

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G11B 7/013 (2006.01)

G11B 20/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 01816151.0

[45] 授权公告日 2008 年 6 月 25 日

[11] 授权公告号 CN 100397501C

[22] 申请日 2001.9.21 [21] 申请号 01816151.0

[30] 优先权

[32] 2000.9.22 [33] JP [31] 00-288346

[32] 2000.9.26 [33] JP [31] 00-292034

[32] 2000.10.24 [33] JP [31] 00-323676

[86] 国际申请 PCT/JP2001/008267 2001.9.21

[87] 国际公布 WO2002/025645 英 2002.3.28

[85] 进入国家阶段日期 2003.3.24

[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 东海林卫 中村敦史 石田隆

石桥广通 宫下晴旬 千贺久司

高桥里枝

[56] 参考文献

CN1100549A 1995.3.22

CN1142663A 1997.2.12

EP0545472A1 1993.6.9

EP0723216A2 1996.7.24

审查员 王 靖

[74] 专利代理机构 中科专利商标代理有限责任公
司

代理人 王 玮

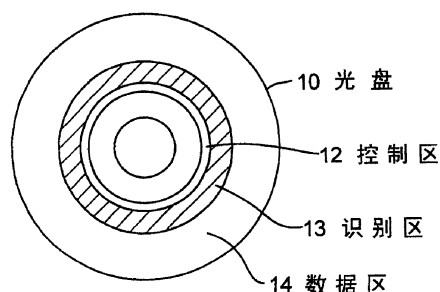
权利要求书 1 页 说明书 55 页 附图 49 页

[54] 发明名称

制造光盘的方法

[57] 摘要

一种制造光盘的方法，包括：将由可光学读取的记录标记记录的主数字数据记录到所述光盘上；和将通过对记录标记的位置或形状略微移位而与主数字数据重叠的子数字数据记录到盘上，从而针对由主数字数据记录的单个内容，所述光盘上的多个区域存储相同子数字数据。



1. 一种制造光盘的方法，包括：

将由可光学读取的记录标记记录的主数字数据记录到所述光盘上；
和

将通过对记录标记的位置或形状略微移位而与主数字数据重叠的子数字数据记录到盘上，从而针对由主数字数据记录的单个内容，所述光盘上的多个区域存储相同子数字数据。

2. 根据权利要求 1 所述的方法，其中该多个区域配置在预定的径向位置单元。

3. 根据权利要求 1 所述的方法，其中该多个区域配置在预定的地址单元。

4. 根据权利要求 1 所述的方法，其中该位移量在每个区域中不同。

5. 根据权利要求 1 所述的方法，其中子数字数据是用于确定该盘或内容是否合法的信息。

6. 根据权利要求 1 所述的方法，还包括：将与根据子数字数据形成的图案具有相关性的图案存储到所述光盘上。

7. 根据权利要求 1 所述的方法，还包括：将指示在何处形成子数字数据的信息存储到所述光盘上。

制造光盘的方法

技术领域

本发明涉及通过向记录介质发射会聚光束，然后检测从记录介质反射的光来再生记录到介质的信息的光记录介质。

背景技术

光盘，通常是 DVD（数字多用/视盘），现在普遍用于大的数字数据量，包括计算机数据和 AV（音频/视频）数据。例如存储两小时或更长时间高质量食品数据的 DVD-ROM 盘已广泛使用。

需要防止把受版权保护的数字材料非法复制到另一个介质的技术，以便确保受版权保护的数字内容的安全分发。

内容加密是防止非法复制的一种现有技术方法（见 Nikkei 电子，1996 年 11 月 18 日第 13-14 页）。图 33 示出普通 DVD 的数据记录区。如图 33 所示，DVD20 的记录区包括存储内容的用户可存取数据区 20a，和用户不能存取的控制数据区 20b。现有技术的方法使用三级保密密钥（题目密钥，盘密钥，和主密钥）对诸如电影之类的压缩数字内容加密，然后，将加密的内容记录到用户可存取的数据区 20a。这三种加密密钥中最重要的是主密钥，主密钥只给经许可的 DVD 设备制造商。需要盘密钥和题目密钥对其上的单独 DVD 和题目解密，并在使用主密钥加密之后将盘密钥和题目密钥记录到用户不能存取的控制数据区 20b（引入区）。

该方法使未许可的 DVD 再生装置不能对加密的内容解密，从而防止非法大量再生和销售记录有受版权保护的未加密数字内容的 DVD。

该现有技术的缺陷在于不能防止所谓的盗版编辑。具体地说，当从 DVD 的所有区对所有的内容，包括控制数据区进行原样复制时，象任何合法复制的 DVD 一样，许可的 DVD 再生装置仍能读取和解密加密的内容。应指出，这种原样防止在此被称为“完全复制”。

下面参考图 13 描述进行完全复制的方法。

参考图 13，作为源盘的光盘 20 与作为目标盘的光盘 20' 的主轴电机的速度是完全同步的，利用再生头 2003 再生来自源盘 20 的数据。然后，再生放大器 2004 放大再生信号，由数字化器 2005 数字化，并输入到 PLL（锁相环）电路 2006。PLL 2006[1006]根据输入信号产生时钟信号。触发器 2007 同步来自数字化器 2005 的输出信号，并在由来自 PLL 的定时信号 2010 控制的定时将该输出信号输出到光调制器 2008。光调制器 2008 从输入至此的信号产生光调制信号，然后由记录头 2009 将该信号记录到目标盘 20'。

该过程产生了与整个源盘完全相同的复制，包括用户不可存取的控制数据区 20b。因此，不能将该与许可的盘区分开来，并且可解密和播放其内容。

这意味着即使能够非法生产包含加密内容的 DVD，也不能防止非法复制包含与原始 DVD 相同的加密内容。低成本销售的这些非法复制品明显侵犯了这些内容的版权。

发明内容

针对上述问题，本发明的一个目的是提供一种能够防止对记录至此的受版权保护的数字内容进行完全相同的复制的光盘。本发明的另一个目的是提供一种用于该光盘的记录和再生装置以及记录和再生方法。

在本发明的第一方面中，提供一种光盘，包括由可光学读取的记录标记记录的主数字数据，和通过对记录标记的位置或形状略微移位而与主数字数据重叠并记录到盘上的子数字数据。在盘上为由主数字数据记录的单独内容设置的各存储相同子数字数据的多个区域。

在本发明的第二方面中，提供一种光盘，包括由可光学读取的记录标记记录的主数字数据，和通过对记录标记的位置或形状略微移位而与主数字数据重叠并记录到盘上的子数字数据。为由主数字数据记录的单独内容设置各存储不同子数字数据的多个区域。

在本发明的第三方面中，提供一种光盘，包括由可光学读取的记录标记记录的主数字数据，和通过对记录标记的位置或形状略微移位而与主数字数据重叠并记录到盘上的子数字数据。为由主数字数据记录的不同内容设置不同的子数字数据。

在本发明的第四方面中，提供一种光盘，包括由可光学读取的记录标记记录的主数字数据，和通过对记录标记的位置或形状略微移位而与主数字数据重叠并记录到盘上的子数字数据。在与由主数字数据记录内容的数据区不同的区域中形成子数字数据。

在本发明的第五方面中，提供一种光盘，包括由可光学读取的记录标记记录的主数字数据，和通过对记录标记的位置或形状略微移位而与主数字数据重叠并记录到盘上的子数字数据。在与由主数字数据记录内容的数据区和记录控制数据的控制区不同的区域中形成子数字数据。

在本发明的第六方面中，提供一种再生光盘的再生方法，该光盘存储由可光学读取的记录标记记录的主数字数据，和子数字数据，其中子数字数据通过在记录标记的轨迹方向对记录标记的位置或形状略微移位而与主数字数据重叠并记录到盘上。该方法包括根据子数字数据构成图案，将该图案与预定密钥信息比较，在未确认图案与密钥信息之间的相关性时限制由主数字数据记录的内容的再生。

在本发明的第七方面中，提供一种光盘，包括由可光学读取的记录标记记录的主数字数据，由可光学读取的记录标记记录的子数字数据，和用于提取子数字数据的子数字数据管理信息。

在本发明的第八方面中，提供一种再生光盘的再生装置。该光盘存储由可光学读取的记录标记记录的主数字数据，通过在盘的轨迹方向对记录标记的边缘位置略微移位的调相记录的子数字数据，和用于提取子数字数据的子数字数据管理信息。该装置包括从光盘再生主数字数据的部分，和提取子数字数据的部分。

在本发明的第九方面中，提供一种通过在盘上形成可光学读取的记录标记而将主数字数据记录到光盘的记录装置。该装置包括通过在盘的轨迹方向将记录标记的边缘位置移位微小的量的调相来记录子数字数据的部分。子数字数据记录部分形成记录标记，以使记录标记的边缘在相位超前或滞后预定较小量的位置与主数字数据对应。子数字数据记录部分包括用于记录提取子数字数据所需的子数字数据管理信息的部分。

在本发明的第十方面中，提供一种光盘，包括由可光学读取的记录标记记录的主数字数据，通过将特定记录标记的位置或形状改变微小量而记录的子数字数据，由子数字数据对主数字数据加密。

在本发明的第十一方面中，提供一种通过在盘上形成记录标记而将主数字数据记录到光盘的记录装置。该装置包括通过把记录标记边缘的位置或形状改变微小量来记录子数字数据的子数字数据记录部分，和根据子数字数据对主数字数据加密的主数字数据加密部分。

在本发明的第十二方面中，提供一种从光盘再生数据的再生装置。该光盘存储由可光学读取的记录标记记录的主数字数据和子数字数据，由子数字数据加密的主数字数据。该装置包括检测光盘上形成的记录标记的检测部分，从与一系列检测的记录标记对应的通道信号提取子数字数据的子数字数据提取部分，和根据由提取部分提取的子数字数据对加密的主数字数据解码的解密部分。

在本发明的第十三方面中，提供一种制造光盘的方法，包括：将由可光学读取的记录标记记录的主数字数据记录到所述光盘上；和将通过对记录标记的位置或形状略微移位而与主数字数据重叠的子数字数据记录到盘上，从而针对由主数字数据记录的单个内容，所述光盘上的多个区域存储相同子数字数据。

通过参考下面结合附图所作的描述和权利要求将更前面地理解本发明的其它目的和实现。

附图说明

图1描绘了本发明第一实施例中的光盘的区域；

图2是图1中的鉴别区的放大示意图；

图3描绘了本发明第一实施例中由子数字数据组成的调相比特；

图4是本发明第一实施例中的光盘再生装置的方框图；

图5A示出其中记录了子数字数据的轨迹；

图5B示出再生图5A所示的轨迹时相位比较器的输出信号波形；

图5C示出再生图5A所示的轨迹时低通滤波器的输出信号波形；

图5D示出再生图5A所示的轨迹时幅度检测器的输出信号波形；

图6描绘了本发明第一实施例中的另一个光盘的区域；

图 7 描绘了本发明第一实施例中的再一个光盘的区域；

图 8 描绘了本发明第一实施例中的再一个光盘的区域；

图 9 描绘了记录到光盘的内容鉴别数据与记录鉴别数据的鉴别区之间的关系；

图 10 描绘了在径向方向移位以记录子数字数据的调制；

图 11 描绘了本发明第一实施例中的再一个光盘的区域；

图 12 描绘了本发明第一实施例中的再一个光盘的区域；

图 13 是根据现有技术的非法复制产生系统的方框图；

图 14A 描绘了光盘的区域；

图 14B 描绘了调制子数字数据的方法；

图 14C 描绘了管理信息的内容；

图 15 是表示根据本发明第二实施例的光盘记录装置的方框图；

图 16 是表示第二实施例的记录装置中的格式化器的详细配置的方框图；

图 17 是表示第二实施例的记录装置中的调相器的详细配置的方框图；

图 18 是表示第二实施例的记录装置中的子数字数据发生器的详细配置的方框图；

图 19 是表示由第二实施例的记录装置形成的凹坑抖动的频率分布曲线；

图 20 是第二实施例的记录装置中的主信号的定时图；

图 21 示出了保密密钥，伪随机数序列，和记录数据之间的关系；

图 22 是根据本发明第二实施例的记录装置中的主信号的定时图；

图 23A 示出光盘的区域；

图 23B 描绘了管理信息的内容；

图 24A 示出光盘的区域；

图 24B 描绘了管理信息的内容；

图 25 是根据本发明第二实施例的光盘再生装置的方框图；

图 26 是表示本发明第二实施例的光盘再生装置中的时钟提取部分的

详细配置的方框图；

图 27A 是表示时钟提取部分中相位误差信号分离器的配置的电路图；

图 27B 是用于描绘相位误差信号分离器的操作的信号的定时图；

图 28 是表示根据本发明第二实施例的光盘再生装置中的再生信号处理器的详细配置的方框图；

图 29 是表示根据本发明第二实施例的光盘再生装置中的同步检测器的详细配置的方框图；

图 30 示出根据本发明第二实施例的光盘再生装置中从积分器输出的模拟信号波的实例；

图 31 是表示根据本发明第二实施例的光盘再生装置中的验证部分的详细配置的方框图；

图 32 是位移图案门脉冲的定时图；

图 33 描绘了现有技术的光盘的记录区；

图 34 描绘了根据本发明第三实施例的光盘中的控制数据区和用户数据区；

图 35 是根据本发明第三实施例的光盘记录装置的方框图；

图 36 是根据本发明第三实施例的光盘记录装置中的主信号的定时图；

图 37 是表示根据本发明第三实施例的光盘记录装置中的加密部分的详细配置的方框图；

图 38 是表示根据本发明第三实施例的光盘记录装置中的格式化器的详细配置的方框图；

图 39 示出了加密密钥，伪随机数序列，和记录数据之间的关系；

图 40 是表示根据本发明第三实施例的光盘记录装置中的伪随机数发生器的配置的电路图；

图 41 是表示根据本发明第三实施例的光盘记录装置中调相器的详细配置的方框图；

图 42 示出了具有由根据本发明第三实施例的光盘记录装置形成的比

特的 DVD 的表面；

图 43 是表示从由根据本发明第三实施例的光盘记录装置形成的凹坑抖动的频率分布的曲线；

图 44 是表示根据本发明第三实施例的光盘记录装置的配置的方框图；

图 45 是表示根据本发明第三实施例的光盘记录装置中的时钟提取部分的详细配置的方框图；

图 46A 是表示时钟提取部分中的相位误差信号分离器的配置的电路图；

图 46B 是用于描绘相位误差信号分离器的操作的信号定时图；

图 47 是表示根据本发明第三实施例的光盘再生装置中的再生信号处理器的详细配置的方框图；

图 48 是表示根据本发明第三实施例的光盘再生装置中的同步检测器的配置的电路图；

图 49 示出从根据本发明第三实施例的光盘再生装置中的积分器输出的模拟信号波的实例；

图 50 是表示根据本发明第三实施例的光盘再生装置中的加密密钥再生电路的详细配置的方框图；

图 51 描绘了在非法产生的启动信号输入到光盘再生装置时的操作；

图 52 示出了不具有识别合法盘和非法盘的功能的光盘再生装置；

图 53 描绘了从外部向光盘再生装置馈送非法加密密钥的输入；

图 54 示出了加密编码器的详细配置；

图 55 示出了典型的加密方法；

图 56 描绘了作为布置到每个 ECC 块的子数字数据记录的加密密钥；

图 57 是表示根据本发明第四实施例的光盘再生装置中的加密密钥再生电路的详细配置的方框图；和

图 58 描绘了作为布置到每个 ECC 块的子数字数据记录的加密密钥。

具体实施方式

下面参考附图描述根据本发明优选实施例的光盘，光盘记录和再生方法。

<实施例 1>

图 1 示出根据本发明第一优选实施例的光盘的配置。

如图 1 所示，光盘 10 具有存储控制数据的控制区 12，鉴别区 13，和存储内容的数据区。

在本地调相的参考时钟的定时将比特序列记录到鉴别区 13。在再生期间检测该调相的比特序列作为高抖动分量。通过在鉴别区 13 中组合高抖动部分和正常抖动部分来将盘鉴别数据叠加到高和低抖动分量的时基序列。

具有与时钟的调相无关的比特序列图案的正常数据被称为“主数字数据”，使用调相的比特和未调相的比特的再生性能中的差异获得的数据在下面被称为“子数字数据”。在本发明的实施例中用该子数字数据作为盘鉴别数据，但不能用于其它数据。

图 2 是图 1 中的鉴别区 13 的放大图。如图 2 所示，轨迹 Tr 具有在参考时钟定时记录的区域 R2 和 R4，以及在调相时钟定时记录的区域 R1，R3，R5。再生期间在区域 R1，R3，R5 中检测高抖动电平。

可以用不同方式确定每个区域 R1 至 R5 的长度。例如，可以以扇区单元测量每个区域的长度，并等于一个或多个扇区的长度。作为替换，可以以纠错块或轨迹单元测量每个区域的长度，并在长度上等于一个或多个纠错块或轨迹。具体地说，每个区域的长度只需要足以启动再生装置（播放机）检测抖动电平的差异。

通过增加在调相时钟定时记录的一个区域的长度，即使在鉴别区中存在划痕或其它缺陷，也可正确地再生鉴别数据。同样，增加在参考时钟定时记录的一个区域的长度，也可降低在被错误地检测为记录鉴别数据的区域的参考时钟定时记录的区域的可能性。

此外，可在调相时钟定时记录区域 R1，R3，R5 中的所有凹坑，或在调相时钟定时可只记录一部分凹坑。图 3 示出了在记录 3T 信号的调相时钟定时记录的凹坑的例子。

图 3 中的凹坑 31 至 35 是 3T 信号中的凹坑，其中 T 时钟周期，垂直行表示时钟定时。凹坑 31 是在参考时钟定时记录的凹坑。凹坑 32 是在调相时钟定时记录的凹坑，以便具有两个相对于时基超前的边缘。凹坑 33 是在调相时钟定时记录的凹坑，以便具有两个相对于时基滞后的边缘。凹坑 34 是在调相时钟定时记录的凹坑，以便具有相对于时基的超前开始边缘和滞后结束边缘。凹坑 35 是在调相时钟定时记录的凹坑，以便具有相对于时基的滞后开始边缘和超前结束边缘。

其它调相图案也是可能的。例如，可在仅调相一个边缘的时钟定时记录凹坑。通过如此在部分调相时钟定时进行记录，增加了区域 R1, R3, R5 中的抖动，并可增加与每个区域中的抖动量对应的盘鉴别数据。最好是设定要加入的实际相位误差，以便可达到足够的检测灵敏度并且不增加再生信号误差。实现该条件的调相量被认为是时钟周期的 1/8 至 1/4。

因此，在鉴别区 13 中存在具有局部高抖动的区域。与其它区域相比，这些区域具有较高的不能被正确再生的可能性。因此，在本实施例中用鉴别区 13 作为确定该盘是否是被许可盘的专用区。就是说，通过提供与控制区 12 和数据区 14 分开的鉴别区 13，可正确地播放用于再生该盘的控制区 12 中记录的数据，和数据区 14 中记录的内容。

此外，通过用鉴别区 13 作为专用区，盘制造商可以根据需要在鉴别区 13 中配置主数字数据，例如，将盘鉴别数据插入主数字数据。通过组合主数字数据中的鉴别数据与子数字数据中的鉴别数据，在进行非法复制时，变得需要准确地复制两组数据，因而使非法盘的生产更困难。

当不需要在写到鉴别区 13 中的主数字数据中插入其它特定信息时，可记录包含具有诸如最短标记之类的高抖动电平并且没有凹坑的图案。这样可以降低时钟不是调相的区域中的抖动，从而增加不存在时钟的调相的区域与时钟被调相的区域之间的动态范围，并且在即使是在作为光盘或再生头被弄脏的结果存在抖动整体下降时，也可降低检测误差。应该指出，在以希望的图案形成具有诸如最短标记之类的高抖动的凹坑时，也可不通过对时钟调相来实现该效果。

在不需要向写入识别区 13 的主数字数据中插入其它特定信息时，也

可以记录包含许多同步图案的图案。这增加了失去 PLL 同步的误差的余量，增加了能够进行时钟的调相的区域，使其能够准确地检测子数字数据。

应该指出，在该实施例中将识别区 13 描述为用于盘识别的专用区，如果在控制区 12 和数据区 14 中反复写入相同的主数字数据，或如果即使是由纠错造成抖动增加时也能正确地再生主数字数据识别区 13 可与控制区 12 或数据区 14 重叠，或一部分识别区 13 可与控制区 12 或数据区 14 重叠。这使其能够增加数据区 14 的容量。

还可以根据有关识别区 13 的位置的信息，就是说，识别区 13 是否是专用区，或是否在控制区 12 中，或是否在数据区 14 中，或识别区 13 的一部分是否与控制区 12 或数据区 14 重叠来确定光盘 10 是否是合法盘。例如，如果识别区 13 的一部分与控制区 12 重叠，在播放盘时如果不能从控制区 12 检测到子数字数据，则可确定该盘不是合法盘。

可将有关识别区在合法盘上的位置的信息记录到光盘 10 的特定区，或可存储在再生装置中。该信息可通过付费系统经网络获得。可通过存储所需信息的 IC 卡，并将其插入再生装置捕获该信息。

如果可通过付费系统获得该信息，可将该信息与专用于再生装置的其它数据相联系。如果将该信息有与专用于再生装置的数据组合，则可在不同的再生装置中播放相同的光盘，可从不同的再生装置收集附加费。

如果该位置信息存储在盘上的特定位置，可将位置信息记录到多个这样的位置。可以保证可靠地获得数据。此外，可记录位置信息作为子数字数据。

图 4 是用于检测作为子数字数据记录到识别区 13 的识别数据和确定该盘是否是合法盘的再生装置的方框图。如图 4 所示，该再生装置包括再生头 401，再生放大器 402，数字化器 403，PLL 电路 404，相位比较器 406，幅度检测器 408，低通滤波器 409，压控振荡器 (VCO) 410，触发器 411，图案比较器 418，和数字信号处理器 420。下面描述盘识别处理。

再生头 401 首先根据上述位置信息再生或播放光盘 10 的识别区 13。

然后由再生放大器 402 放大再生信号，由数字化器 403 进行数字化，并将数字信号 405 输入到 PLL 电路 404。PLL 电路 404 从信号 405 产生时钟信号 414。触发器 411 根据时钟信号 414 的定时同步信号 405，并将得到的再生信号 412 输入到数字信号处理器 420。

PLL 电路 404 的相位比较器 406 把从 VCO410 输出的时钟信号 414 的相位与信号 405 的相位比较，并输出信号 407。低通滤波器 409 限制信号 407 的带宽并产生信号 416。VCO 410 根据信号 416 产生再生时钟信号 414。

如果信号 405 的变化超出 PLL 电路 404 的跟踪操作带宽，时钟信号 414 不跟随信号 405 的变化，PLL 电路 404 不从正常时钟偏移。因此，在时钟和特定调相区 R1, R3, R5 中的信号 407 的信号边缘之间出现相位误差，即抖动。

幅度检测器 408 整流，平滑，和数字化信号 407 以输出信号 413。然后可从该信号 413 的图案识别该识别数据。

图 5 是在再生图 2 所示的区域 R1 至 R5 时产生的各种信号的定时图。图 5A 示出图 2 中的区域 R1 至 R5。图 5B 示出再生每个区域时产生的信号 407。图 5C 示出信号 416。图 5D 示出信号信号 413。

此后，图案比较器 418 将信号 413 的图案与密钥数据 417 的图案比较，并向数字信号处理器 420 输出得到的信号 419。下面进一步描述该密钥数据 417。数字信号处理器 420 应用纠错和解调再生信号 412，如果信号 413 和密钥数据 417 的图案匹配，则输出正常再生信号 421。如果信号 413 和密钥数据 417 的图案不匹配，由信号 419 限制信号再生。很显然，可以以不同方式限制该再生，包括：例如，禁止所有信号再生，降低传送率，以恶化图象质量，或间断的再生。

此外，如果等同地施加如图 3 所示超前凹坑边缘诸如 32 个凹坑的时基的调相和延迟凹坑边缘诸如 33 个凹坑的时基的调相，平均相位误差是 0，并且利用调相记录的凹坑边缘的 PLL 跟踪将更加困难。

在正常数据再生期间，再生时钟因调相而不跟踪再生信号变化，因此能够输出再生信号，其中已从该再生信号移去闭锁从数字化器 403 输

出的信号 405 触发器 411 的结果的抖动。同样，当使用如图 13 所示的装置非法复制光盘时，移去用作识别数据的抖动作为由触发器 2007 同步的结果，从而失去识别数据，并且能够确定该复制是否是非法复制。

下面描述密钥数据 417，为确定该盘是否是非法盘，在制造光盘时，把密钥数据与通过时钟调相记录的识别数据的特定关系作为正常的二进制数据记录到盘的识别区 13 中。再生期间，把密钥数据与从抖动中的波动检测的识别数据进行比较，仅当检测到特定相关时，确定该盘为合法复制。

例如，假设密钥数据 417 的图案为“10101”，从幅度检测器 408 输出的信号 413 中的高电平和低电平分别是 1 和 0。如果在再生光盘 10 的识别区 13 时从 1 开始的图案是“10101”，密钥数据和识别数据则匹配，并且识别光盘 10 为合法复制。

应指出，可以将合法复制的密钥数据记录到光盘 1 的特定区域，或可将其记录在再生装置中，可通过付费系统经网络获得。另外，可通过插入再生装置、存储有所需信息的 IC 卡获得密钥数据。

如果通过付费系统经网络获得密钥数据，可将该信息与专用于再生装置的其它数据结合。如果该数据与专用于再生装置的数据组合，然后在不同的再生装置中播放相同的光盘，可从不同的再生装置收取附加费。

如果将密钥数据存储到盘的特定区，数据则可记录到多个位置。这样确保了可靠地获得数据。此外，可记录该密钥数据作为子数字数据。

在本发明的优选实施例中，在调相的时钟定时记录到特定盘区的数据在特定盘区和在基准时钟定时记录的盘区之间产生抖动差异，并通过向每个区域中的不同抖动的时基安排传递有意义的信息来产生识别数据图案。然而，图案长度和配置不限于此，这种情况下可通过在调相的时钟定时进行记录来构成识别数据。例如，识别数据可以是仅在一个部分包含高抖动电平的简单图案，或是该那些在指示该图案是识别数据的开始处具有特定图案，而其余图案用虚拟数据填充。

此外，当在本优选实施例中使用时图 4 所示的再生装置确定播放的盘是否是合法复制时，可使用不同配置的再生装置，这种情况下，再生装

置检测在调相的时钟定时记录的区域和在基准时钟定时记录的其它区域之间的抖动差异，提取记录的图案，将该图案与密钥数据比较，并根据比较结果确定该盘是否位合法复制。

例如，如果能够确定每个标记是否是在调相时钟定时记录的标记，可对在调相时钟定时在一个区域中记录的标记数量计数。如果计数超过特定阈值，则确定该区域为“1”，如果未超过，则确定该区域为“0”。作为替换，可提供特定选通信号，并对选通信号为高电平期间以调相的时钟定时记录的标记数量计数。

此外，如果能够确定是利用调相的时钟定时记录每个标记的前和后边缘，则可对特定区域中该边缘的数量计数。如果计数超过特定阈值，则确定该区域为“1”，如果未超过，则确定该区域为“0”。此时，可提供特定选通信号，并可对选通信号为高电平期间利用调相的时钟定时记录的边缘数量计数。

下面参考表格进一步描述上述确定过程。当利用标记边缘记录方法记录以行程长度受限（2，10）调制来调制的数据时，存在着范围从最短长度为 3T 到最长长度为 11T 的标记和空间，其中“T”是基准周期。

表 1 是调相的边缘的表。例如，“3S3M”表示 3T 标记在 3T 跟随 3T 空间的信号中的前边缘的调相。同样，“4S4M”表示 4T 标记在 4T 跟随 4T 空间的信号中的前边缘的调相。应该指出，标记和空间比 6T 长的表与用于 6T 的表相同。标记和空间在表中分别分成四个组，但可使用不同的组。还可以产生只有标记或只有空间的表，来代替标记和空间的组合。

表 1

	3T 标记	4T 标记	5T 标记	6T 标记
3T 空间后	3S3M	3S4M	3S5M	3S6M
4T 空间后	4S3M	4S4M	4S5M	4S6M
5T 空间后	5S3M	5S4M	5S5M	5S6M
6T 空间后	6S3M	6S4M	6S5M	6S6M
3T 空间前	3M3S	4M3S	5M3S	5M3S
4T 空间前	3M4S	4M4S	5M4S	6M4S
5T 空间前	3M5S	4M5S	5M5S	6M5S
6T 空间前	3M6S	4M6S	5M6S	6M6S

表 2 示出将阈值插入到表中的值的密钥数据。在这种情况下，在盘的特定区域中对在调相的时钟定时记录的边缘的数量计数。确定该盘的许可的，例如，如果在 3T 标记跟随 3T 空间的信号中 3T 标记的前缘的调相（3M3S）计数是 10 或更大，在 6T 或更长的标记跟随 5T 空间的信号中 6T 或更长标记的前缘的调相（5M6S）计数是 20 或更大，在 5T 空间跟随 4T 标记的信号中 4T 标记的后缘的调相（4M5S）计数是 30 或更大，在所有其它边缘的计数小于 10

表 2

	3T 标记	4T 标记	5T 标记	6T 标记
3T 空间后	10	0	0	0
4T 空间后	0	0	0	0
5T 空间后	0	0	0	20
6T 空间后	0	0	0	0
3T 空间前	0	0	0	0
4T 空间前	0	0	0	0
5T 空间前	0	30	0	0
6T 空间前	0	0	0	0

应该指出，上面的解释使用表格作为确定盘许可的密钥数据，但作为替换，也可用该表作为特定选通信号。这将参考表 3 描述。

这种情况下，对在 3T 标记跟随 3T 空间的信号中的 3T 标记的前缘的调相边缘计数，对在 6T 或更长标记跟随 5T 空间的信号中的 6T 或更长标记的前缘的调相边缘计数，对在 5T 空间跟随 4T 标记的信号中的 4T 标记的后缘的调相边缘计数，如果这些计数在特定范围中，则确定该盘作为合法复制是许可。

表 3

	3T 标记	4T 标记	5T 标记	6T 标记
3T 空间后	1	0	0	0
4T 空间后	0	0	0	0
5T 空间后	0	0	0	1
6T 空间后	0	0	0	0
3T 空间前	0	0	0	0
4T 空间前	0	0	0	0
5T 空间前	0	1	0	0

6T 空间前	0	0	0	0
--------	---	---	---	---

也可以使用通过在调相的时钟定时记录在特定盘区域中的边缘计数，并在计数值是 10 或更高时分配“1”，和在计数值小于 10 时分配“0”获得的表（例如表 3）加扰的数据解扰。

应该指出，如何使用和编译用于盘许可和解扰的表不限于在此描述的这些内容。

如果可对每个边缘识别在调相的时钟定时记录的每个边缘的相位超前和滞后，作为替换，可以进一步，例如，对计数超过阈值时的相位超前边缘的数量计数以确定“1”，或对计数未超过阈值时的相位超前边缘的数量计数以确定“0”。作为替换，可提供选通信号，以便当该选通信号是高时，对相位超前的边缘的数量计数，当该选通信号是低时，对相位滞后的边缘的数量计数。然后，在两个计数值的总和超过一个阈值时，检测“1”，总和未超过该阈值时，检测“0”。

应该进一步指出，在如图 2 中所示的区域 R1 至 R5 邻接的识别区 13 中只有一个区域，但是，很显然，可有多个这样的区域。设置多个这样的区域使得在例如一个这样的邻接区域划伤时，和从该区域不能正确检测到识别数据时，通过从另一个邻接区域检测识别数据进行盘的许可成为可能。

同样，在该实施例中，当只有一个设置在盘的内圆周区的识别区 13 时，可提供多个识别区。设置多个识别区使得在例如一个区域被划伤时，和从该区域不能正确检测到识别数据时，通过从另一个识别区检测识别数据进行盘的许可成为可能。

如图 6 所示，例如，如果在盘的内和外圆周部分设置识别区 13a 和 13b，即使一个识别区被划伤，翘曲，或其它损伤，并且不能检测识别数据时，通过从其它区域检测识别数据，则不能确定该盘是否为合法复制。

此外，可将不同的识别数据写入多个识别区。这种情况下，如果不能检测所有识别数据或如果不能检测识别数据的特定数量，则限制再生。此外，提供多个不同的识别数据使设计用于制造非法复制的设备更加困难，从而进一步加强了版权保护。

也可以将多个不同的识别数据记录的单个识别区，如果不能检测到

所有或特定量的识别数据，则限制再生。以这种方式提供多个不同识别数据也使设计用于制造非法复制的设备更加困难，从而进一步加强了版权保护。

该实施例检测识别区中的密钥数据和识别数据之间的相关性，以确定该盘是否是合法复制，如果该盘不是合法复制则限制再生。作为替换，例如，也可以在规则的时间间隔检测识别区中的密钥数据和识别数据之间的这种相关性，如果不再确认期待的相关性，则禁止再生。在规则的时间间隔检测到该相关性的情况下，当提供了多个识别区时，可再生与该再生数据最近的识别区。因此，不必再生预先再生的识别区。

也不必在数据再生前或刚刚在再生开始后检测密钥数据与识别区中的识别数据之间的相关性。作为替换，例如，可以在内容再生开始后在特定周期检测该相关性。

虽然该方法允许即使从非法复制的盘播放一部分内容，该方法在特定时间周期之后仍限制再生，从而保护合法复制的版权，虽然也能够使用用于播放广告的预定时间。另外，例如当通过付费系统获得密钥数据时，可以提供允许用户从合法复制观看一部分内容的系统，以决定是否付费观看其余内容。

当将多个内容标题记录到单个盘时，作为替换，可将每个标题分开地记录识别数据。这种情况下，也可将未检测到密钥数据和识别数据之间的相关性的内容记录到该盘。

下面参考图 7 和图 8 进一步描述识别数区在盘上的布置。

参考图 7，将第一内容标题记录到数据区 14a，对应的识别数据记录到识别区 13a。第二标题记录到数据区 14b，对应的识别数据记录到识别区 13b。如上所述，识别区 13a 和 13b 可以是专用区，或可完全或部分地与控制区 12 或数据区 14a，14b 重叠。如图 7 所示，通过在内圆周区查找识别区 13a，13b，可以在启动时再生控制区后来再生识别区，并可立即获得限制再生所有盘内容的数据。

在图 8 中，将第一内容标题记录到数据区 14a，对应的识别数据记录到识别区 13a。第二标题记录到数据区 14b，对应的识别数据记录到识别

区 13b。识别区 13a 和 13b 可以是专用区，或可完全或部分地与控制区 12 或数据区 14a, 14b 重叠。如图 8 所示，通过查找最接近对应的数据区 14a, 14b，可以在刚刚播放希望的内容前检测到对应的识别数据。因此，不需要检测或存储不必要的内容识别数据。从而可减少启动时间和存储器的需求。

虽然这样能从非法复制的盘播放某些内容，但保护了特定内容的版权。

当从付费系统获得特定识别数据的密钥数据时，也可将其提供给再生系统，以允许在用户决定是否观看其它各个内容标题前来观看原始盘上的免费内容。另外，也可设定为获得对多个标题访问所付的费用比获得对每个标题访问所付的费用低。

作为替换，也可在特定径向位置或特定地址单元，而不是以特定时间间隔查找识别区，以便当经过识别区时，检测密钥数据和识别区中的识别数据之间的相关性，然后在未确认相关性时限制再生。例如，当在光盘上存在多个较短持续时间的标题时，或当制造该光盘以允许随机存取游戏时，该技术加强了版权保护。

使用如上所述的识别区进行版权保护不限于单层盘介质。同样，通过在每层上提供识别区，也可在具有两层或多层再生层的盘介质中提供版权保护。为各个内容标题提供识别数据对多层盘介质更有效，因为多层盘的容量更大，可向单个盘记录更多内容。

借助如上所述的识别区进行版权保护也不限于只读盘介质。同样，通过向盘或内容提供识别区，也可将版权保护应用到可记录的盘介质。

图 9 示出内容识别数据与记录了识别数据的识别区之间的关系的例子。如图 9A 所示，当在单个盘上提供包括一个识别区 A 和另一个识别区 B 的两个识别区时，例如，可将内容 A 的识别数据记录到诸如图 9B 所示的识别区。

例如，为内容 A 提供识别数据 A1 时，如图 9B 所示，可将识别数据 A1 存储在识别区 A 或识别区 B 中，或识别区 A 和 B 二者中。另外，可将识别数据 A1 记录到识别区 A 中的多个区域（图 9B 中为两个）。

此外，当为内容 A 提供识别数据 A1, A2 时，可将两个识别数据 A1, A2 记录到一个识别区（A 或 B），或分开在识别区（一个到 A，另一个到 B）。也可将相同的识别数据记录到识别区 A 和识别区 B。

很显然，可以用各种方式将识别数据记录到识别区。

在该实施例中，针对光盘作为记录介质的例子进行了上面的描述，但本发明不限于光盘。记录介质可以包括所谓的 CD-ROM, DVD-ROM, CD-R, CD-RW, DVD-RAM, DVD-RW, MD 等等。就是说，本发明不仅可应用于记录到凹凸不平的凹坑，而且可应用于相位改变型的薄膜，磁膜等。本发明可应用于采用不仅使用凹坑，而且可应用于使用相位改变（转移）或磁化之类只要写入凹坑（记录标记），以便通过抖动调制凹坑位置的记录方法的其它记录介质。应该指出，对于记录装置，可将与图 15 所示相同配置和操作的记录装置应用到该实施例。

从上面的描述已知，在本发明的实施例中用在调相的时钟定时记录的凹坑作为写入识别区的识别数据，但用于产生识别数据的方法不限于此，也可使用其它方法。例如，可通过如图 10 所示在径向略微移动该凹坑的调制来产生识别数据。此外，在记录识别数据时利用多个重叠方法可更有效地防止非法复制。

应该指出，本实施例未考虑以不同的线速度旋转盘。然而，在提高线速度可能降低信噪（S/N）比时，不能正确地再生与子数字数据重叠的区域中的主数字数据，甚至因为失去 PLL 同步造成不能再生子数字数据。因此，最好根据用于再生的线速度配置识别区。图 11 示出该例子。

在图 11 中，识别区 13a 是用于以第一线速度再生数据区 14 的识别区。识别区 13b 是用于以第二线速度再生数据区 14 的识别区。如果第二线速度比这种情况下的低于线速度快，识别区 13b 中的相位误差比识别区 13a 中的相位误差少，可以在任何一种线速度正确地检测识别数据。

因此，通过根据线速度提供多个识别区，即使在以各种不同的线速度再生该内容，并因此减少检测所需的时间时，不用恢复特定的线速度即可检测识别区。还应该指出，通过查找线速度比盘的外圆周部分高的识别区可减少电机速度的波动。

还应该指出，记录到识别区的识别数据可以是以不同线速度记录的相同识别数据，或以各不相同线速度记录的不同识别数据。通过根据用于再生的线速度改变识别数据可防止非法的高速再生。此外，当从付费系统获得识别数据的密钥数据时，可根据线速度设定付费系统，以便例如在高线速度的付费比在低线速度的付费高。

在考虑再生头性能中的区别时，也可优选地提供多个识别区。图 12 示出了该例子。在图 12 中，识别区 13a, 13b 使用相同识别数据，在相位中调制时钟定时相位误差不同。因此，通过提供具有不同相位误差等级的多个识别区，当再生头的性能不同时，可在这些识别区之一中正确地检测识别数据。

利用使用在调相时钟定时记录的凹坑产生的数据作为该优选实施例中的盘或识别数据，但本发明不限于此，当该数据用于与盘或内容有关的其它信息时可实现相同的效果。

在本实施例中，通过形成与记录内容的区域分开的识别区，在内容再生期间可不增加抖动地正确再生该内容。另外，盘制造者可以自由设计识别区中的主数字数据，以便例如也可通过将盘识别数据插入主数字数据来加强版权保护。

此外，通过为单个内容标题提供包含相同识别数据的多个识别区，即使在一个识别区被划伤或损坏以致不能由此检测识别数据时，通过从不同识别区检测该识别数据能够可靠地检测该识别数据。

此外，可为单个内容标题提供包含不同识别数据的多个识别区，因此，通过多个识别区使生产非法复制盘更困难。

此外，可为不同内容标题提供不同识别区，并因此可保护各个版权。

<实施例 2>

（光盘记录装置）

图 14 示出根据本发明第二实施例的光盘（光记录介质）的配置。如图 14A 所示，光盘 10 具有用户数据区 10a 和引入区 10b。图 14B 示出写入数据区的子数字数据的调制方法。图 14C 示出写入引入区的管理信息

207 的内容。管理信息 207 包括盘管理信息 208 和子数字数据管理信息 209。子数字数据管理信息 209 包括阈值数据 210, 子数字数据位置数据 212, 和子数字数据位移图案数据 213。

下面参考图 14 描述操作。通过激光切割（暴露）通过根据特定的调制规则形成邻接的凹坑（31）序列在盘制造过程的主图案产生过程中形成轨迹 32。通过在将激光点在扫描方向移动遇到距离，同时在特定位置或以特定长度切割凹坑，在切割凹坑 31 时使凹坑 31 的边缘超前或滞后。

将边缘位移调制到对由特定比特表示的信息的再生信号影响不大的范围，并允许通过累积比特位移来检测比特。通过略微移动凹坑边缘位置作为抖动嵌入盘的信号是子数字数据。另一方面，以规则的间隔，利用记录标记的边缘位置信息记录正常记录的数据（主数字数据）。具有根据本发明的非法复制保护功能的光盘具有读取预先记录到该盘的子数字数据所需的子数字数据管理信息，和检测该子数字数据（保密密钥）并基于检测结果确保版权保护的功能。

下面描述根据本发明制造光盘的方法。图 15 是表示根据本发明的光盘记录装置 100a 的主要部分的方框图。

记录装置 100a 是记录诸如 DVD-ROM 盘之类的光盘的系统。除了使用可光学读取的记录标记记录该主数字数据外，还具有通过对记录标记的边缘调相来将数字水印（下文称为保密密钥）作为子数字数据记录的能力。如图 15 所示，记录装置 100a 具有格式化器 120，子数字数据发生器 121，相位调制器 107，记录通道 108，记录头 109，主轴伺服 123，和主轴电机 125。

格式化器 120 是用于控制主数字数据（记录标记）的调制，指定子数字数据，和记录子数字数据的控制电路。

图 16 是表示格式化器 120 的详细配置的方框图。格式化器 120 具有调制器 102a，初始值存储器 102e，保密密钥存储器 102f，和子数字数据管理详细存储器 102d。调制器 102a 把输入到记录装置 100a 的记录标记调制成适合于光盘 10 的信号。初始值存储器 102e 秘密地预存储子数字数据发生器 121 产生子数字数据所需的伪随机数序列的初始值。保密密

钥存储器 102f 预存储保密密钥。子数字数据管理信息存储器 102d 在盘预存储诸如子数字数据的记录位置信息之类的管理信息（例如，子数字数据，阈值数据，累积值数据，子数字数据位移图案信息）。

如图 20 的定时图所示，调制器 102a 把 8 比特码元（字节）单元中的输入记录数据转换成对应的 16 比特通道代码 A（8 到 16 调制），然后，施加 NRZI 转换以产生通道信号 B，并输出到相位调制器 107。

调制器 102a 输入记录数据以及子数字数据管理信息。调制器 102a 由此产生通道信号 B 并输出到相位调制器 107。

图 18 是表示子数字数据发生器的详细配置的方框图。当调制器 102a 从控制器（图中未示出）接收到开始记录保密密钥的命令时（该操作在下文中被称为“保密密钥记录模式”），每当输入记录数据的一个字节时，它向定时发生器 121a 输出指示字节开始的定时信号。

在保密密钥记录模式开始时，初始值存储器 102e 输出预先秘密存储到伪随机数发生器 121b 的保密的 15 比特数据（初始值）。

在保密密钥记录模式开始时，保密密钥存储器 102f 在从 LSB 开始的时间以一个比特的 NRZ 格式向 XOR（“异”门）121c 秘密地预先存储的 56-比特保密密钥。每当调制器 102a 调制 256 字节的记录数据时，保密密钥存储器 102f 输出下一个最高比特。换句话说，保密密钥存储器 102f 按比特顺序向 XOR 121c 输出单个 56-比特保密密钥，作为与记录数据总共 256×256 个字节对应的保密密钥比特序列。

图 21 示出保密密钥，伪随机数序列，和记录数据之间的相关性。为了把 56-比特保密密钥记录到光盘作为数字水印，把 56-比特伪随机数序列用于保密密钥的每个比特，在 1 字节的记录数据（16-比特通道代码）中嵌入该伪随机数序列的每个比特。应指出，用该 56-比特保密密钥的每个比特作为指示对应的 256-比特伪随机数序列是否被逻辑反转的标志，下文更详细地描述。

定时发生器 121a (i) 根据来自调制器的定时信号向伪随机数发生器 121b 输出与记录数据的每个字节同步的时钟信号（字节时钟），和 (ii) 根据该定时信号和来自时钟振荡器（图中未示出）的时钟信号向伪随机

数发生器 121b 输出指示从格式化器 102 输出的通道信号 B 的中心（相位是 180 度的点）的定时信号。

伪随机数发生器 121b 使用来自初始值存储器 102e 的初始值作为预设值，来自定时发生器 121a 的字节时钟作为移位时钟来产生每个周期具有 2^{15} 个比特序列的伪随机数序列（M 序列）。

应指出，在该实施例中，用伪随机数发生器 121b 产生嵌入到总共 256 X 256 个字节记录数据的伪随机数序列，即，在保密密钥记录模式中为 256 X 56 比特的伪随机数序列。

XOR 121c 对来自伪随机数发生器 121b 和来自保密密钥存储器 102f 的比特序列执行“异”运算，并向 PE 调制器 121d 输出得到的伪随机数序列 D。换句话说，XOR 121c 由选择地直接向 PE 调制器 121d 输入为 56-比特保密密钥的每个比特产生的伪随机数序列，或对其进行逻辑反转，并输入到 PE 调制器 121d。

PE 调制器 121d 根据来自定时发生器 121a 的定时信号对来自 XOR 121c 的伪随机数序列 D 进行 PE 转换，并向调相器 107 输出得到的 PE 调制信号 E。结果是，如图 20 中的定时图所示，当来自 XOR 121c 的伪随机数序列 D 是 0 时，PE 调制信号 E 落在通道信号 B 的中部，当伪随机数序列 D 是 1 时上升，在相同的随机值重复时在通道信号边缘再次反转。

调相器 107 根据来自 PE 调制器 121d 的 PE 调制信号 E 对来自格式化器的通道信号 B 的边缘进行调相，以延迟或超前短的恒定时间，并向记录通道 108 输出得到的调制通道信号 F。应指出，将该短时间预设到在旁路该调相器（不记录子数字数据）和在正常的盘读取器上播放仅记录主数字数据的正常光盘时观察到的抖动的频率分布的标准偏差 σ 的一半值（ $\sigma/2$ ）。

图 17 是表示调相器 107 的详细配置的方框图。调相器 107 具有把输入信号延迟上述短时间的延迟器 107a，2-输入，1-输出选择器 107b。当作为控制信号输入的选通信号是 1 时，选择器 107b 使从格式化器 102 直接输入的通道信号 B 通过。当选通信号是 0 时，选择器 107b 经过延迟器 107a 使输入的通道信号通过。

结果是，当选通信号是 1 时（0 或 180 度），输入到调相器 107 的通道信号 B 的上升和下降沿的相位超前上面指出的短时间，当选通信号是 0 时（180 或 360 度），延迟该短时间。换句话说，根据子数字数据发生器的输出抖动调制输入到调相器 107 的通道信号 B，并转换成调制的通道信号 F。

记录通道产生控制信号并将该控制信号发送到记录头 109，该控制信号与来自调相器 107 的调制的通道信号 F 的输入/输出同步地切换发射到光盘的激光束的通/断。根据从记录通道产生的控制信号，记录头 109 通过发射激光束同时切换激光束通和断将记录标记刻到旋转光盘 10 的表面上的螺旋图案中。结果是，在光盘中形成包括可光学读取的凹坑和纹间表面的调制的记录标记。

图 14B 示出上面由记录头形成凹坑的光盘的记录表面。利用超前（或延迟）位移等于与在未记录子数字数据时形成的边缘位置有关的恒定短时间的相位在凹坑记录子数字数据的光点的扫描方向中形成两个边缘。

图 19 是表示针对在记录子数字数据，即利用抖动调制记录的调制的记录标记时形成的凹坑观察到的抖动的频率分布的曲线。

曲线 A 表示仅在选通信号是 0 时产生的调制记录标记的边缘的抖动分布，并且是其中最高频率是相位在延迟或滞后方向移位该位移的位置 X (L) 的近似高斯分布。曲线 B 是仅在选通信号是 1 时产生的调制记录标记的边缘的抖动分布，并且是其中最高频率是相位在超前或提前方向移位该位移的位置 X (H) 的近似高斯分布。曲线 C 表示组合曲线 A 和 B 的整个抖动分布。

本发明通过用相同伪随机数作为记录该保密密钥的伪随机数的同步检测，使用将曲线 C 的抖动分布分成曲线 A 和 B 的能力。

（子数字数据管理信息）

下面描述用于管理上述子数字数据的子数字数据管理信息。

子数字数据管理信息是指读取（提取）子数字数据所需的信息。其包括：例如，（1）嵌入子数字数据的盘上的位置（子数字数据位置数据），

(2) 读取子数字数据所需的阈值数据, (3) 伪随机数发生器的初始值, 和 (4) 用于读取子数字数据的选通信息 (子数字数据位移图案)。子数字数据管理信息放置在盘上的特定位置。这些位置包括 (A) 引入区或引出区, (B) BCA (脉冲串输出区), 和 (C) 用户数据区。

下面参考图 14 描述将子数字数据管理信息记录到引入区 (上面的情况 (A))。利用抖动调制将子数字数据记录到光盘 10 的用户数据区 10a。将光盘的物理格式, 逻辑格式, 加扰信息, 区码, 和其它信息记录到位于盘的内圆周的引入区 10b。在加载安排内时, 总是可检验引入区 10b 和管理数据区 (例如 CD 的 TOC 区) 的组合。

通过在写入引入区 10b 的管理信息中把子数字数据管理信息 209 分开预记录到盘管理信息 208, 在加载盘时可立即读取解释子数字数据所需的数据。

子数字数据管理信息 209 包括阈值数据 210, 子数字数据位置信息 212, 子数字数据位移图案 213, 和伪随机数发生器的初始值数据。

子数字数据位置信息 212 记录径向位置, 扇区, 或在盘上记录子数字数据的区域。阈值信息 210 和初始值 214 是光盘驱动器再生 (提取) 子数字数据所需的。

参考图 22 更全面地描述子数字数据位移图案 213。利用 PE 调制信号 E 调制通道代码 A 并作为调制的记录标记 G 记录。然而, 可用子数字数据位移图案产生选通信号 J。当选通信号 J 为高电平时, 调制和记录调制的标记, 而在选通信号 J 为低电平时, 不调制并记录调制的标记。应指出, 抖动调制根据选通信号开启/关闭。

子数字数据位移图案确定是否通或断抖动调制。例如, 为利用 (8-16) 调制记录 3T 标记, 关闭抖动调制, 而当记录标记在其它行程中时, 抖动调制开启。

在 8-16 调制中, 3T 标记是最短行程, 和向记录/再生信号提高最差的 S/N 比。因此, 在记录 3T 标记时, 通过关闭抖动调制, 不恶化主数字数据中 3T 标记的信号质量。另外, 由于未嵌入子数字数据, 可降低检测子数字数据时的检测误差。

登记的可以是除去 3T 中的抖动调制的子数字数据位移图案，和类似地，受热干扰和内部码元干扰很大影响的短标记和空间。因此，在读取子数字数据时，可以以良好的质量再生（提取）子数字数据。

在把子数字数据管理信息的内容针对光盘上的不同内容标题分成多个区时，可将子数字数据和子数字数据管理信息分开并记录到每个区域。此外，虽然在本实施例中将子数字数据管理信息记录到引入区，很显然，可将其记录在引出区。

此外，可记录子数字数据管理信息作为 BCA（脉冲串输出区）。下面将参考图 23 描述记录子数字数据管理信息作为 BCA（上面的情况（B））。

图 23A 示出子数字数据管理信息记录到 BCA 的情况。应指出，在位于光盘 10 的内圆周部分的特定区域中发现 BCA。

在完成盘的生产过程后，加入 BCA 10c 作为利用 YAG 激光或其它高能激光写入的代码。该代码如图 23A 所示以内侧到外侧的圆周方向写入条形图案中，并且在形成的部分中反射率较低。

以与加到常规盘管理信息相同的方式把子数字数据管理记录到 BCA。

这种情况下，由于象引入区一样，加载盘时读取 BCA，因此可迅速读取解释子数字数据所需的信息。

此外，虽然如上所述将子数字数据管理信息记录到引入区或 BCA，作为替换，可将其记录到用户数据区的专用区。

下面参考图 24 描述把子数字数据管理信息记录到用户数据区（上面的情况（C））。

图 24 是子数字数据管理信息记录的用户数据区的光盘的示意图。光盘 10 的用户数据区 10a 存储用户数据和管理信息二者。把记录子数字数据管理信息的管理信息 247 写入设置在用户数据和用户数据之间的特定区域。管理信息 247 包括盘管理信息 248 和子数字数据管理信息 249。应指出，可省略盘管理信息。

子数字数据管理信息 249 包括阈值信息 250，子数字数据位置信息

252, 子数字数据位移图案 253, 和伪随机数发生器的初始值 254。子数字数据位置信息 252 记录径向位置, 扇区, 或在盘上记录子数字数据的区域。该阈值信息 250 和初始值 254 是光盘驱动器再生(提取)子数字数据所必需的。

为了识别子数字数据管理信息 249 是在用户数据区中的特定位置, 可把指示径向位置, 记录区, 或定位子数字数据管理信息的盘上的其它位置写入引入区, 引出区, 或 BCA。此外, 作为替换, 可将子数字数据管理信息 249 写到遇到恒定径向位置或区域。这种情况下, 光盘再生驱动器在非易失性存储器中存储子数字数据管理信息的盘位置。

通过在用户数据区放置子数字数据管理信息 249 可改善子数字数据的安全性。也可以将子数字数据管理信息 249 分配到用户数据区中的多个位置。

例如, 通过针对每个区域或标题分开记录子数字数据管理信息, 更容易确保各个内容和标题的版权。由于应用户数据区的存储容量明显大于引入区, 引出区, 或 BCA 的存储容量, 用户数据区还可提供存储大量子数字数据管理信息项的优点。

(光盘再生装置)

下面描述用于播放记录了如上所述的保密密钥的光盘的系统。

图 25 是根据本发明的光盘再生装置 1201 的主要部分的方框图。应指出, 图 25 所示的主信号 H 和 I 的波形与图 20 的定时图中所示的相同。

该再生装置 1201 是与上述记录装置 100a 对应的光盘再生装置。除了根据光盘上的记录标记的位置再生主数字数据, 再生装置 1201 还具有检测在数据再生期间遵守的嵌入记录标记抖动中的子数字数据(保密密钥), 和根据检测的保密密钥保护主数字数据的版权的功能。再生装置 1201 具有再生头 1211, 再生通道 1212, 再生信号处理器 1213, 时钟提取部分 1214, 同步检测器 1215, 验证部分 1216, 和伪随机数发生器 1217。

再生头 1211 是光拾取器。它在旋转光盘上的记录标记上发射聚焦的光束, 产生指示调制的记录标记 G 的边缘位置的模拟读取信号, 和输出

到再生通道 1212。再生通道 1212 把来自再生头 1211 的模拟读取信号转换成数字读取信号，并输出到再生信号处理器 1213 和时钟提取部分 1214。

根据来自再生通道 1212 的读取信号，时钟提取部分 1214 提取并产生 4 个时钟信号，即，(i) 与通道代码的比特同步的通道比特时钟，(ii) 参考通道比特时钟指示读取信号的超前分量的超前相位误差信号 H，(iii) 类似地指示滞后分量的滞后相位误差信号 I，和 (iv) 与读取信号中的（字节单元）记录数据同步的字节时钟。这四个时钟信号分别提供到 (i) 再生信号处理器 1213，(ii) 同步检测器 1215，(iii) 同步检测器 1215，(iv) 再生信号处理器 1213，同步检测器 1215，和伪随机数发生器 1217。

图 26 是表示时钟提取部分 1214 的详细配置的方框图。时钟提取部分 1214 包括 PLL 电路，4-比特计数器 1214d，同步信号检测器 1214e，和相位误差信号分离器 1214f。PLL 电路包括相位比较器 1214a，环路滤波器 1214b，和 VCO（压控振荡器）1214c。

相位比较器 1214a 包括计数器，“异”门，触发器等。根据作为来自 VCO 1214c 的反馈输入的通道比特时钟和来自再生通道 1212 的读取信号，相位比较器 1214a 计算读取的信号的上沿和下沿和最靠近该读取信号边缘的通道比特时钟的上沿之间的相位误差。计算结果作为相位误差信号输出到环路滤波器 1214b 和相位误差信号分离器 1214f。

环路滤波器 1214b 是平滑来自相位比较器 1214a 的相位误差信号，并将其转换成直流电压信号的低通滤波器。VCO 1214c 是产生频率与来自环路滤波器 1214b 的电压信号对应的通道比特时钟的压控振荡器。

同步信号检测器 1214e 检测读取的信号中包含的同步图案，并将其作为复位信号输出到 4-比特计数器 1214d，4-比特计数器 1214d 是对来自 VCO 1214c 的通道比特时钟施加 1/16 分频的计数器，并由来自同步信号检测器 1214e 的复位信号复位。就是说，4-比特计数器 1214d 输出与读取的信号中的记录数据（字节单元）同步的字节时钟。

相位误差信号分离器 1214f 把来自相位比较器 1214a 的相位误差信号

分成超前相位误差信号 H 和滞后相位误差信号 I，并输出到同步检测器 1215。

图 27A 是表示相位误差信号分离器 1214f 的详细配置的示意电路图。相位误差信号分离器 1214f 包括两个倒相器 1330a, 1330b, 和两个“与”门 1330c 和 1330d。图 27B 是用于描述图 27A 所示的相位误差信号分离器 1214f 的操作的信号的定时图。如图 27B 所示，超前相位误差分量和滞后相位误差分量包括在从相位比较器 1214a 输出的相位误差信号中。由于与通道比特时钟同步地分开这些相位误差信号 H 和 I, 从“与”门 1330c 输出的信号（超前相位误差信号 H）波形仅示出了超前相位误差信号分量，从“与”门 1330d 输出的信号（滞后相位误差信号 I）波形仅示出了滞后相位误差信号分量。

再生信号处理器 1213 解调来自再生通道 1212 的读取信号，对子数字数据检测进行控制，并根据检测结果工作以提供版权保护。

图 28 是表示再生信号处理器 1213 的详细配置的方框图。再生信号处理器 1213 包括解调器 1213a, 输出门 1213b, 初始值存储器 1213c, 和位移图案选通发生器 1213d。

解调器 1213a 是与记录装置 100a 的调制器 102a 对应的解调电路。解调器 1213a 与来自时钟提取部分 1214 的通道比特时钟同步地对来自再生通道 1212 的读取信号取样。接下来，解调器 1213a 与来自时钟提取部分 1214 的字节时钟同步地把（16-8 调制）通道代码 A 转换成与每个通道代码对应的 8-比特记录数据，并将记录数据流输出到输出门 1213b。

输出门电路 1213b 是用于版权保护的缓冲门电路。仅在输入来自验证部分 1216 的启动信号（通知已确认将有效保密密钥记录到光盘）时，输出门电路 1213b 外部通过来自解调器 1213a 的记录数据流作为再生信号。

初始值存储器 1213c 是用于存储来自子数字数据管理信息读取的伪随机数发生器的初始值 214（15-比特初始值）的寄存器。当从控制器（图中未示出）接收到指示保密密钥读取（下文称之为“保密密钥读取模式”）的开始信号，初始值存储器 1213c 向伪随机数发生器 1217 输出该初始

值。

根据读取光盘 10 上的子数字数据管理信息 209 中的子数字数据位移图案 213 的结果，位移图案选通发生器 1213d 根据从解调器 1213a 解调的通道代码 A 的数据流中的特定标记的长度和空间来产生选通信号。

图 32 是位移图案门电路的定时图。下面参考图 32 描述在 8-16 调制中从 4T 区分的 3T 行程和更长行程的情况。

如图 32 所示，在通道代码 A 的行程是 3T 时，选通信号 J 输出低电平，在行程是 4T 或更长时，输出高电平。应该指出，虽然该实例描述了从 4T 或更长行程分出 3T，类似地，能够从 5T 或更长行程分出 4T 和更短的行程，从 6T 或更长行程分出 5T 和更短的行程，等等。该信息写入子数字数据位移图案。

伪随机数发生器 1217 具有与光盘再生装置 100a 的伪随机数发生器 121b 相同的功能。来自存储从伪随机数发生器初始值 214 读取的初始值的初始值存储器 102e 的初始值作为预设值，伪随机数发生器初始值 214 写入光盘，使用从时钟提取部分 1214 输入的字节时钟作为移位时钟，伪随机数发生器 1217 产生每个周期具有 2^{15} 个比特序列的伪随机数序列（M 序列）。用盘读取器 1201 中的伪随机数发生器 1217 产生 256 X 56 比特的伪随机数序列。

同步检测器 1215 检测来自伪随机数发生器 1217 的伪随机数序列，从时钟提取部分 1214 输出的超前和滞后相位误差信号 H 和 I 之间的相关性，并向验证部分 1216 输出每个伪随机数（1 比特）的结果（正相关，负相关，或无相关）。

图 29 示出了同步检测器 1215 的详细配置。同步检测器 1215 包括 PE 调制器 1215a，选择器 1215b，积分器 1215c，阈值估算器 1215d，和 8-比特计数器 1215e。

PE 调制器 1215a 具有与光盘再生装置 100a 的定时发生器 121a 和 PE 调制器 121d 有关的功能。根据来自时钟提取部分 1214 的字节时钟，PE 调制器 1215a 向来自伪随机数发生器 1217 的伪随机数序列施加 PE 调制，并将该结果作为选择控制信号输出到选择器 1215b。就是说，PE 调制器

1215a 向来自伪随机数发生器 1217 的伪随机数序列施加 PE 调制，并将该结果作为选择控制信号输出到选择器 1215b。具体地说，当来自伪随机数发生器 1217 的伪随机数是 0 时，PE 调制器 1215a 向选择器 1215b 输出在再生读取信号中的每个记录数据字节的中部下降，在伪随机数是 1 时上升，和在相同的伪随机数重复时在每个记录数据字的边界再次反转的信号波。

选择器 1215b 是具有 2-输入,1-输出的选择器。当来自 PE 调制器 1215a 的控制信号是 1 时，选择器 1215b 把来自时钟提取部分 1214 的超前相位误差信号 H 和滞后相位误差信号 I 分别传送到积分器 1215c 的正和负输入端；当控制信号是 0 时，分别传送跨越积分器 1215c 的正和负输入端的信号 H 和 I。

8-比特计数器 1215e 是向来自时钟提取部分 1214 的字节时钟施加 1/256 分频的计数器。该结果作为复位信号输出到积分器 1215c，阈值估算器 1215d，和验证部分 1216。因此，每当伪随机数发生器 1217 输出 256-比特随机数序列时，该复位信号输出一个复位脉冲。

积分器 1215c 是具有差分输入和双极输出的模拟积分器。积分器 1215c 对输入到正输入端以存储的脉冲区求和，对输入到负输入端以存储的脉冲区相减，和向阈值估算器 1215d 输出与总存储区对应的模拟信号。如果在此期间从 8-比特计数器施加复位信号。积分器 1215c 从零重新开始。

结果是，在来自 PE 调制器 1215a 的 PE 调制信号是 1 时，来自积分器 1215c 的输出波指示超前相位误差信号 H 中的脉冲的相加累积区和滞后相位误差信号 I 中的脉冲的相减累积区的总累积区。当 PE 调制是 0 时，该输出波指示超前相位误差信号 H 中的脉冲的相减累积区和滞后相位误差信号 I 中的脉冲的相加累积区的总累积区。

因此，当其中仅当 PE 调制信号到 1 时在超前相位误差信号 H 中出现脉冲，仅当 PE 调制信号到 0 时在滞后相位误差信号 I 中出现脉冲，正相关继续时，积分器 1215c 的输出波是具有正斜率的斜坡波。反之，当其中仅当 PE 调制信号到 1 时在滞后相位误差信号 I 中出现脉冲，仅当 PE 调制信号到 0 时在超前相位误差信号 H 中出现脉冲，负相关继续时，积

分器 1215c 的输出波是具有负斜率的斜坡波。当正或负相关性都不存在时，就是说，当脉冲在超前相位误差信号 H 和滞后相位误差信号 I 中随机出现，而与 PE 调制信号无关时，由于这些误差信号中的两个脉冲的频率实质上相等，来自积分器 1215c 的输出波近似保持在零电平。

阈值估算器 1215d 是比较器，或用于确定找到来自积分器 1215c 的模拟信号的三个电压范围的其它设备。这些电压范围由从光盘上的子数字数据管理信息读取的预设的正阈值电压和负阈值电压定义。

图 30 描述了阈值估算器 1215d 的操作，并示出从积分器 1215c 输入到阈值估算器 1215d 的模拟信号波。在从 8-比特计数器 11215e 施加复位信号的时刻（具体地说，刚刚在此之前），阈值估算器 1215d (i) 向验证部分 1216 输出 NRZ 格式码元流，当来自积分器 1215c 的信号电压大于正阈值时，该码元流为 1，当小于负阈值时，该码元流为 0。阈值估算器 1215d, (ii) 当来自积分器 1215c 的信号电压处在这些阈值之间世纪，向验证部分 1216 发送指示该状态的篡改信号。

设定阈值以便在应用根据本发明的抖动调制时，积分器 1215c 的输出电压可靠地（即可能性极高）超过阈值电压，但在不应用抖动调制时，输出电压不超过该阈值（可能性极低）。在记录期间（调相器中延迟电路的延迟）根据例如抖动调制，输入到积分器 1215c 的字节数（256），每个字节的平均边缘计数值，或自然（随机出现）抖动分布中的标准偏差来确定特定值。

从阈值估算器 1215d 输出的代码序列表示出了在每个 256-比特伪随机数观察到的相关性的极性（正或负）中的变化。该极性变化是与指示对于每个 256-比特的伪随机数序列，是不进行逻辑反转由抖动调制记录该伪随机数序列，还是在逻辑反转之后记录伪随机数序列的比特序列对应的信息。

验证部分 1216 根据来自同步检测器 1215 的码元流和篡改信号证明当前被读取的光盘是否是由合法光盘再生装置 100a 记录的。仅当该结果为肯定时，验证部分 1216 向再生信号处理器 1213 发送指示该状态的启动信号。

图 31 是验证部分 1216 的详细配置的方框图。验证部分 1216 包括保密密钥存储器 1216a, 移位寄存器 1216b, 识别比较器 1216c, 和输出锁存器 1216d。

保密密钥存储器 1216a 是用于预存与光盘再生装置 100a 的保密密钥存储器 102f 相同的 56-比特保密密钥的寄存器。移位寄存器 1216b 是使用来自时钟提取部分 1214 的复位信号作为移位时钟用于移位和存储来自同步检测器 1215 的代码序列的 56-级(比特)移位寄存器。

在 56-比特代码序列刚刚被输入到移位寄存器 1216b 之后, 识别比较器 1216c 确定码元序列是否与保密密钥存储器 1216a 中存储的 56-比特保密密钥完全匹配, 以便将该结果传送到输出锁存器 1216d。

仅在未从同步检测器 1215 接收到篡改信号并且识别比较器 1216c 报告完全密钥匹配时, 输出锁存器 1216d 向再生信号处理器 1213 输出启动信号。就是说, 仅当确认在从伪随机数发生器 1217 输入到同步检测器 1215 的 256-比特伪随机数序列与读取的信号中包含的相位误差信号之间, 正或负相关性连续存在 56 次(针对 256 X 56 比特伪随机数序列), 并且在相关性的极性变化与存储到保密密钥存储器 1216a 的 56-比特保密密钥之间存在完全匹配时, 验证部分 1216 向再生信号处理器 1213 输出启动信号。

在保密密钥读取模式结束时, 当从验证部分 1216 向再生信号处理器 1213 输出启动信号, 再生信号处理器 1213 确定处理的盘是具有由逻辑光盘再生装置 100a 嵌入的保密密钥的介质。然后, 再生信号处理器 1213 外部输出通过解调来自再生通道 1212 的读取信号获得的再生信号。如果未从验证部分 1216 向再生信号处理器 1213 输出启动信号, 则确定该光盘不是具有由逻辑光盘再生装置 100a 嵌入的保密密钥的介质, 再生信号处理器 1213 不外部地输出再生信号, 从而保护版权。

因此, 能够防止从不能确认嵌入的保密密钥的光盘非法地读取记录数据。结果是, 即使对包含保密密钥的逻辑光盘进行完全复制来生产新光盘, 禁止由该盘读取器 1201 播放光盘, 除非也复制了由抖动调制嵌入的保密密钥, 因此能够保护版权。

上面根据本发明的优选实施例描述了存储抖动调制数据的记录介质和用于该记录介质的记录和再生装置，但很显然，本发明不限于此。

例如，在该实施例中把根据单个 56-比特保密密钥逻辑反转的 256 X 56 比特伪随机数序列嵌入到连续的 56 字节的记录数据。然而，本发明不限于这些数量。例如，也可以把在多个区域中从 1，2，或更多种类的初始值开始的多个伪随机数序列嵌入到特定盘区中的记录数据，或嵌入与 ECC 块，扇区，帧，或其它物理记录结构有关的字节数量。

此外，在该实施例中，确认光盘是合法复制的条件是在每 256 字节中相位误差信号和伪随机数序列之间的正或负相关连续出现 56 次，但也可以减少到 50 次或多于 56 次。如图 19 所示，由于抖动分布具有特定扩展，存在着最好是利用脉冲数或用于估算的抖动调制确定的容线，根据估算标准估算有意义的关系的情况。

此外，在保密密钥与从同步检测器输出的代码序列之间的一致性小于或等于特定值时，该实施例限制主数字数据的再生。然而，也可以简单地把同步检测器积分的相位误差信号与特定的阈值比较，而不是使用保密密钥，在超过该阈值时，确定与伪随机数序列的强相关性，从而限制再生。因此，使用更简单的配置可实现在某个程度进行版权保护。

此外，本实施例通过在相位误差信号的同步检测期间模拟积分超前相位误差信号 H 和滞后相位误差信号 I 的脉冲区来估算相关性。然而，为简化该电路，在加和减脉冲计数时，可以用简单计数的数字技术来代替。

本发明应用到写入光盘的用户数据区 10a 的记录数据的抖动调制可应用到引入区，引出区，和 BCA。也可与根据现有技术的内容加密组合。例如，在把存储的盘密钥和标题密钥记录到控制数据区时，通过应用根据本发明的抖动调制，不改变利用常规内容加密记录的内容（数字数据）可加强版权保护，以阻止盗版制造者生产的非法复制。

此外，该实施例的盘驱动器 1201 仅当验证光盘上的嵌入保密密钥出现时才输出解调的再生信号，但本发明不限于以这种方式使用验证结果。例如，如果不能确认光盘的有效性，可用验证结果允许仅再生记录到光

盘的特定区的标题数据。

此外，在该实施例中，用作子数字数据的保密密钥存储到光盘再生装置 100a 和盘读取器 1201，但也可以借助用户命令或与外部设备的安全通信覆盖保密密钥。作为替换，例如，可以向盘预记录加密作为子数字数据管理信息。

已使用作为例子的光盘记录介质描述了本实施例，但本发明不限于此，而是可应用于 CD-ROM，DVD-ROM，CD-R，CD-RW，DVD-RAW，DVD-RW，磁光和其它此类介质。就是说，本发明可应用于不仅在凹凸的凹坑，而且在相位改变膜或磁膜上记录数据的盘。在利用抖动调制写入凹坑（记录标记）位置的情况下，本发明可应用于使用除凹坑和纹间表面格式外的各种记录方法的介质，包括相位转移（相位改变）和磁化。应该指出，图 15 所示的再生装置的配置和操作可用于该实施例。

根据本发明的抖动调制用于嵌入到光盘的隐藏子数字数据，本发明不限于该隐藏应用。例如，可以用于可记录不同类型的数字数据以便将它们分开再生的应用，从而在非加密的应用中改善记录密度。该应用的例子是把音频信息（子数字数据）叠加到视频信息（主数字数据），以写入记录介质。

根据本发明的该实施例，以难于读取的子数字数据的方式把子数字数据嵌入光盘中的主数字数据。因此，在基于记录标记出现简单地复制光盘时，不复制子数字数据，使其能够在复制的源盘和得到的其复制之间进行区分。这样使其能够防止通过简单地在光盘上直接复制受版权保护的数字资料侵犯版权。

此外，通过把子数字数据管理信息预记录到光盘，可以很容易地把不同的主机密钥分配给每个盘，以便即使暴露了一个密钥，而对其它驱动器没有影响。

还可以分配子数字数据管理信息，以使用于该阈值信息和子数字数据的位置信息在每个盘中不同，通过对包含命令阈值信息或子数字数据的位置信息的子数字数据加密，可进一步增强该信息的安全性。

也可以把子数字数据的随机数序列的初始值作为子数字数据管理信

息预记录到光盘。这使其能够针对每个盘改变随机数序列的初始值，并进一步改善数据安全性。通过改变伪随机数序列，可以在不影响其它盘的版权保护的情况下改善安全性，即使把单个保密密钥用于多个盘。

在累积特定长度的随机数序列的超前或滞后记录标记和根据累积的值是大于还是小于预定阈值产生子数字数据时，可预记录该阈值作为子数字数据管理信息。因此，通过按盘来改变该阈值可以改善数据安全性。另外，当在多个盘上使用单个保密密钥时，通过改变该阈值，可以在不影响其它盘的版权保护的情况下改善数据安全性。

作为替换，可预记录子数字数据位置信息作为子数字数据管理信息，通过按盘自由地改变盘上的子数字数据的位置可改善数据安全性。此外，当在多个盘上使用一个保密密钥时，通过改变子数字数据的位置，在不影响其它盘的版权保护的情况下可改善数据安全性。

在根据记录标记长度切换调相的通开启和关闭时也可记录子数字数据。这用来防止调相在再生信号中产生低 S/N 比的长度的记录标记恶化信号质量。另外，由于未在具有较差 S/N 比的长度的记录标记中嵌入子数字数据，可减少子数字数据的检测误差和可靠地再生（提取）子数字数据。

可预记录确定调相通/断状态的记录标记长度信息作为子数字数据管理信息。因此，可按盘自由地改变调相的记录标记的长度，和改善数据安全性。此外，当在多个盘上使用一个保密密钥时，通过改变确定是否开启或关闭调相的记录标记长度，可在不影响其它盘的版权保护的情况下改善数据安全性。

可把子数字数据管理信息预记录到光盘的控制数据区。因此，在加载该盘时，可读取子数字数据管理信息，并可快速提取子数字数据。

另外，可把子数字数据管理信息预记录到光盘的用户数据区。这使其能够子数字数据和对应的子数字数据管理信息分配到用户数据区中的多个区域。例如，通过按区和内容标题分开放置子数字数据和子数字数据管理信息，可容易地针对每个内容标题改变版权保护。此外，由于用户数据区的存储容量明显大于引入区，引出区，或 BCA 的容量，可提供

许多子数字数据管理信息项。此外，可把子数字数据管理信息预记录到光盘 BCA。对于记录到引入区，能够在加载盘时读取子数字数据管理信息，和快速读取解释子数字数据所需的信息。

对于根据本发明该实施例的光盘再生装置，由于把基于随机数序列的抖动调制应用到记录标记边缘位置，使得对子数字数据解密也很困难，可按盘自由地改变提取子数字数据所需的信息（阈值和位置信息），从而进一步改善数据安全性。通过按盘改变子数字数据管理信息的内容，在不影响其它盘的版权保护的情况下也可改善数据安全性，即使在多个盘上使用一个保密密钥。

此外，通过记录使用抖动调制的保密密钥而在激光点扫描轨迹的方向略微移位记录标记边缘（轨迹方向中端部的两个边缘），不具备读取以抖动嵌入的数据的能力的正常盘读取器不能读取该保密密钥。

这意味着即使使用正常的盘读取器读取记录了保密密钥的光盘上的所有内容，和把读取的内容直接记录到另一个光盘，只能复制主数字数据而不复制以抖动嵌入记录的子数字数据（保密密钥）。因此，能够从非法复制的光盘区分出原始光盘。因此，通过提供具有仅允许再生包含保密密钥的光盘的机构的盘再生装置，可避免通过分发盗版编辑的侵犯版权。

<实施例 3>

在本发明的该实施例中，把用于加密主数字数据的加密密钥作为子数字数据记录到光盘的特定区域。

（光盘）

图 34 示出根据本发明该实施例的 DVD10。当用户数据包括 n 个内容标题（标题 1，标题 2，...，标题 n ），用与标题对应的加密密钥加密每个标题。加密密钥的总数是 n ，等于内容的总数。把这些加密密钥（加密密钥 1，加密密钥 2，...，加密密钥 n ）作为子数字数据记录到控制数据区中的特定区。使用在轨迹方向把记录标记边缘移位微小量的相位调制来记录该子数字数据。加密密钥 1 是对内容 1 加密的密钥，加密密钥 ID

和内容标题 ID 同样针对其它加密密钥 2, 3, ..., n 相关。

用于记录该子数字数据的主数字数据是虚拟数据（即数据本身无含义）。一个子数字数据项的长度是 56 比特，一比特的子数字数据重叠记录到主数字数据的 256 字节块。这意味着使用 14,336 字节的主数字数据记录一个子数字数据项。连续地记录 n 个子数字数据项。

这意味着，即使使用正常的盘读取器读取了包含所记录的加密密钥的 DVD 的所用内容并记录到另一个 DVD，仅复制了原始主数字数据，而未复制以抖动嵌入记录的子数字数据（加密密钥）。因此，该盘读取器不能对非法复制的 DVD 上加密的主数字数据解密。从而避免通过销售盗版 DVD 侵犯版权。

此外，通过把加密密钥记录到控制数据区，具有在加载盘时读取该加密密钥功能的合法 DVD 盘读取器可存取该盘的内容，但没有该功能的非法盘读取器不能对加密的主数字数据解密。从而避免通过销售用于盗版 DVD 的盘读取器来侵犯版权。

此外，当用户数据包含多个内容标题，并且用针对每个内容标题不同的加密密钥加密记录内容标题时，即使读取一个加密密钥并解密对应的内容标题，也不能对所以内容解密。有力地确保了用户数据的安全性。

用户数据内容也可包含未加密的内容标题。加密的内容也可某些未加密的数据。这在希望记录预览电影标题，合作 PR 内容，产品广告，和其它这类信息作为未加密内容是非常有用的。

也可用两个或多个加密密钥对单个年标题加密。这能够使密钥在例如产品 ID 或电子货币组合中被排它地使用。

（光盘记录器）

图 35 是表示根据本发明的光盘再生装置的主要部分。图 35 中的信号 B, D, E, F 的波形如图 36 中的定时所示。

该再生装置 100 是用于通过形成可光学读取的记录标记来记录主数字数据的系统。再生装置 100 是具有根据加密密钥对主数字数据加密的功能，和通过在轨迹的方向略微移位记录标记边缘的相位调制来记录该

加密密钥作为子数字数据的功能的 DVD-ROM 再生装置。再生装置 100 具有记录通道 108, 记录头 109, 用于加密主数字数据的加密部分 101, 格式化器 102, 伪随机数发生器 104, 定时发生器 103, XOR 门 105, PE (相位编码) 调制器 106, 和调相器 107。

在记录内容时, 加密部分 101 使用加密密钥对主数字数据加密, 并把加密的数据传送到格式化器 102。在记录加密密钥时, 加密部分 101 输出加密密钥, 并把未加密主数字数据的数据记录到格式化器 102。

图 37 是表示加密部分 101 的详细配置的方框图。加密部分 101 具有加密密钥选择器 101a, 加密编码器 101b, 和数据选择器 101c。加密密钥选择器 101a 保持多个加密密钥并选择与该内容对应的加密密钥 L。加密编码器 101b 使用加密密钥 L 对输入到再生装置的记录数据 J 加密。在加密启动信号是 1 时, 数据选择器 101c 选择加密的数据 K, 在加密启动信号是 0 时, 选择未加密的记录数据 J。

首先描述把加密密钥记录到控制数据区中的特定位置的操作。加密密钥选择器 101a 内部存储 n 个加密密钥。当加密密钥选择器 101a 接收到开始记录第 i 个内容标题 (内容 ID=i, i=1, 2, ..., n) 的加密密钥的命令 (该操作在下文被称为“加密密钥记录模式”), 来自控制器 (图中未示出) 的识别内容 ID=i 的内容 ID 信号时, 加密密钥选择器 101a 选择加密密钥 i 并输出到格式化器 102。

此时, 数据选择器 101c 从控制器 (图中未示出) 接收加密启动信号 0, 选择未加密的记录数据, 输出该记录数据到格式化器 102。格式化器 102 控制对主数字数据 (记录数据) 的调制, 规定子数字数据, 和记录子数字数据。

图 38 是表示格式化器 102 的详细配置的方框图。格式化器 102 具有调制器 102a, 初始值存储器 102b, 保密密钥存储器 102f, 和加密密钥存储器 102c。调制器 102a 把输入到再生装置 100 的记录数据调制成适合于 DVD10 的信号 (通道信号 B)。初始值存储器 102b 秘密地预存储由伪随机数发生器 104 产生的伪随机数序列的初始值。加密密钥存储器 102c 存储从加密部分输入的 56-比特加密密钥。

如图 36 的定时图所示, 调制器 102a 把 8-比特代码 (字节) 单元中的输入记录数据转换成 16-比特通道代码 A (8-16 转换), 然后施加 NRZI 转换以产生通道信号 B, 并输出到调相器 107。当加密密钥记录模式开始时, 每当输入一个字节的记录数据时, 调制器 102a 向定时发生器 103 输出指示一个字节开始的定时信号。

当加密密钥记录模式开始时, 初始值存储器 102b 向伪随机数发生器 104 输出预记录的 15-比特初始值。

当加密密钥记录模式开始时, 加密密钥存储器 102c 把从加密部分输入的 56-比特的加密密钥一次一个比特以 NRZ 格式从 LSB 输出到 XOR 门 105。每当调制器 102a 调制 256 字节的记录数据时, 加密密钥存储器 102c 输出下一个最高的比特。换句话说, 加密密钥存储器 102c 把单个 56-比特的加密密钥按比特序列输出到 XOR 102c 作为与总共 256×56 字节的记录数据对应的加密密钥比特序列。

图 39 示出了加密密钥, 伪随机数序列, 和记录数据之间的相关性。为了把 56-比特的加密密钥记录到盘作为数字水印, 把 256-比特的伪随机数序列用于加密密钥的每个比特, 该伪随机数序列的每个比特嵌入记录数据 (16 通道代码) 的 1 个字节中。应指出, 用该 56-比特加密密钥的每个比特作为指示对应的 256-比特伪随机数序列是否是被逻辑反转的标志, 下面更详细地描述。

定时发生器 103 (i) 根据来自调制器 102a 的定时信号与记录数据的每个字节同步地输出向伪随机数发生器 104 时钟信号 (字节时钟), 和 (ii) 根据该定时信号和来自时钟振荡器 (图中未示出) 的时钟信号, 把从格式化器 106 输出的通道信号 B 的中心 (180 度相位点) 输出到 PE 调相器 106。

伪随机数发生器 104 使用来自初始值存储器 102b 的预设初始值和来自定时发生器 103 的字节时钟作为移位时钟来产生每个周期具有 2^{15} 个比特序列的伪随机数序列 (M 序列)。

图 40 是表示伪随机数发生器 104 的详细配置的电路图。伪随机数发生器 104 包括用于存储来自初始值存储器 102b 的初始值的 15-比特预设

初始值寄存器 104a, 15 级 (比特) 移位寄存器 104b, 和用于对来自移位寄存器 104b 中的 MSB (第 14 比特) 和第 10 比特进行 “异” 运算的 XOR 门 104。

当在预设初始值寄存器 104a 中设定来自初始值存储器 102b 的初始值时, 在格式化器 102 发送选通信号之后把初始值写到移位寄存器 104b。与来自定时发生器 103 的字节时钟同步, 把存储到移位寄存器 104b 的 15-比特值向左移位一位, 然后返回来自 XOR 门 104c 的输出, 并存储到移位寄存器 104b 的 LSB (第 0 比特)。这样在移位寄存器 104b 的 MSB 产生每个字节具有一个比特的新随机数, 把该新的随机数发送到 XOR 门 105 作为伪随机数序列。

在该实施例中用伪随机数发生器 104 产生在加密密钥记录模式中嵌入 256 X 56 字节的记录数据中的 256 X 56 比特伪随机数序列。

XOR 门 105 对来自伪随机数发生器 104 的伪随机数序列和加密密钥存储器 102c 的比特序列进行 “异” 运算, 并向 PE 调制器 106 输出得到的伪随机数序列 D。就是说, 根据 56-比特的加密密钥的每个比特直接或在 256 比特的伪随机数序列逻辑反转之后, XOR 门 105 有选择地把伪随机数发生器 104 产生的 256 比特伪随机数序列提供到 PE 调制器 106。

根据来自定时发生器 103 的定时信号, PE 调制器 106 向来自 XOR 门 105 的伪随机数序列 D 施加 PE (相位编码) 调制, 并向调相器 107 输出得到的 PE 调制信号 E。结果是, 如图 36 中的定时图所示, 当来自 XOR 门 105 的伪随机数序列 D 是 0 时, PE 调制信号 E 在通道信号 B 的中部下降, 当伪随机数 D 是 1 时上升, 并在相同随机数重复时再次反转通道信号 B 的边界。

根据来自 PE 调制器 106 的 PE 调制信号 E, 调相器 107 进行相位调制, 以使来自格式化器 102 的通道信号 B 的边缘超前或滞后较短时间, 并向记录通道 108 输出得到的调制通道信号 F。应指出, 把该较短时间预设到在正常再生装置上播放通过旁路该调相器 107 (未记录子数字数据) 仅记录主数字数据的正常 DVD 时观察到的抖动的频率分布的标准偏差 (σ) 的一半值 ($\sigma/2$)。

图 41 是表示调相器 107 的详细配置的方框图。调相器 107 具有把输入信号延迟少数较短时间的延迟装置 107a, 和具有两个输入和一个输出的选择器 107b。当作为控制信号输入的 PE 调制信号 E 是 1 时, 选择器 107 传送直接从格式化器 102 输入的通道信号 B。当 PE 调制信号 E 是 0 时, 选择器 107 通过延迟装置 107a 传送输入的通道信号。

结果是, 输入到调相器 107 的通道信号 B 的上升和下降边缘的相位 (在相对时间关系上) 当 PE 调制信号 E 是 0 (0 到 180 度) 时超前上面提到的较短时间, 当 PE 调制信号 E 是 1 (180 到 360 度) 滞后该较短时间。换句话说, 根据伪随机数序列 D 利用抖动来调制输入到调相器 107 的通道信号 B, 并转换成调制的通道信号 F, 如图 36 所示。

记录通道 108 产生与来自调相器 107 的调制通道信号 F 同步地切换发射到 DVD10 的激光束通/断的控制信号, 并把控制信号发送到记录头 109。根据来自记录通道 108 的控制信号, 记录头 109 通过发射激光束, 同时切换激光束的通和断来把记录标记刻到旋转 DVD 10 的表面的螺旋图案中。结果是, 在 DVD 中形成包括可光学读取的凹凸的凹坑的调制的记录标记 G。

图 42 示出上面具有由记录头 109 形成的凹坑的 DVD 上的记录膜的表面。利用超前 (或延迟) 与在加密密钥记录模式中未形成的凹坑的边缘位置有关的恒定短时间对应的位移量的相位形成在加密密钥记录模式中形成的凹坑的两个边缘 (在光点的扫描方向)。

图 43 是表示针对在加密密钥记录模式中形成的凹坑, 即利用抖动调制记录的调制的记录标记 G 观察到的抖动的频率分布的曲线。

曲线 A 表示仅在 PE 调制信号是 0 时产生的调制记录标记 G 的边缘的抖动分布, 并且是其中最高频率是相位在滞后方向移位该位移量的位置 X (L) 的近似高斯分布。曲线 B 是仅在 PE 调制信号是 1 时产生的调制记录标记 G 的边缘的抖动分布, 并且是其中最高频率是相位在超前方向移位该位移量的位置 X (H) 的近似高斯分布。曲线 C 表示组合曲线 A 和 B 的整个抖动分布。

本发明利用了使用与记录该加密密钥使用的相同的伪随机数序列进

行同步检测时可将曲线 C 的抖动分布分成曲线 A 和 B 的事实。

使用上述子数字数据记录方法记录加密密钥 1。该操作针对加密密钥 1 至 n 继续，以便连续将 n 个加密密钥记录到记录区中的特定区域。

下面以加密和记录第 i 个内容标题（内容 ID=i, $i=1, 2, \dots, n$ ）为例来描述内容加密和记录操作。当从控制器（图中未示出）接收到开始加密和记录内容标题 i 的主数字数据，（下文称该操作为“主数字数据加密和记录模式”），识别内容 ID=i 的内容 ID 信号时，加密密钥选择器 101a 选择加密密钥 i 并输出到加密编码器 101b。

加密编码器 101b 把加密密钥 i 的值加到 8 比特的输入记录数据，并输出到数据选择器 101c。例如，当加密密钥 i 是 1 时，把 1 加到 8 比特记录数据。

当数据选择器 101c 从控制器（图中未示出）接收到加密期待信号 1 时，选择该加密数据并输出到格式化器 102。然后，使用加密密钥 i 对该记录数据加密。

调制器 102a 把 8-比特码元（字节）单元中的输入加密数据转换成 16-比特通道代码 A（8-16 转换），然后施加 NRZI 转换以产生通道信号 B，并输出到调相器 107。调相器 107 向记录通道输出未调相的通道信号 B。

根据加密密钥 i 加密记录数据并记录。针对内容 1 至 n 重复该操作，利用为每个内容标题更新的加密密钥加密内容数据并记录。

这意味着，即使使用正常的再生装置读取记录了加密密钥的 DVD 上的所有内容，并把读取的内容直接记录到另一个 DVD，仅复制主数字数据，而未复制以抖动记录嵌入的子数字数据（加密密钥）。因此，再生装置不能从非法复制的 DVD 解密和播放加密的主数字数据。从而避免了通过销售盗版编辑来侵犯版权。

（光盘再生装置）

下面描述再生装置对利用如上所述的加密密钥记录的 DVD 的操作。

图 44 是根据本发明的光盘再生装置 300 的主要部分的方框图。

再生装置 300 是与上述 DVD 再生装置 100 对应的 DVD 再生装置。

除了根据 DVD 上的记录标记的位置再生主数字数据的功能外，再生装置 300 还具有检测在数据再生期间观察到的记录标记的抖动中嵌入的子数字数据（加密密钥），和根据检测的加密密钥对加密的主数字数据解密的功能。

再生装置 300 具有再生头 302，再生通道 303，再生信号处理器 304，时钟提取部分 305，同步检测器 307，加密密钥再生电路 308，和伪随机数发生器 1217。

再生头 302 是光拾取器。它在旋转 DVD 上的记录标记上发射聚焦的光束，产生指示记录标记的边缘位置的模拟读取信号，和输出到再生通道 303。再生通道 303 通过波形均衡和整形把来自再生头 302 的模拟读取信号转换成数字读取信号，并输出到再生信号处理器 304 和时钟提取部分 305。

根据来自再生通道 303 的读取信号，时钟提取部分 305 提取并产生 4 个时钟信号，即，(i) 与通道代码的比特同步的通道比特时钟，(ii) 参考通道比特时钟仅指示读取信号的超前分量的超前相位误差信号 H，(iii) 类似地仅指示滞后分量的滞后相位误差信号 I，和 (iv) 与读取信号中的（字节单元）记录数据同步的字节时钟。然后，时钟提取部分 305 把每个时钟信号分别输出到 (i) 再生信号处理器 304，(ii) 同步检测器 307，(iii) 同步检测器 307，(iv) 再生信号处理器 304，同步检测器 307，和伪随机数发生器 306。

图 45 是表示时钟提取部分 305 的详细配置的方框图。时钟提取部分 305 包括 PLL 电路，4-比特计数器 305d，同步信号检测器 305e，和相位误差信号分离器 305f。PLL 电路包括相位比较器 305a，环路滤波器 305b，和 VCO（压控振荡器）305c。

相位比较器 305a 包括例如计数器，“异”门，或触发器。根据作为来自 VCO 305c 的反馈输入的通道比特时钟和来自再生通道 303 的读取信号，相位比较器 305a 计算读取的信号的上升和下降沿和最靠近该读取信号边缘的通道比特时钟的上升沿之间的相位误差。计算结果作为相位误差信号输出到环路滤波器 305b 和相位误差信号分离器 305f。

环路滤波器 305b 是平滑来自相位比较器 305a 的相位误差信号，并将其转换成直流电压信号的低通滤波器。VCO 305c 产生频率与来自环路滤波器 305b 的电压信号对应的通道比特时钟。

同步信号检测器 305e 检测读取的信号中包含的同步图案，并将其作为复位信号输出到 4-比特计数器 305d，4-比特计数器 305d 是对来自 VCO 305c 的通道比特时钟施加 1/16 分频的计数器，并由来自同步信号检测器 305e 的复位信号复位。就是说，4-比特计数器 305d 输出与读取的信号中的记录数据（字节单元）同步的字节时钟。

相位误差信号分离器 305f 把来自相位比较器 305a 的相位误差信号分成超前相位误差信号 H 和滞后相位误差信号 I，并输出到同步检测器 307。

图 46A 是表示相位误差信号分离器 305f 的详细配置的示意电路图。相位误差信号分离器 305f 包括两个倒相器 350a，350b，和两个“与”门 350c 和 350d。图 46B 是用于描述图 46A 所示的相位误差信号分离器 305f 的操作的信号的定时图。

如图 46B 所示，超前相位误差分量和滞后相位误差分量包括在从相位比较器 305a 输出的相位误差信号中。由于与通道比特时钟同步地分开这些相位误差信号 H 和 I，从“与”门 350c 输出的信号（超前相位误差信号 H）波形仅示出了超前相位误差信号分量，从“与”门 350d 输出的信号（滞后相位误差信号 I）波形仅示出了滞后相位误差信号分量。

再生信号处理器 304 是解调来自再生通道 303 的读取信号，控制子数字数据的检测，并根据检测结果提供版权保护的电路。另外，当再生内容时，再生信号处理器 304 根据加密密钥读取操作期间读取的加密密钥对解调的信号解码，并输出解码的信号作为再生信号。在读出该加密密钥时，输出该解调信号作为再生信号。

图 47 是表示再生信号处理器 304 的详细配置的方框图。再生信号处理器 304 包括解调器 304a，解码器 304b，数据选择器 304c，和初始值存储器 304c。

下面描述读取记录到控制数据区中的特定区域的子数字数据（加密密钥）。如上所述，当用户包含 n 个内容项时，n 个加密密钥作为子数字

数据嵌入控制数据区的特定部分。

将盘插入驱动器后，加密密钥再生电路 308 在引入操作期间从控制数据区中的特定区读取加密密钥，并把 n 个加密密钥存储到加密密钥再生电路 308。

当从控制器（图中未示出）接收到表明开始从控制数据区的特定区读取加密密钥（下文称该操作为“加密密钥读取模式”）的通知时，再生信号处理器 304 把初始值存储器 304d 中存储的初始值输出到伪随机数发生器 306。

伪随机数发生器 306 具有与光盘记录装置 100 的伪随机数发生器 104 相同的功能。伪随机数发生器 306 使用来自初始值存储器 304d 的初始值作为预设值，来自时钟提取部分 305 的字节时钟作为移位时钟，产生每个周期具有 2^{15} 个比特序列的伪随机数序列（M 序列）。在再生装置 300 中，使用伪随机数发生器 306 产生 256×56 比特伪随机数序列。

同步检测器 307 是检测来自伪随机数发生器 306 的伪随机数序列，从时钟提取部分 305 输出的超前相位误差信号 H 和滞后相位误差信号 I 之间的相关性，并向加密密钥再生电路 308 传送每个伪随机数（1 比特）的检测结果（正相关/负相关/无相关）的电路。

图 48 示出了同步检测器 307 的详细配置。同步检测器 307 包括 PE 调制器 307a，选择器 307b，积分器 307c，阈值估算器 307d，和 8-比特计数器 307e。

PE 调制器 307a 是具有与记录装置 100 的定时发生器 103a 和 PE 调制器 106 的响应功能对应功能的调制器。根据来自时钟提取部分 305 的字节时钟，PE 调制器 307a 对来自伪随机数发生器 306 的伪随机数序列进行 PE 调制，并将该结果作为选择控制信号输出到选择器 307b。具体地说，当来自伪随机数发生器 306 的伪随机数是 0 时，PE 调制器 1215a 向选择器 1215b 输出在再生读取信号中的每个记录数据字节的中部下降，在伪随机数是 1 时上升，和在相同的伪随机数重复时在每个记录数据字节的边缘再次反转的信号波。

选择器 307b 是各具有 2 个输入和 1 个输出的两个选择器。当来自 PE

调制器 307a 的控制信号是 1 时, 选择器 307b 把来自时钟提取部分 305 的超前相位误差信号 H 和 I 分别传送到积分器 307c 的正和负输入端。当控制信号是 0 时, 分别传送跨越积分器 307c 的正和负输入端的信号 H 和 I。

8-比特计数器 307e 是向来自时钟提取部分 305 的字节时钟施加 1/256 分频的计数器。该分频结果作为复位信号输出到积分器 307c, 阈值估算器 307d, 和加密密钥再生电路 308。因此, 每当伪随机数发生器 306 输出 256-比特随机数序列时, 该复位信号输出一个复位脉冲。

积分器 307c 是差分输入和双极输出的模拟积分器。与相加和累积输入到正输入端的脉冲区类似, 积分器 307c 相减和累积输入到负输入端的脉冲区, 向阈值估算器 307d 输出与总累积区对应的模拟信号。如果在此期间从 8-比特计数器施加复位信号。积分器 307c 从零重新开始。

结果是, 在来自 PE 调制器 307a 的 PE 调制信号是 1 时, 来自积分器 307c 的输出波指示超前相位误差信号 H 中的脉冲的相加累积区和滞后相位误差信号 I 中的脉冲的相减累积区的总累积区。当 PE 调制是 0 时, 该输出波指示超前相位误差信号 H 中的脉冲的相减累积区和滞后相位误差信号 I 中的脉冲的相加累积区的总累积区。

因此, 当正相关继续时, 积分器 307c 的输出波是具有正斜率的斜坡波 (当正相关连续时, 在 PE 调制信号到 1 时仅在超前相位误差信号 H 中出现脉冲, 当 PE 调制信号到 0 时仅在滞后相位误差信号 I 中出现脉冲)。反之, 在负相关继续时 (当负相关连续时, 在 PE 调制信号到 1 时仅在滞后相位误差信号 I 中出现脉冲, 在 PE 调制信号到 0 时仅在超前相位误差信号 H 中出现脉冲), 积分器 307c 的输出波是具有负斜率的斜坡波。当正或负相关性都不存在时, 就是说, 当脉冲在相位误差信号 H 和 I 中随机出现, 而与 PE 调制信号无关时, 由于这些误差信号中的两个脉冲的频率实质上相等, 来自积分器 307c 的输出波保持在近似零的值。

阈值估算器 307d 是比较器, 或用于确定找到来自积分器 307c 的模拟信号的三个预定电压范围的其它设备。

图 49 描述了阈值估算器 307d 的操作, 并示出从积分器 307c 输入到

阈值估算器 307d 的模拟信号波。在从 8-比特计数器 307e 施加复位信号的时刻（具体地说，刚刚在此之前），阈值估算器 307d 向加密密钥再生电路 308 输出 NRZ 格式的代码序列，当来自积分器 307c 的信号电压大于正阈值时，该代码序列为 1，当小于负阈值时，该代码序列为 0。

设定阈值以便在应用根据本发明的抖动调制时，积分器 307c 的输出电压可靠地（即可能性极高）超过阈值电压，但在不应用抖动调制时，积分器 307c 的输出电压不超过该阈值（即可能性极低）。在记录期间（调相器 107 中延迟电路 107a 的延迟）根据例如抖动调制，输入到积分器 307c 的字节数（256），每个字节的平均边缘计数值，或自然（随机出现）抖动分布中的标准偏差来确定特定值。

从阈值估算器 307d 输出的代码序列表示出了在每个 256-比特伪随机数观察到的相关性的极性（正或负）中的变化。该极性变化是与指示对于每个 256-比特的伪随机数序列，是不进行逻辑反转由抖动调制记录该伪随机数序列，还是在逻辑反转之后记录伪随机数序列的比特序列对应的信息。

加密密钥再生电路 308 根据来自同步检测器 307 的代码序列读取用于加密内容的加密密钥，并在加密密钥选择器中存储多个加密密钥。

图 50 是加密密钥再生电路 308 的详细配置的方框图。加密密钥再生电路 308 包括移位寄存器 308a，计数器 308b，加密密钥选择器 308c，和加密密钥存储器 308d。

移位寄存器 308a 是使用来自同步检测器 307 的复位信号作为移位时钟来移位和存储来自同步检测器 307 的代码序列 56-级（比特）移位寄存器。在 56-比特代码序列刚刚输入到移位寄存器 308a 之后，计数器 308b 向加密密钥选择器 308c 输出加载脉冲。加密密钥选择器 308c 由此接收移位寄存器的值。

在从计数器 308b 接收加载脉冲的同时，加密密钥选择器 308c 从控制器（图中未示出）识别当前第 i 个加密密钥的加密密钥 ID 信号，并把从移位寄存器输入的值存储到存储与加密密钥 ID 对应的加密密钥的位置。

针对加密密钥 1 至 n 重复该操作, 以便从控制数据区读取 n 个加密密钥并存储到加密密钥选择器 308c。

下面使用解密和再生第 i 个内容标题 (内容 ID=i, $i=1, 2, \dots, n$) 为例来描述基于加密密钥的内容解密和再生操作。当加密密钥选择器 308c 接收到开始解密和再生内容标题 i 的主数字数据的命令 (该操作在下文被称为“主数字数据解密和再生模式”), 来自控制器 (图中未示出) 的识别内容 ID=i 的内容 ID 信号时, 加密密钥选择器 308c 选择加密密钥 i, 把加密密钥存储到加密密钥存储器 308d, 并把加密密钥输出到再生信号处理器 304。

解调器 304a 对应光盘再生装置 100 的调制器 102a。解调器 304a 与来自时钟提取部分 305 的通道比特时钟同步地取样来自再生通道的读取信号, 并解调成代码序列 A, 进行 8-16 调制, 以便与来自时钟提取部分 305 的字节时钟同步地把通道代码 A 转换成与每个通道代码对应的 8-比特记录数据, 并把记录数据流发送到解密解码器 304b 和数据选择器 304c。

解密解码器 304b 从 8-比特记录数据 P 减去加密密钥 i 的值 Q, 并向数据选择器 304c 输出解码的数据 R。例如, 加密密钥 i 是 1, 则从 8-比特记录数据 P 减 1。数据选择器 304c 选择用于输出的解码数据 R 作为再生信号。从而根据加密密钥 i 解码读取的信号。

因此, 由于不能对加密的记录数据解密, 能够防止从不能从其读取加密密钥的 DVD 非法再生记录数据。结果是, 即使通过对包含加密密钥的合法 DVD 进行完全复制来生产新 DVD, 除非还复制了由抖动调制嵌入的加密密钥, 由于再生设备不能对主数字数据解密, 可保护 DVD 上记录的内容的版权。

常规 DVD 加密方法记录该盘并把标题密钥记录到该盘作为数据, 使其能够非法读取该密钥。然而, 本发明的方法通过抖动调制嵌入了加密密钥, 从而加密密钥检测更加困难。这改善了加密密钥安全性和保密性。

另外, 现有技术的再生方法使用估算电路来区分合法盘和非法复制, 和仅向再生信号处理器发送启动信号, 以便在识别该盘为合法盘时能够再生。然而, 通过改进电路以便向再生信号处理器输出非法启动信号,

很容易使如图 51 所示的该现有技术方法失效。

然而，利用该实施例的方法，光盘再生装置必须读取与从记录到数据控制区的子数字数据再生的内容对应的加密密钥，并解密利用该加密密钥加密的主数字数据。这意味着，即使如上所述改进该再生装置，由于再生装置不能解密被加密的主数字数据，可保护该盘内容的版权。

此外，上面借助估算电路向再生信号处理器发送启动信号以启动数据再生的方法不能通过没有图 52 所示的该估算功能的光盘再生装置来防止再生非法盘的复制品。

利用本发明的本实施例，光盘再生装置必须读取与从记录到数据控制区的子数字数据再生的内容对应的加密密钥，并利用该加密密钥对加密的主数字数据解密。因此，没有用于检测子数字数据的功能的光盘再生装置不能对加密的主数字数据解密，因而不能保护版权。

此外，即使如图 53 所示从外部设备或软件输入非法的加密密钥，以从合法盘读取数据，必须针对所有内容解密加密密钥。这明显增加了加密密钥解密过程中所涉及的工作，使有效地进行数据读取更加困难。

上面描述了根据本发明的使用子数字数据加密和解密主数字数据的数据记录介质以及记录和再生装置，很显然，本发明不限于此，而是可以以多种方式改变。

例如，在该实施例中，根据单个 56-比特加密密钥逻辑反转的 256 X 56 比特伪随机数序列被嵌入到 256 X 56 连续字节的记录数据。然而，本发明不限于这些数值。例如，也可以把多个区域中从多（1，2，或更多）种初始值开始多个伪随机数序列，或与 ECC 块，扇区，帧，或其它物理记录结构有关的字节数嵌入特定盘数据中的记录数据。

此外，该实施例中的用户数据包括多个内容项，利用该内容特定加密密钥加密每个内容项，但本发明不限于此。例如，可把用户数据分成多个记录数据单元，每个记录数据单元包含特定数量的记录数据字节或与轨迹，ECC 块，扇区，或该盘的其它物理记录结构有关的特定区中的记录数据。然后，利用专用于该记录数据单元的加密密钥加密每个记录数据。随着加密密钥数量的增加，进一步增强了用户数据的安全性。

本发明的该实施例针对每个内容项使用一个加密密钥，并分开对每个比如项加密，但本发明不限于此。例如，可将一个加密密钥用于多个记录数据单元，从而减少主数字数据记录加密密钥的数量。

该实施例按升序把加密密钥 1 至 n 记录到控制数据区的特定部分，但本发明不限于此。例如，可对记录加密密钥的顺序加扰，或根据特定规则确定该顺序。

该实施例利用在轨迹的方向移位微小量的记录标记边缘记录加密密钥作为调相的子数字数据，但本发明不限于此。例如，使用通过在径向方向把记录标记位移微小距离来记录子数字数据的各种其它方法，或使用信号幅度，跟踪误差信号，聚焦误差信号，非对称性，调制因数，或向凹坑形状或信号传递微小改变的其它技术。

此外，该实施例把用于产生伪随机数序列的初始值秘密地存储到光盘再生装置 100 的格式化器 102 和盘读取器 300 的再生信号处理器 304，但本发明不限于此。例如，光盘再生装置可把用于记录子数字数据的初始值记录到 DVD 的控制数据区。当把盘加载到光盘再生装置时，读取器在引入操作期间从控制数据区读取该初始值，并把该初始值存储到初始值存储器。

不限于把初始值记录到控制数据区作为初始值，而是可记录到用户数据区的特定部分。通过为每个记录数据单元定义多个初始值和定义伪随机数序列可进一步增强用户数据的安全性。

本实施例的加密编码器加密密钥值加到 8-比特块中的输入记录数据，但本发明不限于该加密方法。

如图 55 所示，例如，设 La 为加密密钥低位 8 比特的值，Lb 为 9 至 16 位的值，Lc 为 17 至 24 位的值。此后，加密编码器可把 La 加到记录数据 J 的 8 比特以获得加密的数据 Ka。然后，从来自 Ka 的低位的 Lb 定义的比特位置开始，逻辑反转由 Lc 指示的比特的数量以输出加密的数据 K。

此外，如图 56 所示，可利用现有技术的 DVD 加密技术中的盘密钥和标题密钥加密主机密钥，可进一步使用子数字数据加密密钥加密该加

密的主密钥，并可使用得到的密钥加扰该内容。此外，通过记录加密密钥作为子数字数据，本发明的方法可应用于利用加密密钥加扰记录数据的所有加密方法。

该实施例把用作子数字数据的保密密钥预先存储到光盘再生装置100，但可响应用户命令或与外部设备安全通信来写入该保密密钥。

此外，已参考 DVD-ROM 介质描述了该实施例，但本发明不限于此，而是可应用于 CD-ROM，DVD-RAM，和其它介质。此外，在略微改变记录标记的形状或位置时写入凹坑（记录标记）的情况下，本发明可用于使用除用于数据记录的凹坑和纹间表面信息外的各种记录方法的介质，包括相位转移（相位改变）和磁化。

<实施例 4>

在本发明的该实施例中，把用于加密主数字数据的加密密钥作为子数字数据重叠地记录到加密的主数字数据。

（光盘）

图 56 示出了根据本发明该实施例如何由光盘中的块来提供加密密钥。利用用于该块的加密密钥对光盘的每个 ECC 块在中的用户数据加密。用于加密每个块的加密密钥作为子数字数据重叠地记录到 ECC 块中的记录数据。从每个 ECC 块的开始把加密密钥作为子数字数据重叠地记录到主数字数据的前 14,336 个字节（256 字节 X 56-比特加密密钥）。

这导致了用于加密特点 ECC 块的加密密钥重叠到该 ECC 块中的记录数据作为子数字数据。当合法 DVD 再生装置具有用于从 ECC 块读取信号的始端读取加密密钥的功能时，它能够读取加密的主数字数据，没有该功能的非法再生装置不能对加密的主数字数据解密。因此，可避免通过销售非法 DVD 再生装置来侵犯版权。

（光盘记录装置）

本发明该实施例中的光盘再生装置的配置与图 35 所示的相同。下面

描述把子数字数据重叠到主数字数据时加密和记录主数字数据的操作。

为记录 ECC 块 i ($i=1$ 至 n)，加密密钥选择器 101a 从控制器（图中未示出）接收开始主数字数据加密和记录模式，加密密钥记录模式的信号，和指示 ECC 块 i 的内容 ID 信号，然后把加密密钥 i 发送到加密编码器 101b。

如上面实施例 3 所描述的，加密编码器 101b 利用加密密钥 i 对 ECC 块 i 的记录数据 J 加密，并把加密的数据输出到数据选择器 101c。数据选择器 101c 向格式化器 102 发送加密的数据。格式化器 102 的调制器 102a 执行 8-16 调制以转换加密的数据，并向调相器 107 输出通道信号 B。

使用实施例 3 中描述的相同的子数字数据记录方法，把加密密钥重叠记录到通道信号 B。格式化器 102 向伪随机数发生器 104 初始值，向 XOR 门 105 输出加密密钥 i 。伪随机数发生器 104 根据输入至此的初始值和字节时钟来向 XOR 门 105 输出伪随机数序列。XOR 门 105 根据输入的伪随机数序列向 PE 调制器 106 输出伪随机数序列。PE 调制器 106 执行 PE 调制，以便根据来自定时发生器 103 的定时信号转换来自 XOR 门 105 的伪随机数序列 D，并把得到的 PE 调制信号 E 输出到 PE 调制器 106。

PE 调制器 107 执行相位调制以便根据来自 PE 调制器 106 的 PE 调制信号 E 略微延迟或超前来自格式化器 102 的通道信号 B 的边缘，和向记录通道 108 输出调制的通道信号 F。

记录通道 108 与来自调相器 107 的调制通道信号 F 的 1/0 同步地产生开启/关闭发射到 DVD 10 的激光束的控制信号，并把控制信号发送到记录头 109。记录头 109 根据来自记录通道 108 的控制信号，通过在切换激光束通和断时发射激光束来把记录标记刻到旋转 DVD 10 的表面的螺旋图案。结果是，在 DVD 10 中形成了由可光学读取的凹坑和纹间表面组成的调制的记录标记 G。

作为该操作的结果，把加密密钥 i 作为子数字数据重叠记录通道信号 B，该子数字数据等同于在 ECC 块始端的 256 X 56 字节的加密数据。

这意味着，即使使用正常的盘读取器读取记录了加密密钥的 DVD 上

的所有内容，并把读取的内容直接记录到另一个 DVD，仅能复制主数字数据，而不能复制以抖动嵌入记录的子数字数据（加密密钥）。因此，盘读取器不能从非法复制的 DVD 解密和播放加密的主数字数据。从而避免了通过销售盗版编辑而侵犯版权。

此外，已参考 DVD-ROM 介质描述了该实施例，但本发明不限于此，而是可应用于 CD-ROM，DVD-RAM，和其它介质。此外，在略微改变记录标记的形状或位置时可写入凹坑（记录标记）的情况下，本发明可应用于使用除用于数据记录的凹坑和纹间表面信息外的各种记录方法的介质，包括相位转移（相位改变）和磁化。图 35 所示的记录装置可应用于该实施例，以具有相同的操作和配置。

（光盘再生装置）

根据本发明该实施例的光盘再生装置的配置与图 44 所示的相同。如图 57 所示加密密钥再生电路的内部配置。

下面参考解密和再生再生记录 ECC 块 i ($i=1$ 至 n) 来描述提取重叠到主数字数据的子数字数据时该再生装置解密和再生主数字数据的操作。

当再生信号发生器 304 从控制器（图中未示出）接收通知开始“加密密钥读取模式”和“内容解密和再生模式”，和识别 ECC 块 i 的内容 ID 信号，解调器 304a 对从再生通道输入的读取信号应用 16-8 解调，并把解调信号 P 输出到解码器 304b 和数据选择器 304c。再生信号处理器 304 还向伪随机数发生器 306 输出存储到初始值存储器 304d 的初始值。伪随机数发生器 306 根据该初始值产生伪随机数序列（ M 序列）。

同步检测器 307 检测来自伪随机数发生器 306 的伪随机数序列与从时钟提取部分 305 输出的超前相位误差信号 H 和滞后相位误差信号 I 之间的相关性，并向加密密钥再生电路 800 输出每个伪随机数（1 比特）的结果（正相关，负相关，无相关）。

加密密钥再生电路 800 根据输入的复位信号和代码序列读取该加密密钥。移位寄存器 800a 是使用来自时钟提取部分 305 的复位信号作为移

位时钟来移位和存储来自同步检测器 307 的代码序列的 56-比特（56 级）移位寄存器。在 56-比特代码序列刚刚输入到移位寄存器 800a 后，计数器 800b 向加密密钥存储器 800c 输出加载脉冲/加密密钥存储器 800c 此时存储来自移位寄存器 800a 的值/在刚刚存储加密密钥 i 后，加密密钥存储器 800c 向再生信号处理器 304 输出加密密钥 i。

解密解码器 304b 从由再生通道 303 输入的 8-比特解调信号数据减去由加密密钥存储器 800c 输入的加密密钥 i 的值，并输出到数据选择器 304c。例如，如果加密密钥 i 是 1，从 8-比特记录数据减 1。数据选择器 304c 选择解密编码器 304b 的输出作为再生信号。从而根据加密密钥 i 解密该解调信号。

除了上面第一实施例的优点外，本发明的该第四实施例记录用于加密重叠到每个 ECC 块的加密数据的每个 ECC 块的加密密钥。因此，当再生该数据以再生每个 ECC 块时，需要读取嵌入主数字数据中的加密密钥，并对加密的数据解密。因此，能够在没有加密密钥解密功能的情况下防止从 DVD 非法读取数据。

此外，即使从外部设备或软件把非法加密密钥输入到来自合法复制的读取数据。必须针对每个 ECC 块解密该加密密钥。这明显增加了加密密钥解密过程中所涉及的工作，并有效地使读取数据更困难。

本实施例使用专用于每个块的加密密钥对该块加密，但本发明不限于此。例如，可将用户数据分成多个记录数据单元，每个记录数据单元包含与轨迹，ECC 块，扇区，或盘的其它物理记录结构有关的特定区中的特定数量的记录数据字节或记录数据。利用专用于该记录数据单元的加密密钥对每个记录数据单元加密。随着加密密钥数量的增加进一步增强了用户数据的安全性。

此外，该实施例把特定数据块的加密密钥记录到该块中的记录数据流，但本发明不限于此。例如，如图 58 所示，可以与记录数据的前一个单元的记录数据重叠记录用于记录数据的特定单元的加密密钥。当连续再生短暂连续的记录数据单元时，由于在再生前一个单元时预先读取了再生该数据所需的加密密钥，该方法立即启动要再生的希望的记录数据

单元（即不需等待读取该加密密钥）。因此，能够记录用于加密记录数据的特定单元的加密密钥，与不同单元的记录数据中的记录数据重叠。

在根据本发明第三和第四实施例的光盘中，加密密钥以使其难以读取的方式作为子数字数据嵌入到主数字数据。因此，在根据记录标记的出现简单地复制光盘时，不复制该加密密钥。从而可防止解密该加密的主数字数据，防止了通过准确地复制光盘上的数字内容侵犯版权。

此外，利用抖动调制嵌入加密密钥使在根据本发明第三和第四实施例的光盘中解密该加密密钥更加困难。

此外，由于使用不能读取加密密钥的光盘不能对加密的记录数据解密，根据本发明的第三和第四实施例，可利用光盘防止非法读取记录的数据。因此，即使完全复制包含该加密密钥的光盘，除非也复制利用抖动调制嵌入的加密密钥，否则不能解密光盘复制品上加密的主数字数据，因而可保护版权。

本发明以难以进行读取的方式把读取盘内容所需的密钥作为子数字数据嵌入主数字数据。因此，在根据记录标记出现简单地复制光盘时，未记录子数字数据。这防止在光盘上对受版权保护的数字内容的完全非法复制，并防止了解密主数字数据。结果是，本发明能够防止通过在光盘上完全复制受版权保护的数字内容来侵犯版权。

已经描述了本发明，很显然，可以以多种方式改变本发明。这些改变不脱离本发明的精神和范围，很显然，对于本领域技术人员来说，所有这些改变包括在下面权利要求的范围中。

图 1

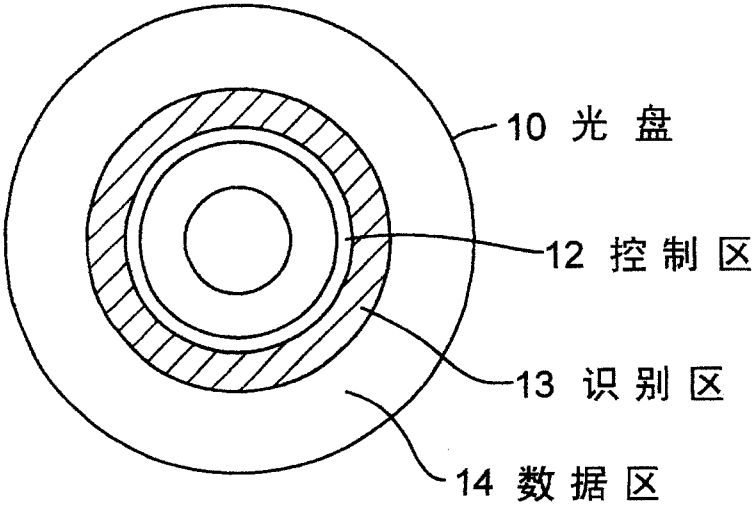


图 2

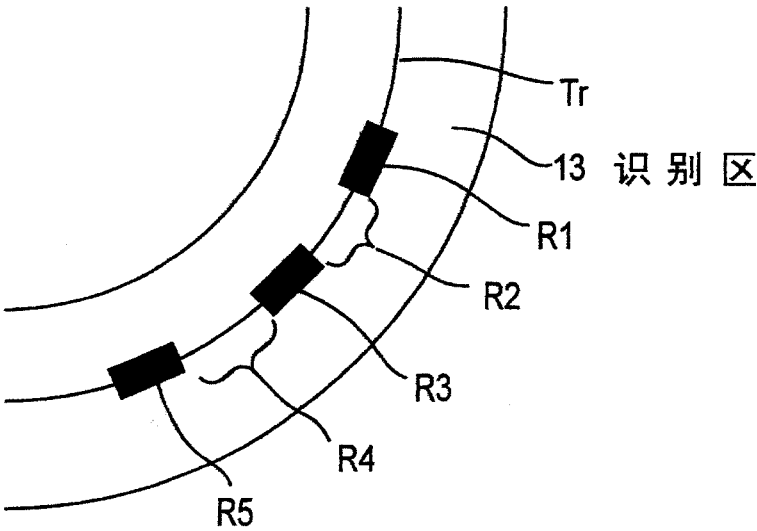


图 3

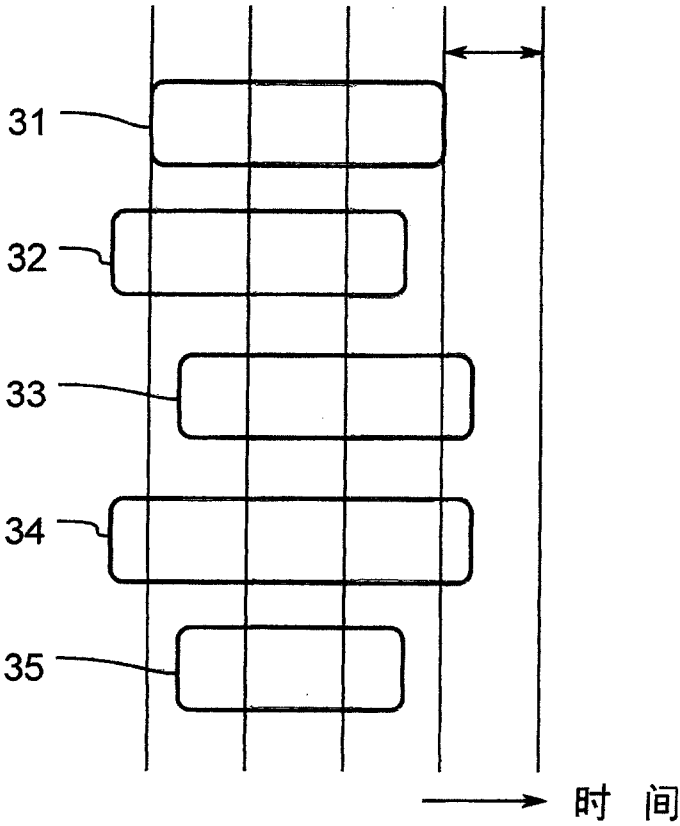
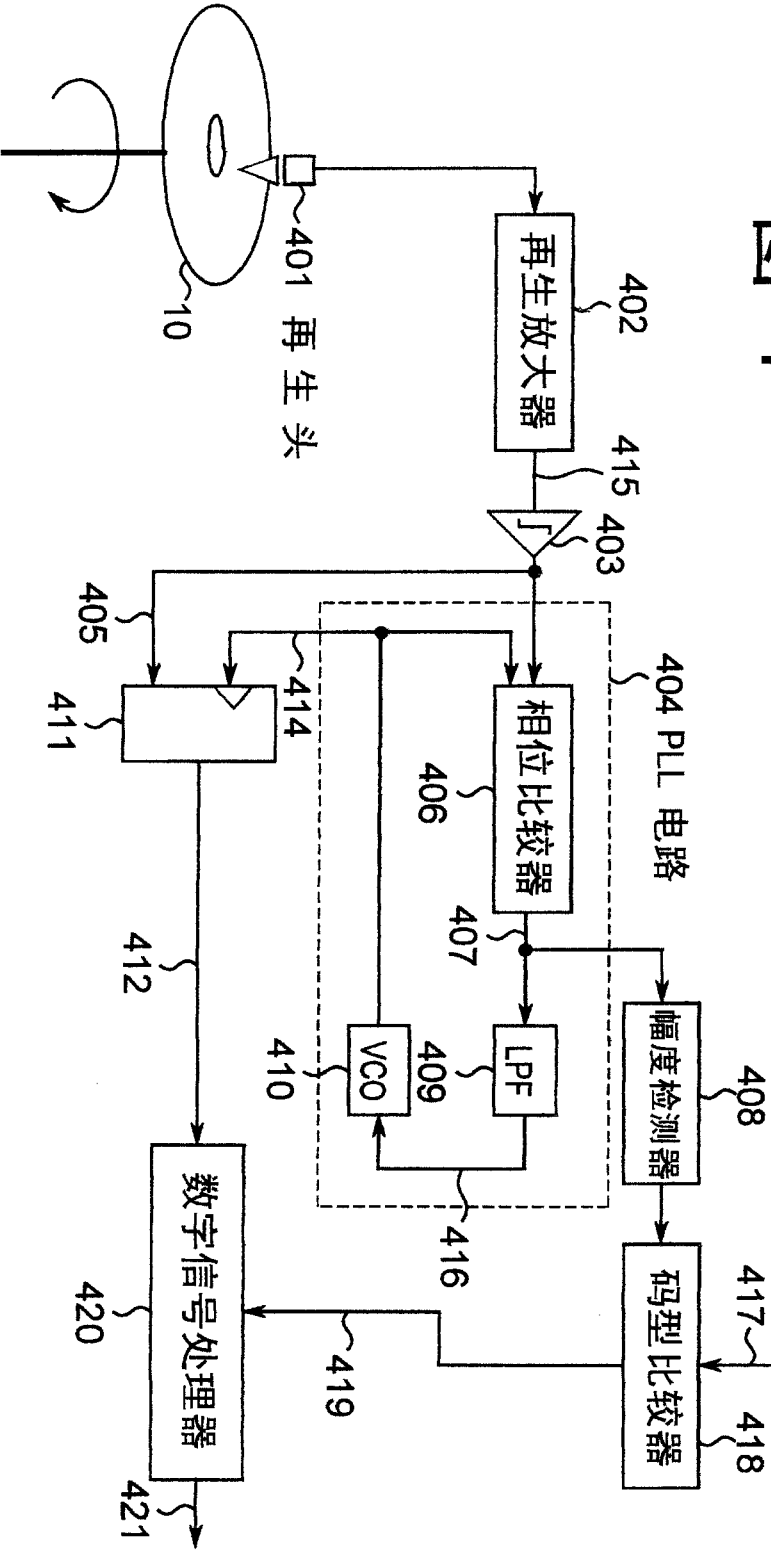


图 4



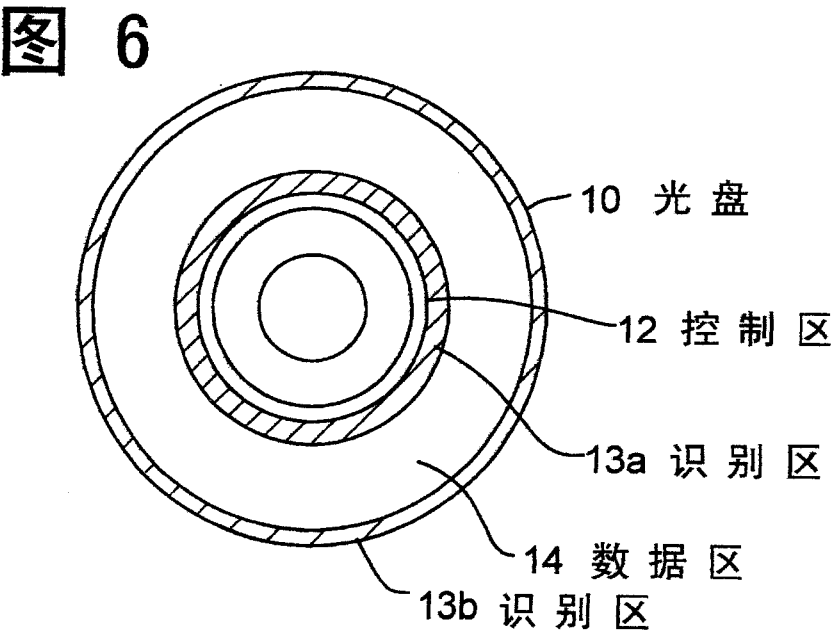
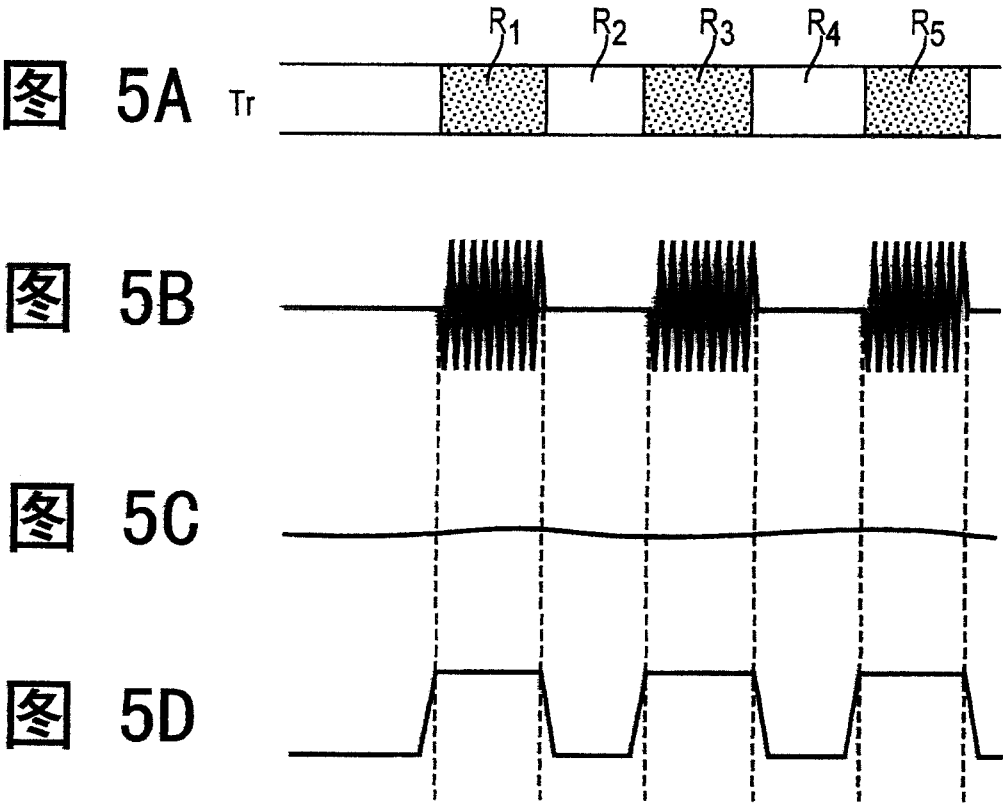


图 7

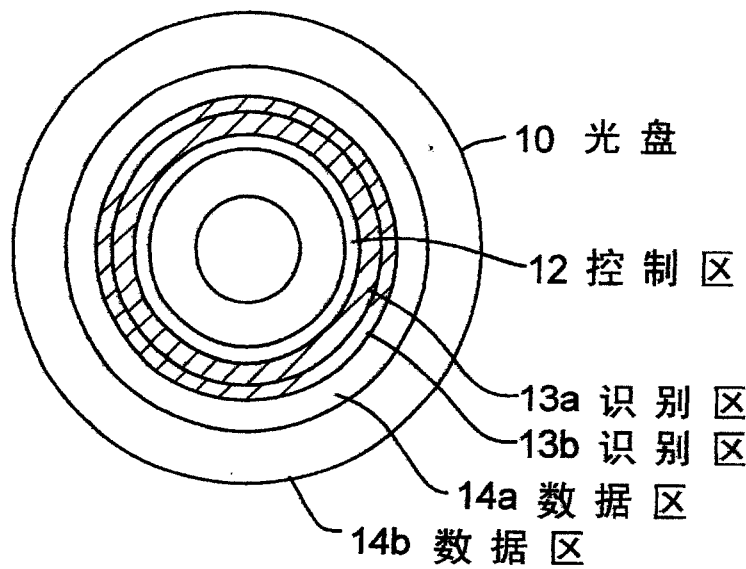


图 8

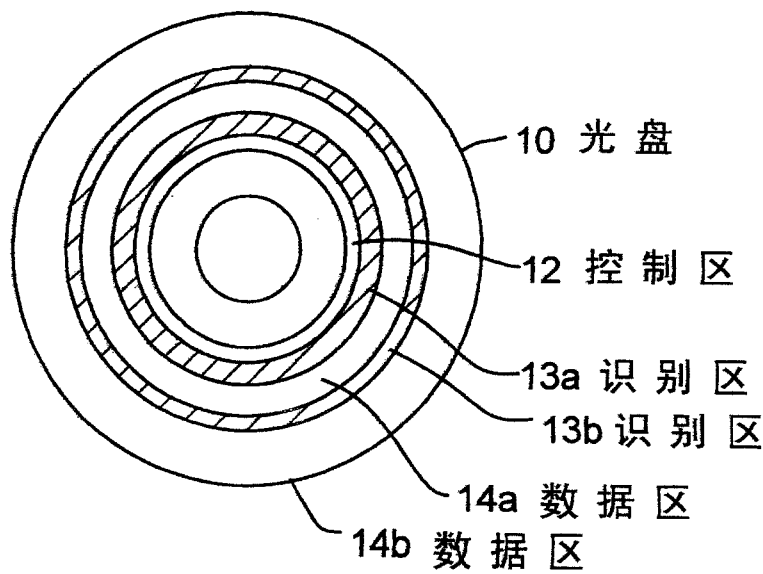


图 9A

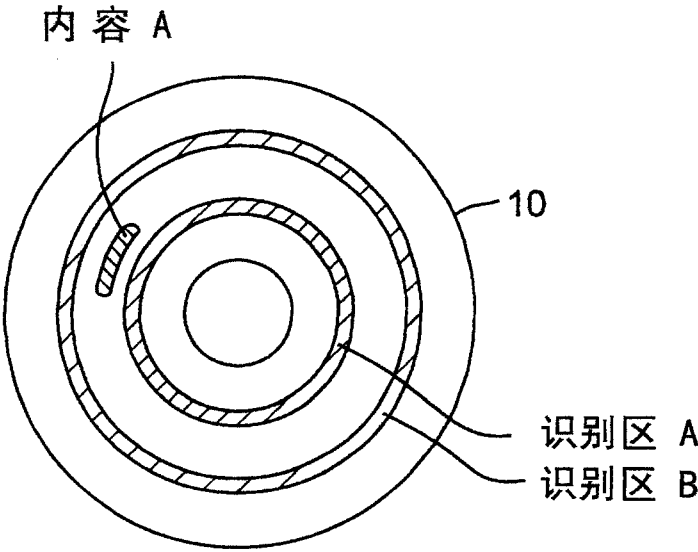


图 9B

	识别区 A	识别区 B
内容 A 的 识别信息	A1	
		A1
	A1	A1
	A1, A2	
	A1	A2
	A1, A1	
	A1, A1	A1, A1
	A1, A2	A1, A2
	A1, A1	A2, A2

图 10

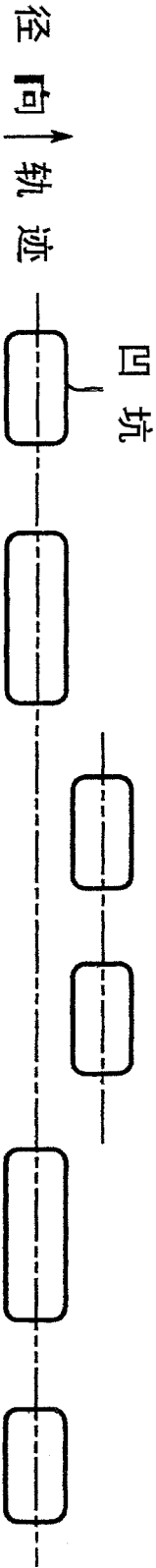


图 11

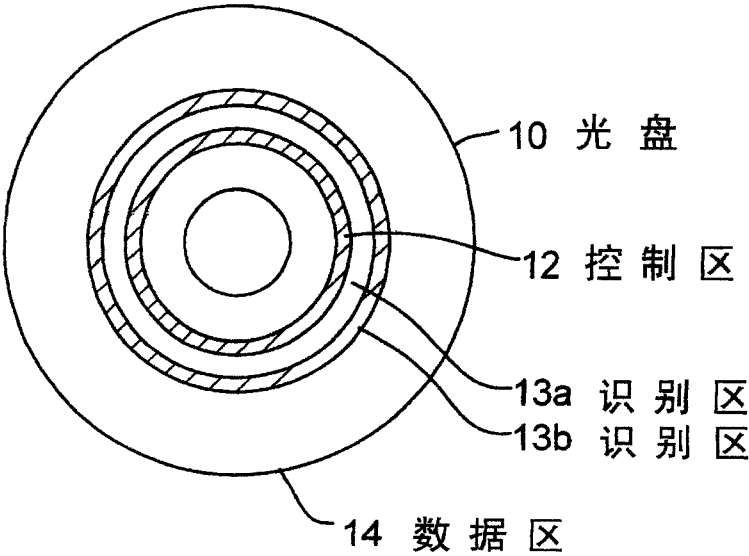


图 12

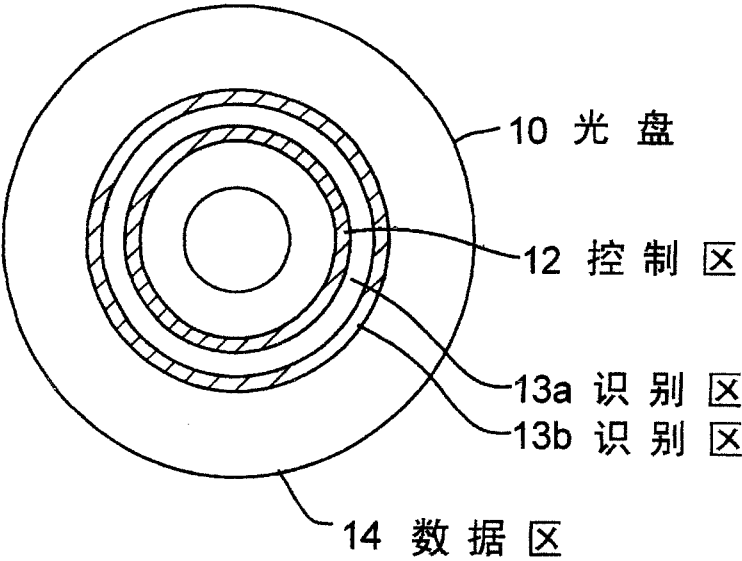
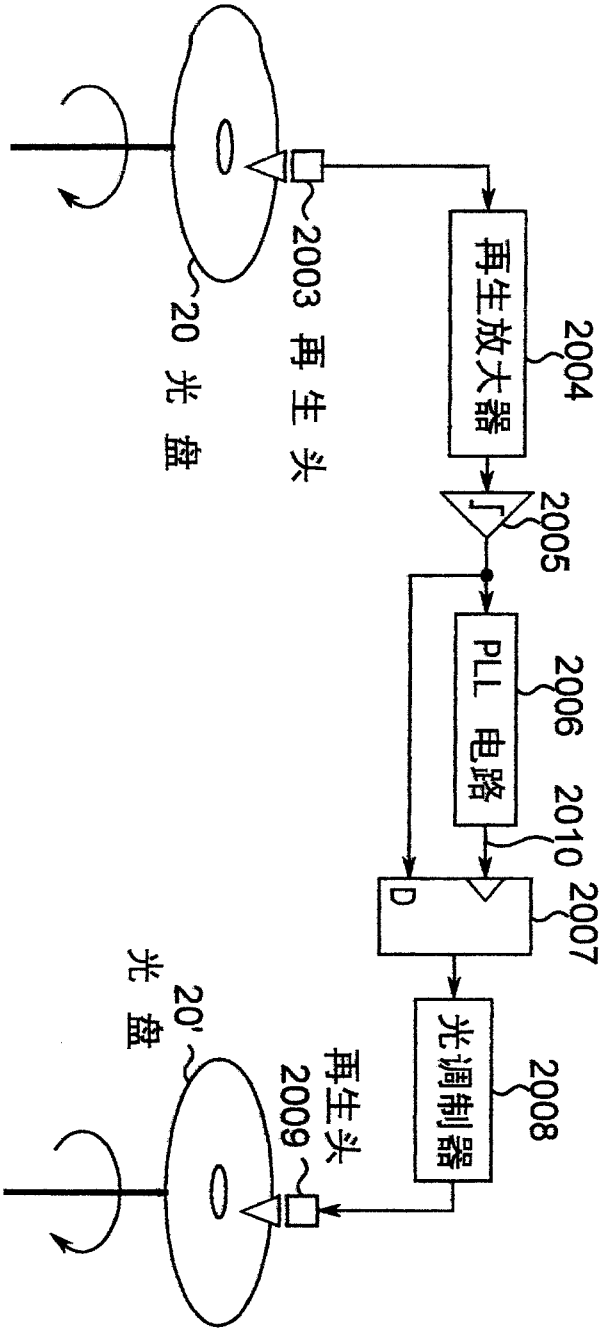
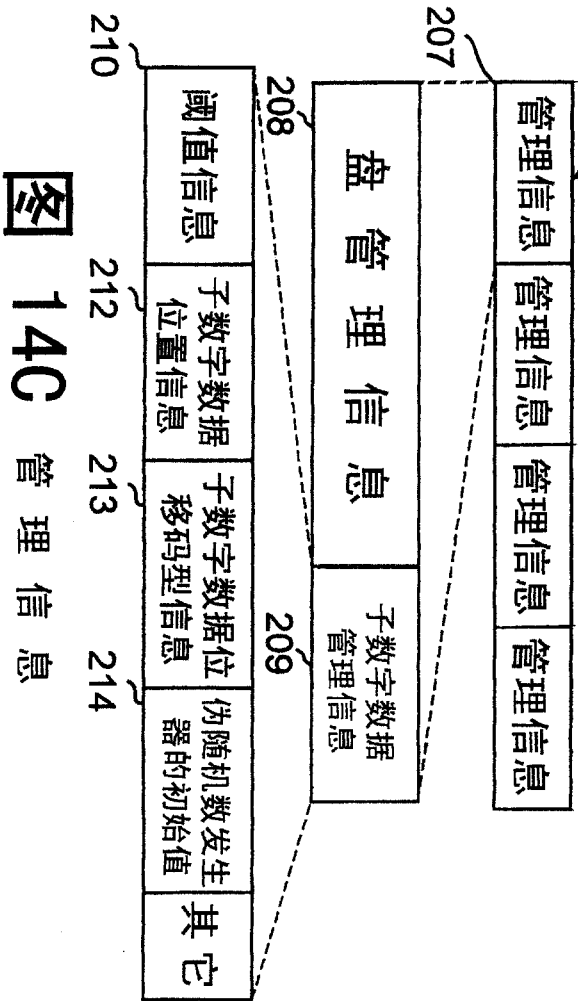
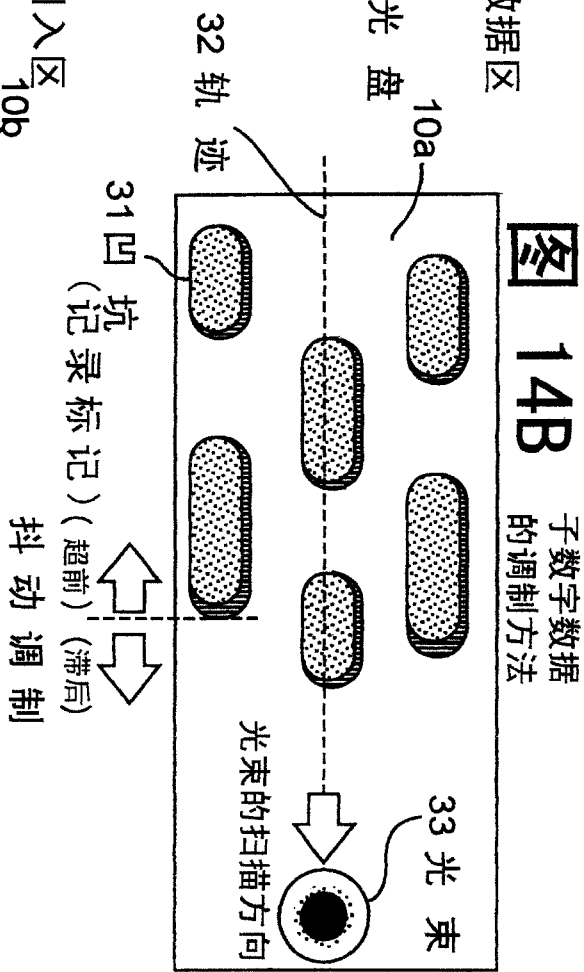
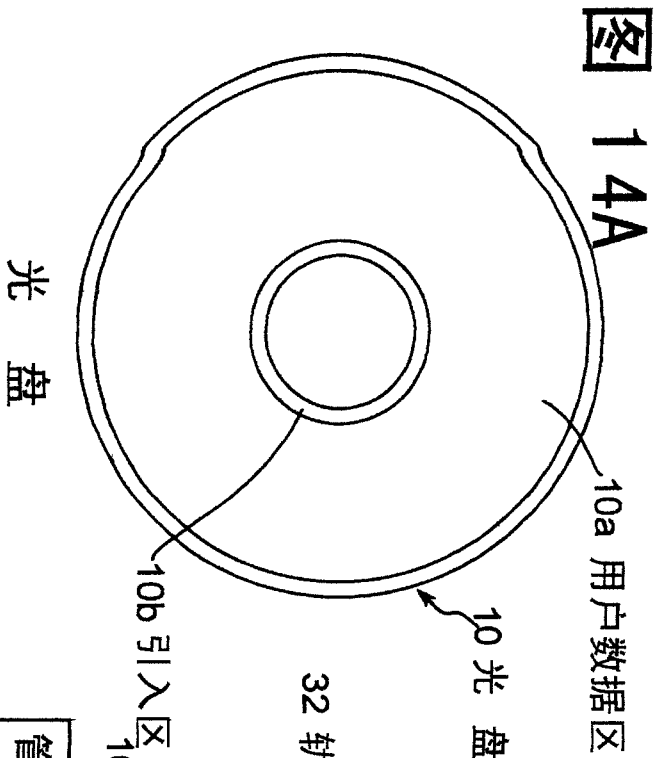


图 13





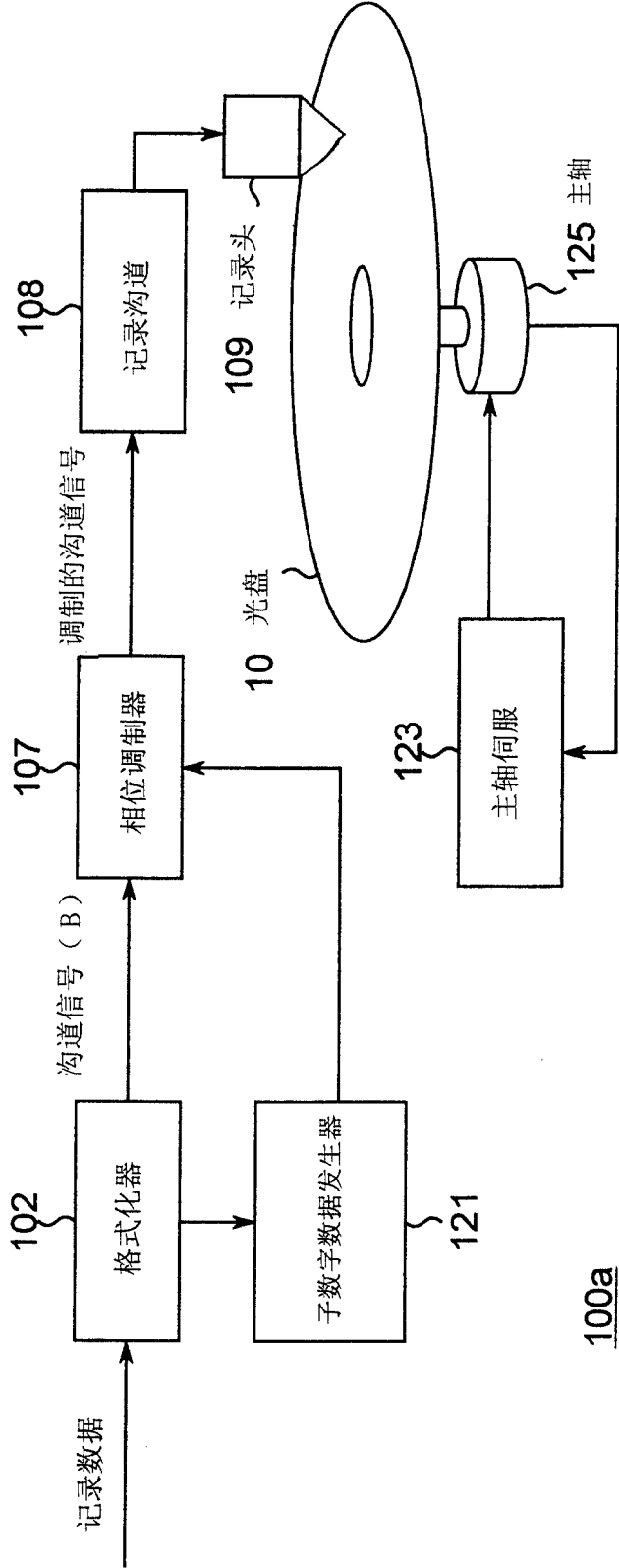


图 15

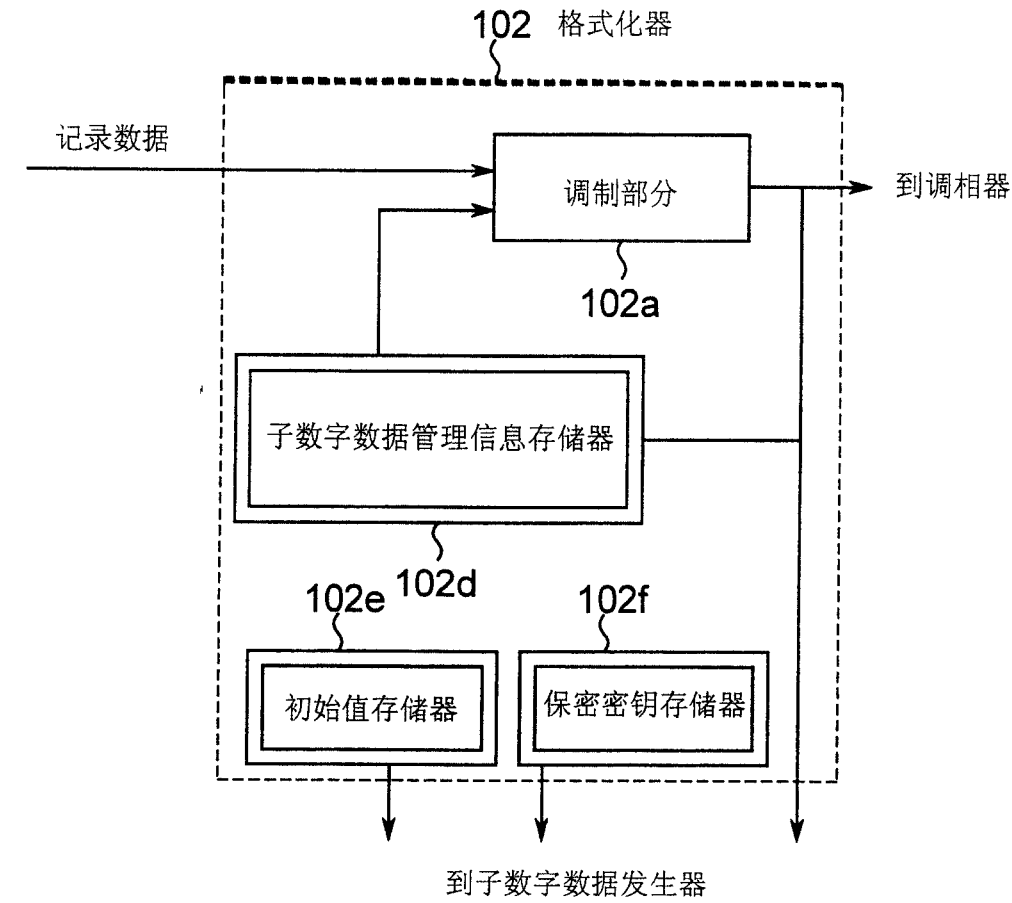


图 16

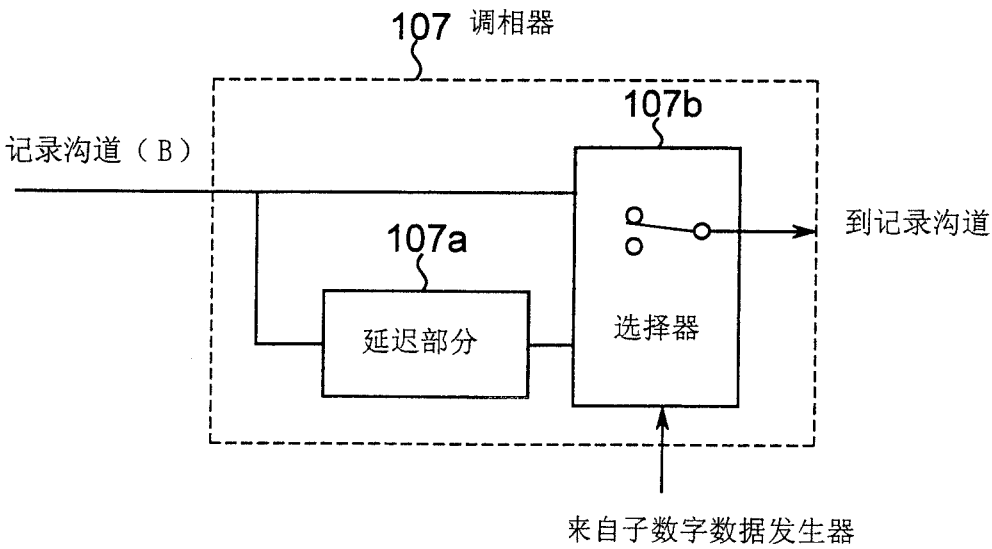


图 17

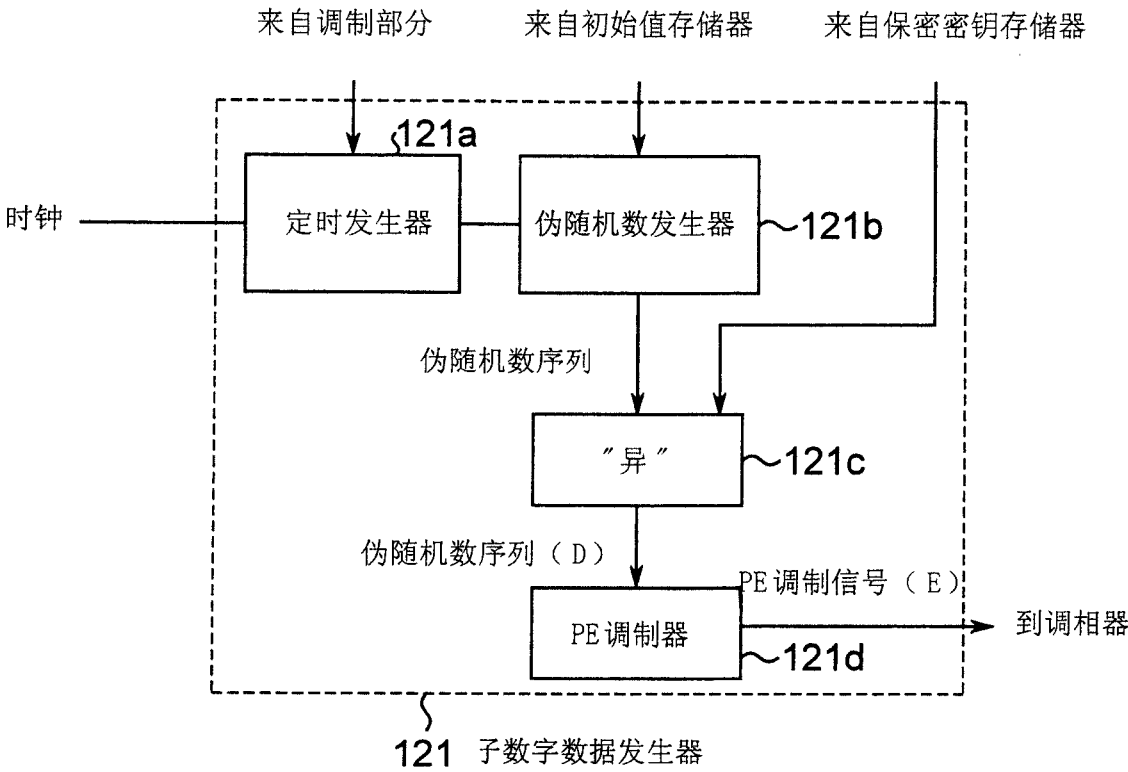


图 18

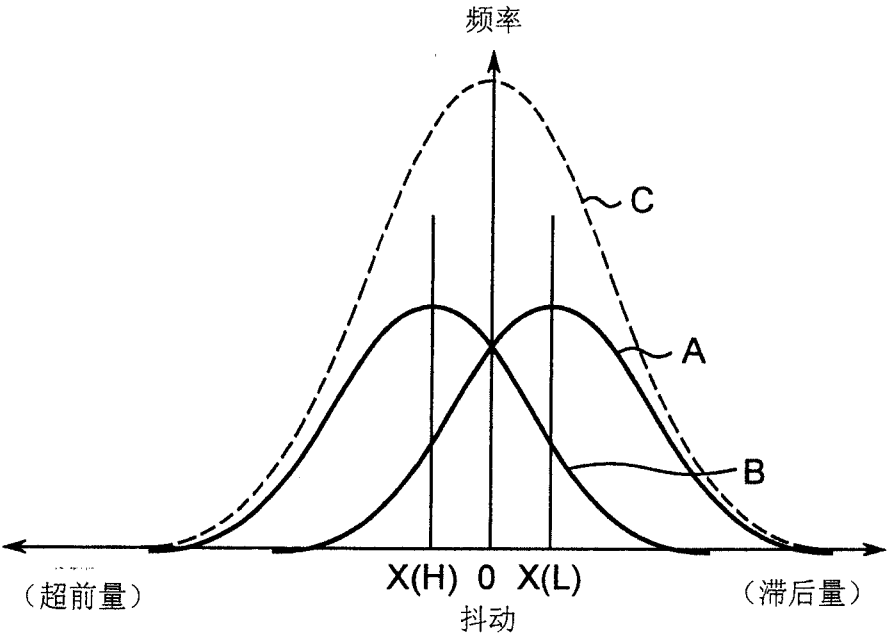


图 19

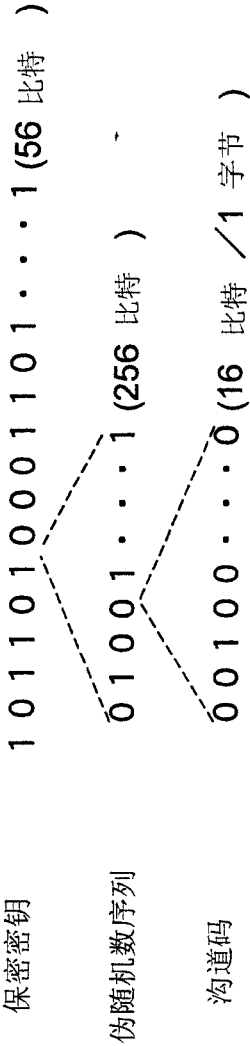
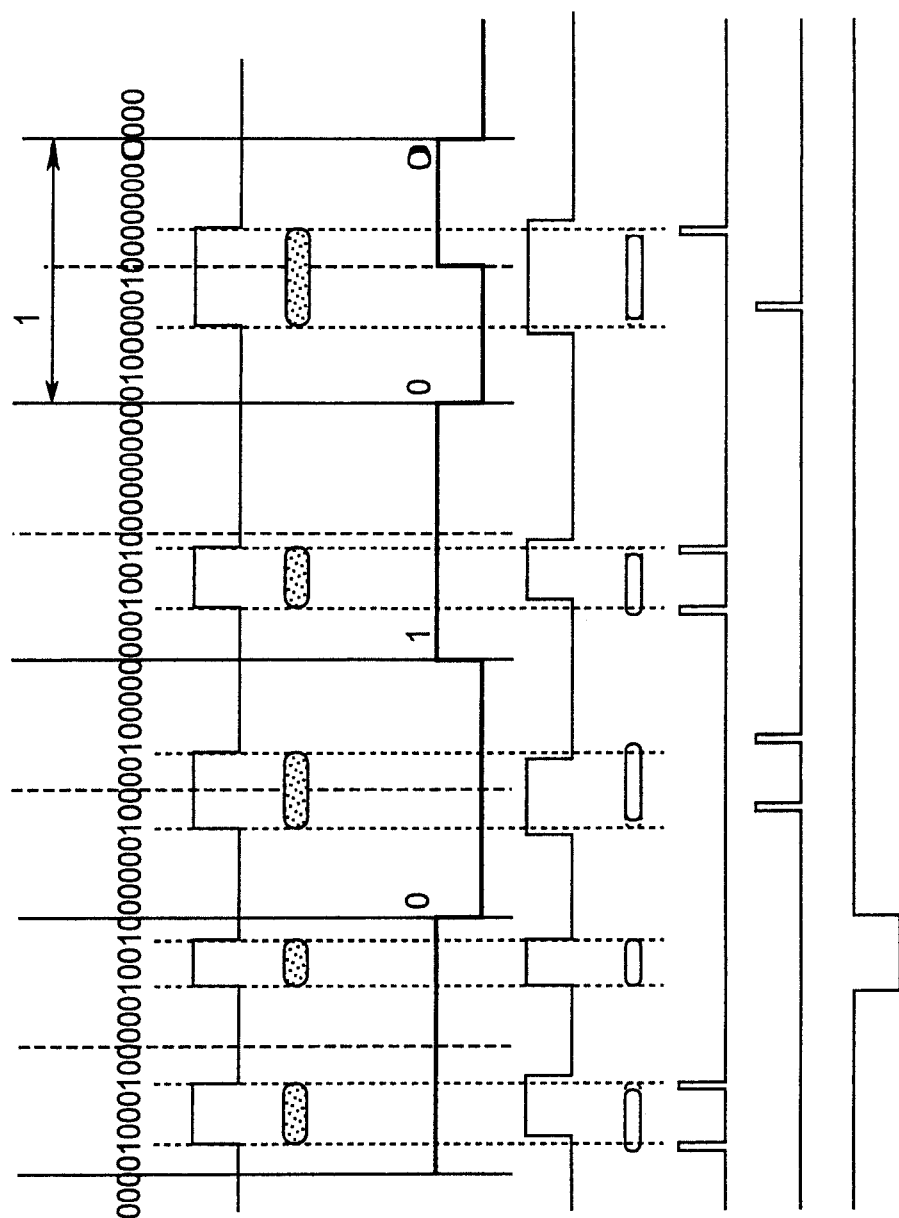


图 21



22

A. 沟道码

B. 沟道信号

C. 标准记录标记

D. 伪随机数序列

E. PE调制信号

F. 调制的沟道信号

G. 调制的记录标记

H. 超前相位误差信号

1. 滞后相位误差信号

J. 选通信号

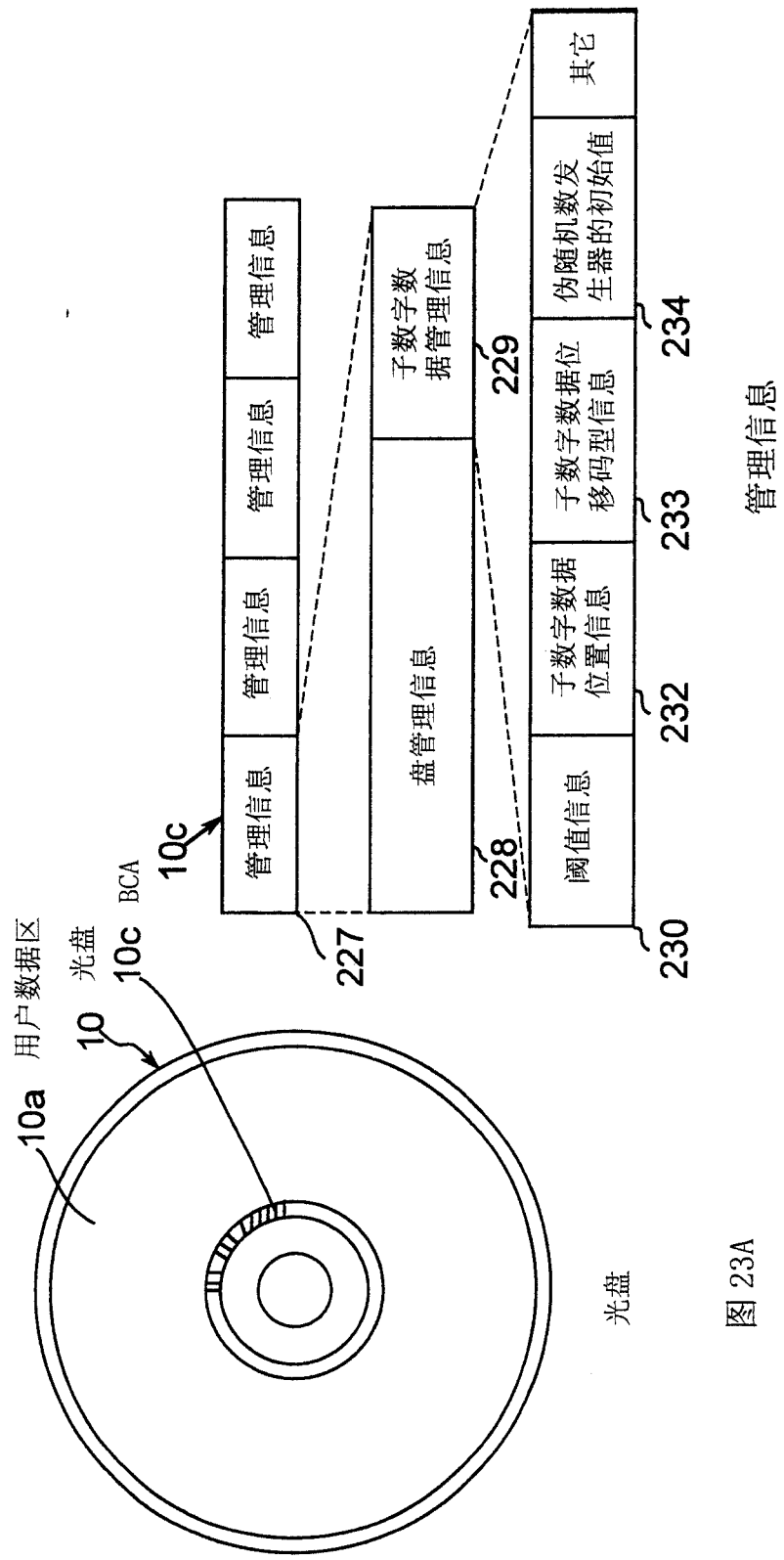


图 23B

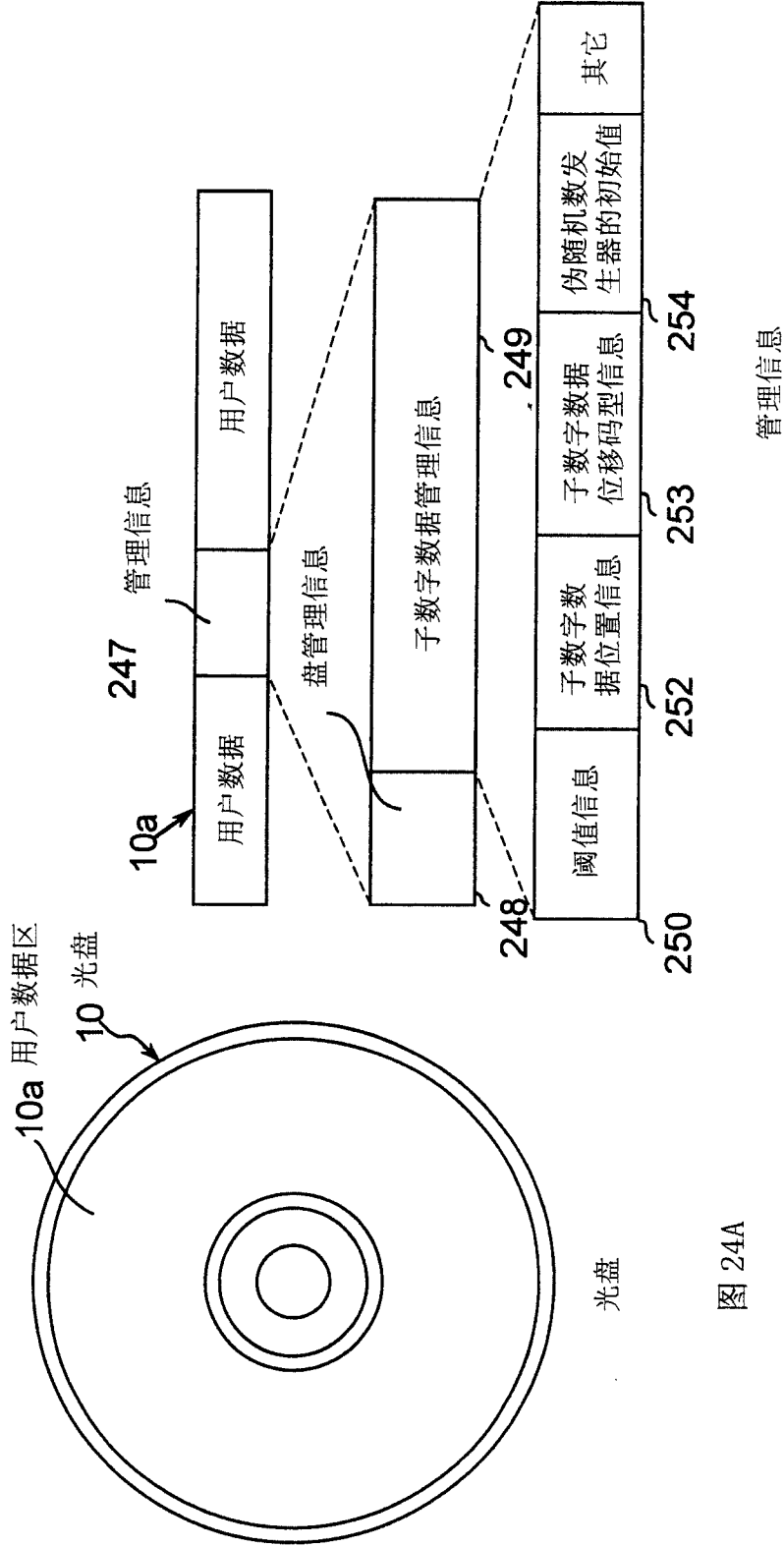


图 24A

图 24B

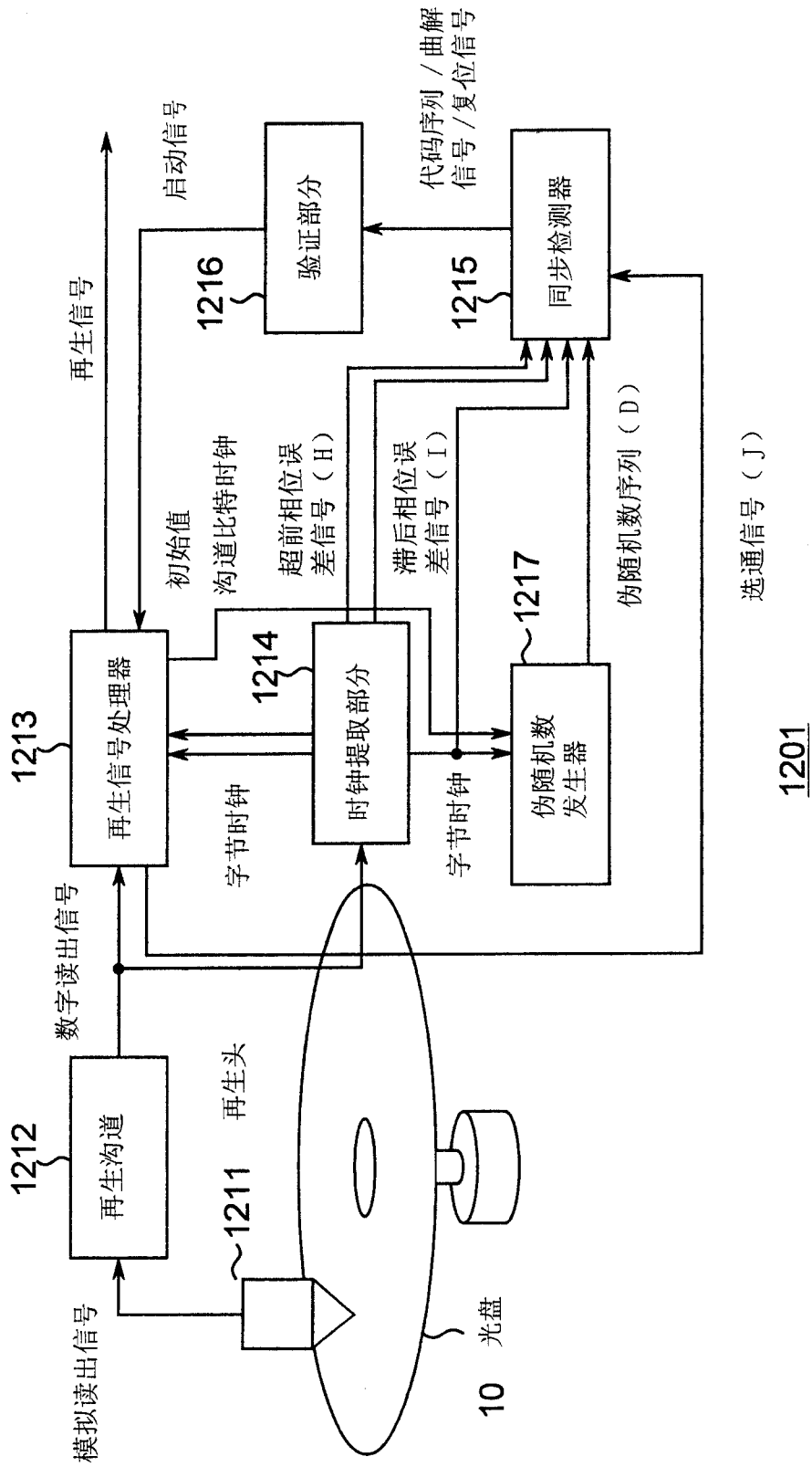


图 25

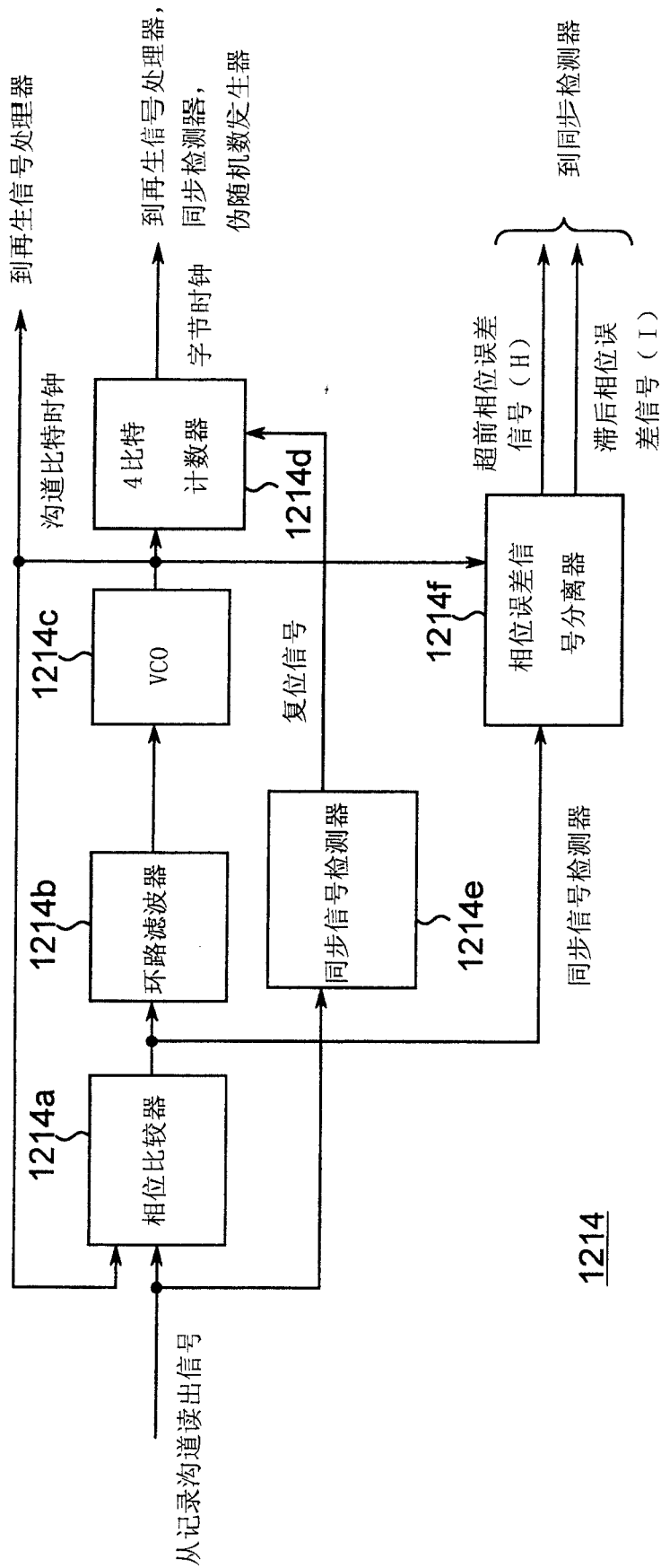


图 26

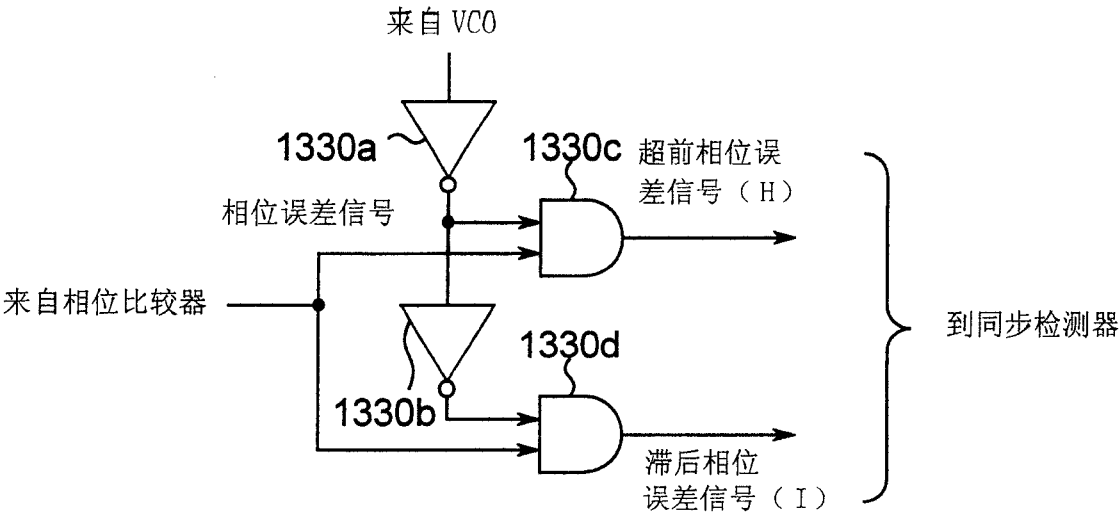


图 27A

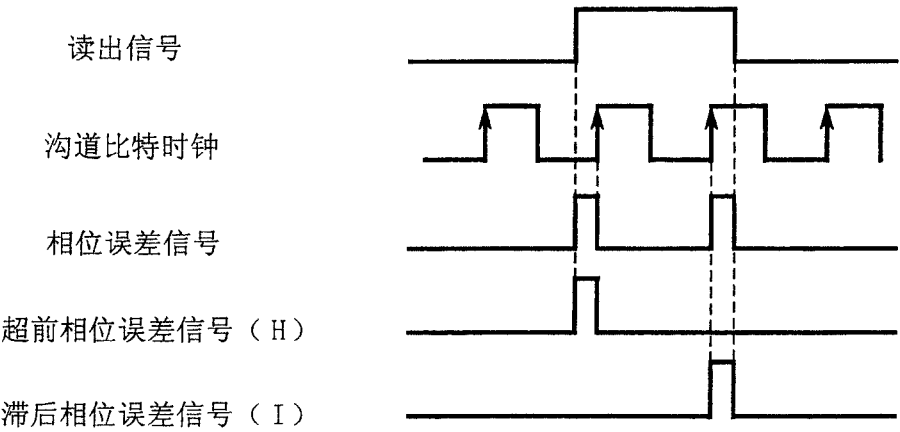


图 27B

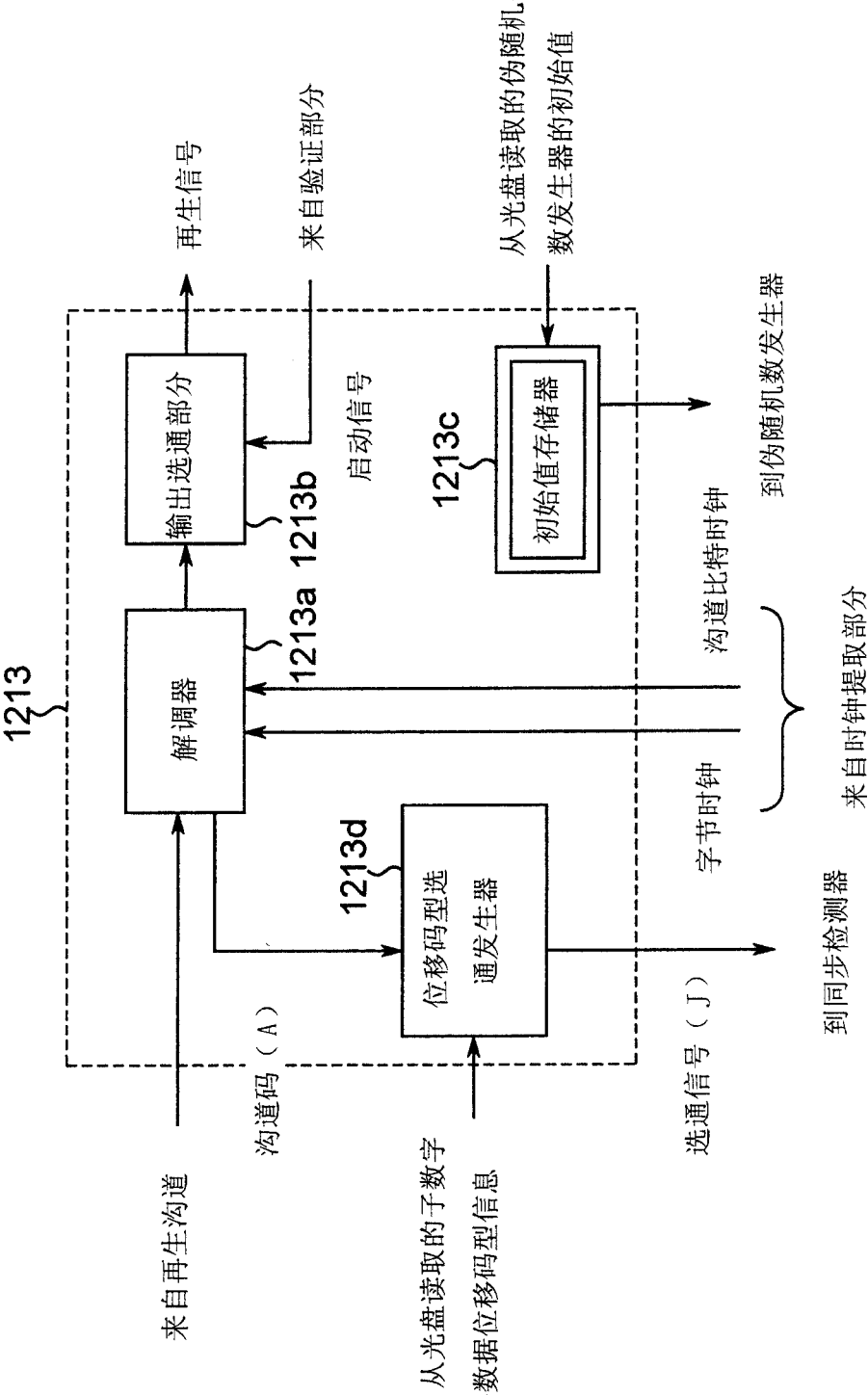


图 28

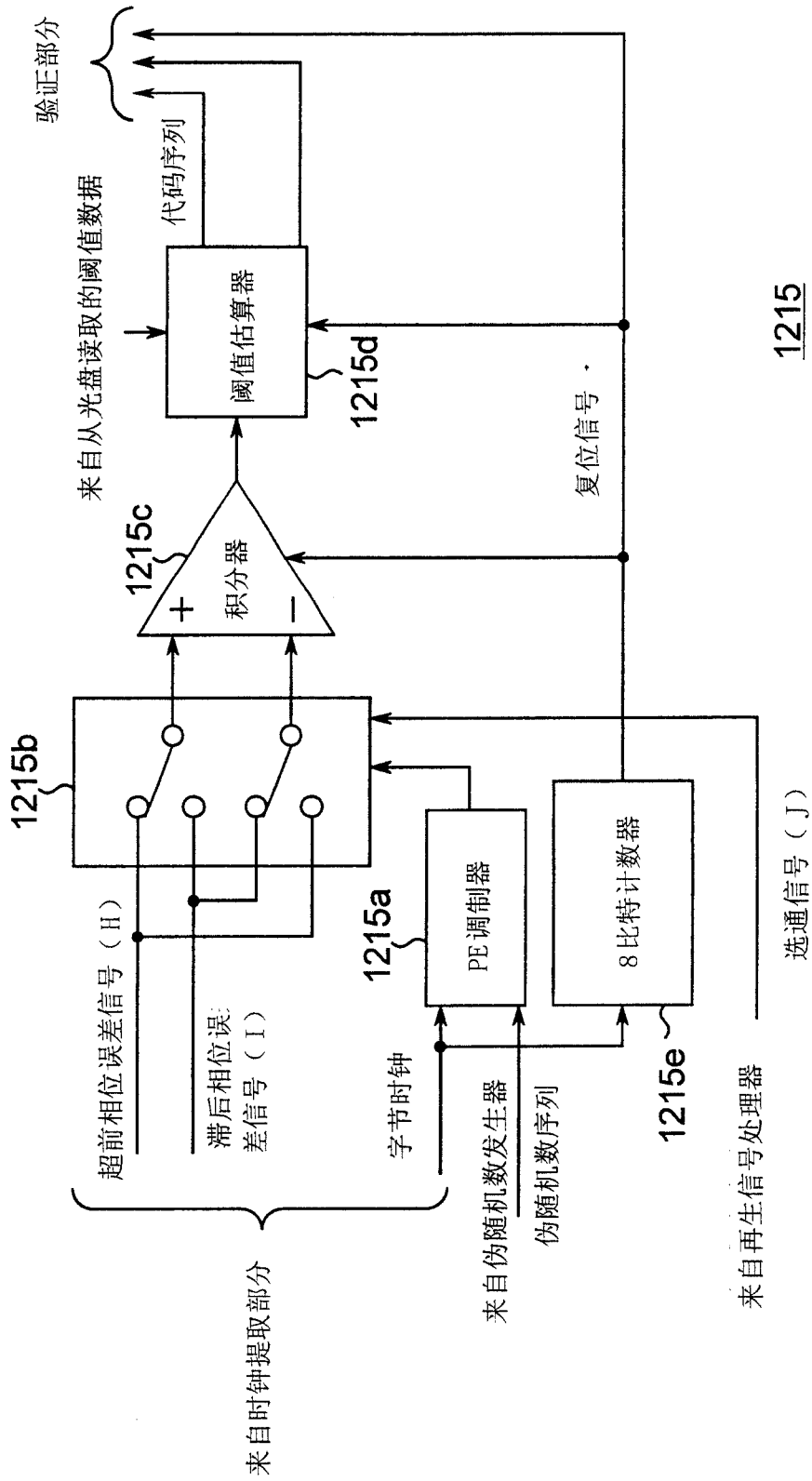


图 29

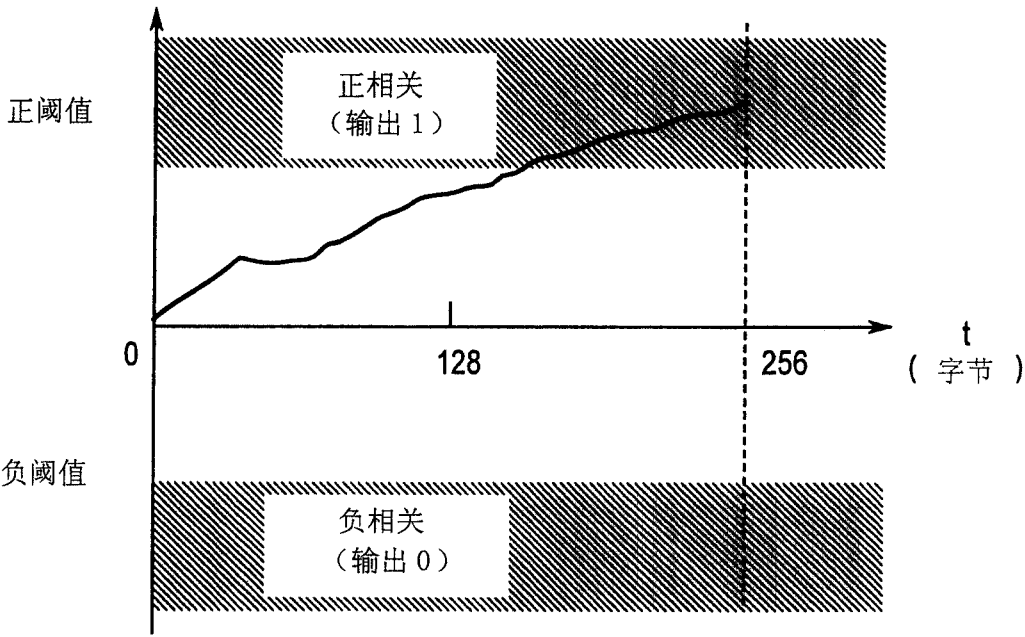


图 30

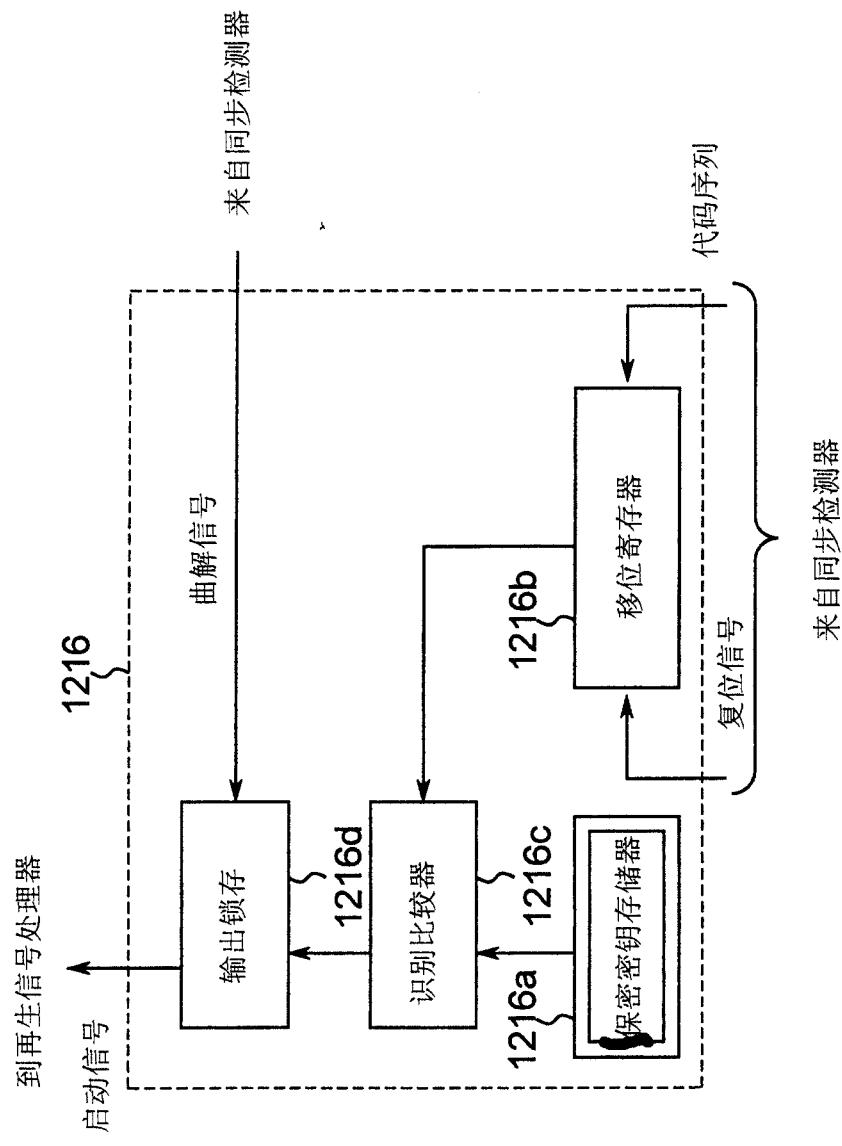
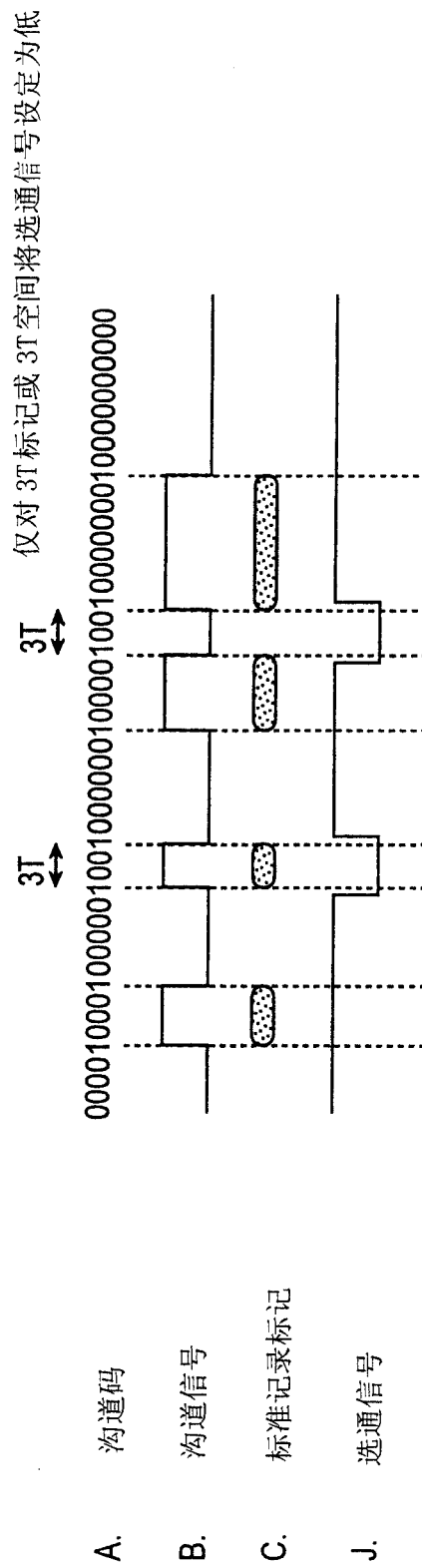


图 31



32

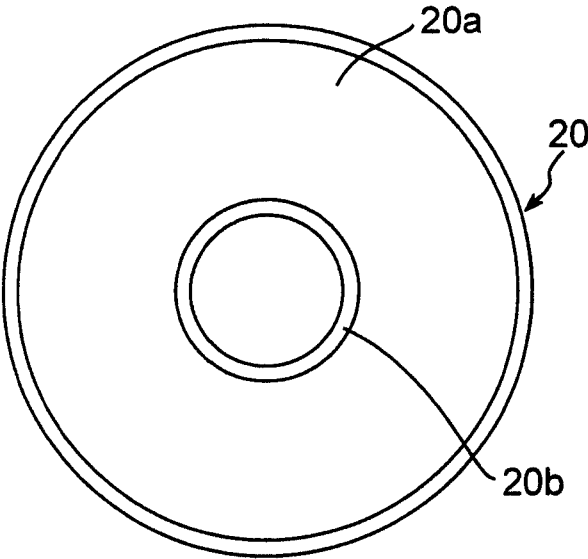


图 33

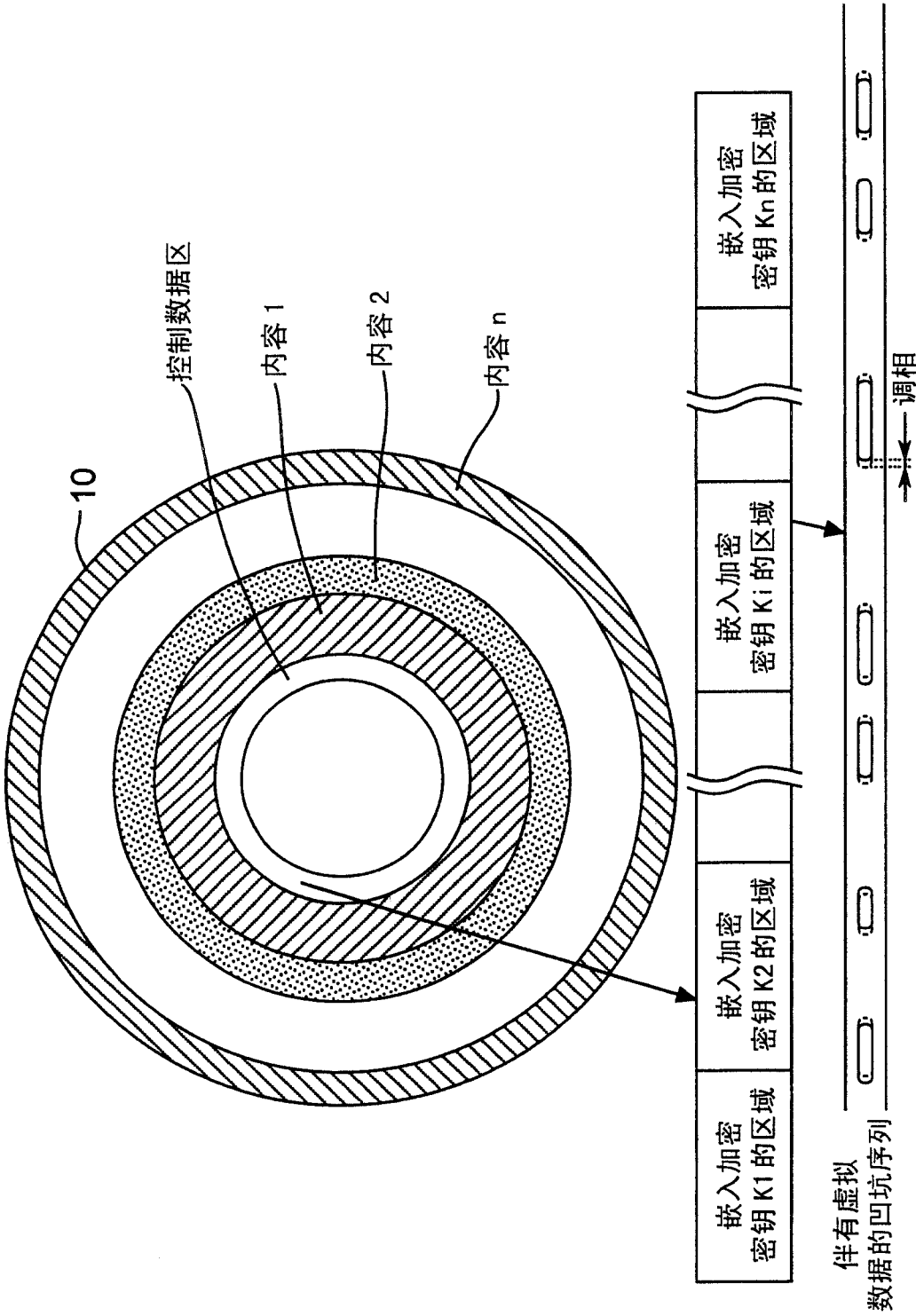


图 34

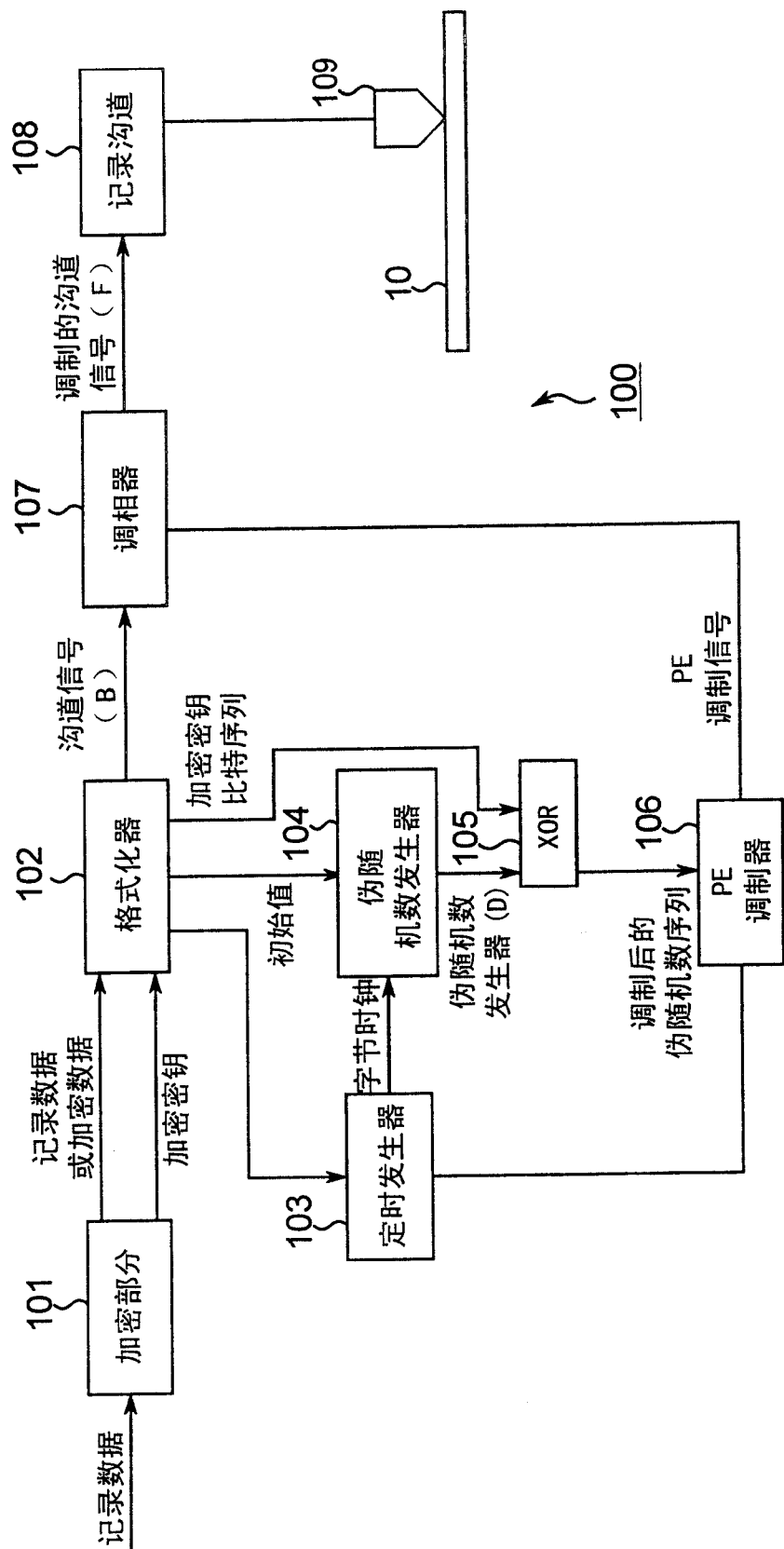
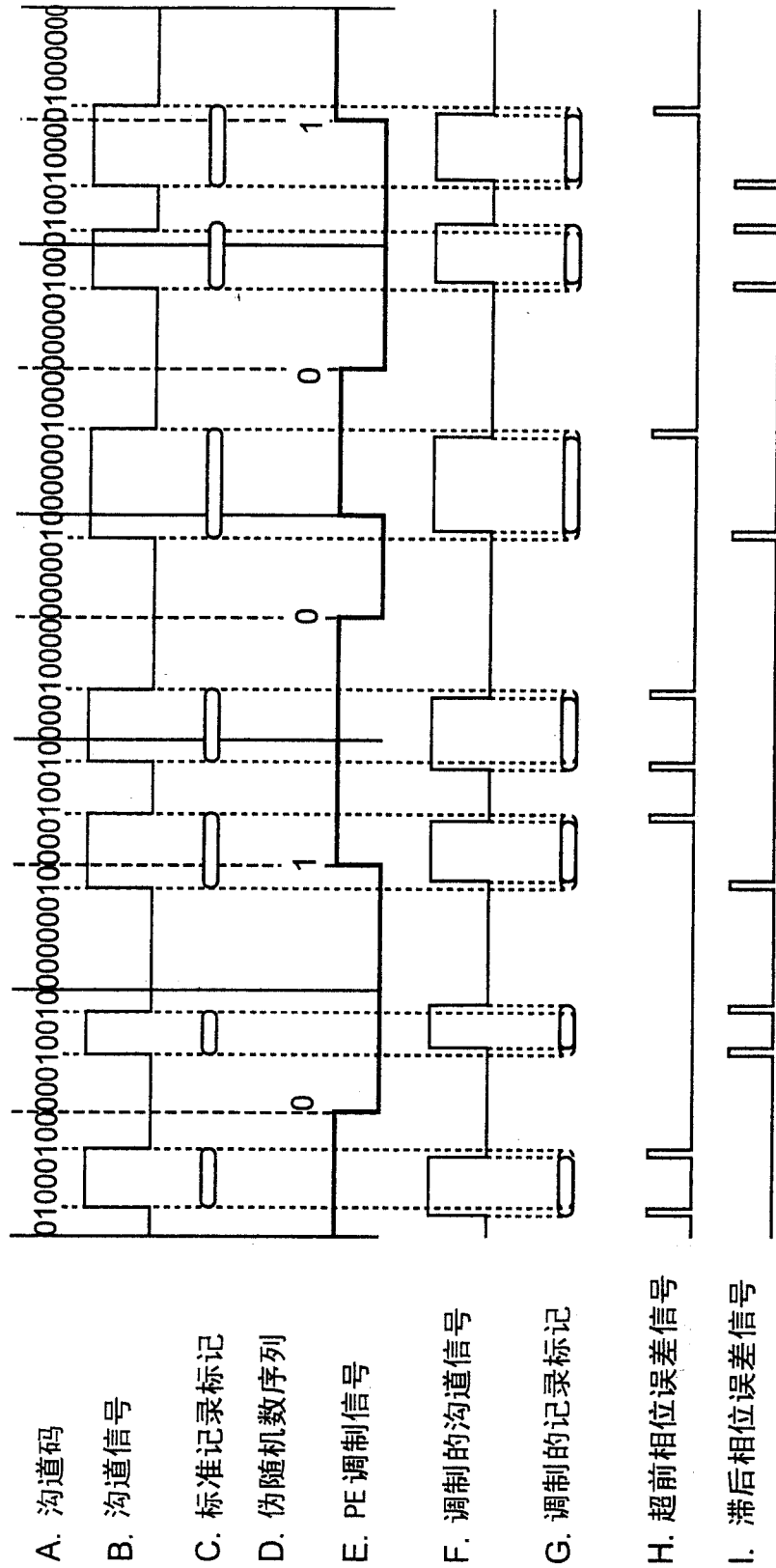


图 35



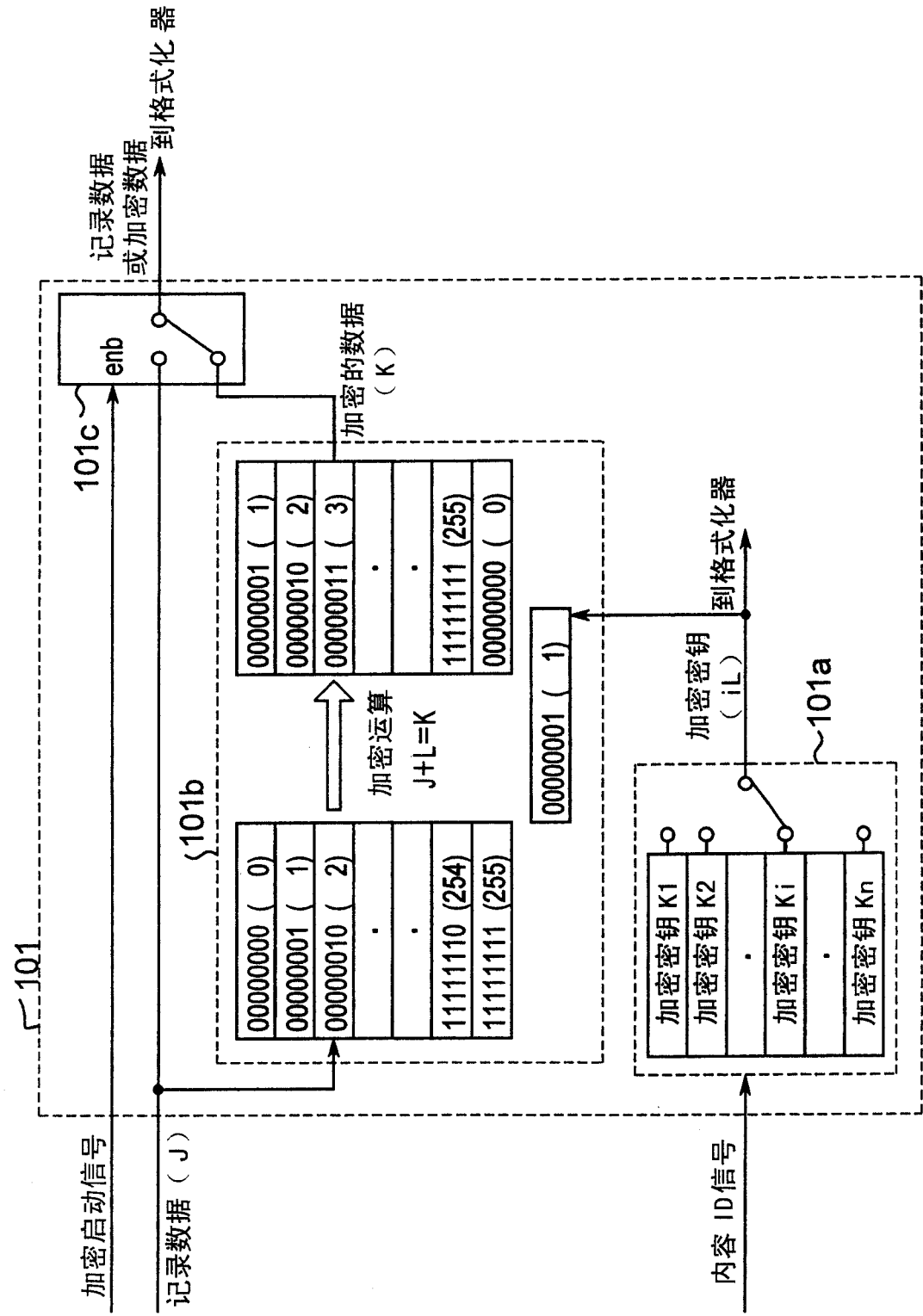


图 37

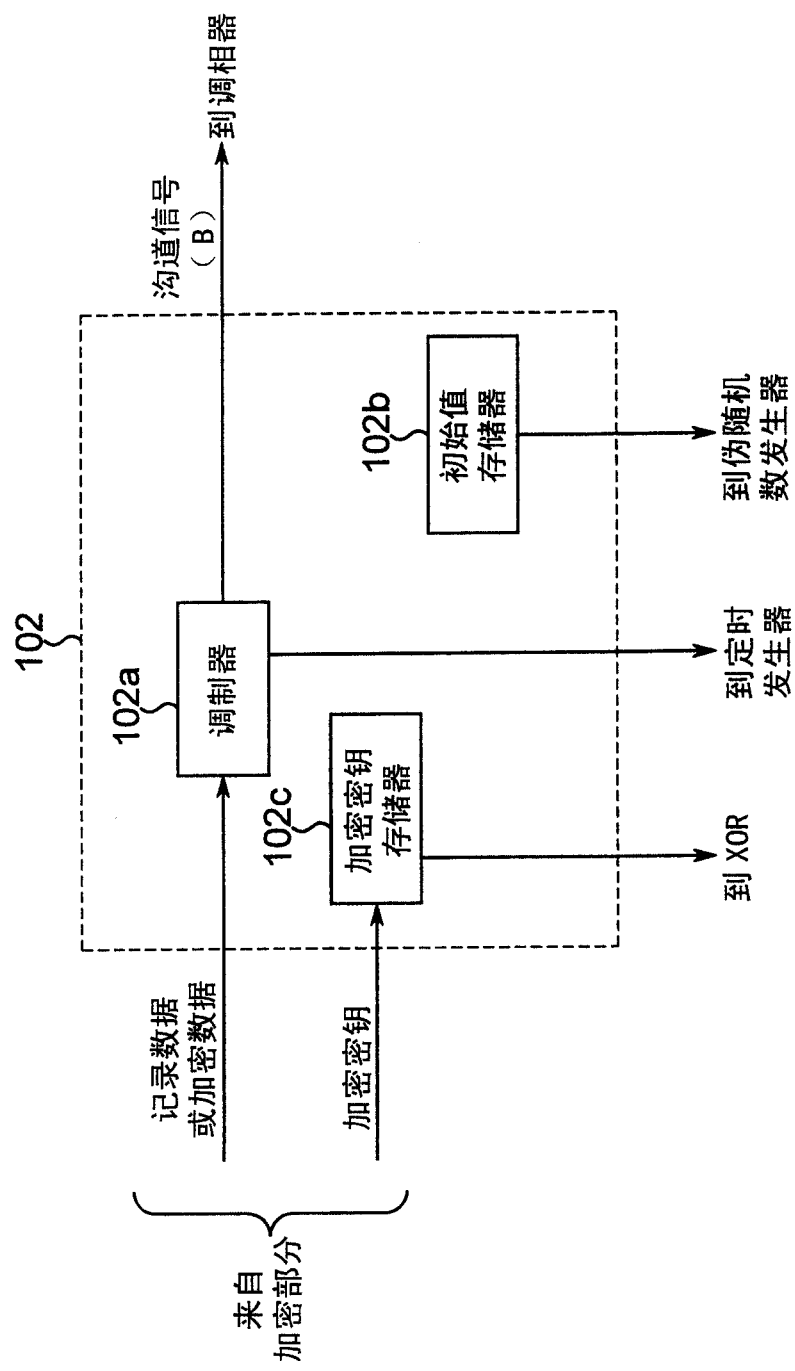


图 38

加密密钥 1011010001101 . . . 1 (56比特)

伪随机数 01001 . . . 1 (256比特)

沟道代码 00100 . . . 0 (16字节/1字节)

图 39

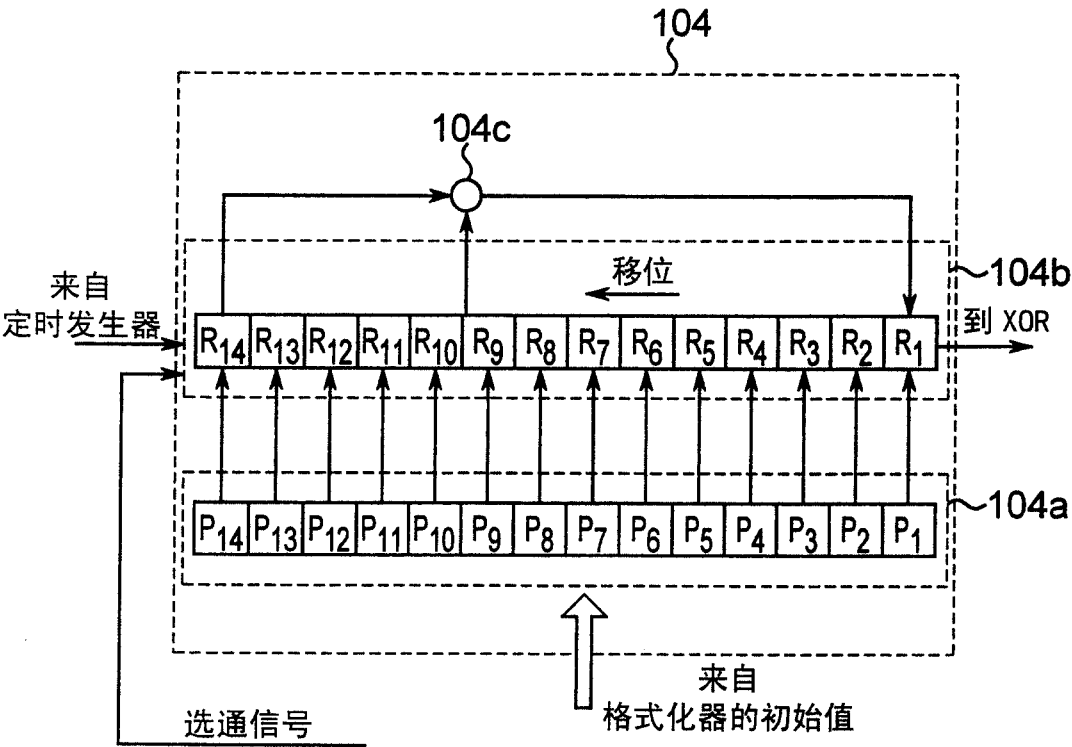


图 40

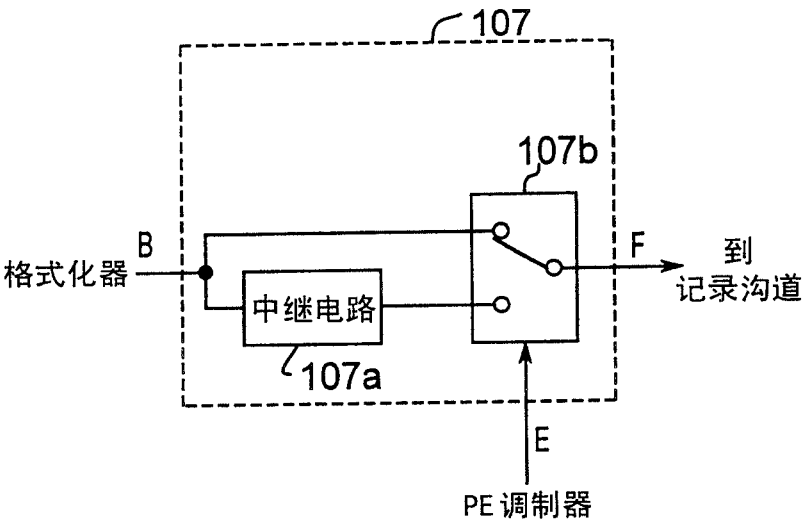


图 41

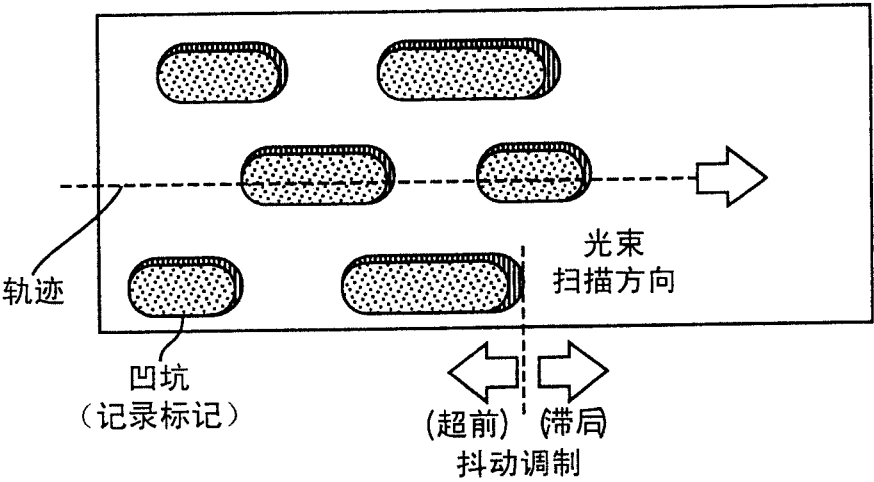


图 42

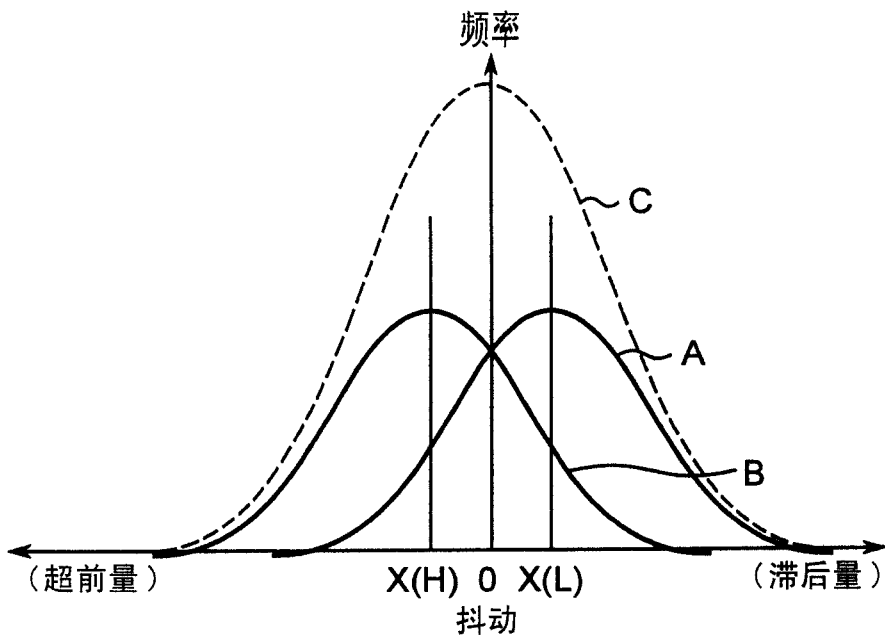


图 43

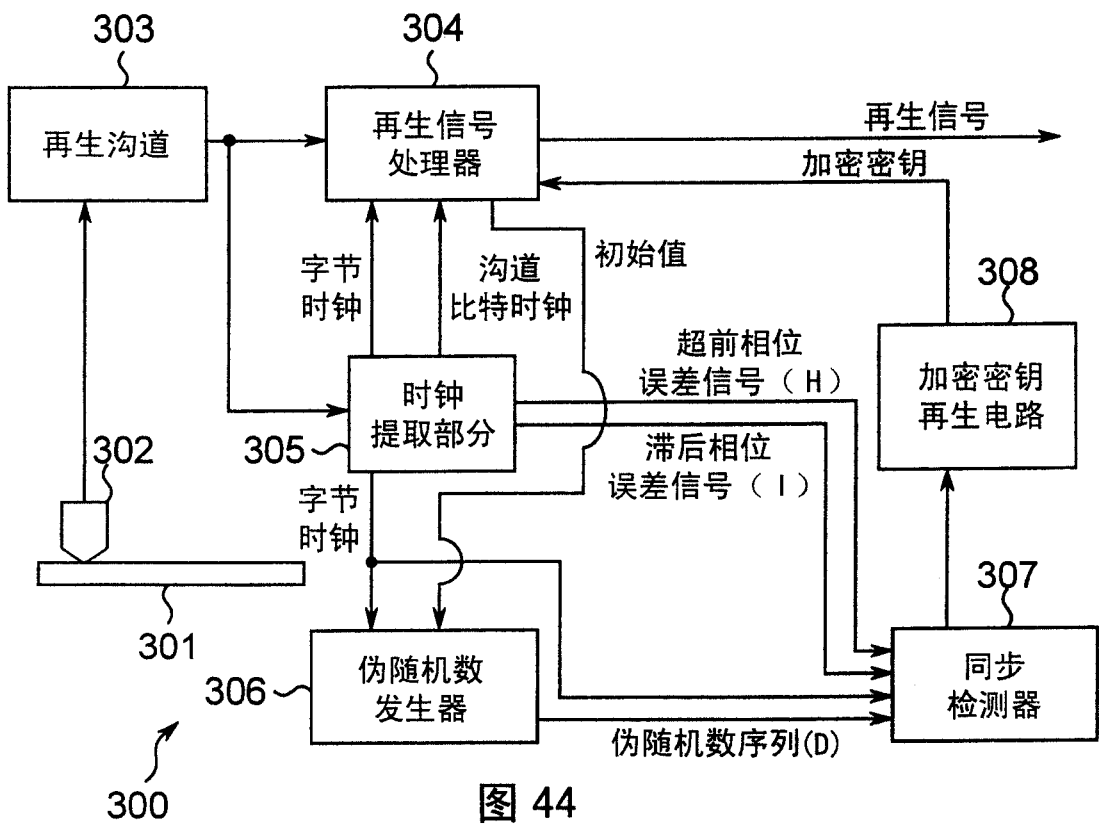


图 44

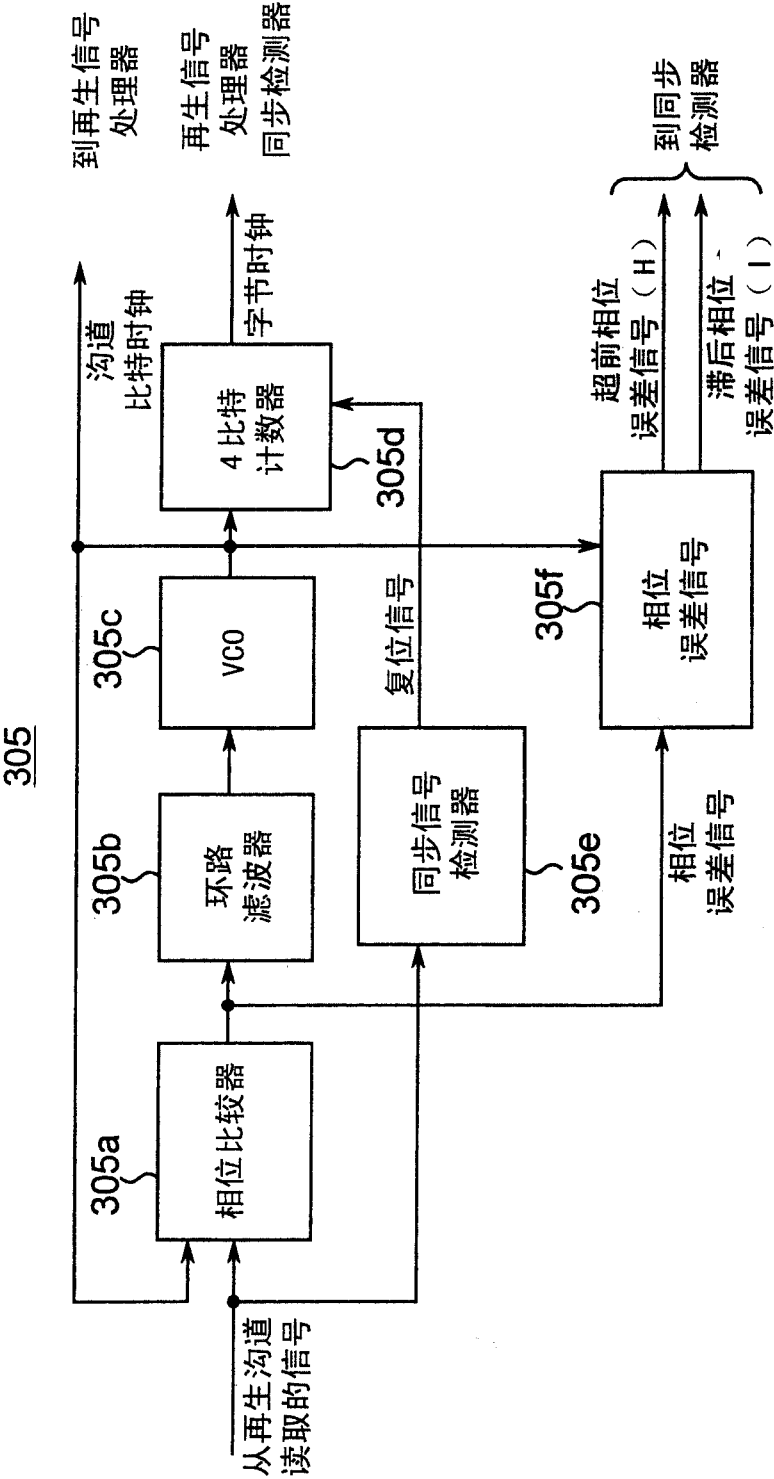


图 45

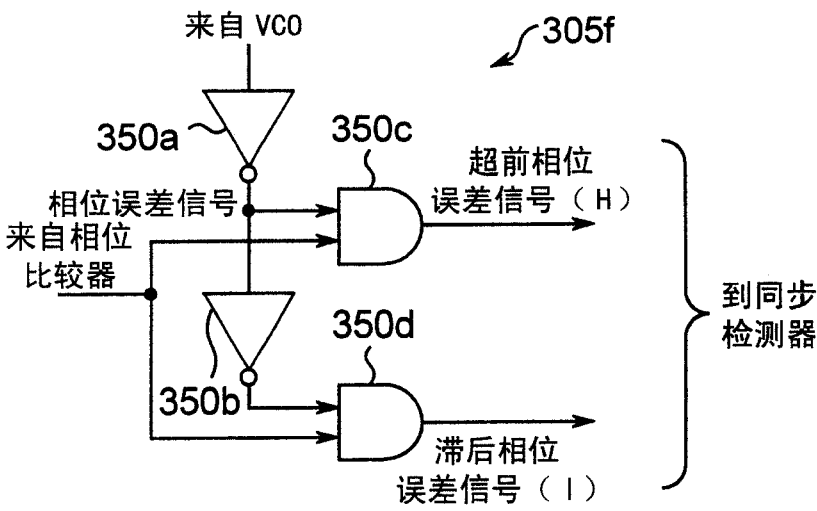


图 46A

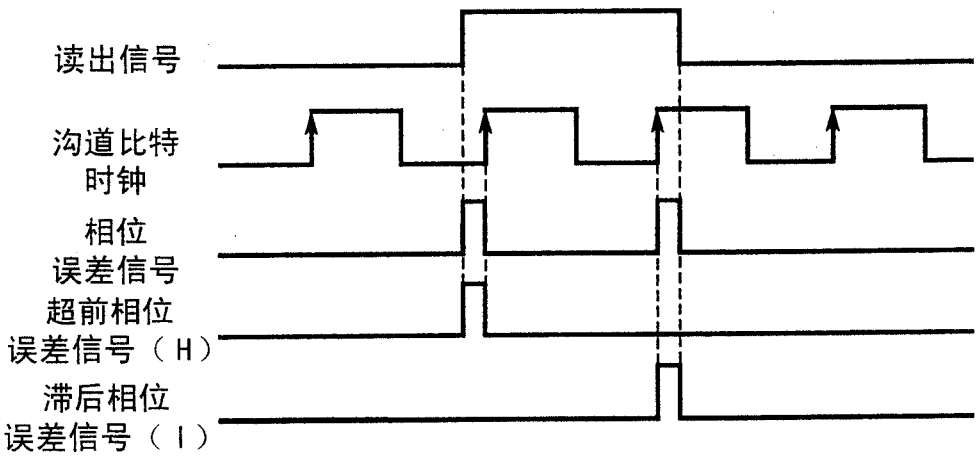


图 46B

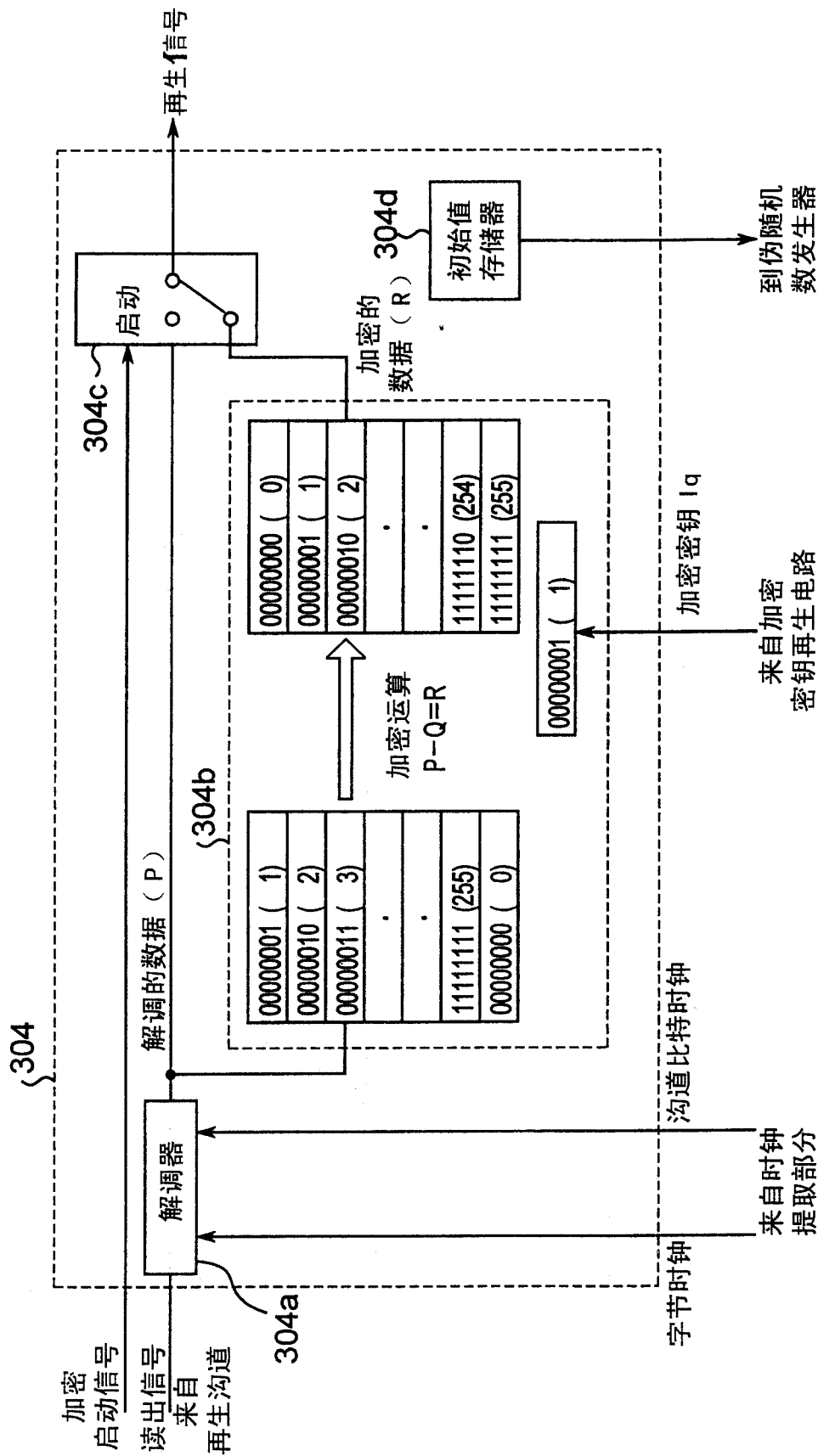


图 47

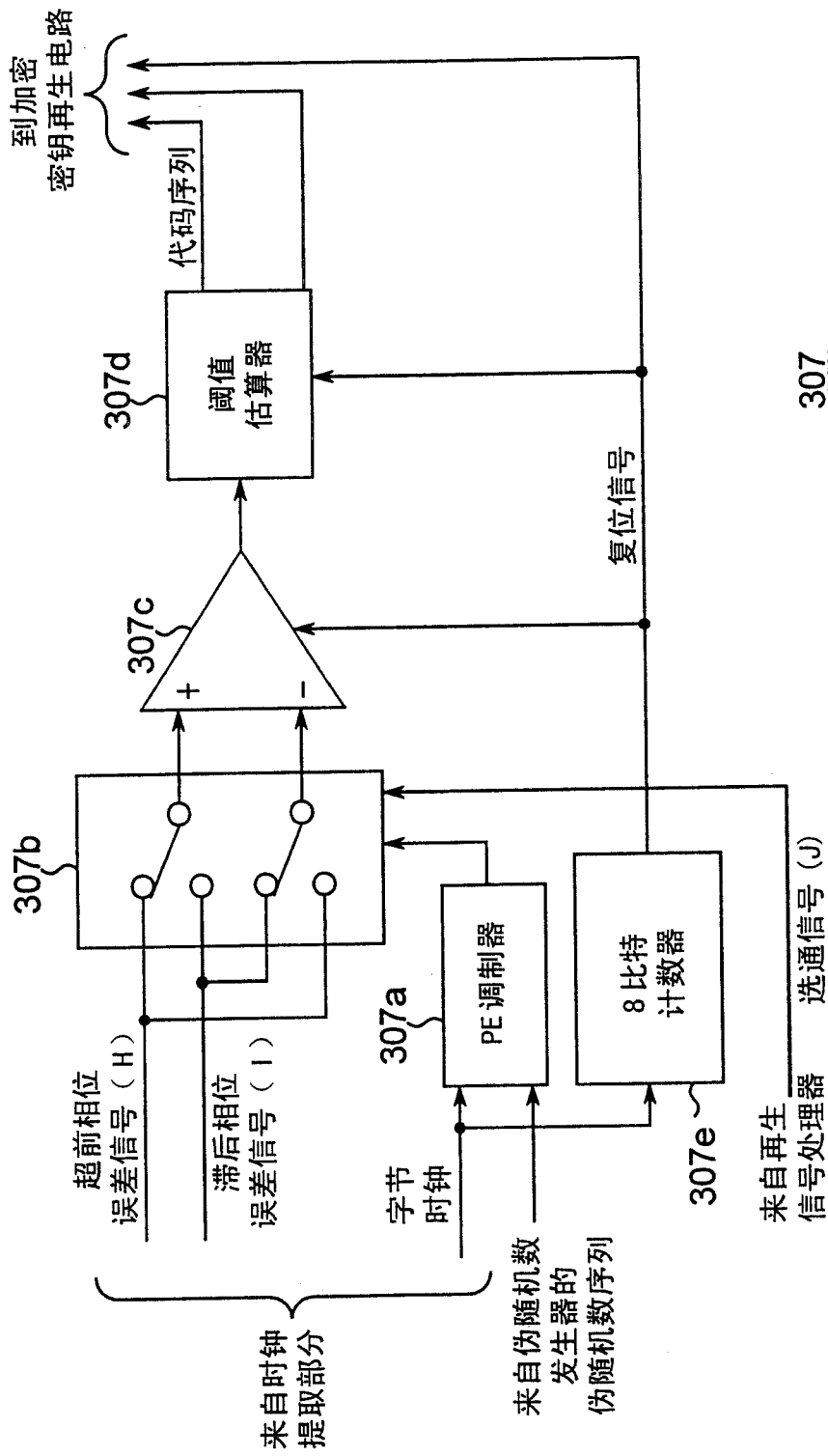


图 48

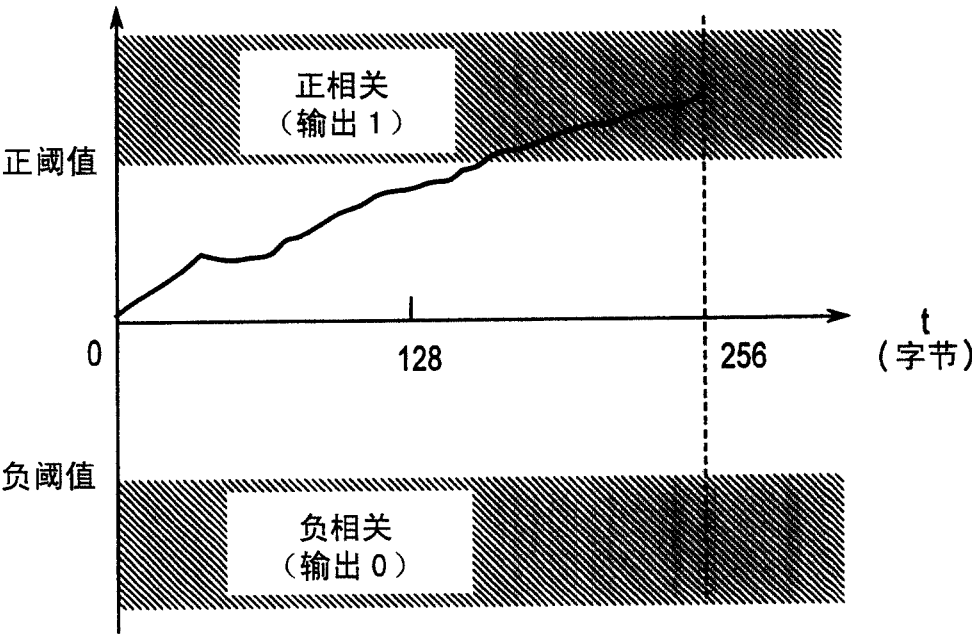


图 49

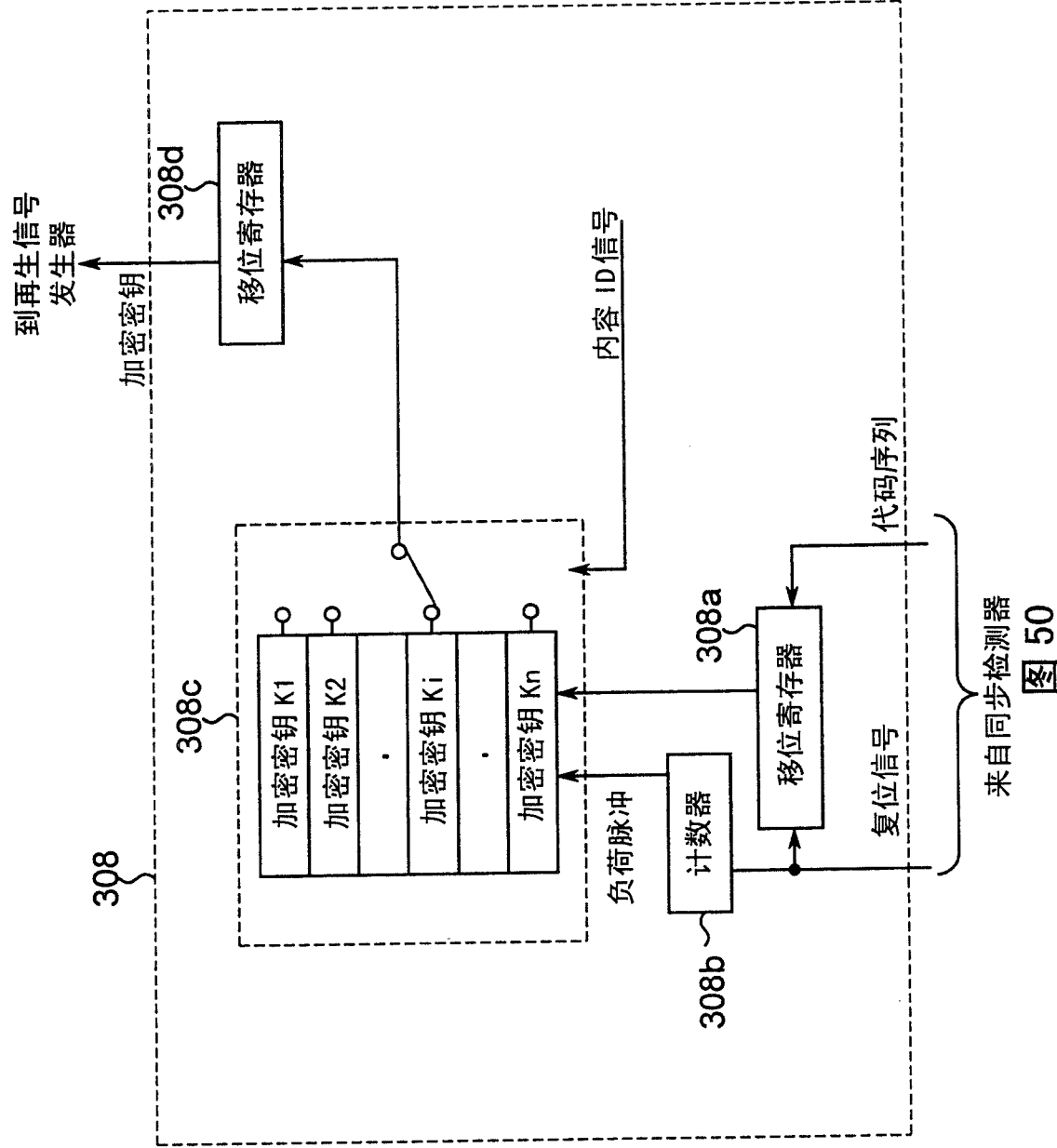


图 50

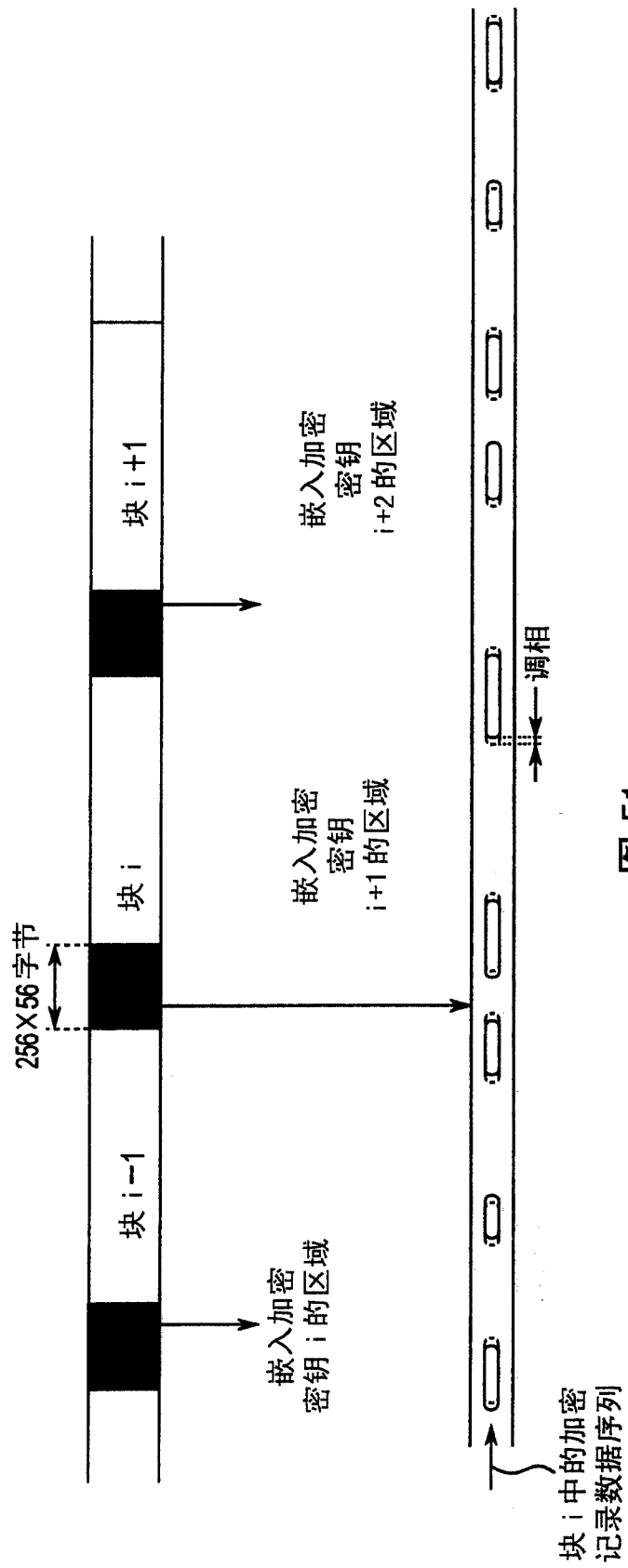


图 51

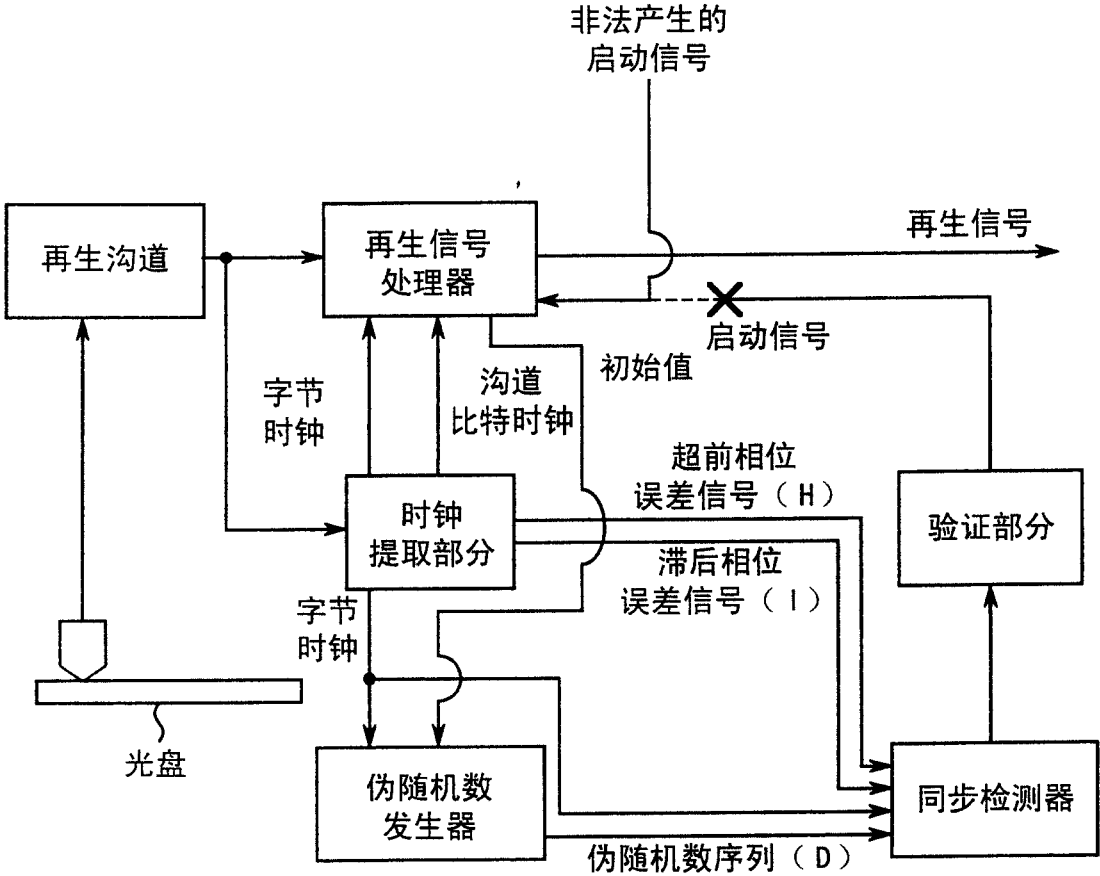


图 52

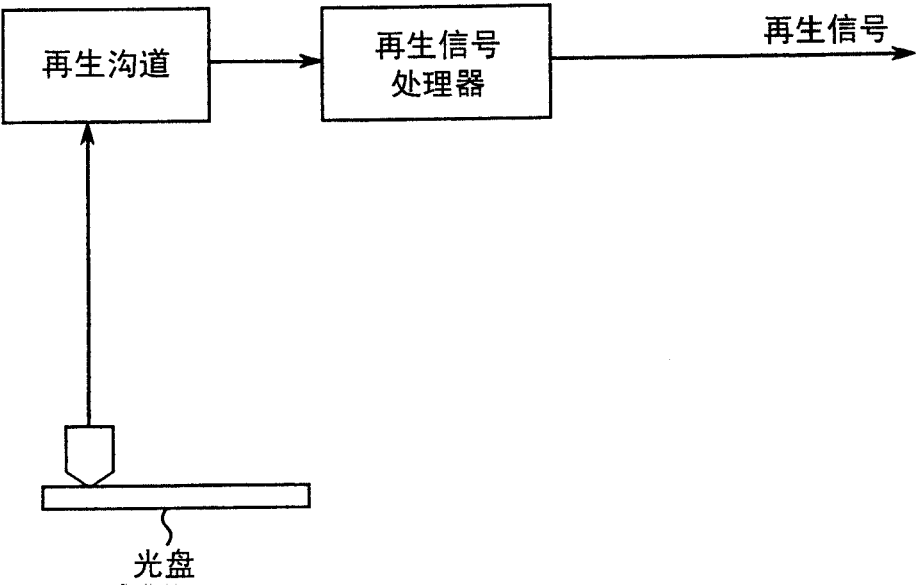


图 53

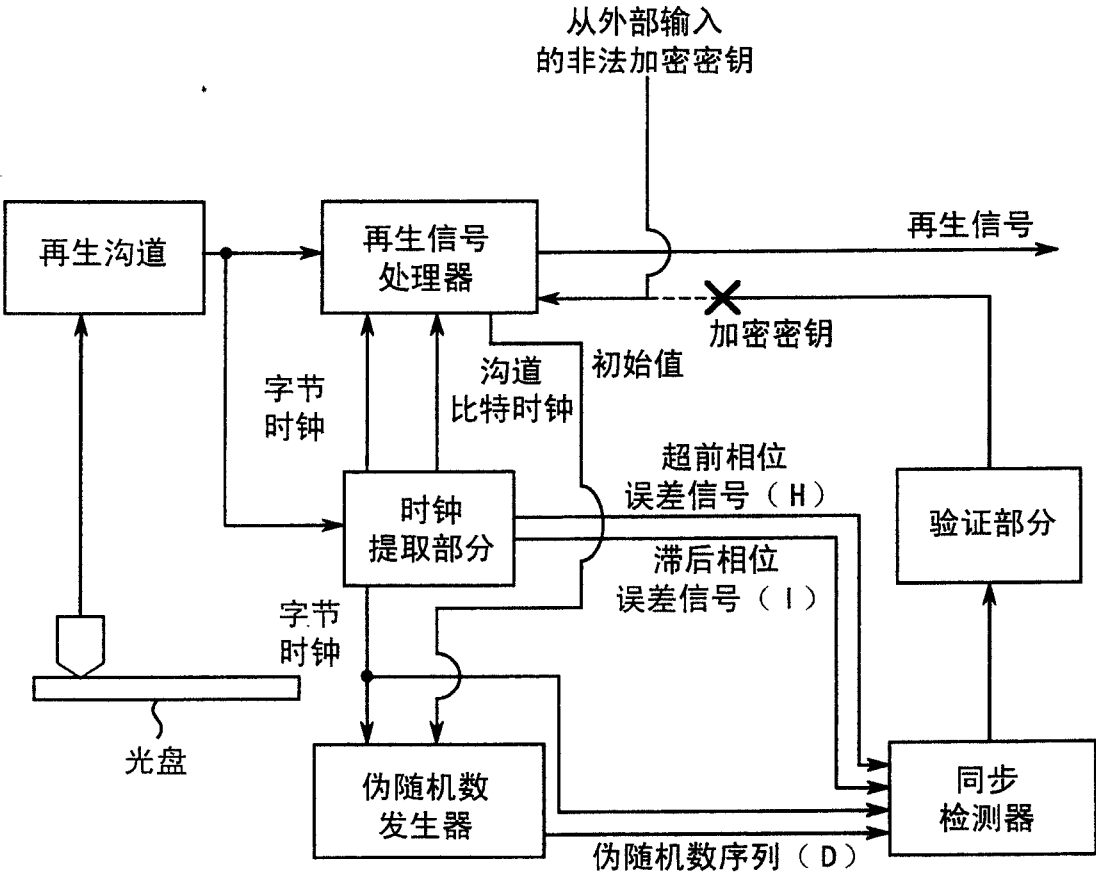


图 54

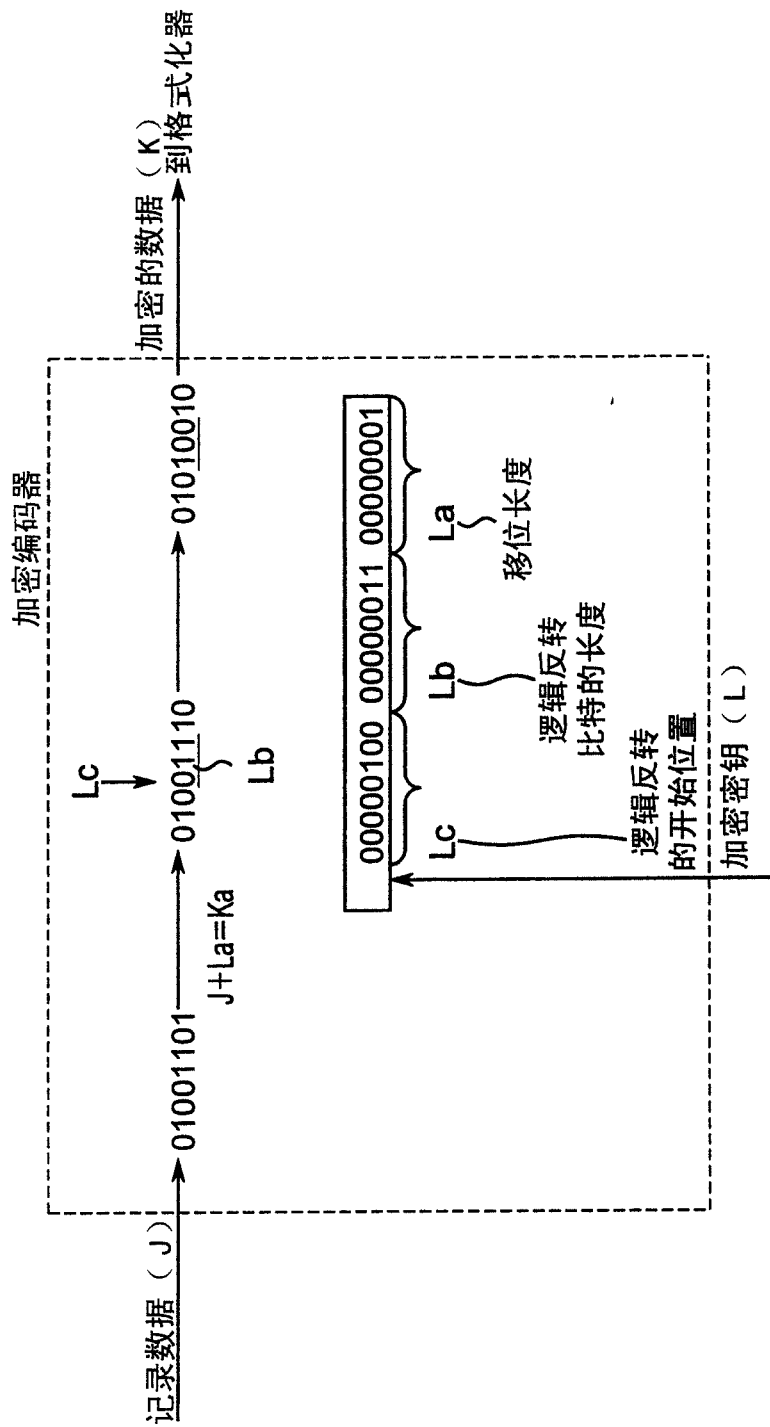


图 55

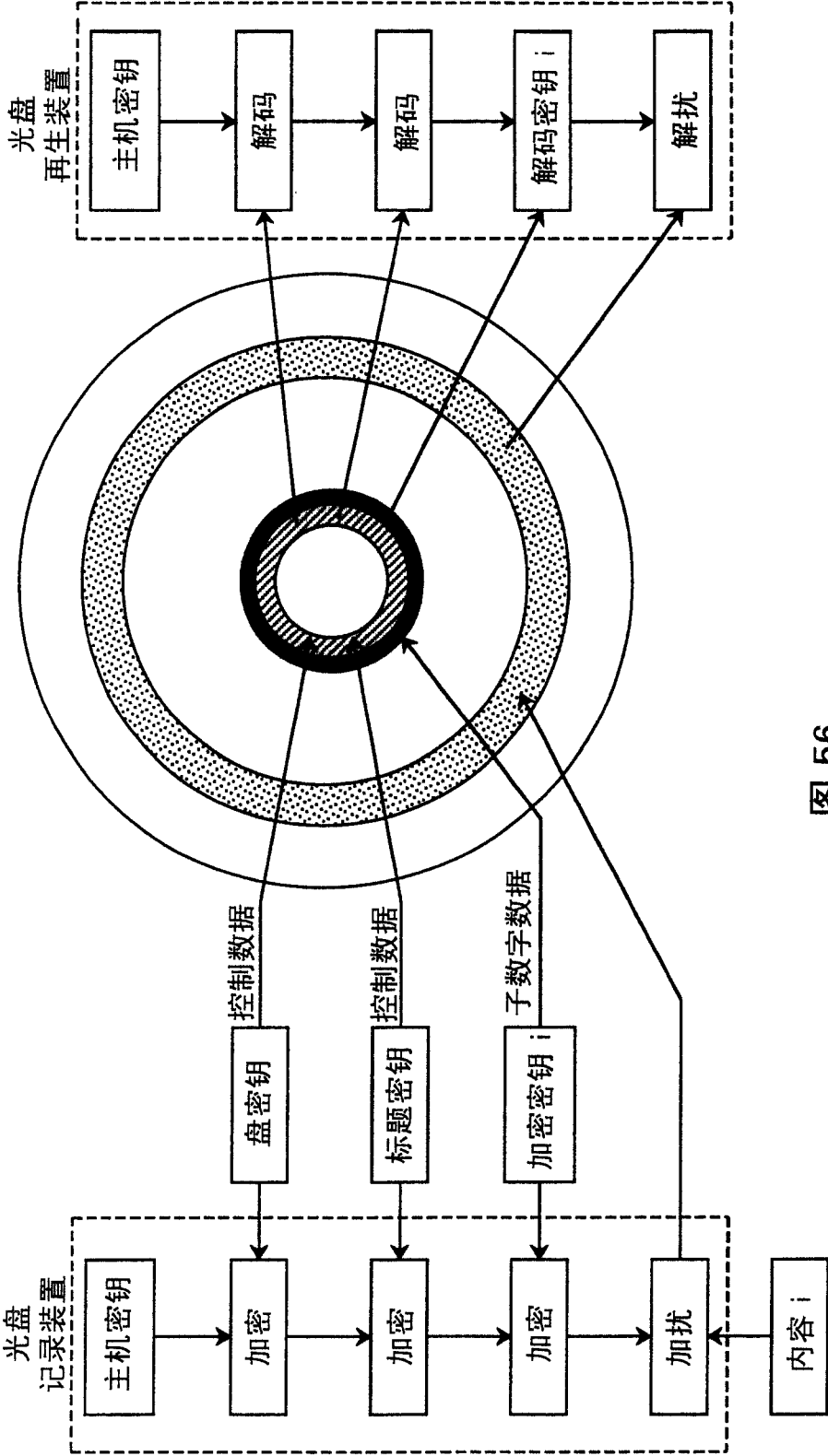


图 56

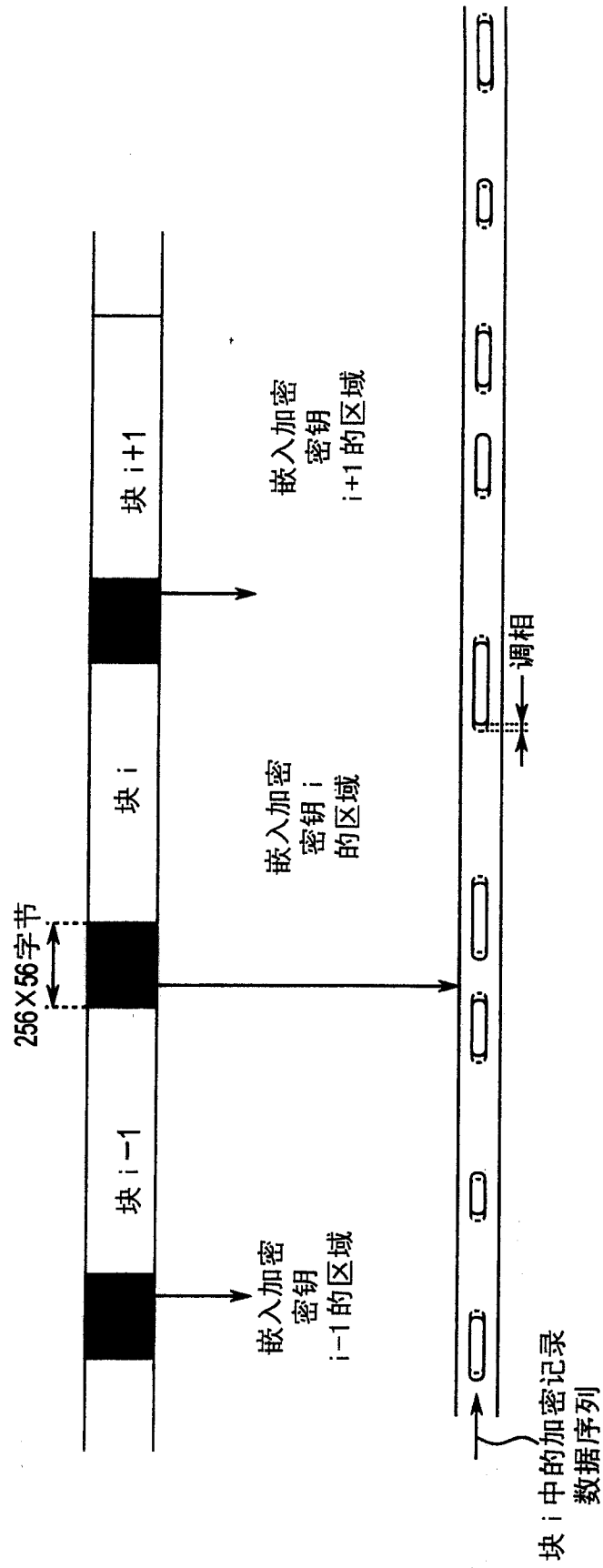


图 57

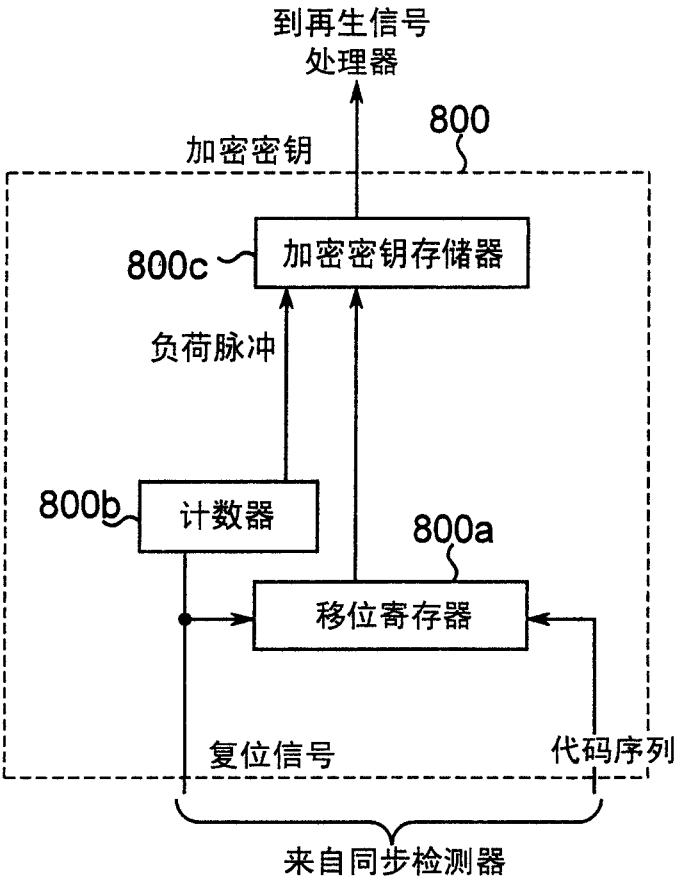


图 58