

[0721] 内容密钥生成部件 1102 根据输入部件 1101 的指令产生内容密钥（步骤 S5012），并且将产生的内容密钥输出给密钥块生成部件 1103 和加密处理部件 5106。

[0722] 密钥块生成部件 1103 接收内容密钥。接收内容密钥的时候，密钥块生成部件 1103 从执行装置信息存储部件 1104 读取装置标识表（步骤 S5013），并且基于收到的内容密钥和读取的装置标识表产生密钥块（步骤 S5016）。下一步，密钥块生成部件 1103 将产生的密钥块输出给记录部件 5114。

[0723] 接收内容的时候，单元生成部件 5105 将构成接收到的内容的每 个文件分裂成单元来产生分裂内容（步骤 S5017）。已经产生了分裂内容的时候，单元生成部件 5105 产生由分别对应于分裂文件的多则文件信息组成的单元拾取信息（步骤 S5018），并且在将分裂内容输出给加密处理部件 5106 的同时将产生的单元拾取信息输出给填充内容生成部件 5108。

[0724] 接收内容密钥和分裂内容的时候，加密处理部件 5106 通过利用内容密钥对收到的分裂内容中包括的内容的每一个单元进行加密来产生已加密分裂内容（步骤 S5019）。加密处理部件 5106 提取所产生的已加密分裂内容中包括的已加密单元，产生已加密内容（步骤 S5021），并且将所产生的已加密内容输出给记录部件 5114 和填充内容生成部件 5108，同时输出所产生的已加密分裂内容给报头信息生成部件 5107。

[0725] 接收单元拾取信息和已加密内容的时候，填充内容生成部件 5108 通过记录部件 5114 获得 DVD 5500 的最大存储容量（步骤 S5022），并且测量收到的已加密内容的数据大小（步骤 S5023）。

[0726] 下一步，填充内容生成部件 5108 基于收到的单元拾取信息计算报头信息的数据大小和签名信息的数据大小（步骤 S5026），并且进一步基于获得的最大存储容量、报头信息和签名信息的数据大小等等计算填充容量（步骤 S5028）。

[0727] 下一步，填充内容生成部件 5108 通过将不能回放信息和随机数组合起来产生具有计算出来的填充容量的数据大小的填充内容（步骤 S5029），并且产生与填充内容对应的文件标识符和文件标识信息（步骤 S5031）。

[0728] 填充内容生成部件 5108 通过基于储存的分裂数 j 将产生的分裂内容分裂成 j 个单元来产生分裂填充内容（步骤 S5032）。

[0729] 下一步，填充内容生成部件 5108 产生包括所产生的文件标识符和标识信息的文件信息，以及表明所产生的单元数量的单元数，并且将所产生的文件信息添加到收到的单元拾取信息中去（步骤 S5033）。填充内容生成部件 5108 将所产生的填充内容和单元拾取信息 5140 输出给记录部件 5114；将所产生的文件标识符和分裂填充内容 5120 组 成的填充文件信息 5156 输出给报头信息生成部件 5107；以及将单元拾取信息 5140 输出给签名信息生成部件 5111。

[0730] 接收已加密分裂内容和填充文件信息 5156 的时候，报头信息生成部件 5107 从收到的已加密分裂内容中包括的 c 个已加密分裂文件产生 c 个第一散列表（步骤 S5034）。接下来，报头信息生成部件 5107 从收到的填充文件信息 5156 中包括的分裂填充内容产生第一散列表（步骤 S5036）。

[0731] 报头信息生成部件 5107 基于所产生的 (c+1) 个第一散列表产生第二散列表（步骤 S5037），产生包括 (c+1) 个第一散列表和第二散列表的报头信息（步骤 S5039），并且将产生的报头信息输出给记录部件 5114，同时将产生的第二散列表输出给签名信息生成部件 5111。

[0732] 接收单元拾取信息 5140 和第二散列表的时候，签名信息生成部件 5111 通过将签名生成算法应用于收到的单元拾取信息和第二散列表来产生签名信息（步骤 S5041），并且将产生的签名信息输出给记录部件 5114。

[0733] 接收密钥块、已加密内容、填充内容、单元拾取信息、报头信息和签名信息的时候，记录部件 5114 将收到的密钥块、已加密内容、填充内容、单元拾取信息、报头信息和签名信息写入 DVD 5500（步骤 S5042）。

[0734] 5.5.2 执行装置 5600 的工作状况

[0735] 下面在图 64 和 65 所示的流程图的帮助下描述执行装置 5600 的工作状况。

[0736] 装载了 DVD 5500 的时候，获取部件 1601 从 DVD 5500 读取密钥块 5510、单元拾取信息 5530 和签名信息 5570，并且将密钥块 5510 输出给内容密钥获取部件 1602，同时将单元拾取信息 5530 和签名信息 5570 输出给签名信息验证部件 1611（步骤 S5061）。

[0737] 签名信息验证部件 5611 接收单元拾取信息 5530 和签名信息 5570，利用随机数和单元拾取信息 5530 从已加密内容 5580 中包括的多个已加密单元以及填充内容 5590 中包括的 j 个单元里选择出 i 个，利用被选 i 个和报头信息产生 i 个被替换第一散列表（步骤 S5063）。

[0738] 签名信息验证部件 5611 从所产生的 i 个被替换散列表中的每一个计算替换文件散列值（步骤 S5064）。

[0739] 下一步，签名信息验证部件 5611 从 DVD 5500 读取第二散列表（步骤 S5066），并且通过利用替换散列值替换与所产生的 i 个替换文件散列值相对应的文件散列值来产生被替换第二散列表（步骤 S5068）。签名信息验证部件 5611 利用所产生的被替换第二散列表、收到的单元拾取信息 5530 和验证密钥存储部件 1612 中储存的验证密钥 1613 来验证签名信息 5570（步骤 S5069）。如果签名信息 5570 的验证不成功（步骤 S5071 :否），签名信息验证部件 5611 就将回放禁止信息输出给执行部件 5606（步骤 S5073）。

[0740] 签名信息 5570 的验证成功的时候（步骤 S5071 :是），签名信息验证部件 5611 就结束这一验证。

[0741] 内容密钥获取部件 1602 接收密钥块 5510，并且从装置密钥存储部件 1604 读取装置标识符和装置密钥（步骤 S5074）。内容密钥获取部件 1602 从读取的装置标识符、装置密钥和密钥块 5510 产生内容密钥 CK，并且将产生的内容密钥 CK 输出给执行部件 5606（步骤 S5076）。

[0742] 执行部件 5606 从内容密钥获取部件 1602 接收内容密钥。在这里，如果从签名信息验证部件 5611 接收回放禁止信息（步骤 S5077 :是），执行部件 5606 就通知用户 DVD 5500

中储存的内容不能回放（步骤 S5079），并且退出后续回放。

[0743] 如果没有接收回放禁止信息（步骤 S5077 ：否），执行部件 5606 就读取构成已加密内容和填充内容的 c 个已加密文件之一（步骤 S5081）。执行部件 5606 将读取的已加密文件或者前 56 比特填充内容与预存的不能回放信息进行比较（步骤 S5082）。当这两者一致的时候（步骤 S5084 ：是），执行部件 5606 返回步骤 S5077。

[0744] 当这两者不一致的时候（步骤 S5084 ：否），读取的文件就是已加密文件并且是可播放的。因此，执行部件 5606 通过利用收到的内容密钥对已加密文件进行解密来产生文件（步骤 S5086），扩展产生的文件（步骤 S5087），并且让监视器播放扩展的文件（步骤 S5089）。 已经读取了构成已加密内容和填充内容的全部已加密文件，或者从用户得到指令完成回放的时候（步骤 S5091 ：是），执行部件 5606 结束回放。如果没有读完构成已加密内容和填充内容的所有已加密文件，并且执行部件 5606 没有从用户收到结束回放的指令（步骤 S5091 ：否），执行部件 5606 就回到步骤 S5077，重复步骤 5077 到 5091 的处理。

[0745] 5.6 综述和有益效果

[0746] 如同已经描述的一样，在本实施例中，除了包括已加密内容的各种信息以外，DVD 5500 储存具有适当数据大小的填充内容，从而不在 DVD 5500 中留下可写存储区域。更进一步，报头信息和签名信息不仅是基于已加密内容而且是还基于填充内容而产生的。

[0747] 构成执行装置 5600 的执行部件 5606 顺序读取 DVD 5500 上写下的文件，并且将各个读取的文件的前 56 比特与预存的不能回放信息进行比较。当这两者一致的时候，提取部件 5606 判定读取的文件是填充内容，并避免回放这一文件。

[0748] 当 DVD 5500 没有储存这种填充内容的时候，可以推断存在下面描述的两种欺骗行为。

[0749] 图 65 说明 DVD 5500b 的结构，它是通过将包含未授权内容的文件添加到合法权利持有人产生的 DVD 5500a 而创建的。

[0750] DVD 5500a 将报头信息、单元拾取信息、签名信息存入区域 5703，同时在区域 5704、5705、……、5707 中储存构成已加密内容的各个已加密文件。除了这些组信息以外，DVD 5500a 还分别在区域 5701 和区域 5702 里储存文件表和回放顺序文件。

[0751] 储存在区域 5701 里的文件表包括 DVD 5500 中储存的所有文件的文件标识符、文件的起始地址以及 DVD 上各个文件占据的扇区号，将各个文件的文件标识符、起始地址和扇区号联系起来。例如，将具有文件标识符 FID1 的文件储存在从地址 0xAA1 开始的 70 个扇区里。

[0752] 区域 5702 里储存的回放顺序文件说明 DVD 中储存的文件的回放顺序。在这里的实例中，将按照从具有文件标识符 FIF1 的文件到具有文件标识符 FIDc 的文件的顺序播放文件。

[0753] 另外，DVD 5500a 上的区域 5711 里没有储存任何东西。

[0754] 在这种情况下，假设未授权第三人已经将包括未授权内容的文件写入 DVD 5500a 的区域 5711 中，并且通过伪造文件表和回放顺序文件产生了 DVD 5500b。

[0755] 在 DVD 5500b 上的区域 5701 里，添加了对应于未授权文件的文件标识符 FIDx、未授权文件的起始地址 0xAAx 和扇区号 200。另外，还伪造了区域 5702 中储存的回放顺序文件，从而将利用具有文件标识符 FIDx 的文件开始回放。

[0756] 另外，还考虑通过将未授权内容添加到DVD 5500a中的有效文件里去产生图66所示DVD 5500c的情况。

[0757] DVD 5500c将未授权内容存入区域5711，该区域紧跟在区域5707里有效地记录的文件后面。已经将文件表中与区域5707里储存的文件对应的扇区号伪造成320，它是通过将原来存入文件的扇区号加上储存了添加了未授权内容的扇区数得到的。已经改变了回放顺序文件，因而回放将从具有文件标识符FIDc的文件中的第51个扇区，也就是添加的未授权内容开始。

[0758] 于是，已经进行了未授权伪造的时候，由于报头信息、单元拾取信息、签名信息和已加密内容还根本没有被伪造，因此一旦签名信息的验证正常完成，执行装置会根据顺序文件表明的顺序读取未授权文件和开始回放。

[0759] 在本实施例中，在DVD 5500上没有留下可写存储区域，因为存在填充内容。另外，还将填充内容用于产生签名信息。因此，如果用未授权文件替换填充内容，那么执行装置5600中签名信息的验证将不会成功，回放将会退出。

[0760] 6. 第六实施例

[0761] 下面描述本发明的第六实施例。

[0762] 6.1 未授权内容检测系统

[0763] 第六实施例的未授权内容检测系统由分发装置、执行装置和监视器组成，如同第一实施例中的未授权内容检测系统一样。

[0764] 除了第一实施例中描述的密钥块、单元拾取信息、已加密内容、 报头信息和签名信息以外，分发装置产生区域信息，用于表明DVD上储存了分发装置有效地写下的信息的存储区域，并且将产生的区域信息写在DVD上。

[0765] 执行装置从DVD读取区域信息，并且只读取被读取的区域信息表明的存储区域内储存的信息。

[0766] 6.2 分发装置6100

[0767] 图67说明构成第六实施例的未授权内容检测系统的分发装置的结构。如图67所示，分发装置6100由输入部件1101、内容密钥生成部件1102、密钥块生成部件6103、执行装置信息存储部件1104、单元生成部件6105、加密处理部件6106、报头信息生成部件6107、分配生成部件6108、区域信息生成部件6109、签名信息生成部件6111、签名密钥存储部件1112和记录部件6114组成。

[0768] 下面描述组成分发装置6100的各个组件。注意，由于输入部件1101、内容密钥生成部件1102、执行装置信息存储部件1104和签名密钥存储部件1112与第一实施例中的分发装置1100中的一样，因此省去了对这些组件的描述。

[0769] 在这里，代替记录部件输出密钥块、单元拾取信息、已加密内容和报头信息，密钥块生成部件6103、单元生成部件6105、加密处理部件6106以及报头信息生成部件6107各自输出自己产生的信息到分配生成部件6108。除了这一点以外，密钥块生成部件6103、单元生成部件6105、加密处理部件6106和报头信息生成部件6107分别与第一实施例中的密钥块生成部件1103、单元生成部件1105、加密处理部件1106和报头信息生成部件1107一样，因此省去了对这些组件的描述。

[0770] 6.2.1 分配生成部件6108

[0771] 分配生成部件 6108 预存签名信息生成部件 6111 产生的签名信息的最大数据大小。另外，分配生成部件 6108 储存区域信息生成部件 6109 产生的区域信息的数据大小。

[0772] 分配生成部件 6108 从密钥块生成部件 6103 接收密钥块；从单元生成部件 6105 接收单元拾取信息；从加密处理部件 6106 接收已加密 内容；并且从报头信息生成部件 6107 接收报头信息。

[0773] 接收这些组信息的时候，分配生成部件 6108 产生如图 68 所示的写入分配信息 6120。写入分配信息 6120 是通过按照在 DVD 上一样的结构安排收到的所述多组信息，并且将安排好的所述多组信息写在存储器上来创建的。下面在图 68 的帮助下描述产生写入分配信息 6120 的程序。

[0774] 分配生成部件 6108 将密钥块写入存储器上的区域 6121 里；将单元信息写入区域 6122 里；并且将报头信息写入区域 6123 里。

[0775] 下一步，分配生成部件 6108 获得分别与储存的区域信息和签名信息的最大数据大小相对应的区域 6124 和 6125。然后，分配生成部件 6108 将已加密内容写入区域 6125 后面的区域 6126。

[0776] 分配生成部件 6108 将产生的写入分配信息 6120 输出给区域信息生成部件 6109 和记录部件 6114。

[0777] 注意，图 68 所示的信息组的分配顺序仅仅是一个实例，本发明不限于这个实例。

[0778] 在这里，分配生成部件 6108 储存签名信息的最大数据大小。但是，分配生成部件 6108 可以例如按照与第五实施例的填充内容生成部件 5108 一样的方式计算签名信息的数据大小。

[0779] 6.2.2 区域信息生成部件 6109

[0780] 区域信息生成部件 6109 从分配生成部件 6108 接收写入分配信息 6120。接收写入分配信息 6120 的时候，区域信息生成部件 6109 从收到的写入分配信息 6120 产生区域信息。区域信息是用于表明在上面储存了分发装置 6100 写入的有效信息的 DVD 上的区域的信息。区域信息是例如将写入分配信息 6120 写在 DVD 上的起始位置（以后叫做起始地址）和结束位置（结束地址）构成的一对。

[0781] 区域信息不限于这一实例，可以采用任何信息，比如储存有效信息的起始地址和扇区数构成的一对，只要这些信息能够表明有效信息储存的区域就行。

[0782] 区域信息生成部件 6109 将产生的区域信息输出给签名信息生成部件 6111 和记录部件 6114。

[0783] 6.2.3 签名信息生成部件 6111

[0784] 签名信息生成部件 6111 从单元生成部件 6105 接收单元拾取信息；从报头信息生成部件 6107 接收第二散列表；并且从区域信息生成部件 6109 接收区域信息。

[0785] 接收这些组信息的时候，签名信息生成部件 6111 从签名密钥存储部件 1112 读取签名密钥 1113。

[0786] 下一步，签名信息生成部件 6111 通过将签名生成算法 S 应用于组合结果，利用读取的签名密钥 1113 来产生签名信息，其中的组合结果是通过将收到的第二散列表中包括的 c 个文件散列值，构成单元拾取信息的 c 则文件信息，以及收到的区域信息组合在一起形成的。

[0787] 下一步，签名信息生成部件 6111 将产生的签名信息输出给记录部件 6114。

[0788] 6.2.4 记录部件 6114

[0789] 记录部件 6114 装载了 DVD。

[0790] 记录部件 6114 从分配生成部件 6108 接收写入分配信息 6120；从区域信息生成部件 6109 接收区域信息；并且从签名信息生成部件 6111 接收签名信息。

[0791] 接收这些组信息的时候，记录部件 6114 将收到的区域信息插入写入分配信息 6120 中的区域 6124，同时将签名信息插入区域 6125。

[0792] 已经将区域信息和签名信息插入写入分配信息 6120 以后，记录部件 6114 将写入分配信息 6120 写入 DVD。

[0793] 6.3DVD 6500

[0794] 图 69 说明第六实施例的 DVD 中储存的信息。如图 69 所示，DVD6500 储存密钥块 6510、单元拾取信息 6530、报头信息 6550、区域信息 6560、签名信息 6570 和已加密内容 6580。这些已经由分发装置 6100 写入，因此省去了对它们的描述。

[0795] 6.4 执行装置 6600

[0796] 图 70 说明第六实施例的执行装置的结构。如图 70 所示，执行装置 6600 由驱动部件 6620 和内容执行部件 6625 组成。

[0797] 驱动部件 6620 由获取部件 6601、区域信息存储部件 6603、加密 通信部件 6604 和加密密钥存储部件 6605 组成。

[0798] 内容执行部件 6625 由内容密钥获取部件 1602、装置密钥存储部件 1604、解密通信部件 6607、解密密钥存储部件 6608、签名信息验证部件 6611、验证密钥存储部件 1612 和执行部件 6606 组成。

[0799] 下面描述构成执行装置 6600 的各个组件。注意，由于内容密钥获取部件 1602、装置密钥存储部件 1604 和验证密钥存储部件 1612 与第一实施例中的执行装置 1600 中的一样，因此省去了对这些组件的描述。

[0800] 6.4.1 获取部件 6601

[0801] 获取部件 6601 装载了 DVD 6500。装载了 DVD 6500 的时候，获取部件 6601 首先读取区域信息 6560，然后将读取的区域信息写入区域信息存储部件 6603，并且将读取的区域信息 6560 输出给加密通信部件 6604。

[0802] 下一步，获取部件 6601 从 DVD 6500 读取密钥块 6510、单元拾取信息 6530 和签名信息 6570，并且将读取的密钥块 6510 输出给内容密钥获取部件 1602，同时将读取的单元拾取信息 6530 和签名信息 6570 输出给签名信息验证部件 6611。

[0803] 另外，获取部件 6601 从签名信息验证部件 6611 和执行部件 1606 接收读取各组信息的请求。接收读出请求的时候，签名信息验证部件 6611 从区域信息存储部件 6603 读取区域信息。将被请求的一组信息储存在区域信息表明的区域里的时候，获取部件 6601 从 DVD 6500 读取被请求的信息，并且将读取的信息输出给请求源，也就是签名信息验证部件 6611 或者执行部件 1606。

[0804] 被请求的那组信息没有储存在读取的区域信息表明的区域里的时候，获取部件 6601 输出表明不能读取被请求的那组信息的一个错误通知信号。

[0805] 6.4.2 区域信息存储部件 6603

[0806] 区域信息存储部件 6603 由例如 RAM 组成，并且储存获取部件 6601 写入的区域信息。

[0807] 6.4.3 加密通信部件 6604 和加密密钥存储部件 6605

[0808] 加密密钥存储部件 6605 由例如 ROM 组成，并且储存 56 比特长度的加密密钥。

[0809] 加密通信部件 6604 从获取部件 6601 接收区域信息 6560。接收区域信息 6560 的时候，加密通信部件 6604 从加密密钥存储部件 6605 读取加密密钥，并且通过将加密算法 E2 应用于读取的加密密钥来产生已加密区域信息。在这里，作为一个实例，将 DES（数据加密标准）用作加密算法 E2。

[0810] 下一步，加密通信部件 6604 将产生的已加密区域信息输出给解密通信部件 6607。

[0811] 6.4.4 解密通信部件 6607 和解密密钥存储部件 6608

[0812] 解密密钥存储部件 6608 由例如 ROM 组成，并且储存 56 比特长度的解密密钥。在这里，解密密钥与加密密钥存储部件 6605 储存的加密密钥相同。

[0813] 解密通信部件 6607 从加密通信部件 6604 接收已加密区域信息。接收已加密区域信息的时候，解密通信部件 6607 从解密密钥存储部件 6608 读取解密密钥，并且通过将解密算法 D2 应用于收到的已加密区域信息，利用读取的解密密钥来产生区域信息。在这里，解密算法 D2 是用于对使用加密算法 E2 产生的已加密文本进行解密时使用的算法。

[0814] 下一步，解密通信部件 6607 将产生的区域信息输出给签名信息验证部件 6611。

[0815] 给出上面的描述的时候假定了加密密钥和解密密钥相同，并且解密通信部件 6607 使用对称密钥加密系统。但是，本发明不限于这样，而是可以使用公钥加密系统。也可以将公钥加密系统和对称密钥加密系统组合在一起，在每次进行通信的时候产生不同的密钥，并且可以使用产生的密钥进行密码通信 (cipher communication)。

[0816] 另外，在这里只是对区域信息进行加密，然后输出给内容执行部件 6625，但是，在内容执行部件 6625 和驱动部件 6620 之间发送和接收的所有信息都可加密。

[0817] 6.4.5 签名信息验证部件 6611

[0818] 签名信息验证部件 6611 从获取部件 6601 接收单元拾取信息 6530 和签名信息 6570；并且从解密通信部件 6607 接收区域信息。

[0819] 接收单元拾取信息 6530 和签名信息 6570 的时候，签名信息验证部件 6611 基于已收到单元拾取信息 6530 和已加密内容 6580 以及 DVD 6500 中储存的报头信息 6550 来产生被替换的第二散列表。产生被替换的第二散列表的程序与第一实施例的签名信息验证部件 1611 执行的被替换第二散列表的产生程序相同，因此省去了对它的描述。

[0820] 下一步，签名信息验证部件 6611 从验证密钥存储部件 1612 读取验证密钥 1613。然后，签名信息验证部件 6611 通过将签名验证算法 V 应用于组合结果，利用读取的验证密钥 1613 来产生签名验证信息，其中的组合结果是通过将产生的被替换第二散列表中包括的所有文件散列值和替换文件散列值，收到的单元拾取信息 6530 中包括的所有则文件信息，以及区域信息组合起来形成的。签名信息验证部件 6611 将产生出来的签名验证信息与收到的签名信息 6570 进行比较。

[0821] 这两者不一致的时候，签名信息验证部件 6611 判定签名信息的验证不成功，并且将回放禁止信息输出给执行部件 1606。

[0822] 这两者一致的时候，签名信息验证部件 6611 判定收到的签名信息 6570 的验证成

功，并结束验证处理。

[0823] 在以上处理过程中，签名信息验证部件 6611 指令获取部件 6601 读取部分已加密内容和报头信息。但是，在这一点，签名信息验证部件 6611 可能收到表明不可能读取的错误通知信号。

[0824] 接收错误通知信号的时候，签名信息验证部件 6611 退出签名信息的验证处理，并且将回放禁止信息输出给执行部件 1606。

[0825] 6.4.6 执行部件 6606

[0826] 执行部件 6606 从内容密钥获取部件 1602 接收内容密钥，并且开始已加密文件的重复读出、解密和回放，如同构成第一实施例的执行装置 1600 的执行部件 1606 的那种情形一样。

[0827] 在重复过程中，执行部件 6606 可以从签名信息验证部件 6611 接收回放禁止信息。

[0828] 另外，在重复过程中，执行部件 6606 请求获取部件 6601 读取构成已加密内容 6580 的已加密文件。但是在这一点，执行部件 6606 可以从获取部件 6601 接收表明不能读出的错误通知信号。

[0829] 接收回放禁止信息或者错误通知信号的时候，执行部件 6606 退出回放处理，并且通知用户不能回放载入的 DVD。

[0830] 6.5 综述和有益效果

[0831] 如同已经描述的一样，构成本实施例未授权内容检测系统的分发装置 6100 产生区域信息，表明分发装置 6100 有效地写入的信息所储存的区域，并且将所产生的区域信息写入 DVD。更进一步，分发装置 6100 从第二散列表、单元拾取信息和区域信息产生签名信息，并且将这些写入 DVD。

[0832] 载入了 DVD 6500 的时候，执行装置 6600 的获取部件 6601 首先从 DVD 6500 读取区域信息，然后只读取已读取的区域信息表明的区域内的信息，而不读取其它区域中写入的信息。

[0833] 在这里，如同第五实施例一样，即使发生了将未授权内容写入 DVD 6500 上自由空间的欺骗行为，在执行装置 6600 中也无法播放未授权内容。

[0834] 另外，储存在 DVD 6500 里的签名信息是利用区域信息产生的，并且执行装置 6600 的签名信息验证部件 6611 使用从 DVD 6500 读取的区域信息，以便验证签名信息。因此，即使未授权第三人冒充区域信息，同时插入未授权内容，签名信息验证部件 6611 执行的签名信息验证也不会成功，因此不会播放未授权内容。

[0835] DVD 中没有任何自由空间剩余的时候，有可能发生欺骗行为，比如将有效 DVD 上储存的所有数据复制到具有比这个有效 DVD 的存储容量更大的另一个介质上去，并且将未授权内容添加到这一介质的自由空间上去。即使是在这种情况下，本实施例的未授权内容检测系统中的执行装置 6600 也不读取区域信息表明的区域以外存储区域中的信息。因此，本实施例不能防止这种欺骗行为。

[0836] 6.6 第六实施例的变型

[0837] 在第六实施例中，分发装置 6100 产生的区域信息是表明在其中 储存了分发装置有效地写入的信息的区域的信息。区域信息也可以是分发装置 6100 有效地写入的信息的总的数据大小。

[0838] 在这种情况下，执行装置6600的获取部件6601首先从DVD 6500读取总的数据大小，然后测量DVD 6500中储存的信息的总的数据大小。当被测数据大小大于读取的数据大小的时候，获取部件6601退出从DVD 6500读取数据，并且将错误通知信号输出给执行部件6606。

[0839] 7. 其它变型

[0840] 虽然已经基于上述实施例描述了本发明，但是本发明当然不局限于这些实施例。本发明还包括以下情形：

[0841] [1] 在上述第一、第五和第六实施例中，分发装置通过将已加密单元赋予散列函数来计算单元散列值，并且基于计算出来的单元散列值来产生报头信息和签名信息，同时执行装置使用被选 i 个已加密单元来验证签名信息。但是，分发装置可以在加密之前通过使用单元来计算单元散列值，并且执行装置可以通过对被选 i 个已加密单元进行解密来产生 i 个单元，并且通过使用产生的 i 个单元来验证签名信息。

[0842] [2] 另一方面，在第二到第四实施例中，分发装置通过将多项部分内容赋予散列函数来计算部分散列值，并且基于计算出来的部分散列值来产生报头信息和签名信息。但是，分发装置可以通过将已加密部分内容赋予散列函数来计算部分散列值，其中的已加密部分内容是通过对各项部分内容进行加密来产生的，并且基于计算出来的部分散列值来产生报头信息和签名信息。

[0843] 在这种情况下，执行装置使用已加密部分内容来验证报头信息。这样就没有必要配备代表性的部分内容解密部件和部分内容解密部件，这样做导致检测系统的电路的尺寸减小。

[0844] [3] 在第二到第四实施例中，在签名信息和报头信息的验证已经成功以后，执行部件开始对已加密内容进行解密、扩展和回放。但是，执行部件可以与验证并行开始与回放有关的处理。在这种情况下，签名信息验证部件和报头信息验证部件分别进行的各个验证不成功的时候，签名信息验证部件和报头信息验证部件指示执行部件退出回放。

[0845] 在第一、第五和第六实施例中，签名信息验证部件可以有一个定时器，用于测量经过时间，并且如果在预定的时间内签名信息的验证没有完成就判定验证不成功。 在与回放并行进行签名信息的验证的情况下，如果内容、签名信息或者报头信息遭到伪造，将会播放未授权内容，直到完成验证。 因此，为签名信息的验证设置时限能够对付通过伪造来延长未授权内容的回放时间，从而延迟签名信息验证的完成的欺骗行为。 另外，变型 [3] 中的签名信息验证部件和报头信息验证部件也可以以类似的方式有一个定时器。

[0846] 在上面的第一到第六实施例中，分发装置具有签名密钥，而执行装置则有对应的验证密钥，并且这些装置利用DSA这种签名生成算法产生和验证签名信息。总之，许多签名生成算法都是建立在公钥密码系统基础之上的，如同 DSA 和 RSA(Rivest-Shamir-Adleman) 所代表的一样。但是，在本发明中，可以使用任何签名生成算法，例如建立在对称密钥密码系统基础之上的，只要能够证明 DVD 上记录的签名信息是由合法权利持有人产生的信息就行。 作为另一个实例，可以在所公开的处理中使用单向函数。在这种情况下，分发装置和执行装置分别将同样的单向函数储存在外部装置不能读取的存储区域内。分发装置利用单向函数来产生签名信息，而执行装置则利用同样的单向函数来产生签名验证信息。

[0847] 产生签名信息的时候用于签名生成算法的信息不限于以上实施例中描述的那些。

例如，在第一实施例中，将签名生成算法同时应用于第二散列表和单元拾取信息，但是，可能只能将签名生成算法应用于第二散列表，或者除了第二散列表以外，还可以将它应用于内容密钥 CK 和已加密内容的数据大小。在第二实施例的情形中，可以将签名生成算法应用于所述多项代表性的部分内容本身，而不是将签名生成算法应用于从多项代表性的部分内容产生的部分散列值。

[0848] 特别是，在第二实施例中，从多项代表性的部分内容产生签名信 息的时候，可以通过将签名生成算法分别应用于 k 项代表性的部分内容来产生 k 则签名信息。

[0849] 在这种情况下，执行装置基于被选位置信息产生 k 项代表性的部分内容，并且利用产生的 k 项代表性的部分内容验证 k 则签名信息。

[0850] 分发装置也可以通过将签名生成算法应用于组合结果来产生签名信息，其中所述组合结果是通过组合 k 项代表性的部分内容形成的，同时执行装置利用组合结果来验证签名信息。

[0851] 在这种情况下，如果签名信息的验证成功，就一次确认以下两件事 ：签名信息是由合法权利持有人产生的 ；代表性的部分内容没有被伪造。这样就不必产生报头信息，并且将报头信息写入 DVD，从而减小写入 DVD 的数据的大小。

[0852] [7] 在第二和第三实施例中，执行装置可以预存被选位置信息，并且不能将已加密被选位置信息记录在 DVD 上。在这里，有效执行装置能够利用预存的被选位置信息验证报头信息。

[0853] [8] 在第三实施例中，将报头选择信息和 x 个报头组写入 DVD。但是，在变型 [7] 的情况下，分发装置可以选择第一到第 x 个报头组之一，提取被选报头组中包括的报头标识符、报头信息和签名信息，并且将这些写入 DVD。

[0854] 执行装置可以预存 x 个被选位置信息和报头标识符对，基于写入 DVD 的报头标识符选择一则被选位置信息，在随后的处理中使用被选的一则被选位置信息。

[0855] [9] 上面的第一到第七实施例是在假设执行装置是单个装置的情况下描述的。但是，可以采用多个装置来完成执行装置的功能。

[0856] [10] 在第三实施例中，执行装置的获取部件选择 x 个报头标识符之一。但是，本发明不限于这样，而是可以换成选择两个或者多个标识符，并且签名信息和报头信息的验证可以重复两次或更多次。这样就能够更加可靠地检测未授权内容。

[0857] [11] 在以上实施例和变型中，分发装置的签名密钥存储部件和执行装置的验证密钥存储部件分别储存一则密钥信息，但是本发明不局限于这样。

[0858] [11-1] 例如，签名密钥存储部件可以储存签名密钥以及与签名密钥对应的密钥标识符，并且记录部件将签名信息与密钥标识符一起写入 DVD。

[0859] 执行装置的验证密钥存储部件储存多个验证密钥以及与验证密钥一一对应的密钥标识符。签名信息验证部件与签名信息一起接收密钥标识符，从验证密钥存储部件储存的多个密钥标识符提取与收到的密钥标识符一致的密钥标识符，读出与提取的验证密钥标识符一致的验证密钥，并且用读取的验证密钥来验证签名信息。

[0860] 在这里，即使有多个不同的分发装置也能够应用本发明。

[0861] [11-2] 执行装置可能没有验证密钥存储部件，并且签名密钥以及与签名密钥对应的验证密钥可以储存在分发装置的签名密钥存储部件里。在这种情况下，记录部件将验证

密钥与签名信息一起写入 DVD。

[0862] [11-3] 除了签名密钥和验证密钥以外，分发装置可以储存公平 (impartial) 第三方实体产生的验证密钥的鉴别信息。在这里，假设鉴别信息是通过将签名生成算法应用于验证密钥，利用第三方实体的秘密密钥产生的密钥签名。

[0863] 记录部件将验证密钥和密钥签名与签名信息一起写入 DVD。

[0864] 执行装置的验证密钥存储部件储存密钥验证信息，而不是验证密钥。密钥验证信息是用于验证密钥签名的信息，在这种情况下，是与产生了密钥签名的公平第三方实体的秘密密钥配对的公钥。

[0865] 签名信息验证部件接收密钥签名和验证密钥，并且在验证签名信息之前利用收到的密钥和密钥验证信息来验证密钥签名。只有当验证成功的时候，签名信息验证部件才开始象上面的实施例描述的一样验证签名信息。

[0866] 在这里，即使有多个分发装置，执行装置也只要保持第三方实体的密钥验证信息，而不必有多个验证密钥。

[0867] [12] 在变型 [11] 中，执行装置可以储存表明无效验证密钥的撤销清单。签名信息验证部件判断是否已经将收到的密钥标识符或者验证密钥登记在撤销清单里，并且在已经登记了以后退出签名信息的验 证。

[0868] [13] 执行装置可以从外部源获得变型 [12] 里描述的撤销清单。例如，可以通过 DVD 这种记录介质获得撤销清单，或者可以通过因特网、广播之类提取。执行装置也可以周期性地获得更新过的撤销清单。

[0869] 在这里，本发明能够对付需要被无效的验证密钥是新发现的这种情形。

[0870] [14] 分发装置通过 DVD 分发各种信息给执行装置，例如已加密内容和签名信息。但是，本发明不限于 DVD，信息可以通过光盘例如 CD-ROM 和 DVD-ROM，可写光盘例如 CD-R、DVD-R 和 DVD-RAM，磁光盘，以及存储卡来分发。也可以将半导体存储器，例如闪存和硬盘结合到执行装置里。

[0871] 更进一步，本发明不限于这种记录介质，信息能够通过因特网这样的通信系统分发，或者能够通过广播分发。

[0872] [15] 虽然描述上面的实施例和变型的时候假设了内容是图像和音频组成的视频内容，但是这些内容也可以是计算机程序。例如，假设执行装置是游戏控制台；内容是结合在游戏控制台里的闪存中储存的计算机程序。在这里，计算机程序是用于判断载入游戏控制台的游戏软件（例如光盘和存储卡）是不是有效软件的判断程序。在这种情况下，即使未授权用户伪造了判断程序，从而能够执行未授权游戏软件，本发明也能够通过利用签名信息和报头信息，验证是否包括未授权内容，来检测这种伪造，从而防止或者退出判断程序本身的执行。这样，通过停止执行本身，能够防止通过已经在上面进行了未授权的伪造的判断程序实现的未授权操作，也就是防止执行未授权游戏软件。

[0873] [16] 如同上面的变型所描述的一样，在所述内容是执行装置里结合的微型计算机上装载的闪存里储存的计算机程序的情况下，就会发生第五实施例中描述的欺骗行为。具体而言，首先将未授权程序添加到闪存的自由空间里，而不伪造所涉及闪存里储存的有效计算机程序。然后，通过使用有效的计算机程序里的缺陷引起缓冲器溢出，从而使程序的起始点跳到添加的未授权程序的开头，开始执行未授权程 序。

[0874] 在这里，可以通过在闪存里写入填充内容，从而在闪存中不留自由空间来防止上面提到的欺骗行为，如同在第五实施例中一样，因为不能添加未授权内容。

[0875] 也可以象第六实施例中一样，可以将表明分发装置写入的有效信息储存的区域的区域信息事先写入闪存，并且将执行装置设计成不读出区域信息表明的区域以外的区域里的信息。因而即使添加了未授权程序，执行装置也不执行未授权程序。

[0876] [17] 描述上面的第一到第六实施例和变型的时候假设了执行部件是播放由视频和音频组成的内容的组件，但是，执行部件也可以是将内容输出给外部记录介质的组件，或者是具有打印功能并且在纸上打印图像之类的组件。

[0877] [18] 在上述实施例中，将一组内容输入分发装置的时候，内容密钥生成部件每次都产生内容密钥。但是，内容密钥生成部件可以预存多个内容密钥，并且选择和输出储存的内容密钥之一。

[0878] [19] 在以上实施例中，将执行装置设计成在装载了 DVD 的时候开始验证报头信息、签名信息之类，但是本发明不限于这样。

[0879] 例如，执行装置可以在得到指令按照用户的按钮操作回放的时候开始这种验证，或者可以从装载了 DVD 的时候开始按照有规律的间隔进行验证。

[0880] [20] 在第二和第三实施例中，不必将报头信息写入 DVD。

[0881] 不将报头信息写入 DVD 的时候，执行装置基于被选位置信息提取 k 项代表性的部分内容，并且通过将所提取的多项代表性的部分内容赋予散列函数来计算验证散列值。

[0882] 然后，执行装置通过将签名验证算法 V 应用于组合结果，利用验证密钥来产生签名验证信息，其中的组合结果是通过将计算出来的验证散列值组合起来形成的。执行装置通过与所产生的签名验证信息进行比较来验证签名信息。

[0883] 在这种情况下，执行装置不再需要报头信息验证部件，这会导致检测系统的电路尺寸减小。另外，是否包括未授权内容的验证可以与 验证签名信息同时完成。

[0884] [21] 在第四实施例中，在签名信息验证部件 4606 进行的签名信息的验证成功以后，执行装置 4600 只验证报头信息中包括的 c 个部分散列值中的 k 个。但是，可以用 k 项已加密部分内容和报头信息，用单次验证来验证签名信息和报头信息。

[0885] 更具体地说，执行装置基于内容位置信息，从已加密内容提取 k 项已加密部分内容，并且通过对所提取的 k 项已加密部分内容进行解密来产生 k 项部分内容。然后，执行装置通过相应地将所产生的 k 项部分内容赋予散列函数来计算替换部分散列值。

[0886] 下一步，执行装置从报头信息中包括的 c 个部分散列值，利用计算出来的替换部分散列值替换与被选 k 项已加密部分内容对应的部分散列值。

[0887] 执行装置利用验证密钥和组合结果来验证签名信息，其中的组合结果是通过将替换部分散列值与被替换报头信息中包括的部分散列值进行组合形成的。

[0888] 在这种情况下，执行装置不再需要报头信息验证部件，这样就能够减小检测系统的电路尺寸。另外，是否包括未授权信息的验证可以在验证签名信息的同时完成。

[0889] [22] 在上述第一到第六实施例中，写入 DVD 的仅仅是一组已加密内容，以及与这一组已加密内容对应的签名信息和报头信息之一。但是，也可以换成储存与这些组分别相对应的多组不同的已加密内容和多则报头以及签名信息。

[0890] 另外，DVD 可以只包括在所有则报头信息基础之上产生的一则签名信息。更进一

步，除了这些组已加密内容以外，DVD 可以包括不需要版权保护的内容，例如，广告、开机画面、菜单画面等等。可以在验证签名信息和报头信息的同时播放不需要版权保护的这些内容。

[0891] [23] 在第一到第六实施例和变型中，当签名信息的验证和报头信息的验证中有至少一个不成功的时候，执行装置可以储存用于识别装载在获取部件上的 DVD 的盘标识符以及用于识别正在播放的点上 的一组内容的内容标识符。

[0892] 装载了具有与记录的相同的盘标识符的 DVD 的时候，执行装置退出内容的回放。得到指令播放具有与记录的相同的标识符的一组内容的时候，执行装置也可以退出这一组内容的播放。

[0893] [24] 在以上实施例和变型中，当签名信息的验证和报头信息的验证中至少有一样不成功的时候，执行装置退出内容的回放，并且通过例如在监视器上显示一个错误通知画面来通知用户内容没有得到授权。验证失败的时候执行装置的工作状况不限于此，还可以考虑以下情况。更进一步，可以将以下三个变型组合起来。

[0894] [24-1] 分发装置和执行装置都连接到因特网。当签名信息的验证和报头信息的验证至少有一个不成功的时候，执行装置通过因特网通知分发装置验证失败。在这一点上，执行装置也发送表明验证不成功的内容的一个内容标识符。

[0895] 分发装置预存内容标识符和内容标识符表明的内容的创建日期，将这两者互相联系起来。

[0896] 分发装置通过因特网从执行装置接收验证失败通知和内容标识符。分发装置根据与收到的内容标识符相对应的创建日期，产生表明允许回放内容的回放允许信息，或者表明禁止回放的回放禁止信息。例如，当内容标识符表明新内容从创建日期开始少于半年，分发装置就产生回放禁止信息。另一方面，当内容标识符表明旧内容从创建日期开始已经半年或者更久，分发装置就产生回放允许信息。

[0897] 下一步，分发装置通过因特网发送所产生的回放允许信息或者回放禁止信息给执行装置，只有在收到回放允许信息的时候，执行装置才对 DVD 中储存的已加密内容进行解码和播放。

[0898] 假设从发行开始计算内容已经发行了一个设定的时间周期，并且对内容的要求已经在某种程度得到了满足，并且因此预期这些内容的未来销售量不大。在这种情况下，上述变型允许通过允许用户观看这些内容来给购买了这一 DVD 的用户的利益以优先权。另一方面，当这些内容是最近才发行的，并且预期这些内容的未来销售量很大，那么这一变型就通过禁止回放来给与版权持有人的权利以优先权。也就 是说，这一变型能够调整用户的利益和版权持有人的利益。

[0899] 注意，确定是发送回放禁止信息还是回放允许信息的方式不限于此，并且针对每一组内容，分发装置可以储存反映例如内容组的版权持有人和销售商的意图的允许条款。

[0900] [24-2] 如同已经描述的一样，记录内容的介质不限于 DVD，而是可以是可重写记录介质。在这里，将配备了闪存的存储卡用作实例。

[0901] 签名信息或者报头信息的验证不成功的时候，执行装置删除存储卡中记录的已加密内容的部分或者全部信息。

[0902] 这样就能够可靠地防止未授权内容的未来使用。

[0903] [24-3] 在内容是HD（高清晰度）视频数据的情况下，如果验证不成功，执行装置在将它转换成SD（标准清晰度）以后播放视频数据。

[0904] 在内容是高质量声音（5.1声道）音频数据的时候，如果验证不成功，执行装置在将它转换成标准质量声音（2声道）音频数据以后播放音频数据。

[0905] 这样，通过在降低回放质量的条件下允许回放，能够将用户的方便性和版权持有人的利益调整到某种程度。

[0906] [25] 在第二和第三实施例中，当DVD被载入其中的时候，执行装置读出密钥块、已加密被选位置信息、报头信息签名信息和已加密内容。但是，执行装置可以根据每个组件的处理进程通过获取部件只读出需要的信息。

[0907] 例如，装载了DVD的时候，执行装置只读出密钥块；内容密钥的产生完成的时候，执行装置只读出已加密被选位置信息；并且在已加密被选位置信息的解密已经完成的时候，执行装置只读出签名信息和报头信息，并且随后验证签名信息。一旦签名信息的验证完成，执行装置读取被选位置信息表明的k个已加密块。

[0908] 在第四实施例中，同样只按照需要用类似的方式读取需要的信息。

[0909] [26] 在第一实施例中，当读取被选i个已加密单元的时候，通过按照下面描述的读出顺序能够提高读出速度。

[0910] 为了简化描述，这里假设i＝4，考虑要读出四个已加密单元的情况。

[0911] 在DVD这种光盘上，将用于记录数据的区域划分成多个部分，将树木年轮形状的区域相应地叫做轨道。每个轨道中包括几个扇区，数据是一个扇区一个扇区地读取和写入的。一个扇区的大小是例如512字节。在这种情况下，DVD上要读出的多项数据可以用轨道标识号、扇区标识号或者扇区大小来标识。

[0912] 图71说明DVD 1500的结构和获取部件1601的结构。图中的同心区域是轨道。

[0913] 如图71所示，获取部件1601具有首部（也叫作拾取）1628和转轴1629。通过转动转轴1629，DVD 1500在逆时针方向上转动。图中虚线画出的箭头表明转动方向。通过指定轨道标识号、扇区标识号或者扇区大小，获取部件1601移动首部1628，获取要读出的一项数据。

[0914] 总之，已知将首部1628移动到储存了作为读出目标的数据的轨道需要时间。换句话说，随着DVD上从里到外的移动距离或者从外到里的移动距离增大，需要更长的时间来读出数据。

[0915] 在这里，四个已加密单元EU1_3、EU3_1、EU8_7和EU9_2是读出目标，分别储存在DVD 1500上的部分1591、1592、1593和1594中。

[0916] 在DVD 1500上，假设首部1628在图71所示的位置中。

[0917] 在这种情况下，根据第一实施例中描述的程序，获取部件1601首先将首部1628移动到上面存在部分1591的轨道1501，并且读出部分1591中记录的已加密单元EU1_3。然后，获取部件1601将首部1628移动到轨道1504，并且从部分1592读出已加密单元EU3_1。接下来，用类似的方式，获取部件1601将首部1628移动到轨道1502，以便读出部分1593里的已加密单元EU8_7，接下来移动到轨道1503，以便读出部分1594里的已加密单元EU9_2。

[0918] 这样，采用第一实施例中描述的程序的时候，首部1628的移动距离变长，结果，需要长时间来读出所有已加密单元。

[0919] 在这里，改变四个已加密单元的读出顺序，从而使首部 1628 总是从这个时候它所在的轨道移向最接近的的轨道。也就是说，获取部件 1601 将表明首部 1628 的位置的轨道号与表明储存了四个已加密单元的部分 1591、1592、1593 和 1594 的位置的扇区号和轨道号进行比较。然后获取部件 1601 重新安排四个部分的被获得的扇区号和轨道号的顺序，从而使首部 1628 为读出采用最短的移动距离，并且按照重新安排的顺序访问每个部分。

[0920] 在这里，能够缩短读出数据所需要的时间。另外，在要读出的已加密单元位于相同轨道或者在相近轨道上的情况下，可以根据首部 1628 的当前位置和表明储存了各个已加密单元的部分的扇区号来改变读出顺序。

[0921] 注意，优化读出顺序的方式依赖于获取部件 1601 的转轴和首部的工作属性，因此这里描述的优化程序仅仅是一个实例。例如，光盘的转动控制方法包括恒定角速度法和恒定线速度法，可以将这种方法的特性考虑在内。另外，用硬盘代替象 DVD 这样的光盘的时候，可以按照类似的方式安排读出顺序。

[0922] 在第五和第六实施例中，可以按类似的方式改善读出速度。这也是按照第二到第四实施例变型 [20] 的那种情形。

[0923] [27] 在第一、第五和第六实施例中，执行装置随机地选择 i 个已加密文件，并且进一步从每一个被选已加密文件选择一个已加密单元。但是，选择程序不限于此，可以从一个已加密文件选择多个已加密单元，只要被选项总数为 i。

[0924] [28] 在第一、第五和第六实施例中，执行装置选择的已加密单元的个数 i 可以预存在执行装置里，或者可以写入 DVD 里。

[0925] 随着被选已加密单元的数量 i 变大，是否包括未授权内容的有效性的准确度增大，而签名信息验证所涉及的处理负荷也增大。

[0926] 这样，将要选择的已加密单元的数量 i 记录在 DVD 上，然后执行装置根据从 DVD 获得的 i 验证签名信息。这样就能够反映验证中 DVD 制造商的意图。

[0927] 另外，这一技术也能够用于第四实施例中选择 k 项已加密部分内 容。

[0928] [29] 在第一、第五和第六实施例中，签名信息是通过将签名生成算法应用于组合结果产生的，其中的组合结果是通过组合 c 个文件散列值形成的。但是，可以通过进一步将组合结果赋予散列函数，将签名生成算法应用于已经计算出来的组合散列值，通过计算组合后的散列值来产生签名信息。

[0929] [30] 在第一、第五和第六实施例中，报头信息由具有两层结构的散列值组成。也就是说，这个两层结构由以下内容构成 ：从相应的已加密单元产生的单元散列值 ；从基于同一个文件产生的 m 个单元散列值产生的文件散列值。另一方面，签名信息由 c 个文件散列值组成。

[0930] 取而代之，报头信息可以包括具有三层结构的散列值。具体而言，报头信息包括 y 个组合文件散列值。这 y 个组合文件散列值是通过首先将 c 个文件散列值划分成 y 个组，然后一个一个地将组合结果赋予散列函数而产生的，其中的组合结果是通过将每一组的文件散列值组合起来形成的。在这种情况下，签名信息是通过利用 y 个组合文件散列值产生的。

[0931] 这样，通过增加结构中的层数，能够减少要从 DVD 读取的信息。

[0932] [31] 如同在第五实施例中描述的一样，有时说明内容回放顺序的回放顺序文件储

存在 DVD 中。在这种情况下，DVD 可以包括回放顺序文件的签名信息。

[0933] 这样，如同第五实施例所描述的一样，即使未授权的第三人添加或者替换未授权内容，并且伪造回放顺序文件，这一伪造也会被对回放顺序文件的签名信息的验证检测到，因此不会回放未授权内容。

[0934] [32] 在第三实施例中，分发装置 3100 的选择部件 3105 从一组内容选择出来的代表性部分内容的总项数是 (k×k) 项。

[0935] 在这种情况下，可以设计成 c 项部分内容中的全部都要被选中至少一次，作为一项代表性的部分内容。这样，在替换了 DVD 中储存的部分已加密内容的一部分的情况下，可以提高检测未授权内容的准确度。

[0936] [33] 在第一、第五和第六实施例中，分发装置将单元拾取信息写入 DVD。分发装置可以向 DVD 写入通过利用内容密钥对单元拾取信息进行加密产生的已加密单元拾取信息。

[0937] 另外，在第四实施例中，分发装置将内容位置信息写入 DVD。取而代之，分发装置可以向 DVD 写入通过利用内容密钥对内容位置信息进行加密产生的已加密内容位置信息。

[0938] [34] 在第一到第六实施例和变型中，通过相应地将已加密单元赋予散列函数来计算单元散列值，而部分散列值则通过分别将多项部分内容赋予散列函数来计算出来。但是，每一个单元散列值都可以从组合结果计算出来，其中的组合结果是通过将对应于已加密单元的标识符、一则标识信息和已加密单元组合起来形成的。按照类似的方式，可以从组合结果计算出每一个部分散列值，这里的组合结果是通过将对应于一项部分内容的标识符、一则标识信息和所述项部分内容组合起来形成的。

[0939] [35] 在第五实施例中，要产生的填充内容的数据大小与填充容量一样。但是，数据大小不限于此，只要数据大小能够使得 DVD 上剩下的自由空间足够小就行。

[0940] [36] 在第一到第六实施例中，执行装置通过将视频和音频信号输出给外部监视器来播放内容。但是，执行装置也可以内置一个监视器。

[0941] [37] 可以将构成上述各个装置的部分或全部组件组装成单独一个系统 LSI（大规模集成）。系统 LSI 是通过将多个组件集成在一个芯片上产生的超级多功能 LSI，更加具体地说，是由微处理器、ROM、RAM 之类组成的一个计算机系统。计算机程序储存在 RAM 中。微处理器按照计算机程序运行，系统 LSI 由此实现它的功能。也可以换成在单个集成电路上构建每个组件。

[0942] 虽然在这里将它叫做系统 LSI，但是也可以将它叫做 IC、LSI、超 LSI 和超级 LSI，具体怎么称呼取决于集成度。另外，组装集成电路的方法不限于 LSI，也可以用专用通信电路或者通用处理器来实现这一目的。可以使用 FPGA（现场可编程门阵列），它在生产出这个 LSI 以后是可编程的，或者可以使用可重构处理器，它允许重构 LSI 内部电路单元的连接和设置。

[0943] [38] 本发明可以是实现上面描述的未授权内容检测系统的一种方法。本发明可以是用计算机实现这种方法的计算机程序，或者可以是表示这一计算机程序的数字信号。

[0944] 本发明也可以用计算机可读记录介质实现，例如用上面记录了上述计算机程序或者数字信号的软盘、硬盘、CD-ROM（光盘只读存储器）、MO（磁光）盘、DVD、DVD-ROM（数字多功能盘只读存储器）、DVD-RAM（数字多功能盘随机存取存储器）、BD（蓝光盘）或者半导体存储器实现。本发明也可以是记录在这样的存储介质上的计算机程序或者数字信号。

[0945] 本发明还可以是要通过网络或者通过数据广播发送的计算机程序或者数字信号，电信、有线 / 无线通信和因特网代表了这些网络。

[0946] 本发明还可以是具有微处理器和存储器的计算机系统，其中的存储器储存计算机程序，微处理器按照计算机程序工作。

[0947] 计算机程序或者数字信号可以记录在上述存储介质上，并且传送给独立的计算机系统，也可以通过上述网络传送给独立的计算机系统。然后，独立的计算机系统可以执行计算机程序或者数字信号。

[0948] [39] 本发明包括其中组合了上述实施例和变型中两个或者更多个的结构。

[0949] 工业实用性

[0950] 可以将本发明操作性地、连续地和重复地应用于产生、销售、传送和使用内容的行业，也可以将本发明应用于制造、销售和使用各种电子设备用来播放、编辑和处理这些内容的行业。

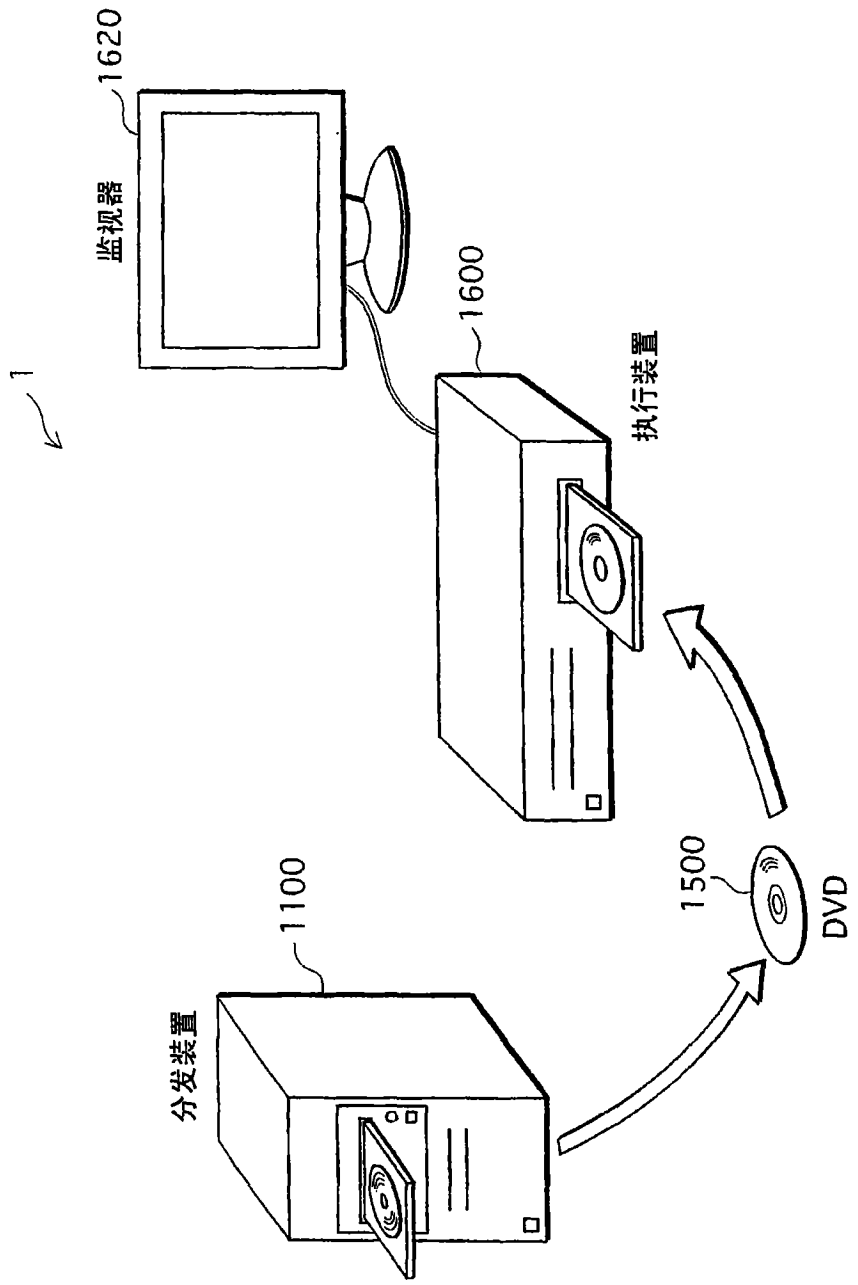


图1

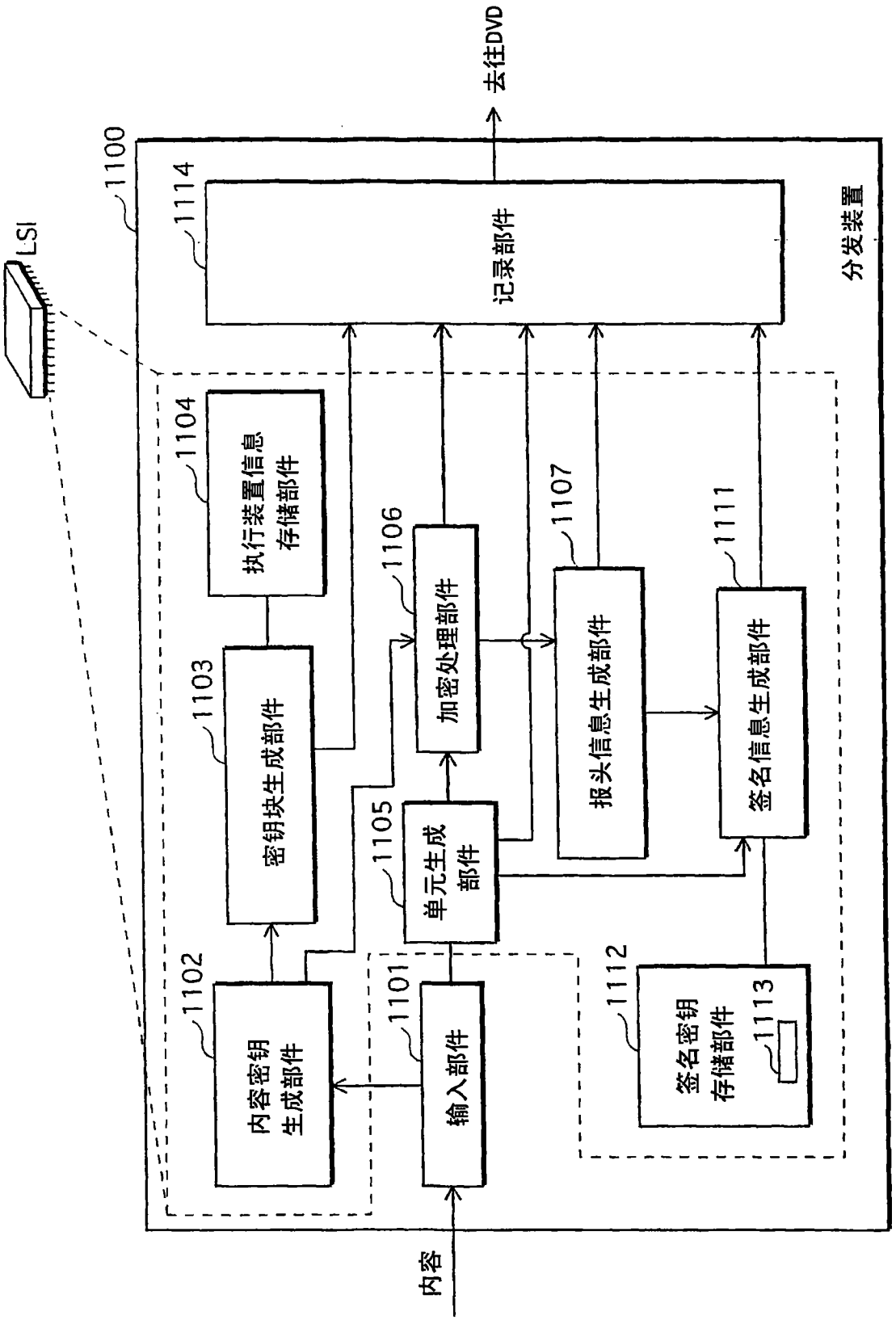

去往DVD
1100
1114
记录部件
分发装置
LSI
1104
执行装置信息存储部件
1106
加密处理部件
1107
1111
1103
密钥块生成部件
报头信息生成部件
签名信息生成部件
1105
单元生成部件
1102
内容密钥生成部件
1101
输入部件
1112
签名密钥存储部件
1113
内容

图2

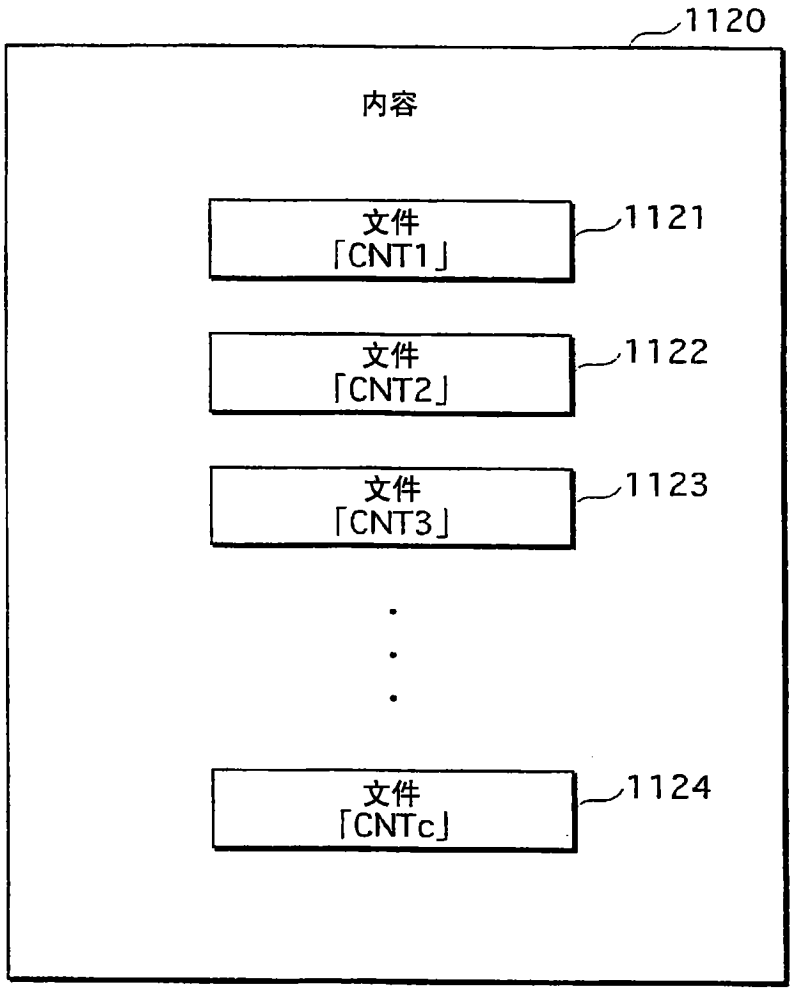


图 3

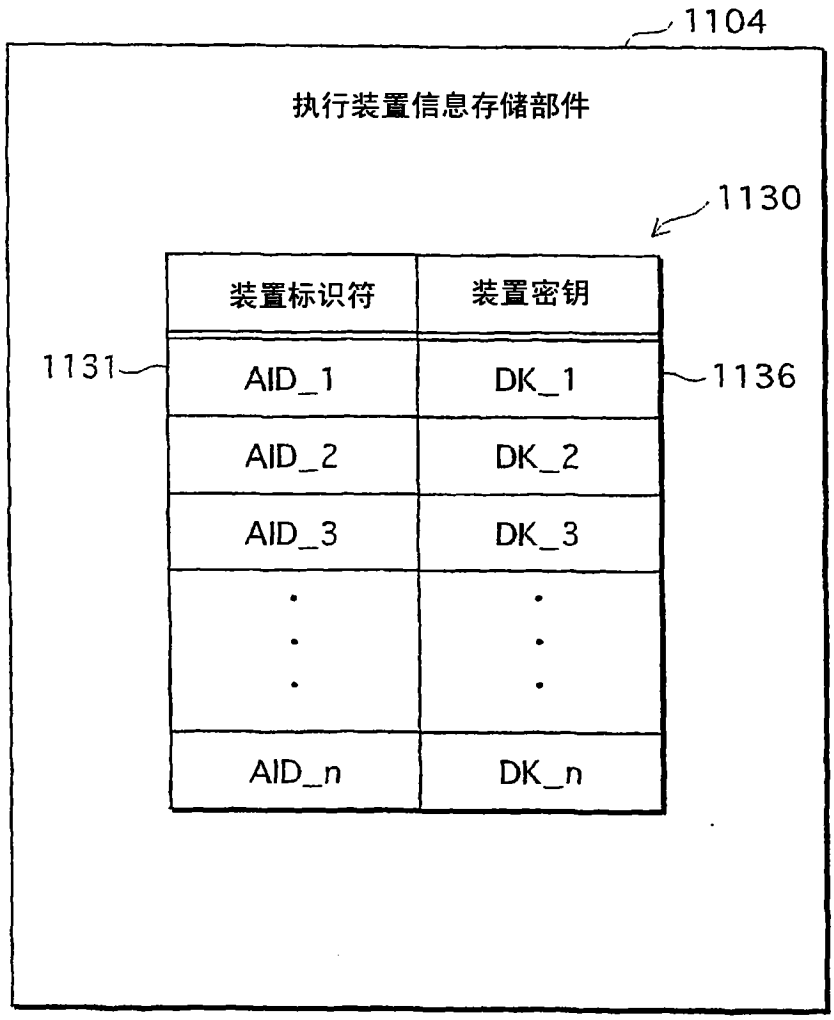

1104
执行装置信息存储部件
1130
装置标识符
装置密钥
1131
AID_1
DK_1
1136
AID_2
DK_2
AID_3
DK_3
AID_n
DK_n

图 4

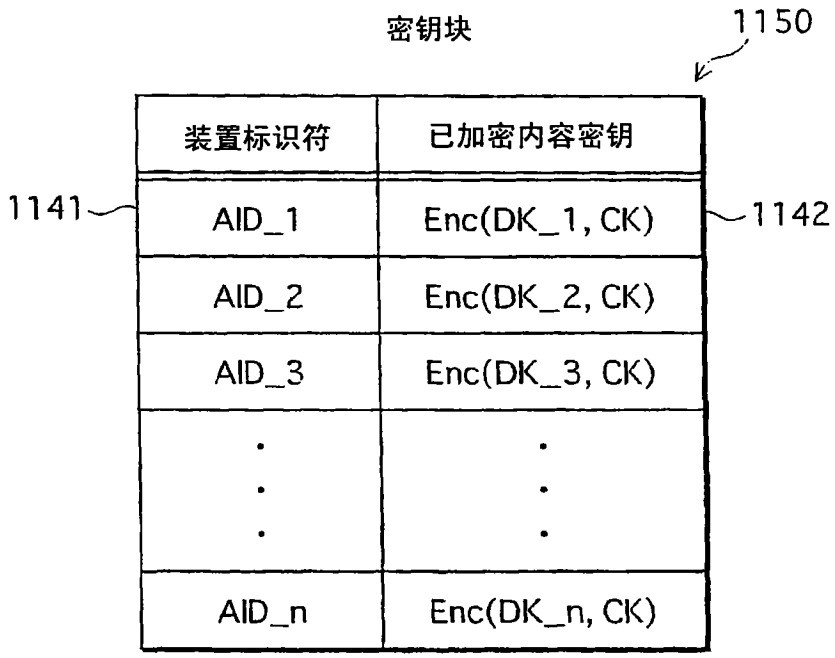

密钥块
1150
装置标识符
已加密内容密钥
1141
1142
AID_1
Enc(DK_1, CK)
AID_2
Enc(DK_2, CK)
AID_3
Enc(DK_3, CK)
AID_n
Enc(DK_n, CK)

图 5

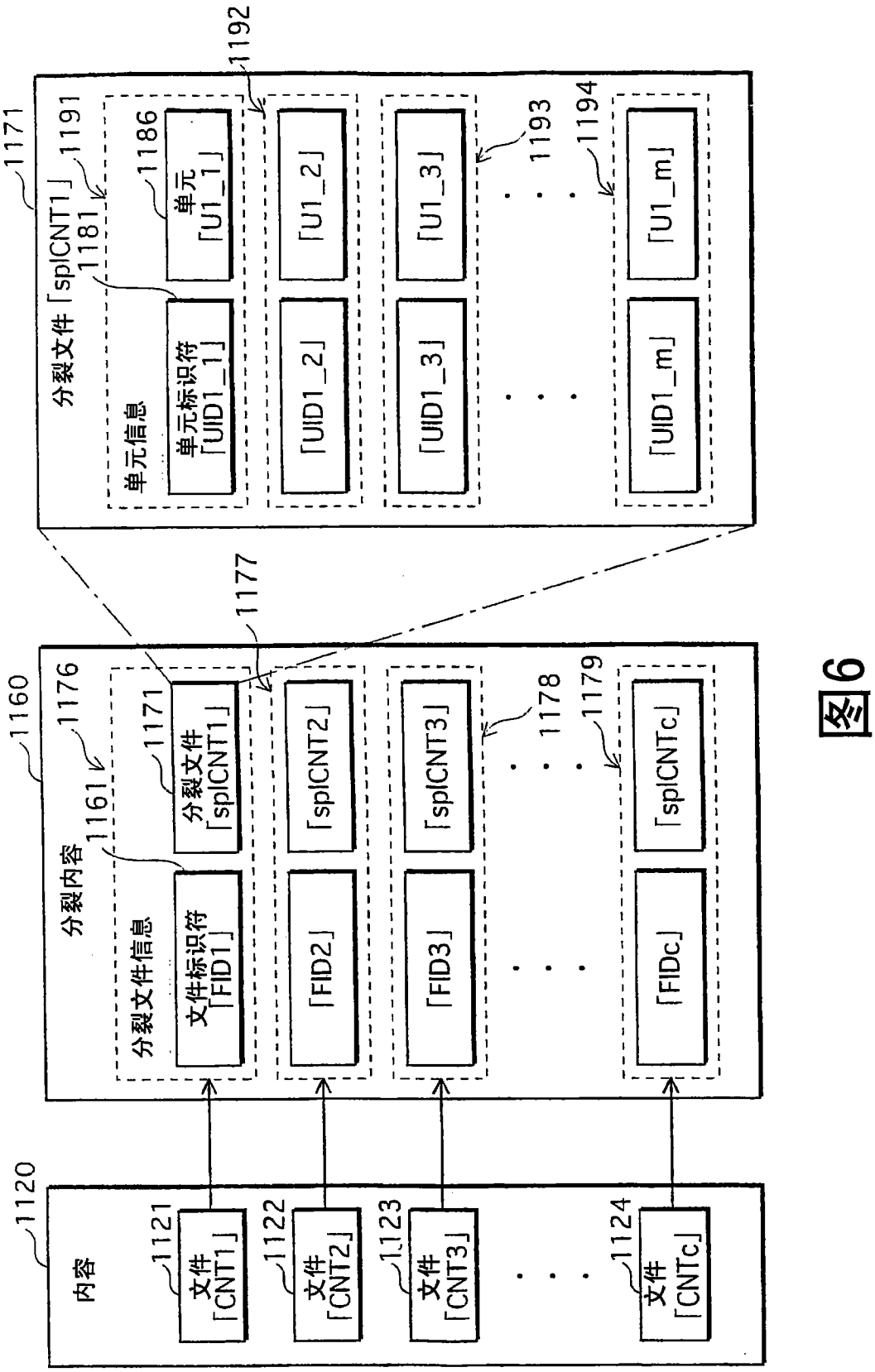

1171
分裂文件「splCNT1」
1191
1181
单元信息
1186
单元标识符「UID1_1」
单元「U1_1」
「UID1_2」
「U1_2」
「UID1_3」
「U1_3」
「UID1_m」
「U1_m」
1192
1193
1194
1177
1160
分裂内容
1176
1161
分裂文件信息
1171
文件标识符「FID1」
分裂文件「splCNT1」
「FID2」
「splCNT2」
「FID3」
「splCNT3」
「FIDc」
「splCNTc」
1178
1179
1120
内容
1121
文件「CNT1」
1122
文件「CNT2」
1123
文件「CNT3」
1124
文件「CNTc」

图6

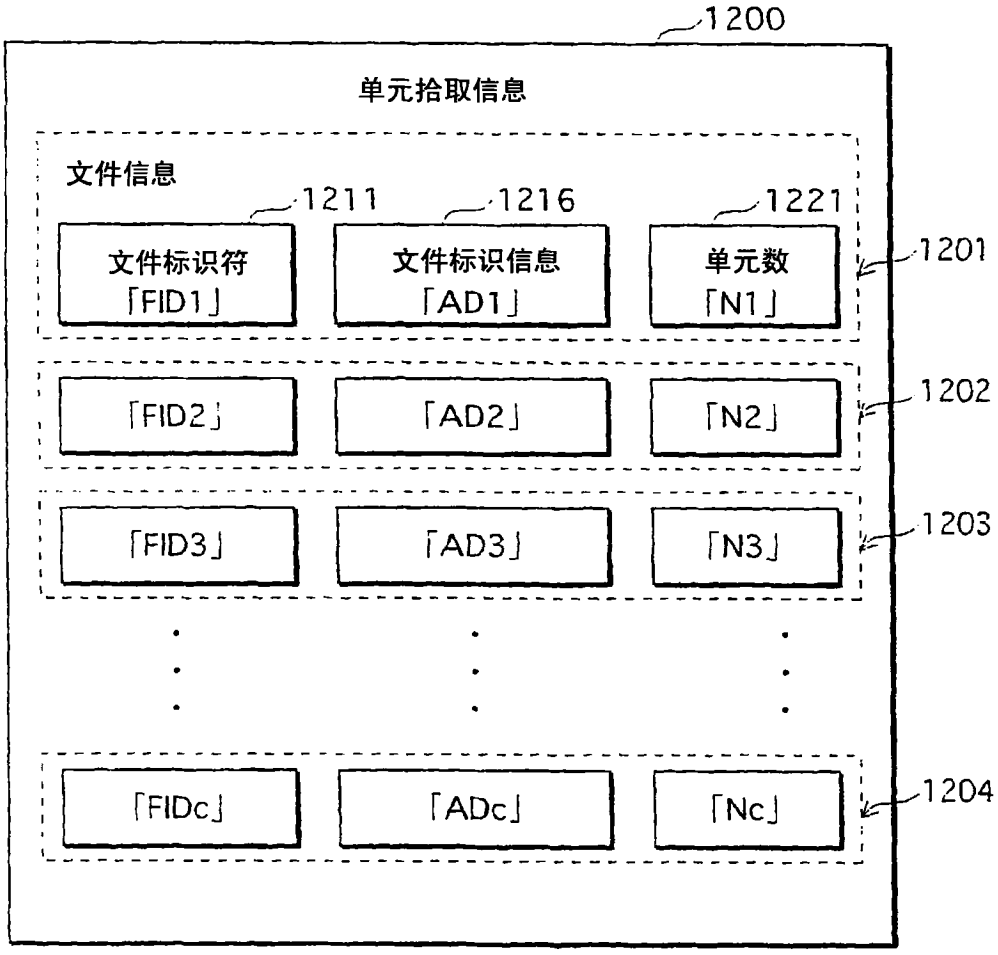

1200
单元拾取信息
文件信息
1211
1216
1221
文件标识符
「FID1」
文件标识信息
「AD1」
单元数
「N1」
1201
「FID2」
「AD2」
「N2」
1202
「FID3」
「AD3」
「N3」
1203
「FIDc」
「ADc」
「Nc」
1204

图 7

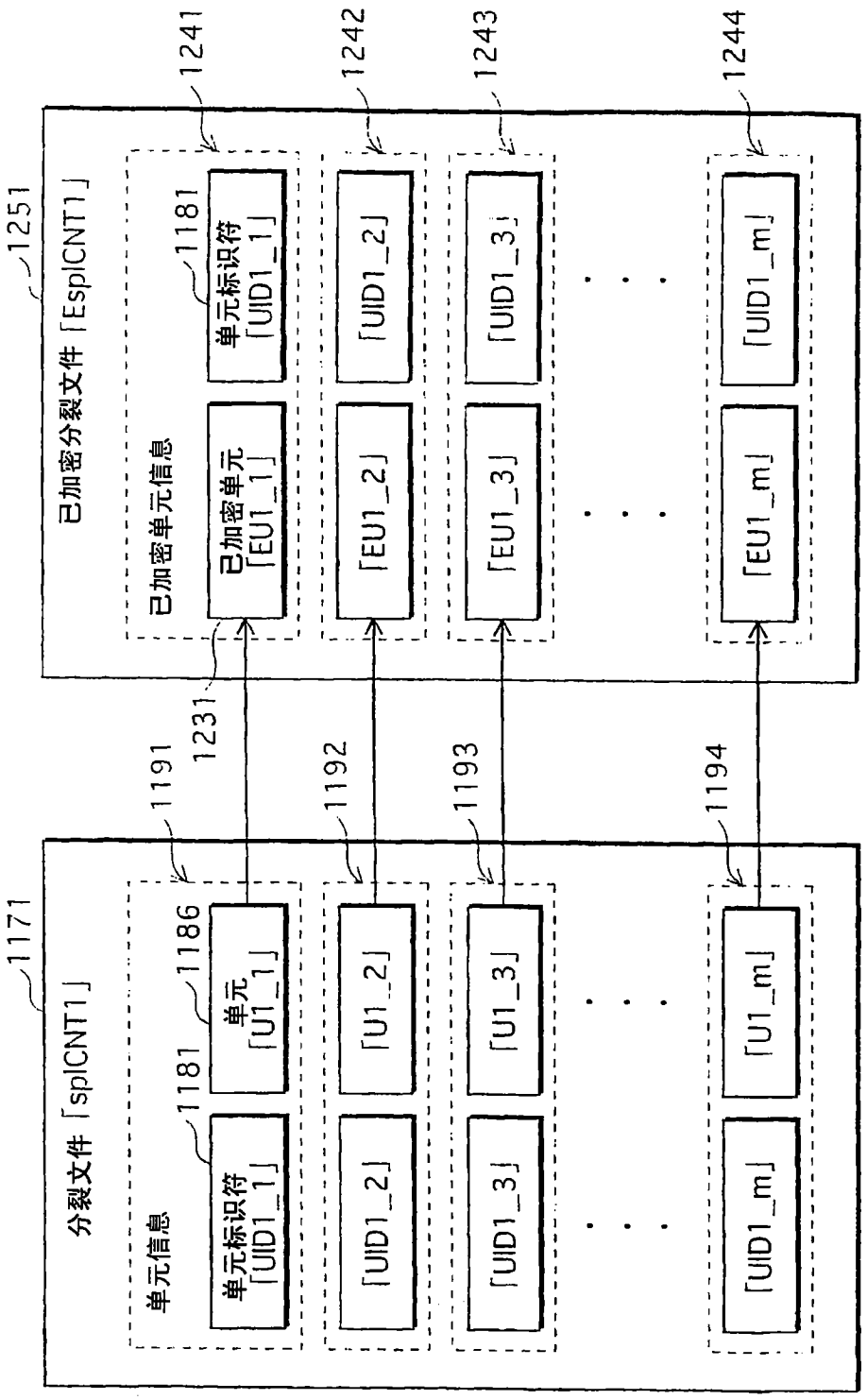

1171
分裂文件「splCNT1」
单元信息
1181
单元标识符「UID1_1」
1186
单元「U1_1」
「UID1_2」
「U1_2」
「UID1_3」
「U1_3」
「UID1_m」
「U1_m」
1191
1192
1193
1194
1231
1251
已加密分裂文件「EsplCNT1」
已加密单元信息
1181
单元标识符「UID1_1」
已加密单元「EU1_1」
1241
「UID1_2」
「EU1_2」
1242
「UID1_3」
「EU1_3」
1243
「UID1_m」
「EU1_m」
1244

图8

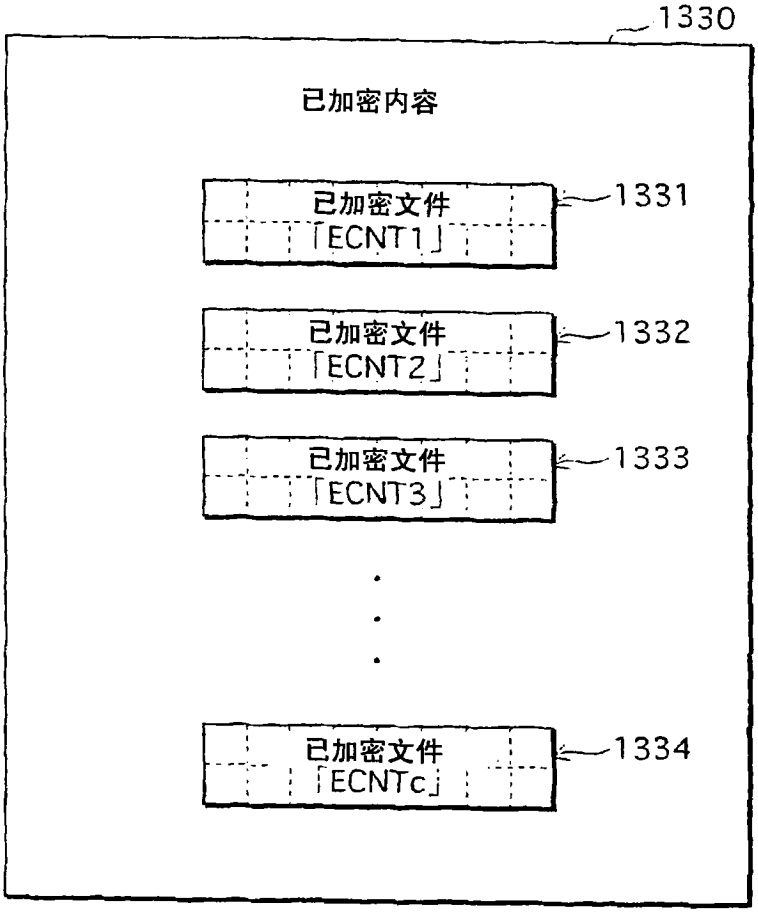

1330
已加密内容
已加密文件
「ECNT1」
1331
已加密文件
「ECNT2」
1332
已加密文件
「ECNT3」
1333
已加密文件
「ECNTc」
1334

图 9

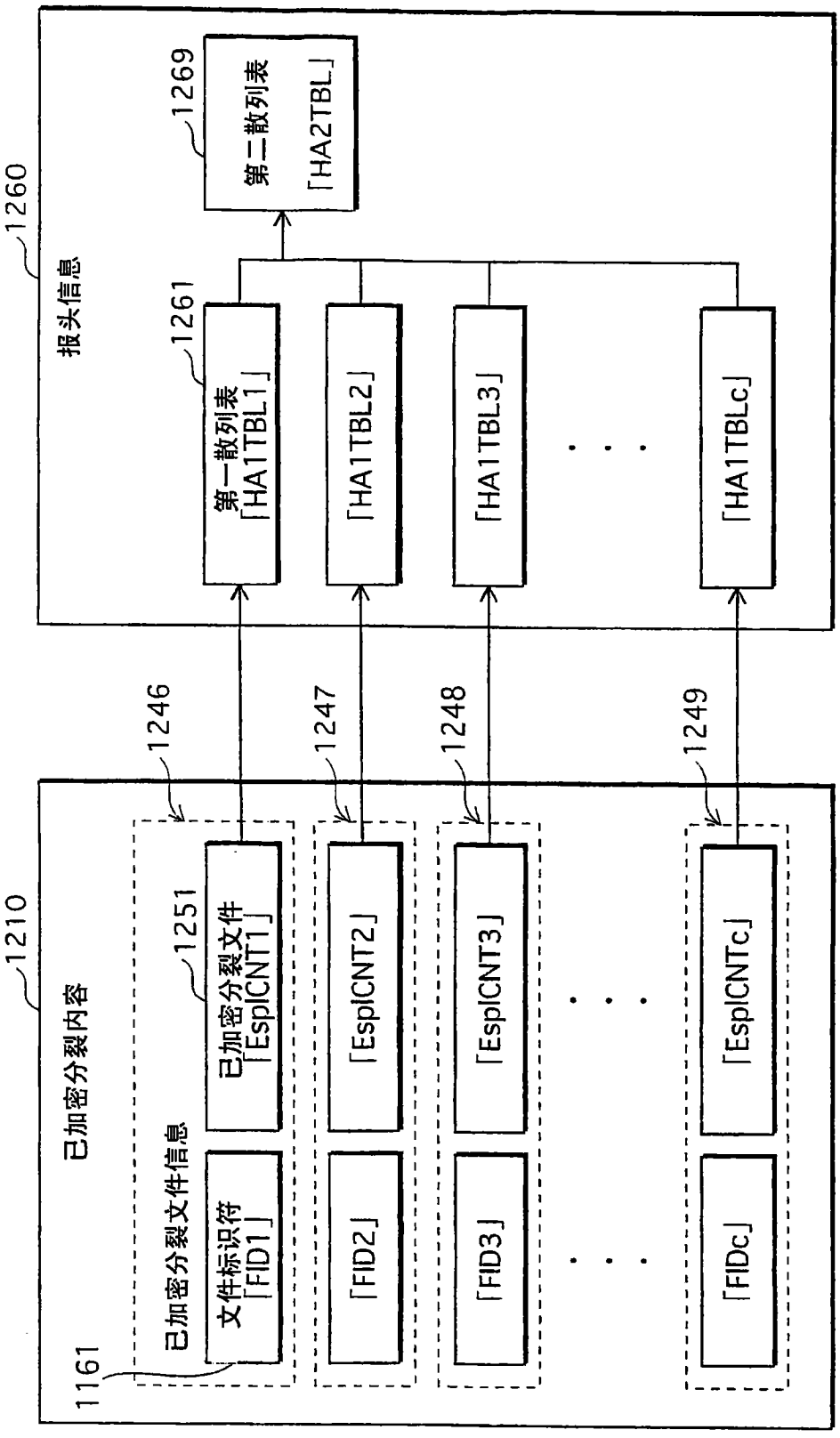

1260
报头信息
1269
第二散列表
「HA2TBL」
1261
第一散列表
「HA1TBL1」
「HA1TBL2」
「HA1TBL3」
「HA1TBLc」
1246
1247
1248
1249
1210
已加密分裂内容
1251
已加密分裂文件
「EsplCNT1」
「EsplCNT2」
「EsplCNT3」
「EsplCNTc」
已加密分裂文件信息
文件标识符
「FID1」
「FID2」
「FID3」
「FIDc」
1161

图10

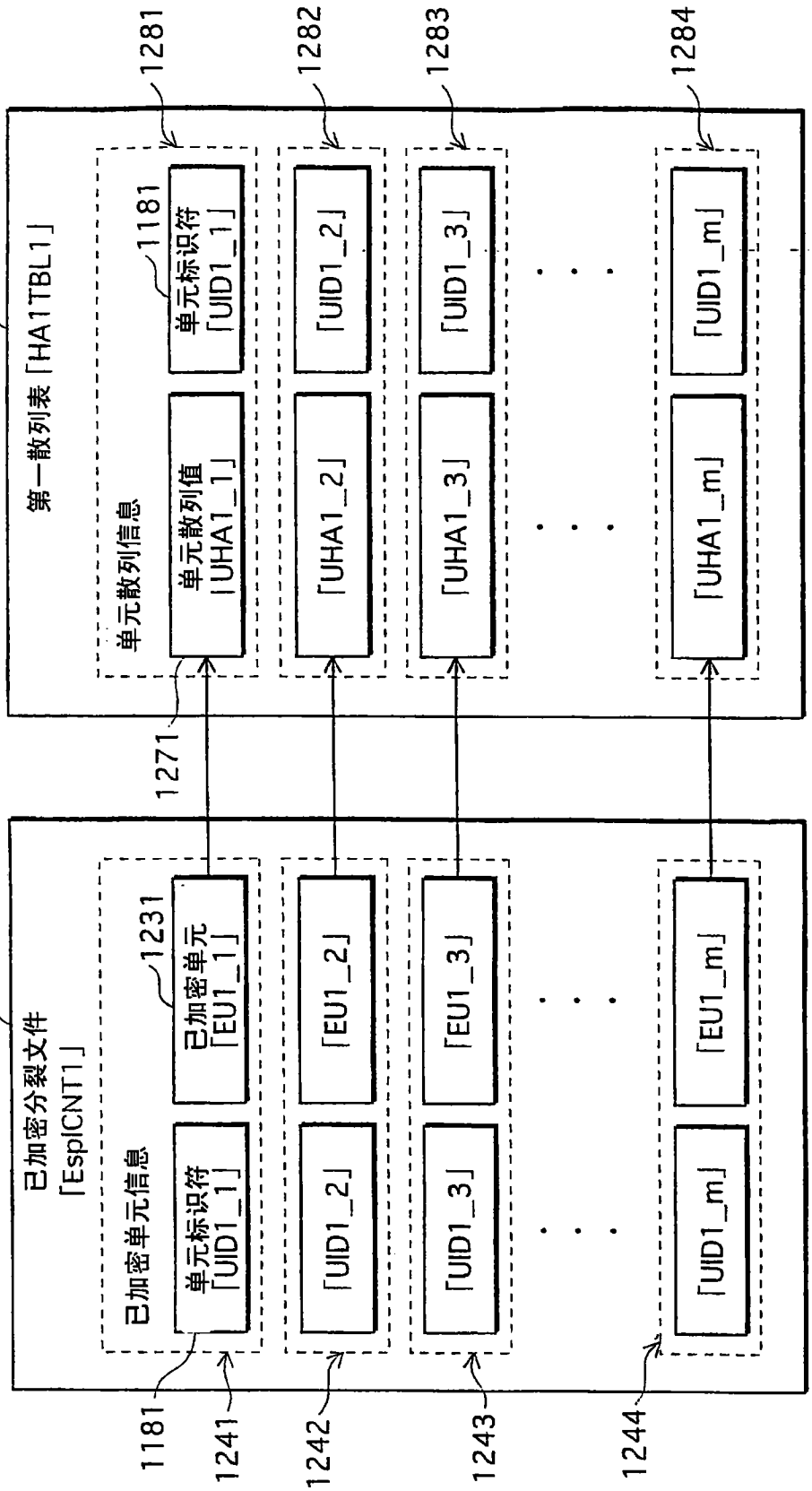

1261
第一散列表「HA1TBL1」
1281
1282
1283
1284
1181
单元标识符「UID1_1」
单元散列信息
单元散列值「UHA1_1」
「UID1_2」
「UID1_3」
「UID1_m」
「UHA1_2」
「UHA1_3」
「UHA1_m」
1271
1251
已加密分裂文件「EsplCNT1」
1231
已加密单元「EU1_1」
已加密单元信息
「EU1_2」
「EU1_3」
「EU1_m」
1181
1241
1242
1243
1244

图11

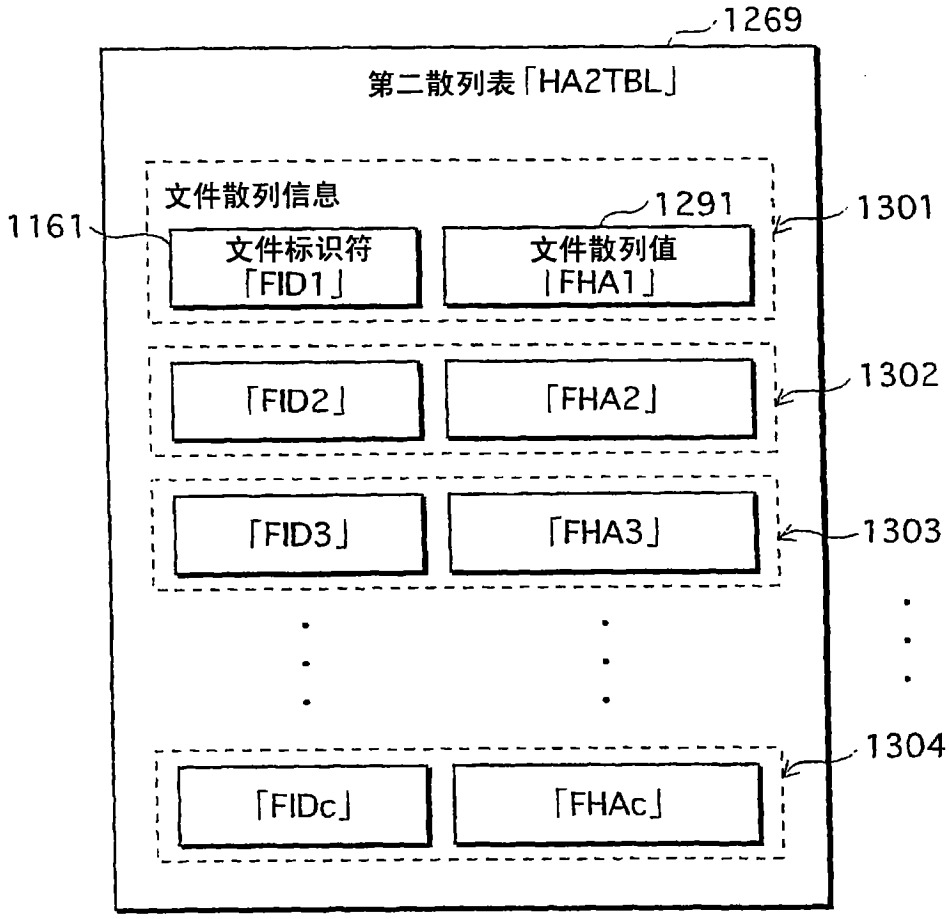

1269
第二散列表「HA2TBL」
文件散列信息
1161
文件标识符
「FID1」
1291
文件散列值
「FHA1」
1301
「FID2」
「FHA2」
1302
「FID3」
「FHA3」
1303
「FIDc」
「FHAc」
1304

图 12

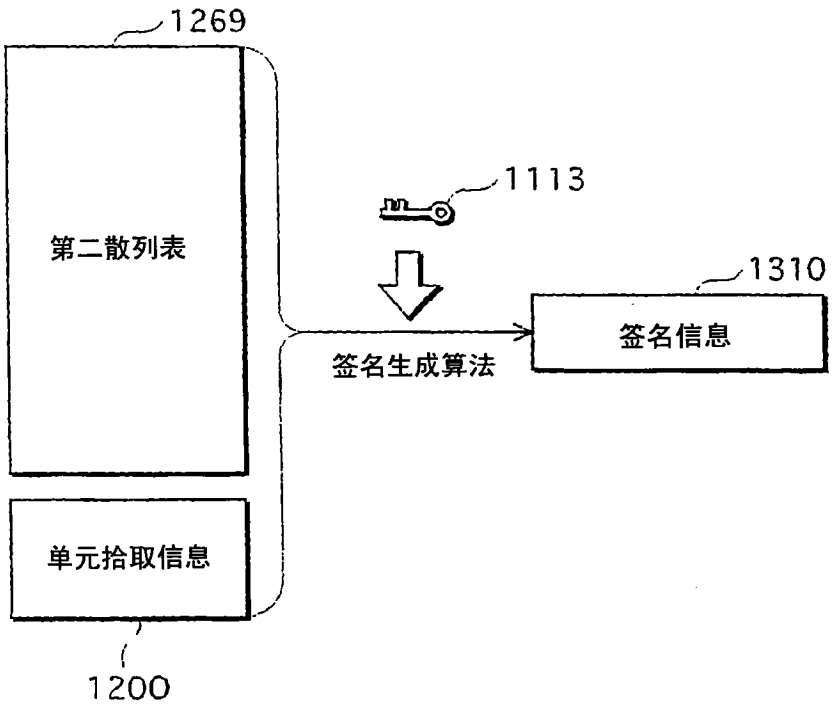


图 13

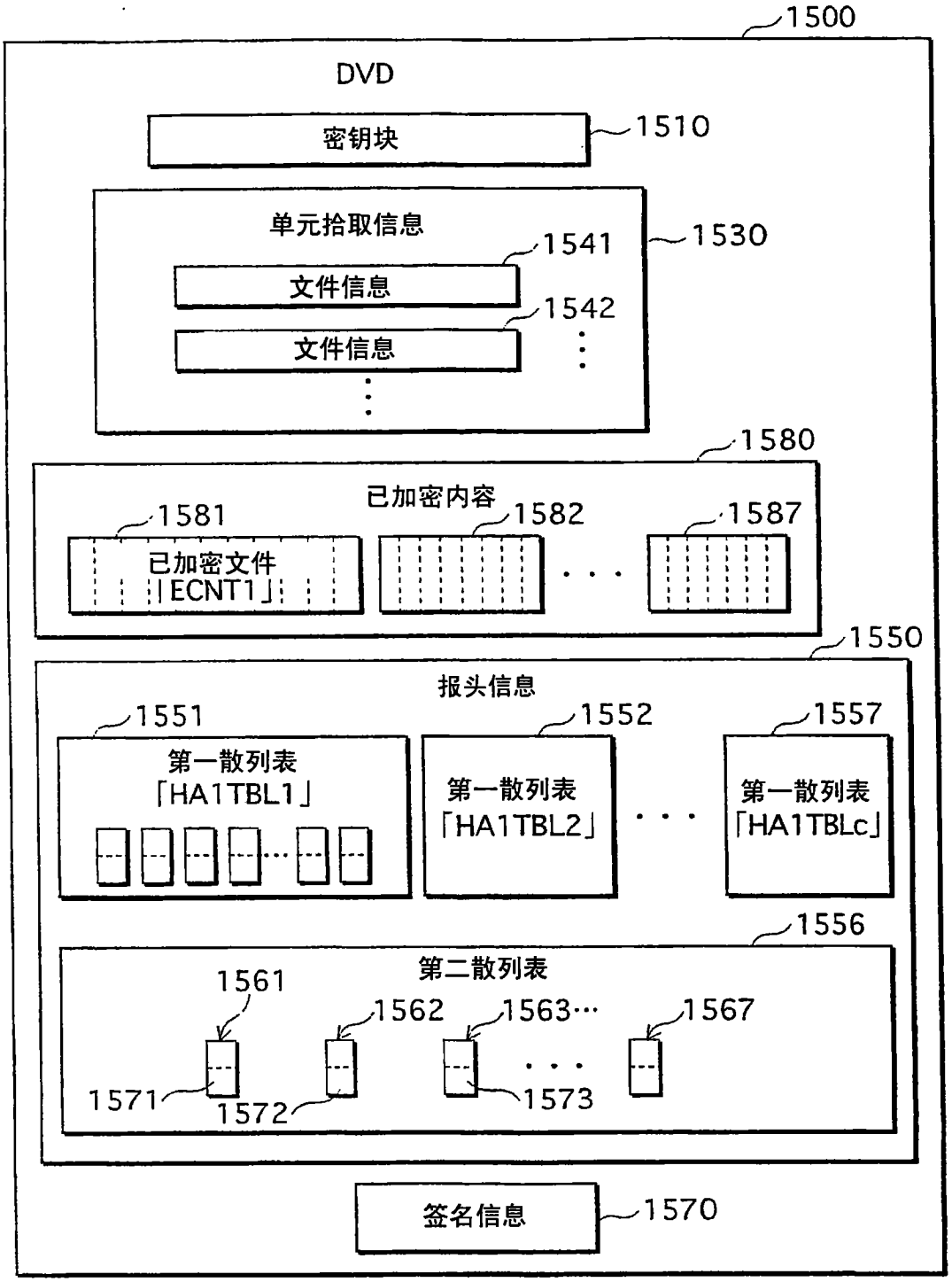

1500
DVD
密钥块
1510
单元拾取信息
1541
1530
文件信息
1542
文件信息
1580
已加密内容
1581
1582
1587
已加密文件
「ECNT1」
1550
报头信息
1551
1552
1557
第一散列表
「HA1TBL1」
第一散列表
「HA1TBL2」
第一散列表
「HA1TBLc」
1556
第二散列表
1561
1562
1563…
1567
1571
1572
1573
签名信息
1570

图 14

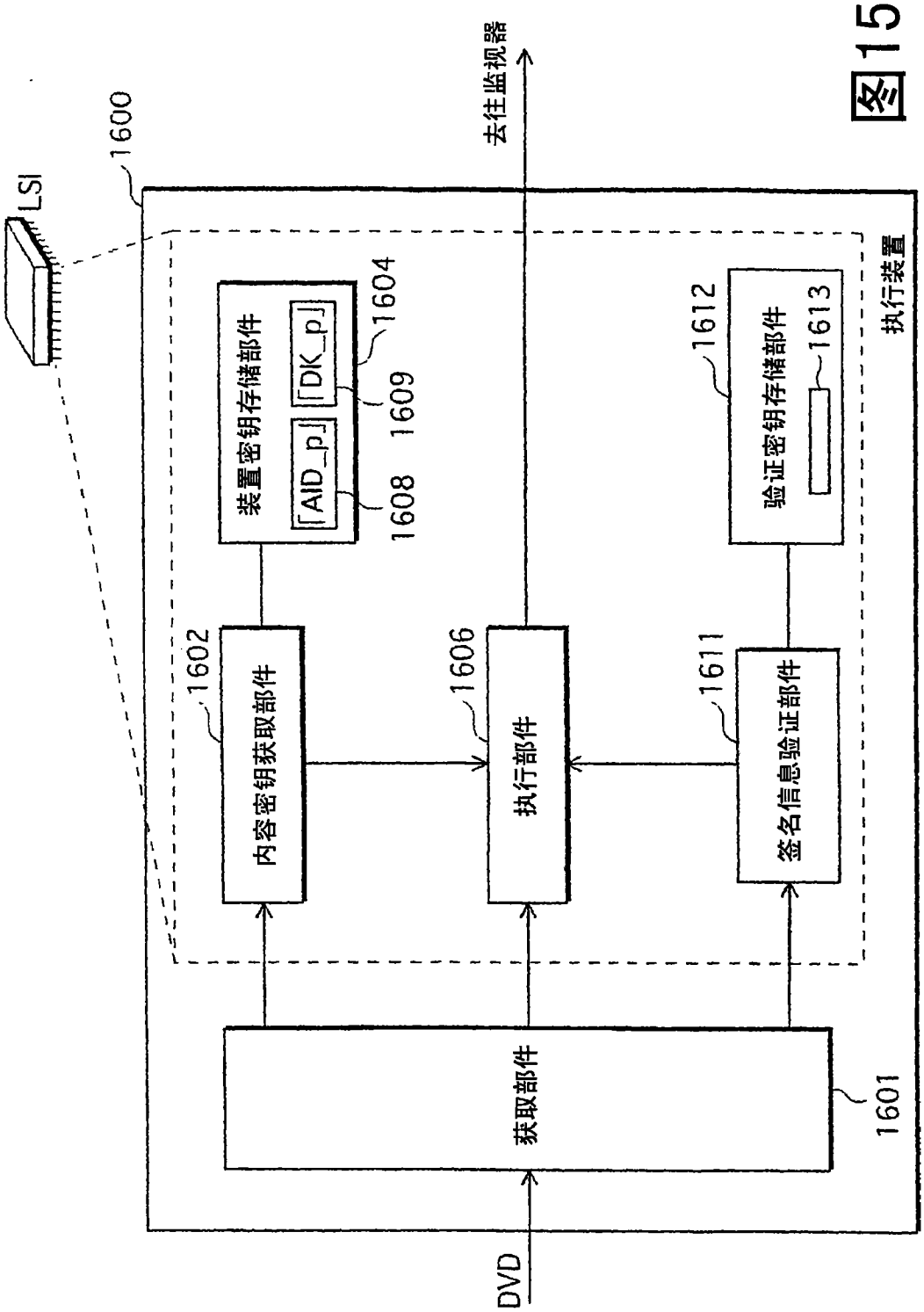

去往监视器
1600
LSI
装置密钥存储部件
「AID_p」
「DK_p」
1604
1609
1608
1602
内容密钥获取部件
1606
执行部件
1611
签名信息验证部件
1612
验证密钥存储部件
1613
执行装置
获取部件
1601
DVD

图15

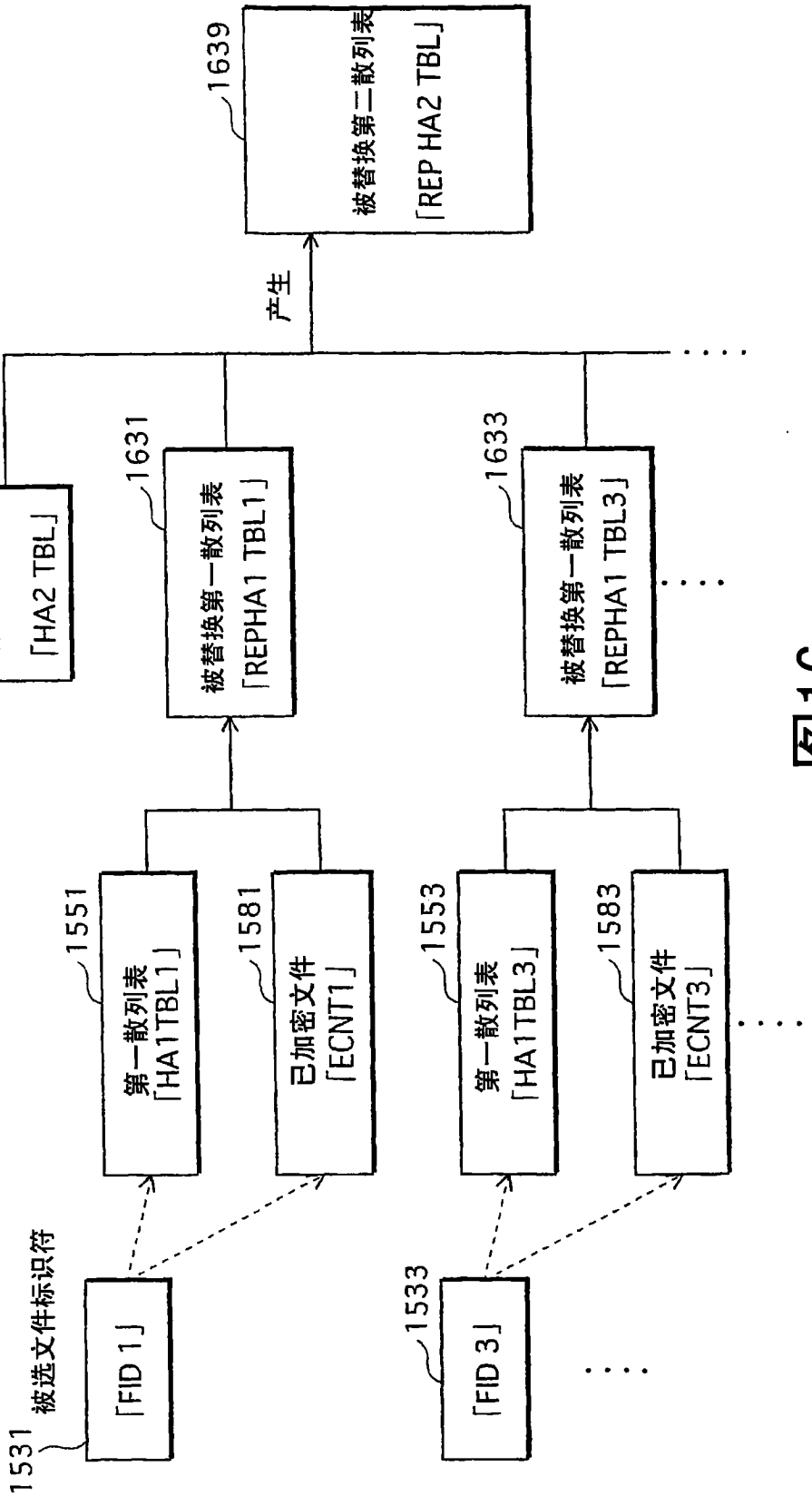

被选文件标识符
1531
「FID 1」
1533
「FID 3」
第一散列表
「HA1TBL1」
1551
第一散列表
「HA1TBL3」
1553
已加密文件
「ECNT1」
1581
已加密文件
「ECNT3」
1583
第二散列表
「HA2 TBL」
1556
被替换第一散列表
「REPHA1 TBL1」
1631
被替换第一散列表
「REPHA1 TBL3」
1633
产生
被替换第二散列表
「REP HA2 TBL」
1639

图16

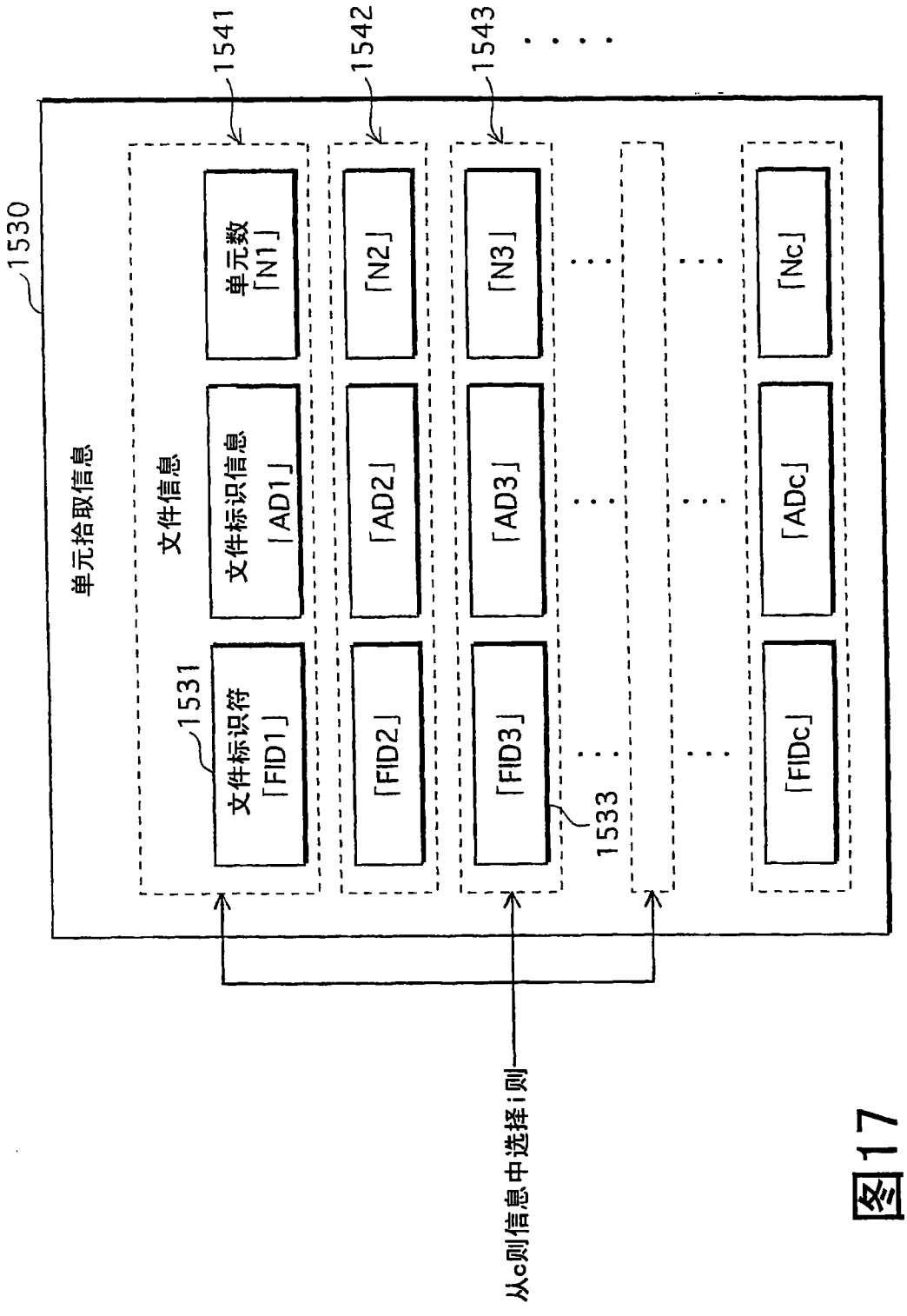

1530
单元拾取信息
文件信息
1531
文件标识符
「FID1」
文件标识信息
「AD1」
单元数
「N1」
1541
「FID2」
「AD2」
「N2」
1542
「FID3」
「AD3」
「N3」
1543
1533
「FIDc」
「ADc」
「Nc」
从c则信息中选择i则

图17

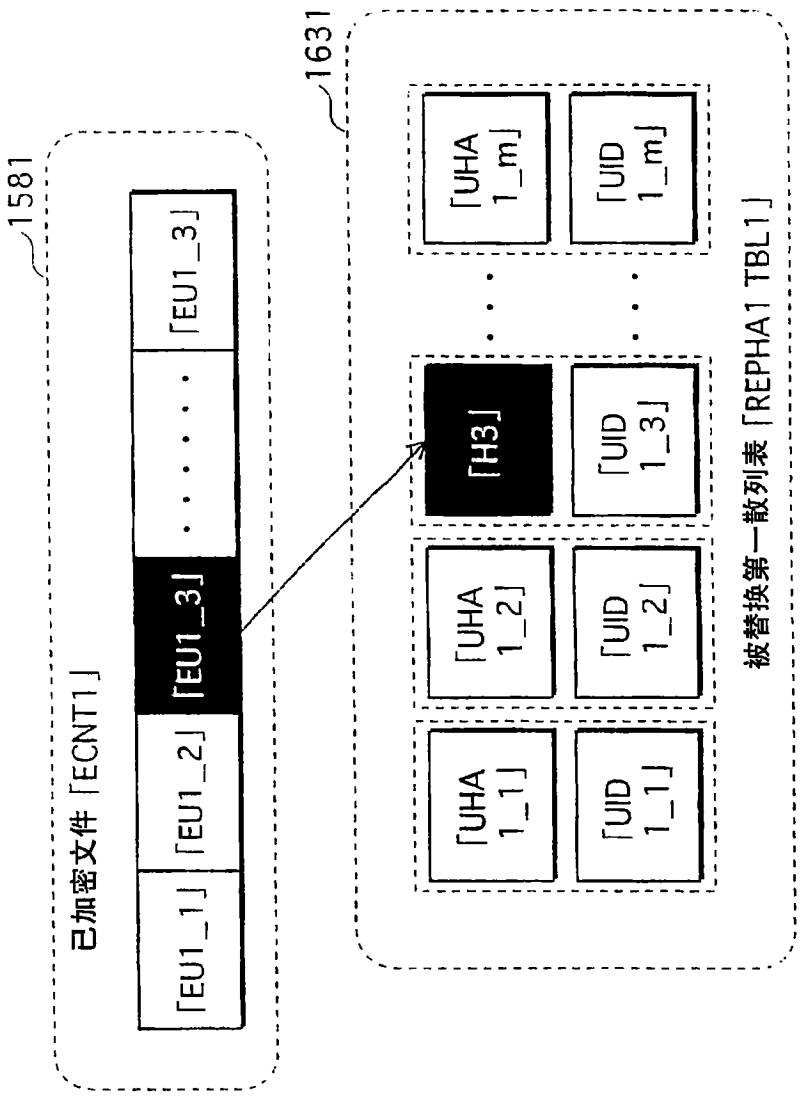

1581
已加密文件「ECNT1」
「EU1_1」
「EU1_2」
「EU1_3」
「EU1_3」
1631
被替换第一散列表「REPHA1 TBL1」
「UHA 1_1」
「UID 1_1」
「UHA 1_2」
「UID 1_2」
「H3」
「UID 1_3」
「UHA 1_m」
「UID 1_m」

图18

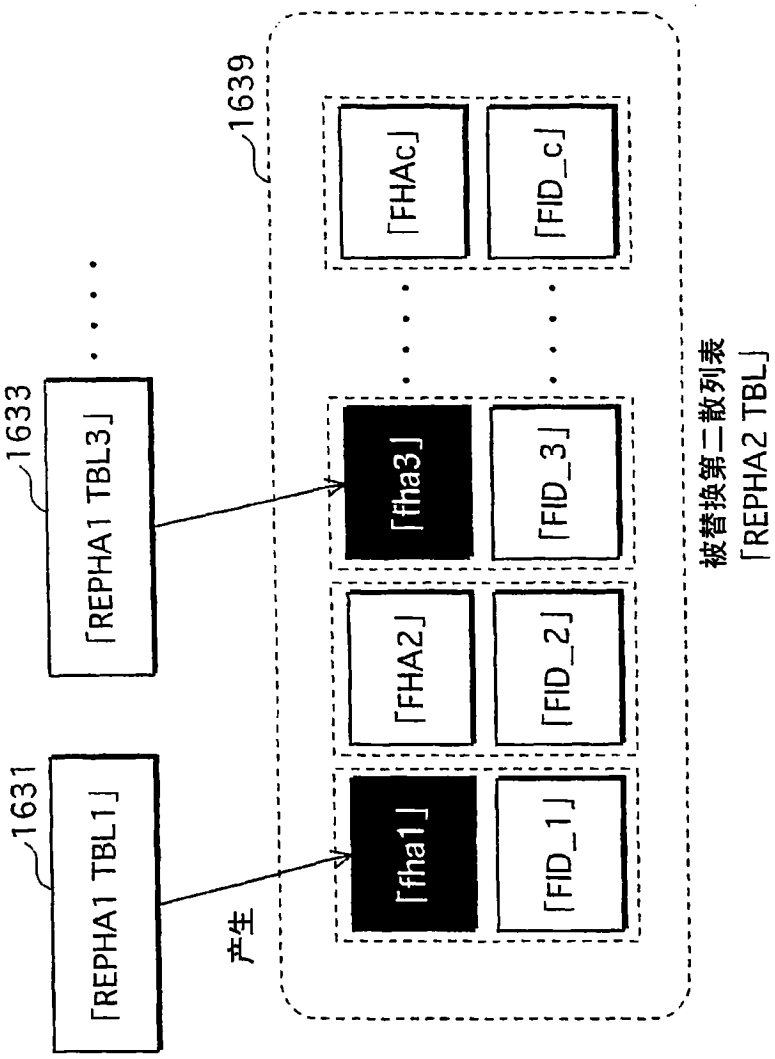

1639
「FHAc」
「FID_c」
1633
「REPHA1 TBL3」
「fha3」
「FID_3」
「FHA2」
「FID_2」
1631
「REPHA1 TBL1」
「fha1」
「FID_1」
产生
被替换第二散列表
「REPHA2 TBL」

图19

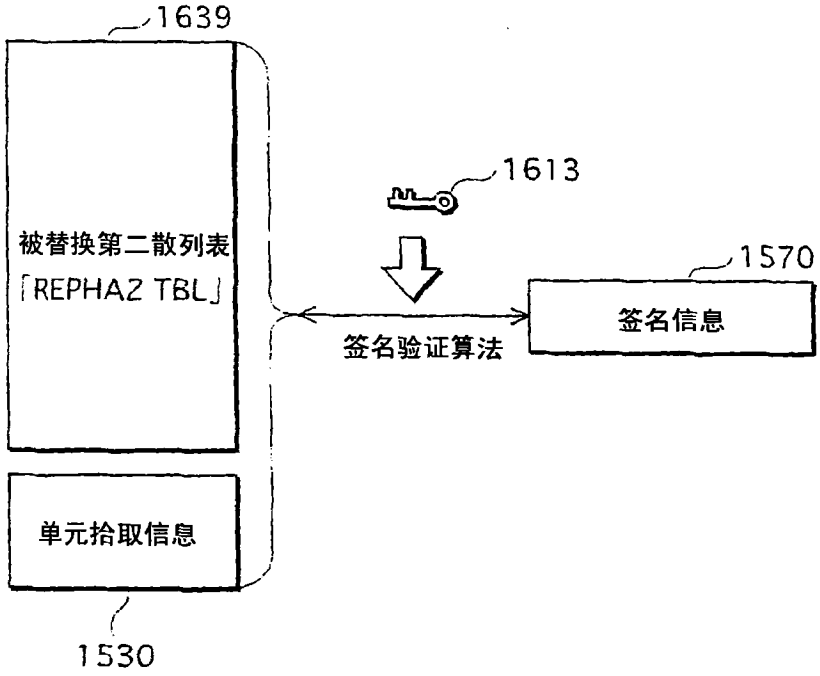


图 20

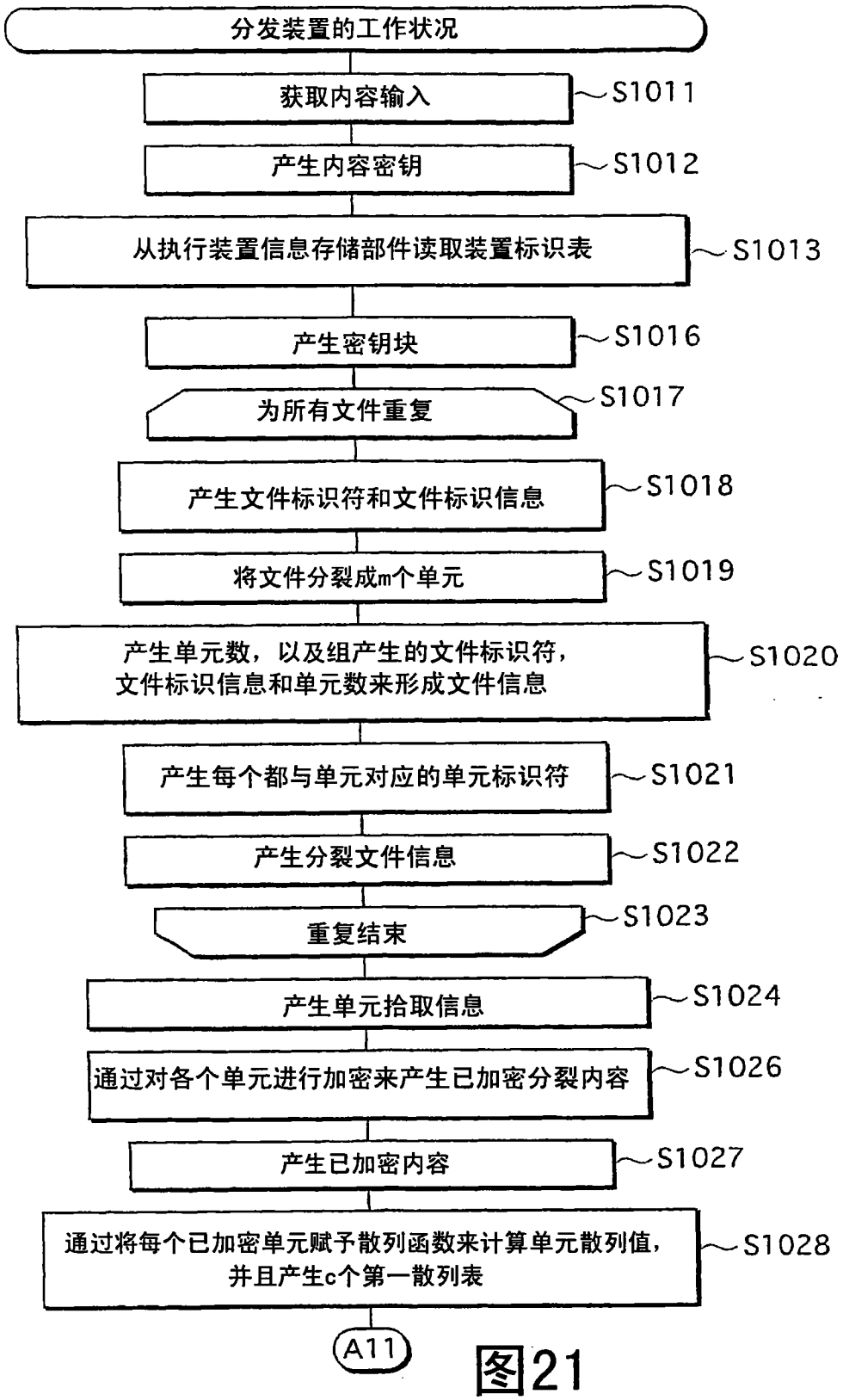

分发装置的工作状况
获取内容输入
S1011
产生内容密钥
S1012
从执行装置信息存储部件读取装置标识表
S1013
产生密钥块
S1016
为所有文件重复
S1017
产生文件标识符和文件标识信息
S1018
将文件分裂成m个单元
S1019
产生单元数，以及组产生的文件标识符，
文件标识信息和单元数来形成文件信息
S1020
产生每个都与单元对应的单元标识符
S1021
产生分裂文件信息
S1022
重复结束
S1023
产生单元拾取信息
S1024
通过对各个单元进行加密来产生已加密分裂内容
S1026
产生已加密内容
S1027
通过将每个已加密单元赋予散列函数来计算单元散列值，
并且产生c个第一散列表
S1028
A11

图21

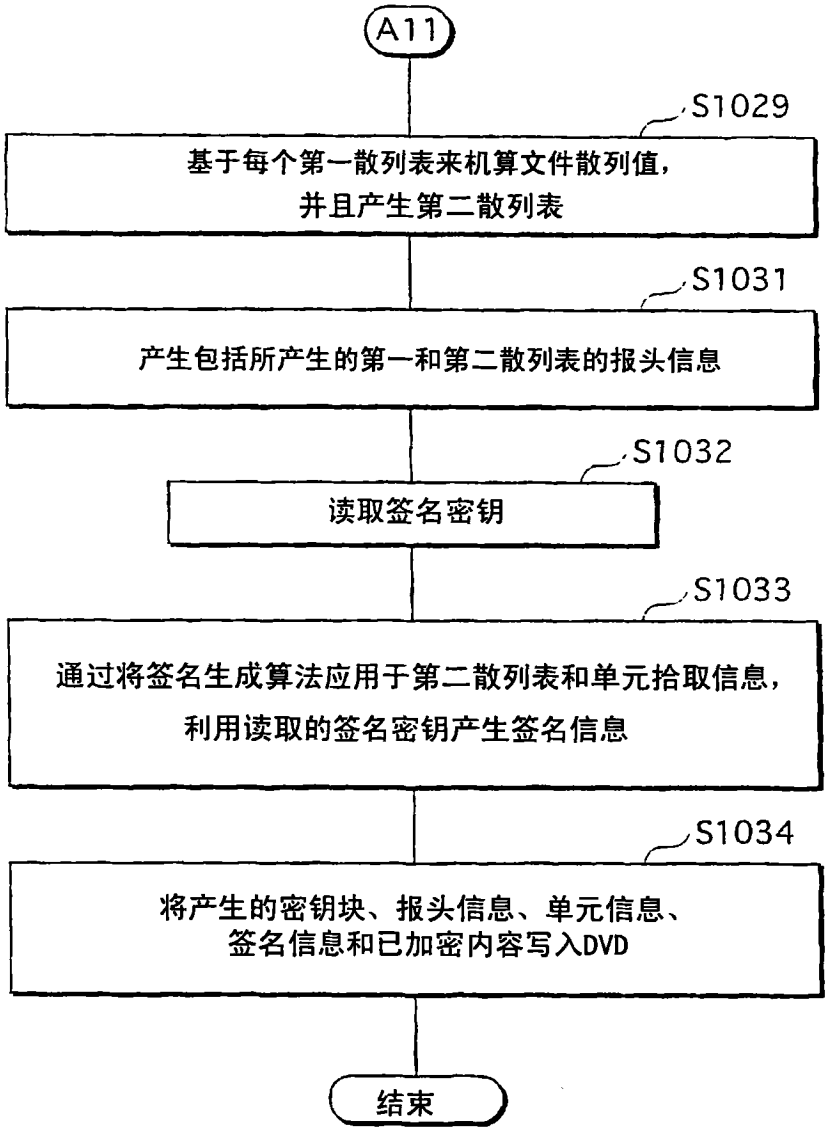

A11
S1029
基于每个第一散列表来机算文件散列值，
并且产生第二散列表
S1031
产生包括所产生的第一和第二散列表的报头信息
S1032
读取签名密钥
S1033
通过将签名生成算法应用于第二散列表和单元拾取信息，
利用读取的签名密钥产生签名信息
S1034
将产生的密钥块、报头信息、单元信息、
签名信息和已加密内容写入DVD
结束

图 22

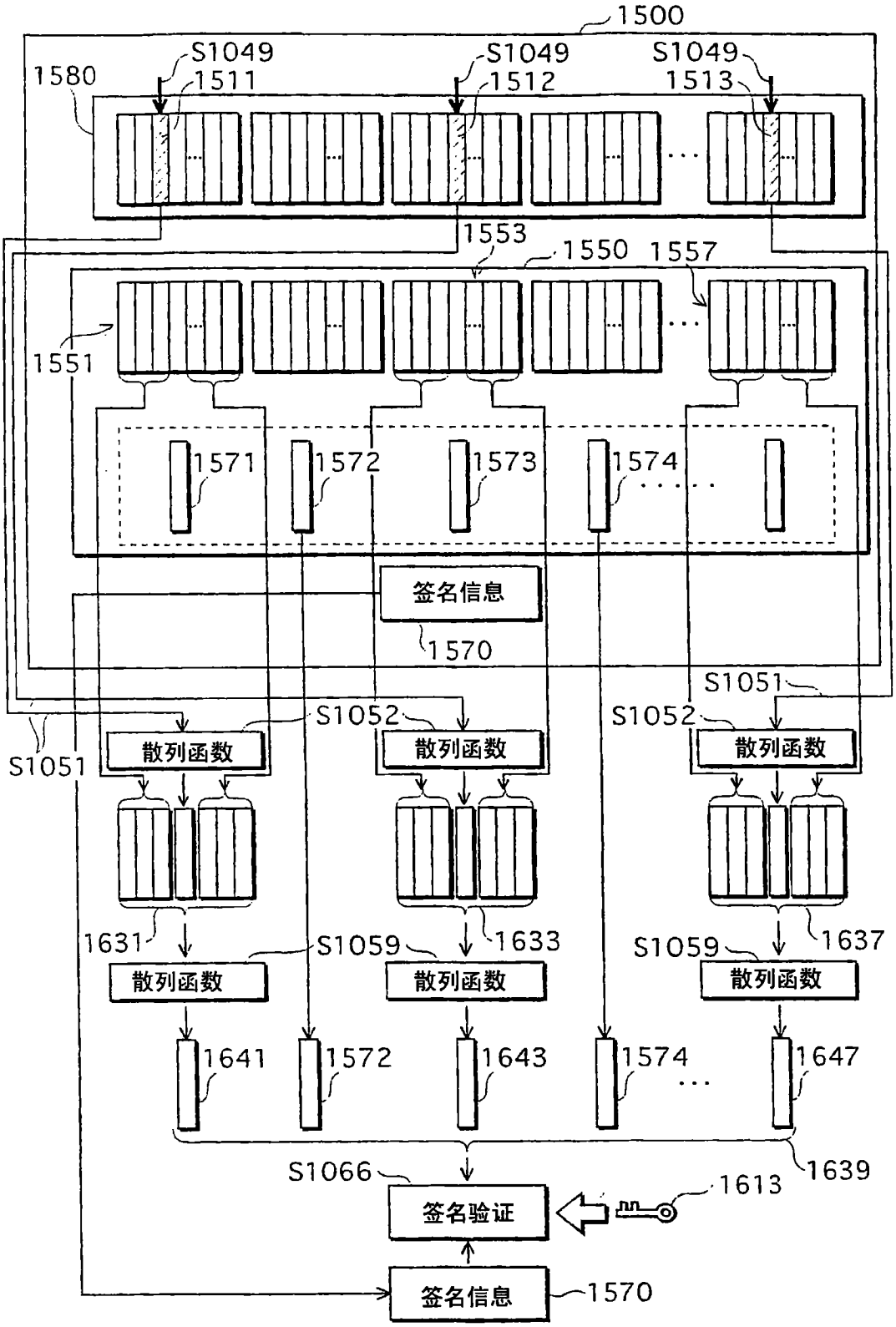

1500
S1049
S1049
S1049
1580
1511
1512
1513
1553
1550
1557
1551
1571
1572
1573
1574
签名信息
1570
S1051
S1052
S1052
S1051
散列函数
散列函数
散列函数
1631
S1059
1633
S1059
1637
散列函数
散列函数
散列函数
1641
1572
1643
1574
1647
1639
S1066
1613
签名验证
签名信息
1570

图 23

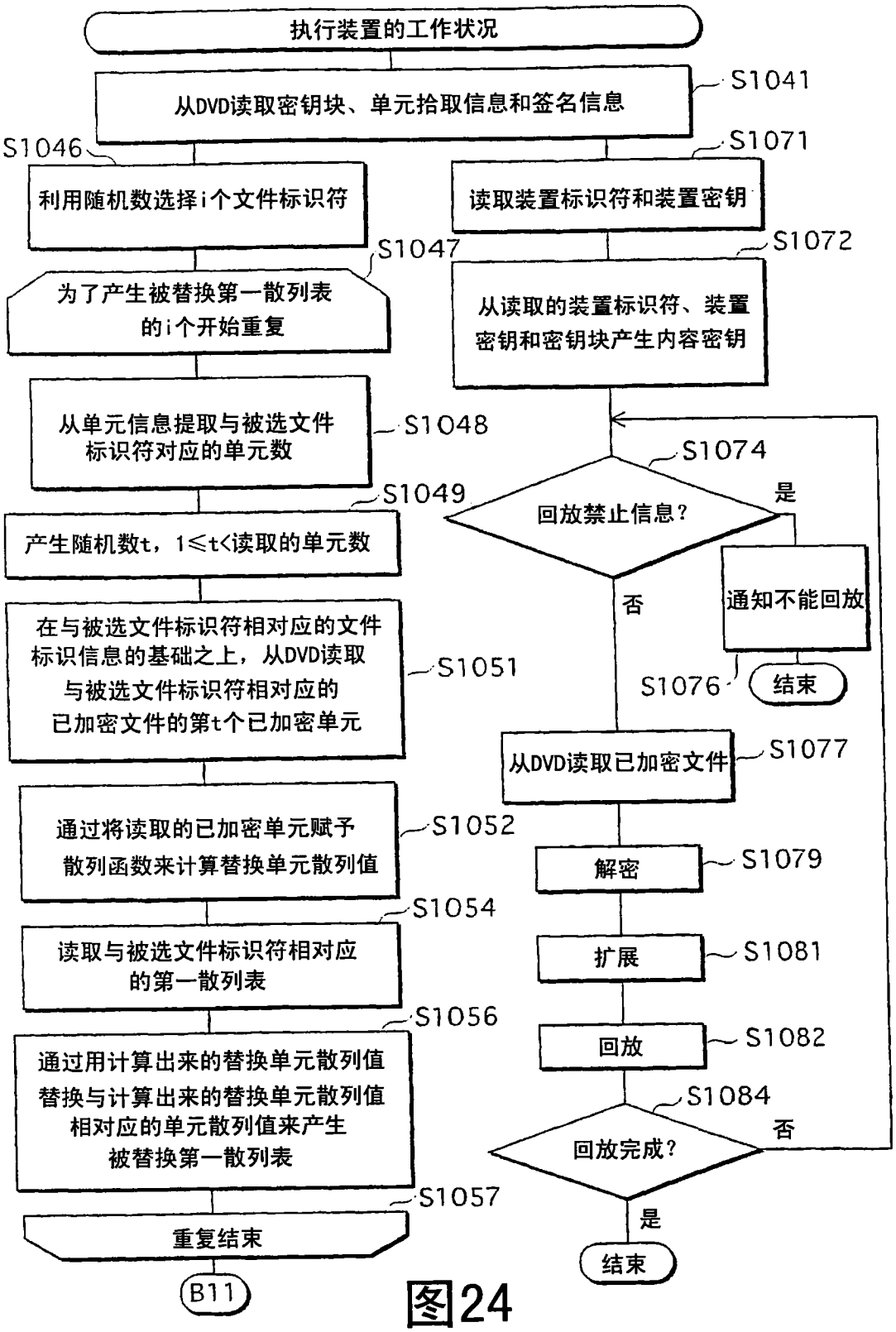

执行装置的工作状况
从DVD读取密钥块、单元拾取信息和签名信息
S1041
S1046
利用随机数选择i个文件标识符
S1071
读取装置标识符和装置密钥
S1047
为了产生被替换第一散列表的i个开始重复
S1072
从读取的装置标识符、装置密钥和密钥块产生内容密钥
从单元信息提取与被选文件标识符对应的单元数
S1048
S1074
回放禁止信息？
是
S1049
产生随机数t，1≤t<读取的单元数
否
通知不能回放
在与被选文件标识符相对应的文件标识信息的基础之上，从DVD读取与被选文件标识符相对应的已加密文件的第t个已加密单元
S1051
S1076
结束
从DVD读取已加密文件
S1077
通过将读取的已加密单元赋予散列函数来计算替换单元散列值
S1052
解密
S1079
S1054
读取与被选文件标识符相对应的第一散列表
扩展
S1081
S1056
通过用计算出来的替换单元散列值替换与计算出来的替换单元散列值相对应的单元散列值来产生被替换第一散列表
回放
S1082
S1084
回放完成？
否
S1057
重复结束
是
结束
B11

图24

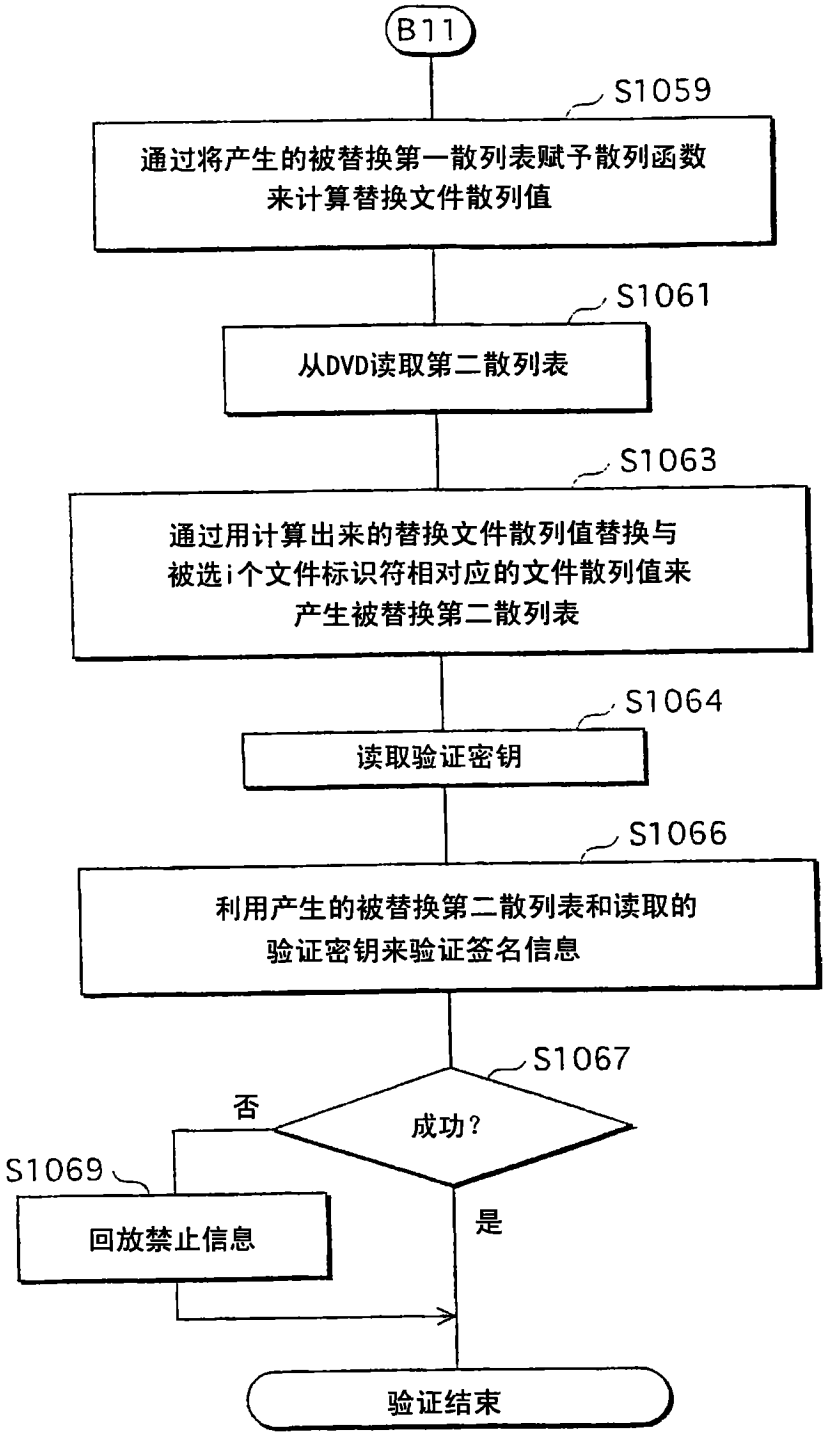

B11
S1059
通过将产生的被替换第一散列表赋予散列函数
来计算替换文件散列值
S1061
从DVD读取第二散列表
S1063
通过用计算出来的替换文件散列值替换与
被选i个文件标识符相对应的文件散列值来
产生被替换第二散列表
S1064
读取验证密钥
S1066
利用产生的被替换第二散列表和读取的
验证密钥来验证签名信息
S1067
成功?
否
是
S1069
回放禁止信息
验证结束

图 25

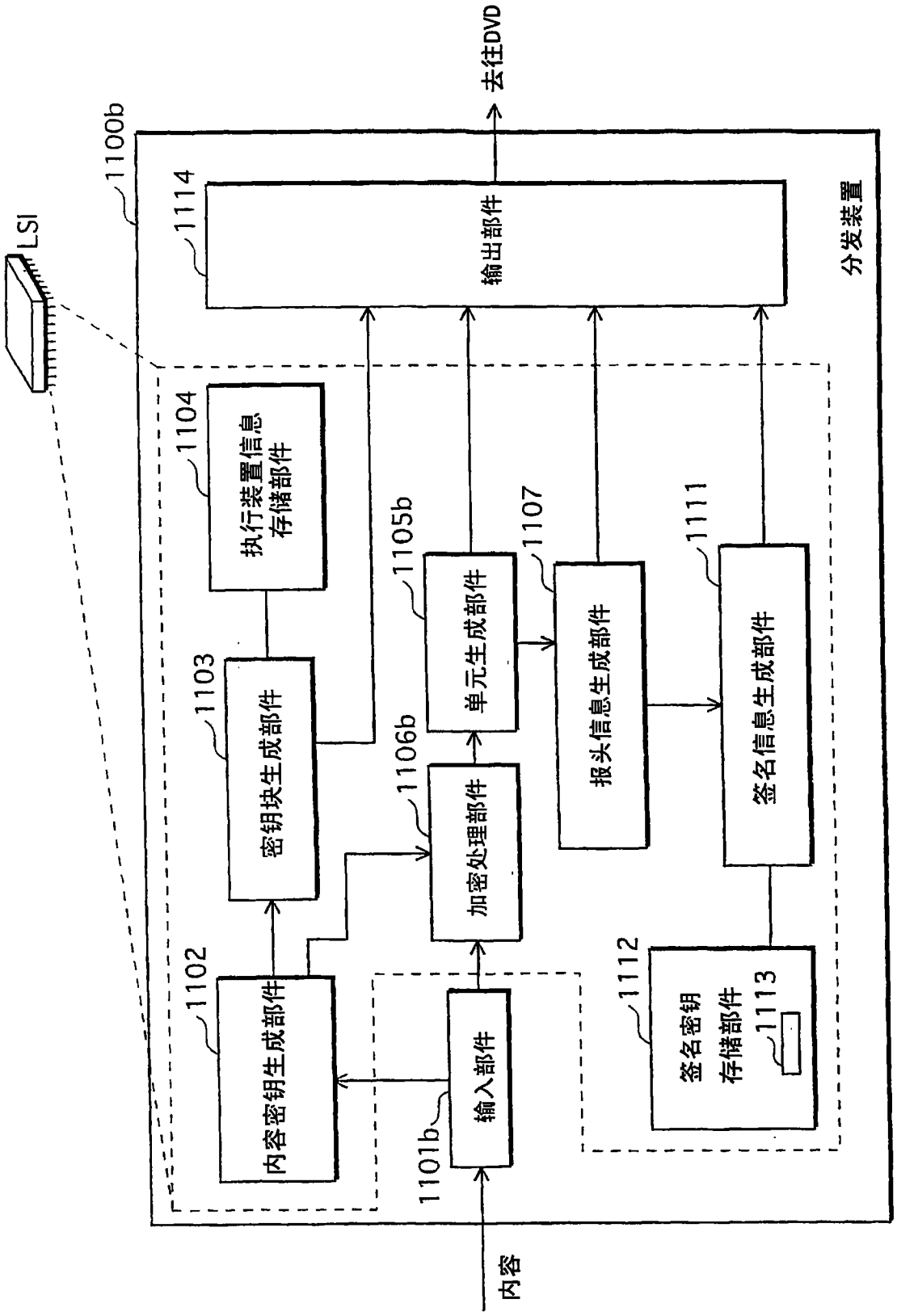

去往DVD
1100b
LSI
1114
输出部件
分发装置
1104
执行装置信息存储部件
1103
密钥块生成部件
1105b
单元生成部件
1107
报头信息生成部件
1111
签名信息生成部件
1106b
加密处理部件
1102
内容密钥生成部件
1112
签名密钥存储部件
1113
1101b
输入部件
内容

图26

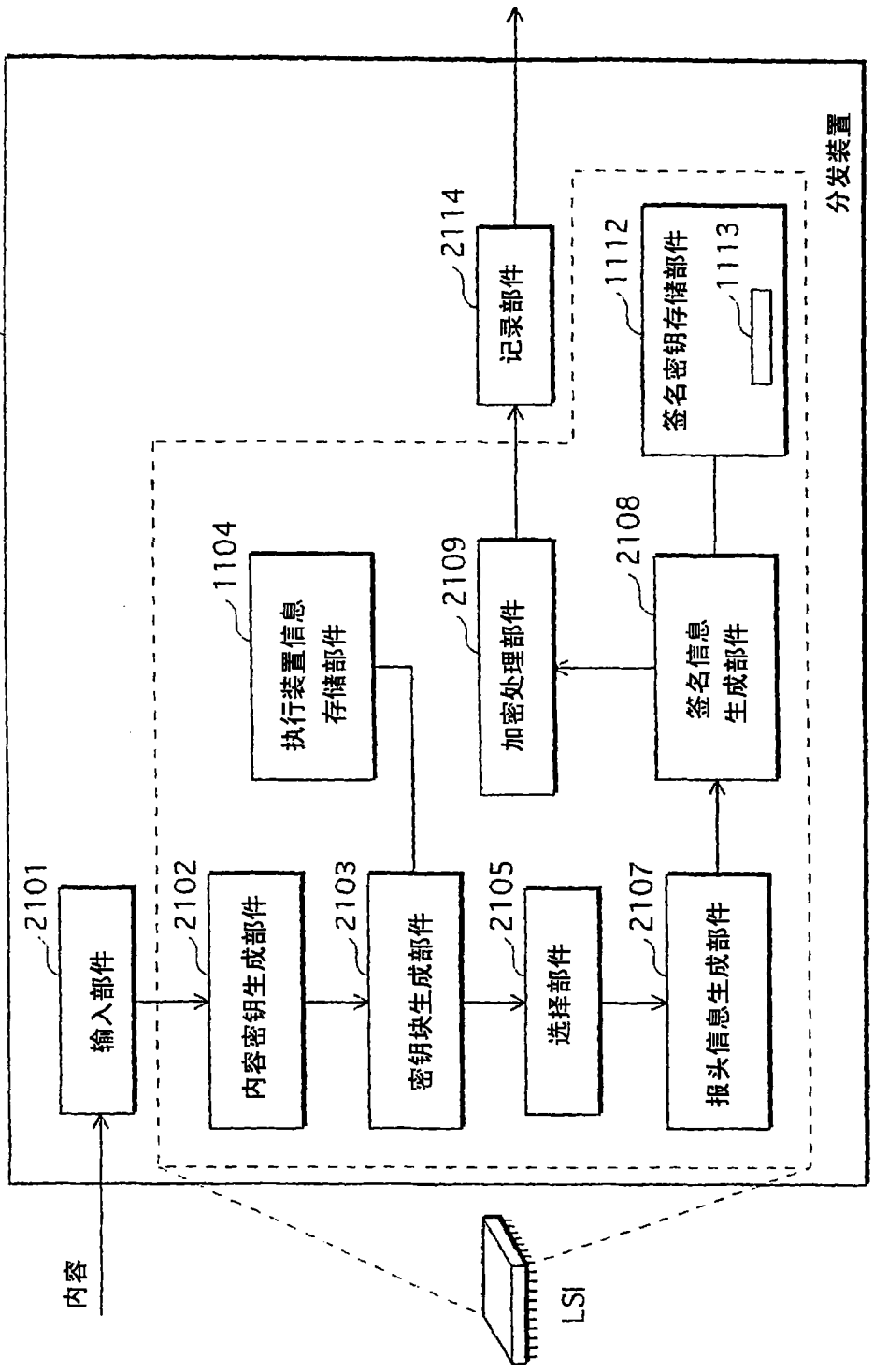

2100
分发装置
2101
输入部件
2102
内容密钥生成部件
2103
密钥块生成部件
2105
选择部件
2107
报头信息生成部件
2108
签名信息生成部件
2109
加密处理部件
1104
执行装置信息存储部件
2114
记录部件
1112
签名密钥存储部件
1113
内容
LSI

图27

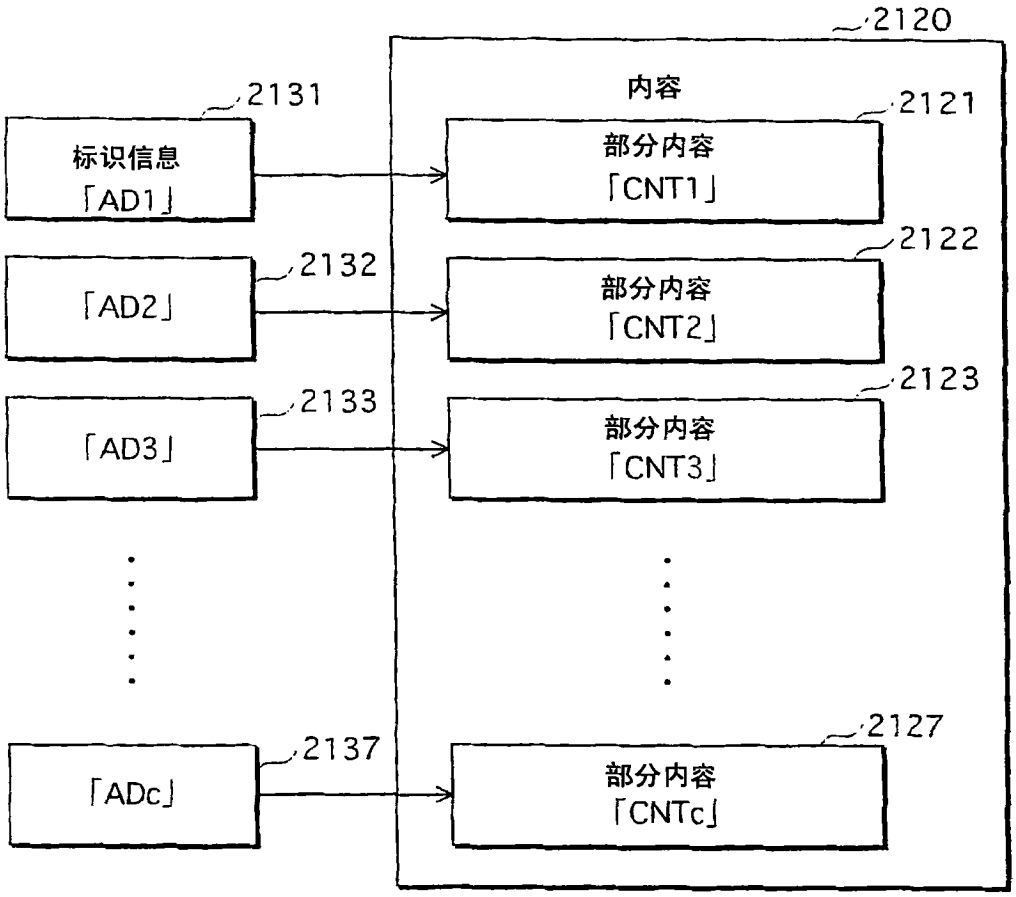

2120
内容
2131
标识信息
「AD1」
2121
部分内容
「CNT1」
2132
「AD2」
2122
部分内容
「CNT2」
2133
「AD3」
2123
部分内容
「CNT3」
2137
「ADc」
2127
部分内容
「CNTc」

图 28

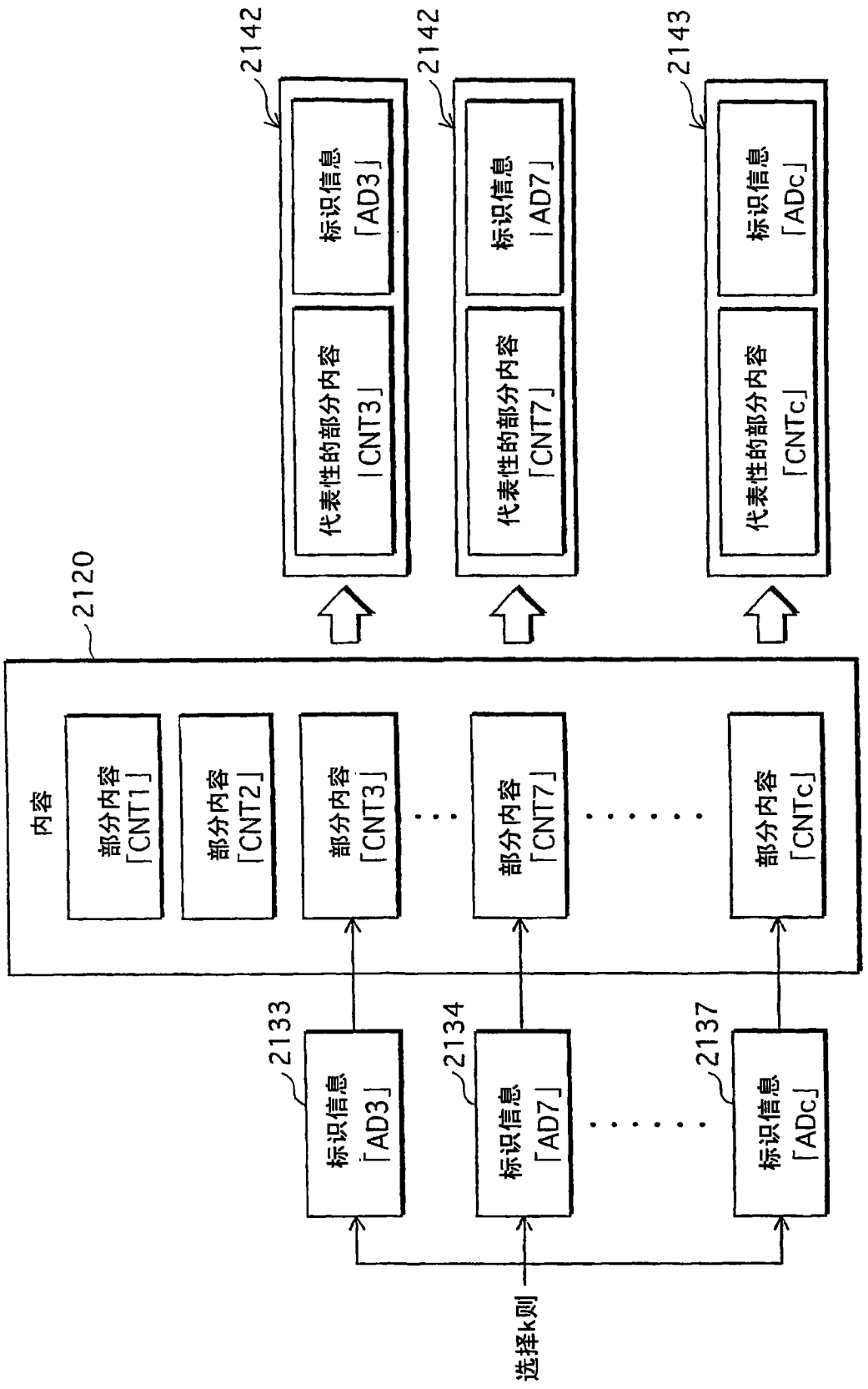

2142
2142
2143
标识信息「AD3」
代表性的部分内容「CNT3」
标识信息「AD7」
代表性的部分内容「CNT7」
标识信息「ADc」
代表性的部分内容「CNTc」
2120
内容
部分内容「CNT1」
部分内容「CNT2」
部分内容「CNT3」
部分内容「CNT7」
部分内容「CNTc」
2133
2134
2137
标识信息「AD3」
标识信息「AD7」
标识信息「ADc」
选择k则

图29

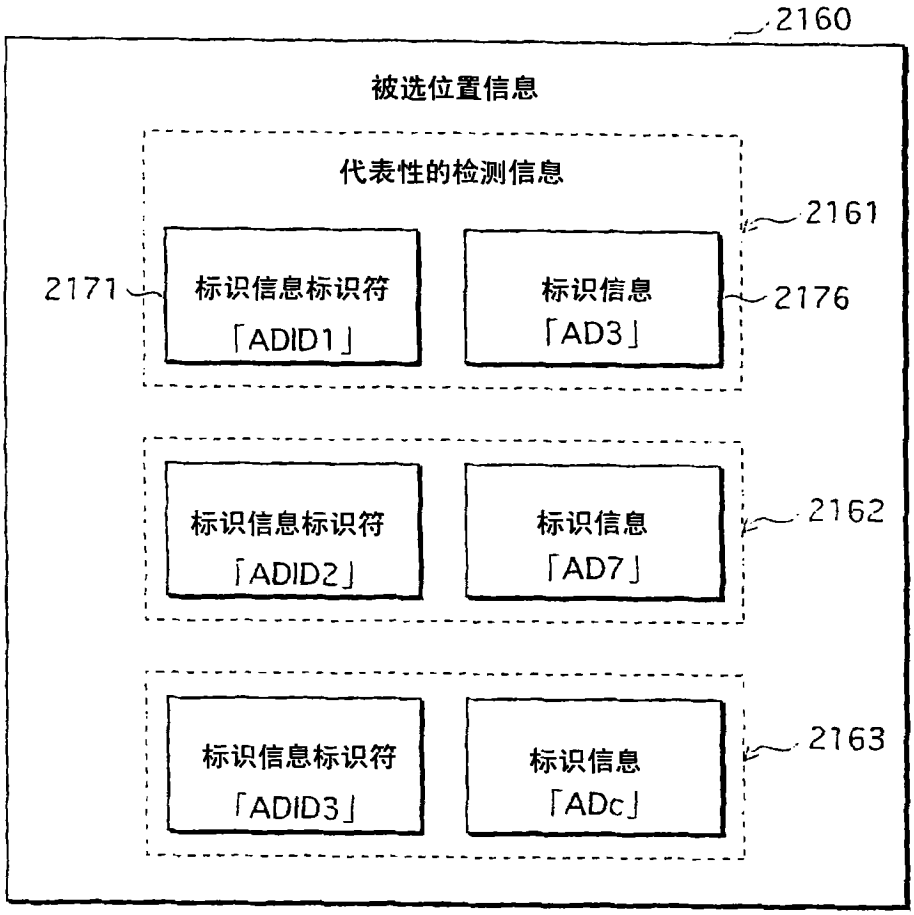

2160
被选位置信息
代表性的检测信息
2161
2171
标识信息标识符
「ADID1」
标识信息
「AD3」
2176
2162
标识信息标识符
「ADID2」
标识信息
「AD7」
2163
标识信息标识符
「ADID3」
标识信息
「ADc」

图 30

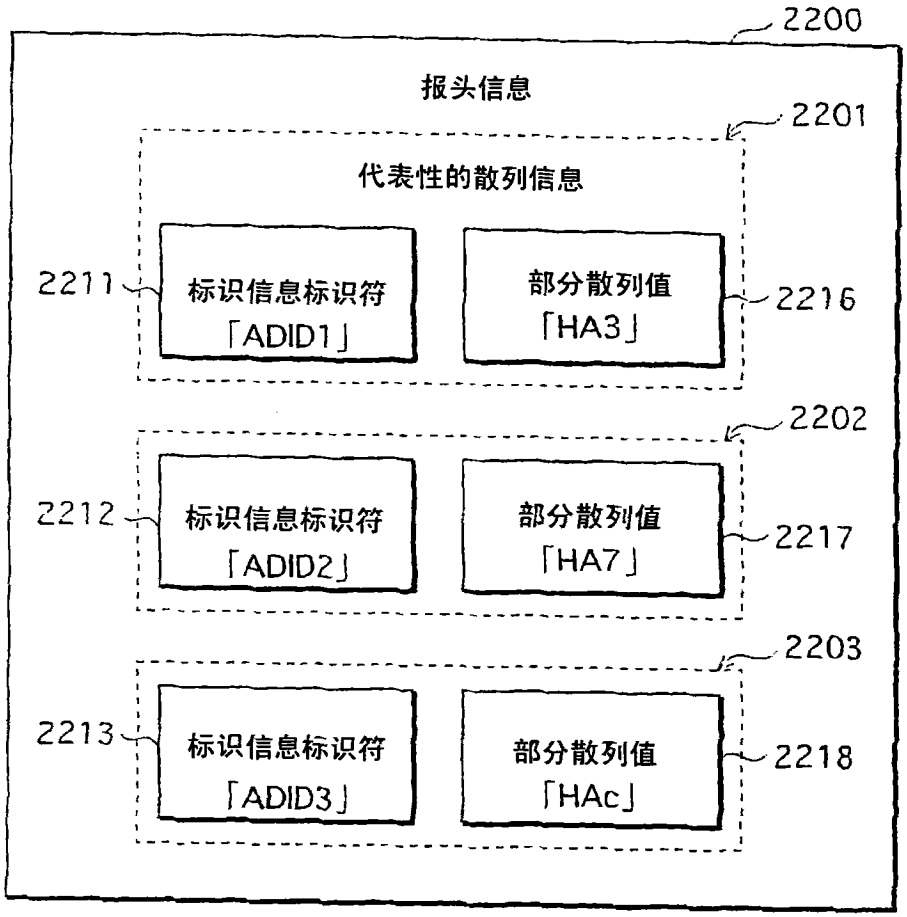

2200
报头信息
2201
代表性的散列信息
2211
标识信息标识符
「ADID1」
部分散列值
「HA3」
2216
2202
2212
标识信息标识符
「ADID2」
部分散列值
「HA7」
2217
2203
2213
标识信息标识符
「ADID3」
部分散列值
「HAc」
2218

图 31

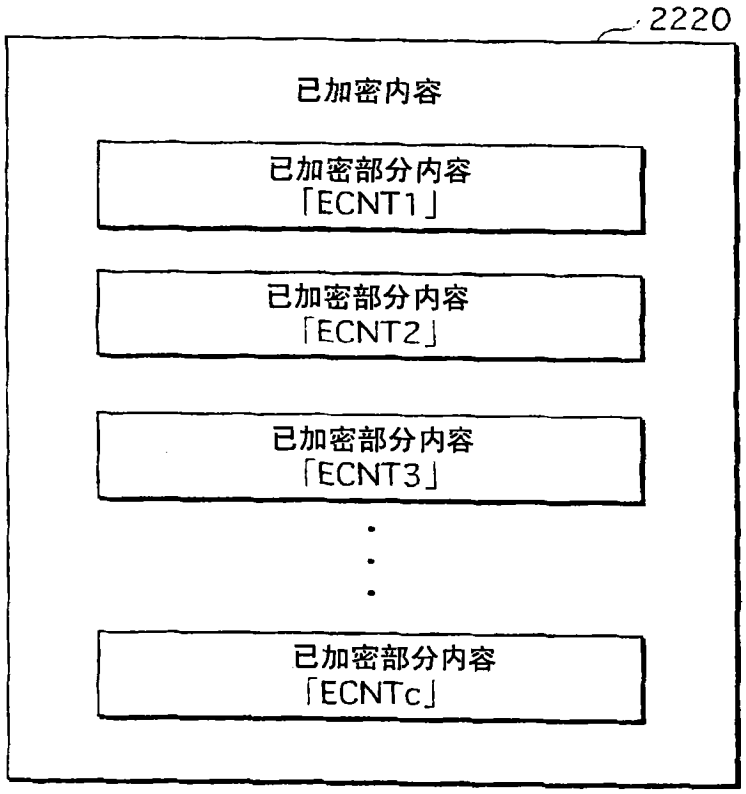

2220
已加密内容
已加密部分内容
「ECNT1」
已加密部分内容
「ECNT2」
已加密部分内容
「ECNT3」
已加密部分内容
「ECNTc」

图 32

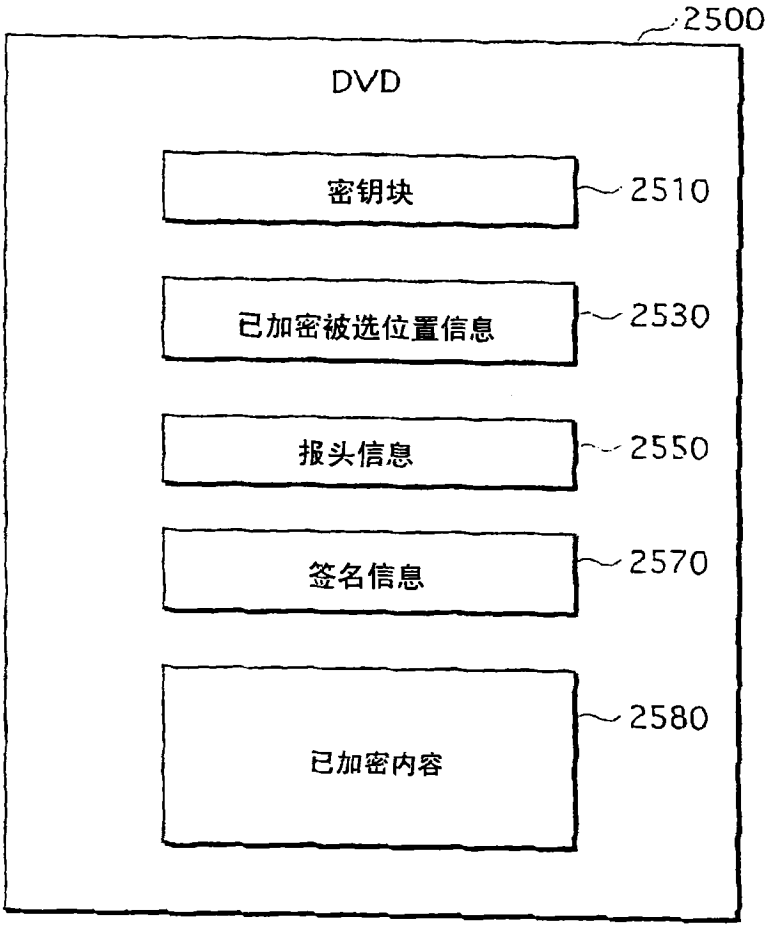

2500
DVD
密钥块
2510
已加密被选位置信息
2530
报头信息
2550
签名信息
2570
已加密内容
2580

图 33

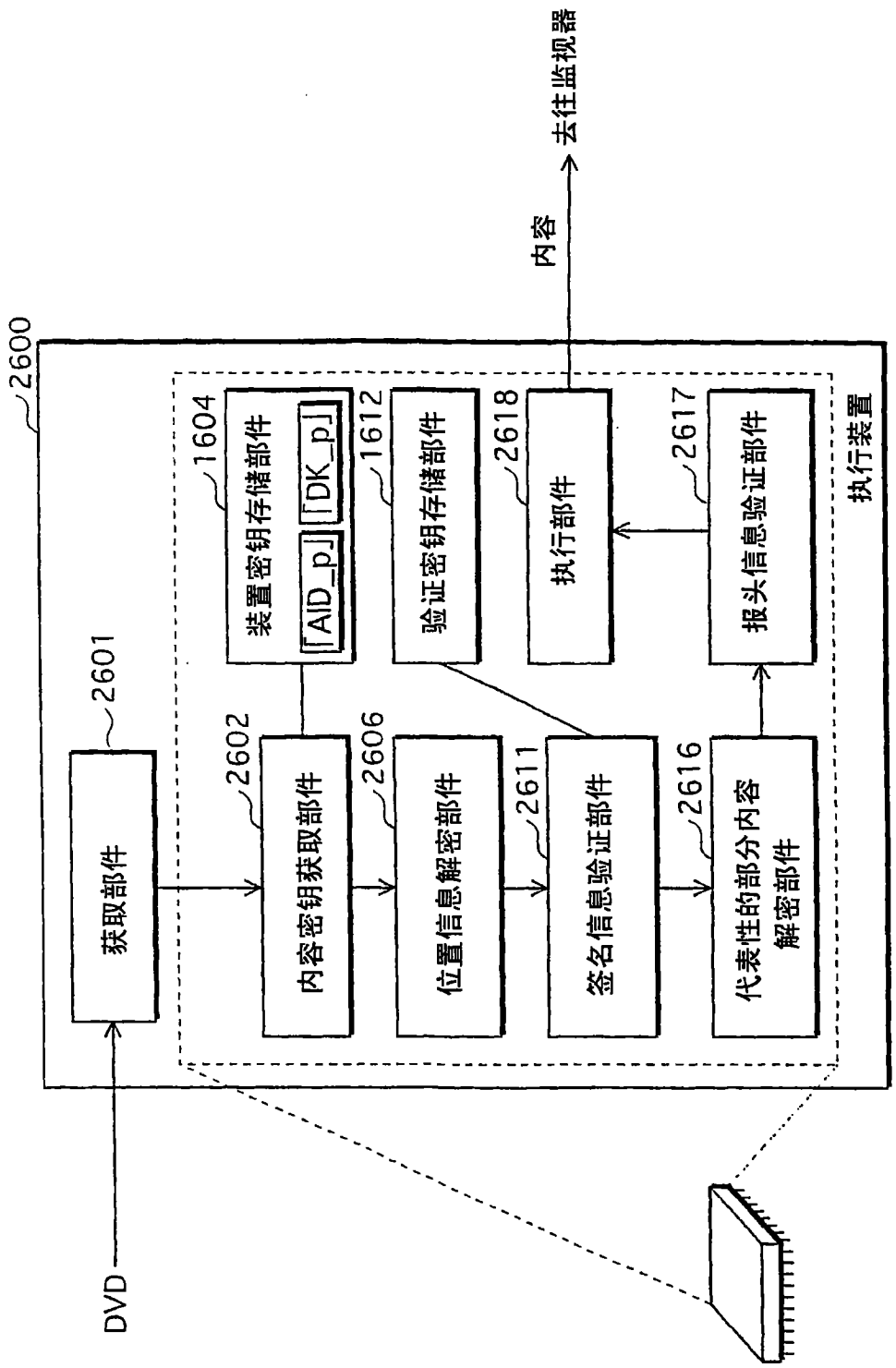

2600
执行装置
内容
去往监视器
1604
装置密钥存储部件
「AID_p」
「DK_p」
1612
验证密钥存储部件
2618
执行部件
2617
报头信息验证部件
2601
获取部件
2602
内容密钥获取部件
2606
位置信息解密部件
2611
签名信息验证部件
2616
代表性的部分内容
解密部件
DVD

图34

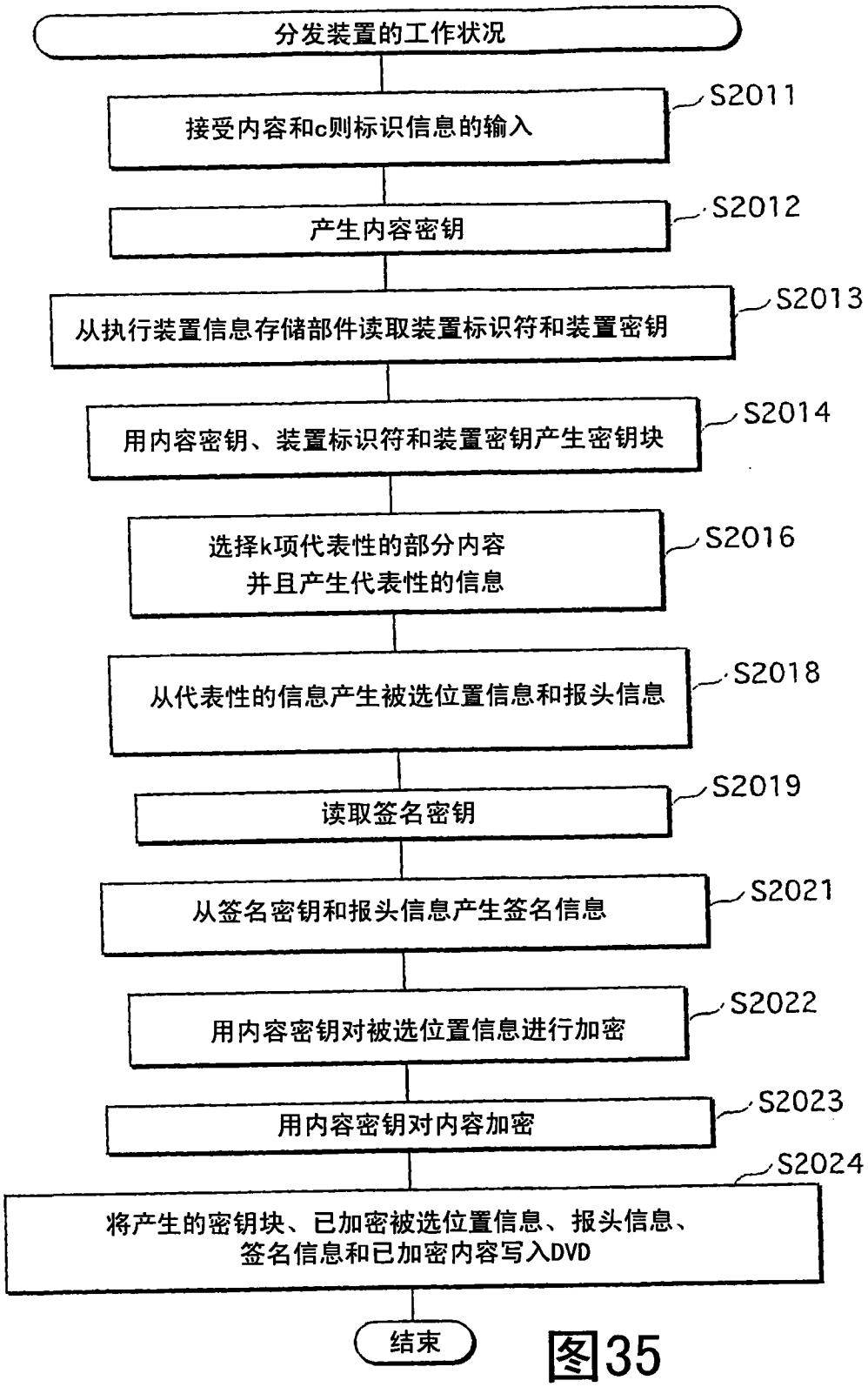

分发装置的工作状况
接受内容和c则标识信息的输入
S2011
产生内容密钥
S2012
从执行装置信息存储部件读取装置标识符和装置密钥
S2013
用内容密钥、装置标识符和装置密钥产生密钥块
S2014
选择k项代表性的部分内容
并且产生代表性的信息
S2016
从代表性的信息产生被选位置信息和报头信息
S2018
读取签名密钥
S2019
从签名密钥和报头信息产生签名信息
S2021
用内容密钥对被选位置信息进行加密
S2022
用内容密钥对内容加密
S2023
将产生的密钥块、已加密被选位置信息、报头信息、
签名信息和已加密内容写入DVD
S2024
结束

图35

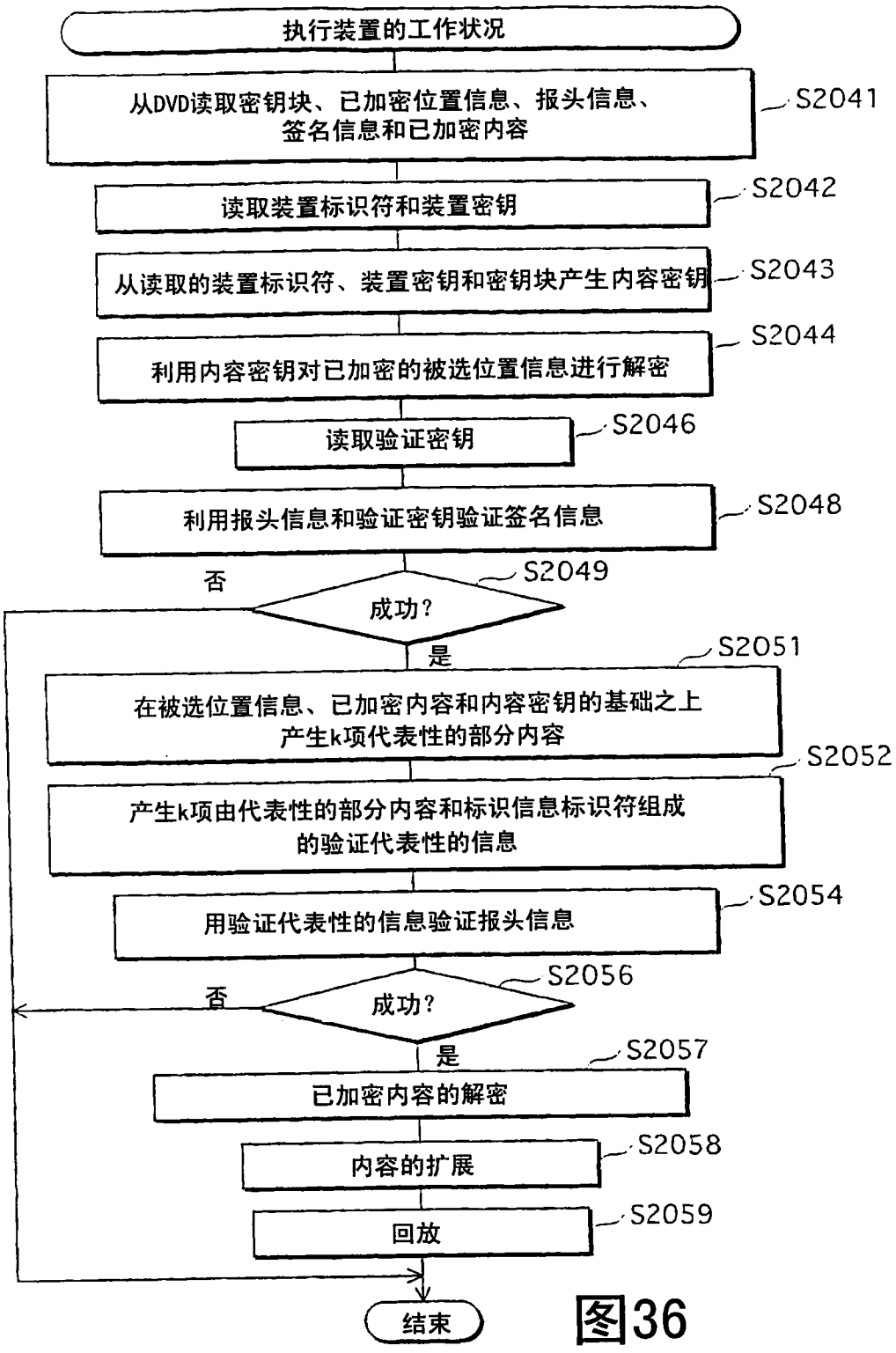

执行装置的工作状况
从DVD读取密钥块、已加密位置信息、报头信息、签名信息和已加密内容
S2041
读取装置标识符和装置密钥
S2042
从读取的装置标识符、装置密钥和密钥块产生内容密钥
S2043
利用内容密钥对已加密的被选位置信息进行解密
S2044
读取验证密钥
S2046
利用报头信息和验证密钥验证签名信息
S2048
否
成功?
S2049
是
在被选位置信息、已加密内容和内容密钥的基础之上产生k项代表性的部分内容
S2051
产生k项由代表性的部分内容和标识信息标识符组成的验证代表性的信息
S2052
用验证代表性的信息验证报头信息
S2054
否
成功?
S2056
是
已加密内容的解密
S2057
内容的扩展
S2058
回放
S2059
结束

图36

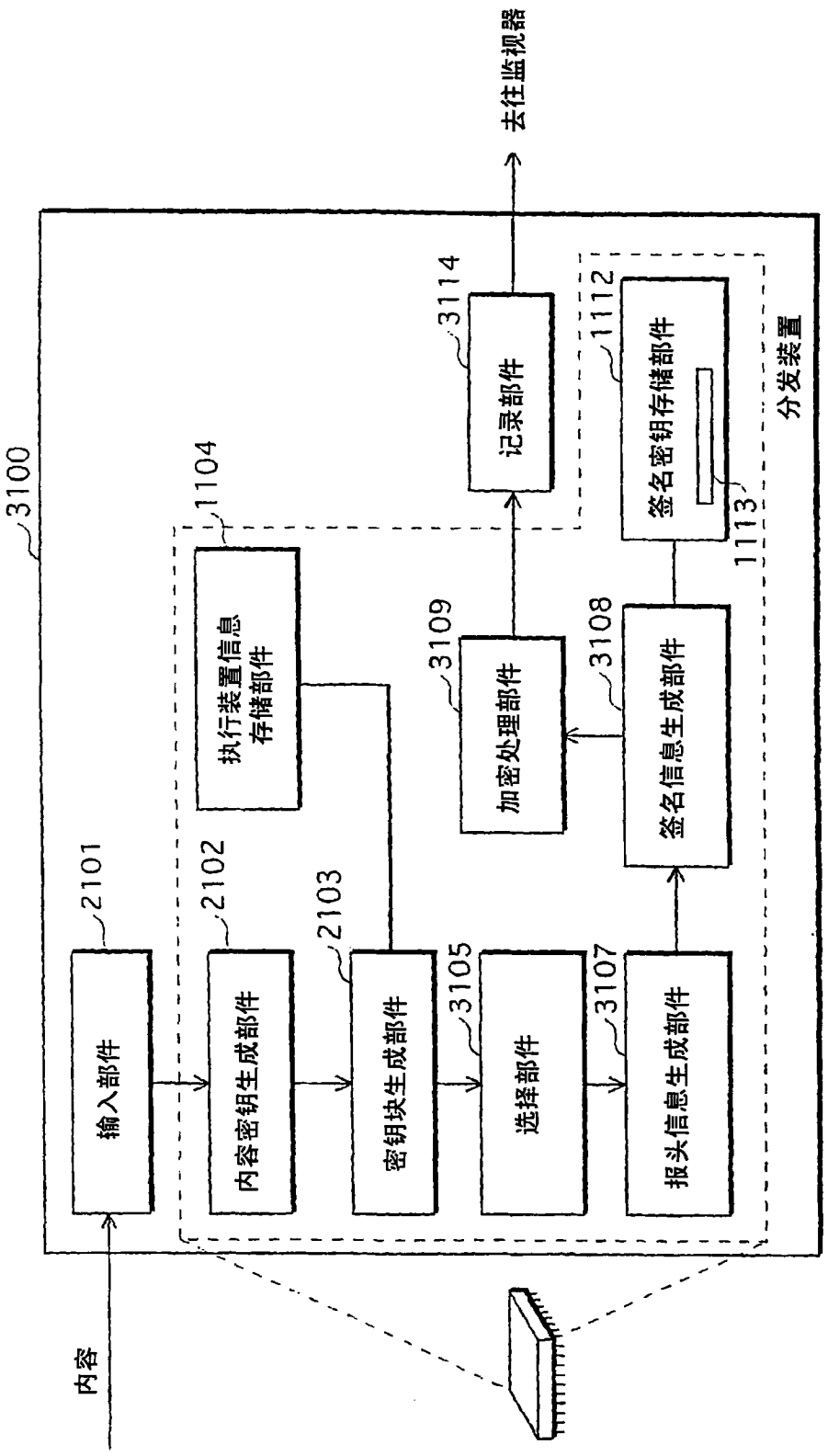

去往监视器
3100
分发装置
3114
记录部件
1112
签名密钥存储部件
1113
1104
执行装置信息存储部件
3109
加密处理部件
3108
签名信息生成部件
2101
输入部件
2102
内容密钥生成部件
2103
密钥块生成部件
3105
选择部件
3107
报头信息生成部件
内容

图37

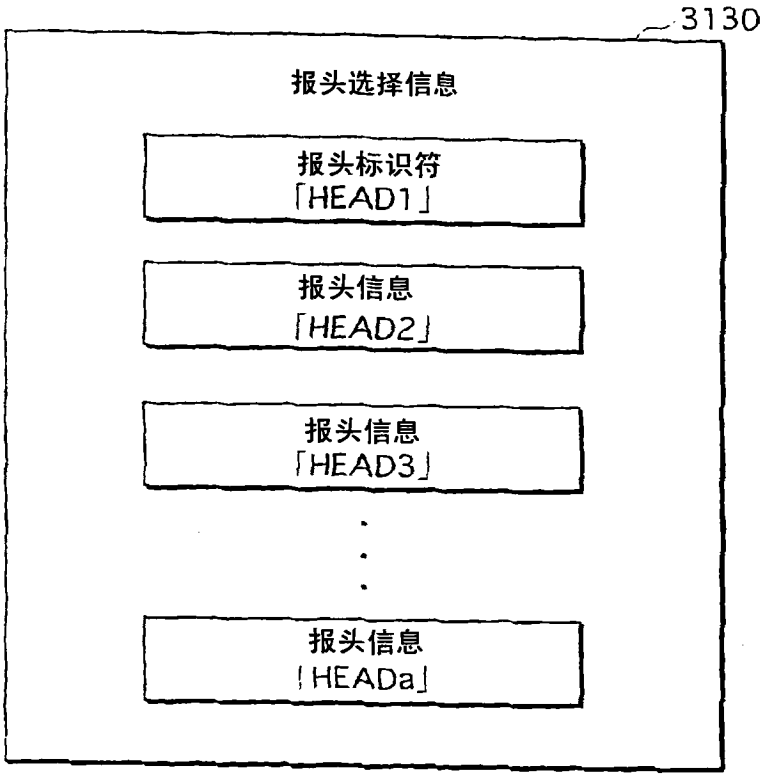


图 38

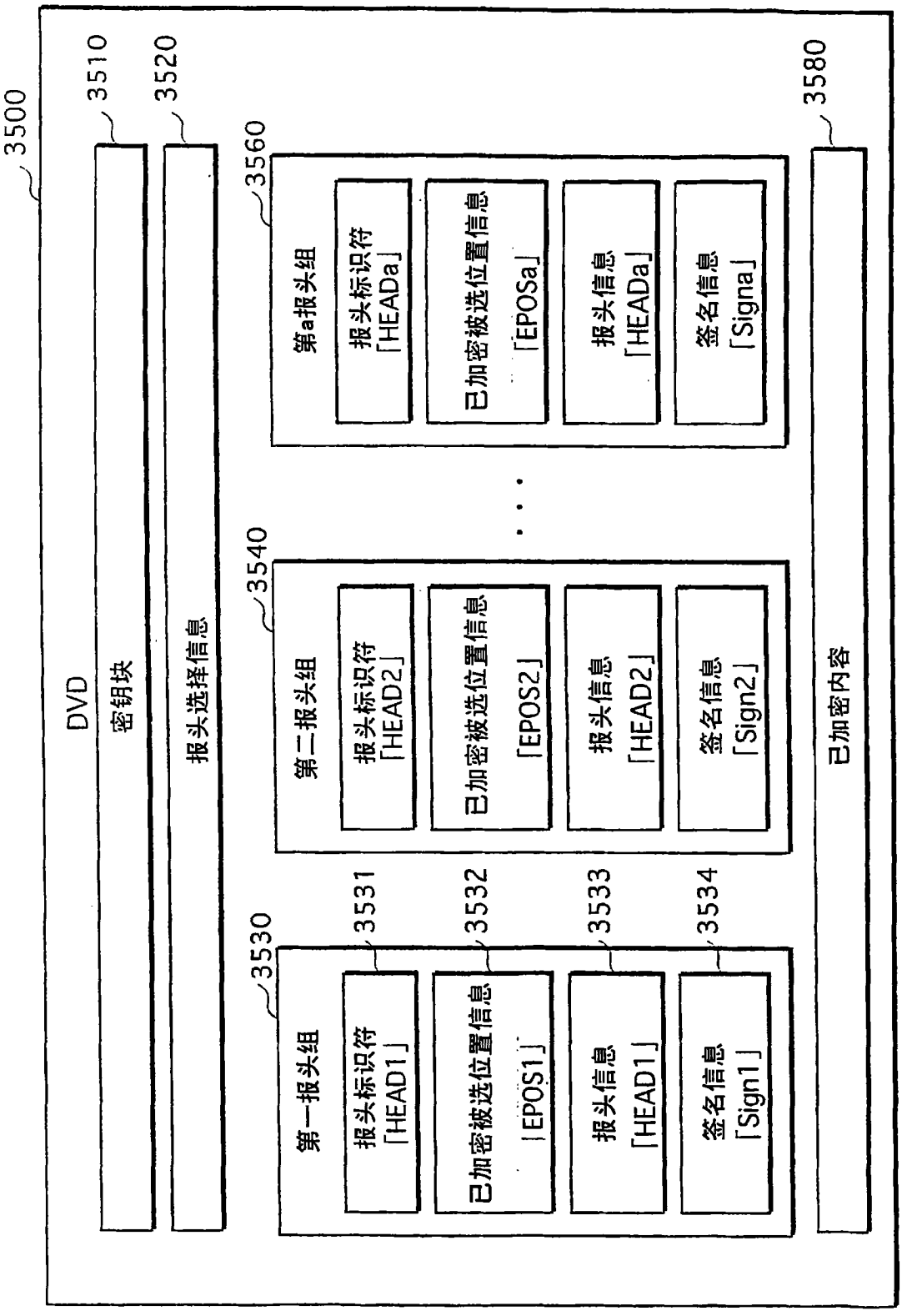

3500
DVD
3510
密钥块
3520
报头选择信息
3530
第一报头组
3531
报头标识符
「HEAD1」
3532
已加密被选位置信息
「EPOS1」
3533
报头信息
「HEAD1」
3534
签名信息
「Sign1」
3540
第二报头组
报头标识符
「HEAD2」
已加密被选位置信息
「EPOS2」
报头信息
「HEAD2」
签名信息
「Sign2」
3560
第a报头组
报头标识符
「HEADa」
已加密被选位置信息
「EPOSa」
报头信息
「HEADa」
签名信息
「Signa」
3580
已加密内容

图39

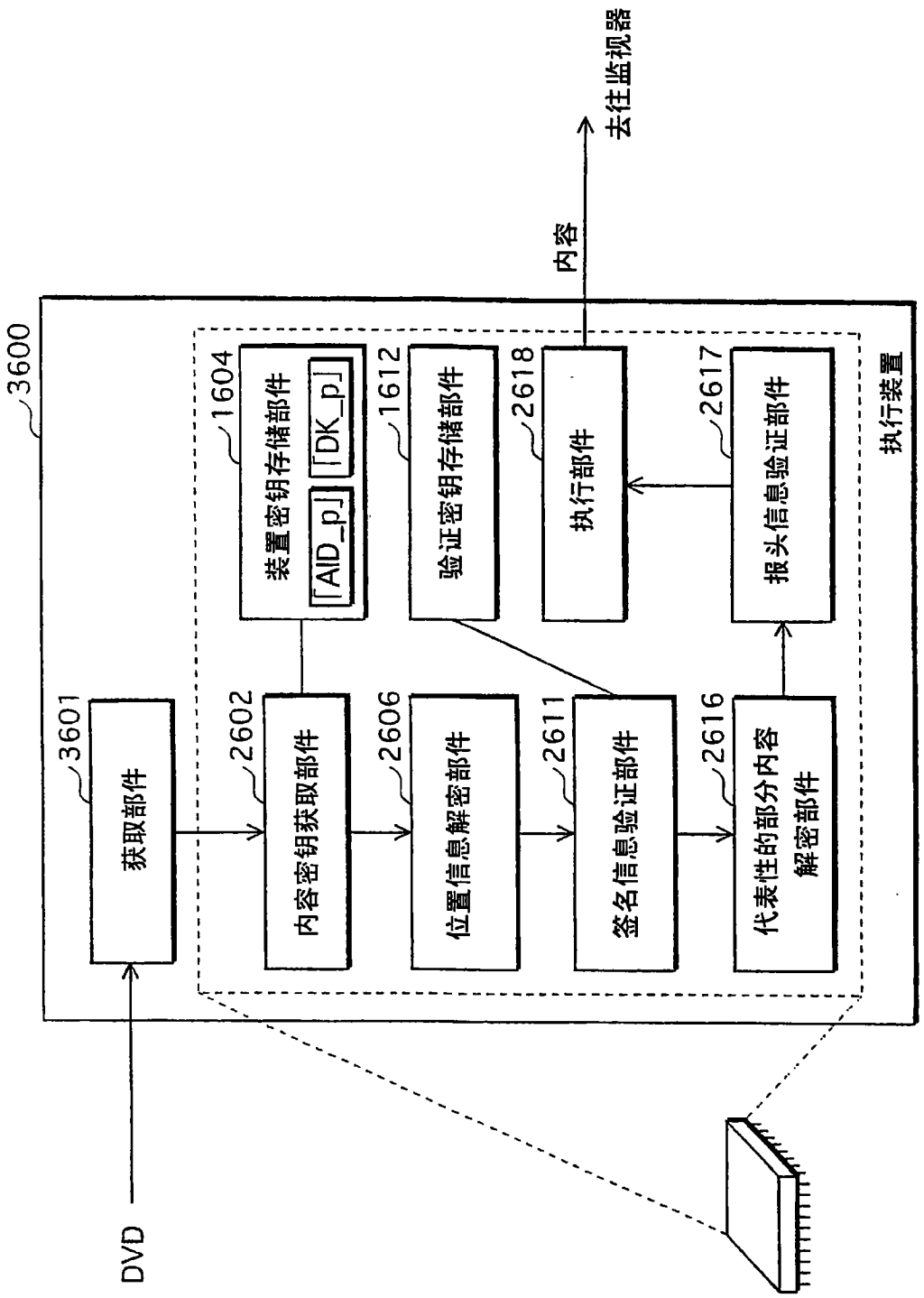

去往监视器
内容
3600
执行装置
1604
装置密钥存储部件
[AID_p]
[DK_p]
1612
验证密钥存储部件
2618
执行部件
2617
报头信息验证部件
3601
获取部件
2602
内容密钥获取部件
2606
位置信息解密部件
2611
签名信息验证部件
2616
代表性的部分内容解密部件
DVD

图40

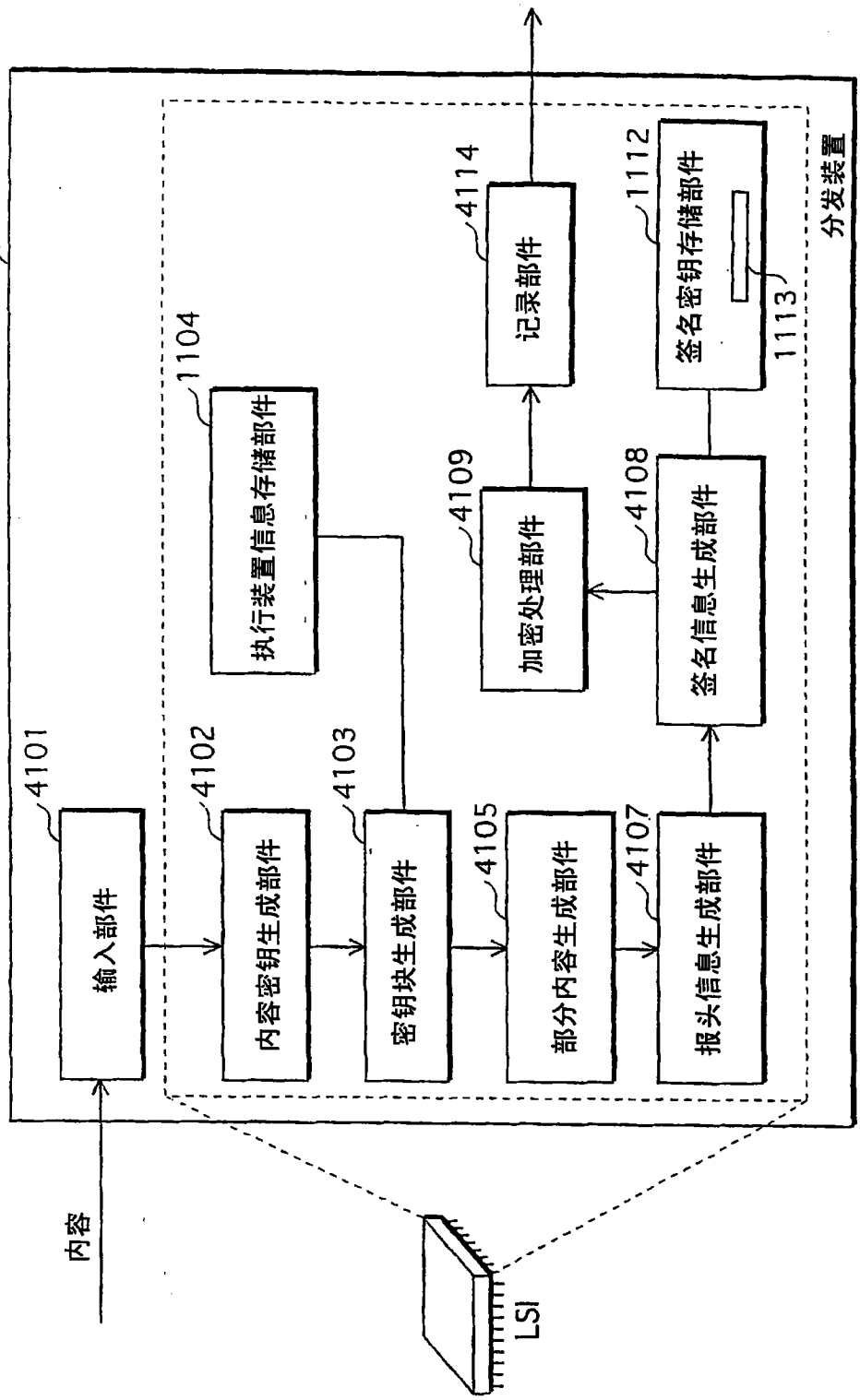

4100
分发装置
4101
输入部件
4102
内容密钥生成部件
4103
密钥块生成部件
4104
执行装置信息存储部件
4105
部分内容生成部件
4107
报头信息生成部件
4108
签名信息生成部件
4109
加密处理部件
4112
签名密钥存储部件
1113
4114
记录部件
内容
LSI

图41

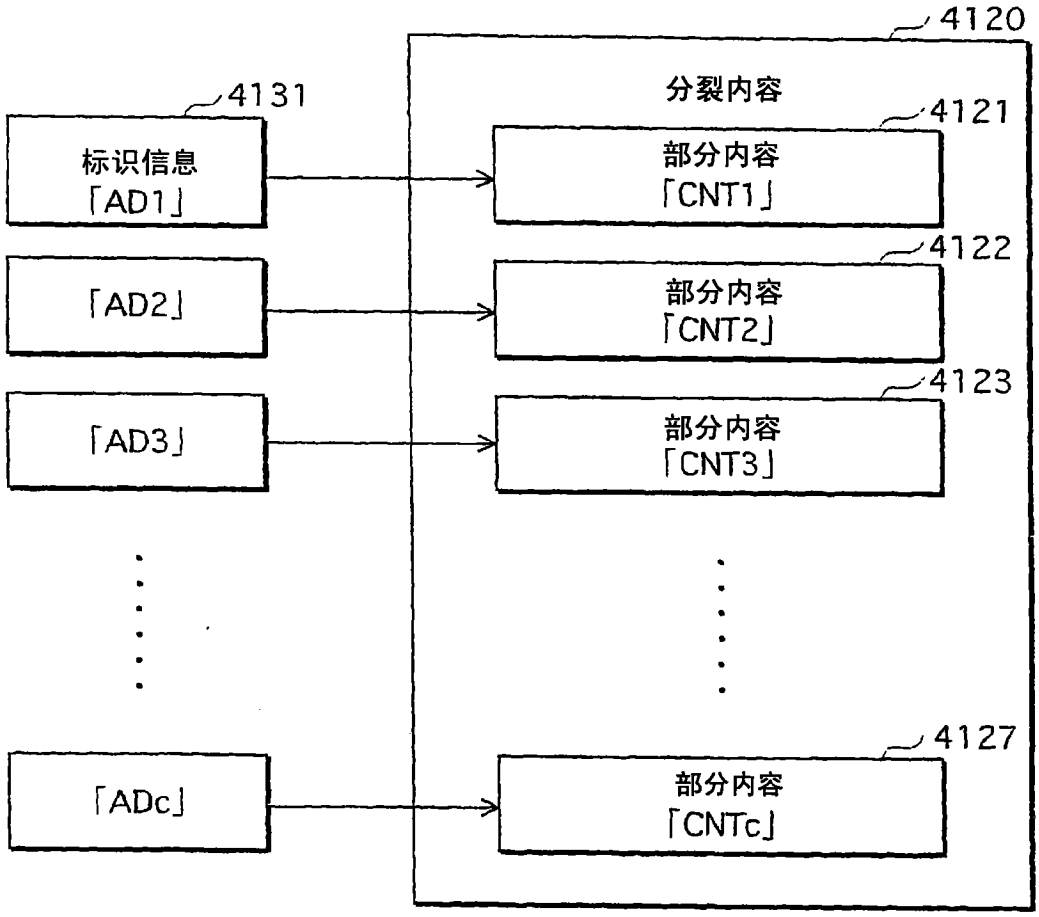

4120
分裂内容
4131
标识信息
「AD1」
4121
部分内容
「CNT1」
「AD2」
4122
部分内容
「CNT2」
「AD3」
4123
部分内容
「CNT3」
「ADc」
4127
部分内容
「CNTc」

图 42

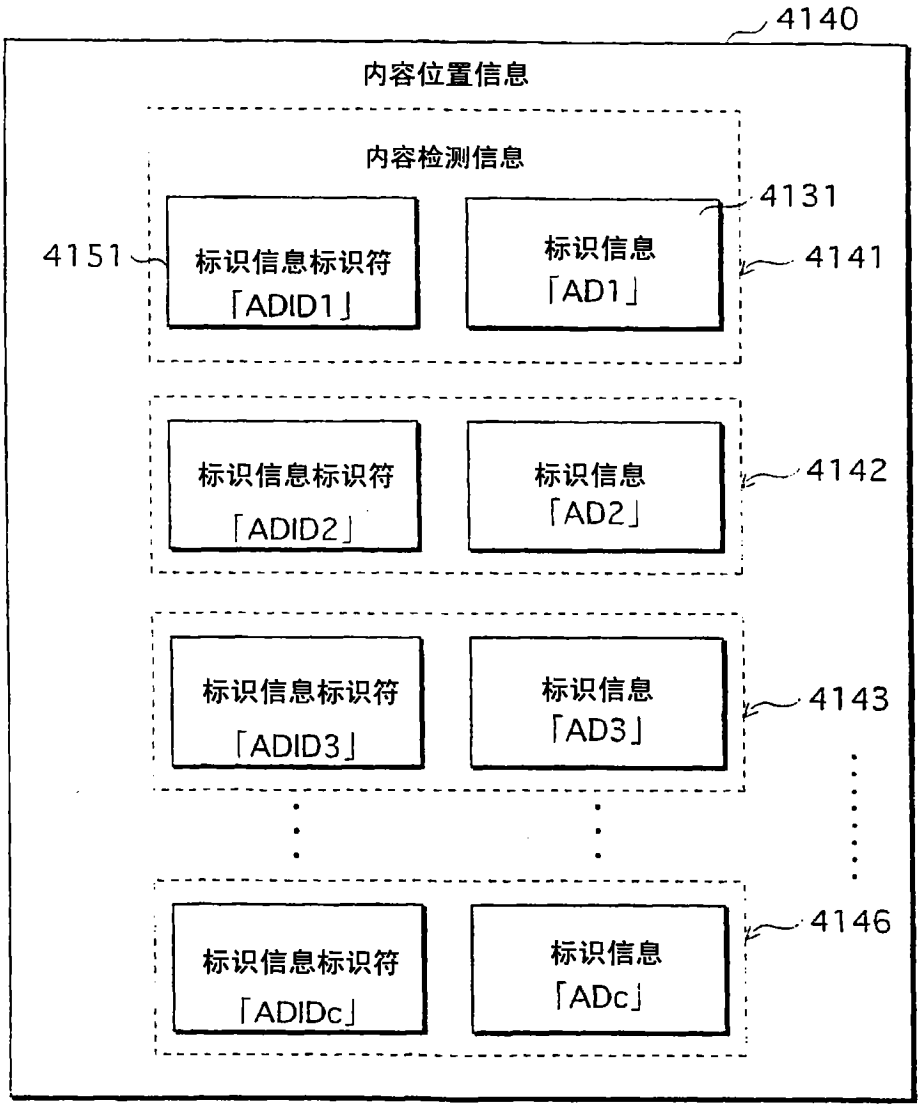

4140
内容位置信息
内容检测信息
4131
4151
标识信息标识符
「ADID1」
标识信息
「AD1」
4141
标识信息标识符
「ADID2」
标识信息
「AD2」
4142
标识信息标识符
「ADID3」
标识信息
「AD3」
4143
标识信息标识符
「ADIDc」
标识信息
「ADc」
4146

图 43

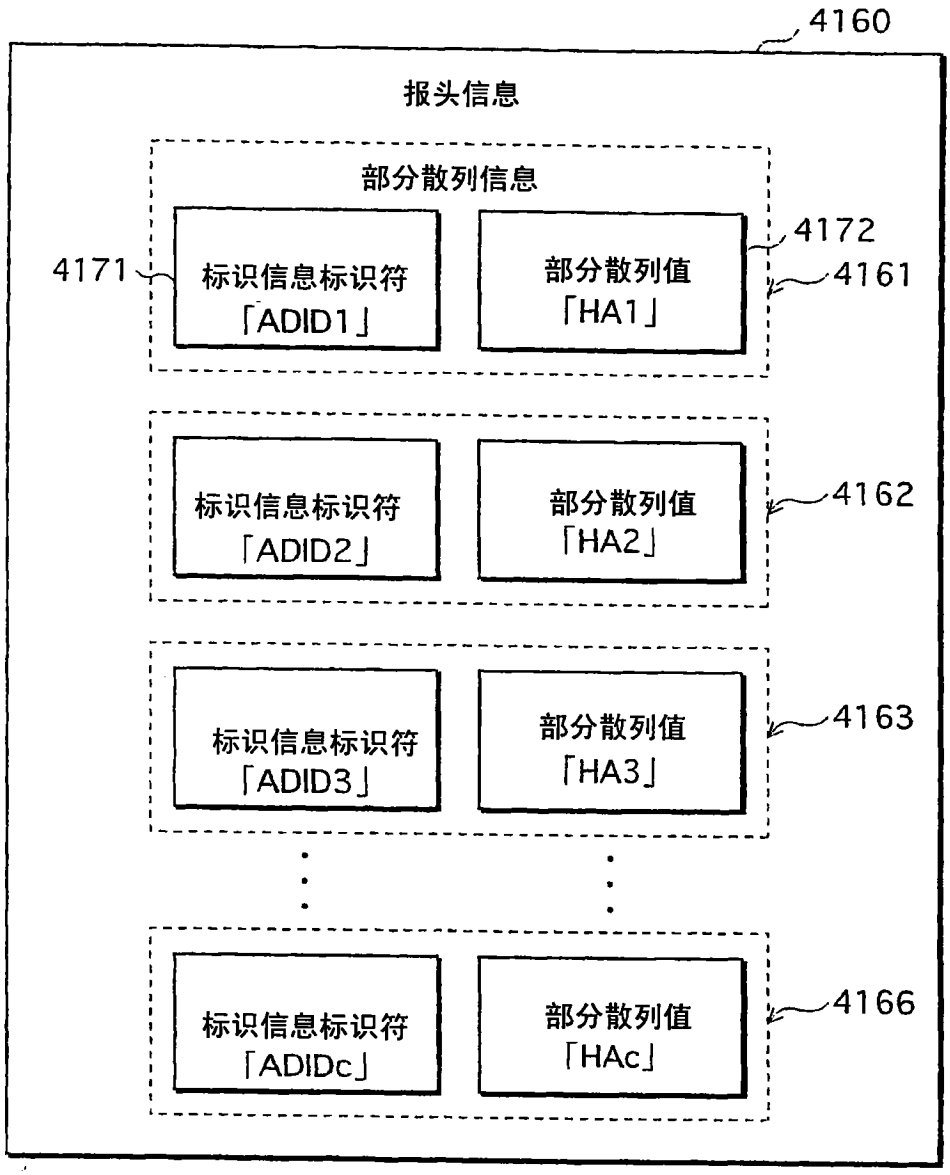

4160
报头信息
部分散列信息
4171
标识信息标识符
「ADID1」
部分散列值
「HA1」
4172
4161
标识信息标识符
「ADID2」
部分散列值
「HA2」
4162
标识信息标识符
「ADID3」
部分散列值
「HA3」
4163
标识信息标识符
「ADIDc」
部分散列值
「HAc」
4166

图 44

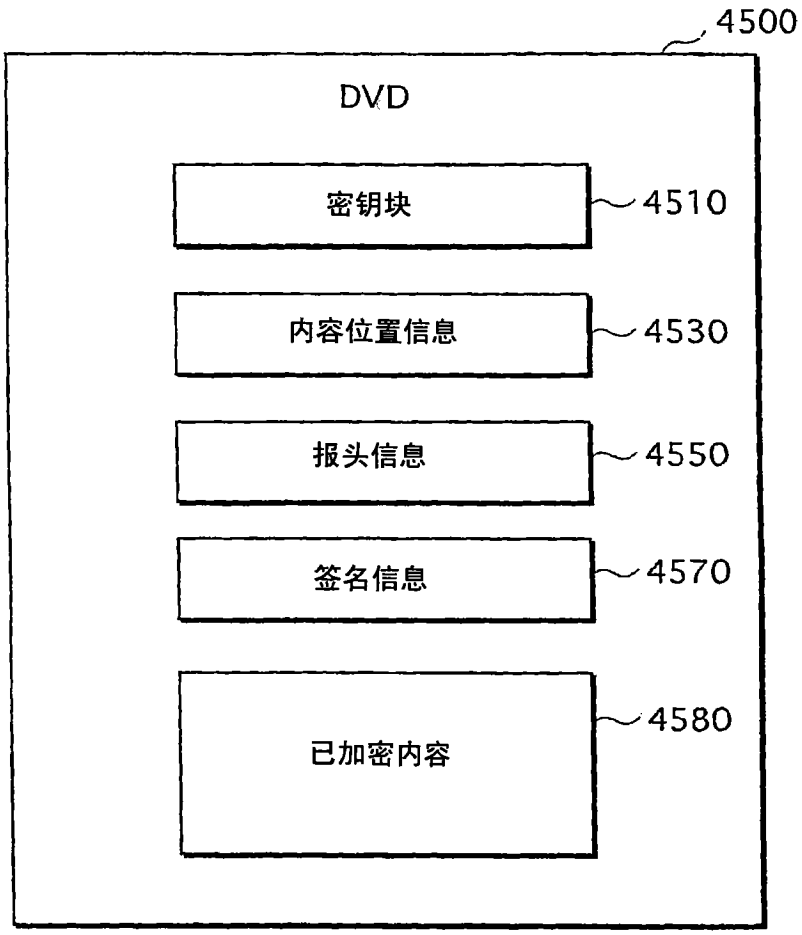


图 45

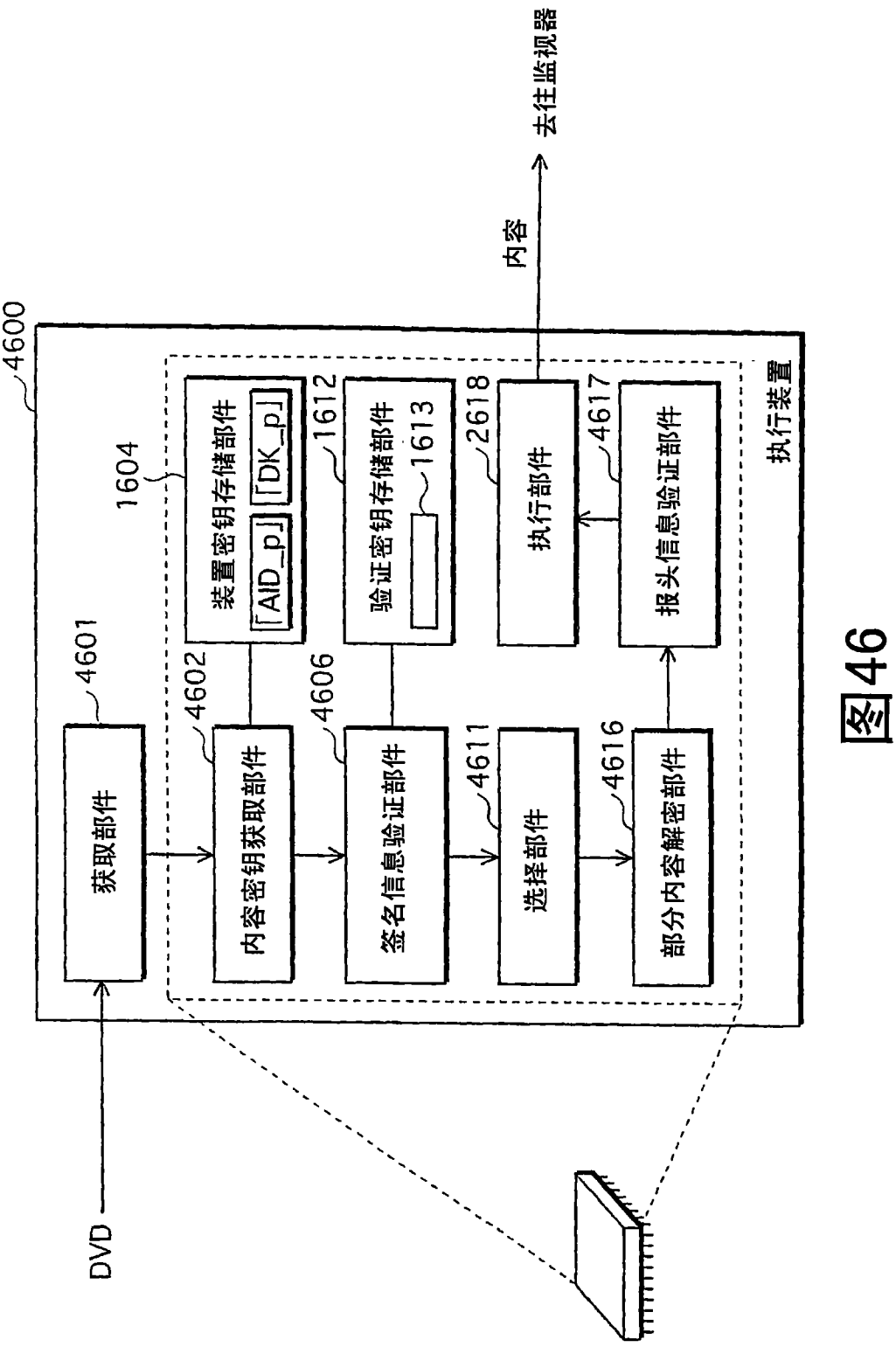

4600
执行装置
1604
装置密钥存储部件
「AID_p」
「DK_p」
1612
验证密钥存储部件
1613
2618
执行部件
4617
报头信息验证部件
4601
获取部件
4602
内容密钥获取部件
4606
签名信息验证部件
4611
选择部件
4616
部分内容解密部件
内容
去往监视器
DVD

图46

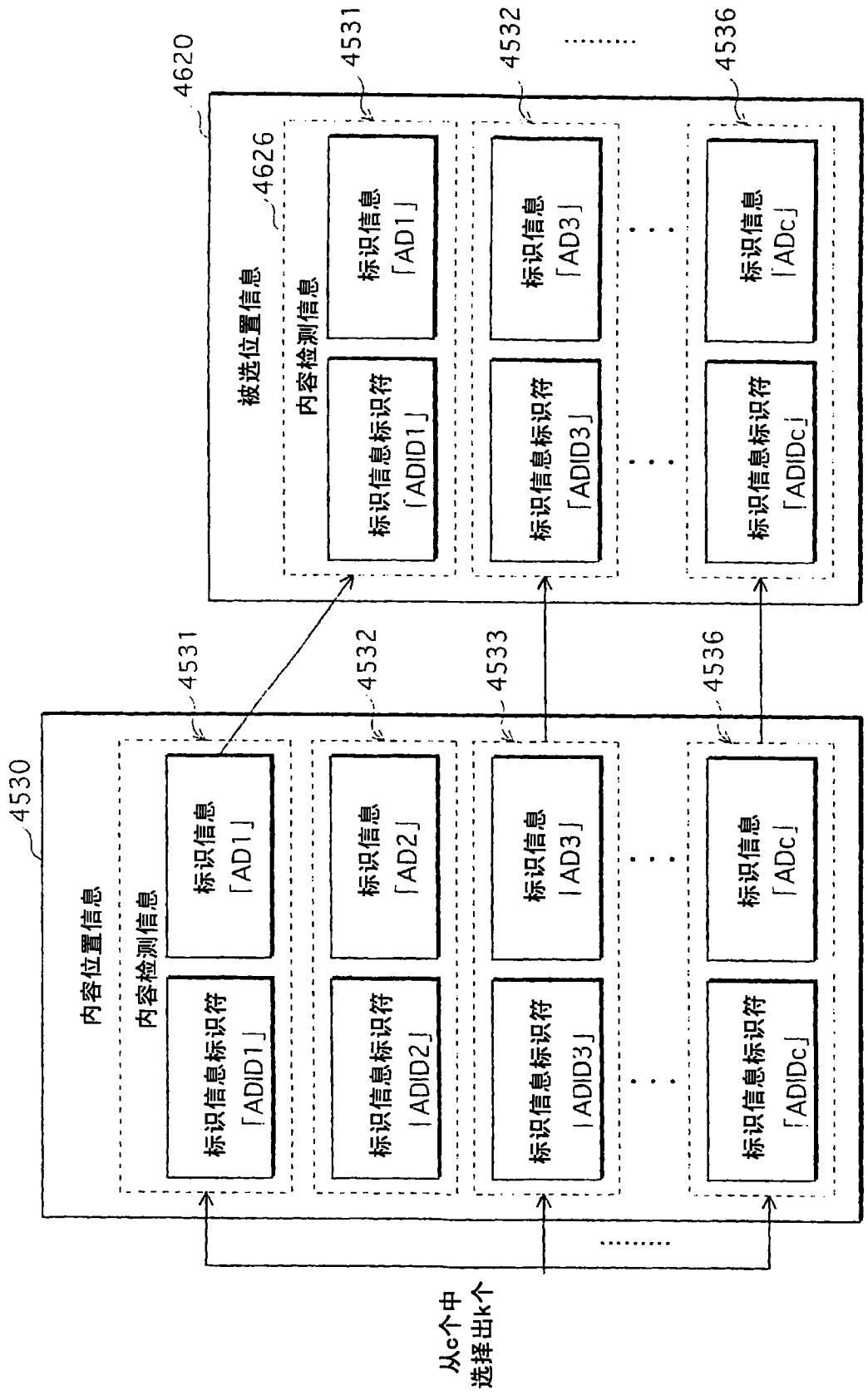

4620
4531
4532
4536
被选位置信息
4626
内容检测信息
标识信息「AD1」
标识信息「AD3」
标识信息「ADc」
标识信息标识符「ADID1」
标识信息标识符「ADID3」
标识信息标识符「ADIDc」
4530
内容位置信息
内容检测信息
4531
4532
4533
4536
标识信息「AD1」
标识信息「AD2」
标识信息「AD3」
标识信息「ADc」
标识信息标识符「ADID1」
标识信息标识符「ADID2」
标识信息标识符「ADID3」
标识信息标识符「ADIDc」
从c个中选择出k个

图47

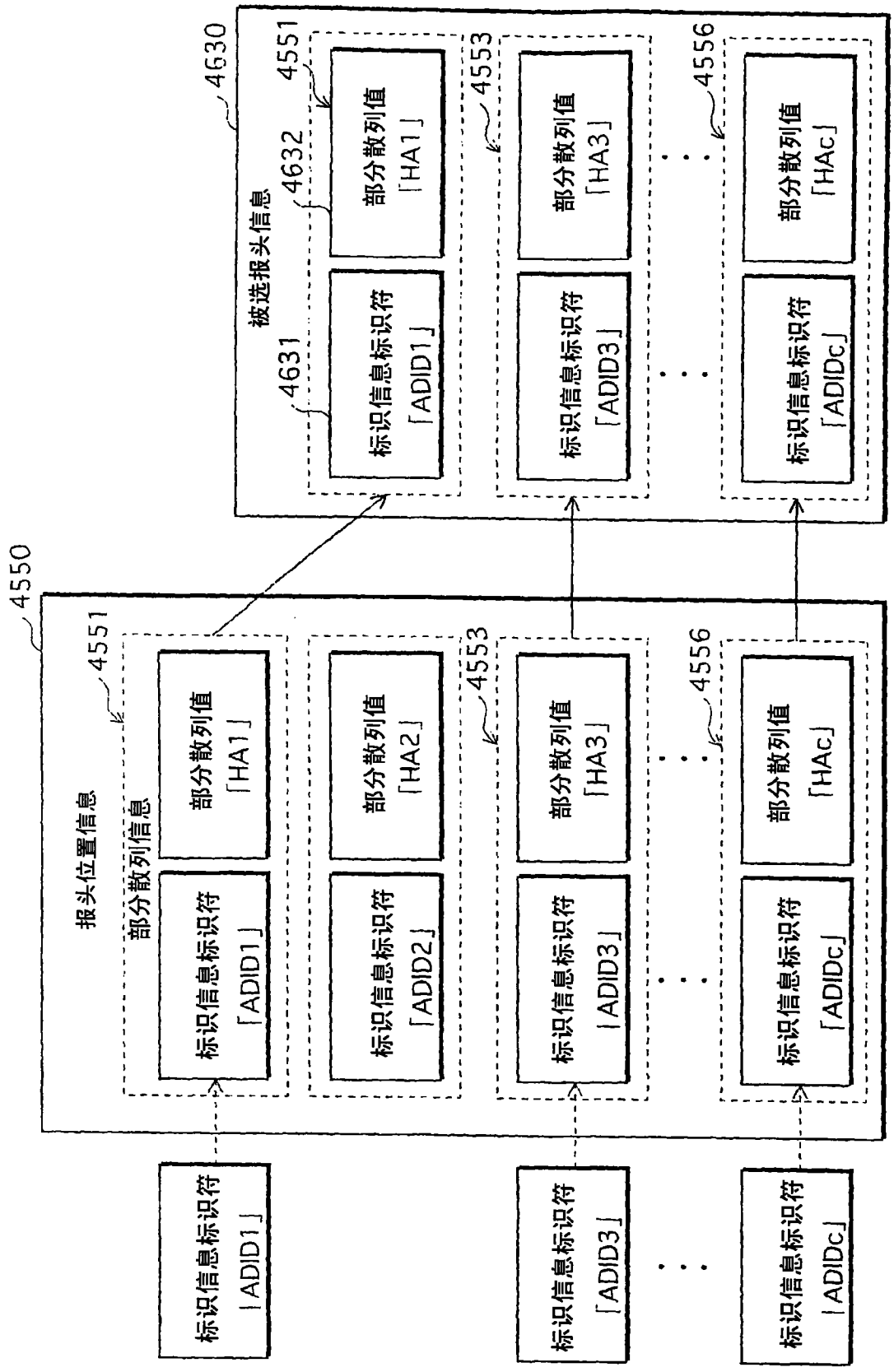

4550
报头位置信息
4551
部分散列信息
标识信息标识符「ADID1」
部分散列值「HA1」
标识信息标识符「ADID2」
部分散列值「HA2」
4553
标识信息标识符「ADID3」
部分散列值「HA3」
4556
标识信息标识符「ADIDc」
部分散列值「HAc」
标识信息标识符「ADID1」
标识信息标识符「ADID3」
标识信息标识符「ADIDc」
4630
被选报头信息
4631
4632
4551
4553
4556
标识信息标识符「ADID1」
部分散列值「HA1」
标识信息标识符「ADID3」
部分散列值「HA3」
标识信息标识符「ADIDc」
部分散列值「HAc」

图48

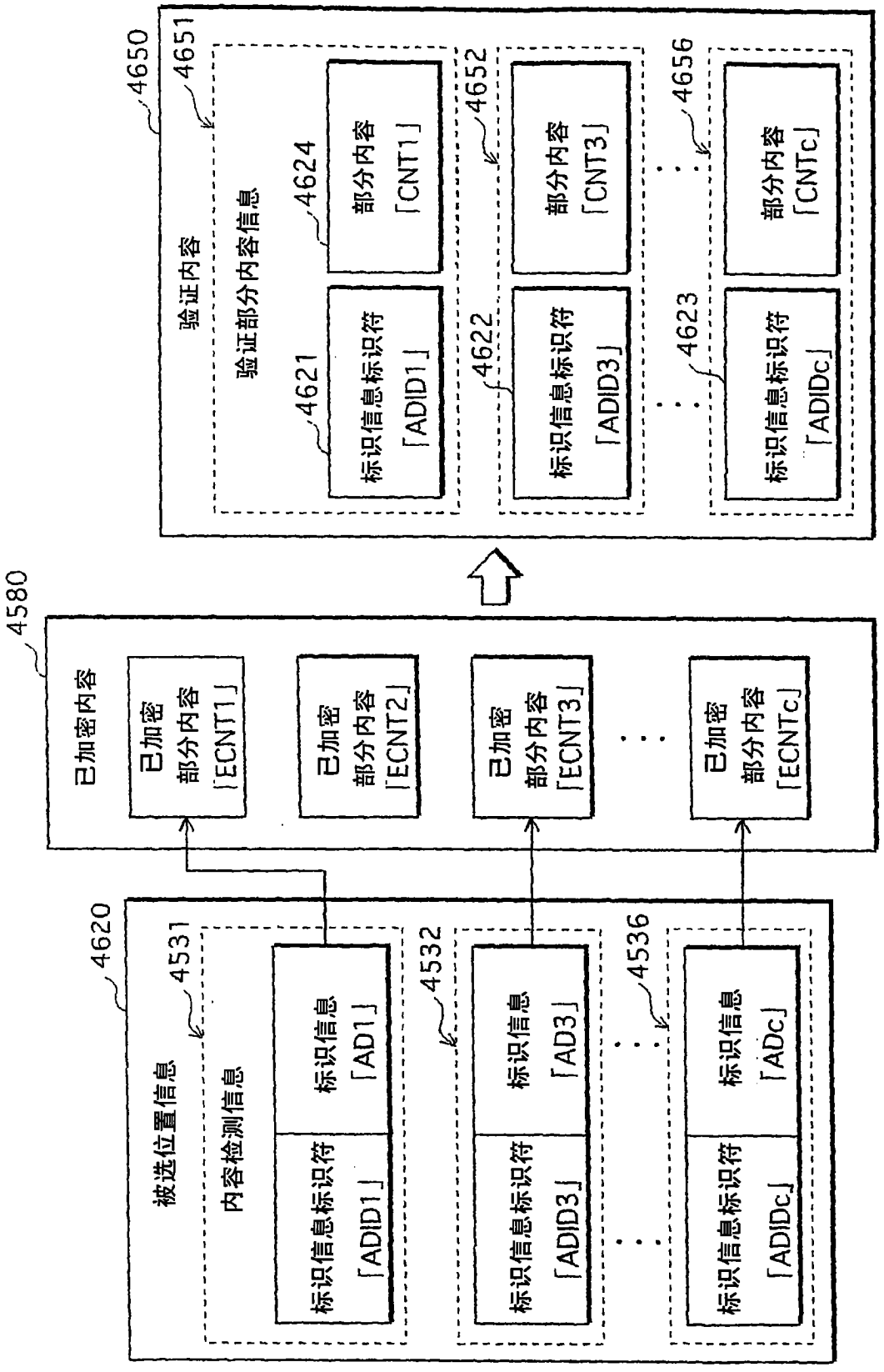

4650
4651
验证内容
验证部分内容信息
4621
标识信息标识符
「ADID1」
4624
部分内容
「CNT1」
4622
4652
标识信息标识符
「ADID3」
部分内容
「CNT3」
4623
4656
标识信息标识符
「ADIDc」
部分内容
「CNTc」
4580
已加密内容
已加密
部分内容
「ECNT1」
已加密
部分内容
「ECNT2」
已加密
部分内容
「ECNT3」
已加密
部分内容
「ECNTc」
4620
被选位置信息
4531
内容检测信息
标识信息
「AD1」
标识信息标识符
「ADID1」
4532
标识信息
「AD3」
标识信息标识符
「ADID3」
4536
标识信息
「ADc」
标识信息标识符
「ADIDc」

图49

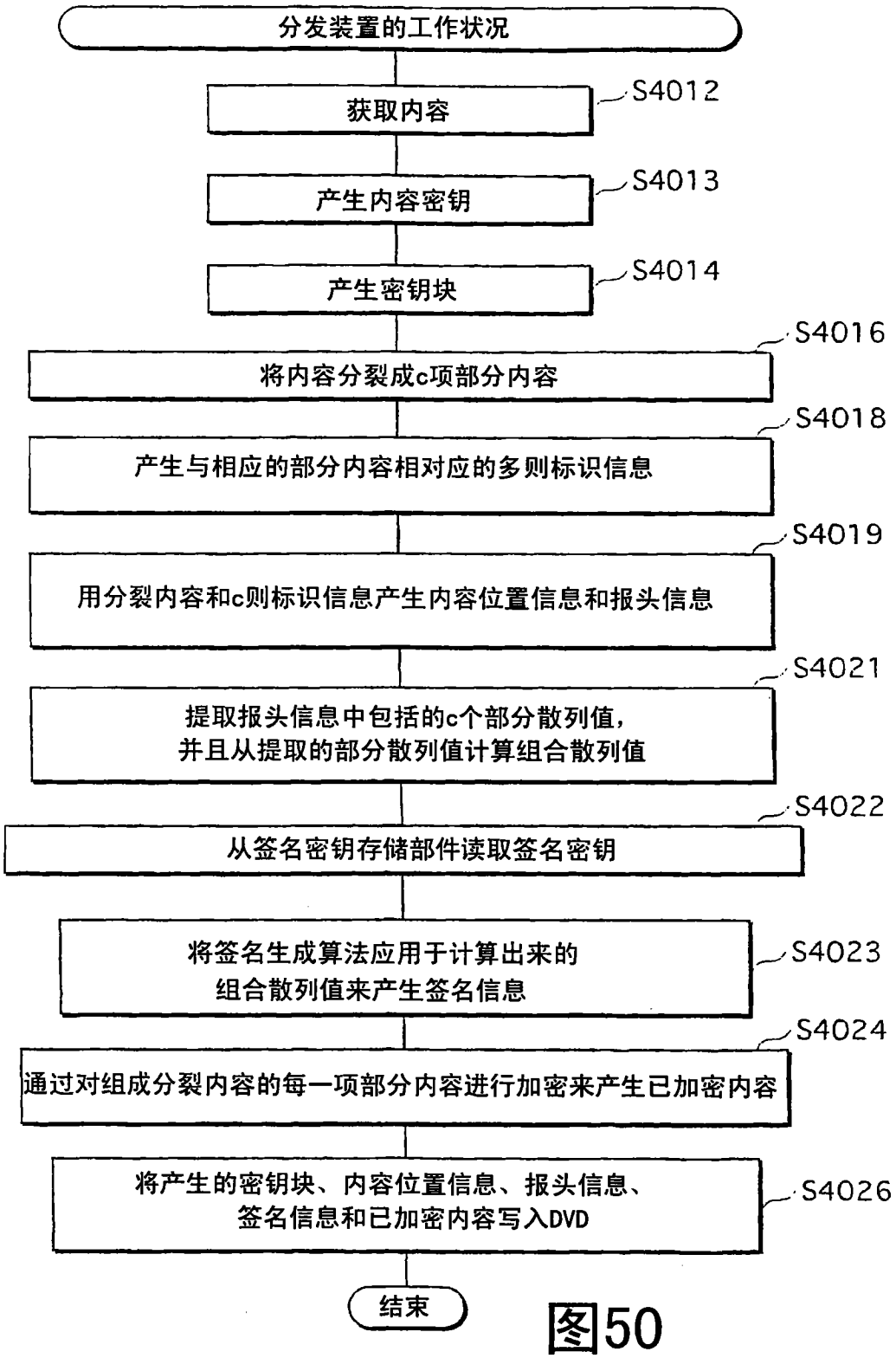

分发装置的工作状况
获取内容
S4012
产生内容密钥
S4013
产生密钥块
S4014
S4016
将内容分裂成c项部分内容
S4018
产生与相应的部分内容相对应的多则标识信息
S4019
用分裂内容和c则标识信息产生内容位置信息和报头信息
S4021
提取报头信息中包括的c个部分散列值，
并且从提取的部分散列值计算组合散列值
S4022
从签名密钥存储部件读取签名密钥
将签名生成算法应用于计算出来的
组合散列值来产生签名信息
S4023
S4024
通过对组成分裂内容的每一项部分内容进行加密来产生已加密内容
将产生的密钥块、内容位置信息、报头信息、
签名信息和已加密内容写入DVD
S4026
结束

图50

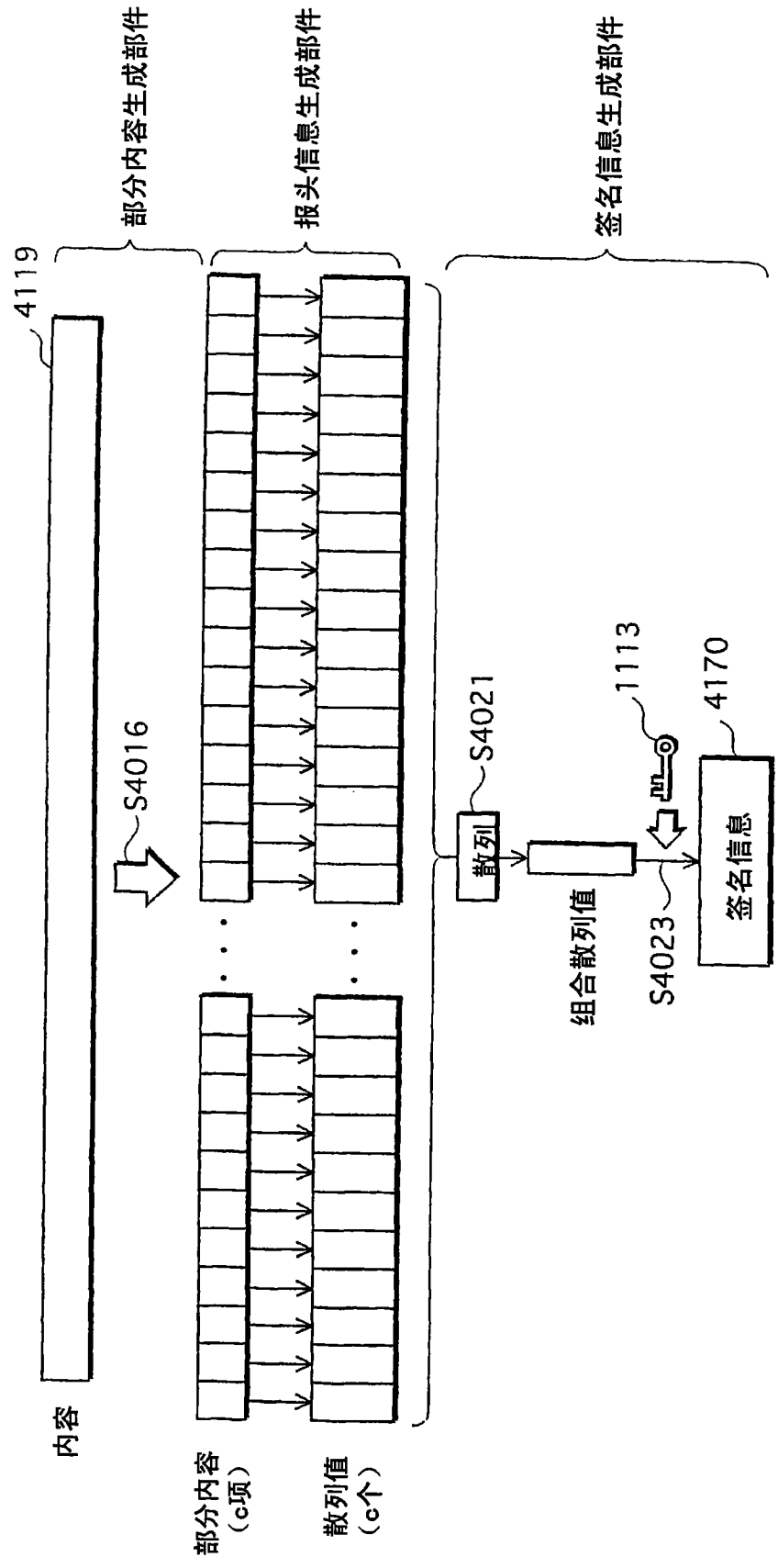

部分内容生成部件
报头信息生成部件
签名信息生成部件
4119
S4016
S4021
1113
4170
散列
组合散列值
S4023
签名信息
内容
部分内容
（c项）
散列值
（c个）

图51

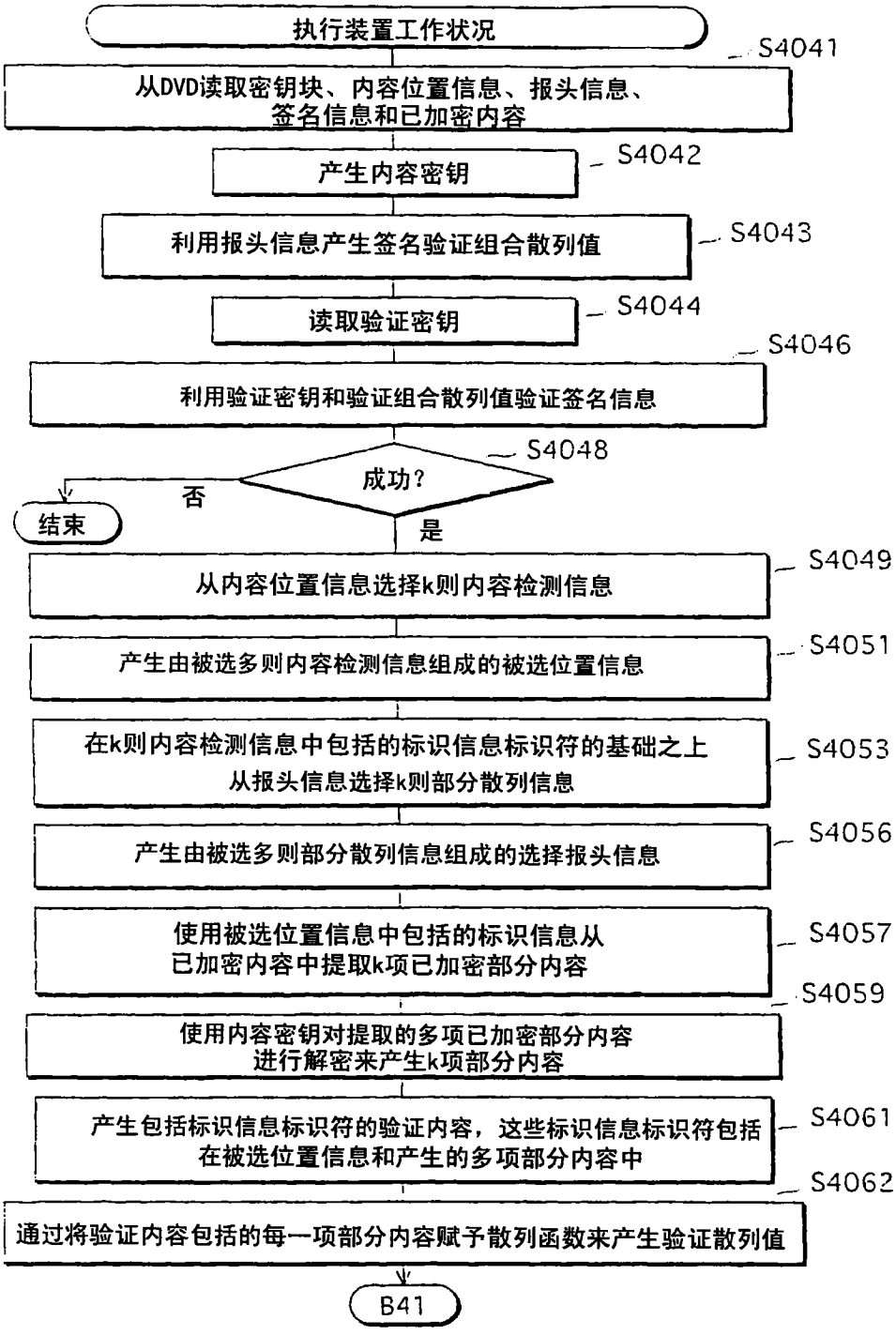

执行装置工作状况
S4041
从DVD读取密钥块、内容位置信息、报头信息、签名信息和已加密内容
S4042
产生内容密钥
S4043
利用报头信息产生签名验证组合散列值
S4044
读取验证密钥
S4046
利用验证密钥和验证组合散列值验证签名信息
S4048
成功?
否
结束
是
S4049
从内容位置信息选择k则内容检测信息
S4051
产生由被选多则内容检测信息组成的被选位置信息
S4053
在k则内容检测信息中包括的标识信息标识符的基础之上
从报头信息选择k则部分散列信息
S4056
产生由被选多则部分散列信息组成的选择报头信息
S4057
使用被选位置信息中包括的标识信息从
已加密内容中提取k项已加密部分内容
S4059
使用内容密钥对提取的多项已加密部分内容
进行解密来产生k项部分内容
S4061
产生包括标识信息标识符的验证内容，这些标识信息标识符包括
在被选位置信息和产生的多项部分内容中
S4062
通过将验证内容包括的每一项部分内容赋予散列函数来产生验证散列值
B41

图 52

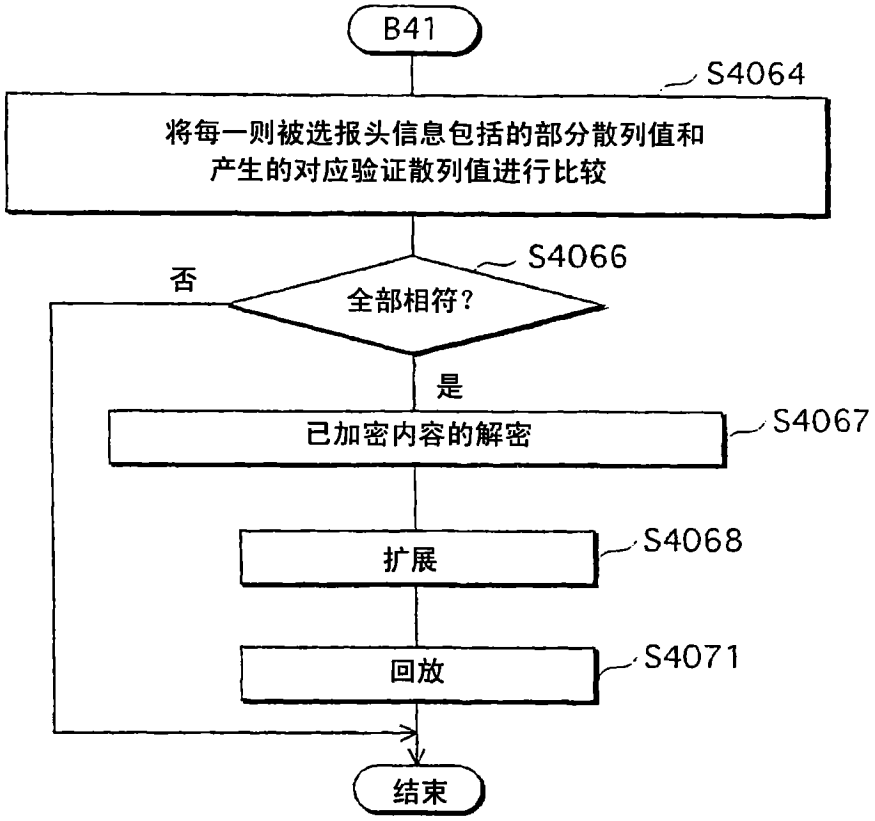

B41
S4064
将每一则被选报头信息包括的部分散列值和
产生的对应验证散列值进行比较
S4066
否
全部相符?
是
已加密内容的解密
S4067
扩展
S4068
回放
S4071
结束

图 53

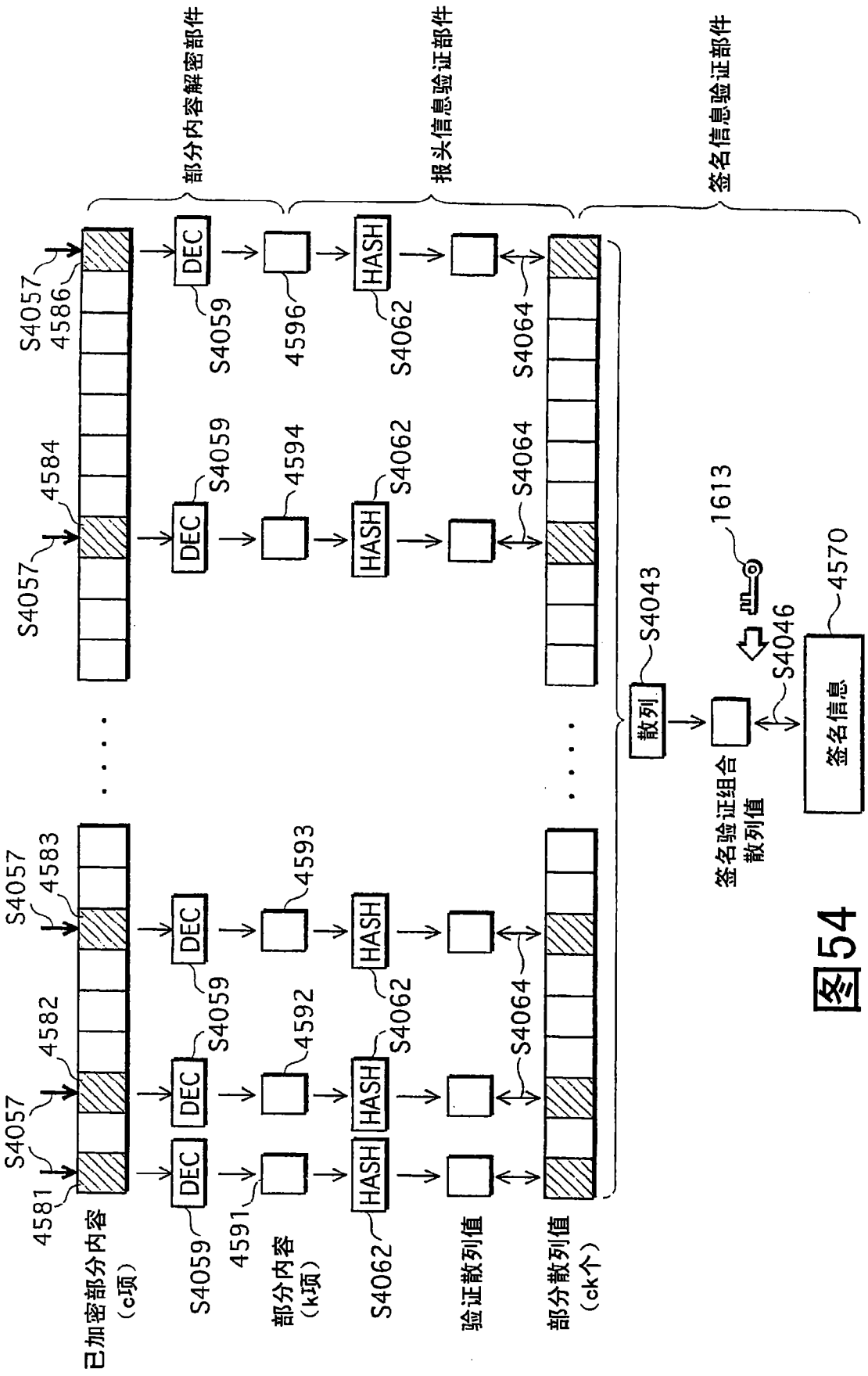

部分内容解密部件
报头信息验证部件
签名信息验证部件
已加密部分内容
（c项）
部分内容
（k项）
验证散列值
部分散列值
（ck个）
签名验证组合
散列值
签名信息
DEC
HASH
散列
S4057
S4059
S4062
S4064
S4043
S4046
4581
4582
4583
4584
4586
4591
4592
4593
4594
4596
1613
4570

图54

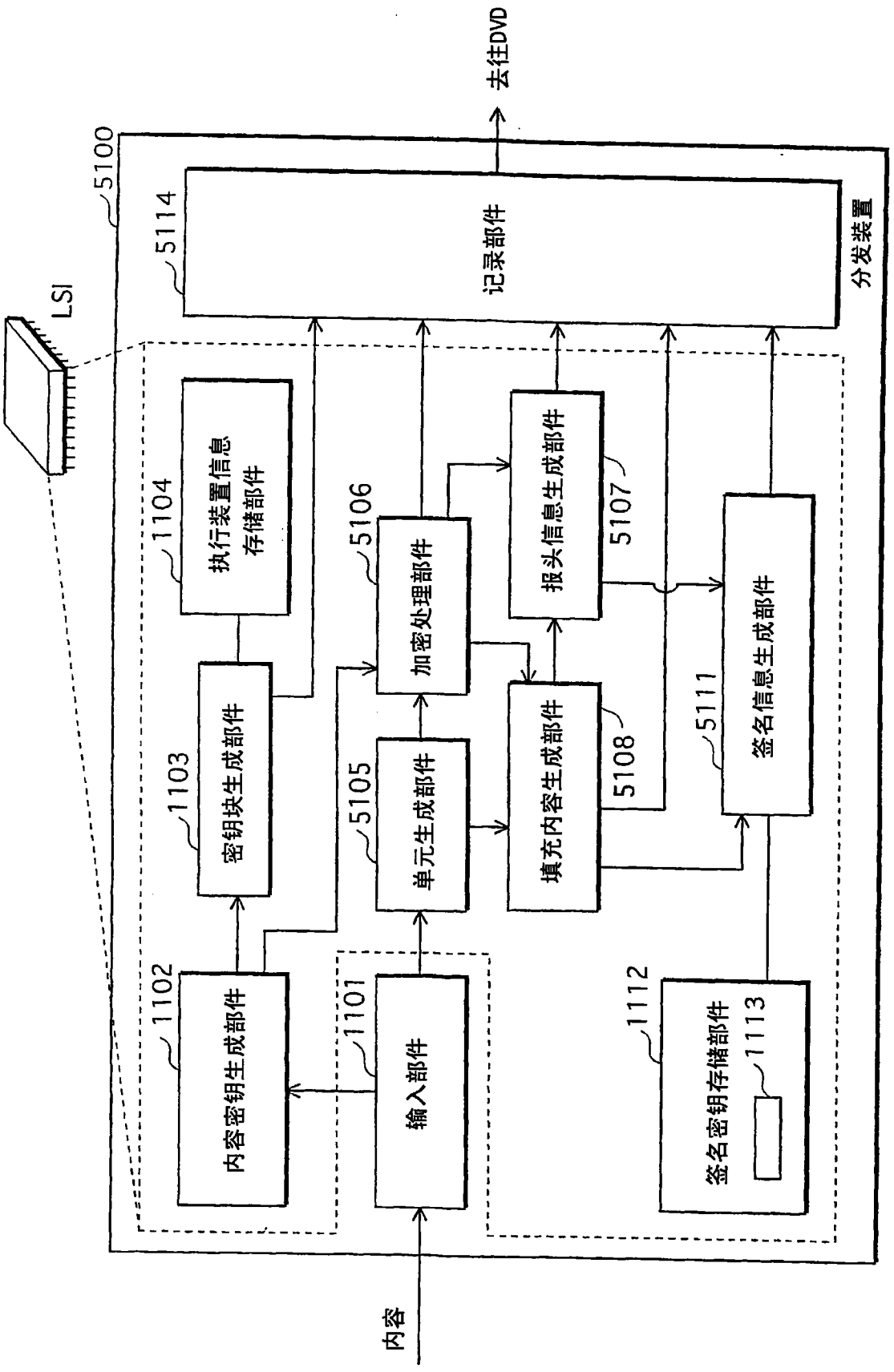

去往DVD
5100
5114
记录部件
分发装置
LSI
1104
执行装置信息存储部件
5106
加密处理部件
报头信息生成部件
5107
1103
密钥块生成部件
5105
单元生成部件
填充内容生成部件
5108
5111
签名信息生成部件
1102
内容密钥生成部件
1101
输入部件
1112
签名密钥存储部件
1113
内容

图55

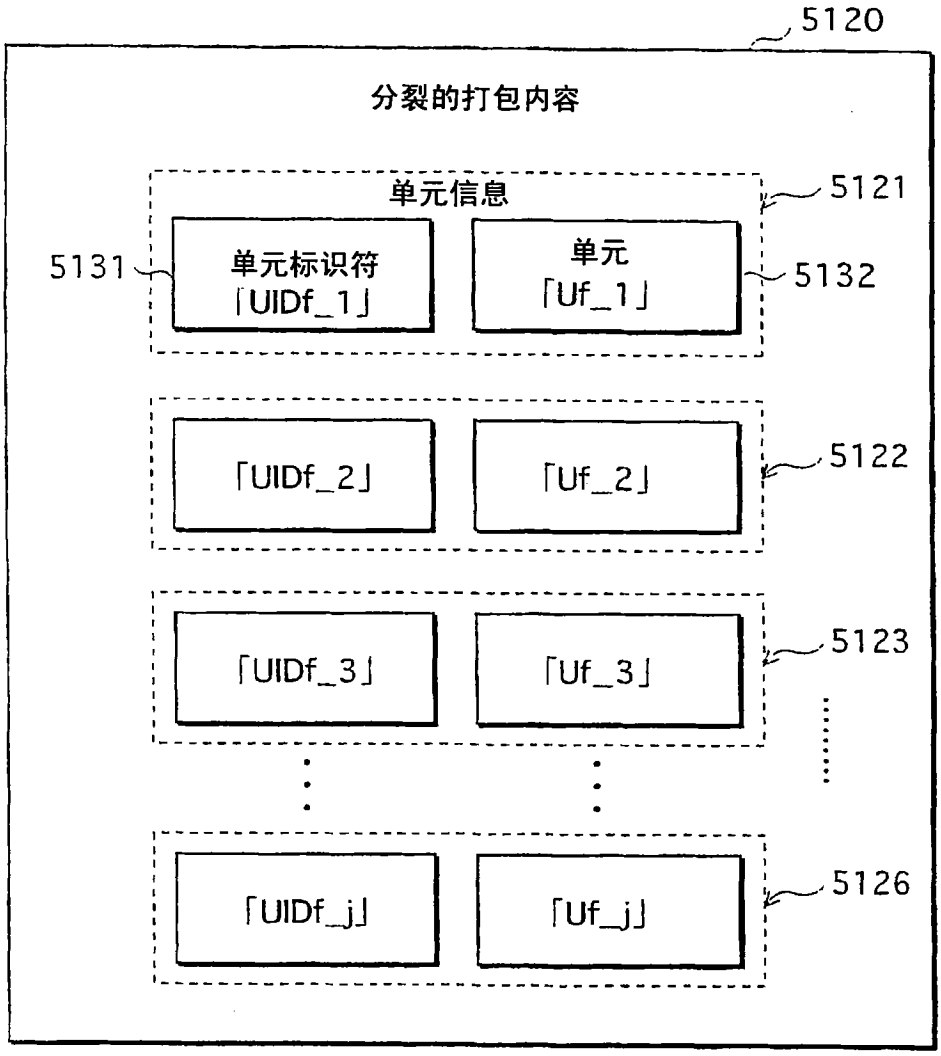

5120
分裂的打包内容
单元信息
5121
5131
单元标识符
「UIDf_1」
单元
「Uf_1」
5132
「UIDf_2」
「Uf_2」
5122
「UIDf_3」
「Uf_3」
5123
「UIDf_j」
「Uf_j」
5126

图 56

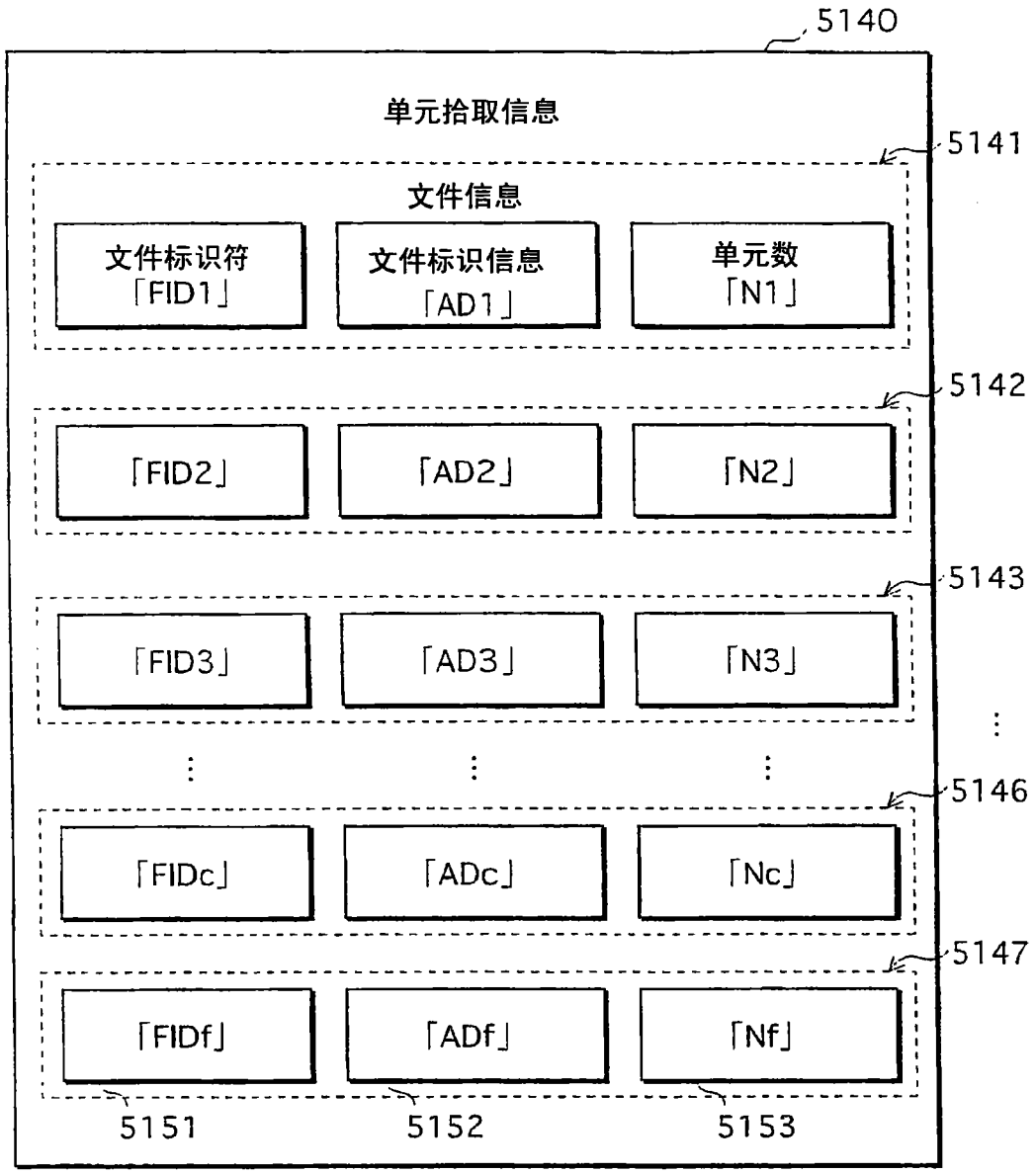

5140
单元拾取信息
5141
文件信息
文件标识符
「FID1」
文件标识信息
「AD1」
单元数
「N1」
5142
「FID2」
「AD2」
「N2」
5143
「FID3」
「AD3」
「N3」
5146
「FIDc」
「ADc」
「Nc」
5147
「FIDf」
「ADf」
「Nf」
5151
5152
5153

图 57

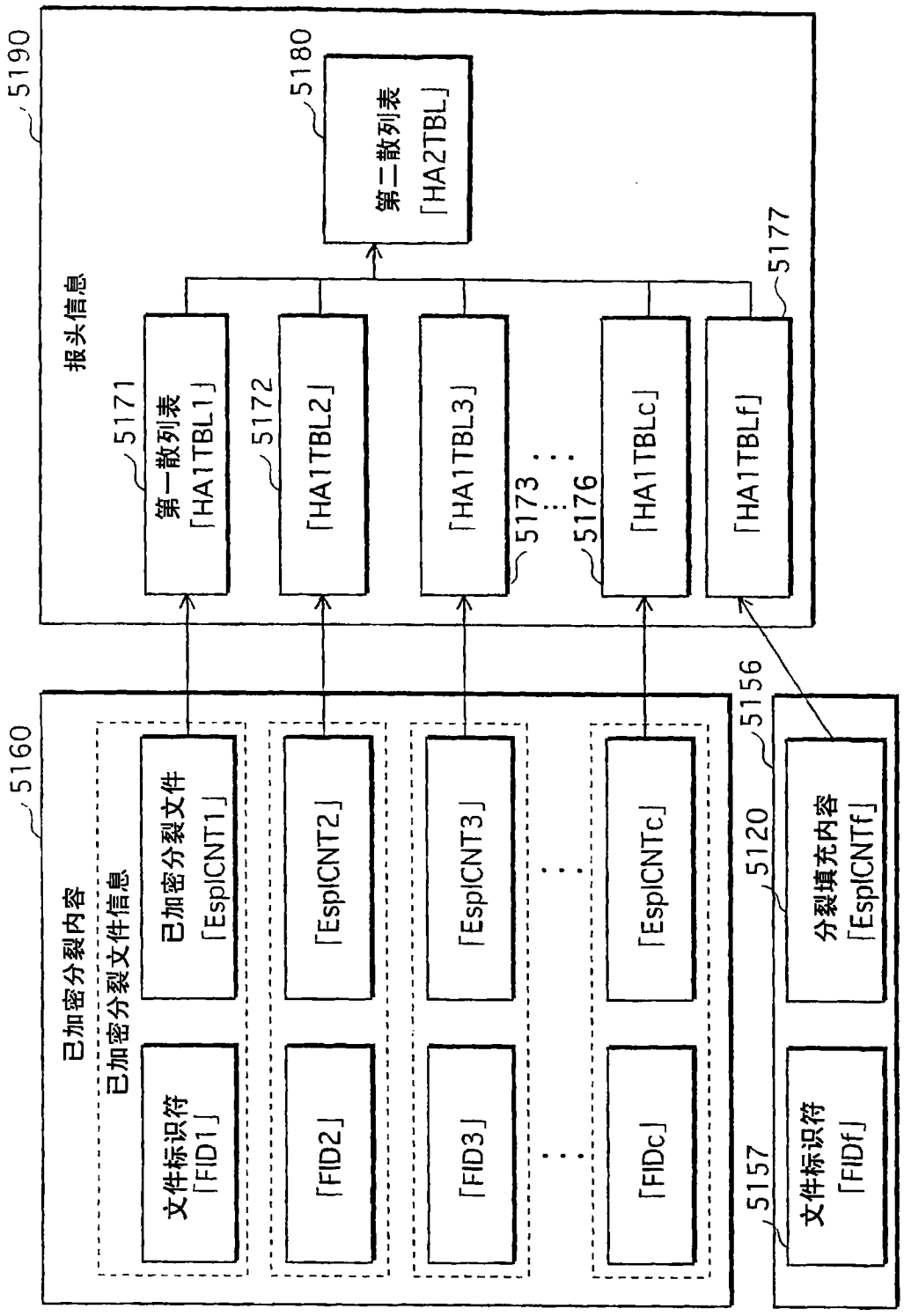

5190
报头信息
5180
第二散列表
「HA2TBL」
5171
第一散列表
「HA1TBL1」
5172
「HA1TBL2」
「HA1TBL3」
5173
5176
「HA1TBLc」
「HA1TBLf」
5177
5160
已加密分裂内容
已加密分裂文件信息
文件标识符
「FID1」
已加密分裂文件
「EsplCNT1」
「FID2」
「EsplCNT2」
「FID3」
「EsplCNT3」
「FIDc」
「EsplCNTc」
5156
5120
分裂填充内容
「EsplCNTf」
5157
文件标识符
「FIDf」

图58

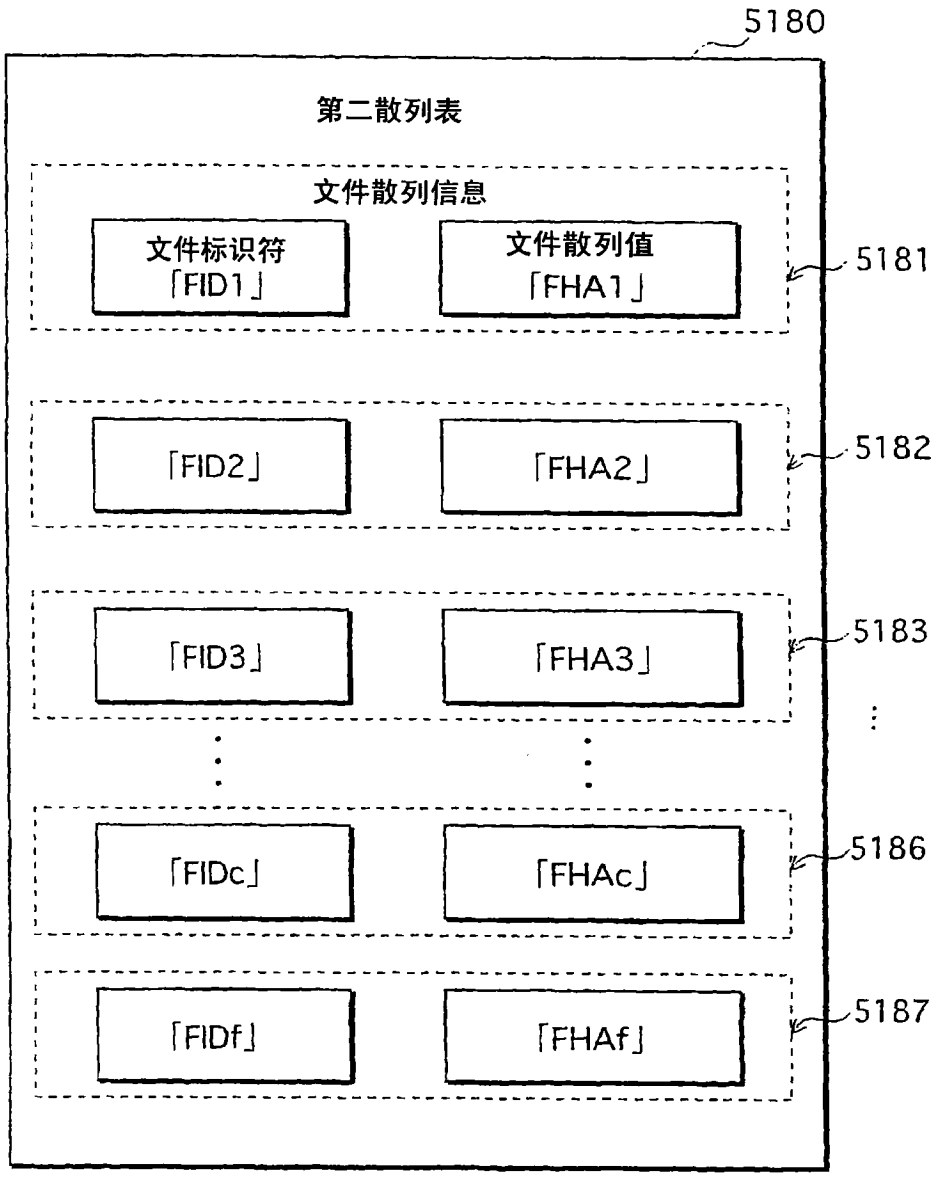

5180
第二散列表
文件散列信息
文件标识符
「FID1」
文件散列值
「FHA1」
5181
「FID2」
「FHA2」
5182
「FID3」
「FHA3」
5183
「FIDc」
「FHAc」
5186
「FIDf」
「FHAf」
5187

图 59

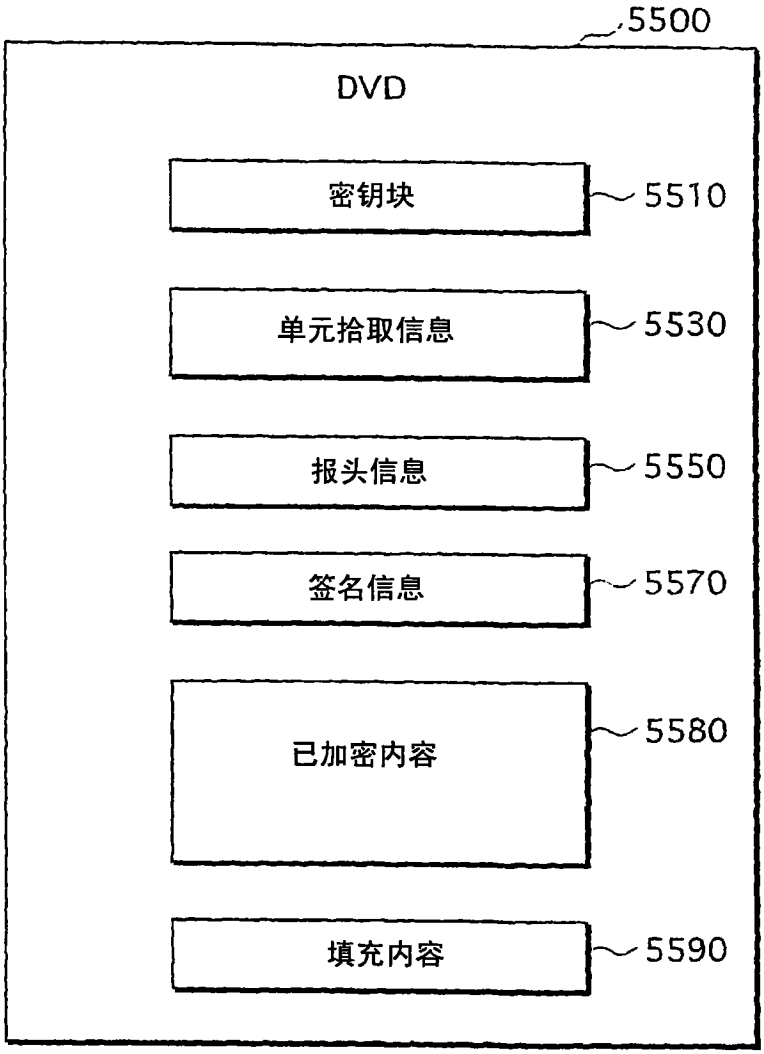

5500
DVD
密钥块
5510
单元拾取信息
5530
报头信息
5550
签名信息
5570
已加密内容
5580
填充内容
5590

图 60

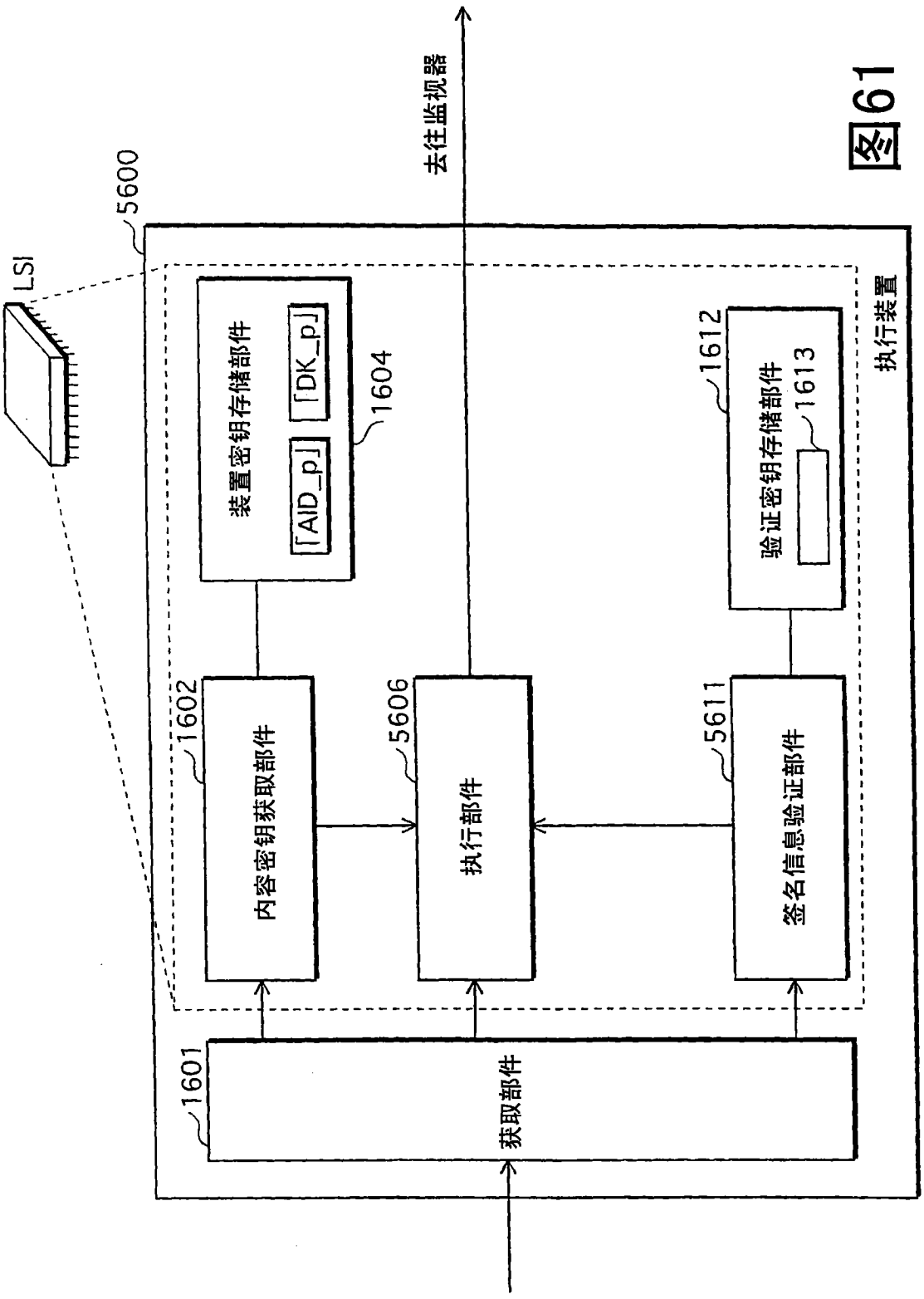

去往监视器
5600
LSI
执行装置
装置密钥存储部件
「AID_p」
「DK_p」
1604
1612
验证密钥存储部件
1613
1602
内容密钥获取部件
5606
执行部件
5611
签名信息验证部件
1601
获取部件

图61

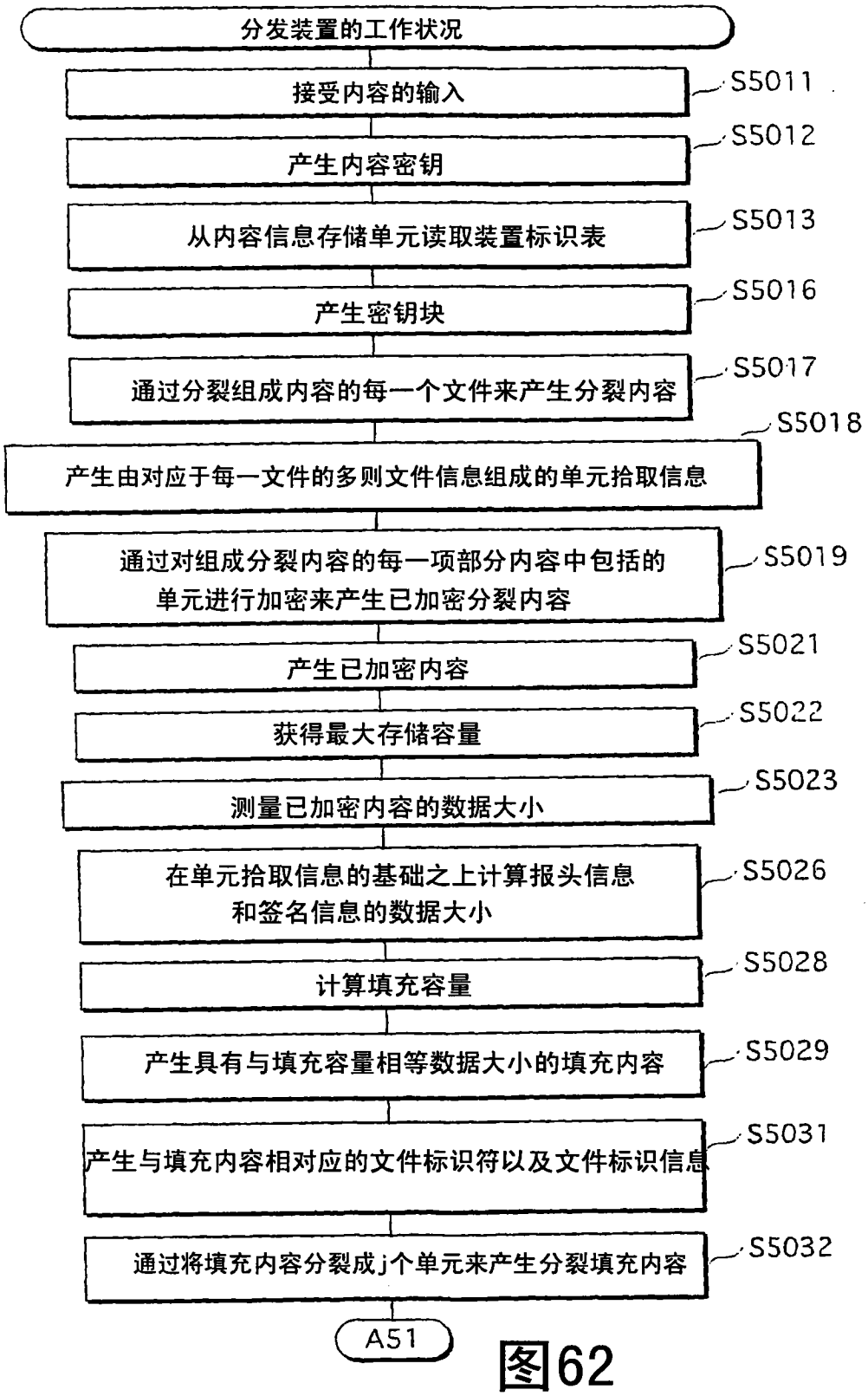

分发装置的工作状况
接受内容的输入
S5011
产生内容密钥
S5012
从内容信息存储单元读取装置标识表
S5013
产生密钥块
S5016
通过分裂组成内容的每一个文件来产生分裂内容
S5017
S5018
产生由对应于每一文件的多则文件信息组成的单元拾取信息
通过对组成分裂内容的每一项部分内容中包括的单元进行加密来产生已加密分裂内容
S5019
产生已加密内容
S5021
获得最大存储容量
S5022
测量已加密内容的数据大小
S5023
在单元拾取信息的基础之上计算报头信息和签名信息的数据大小
S5026
计算填充容量
S5028
产生具有与填充容量相等数据大小的填充内容
S5029
产生与填充内容相对应的文件标识符以及文件标识信息
S5031
通过将填充内容分裂成j个单元来产生分裂填充内容
S5032
A51

图62

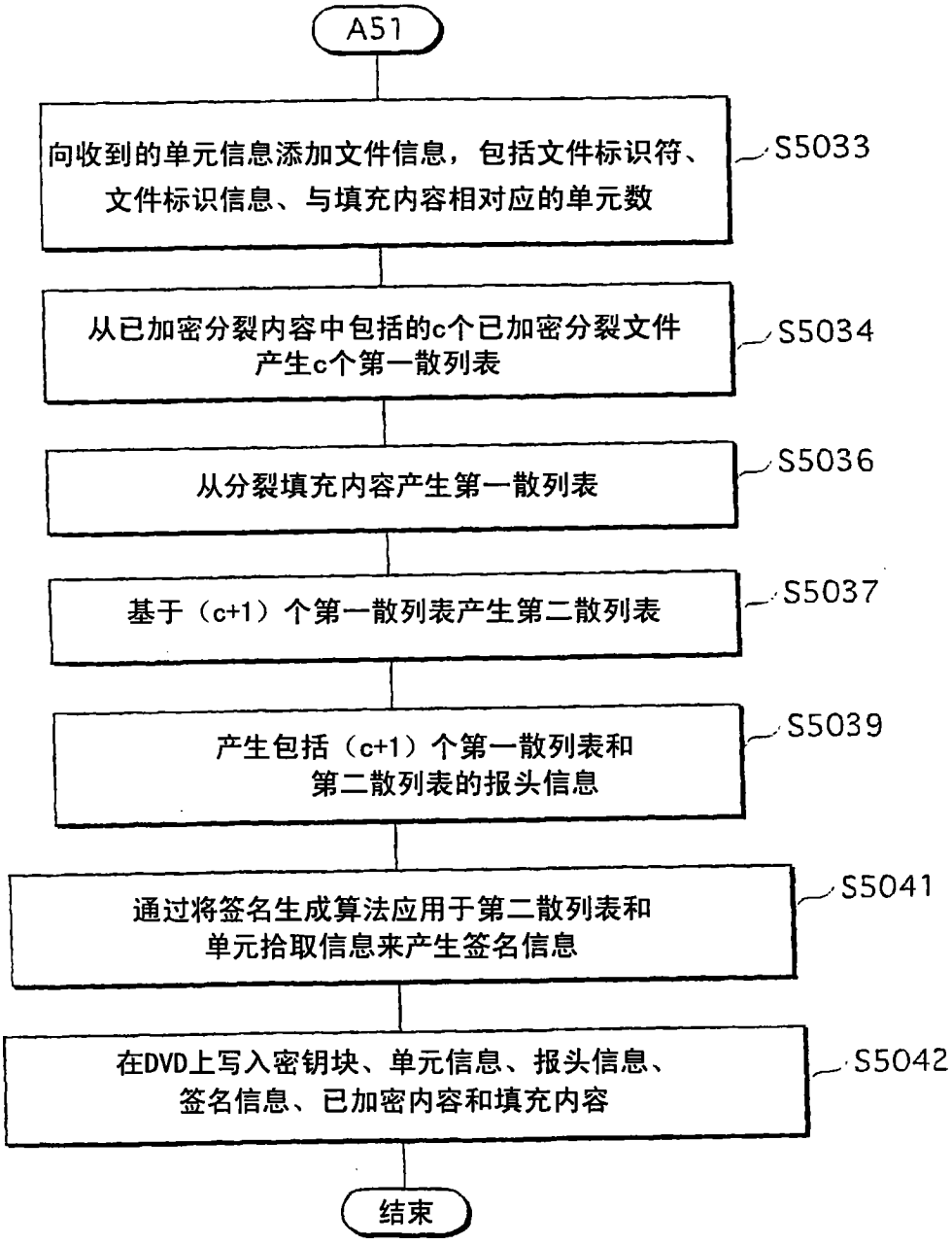

A51
向收到的单元信息添加文件信息，包括文件标识符、文件标识信息、与填充内容相对应的单元数
S5033
从已加密分裂内容中包括的c个已加密分裂文件产生c个第一散列表
S5034
从分裂填充内容产生第一散列表
S5036
基于（c+1）个第一散列表产生第二散列表
S5037
产生包括（c+1）个第一散列表和第二散列表的报头信息
S5039
通过将签名生成算法应用于第二散列表和单元拾取信息来产生签名信息
S5041
在DVD上写入密钥块、单元信息、报头信息、签名信息、已加密内容和填充内容
S5042
结束

图 63

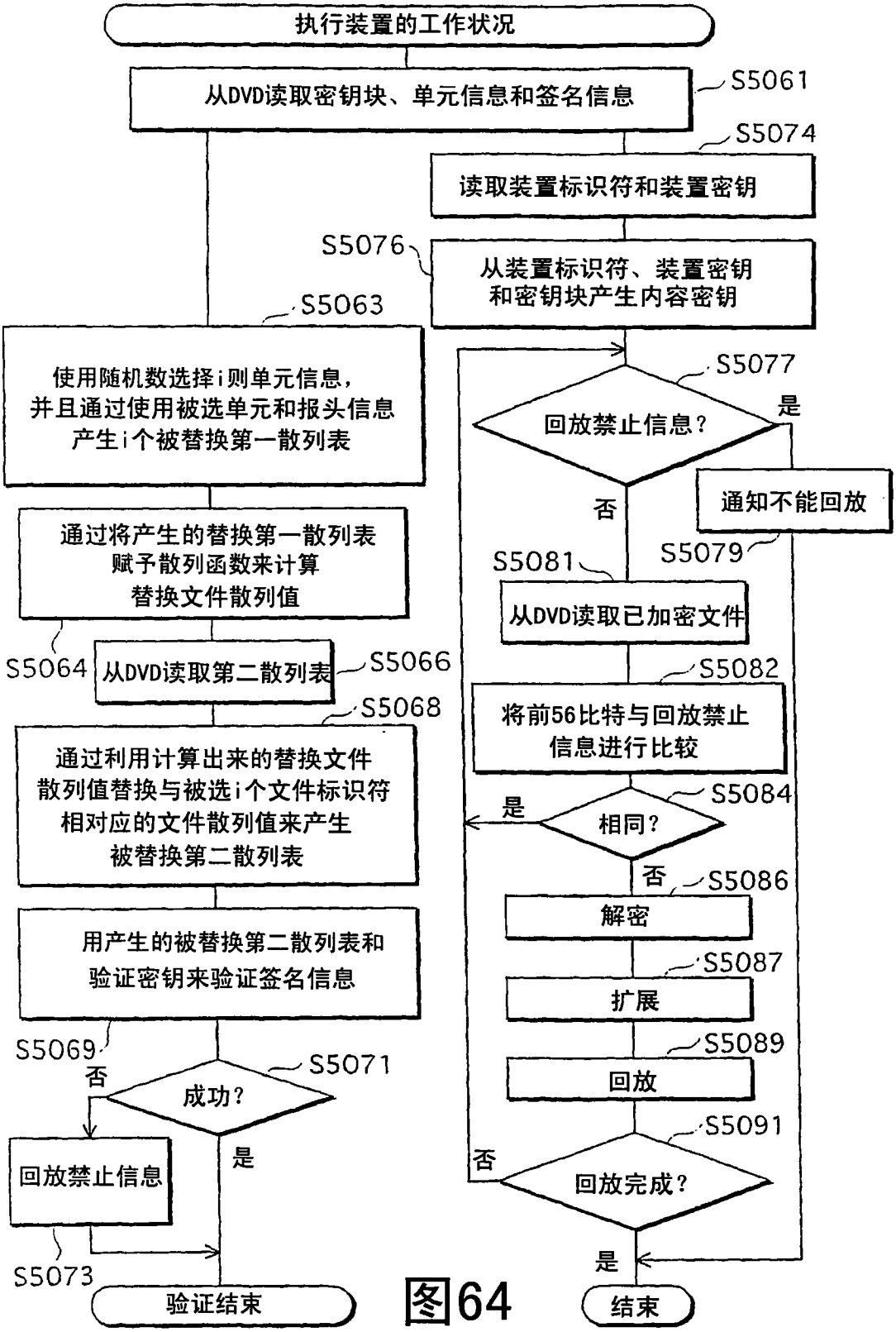

执行装置的工作状况
从DVD读取密钥块、单元信息和签名信息
S5061
S5074
读取装置标识符和装置密钥
S5076
从装置标识符、装置密钥
和密钥块产生内容密钥
S5063
使用随机数选择i则单元信息，
并且通过使用被选单元和报头信息
产生i个被替换第一散列表
通过将产生的替换第一散列表
赋予散列函数来计算
替换文件散列值
S5064
从DVD读取第二散列表
S5066
S5068
通过利用计算出来的替换文件
散列值替换与被选i个文件标识符
相对应的文件散列值来产生
被替换第二散列表
用产生的被替换第二散列表和
验证密钥来验证签名信息
S5069
否
成功?
S5071
是
回放禁止信息
S5073
验证结束
S5077
回放禁止信息?
是
否
通知不能回放
S5079
S5081
从DVD读取已加密文件
S5082
将前56比特与回放禁止
信息进行比较
是
相同?
S5084
否
S5086
解密
S5087
扩展
S5089
回放
S5091
否
回放完成?
是
结束

图64

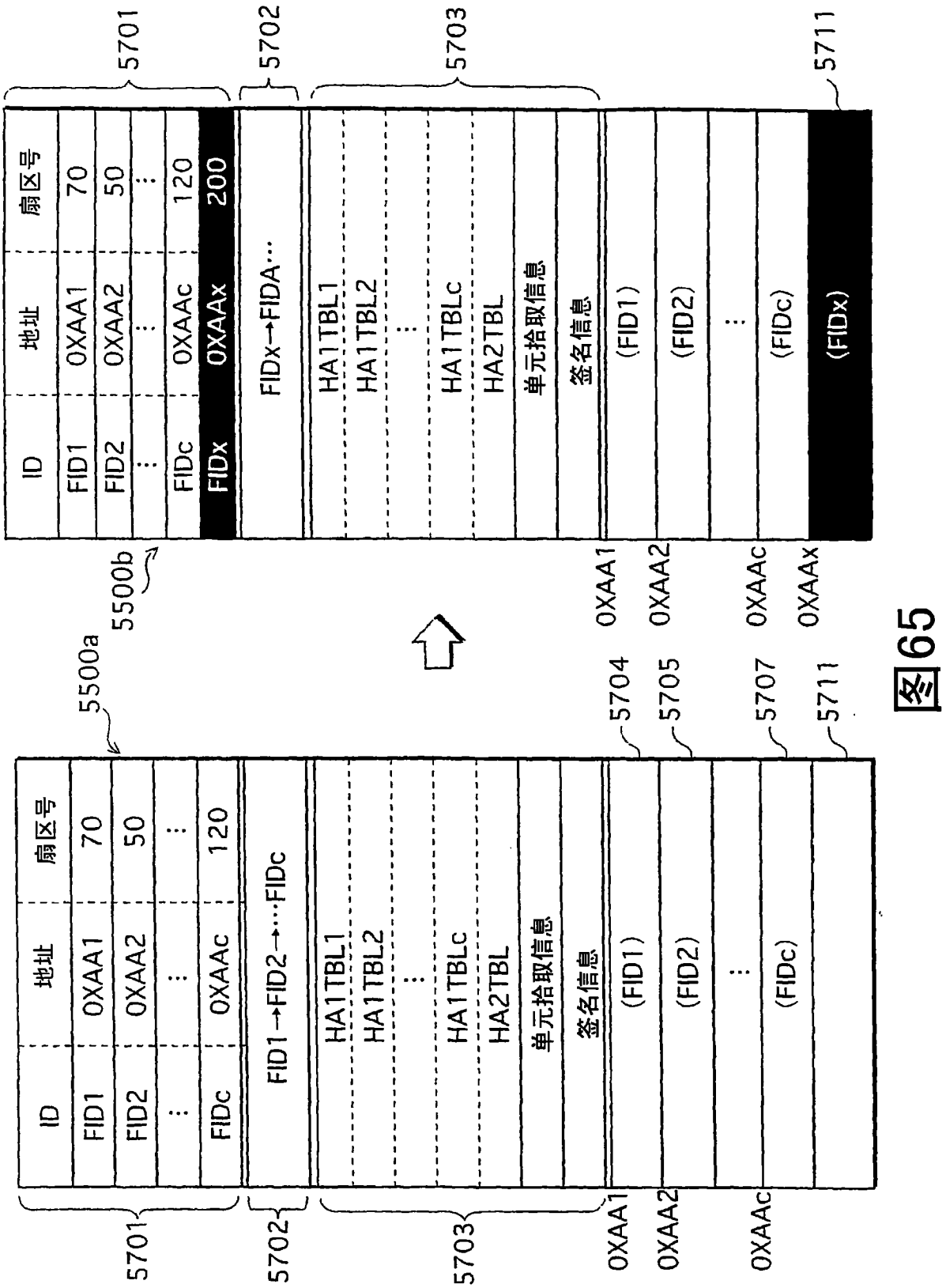

5500a
5500b
5701
5702
5703
5711
ID
地址
扇区号
FID1
OXAA1
70
FID2
OXAA2
50
FIDc
OXAAc
120
FIDx
OXAAx
200
FID1→FID2→…FIDc
FIDx→FIDA…
HA1TBL1
HA1TBL2
HA1TBLc
HA2TBL
单元拾取信息
签名信息
(FID1)
(FID2)
(FIDc)
(FIDx)
5704
5705
5707
OXAA1
OXAA2
OXAAc
OXAAx

图65

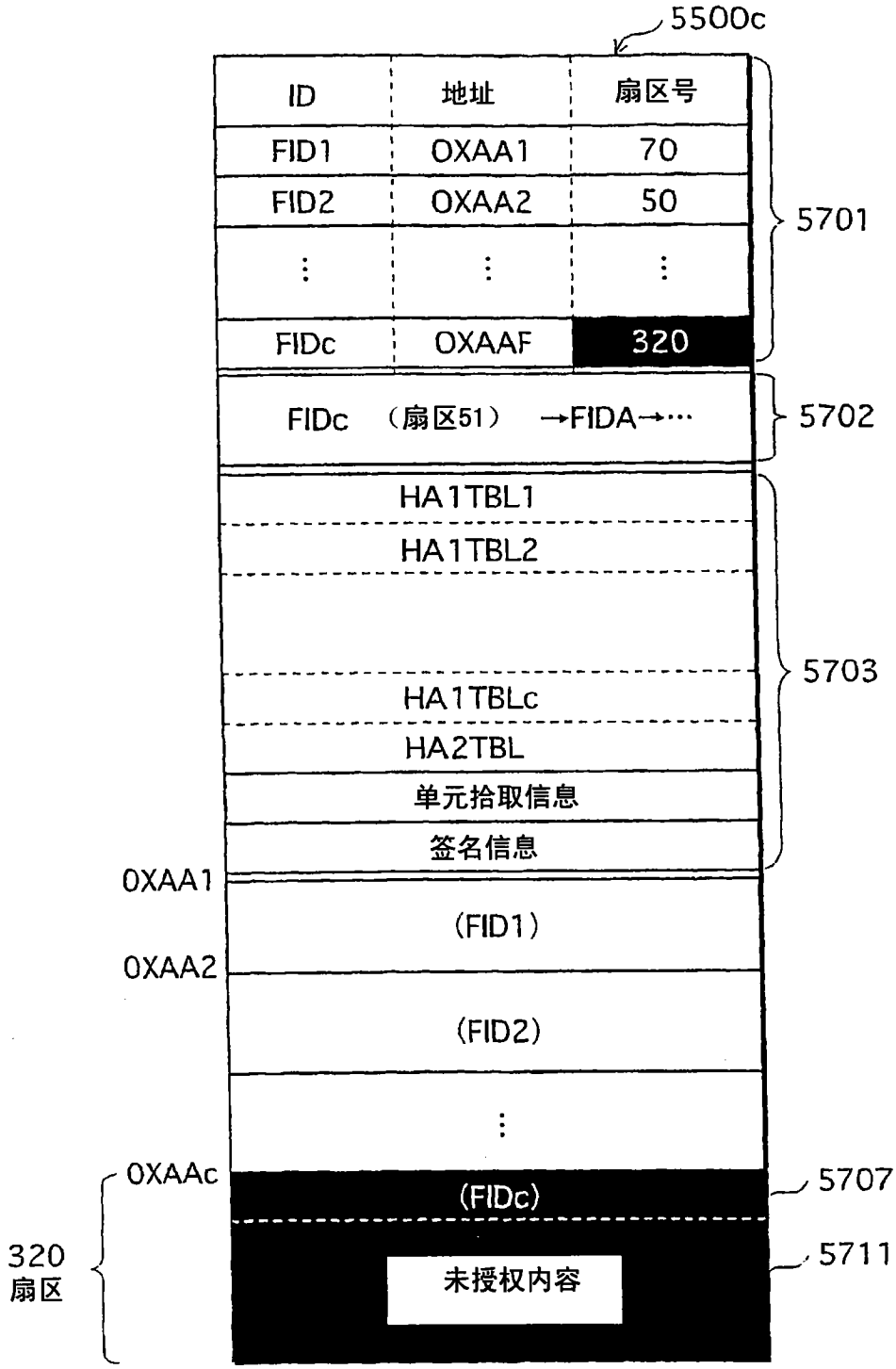

5500c
ID
地址
扇区号
FID1
OXAA1
70
FID2
OXAA2
50
FIDc
OXAAF
320
5701
FIDc （扇区51） →FIDA→…
5702
HA1TBL1
HA1TBL2
HA1TBLc
HA2TBL
单元拾取信息
签名信息
5703
0XAA1
(FID1)
0XAA2
(FID2)
0XAAc
(FIDc)
5707
5711
未授权内容
320
扇区

图 66

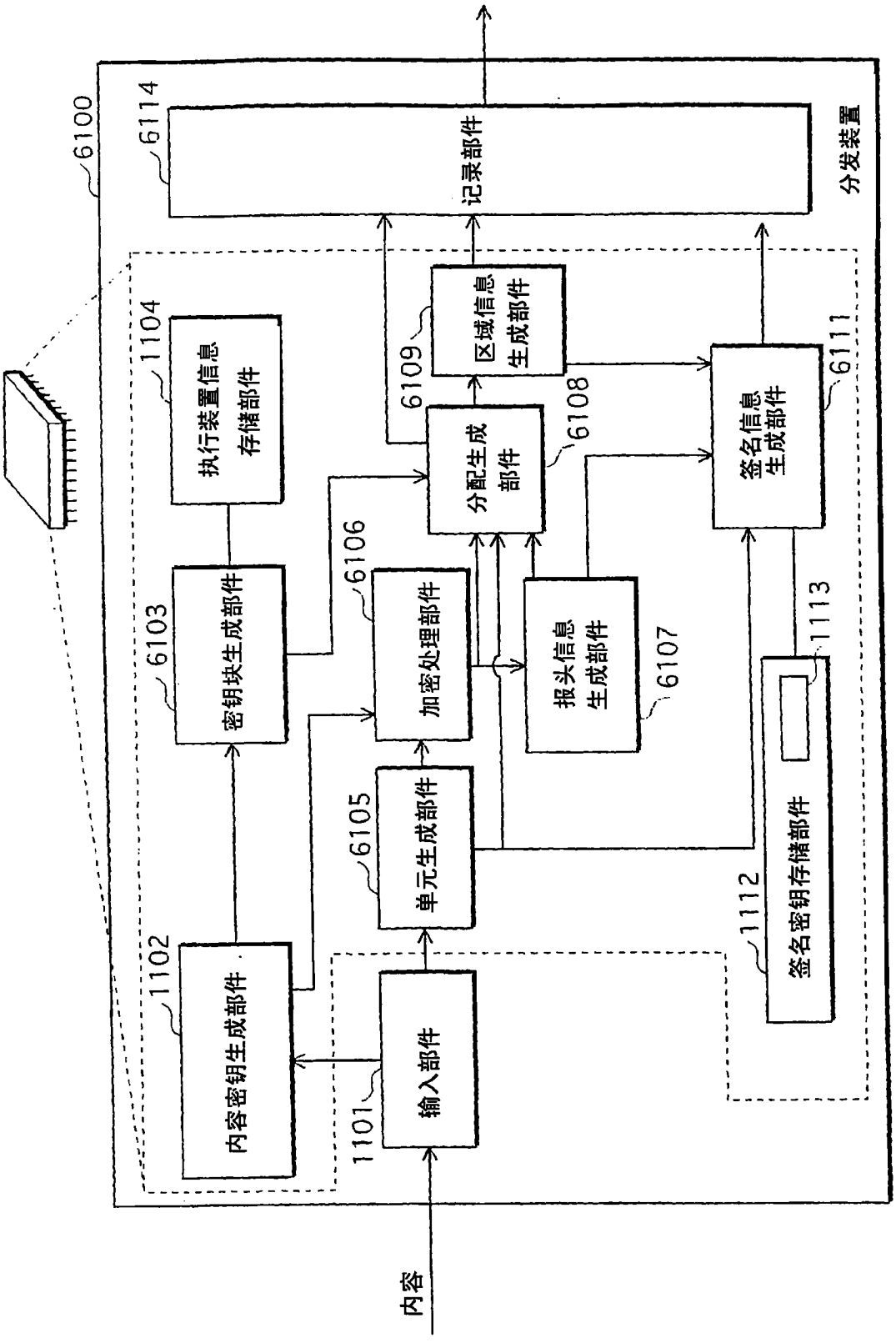

6100
分发装置
6114
记录部件
1104
执行装置信息存储部件
6109
区域信息生成部件
6111
签名信息生成部件
6108
分配生成部件
6103
密钥块生成部件
6106
加密处理部件
6107
报头信息生成部件
1113
1112
签名密钥存储部件
6105
单元生成部件
1102
内容密钥生成部件
1101
输入部件
内容

图67

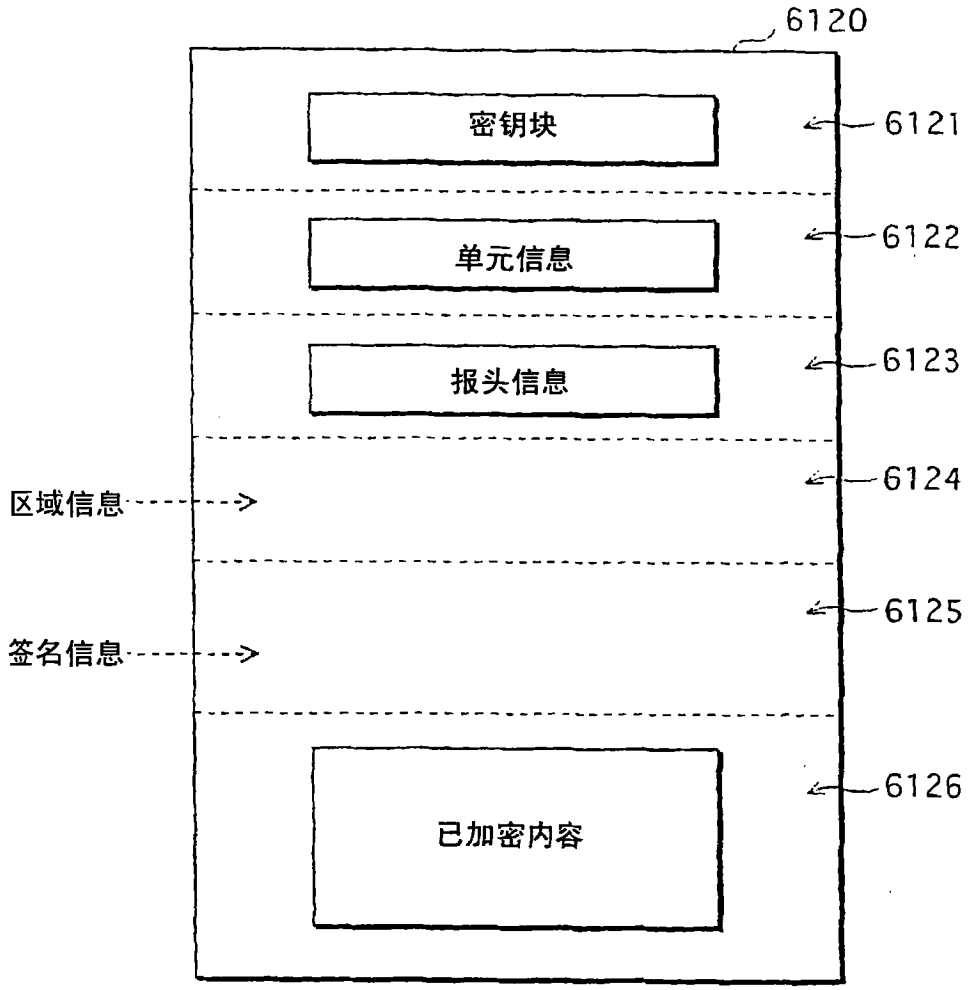

6120
密钥块
6121
单元信息
6122
报头信息
6123
区域信息
6124
签名信息
6125
已加密内容
6126

图 68

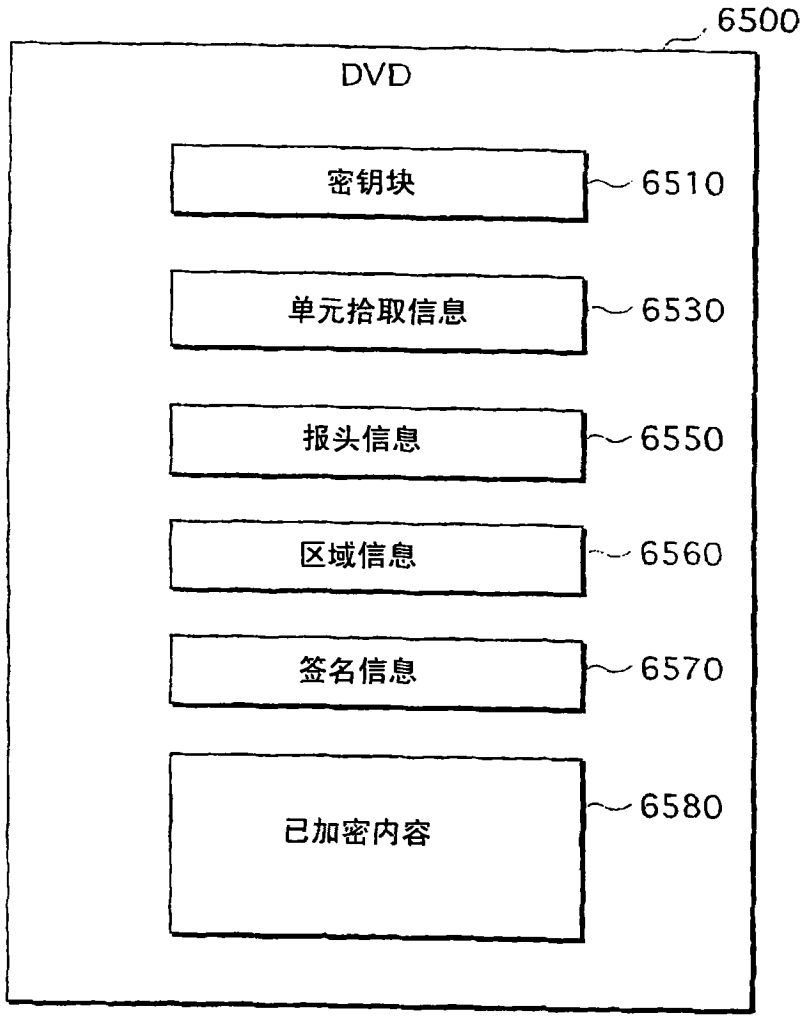

6500
DVD
密钥块
6510
单元拾取信息
6530
报头信息
6550
区域信息
6560
签名信息
6570
已加密内容
6580

图 69

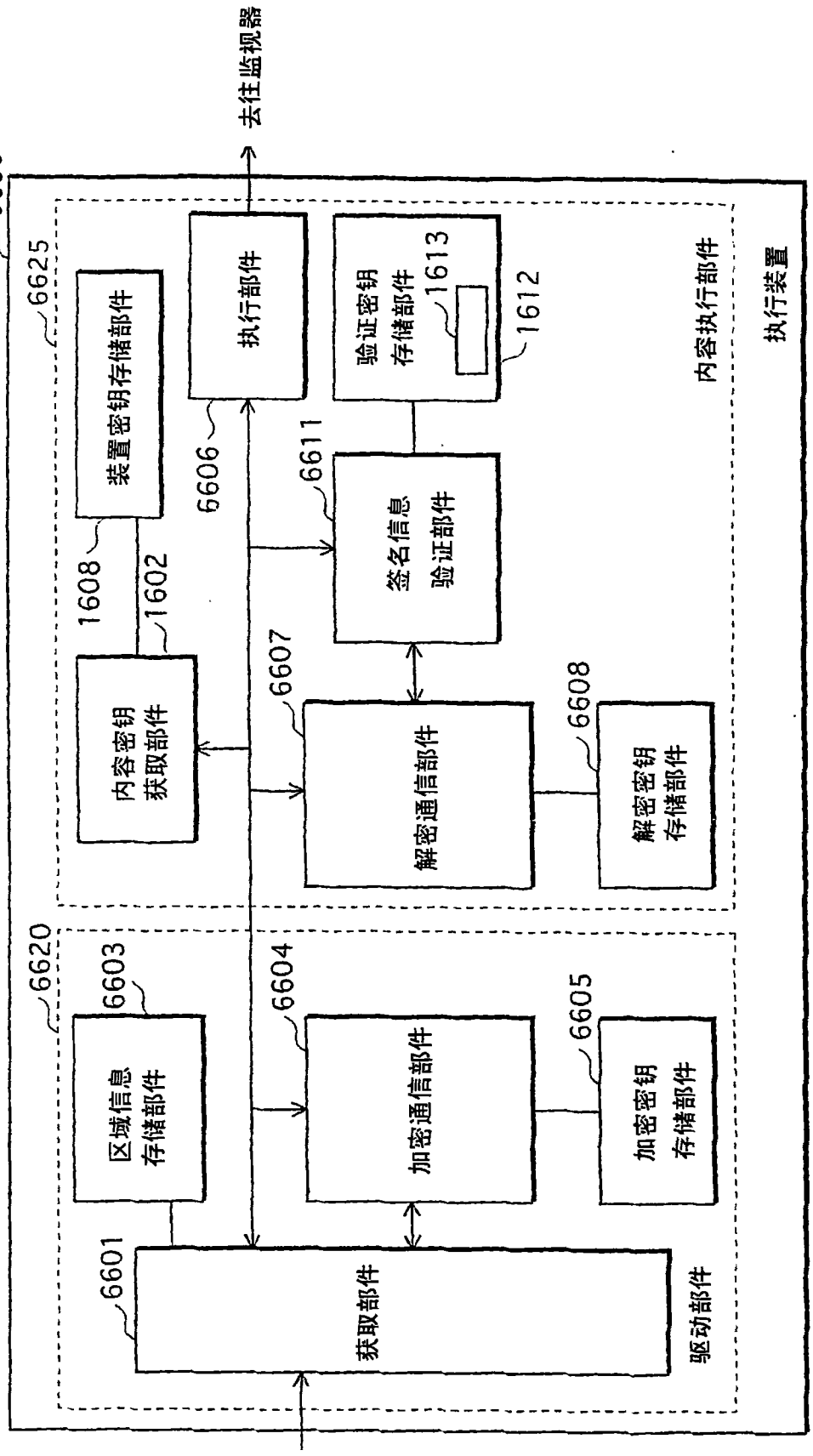

去往监视器
6600
6625
装置密钥存储部件
执行部件
验证密钥存储部件
1613
1612
内容执行部件
执行装置
1608
1602
6606
6611
签名信息验证部件
内容密钥获取部件
6607
解密通信部件
6608
解密密钥存储部件
6620
6603
区域信息存储部件
6604
加密通信部件
6605
加密密钥存储部件
6601
获取部件
驱动部件

图70

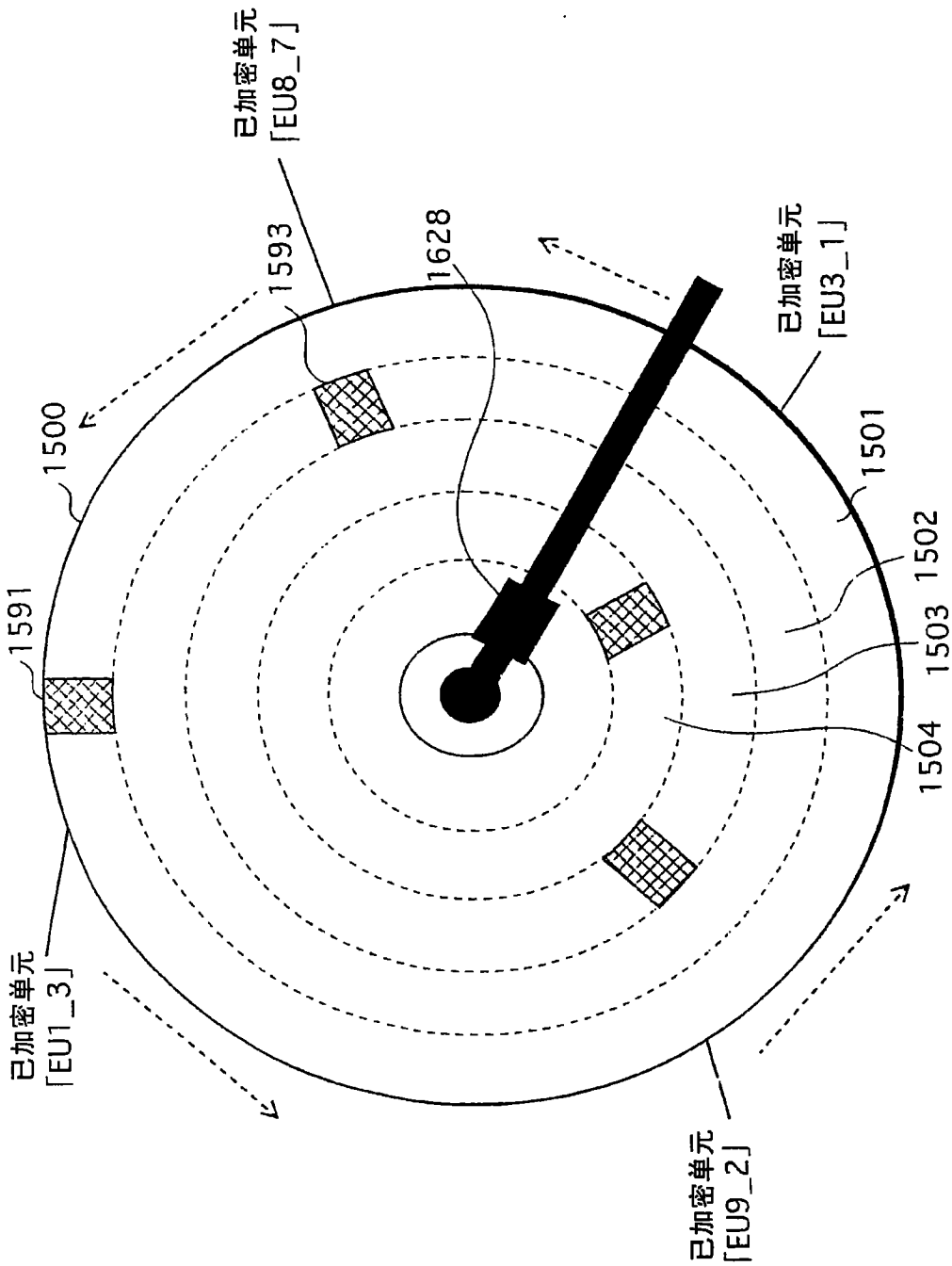

已加密单元
「EU8_7」
1593
1628
1
已加密单元
「EU3_1」
1500
1501
1502
1503
1504
1591
已加密单元
「EU1_3」
已加密单元
「EU9_2」

图71