[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
G11B 20/10

[12]发明专利申请公开说明书

[21]申请号 99801186.X

[43]公开日 2000年11月22日

[11]公开号 CN 1274461A

[22]申请日 1999.7.21 [21]申请号 99801186.X

[30]优先权

[32]1998.7.22 [33]JP [31]206967/1998

[32]1998.10.12 [33]JP [31]289831/1998

[86]国际申请 PCT/JP99/03887 1999.7.21

[87]国际公布 WO00/05716 日 2000.2.3

[85]进入国家阶段日期 2000.3.21

[71]申请人 松下电器产业株式会社

地址 日本大阪府门真市

[72]发明人 田川健二 南贤尚

小濑雅之

[74]专利代理机构 中国专利代理(香港)有限公司

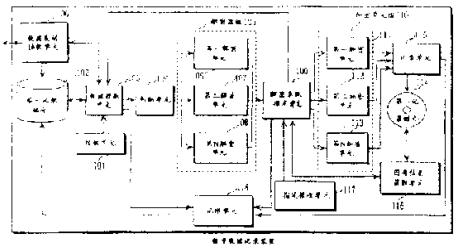
代理人 梁 永 陈景峻

权利要求书3页 说明书36页 附图页数25页

[54]发明名称 保护版权的数字数据记录装置和方法,其使记录在记录媒介上的加密的数字数据易于再现,以及记录了该方法的程序的计算机可读的记录媒介

[57]摘要

数据发送/接收单元接收电子音乐传播系统传播的加密的数字数据并将数字数 据记录在第一记录媒介上。数字数据在不同传播商的不同的加密系统中被加密 ,并包含有表示加密系统的属性信息。加密数据提取单元提取的数字数据加密 的加密系统由判断单元选取并由相对应的解密单元解密。固有信息获取单元根 据第二记录媒介是否可以从播放装置中取出,获取第二记录媒介或播放装置的 标志信息。加密系统指定单元根据获取的标志信息选择多个加密单元中的一个 加密单元。所选的加密单元根据标志信息产生一个加密密匙并加密数字数据。记录单元将数字数据记录在第二记录媒介上。计帐单元根据属性信息中的计帐 信息付费。



ISSN1008-4274

权　利　要　求　书

1、 将数字数据记录在记录媒介上的数字数据记录装置，它包括：

通过数字网络接收加密的数字数据的通讯装置；

解密通讯装置接收到的加密数字数据的解密装置；

包括将解密的数字数据在有不同安全级的加密系统中再次加密的多个加密单元的加密装置；

将加密装置再次加密的数字数据记录到记录媒介上的记录装置；及

控制解密装置和加密装置的控制单元，其中控制单元使多个加密单元中的一个加密单元再次加密由解密装置解密的数字数据。

2、 根据权利要求 1 的数字数据记录装置，其中：

记录在记录媒介上的数字数据由播放装置再现，

加密装置包括：

第一加密单元，它用根据记录媒介的标志信息产生的加密密匙再次加密数字数据；

第二加密单元，它用根据播放装置的标志信息产生的加密密匙再次加密数字数据；

控制单元判断记录媒介是否可以从播放装置中取出，当记录媒介可从播放装置中取出时，使第一加密单元再次加密解密的数字数据，当记录媒介不可以从播放装置中取出时，使第二加密单元再次加密解密的数字数据。

3、 根据权利要求 1 的数字数据记录装置，还包括通过数字网络进行财务处理的计帐装置，其中：

控制单元根据再次加密已解密的数字数据的加密单元确定一个计帐值，并控制计帐装置，使控制单元根据确定的计帐值进行财务处理。

4、 根据权利要求 3 的数字数据记录装置，其中

已记录在记录媒介上的数字数据由播放装置复制；

加密装置包括：

第一加密单元，它用根据记录媒介的标志信息产生的加密密匙再次加密数字数据；

第二加密单元，它用根据播放装置的标志信息产生的加密密匙再次加密数字数据；

控制单元判断记录媒介是否可以从播放装置中取出，当记录媒介可

从播放装置中取出时，使第一加密单元再次加密解密的数字数据，当记录媒介不可以从播放装置中取出时，使第二加密单元再次加密解密的数字数据。

5、根据权利要求 4 的数字数据记录装置，其中当加密装置未产生任何加密密匙时控制单元禁止解密装置解密已加密的数字数据。

6、 根据权利要求 1 的数字数据记录装置，其中多个加密单元再次加密解密的数字数据的加密系统的安全级低于用于加密由通讯装置接收到的加密的数字数据的加密系统的安全级。

7、 根据权利要求 1 的数字数据记录装置，其中

通讯装置接收到的加密的数字数据在有不同安全级的加密系统之一中被加密并且加密的数字数据包括表示加密系统的属性信息；

解密装置包括一个解密单元组，它解密在加密系统中被加密的加密数字数据；

控制单元根据属性信息判断加密数字数据的加密系统，并控制解密装置使多个解密单元的一个解密单元与判断的加密系统对应，解密加密的数字数据。

8、 根据权利要求 7 的数字数据记录装置，还包括通过数字网络进行财务处理的计帐装置，其中：

控制单元根据解密已加密的数字数据的解密单元和再次加密解密的数字数据的加密单元确定一个计帐值，并控制计帐装置使控制单元根据确定的计帐值进行财务处理。

9、 一种将数字数据记录在记录媒介上的数字数据记录方法，包括：

通过数字网络接收加密的数字数据的通讯步骤：

解密通讯步骤中接收到的加密的数字数据的解密步骤；

在有不同安全级的多个加密系统中的一个加密单元中再次加密解密的数字数据的加密步骤；

将加密步骤中已再次加密的数字数据记录在记录媒介上的记录步骤。

10、 根据权利要求 9 的数字数据记录方法，其中

通讯步骤中收到的加密的数字数据已在有不同安全级的加密系统之一中被加密并且加密的数字数据包括表示加密系统的属性信息；

数字数据记录方法，还包括根据属性信息判决多个加密系统之一的判断步骤，其中：解密步骤根据判断步骤中的判断结果解密加密的数字数据。

11、计算机可读的记录媒介，它应用于将数字数据记录在第一记录媒介上的数字数据记录装置，计算机可读的记录媒介存储了一个程序，它使计算机执行以下步骤：

通过数字网络接收加密的数字数据的通讯步骤；

解密通讯步骤中接收到的加密的数字数据的解密步骤；

将解密的数字数据在有不同安全级的多个加密系统之一中再次加密的加密步骤；

将加密步骤中被再次加密的数字数据记录到记录媒介上的记录步骤。

12、 根据权利要求 11 的计算机可读的记录媒介，其中

在通讯步骤中接收到的加密的数字数据在有不同安全级的多个加密系统之一中被加密并且它包括表明加密系统的属性信息；

数字数据记录方法，还包括根据属性信息判断多个加密系统之一的判断步骤，其中

解密步骤根据判断步骤得到的判断结果解密加密的数字数据。

说　明　书

保护版权的数字数据记录装置和方法，其使记录在记录媒介上的加密的数字数据易于再现，以及记录了该方法的程序的计算机可读的记录媒介

本发明涉及了保护数字数据版权的数字数据记录装置，数字数据记录方法和一种计算机可读的记录媒介。

受惠于当前因特网（INTERNET）的广泛应用，音乐和被称为EC（电子商务）的传播得到了发展，例如，可用一台PC机（个人电脑）从主页下载想要的音乐数据，并用信用卡结帐。利用EC（在此称为“电子音乐传播”）通过INTERNET传播音乐的广为应用可以减少消费者去音像店，并且可完全改变以CD（光盘）传播为主的音乐的传播方式。

另外，许多人不只是在家里听音乐，他们还在上班、上学和回家的路上以及在汽车里用便携式播放机等听音乐。在这些情况下，音乐数据必须记录在便携式媒介上，如MD（迷你盘）上。

考虑到电子音乐的传播，传播公司应用各种加密系统来保护版权。更具体地说，针对制造公司，传播途径，使用方式等采用不同的最佳加密系统。在这种情况下，通过电子音乐传播系统传播的音乐数据被记录在一张MD上时，播放机需要根据所采用的加密方法对MD上的音乐数据解密。其结果是，播放机体积庞大并且很贵。这样用户就无法使用。

当通过电子音乐传播系统传播的音乐数据在记录到MD上的同时被解密时，这样播放机就不会很贵，用户就可以使用。

但是，在这种情况下，就会刺激音乐数据的非法复制，音乐数据的版权不能得到完全保护。

本发明的目的是提供一种可以保护版权的数字数据记录装置，数字数据记录方法和计算机可读的记录媒介，并可用一种廉价的数字数据播放机再现记录在记录媒介上的音乐数据。

上述的目的可由一台将数字数据记录在记录媒介上的数字数据记录装置实现，它包括：一个通过数字网络接收加密的数字数据的通讯单元；一个对通讯单元接收到的加密的数字数据进行解密的解密单元；一个包含多个加密子单元组的加密单元，它在有不同安全级的加密系统中再次加密已解密的数字数据；一个将加密单元再次加密的数字数据记录

到记录媒介上的记录单元；一个控制解密单元和加密单元的控制单元，控制单元使多个加密子单元中的一个对解密单元解密的数字数据再次加密。

其结果是，可以记录由加密单元再次加密的数字数据，并且可由播放机很容易地实现再现。由于数字数据被再次加密，所以也可以保护版权。

上述目的还可以由一种数字数据记录装置实现，其中记录在记录媒介上的数字数据由播放机再现，加密单元包括：第一加密子单元，它用根据记录媒介的标志信息产生的加密密匙再次加密数字数据；第二加密子单元，它用根据播放机的标志信息产生的加密密匙再次加密数字数据；控制单元，它判断记录媒介是否可从播放机中取出，当记录媒介可从播放机中取出时，命令第一加密子单元再次加密已解密的数字数据，当记录媒介不可从播放机中取出时，命令第二加密子单元再次加密已解密的数字数据。

其结果是，当记录媒介上的数字数据由播放机再现时，数字数据可以用根据记录媒介的标志信息产生的加密密匙对数字数据再次加密实现再现。另一方面，当记录媒介上的数字数据由特殊的播放机再现时，数字数据可以由特殊的播放机用根据特殊的播放机的标志信息产生的加密密匙对数字数据再次加密实现再现。

上述目的还可以由这种数字数据记录装置实现，它可包含通过数字网络进行财务处理的记帐单元，其中控制单元根据再次加密已解密的数字数据的加密子单元确定记帐值，并且控制记帐单元使控制单元根据确定的记帐值进行财务处理。

其结果是，可以选择加密子单元组之一在有不同安全级的加密系统中再次加密数字数据，并且使它根据所选的加密子单元付费。

上述目的还可以由这种数字数据记录装置实现，其中当加密单元未产生加密密匙时，控制单元禁止解密单元解密已加密的数字数据。

其结果是，当加密单元未产生加密密匙时，可防止数字数据被不必要地解密。

上述目的还可以由这种数字数据记录装置实现，其中加密子单元组再次加密已解密的数字数据的加密系统的安全级低于其中加密通讯单元将接收到的加密数字数据已被加密的加密系统的安全级。

其结果是，播放机可很容易地再现数字数据，并可得到较廉价的播放机。

上述目的还可以由一种数字数据记录装置实现，其中通讯单元接收到的加密的数字数据已在有不同安全级的加密系统中被加密，并包含了表明加密系统的属性信息，解密单元包含多个解密子单元组，它对在加密系统中已被加密的加密数字数据进行解密，并且控制单元根据属性信息判断加密的数字数据在哪个加密系统被加密，并控制解密单元使与判定的加密单元相对应的多个解密子单元组中的一个对加密的数字数据解密。

其结果是，即使当接收到的数字数据在有不同安全级的加密系统中被加密时，可以根据加密数字数据所在的加密系统来选择一个解密子单元对数字数据解密。

上述目的还可以由一种数字数据记录装置实现，它还可以包括一个通过数字网络进行财务处理的记帐单元，其中控制单元根据解密已加密的数字数据的解密子单元和再次加密解密的数字数据的加密子单元确定一个记帐值，并且控制记帐单元使控制单元根据确定的记帐值进行财务处理。

其结果是，可以根据数字数据的解密和再次加密来付费，并且可以保护版权。

上述目的还可以由一种将数字数据记录在记录媒介上的数字数据记录方法实现，数字数据记录方法可包括：通过数字网络接收加密的数字数据的通讯步骤；解密在通讯步骤中接收到的已加密的数字数据的解密步骤；有不同安全级的加密系统组之一对已解密的数字数据再次加密的加密步骤；及将加密步骤中再次加密的数字数据记录到记录媒介上的记录步骤。

其结果是，可以将在一个加密系统中再次加密的数字数据记录到记录媒介上，从而使数字数据很容易地由播放机再现。另外，由于数字数据被再次加密，版权也可得到保护。

上述目的还可以由这种数字数据记录方法实现，其中在通讯步骤中接收到的加密的数字数据在有不同安全级的加密系统中被加密，并且它包含了表明该加密系统的属性信息，该数字数据记录方法，还包括有根据属性信息判断出加密系统组中的一个的判断步骤，其中解密步骤根据

判断步骤中的判断结果解密已加密的数字数据。

其结果是，记录在记录媒介上的数字数据可以由任一播放机或只由特定的播放机再现。

上述目的还可以由一种计算机可读的记录媒介实现，它用于将数字数据记录在第一记录媒介上的数字数据记录装置，计算机可读的记录媒介存储了一个程序，使计算机执行以下步骤：通过数字网络接收加密的数字数据的通讯步骤；解密通讯步骤中接收到的加密的数字数据的解密步骤；在有不同安全级的加密系统组之一中再次加密已解密的数字数据的加密步骤；将加密步骤中再次加密的数字数据记录到记录媒介上的记录步骤。

其结果是，可以将在加密系统中再次加密的数字数据记录在记录媒介上，从而使数字数据可很容易地由播放机再现。另外，可以通过在没有版权保护功能的数字数据记录装置中使用该记录媒介来保护版权。

上述目的还可以由一种计算机可读的记录媒介实现，其中通讯步骤中接收到的加密的数字数据已经在有不同安全级的一个加密系统中被加密，并包含了表明该加密系统的属性信息，该数字数据记录方法还可包含一个判断步骤，它根据属性信息判决加密系统组中的一个加密系统，其中解密步骤根据判决步骤的判决结果解密已加密的数字数据。

其结果是，可以由任一播放机或特定的播放机再现记录在第一记录媒介上的数字数据。

本发明的这些和其他目的，优点和特性将通过以下的描述和与其相配的说明本发明的特殊实现方案的附图得到显现。附图中：

图 1 所示为根据本发明的第一实施方案的一种数字数据记录装置的结构；

图 2 是本发明的第一实施方案的硬件结构的外观图和根据本发明的第一实施方案的记录媒介的播放装置的外观图；

图 3 所示是根据本发明的第一实施方案购买音乐数据的主页的屏幕显示的一个实例；

图 4 所示是根据本发明的第一实施方案下载到第一记录媒介上的音乐数据的数据结构的一个实例。

图 5 所示是根据本发明的第一实施方案购买音乐数据的主页的屏幕显示的一个实例；

图 6 是说明本发明的第一实施方案的工作过程的第一流程图;

图 7 是说明本发明的第一实施方案的工作过程的第二流程图;

图 8 所示为根据本发明的第二实施方案的一种数字数据记录装置的结构;

图 9 是第二实施方案中当由信息提供商提供的数字信号被记录时,显示单元上显示的信息的一个实例;

图 10 是说明本发明的第二实施方案中的工作过程的流程图;

图 11 所示为根据本发明的第三实施方案的一种数字数据记录装置的结构;

图 12 所示是第三实施方案中的数据的属性信息;

图 13 是说明第三实施方案中的工作过程的流程图;

图 14 是说明第三实施方案中的工作过程的流程图;

图 15 所示为根据本发明的第四实施方案的数字数据记录装置的结构;

图 16 所示为根据本发明的第六实施方案的数字数据记录装置的结构;

图 17 是属性信息的一个实例;

图 18 是管理信息的一个实例;

图 19 是说明第六实施方案中的工作过程的流程图;

图 20 所示是第六实施方案中再现记录的数字数据的播放机的结构;

图 21 是说明第六实施方案中的数字数据播放机的工作过程的流程图;

图 22 所示为根据本发明的第七实施方案的数字数据记录装置的结构;

图 23 所示是第七实施方案中传送数字数据时附属在数字数据上的属性信息的数据结构的一个实例;

图 24 是第七实施方案中的工作过程的流程图;

图 25 所示是第七实施方案的另一个实例中,传送数字数据时附属在数字数据上的属性信息的数据结构的一个实例。

下面将参照附图说明根据本发明的数字数据记录装置的优选实施方案。

（第一实施方案）

图 1 所示是根据本发明的第一实施方案的一种数字数据记录装置的结构. 数字数据记录装置包括数据发送/接收单元 100，接收单元 101，第一记录媒介 102，数据提取单元 103，判决单元 104，解密单元组 105，加密系统指定单元 109，加密单元组 110，第二记录媒介 114，记录单元 115，固有信息获取单元 116，指定接收单元 117，和记帐单元 118。

可见，除了第二记录媒介 114 和记录单元 115 以外，数字数据记录装置的每个单元都可由图 2 所示的一台 PC 机（个人电脑）201 实现。例如，记录单元 115 可由一台 DVD-RAM（数字通用盘）驱动单元 202 实现，而第二记录媒介 114 可由 DVD-RAM 盘 203 实现。

数字数据记录装置接收音乐数据即通过 INTERNET 传播的加密的数字数据并将接收到的音乐数据下载到第一记录媒介 102 上。然后数字数据记录装置在解密单元组 105 中将数字数据解码，已解密的数字数据在加密单元组 110 中再次加密，并将再次加密的数字数据记录在第二记录媒介上。

可见，虽然本发明给出的是电子音乐传播的一个例子，但是传播的数字数据并不局限于音乐。传播的数字数据可以是视频数据，字符数据或者是这些类型的数据的组合。

数据发送/接收单元 100 是由一台调制解调单元和控制软件实现的通讯单元，它通过电话线连接到信息提供商的主计算机（未作图示）上。当得知想购买由接收单元 101 通过数据提取单元 103 接收到的一段音乐时，数据发送/接收单元 100 向主计算机发送购买申请。数据发送/接收单元 100 根据购买申请通过 INTERNET 从主计算机上下载音乐数据，并将下载的音乐数据记录在第一记录媒介上。同时，数据发送/接收单元 100 将购买音乐时产生的帐务信息发送给主计算机。

这里，将对信息提供商提供的信息做一说明。信息提供商设置一个站点即出售音乐数据的主页，它提供给用户购买音乐数据所必需及能引起用户兴趣的信息如音乐的曲目和价格。用户根据信息提供商所提供的信息购买想要的音乐数据。

图 3 所示的是信息供应商提供的出售音乐数据的主页的一个实例。该信息包括曲目 301，演唱者 302，时间 303 和价格 304。曲目 301 和演唱者 302 表示一段音乐数据的曲目和演唱者。时间 303 表示记录（播

放）一段音乐数据所需的时间，价格 304 表示一段音乐数据的售价．用户根据这些信息选择一段音乐并通过接收单元 101 向数据发送/接收单元 100 提出购买申请．当然，信息提供商提供的信息并不局限于图 3 所示的字符信息．信息还可以是图象如图片和试听的音乐数据．

接收单元 101 包括键盘和鼠标，它接收用户的购买申请，用户在 PC 机的屏幕上看到图 3 中所示的信息．收到的购买申请通过数据提取单元 103 发送给数据发送/接收单元 100．

第一记录媒介 102 由 PC 机上的硬盘实现，它存储音乐数据即由数据发送/接收单元 100 接收到的加密的数字数据．同时，当下载的音乐数据被记录在第二记录媒介 114 上时，由计帐单元 118 将加密的计帐信息记录到第一记录媒介 102 的安全区中．

图 4 所示是第一记录媒介 102 上存储的下载的音乐数据即信息提供商提供的音乐数据的数据结构的一个实例．信息提供商提供的音乐数据主要包括含有音乐数据的曲目，演唱者和价格的属性信息 401 和音乐数据单元 402 即音乐数据本身．

属性信息 402 包括 ISRC（国际标准记录码）信息 403，曲目 404，演唱者 405，价格 406，信息提供商 407，和加密格式 408．下面将说明属性信息 401．

ISRC 信息 403 是给每段音乐数据设置的特性信息，它包括一个国家代码（两个 ASCII（国际交换美国标准码）字符），一个所有权人代码（三个 ASCII 字符），记录年份（两位数字）和一个序列号（5 位数字）．曲目 404 是表示音乐数据的曲目的字符信息，演唱者 405 是表示音乐数据的演唱者的字符信息．价格 406 是表示音乐数据的价格的信息．可见，价格 406 是当使用本发明的数字数据记录装置将下载的音乐数据记录到第二记录媒介 114 上时，所要的总费用．

信息供应者 407 表示的是音乐数据的供应商或版权所有者的信息，即表示当用户用数字数据记录装置记录音乐数据时，总费用的接受者．

加密格式 408 是表示下载的音乐数据以何种加密格式被加密的信息，因为音乐数据的加密格式与信息提供者相关．例如，当信息提供商 A，B 和 C 提供音乐数据时，信息提供商 A 提供的音乐数据以格式 A 加密，信息提供商 B 提供的音乐数据以格式 B 加密，信息提供商 C 提供的音乐数据以格式 C 加密．可见本实施方案中的发明的主要目的是当信息提供

商提供的信息以不同的格式加密时，用播放装置很容易解密的加密格式将数据变换到第二记录媒介 114 上并保护版权。这里不详细说明加密算法。

在属性信息 401 中，价格 406 和信息提供商 407 必要时也加密，因为价格 406 和 407 的泄露可给信息提供商造成损失。

当接收到加密系统指定单元 109 发出的提取数字数据的指令时，数据提取单元 103 从第一记录媒介 102 上提取属性信息 401，并将属性信息 401 通知给计帐单元 118。同时，数据提取单元 103 将加密格式 408 的信息给判决单元 104。可见，当属性信息 401 中的价格 406 被加密时，数据提取单元 103 将解密单元组 105 解密后的价格 406 通知给计帐单元 118。然后，数据提取单元 103 从第一记录媒介 102 提取音乐数据部分 402，并将提取出的音乐数据部分 402 输出给判决单元 104。如上所述，数据提取单元 103 提取的数据已在信息提供商特定的加密系统中加密。

判决单元 104 根据数据提取单元 103 给出的加密格式 408 的信息判断音乐数据输出给哪个解密单元。

解密单元组 105 包括“N”个解密单元。第一解密单元 106 解密以格式 A 加密的数字数据，第二解密单元 107 解密以格式 B 加密的数字数据，第 N 解密单元 108 解密以格式 N 加密的数字数据。第一，第二和第 N 个解密单元 106，107 和 108 都包含不同信息提供商的解密模块。

例如，当加密格式 408 的信息表示为格式 B 时，判决单元 104 将音乐数据中的音乐数据部分 402 的数字数据输出给第二解密单元 107。第二解密单元 107 解密输入的数字数据并将解密的数字数据输出给加密系统指定单元 109。

当第一，第二和第 N 解密单元 106，107 和 108 之一需要一个解密钥匙来解密加密的数据时，数据发送/接收单元 100 根据数据的加密系统得到一个解密钥匙来解密数据。第一，第二和第 N 个解密单元 106，107 和 108 之一解密根据信息提供商而在不同的加密系统中加密的数据。

当接收到指定接收单元 117 发出的加密系统的类型的指定信息时，加密系统指定单元 109 根据指定信息命令固有信息获取单元 116 获取固有信息。当固有信息获取单元 116 得到固有信息时，加密系统指定单元 109 命令数据提取单元 103 提取音乐数据。当固有信息获取单元 116 未

得到与指定信息相关的固有信息时，加密系统指定单元109显示单元（未作图示）上显示出不能用指定的加密系统再次加密数据。同时，当未从指定接收单元117中接收到加密系统类型的指定信息时，加密系统指定单元109命令固有信息获取单元116根据第二记录媒介114的属性获取固有信息。当接收到固有信息获取单元116发出的获取固有信息的命令时，加密系统指定单元109命令数据提取单元103提取音乐数据。当得知不能获取固有信息时，加密系统指定单元109产生随机数。

当接收到指定接收单元117发出的加密系统类型的指定命令时，加密系统指定单元109根据指定信息选择一个加密单元。当接收第一，第二和第N解密单元106，107和108中输出的解密的数字数据时，加密系统指定单元109将固有信息获取单元116给出的固有信息及解密的数字数据送给所选的加密单元。

当未接收到指定接收单元117发出的加密系统类型的指定信息时，加密系统指定单元109根据固有信息获取单元116给出的固有信息的类型选择一个加密单元。当接收第一，第二和第N解密单元106，107和108之一输出的解密的数字数据时，加密系统指定单元109将固有信息获取单元116给出的固有信息及解密的数字数据送给所选的加密单元。同时，当接收到固有信息获取单元116发出的不能获取到固有信息的信息时，加密系统指定单元109将数字数据和已产生的随机数输出给加密单元组之一。

加密单元组110包括“N”个加密单元，第一，第二，...，第N加密单元111，112，...，113。加密单元111，112，...113均用不同的加密密匙再次加密所得到的数字数据。更具体的说，第一加密单元111用根据固化在第二记录媒介114上的标志信息所产生的一个加密密钥再次加密数据。第二加密单元112用根据在回放第二记录媒介114的播放机（未作图示）上固有的标志信息所产生的加密密匙再次加密数据。第N加密单元113用根据随机数所产生的加密密匙再次加密数据。每个加密密匙的数据大小均设置为小于记录在第一记录媒介102上的加密的数字数据的加密密匙的数据大小。

当记录在第二记录媒介114上的再次加密的数字数据的加密密匙的数据大小相对小时，解密数字数据就相对容易。其结果是，解密数字数据从而再现数字数据的播放机所必需的结构就简单，从而减小了播放机

的价格。

例如，当没有接收到来自指定接收单元 117 的指令而得到来自固有信息获取单元 116 的第二记录媒介 114 的属性信息时，加密系统指定单元 109 将第二记录媒介 114 的属性信息送给第一加密单元 111。第一加密单元 111 根据所给的属性信息产生一个加密密匙，改写由加密系统指定单元 109 所给出的音乐数据的属性信息 401 中的加密格式 408，并且用所产生的加密密钥再次加密音乐数据。第一加密单元 111 将再次加密的数字数据送给记录单元 115。

当接收到来自指定接收单元 117 的回放第二记录媒介 114（未作图示）的播放机的固有信息再次加密数据的指令时，加密系统指定单元 109 命令固有信息获取单元 106 获取固化在播放机中的标志信息。当得到固有信息获取单元 116 发出的在播放机中固有的标志信息时，加密系统指定单元 109 将所得到的标志信息和来自解密单元组 105 的已解密的数字数据送给第二加密单元 112。

第二加密单元 112 根据加密系统指定单元 109 发出的标志信息产生一个加密密钥，用所产生的加密密匙再次加密数字数据，并将再次加密的数字数据送给记录单元 115。在没有接收到指定接收单元 117 发出的指令的情况下，属性信息 401 中的加密格式 408 的内容将被改写。

第二记录媒介 114 包括 DVD-RAM 盘（图 2 中所示），MD 和根据播放机（未作图示）的类型为可移去或不可移去的小型半导体存储单元，等等。加密单元组 110 再次加密的音乐数据通过由记录单元 115 记录在第二记录媒介 114 上。例如，当数字数据被记录在 DVD-RAM 盘 203 上时，DVD-RAM 盘 203 插入 DVD 播放机 204 中放出音乐，如图 2 中所示。

例如，记录单元 115 可由图 2 中所示的 DVD-RAM 驱动单元 202 实现。记录单元 115 将来自加密单元组 110 的数字数据记录到第二记录媒介 114 上。当完成记录时，记录单元 115 将记录完成的信息送给计帐单元 118。

当加密系统指定单元 109 命令获取第二记录媒介 114 上内部固有的标志信息时，例如，当第二记录媒介 114 是 DVD-RAM 时，固有信息获取单元 116 读取写在 BCA（Bursting Cutting Area）上的信息，并将读到的信息送给加密系统指定单元 109。可见，每个第二记录媒介 114 在产生时就已经记录有其不同的内部标志信息，所以普通用户的操作不可

能读出或改写标志信息。

根据标志信息产生一个加密密匙，用该加密密匙加密的数字数据被记录在DVD-RAM盘上。其结果是，即使有人怀有恶意的企图用位拷贝的方法将DVD-RAM盘上的内容复制到另一记录媒介上并企图回放该记录媒介上复制的数据，由于该记录媒介上的解密密匙的信息与DVD-RAM盘上的不同，所以复制的数据不能被正常解密。这样，音乐数据的版权得到了完全的保护。

同时，当加密系统指定单元109命令获取在第二记录媒介114所在的播放机中固有的标志信息时，固有信息获取单元116读取播放机的标志信息并将所读的标志信息送给加密系统指定单元109。每个播放机在其生产时设置了不同的内部标志信息，所以普通用户的操作不能读出或改写该标志信息。其结果是，当根据标志信息再次加密数据时，再次加密的数据只能由特定的播放机在再现。

可见，当固有信息获取单元116不能获取由加密系统指定单元109指定的内部标志信息时，即第二记录媒介114和播放机上没有设置标志信息时，固有信息获取单元116告知加密系统指定单元109没有获取指定的内部标志信息。

当接收到获取内部标志信息的指令而没有内部标志信息类型的指令时，固有信息获取单元116判断第二记录媒介114是一种可从播放机中取出的记录媒介如DVD-RAM盘还是固定在播放机中的记录媒介如小型半导体存储单元。当第二记录媒介114是可移去的记录媒介时，固有信息获取单元116读取第二记录媒介114的内部标志信息，并将所读的内部标志信息告知给加密系统指定单元109。同时，当第二记录媒介114是不可移去的记录媒介时，固有信息获取单元116读取播放机的内部标志信息，并将所读的内部标志信息告知给加密系统指定单元109。当没有获取到标志信息时，固有信息获取单元116告知加密系统指定单元109没有获取到标志信息。

指定接收单元117由PC的键盘和鼠标实现。指定接收单元117接收用户给出的加密系统的类型的指令，并将加密系统的类型告知加密系统指定单元109。

图3中的主页信息只显示了一种价格，图5中的主页显示了两种价格即价格（1）501和价格（2）502。

价格（1）501表示记录的同时根据在第二记录媒介114中固有的标志信息再次加密数字数据的价格，价格（2）502表示记录的同时根据在回放第二记录媒介114的播放机中固有的标志信息再次加密数字数据的价格。可见，价格（1）501和（2）502均可由信息提供商任意设置。

用户使用指定接收单元117，根据第二记录媒介114的使用格式并参考图5中所示的音乐及价格信息命令以想要的加密格式加密数字数据。例如，当数字数据由特定的播放机回放时，即第二记录媒介114不由其他的播放机回放时，用户根据在特定的播放机中固有的标志信息命令再次加密数字数据。如图5中的价格（2）所示，当根据播放机的标志信息再次加密数据时，价格通常较便宜。这是因为再次加密的数据不能在其他的播放机上回放，所以其自由度低于根据在第二记录媒介114中固有的标志信息加密的自由度。当数字数据可由任一播放机回放时，用户根据在第二记录媒介114中固有的标志信息命令再次加密数字数据。

虽然指定接收单元117和接收单元101是集成在一起，但是为了方便说明，指定接收单元117和接收单元101被描述为分立的部分。

计帐单元118接收数据提取单元103发出的音乐数据的属性信息401的信息并存储接收到的属性信息401。当得知再次加密的数字数据由记录单元115记录在第二记录媒介114上时，计帐单元118参照属性信息401中的价格406来决定费用并将所定的费用和属性信息401一起写入第一记录媒介102上的一个安全区中作为计帐信息。

当价格406包括图5中所示的价格（1）501和（2）502时，根据送给计帐单元118的第一至第N加密单元111-113中的一个加密单元，即加密系统指定单元109指定的所用的加密单元来决定费用。

这里，将参照图6和7中的流程图说明本实施方案的工作过程。

接收单元101接收来自用户的主页申请，数据发送/接收单元100读取音乐数据的供应商提供的一个主页，而数据提取单元103将主页（参见图3和5）显示在显示单元（未作说明）上（步骤S602）。

数据提取单元103等待接收单元101发出的购买用户指定的音乐数据的指令，并命令数据发送/接收单元100接收指定的音乐数据（步骤S604）。当接收音乐数据时，数据发送/接收单元100将接收到的音乐数据下载到第一记录媒介102上（步骤S606）。

观看显示的主页，用户根据第二记录媒介 114 的使用方式使用指定接收单元 117 输入加密系统的类型。

加密系统指定单元 109 判断指定接收单元 117 是否将指定的加密系统的类型告知加密系统指定单元 109（步骤 S608）。当得到加密系统的类型的指定信息时，加密系统指定单元 109 命令固有信息获取单元 116 获取指定的类型的加密系统所用的固有信息（步骤 S610）。加密系统指定单元 109 判断固有信息获取单元 116 是否已告知不能获取固有信息（步骤 S612）。当得知不能获取固有信息时，加密系统指定单元 109 使显示单元（未作说明）显示不能根据所选类型的加密系统再次加密音乐数据（步骤 S614）并完成整个过程。同时，当得到所选加密系统的类型的固有信息时，加密系统指定单元 109 命令数据提取单元 103 提取数字数据。

数据提取单元提取记录在第一记录媒介 102 上的音乐数据（步骤 S616）。

在步骤 S608 中，当判断到指定接收单元 117 没有将指定的加密系统的类型的信息告知加密系统指定单元 109 时，加密系统指定单元 109 命令固有信息获取单元 116 获取没有指定固有信息的类型的固有信息（步骤 S618）。

固有信息获取单元 116 判断第二记录媒介 114 的属性，即判断播放机中的第二记录媒介是否为可移去的。当第二记录媒介 114 是可移去时，固有信息获取单元 116 获取第二记录媒介 114 的标志信息，而当第二记录媒介 114 是不可移去的时，固有信息获取单元 116 获取播放机的标志信息（步骤 S620）。

当固有信息获取单元 116 发出内部（标志）信息时，或当未获取到固有信息时（步骤 S622），加密系统指定单元 109 命令数据提取单元 103 提取数字数据。过程进到步骤 S616。

然后，判断单元 104 参照数据提取单元 103 提取的音乐数据的属性信息 401 中的加密格式 408 并判断解密单元组 105 中的第一至第 N 解密单元 106 至 108 中的哪一个解密音乐数据（步骤 S702）。

由判断单元 104 判断出第一至第 N 解密单元 106 至 108 中的一个解密单元解密通过判断单元 104 输入的数字数据并将解密的数字数据输出给加密系统指定单元 109（步骤 S704）。

加密系统指定单元109根据来自固有信息获取单元116的固有信息（包括不能获取固有信息的 信息)选择加密单元组110中的第一至第N加密单元111至113之一，并将固有信息（在不能获取固有信息的情况下产生的随机数）和解密的数字数据送给所选的加密单元（步骤S706）。

加密单元根据内部（标志）信息（在产生随机数的信息的情况下根据随机数）产生一个加密密匙，并用产生的加密密匙再次加密数字数据。同时，改写属性信息401中的加密格式408的内容（步骤S708）。

记录单元115将已由第一至第N加密单元111至113中的一个加密单元发送的数字数据记录在第二记录媒介114上（步骤S710）。当完成记录时，记录单元115将记录完成的信息告知给计帐单元118。

当接收来自记录单元115的信息时，计帐单元118根据来自数据提取单元 103 的价格 406 等得出费用值并将费用值记录在第一记录媒介102上（步骤S712）以完成整个过程。

在本实施方案中，解密单元组105包括针对不同信息提供商的解密模块（第一至第N解密单元106至108）。解密单元组可包括针对不同音乐数据的质量的不同的解密单元，例如，针对24位的LPCM（线性脉码调制）的数字数据，MP3（动画专家组1音频播放机3）等等。更具体的说，即高质量的24位LPCM可设置为难于解密的加密的数字数据，普通的MP3可设置不太难于解密的加密的数字数据，第一解密单元106可以解密24位LPCM格式的数字数据，而第二解密单元107可以解密MP3格式的数字数据。

在本实施方案中，加密单元组110包括针对不同类型的固有信息的第一至第N加密单元111至113。这些加密单元可对应不同的音乐数据的质量。详细地说，第一加密单元111再次加密由第一解密单元106解密的数字数据，第二加密单元112再次加密由第二解密单元107解密的数字数据，而第N加密单元113再次加密由第N解密单元108解密的数字数据。这样，用于第一加密单元111加密的加密密匙的数据长度大于用于第二加密单元112的加密密匙的数据长度，而于第二加密单元112的加密密匙的数据长度大于用于第N加密单元113的加密密匙的数据长度。计帐单元根据解密数字数据的解密单元和再次加密数字数据的加密单元得出数字数据的计帐值。其结果是，数字数据的质量越高，越能保证保护版权。这样，信息供应商可以对质量较高的音乐数据设置较高的

价格。

图 1 中所示是根据本实施方案的数字数据记录装置的结构。可以在计算机可读的记录媒介如软盘上记录一个程序使计算机实现数字数据记录装置的各部分的功能，并通过将计算机可读的记录媒介应用于无版权保护功能的数字数据记录装置来保护版权。

在本实施方案中，当用户申请购买数字化数据时，从主机下载数字数据。不论用户是否购买，可以将音乐数据或只是属性信息暂时记录在用户的 PC 机中的第一记录媒介上，并购买已记录在第一记录媒介 102 上的数字数据。

在本实施方案中，属性信息 401 和音乐数据单元 402 是分别描述的，而属性信息 401 可以用水印（电子水印）技术嵌入音乐数据 402 的数字数据中。

在本实施方案中，没有特别说明经过加密系统指定单元 109 的在解密单元组 105 和加密单元组 110 之间输入和输出的数据。可以通过在授权之后发送数据或在一个芯片上实现解密单元组 105，加密系统指定单元 109 和加密单元组 110 来防止解密数据的泄露以达到安全的目的。

另外，在本实施方案中，计帐信息记录是在第一记录媒介 102 的一个安全区中，计帐信息还可以记录在另一记录媒介上，如一个 IC 卡上。

在本实施方案中没有说明计帐的时序。可以设定当数字数据记录在第二记录媒介 114 上时，调制解调单元被连接到主机上，还可以设定当费用值达到了一个设定值时，调制解调单元被自动连接到主机上，或者可以设定当记录计帐信息超过了一个设置的时间段时，调制解调单元被连接到主机上。

另外，在本实施方案中信息供应商只提供音频信息，而其还可以提供视频信息，音频信息，字符信息，视频信息、音频信息、和字符信息的组合信息。

（第二实施方案）

图 8 所示是根据本发明的第二实施方案的数字数据记录装置的结构。该数字数据记录装置一般由一台个人计算机实现。该数字数据记录装置包括数据发送/接收单元 2101，第一记录媒介 2101，数据提取单元 2103，加密系统判断单元 2104，第一解密单元 2105，第二解密单元

2106，第三解密单元 2107，加密单元 2108，记录单元 2109，第二记录媒介 2110，输入单元 2111，显示单元 2112 和记录媒介固有信息获取单元 2113. 解密单元组 2115 包括第一、第二、第三解密单元 2105、2106、2107，解密单元的数量不局限于三个. 解密单元组可包括多个解密单元。

在本实施方案中，记录的数据是通过 INTERNET 传播的音乐数据. 音乐数据在不同的供应商的不同的加密系统中被加密。

信息供应商提供用户在购买时所需音乐数据和包括音乐曲目，价格，复制控制信息等信息（在本例中为“属性信息”），并其全部或部分引起用户的兴趣. 在本实施方案中，假设属性信息和音乐数据是分别提供的。

数据发送/接收单元 2101 是由一台调制解调单元实现的一个通讯单元，它通过电话线连接到信息供应商的主机（未作图示）上。数据发送/接收单元 2101 获取的属性信息记录在第一记录媒介 2102 上，其全部或部分的属性信息显示在显示单元 2112 上。图 9 是在显示单元 2112 上显示的信息的一个实例。其显示的信息是如曲目 2201，曲目代码 2202，演唱者 2203，数据来源 2204. 这里，曲目 2201 和演唱者 2203 表示一段音乐数据的曲目和演唱者。曲目代码 2202 是区分一段音乐数据和另一段音乐数据的标志。例如对曲目代码 2202 来说，加上一段 ISRC（国际标准记录码）信息。根据该信息，用户选择一段想要的音乐并用输入单元 2111 发送购买申请。数据来源 2204 是确定一段音乐数据的位置的一个 URL（均匀源定位器）. 当 ISRC 信息加到曲目代码 2202 上时，数据来源可由曲目代码 2202 确定。

输入单元 2111 由鼠标，键盘及类似物实现. 输入单元 2111 接收购买音乐的指令，即记录指令并将该指令告知给数据发送/接收单元 2101. 用户根据显示在显示单元 2112 上的信息用鼠标点击所选的音乐的曲目等命令记录音乐数据.

当接收到记录音乐数据的指令时，数据发送/接收单元 2101 通过电话线从供应商的主机上下载想要的音乐数据. 这时，音乐数据的位置根据属性信息中的 URL 确定. 下载的音乐数据被记录在第一记录媒介 2102 上.

第一记录媒介 2102 一般是 PC 机中的硬盘，它记录未解密的想要的

音乐数据。其结果上，在下面的工作过程中数字数据记录装置不需连接到供应商的主机上。

数据提取单元 2103 从第一记录媒介 2102 中提取记录的音乐数据。同时，用户根据显示单元 2112 上显示的信息，其信息大部分与图 9 中显示的信息相同，选择要记录到第二记录媒介 2110 上的音乐数据。数据提取单元 2103 提取的数据已经在信息供应商的加密系统中加密，所以加密系统判断单元 2104 判决一个相应的系统来解密该数据。例如，表明数字数据的加密系统的信息加在数据前部，或用属性信息表明加密系统，加密系统判断单元 2104 根据该信息判决加密数据。

第一、第二和第三解密单元 2105、2106 和 2107 表示根据不同的信息供应商在不同的系统中解密数字数据。解密单元的数量不局限于三个。加密系统判断单元 2104 选择一个相应的解密单元，所选的解密单元解密加密的数据。详细地说，加密系统判断单元 2104 获取或产生一个与获取的数据所在的加密系统相对应的解密密匙，所选的解密单元用该加密密匙解密数据。其结果是，在不同加密系统中加密的数据由一个解密单元解密。

加密单元 2108 再次加密已解密的数据。在本实施方案中，在记录媒介上固有的信息被设为用作加密时的加密密匙信息。根据在记录媒介中固有的信息加密的方法在《日本公开专利申请 NO.05-257816》中已描述了，所以这里不再作详细说明。

记录媒介固有信息获取单元 2113 根据来自加密单元 2108 的指令从第二记录媒介 2110 中提取固有信息，并将提取的固有信息传送给加密单元 2108。

加密单元 2108 用记录媒介固有信息获取单元 2113 获取的固有信息作为加密密匙再次加密数据。

这里，将说明在第二记录媒介 2110 上固有的信息。

每个第二记录媒介 2110 有不同的内部标志信息。当第二记录媒介 2110 是 DVD-RAM 时，内部标志信息是写在 BCA 中的信息。每张盘在 BCA 中的信息不同，信息在制造时被存储并且不能改写。其结果是，即使用户怀有恶意的企图用位拷贝的方法将盘上的内容复制到另一记录媒介上时，由于另一记录媒介的解密密匙信息不同于该盘的信息，所以拷贝的数据不能被解密。这样，保证了数据的版权得到保护。

记录单元 2109 将将再次加密的数据记录到第二记录媒介 2110 上。

已经说明了数字数据记录装置的结构，下面参照图 10 中的流程图说明其工作过程。

数据发送/接收单元 2101 下载属性信息（步骤 S2301），并等待用户发生的记录数字数据的指令（步骤 S2302）。数据发送/接收单元 2101 下载指定的数字数据并将数字数据记录在第一记录媒介 2102（步骤 S2303）。判断下载的数字数据的加密系统，命令第一、第二、第三解密单元 2105，2106 和 2107 中相应的一个解密数据（步骤 S2304）。第一、第二和第三解密单元 2105，2106 和 2107 之一解密数据（步骤 S2305）。当输入已解密的数据时，加密单元 2108 获取记录媒介固有信息获取器 2113 发出的第二记录媒介 2110 的内部信息（步骤 S2306）。利用获取的固有信息作为加密密匙的一部分产生一个加密密匙，加密单元 2108 再次加密数据（步骤 S2307）。记录单元 2109 将再次加密的数据记录到第二记录媒介 2110 上（步骤 S2308），就此完成整个过程。

这里已经说明了根据本发明的第二实施方案的数字数据记录装置。

下面将说明根据本发明的第三实施方案的数字数据记录装置。

（第三实施方案）

图 11 所示是根据本发明的第三实施方案的数字数据记录装置的结构。该数字数据记录装置一般由一台 PC 机实现。该数字数据记录装置包括数据发送/接收单元 2101，第一记录媒介 2102，数据提取单元 2103，加密系统判断单元 2104，解密单元组 2115，属性信息获取单元 2401，拷贝控制信息检测判断单元 2402，拷贝控制信息转换单元 2403，帐目信息计算单元 2404，加密单元 2108，第二记录媒介 2110，输入单元 2111，显示单元 2112，和记录媒介固有信息获取单元 2113。

在第二和第三实施方案中的数字数据记录装置中相同的部分用相同的标号，下面不再说明这些部分。

图 12 所示是本实施方案中的数据的属性信息。图 12 中的属性信息除图 9 中所示的属性信息之外包括复制控制信息 2501 和帐目信息 2502。复制控制信息 2501 表示可以再次复制或复制数据的次数。例如，用数字表示数据可以再次复制的次数时，可以用对应于“无数次”“只能复制（不能再次复制）”“不能复制”等的值表示。另外，可以复制数

据的次数是一个大于“0”的整数。详细地说，“不能再次复制”表示记录在第二记录媒介2110上的数字数据不能再次复制。“无数次”表示数据可以任意次复制。复制次数如“两次复制”表示数据可以复制到两个第二记录媒介2110上。

属性信息获取单元2401从第一记录媒介2102中获取相应的要再现的数据的属性信息。在本实施方案中，提取复制控制信息和帐目信息2502。由于属性信息包括版权保护信息和帐目信息2502，所以可以将属性信息记录在第一记录媒介2102上的一个安全区中使普通用户的操作不能存取该属性信息。

复制控制信息检测判断单元2402从属性信息中提取复制控制信息以获取表明是否允许复制或再次复制的信息和数据可以复制或再次复制的次数。

当允许复制或再次复制时，复制控制信息转换单元2403必须改写复制控制信息。例如，当禁止再次复制时，复制控制信息转换单元2403改变复制控制信息2501的值以禁止再次复制。当数据复制的次数有限时，复制控制信息转换单元2403改变其值使该值比允许复制的次数小“1”。

当设置允许复制次数时，重要的数据是将第一记录媒介2102上的数据记录在第二记录媒介2110上的次数．改写复制控制信息就是改写记录在第一记录媒介2102上的数据。其结果是，记录在第一记录媒介2102上的允许复制的次数以“1”递减，记录到第二记录媒介上的允许复制的次数是“0”。

帐目信息计算单元2404从属性信息获取单元2401得到的属性信息中获取想要的音乐数据的计帐信息，根据计帐信息计算出费用值，并将计算出的费用值记录在第一记录媒介2102中的一个安全区中。

上面已经说明了数字数据记录装置的结构，下面将参照图13和14中的流程图说明其工作过程。

首先，数据发送/接收单元2101下载属性信息（步骤S2601），等待来自用户的记录数字数据的指令（步骤S2602），下载所选的数字数据，并将下载的数字数据记录在第一记录媒介2102（步骤S2603）上。然后，数据发送/接收单元2101从属性信息获取单元2401中获取将要记录的数据的属性信息（步骤S2604）。复制控制信息检测判断单元2402

判读属性信息中的复制控制信息 2501 并判断是否允许复制（步骤 S2605）。当允许复制时，获取允许再次复制或复制的次数，并必须由复制控制信息变换单元 2403 改写得到的次数（步骤 S2606）。当不允许复制时，中断整个过程（步骤 S2607）。然后，判断加密系统，命令解密单元组 2115 中相应的解密单元解密数字数据（步骤 S2608）。第一、第二和第三解密单元中的一个解密单元解密数字数据（步骤 S2609）。解密后，根据属性信息获取单元 2401 获取的计帐信息计算费用值（步骤 S2610）。

接收到解密数据后，加密单元 2108 从记录媒介固有信息获取单元 2113 中获取第二记录媒介 2110 的固有信息（步骤 S2611）。产生的加密密匙中有一部分是获取的固有信息，加密单元 2108 再次加密数据（步骤 S2612）。记录单元 2109 将再次加密的数据记录在第二记录媒介 2110 上（步骤 S2613），整个过程就此完成。

至此，完成了对本发明的第三实施方案的说明。

（第四实施方案）

下面将说明根据本发明的第四实施方案的数字数据记录装置。该数字数据记录装置不同于第二实施方案中的数字数据记录装置，其不同在于加密密匙信息及其在第二数字数据记录装置 2801 中包括固有信息获取/发送单元 2803，记录单元 2109 和第二记录媒介 2110。图 15 所示是根据本发明的第四实施方案的数字数据记录装置的结构。该数字数据记录装置包括第一和第二数字数据记录装置 2800 和 2801。

第一数字数据记录装置 2800 包括数据发送/接收单元 2101，第一记录媒介 2102，数据提取单元 2103，加密系统判断单元 2104，解密单元组 2115，加密单元 2108，输入单元 2111，显示单元 2112，固有信息获取单元 2802。

第二数字数据记录装置 2801 包括固有信息获取/发送单元 2803，记录单元 2109，第二记录媒介 2110。

可见第四实施方案中数字数据记录装置与第二实施方案相同的部分采用了相同的标号标识，下面不再说明这些部分。

当在解密单元组 2115 中解密的数据输入到加密单元 2108 时，固有信息获取单元 2802 命令第二数字数据记录装置 2801 中的固有信息获取

/发送单元 2803 发送固有信息。固有信息获取/发送单元 2803 获取在第二数字数据记录装置 2801 中的第二记录媒介 2110 上固有的标志信息，或者在第二数字数据记录装置 2801 中固有的标志信息，并将获取的标志信息发送给固有信息获取单元 2802。

加密单元 2108 利用在第二数字数据记录装置中固有的第二记录媒介 2110 上的标志信息，在第二数字数据记录装置 2801 中固有的标志信息，或者这些标志信息的组合信息产生一个加密密匙，并再次加密已解密的数据，并将再次加密的数据输出给第二数字数据记录装置 2801。第二数字数据记录装置 2801 中的记录单元 2109 将再次加密的数据记录到第二记录媒介 2110 上。

当第二记录媒介 2110 是固定在第二记录装置 2801 中时，由固有信息获取/发送单元 2803 获取并发送的固有信息是在第二数字数据记录装置 2801 固有的标志信息，当第二记录媒介 2110 是可从第二数字数据记录装置 2801 中取出的时，获取并发送的固有信息是在第二数字数据记录媒介 2110 中固有的标志信息或是在第二数字数据记录装置 2801 固有的标志信息和在第二数字数据记录媒介 2110 中固有的标志信息的组合信息。其结果是，可以得到较灵活的加密系统。

至此，完成了对本发明的第四实施方案的说明。

（第五实施方案）

这里，将说明根据本发明的第五实施方案的数字数据记录装置。该数字数据记录装置与第二、第三和第四实施方案中的基本相同。下面将参照用于第四实施方案的图 15 中的方框图说明本数字数据记录装置。第五实施方案中的数字数据记录装置与第四实施方案中的不同之处在于在记录的同时采用一个与第二记录媒介相对应的加密系统。更具体地说，由于对 DVD-RAM 和半导体存储单元来说，写加密数据时的数据的最小单位或者数据量的单位不同，所以固有信息获取单元 2802 从固有信息获取/发送单元 2803 中获取媒介的信息以最佳的数据单位再次加密数据。其结果是，其包含多个加密单元 2108 并且将固有信息和媒介信息都发送给一个相对应的加密单元。这样，不只是 DVD-RAM，半导体存储单元，IC 卡和硬盘也可用作第二记录媒介 2110。

至此，完成了对本发明的第五实施方案的说明。

对第二至第五实施方案的说明是以期望有最佳效果的系统为例的。这些实施方案可以在本发明的基本原则范围内变化。下面将给出一些变化的实施方案的实例。

在第二至第五实施方案中，当用户申请购买数字数据时，数字数据从主机下载。不论购买与否，可以将数字数据记录在用户的 PC 机中的第一记录媒介 2102 上，然后申请购买记录在第一记录媒介 2102 上的数字数据。

在第二至第五实施方案中，属性信息中表明了复制控制信息。可以用水印技术将复制控制信息嵌入数字数据中。

已经说明过的一点是，计帐信息记录在第一记录媒介 2102 上的一个安全区中，可以提供另一记录媒介如 IC 卡代替第一记录媒介 2102 记录计帐信息。

第二至第五实施方案中信息提供商提供的信息是音频信息，而信息不局限于音频信息。信息可以是视频信息、音频信息、字符信息，或者是视频、音频和字符信息的组合信息。

（第六实施方案）

图 16 所示是根据本发明的第六实施方案的数字数据记录装置的结构。

该数字数据记录装置包括通讯单元 3101，记录媒介 3102，接收数据记录/判断单元 3103，显示单元 3104，输入操作单元 3105，记录媒介固有信息获取单元 3106，加密单元 3107，记录单元 3108，财务信息记录单元 3109，财务信息记录媒介 3110，计帐单元 3111。该数字数据记录装置由一台 PC 机实现。

通讯单元 3101 是由一台调制解调单元实现。它通过电话线连接到数据供应商和财务中心（未作说明）的主机（未作说明）上。当接收来自主机的数字数据和属性信息时，通讯单元 3101 将接收到的信息告知接收数据记录/判断单元 3103。

当接收到来自财务中心的费用查询时，通讯单元 3101 将查询信息告知计帐单元 3111。当计帐单元 3111 得到财务信息时，通讯单元 3101 通过电话线将财务信息告知给财务中心。

假设本实施方案中数据供应商提供的数字数据是音乐数据。假设提

供的音乐数据是加密的数字数据，一个信息标志加在一段数字数据上。假设一段音乐的标志是区分一段音乐和另一段音乐的曲目代码。

假定将属性信息加在一段数字数据上。属性信息包括表明费用和数字数据供应商的信息。

图 17 是属性信息的一个实例。属性信息 3201 包括曲目 3202，演奏者（演唱者）3203，曲目代码 3204，记录费用 3205，复制一次的费用 3206，可复制的最大次数 3207，加密情况 3208 和复制许可 3209。

曲目 3202 和演奏者 3203 显示在显示单元 3104 上。用户根据曲目 3202 和演奏者 3203 命令复制（复制）数字数据。每段音乐的曲目代码是唯一的，以区分一段音乐和另一段音乐。例如，一个 ISRC 用作曲目代码 3204。ISRC 包括国家代码（二个 ASCII 字符），一个用户代码（三个 ASCII 字符），一个录制年份（两位数字），一个序列号（5 位数字）。

记录费用 3205，复制一次的费用 3206，可录制的最大次数 3207 等包含于一个帐目标准数据中，作为计算一段音乐的费用的信息。

记录费用 3205 表示当通讯单元 3101 接收到的数字数据记录在记录媒介 3102 上的费用。复制一次的费用 3206 表示复制记录在记录媒介 3102 上的数字数据一次的费用。可复制的最大次数 3207 表示可以复制记录在记录媒介 3102 上的数字数据的最大次数。例如，当可复制的最大的次数 3207 是“100”时，数字数据最多可复制 100 次。可见，可以设置可复制的最大次数 3207 使复制的次数达到某个次数后不需增加费用。

加密情况 3208 是一个标识位，表示通讯单元 3101 接收到的数字数据是否为加密的数据。

复制许可 3209 是由用户记录的一个标识位，它表示是否允许将接收到的音乐数据记录到记录媒介 3102 上。例如，“只许一次”表示只许音乐数据被记录一次，而“允许”表示音乐数据允许被记录任意次。

本发明的主要目的是当音乐数据记录（复制）在记录媒介 3102 上时保护接收到的音乐数据的版权，所以下面将简要说明只允许收听音乐数据的情况。在这种情况下，复制许可 3209 是“不允许”。图 16 中所示的结构中未包括解密单元和输入单元，通讯单元 3101 接收到的数字数据由解密单元解密，并由输入单元输入音乐。这时，帐目标准数据包括收听音乐的费用。

记录媒介 3102 包括可改写的存储单元如 DVD-RAM，并可以从数字数据记录装置中取出。

在记录媒介 3102 上不可改写的安全区中，事先记录了记录媒介 3102 的固有信息。

在记录媒介 3102 上记录了由记录单元 3108 记录的加密单元 3107 再次加密的数字数据。

另外，记录的数字数据的管理信息和属性信息由记录单元 3108 记录在记录媒介 3102 上。

当得到来自通讯单元 3101 的数字数据和属性信息时，接收数据记录/判断单元 3103 存储属性信息 3201，并让显示单元 3104 显示曲目 3202，演唱者 3203，记录费用 3205，复制一次的费用 3206 等等，并将数字数据送给加密单元 3107.

当接收到复制（复制）音乐的指令时，接收数据记录/判断单元 3103 参照复制许可 3209 判断与指定的音乐的曲目代码 3204 相对应的数字数据是否可以复制.当数字数据可以复制时，接收数据记录/判断单元 3103 命令记录媒介固有信息获取单元 3106 获取记录媒介 3102 的固有信息，并将曲目代码 3204 和加密情况 3208 送给加密单元 3107.

当不允许复制数字数据时，接收数据记录/判断单元 3103 让显示单元 3104 显示判断结果。

当得知记录单元 3108 已经复制了数字数据时，接收数据记录/判断单元 3103 改写储存的属性信息 3201 中的复制许可 3209. 更具体地说，当复制许可 3209 是“只许一次”时，“只许一次”被改写为“不允许”。当复制的次数大于“1”时，次数以“1”递减. 存储属性信息 3201 的贮存区是在 EEPROM（电可擦除可编程 ROM）中，这样，当数字数据记录媒介掉电时，存储的内容不会被擦除。

例如，当把曲目代码 3204“歌曲 1”送给加密单元 3107 后得知记录单元 3108 完成了复制时，接收数据记录/判断单元 3103 将与曲目代码“歌曲 1”相对应的复制许可 3209 从“只许一次”改为“不允许”。其结果是，数据供应商的版权可以得到保护。

显示单元 3104 包括液晶显示器或 CRT（阴极射线管）。显示单元 3104 显示音乐数据（数字数据）的曲目或表示在接收数据记录/判断单元 3103 的控制下数字数据不能被复制。

输入操作单元 3105 包括鼠标及其类似物。输入操作单元 3105 接收用户的复制数据指令并将该指令告知给接收数据记录/判断单元 3103。当参照显示单元 3104 显示的曲目和演奏者下载一段音乐时，用户用鼠标点击该曲目等并命令复制音乐。

当接收到接收数据记录判断单元 3103 发出的获取固有信息的指令时，记录媒介固有信息获取单元 3106 读取记录在记录媒介 3102 上的安全区中的固有信息并将读取的固有信息告知给加密单元 3107。

加密单元 3107 根据来自记录媒介固有信息获取单元 3106 的固有信息产生一个加密密匙。加密单元 3107 利用该加密密匙对来自接收数据记录/判断单元 3103 的数字数据再次加密并且将再次加密的数字数据送给记录单元 3108。

当得知来自接收数据记录/判断单元 3103 的数字数据已经加密时，加密单元 3107 使数字数据解密或使用未解密的数字数据。

更具体地说，当由接收数据记录/判断单元 3103 得到将要记录在记录媒介 3102 上的数字数据“数据 A”时，加密单元 3107 根据记录媒介 3102 的固有信息产生一个加密密匙“KM”并再次加密数字数据“数据 A”产生一个加密的数字数据“E（KM，数据 A）”。当要将数字数据“数据 A”记录在另一记录媒介上并且根据另一记录媒介的固有信息产生一个加密密匙“K’ M”时，该加密的数字数据“E”为加密数字数据“E（K’ M，数据 A）”。

《日本公开的专利申请 NO.05-257816》中讲述了数字数据的加密技术。

记录单元 3108 将来自加密单元 3107 的加密的数字数据记录在记录媒介 3102 上。这时，记录单元 3108 在记录媒介 3102 上产生记录的数字数据的管理信息。

图 18 所示是管理信息的一个实例。管理信息 3301 包括曲目代码 3204，它是记录的数字数据的标识，被记录的数字数据的记录起始地址 3302，和记录结束地址 3303。在管理信息 3301 中，每个曲目代码 3204 对应不同的记录起始地址 3302 和记录结束地址 3303。

当复制记录在记录媒介 3102 上的数字数据时，需要参考管理信息 3301。

当完成将加密的数字数据和管理信息记录到记录媒介 3102 上时，

记录单元3108读取与记录的数字数据相对应的已贮存在接收数据记录/判断单元3103中的属性信息3201，并将读取的属性信息3201写入记录媒介3102中。另外，记录单元3108将完成复制的信息告知给接收数据记录/判断单元3103，并将记录的数字数据的曲目代码告知给帐目信息记录单元3109。

当记录单元3108将曲目代码3204送给财务信息记录单元3109时，财务信息记录单元3109读取与存储在接收数据记录/判断单元3103中的与曲目代码3204相对应的属性信息3201中的录制费用3205。当发现必须交付记录费3205时，财务信息记录单元3109将曲目代码3204和记录费3205记录到财务信息记录媒介3110上作为财务信息。

财务信息记录媒介3110包括RAM卡及其类似物。财务信息记录单元3109将已下载到记录媒介3102上的数字数据的财务信息记录到财务信息记录媒介3110上。

当通过通讯单元接收到来自财务中心（未作图示）的费用查询时，计帐单元3111读取记录在财务信息记录媒介3110上的未付清的财务信息，并且将读取的未付清的财务信息告知给通讯单元3101。将未付清的财务信息告知给通讯单元3101后，计帐单元3111记录一个标识位表示财务中心已经将未付清的财务信息（表示结算）记录在财务信息记录媒介3110上。

这里，将参照图19中的流程图说明本实施方案的工作过程。

接收数据记录/判断单元3103等待来自用户的记录数字数据的指令（步骤S3402），并根据属性信息201判断指定的数字数据是否允许复制（步骤S3404）。当不允许复制数字数据时，接收数据记录/判断单元3103使显示单元3104显示不允许复制（步骤S3406）并结束整个过程。

当允许复制数字数据时，记录媒介固有信息获取单元3106获取记录在记录媒介3102的安全区中的记录媒介3102的固有信息，并将获取的固有信息送给加密单元3107（步骤S3408）。

加密单元3107根据固有信息产生一个加密密匙并再次加密数字数据（步骤S3410）。

记录单元3108将加密的数字数据记录到记录媒介3102上（步骤S3412）。

然后，财务信息记录单元3109判断是否必须交付记录的数字数据

的记录费用（步骤 S3414）。当记录免费时，整个过程就完成了。当必须付费时，财务信息记录单元 3109 将财务信息记录到财务信息记录媒介 3110 上（（步骤 S3416）从而完成整个过程。

图 20 所示是再现由数字数据记录装置记录在记录媒介 3102 上的数字数据的播放机的结构。

数字数据的播放机包括记录媒介 3102，输入操作单元 3501，再现信息读取单元 3502，显示单元 3504，解密单元 3505，再现单元 3506，财务信息记录单元 3507 和财务信息记录媒介 3508。

在记录媒介 3102 上，记录了在数字数据记录装置中再次加密的数字数据，管理信息 3301，属性信息 3201，和已存储的标识记录媒介 3102 的固有信息。

当接收到开始再现的指令时，输入操作单元 3501 将一个开始工作的指令发给再现信息读取单元 3502。当接收到来自用户的指定的曲目时，输入操作单元 3501 将曲目告知给再现信息读取单元 3502。可见不只是接收到开始工作的指令时，而且当记录媒介 3102 插入数字数据播放机中时，将自动播放方式的指令送给再现信息读取单元 3502。

当接收到开始工作的指令时，再现信息读取单元 3502 读取记录在记录媒介 3102 上的属性信息 3201，并且让显示单元 3503 显示属性信息 3201 中如曲目 3202 和演奏者 3203 等信息。

当接收到来自输入操作单元 3501 的一段音乐的指令或自动播放方式的指令时，再现信息读取单元 3502 判断属性信息 3201 中的最大再现的次数 3207 是否等于或大于“1”。当再现的最大次数 3207 等于或大于“1”时，再现信息读取单元 3502 从记录起始地址 3302 到记录结束地址 3303 中读取曲目代码 3204 和记录的加密数字数据，并将读取的数字数据送给解密单元 3505。这时，再现信息读取单元 3502 命令记录媒介固有信息获取单元 3504 获取固有信息，并将曲目代码 3204 和每次再现的费用送给财务信息记录单元 3507。然后，当读取完数字数据时，再现信息读取单元 3502 改写作为属性信息 3201 中的一项的可再现的最大次数 3207，可再现的最大次数的值减 1。可见当可再现的最大次数 3207 是“无数次”时，不改写可再现的最大次数。

当判断得到可再现的最大次数小于“1”时，再现信息读取单元 3502 使显示单元 3502 显示出数字数据不能再现了。

显示单元 3503 包括液晶显示器及其类似物，它显示再现信息读取单元 3502 读取的曲目表和其他信息。另外，当用户指定一段已经以最大次数再现过的音乐数据时，显示单元 3503 显示出音乐数据不能再现了。

当再现信息读取单元 3502 命令获取固有信息时，记录媒介固有信息获取单元 3504 从记录媒介 3102 的安全区中获取作为记录媒介 3102 的标志的固有信息，并将获取的固有信息送给解密单元 3505。

当得到记录媒介固有信息获取单元 3504 给出的固有信息和再现信息读取单元 3502 给出的加密的数字数据时，解密单元 3505 根据固有信息产生一个解密密匙，解密加密的数字数据，并将解密的数字数据送给再现单元 3506。

当得到解密单元 3505 给出的解密的数字数据时，再现单元 3506 解码数字数据以再现音乐。音乐再现后，再现单元 3506 告知财务信息记录单元 3507 再现已完成。

当得到再现单元 3506 给出的再现已完成的信息时，财务信息记录单元 3507 将接收到的来自再现信息读取单元 3502 的曲目代码 3204 和再现一次的费用 3206 和再现日期作为财务信息记录到财务信息记录媒介 3508 上。可见当再现一次的费用 3206 是“免费”时，不记录再现一次的费用 3206。

财务信息记录媒介 3508 包括 RAM 卡及其类似物。在财务信息记录媒介 3508 上记录了由财务信息记录单元 3507 记录的财务信息。

这里，将参照图 21 中所示的流程图说明数字数据播放机的工作过程。

首先，用户命令开始再现，例如遥控输入操作单元 3501，并指定显示单元 3503 上显示的音乐的曲目。再现信息读取单元 3502 将指定指令作为再现该曲目的音乐数据（数字数据）的申请（步骤 S3602），并根据属性信息 3201 判断再现音乐的最大次数 3207 是否等于或大于“1”（步骤 S3604）。当最大再现次数小于“1”时，再现信息读取单元 3502 使显示单元 3503 显示音乐数据已经被再现了最大次数（步骤 S3606）从而完成整个过程。

当最大再现次数 3207 等于或大于“1”时，再现信息读取单元 3502 从记录媒介 3102 中读取加密的数字数据并将读取的数字数据送给解密

单元 3505（步骤 S3608）。

同时，记录媒介固有信息获取单元 3504 从记录媒介 3102 中获取固有信息并将获取的固有信息送给解密单元 3505（步骤 S3610）。

解密单元 3505 将固有信息用作解密密匙解密已加密的数字数据（步骤 S3612）。

再现单元 3506 解码数字数据以再现并输出音乐（步骤 S3614）。

然后，财务信息记录单元 3507 判断是否必须支付再现一次的费用 3206（步骤 S3616）。当再现一次的的费用 3206 为“免费”时，整个过程就此完成。当必须支付再现一次的费用 3206 时，财务信息记录单元 3507 将财务信息记录在财务信息记录媒介 3508（步骤 S3618）上从而完成整个过程。

（第七实施方案）

图 22 所示是根据本发明的第七实施方案的数字数据记录装置的结构。该数字数据记录装置包括第一数字数据记录装置 3700 和第二数字数据记录/播放装置 3710。

第一数字数据记录装置 3700 包括第一记录媒介 3701，通讯单元 3101，接收数据第一记录/判断单元 3702，显示单元 3104，输入操作单元 3105，第一记录媒介 3703，接收数据读取/判断单元 3704，固有信息获取单元 3705，加密单元 3706，财务信息记录单元 3109，财务信息记录媒介 3110 和计帐单元 3111。第一数字数据记录装置由一台 PC 机实现。

第二数字数据记录/播放装置包括固有信息获取/发送单元 3707，第二记录单元 3708，第二记录媒介 3709，输入操作单元 3501，再现信息读取单元 3502，显示单元 3503，解密单元 3505，再现单元 3506，财务信息记录媒介 3508。

第七实施方案中的第一数据记录装置 3700 和第二数字数据记录/播放装置中与第六实施方案中的数字数据记录装置和数字数据播放装置中相同的部分用相同的符号表示，以下不再说明这些部分。

首先，将说明第一数字数据记录装置 3700。第一数字数据记录装置 3700 不同于第六实施方案中的数字数据记录装置之处在于第一记录媒介 3701 是固定在第一数字数据记录装置 3700 中，并且记录在第一记录

媒介 3701 上的数字数据被加密后输出给第二次记录。

第一记录媒介 3701 包括可改写的记录体如固定在第一数字数据记录装置 3700 中的硬盘。在第一记录媒介 3701 上，记录了由第一记录单元 3703 记录的通讯单元 3101 接收到的数字数据（音乐数据）和数字数据的管理信息。

接收数据第一记录/判断单元 3702 将附着在通讯单元 3101 接收到的数字数据上的属性数据写入 EEPROM 的存储区中。图 23 中所示的是本实施方案中接收到的属性信息的一个实例。属性信息 3801 不同于第六实施方案中的属性信息 3201 之处在于它具有表明第二次记录的费用 3802，复制许可（第一级）3803 和复制许可（第二级）的信息。

属性信息 3801 表示不允许第一级和第二级复制并且只允许实时收听曲目代码为“歌曲 05”的曲目“音乐 E”。

当用户命令第二级记录音乐时，接收数据第一记录/判断单元 3702 根据属性信息 3801 中的复制许可项判断是否允许第一级记录音乐。当不允许第一级记录时，接收数据第一记录/判断单元 3702 使显示单元 3104 显示不允许第一级记录音乐。当允许第一级记录时，接收数据第一记录/判断单元 3702 将音乐的数字数据送给第一级记录单元 3703。接收数据第一记录/判断单元的另一功能与接收数据记录/判断单元 3103 相同。

第一记录单元 3703 将接收到的数字数据记录在第一记录媒介 3701 上。同时，管理信息也被记录上，其写入的情况与第六实施方案中的记录单元 3108 相同。可见在第六实施方案中根据记录媒介 3102 的固有信息产生一个加密密匙来再次加密数字数据，而在本实施方案中由于第一记录媒介 3701 不能从第一数字数据记录装置 3700 中取出即不能用其他装置，所以数字数据将不被再次加密。

另外，当数字数据已记录在第一记录媒介 3701 上时，第一记录单元 3703 将记录的数字数据的曲目代码 3805 送给接收数据读取/判断单元 3704。

当得到第一记录单元 3703 给出的曲目代码 3805 时，接收数据读取/判断单元 3704 根据接收数据第一级记录/判断单元 3702 中的属性信息 3801 中的复制许可（第二级）3804 判断是否允许第二级记录音乐。当不允许第二级记录时，或当允许记录的最大次数小于“1”时，接收数

据读取/判断单元 3704 使显示单元 3104 显示不允许第二级记录音乐。

当允许第二级记录时，接收数据读取/判断单元 3704 参照管理信息（参见图 18）读取与记录在第一记录媒介 3701 上的曲目代码相应的数字数据。接收数据读取/判断单元 3704 将数字数据送给加密单元 3706，并命令固有信息获取单元 3705 获取固有信息。

当读取到数字数据时，接收数据读取/判断单元 3704 将存储在接收数据第一记录/判断单元 3702 中的属性信息 3701 中的允许复制（第二级）的次数 3804 减 1。例如，将“只许一次”变为“不允许”，由于“允许”表示次数不限，所以不改写。

将数字数据送给加密单元 3706 后，接收数据读取/判断单元 3704 将读取存储在接收数据第一记录/判断单元 3702 中的属性信息。

当接收数据读取/判断单元 3704 命令获取固有信息时，固有信息获取单元 3705 命令与第一数字数据记录装置 3700 相连的第二数字数据记录/播放装置 3710 中的固有信息获取/发送单元 3707 发送固有信息。当由固有信息获取/发送单元 3707 发出固有信息时，固有信息获取单元 3705 将固有信息送给加密单元 3706。

加密单元 3706 根据固有信息获取单元 3705 发送的固有信息产生一个加密密匙，加密接收数据读取/判断单元 3704 发出的数字数据，并将加密后的数字数据传送给第二数字数据记录/播放装置 3710 中的第二记录单元 3708。传送完加密的数字数据后，加密单元 3706 发送接收到的属性信息。

这里，将说明第二数字数据记录/播放装置 3710。例如第二数字数据记录/播放装置 3710 由一台随身听实现。第二记录媒介 3709 包括半导体存储单元如可从第二数字数据记录/播放装置 3710 中取出的 IC 卡。

当第一数字数据记录装置 3700 中的固有信息获取单元 3705 请求发送固有信息时，固有信息获取/发送单元 3707 获取事先记录在第二记录媒介 3709 上的媒介的标志信息和在第二数字数据记录/播放装置 3710 中固有的装置的标志信息，并将获取的媒介的标志信息和装置的标志信息送给固有信息获取单元 3705。同时，当再现信息读取单元 3502 命令获取固有信息时，固有信息获取/发送单元 3707 将获取的媒介的标志信息和装置的标志信息送给解密单元 3505。

当接收来自第一数字数据记录装置3700中的加密单元3706输出的加密的数字数据和属性信息时，第二记录单元3708将接收到的加密的数字数据和属性信息记录到第二记录媒介3709上。另外，第二记录单元3708将图18中所示的管理信息3301记录在第二记录媒介3709上。解密单元3505根据固有信息获取/发送单元3707发送来的媒介的标志信息和装置的标志信息产生一个解密密匙，并用产生的解密密匙解密由再现信息读取单元3502发送来的加密的数字数据。可见第二数字数据记录/播放装置3710的结构的其它部分与第六实施方案中的数字数据播放装置基本相同。

这里，将说明当第二记录媒介3709包括固定在第二数字数据记录/播放装置3710中的IC卡时的情况。在这种情况下，由于第二记录媒介3709只用于第二数字数据记录/播放装置3710，所以固有信息获取/发送单元3707不获取媒介的标志信息并将固有信息获取/发送单元3707存储的装置的标志信息送给固有信息获取单元3705。同时，固有信息获取/发送单元3707将装置的标志信息送给解密单元3505。

如上所述，根据第二数字数据记录/播放装置3710中的第二记录媒介3709是否为可移去的判断出是根据媒介的标志信息和装置的标志信息的组合信息还是根据装置的标志信息产生一个加密密匙来加密数字数据。这样做可以防止数字数据非法复制和翻版。

这里，将参照图24中所示的流程图说明第七实施方案的工作过程。

首先，接收数据第一记录/判断单元3702等待来自输入操作单元3105的第二记录的数字数据的指令(步骤S3902)，并根据属性信息3801判断是否允许数字数据第一次记录(步骤3904)。当不允许第一级记录，接收数据第一记录/判断单元3702使显示单元3104显示不允许第一级记录(步骤S3906)，从而完成整个过程。当允许第一级记录时，接收数据第一记录/判断单元3702将数字数据送给第一记录单元3703。第一记录单元3703将数字数据和管理信息记录到第一记录媒介3701上(步骤S3908)。

其次，信息记录单元3109判断第一级记录是否付费(步骤S3910)，并且当第一级记录要付费时，将财务信息记录在财务信息记录媒介3110上(步骤S3912)。

然后，接收数据读取/判断单元3704根据存储在接收数据第一记录

/判断单元3702中的属性信息3801判断记录在第一记录媒介3701上的数字数据是否允许第二级记录（步骤S3914）。当不允许第二级记录时，接收数据读取/判断单元3704使显示单元3104显示不允许第二级记录（步骤S3916）从而完成整个过程。

当允许第二级记录时，接收数据读取/判断单元3704从第一记录媒介3701上读取数字数据，将读取的数字数据送给加密单元3706，并命令固有信息获取单元3705从第二数字数据播放装置3710中获取固有信息。固有信息获取单元3705获取固有信息并将获取的固有信息送给加密单元3706（步骤S3918）。加密单元3706根据接收到的固有信息产生一个加密密匙（步骤S3920），加密接收到的数字数据，并将加密后的数字数据输出给第二数字数据记录/播放装置3710中的第二记录单元3708。

第二记录单元3708将加密的数字数据，属性信息和管理信息记录到第二记录媒介3709上（步骤S3922）。

财务信息记录单元3109判断第二级记录是否付费（步骤S3924），并且当第二级记录要付费时，将财务信息记录在财务信息记录媒介3110上（步骤S3926），从而完成整个过程。

第二数字数据记录/播放装置3710再现数字数据的工作过程基本与第六实施方案中的数字数据播放装置的工作过程相同，所以在此不再说明。

（另一实例）

当第二记录媒介3709是可移去的时，用根据第二数字数据记录/播放装置3710的装置的标志信息和第二记录媒介3709的媒介的标志信息的组合信息产生的加密密匙加密第七实施方案中的数字数据，加密的格式由用户指定（即用户指定是只根据媒介的标志信息还是媒介的标志信息和装置的标志信息的组合信息产生加密密匙），以增加第七实施方案的本例中使用形式的自由度。更具体地说，当用第二数字数据记录/播放装置3710再现时，在记录的同时用媒介的标志信息和装置的标志信息将记录在第二记录媒介3709上的音乐的数字数据加密。当用另一数据播放装置（用媒介的标志信息作为解密密匙解密加密的数字数据的装置）再现时，在记录的同时用媒介的标志信息加密数字数据。其结果是，

可以根据使用形式选择加密的形式。

另一方面，根据使用格式的自由度确定第二级记录的费用来保护版权。

这里，将说明第七实施方案的其他实例中的第一数字数据记录/播放装置和第二数字数据记录/播放装置的结构。该实例中的第一数字数据记录装置和第二数字数据记录/播放装置的功能可在图22中所示的第一数字数据记录装置3700的功能中添加一些功能来实现。其结果是，将参照用于说明第七实施方案的图22来说明不同于第七实施方案的结构部分。

图25所示是存储在接收数据第一记录/判断单元3702中的属性信息31001部分。属性信息31001不同于图23中所示的属性信息3801之处在于第二级记录的费用3802和第二级记录的费用31002的内容。

第二级记录的费用31002取决于用于数字数据加密的加密密匙是根据媒介的标志信息(媒介ID)31003，装置的标志信息(装置ID)31004，还是媒介标志信息和装置的标志信息的组合信息产生的。当根据媒介的标志信息31003产生加密密匙时，可以用另一装置中的第二记录媒介3709再现音乐数据并且增加了用户的自由度。其结果是，第二级记录的费用(第二级再现的费用)高于当加密密匙是根据装置的标志信息31004和媒介的标志信息和装置的标志信息的组合信息31005产生时的第二级记录的费用。这样，再现的费用取决于使用形式。

当得到固有信息获取/发送单元3707发出的装置的标志信息和媒介的标志信息时，固有信息获取单元3705使显示单元3104显示第二记录媒介3709是用于第二数字数据记录/播放装置3710中还是用于另一装置中，并等待用户选择。

用户用输入操作单元3105指定是第二数字数据记录/播放装置3710还是另一装置，即是根据媒介的标志信息产生加密密匙还是根据媒介的标志信息和装置的标志信息的组合信息产生的加密密匙。

输入操作单元3105将用户的选择送给接收数据第一记录/判断单元3702。

当输入操作单元3105给出使用另一装置时，接收数据第一记录/判断单元3702告知给财务信息记录单元3109，第二级记录的费用31002根据媒介的标志信息31003产生的加密密匙确定。另一方面，当得知只

用第二数字数据记录/播放装置时，接收数据第一记录/判断单元 3702 告知给财务信息记录单元 3109，第二级记录的费用 31002 根据媒介的标志信息和装置的标志信息的组合信息 31005 产生的加密密匙确定。

当由输入操作单元 3105 给出使用另一装置时，固有信息获取单元 3705 只将媒介的标志信息 31003 送给加密单元 3706。另一方面，当由输入操作单元 3105 给出只使用第二数字数据记录/播放装置时，固有信息获取单元 3705 将媒介的标志信息和装置的标志信息的组合信息 31005 送给加密单元 3706。

当加密单元 3706 给出加密的数字数据已传送给第二记录单元 3708 时，财务信息记录单元 3109 参考接收数据第一记录/判断单元 3702 给出的属性信息 31001 中的第二级记录的费用 31002，并将财务信息记录到财务信息记录媒介 3110 上。

在本例中，不用说，当第二记录媒介 3709 是可移去的 DVD-RAM 时，只根据在 DVD-RAM 中固有的标志信息可产生加密密匙，可以用产生的加密密匙再次加密数字数据，并且再次加密的数字数据可被记录，如第六实施方案中的情况。

同时，本例中的工作过程与第七实施方案的基本相同，所以不再说明。

可见，例如可以假设财务信息记录媒介 3110 和 3508 由 IC 卡实现，在第六和第七实施方案及本例中不放置 IC 卡就不记录和再现数字数据。

另外，假定在第六和第七实施方案及本例中由通讯单元 3110 接收的数字数据是音乐数据，数字数据还可以是视频数据、音频数据、字符数据、及它们的组合数据。

图 16，20 和 22 中所示的是数字数据记录装置，数字数据播放装置和数字数据记录/播放装置的结构。它可以将实现各部分的功能的程序记录在计算机可读的记录媒介上如软盘，可以在没有版权保护功能的数字数据记录/播放装置中使用计算机可读的记录媒介，使数字数据记录/播放装置具有版权保护的功能。

虽然已经参照附图及实例全面说明了本发明，但是对专业人员来说很显然的是，本发明还有多种变化和改进。因此，无论这些变化和改进与本发明的范围相差多远，它们也应包含其中。

如上所述根据本发明的数字数据记录装置可保护版权，减少播放机的费用。其结果是，该数字数据记录装置适用于记录在不同的加密系统中加密了的电子传播的数字数据，特别是记录电子传播的音乐数据。

说 明 书 附 图

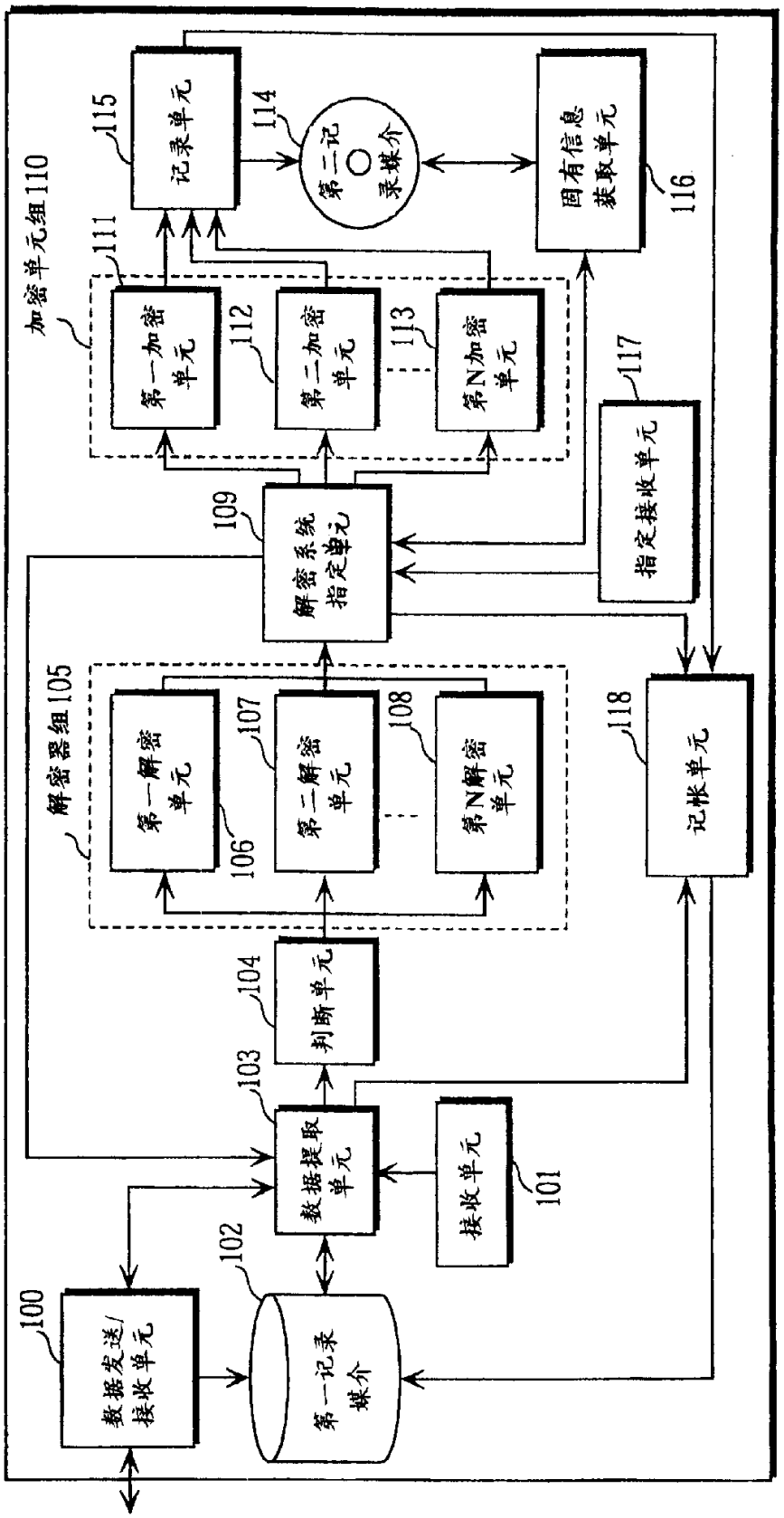

数字数据记录装置
加密单元组110
解密器组105
数据发送/接收单元
第一记录媒介
数据提取单元
接收单元
判断单元
第一解密单元
第二解密单元
第N解密单元
解密系统指定单元
第一加密单元
第二加密单元
第N加密单元
记录单元
第二记录媒介
固有信息获取单元
指定接收单元
记帐单元
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118

图 1

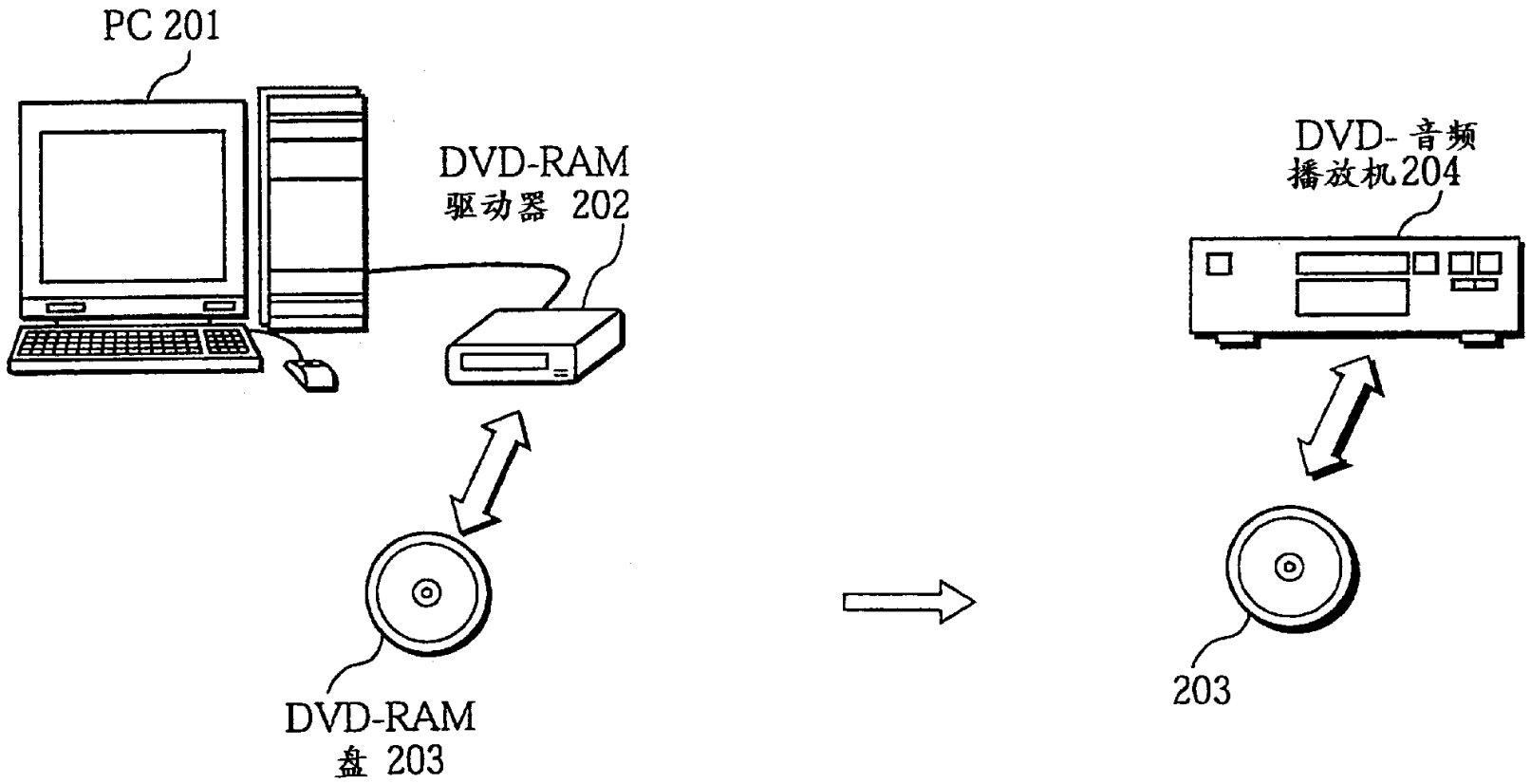


图 2

301 曲名	302 演唱者	303 时间	304 价格
歌曲1	演唱者A	4'20"	¥100
歌曲2	演唱者B	3'53"	¥50
歌曲3	演唱者C	4'48"	¥75
歌曲4	演唱者D	4'06"	¥100
:	:	:	:
:	:	:	:

图 3

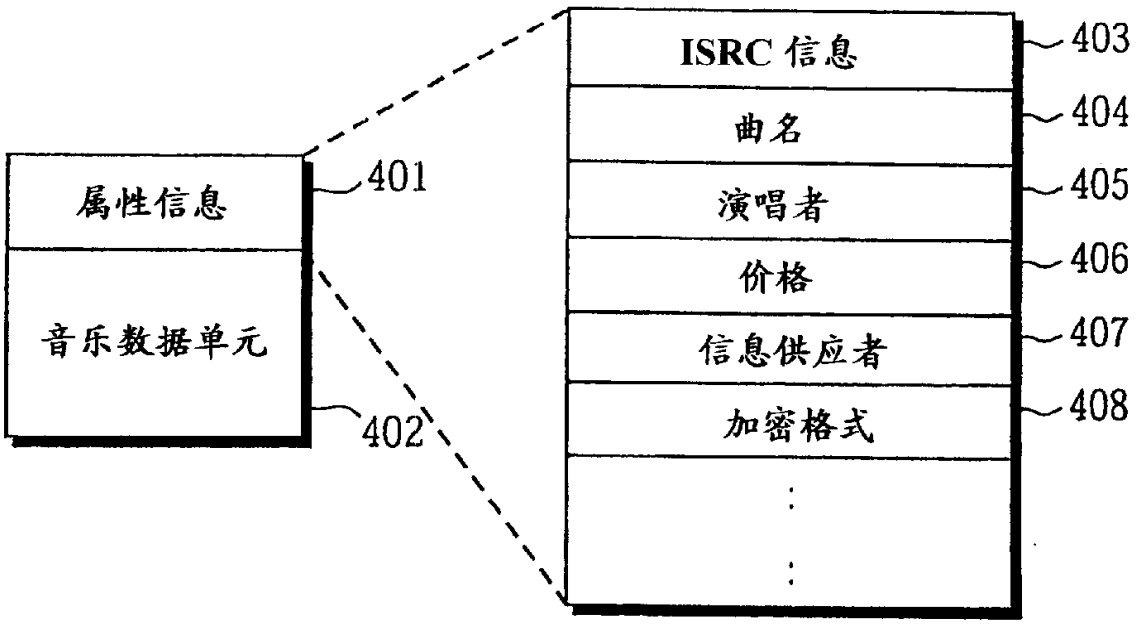

属性信息
401
音乐数据单元
402
ISRC 信息
403
曲名
404
演唱者
405
价格
406
信息供应者
407
加密格式
408

图 4

301 曲名	302 演唱者	303 时间	501 价格 (1)	502 价格 (2)
歌曲1	演唱者A	4'20"	¥100	¥70
歌曲2	演唱者B	3'53"	¥50	¥35
歌曲3	演唱者C	4'48"	¥75	¥50
歌曲4	演唱者D	4'06"	¥100	¥100
:	:	:	:	:
:	:	:	:	:

图 5

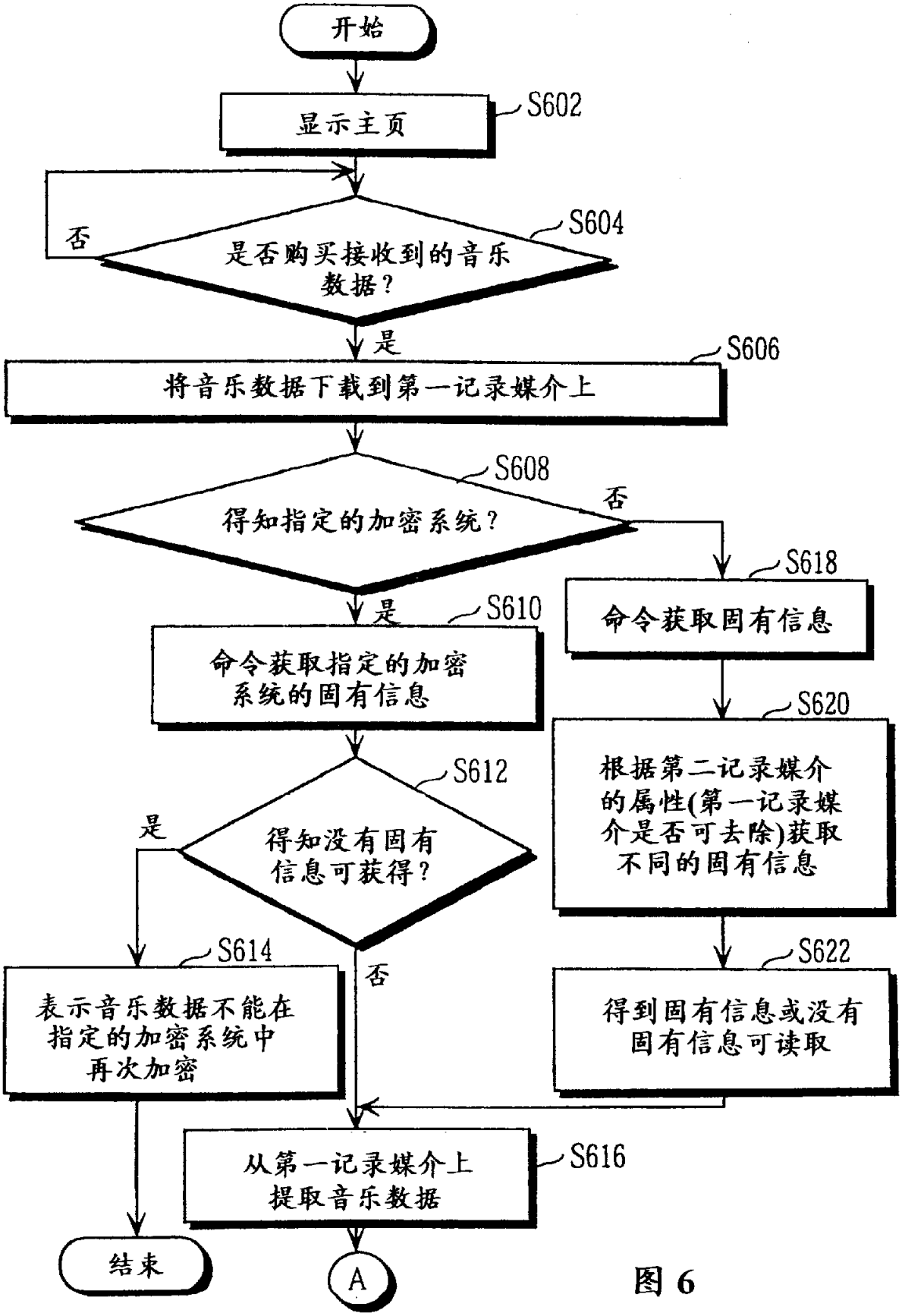

开始
显示主页
S602
否
是否购买接收到的音乐数据？
S604
是
将音乐数据下载到第一记录媒介上
S606
得知指定的加密系统？
S608
否
是
命令获取指定的加密系统的固有信息
S610
命令获取固有信息
S618
根据第二记录媒介的属性(第一记录媒介是否可去除)获取不同的固有信息
S620
得知没有固有信息可获得？
S612
是
否
表示音乐数据不能在指定的加密系统中再次加密
S614
得到固有信息或没有固有信息可读取
S622
从第一记录媒介上提取音乐数据
S616
结束
A

图 6

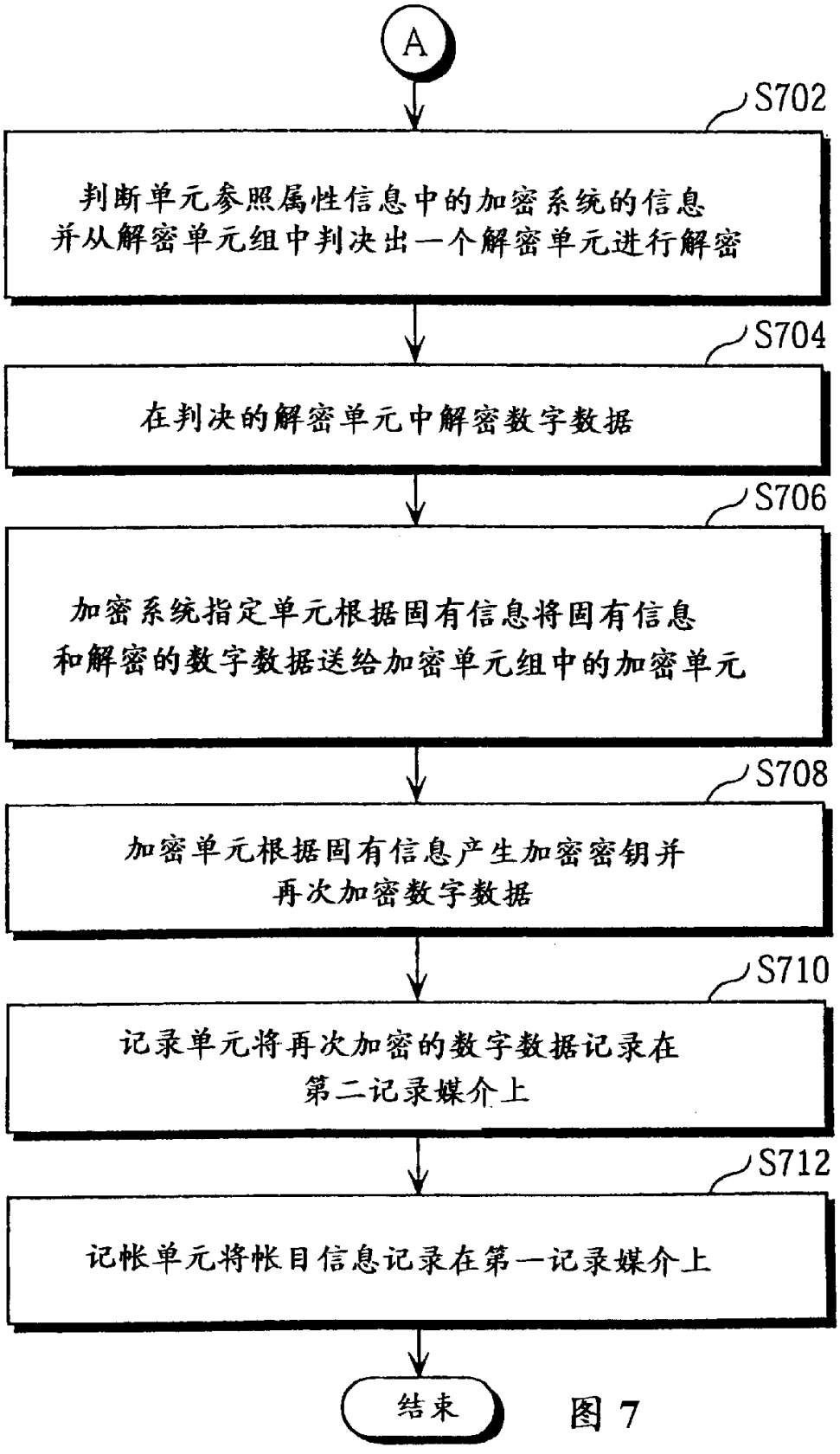

A
S702
判断单元参照属性信息中的加密系统的信息
并从解密单元组中判决出一个解密单元进行解密
S704
在判决的解密单元中解密数字数据
S706
加密系统指定单元根据固有信息将固有信息
和解密的数字数据送给加密单元组中的加密单元
S708
加密单元根据固有信息产生加密密钥并
再次加密数字数据
S710
记录单元将再次加密的数字数据记录在
第二记录媒介上
S712
记帐单元将帐目信息记录在第一记录媒介上
结束

图 7

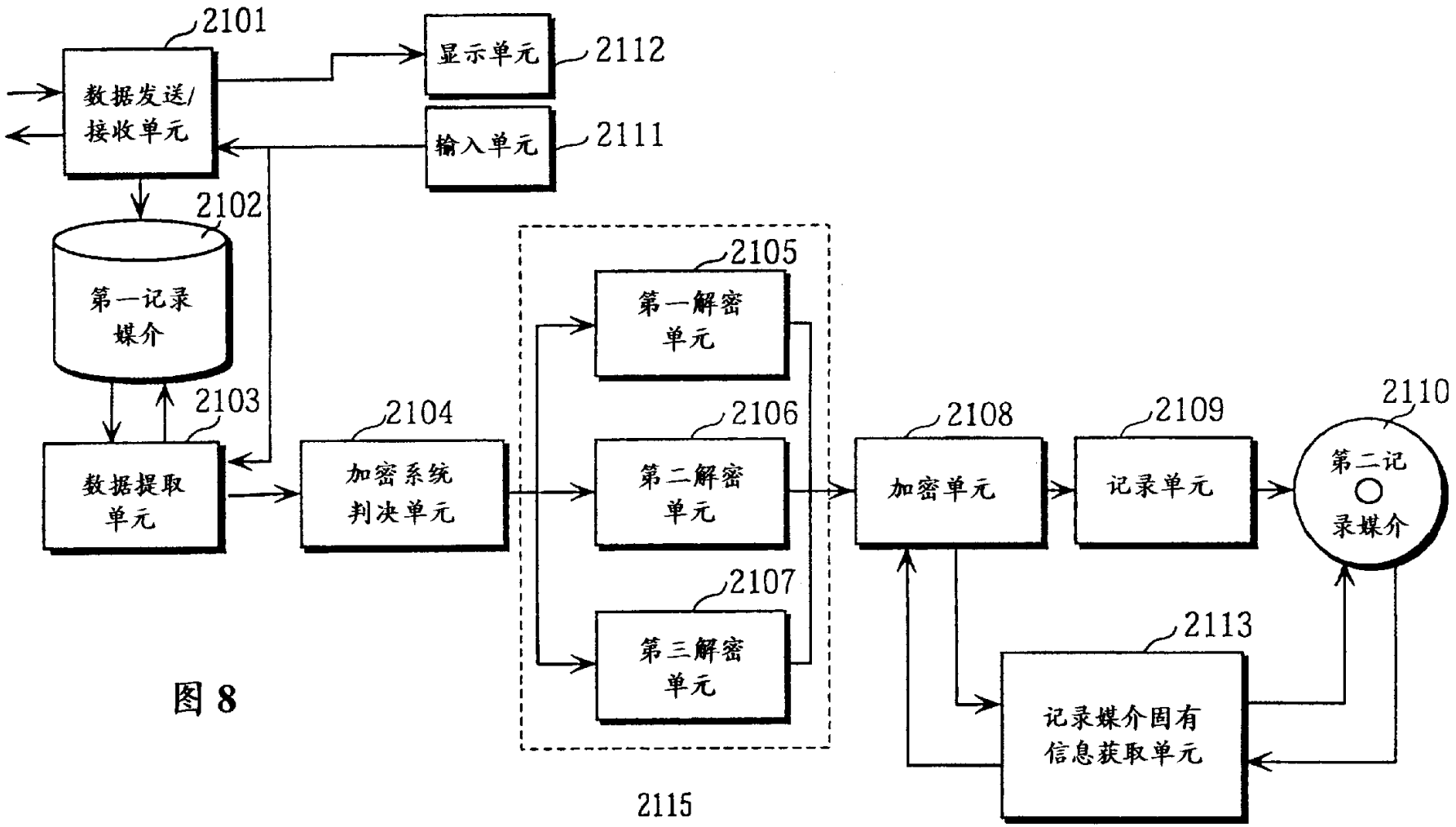

2101
数据发送/
接收单元
显示单元
2112
输入单元
2111
2102
第一记录
媒介
2103
数据提取
单元
2104
加密系统
判决单元
2105
第一解密
单元
2106
第二解密
单元
2107
第三解密
单元
2115
2108
加密单元
2109
记录单元
2110
第二记
录媒介
2113
记录媒介固有
信息获取单元

图 8

2201 曲名	2202 曲名代码	2203 演唱者	2204 数据来源
歌名A	歌曲01	A	www. song/song01
歌名B	歌曲02	B	www. song/song02
歌名C	歌曲03	C	www. song/song03
歌名D	歌曲04	D	www. song/song04
歌名E	歌曲05	E	www. song/song05

图 9

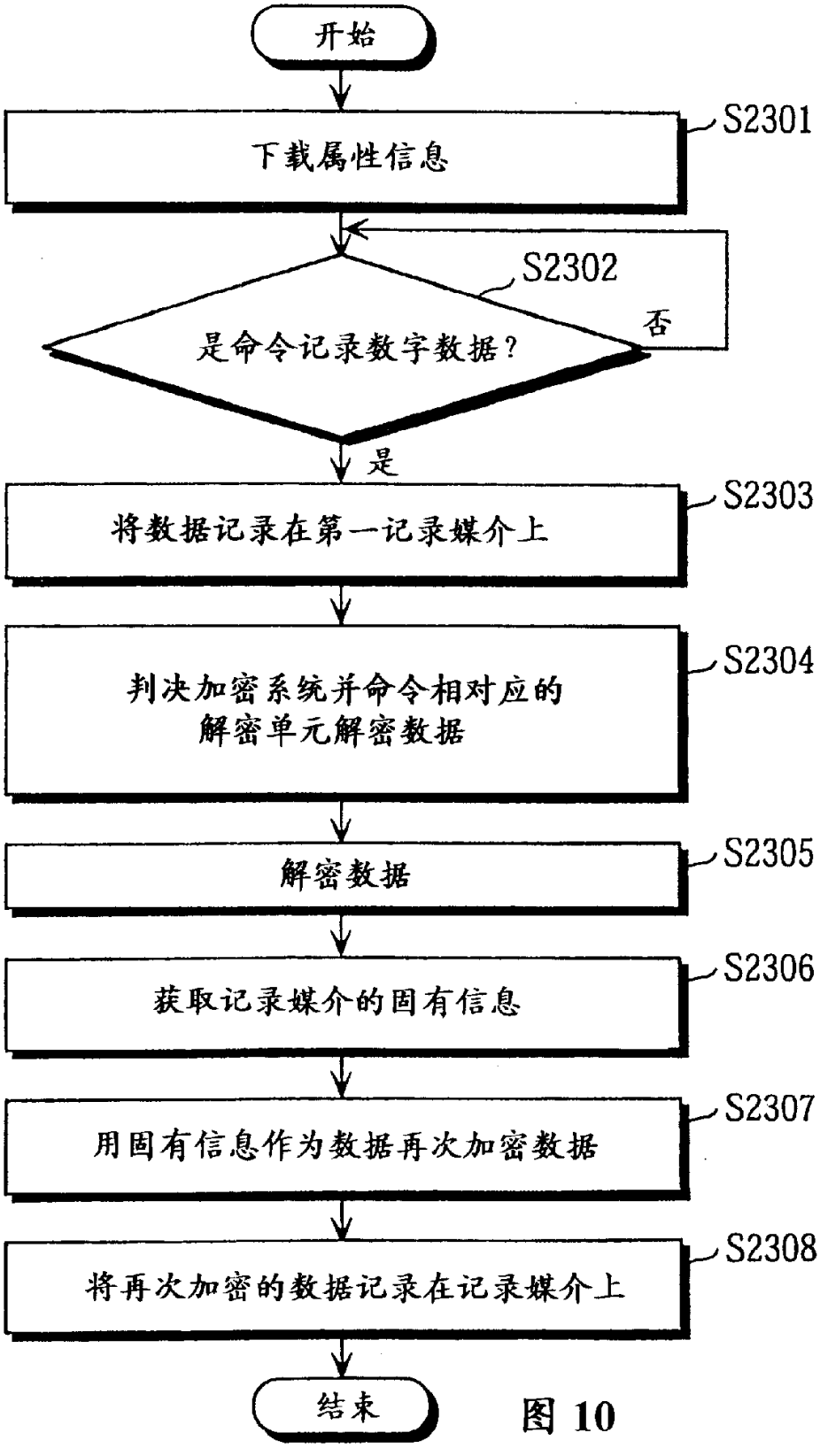

开始
下载属性信息
S2301
S2302
是命令记录数字数据？
否
是
将数据记录在第一记录媒介上
S2303
判决加密系统并命令相对应的
解密单元解密数据
S2304
解密数据
S2305
获取记录媒介的固有信息
S2306
用固有信息作为数据再次加密数据
S2307
将再次加密的数据记录在记录媒介上
S2308
结束

图 10

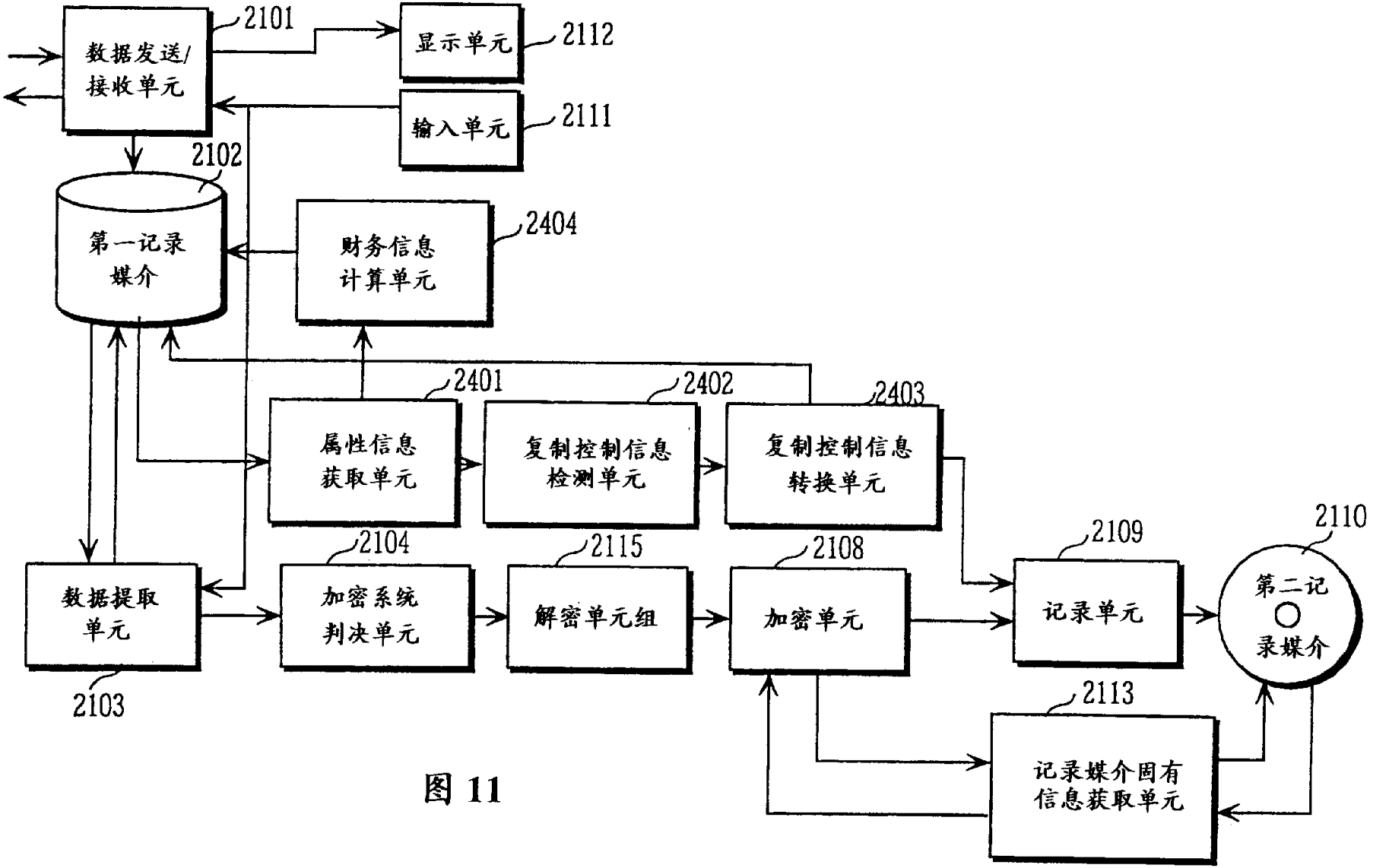

数据发送/
接收单元
2101
显示单元
2112
输入单元
2111
2102
第一记录
媒介
财务信息
计算单元
2404
2401
2402
2403
属性信息
获取单元
复制控制信息
检测单元
复制控制信息
转换单元
2104
2115
2108
2109
2110
数据提取
单元
加密系统
判决单元
解密单元组
加密单元
记录单元
第二记
录媒介
2103
2113
记录媒介固有
信息获取单元

图 11

2201 曲名	2202 曲名代码	2203 演唱者	2204 数据来源	2501 复制控制信息	2502 价格
歌名A	歌曲01	A	www. song/song01	不许再复制	¥100
歌名B	歌曲02	B	www. song/song02	无限制	¥10
歌名C	歌曲03	C	www. song/song03	不许再复制	¥0
歌名D	歌曲04	D	www. song/song04	不许再复制	¥30
歌名E	歌曲05	E	www. song/song05	复制两次	¥10

图 12

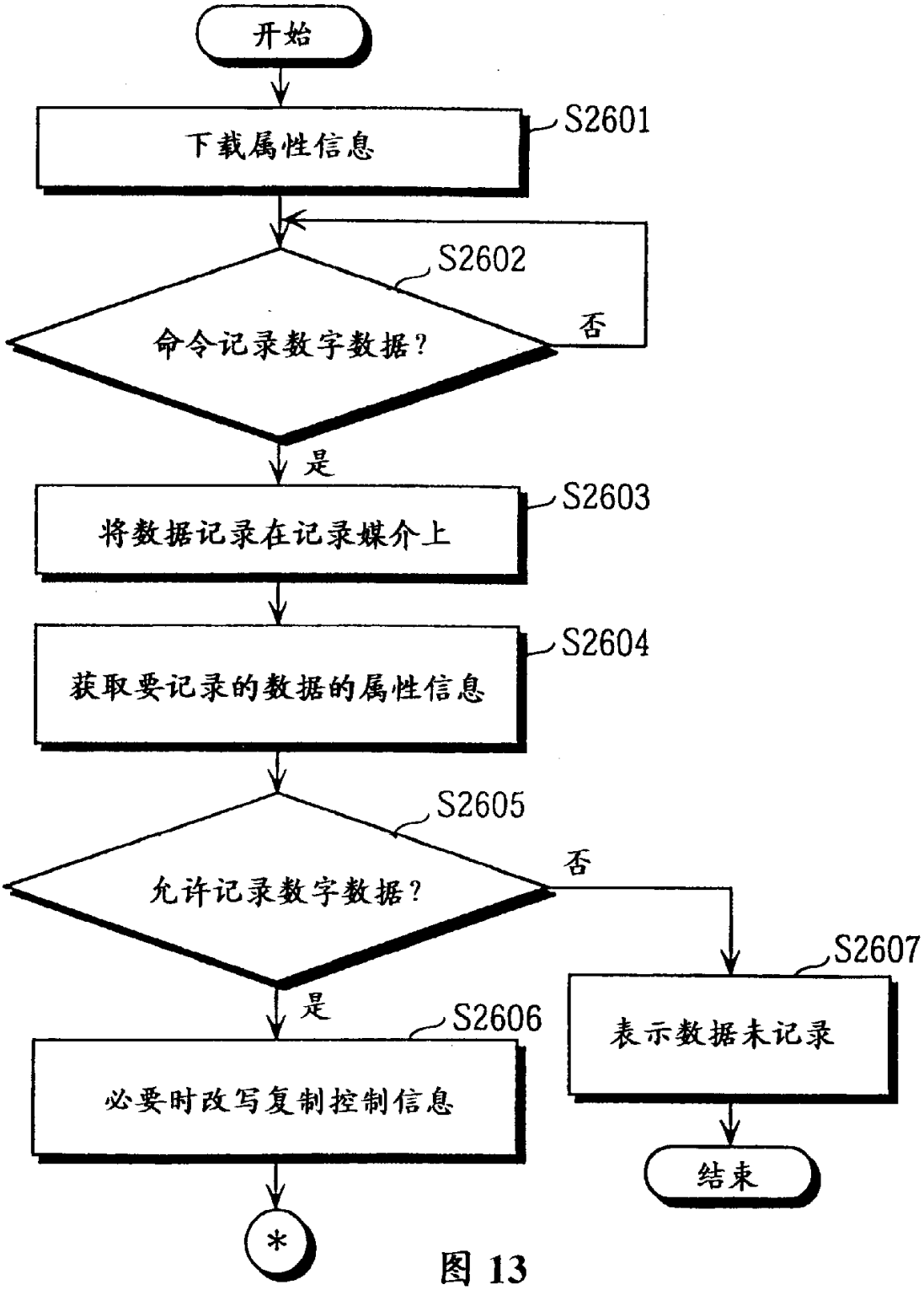

开始
下载属性信息
S2601
S2602
命令记录数字数据？
否
是
将数据记录在记录媒介上
S2603
获取要记录的数据的属性信息
S2604
S2605
允许记录数字数据？
否
是
S2606
必要时改写复制控制信息
*
S2607
表示数据未记录
结束

图 13

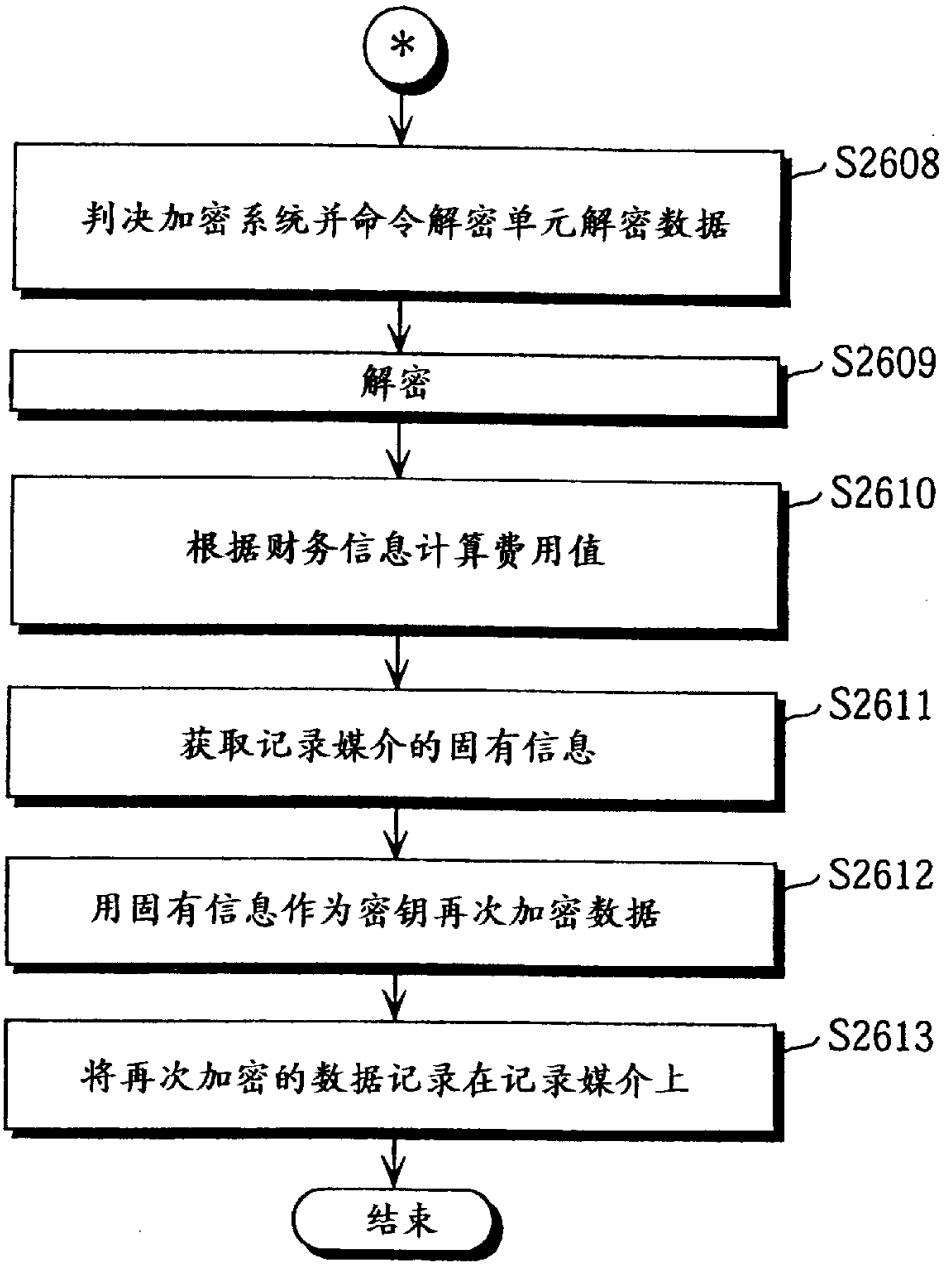

*
判决加密系统并命令解密单元解密数据
S2608
解密
S2609
根据财务信息计算费用值
S2610
获取记录媒介的固有信息
S2611
用固有信息作为密钥再次加密数据
S2612
将再次加密的数据记录在记录媒介上
S2613
结束

图 14

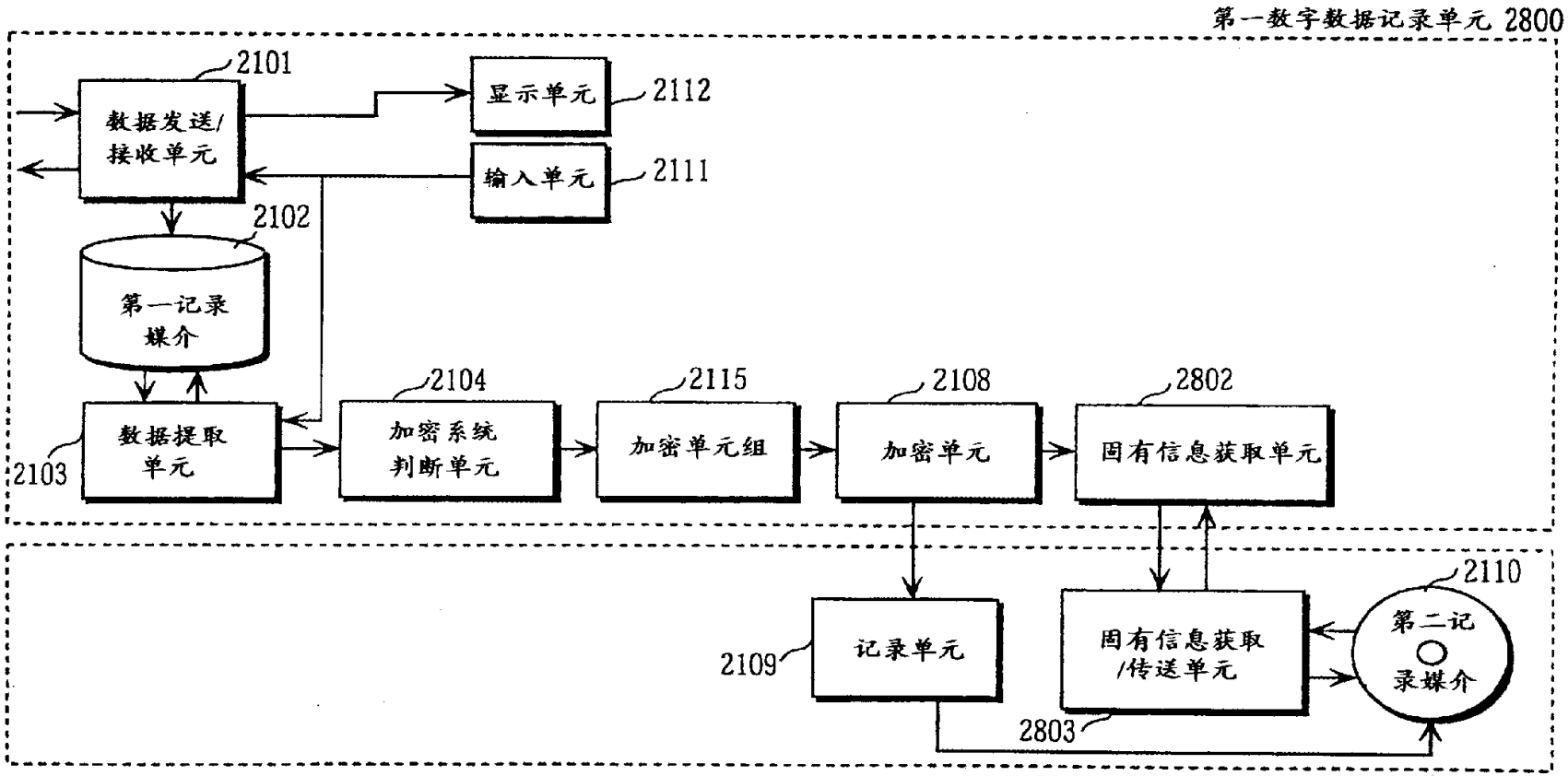

第一数字数据记录单元 2800
2101
数据发送/
接收单元
显示单元
2112
输入单元
2111
2102
第一记录
媒介
2103
数据提取
单元
2104
加密系统
判断单元
2115
加密单元组
2108
加密单元
2802
固有信息获取单元
2109
记录单元
固有信息获取
/传送单元
2110
第二记
录媒介
2803
第二数字数据记录装置 2801

图 15

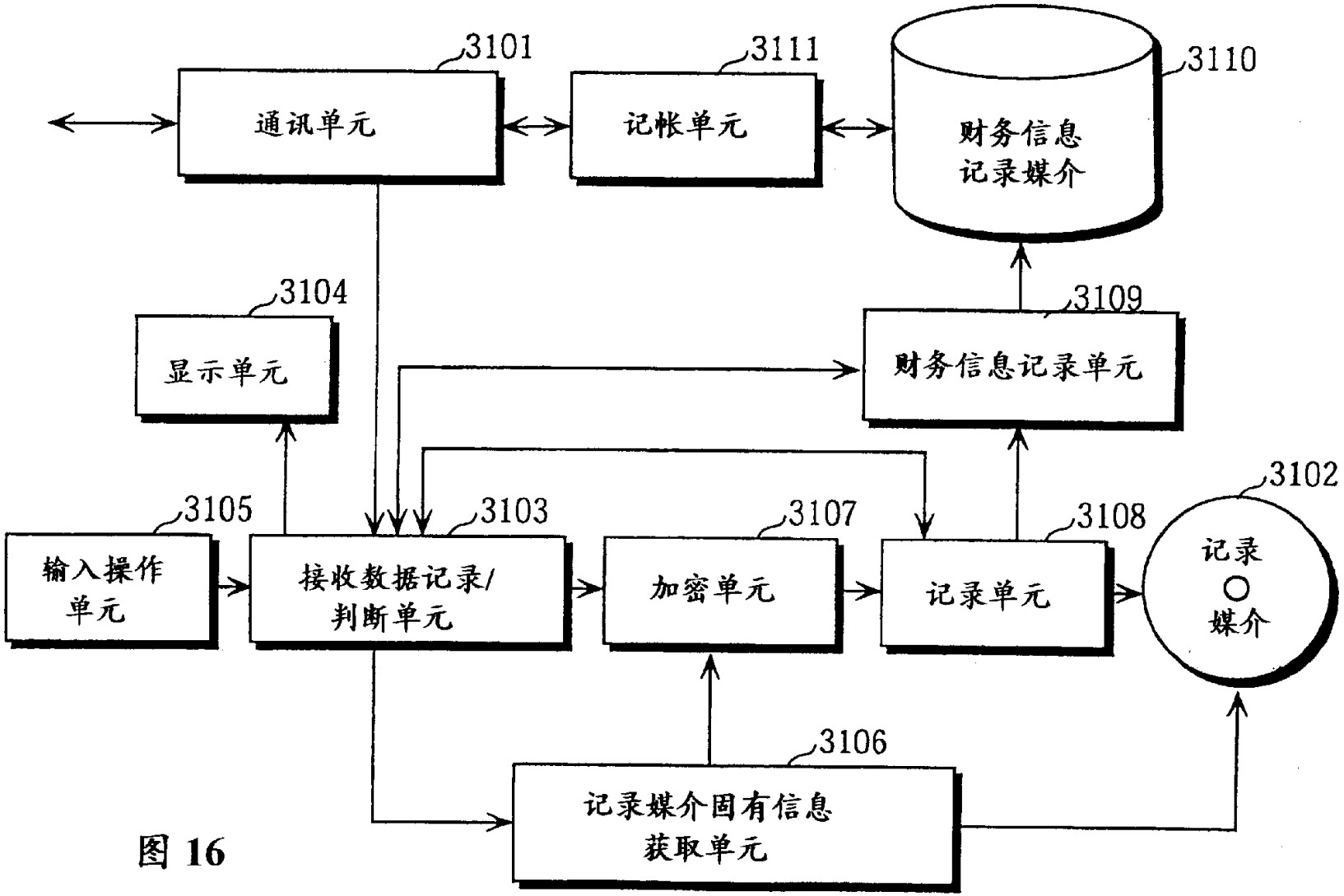

3101
通讯单元
3111
记帐单元
3110
财务信息
记录媒介
3104
显示单元
3109
财务信息记录单元
3105
输入操作
单元
3103
接收数据记录/
判断单元
3107
加密单元
3108
记录单元
3102
记录
媒介
3106
记录媒介固有信息
获取单元

图 16

属性信息 3201

3202 曲名	3203 表演者	3204 曲名代码	3205 记录费用	3206 再现一次的费用	3207 再现的最大次数	3208 加密情况	3209 复制许可	…
音乐A	a	歌曲01	¥100	¥0.5	100次	已加密	只许一次	…
音乐B	b	歌曲02	¥10	¥0	无数次	未加密	允许	…
音乐C	c	歌曲03	¥0	¥1	50次	已加密	只许一次	…
音乐D	d	歌曲04	¥30	¥5	50次	已加密	只许一次	…
音乐E	e	歌曲05	¥10	¥0	10次	未加密	允许	…

图 17

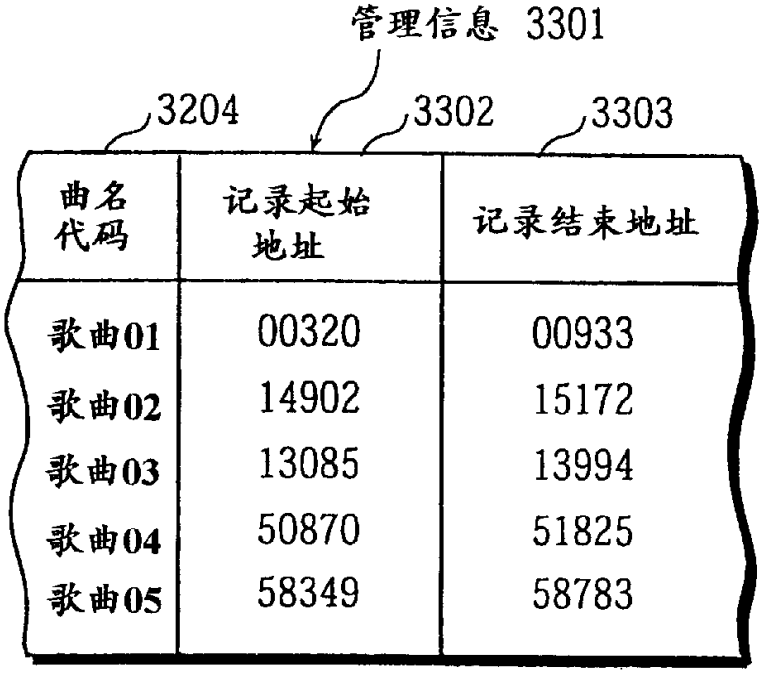

管理信息 3301
3204
3302
3303
曲名代码
记录起始地址
记录结束地址
歌曲01
00320
00933
歌曲02
14902
15172
歌曲03
13085
13994
歌曲04
50870
51825
歌曲05
58349
58783

图 18

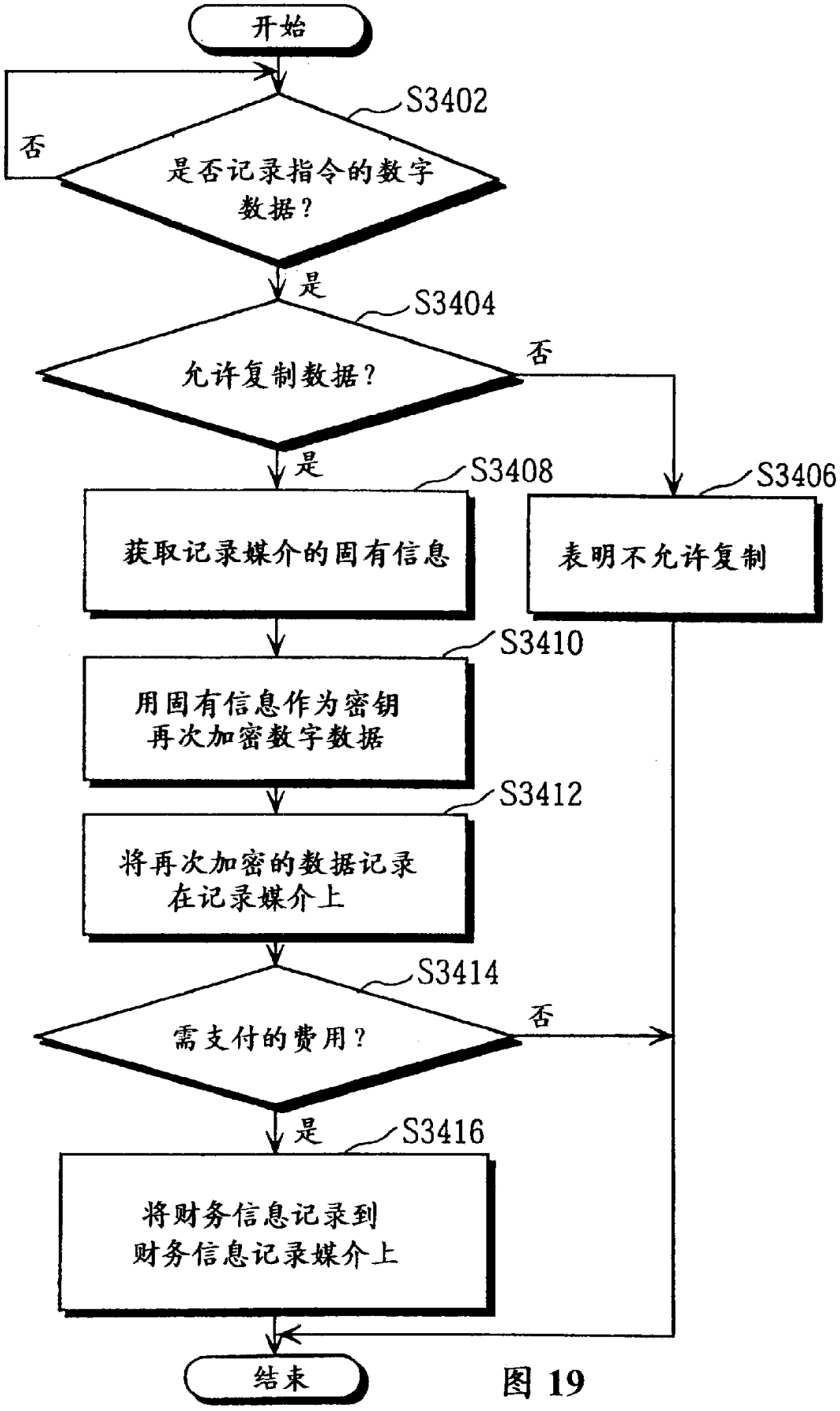

开始
S3402
否
是否记录指令的数字数据？
是
S3404
允许复制数据？
否
是
S3408
获取记录媒介的固有信息
S3406
表明不允许复制
S3410
用固有信息作为密钥再次加密数字数据
S3412
将再次加密的数据记录在记录媒介上
S3414
需支付的费用？
否
是
S3416
将财务信息记录到财务信息记录媒介上
结束

图 19

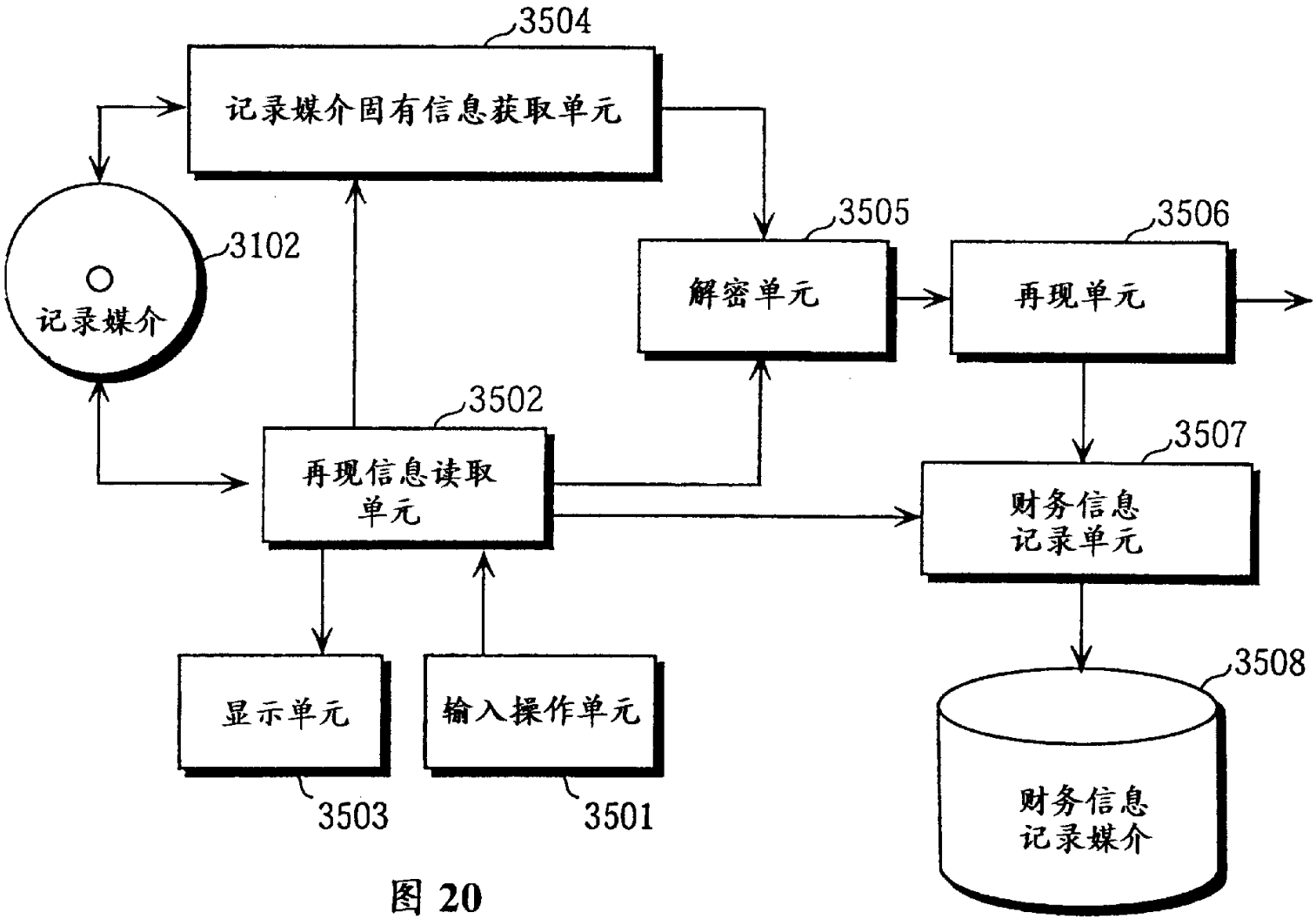

3504
记录媒介固有信息获取单元
3102
记录媒介
3505
解密单元
3506
再现单元
3502
再现信息读取单元
3507
财务信息记录单元
3508
显示单元
输入操作单元
财务信息记录媒介
3503
3501

图 20

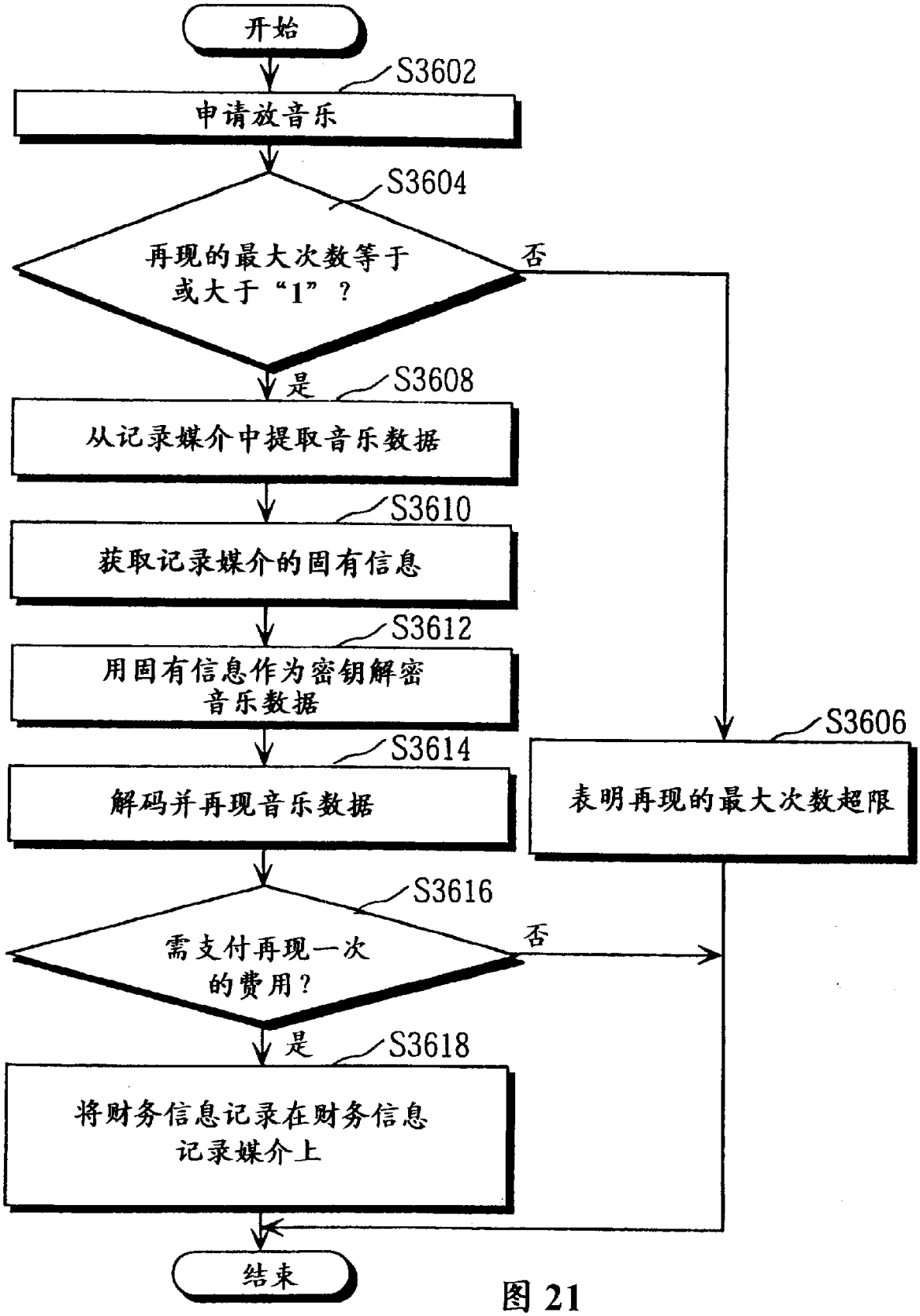
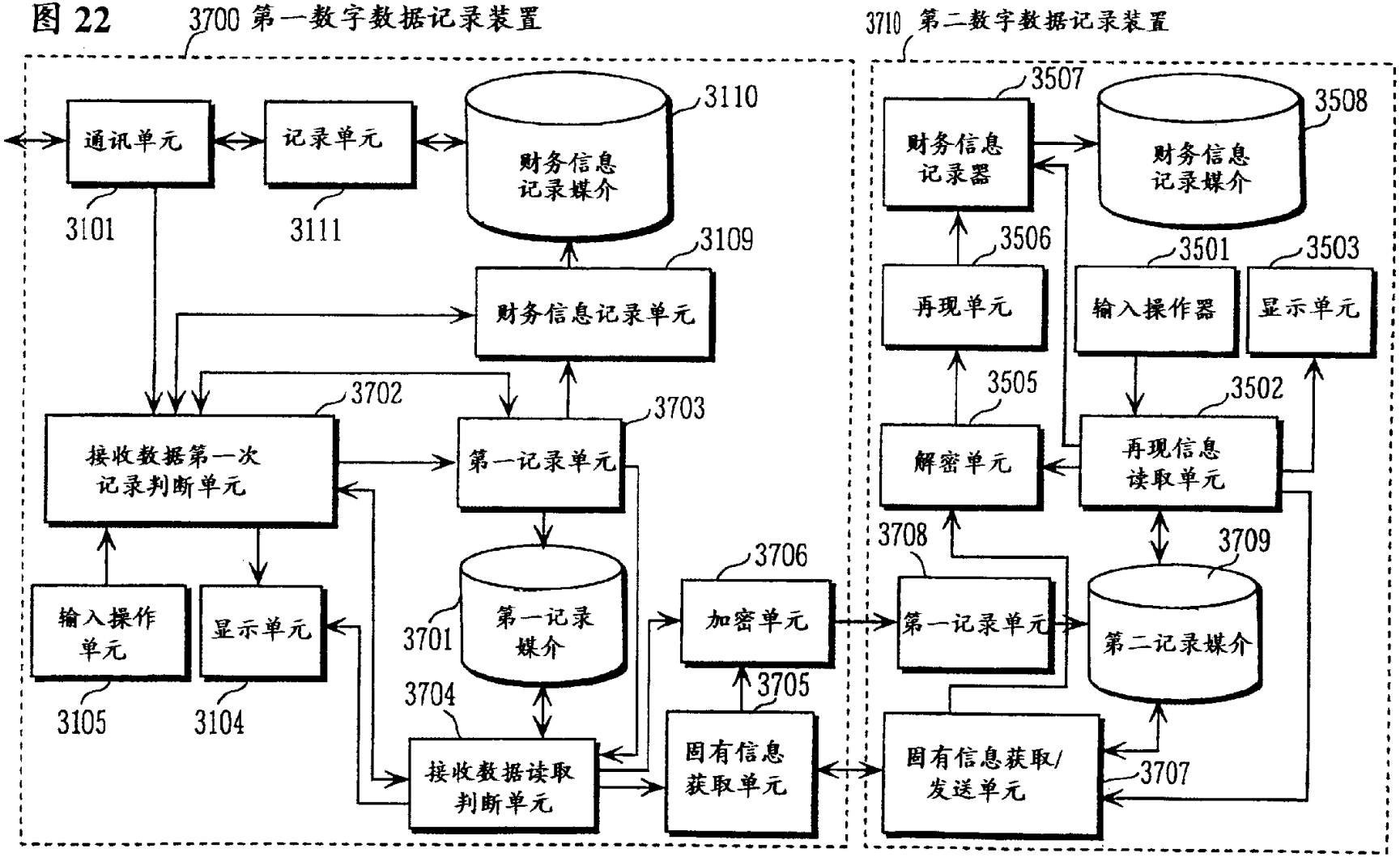

开始
S3602
申请放音乐
S3604
再现的最大次数等于或大于“1”？
否
是
S3608
从记录媒介中提取音乐数据
S3610
获取记录媒介的固有信息
S3612
用固有信息作为密钥解密音乐数据
S3614
解码并再现音乐数据
S3606
表明再现的最大次数超限
S3616
需支付再现一次的费用？
否
是
S3618
将财务信息记录在财务信息记录媒介上
结束

图 21

图 22


3700 第一数字数据记录装置
3710 第二数字数据记录装置
通讯单元
记录单元
财务信息记录媒介
3110
3101
3111
3109
财务信息记录单元
3702
3703
接收数据第一次记录判断单元
第一记录单元
输入操作单元
显示单元
第一记录媒介
3701
3706
加密单元
3705
3704
3105
3104
接收数据读取判断单元
固有信息获取单元
3507
财务信息记录器
财务信息记录媒介
3508
3506
3501
3503
再现单元
输入操作器
显示单元
3505
3502
解密单元
再现信息读取单元
3708
3709
第一记录单元
第二记录媒介
固有信息获取/发送单元
3707

属性信息 3801

曲名	表演者	曲名代码 (3805)	第一次记录费用	第二次记录费用 (3802)	再现一次的费用	再现的最大次数	加密情况	复制许可 (3803)	复制许可 (3804)	…
音乐A	a	歌曲01	¥0	¥100	¥0.5	100次	已加密	只许一次	只许一次	…
音乐B	b	歌曲02	¥10	¥10	¥0	无数次	未加密	允许	允许	…
音乐C	c	歌曲03	¥0	¥0	¥1	50次	已加密	只许一次	只许一次	…
音乐D	d	歌曲04	¥0	¥30	¥5	50次	已加密	只许一次	只许一次	…
音乐E	e	歌曲05	—	—	—	—	未加密	不允许	不允许	…

图 23

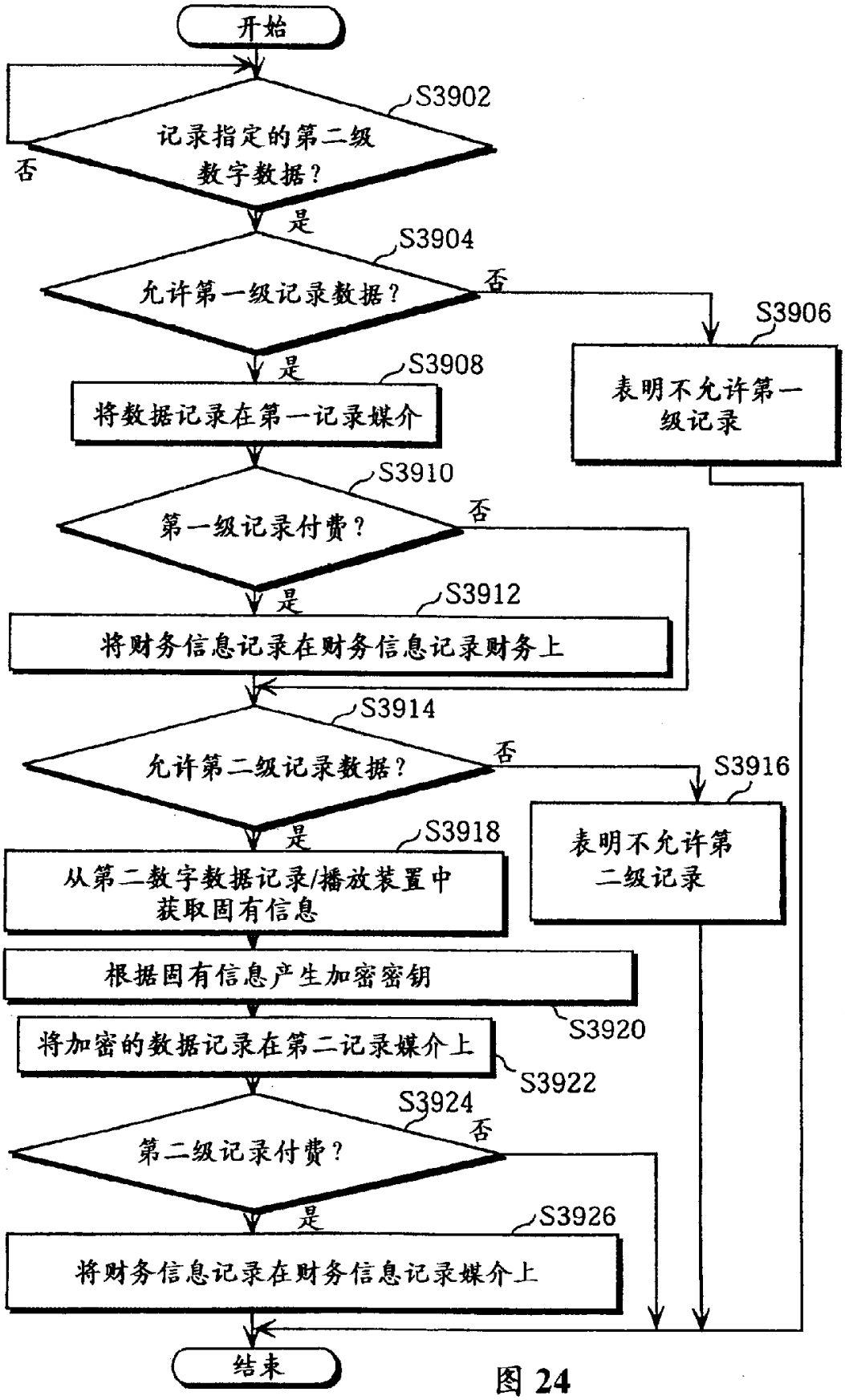

开始
S3902
记录指定的第二级数字数据？
否
是
S3904
允许第一级记录数据？
否
S3906
表明不允许第一级记录
是
S3908
将数据记录在第一记录媒介
S3910
第一级记录付费？
否
是
S3912
将财务信息记录在财务信息记录财务上
S3914
允许第二级记录数据？
否
S3916
表明不允许第二级记录
是
S3918
从第二数字数据记录/播放装置中获取固有信息
根据固有信息产生加密密钥
S3920
将加密的数据记录在第二记录媒介上
S3922
S3924
第二级记录付费？
否
是
S3926
将财务信息记录在财务信息记录媒介上
结束

图 24

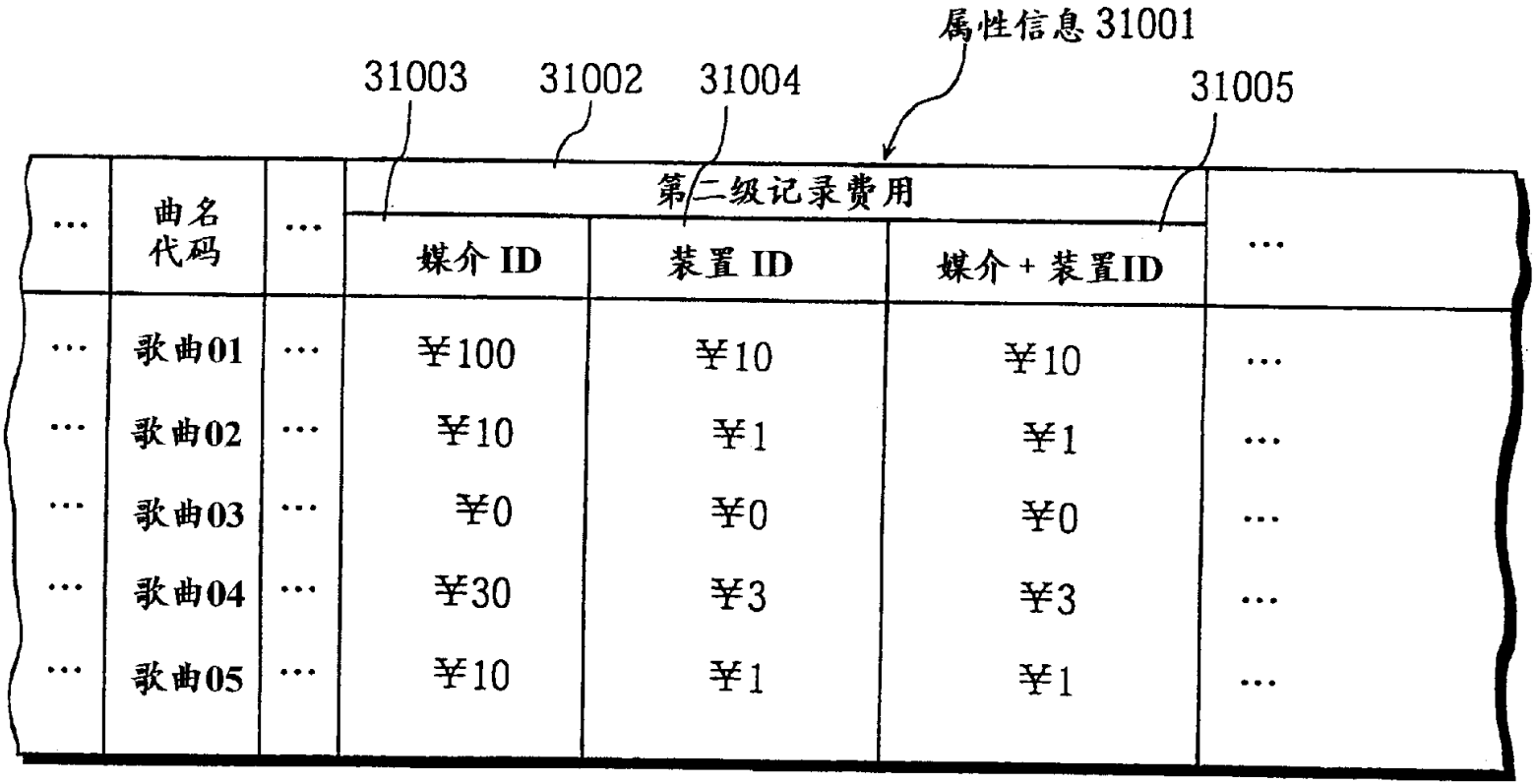

属性信息 31001
31003
31002
31004
31005
…
曲名代码
…
第二级记录费用
媒介 ID
装置 ID
媒介 + 装置ID
…
…
歌曲01
…
¥100
¥10
¥10
…
…
歌曲02
…
¥10
¥1
¥1
…
…
歌曲03
…
¥0
¥0
¥0
…
…
歌曲04
…
¥30
¥3
¥3
…
…
歌曲05
…
¥10
¥1
¥1
…

图 25