

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 9/14 (2006.01)

H04L 9/28 (2006.01)

G11B 7/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 01122170.4

[45] 授权公告日 2006 年 8 月 2 日

[11] 授权公告号 CN 1268087C

[22] 申请日 2001.4.21 [21] 申请号 01122170.4

[30] 优先权

[32] 2000.4.21 [33] JP [31] 121636/00

[71] 专利权人 日本先锋公司

地址 日本东京都

[72] 发明人 吉田和幸 守山义明 黑田和男

铃木敏雄

审查员 史永良

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 梁 永

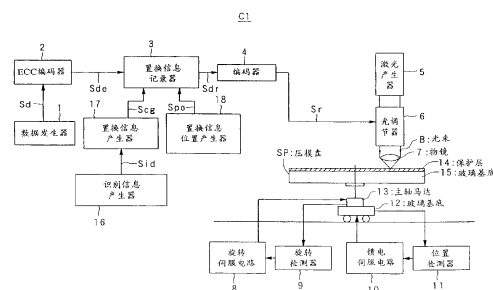
权利要求书 4 页 说明书 41 页 附图 12 页

[54] 发明名称

信息记录设备和方法

[57] 摘要

提供一种信息记录设备(C1, C2, R1, R2)等,即使记录信息(Sd)没有解码被非法地从一个信息记录介质(100)复制到另外一个信息记录介质(SP, 100)中,能够防止被非法复制的记录信息(Sd)被再现出。刻槽装置(C1)包括一个置换信息产生器(17),用来通过使用对每一个记录信息(Sd)将被记录在其中的DVD为唯一的识别信息(Sid)产生置换信息(Scg),一个置换信息记录器(3),用来通过使用置换信息(Scg)对部分记录信息(Sd)置换产生置换过的数据信号(Sdr),和一个光调节器(6),用来把产生的置换过的数据信号(Sdr)记录在相应于用来产生置换信息(Scg)的识别信息(Sid)的DVD中。



1.一种信息记录设备（C1，C2，R1，R2），其特征在于，这种信息记录设备（C1，C2，R1，R2）包括：

一个置换信息产生装置（17），通过使用对于记录信息（Sd）将被记录在其中的每一个信息记录介质（SP，100）为唯一的识别信息（Sid），用来产生置换信息（Scg）；

一个置换装置（3），通过使用已产生的置换信息（Scg）对部分记录信息（Sd）置换，用来产生置换过的记录信息（Sdr）；和

一个记录装置（6，50），用来记录已产生的置换过的记录信息（Sdr）到相应于用来产生置换信息（Scg）的识别信息（Sid）的信息记录介质（SP，100）中；

其中所述置换过的记录信息（Sdr）具有在错误纠正过程能够纠正的范围中的数据长度。

2. 根据权利要求 1 的信息记录设备，其特征在于所述置换过的记录信息（Sdr）的记录位置是预先设定的，且在所述信息记录设备和一个再现设备之间是被共用的。

3. 根据权利要求 1 的信息记录设备（C1，C2，R1，R2），其特征在于，该信息记录设备（C1，C2，R1，R2）还包括一个产生装置（76），通过使用预定的密钥信息（Sk），用来加密记录信息（Sd）来产生加密的记录信息（Sad），其中，置换装置（3）通过使用产生的置换记录信息（Sdr）对部分产生的加密记录信息（Sad）进行置换，产生置换过的记录信息（Sdr），并且记录装置（6，50）把密钥信息（Sk）和已产生的置换过的记录信息（Sdr）一起记录到相应于用来产生置换信息（Scg'）的识别信息（Sid）的信息记录介质（SP，100）中。

4. 根据权利要求 3 的信息记录设备（C1，C2，R1，R2），其特征在于，置换信息产生装置（17）产生包括密钥信息（Sk）的置换信息（Scg'）。

5. 根据权利要求 3 的信息记录设备（C1，C2，R1，R2），其特征在于，该信息记录设备（C1，C2，R1，R2）还包括一个密钥信息加密装置（75，95），用来通过使用识别信息（Sid）加密密钥信息（Sk）来产生加密的密钥信息（Sks），其中，记录装置（6，50）把已产生的加密的密钥信息（Sks）代替密钥信息（Sk）记录在信息记录介质（SP，100）中。

6. 根据权利要求 5 的信息记录设备（C1，C2，R1，R2），其特征在

于, 该信息记录设备 (C1, C2, R1, R2) 还包括一个识别信息加密装置 (75, 97, 98), 用来通过执行预定的加密过程, 加密识别信息 (Sid) 来产生已加密的识别信息 (Sfid, Sdid), 其中, 密钥信息加密装置 (75, 95) 通过使用已产生的加密识别信息 (Sfid, Sdid) 加密密钥信息 (Sk) 来产生加密过的密钥信息 (Skss, Sks)。

7. 根据权利要求 1 的信息记录设备 (C1, C2, R1, R2), 其特征在于, 置换信息产生装置 (17) 通过使用被加密的识别信息 (Sdid) 产生置换信息 (Scg'), 该被加密的识别信息 (Sdid) 是通过对识别信息 (Sid) 执行一个预定的加密过程获得的。

8. 根据权利要求 6 的信息记录设备 (C1, C2, R1, R2), 其特征在于, 该加密过程是一个通过使用一个预定的单向加密函数来加密识别信息 (Sid) 的过程。

9. 根据权利要求 1 的信息记录设备 (C1, C2, R1, R2), 其特征在于, 该信息记录设备 (C1, C2, R1, R2) 还包括一个加法器 (2), 用来对记录信息 (Sd) 增加一个用于错误校正的校正码 (31, 32), 来产生被增加的记录信息 (Sde), 其中, 置换装置 (3) 使用已产生的置换信息 (Scg) 对部分已增加的记录信息 (Sde) 进行置换, 来产生被置换的记录信息 (Sdr)。

10. 根据权利要求 1 的信息记录设备 (C1, C2, R1, R2), 其特征在于, 记录装置 (6, 50) 把用来产生置换信息 (Scg) 的识别信息, 与已产生的置换过的记录信息 (Sdr), 一起记录在相应于识别信息 (Sid) 的信息记录介质 (SP, 100) 中。

11. 根据权利要求 1 的信息记录设备 (C1, C2, R1, R2), 其特征在于, 识别信息 (Sid) 被预先被记录在相应的信息记录介质 (SP, 100) 上, 并且置换信息产生装置 (17) 检测该被记录的识别信息 (Sid), 使用它用来产生置换信息 (Scg)。

12. 根据权利要求 1 的信息记录设备 (C1, C2, R1, R2), 其特征在于, 所述置换过的记录信息 (Sdr) 的记录位置是基于所述识别信息 (Sid) 而被设置的。

13. 一种信息记录设备 (C1, C2, R1, R2), 其特征在于, 这种信息记录设备 (C1, C2, R1, R2) 包括:

一个产生装置 (76), 通过使用预定的密钥信息 (Sk), 用来对被记

录在信息记录介质 (SP, 100) 中的记录信息 (Sd) 加密, 来产生加密的记录信息 (Sad);

一个加密密钥信息产生装置 (75, 95), 通过使用对每一个信息记录介质 (SP, 100) 是唯一的被记录在信息记录介质 (SP, 100) 上的识别信息 (Sid, Sfid), 用来加密密钥信息 (Sk), 来产生加密密钥信息 (Sks, Skss); 和

一个记录装置 (6, 50), 用来把已产生的加密记录信息 (Sad) 和产生的加密密钥信息 (Sks, Skss), 记录在相应于用来产生加密密钥信息 (Sks, Skss) 的识别信息 (Sid, Sfid) 的信息记录介质 (SP, 100) 中;

其中所述加密密钥信息 (Sks, Skss) 具有在错误纠正过程能够纠正的范围中的数据长度。

14. 根据权利要求 13 的信息记录设备, 其特征在于所述加密密钥信息 (Sks, Skss) 的记录位置是预先设定的, 且在所述信息记录设备和一个再现设备之间是被共用的。

15. 根据权利要求 13 的信息记录设备 (C1, C2, R1, R2), 其特征在于, 该信息记录设备 (C1, C2, R1, R2) 还包括一个置换装置 (3), 使用已产生的加密密钥信息 (Sks, Skss) 对部分产生的加密记录信息 (Sad) 置换, 来产生置换过的记录信息 (Sdr), 其中, 记录装置 (6, 50) 把已产生的置换过的记录信息 (Sdr) 记录在相应于用来产生加密密钥信息 (Sks, Skss) 的识别信息 (Sid, Sfid) 的信息记录介质 (SP, 100) 中。

16. 一种信息记录方法, 其特征在于该信息记录方法包括:

一个产生步骤, 通过使用一个预定的密钥信息 (Sk), 加密将要被记录在信息记录介质 (SP, 100) 中的记录信息 (Sd) 来产生加密过的记录信息 (Sad);

25 一个加密密钥信息产生步骤, 通过使用被记录在信息记录介质 (SP, 100) 中对每一个信息记录介质 (SP, 100) 是唯一的识别信息 (Sid), 加密密钥信息 (Sk) 来产生加密密钥信息 (Sks, Skss); 和

一个记录步骤, 把产生的加密记录信息 (Sad) 和产生的加密密钥信息 (Sks, Skss), 记录在相应于用来产生加密密钥信息 (Sks, Skss) 的识别信息 (Sid, Sfid) 的信息记录介质 (100) 中;

其中所述加密密钥信息 (Sks, Skss) 具有在错误纠正过程能够纠正的范围中的数据长度。

17. 根据权利要求 16 的信息记录方法, 其特征在于所述加密密钥信息 (Sks, Skss) 的记录位置是预先设定的, 且在所述信息记录设备和一个再现设备之间是被共用的。

信息记录设备和方法

5 技术领域

本发明涉及一种包括信息记录设备，记录信息的方法，信息再现设备，再现信息的方法，和信息记录介质的技术领域。特别地，本发明涉及一种技术领域，其包括用来把这种信息例如图象信息记录到例如光盘的信息记录介质上的设备和方法，信息记录介质，其上包含着被这种设备例如信息记录设备记录的信息，用来从信息记录介质上再现被记录的信息的方法，和记录在介质上的程序信息，它包含用于记录信息或以计算机能读取的方式再现信息的控制程序。

背景技术

通常，视频信息，例如电影和例如音乐插曲的音频信息，常常受版权保护。在这种情况下，作为一个原则，未经授权复制信息和再现未授权的复制信息是被法律所不允许的。

对版权的所有者，必须采取措施，有效地防止未授权的复制和再现信息。

作为用来防止未经授权复制的传统的措施，有时使用这种方法，即用来限制视频信息的复制次数的控制信息被叠加到视频信息上，并且控制信息与视频信息被记录在记录介质中。用这种方法，当视频信息被播放和复制时，基于控制信息，复制被控制来防止未经授权的复制。

这里将给出关于这种方法的更详细的描述，其中控制信息用来防止未经授权的复制。例如，信息，诸如视频信息，与指示被授权仅复制一次的控制信息一起被记录在信息记录介质上。那么，当被记录的视频信息等被播放和复制到另一个信息记录介质上时，指示被授权仅复制一次的控制信息被改变成另外一种表明没有更多的复制被授权的控制信息。那么，这种被改变的控制信息被叠加到被记录到另一个记录介质上的视频信息等等之上。用这种安排，即使试图从另一信息记录介质中读取视频信息等，和把它复制到其它的记录介质上，由于指示复制被禁止的控制信息被叠加在信息上，不能从另一个记录介质象其它的记录介质上复制信息。

然而，根据上面的所述的方法，其中使用控制信息来防止未经授权的

复制，假如进行非法的从一个包括控制信息的信息记录介质向另一个信息记录介质上的复制，导致视频和其它信息象被记录一样被复制，即没有解码视频信息等，存在未经授权的复制不能被有效地禁止的情况。换句话说，假如信息当作 RF（无线电频率）格式信号被复制，控制信息也被象记录一样被复制，即它指示能授权复制一次，因此，有可能进行从另一个信息记录介质到其它记录介质的另一个复制。这样，不能有效地禁止未经授权的复制。

发明内容

本发明是在考虑到上面所述情况下作出的，因此本发明的一个目的是提供一种用来把视频信息等记录到信息记录介质上的设备和方法，即使由于视频信息没有被解码，被非法地从信息记录介质复制到另一个信息记录介质上，能够防止非法复制的视频信息在另一个信息记录介质上被再现。本发明的另外一个目的是提供一种信息记录介质，在其中利用这种设备记录视频信息等信息。本发明的其它目的是提供一种用来从信息记录介质中再现视频信息等的设备和方法，和一种程序信息记录介质，其中包含一种能被计算机识别的用于信息记录或信息再现的控制信息。

本发明的上述目的能通过本发明的一种信息记录设备实现。所述信息记录设备包括：一个置换信息产生装置，通过使用对于记录信息将被记录在其中的每一个信息记录介质为唯一的识别信息，用来产生置换信息；一个置换装置，通过使用已产生的置换信息对部分记录信息置换，用来产生置换过的记录信息；和一个记录装置，用来记录已产生的置换过的记录信息到相应于用来产生置换信息的识别信息的信息记录介质中；其中所述置换过的记录信息具有在错误纠正过程能够纠正的范围中的数据长度。

根据本发明，将被记录在信息记录介质中的被置换过的记录信息，相对信息记录介质的每一个识别信息是变化的。结果，记录在信息记录介质中的被置换过的记录信息，在每一个信息记录介质中是变化的。因此，在再现已被置换过的记录信息的时候，当被记录在信息记录介质中的被置换过的记录信息与对应于其中记录着已置换过的记录信息的信息记录介质的识别信息相比较时，仅仅假如这两种信息完全地彼此相关，允许再现。结果，当记录信息被非法地复制的时候，由于识别信息不能完全地与已被置换过的记录信息相关，有可能防止被非法复制的记录信息被再现出。

因此，即使记录信息被非法地从一个信息记录介质复制到另外一个信

息记录介质中，此时它没有解码被记录到信息记录介质上，在另一个信息记录介质中，由于识别信息和已置换过的记录信息之间不完全一致，能够防止被非法复制的记录信息被再现出。

在本发明的信息记录设备的一方面，一个产生装置通过使用预定的密钥信息加密记录信息来产生已加密的记录信息。那么，置换装置通过用已产生的置换信息置换已产生的加密过的部分记录信息，从而产生置换过的记录信息。另外，记录装置把密钥信息和已产生的置换过的记录信息一起记录到相应于用来产生置换信息的识别信息的信息记录介质中。

根据这一方面，由于记录信息被加密，能够更有效地防止非法复制的记录信息被再现出。

在本发明的信息记录设备的另一方面，置换信息产生装置产生包括密钥信息的置换信息。

根据这方面，在再现的时候读取密钥信息变得更困难，并且再现非法复制的记录信息变得更加困难。

在本发明的信息记录设备的另一方面，一个密钥信息加密装置通过使用识别信息加密密钥信息来产生已加密的密钥信息。然后，记录装置把已产生的加密过的密钥信息代替密钥信息记录在信息记录介质中。

根据这方面，在再现的时候，非法读取密钥信息和解码记录信息能被防止。

在本发明的信息记录设备的另一方面，一个识别信息加密装置，通过执行预定的加密过程来加密识别信息从而产生已加密过的识别信息。然后，密钥信息加密装置通过使用所产生的加密过的识别信息加密密钥信息从而产生加密过的密钥信息。

根据这方面，在再现的时候，有可能使得非法获得对于解码记录信息必须的密钥信息变得困难。

在本发明的信息记录设备的另一方面，置换信息产生装置通过使用被加密的识别信息产生置换信息，该被加密的识别信息是通过识别信息进行一个预定的加密处理过程获得的。

根据这个方面，在再现的时候，能够使得非法地获得与置换记录信息相比所必须的识别信息是困难的。

在本发明的信息记录设备的另一个方面，加密过程是通过使用一个预定的单向加密函数来加密识别信息的过程。

根据这方面，在再现的时候获得识别信息可能变得更困难。

在本发明信息记录设备的另一个方面，一个加法器载记录信息中增加一个用于错误校正的校正码，来产生被附加的记录信息。置换装置用已产生的置换信息来置换部分已增加的记录信息，来产生被置换的记录信息。

5 根据这方面，在再现的时候，记录信息能被准确地再现出。

在本发明的信息记录设备的另一方面，记录装置把用来产生置换信息的识别信息，与已产生的被置换过的记录信息一起记录在相应于识别信息的记录介质中。

10 根据这方面，在再现的时候，通过比较与被置换过的记录信息一起被记录的识别信息和这个特殊的被置换过的记录信息的内容，只有被授权者能够再现被置换的记录信息。

在本发明的信息记录介质的另一个方面，识别信息被预先被记录在相应的信息记录介质上。那么，置换信息产生装置检测这个被记录的识别信息，使用它用来产生置换信息。

15 根据这个方面，在再现的时候，通过比较预先被记录的识别信息和被置换的记录信息的内容，只有被授权者能够再现被置换的记录信息。

在本发明的信息记录设备的另一个方面，所述置换过的记录信息的记录位置是基于所述识别信息而被设置的。

20 根据这个方面，由于置换模式通过识别信息被改变，再现被非法复制的记录信息变得更加困难。

上面的本发明的目的能够通过本发明的一种信息记录设备实现。该信息记录设备设有：一个产生装置，通过使用预定的密钥信息，用来对被记录在信息记录介质中的记录信息加密，来产生加密的记录信息；一个加密密钥信息产生装置，通过使用对每一个信息记录介质是唯一的被记录在信息记录介质上的识别信息，用来加密密钥信息，来产生加密密钥信息；和
25 一个记录装置，用来把已产生的加密记录信息和产生的加密密钥信息，记录在相应于用来产生加密密钥信息的识别信息的信息记录介质中；其中所述置换过的记录信息具有在错误纠正过程能够纠正的范围中的数据长度。

30 根据本发明的信息记录设备，被加密的密钥信息，在每一个信息记录介质中以唯一不同的模式，被记录在信息记录介质中。这样，必须通过使用识别信息对加密过的密钥信息进行解密，并且通过使用加密过的密钥信息进行加密过的记录信息的解密。于是记录信息被再现。其结果，除非识

别信息和加密的密钥信息完全地彼此相关，否则记录信息不能被解密和再
现出。由于当记录信息被非法复制的时候，识别信息不能与置换过的记录
信息完全相关，因此，能够防止非法复制的记录信息被再现。

5 因此，即使由于没有被解码被记录在信息记录介质中的记录信息被非
法地复制到另一个信息记录介质中，由于在识别信息和加密过的密钥信息
之间不完全地相关，用来解密已加密的记录信息的必须的密钥信息不能被
获得，并且能够防止非法复制的记录信息被再现。

10 在本发明的信息记录设备的一个方面，一个置换装置，用已产生的加
密过的密钥信息来置换所产生的加密过部分的记录信息，从而产生置换过
的记录信息，其中，记录装置把已产生的置换过的记录信息记录在相应于
用来产生加密过密钥信息的识别信息的信息记录介质中。

根据这方面，由于部分加密记录信息被提供加密过的密钥信息，在再
现的时候，获得加密过的密钥信息可能变得困难。

15 本发明的上面目的通过本发明的一种信息记录介质能够实现。这种信
息记录介质设置有：一个信息记录区域，用来记录置换过的记录信息，该
置换过的记录信息通过对部分记录信息用置换信息置换获得，该置换信息
通过使用对每一个其中将被记录记录信息的信息记录介质而言是唯一的识
别信息来产生；和一个识别信息记录区域，其中记录了相应于信息记录介
质的识别信息。

20 根据本发明的信息记录介质，将被记录的置换过的记录信息，随着每
一个相应于信息记录介质的识别信息变化。其结果，将被记录的置换过的
记录信息在每一个信息记录介质中是变化的。这样，当置换过的记录信息
与其中记录置换过的记录信息的信息记录介质中的相应识别信息比较的时
候，只有这两个信息完全地彼此相关的时候，再现被允许。其结果，当记
25 录信息被非法复制的时候，由于识别信息不能完全地与替换过的记录信息
相关，能够防止被非法复制的记录信息被再现。

因此，即使当被记录在信息记录介质中没有被解码，被非法复制到另
一个信息记录介质中的记录信息，由于在识别信息和置换过的记录信息之
间不完全一致，能够防止非法复制的记录信息被再现。

30 在本发明的信息记录介质的一个方面，被记录在信息记录区域中的信
息是通过用已产生的置换信息置换部分加密的记录信息所获得的被置换过
的记录信息，已加密的记录信息是通过使用预定的密钥信息对记录信息加

密获得的。

根据这方面，由于记录信息被加密，能够进一步防止非法复制的记录信息被再现。

本发明的上面目的能通过本发明的一种信息记录介质实现。这种信息记录介质设置有：（i）一个信息记录区域，用来记录已加密的记录信息，已加密的记录信息是通过使用预定的密钥信息和加密过的密钥信息对将被记录在信息记录介质中的记录信息加密来获得，该加密过的密钥信息是通过使用对于每一个信息记录介质为唯一的识别信息，加密密钥信息获得的。（ii）一个识别信息记录区域，相应于信息记录介质的识别信息被记录在其中。

根据本发明的信息记录介质，被记录在信息记录介质中的加密过的密钥信息是以在每一个不同的信息记录介质中不同的唯一的模式进行的。这样，通过使用识别信息，必须进行加密过的密钥信息的解密，和通过使用加密过的密钥信息，必须进行加密过的记录信息的解密。于是，记录信息被再现。结果，除非识别信息和加密过的密钥信息完全地彼此相关，记录信息才能被解密和再现。因此，由于当记录信息被非法复制的时候，识别信息与置换过的记录信息不完全地相关，能够防止被非法复制的记录信息被再现。

因此，即使当被记录在信息记录介质中没有被解码，被非法复制到另一个信息记录介质中的记录信息，由于在识别信息和加密过的密钥信息之间不存在适当的相关性，所以用来解密加密过的记录信息的必须的密钥信息不能获得，能够防止非法复制的记录信息被再现。

本发明的上面的目的能够通过本发明的一种信息再现设备实现。这种信息再现设备从一个信息记录介质中再现信息，该信息记录介质中，置换过的记录信息和相应于这个信息记录介质的识别信息被记录在其中，该置换过的记录信息是通过用置换信息置换部分记录信息获得的，该置换信息是通过使用对每一个信息记录介质为唯一的识别信息产生的。这种再现设备设置有：一个检测装置，用来从信息记录介质中检测置换过的记录信息；一个识别信息检测装置，用于从信息记录介质中检测识别信息；一个置换信息提取装置，用来从检测到的置换过的记录信息中提取置换信息；一个识别信息提取装置，用来从已提取的置换信息中提取识别信息；一个比较装置，用来把从置换信息中提取的识别信息与从信息记录介质中检测出的

识别信息比较；和一个再现装置，只有从置换信息中提取的识别信息与从信息记录介质中检测到的识别信息相互匹配，能用来再现从检测到的置换过的记录信息中获得的记录信息。

根据本发明的信息再现设备，被记录在信息记录介质中的置换过的记录信息随着相应于信息记录介质的每一个识别信息而变化。其结果，在每一个信息记录介质中的置换过的记录信息是变化的。此外，只有检测到的置换过的记录信息与检测到的识别信息是一样的，才能执行再现。因此，当记录非法复制的记录信息的时候，由于识别信息与置换过的记录信息不相同，能够防止非法复制的记录信息被再现出。

因此，即使当没有被解码的情况下记录信息被记录在信息记录介质中时这个记录信息被非法复制到另外一个信息记录介质中，当在另一个信息记录介质上的记录信息被再现的时候，由于在这时在识别信息和置换过的记录信息不完全地相一致，能够防止非法复制的记录信息被再现。

在本发明信息记录设备的一个方面，置换过的记录信息通过用已产生的置换信息置换部分加密过的记录信息所获得的，加密过的记录信息通过使用预定的密钥信息加密记录信息获得。于是，密钥信息和已获得的置换过的记录信息被记录在相应于用来产生置换信息的识别信息的信息记录介质中。另外，信息记录设备还包括一个密钥信息检测装置，用来检测从信息记录介质中检测密钥信息。于是，再现装置解密加密过的记录信息，加密过的记录信息是通过使用检测到的密钥信息从检测到的已置换过的记录信息中获得的，并且只有从置换信息中提取的识别信息与从信息记录介质中检测到的识别信息相匹配时，再现记录信息。

根据这方面，由于记录信息被加密记录，并且它的再现是通过使用检测到的密钥信息执行的，所以能够进一步防止非法复制的记录信息被再现。

在本发明的信息记录设备的另一个方面，密钥信息被包含在置换信息中并被记录在信息记录介质中，并且密钥信息检测装置从被提取的置换信息中检测密钥信息。

根据这方面，在再现的时候获得密钥信息变得更加困难。因此，解密和再现非法复制的加密过的记录信息变得更加困难。

在本发明的信息记录设备的另一个方面，通过使用识别信息对密钥信息的加密获得加密过的密钥信息，代替密钥信息被记录在信息记录介质

中。于是，密钥信息检测装置从信息记录介质中检测加密过的密钥信息。

另外，信息再现装置还包括用来产生密钥信息的密钥信息产生装置，产生
5 密钥信息是通过使用检测到的识别信息对检测到的已加密的密钥信息进行
解密来获得的。于是，再现装置解密通过使用已产生的密钥信息从检测到
的置换过的记录中获得的已加密过的记录信息，并且只有从置换信息中提
取的识别信息与从信息记录介质中检测到识别信息相互匹配的时候，再现
这些记录信息。

根据这个方面，能够防止读取解密已加密的记录信息和它的解码所必
要的密钥信息。

10 在本发明的信息再现设备的另一个方面，已加密的密钥信息通过使用
已加密的识别信息对密钥信息的加密获得的，加密过的识别信息信息是对
识别信息进行预定的加密过程获得的，并且加密过的密钥信息被记录在信
息记录介质中。于是，通过使用从对检测到的识别信息进行加密过程获得
的加密过的识别信息，密钥信息产生装置解密检测到的加密过的密钥信
15 息。

根据这个方面，在再现的时候，非法地获得解码记录信息必须的密钥
信息变得更加困难。

在本发明的信息再现设备的另一个方面，通过使用预定的单向加密函
数的加密过程加密信息。

20 根据这个方面，非法地获得对解密加密过的密钥信息必须的加密过的
识别信息有可能变得更加困难。

在本发明的信息再现设备的另一个方面，非法地获得识别信息能变得
更加困难，该识别信息将要与从信息记录介质中检测到的识别信息相比
较。

25 根据这方面，非法地获得用于与从信息记录介质中检测到的识别信息
比较的必须的识别信息能变得困难。

在本发明的信息再现设备的一个方面，通过使用加密过的识别信息产
生置换信息，该加密过的识别信息通过一个预定的加密过程使用一个预定
的单向加密函数进行对识别信息的处理获得的，该识别信息相应于其中将
30 要记录置换过的记录信息的信息记录介质。另外，该信息再现设备还包括：
一个加密过的识别信息提取装置，用来从提取的置换信息中提取加密过的
识别信息；和一个加密识别信息产生装置，通过使用对检测到的识别信息

执行的加密函数的加密过程，用来产生第二个加密过的识别信息。于是，只有产生的第二个加密识别信息与提取的加密识别信息相匹配时，再现装置才能再现记录信息。

根据这个发明，由于只有被提取的加密识别信息与第二加密识别信息完全相同时，才能执行记录信息的再现，能够防止非法复制的记录信息被再现。

在本发明的信息再现设备的另一个方面，通过用已产生的置换信息置换部分更多的记录信息从而产生被置换过的记录信息，该附加记录信息通过对记录信息附加用来错误校正的校正码产生的，并且该置换过的记录信息被记录在信息记录介质中。于是，在进行错误校正之前，置换信息提取装置从置换过的记录信息中提取置换信息。另外，信息再现设备还包括一个校正装置，通过使用校正码，对检测到的置换过的记录信息进行错误校正过程。

根据这个方面，能够准确地校正错误和再现记录信息。

在本发明的信息再现设备的另一个方面，在置换过的记录信息中使用识别信息的置换模式是随着使用置换信息变化的。于是，置换信息提取装置通过使用检测到的识别信息，基于置换的特定的模式，从检测到的置换过的记录信息中提取置换信息。

根据这方面，由于对每一个识别信息置换模式是不同的，并且必须通过使用识别信息来识别置换的模式以便于能够再现，因此能够使得再现非法复制的记录信息更加困难。

本发明的上面目的能够通过本发明的一种信息再现设备来实现。该信息再现设备从信息记录介质中再现信息，在信息记录介质中记录了对每一个信息记录介质是唯一的识别信息，记录了通过对记录信息的加密获得的加密记录信息将要通过使用预定的密钥信息，并且记录了通过使用识别信息对密钥信息的加密获得的加密密钥信息。这种信息再现设备设置有：一个检测装置，用来从信息记录介质中检测加密过的记录信息和加密过的密钥信息；一个识别信息检测装置，用来从信息记录介质中检测识别信息；一个密钥信息产生装置，用来通过使用检测到的识别信息解密检测到的加密密钥信息来产生密钥信息；和一个再现装置，用来通过使用产生的密钥信息解密检测到的加密过的记录信息来再现记录信息。

根据本发明的信息再现设备，加密过的密钥信息对每一个信息记录介

质以唯一不同的方式被记录在信息记录介质中。另外，加密过的密钥信息必须通过使用检测到的识别信息解密，并且加密过的记录信息必须通过使用解密的密钥信息来解密。这样，除非识别信息与加密过的密钥信息完全相关，密钥信息才能被获得。结果，记录信息不能被解密和再现。因此，
5 由于识别信息与置换过的记录信息不完全相关，能够防止非法复制的记录信息被再现。

因此，即使当记录信息没有被解码记录在信息记录介质时记录信息被非法复制到另一个信息记录介质中，由于在识别信息和加密过的密钥信息之间不完全一致，对解密加密过的记录信息必须的密钥信息不能获得。结果，
10 能够防止非法复制的记录信息被再现。

在本发明的信息再现设备的另一个方面，通过用产生的加密过的密钥信息置换部分产生的加密过的记录信息从而产生的置换过的记录信息被记录在信息记录介质中。于是，检测装置从信息记录介质中检测置换过的记录信息。另外，信息再现设备还包括一个密钥信息提取装置，用来从检测
15 到的置换过的记录信息中提取加密过的密钥信息。

根据这个方面，获得加密过的密钥信息变得更加困难，并能防止防止非法复制的加密过的记录信息被解密和再现。

本发明的上面的目的能够通过本发明的一种信息记录方法来实现。这种信息记录方法包括有：一个置换信息产生步骤，通过使用对每一个记录
20 信息被记录在其中的信息记录介质唯一的识别信息产生置换信息；一个置换步骤，通过用已产生的置换过信息置换部分记录信息置换来产生的记录信息；和一个记录步骤，把产生的置换过的记录信息记录到相应于用来产生置换信息的识别信息的信息记录介质中。

根据本发明的信息记录方法，将被记录在信息记录介质中的置换过的
25 记录信息对相应于信息记录介质的每一个识别信息是变化的。结果，被记录在信息记录介质中的置换过的记录信息随着每一个信息记录介质变化。这样，在再现置换过的记录信息的时候，当被记录在信息记录介质中的置换过的记录信息与识别信息比较，该识别信息相应于其中被记录着置换过的记录信息的信息记录介质，只有这两种信息彼此完全地相关，才能允许
30 再现。结果，当记录信息被非法复制的时候，由于识别信息与置换过的记录信息不能完全地相关，能够防止非法复制的记录信息被再现。

因此，即使当记录信息被记录在信息记录介质中的时候没有被解码，

记录信息被从信息记录介质非法复制到另一个信息记录介质中，在另一个信息记录介质中，由于在识别信息与置换过的记录信息之间不完全一致，能够防止非法复制的记录信息被再现。

在本发明的信息记录方法的一个方面，一个产生步骤，通过使用预定的
5 的密钥信息加密记录信息来产生加密的记录信息。然后，置换步骤通过用产生的置换信息置换产生的加密过的部分记录信息来产生置换过的记录信息。另外，记录步骤把密钥信息与产生的置换过的记录信息一起记录到相应于用来产生置换信息的识别信息的信息记录介质中。

根据这个方面，由于记录信息被加密，能够更有效地防止非法复制的
10 记录信息被再现。

本发明的上面目的能够通过本发明的一种信息记录方法来实现。这种信息记录方法包括：一个产生步骤，通过使用一个预定的密钥信息，加密将要被记录在信息记录介质中的记录信息来产生加密过的记录信息；一个加密过的密钥信息产生步骤，通过使用被记录在信息记录介质中对每一个
15 信息记录介质是唯一的识别信息，加密密钥信息来产生加密过的密钥信息；和一个记录步骤，把产生的加密过的记录信息和产生的加密过的密钥信息，记录在信息记录介质中，该信息记录介质对应于用来产生加密密钥信息的识别信息；其中所述加密密钥信息具有在错误纠正过程能够纠正的范围中的数据长度。

根据本发明的信息记录方法，加密过的密钥信息以在每一个信息记录
20 介质中唯一不同的模式被记录在信息记录介质中。这样，必须通过使用识别信息进行加密密钥信息的解密，并且解密加密过的记录信息必须通过使用解密的密钥信息进行。然后记录信息被再现。结果，除非识别信息与解密的密钥信息彼此完全相关，记录信息才能被解密和再现。因此，当记录
25 信息被非法复制的时候，由于识别信息与置换过的记录信息不完全地相关，能够防止非法复制的记录信息被再现。

因此，即使当记录信息被记录在信息记录介质中的时候没有被解码，记录信息被非法地复制，在另一个信息记录介质中，由于在识别信息和加密过的密钥信息之间不完全一致，对解密加密的记录信息必须的密钥信息
30 不能被获得，并且能够防止非法复制的记录信息被再现。

本发明的上面目的能够通过本发明的一种信息再现方法实现。在这种信息再现方法中，信息被从一个信息记录介质中再现，置换过的记录信息

和相应于信息记录介质的识别信息被记录在该信息记录介质中，置换过的记录信息是通过对部分记录信息置换通过使用对每一个信息记录介质为唯一的识别信息产生的置换信息获得的。这种信息再现方法包括有：一个从信息记录介质中检测置换过的记录信息的检测步骤；一个识别信息检测步骤，从信息记录介质中检测识别信息；一个置换信息提取步骤，从检测到的置换过的记录信息中提取置换信息；一个识别信息提取步骤，从提取置换信息中提取识别信息；一个比较步骤，把从置换信息中提取的识别信息与从信息记录介质中检测到的识别信息相比较；和一个再现步骤，只有从置换信息中提取的识别信息与从信息记录介质中检测到的识别信息相匹配时，再现从检测到的置换过的记录信息中获得的记录信息。

根据本发明的信息再现方法，记录在信息记录介质中的置换过的记录信息依据相对于信息记录介质的每一个识别信息是变化的。结果，在每一个信息记录介质中置换过的记录信息是变化的。此外，只有检测到的置换过的记录信息与检测到的识别信息相一致时，再现能被执行。因此，当非法复制记录信息的时候，由于识别信息与置换过的记录信息是不一致的，能够防止非法复制的记录信息被再现。

因此，即使当记录信息被记录在信息记录介质中的时候没有被解码，记录信息被非法地复制，在另一个信息记录介质中，当在另一个信息记录介质中的记录信息被再现的时候，由于在此时识别信息和置换过的记录信息不完全一致，能够防止非法复制的记录信息被再现。

在本发明的信息再现方法的一个方面，置换过的记录信息通过用已产生的置换信息置换部分加密的记录信息获得，加密过的记录信息是通过使用预定密钥信息加密记录信息获得的。于是，密钥信息和获得的置换过的记录信息被记录在信息记录介质中，该信息记录介质相应于用来产生置换信息的识别信息。此外，信息再现方法还包括一个密钥信息检测步骤，从信息记录介质中检测密钥信息。于是，再现步骤解密通过使用检测到的密钥信息从检测到置换过的记录信息中获得的加密记录信息，和只有从置换信息中提取的识别信息与从信息记录介质中检测到的识别信息相匹配时，再现记录信息。

根据这方面，由于记录信息被加密记录并通过使用检测到的密钥信息执行它的再现，能够进一步防止非法复制的记录信息被再现。

本发明的上面目的能够通过本发明的信息再现方法来实现。在这种信

息再现方法中，信息被从一种信息记录介质中再现，在该信息记录介质中记录了对每一个信息记录介质是唯一的识别信息，记录了通过使用预定的密钥信息，通过对将要被记录在其中的记录信息加密获得的加密记录信息，和记录了通过使用识别信息，通过对密钥信息加密获得的加密密钥信息。这种信息再现方法包括有：一个检测步骤，从信息记录介质中检测加密的记录信息和加密的密钥信息；一个识别信息检测步骤，从信息记录介质中检测识别信息；一个密钥信息产生步骤，通过使用检测到的识别信息解密检测到的加密的密钥信息来产生密钥信息；和一个再现步骤，通过使用产生的密钥信息解密检测到的加密的记录信息来再现记录信息。

根据本发明的信息再现方法，加密的密钥信息以对每一个信息记录介质唯一不同的方式被记录在信息记录介质中。另外，加密的密钥信息必须通过使用检测到的识别信息被解密，并且加密的记录信息必须通过使用解密的密钥信息被解密。这样，除非识别信息与加密的密钥信息完全地相关，密钥信息能被获得。结果，记录信息不能被解密和再现。因此，由于识别信息与置换过的记录信息不完全地相关，能够防止非法复制的记录信息被再现。

因此，即使当记录信息被记录在信息记录介质中的时候没有被解码，记录信息被非法地复制，在另一个信息记录介质中，由于在识别信息和加密的密钥信息之间不完全一致，对解密加密的记录信息必须的密钥信息不能获得。结果，能够防止非法复制的记录信息被再现。

本发明的上面目的能够通过本发明的一种程序信息记录介质实现。在该程序信息记录介质中，一个信息记录控制程序通过一个包括在用来记录信息的信息记录设备中的计算机被可读取地记录到信息记录介质中，该信息记录控制程序促使计算机起到信息记录控制装置的作用。这种信息记录控制装置包括有：一个置换信息产生装置，通过使用对其中要被记录记录信息的每一个信息记录介质为唯一的识别信息，用来产生置换信息；一个置换装置，通过用已产生的置换信息对部分记录信息置换从而产生置换过的记录信息；和一个记录装置，把已经产生的置换过的记录信息记录在信息记录介质中，该信息记录介质相应于用来产生置换信息的识别信息。

根据本发明的程序信息记录介质，当计算机读取被记录在程序信息记录介质中的程序的时候，记录信息的记录步骤被执行。因此，将要被记录在信息记录介质中的置换过的记录信息随着每一个相应于信息记录介质的

识别信息是变化的。结果，被记录在信息记录介质中的置换过的记录信息随着每一个信息记录介质而变化。这样，在再现置换过的记录信息的时候，当被记录在信息记录介质中的置换过的记录信息与相应于其中记录着置换过的记录信息的信息记录介质的识别信息相互比较的时候，只有这两种信息彼此完全地相关，再现被允许。结果，当记录信息被非法复制的时候，由于识别信息与置换过的记录信息不完全地相关，能够防止非法复制的记录信息被再现。

因此，即使当记录信息被记录在信息记录介质上的时候没有被解码，记录信息被从这个信息记录介质非法地复制到另一个信息记录介质上，在另一个信息记录介质中，由于在识别信息和置换过的记录信息之间不完全地一致，能够防止非法复制的记录信息被再现。

在本发明的程序信息记录介质的一个方面，信息记录控制程序促使计算机起到信息记录控制装置的作用，信息记录控制装置还设置有一个产生装置，用来通过使用预定的密钥信息加密记录信息来产生加密过的记录信息。于是，计算机起到置换装置的作用，通过用产生的置换信息对部分产生的加密的记录信息置换产生置换过的记录信息，并且这个记录装置把密钥信息与产生的置换过的记录信息一起记录到信息记录介质中，该信息记录介质相应于用来产生置换信息的识别信息。

根据本发明的程序信息记录介质，当计算机读取记录在程序信息记录介质中的程序的时候，记录信息的记录步骤被执行。结果，由于记录信息被加密，能够更有效地防止非法复制的记录信息被再现。

本发明的上面目的能够通过本发明的一种程序信息记录介质实现。在这种程序信息记录介质中，一个信息记录控制程序通过一个包括在用来记录信息的信息记录设备中的计算机被可读取地记录到信息记录介质中，该信息记录控制程序促使计算机起到信息记录控制装置的作用。这种信息记录控制装置包括有：一个产生装置，用来通过使用预定的密钥信息加密将要被记录在信息记录介质中的记录信息来产生加密的记录信息；一个加密过的密钥信息产生装置，通过使用被记录在信息记录介质中的对每一个信息记录介质为唯一的识别信息，用来加密密钥信息来产生加密过的密钥信息；和记录装置，用来把产生的加密过的记录信息和产生的加密过的密钥信息，记录到相应于用来产生加密过的密钥信息的识别信息的信息记录介质中。

根据本发明的程序信息记录介质，当计算机读取被记录在程序信息记录介质中的程序的时候，记录信息的记录步骤被执行。结果，加密过的密钥信息以对每一个信息记录介质唯一不同的方式被记录在信息记录介质中。于是，加密的密钥信息的解密必须通过使用识别信息被进行，并且加密的记录信息的解密必须通过使用解密的密钥信息进行。于是记录信息被再现。结果，只有识别信息与加密的密钥信息完全地彼此相关时，记录信息才能被解密和再现。因此，当记录信息被非法复制的时候，由于识别信息与置换过的记录信息不完全地相关，能够防止非法复制的记录信息被再现。

因此，即使当记录信息被记录在信息记录介质中的时候没有被解码，记录信息被非法复制在另一个信息记录介质中，由于在识别信息与加密过的密钥信息之间不完全地一致，不能获得解密加密的记录信息所必须的密钥信息，并能够防止非法复制的记录信息被再现。

本发明的上面的目的能够通过本发明的程序信息记录介质来实现。在这种程序信息记录介质中，一个信息再现控制程序通过一个包括在用来从一个信息记录介质中再现信息的信息再现设备中的计算机被可读取地记录，该信息记录介质中，置换过的记录信息和识别信息被记录在其中，该置换过的记录信息是通过使用通过使用对每一个信息记录介质为唯一的识别信息产生的置换信息对部分记录信息置换获得的，该识别信息相应于该信息记录介质，这种信息再现控制程序促使计算机起到信息再现控制装置的作用。这种信息再现控制装置包括有：一个检测装置，用来从信息记录介质中检测置换过的记录信息；一个识别信息检测装置，用来从信息记录介质中检测识别信息；一个置换信息提取装置，用来从检测到的置换过的记录信息中提取置换信息；一个识别信息提取装置，用来从提取出的置换信息中提取识别信息；一个比较装置，用来把从置换信息中提取的识别信息与从信息记录介质中检测到的识别信息相互比较；和一个再现装置，只有从置换信息中提取的识别信息与从信息记录介质中检测到的识别信息相互匹配时，用来再现从检测到的置换过的记录信息中获得的记录信息。

根据本发明的程序信息记录介质，当计算机读取被记录在程序信息记录介质中的程序的时候，记录信息的再现步骤被执行。结果，被记录在信息记录介质中的置换过的记录信息随相应于信息记录介质的识别信息是变化的。结果，置换过的记录信息随着每一个信息记录介质是变化的。另外，

只有检测到的置换过的记录信息与检测到的识别信息是一致时，再现才被执行。因此，当非法复制的记录信息记录的时候，由于识别信息与置换过的记录信息不一致，能够防止非法复制的记录信息被再现。

因此，即使当记录信息被记录在信息记录介质中的时候没有被解码，
5 记录信息被非法地复制，在另外一个信息记录介质中，当在另外一个信息记录介质中的记录信息被再现的时候，由于识别信息与置换过的记录信息之间不完全地一致，能够防止非法复制的记录信息被再现。

在本发明的程序信息记录介质的一个方面，置换过的记录信息通过使用产生的置换信息对部分加密的记录信息置换获得，加密的记录信息是通过使用预定的密钥信息对记录信息加密获得的。于是，密钥信息和获得的置换过的记录信息被记录在信息记录介质中，该信息记录介质相应于用来产生置换信息的识别信息。此外，信息再现控制程序促使计算机起到信息再现控制装置的作用，这种信息再现控制装置还设置有一个密钥信息检测装置，用来从信息记录介质中检测密钥信息。于是，再现装置解密加密的
10 记录信息并且只有从置换信息中提取的识别信息与从信息记录介质中检测到的识别信息相互匹配时再现该记录信息，该加密的记录信息是通过使用检测到的密钥信息从检测到的置换过的记录信息中获得的。

根据这个方面，当计算机读取被记录在程序记录介质中的程序时候，该记录信息的再现步骤被执行。结果，由于记录信息被加密记录并且它的
20 再现通过使用检测到的密钥信息来执行，能够进一步防止非法复制的记录信息被再现。

本发明的上面目的能够通过本发明的一种程序信息记录介质实现。在这种程序信息记录介质中，一个信息再现控制程序通过一个包含在用来从一个信息记录介质中再现信息的信息再现设备中的计算机被可读取地记录，该信息记录介质中，置换过的记录信息和识别信息被记录在其中，该置换过的记录信息是通过使用通过使用对每一个信息记录介质为唯一的识别信息产生的置换信息对部分记录信息置换获得的，该识别信息相应于该信息记录介质，这种信息再现控制程序促使计算机起到信息再现控制装置的作用。这种信息再现控制装置包括有：一个检测装置，用来从信息记录
25 介质中检测加密过的记录信息和加密过的密钥信息；一个识别信息检测装置，用来从信息记录介质中检测识别信息；一个密钥信息产生装置，用来通过使用检测到的识别信息解密检测到的加密过的密钥信息来产生密钥信

息；和一个再现装置，用来通过使用产生的密钥信息解密检测到的加密过的记录信息来再现记录信息。

根据本发明的程序信息记录介质，当计算机读取被记录在程序信息记录介质中的程序的时候，记录信息的再现步骤被执行。结果，加密的密钥信息以对每一个信息记录介质唯一不同的方式被记录在信息记录介质中。另外，加密的密钥信息必须通过使用检测到的识别信息被解密，并且加密过的记录信息必须通过使用解密的密钥信息被解密。这样，除非识别信息与加密的密钥信息完全相关，密钥信息才能被获得。结果，记录信息不能被解密和再现。因此，由于识别信息与置换过的记录信息不完全地相关，能够防止非法复制的记录信息被再现。

因此，即使当记录信息被记录在信息记录介质中的时候没有被解码，记录信息被非法地复制，在另一个信息记录介质中，由于在识别信息和加密的密钥信息之间不完全地一致，不能获得解密加密的记录信息所必须的密钥信息。结果，能够防止非法复制的记录信息被再现。

附图说明

图 1 是显示本发明的第一个实施例的刻录装置 (cutting apparatus) 概要结构的方框图；

图 2 是显示第一个实施例的刻录装置 (cutting apparatus) 的流程图；

图 3A 是显示根据第一个实施例的数据扇区结构图；

图 3B 是显示根据第一个实施例的 ECC 块结构图；

图 4 是显示根据第一个实施例的在置换信息被插入之后 ECC 块结构图；

图 5 是显示根据第一个实施例的数据物理结构图；

图 6 是显示根据第一个实施例的信息记录设备的概要结构的方框图；

图 7 是显示根据第一个实施例的信息再现设备的概要结构的方框图；

图 8 是显示根据第一个实施例的再现操作的流程图；

图 9 是显示根据本发明的第二个实施例的刻录装置 (cutting apparatus) 的概要结构的方框图；

图 10A 是显示根据第二个实施例的置换信息产生器的第一个例子的详细结构方框图；

图 10B 是显示根据第二个实施例的置换信息产生器的第二个例子的详细结构方框图；

图 10C 是显示根据第二个实施例的置换信息产生器的第三个例子的详细结构方框图；

图 10D 是显示根据第二个实施例的置换信息产生器的第四个例子的详细结构方框图；

5 图 10E 是显示根据第二个实施例的置换信息产生器的第五个例子的详细结构方框图；

图 11 是显示根据第二个实施例的信息记录设备的概要结构的方框图；

图 12 是显示根据第二个实施例的信息再现设备的方框图。

10 具体实施方式

下面，将参考附图详细描述本发明的最佳实施例。

这里应该注意到，下文中所描述的每一个实施例是本发明的一个应用，应用到一个包括一个刻录装置的防止非法复制的系统中，该刻录装置用来制造使用在 DVD 大规模生产中的压模盘。DVD 是能够存储比通常的
15 CD (compact disc) 7 倍容量还多的信息的一类光盘。这种刻录装置，换句话说，是用来制造只读 DVD 的装置。非法复制防止系统也包括一个用来向可记录 DVD 上记录信息的信息记录设备和一个用来从 DVD 上再现信息的信息再现设备。

(I) 非法复制防止系统的第一个实施例

20 根据本发明的防止非法复制系统的第一个实施例将参考图 1 到图 8 描述。

(A) 刻槽装置的第一个实施例

首先，根据防止非法复制系统的第一个实施例的刻槽装置的一个实施例将参考图 1 到图 5 描述。

25 将首先参考图 1 描述根据第一个实施例的刻槽装置的结构。

如图 1 所示，根据第一个实施例的刻槽装置 C1 包括：一个数据发生器 1；一个 ECC (错误纠正码) 编码器 2；一个用作置换装置的置换信息记录器 3；一个编码器 4；一个激光发生器 5；一个用作记录装置的光调制器 6；一个物镜 7；一个旋转伺服电路 8；一个旋转检测器 9；一个馈电伺
30 服电路 10；一个位置检测器 11；一个输送单元 12；一个主轴马达 13；一个识别信息产生器 16；一个用作置换信息产生装置的置换信息产生器 17；和一个置换信息位置产生器 18。

另一方面，压模盘 SP 包括保护层 14 和玻璃基底 15。保护层 14 暴露于后面将要描述的光线 B 中，并且根据光束 B 的强度改变在保护层中形成信息凹坑的相应图案。

下面，将大概描述概要操作。

- 5 首先，数据发生器 1 执行产生的数据扇区的处理过程，该数据扇区相应于被记录在 DVD 上的数据，例如图象信息，音频信息或者是要在计算机中被使用的数据，并且然后输出数据信号 Sd 到 ECC 编码器 2 中。

然后，ECC 编码器 2 形成用于包括在数据信号 Sd 中将被记录的数据的后面将描述的 ECC 块，并且输出附加的数据信号 Sde 到置换信息记录器 3 中。

- 10 置换信息记录器 3 用后面将描述的置换信息 Scg 置换包括在附加数据信号 Sde 中的 ECC 块部分，并产生置换过的数据信号 Sdr。置换信息 Scg 可以是或不是后面将描述的加密信息。

编码器 4 对包括在置换过的数据信号 Sdr 中的 ECC 块执行交错存取和 8-16 调制，并产生一记录数据信号 Sr。

- 15 识别信息产生器 16 产生对每一个将被记录记录数据信号 Sr 的 DVDs 为唯一的识别信息 Sid，并把它输出到置换信息产生器 17 中。换句话说，通过使用通过刻槽装置 C1 生产的压模盘 SP 大规模生产的每一个 DVDs 被给出了对于自己为唯一的识别信息。

- 20 置换信息产生器 17 执行一个预定的对识别信息 Sid 加密过程。具体地说，加密过程包括位倒置，位之间的转换，通过根据一个外部元件定义的规则变形，通过使用如后面第二个实施例中描述的一个单向的加密函数变形。置换信息产生器 17 也产生对每一个 DVDs 为唯一的置换信息 Scg 并且输出它到置换信息记录器 3 中。

- 25 假如置换信息 Scg 被插入到 ECC 块中，置换信息 Scg 的数据长度（二进制数字的个数）被设置成其中错误纠正能够在错误纠正过程中被执行的一定的范围内，，当信息被再现的时候，对 ECC 块执行错误纠正过程。

- 30 置换信息位置产生器 18 产生位置信息 Spo，位置信息 Spo 指示着其中将产生的置换信息 Scg 的每一个位插入到包括在附加的数据信号 Sde 每一个 ECC 块中的位置，并且输出它到置换信息记录器 3 中。置换信息位置产生器 18 基于一个插入表产生位置信息 Spo，该插入表是一个预定的插入表，与后面将描

述的信息再现装置 S1 共同被使用。

用上面的布置，置换信息记录器 3 把来自置换信息 Scg 每一位的位信息插入到被位置信息 Spo 指示的 ECC 块中的位置上，并产生置换过的数据信号 Sdr。换句话说，置换信息记录器 3 用位信息置换存在于每一个插入位置的信息。

- 5 激光产生器 5 发射光束 B 到压模盘 SP 上形成对 DVD 所必须的信息凹坑。
 于是，通过使用记录数据信号 Sr，光调节器 6 执行来自激光产生器 5 的光束 B 的强度调节。

物镜 7 聚焦调节过的光束 B 在压模盘 SP 的保护层 14 上。

此时，主轴马达 13 旋转压模盘 SP。

- 10 旋转检测器 9 检测压模盘 SP 的旋转圈数。

用上面的安排，旋转伺服电路 8 基于检测到的旋转圈数控制压模盘 SP 的旋转。

为了在压模盘 SP 上形成由单线信息凹坑构成的螺旋轨道，输送单元 12 根据压模盘 SP 的旋转在压模盘 SP 的半径方向上移动主轴马达 13 和压模盘 SP。

- 15 位置检测器 11 检测输送单元 12 的位置。

于是，输送伺服电路 10 基于检测到的输送单元 12 的位置，执行输送单元 12 的伺服控制。

- 根据上述操作，相应于记录数据信号 Sr 的信息凹坑以螺旋轨道方式形成在压模盘 SP 的保护层 14 上，并且作为用来制造 DVDs 的模盘的压模盘 SP 完
20 成了。

此后，通过使用完成的压模盘 SP，一个称为复制过程包括树脂形成，反射膜形成，保护层形成等等被执行，所以，每一个具有相应于记录数据信号 Sr 的信息凹坑的作为复制盘的 DVDs 被大规模生产。

- 这里应该注意到，在 DVDs 的大规模生产过程中，在压模盘 SP 的制造之前或之后，另一个与包括在置换信息 Scg 中的识别信息 Sid 相同的识别信息 Sid
25 作为例如条形码被记录在每一个 DVDs 的不同于预留的 DVD 数据区域中，例如光盘的最内侧半径区域。

- 这样一来，每一个制造的 DVDs 使得识别信息 Sid 作为记录数据信号 Sr 被记录在预留的数据区域，并且例如条形码形式的相同的识别信息 Sid 被记录
30 在它的最内侧半径区域。另外，每一个制造的 DVDs 有对于它自己为唯一的特

定识别信息 Sid, 区别于任何其它的 DVD 的识别信息。

下面, 将参考图 1 到图 5 描述根据本发明的产生记录数据信号 Sr 的详细操作。图 2 是显示该操作的流程图。图 3 到图 5 是显示根据本发明产生的数据 (包括在记录信号 Sr 中的数据) 的结构。

5 当记录数据信号 Sr 产生在第一个实施例的刻槽装置 C1 中的时候, 首先, 将被记录的原始数据的结构被改变成包括称作数据扇区的大量信息单元的结构。

明确地, 如图 2 所示, 将被记录的原始数据被分成每一个具有 2048 字节的几段。对每一段, 一个指示数据扇区的开始位置的 ID 数据, 和用来校正 ID
10 数据中的错误的 ID 数据校正码 (IEC) 被附加 (S1 步)。

下面, 准备数据和用来检测在分开的 2048 字节数据段中的错误的错误检测码 (EDC) 被附加到在 S1 步中产生的每一个数据中。这完成了一数据扇区的构成 (S2 步)。

现在, 将描述数据扇区的特定结构。如图 3A 所示, 数据扇区 20 开始为 ID
15 数据 21, 接着为 ID 数据校正码 22, 准备数据 23, 由分开的原始数据创造的数据段 24, 和错误检测码 25。数据扇区 20 的图案重复以形成由多个数据扇区组成的连续的环, 构成将被记录的数据。

在数据扇区 20 形成后, 通过使用预定的密钥数据对数据 24 进行加密调制 (S3 步)。

20 上面所描述的从 S1 步到 S3 步的过程在数据产生器 1 中执行, 并且上面提到的包括已经进行加密调制的数据 24 的数据信号 Sd 被输出。用来加密的密钥数据与图像信息等一起被记录作为数据 24。

下面, ECC 编码器 2 用包括在数据信号 Sd 中的数据扇区 20 产生 ECC 块。ECC 块是基于记录在 DVD 上的数据的再现所执行的错误校正过程中的一个校正单位。于是, 包括 ECC 块的附加的数据信号 Sde 被输入到置换信息记录器 3
25 中 (S4 步)。

这里将更详细地描述 ECC 块的产生过程。如图 3B 所示, 数据扇区 20 被分成每一个包含 172 字节的块。于是, 每一个被分的数据块 (下文中称为数据块 33) 在垂直方向上被连续地配置 (看图 3B 的左边图表), 用这种安排, 12
30 行数据块 33 被放置在垂直方向上。

于是，对于放置在垂直方向上的每一个数据块 33，一个 ECC 内码 31（也被称为 PI（奇偶校验）码，并是用来校正正在 ECC 块中的单侧行中的数据的错误校正码）被加到相应的数据块 33 的末端，以形成校正块 34（看图 3B 的右边图表）。因此在这点，具有 ECC 内码 31 的 12 行校正块 34 的每一行排列在垂直方向上。此后，对于 16 个数据扇区重复这个过程。因此，获得整个 192 行校正块 34。

下面，用 192 行排列在垂直方向上的校正块 34，在从块头的每一个字节，于是 192 行校正块 34 被分成垂直数据行。于是，对于获得的每一个垂直数据行，16 个 ECC 外码 32（也称 PO（奇偶校验）码，是用来校正正在 ECC 块中的一个单垂直行中数据的错误校正码）被附加。ECC 外码 32 也被加到校正块 34 的 ECC 内码 31 部分。

上面所述过程的结果，如图 3B 的右侧图所示，形成一个包括 16 个数据扇区 20 的一个 ECC 块 30，这样，包括 ECC 块 30 的附加的数据 Sde 被输出到置换信息记录器 3 中。

在此时，包括在一 ECC 块 30 中的总信息数量按如下给出：

$$(172+10) \text{ 字节} \times (192+6) \text{ 行} = 37856 \text{ 字节}$$

其中，实际的数据 24 的数量按如下给出：

$$2048 \text{ 字节} \times 16 = 32768 \text{ 字节}$$

应该注意到，显示在图 3B 的右侧图中的 ECC 块 30 中，数据的一个字节显示为“Dm.n”。例如，“D1.0”是放置在 1 行，零列的 1 字节数据。同样地，“D190.170”是放置在 190 行，170 列的 1 字节数据。这样，ECC 内码 31 被放置在 172 列到 181 列，而 ECC 外码 32 被放置在 192 列到 207 列。

另外，校正块 34 作为一个连续的环境被记录在 DVD 上（压模盘 SP）。

如图 3B 的右侧图所示，ECC 块 30 由包括 ECC 内码 31 和 ECC 外码 32 二者构成。因为这种安排，在水平方向排列在图 3B 的右侧图中的数据的校正能够通过使用 ECC 内码 31 进行，而在垂直方向排列在图 3B 的右侧图中的数据的校正能够通过使用 ECC 外码 32 进行。

特别地，根据显示在图 3B 的右侧图中的 ECC 块 30，错误校正能够在水平方向和垂直方向双重地进行。这导致比用在传统的 CD 等的先前技术中的错误校正程序更强的错误校正能力。

关于这一点将给出更详细的描述。例如，即使错误校正块 34（它是一行整个 182 字节连续的数据，包括用于该行以及如上所述被连续地记录在 DVD 上的 ECC 内码，由于例如 DVD 上的擦伤被整个破坏，当该块在垂直方向被观看时，损害表现为每一列 ECC 外码 32 仅仅丢失一个字节。因此，当通过使用
5 每一列中的 ECC 外码 32 进行错误校正的时候，即使一个校正块 34 的全部被破坏，仍然能够实现正确的错误校正，并且因此能够执行准确地重放。

下面，置换信息记录器 3 用置换信息 Scg 置换数据，该数据包括在如上所述产生的 ECC 块 30 中在被位置信息 Spo 指示的位置上（S5 步）。

这里将参考图 4 描述该置换过程。通过作为位于置换信息 Scg 每一位中的
10 数据的置换信息 35 来置换部分一字节数据，该一字节数据的一部分是位于由上述对应于位置信息 Spo 的插入表所指示的 ECC 块 30 中的每一个位置。如上面所述，插入表通常与后面将要描述的信息再现装置 S1 一起使用。

在 S5 步中写入置换信息 35 之后，由包括置换信息 35 的 ECC 块 30 构成的置换过的数据信号 Sdr 被输出到编码器 4 中。

15 下面，编码器 4 对包括在置换过的数据信号 Sdr 中的 ECC 块 30 执行交错和 8-16 调制，并且输出该记录数据信号 Sr（S6 和 S7 步）。

在 S6 和 S7 步中执行的过程将参考图 5 被详细地描述。显示在图 5 中的“Dm.n”格式的数据相应于显示在图 3B 的右侧表中的数据。

首先，在 S6 步中当对 ECC 块 30' 执行交错的时候，首先，如图 5 中的最
20 上面所示，ECC 块 30' 被排列成一连续的连接校正块 34 的水平串。于是，在一预定的规则下通过重新排列数据串执行交错。结果，在 ECC 块 30' 中的信息被分成 16 个记录扇区 40。这个时候，每一个记录扇区 40 包括 2366 字节（37856 字节被 16 除）的信息，它是数据扇区 20 和 ECC 内码或 ECC 外码 31 和识别信息 35 的混合。然而，数据扇区 20 的 ID 数据 21（看图 3A）被放置在每一个
25 记录扇区 40 的报头。

每一个记录扇区 40 被分成若干个 91 字节的数据段 41，并且每一个数据段被给一个头 H。据此，在这种状态下，通过对记录扇区 40 执行 8-16 调制，对每一个数据段 41 形成一个同步帧 42。在这一点，每一个同步帧 42 由一个标题 H' 和一个数据 43 构成。在每一个同步帧 42 中的信息量按如下给出：

30 $91 \text{ 字节} \times 8 \times (16/8) = 1456 \text{ 字节}$

用上述布置，写在 DVD 中的信息采用同步帧 42 连续的字符串格式，在其中每一个记录扇区 40 包含 26 个同步帧 42。

由于向 DVD（压模盘 SP）中数据记录的执行按上面所述的形式进行，原始 ECC 块 30'能够通过执行 8-16 解码和反交错再现（看图 5）。如上所述，通过有力的错误校正，信息能够被准确地再现。

(B) 信息记录装置的第一个实施例

下面，将参考图 6 描述根据第一个实施例的信息记录装置的一个实施例。

在图 6 中，与显示在图 1 中的刻槽装置执行相同功能的部件将用相同的数字标号标明，并且将不再详细地描述。

首先，将描述根据第一个实施例的信息记录装置的构成。

如图 6 所示，与刻槽装置 C1 相似，根据第一个实施例的信息记录装置 R1 包括，一个数据产生器 1，一个 ECC 编码器 2，一个置换信息记录器 3，一个编码器 4，一个置换信息产生器 17，一个置换信息位置产生器 18，一个拾取器 50，一个主轴马达 51，一个伺服 IC（集成电路）52，一个系统控制器 53，和一个策略电路 54。

这里应该注意到，信息记录装置 R1 将用来记录的 DVD100 是一种可记录 DVD，例如 DVD-R（仅能记录一次的可记录的 DVD），DVD-RW（能记录多次的可记录的 DVD）等等。每一个 DVD100 有它唯一的预先记录在它的例如最内半径区域的识别信息 Sid，并且是以例如条形码的形式记录的。

下面，将描述每一个部件的操作。

首先，数据产生器 1，ECC 编码器 2，置换信息记录器 3，编码器 4，置换信息产生器 17，和置换信息位置产生器 18 与它们在上面所述的刻槽装置 C1 中以相同的方式操作，因此，包括 ECC 块 30'的产生记录数据信号 Sr 的格式上面已经描述，并且输出它到策略电路 54 中。

在此时，在开始记录前，置换信息产生器 17 通过使用从 DVD100 中检测到的识别信息 Sid 执行象在刻槽装置 C1 中相同的操作，并且产生置换信息 Scg。

另外，置换信息产生器 17 和置换信息位置产生器 18 的操作通过来自系统控制器 53 的控制信号 Sci 和 Ccp 被集中地控制。

接着，策略电路 54 执行所谓的策略过程，它是用来在后面所述的 DVD100 上形成清楚形状的信息凹坑，并且产生输出到拾取器 50 中去的记录信号 Srs。

于是，拾取器 50 基于记录信号 S_{rs} 控制记录光束 B 的强度，并且在形成在 DVD100 的数据区中的信息轨道上形成信息凹坑，从而把记录信号 S_{rs} 记录到 DVD100 上。在记录之前，然而，拾取器 50 从 DVD100 的记录位置检测识别信息 S_{id} 并且输出检测到的信息到置换信息产生器 17 中。

5 主轴马达 51 的旋转基于来自伺服 IC52 中的主轴控制信号 S_{ss} 被控制，通过主轴马达 51，以一个预定的旋转数旋转 DVD100。

一个拾取器 50 中的用来聚焦光束 B 的物镜，基于来自伺服 IC52 中的拾取控制信号 S_{sp} 在水平方向和垂直方向移动，结果在光束 B 的焦点和水平方向上 DVD100 上的信息轨道的位置之间的偏差被消除。

10 为了这个目的，除了控制信号 S_{ci} 和 S_{cp} ，系统控制器 53 产生控制信号 S_{cs} ，并且把它输出到伺服 IC52 中，结果伺服 IC52 输出主轴控制 S_{ss} 和拾取控制信号 S_{sp} 。

通过上述信息记录装置 R1 将被记录在 DVD100 中的记录数据信号 S_r 的物理数据结构与在刻槽装置 C1 中的相同。

15 与这些过程平行，系统控制器 53 通过产生上述的控制信号 S_{ci} ， S_{cs} 和 S_{cp} 控制上面提到的每一个部件的操作，并且同时执行信息记录装置 R1 的整体的控制过程。对控制过程必须的信息通过一个操作面板（未示出）从外部输入。

另外，信息记录装置 R1 的操作状态等被显示在例如液晶显示器的显示器中（未示出）。

20 通过上述的信息记录装置 R1 的操作，具有记录在它的最内侧半径区域中的识别信息 S_{id} （这种唯一的识别信息 S_{id} 在每一个 DVD100 中是不同的）的 DVD100，现在具有被记录在这种特定的 DVD100 的数据区中准确地带有相同的识别信息 S_{id} （或者这种被加密过的或其它方式被处理过的识别信息 S_{id} ）的记录数据信号 S_r 。

25 (C) 信息再现装置的第一个实施例

下面，参考图 7 和图 8，将描述用来再现被记录在 DVD 上的数据的信息再现装置的第一个实施例，该 DVD 是通过使用其数据是通过刻槽装置被记录的压模盘 SP 来制造的，或者是用来再现被记录在 DVD 上的数据，该 DVD 的数据是通过信息记录装置 R1 被记录的。

30 假如这种 DVD 具有包括图象信息和音频信息的记录数据，下文中描述的

信息再现装置是一种能够再现图像信息和音频信息的信息再现装置。

首先,参考图7描述根据第一个实施例的信息再现装置的构成。

如图7所示,根据第一个实施例的信息再现装置S1包括一个用作检测装置的拾取器60,一个识别信息检测装置和一个密钥信息检测装置,一个主轴马达61,一个RF(无线电频率)放大器62,一个解码器63,一个用作置换信息提取装置的置换信息提取器64,一个错误校正电路65,一个用作再现装置的输出控制器66,一个置换信息位置产生器67,一个用作识别信息提取装置的识别信息提取器68,一个用作比较装置的识别信息比较器69,一个系统控制器70和一个伺服IC71。

接着,描述其操作。

DVD100是一种通过使用上面所述的压模盘SP制造的DVD,或是一种包括通过信息记录装置R1记录的信息的DVD。这两种DVDs具有分别记录在其中的上面所述的唯一的识别信息Sid,在下文中简单地称之为DVD。这种基于来自伺服IC71的主轴控制信号Sssp控制其旋转的主轴马达61以一个预定的转速旋转DVD100。

拾取器60向旋转的DVD100上照射一种信息再现光束B,并且基于反射光,产生相应于形成在DVD100上的信息凹坑的检测信号Sp,并且输出产生的信号到RF放大器62中。

应该注意到,检测信号Sp包括识别信息Sid,该识别信息Sid被记录在例如DVD100的最内半径区域中,并且基于通过上面提到的照射光束B到光盘的最内半径区域获得的反射光将其检测。

一个在拾取器60中的物镜(未示出)基于来自伺服IC71中的拾取控制信号Sspp在水平和垂直方向移动,结果在水平方向上在光束B的焦点和DVD100上的信息轨道的位置之间的偏差被消除。

为了这个目的,系统控制器70产生一个控制信号Scsp,并且输出它到伺服IC71中,结果伺服IC71输出主轴控制信号Sssp和拾取控制信号Sspp。

下面,基于输入检测信号Sp,RF放大器62产生相应于被记录在DVD100中的数据的一种RF信号Srf,并且输出它到解码器63中。另外,实际上RF放大器62输出检测到的识别信息Sid到识别信息比较器69中。

于是,解码器63对RF信号执行反交错和8-16调制(看图5)来获得一

种包括 ECC 块 30' 的再现信号 Sdc，并且输出获得的信号到置换信息提取器 64 中。

下面，通过复制，置换信息提取器 64 从被后面将描述的位置信息 Sp0 指示的位置提取包括在再现信号 Sdc 中的 ECC 块 30' 中的插入的置换信息 Scg，
5 然后输出提取的信息到识别信息提取器 68 中，并在复制提取的置换信息 Scg 之后输出再现信号 Sdc 到错误校正电路 65 中。

在上述描述中，可转换地，在输出到错误校正电路 65 之前，置换信息提取器 64 不仅可以从再现信号 Sdc 中复制提取置换信息 Scg，而且可以在从其中置换信息 Scg 被包括的位置中的所有信息中提取置换信息 Scg 之后，置换零数
10 据。

与这些平行，置换信息位置产生器 67 基于来自系统控制器 70 的控制信号 Scpp，和通过利用与置换信息位置产生器 18 共享的插入表，对每一个 ECC 块 30'，产生位置信息 Sp0，位置信息 Sp0 指示着其中置换信息 Scg 被插进包括在再现信号 Sdc 中的相应的 Ecc 块 30' 中的位置，并且输出产生的信息到置换信息提取器 64 中。
15

于是，基于来自系统控制器 70 中的控制信号 Spu，识别信息提取器 68 执行一个解密过程，是与上面所述的置换信息产生器 17 中执行的加密过程相反的操作，并从输入的置换信息 Scg 中提取存储在 DVD100 的数据区域中的作为数据的识别信息 Sidp，并且输出提取到的信息到识别信息比较器 69 中。

只有从 RF 放大器 62 中输出的识别信息 Sid 与上面所述的识别信息 Sidp 相同时，识别信息比较器 69 产生一个许可信号 Sco，它允许从输出控制器 66 输出一个后面将要描述的输出信号 Sout，并且输出它到输出控制器 66 中。也就是说，只有被插进记录数据信号 Sr 中的识别信息 Sid 被发现与被记录在 DVD100 的例如最内半径区域中的识别信息 Sid 相一致时，识别信息比较器 69
20 产生一允许信号 Sco。

另一方面，错误校正电路 65 通过使用 ECC 内码 31 和 ECC 外码 32，对包括在输入的再现信号 Sdc（即在置换信息 Scg 的复制提取之后的 ECC 块 30'）中的 ECC 块 30' 执行错误校正过程，产生错误校正过的信号 Scr 和输出产生的信号到输出控制器 66。

只有允许信息 Sco 允许输出信号 Sout 的输出时，输出控制器输出错误校
30

正过的信号 Scr 作为输出信号 Sout 到外部显示器，扬声器等等。

与这些过程平行，系统控制器 70 产生控制信号 Scpp, Spu 和 Scsp, 并且控制上述部件的操作，并且同时执行信息再现装置 S1 的整个控制过程。控制过程必须的信息通过一个操作面板（未示出）从外部输入。

5 另外，信息再现装置 S1 的操作状态等载需要时可以显示在例如液晶显示器的显示部分。

如图 7 所示，输出控制器 66 可以选择地被放置在错误校正电路 65 之前而不是在错误校正电路 65 之后，使得输出信号 Sout 的输出在这个阶段能够根据允许信号 Sco 被控制。

10 接着，将参考图 7 和图 8 描述根据本发明的被记录在 DVD100 中的数据的数据的再现操作。图 8 是显示该再现操作的流程图。

如图 8 所示，在再现操作中，首先，光拾取器 60 发射信息再现光束 B 到旋转的 DVD100 上，并且通过使用反射光（S10 步）再现被记录在 DVD100 上的数据。此时，RF 放大器 62 产生 RF 信号 Srf 并且输出它到解码器 63 中。与
15 此同时，RF 放大器 62 也检测识别信息 Sid 并输出它到识别信息比较器 69 中。

接着，解码器 63 对 RF 信号 Srf 执行反交错和 8-16 解调(S11 步)，并且产生再现信号 Sdc。

在再现信号 Sdc 的这个阶段，从 DVD100 中检测到的数据包括作为反交错和 8-16 解调的结果的显示在图 4 中的大量的 ECC 块 30'。

20 接着，置换信息提取器 64 检测被存储在其中置换信息 35 被记录（看图 4）在包含在再现信号 Sdc 中的 ECC 块 30'中的区域中的数据，并且作为置换信息 Scg 输出它到识别信息提取器 68 中（S12 步）。

在此时，在 ECC 块 30'中包括置换信息 35 的 ECC 块 30'的区域的位置被位置信息 Spo 指示并被输入到置换信息提取器 64 中。因而，通过参考位置信
25 息 Spo 的内容，置换信息 Scg 被检测到。

另外，在从输入的再现信号 Sdc 中复制提取置换信息 Scg 之后，置换信息提取电路 64 输出该信息到错误校正电路 65 中。

于是，错误校正电路 65 通过使用存储在 ECC 块 30'中的 ECC 内码 31 和 ECC 外码 32 校正包括在再现信号 Sdc 中的错误，产生上面所述的校正过的错误信号 Scr 并且输出它到输出控制器 66 中。
30

应该注意到，错误校正信号 Scr 在被输出到输出控制器 66 之前进行一个非搅乱操作（13 步）。

接着，识别信息比较器 69 用识别信息 Sidp 比较识别信息 Sid（S14 步），并且只有两者被发现彼此相同时（S14 步；是），从输出控制器 66 中产生允许
5 后面将描述的输出信号 Sout 输出的允许信号 Sco，并且输出该输出信号 Sout 到外部（S15 步）。

在 ECC 块 30' 中的置换信息 35 被确认并因此在错误校正电路 65 中执行的错误校正中作为错误被校正，并且因此不被包括在被再现和输出的输出信号 Sout 中。

10 另一方面，假如在 S14 步确定两个识别信息 Sidp 和 Sid 彼此不相同（S14 步；否），于是这个过程转到结束而不执行输出过程，得出结论为被记录在 DVD100 中的数据不是授权的记录和因此是一个非法拷贝。

应该注意到，假如置换信息 Scg 包括通过使用一单向加密函数被加密的识别信息 Sid，在信息再现装置 S1 中的再现过程将如下所述。明确地，从 DVD100
15 中检测到的识别信息 Sid 通过使用加密函数被加密，并且提取的识别信息 Scg 被进一步处理成提取加密的识别信息 Sidp，并且这两个信息被比较。假如两者被发现一致，于是 S15 步和其它的再现程序被执行。

如上所述，根据第一个实施例的防止非法复制系统的操作，每一个 DVD100 有它的唯一的用来产生置换信息 Scg 的识别信息 Sid。另外，置换信息 Scg 为
20 部分附加的数据信号 Sde 被置换，从而记录数据信号 Sr 被产生记录在上面特殊的 DVD100 中，该 DVD100 具有特别用来产生上面特定的置换信息 Scg 的识别信息 Sid。因此，被记录在 DVD100 中的记录数据信号 Sr 由于被包括在 DVD100 中的每一个识别信息 Sid 而不同。结果，每一个 DVD100 的记录数据信号 Sr 不同。

25 另外，在再现记录数据信号 Sr 期间，一个在记录数据信号 Sr 中的识别信息 Sid 和另一个包括在识别信息 Sid 被记录在其中的 DVD100 中的识别信息 Sid 被彼此相互比较，只有二者彼此相互一致时，允许再现。因此，能够防止记录数据信号 Sr 的非法拷贝被再现。即，假如记录数据信号 Sr 的复制以这样一种方式进行，即特定被给予 DVD100 的识别信息 Sid 与被存储在记录数据信号 Sr
30 中的识别信息 Sid 不一致，记录数据信号 Sr 不被再现。

另外，由于在 ECC 块 30 中的置换信息 Scg 被插入的位置在每一个 ECC 块 30 中变化的，这能够使得再现记录数据信号 Sr 的非法拷贝变得更加困难。

应该注意到，根据上面所述第一个实施例，通过对识别信息 Sid 执行预定的加密过程，在写置换信息 Scg 的时候产生置换信息 Scg。然而可转换地，识别信息 Sid 本身可以作为置换信息 Scg，不执行任何加密处理，被写进 ECC 块中。

根据上面的安排，当信息被再现的时候，能除去解密过程，并且识别信息 Sid 能够容易地被获得。

(II) 非法复制防止系统的第二个实施例

首先，将参考附图 9 到 12 描述根据本发明的非法复制防止系统的第二个实施例。

根据上面所述的第一个实施例，将被记录在 DVD100 中的记录数据信号 Sr 通过对部分 ECC 块 30 置换置换信息 Scg 产生，置换信息 Scg 包括着对每一个 DVD 为唯一的识别信息 Sid。另外，当记录数据信号 Sr 被再现的时候，通过把被存储在记录数据 Sr 中的识别信息 Sid 与作为这个特定的 DVD100 的唯一代码的从 DVD100 中分别检测到的识别信息 Sid 相比较，得出在合法拷贝和非法拷贝之间的差别。根据下文中将描述的第二个实施例，置换信息 Scg 本身，包括识别信息 Sid，被进一步加密到高级，并且同时，作为被记录在 DVD100 中的原始数据的数据信号 Sd 本身，通过使用密钥信息也被进一步加密到高级。

(A) 刻槽装置的第二个实施例

首先，将参考图 9 和图 10 描述根据第二个实施例的刻槽装置。

在图 9 中，与在第一个实施例的刻槽装置 C1 中的执行同样功能的部件将用相同的数字代码标明，并且将不再详细地描述。

如图 9 所示，与根据第一个实施例的刻槽装置 C1 相似，根据第二个实施例的刻槽装置 C2 包括，一个数据产生器 1，一个 ECC 编码器 2，一个置换信息记录器 3，一个编码器 4，一个激光产生器 5，一个光调节器 6，一个物镜 7，一个旋转伺服电路 8，一个旋转检测器 9，一个馈电伺服电路 10，一个位置检测器 11，一个输送单元 12，一个主轴马达 13，一个识别信息产生器 16，并且另外包括一个用作密钥信息加密装置和识别信息加密装置的置换信息产生器 75，一个用作产生装置的数据加密器 76，置换信息位置产生器 77，和一个密

钥信息产生器 78。

接着，将概要描述其操作。

首先，密钥信息产生器 78 产生密钥信息 Sk 并且输出它到数据加密器 76 中和置换信息产生器 75 中。密钥信息 Sk 是通过后面将描述的预定的加密方法
5 用来加密数据信号 Sd 。

识别信息产生器 16 以与在第一个实施例中相同的方式产生识别信息 Sid 并且输出产生的信息到置换信息产生器 75 和置换信息位置产生器 77 中。

数据产生器 1 以在第一个实施例中相同的方式产生数据信号 Sd ，并且然后输出产生的信号到数据加密器 76 中。

10 使用这些信息，数据加密器 76 通过应用预定的使用密钥信息 Sk 的加密方法，加密包括在数据信号 Sd 中的数据，并且产生加密过的数据信号 Sad ，输出它到 ECC 编码器 2 中。

ECC 编码器 2 以在第一个实施例中相同的方式对加密的数据信号 Sad 执行 ECC 块格式，并输出附加的数据信号 Sde 到置换信息记录器 3 中。

15 下面，置换信息记录器 3 用置换信息 Scg' 置换包括在附加的数据信号 Sde 中的部分 ECC 块，并与在第一个实施例中相同的方式产生置换过的数据信号 Sdr 。

于是，编码器 4 与在第一个实施例中相同的方式产生记录数据信号 Sr 。

识别信息产生器 75，使用显示在图 10 中的任一种方式，并且把来自密钥
20 信息产生器 78 的密钥信息 Sk 附加到来自识别信息产生器 16 的识别信息 Sid 上。识别信息 Sid 对每一个 DVD 是唯一的，DVD 是通过使用通过刻槽装置 C2 精制的压模盘 SP 大规模生产的。于是，识别信息产生器 75 产生对第二个实施例为唯一的置换信息 Scg' 并且输出它到置换信息记录器 3 中。

与此平行，置换信息位置产生器 77 产生位置信息 Spo ，该位置信息 Spo
25 指示着其中将被插进包括在附加数据信号 Sde 中的每一个 ECC 块中的置换信息 Scg' 的每一个产生的位的位置，并输出产生的信息到置换信息记录器 3 中。

更具体地说，置换信息产生器 77 基于任何一个插入表，产生位置信息 Spo ，这些插入表与后面将被描述的信息再现装置 S2 共享，并且以在第一个实施例中相同的方式被使用。被实际用来产生位置信息 Spo 的插入表通过识别信息 Sid
30 依照一预定的规则被选择，识别信息 Sid 是通过识别信息产生器 16 被输入的。

这样，位置信息 Sp_o 的内容对每一个识别信息 Sid 变得不同。

用上述布置，置换信息记录器 3 把来自置换信息 Scg' 每一位的位信息插入到 ECC 块中被位置信息 Sp_o 指示的位置，并产生上面提到的置换过的数据信号 Sdr 。

5 据此，激光产生器 5，光调节器 6，物镜 7，旋转伺服电路 8，旋转检测器 9，一个馈电伺服电路 10，一个位置检测器 11，一个输送单元 12，一个主轴马达 13 被与在第一个实施例中相同的方式操作，来在压模盘 SP 的保护层 14 上以螺旋轨道形成相应于记录数据信号 Sr 的信息凹坑，并且作为用来生产 DVD's 的模盘的压模盘 SP 完成了。

10 据此，在每一个具有相应于记录数据信号 Sr 的信息凹坑的作为复制盘的 DVDs 的大规模生产过程中，通过使用完成的压模盘 SP ，一个所谓的包括树脂形成，反射膜形成，保护层形成等的复制过程被执行。

这里应该注意到，在 DVDs 的大规模生产过程中，与在第一个实施例中相同的方式，另一个与包括在置换信息 Scg' 中的识别信息 Sid 相同的识别信息
15 Sid 作为例如条形码被记录在每一个 DVDs 的不同于预留的 DVD 数据区域的区域中，例如光盘的最内侧半径区域。

这样一来，每一个制造完的 DVDs 把作为部分记录数据信号 Sr 的记录在上面提到的数据区域中的识别信息 Sid ，和例如条形码形式的相同的识别信息 Sid ，记录在它的例如最内测半径区域。另外，每一个制造完的 DVDs 有对于
20 它自己为唯一的该特定识别信息 Sid ，区别于任何其它的 DVD。

下面，将参考图 10 描述在置换信息产生器 75 中被执行的在置换信息 Scg' 的产生过程中的变化。

首先，作为第一个变化，如图 10 所示，置换信息产生器 75 包括一个加密器 95 和一个加法器 95。

25 根据这种结构，使用识别信息 Sid ，依靠一预定的加密方法，加密器 95 把密钥信息 Sk 加密成为加密过的密钥信息 Sks 。于是，产生的加密密钥信息 Sks 和识别信息 Sid 通过加法器 96 被彼此相加，来成为置换信息 Scg' 。

用上面的构成，作为加法的一个特殊的方式，加密的密钥信息可以规定为置换信息 Scg' 的最高三位，而识别信息 Sid 可以规定为置换信息 Scg' 的最低三
30 位，结果置换信息 Scg' 形成例如 6 位的信息。

如图 10B 所示, 第二个变化, 置换信息产生器 75 包括一个加密器 95, 一个加法器 96 和一个函数器 (functionalizer) 97。

在这种变化中, 函数器 97 通过使用一个预定的单向加密函数处理识别信息 Sid, 从而产生函数化的识别信息 Sfid, 并输出产生的信息到加密器 95 中。

5 这种单向的加密函数是这样一种函数, 计算来自识别信息 Sid 的函数化的识别信息 Sfid 是可能的, 而计算来者函数化的识别信息 Sfid 的原始识别信息是困难的, 实际上不可能的或者是完全不可能的。具体的例子是一个重复压缩处理的函数和一个单向函数。

用上面所述的过程, 加密器 95 使用函数化的识别信息 Sfid 和上述的加密方法, 并产生加密的密钥信息 Skss。于是, 与显示在图 10A 中的情况相同的方式, 加法器 96 把加密的密钥信息 Skss 加到识别信息 Sid 中, 来产生置换信息 Scg'。

另外, 第三个变化, 如图 10C 所示, 置换信息产生器 75 包括加密器 95 和 98, 和一个加法器 96。

15 用这种布置, 首先, 加密器 98 通过上面所述的加密方法加密识别信息 Sid, 从而产生加密的识别信息 Sdid, 并输出产生的信息到加法器 96 中。

与此同时, 通过使用识别信息 Sid 和通过上述的加密方法, 加密器 95 加密密钥信息 Sk, 从而产生加密的密钥信息 Sks。于是, 与显示在图 10A 中相同的方式, 加法器 96 把加密的密钥信息 Sks 加到识别信息 Sdid 中, 来产生置换信息 Scg'。

另外, 第四个变化, 如图 10D 所示, 置换信息产生器 75 包括加密器 95 和 98, 一个函数器 97 和一个加法器 96。

用这种构成, 首先, 函数器 97 通过使用上述的加密函数, 处理识别信息 Sid, 从而产生函数化的识别信息 Sfid, 并输出产生的信息到加密器 95 中。

25 与此平行, 通过上面的加密方法, 加密器 98 加密识别信息 Sid, 从而产生加密的识别信息 Sdid, 并且输出加密的识别信息到加法器 96 中。此时, 例如, 加密器 98 能够通过使用一单向的加密函数被构成。这个加密函数可以是与使用在函数器 97 中相同的加密函数或可以是具有不同的单向加密函数。

于是, 加密器 95 使用函数化的识别信息 Sfid 和通过上述的加密方法, 加密的密钥信息 Sk, 从而产生函数化的密钥信息 Skss。于是, 以与显示在图 10A

中的情况相同的方式,加法器 96 把加密的密钥信息 Skss 加到加密识别信息 Sdid 中,来产生置换信息 Scg'。

最后,第五个变化,如图 10E 所示,置换信息产生器 75 包括一个加密器 95,一个函数器 97 和一个加法器 96。

5 用这种构成,首先,函数器 97 通过使用上述的加密函数,处理识别信息 Sid,从而产生函数化的识别信息 Sfid,并输出产生的信息到加法器 96 中。

于是,加密器 95 通过使用识别信息 Sid 和通过上述的加密方法,加密的密钥信息 Sk,从而产生加密的识别信息 Sks。于是,以与显示在图 10A 中的情况相同的方式,加法器 96 把函数化的密钥信息 Sks 加到函数化的识别信息 Sfid
10 中,来产生置换信息 Scg'。

这里应该注意到,在显示在图 10 中的每一种情况中,密钥信息 Sk 通过加密器 95 被加密,然后被包括在置换信息 Scg'中。可选择地,密钥信息 Sk 实际上可以不加密被包括在置换信息 Scg'中。

另外,根据这两种情况,即显示在图 10 中的图 10B 和图 10D 的情况,识别信息 Sid 通过单向加密函数被加密,并且这个加密的信息被用在密钥信息 Sk 的加密中。然而可选择地,通过另一个不同于用单向加密函数的加密过程,识别信息 Sid 可以被加密,并且通过另一个加密过程准备好的加密识别信息可以被用在密钥信息 Sk 的加密中。

另外,根据上面所述的刻槽装置 C2,密钥信息 Sk(或者加密密钥信息 Sks 等等)被包括在置换信息 Scg'中。然而可选择地,在 DVD100 的最内侧半径的预定位置,包含的内容可以不是置换信息 Scg'。

(B) 信息记录装置的第二个实施例

接着,将参考图 11 描述根据第二个实施例的信息记录装置。

在图 11 中,与显示在图 9 中的刻槽装置 C2 执行相同功能的部件将用相同的数字标号标明,并且将不再详细地描述。

首先,将描述根据第二个实施例的信息记录装置的构成。

如图 11 所示,根据第二个实施例的信息记录装置 R2 包括与刻槽装置 C2 相似的这些部件,例如一个数据产生器 1,一个 ECC 编码器 2,一个置换信息记录器 3,一个编码器 4,一个密钥信息产生器 78,一个置换信息产生器 75,
30 一个置换信息位置产生器 77,并且还包括与在信息记录装置 R1 中相识的这些

部件，例如一个拾取器 50，一个主轴马达 51，一个伺服 IC52，一个系统控制器 53，和一个策略电路 54。

同样地，通过信息记录装置 R1 将用来记录的 DVD100 是一种可记录 DVD，例如 DVD-R，DVD-RW 等等，并且每一个 DVD100 预先记录在它的
5 例如最内半径区域有它唯一的识别信息 Sid，并且例如条形码的形式。

下面，将描述每一个部件的操作。

首先，数据产生器 1，ECC 编码器 2，置换信息记录器 3，编码器 4，置换信息产生器 75，和置换信息位置产生器 77 与它们在早些时候所描述的刻槽装置 C2 中以相同的方式操作，从而产生上面已经描述的格式的包括 ECC 块 30'
10 （看图 4）的记录数据信号 Sr，并且输出它到策略电路 54 中。

在此时，在记录数据前，通过使用显示在图 10 中的任何一种变化和通过使用上面所述的识别信息 Sid 和从通过拾取器 50 从 DVD100 检测到的密钥信息 Sk，置换信息产生器 75 产生上述的置换信息 Scg'。

另外，以与在第一个实施例中相同的方式，置换信息产生器 75 和置换信息位置产生器 77 的操作通过来自系统控制器 53 的控制信号 Sci 和 Scp 被集中地控制。
15

此后，策略电路 54，拾取器 50，主轴马达 51 和伺服 IC52 和系统控制器 53 以与在第一个实施例中执行相关部件的伺服控制中相同的方式操作，从而把记录信号 Srs 记录在旋转的 DVD100 上。

20 通过上述的信息记录装置 R2 的操作，与记录在它的最内侧半径区域中的识别信息 Sid（这种唯一的识别信息 Sid 在每一个 DVD100 中是不同的）相同的识别信息 Sid，和密钥信息 Sk（或者加密的识别信息 Sfid 或 Sdid 和加密的密钥信息 Sks 或 Skss）被插入到记录数据信号 Sr 中。于是，将被记录在 DVD100 的数据区域中的记录数据信号 Sr 被加密。

25 (C) 信息再现装置的第二个实施例

下面，将参考图 12 描述信息再现装置的第二个实施例，该信息再现装置是一种装置，用来再现被记录在 DVD 上的数据，该 DVD 是通过使用其上的数据是通过刻槽装置 C2 被记录的压模盘 SP 来制造的，或者是用来再现被记录在 DVD 上的数据，该 DVD 的数据是通过信息记录装置 R2 被记录的。

30 应该注意到，在根据显示在图 12 中的第二个实施例的信息再现装置中，

与根据第一个实施例的信息再现装置 R1 中执行相同功能的部件将用相同的数字标号标明，并且将不再详细地描述。

首先，将参考图 12 描述根据第二个实施例的信息再现装置的构成。

如图 12 所示，根据第二个实施例的信息再现装置 S2 包括这些与在第一个
5 实施例中相似的部件，例如一个拾取器 60，一个主轴马达 61，一个 RF 放大器
62，一个解码器 63，一个置换信息提取器 64，一个用作错误校正装置的错误
校正电路 65，一个识别信息比较器 69，一个系统控制器 70，一个伺服 IC71，
一个用作再现装置的数据解码器 80，一个置换信息位置产生器 81，和一个用
作密钥信息提取装置的置换信息解码器 82，一个密钥信息产生装置，一个识别
10 信息产生装置，和一个加密识别信息产生装置。

接着，描述其操作。

首先，以在第一个实施例中相同的方式执行操作。这样，在相关的伺服控制下，用作信息再现的光束 B 被照射到旋转的 DVD100 上，并且，并且基于
15 反射光，产生相应于形成在 DVD100 上的信息凹坑的检测信号 Sp，并且输出
到 RF 放大器 52 中。

应该注意到，检测信号 Sp 包括基于反射光检测到的识别信息 Sid。

接着，以与在第一个实施例中相同的方式，RF 放大器 62 产生 RF 信号 Srf
并且输出它到解码器 63 中，并且此外，实际上输出检测到的识别信息 Sid 到每
一个识别信息比较器 69，置换信息位置产生器 81 和置换信息解密器 82 中。

20 于是，解密器 63 对 RF 信号 Srf 执行反交错和 8-16 调制来产生包括 ECC
块 30'的再现信号 Sdc，并且输出产生的信号到置换信息提取器 64 中。

接着，通过复制，置换信息提取器 64 从被后面将描述的位置信息 Spo 指
示的位置提取包括在再现信号 Sdc 中的 ECC 块 30'中的插入的置换信息 Scg'，
然后输出提取的信息到置换信息解码器 82 中，并在置换信息 Scg'的复制提取
25 之后输出再现信号 Sdc 到错误校正电路 65 中。

在此时，置换信息位置产生器 81 执行与通过上面所述的刻槽装置 C2 中
的置换信息位置产生器 77 或者信息记录装置 R2 执行的操作相似的操作。该操
作基于来自系统控制器 70 的控制信号 Scpp 和识别信息 Sid，并通过利用一个
与置换信息位置产生器 77 共享的插入表被执行。插入表的选择相应于识别信
30 息 Sid 预定的规则进行的。于是，置换信息位置产生器 81 对每一个 ECC 块 30'

产生位置信息 Spo, 该位置信息 Spo 不同于每一个识别信息 Sid, 并且输出它到置换信息提取器 64 中。

用上面的安排, 通过使用识别信息 Sid, 置换信息解密器 82 对置换信息 Scg' 执行一个解密过程。这个解密的过程是一个与上面所述的置换信息产生器 75 中执行的过程相反的过程。于是, 与在第一个实施例中相似, 置换信息解密器 82 产生来自置换信息 Scg' 的密钥信息 Sk 和识别信息 Sidp, 并且输出密钥信息 Sk 到数据解码器 80 中。此外, 置换信息解密器 82 输出识别信息 Sidp 到识别信息比较器 69 中。

依据显示在图 10 中的这些变化, 在置换信息解密器 82 中的解密过程被用作置换信息产生器 75。

明确地, 假如置换信息产生器 75 根据显示在图 10A 中的第一种变化被构成, 于是, 置换信息解密器 82 首先把置换信息 Scg' 分成高三位和低三位, 从而产生识别信息 Sidp 和加密的密钥信息 Sk_s。

于是, 实际上置换信息解密器 82 输出识别信息 Sidp 到识别信息比较器 69 中。另一方面, 通过使用一种解密方法, 该解密方法相应于通过使用被记录在 DVD100 的最内半径区域中的识别信息 Sid 在加密器 95 中执行的加密方法, 置换信息解密器 82 处理加密的密钥信息 Sk_s。于是, 置换信息解密器 82 产生密钥信息 Sk 来输出它到数据解码器 80 中。

可选择地, 当加密的密钥信息 Sk_s 被解密的时候, 通过使用识别信息 Sidp, 可以执行解密。

另一方面, 假如置换信息产生器 75 根据显示在图 10B 中的第二中变化构成, 于是置换信息解密器 82 被装备有上面提到的函数器。

特别地, 首先, 通过把置换信息 Scg' 分成高三位和低三位, 置换信息解密器 82 产生识别信息 Sidp 和加密的密钥信息 Sk_{ss}。

此后, 置换信息解密器 82 输出识别信息 Sidp 到识别信息比较器 69 中。通过函数器 97, 置换信息解密器 82 处理被记录在 DVD100 的最内半径区域中的识别信息 Sid, 并且产生函数化的识别信息 Sfid。

于是, 置换信息解密器 82 处理加密的密钥信息 Sk_{ss}, 该密钥信息 Sk_{ss} 是通过使用一种解密方法被分离的, 该解密方法相应于通过使用函数化的识别信息 Sfid 在加密器 95 中执行的加密方法。于是, 置换信息解密器 82 产生密钥信

息 Sk 来输出它到数据解码器 80 中。

可选择地, 当加密的密钥信息 Skss 被解密的时候, 通过使用通过函数器 97 对识别信息 Sidp 函数化获得的函数化的识别信息, 解密可以被执行。

下面, 假如置换信息产生器 75 根据显示在图 10C 中的第三中变化被构成,
5 首先, 置换信息解密器 82 把置换信息 Scg' 分成高三位和低三位, 并产生加密的识别信息 Sdid 和加密的密钥信息 Skss。

此后, 通过使用一种解密方法, 该解密方法相应于通过使用被记录在 DVD100 的最内半径区域中的识别信息 Sid 在加密器 98 中执行的加密方法, 置换信息解密器 82 处理加密的识别信息 Sdid。于是, 置换信息解密器 82 产生识
10 别信息 Sidp 来输出它到识别信息比较器 69 中。

另外, 通过一种解密方法, 该解密方法相应于使用上面提到的识别信息 Sid 在加密器 95 中执行的加密方法, 置换信息解密器 82 处理加密密钥信息 Skss。于是, 置换信息解密器 82 产生密钥信息 Sk 来输出它到数据解码器 80 中。

可选择地, 当加密密钥信息 Skss 被解密的时候, 可以通过使用识别信息 Sidp
15 执行解密。

另一方面, 假如置换信息产生器 75 根据显示在图 10D 中的第四个变化构成, 于是置换信息解密器 82 配备有上面所述的函数器 97。

在这种情况下, 首先, 置换信息解密器 82 把置换信息 Scg' 分成高三位和低三位, 并分别产生加密识别信息 Sdid 和加密密钥信息 Skss。

20 此后, 通过使用一种解密方法, 该解密方法相应于通过使用被记录在 DVD100 的最内半径区域中的识别信息 Sid 在加密器 98 中执行的加密方法, 置换信息解密器 82 处理加密的识别信息 Sdid。于是, 置换信息解密器 82 产生识别信息 Sidp 来输出它到识别信息比较器 69 中。

此后, 函数器 97 处理识别信息 Sid, 并且产生函数化的识别信息 Sfid。

25 通过一种解密方法, 该解密方法相应于使用上面提到的函数化的识别信息 Sfid 在加密器 95 中执行的加密方法, 置换信息解密器 82 处理加密密钥信息 Skss。于是, 置换信息解密器 82 产生密钥信息 Sk 来输出它到数据解码器 80 中。

可选择地, 当加密密钥信息 Skss 被解密的时候, 通过使用通过函数器 97
30 对识别信息 Sidp 函数化获得的函数化识别信息, 可以执行解密。

最后，假如置换信息产生器 75 根据显示在图 10E 中的第 5 种变化构成，首先，置换信息解密器 82 把置换信息 Scg'分成高三位和低三位，并且产生加密识别信息 Sfid 和加密密钥信息 Sk_s。

在上面，通过上述的单向加密函数，函数化的识别信息 Sfid 被加密。因此，
5 不可能从这种函数化的识别信息 Sfid 中恢复原始的识别信息 Sid。

置换信息解密器 82 处理另一种被分离的信息，也就是通过一种解密方法被加密的密钥信息 Sk_s，该解密方法相应于使用被记录在 DVD100 的最内半径区域中的识别信息 Sid 在加密器 95 中执行的加密方法。于是，置换信息解密器 82 产生密钥信息 Sk 来输出它到数据解码器 80 中。

10 这里应该注意到，假如事实上包括在上述的置换信息 Scg'中的密钥信息 Sk 没有被加密，于是从置换信息 Scg'中被分离的密钥信息 Sk 事实上应该简单地被输入到数据解码器 80 中。

接着，识别信息比较器 69 产生一个允许信号 Sco，它允许来自数据解码器 80 中的输出信号 Sout 的输出，只有从 RF 放大器 62 中输出的识别信息 Sid
15 与在上面的变化中所述的一种格式中产生的识别信息 Sidp 相一致时（也就是只有被插进记录数据信号 Sr 中的识别信息 Sid 与被记录在例如 DVD100 的最内半径区域中的识别信息 Sid 相同时），输出到数据解码器 80 中。

在上面中，如上所述，假如置换信息产生器 75 根据显示在图 10E 中的第 5 种变化构成，不能从分离的函数化的识别信息 Sfid 中还原原始的识别信息
20 Sid。这样，通过与在函数化识别信息 Sfid 产生中使用的相同加密函数，从 DVD100 中的最内侧半径区域中检测到的识别信息被加密，并且加密的结果与上面提到的函数化识别信息 Sfid 相比较。假如这两块信息彼此一致，那么来自数据解码器 80 的允许输出信号 Sout 输出的允许信号 Sco 被输出。

通过使用 ECC 内码 31 和 ECC 外码 32，错误校正电路 65 对包括在输入的再现信号 Sdc 中的 ECC 块 30'（即在置换信息 Scg 的提取之后的 ECC 块 30'）
25 执行错误校正过程，产生一错误校正信号 Scr 和输出产生的信号到数据解码器 80 中。

那么，只有允许信号 Sco 允许输出信号 Sout 输出时，通过使用密钥信息 Sk，该密钥信息是通过上述的任何一种变化和通过相应于在刻槽装置 C2 或信息记录装置 R2 中在加密器 76 使用的加密过程产生的，数据解码器 80 解密错误校
30

正过的信号 Scr。那么，数据解码器 80 输出信号 Sout 到外部显示器，扬声器等等。

与此这些过程平行，系统控制器 70 产生控制信号 Scpp, Spu 和 Scsp, 和控制上述部件的操作，并且同时，执行信息再现装置 S1 的整个控制过程。

- 5 这里应该注意到，象在第一个实施例中的输出控制器 66 一样，如图 12 所示，数据解码器 80 可以选择地放置在错误校正电路 65 之前而不是在错误校正电路 65 之后，所以在这个阶段能依照允许信号 Sco 进行输出信号 Sout 的输出控制。

- 10 如上所述，根据通过第二个实施例提供的非法复制防止系统的操作，获得比通过第一个实施例获得的效果另外的优点。明确地，由于置换信息 Scg' 的产生包括了加密过程或函数化过程的各种变化（看图 10），并且在信息再现的时候被相对地解密，能够使得非法获得密钥信息 Sk 和识别信息 Sidp 变得更加困难，并且因此更有效地防止记录的非法复制。

- 15 这里应该注意到，根据第二个实施例，仅仅描绘了其中置换信息 Scg' 由密钥信息 Sk 的加密形式，即加密的密钥信息 Sks 和识别信息 Sid 的加密形式，即加密的识别信息 Sdid, 构成的情况。然而可以选择地，置换信息可以通过仅仅使用加密的密钥信息 Sks 产生。

- 20 在这种特殊的情况中，由于置换信息被记录在相应于在加密密钥信息 Sks 的产生中使用的识别信息 Sid 的 DVD100 中，这种加密的密钥信息 Sks 以对每一个 DVD 唯一的形式被记录在 DVD100 中。因此，可以作这样一个布置，即通过使用识别信息 Sid 执行加密密钥信息 Sk 的解密，和通过使用这种因为加密的密钥信息 Sk 进行错误校正过的信号 Scr 的加密。用这种布置，除非识别信息 Sid 与加密的密钥信息 Sk 完全地相关联，才能执行解密，并且因此能够防止记录数据信号 Sr 的非法拷贝（其中识别信息 Sid 与加密密钥信息不完全地
25 相关）被再现。

- 30 另外应该注意到，根据上面所述的每一个实施例，每一个 DVD100 具有对它自己为唯一的识别信息 Sid。然而，可选择地，特别是在通过使用压模盘 SP 的仅仅再现的 DVD100 的大规模生产中，通过提供这样一种安排，例如所有的包括相同记录数据 Sd 的 DVDs 具有被记录在其中的相同识别信息 Sid，通常地在上面所述的每一个实施例中能够获得相同的效果。

另外,对于如上所述的这些其中被记录相同的记录数据 Sr 的 DVDs100 中,可以作另外一种安排,其中相同的识别信息 Sid 被用作这些被分配相同批号的 DVDs。

这里还应该注意到,根据上面所述的每一个实施例,仅仅对一种情况进行描述,其中相应于 DVD100 自身的识别信息 Sid 被记录在 DVD100 的非预定数据记录区域的最内侧半径区域。然而,可选择地,识别信息 Sid 本身可以被记录在从包括置换信息 Scg 或 Scg'的位置分离出的预留的数据记录区域中的位置上。

在这种情况下,由于识别信息 Sid 的记录能与记录数据信号 Sr 的记录平行地执行,刻槽过程和信息记录过程能够简化。

还应注意到根据所描述的每一个实施例其中在 DVD100 上置换信息 Scg 或 Scg'被插入的位置。对如上所述的数据记录区域可选择地,只要该位置是在可记录区域,该位置可以是包括读入区域等的任何位置。

然而,在这种特殊情况中,考虑到记录信息的再现操作能被取消的可能性,该位置最好是在导入区或是在分配作为记录管理信息的数据记录区域中的一个区域中。

这里应该注意到,根据上面所述的每一个实施例的相应于记录过程或再现过程的程序能预先地被记录在软盘上,硬盘上或者其它的信息记录介质中。通过例如个人计算机通过读取和执行该程序,通过由例如个人计算机构成的信息记录/再现系统,记录过程或再现过程能够变得可执行的。

还应注意到,上面所述的每一个实施例是对例如一种可记录 DVD 的本发明的一个应用。然而,本发明也能被应用到其它的信息记录介质例如可记录 CD 中,从而能够防止记录信息的非法复制。

本发明可以在不脱离其精神或实质特征的其它特定方式被执行。本发明因此将被考虑在所说明的和没有限制的所有方面,被附加的权利要求所指示的本发明的范围优于前面所描述的,并且在权利要求的含意范围内和相等的范围内的所有变化将被包含在其中。

包括说明书,权利要求,附图和摘要的在 2000 年 4 月 21 日申请的日本专利申请号 2000-121636 的全部公开内容在这里参考它的整体被合并成一体。

C1

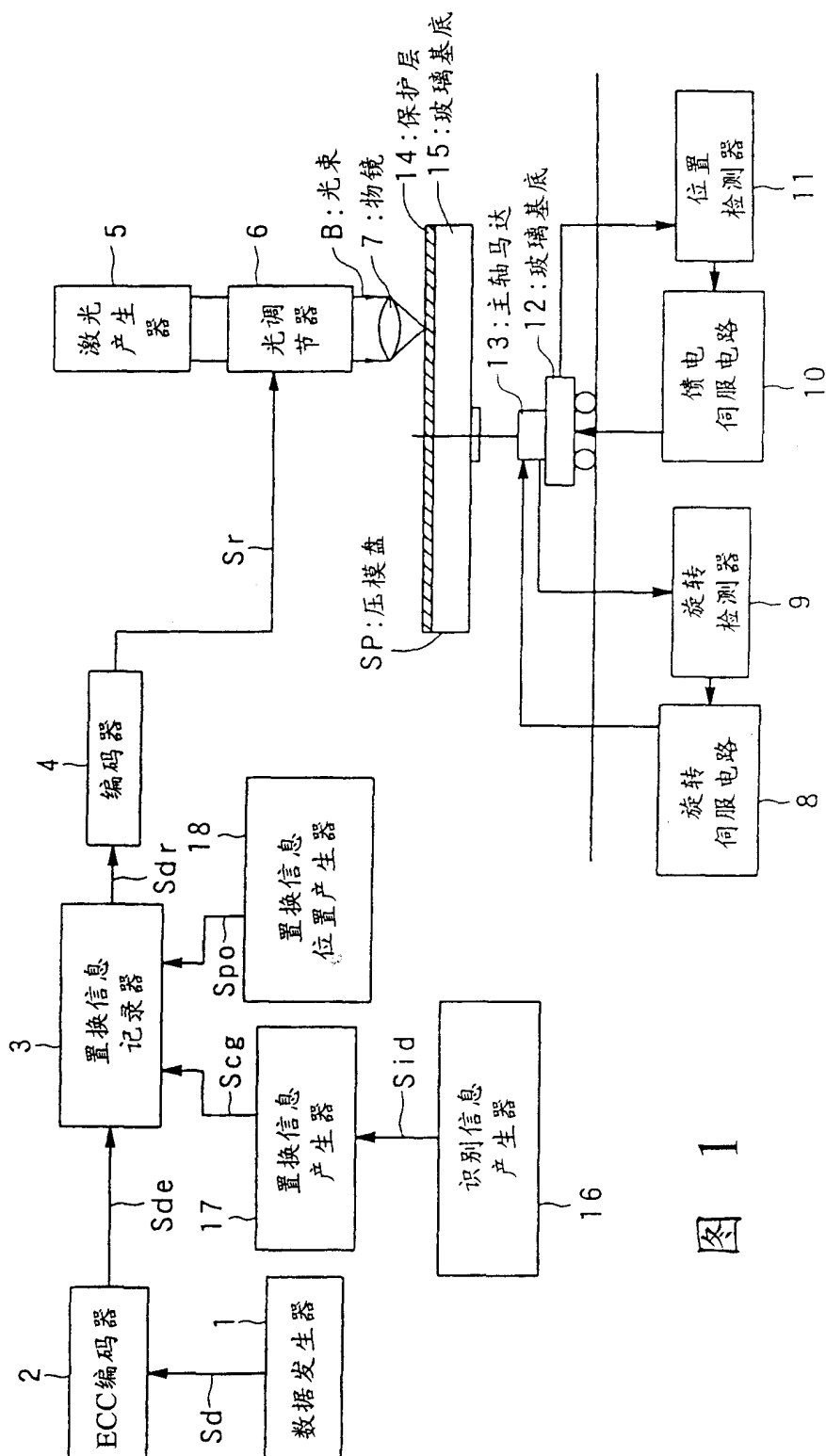


图 1

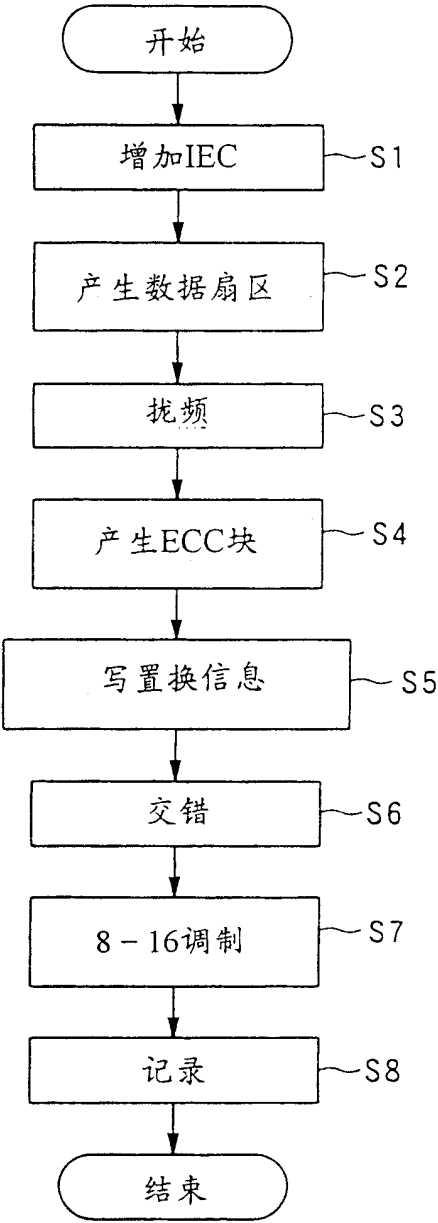


图 2

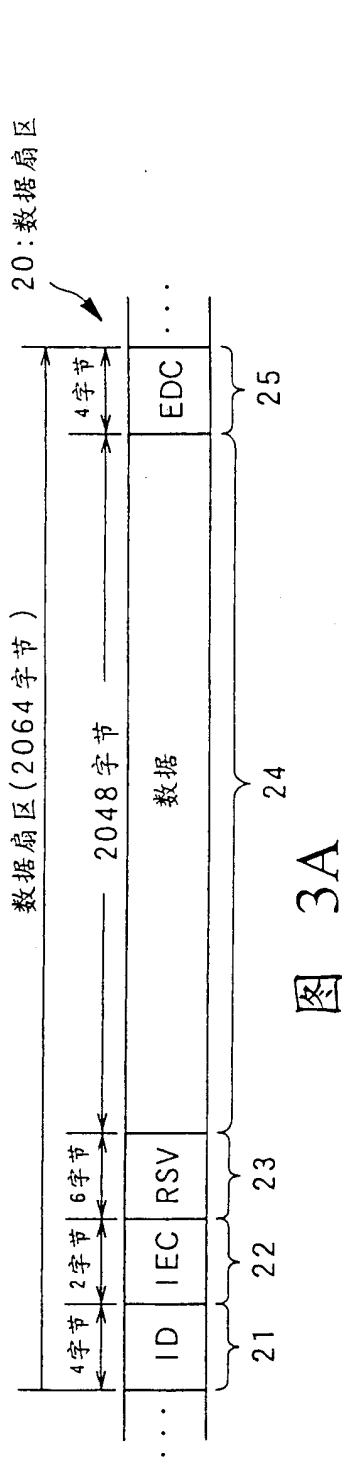


图 3A

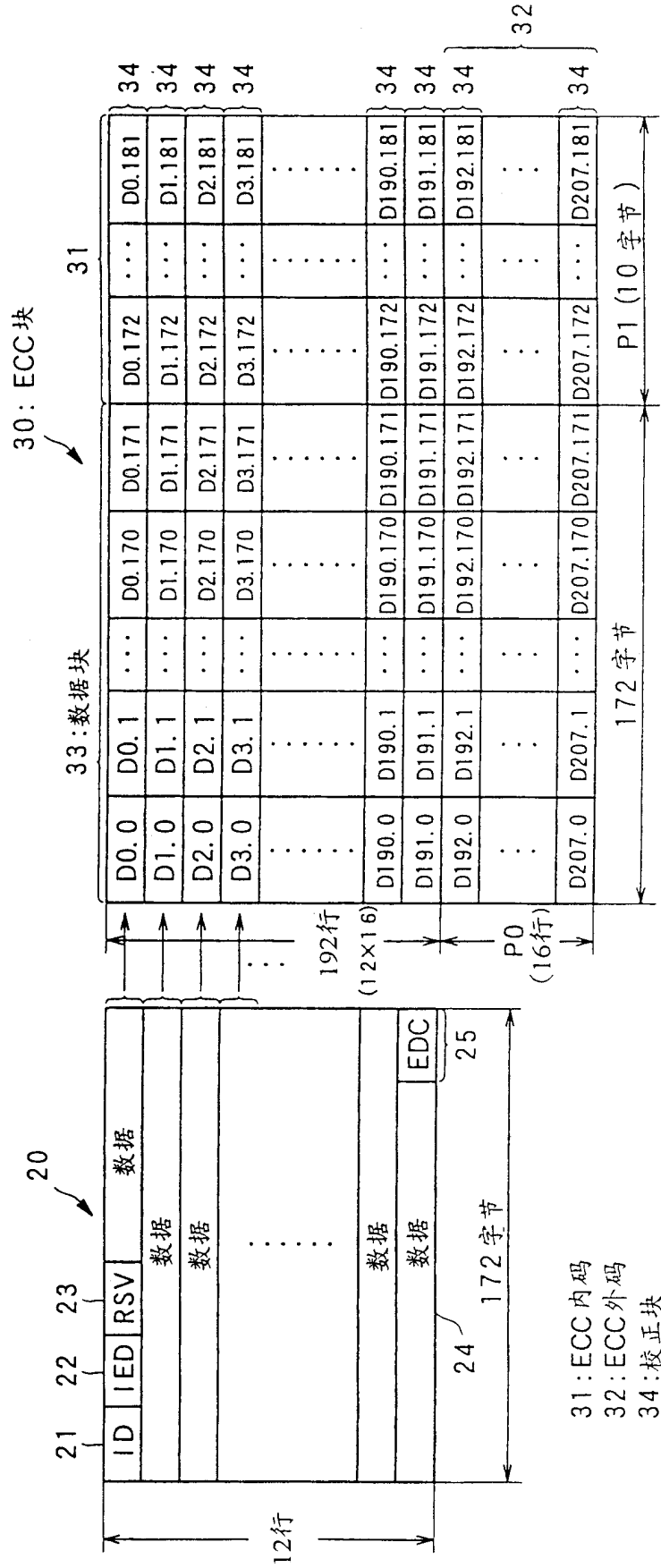


图 3B

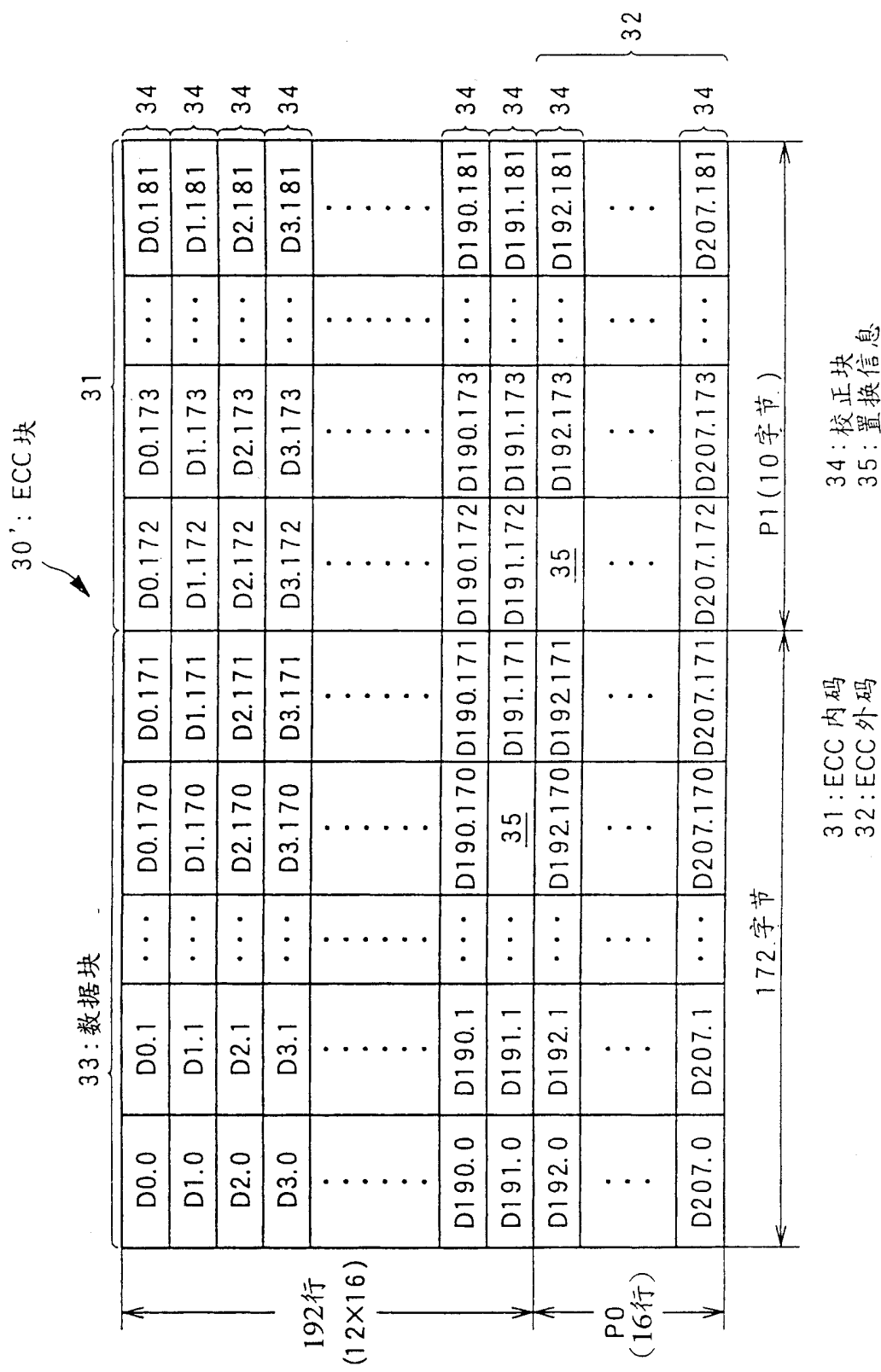


图 4

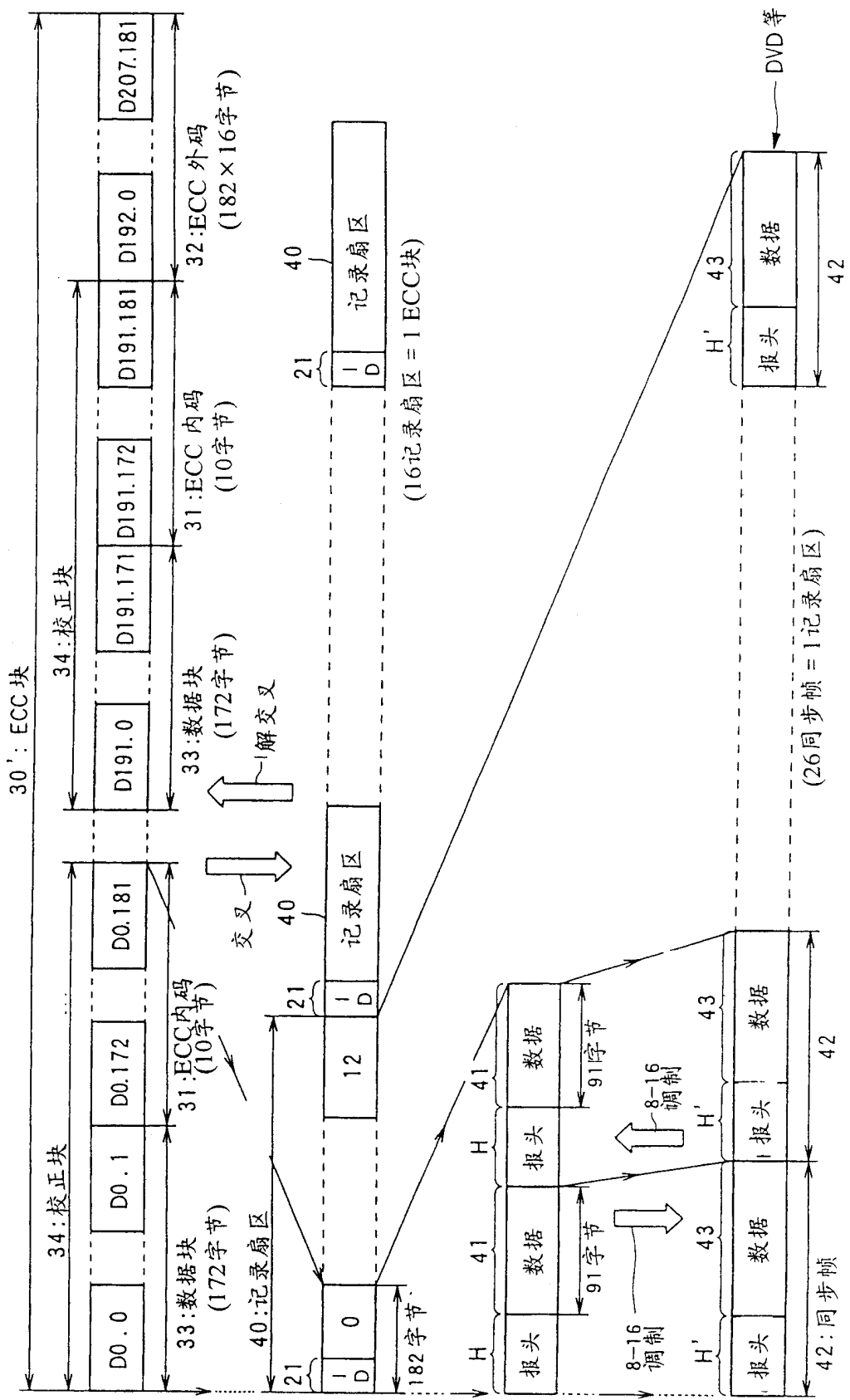


图 5

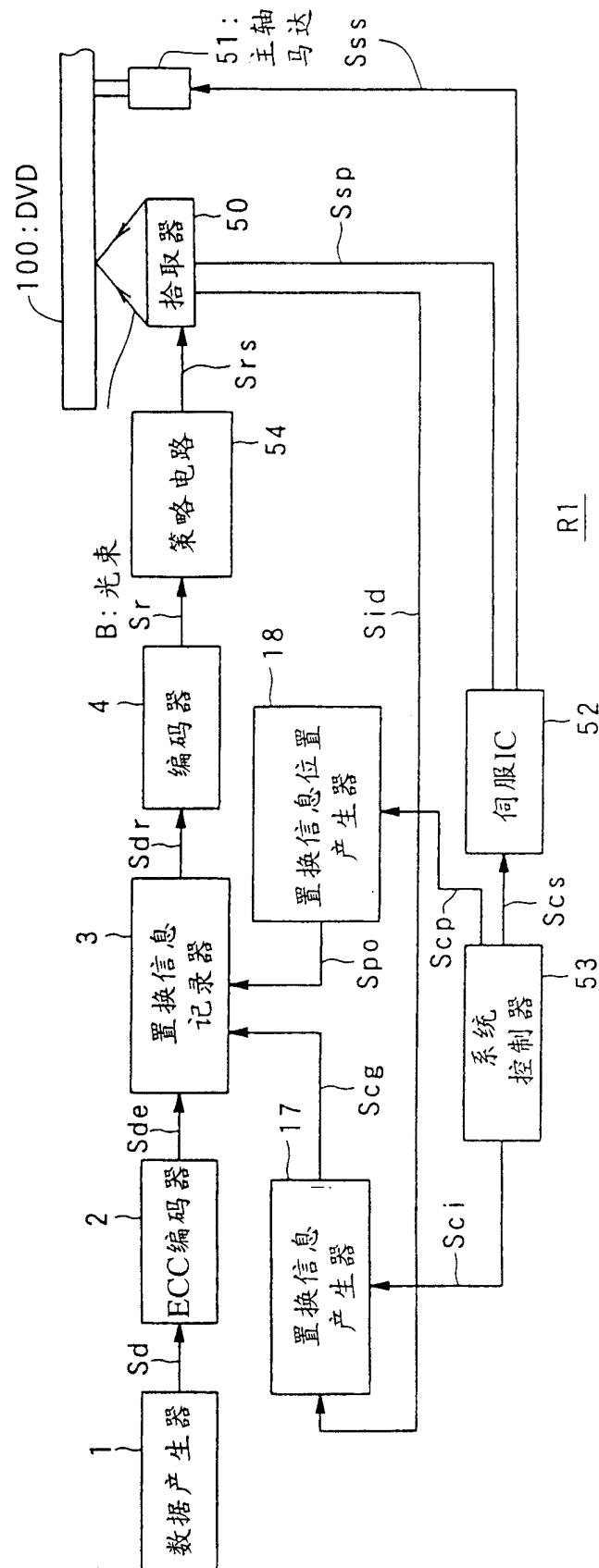
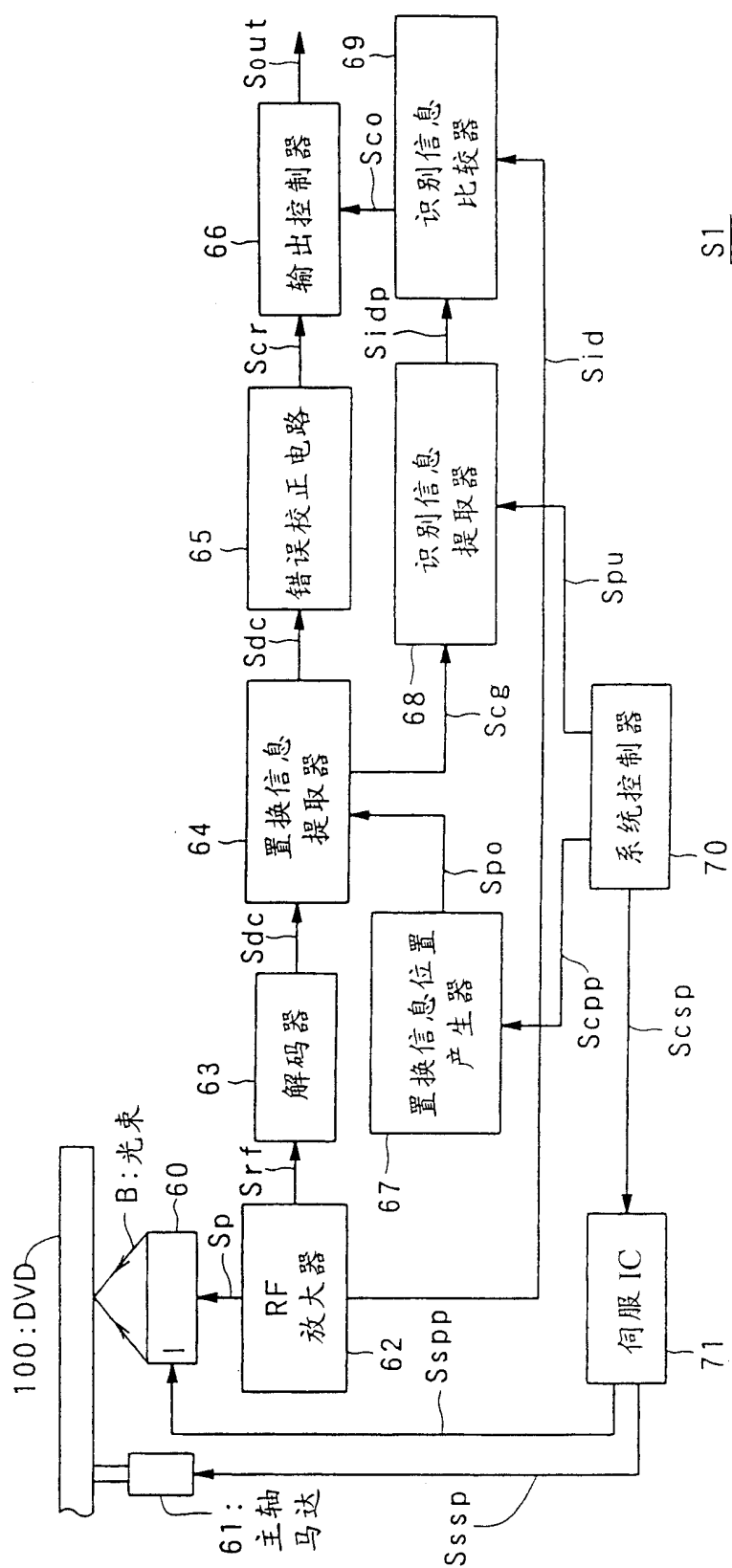


图 6

7
[X-1]

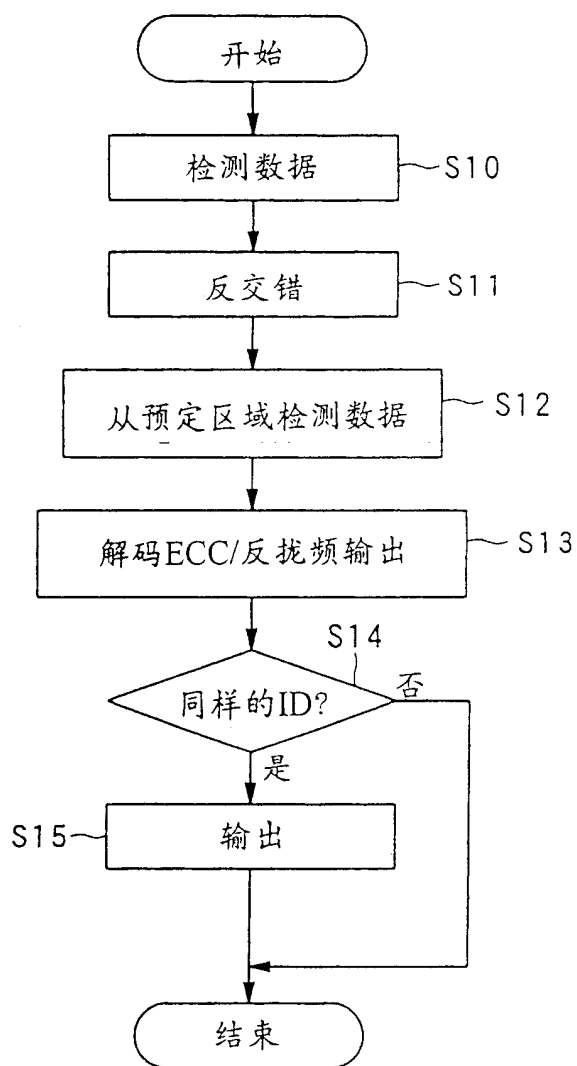


图 8

C2

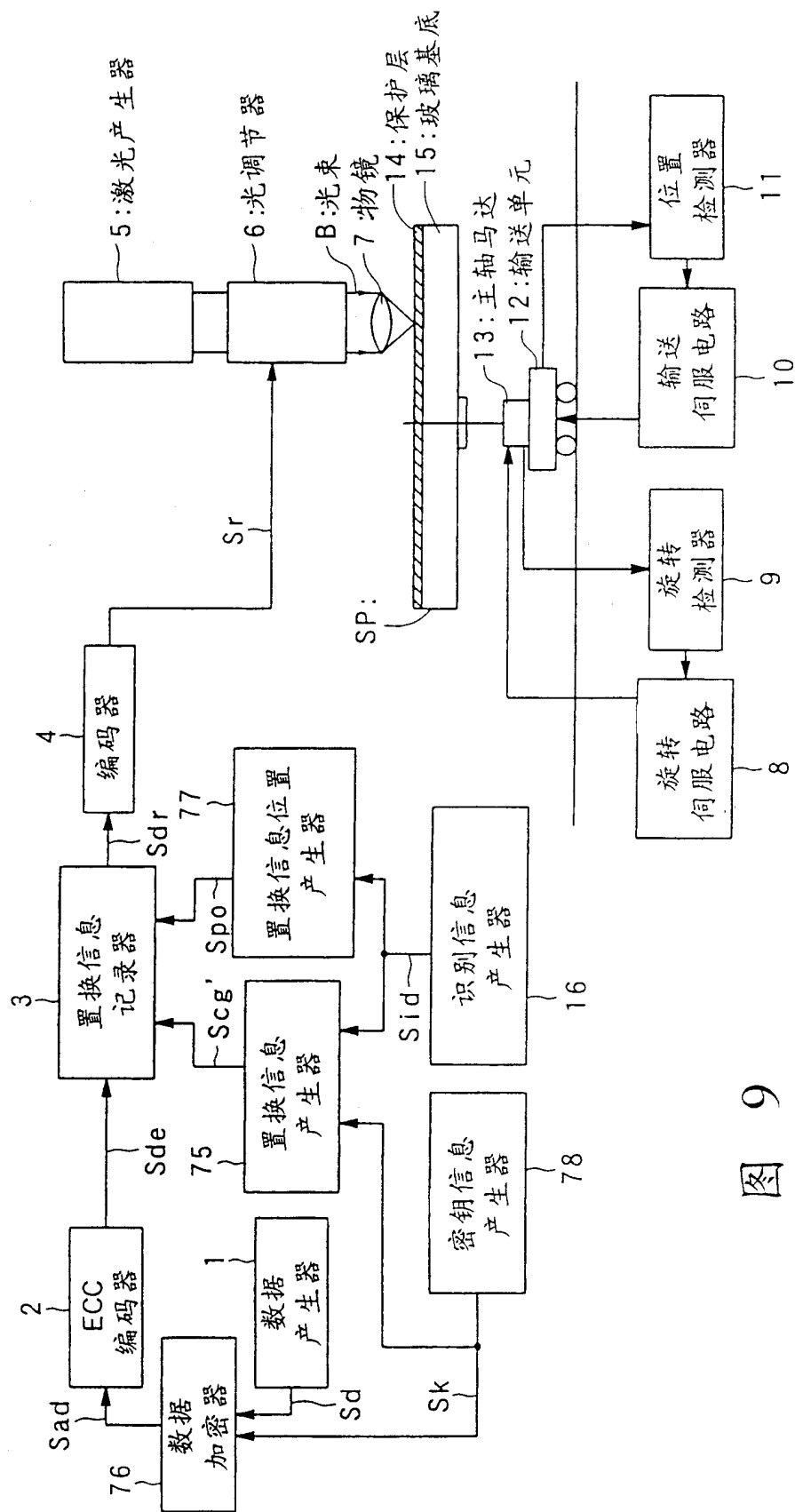


图 9

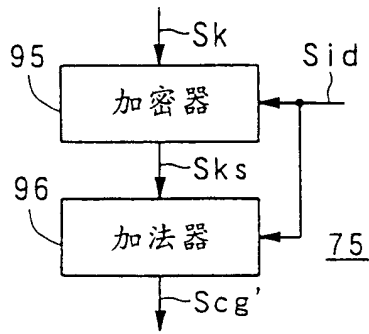


图 10A

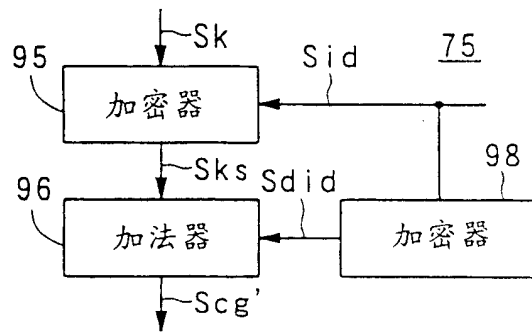


图 10C

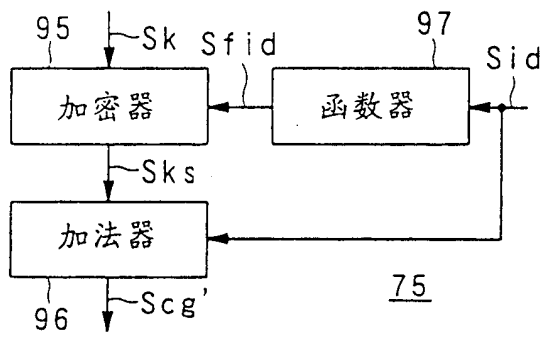


图 10B

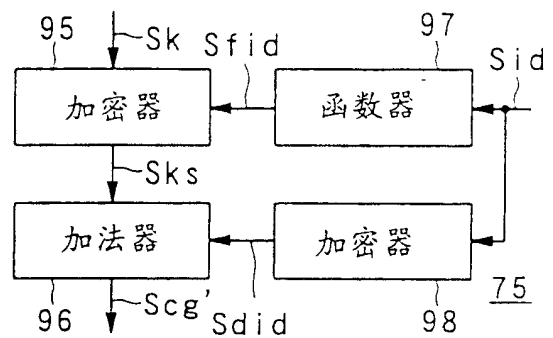


图 10D

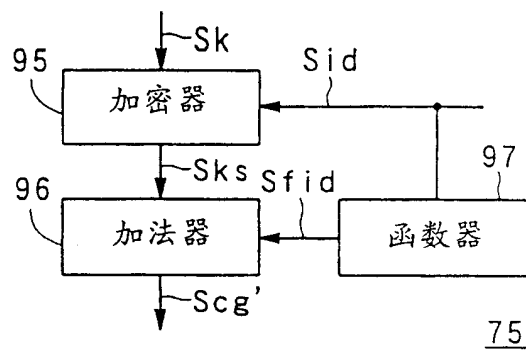


图 10E

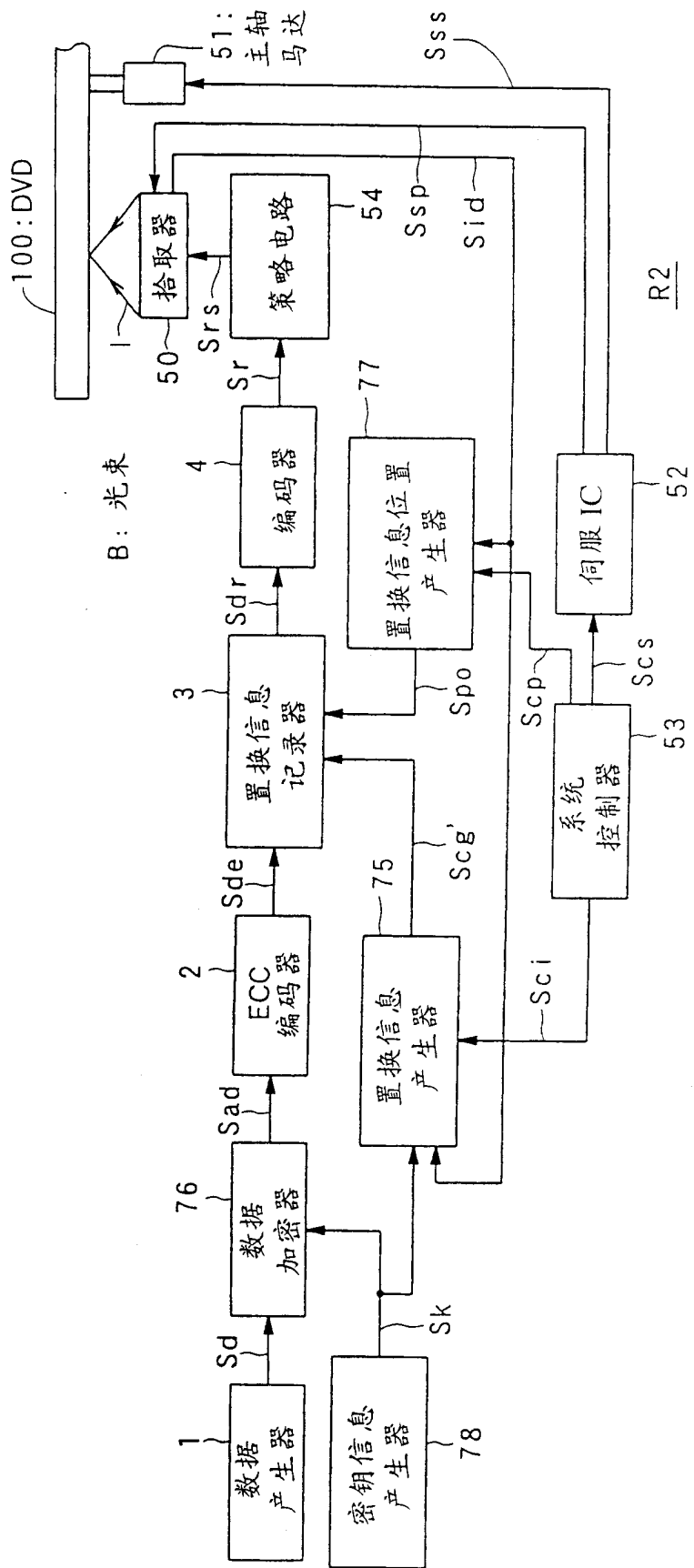


图 11

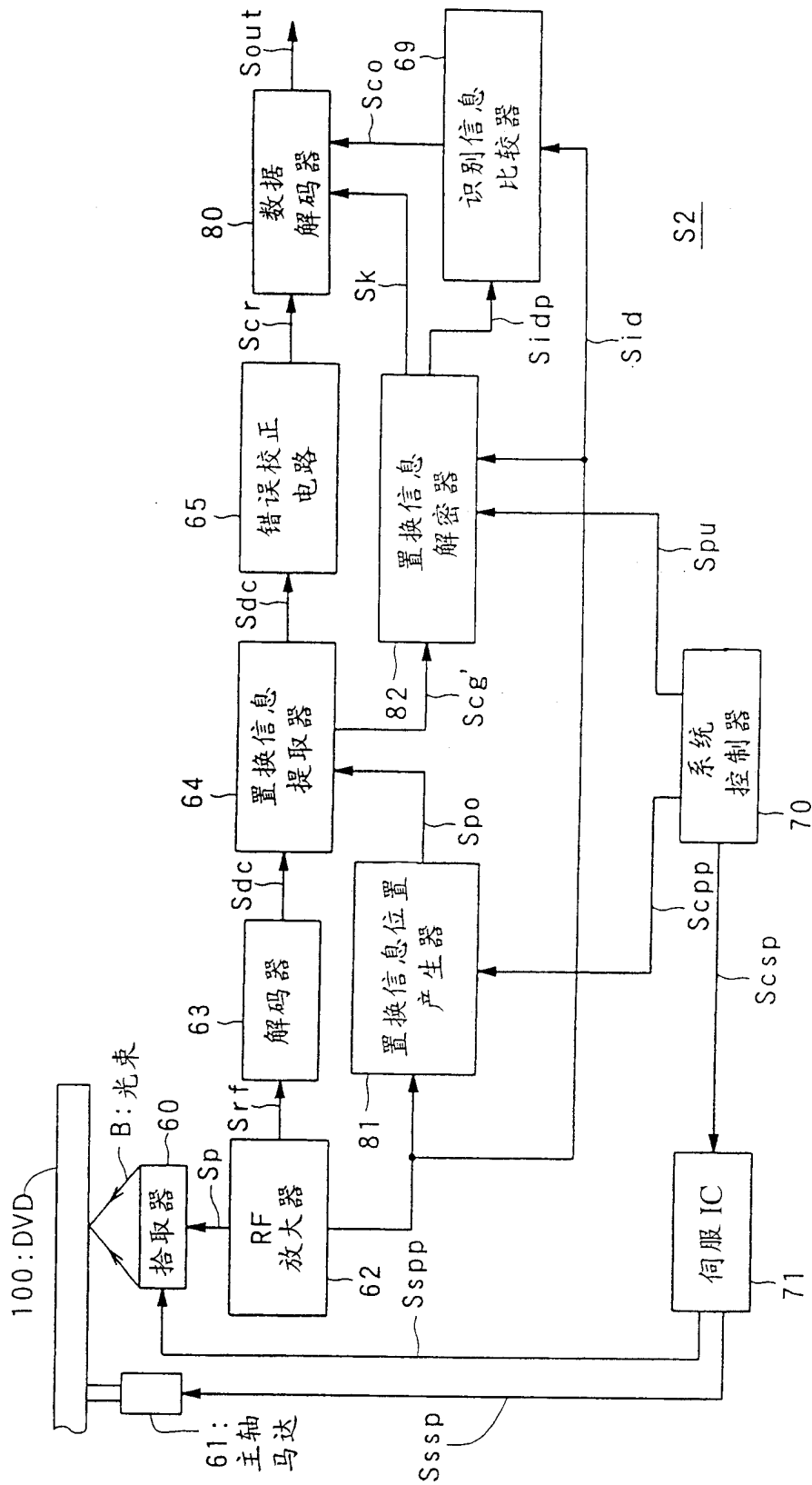


图 12