

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G11B 20/14 (2006.01)

G11B 20/10 (2006.01)

H04L 9/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 02802053.7

[45] 授权公告日 2006年5月17日

[11] 授权公告号 CN 1256728C

[22] 申请日 2002.6.12 [21] 申请号 02802053.7

[30] 优先权

[32] 2001.6.12 [33] JP [31] 177571/01

[86] 国际申请 PCT/JP2002/005856 2002.6.12

[87] 国际公布 WO2002/101743 日 2002.12.19

[85] 进入国家阶段日期 2003.2.12

[71] 专利权人 索尼株式会社

地址 日本东京

[72] 发明人 佐古曜一郎

审查员 马克

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

代理人 李强

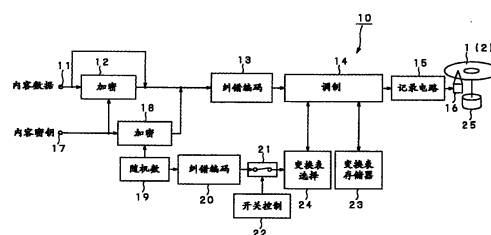
权利要求书 6 页 说明书 14 页 附图 7 页

[54] 发明名称

用于记录媒体的记录设备和记录方法，以及
用于记录媒体的重放设备和重放方法

[57] 摘要

本发明涉及一种对数据进行调制并对记录媒体记录该调制数据的记录方法，其中，在对记录媒体记录数据的过程中，根据对记录媒体记录的数据的类型，转换选择存储在存储单元内的多个变换表的方式，以利用选择的变换表将 m 位输入数据调制为 n 位数据，从而将调制数据记录到记录媒体上，所述存储单元中存储用于将 m 位数据变换为 n ($m < n$) 位数据的多个变换表。



1.一种用于记录媒体的记录设备，该记录设备包括：

存储单元，在其内存储用于将 m 位数据变换为 n 位 ($m < n$) 数据的多个变换表；

选择控制单元，用于根据对记录媒体记录的 m 位数据的类型来转换选择存储在存储单元内的多个变换表的方式；

调制处理单元，用于利用选择控制单元选择的变换表将输入的 m 位数据调制为 n 位数据；以及

记录单元，用于对记录媒体记录调制处理单元的输出数据，

其中选择控制单元根据对记录媒体记录 m 位加密内容数据的情况以及对记录媒体记录进行加密时使用的 m 位密钥数据的情况，转换选择存储在存储单元内的多个变换表的方式。

2.根据权利要求 1 所述的用于记录媒体的记录设备，其中选择控制单元根据在加密 m 位内容数据时所使用的数据来选择存储在存储单元内的多个变换表。

3.根据权利要求 2 所述的用于记录媒体的记录设备，其中该设备还包括根据随机数数据对 m 位内容数据进行加密处理的加密电路单元，而且选择控制单元根据该随机数数据来选择存储在存储单元内的多个变换表。

4.根据权利要求 1 所述的用于记录媒体的记录设备，其中选择控制单元以这样的方式运行，以便在对记录媒体记录加密内容数据时，它根据预定规则选择存储在存储单元内的多个变换表，以使信号的直流分量变得小于预定值，而在对记录媒体记录密钥数据时，它根据不同于预定规则的规则选择存储在存储单元内的多个变换表，

其中该设备还包括加密电路单元，该加密电路单元根据随机数数据对 m 位密钥数据进行加密处理，而选择控制单元根据该随机数数据选择存储在存储单元内的多个变换表。

5.根据权利要求 1 所述的用于记录媒体的记录设备，其中调制处

理单元根据 8-16 调制系统进行调制处理，其中 $m=8$ ， $n=16$ 。

6.一种用于记录媒体的记录方法，该记录方法包括以下步骤：

在对记录媒体记录数据时，根据对记录媒体记录的数据的类型，转换选择存储在存储单元内的多个变换表的方式，该存储单元中存储用于将 m 位数据变换为 n 位数据 ($m < n$) 的多个变换表；

利用选择的变换表，将输入的 m 位数据调制为 n 位数据；以及对记录媒体记录调制数据，

其中该方法还包括根据对记录媒体记录 m 位加密内容数据的情况以及对记录媒体记录进行加密时使用的 m 位密钥数据的情况，转换选择存储在存储单元内的多个变换表的方式的步骤。

7.根据权利要求 6 所述的用于记录媒体的记录方法，其中该方法包括根据对 m 位内容数据进行加密时使用的数据来选择存储在存储单元内的多个变换表的步骤。

8.根据权利要求 7 所述的用于记录媒体的记录方法，其中该方法还包括根据随机数数据加密 m 位内容数据以根据该随机数数据来选择存储在存储单元内的多个变换表的步骤。

9.根据权利要求 6 所述的用于记录媒体的记录方法，其中该方法包括以下步骤：在对记录媒体记录加密内容数据时，根据预定规则选择存储在存储单元内的多个变换表，以使信号的直流分量变得小于预定值；以及在对记录媒体记录密钥数据时，根据不同于预定规则的规则选择存储在存储单元内的多个变换表，

其中该方法还包括以下步骤：根据随机数数据加密 m 位密钥数据；以及根据该随机数数据选择存储在存储单元内的多个变换表。

10. 根据权利要求 6 所述的用于记录媒体的记录方法，其中，在该方法中的调制处理过程中，根据 8-16 调制系统进行调制处理，其中 $m=8$ ， $n=16$ 。

11. 一种用于记录媒体的重放设备，该重放设备包括：

头单元，用于从在其上记录了 n 位数据的记录媒体上读出数据；

存储单元，在其内存储用于将 n 位数据变换为 m 位 ($m < n$) 数据

的多个变换表;

选择控制单元, 用于根据对记录媒体记录的 n 位数据的类型来转换选择存储在存储单元内的多个变换表的方式; 以及

解调处理单元, 用于利用选择控制单元选择的变换表将基于头单元的输出信号的 n 位数据解调为 m 位数据,

其中选择控制单元包括核对单元, 该核对单元用于鉴别对基于头单元的输出信号的 n 位数据进行调制处理时使用的调制变换表的类型, 而且选择控制单元根据核对单元的鉴别结果将用于选择变换表的选择控制信号发送到解调处理单元。

12. 根据权利要求 11 所述的用于记录媒体的重放设备, 其中该设备还包括: 提取单元, 根据核对单元的核对结果提取用于解码 n 位内容数据的密码的数据; 以及密码分析单元, 利用提取单元提取的用于解码密码的数据, 对解调处理单元的输出数据的密码进行解码。

13. 根据权利要求 11 所述的用于记录媒体的重放设备, 其中该设备首先读出对记录媒体记录的加密密钥数据, 然后选择控制单元根据核对单元的鉴别结果, 将用于选择变换表的选择控制信号发送到解调处理单元以解调加密密钥数据。

14. 根据权利要求 13 所述的用于记录媒体的重放设备, 其中该设备进一步根据核对单元的核对结果提取用于对加密密钥数据的密码进行解码的数据, 以利用所提取的用于解码密码的数据对解调处理单元输出的加密密钥数据的密码进行解码。

15. 根据权利要求 14 所述的用于记录媒体的重放设备, 其中该设备利用已被解码的密钥数据对解调处理单元输出的加密内容数据的密码进行解码。

16. 根据权利要求 14 所述的用于记录媒体的重放设备, 其中解调处理单元根据 8-16 调制系统进行解调处理, 其中 m 是 8 而 n 是 16。

17. 一种用于记录媒体的重放方法, 该重放方法包括以下步骤:

根据从记录媒体读出的 n 位数据类型, 转换选择存储在存储单元内的多个变换表的方式, 该存储单元中存储用于将 n 位数据变换为 m

位 ($m < n$) 数据的多个变换表; 以及

利用选择的变换表, 将读出的 n 位数据解调为 m 位数据,

其中该方法还包括以下步骤: 对在调制处理从记录媒体读出的 n 位数据中使用的调制变换表的类型进行鉴别核对; 以及根据核对结果选择存储在存储单元内的多个变换表。

18. 根据权利要求 17 所述的用于记录媒体的重放方法, 其中该方法还包括以下步骤: 根据核对结果, 提取用于解码 n 位内容数据的密码的数据; 以及利用所提取的用于解码密码的数据, 对解调后的数据的密码进行解码。

19. 根据权利要求 17 所述的用于记录媒体的重放方法, 其中对记录媒体记录了 n 位加密内容数据和用于解码该内容数据的密码的 n 位加密密钥数据, 而且该方法包括以下步骤: 在从记录媒体上读出 n 位内容数据时, 根据预定规则选择存储在存储单元内的多个变换表之一; 以及在从记录媒体上读出密钥数据时, 根据核对结果选择变换表,

其中该方法还包括以下步骤: 首先读出对记录媒体记录的加密密钥数据; 根据核对结果, 发送用于选择变换表的选择控制信号; 以及解调加密密钥数据。

20. 根据权利要求 19 所述的用于记录媒体的重放方法, 其中该方法还包括以下步骤: 根据核对结果, 提取用于解码加密密钥数据的密码的数据; 以及利用所提取的用于解码密码的数据, 对解调后的加密密钥数据密码进行解码。

21. 根据权利要求 20 所述的用于记录媒体的重放方法, 其中该方法包括利用已被解码的密钥数据对解调后的加密内容数据的密码进行解码的步骤。

22. 根据权利要求 17 所述的用于记录媒体的重放方法, 其中在该方法中的解调处理过程中, 根据 8-16 调制系统进行解调处理, 其中 m 是 8 而 n 是 16。

23. 一种数据输出方法, 该方法包括以下步骤:

在输出数据的过程中, 根据输出数据的类型, 转换选择存储在存

储单元内的多个变换表的方式, 该存储单元中存储用于将 m 位数据变换为 n ($m < n$) 位数据的多个变换表;

利用选择的变换表, 将读出的 m 位数据调制为 n 位数据; 以及输出调制数据,

其中该方法还包括: 根据输出 m 位加密内容数据的情况以及输出在对内容数据进行加密过程中使用的 m 位密钥数据的情况, 转换选择存储在存储单元内的多个变换表的方式。

24. 根据权利要求 23 所述的数据输出方法, 其中该方法包括根据在对 m 位内容数据进行加密过程中使用的数据, 选择存储在存储单元内的多个变换表的步骤。

25. 根据权利要求 24 所述的数据输出方法, 其中该方法还包括以下步骤: 根据随机数数据, 对 m 位内容数据进行加密; 以及根据该随机数数据, 选择存储在存储单元内的多个变换表。

26. 根据权利要求 23 所述的数据输出方法, 其中该方法包括以下步骤: 在输出加密内容数据时, 根据预定规则选择存储在存储单元内的多个变换表, 以使信号的直流分量变得小于预定值; 以及在输出密钥数据时, 根据不同于预定规则的规则选择存储在存储单元内的多个变换表, 其中该方法还包括以下步骤: 根据随机数数据, 加密 m 位密钥数据; 以及根据该随机数数据, 选择存储在存储单元内的多个变换表。

27. 根据权利要求 23 所述的数据输出方法, 其中, 根据其中 m 是 8 而 n 是 16 的 8-16 调制系统, 执行该方法中的调制处理过程。

28. 一种数据解码方法, 该方法包括以下步骤:

根据传送的 n 位数据的类型, 转换选择存储在存储单元内的多个变换表的方式, 该存储单元中存储用于将 n 位数据变换为 m ($m < n$) 位数据的多个变换表; 以及

利用选择的变换表, 将读出的 n 位数据解调为 m 位数据,

其中该方法还包括以下步骤: 鉴别核对在对 n 位数据进行调制处理过程中使用的调制变换表的类型; 以及根据核对结果, 选择存储在

存储单元内的多个变换表。

29. 根据权利要求 28 所述的数据解码方法,其中该方法还包括以下步骤:根据核对结果,提取用于对 n 位内容数据的密码进行解码的数据;以及利用所提取的用于解码密码的数据,对解调后数据的密码进行解码。

30. 根据权利要求 28 所述的数据解码方法,其中该方法包括以下步骤:在对 n 位内容数据进行解调时,根据预定规则,选择存储在存储单元内的多个变换表之一;以及在对密钥数据进行解调时,根据核对结果选择变换表。

31. 根据权利要求 28 所述的数据解码方法,其中该方法包括以下步骤:为了解调加密密钥数据,首先根据核对结果发送用于选择变换表的选择控制信号;以及解调加密密钥数据。

32. 根据权利要求 31 所述的数据解码方法,其中该方法还包括以下步骤:根据核对结果,提取用于对加密密钥数据的密码进行解码的数据;以及利用所提取的用于解码密码的数据,对解调后的加密密钥数据的密码进行解码。

33. 根据权利要求 32 所述的数据解码方法,其中该方法包括利用已被解码的密钥数据对解调后的加密内容数据的密码进行解码的步骤。

34. 根据权利要求 28 所述的数据解码方法,其中,根据其中 m 是 8 而 n 是 16 的 8-16 调制系统进行该方法中的解调处理过程。

用于记录媒体的记录设备和记录方法，
以及用于记录媒体的重放设备和重放方法

技术领域

本发明涉及对记录媒体记录调制数据的记录设备和记录方法，还涉及用于从记录有调制数据的记录媒体解调数据以重放数据的重放设备和重放方法。

背景技术

为了保护待记录到数字多功能光盘（以下在需要时简称为 DVD）上的数据的版权，在基于诸如 CSS（内容置乱系统）等的访问限制系统进行置乱操作之后记录数据。这种 DVD 被设置成能够利用只重放设备重放记录在 DVD 上的数据，而且还能够利用诸如个人计算机等的通用设备重放记录在 DVD 上的数据。利用存储在该设备中的存储器内的密码分析密钥，这种只重放设备和/或通用设备解除记录在 DVD 上的数据置乱，从而可以重放记录在 DVD 上的数据。

同时，出现了一种利用软件非正当地解除数据置乱，将记录在 DVD 上的数据拷贝到个人计算机的硬盘等上的方法。为了防止发生这种事情，要求在使用个人计算机等时不能拷贝用于解除数据置乱的数据。

发明内容

本发明的一个目的是提供：一种用于记录媒体的记录设备和记录方法，以这样的方式对数据记录媒体保密数据进行记录，即在使用个人计算机等时不能拷贝诸如用于解除或解码密码的数据的保密数据，能够防止不正当拷贝数字数据；一种用于记录媒体的重放设备和重放方法，用于重放利用所述记录设备和记录方法在其上记录了数据的记

录媒体；以及一种数据输出方法和数据解码方法。

为了实现上述目的，建议了一种根据本发明的用于记录媒体的记录设备，该记录设备包括：存储单元，在其内存储用于将 m 位数据变换为 n 位 ($m < n$) 数据的多个变换表；选择控制单元，用于根据对记录媒体记录的 m 位数据的类型来转换选择存储在存储单元内的多个变换表的方式；调制处理单元，用于利用选择控制单元选择的变换表将输入的 m 位数据调制为 n 位数据；以及记录单元，用于对记录媒体记录调制处理单元的输出数据。

这种用于记录媒体的记录设备还包括根据随机数数据对 m 位数据进行加密处理的加密电路单元，而且选择控制单元根据随机数数据选择存储在存储单元内的多个变换表。

根据本发明用于记录媒体的记录方法包括以下步骤：在对记录媒体记录数据时，根据对记录媒体记录的数据类型，转换选择存储在存储单元内的多个变换表的方式，该存储单元存储用于将 m 位数据变换为 n 位数据 ($m < n$) 的多个变换表；利用选择的变换表，将输入的 m 位数据调制为 n 位数据；以及对记录媒体记录调制数据。

根据本发明用于记录媒体的重放设备包括：头单元，用于从在其上记录了 n 位数据的记录媒体上读出数据；存储单元，在其内存储用于将 m 位数据变换为 n 位 ($m < n$) 数据的多个变换表；选择控制单元，用于根据对记录媒体记录的 n 位数据的类型来转换选择存储在存储单元内的多个变换表的方式；以及解调处理单元，用于利用选择控制单元选择的变换表将基于头单元的输出信号的 n 位数据解调为 m 位数据。

这种用于记录媒体的重放设备还包括：提取单元，根据一个核对单元的核对结果提取用于解码 n 位数据的密码的数据；以及密码分析单元，利用提取单元提取的用于解码密码的数据，对解调处理单元的输出数据的密码进行解码。

根据本发明用于记录媒体的重放方法包括以下步骤：根据从记录媒体读出的 n 位数据的类型，转换选择存储在存储单元内的多个变换

表的方式，该存储单元存储用于将 n 位数据变换为 m 位 ($m < n$) 数据的多个变换表；以及利用选择的变换表，将读出的 n 位数据解调为 m 位数据。

根据本发明的数据输出方法包括以下步骤：在输出数据的过程中，根据输出数据的类型，转换选择存储在存储单元内的多个变换表的方式，该存储单元存储用于将 m 位数据变换为 n ($m < n$) 位数据的多个变换表；利用选择的变换表，将读出的 m 位数据调制为 n 位数据；以及输出调制数据。

根据本发明的数据解码方法包括以下步骤：根据传送的 n 位数据的类型，转换选择存储在存储单元内的多个变换表的方式，该存储单元存储用于将 n 位数据变换为 m ($m < n$) 位数据的多个变换表；以及利用选择的变换表，将读出的 n 位数据解调为 m 位数据。

通过以下参考附图对实施例进行说明，本发明的其它目的和更多实用的优点将变得更加明显。

附图说明

图 1 是用于说明应用本发明的一种光盘的配置的示意图。

图 2 是用于说明根据本发明的光盘的另一个例子的示意图。

图 3 是示出应用本发明的记录设备的方框图。

图 4 是用于说明进行 8-16 调制的主变换表的示意图。

图 5 是用于说明进行 8-16 调制的辅助变换表的示意图。

图 6 是用于说明用于光盘的重放设备的方框图。

图 7 是用于说明提取随机数数据的过程的流程图。

图 8 是用于说明利用代码号提取随机数数据的过程的流程图。

图 9 是用于说明利用偶数/奇数代码号提取随机数数据的过程的流程图。

实现本发明的最佳方式

现在将参考附图，对应用了本发明的数据记录媒体、数据记录设

备以及数据记录方法进行说明。

应用了本发明的数据记录媒体指可记录光盘。如图 1 所示，对光盘 1 进行设置，以便在内圆侧设置用于记录 TOC（内容表）等的导入区 1a，在此导入区 1a 往外圆侧设置用于记录加密之后的内容数据的节目区 1b，在此节目区 1b 往外圆侧设置导出区 1c。在导入区 1a 与节目区 1b 之间，设置用于存储对记录在节目区 1b 内的内容数据进行加密的内容密钥数据的密钥锁定区 1d。在利用保密密钥数据，例如进行记录时的随机数数据对此内容密钥数据进行加密后，将它存储到密钥锁定区 1d 内。

应用本发明的光盘还可以具有如图 2 所示的构造。如图 2 所示，设置此光盘 2 以便在内圆侧设置第一光道 3，而在第一光道 3 往外圆侧设置第二光道 4。设置各光道 3、4，以便分别设置导入区 3a、4a，其中在导入区 3a、4a 后设置用于记录内容数据的节目区 3b、4b，在节目区 3b、4b 后设置导出区 3c、4c。在此，设置第一光道 3 以便例如以与所谓压缩光盘的记录密度相同的记录密度记录数据，设置第二光道 4 以便以比第一光道 3 的记录密度高的记录密度记录数据。在第二光道 4 的导入区 4a 与节目区 4b 之间，设置其中存储用于将内容数据经过加密之后记录到节目区 4b 的内容密钥数据的密钥锁定区 4d。在利用保密密钥数据，例如进行记录时的随机数数据对内容密钥数据进行加密后，将该内容密钥数据存储到密钥锁定区内。

对具有上述构造的光盘 2 进行设置，以便例如将内容数据记录到外圆侧的第二光道 4，而将记录到第二光道 4 的内容数据的广告数据等记录到内圆侧的第一光道 3 上。在此光盘 2 上，与第一光道 3 相比，可以将更高质量的数据记录到第二光道 4 上。

下面，将参考图 3 说明作为用于应用了本发明的记录媒体的记录设备的数据记录设备 10。此数据记录设备 10 包括：加密电路 12，对从输入端 11 输入的内容数据进行加密；纠错编码电路 13，用于对被加密电路 12 加密的内容数据进行纠错编码处理；调制电路 14，用于调制经过纠错编码处理的内容数据；记录处理电路 15，用于对进行了

调制处理的内容数据进行记录处理；光学头 16，用于将数据记录到光盘 1 或 2 上；以及纺锤形电机 25，用于旋转驱动光盘 1 或 2。

此数据记录设备 10 还包括：加密电路 18，用于对加密从输入端 17 输入的内容数据的内容密钥数据进行加密；随机数生成电路 19，产生用于在加密电路 18 对内容密钥数据进行加密的随机数数据；纠错编码电路 20，用于对随机数生成电路 19 产生的随机数数据进行纠错编码处理；开关 21，用于接通或断开输出对其进行了纠错编码处理的随机数数据；开关控制单元 22，用于接通/断开开关 21；存储器 23，在其内存储用于调制内容数据的多个变换表；以及变换表选择单元 24，用于根据随机数数据选择调制表。

将要记录到光盘 1 或光盘 2 的内容数据从输入端 11 输入到加密电路 12。将用于对从输入端 17 输入的内容数据进行加密的内容密钥数据输入到对内容数据进行加密的加密电路 12。加密电路 12 利用内容密钥数据对输入内容数据进行加密，并将它输出到纠错编码电路 13。请注意，要记录在光盘 2 第一光道 3 上的内容数据被直接输入到纠错编码电路 13，而无需输入到加密电路 12。

将从输入端 17 输入的内容密钥数据输入到对内容数据进行加密的加密电路 12，并输入到加密内容密钥数据的加密电路 18。从随机数生成电路 19 输入在对内容密钥数据进行加密中用作保密密钥数据的随机数数据，例如：8 位数据（10100100）。加密电路 18 利用随机数数据对内容密钥数据进行加密，然后，将利用随机数数据加密的内容密钥数据输入到纠错编码电路 13。

对其提供加密或非加密内容数据以及加密内容密钥数据的纠错编码电路 13 进行编码处理，产生诸如 CIRC（交叉交错 RS 码）等的纠错码以将它加到输入数据中。然后，纠错编码电路 13 将经过纠错编码处理的数据输出到调制电路 14。

同时，为了对内容密钥数据进行加密，上述随机数生成电路 19 产生随机数数据以将此随机数数据输出到对内容密钥数据进行加密的加密电路 18，并将它输出到纠错编码电路 20 以进行处理，用于将随机

数数据记录到光盘 1 或光盘 2 上。被提供随机数数据的纠错编码电路 20 对随机数数据进行纠错编码处理。通过开关 21, 纠错编码电路 20 将随机数数据输出到变换表选择单元 24, 以将它记录到光盘 1 或光盘 2。设置开关 21 以便在开关控制单元 22 的开关控制下使其接通/断开。仅在对光盘 1 或光盘 2 的密钥锁定区 1d、4d 记录加密内容密钥数据时, 开关控制单元 22 使开关 21 接通, 以将对其进行了纠错编码处理的随机数数据输出到变换表选择单元 24。

调制电路 14 对输入数据进行例如 8-16 调制处理。将进行 8-16 调制处理的多个变换表存储到存储器 23 内。从更实用的意义上说, 存储在存储器 23 内的变换表具有 4 个用于将输入数据从 8 位变换为 16 位的代码表, 如图 4 所示。设置此变换表以确定用于随后各 8 位输入数据的代码表号。

如图 5 所示, 将图 4 所示变换表的辅助变换表存储到存储器 23。例如, 如果图 4 所示的变换表用于进行 8-16 调制, 则在信号的直流分量, 即 DSV (数字和变量) 的绝对值为预定值或者更大时, 利用此辅助变换表使 DSV 小于预定值。该辅助变换表也具有 4 个用于将 8 位输入数据变换为 16 位数据的代码表, 其中确定用于随后各 8 位输入数据的代码表号。

在通常情况下, 即调制电路 14 调制内容数据时, 使用图 4 所示变换表, 根据变换表规定的规则选择代码表 1 至 4。例如, 如图 4 所示, 调制电路 14 可以在它利用代码表 1 将输入代码号为 2 的 8 位数据变换为 16 位时, 它利用代码表 2 将随后的 8 位数据变换为 16 位数据。同样, 在调制电路 14 选择图 5 所示的辅助变换表以使 DSV 小于预定值时, 调制电路 14 根据该辅助变换表规定的规则选择代码表 1 至 4。调制电路 14 将调制后的内容数据, 即 16 位数据输出到记录处理电路 15。

在调制电路 14 将加密内容密钥数据记录到光盘 1 或 2 的密钥锁定区 1d、4d 时, 调制电路 14 以如下方式运行。首先, 将纠错编码处理后的加密内容密钥数据从纠错编码电路 13 输入到调制电路 14。在将加密内容密钥数据记录到密钥锁定区 1d、4d 时, 开关控制单元 22 使

开关 21 接通。因此，将纠错处理后的随机数数据从纠错编码电路 20 输入到变换表选择单元 24。

根据输入随机数数据，利用与例如图 4 所示的变换表和图 5 所示的辅助变换表规定的规则不同的规则，变换表选择单元 24 选择图 4 所示的变换表和图 5 所示的辅助变换表。也就是说，变换表选择单元 24 选择变换表，以便在解调时通过自身选择图 4 所示的变换表和图 5 所示的辅助变换表使数据成为随机数数据。

在选择图 4 所示的变换表或图 5 所示的辅助变换表时，变换表选择单元 24 以这样的方式选择图 4 所示的变换表或图 5 所示的辅助变换表，以使游程长度等于 $(RLL(2, 10))$ ，即“0”最小游程等于“2”，而其最大游程等于“10”。此外，变换表选择单元 24 还以这样的方式选择图 4 所示的变换表或图 5 所示的辅助变换表，以使 DSV 不等于预定值或者更大。

变换表选择单元 24 将选择的变换表或辅助变换表以及代码表号输出到调制电路 14。调制电路 14 根据存储在存储器 23 内的变换表调制加密内容密钥。调制电路 14 将当前调制处理过程使用的变换表或辅助变换表的类型以及代码表号输出到变换表选择单元 24，从而能够选择变换表选择单元 24 后续使用的图 4 所示的变换表或图 5 所示的辅助变换表，以使游程长度等于 $(RLL(2, 10))$ 而 DSV 不等于预定值或者更大。根据上述随机数数据，变换表选择单元 24 选择图 4 所示的变换表或图 5 所示的辅助变换表用于后续调制处理。调制电路 14 将调制后的内容密钥数据输出到记录处理电路 15。记录处理电路 15 对调制后的内容数据或内容密钥数据的数据进行处理，例如进行二进制编码处理等以转换为记录数据，从而将它作为存储数据输出到光学头 16。

光学头 16 对利用纺锤形电机 25 使其以例如 CLV（恒定线速度）旋转的光盘 1 或 2 的信号记录层照射光束，以将数据记录到光盘 1 或 2 上。从更实际的意义说，光学头 16 将 TOC（内容表）数据等作为待记录到节目区 1b 或 3b、4b 的记录数据的管理数据，记录到导入区 1a 或 3a、4a，将内容密钥记录到密钥锁定区 1d、4d，将作为记录数

据的内容数据记录到节目区 1b 或区域 3b、4b。尤其在使节目区 4b 的记录密度高于节目区 3b 的记录密度状态下，将内容数据即记录数据记录到光盘 2 的节目区 4b。

在利用上述数据记录设备进行记录的光盘 1、2 内，当利用现有数据重放设备重放该光盘时，因为利用不同于常规的规则，即利用不同于对作为记录数据的内容数据进行调制规则的规则对存储在密钥锁定区 1d、4d 内的内容密钥数据进行调制，所以不可能解调此内容密钥数据。因此，在光盘 1、2 内，可以防止利用诸如现有数据重放设备的无权数据重放设备重放加密内容数据。也就是说，如上所述，即使在利用诸如作为现有数据重放设备的个人计算机等的硬盘的记录媒体，对其上记录了内容密钥数据的光盘 1、2 上读取的数据进行拷贝时，也不能解调加密内容密钥数据，而且也不能提取用于加密内容密钥数据的随机数数据。根据此事实，如在现有技术中所述，可以防止通过不正当解码内容密钥数据的密码来对记录在光盘上的内容数据密码进行解码。

尽管对上述作为例子的实例进行了说明，但是在对内容密钥数据进行调制处理过程中，在对记录在光盘 1、2 的节目区 1b 或区域 3b、4b 内的数据进行调制处理时改变选择变换表的规则的情况下，还可以采用一种根据随机数数据而不根据内容密钥数据对伪数据进行加密的方法，以使图 4 所示的变换表或图 5 所示的辅助变换表具有基于此随机数数据的选择转换量。在这种情况下，变换表选择单元 24 足以根据随机数数据变换为代码表号，以实现调制电路 14 根据此代码表将伪数据变换为 16 位数据的调制处理过程。变换表选择单元 24 足以根据随机数数据选择图 4 或图 5 所示变换表的偶数和奇数代码表号，而且调制电路 14 利用选择的偶数或奇数代码表号的变换表对伪数据进行调制。当然，根据随机数数据足以选择图 4 所示变换表和图 5 所示辅助变换表，以便根据选择的变换表对伪数据进行调制处理。在这种情况下，将内容密钥数据记录并存储到密钥锁定区 1d、4d 内，而且将伪数据记录到密钥锁定区 1d、4d 内，即记录到光盘 1 的导入区 1a、节目

区 1b 和导出区 1c, 以及记录到光盘 2 的导入区 3a、4a, 节目区 3b、4b 和导出区 3c、4c。

然后, 将参考图 6 说明数据重放设备 30, 数据重放设备 30 重放由数据记录设备 10 将数据记录到其上的光盘 1、2。数据重放设备 30 包括: 纺锤形电机 31, 用于以例如 CLV (恒定线速度) 旋转光盘 1、2; 光学头 32, 用于读取记录在光盘 1、2 上的数据; RF 放大器 33, 用于放大光学头 32 的输出信号; 伺服电路 34, 用于对纺锤形电机 31 和光学头 32 进行伺服控制; 子码提取单元 35, 用于从 RF 信号中提取 TOC 数据等; 解调电路 36, 用于对从 RF 放大器 33 输入的信号进行解调处理, 以对内容数据或内容密钥数据进行解调; 纠错解码电路 37, 对解调电路 36 的输出数据进行纠错处理; 以及密码分析电路 38, 用于对电路 37 输出的加密数据进行解码。数据重放设备 30 还包括: 存储器 39, 在其内存储解调电路 36 对数据进行解调处理时使用的变换表; 核对单元 40, 用于核对调制过程使用的变换表; 提取单元 41, 用于提取用于对内容密钥数据的密码进行解码的随机数数据; 开关 42, 用于选择使数据从核对单元 40 输出到提取单元 41; 纠错解码电路 43, 用于对提取单元 41 提取的随机数数据进行纠错处理; 以及控制单元 44, 用于对诸如开关 42 的重放设备 30 的整个操作进行控制。

在利用物镜 (未示出) 聚焦光束的状态下, 光学头 32 将光束照射到利用纺锤形电机 31 以例如 CLV (恒定线速度) 旋转的光盘 1 或 2 上, 从而利用光检测器 (未示出) 检测被光盘 1 或 2 反射的返回光束以进行光电转换, 随后将相应信号作为输出信号输出到 RF 放大器 33。在从光学头 32 输入信号时, RF 放大器 33 产生 RF 信号作为记录在光盘 1 或 2 上的数据的读出信号, 而且根据光学头 32 的输出信号产生聚焦误差信号和跟踪误差信号。RF 放大器 33 将 RF 信号输出到解调电路 36, 而将聚焦误差信号和跟踪误差信号输出到伺服电路 34。伺服电路 34 根据发送的聚焦误差信号和跟踪误差信号产生聚焦伺服信号和跟踪伺服信号, 并将它们输出到光学头 32。根据聚焦伺服信号和跟踪伺服信号, 光学头 32 利用致动器 (未示出) 对物镜进行聚焦控制和伺

服控制。伺服电路 34 根据 RF 放大器 33 输出的 RF 信号产生用于纺锤形电机 31 的伺服信号，并将它发送到纺锤形电机 31。因此，旋转控制纺锤形电机 31，从而以恒定线速度旋转光盘 1 或 2。子码提取单元 35 从 RF 放大器 33 输出的 RF 信号中提取子码数据等，并将 TOC 数据或子码数据等输出到控制单元 44。

解调电路 36 对在记录到光盘 1 或 2 上时进行了 8-16 调制的数据进行解调处理。在此，将与图 4 所示变换表和图 5 所示辅助变换表成对的、用于执行图 4 所示变换表和图 5 所示辅助变换表的逆变换的变换表和辅助变换表存储到存储器 39。图 4 所示变换表和图 5 所示辅助变换表用于将 8 位变换为 16 位，而成对的变换表和辅助变换表用于将 16 位变换为 8 位。

在对密钥锁定区 1d、4d 进行读取时，为了提取用于加密内容密钥数据的随机数数据，控制单元 44 闭合开关 42，即使它接通。如图 7 所示，在步骤 S1 从 RF 放大器 33 输入 RF 信号后，在步骤 S2，核对单元 40 判别对输入的加密内容密钥数据进行调制使用的表是图 4 所示的变换表还是图 5 所示的辅助变换表。在此，核对单元 40 将核对结果，即有关根据对内容密钥数据进行调制时使用的变换表的类型和/或组合的规则的数据输出到解调电路 36，然后，解调电路 36 根据从核对单元 40 输入的数据并根据存储在存储器 39 的、与图 4 所示变换表和图 5 所示辅助变换表成对的变换表和辅助变换表之一，对内容密钥数据进行解调。在这种情况下，将 16 位内容密钥数据解调为 8 位内容密钥数据。解调电路 36 将这样获得的内容密钥数据输出到纠错解码电路 37。

在步骤 S3，核对单元 40 判别是否利用图 4 所示的变换表对输入的加密内容密钥数据进行调制。在核对单元 40 判定采用与图 4 所示变换表成对的变换表时，则在步骤 S4，它将数据“1”输出到提取单元 41，而在核对单元 40 判定未采用图 4 所示变换表时，则在步骤 S5，它将数据“0”输出到提取单元 41。在控制单元 44 根据从子码提取单元 35 输入的地址数据判定已完成从密钥锁定区 1d、4d 读取数据时，

它断开开关 42，即使开关 42 断开以完成读出内容密钥数据，而在未完成读出数据时，控制单元 44 重复从步骤 S1 开始的处理过程。

在步骤 S7，在根据输入数据对内容密钥数据进行了加密时，收到对内容密钥数据进行调制时使用的变换表和辅助变换表的选择数据“1”或“0”的提取单元 41 提取随机数数据。提取单元 41 将随机数数据输出到纠错解码电路 43，然后纠错解码电路 43 对随机数数据进行纠错处理，以将纠错处理后的随机数数据输出到密码分析电路 38。

另一方面，在从解调电路 36 输入解调后的加密内容密钥数据时，纠错解码电路 37 对输入密钥数据进行纠错处理，并将它输出到密码分析电路 38。密码分析电路 38 根据从纠错解码电路 43 输入的随机数数据对从纠错解码电路 37 输入的内容密钥数据进行密码分析。为了能够对加密内容数据进行密码分析，密码分析电路 38 将经过密码分析的内容密钥数据保存或存储到设置在重放设备 30 内的存储器（未示出）内或控制单元 44 等的存储部分等内。

然后，在读出被加密之后记录到光盘 1 的节目区 1b 或光盘 2 的节目区 4b 的内容数据时，解调电路 36 根据常规规则利用图 4 所示的变换表对加密内容数据进行解调。纠错解码电路 37 对解调过的内容数据进行纠错处理，然后将它输入到密码分析电路 38。密码分析电路 38 利用经过密码分析的内容密钥数据对内容数据进行密码分析处理。密码分析电路 38 将解码后的内容数据输出到输出端 45。监视器和/或扬声器与输出端 45 相连。在经过密码分析的内容数据是图像时，将它显示在监视器上，而在该内容数据是音频数据时，从扬声器输出该音频数据。

如上所述，应用本发明的数据重放设备可以重放利用数据记录设备 10 将数据记录在其上的光盘 1、2。也就是说，数据重放设备 30 可以解调利用不同于对存储在密钥锁定区 1d、4d 内的内容数据进行调制处理的规则调制的内容密钥数据。在此，由于此数据重放设备 30 具有图 4 和图 5 所示的现有变换表和辅助变换表，因此还可以与传统光盘实现兼容。

在此，将对利用图 4 所示变换表或图 5 所示辅助变换表，根据随机数数据而非根据内容密钥数据对伪数据进行调制情况下的解调方法进行说明。

首先，在代码表号是随机数数据情况下，在控制单元 44 开始对光盘 1、2 上记录了伪数据的区域进行读出时，如图 8 所示，控制单元 44 使开关 42 处于接通状态。首先，在步骤 S11，将从光盘 1、2 读出的伪数据输入到核对单元 40。在步骤 S12，核对单元 40 提取在对伪数据进行调制过程中使用的图 4 所示或图 5 所示代码表号。在步骤 S13，将核对单元 40 提取的代码表号输入到提取单元 41。提取单元 41 根据代码表号产生对内容密钥数据的密码进行解码所需的随机数数据。提取单元 41 将产生的随机数数据输出到密码分析电路 38。另一方面，根据与对内容数据进行解调时使用的规则相同的规则，解调电路 36 对存储在密钥锁定区 1d、4d 内的内容密钥数据进行解调，而纠错解码电路 37 对此内容密钥数据进行纠错处理。密码分析电路 38 根据随机数数据对内容密钥数据的密码进行解码。密码分析电路 38 可以在以上述图 7 所示同样方式输入加密内容数据时，利用经过密码分析的内容密钥数据对内容数据进行密码分析，以从输出端 45 输出该内容数据。

此外，在利用偶数或奇数代码表号表示随机数数据情况下，在控制单元 44 开始对光盘 1、2 上记录了伪数据的区域进行读出时，如图 9 所示，控制单元 44 使开关 42 处于接通状态。首先，在步骤 S21，将 RF 信号从 RF 放大器 33 输入到核对单元 40，在步骤 S22，核对单元 40 提取在对伪数据进行调制过程中使用的图 4 所示或图 5 所示代码表号。在步骤 S23，提取单元 41 判别代码表号是偶数还是奇数。核对单元 40 以这样的方式运行，以便在代码表号是偶数时，它在步骤 S24 将数据“1”输出到提取单元 41，而在代码表号是奇数时，它在步骤 S25 将数据“0”输出到提取单元 41。控制单元 44 以这样的方式运行，以便在根据从子码提取单元 35 输入的地址数据判定已完成对光盘 1 或 2 上记录了伪数据的区域进行读出时，它使开关 42 转入断开状态以完成读出内容密钥数据，而在未完成读出数据时，重复从步骤 S21 开始

的处理过程。在步骤 S27, 在根据输入数据对内容密钥数据进行了加密时, 根据对代码表号是偶数还是奇数进行鉴别获得的结果而收到数据“1”或“0”的提取单元 41 提取随机数数据。提取单元 41 将随机数数据输出到纠错解码电路 43, 然后纠错解码电路 43 对输入的随机数数据进行纠错处理, 并将经过纠错处理的随机数数据输出到密码分析电路 38。另一方面, 根据对内容数据进行解调处理时采用的规则, 解调电路 36 对存储在密钥锁定区 1d、4d 内的内容密钥数据进行解调, 而纠错解码电路 37 对此内容密钥数据进行纠错处理。密码分析电路 38 根据随机数数据对内容密钥数据的密码进行解码。在输入加密内容数据时, 密码分析电路 38 利用经过密码分析的内容密钥数据对内容数据进行密码分析, 以从输出端 45 输出内容数据。

尽管以可记录光盘为例进行了说明, 但是本发明还可以应用于只重放光盘。根据本发明, 可以根据光盘类型, 即只重放光盘、只写一次光盘或重写光盘, 来改变进行调制处理的规则。尽管在上述例子中以 8-16 调制系统作为调制系统进行了说明, 但是除了上述调制系统之外, 还可以采用 8-10 调制系统等。尽管以用于加密内容数据的内容密钥数据作为主数据、而用于加密此内容密钥数据的随机数数据作为辅助数据为前提对上述例子进行了说明, 但是还可以采用例如使主数据作为内容数据, 而使辅助数据作为用于对内容数据进行加密的内容密钥数据的方法。

本发明还可以应用于将利用上述数据记录设备记录的数据发送到数据接收设备的发送设备。本发明还可以应用于接收并解调此数据发送设备发来的数据的数据接收设备。

工业应用性

本发明根据辅助数据选择变换表以对主数据进行调制。在进行重放时, 提取对主数据进行调制时使用的变换表作为数据, 以根据此数据产生主数据的辅助数据。因此, 允许现有设备重放主数据, 但是不允许它重放辅助数据。例如, 在使主数据作为内容数据, 并且在利用

作为辅助数据的加密密钥数据对此内容数据进行加密时，利用现有设备不可能获取此加密密钥数据，而且不可能利用现有设备重放此加密密钥数据。也就是说，只有利用正当设备才能对内容数据的密码进行解码从而重放这种内容数据。

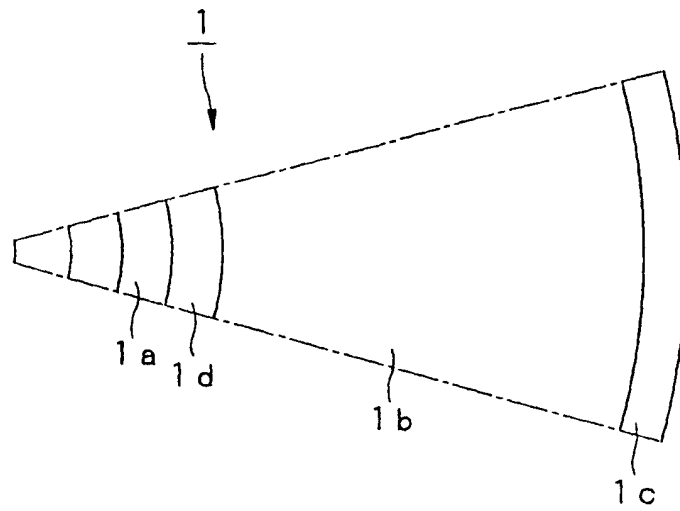


图1

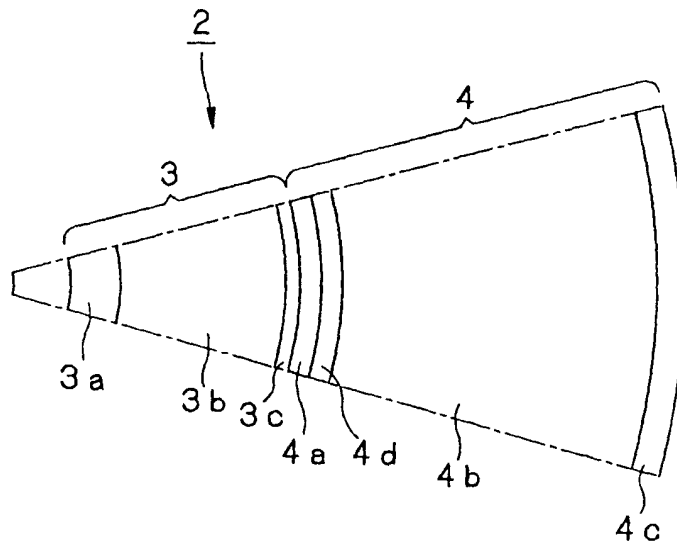


图2

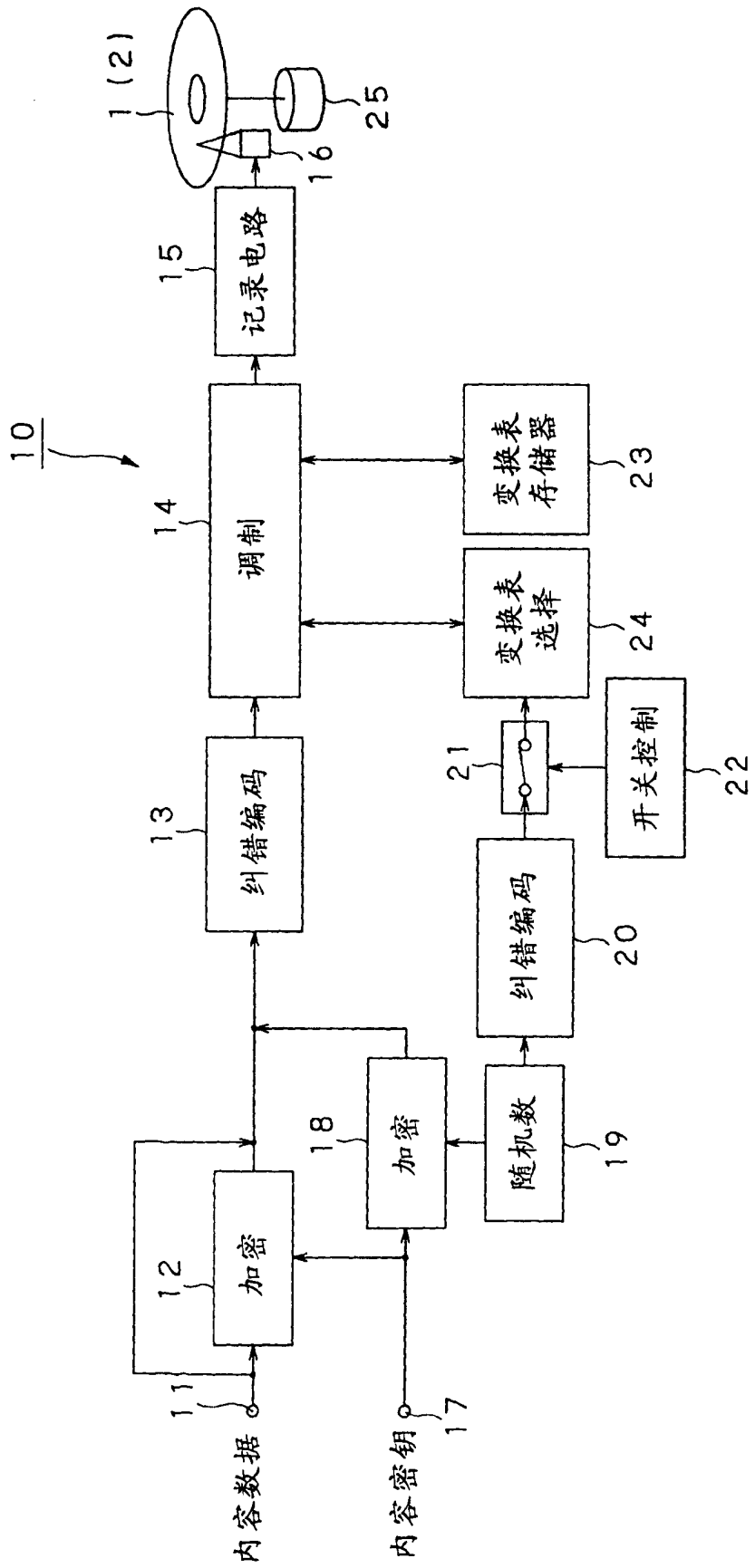


图3

8位输入数据 (代码号)	代码表1		代码表2		代码表3		代码表4	
	输出数据 (16位)	下一个 代码 表号	输出数据 (16位)	下一个 代码 表号	输出数据 (16位)	下一个 代码 表号	输出数据 (16位)	下一个 代码 表号
0	0010...	1	0100...	2	0010...	1	0100...	2
1	0010...	1	0010...	1	1000...	3	1000...	3
2	0010...	2	0010...	2	1000...	1	1000...	1
3	0010...	2	0100...	4	0010...	2	0100...	4
.
.
.
255

图4

8位输入数据 (代码号)	代码表1		代码表2		代码表3		代码表4	
	输出数据 (16位)	下一个 代码 表号	输出数据 (16位)	下一个 代码 表号	输出数据 (16位)	下一个 代码 表号	输出数据 (16位)	下一个 代码 表号
0	0000...	4	0000...	4	0100...	2	0100...	2
1	0000...	4	0000...	4	0100...	3	0100...	3
2	0001...	4	0001...	4	0100...	1	0100...	1
3	0000...	4	0100...	1	1000...	4	0100...	1
.
.
.
127

图5

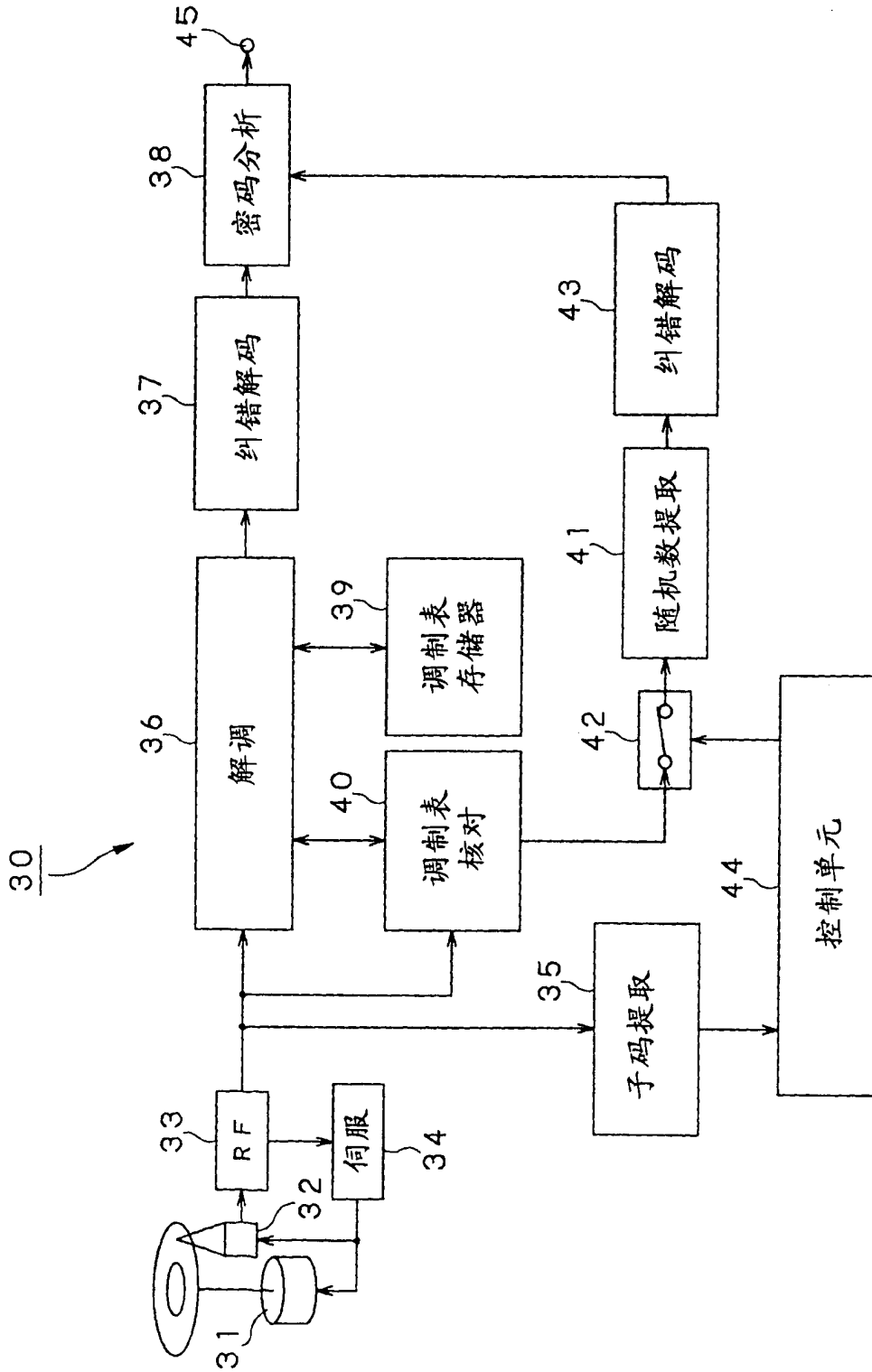
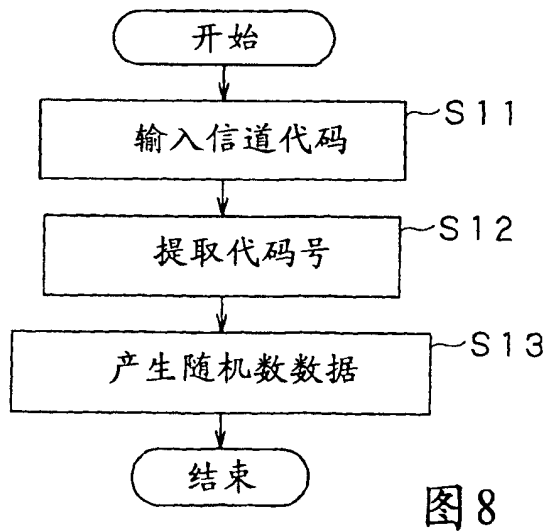
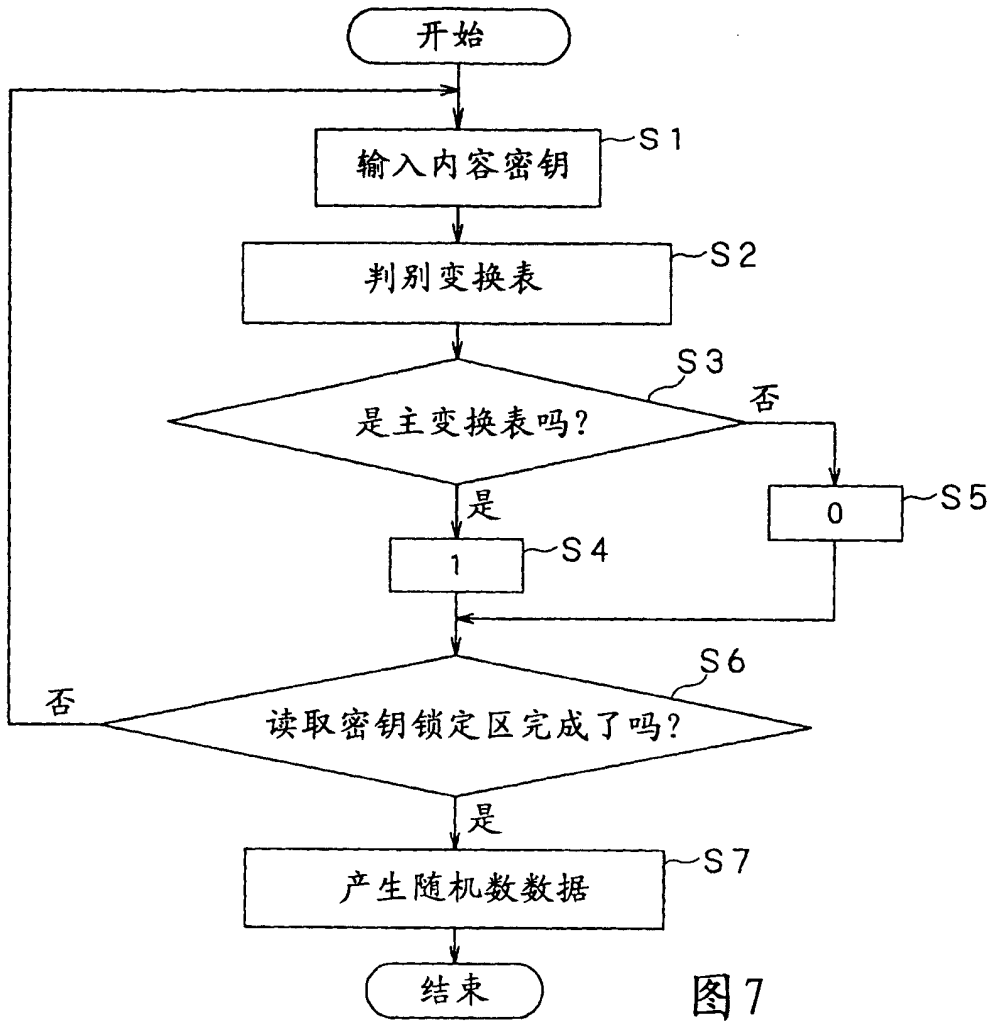


图6



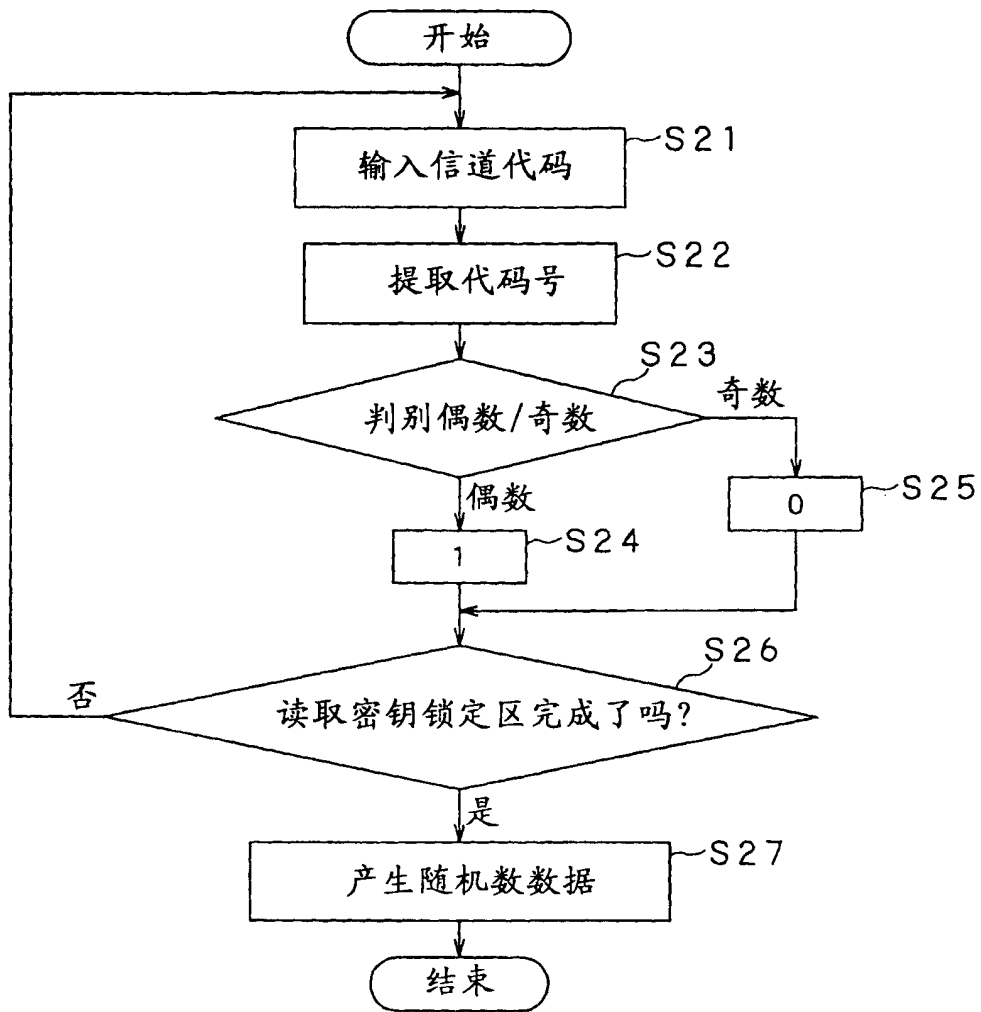


图9