[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G11B 20/10
G11B 19/02 G06F 12/14

[12] 发明专利说明书

[21] ZL 专利号 00124873.1

[45] 授权公告日 2003 年 12 月 10 日

[11] 授权公告号 CN 1130716C

[22] 申请日 2000.9.20 [21] 申请号 00124873.1

[30] 优先权

[32] 1999. 9.30 [33] JP [31] 280075/1999

[71] 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 弓场隆司 石原秀志 福岛能久
馆林诚 横田薰

审查员 邓 巍

[74] 专利代理机构 中科专利商标代理有限责任公司

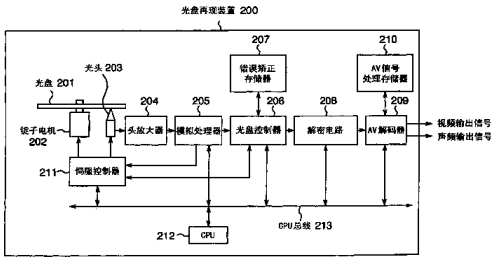
代理人 刘晓峰

权利要求书 3 页 说明书 25 页 附图 7 页

[54] 发明名称 信息再现方法及信息再现装置

[57] 摘要

一种用于再现信息记录媒体中的信息的方法，其中的信息记录媒体用于至少记录密钥信息和内容信息，部分内容信息被加密，并记录在所述信息记录媒体中，该方法包含如下的步骤：通过使用预定的密钥信息将记录在所述信息记录媒体中的所述密钥信息解码为被解码的密钥信息；通过使用所述内容信息的未加密内容信息将所述被解码的密钥信息转换为被转换的解码密钥信息；及通过使用所述被转换的解码密钥信息对所述加密和记录的部分内容信息进行解密。 同时本发明还公开了一种用于对记录在信息记录媒体中的信息进行再现的装置。



ISSN1008-4274

1．一种用于再现信息记录媒体中的信息的方法，其中的信息记录媒体用于至少记录密钥信息和内容信息，部分内容信息被加密，并记录在所述信息记录媒体中，该方法包含如下的步骤：

通过使用预定的密钥信息将记录在所述信息记录媒体中的所述密钥信息解码为被解码的密钥信息；

通过使用所述内容信息的未加密内容信息将所述被解码的密钥信息转换为被转换的解码密钥信息；及

通过使用所述被转换的解码密钥信息对所述加密和记录的部分内容信息进行解密。

2．一种用于对记录在信息记录媒体中的信息进行再现的装置，其中的记录媒体用于至少记录密码密钥信息和内容信息，部分内容信息被加密和记录，所述装置包含：

密码密钥信息解码装置，用于通过由预定的密钥信息将记录在所述信息记录媒体中的所述密码密钥信息解码为解码的密钥信息；

密钥信息转换装置，用于通过由所述内容信息的未加密内容信息将从所述密码密钥信息解码装置输出的所述解码的密钥信息转换为转换的解码密钥信息；及

解密装置，用于通过由从所述密钥信息转换装置输出的所述转换的解码密钥信息对所述加密和记录的部分内容信息进行解密。

3．一种用于再现信息记录媒体中的信息的方法，其中的信息记录媒体至少具有数据记录区和导引区，至少第一密码密钥信息和内容信息被记录在所述数据记录区中，第二密码密钥信息被记录在所述导引区中，而被记录在所述数据记录区中的部分内容信息被加密和记录，该方法包含如下的步骤：

通过使用预定的密钥信息将记录在所述数据记录区中的所述第一密码密钥信息解码为第一密钥信息；

通过使用所述第一密钥信息将被存储在所述导引区中的所述第二密码密钥信息解码为第二密钥信息；

通过使用被存储在所述数据记录区中的未加密内容信息将所述第二密钥信息转换为转换的第二密钥信息；及

通过使用所述转换的第二密钥信息对所述加密和记录的部分内容信息进行解密。

4．一种用于再现被记录在信息记录媒体中的信息的装置，其中的信息记录媒体至少具有一个数据记录区和一个导引区，在所述数据记录区中至少记录第一密码密钥信息和内容信息，在所述导引区中记录第二密码密钥信息，对记录在所述数据记录区中的部分内容信息进行加密和记录，该装置包含：

第一密钥信息解码装置，用于通过使用预定的密钥信息将被存储在所述数据记录区中的所述第一密码密钥信息解码为第一密钥信息；

第二密钥信息解码装置，用于将被存储在导引区中的所述第二密码密钥信息通过使用从所述第一密钥信息解码装置输出的所述第一密钥信息解码为第二密钥信息；

密钥转换装置，用于将从所述第二密钥信息解码装置输出的所述第二密钥信息通过使用所述内容信息的未加密内容信息转换为转换的第二密钥信息；及

解密装置，用于通过使用从所述密钥转换装置输出的所述转换的第二密钥信息对所述加密和记录的部分内容信息进行解密。

5．根据权利要求 4 所述的装置，其特征在于用于将第二密钥信息转换为被转换的第二密钥信息的所述内容信息的未加密部分至少包含复制控制信息。

6．一种用于对被记录在信息记录媒体中的信息进行再现的方法，其信息记录媒体至少具有导引区和数据记录区，第一密码密钥信息被记录在所述导引区中，至少第二密码密钥信息和内容信息被记录在所述数据记录区中，被记录在所述数据记录区中的部分所述内容信息被在所述信息记录媒体中进行加密和记录，该方法包含如下的步骤：

通过使用预定的密钥信息将所述导引区中的所述第一密码密钥信息

解码为第一密钥信息；

将被存储在所述数据记录区中的所述第二密码密钥信息通过使用所述第一密钥信息解码为第二密钥信息；

通过使用被存储在所述数据记录区中的未加密内容信息将所述第二密钥信息转换为转换的第二密钥信息；及

通过使用所述转换的第二密钥信息对所述加密和记录的部分内容信息进行解密。

7．一种用于对被记录在信息记录媒体中的信息进行再现的装置，该信息记录媒体至少具有导引区和数据记录区，第一密码密钥信息被记录在所述导引区中，在所述数据记录区中至少记录第二密码密钥信息和内容信息，将被记录在所述数据记录区中的部分内容信息加密并记录在所述信息记录媒体中，该装置包含：

第一密钥信息解码装置，用于将被存储在所述导引区中的所述第一密码密钥信息通过使用预定的密钥信息解码为第一密钥信息；

第二密钥信息解码装置，用于将被存储在所述数据记录区中的所述第二密码密钥信息通过使用从所述第一密钥信息解码装置输出的所述第一密钥信息解码为第二密钥信息；

密钥信息转换装置，用于将从所述第二密钥信息解码装置输出的所述第二密钥信息通过使用被存储在所述数据记录区中的未加密的内容信息转换为转换的第二密钥信息；及

解密装置，用于通过使用从所述密钥信息转换装置输出的所述转换的第二密钥信息对所述加密和记录的部分内容信息进行解密。

8．根据权利要求 7 所述的装置，其特征在于所述内容信息的未加密部分至少包含复制控制信息。

信息再现方法及信息再现装置

技术领域

本发明涉及一种用于记录视频信息、声频信息等的信息记录媒体，用于对记录在信息记录媒体上的信息进行再现的方法，和对记录在信息记录媒体中的信息进行再现的装置。尤其是，本发明涉及一种信息记录媒体，在其中记录了拥有版权的内容信息，用于对被记录在信息记录媒体中的拥有版权的内容信息进行再现的方法和用于对被记录在信息记录媒体中的拥有版权的内容信息进行再现的装置。

背景技术

最近，用于记录模拟信号的记录媒体（诸如压缩磁带、模拟记录等）已经被用于记录数字信号的记录媒体所替代，并成为记录媒体的主流（诸如压缩盘 CD，小型盘 MD）。因此，数字记录媒体已经发展成为用于记录视频信号的记录媒体，诸如在 CD 上通过被称为 MPEG1 的压缩方法记录视频信号的视频 CD 和用于通过被称为 MPEG2 的在具有 4.7GB 的大容量的光盘上通过高质量压缩方法记录被压缩的视频信号的 DVD（数字视频盘）。这些数字记录媒体已经被商业化，成为用于记录视频信息和声频信息的记录媒体。

图 7 为表示第一现有技术的光盘再现装置 400 的内部结构的方框图。光盘再现装置 400 对从光盘 201 中读出的信息数据进行错误矫正和扩展处理 ，从而进行解码并输出所需的视频和声频信号。

参考图 7，光盘再现装置 400 配备有光盘 201。光盘再现装置 400 包含锭子电机 202、光头 203、头放大器 204、模拟处理器 205、光盘控制器 206、误差矫正存储器 207、声频和视频解码器 209（此后简称为 AV 解码器）、声频和视频信号处理存储器 210（此后简称为 AV 信号处理存储器）、伺服控制器 211、CPU 212 和 CPU 总线 213。

锭子电机 202 根据来自伺服控制器 211 的控制信号旋转光盘 201。光头 203 包含光学拾音器。光头 203 用通过驱动激光二极管产生的激光辐射光盘 201。光头 203 检测来自光盘 201 的反射光，然后，对反射光进行光电转换。然后，光头 203 通过头放大器 204 将进行了光电转换的再现信号输出到模拟处理器 205。模拟处理器 205 具有用于 AGC（自动增益控制）、平衡、数据限制和 PLL 的功能。模拟处理器 205 提供处理为输入再现信号的预定的模拟信号，然后将被处理的再现信号输出到光盘控制器 206。接着，光盘控制器 206 将输入的再现信号通过 A/D 转换转换为再现的数字信号，然后对再现数据进行解调。光盘控制器 206 通过作为缓冲存储器的错误矫正存储器 207 对被解调的再现数据进行错误矫正。然后，光盘控制器 206 向 AV 解码器 209 输出处理的再现数据。另外，AV 解码器 209 对视频数据和声频数据进行包含扩展的解码，通过使用 AV 信号处理存储器 210 根据输入的扩展数据将其压缩为上述的输入再现数据，其中的信号处理存储器 210 为在扩展视频数据和声频数据中使用的扩展缓冲存储器。然后，AV 解码器 209 输出被处理的视频和声频信号。

伺服控制器 211 根据来自模拟处理器 205、光盘控制器 206 和 CPU212 的信号控制锭子电机 202、光头 203、光盘控制器 206 等，以进行光头 203 的聚焦、跟踪等的伺服控制，用于从光盘 201 读出数据。通过 CPU 总线 213 将伺服控制器 211、模拟处理器 205、光盘控制器 206 和 AV 解码器 209 与 CPU212 相连。CPU212 通过 CPU 总线 213 控制模拟处理器 205、光盘控制器 206、AV 解码器 209 和伺服控制器 211，以控制整个光盘再现装置 400 的操作。

下面将参考图 7 对第一现有技术的光盘再现装置进行描述。CPU212 按照预定的顺序控制光头 203，从而通过使用光头 203 从光盘 201 读出数据，然后将再现的数据通过头放大器 204 和模拟处理器 205 输出到光盘控制器 206，接着将进行了错误矫正的再现数据存储到错误矫正存储器 207 中。此时，CPU212 读出存储在错误矫正存储器 207 中的再现数据的控制信息和数据识别信息，因此控制伺服控制器 211 和 AV 解码器 209，从而再现视频数据和声频数据。

另一方面，随着个人计算机性能的提高和硬盘容量的增大，个人计

算机的应用程序的容量也增大。通过利用其大容量的特性，不仅使用 DVD 作为用于记录视频数据和声频数据的记录媒体，而且作为对个人计算机分布应用软件的媒体。因此，作为个人计算机的外围设备的 DVD 驱动装置快速扩展。另外，用于个人计算机的具有 MPEG 扩展功能的 AV 解码卡、用于通过个人计算机的主处理器借助软件处理进行 MPEG 扩展功能的程序已经商业化。

然而，在系统中通过总的计算机总线将 DVD 驱动部分和 AV 解码卡相连，在该系统中，个人计算机通过使用 DVD 驱动装置和 AV 解码卡从 DVD 再现视频数据和声频数据。因此，会产生诸如通过通讯线路传输的数据的被盗版和分布篡改数据的行为。结果，就产生一个很难保护版权的问题。

为了解决上述的问题，在日本专利公开 No.7-249264（此后称为第二现有技术）中已经提出了对具有版权的数据的加密和记录。在所提出的方法中，在第二现有技术的图 3 中所示的 CD-ROM 中，密钥被记录在加密数据扇区的不同扇区的主数据区中。在第二现有技术中，在记录时加密的数据和数据的密钥被记录在 CD-ROM 中。在再现时，个人计算机发出一个命令，对再现装置读出一个密钥，然后读出加密数据，通过事先读出的密钥对加密数据进行解密，这将导致数据被再现。

然而，在第二现有技术中，密钥被记录在扇区的主数据区中，通过普通的读命令可读出密钥。因此，通过普通的个人计算机可容易的读出密钥。由此，用户可读出密钥和加密数据。这样，第二现有技术就存在很大的被解密的危险。第二现有技术存在的另外的一个问题在于，通过复制硬盘存储器中的密钥和解密数据可进行个人私下的复制。

因此，扇区的所有的主数据区被解密和记录。由此，当 DVD 播放机的 CPU 试图从光盘读出内容控制信息以便控制 DVD 播放机时，该信息被包含在扇区的主数据中并包含内容识别信息、内容复制控制信息等，CPU 仅通过对加密的数据进行一次解密就可获得正确的信息。

上述的问题产生下面的不足。当以明文形式记录包含内容控制信息的区域时，在复制控制信息被篡改的情况下，会发生未被授权的再现的情况。

发明内容

为了解决上述的不足，本发明的一个目的是提供一种信息记录媒体，其具有可防止轻易的读出在加密中使用的密钥信息的数据结构。

为了解决上述的问题，本发明的另外的一个目的在于提供一种信息记录媒体，其中用于控制诸如 DVD 播放机等的信息再现装置的 CPU 可从信息记录媒体容易的读出复制控制信息，因此容易的控制信息再现装置，并且当被记录在信息记录媒体中的复制控制信息被篡改时，可防止对数据进行再现。

为了解决上述的问题，本发明的另外的一个目的是提供一种用于对存储在信息记录媒体中的信息进行再现的方法和装置，其中用于控制诸如 DVD 播放机等信息再现装置的 CPU 可容易的从信息记录媒体读出复制控制信息等，并由此容易的控制信息再现装置，当被记录在信息记录媒体中的复制控制信息等被篡改时可防止对数据进行再现。

为了实现上述的目的，根据本发明的一个方面，其提供一种信息记录媒体，用于至少记录具有版权的内容信息和密钥信息。

其中部分内容信息被加密并记录在信息记录媒体中，及

其中通过使用密钥信息通过加密而获得内容信息的加密和记录部分，其是通过使用内容信息的未-加密部分对密钥信息的转换而获得的。

在上述的信息记录媒体中，用于产生密钥信息的内容信息的未加密部分最好包含复制控制信息。

在上述的信息记录媒体中，信息记录媒体最好包含一个被划分为多个扇区的记录区；

其中分别在扇区中记录内容信息被划分的多个数据；及

其中用于产生密钥信息的内容信息的未加密部分包含复制控制信息和逐扇区进行改变的部分内容信息。

根据本发面的另外的一个方面，提供一种用于再现信息记录媒体中的信息的方法，其中的信息记录媒体用于至少记录密钥信息和内容信息，部分内容信息被加密，并记录在信息记录媒体中，该方法包含如下的步骤：

通过使用预定的密钥信息将记录在信息记录媒体中的密钥信息解码为被解码的密钥信息；

通过使用内容信息的未加密内容信息将被解码的密钥信息转换为被转换的解码密钥信息；及

通过使用被转换的解码密钥信息对加密和记录的内容信息进行解密；

根据本发明的另外的一个方面，其提供一种用于对记录在信息记录媒体中的信息进行再现的装置，其中的记录媒体用于至少记录密码密钥信息和内容信息，和被加密和记录的部分内容信息，装置包含：

密码密钥信息解码装置，用于通过使用预定的密钥信息将记录在信息记录媒体中的密码密钥信息解码为解码的密钥信息；

密钥信息转换装置，用于通过使用内容信息的未加密内容信息将从密码密钥信息解码装置输出的被解码的密钥信息转换为被转换的解码密钥信息；及

解密装置，用于通过使用从信息转换装置输出的被转换的密钥信息对被加密和记录的内容信息进行解密；

根据本发明的另外的一个方面，其提供一种信息记录媒体，其至少具有一个用于记录拥有版权的内容信息的数据记录区；

其中在数据记录区中至少记录密码密钥信息和内容信息；

其中对被记录在数据记录区中的部分内容信息和进行加密和记录；及

通过使用加密密钥信息通过加密获得内容信息的被加密和记录部分，其是通过使用内容信息的未加密部分对密码密钥信息进行转换而获得的。

根据本发明的另外的一个方面，其提供一种信息记录媒体，其至少具有数据记录区和导引区，将拥有版权的内容信息记录在信息记录媒体中，

其中在数据记录区中至少记录第一密码密钥信息和内容信息；

其中第二密码密钥信息被记录在导引区中；

其中对被记录在数据记录区中的部分内容信息进行加密和记录；及

其中通过使用加密密钥信息通过加密获得被加密和记录的内容信息，其是通过使用内容信息的未加密部分对第二密码密钥信息进行转换而获得的。

在上述的信息记录媒体中，用于产生密钥信息的内容信息的未加密部分最好至少包含复制控制信息。

在上述的信息记录媒体中，信息记录媒体最好包含一个被划分为多个扇区的记录区；

其中分别在扇区中记录内容信息被划分的多个数据；及

其中用于产生密钥信息的内容信息的未加密部分包含复制控制信息和逐扇区进行改变的部分内容信息。

根据本发面的另外的一个方面，提供一种用于再现信息记录媒体中的信息的方法，其中的信息记录媒体具有至少数据记录区和导引区，至少第一密码密钥信息和内容信息被记录在数据记录区中，第二密码密钥信息被记录在导引区中，而被记录在数据记录区中的部分内容信息被加密和记录，该方法包含如下的步骤：

通过使用预定的密钥信息将记录在数据记录区中的密钥信息解码为被解码的密钥信息；

通过使用内容信息的未加密内容信息将被解码的密钥信息转换为被转换的解码密钥信息；及

通过使用被转换的解码密钥信息对加密和记录的部分内容信息进行解密；

根据本发明的另外的一个方面，其提供一种用于对记录在信息记录媒体中的信息进行再现的装置，其中的记录媒体用于至少记录密码密钥信息和内容信息，部分内容信息被加密和记录，该装置包含：

密码密钥信息解码装置，用于通过使用预定的密钥信息将记录在信息记录媒体中的密码密钥信息解码为解码的密钥信息；

密钥信息转换装置，用于通过使用内容信息的未加密内容信息将从密码密钥信息解码装置输出的解码的密钥信息转换为转换的解码密钥信息；及

解密装置，用于通过使用从密钥信息转换装置输出的转换的解码密

钥信息对加密和记录的部分内容信息进行解密；

根据本发明的另外的一个方面，其提供一种信息记录媒体，其至少具有一个用于记录拥有版权的内容信息的数据记录区；

其中在数据记录区中至少记录密码密钥信息和内容信息；

其中对被记录在数据记录区中的部分内容信息和进行加密和记录；及

通过使用加密密钥信息的加密所获得的内容信息的被加密和记录的部分，其是通过使用内容信息的未加密部分对密码密钥信息进行转换而获得的。

根据本发明的另外的一个方面，其提供一种信息记录媒体，其至少具有数据记录区和导引区，将拥有版权的内容信息记录在信息记录媒体中，

其中在数据记录区中至少记录第一密码密钥信息和内容信息；

其中第二密码密钥信息被记录在导引区中；

其中对被记录在数据记录区中的部分内容信息进行加密和记录；及

通过使用加密密钥信息的加密获得被加密和记录的内容信息，其是通过使用内容信息的未加密部分对第二密码密钥信息进行转换而获得的。

在上述的信息记录媒体中，用于产生加密密钥信息的内容信息的未加密部分最好至少包含复制控制信息。

在上述的信息记录媒体中，信息记录媒体最好具有被划分为多个扇区的记录区，

其中分别在扇区中记录内容信息被划分的多个数据，及

其中用于产生加密密钥信息的内容信息的未加密部分包含复制控制信息，和内容逐一扇区改变的部分内容信息。

根据本发明的另外的一个方面，其提供一种对记录在信息记录媒体中的信息进行再现的方法，其中的信息记录媒体至少具有一个记录区和一个导引区，在数据记录区中至少记录第一加密密钥信息和内容信息，在导引区中记录第二密码密钥信息，对被记录在数据记录区中的部分内容信息进行加密和记录，该方法包含如下的步骤：

将被存储在数据记录区中的第一密码密钥信息通过使用预定的密钥信息解码为第一密钥信息；

通过使用第一密钥信息将被存储在导引区中的第二密码密钥信息解码为第二密钥信息；

将第二密钥信息通过使用被存储在数据记录区中的未加密内容信息转换为转换的第二密钥信息；及

通过使用转换的第二密钥信息对被加密和记录的部分内容信息进行解密。

根据本发明的另外的一个方面，其提供一种用于再现被记录在信息记录媒体中的信息的装置，其中的信息记录媒体至少具有一个数据记录区和一个导引区，在数据记录区中至少记录第一密码密钥信息和内容信息，在导引区中记录第二密码密钥信息，对记录在数据记录区中的部分内容信息进行加密和记录，该装置包含：

第一密钥信息解码装置，用于通过使用预定的密钥信息将被存储在数据记录区中的第一密码密钥信息解码为第一密钥信息；

第二密钥信息解码装置，用于将被存储在导引区中的第二密码密钥信息通过使用从第一密钥信息解码装置输出的第一密钥信息解码为第二密钥信息；

密钥转换装置，用于将从第二密钥信息解码装置输出的第二密钥信息通过使用内容信息的未加密内容信息转换为转换的第二密钥信息；及

解密装置，用于通过使用从密钥转换装置输出的转换的第二密钥信息对加密和记录的部分内容信息进行解密。

在上述的装置中，用于将第二密钥信息转换为被转换的第二密钥信息的内容信息的未加密部分至少包含复制控制信息。

根据本发明的另外的一个方面，其提供一种信息记录媒体，至少具有导引区和数据记录区，在信息记录媒体上记录拥有版权的内容信息，

其中第一密码密钥信息被记录在导引区中，

在数据记录区中至少记录第二密码密钥信息和内容信息，

其中对被记录在数据记录区中的内容信息进行加密和记录；及

通过使用加密密钥信息进行加密而获得被加密和记录的内容信息，

其是通过使用内容信息的未加密部分对第二密码密钥信息进行转换而获得的。

在上述的信息记录媒体中，数据记录区最好被划分为多个扇区，每个扇区由扇区标题区和主数据区构成，其中的扇区标题区用于记录识别扇区的信息，而主数据区用于记录内容信息，

其中第二密码密钥信息被记录在扇区标题区中，

其中的部分内容信息在主数据区中被进行加密和记录，及

其中通过使用加密密钥信息的加密所获得的内容信息的被加密和记录部分，其是通过使用每个扇区的未加密部分的内容信息对第二密码密钥信息进行转换而获得的。

在上述的信息记录媒体中，用于产生加密密钥信息的内容信息的未-加密部分最好至少包含复制控制信息。

在上述的信息记录媒体中，用于产生加密密钥信息的内容信息的未加密部分最好至少包含复制控制信息和逐一扇区改变的部分内容信息。

在上述的信息记录媒体中，被记录在扇区标题中的第二密码密钥信息最好是通过使用被记录在导引区中的第一密码密钥信息对预定的第二密钥信息进行解密二获得的。

根据本发明的另外的一个方面，其提供一种用于对被记录在信息记录媒体中的信息进行再现的方法，其信息记录媒体至少具有导引区和数据记录区，第一密码密钥信息被记录在导引区中，至少第二密码密钥信息和内容信息被记录在数据记录区中，被记录在数据记录区中的部分内容信息被在信息记录媒体中进行加密和记录，该方法包含如下的步骤：

通过使用预定的密钥信息将导引区中的第一密码密钥信息解码为第一密钥信息；

将被存储在数据记录区中的第二密码密钥信息通过使用第一密钥信息解码为第二密钥信息；

通过使用被存储在数据记录区中的未加密内容信息将第二密钥信息转换为被转换的第二密钥信息；及

通过使用转换的第二密钥信息对加密和记录的部分内容信息进行解密。

根据本发明的另外的一个方面，其提供一种装置，用于对被记录在信息记录媒体中的信息进行再现，该信息记录媒体至少具有导引区和数据记录区，第一密码密钥信息被记录在导引区中，在数据记录区中至少记录第二密码密钥信息和内容信息，将被记录在数据记录区中的部分内容信息加密并记录在信息记录媒体中，该装置包含：

第一密钥信息解码装置，用于将被存储在导引区中的第一密码密钥信息通过使用预定的密钥信息解码为第一密钥信息；

第二密钥信息解码装置，用于将被存储在数据记录区中的第二密码密钥信息通过使用从第一密钥信息解码装置输出的第一密钥信息解码为第二密钥信息；

密钥信息转换装置，用于将从第二密钥信息解码装置输出的第二密钥信息通过使用被存储在数据记录区中的未加密的内容信息转换为转换的第二密钥信息；及

解密装置，用于通过使用从密钥信息转换装置输出的所述转换的第二密钥信息对加密和记录的部分内容信息进行解密。

在上述的装置中，内容信息的未加密部分最好至少包含复制控制信息。

附图说明

通过下面结合相应附图对本发明的最佳实施例的详细描述会对本发明的上述的和其他的目的和优点有更清楚的了解，其中相同的标号用于表示类似的部分，其中：

图 1 为根据本发明的第一实施例的光盘 201 的数据结构的分级示意图；

图 2 为图 1 中所示的光盘 201 的记录区的平面示意图；

图 3 为用于对被记录在图 1 和图 2 中所示的光盘 201 中的信息进行再现的光盘再现装置 200 的内部结构方框图；

图 4 为图 3 中所示的解密电路 208 的内部结构的方框图；

图 5 为根据本发明的第二实施例的光盘 201 的数据结构的分级示意图；

图 6 为在第二最佳实施例中使用的解密电路 208 的内部结构的方框图；及

图 7 为第一现有技术的光盘再现装置 400 的内部结构的方框图。

具体实施方式

下面将参考相应的附图对根据本发明的最佳实施例的用于对被记录在光盘中的信息进行再现的装置和用于再现记录在光盘中的信息的方法进行描述。这里，光盘包含诸如 CD、视频 CD、CD-ROM、CD-R、CD-RW、MD、DVD、DVD-ROM、DVD-RAM、DVD-RW 等光盘和磁-光盘。

图 1 为根据本发明的第一最佳实施例的光盘 201 的数据结构的分级示意图，图 2 为图 1 中所示的光盘 201 的记录区的平面示意图。

在图 1 中，标号 100A 表示整个光盘 201 的信息记录区的数据结构，数据结构 100A 包含一个引入区 100，用于记录控制信息，和数据记录区 101，用于记录由内容控制信息 134 和内容数据 135 构成的内容信息 138，和引出区 102。如图 2 中所示，光盘 201 具有一个位于其中心的旋转驱动孔 201h，而引入区 100、数据记录区 101 和引出区 102 按照从光盘 201 的内部向着其外部的顺序定位。

参考图 1，引入区 100 包含控制数据区 110，用于记录图 3 中所示的光盘再现装置 200 所需的记录信息以对来自光盘的信息进行再现。控制数据区 110 包含一个物理信息扇区 111、一个用于存储第二密码密钥信息的扇区 150 等，如标号 100B 所示。在物理信息扇区 111 中记录诸如盘直径、盘结构、记录密度等关于光盘 201 的物理信息。通过解密预定的第二密钥信息而获得的第二密码密钥信息被记录在用于存储第二密码密钥信息的扇区 150 中。

用于记录第一密码密钥信息和诸如压缩电影、音乐等的内容信息 138 的加密信息扇区 151 被加密，然后作为加密文件 130 被记录在数据记录区 101 中。如图 1 中的标号 100A 所表示的，第一密码密钥信息被作为加密信息文件 120 记录在数据记录区 101 中。拥有版权的内容信息 138 被加密并被作为加密的文件 130 记录在数据记录区 101 中。不具有版权的内容信息 138 不被加密并被作为未加密文件 140 记录在数据记录区 101

中。

将数据记录区 101 划分为多个被称为扇区的单元。即，数据记录区 101 被划分为多个扇区。如标号 100C、100D 和 100E 所表示的，被记录在数据记录区 101 中的文件 120、130 和 140 包含多个加密的信息扇区 151、多个加密的扇区 152 和多个未加密的扇区 153。每个加密扇区 152 都包含 12 字节的扇区标题区 131，用于记录地址信息 161 等以便识别扇区，而 2048 字节的主数据区 132，用于记录内容信息 138，如标号 100F 所示。每个未加密扇区 153 包含 12 字节的扇区标题区 141，用于记录地址信息 161 等以便识别扇区，而 2048 字节的主数据区，用于记录内容信息 138，如标号 100G 所示。每个具有标号 100C 所表示的数据结构的加密信息扇区 151 具有扇区标题区和主数据区，与每个加密扇区 152 和每个未加密扇区 153 相类似。

另外，除了上述的地址信息 161 外，加密标志 162 被记录在各个扇区 152 和 153 的扇区标题区 131 和 141 中。被记录在扇区标题区 131 和 141 中的加密标志 162 为表示扇区 152 和 153 的各个主数据区 132 和 142 的预定的区域是否被加密。“1”的加密标志 162 被记录在具有加密信息的加密扇区中，而“0”的加密标志 162 被记录在具有未加密信息的未加密扇区中。

另外，被记录在导引区 100 中的用于存储密码密钥信息的扇区 150 中的第二密码密钥信息通过使用第一密钥信息被解码为第二密钥信息，其是通过使用预定的固定的密钥信息对包含在数据记录区 101 的加密信息文件 120 中的第一密码密钥信息进行解码而获得的。通过解码获得的第二密钥信息通过使用存储在内容信息 138 中的复制控制信息 136 和参考数据 137 被转换为在主数据的解密中使用的解密的密钥信息。在最佳实施例中，解密密钥信息与通过对应于解密电路 208 的加密电路进行解密使用的加密密钥信息相一致。参考数据 137 为部分内容数据 135。

如图 1 中的标号 100H 所示，并不是加密扇区 152 的所有的主数据区 132 都被加密。主数据区 132，除了包含内容控制信息 134 和部分内容数据的区域之外，均被加密。复制控制信息 136 包含诸如内容信息 138 的复制次数极限等信息，在对存储在光盘中的信息进行再现时进行下载

（downsampling）控制。通过使用加密密钥信息对存储在预定区域中的内容信息 138 的部分进行加密和复制而获得加密的内容信息，其为被转换的第二密钥信息，在其中通过使用复制控制信息 136 和部分压缩内容数据 135（即标号 100H 所示的数据结构中的参考数据 137）对通过解码获得的第二密钥信息进行转换，其中的复制控制信息 136 包含在内容控制信息 134 中。

图 3 为用于对被记录在图 1 和图 2 中所示的光盘 201 中的信息进行再现的光盘再现装置 200 的内部结构的方框图。下面将参考图 3 对光盘再现装置 200 进行描述。

本最佳实施例的光盘再现装置 200 对从光盘 201 中读出的被再现的数据进行解密和扩展，从而解码和输出所需的视频和音频信号。在图 3 中，用相同的标号表示与图 7 中所示的具有相同结构的元件，并省略了对其的详细描述。

现在参考 3，光盘再现装置 200 配备有光盘 201。光盘再现装置 200 包含一个锭子电机 202、一个光头 203、一个头放大器 204、一个模拟处理器 205、一个光盘控制器 206、一个错误矫正存储器 207、解密电路 208、AV 解码器 209、AV 信号处理存储器 210、伺服控制器 211、CPU212、和 CPU 总线 213。即，与图 7 中所示的光盘再现装置 400 相比，图 3 中所示的光盘再现装置 200 的特征在于，用于对加密和记录信息进行解密的解密电路 208 被设置在光盘控制器 206 和 AV 解码器 209 之间。

再参考图 3，光盘控制器 206 向解密电路 208 输出被处理的再现的数据。解密电路 208 对输入的被处理的再现数据进行解密，然后向 AV 解码器 209 输出解密的再现数据。伺服控制器 211、模拟处理器 205、光盘控制器 206、解密电路 208 和 AV 解码器 209 通过 CPU 总线 213 与 CPU212 相连。CPU212 通过 CPU 总线 213 控制模拟处理器 205、光盘控制器 206、解密电路 208、AV 解码器 209 和伺服控制器 211，从而控制整个的光盘再现装置 200 的操作。

被存储在加密信息文件 120 中并记录在数据记录区 101 中的第一密码密钥信息、包含在扇区 150 中用于存储导引区 100 中的第二密码密钥信息的第二密码密钥信息和作为部分内容信息 138 的复制控制信息和参

考数据 137 被输入到解密电路 208。解密电路 208 将输入的第一密码密钥信息通过使用预定的固定密钥信息解码为第一密钥信息。然后，解密电路 208 将输入的第二密码密钥信息通过使用上述的第一密钥信息解码为第二密钥信息。接着，解密电路 208 通过使用预定的转换方程（例如高阶方程，具有两个变量）利用输入的部分内容信息 138 将上述的第二密钥信息转换为被转换的第二密钥信息，即解密的密钥信息。另外，解密电路 208 通过使用上述的解密密钥信息将主数据解密为具有图 1 中标号 100D 所表示的数据结构的多个解密的扇区 152。

图 4 为图 3 中所示的加密电路的内部结构的方框图。下面将参考图 4 对解密电路 208 的结构和操作进行描述。

参考图 4，解密电路 208 包含第一信号选择器 301，固定密钥信息存储器 302、第二信号选择器 303、第一密钥信息解码器 304、第二密钥信息解码器 305、数据解密器 306、第三信号选择器 307 和包含第一密钥信息转换器 311 和第二密钥信息转换器 312 的密钥转换器部分 310。第一、第二和第三信号选择器 301、303 和 307 中的每个都包含多路转换器或开关电路。

再参考图 4，第一信号选择器 301 选择内部电路，对其根据通过 CPU 总线 213 从 CPU212 输入的解码模式将从光盘控制器 206 输入到解密电路 208 的数据输出。更具体的，当输入数据为被记录到导引区 100 中的第二密码密钥信息时，第一信号选择器 301 将输入的第二密码密钥信息输出到第二密钥信息解码器 305。另一方面，当输入数据为被记录到数据记录区 101 中的扇区数据时，第一信号选择器 301 向第二信号选择器 303 输出输入的扇区数据。固定密钥信息存储器 302 存储预定的固定的密钥用于对第一密码密钥信息进行解码。将从第一信号选择器 301 输出的扇区数据输入到第二信号选择器 303。第二信号选择器 303 选择电路，对其根据在扇区中的扇区数据的位置（即扇区数据的计数）输出扇区数据。如图 1 中所示，根据扇区中扇区数据的位置确定数据记录区 101 中被记录的扇区数据的类型。因此，根据扇区数据的计数，如图 4 中所示，第二信号选择器 303 进行下面的步骤：

（a）当输入的扇区数据为第一密码密钥信息时将输入的第一密码密

钥信息输出到第一密钥信息解码器 304；

（b）当输入的扇区数据为复制控制数据时将输入的复制控制数据输出到密钥转换部分 310 的第一密钥信息转换器 311；

（c）当输入的扇区数据为参考数据时将输入的参考数据输出到密钥转换器部分的第二密钥信息转换器 312；

（d）当输入的扇区数据为加密标志时将输入的加密标志输出到第三信号选择器 307；或

（e）当输入的扇区数据为主数据时，将输入的主数据输出到数据解密器 306 和第三信号选择器 307。

第一密钥信息解码器 304 通过对本领域中的技术人员所公知的诸如 DES 密码系统、RSA 密码系统等利用从固定密钥信息存储器 302 读出的固定的密钥信息对从第二信号选择器 303 输出的包含在数据记录区 101 中的第一密码密钥信息进行解码。因此，第一密钥信息解码器 304 将第一密码密钥信息解码为第一密钥信息，并将解码的第一密钥信息输出到第二密钥信息解码器 305。接着，第二密钥信息解码器 305 通过使用对本领域所公知的诸如 EDS 密码系统、RSA 密码系统等通过使用通过解码并从第一密钥信息解码器 304 输出的第一密钥信息以与第一密钥信息解码器 304 类似的方法对存储在扇区 150 中的第二密码密钥信息进行解码，其中扇区 150 用于存储第二密码密钥信息，该信息存储在导引区 100 中，并从第一信号选择器 301 输入。因此，第二密钥信息解码器 305 将第二密码密钥信息解码为第二密钥信息，并将第二密钥信息输出到密钥转换部分 310 的第一密钥信息转换器 311。

密钥转换部分 310 包含第一和第二密钥信息转换器 311 和 312。密钥转换部分 310 将从第二密钥信息解码器 305 输出的第二密钥信息转换为被转换的第二密钥信息（即解密密钥信息），即通过使用从第二信号选择器 303 输出的复制控制信息和参考数据。然后，密钥转换部分 310 将解密的密钥信息输出到数据解密器 306。第一密钥信息转换器 311 通过利用预定的第一转换方程(诸如预定的高阶方程)将从第二密钥信息解码器 305 输出的第二密钥信息转换为进行第一密钥信息转换的第二密钥信息，在该方法中，将两个输入数据代入到具有两个变量的高阶方程中，从而利

用从第二信号选择器 303 输出的复制控制信息计算高阶方程的值。然后，第一密钥信息转换器 311 将被转换的密钥信息输出到第二密钥信息转换器 312。接着，第二密钥信息转换器 312 通过使用预定的诸如预定高阶方程的二次变换方程将进行了第一密钥信息转换并从第一密钥信息转换器 311 输出的第二密钥信息转换为进行第二密钥信息转换的第二密钥信息，即被转换的第二密钥信息，在该方法中，将两个输入数据带入到具有两个变量的高阶方程，从而以与第一密钥信息转换器 311 相类似的方式通过使用从第二信号选择器 303 输出的参考数据计算高阶方程的值。然后，第二密钥信息转换器 312 将被转换的第二密钥信息输出到数据解密器 306。

数据解密器 306 通过使用从密钥转换部分 310 的第二密钥信息转换器 312 输出的解密的密钥信息对从第二信号选择器 303 输出的主数据进行解密。因此，数据解密器 306 产生解密的主数据，并将解密的主数据输出到第三信号选择器 307。按照下面的方式进行解密：通过使用用于有限长度的移位寄存器和加法器以与发射方相类似的方式产生具有预定长度的伪随机图形信号，例如 M-系列信号等，然后计算所产生的伪随机图形信号和输入数据的“异-或”操作。

接着，第三信号选择器 307 根据从第二信号选择器 303 输出的加密标志和在第三信号选择器 307 中计算的扇区数据的计数或者选择从第二信号选择器 303 输出的未解密主数据或者选择从数据解密器 306 输出的解密主数据。然后，第三信号选择器 307 向 AV 解码器 209 输出所选择的主数据。当加密标志等于“1”且计数不表示用于未加密数据 163 的存储区时，即当主数据被加密时，第三信号选择器 307 选择从数据解密器 306 输出的解密主数据，并将解密的主数据输出到 AV 解码器 209。另一方面，当加密标志等于“1”且计数表示用于未加密数据 163 的存储区时，或当加密标志等于“0”，即当主数据未被加密时，第三信号选择器 307 选择从第二信号选择器 303 输出的未加密主数据，并将未加密主数据输出到 AV 解码器 209。

下面将参考图 3 和图 4 对根据本发明的最佳实施例的光盘再现装置 200 的操作进行描述。

当将光盘201插入到接通电源的光盘再现装置200中时，或当光盘201重新被插入到光盘再现装置200中时，CPU212控制伺服控制器211，从而光头203可从光盘201读出存储在扇区150中的信息数据，其中扇区150用于存储密码密钥信息，该信息被存储在图1的导引区100中的控制数据区110中。放大读出信息数据的电信号，并通过头放大器204、模拟处理器205和光盘控制器206对其进行解调和错误矫正。然后，CPU212控制错误矫正存储器207将数据存储到被处理的第二密码密钥信息中。

接着，CPU212控制伺服控制器211，从而从光盘201中读出被存储在图1的加密信息文件（第一密码密钥信息）120中的扇区。通过头放大器204、模拟处理器205和光盘控制器206对读出的信息数据的电信号进行放大、解调和进行错误矫正。此时，在解密电路208中，根据来自CPU212的解码模式设定信息，设定解码第一密码密钥信息的模式。从光盘控制器206输入的第一密码密钥信息被通过第一信号选择器301和第二信号选择器303转换到第一密钥信息解码器304。然后，通过第一密钥信息解码器304使用从固定密钥信息存储器302读出的固定密钥信息，对被转换的第一密码密钥信息进行解码。接着，将通过解码获得的第一密钥信息输出到第二密钥信息解码器305。在将第一密码密钥信息解码为第一密钥信息的模式中，不从解密电路208输出任何数据。

接着，通过解密电路208的第一信号选择器301将已经存储到错误矫正存储器207中的第二密码密钥信息读出并输出到第二密钥信息解码器305。如上所述，通过第一密钥信息解码器304的解码已经获得的第一密钥信息被输入到第二密钥信息解码器305。第二密钥信息解码器305通过使用由解码获得的第一密钥信息对输入的第二密码密钥信息进行解码。因此，第二密钥信息解码器305将第二密码密钥信息解码为第二密钥信息，并将第二密钥信息输出到密钥转换部分310的第一密钥信息转换器311。

接着，将对装置使用者根据操作选择文件然后再现视频信号和声频信号的操作进行描述。

CPU212控制伺服控制器211、光头203、模拟处理器205和光盘控制器206，从而从光盘201读出所需的信息数据并使得操作矫正存储器207

存储进行错误矫正的信息数据。因此，CPU212 对解密电路 208 设定解密数据的模式。CPU212 设定 AV 解码器 209 所需的信息，然后控制错误矫正存储器 207 以将进行了错误矫正的信息数据转换到解密电路 208。

在解密电路 208 中，将解密数据的模式设定为解码模式设定信息。因此，通过第一信号选择器 301 将输入扇区数据转换到第二信号选择器 303。第二信号选择器 303 计算输入的扇区数据的数，并根据计数按照下面的方法输出输入扇区数据。

（a） 当上述的计数表示包含复制控制信息的数据位置时，输入扇区数据被输出到第一密钥信息转换器 311。

（b） 当上述的计数表示包含参考数据的数据位置时，输入扇区数据被输出到第二密钥信息转换器 312。

（c） 当上述的计数表示包含主数据的数据位置时，将输入扇区数据输出到数据解密器 306 和第三信号选择器 307。

通过解码获得并从第二密钥信息解码器 305 输出的第二密钥信息被通过第一密钥信息转换器 311 利用包含在主数据中的 复制控制信息进行第一密钥信息转换为第二密钥信息。然后，将被转换的第二密钥信息输出到第二密钥信息转换器 312。接着，进行第一密钥信息转换并从第一密钥信息转换器 311 输出的第二密钥信息被通过第二密钥信息转换器 312 利用包含在主数据中的参考数据转换为第二密钥信息，即解密密钥信息。然后，将解密的密钥信息输出到数据解密器 306。另外，通过使用从密钥转换部分 310 输出的解密密钥信息对输入到数据解密器 306 的主数据进行解密。然后，将被解密的主数据输出到第三信号选择器 307。

第三信号选择器 307 接收通过第二信号选择器 303 所选择的解密标志，计算其中的扇区数据数，根据加密标志和计数产生选择信号，并选择性的根据所产生的选择信号输出来自数据解密器 306 的主数据，或来自第二信号选择器 303 的主数据。根据所产生的选择信号，当解密标志等于“1”且当扇区数据的计数表示用于记录未加密数据 163 的记录区时，从第三信号选择器 307 输出从第二信号选择器 303 输出的未加密主数据。另一方面，当加密标志等于“1”且扇区数据的计数表示用于加密数据 164 的存储区时，从第三信号选择器 307 输出从数据解密器 306 输出的主数

据。根据所产生的选择信号，当加密标志等于“0”，在与扇区数据的计数无关的情况下，从第三信号选择器 307 输出由第二信号选择器 303 输出的未加密主数据。

如上所述，根据加密标志和扇区数据的计数被解密的主数据从解密电路 208 向 AV 解码器 209 输出。AV 解码器 209 多路转换被多压缩的声频和视频数据，扩展声频和视频数据，然后输出扩展的视频和声频信号。

如上所述，本发明的最佳实施例具有下面的特定的优点。

首先，图 3 中的 CPU212，其作为 DVD 播放机等的光盘再现装置的系统控制装置，在内容控制信息 134 中读出诸如复制次数的限制和在再现时进行下载控制的信息。在对光盘再现装置 200 进行控制时，由于记录了未加密内容控制信息，因此可容易的参考内容控制信息。

记录上述的未加密的内容控制信息 134。当内容控制信息被篡改时，由于设置了密钥转换部分 310，无法产生正确的解密密钥信息。因此，可防止未被授权的再现。

以扇区为单位可容易地使改变的内容数据用于从第二密码密钥信息通过使用内容控制信息 134 获得加密密钥信息。因此，即使如图 1 中所示在上述的文件中记录了内容控制信息 134 且在单位盘中记录了第二密钥信息，由于密钥信息是逐一扇区进行改变的，因此可增强通过加密对内容的保护强度。

图 5 为根据本发明的第二最佳实施例的光盘的数据结构的分级图，图 6 为在第二最佳实施例中使用的解密电路 208a 的内部结构的方框图。在图 5 和图 6 中，与图 1 和图 4 中相同的元件用相同的标号表示。下面将详细描述根据第二最佳实施例的光盘的数据结构和解密电路 208a 的操作和结构，更具体的为第一和第二最佳实施例之间的差别。

在第一最佳实施例中，第一密码密钥信息被作为加密信息 120 存储在数据记录区 101 中，如图 1 中所示。在第二最佳实施例中，第一密码密钥信息被存储在导引区 100 中的控制数据区 110 内的加密信息扇区 112 中，如图 5 中所示。在第一最佳实施例中，第二密码密钥信息被存储在扇区 150 中，用于存储被存储在导引区 100 的控制数据区 110 中的第二密码密钥信息，如图 1 中所示。在第二最佳实施例中，如图 5 中所示，

第二密码密钥信息被和地址信息一起存储在数据记录区 101 中的加密文件 130 的加密扇区 152 的扇区标题区 131 中。

下面将参考图 6 描述具有如上结构的用于再现被记录在光盘 201 中的信息的光盘再现装置 200。第二最佳实施例的特征在于用图 6 中所示的解密电路 208a 代替图 4 中所示的解密电路 208。更具体的，图 6 中所示的解密电路 208a 与图 4 中所示的解密电路 208 的区别在于下面的各个方面。

（a） 用第一信号选择器 301a 代替第一信号选择器 301。用第二信号选择器 303a 代替第二信号选择器 303。

（b） 在图 4 中所示的解密电路 208 中，通过第一和第二信号选择器 301 和 303 选择第一密码密钥信息，然后输出到第一密钥信息解码器 304。然而，在图 6 中所示的解密电路 208a 中，通过第一信号选择器 301a 选择第一密码密钥信息，然后输出到第一密钥信息解码器 304。

（c） 在图 4 中所示的解密电路 208 中，通过第一信号选择器 301 选择第二密码密钥信息，然后输出到第二密钥信息解码器 305。然而，在图 6 中所示的解密电路 208a 中，通过第一和第二信号选择器 301a 和 303a 选择第二密码密钥信息，然后输出到第二密钥信息解码器 305。

换句话说，图 6 中所示的解密电路 208a 对被记录在导引区 100 的加密信息扇区 112 中并从光盘控制器 206 输入的第一密码密钥信息进行解码。因此，解密电路 208a 解码第二密码密钥信息并解密主数据，以便对具有图 5 中所示的用标号 110C 所表示的数据结构的扇区数据进行处理。

接着，将参考图 6 对解密电路 208a 的操作，更具体的对解密电路 208a 和图 4 中所示的根据第一最佳实施例的解密电路 208 之间的差别进行详细描述。

当输入数据为被记录在导引区 100 中的控制数据区 110 的加密信息扇区 112 中的第一密码密钥信息时，第一信号选择器 301a 将输入的第一密码密钥信息输出到第一密钥信息解码器 304。另一方面，当输入数据为被记录在数据记录区 101 中的扇区数据时，第一信号选择器 301a 将输入扇区数据输出到第二信号选择器 303a。接着，将从第一信号选择器 301a 输出的扇区数据输入到第二信号选择器 303a。第二信号选择器 303a 选择

一个电路，对其根据扇区中扇区数据的位置和扇区数据的计数输出扇区数据。如图 1 中所示，根据扇区中扇区数据的位置确定记录在数据记录区 101 中的扇区数据的类型。因此，根据扇区数据的计数，如图 6 中所示，第二信号选择器 303a 进行下面的操作：

（a）当输入扇区数据为第二密码密钥信息时，将输入的密码密钥信息输出到第二密钥信息解码器 305。

（b）当输入扇区数据为复制控制数据时，将输入复制控制数据输出到第一密钥信息转换器 311。

（c）当输入扇区数据为参考数据时将输入参考数据输出到密钥转换部分 310 的第二密钥信息转换器 312；

（d）当输入扇区数据为加密标志时将输入加密标志输出到第三信号选择器 307；

（e）当输入扇区数据为主数据时将输入主数据输出到数据解密器 306 和第三信号选择器 307。

下面将参考图 3 和图 6 对根据本发明的具有如上结构的光盘再现装置 200 的操作进行描述。在图 3 中，用解密电路 208a 代替解密电路 208。

当将光盘 201 插入到接通电源的光盘再现装置 200 中时，或当光盘 201 重新被插入到光盘再现装置 200 中时，光盘再现装置 200 对记录在导引区 100 中的控制数据区 110 的加密信息扇区 112 中的第一密码密钥信息进行解码。CPU212 控制伺服控制器 211，从而光头 203 可从光盘 201 通过使用光头 203 读出导引区 100 中的控制数据区 110 中的加密信息扇区 112 内的信息数据，放大读出信息数据的电信号，并通过头放大器 204、模拟处理器 205 和光盘控制器 206 对其进行解调和错误矫正。然后，对信息数据进行错误矫正并存储到存储器 207 中。因此，CPU212 解码作为用于解密电路 208a 的解码模式设定信息的解码第一密码密钥信息的模式。CPU212 控制光盘控制器 206 和解密电路 208a，从而在加密信息扇区 112 中的被进行错误矫正的第一密码密钥信息上的数据被从光盘控制器 206 传递到解密电路 208a。

在解密电路 208a 中设定解码第一密码密钥信息的模式。因此，将存储在加密信息扇区 112 中的第一密码密钥信息上的输入数据通过第一信

号选择器 301a 传递到第一密钥信息解码器 304。将被传递的第一密码密钥信息通过使用从固定密钥信息存储器 302 读出的固定密钥信息借助第一密钥信息解码器 304 解码为第一密钥信息。然后，将第一密钥信息输出到第二密钥信息解码器 305。在解码第一密码密钥信息的模式中，从解密电路 208a 不输出数据。

接着，将描述通过装置用户根据操作选择文件然后再现音频信号和声频信号的操作。

CPU 212 控制伺服控制器 211、光头 203、模拟处理器 205 和光盘控制器 206，从而从光盘 201 读出所需的信息数据，接着使得错误矫正存储器 207 存储进行了错误矫正的信息数据。因此，CPU212 设定用于解密电路 208a 的解密数据的模式。CPU212 设定 AV 解码器 209 所需的信息数据，然后控制错误矫正存储器 207 将进行错误矫正的信息数据传递到解密电路 208a。

在解密电路 208a 中，将解密数据的模式设定为解码模式设定信息。因此，通过第一信号选择器 301a 将输入扇区数据传递到第二信号选择器 303a。第二信号选择器 303a 计算输入扇区数据的计数并根据计数按照下面的方式选择的输出输入扇区数据。

（a） 当扇区标题区 131 中上述的计数表示第二密码密钥信息 133 时，扇区数据中的第二密码密钥信息 133 被输出到第二密钥信息解码器 305。

（b） 当上述的计数表示包含复制控制信息 136 的数据位置时，扇区数据中的复制控制信息 136 被输出到第一密钥信息转换器 311。

（c） 当上述的计数表示包含参考数据的数据位置时，扇区数据中的参考数据 137 被输出到第二密钥信息转换器 312。

（d） 当上述的计数表示包含主数据的数据位置时，将主数据输出到数据解密器 306 和第三信号选择器 307。

将输入到第二密钥信息解码器 305 中的第二密码密钥信息通过使用作为密钥的从第一密钥信息解码器 304 输出的第一密钥信息解码为第二密钥信息。将通过解码获得的第二密钥信息输出到密钥转换部分 310 的第一密钥信息转换器 311。

接着，将通过解码获得的第二密钥信息转换为通过第一密钥信息转换器 311 借助使用包含在主数据中的复制控制信息 136 进行了第一密钥信息转换的第二密钥信息。然后，将被转换的第二密钥信息输出到第二密钥信息转换器 312。通过第二密钥信息转换器 312 借助使用包含在主数据中的参考数据将进行了第一密钥信息转换的第二密钥信息转换为被转换的第二密钥信息。将被转换的第二密钥信息作为解密密钥信息输出到数据解密器 306。接着，通过使用从密钥转换部分 310 的第二密钥信息转换器 312 输出的解密密钥信息对输入到数据解密器 306 的主数据进行解密。然后，将被解密的主数据输出到第三信号选择器 307。

接着，第三信号选择器 307 根据从第二信号选择器 303a 输出的解密标志和在第三信号选择器 307 中计算的扇区数据的计数，选择从第二信号选择器 303a 输出的未加密的主数据或从数据解密器输出的解密的主数据。然后，第三信号选择器 307 将所选的主数据输出到 AV 解码器 209。当加密标志等于“1”且计数不表示用于未加密数据 163 的存储区时，即当主数据被加密时，第三信号选择器 307 选择从数据解密器 306 输出的被解密的主数据，并将解密的主数据输出到 AV 解码器 209。另一方面，当加密标志等于“1”而计数表示用于未加密数据 163 的存储区时，或当加密标志等于“0”，即当主数据未被加密时，第三信号选择器 307 选择从第二信号选择器 303a 输出未解密主数据 ，并将未解密的主数据输出到 AV 解码器 209。

在最佳实施例中，可将第二密码密钥信息存储在一个加密扇区 152 中，或将通过划分第二密码密钥信息而得到的多个数据存储在多个加密扇区 152 的加密文件 130 中。

如上所述，根据第二最佳实施例，除了第一最佳实施例的优点外，第二密码密钥信息可以扇区或文件为单位进行存储。因此，可以扇区或文件为单位对第二密码密钥信息进行改变。因此，可进一步增强通过加密对版权保护的强度。

在上述的最佳实施例中，所进行的描述主要针对光盘，和对存储在光盘中的信息进行再现的方法和用于再现记录在光盘中的信息的装置。然而，本发明并不限于此。本发明可应用在信息记录媒体，其包含诸如

软盘等磁记录介质和诸如快速存储器、EPROM 或 EEPROM 等的存储器，和用于对记录在信息记录媒体中的信息进行再现的方法和用于对记录在信息记录媒体中的信息进行再现的装置。

在上述的最佳实施例中，通过利用加密密钥信息的加密获得内容信息 138 的被加密和记录的部分，其是通过使用内容信息 138 的未加密部分对第一和第二密钥信息进行转换而获得的。然而，本发明并不限于此。通过使用加密密钥信息的加密获得内容信息 138 的加密和记录部分，其是通过使用内容信息 138 的未加密部分至少对第一和第二密钥信息中的一个进行转换而得到的。

在上述的最佳实施例中，装置包含第一和第二密钥信息解码器 304 和 305。然而，本发明并不限于此。装置可至少包含第一和第二密钥信息解码器 304 和 305 中的一个。当装置只包含第一密钥信息解码器 304 时，通过借助第一密钥信息解码器的解码获得的第一密钥信息被输出到密钥转换部分 310。当装置只包含第二密钥信息解码器 305 时，第二密钥信息解码器 305 通过使用从固定密钥信息存储器 302 读出的固定密钥信息将第二密码密钥信息解码为第二密钥信息，然后将第二密钥信息输出到密钥转换部分 310。

在上述的最佳实施例中，密钥转换部分 310 包含第一和第二密钥转换部分 311 和 312。然而，本发明并不限于此。密钥转换部分 310 至少包含第一和第二密钥信息转换器 311 和 312 中的一个。即，通过使用部分内容信息 138（即至少复制控制信息和参考数据 137 中的一个）对第二密钥信息进行转换，其中的第二密钥信息是通过借助第二密钥信息解码器 305 获得的并从第二密钥信息解码器 305 输出，而被转换的第二密钥信息可被用做解密密钥信息。

在上述的最佳实施例中，每个密钥信息解码器 304 和 305 通过使用预定的密钥信息将预定的密钥信息解码为通过解码获得的密钥信息。然而，本发明并不限于此。每个密钥信息解码器 304 和 305 可通过使用预定的变换方程借助预定的密钥信息将预定的密码密钥信息转换为被转换的密码密钥信息。

在上述的实施例中，每个密钥信息转换器 311 和 312 通过使用预定

的变换方程借助预定的信息将预定的密码密钥信息转换为被转换的密码密钥信息。然而，本发明并不限于此。每个密钥信息转换器 311 和 312 可通过使用预定的密钥信息将预定的密码密钥信息解码为通过解码获得的密钥信息。

如上所述，根据本发明，其提供一种信息记录媒体，用于至少记录拥有版权的内容信息和密码密钥信息，且在上述的信息记录媒体中，部分内容信息被加密和记录，而内容信息的被加密和记录的部分是通过使用加密密钥信息进行加密而获得的，其中的加密密钥信息是通过使用内容信息的未加密部分对密码密钥信息进行转换而获得的。因此，本发明具有下面的优点。

诸如 DVD 播放机等的信息再现装置的系统控制器读出一部分内容信息，其是一种内容控制信息，诸如复制的次数的限制和在再现时对下载的控制信息等。在对信息再现装置进行控制时，由于记录了未加密内容控制信息，因此可容易的参考内容控制信息。

因此，诸如内容控制信息等部分内容信息未被加密并被记录。当诸如内容控制信息等部分内容信息被篡改时，无法产生正确的解密密钥信息。因此，可防止未被授权的再现。

另外，以扇区为单位可容易进行改变的内容数据用于从第二密码密钥信息通过使用内容控制信息获得加密密钥信息，因此，即使在文件中记录了内容控制信息且在单位盘中记录了第二密钥信息，由于密钥信息是逐扇区进行改变的，因此可增强通过加密对内容的保护强度。

另外，未加密数据被用做参考数据产生加密密钥信息。因此，例如，即使密码密钥信息或复制控制信息被设定在文件的单位中，加密密钥信息也以扇区为单位进行改变。因此，可防止盗版行为的发生。

另外，当以扇区或文件为单位记录密码密钥信息时，可以扇区或文件为单位对密码密钥信息进行改变。因此，可增强通过加密对版权的保护强度。

虽然已经结合相应的附图通过具体的实施例对本发明进行了具体的描述，但对本领域中的技术人员来说，可做各种的变化和修改。但这种变化和修改都在本发明所附的权利要求的范围之内。

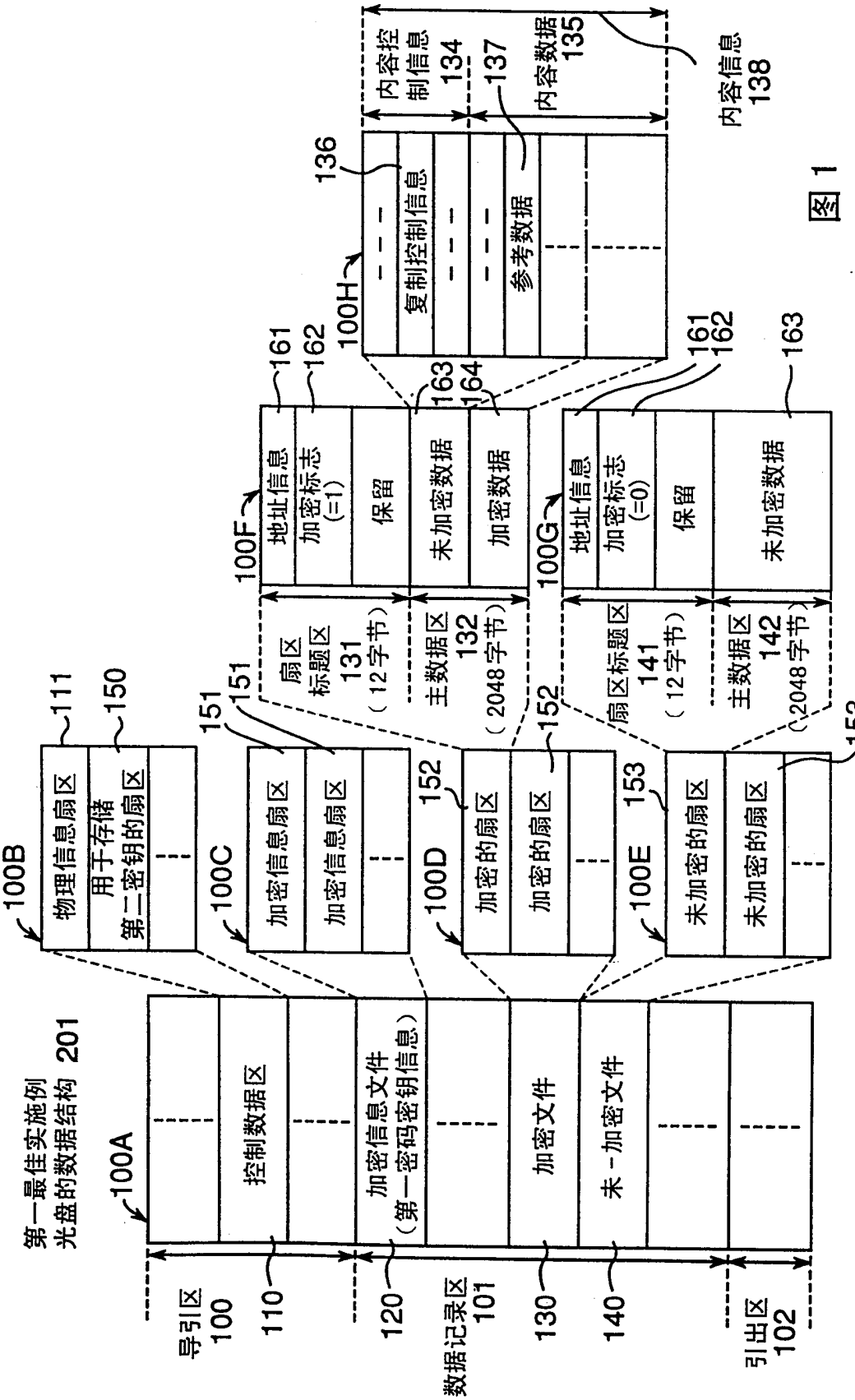

第一最佳实施例
光盘的数据结构 201
100A
导引区
100
110
控制数据区
120
加密信息文件
（第一密码密钥信息）
数据记录区
101
130
加密文件
140
未－加密文件
引出区
102
100B
物理信息扇区
用于存储
第二密钥的扇区
150
111
100C
加密信息扇区
加密信息扇区
151
100D
加密的扇区
加密的扇区
152
100E
未加密的扇区
未加密的扇区
153
100F
地址信息
加密标志
(=1)
保留
未加密数据
加密数据
扇区
标题区
131
（12字节）
主数据区
132
（2048字节）
161
162
163
164
100G
地址信息
加密标志
(=0)
保留
未加密数据
扇区标题区
141
（12字节）
主数据区
142
（2048字节）
100H
- - -
复制控制信息
- - -
参考数据
136
内容控
制信息
134
137
内容数据
135
内容信息
138

图 1

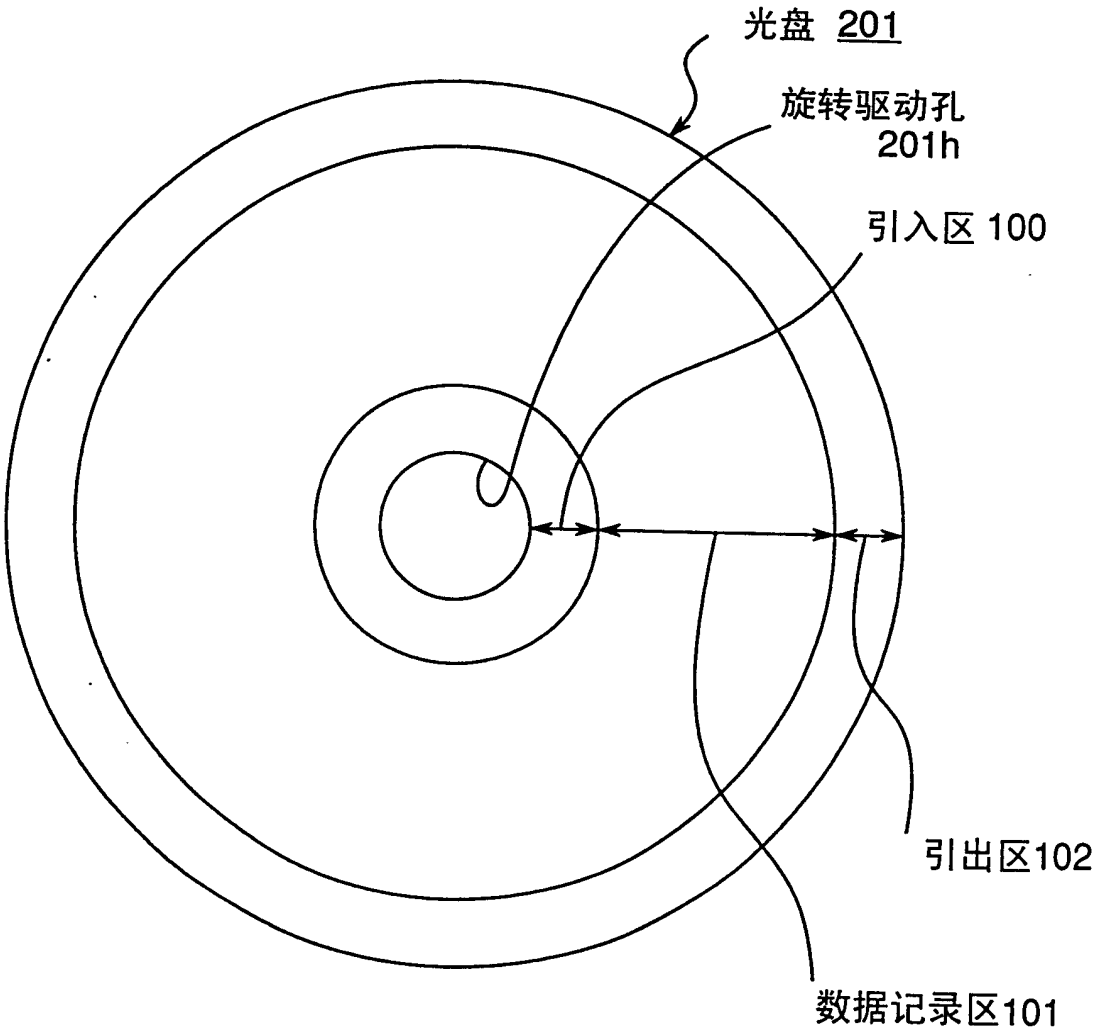


图 2

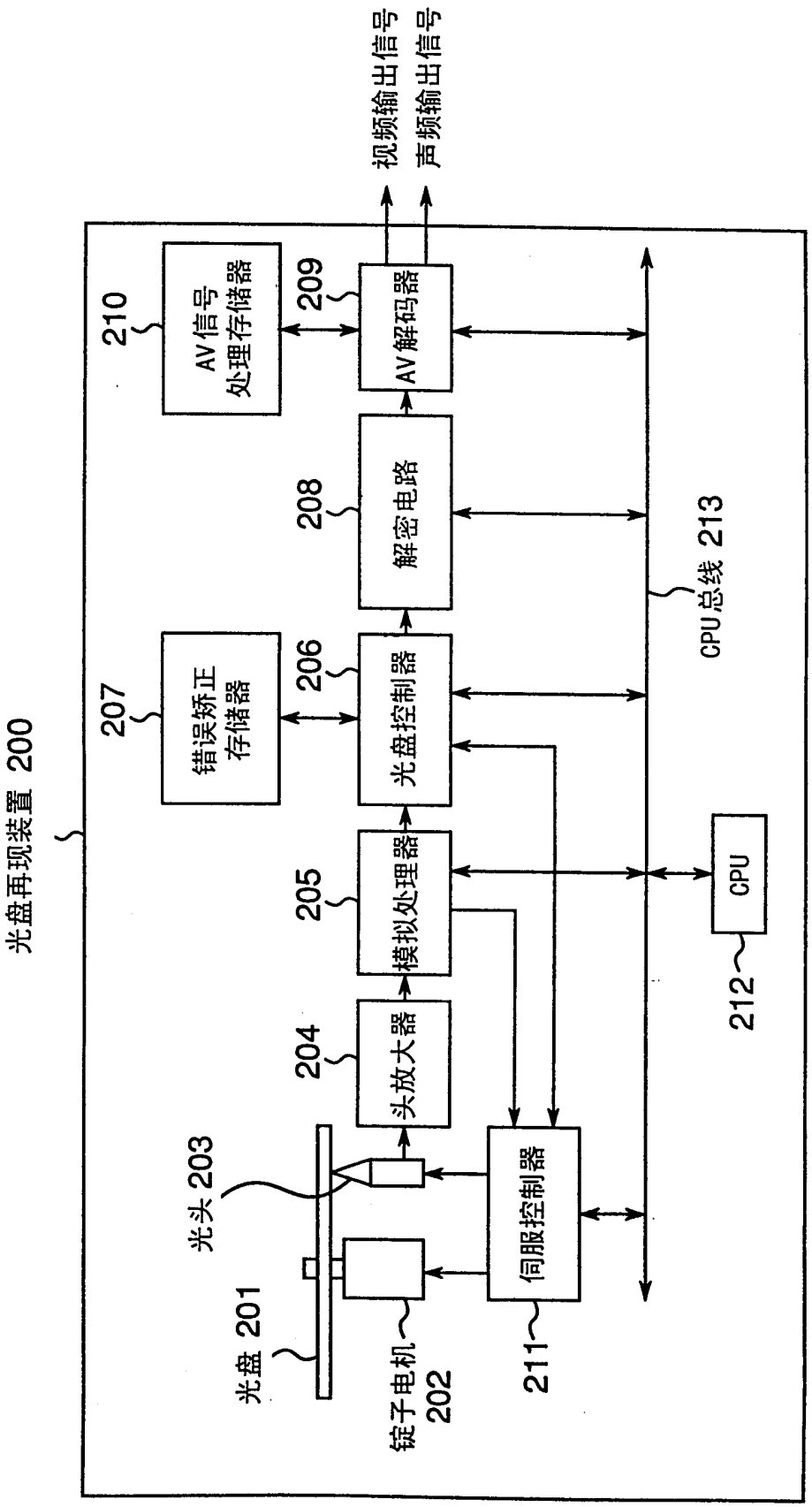

光盘再现装置 200
视频输出信号
声频输出信号
AV信号
处理存储器
210
209
AV解码器
208
解密电路
207
错误矫正
存储器
206
光盘控制器
CPU总线 213
205
模拟处理器
CPU
212
204
头放大器
光头 203
光盘 201
锭子电机
202
伺服控制器
211

图 3

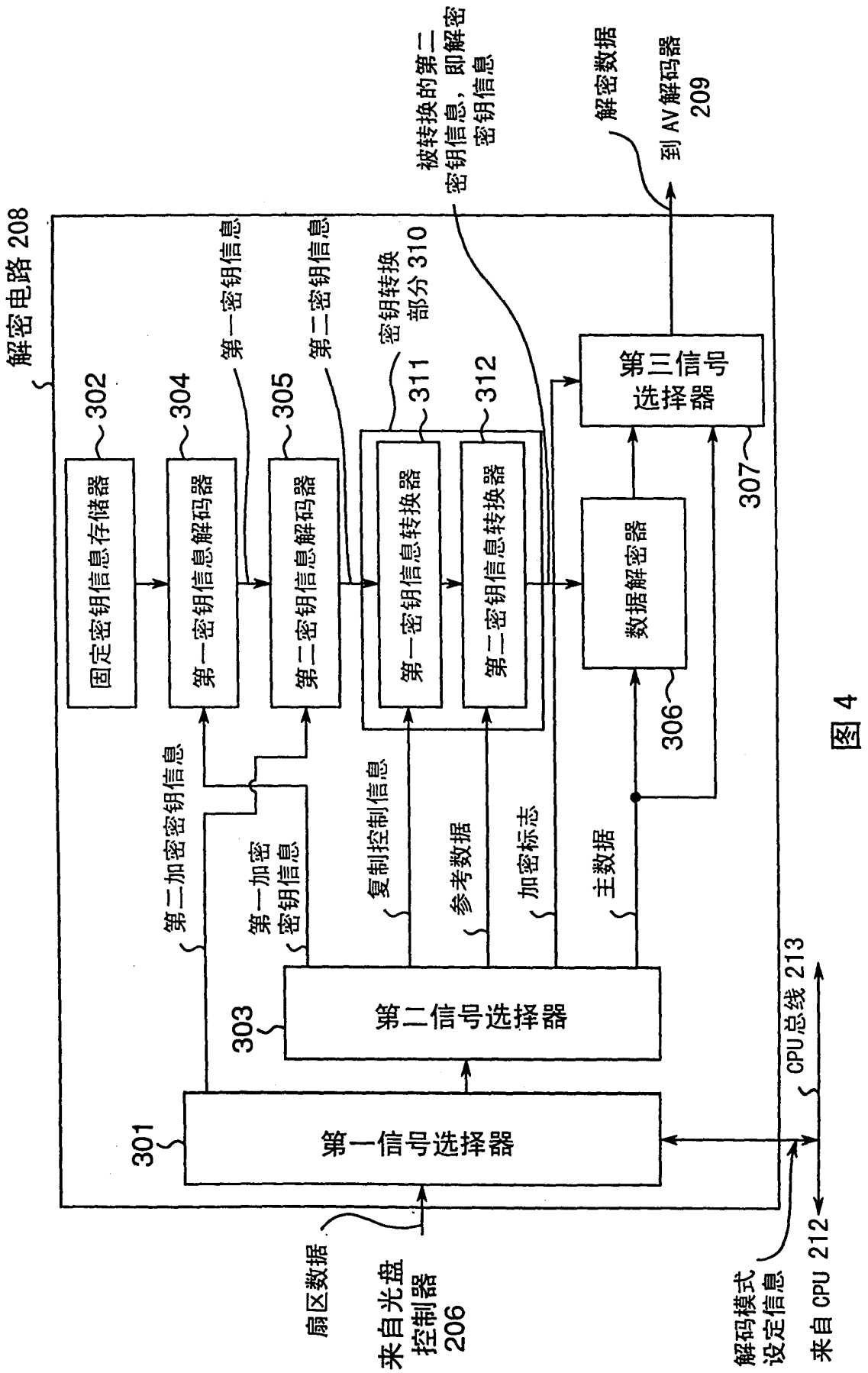

解密电路 208
固定密钥信息存储器
302
第一密钥信息解码器
304
第二密钥信息解码器
305
第一密钥信息
第二密钥信息
密钥转换部分 310
第一密钥信息转换器
311
第二密钥信息转换器
312
被转换的第二密钥信息，即解密密钥信息
解密数据
到 AV 解码器 209
第二信号选择器
307
数据解密器
306
第二加密密钥信息
第一加密密钥信息
复制控制信息
参考数据
加密标志
主数据
303
第二信号选择器
301
第一信号选择器
CPU 总线 213
扇区数据
来自光盘控制器 206
解码模式设定信息
来自 CPU 212

图 4

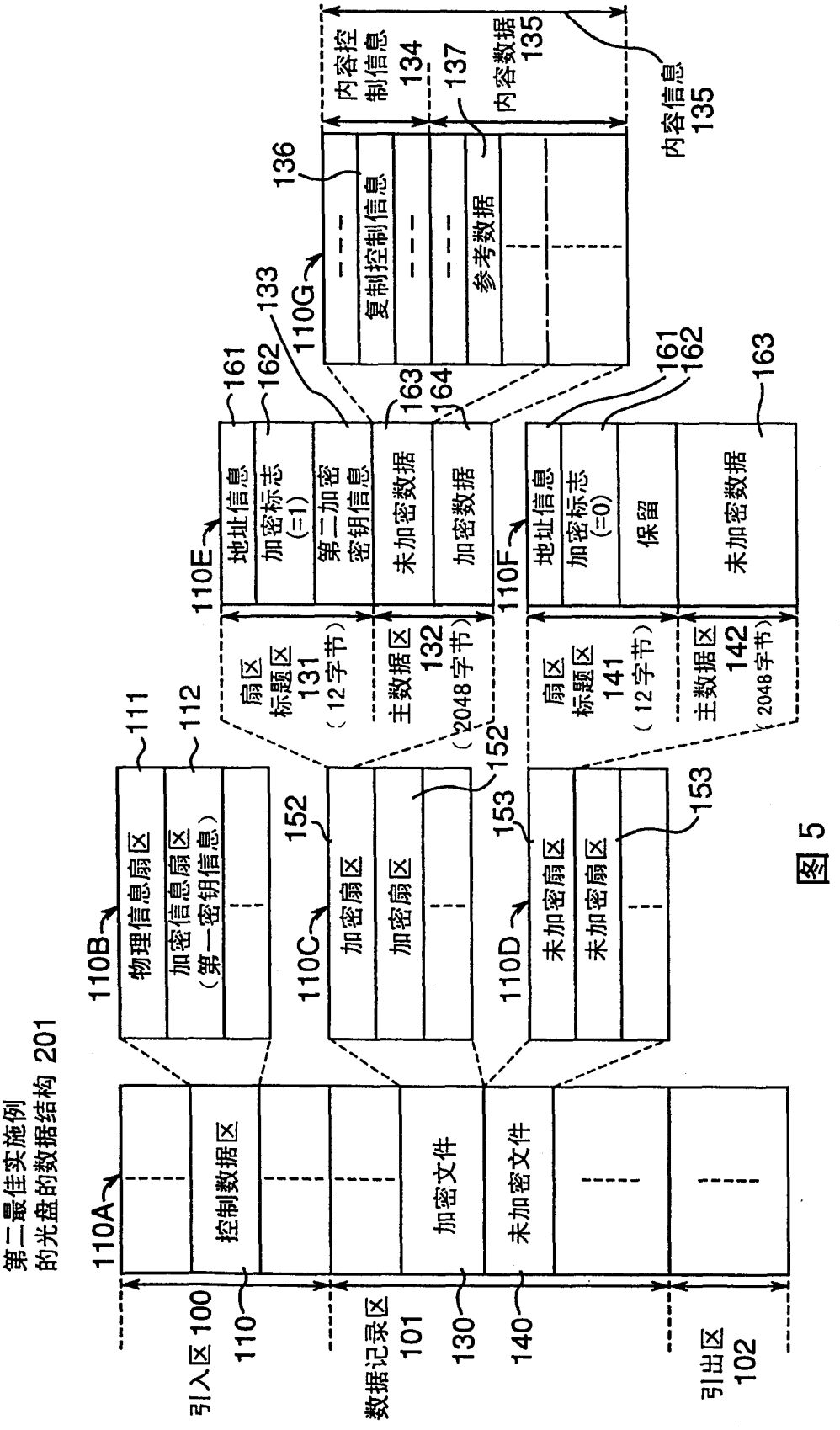

第二最佳实施例
的光盘的数据结构 201
引入区 100
数据记录区
101
引出区
102
110
130
140
110A
控制数据区
110B
物理信息扇区
加密信息扇区
（第一密钥信息）
110C
加密扇区
加密扇区
110D
未加密扇区
未加密扇区
加密文件
未加密文件
111
112
152
153
扇区
标题区
131
（12字节）
主数据区
132
（2048字节）
扇区
标题区
141
（12字节）
主数据区
142
（2048字节）
110E
地址信息
加密标志
(=1)
第二加密
密钥信息
未加密数据
加密数据
110F
地址信息
加密标志
(=0)
保留
未加密数据
161
162
163
164
110G
复制控制信息
参考数据
136
133
内容控
制信息
134
137
内容数据
135
内容信息
135

图 5

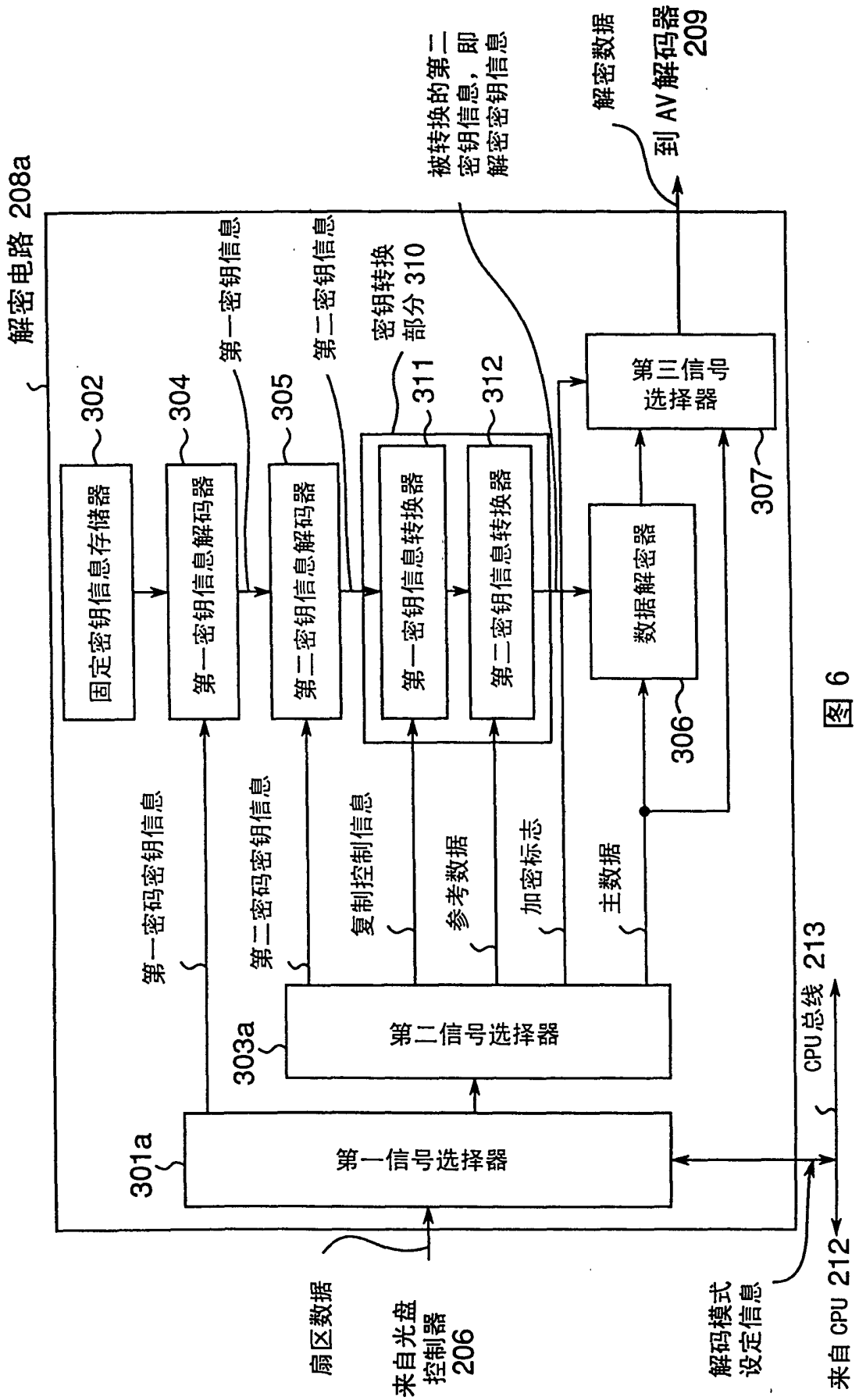

解密电路 208a
固定密钥信息存储器
302
第一密钥信息解码器
304
第二密钥信息解码器
305
第一密钥信息转换器
311
第二密钥信息转换器
312
密钥转换部分 310
第一密钥信息
第二密钥信息
被转换的第二密钥信息，即解密密钥信息
解密数据
到 AV 解码器 209
第二信号选择器
307
数据解密器
306
第一密码密钥信息
第二密码密钥信息
复制控制信息
参考数据
加密标志
主数据
303a
第一信号选择器
301a
CPU 总线 213
扇区数据
来自光盘控制器 206
解码模式设定信息
来自 CPU 212

图 6

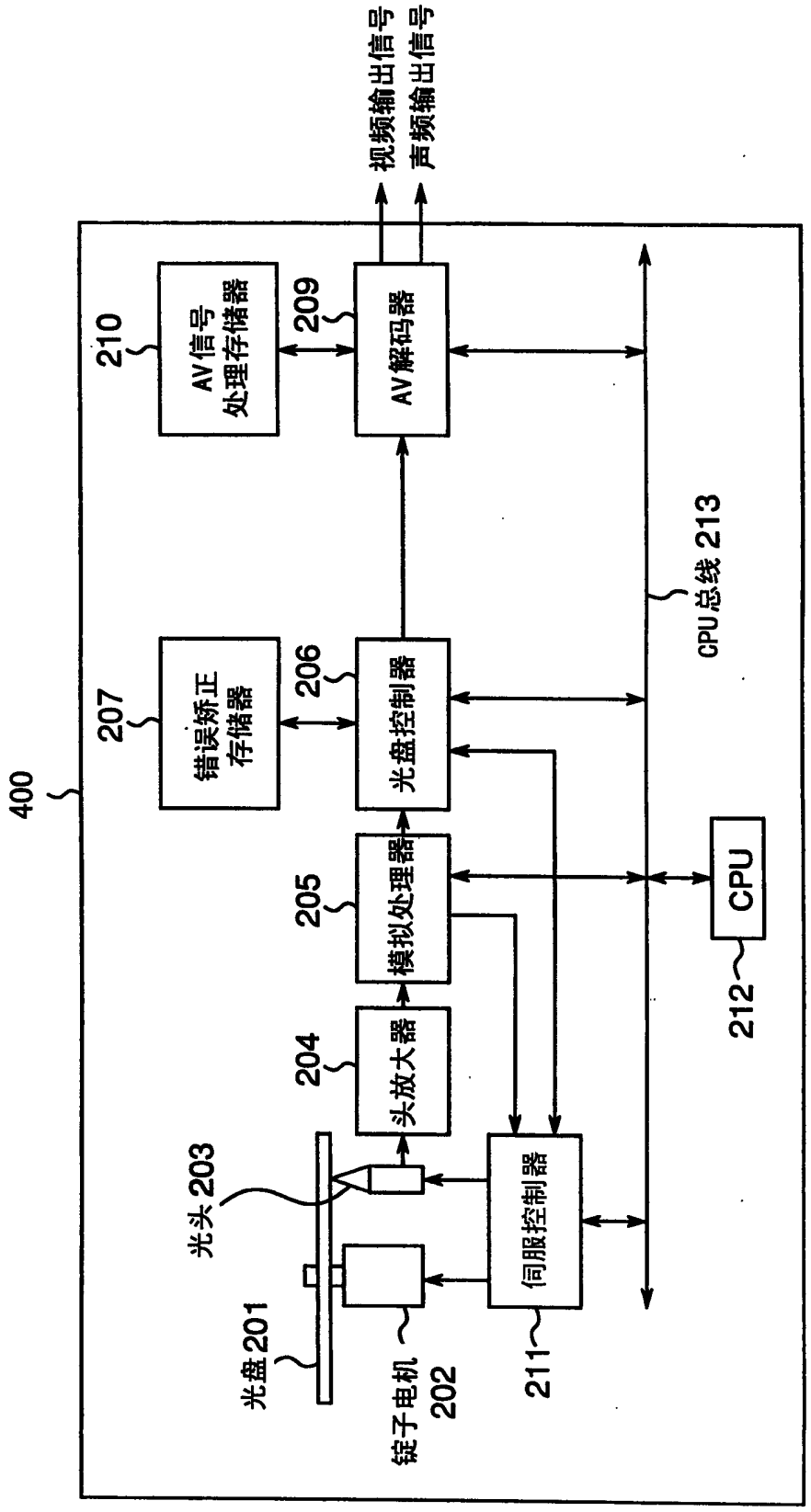

视频输出信号
声频输出信号
400
210
AV信号
处理存储器
209
AV解码器
207
错误矫正
存储器
206
光盘控制器
CPU总线 213
205
模拟处理器
CPU
212
204
头放大器
光头 203
伺服控制器
光盘 201
锭子电机
202
211

图 7