

[19] 中华人民共和国国家知识产权局

[ 51 ] Int. Cl<sup>7</sup>

G11B 20/00

H04N 7/167

H04N 7/26

H04N 5/913

G06F 1/00



# [12] 发 明 专 利 说 明 书

专利号 ZL 99802770.7

[45] 授权公告日 2005 年 12 月 14 日

[11] 授权公告号 CN 1231911C

[22] 申请日 1999. 10. 7 [21] 申请号 99802770.7

[30] 优先权

[32] 1998. 10. 8 [33] JP [31] 286177/98

[32] 1998. 10. 19 [33] JP [31] 297159/98

[32] 1998. 10. 19 [33] JP [31] 297142/98

[86] 国际申请 PCT/JP1999/005516 1999. 10. 7

[87] 国际公布 WO2000/021087 英 2000. 4. 13

[85] 进入国家阶段日期 2000. 8. 8

[71] 专利权人 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 小塚雅之

青山升一 德田克己 平田升

审查员 郭 雯

[74] 专利代理机构 中国专利代理(香港)有限公司

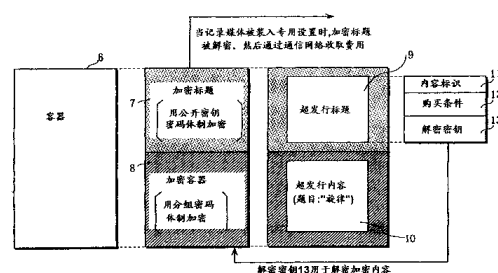
代理人 吴立明 王忠忠

权利要求书 3 页 说明书 29 页 附图 20 页

[54] 发明名称 用于实现超发行的系统

[57] 摘要

一种记录媒体, 存储已按照分组密码体制被加密的零售内容和超发行内容。超发行标题被附于该超发行内容, 并按照公开密钥密码体制被加密。该超发行标题包含用于解密上述的分组密码体制的解密密钥。公开密钥密码体制的特征在于利用与通信网络相连的设备来解密。解密在该记录媒体被装入该设备时被实现, 同时通过该通信网络来收取费用。



1. 一种用于在通过柜台销售的产品的发行路线上实现超发行的系统，该系统包括：

5        一个记录设备(100)，用于通过加密超发行内容而生成加密的超发行内容，并且把所加密的超发行内容记录到第一记录媒体(200)中，第一记录媒体(200)还记录了要销售的内容并且作为产品销售；

10        一个专用设备(300)，当把第一记录媒体(200)插入到所述专用设备中时，所述专用设备向用户提供基于收费地使用所加密的超发行内容，并且在所述用户接受所述提供的情况下，通过解密所加密的超发行内容来恢复所述超发行内容，并且再现所述超发行内容或者将所述超发行内容拷贝到第二记录媒体(650)；和

15        一个收费中心(600)，所述收费中心，在所述用户接受所述提供的情况下，通过在因特网上与所述用户进行通信来向所述用户收取其使用所述超发行内容的费用。

2. 如权利要求1所述的系统，其中

      第一记录媒体(200)包括向所述用户推销所述超发行内容的推销信息；和

20        所述专用设备通过再现所述推销信息来向所述用户提供对所述超发行内容的使用。

3. 如权利要求2所述的系统，其中

25        所述基于收费地使用超发行内容受到如下两项之一的限制：(i) 用户能够再现所述超发行内容或者将所述超发行内容拷贝到第二记录媒体(650)的次数，或者(ii) 用户能够再现所述超发行内容或者将所述超发行内容拷贝到第二记录媒体(650)的时间段，和

      所述专用设备，在显示所述推销信息时，显示要收取费用的数额，该数额与(a)用户能够再现或者拷贝所述超发行内容的多个次数或(b)多个时间段对应。

4. 如权利要求1所述的系统，其中

30        所述记录设备(100)包括：

      存储装置，用于存储要被记录到所述第一记录媒体上的至少一个内容；

选择装置，用于选择作为超发行内容的内容，对该内容进行再现和/或将其拷贝到第二记录媒体（650）需要收取费用；

5 第一加密装置，用于按照第一密码系统对所选择的超发行内容进行加密，以防止超发行内容在收取费用之前被再现以及被拷贝到第二记录媒体（650）；

生成装置，用于生成超发行信息头，该信息头包含用于解密所加密的超发行内容的密钥信息；

10 第二加密装置，用于按照能比第一密码系统保证更高安全性的第二密码系统来加密所生成的超发行信息头，并用于把所加密的超发行信息头附加到所加密的超发行内容上；以及

记录装置，用于把所加密的超发行内容和所加密的超发行信息头记录到第一记录媒体（200）上。

5. 如权利要求 1 所述的系统，其中

所述专用设备包括：

15 加载装置，用于加载第一记录媒体（200）或第二记录媒体（650），其中第二记录媒体（650）只供在家使用；

读取装置，用于在所加载的记录媒体是第一记录媒体（200）时，从所述加载的第一记录媒体（200）中读取所述超发行内容；

20 提供装置，用于向所述用户提供把所述超发行内容拷贝到第二记录媒体（650）；

接收装置，用于接收来自所述用户的输入；

解密装置，用于在所接收到的输入表明所述用户接受把所述超发行内容拷贝到第二记录媒体（650）的提供的情况下，解密所读取的超发行内容；

25 收费装置，用于在所接收到的输入表明所述用户接受所述提供的情况下，向所述用户收取费用；以及

记录装置，用于在所加载的记录媒体是第二记录媒体（650）时，把已解密的超发行内容记录到第二记录媒体（650）上。

6. 如权利要求 5 所述的系统，其中

30 所述专用设备还包括：

提取装置，用于在所述加载装置加载了第二记录媒体（650）的情况下，从第二记录媒体中提取第二记录媒体的唯一标识信息；以

及

重新加密装置，用于把所提取的标识信息用作加密密钥来重新加密已被解密的超发行内容，

5 其中，所述记录装置把重新加密的超发行内容记录到已从其提取了标识信息的第二记录媒体上。

7. 如权利要求 1 所述的系统，其中

所述专用设备包括：

加载装置，用于加载第一记录媒体（200）；

10 读取装置，用于从所述加载的第一记录媒体（200）中读取所述超发行内容；

提供装置，用于向用户提供（a）再现所述超发行内容的受限次数或者（b）在受限的时间段期间再现所述超发行内容的受限次数；

接收装置，用于接收来自所述用户的输入；

15 解密装置，用于在所接收到的输入表明所述用户接受所述提供的情况下，解密所读取的超发行内容；

收费装置，用于在所接收到的输入表明所述用户接受所述提供的情况下，向所述用户收取再现费用；以及

再现装置，用于再现所解密的超发行内容。

## 用于实现超发行的系统

5           本发明涉及一种存储比如音乐的内容（有版权的数字产品）的记录媒体，一种把内容录制到记录媒体上的设备，一种播放记录媒体上所录制内容的设备，一种将多个内容打包而产生数据包的设备，一种计算机可读的记录媒体，一种录制方法，一种回放方法，以及一种打包方法。

10           近来，关于有版权音乐发行的下一代形式的大量讨论发生在主要的音乐公司，音频设备制造商，和知识分子之间。目前，所有形式的音乐，不论流行、摇滚、或古典，在出售时都是录制在一种记录媒体，比如 CD（光盘）或磁带上的。这种用户通过购买一种记录媒体而获得所录制音乐的方法在世界各地都很普遍。

15           当前许多注意力集中到了将电子音乐发行作为一种可供选择的替代采用记录媒体的传统发行形式的方法。电子音乐发行指的是通过不断扩展的互联网进行音乐“内容”的收费发送。此处的“内容”指的是数字形式的有版权产品，因而“音乐内容”是数字形式的音乐。这种电子音乐发行的一个特征就是，音乐内容可利用电子商务被订购和支付。详细地，音乐公司可以在它们的主页上介绍各种音乐，因而用户能通过访问这些音乐公司的主页而浏览各种音乐内容。当找到想要的音乐内容时，该用户发送必要的信息，比如对该音乐内容的订购单和用户标识，到运行该主页的音乐公司，然后音乐公司通过与该用户预先所登记的信用卡号所对应的银行帐户为此音乐内容向该用户收费。该用户被收费后，该用户将该音乐内容下载到他的计算机里。这样，用户便能获得想要的音乐内容。

25           电子音乐发行允许用户交互地选择要下载的音乐内容。这极大地简化了用户购买音乐的过程，因此可以提高唱片公司的销售量。作为一个例子，唱片公司可以利用介绍流行的新发行唱片的主页来促销其它相关的同一艺术家和/或同一歌曲作者发行的唱片。因为用户很有可能也对这些其它的发行唱片感兴趣，所以很有可能用户会进行进一步的购买。

然而，目前电子音乐发行所要求的基础结构还未完全实现，因此用户在电子购买音乐时面临着各种困难。

5 音乐内容的电子发行的一个基本要求是提供高速通信线，它能在短时间内传送音乐内容中的几兆字节数据。目前，大多数用户访问互联网是通过公共网络，其传输速率对于实现这个目标完全不够。这意味着通过公共网络下载多个音乐内容会花较长时间。在此期间，用户会招致大量通信费用，这可能甚至会超过这些音乐内容的价钱。这自然阻碍了用户电子购买音乐，还有用户必须等待的长时间也是。这会导致用户在一个内容还正在下载时取消购买。

10 与电子音乐零售一样，采用记录媒体的传统零售方法也能促销与给定产品相关的发行唱片。这通常是通过在给定产品的唱片封套上印刷其它发行唱片的促销材料和销售信息来实现的。如果该促销材料成功地引起了用户的兴趣，该用户就会去访问唱片店再购买包含了相关发行唱片的另一记录媒体。

15 音乐媒体的零售价格是由与制造和发行该媒体相关的各种成本决定的。这意味着购买存储了新发行唱片的记录媒体和存储了相关音乐的记录媒体的用户必须为这两种记录媒体支付相对较高的费用。如上所述，用户必须访问唱片店以购买相关的发行唱片。因为对相关发行唱片感兴趣的户不能立即购买它们，等这些用户去唱片店时他们可能已经不再想要这些发行唱片了，唱片公司因此而冒风险。

20 如上所述，音乐可由多种方式发行，包括录制到媒体上和通过通信线比如互联网传输。

25 各种记录媒体，比如 DVD - Audio（数字多功能盘-音频）唱片和 CD，可用于录制音乐。通常，录制在不同媒体上的音乐是采用不同方式编码的。音乐内容也常常利用广播波通过卫星，CATV（共用天线电视）电缆等来发行。这类服务通常是收费的，但有时为了促销目的音乐也被免费提供。

30 然而，当采用不同方法发行同一音乐时，为了下述的原因该音乐必须用多种方式编码来为每种发行方法产生合适的音乐内容。关于版权保护系统、加密密钥的安全性、以及回放功能的提供（或缺乏）在新老回放设备间存在着巨大的差异，因此对每种回放设备只

产生和发行一种音乐内容会使某些回放设备不能使用它们的版权保护系统或实现它们的大多数回放功能。

5 如果某一音乐内容被分发到某些配备了版权保护系统的回放设备，将该音乐内容的所有发行形式用安全加密密钥进行加密似乎是明智的。然而，用这种方式发行的一些音乐内容是仅用于促销的样品，因而并未进行高质量的编码。如果这些内容也用安全加密密钥进行加密的话，不能解密这些内容的回放设备就不能播放该样品。这限制了提供样品给用户的促销效果。

10 当更多数量的音乐内容由于上述原因而需要采用不同的编码方法来进行编码时，就要求内容供应商更加小心地管理和发行这些内容，以防止这些内容被发行到错误的目的地去。例如，如果这么大量的用于销售的音乐内容错误地代替免费促销的内容而被发行，这将会导致内容供应商的重大损失。

15 本发明的第一目的是提供一种记录媒体，购买音乐内容的用户因此可以方便地以较低的价格获得其它相关的音乐内容。

本发明的第二目的是提供一种内容打包设备，它能把音乐内容传送到不同类型的回放设备，不论是否提供（或缺乏）版权保护系统，加密密钥的安全性，和该回放设备的回放性能。

20 第一目的可由一种记录媒体来实现，它存储：第一内容；已按照第一密码体制加密的第二内容；以及已按照第二密码体制加密的标题，标题包含用于解密第二内容的第一密钥信息，标题附于第二内容，其中的第二密码体制的特征是利用第二密钥信息来解密，该第二密钥信息预先被提供给预定设备。

25 当上述记录媒体存储新的发行唱片作为第一内容，相关的发行唱片作为第二内容时，购买该记录媒体中第一内容的用户可以通过解密上述的第一和第二密码体制来购买相关的发行唱片。这些密码体制可以这样被解密，把该记录媒体加载到上述的预定设备上以获得第二密钥信息来解密第二密码体制，第二密钥信息是预先被提供给该预定设备的。相应地，拥有该预定设备的用户不必通过通信网  
30 络下载这些内容，而这会花较长时间，还能方便地购买相关的发行唱片，而不必访问唱片店。

另外，用户只需支付一种记录媒体制造和发行的成本，因此该

第二内容的价格可以定得较低。

如果一个内容的再现或录制到另一记录媒体上是收费的，则有  
必要防止该内容在未收费时被再现或录制。为此，采用高安全性的  
加密算法，比如采用公开密钥的算法来加密该内容似乎是明智的，  
5 然而高安全性算法的解密需要高负荷运行和较长的解密时间，尤其  
当此内容有几兆字节时。利用本发明，通过把超发行  
(superdistribution)内容存储为上述的第二内容，并采用复杂的公  
开密钥加密算法作为上述的第二密码体制，仅用于加密标题，这样  
用来解密该第二内容的时间会更短，比起该第二内容按此复杂的第  
10 二密码体制被加密的情况。当用户决定播放或购买该第二内容时，  
该第二内容可被迅速解密，利用从标题获得并提供给用户的解密密  
钥信息。这样解密所需的时间远远短于电子下载同样内容所需的时  
间。这样，本技术成功地让用户可以迅速再现或购买该超发行内容。

这里的预定设备也许能够收费，其中的标题可能包含使用限制  
15 信息来显示：该第二内容的再现是否允许；允许再现的次数；是否  
允许把该第二内容录制到另一记录媒体；以及允许录制的次数，和  
费用信息来显示，当该第二内容的再现被允许时，由预定设备对此  
第二内容的再现将收取的费用，以及当把该第二内容录制到另一记  
录媒体上被允许时，由该预定设备对此录制将收取的费用。

20 采用上述结构，该记录媒体会限制该第二内容的再现次数和把  
该第二内容录制到另一记录媒体上的次数，以防止该第二内容被再  
现和录制到另一媒体。这使得制造商能够阻止人们复制该第二内容，  
或者过度地再现该第二内容，从而阻止该第二内容的艺术吸引力衰  
减。

25 这里的预定设备也许能够收费，其中的标题可能包含使用限制  
信息来显示：该第二内容的再现是否允许；允许再现的时期；把该  
第二内容录制到另一记录媒体是否允许；以及允许录制的时期，和  
费用信息来显示，当该第二内容的再现被允许时，由该预定设备对  
此第二内容的再现将收取的费用，以及当把该第二内容录制到另一  
30 记录媒体被允许时，由该预定设备对此录制将收取的费用。

采用上述结构，只有在使用限制信息所显示的时期内该第二内  
容才可被再现和录制到另一记录媒体。这使得制造商能够提高该第

二内容的价值，通过仅把它提供给用户一段有限的时间。

第一目的可以这样实现，由一台数字数据录制设备来把包含至少一个内容的数字数据录制到一种记录媒体，该数字数据录制设备包括：存储单元，用于存储要被录制到该记录媒体上的至少一个内容；选择单元，用于选择一个内容，其再现和/或录制到另一记录媒体需要作为超发行内容来收费；第一加密单元，用于按照第一密码体制来对所选的超发行内容加密以防止该超发行内容在收费前被再现或录制到另一记录媒体；发生单元，用于产生超发行标题，包含密钥信息以解密上述被加密的超发行内容；第二加密单元，用于按照比第一密码体制保证更高安全性的第二密码体制来加密所产生的超发行标题，并把该加密的超发行标题附于上述加密的超发行内容；以及录制单元，用于把加密的超发行内容和加密的超发行标题录制到该记录媒体上。

采用上述结构，该数字数据录制设备从多个要被录制到另一记录媒体上的内容中选择一个内容，其再现和录制到另一记录媒体应作为超发行内容来收费。接着该数字数据录制设备加密该超发行内容以防止该超发行内容在未收费时被再现或录制到另一记录媒体上。由于该超发行标题被附于该加密的超发行内容，该超发行标题中包含密钥信息，供专用设备在该超发行内容被再现或/和购买时使用，这样每当用户播放该超发行内容时或者当用户把该超发行内容录制到另一记录媒体上时，都能付款给内容供应商。

第一目的也可这样实现，由一台数字数据录制设备来把包含超发行内容的数字数据从第一记录媒体录制到第二记录媒体上，该超发行内容已被加密以防止该超发行内容在收费前被录制到另一记录媒体上，该数字数据录制设备包括：加载单元，用于把第一记录媒体和第二媒体之一装入该数字数据录制设备；读取单元，用于在被加载的记录媒体是第一记录媒体时从该被加载的第一记录媒体中读取该超发行内容；显示单元，用于向用户显示录制的费用；接收单元，用于接收用户的输入；解密单元，如果接收到的输入显示用户同意付费时，用于解密读取的超发行内容；收费单元，用于如果接收到的输入显示用户同意付费时向用户收费；以及录制单元，当被加载的记录媒体是第二记录媒体时，用于把已解密的超发行内容录

制到该第二记录媒体上。

按照上述结构，只有当用户同意购买该用户已购买的第一记录媒体上的超发行内容时，上述的数字数据录制设备才会对该超发行内容收费。由于用户不需要通过通信网络下载该超发行内容，在电子音乐发行所要求的基础结构还未完全实现，从而通信网络的传输速度也较低的状态下，用户被收取的通信费用可减到最少。因此，该超发行内容可以很低成本出售。

第一目的也可这样实现，由一台回放设备来再现写在一种记录媒体上的包含至少一个超发行内容的数字数据；该超发行内容已被加密以防止该超发行内容在收费前被再现，该回放设备包括：加载单元，用于把该记录媒体装入该回放设备；读取单元，用于从该被加载的记录媒体中读取上述的超发行内容；显示单元，用于向用户显示再现费用；接收单元，用于接收用户的输入；解密单元，如果接收到的输入显示该用户同意支付再现费用时，用于解密所读取的超发行内容；收费单元，用于向用户收取再现费用，如果接收到的输入显示该用户同意支付再现费用时；以及再现单元，用于再现已解密的超发行内容。

采用上述的回放设备，如果接收到的输入显示用户同意支付再现费用，收费单元便向该用户收取再现费用。这样使得内容供应商可以在每次该超发行内容被再现时向该用户收费。

第二目的可这样实现，由一台内容打包设备来产生包含多个内容的数据包，该内容打包设备包括：编码单元，用于利用不同方法来对要被发行的产品编码以产生多个内容，每个内容的再现质量都不同；分级单元，用于给每个产生的内容划分等级，按照该内容的再现质量；表存储单元，用于存储包含了多个等级和多个对的表，每个对包含加密密钥信息和加密算法信息，并与由分级单元所划分等级中的一个不同的等级对应；加密单元，用于参考上表和加密已被划分等级的每个内容，加密是利用对应于该等级的对所指示的加密密钥和加密算法；以及打包单元，用于将这多个已被加密的内容打包以产生该数据包。

采用上述结构，该内容打包设备利用不同方法对要被发行的产品编码以产生多个内容，每个内容的再现质量都不同。接着该内容

打包设备把这多个内容打包以产生一个数据包。因此，每个目标内容回放设备能从传来的内容包中选择一个内容，按照该内容回放设备的硬件性能。于是，内容供应商可以发送不同质量的内容，而不需考虑目标内容回放设备的不同再现条件，同时这些内容的版权受到保护。

第二目的可以这样实现，由一台内容打包设备来产生包含多个内容的数据包，该内容打包设备包括：编码单元，用于利用不同方法来对被发行的产品编码，于是该产品的一部分作为样品内容加密，该产品的剩余部分作为主内容加密；分级单元，用于把某预定等级划分给上述的样品内容，更高的等级划分给上述的主内容；表存储单元，用于存储包含了上述的预定等级、更高等级、和两个对的表，每个对包含加密密钥信息和加密算法信息，一对与该预定等级对应，另一对与该更高等级对应；加密单元，用于在参考上表后，利用上述的一对所指示的加密密钥和加密算法加密已分级的样品内容，并利用上述的另一对所指示的加密密钥和加密算法加密已分级的  
主内容；以及打包单元，用于将已被加密的样品内容和已被加密的主内容打包以产生该数据包。

按照上述内容打包设备，较小的内容包可通过每种发行方法被传送，也可被录制到一种记录媒体上，比如硬盘或采用较小存储区的 CD-ROM（光盘只读存储器）。

本发明的这些和其它目的、优点和特征从下面的描述连同其附图中将会变得明显，附图中举例说明了本发明的一个具体实施方案。

在附图中：

- 图 1A 显示了增强 CD 的外观；
- 图 1B 显示了该增强 CD 的数据结构；
- 图 2A 显示了 DVD 唱片的外观；
- 图 2B 显示了该 DVD 唱片的逻辑格式；
- 图 3 显示了内含一种零售记录媒体的塑料外壳，；
- 图 4 显示了容器 6 的数据结构；
- 图 5 显示了购买条件 12 的例子；
- 图 6 显示了零售内容 3 和超发行内容 10 是如何被发行的；
- 图 7A - 7D 显示了一些状态，其中超发行内容从一种零售记录媒

体 200 被录制到买来拷贝的记录媒体 650 上;

图 8 显示了交互屏幕的一个例子, 由回放设备利用回放控制命令表 4 和静态图象数据 5 显示;

图 9 显示了第二实施方案的数字数据录制设备 100 的结构;

5 图 10 是个流程图, 显示了数字数据录制设备 100 的处理流程;

图 11 显示了第三实施方案的数字数据录制设备 300 的内部结构;

图 12 是个流程图, 显示了数字数据录制设备 300 中的编码单元 303 的处理流程;

10 图 13 显示了第四实施方案的数字数据回放设备 400 的内部结构;

图 14 是个流程图, 显示了数字数据回放设备 400 中的编码单元 303 的处理流程;

图 15 显示了按照第五实施方案发行内容包的各种方法;

15 图 16 显示了按照第五实施方案的内容打包设备 700 和内容回放设备 801-809 的内部结构;

图 17A 显示了第一对应表的一个例子;

图 17B 显示了第二对应表的一个例子;

20 图 17C 显示了按照第五实施方案存储在硬件等级/解密对应表存储单元中的表的一个例子;

图 18 显示了按照第五实施方案由内容打包单元 709 来打包的一个内容包;

图 19 显示了按照第六实施方案的内容打包设备 700 和内容回放设备 801-809 的内部结构;

25 图 20 显示了按照第六实施方案由内容打包单元 709 来打包的一个内容包;

下面参考几种实施方案描述了本发明的记录媒体、回放设备、和录制设备。为便于说明, 记录媒体、回放设备和录制设备将分别采用第一到第六实施方案来进行说明。

### 30 第一实施方案

第一实施方案描述了一种用于音乐内容的零售的记录媒体。待售的音乐内容称为零售内容, 它们在买卖前已被录制到称为零售记

录媒体的记录媒体上。本实施方案中用到了两种类型的零售记录媒体。第一种是增强 CD，它是由内区和外区组成的一张盘，内区的物理结构与 CD 相同，比如数字音频光盘（CD-DA），外区的物理结构同 CD-ROM。增强 CD 因此同时起到 CD-DA 和 CD-ROM 的作用。图 1A 显示了增强 CD 的外观，图 1B 显示了该增强 CD 的数据结构。如图 1A 和 1B 所示，增强 CD 的内区称为 CD-DA 区，外区称为 CD-ROM 区。按功能，CD-DA 区可被称为内容区 1，因为它存储零售内容 3，CD-ROM 区可被称为增值区 2，因为它存储的数据向整个记录媒体增值。这种记录媒体是一种零售记录媒体，用于销售存储在内容区 1 中的零售内容 3。

本实施方案中用到的第二种类型的记录媒体是存储零售内容 3 的 DVD 唱片。图 2A 显示了该 DVD 唱片的外观，图 2B 显示了该 DVD 唱片的逻辑格式。尽管 DVD 唱片并不象增强 CD 唱片那样有 CD-DA 区或 CD-ROM 区，它把回放控制命令表 4，静态图象数据 5，和容器 6 保存为可被个人电脑访问的不同文件，并有与增强 CD 唱片相同的功能数据结构，也就是说，DVD 唱片包括存储零售内容 3 的内容区 1 和存储向整个记录媒体增值的数据的增值区 2。增强 CD 和 DVD 唱片的主要区别是，零售内容 3 是按照原状被录制到增强 CD 的内容区 1 的，而它在被录制到 DVD 唱片的内容区 1 之前已用对这一张 DVD 唱片唯一的标识信息被加密。

这些记录媒体均分别封装于一个塑料盒内，连同印好的插件。图 3 显示了一个专门为采用象传统音乐 CD 那样的方式来封装这些记录媒体而设计的塑料盒。当内容区中的零售内容 3 是以“歌曲”为标题的音乐时，该标题“歌曲”和相关图象被印刷在该记录媒体的封套上，如图 3 所示。

如上所述，内容区 1 和增值区 2 在增强 CD 和 DVD 唱片上都有。下面说明增值区 2 保存的内容。图 1B 和 2B 的右列显示了增值区 2 所存储的内容。如图所示，增值区 2 存储回放控制命令表 4，静态图象数据 5，和容器 6。

回放控制命令表 4 是描述，当本实施方案的记录媒体被装入一台设备时，应该显示在该设备的交互屏幕上的信息。回放控制命令表 4 是用比如 MACROMEDIA DIRECTOR 或 HTML 的格式来写的。

MACROMEDIA DIRECTOR 格式是用来描述编辑过程的,可被运行在 MS - WINDOWS 或 MAC OS 上的软件解释,而 HTML 是用来写网页的,由浏览器显示。

5 静态图象数据 5 是根据回放控制命令表 4 要被显示在该设备的交互屏幕上的静态图象。

传统的增强 CD 存储回放控制命令表和静态图象数据用于显示信息,比如歌词,或是该零售内容的宣传录象,或是一个歌迷俱乐部的介绍,或是关于其它新发行唱片的信息。然而,本实施方案中的回放控制命令表 4 和静态图象数据 5 不是用来显示零售内容 3 的信息,而是用来显示推荐另一不同音乐内容的购买和回放的信息。

例如,如果零售内容 3 是一位流行艺术家的新发行唱片,回放控制命令表 4 能显示信息来推荐购买和回放该同一艺术家以前的热门歌曲。从下面的说明中可以清楚由回放控制命令表 4 所引荐的具体音乐内容。

15 下面说明本实施方案的增强 CD 和 DVD 唱片中均包含了的增值区 2 中的容器 6。图 4 显示了容器 6 的结构。如图所示,容器 6 包括加密标题 7 和加密内容 8。加密标题 7 是已被加密的超发行标题 9,加密内容 8 是也已被加密的超发行内容 10。

20 “超发行”是一种发行内容的方法的名称,是由 Tsukuba 大学的荣誉退休教授 Ryoichi Mori 所提倡的。在超发行中,预定的超发行标题被附于要被发行和销售的内容。这样的超发行标题包含贷方信息来指示要被付款的债权人,和购买信息来指示购买条件。当用户使用该内容时,用户的设备翻译该贷方信息和购买信息以建立一个用户记录。该用户按照该用户记录向债权人支付。

25 超发行标题 9 和超发行内容 10 保存在容器 6 内,其前提是它们适于超发行。由静态图象数据 5 和回放控制命令表 4 所推荐的正是已被加密和保存在容器 6 内的这个超发行内容 10。

30 如上所述,超发行标题 9 指示机密信息用于安全地实现超发行,比如贷方信息和购买信息,它们需要保护来防止欺诈行为,比如篡改。为此,本实施方案的超发行标题 9 包括一个数据区,它已按照基于公开密钥加密算法的密码体制被加密。注意整个超发行标题 9 可被加密来作为代替,这正是下面说明中的案例。广泛应用的公开

密钥加密系统包括椭圆曲线加密系统和 Rivest, Shamir, Adleman 加密 (RSA)。公开密钥密码体制是高度安全的, 因为已用公开密钥加密的数据只能由不同的密钥来解密。本实施方案采用公开密钥密码体制来加密超发行标题 9, 但这个公开密钥密码体制被改进了, 体现在用于解密加密的超发行标题 9 的解密密钥被预先提供给一台专用设备, 以及该加密的超发行标题 9 在零售记录媒体被装入该专用设备时被解密。更详细地, 该专用设备与通信网络连接, 并通过该通信网络向用户正确收费, 当该超发行内容 9 被解密和该专用设备再现超发行内容 10 或把它录制到另一记录媒体上时。这保证了用户会为使用超发行内容 10 而向版权所有者的付款。

注意当不同的超发行内容需要被录制到一张零售记录媒体上时, 每个超发行内容的超发行标题都用不同的公开密钥加密, 而该专用设备用公共解密密钥来解密这些超发行标题。注意尽管在本实施方案中用于回放和/或购买超发行内容的费用通过通信网络收取, 该费用也可由另一设备收取, 通过传送费用信息到另一记录媒体, 比如 IC 卡或预付卡, 并令上述的另一设备按照该 IC 卡或预付卡操作。

对于上述结构, 用于解密超发行标题的解密密钥不是被提供给零售记录媒体, 而是提供给专用设备的。因此, 如果购买了该零售记录媒体的人试图用未授权的设备来解密该超发行标题 9, 要解密加密的超发行标题 9 将是极其困难的。这是因为用于解密超发行内容 10 的解密密钥包含于超发行标题 9 内。这种解密密钥将在后面描述。因此, 超发行内容 10 的解密也变得很难, 于是超发行内容 10 可以安全地被发行。

注意在零售记录媒体的封套上没有给出超发行内容 10 的指示, 如图 3 所示。这是为了防止用户在购买存储了零售内容 3 的零售记录媒体时认为超发行内容 10 是被免费提供的。

下面参考图 4 说明存储在超发行标题 9 中的元素。如图 4 所示, 该超发行标题 9 包含内容标识 11, 购买条件 12, 和解密密钥 13。

内容标识 11 是用来把超发行内容 10 从其它内容中识别出来的标识信息。由于超发行内容 10 是音乐内容, 例如国际标准记录代码 (ISRC) 的标识信息被写作内容标识 11。ISRC 是提供给每首歌曲的

标识信息，包含国家代码（两个 ASCII 字符），录制年份（一个两位数），和系列号（一个五位数）。

5 购买条件 12 是关于超发行内容 10 的购买条件的信息。图 5 示出了购买条件 12 的一个例子。如图 5 的右列所示，购买条件 12 指示如下：“允许播放次数”；“数字输出允许”；“回放允许到期时间”；“回放允许到期日期”；以及“费用信息”。

“允许播放次数”是一个整数，指示该超发行内容 10 可被再现的次数限制。

10 “数字输出允许”指示超发行内容 10 是否允许通过专用设备的数字输出终端被输出，如果该专用设备有这样的终端。如果这样，“数字输出允许”还用了一个整数来指示数字输出的次数限制。

“回放允许到期时间”指出超发行内容 10 不能继续被再现的到期时间点。

15 “回放允许到期日期”指出该回放允许到期的日期。过了这个到期日期之后，超发行内容 10 不能继续被再现。

20 “费用信息”指出当用户再现超发行内容 10 时所收取的费用和用于购买超发行内容 10 的费用。注意购买费用是在用户把容器 6 中的超发行内容 10 录制到另一记录媒体上时收取的，而回放费用是在使用基础上按用户已经再现超发行内容 10 的次数来收取的。在电子商务中，该费用信息是带有购买签名的申请表，也就是说，拥有零售记录媒体的用户申请超发行内容 10 的购买或回放是通过令专用设备把费用信息连同用户标识传送给音乐公司的帐单办公室的主机。已装入了零售记录媒体的专用设备通过通信网络实现上述传送。帐单办公室知道用户预先登记的信用卡号，便向用户收取购买或回放费用，通过参考发送用户的标识从相应于该用户信用卡号的银行帐户提取该费用。

30 解密密钥 13 解密加密内容 8 以产生超发行内容 10。该超发行内容 10 是某种格式的音乐内容，比如线性脉冲编码调制（LPCM），高级音频编码（AAC），或数字影院系统（DTS），并用分组密码体制加密。分组密码体制把要被加密的内容分成一定长度的块，并以块为单位加密内容。DES（数据加密标准），其中的一块为 64 位长，或 RC5，其中的块长度可变，是分组密码体制的例子。在分组密码体

制中，同一密钥被用于加密和解密，于是分组密码体制的安全性比公开密钥密码体制低。然而，在本实施方案中，用于解密加密内容 8 的解密密钥 13 包含于超发行标题 9 中，超发行标题 9 本身是用较高安全性的公开密钥密码体制加密的。因此，未经授权的用户要解密超发行内容 10 是极其困难的。

正如所述，采用上述结构的容器 6，解密超发行标题 9 和篡改费用信息是极其困难的，因为购买条件 12 包含在超发行标题 9 中，而超发行标题 9 已用公开密钥来加密以保证高安全性。如上所述，超发行标题 9 是用复杂的公开密钥加密来加密的，超发行内容 10 是通过简单的分组加密技术利用在超发行标题 9 中给出的解密密钥 13 来加密的。当用户决定播放或购买超发行内容 10 时，超发行内容 10 可利用从超发行标题 9 获得的解密密钥 13 迅速解密，并呈现给用户。这个解密过程所需时间会比电子下载同一内容所需的时间大大缩短。这样，本技术成功地使得用户能够迅速再现或购买超发行内容 10。

下面描述超发行标题和超发行内容上的管理信息。尽管零售内容是由存储该零售内容的 CD 或 DVD 唱片所提供的管理信息来管理的，从而该内容会被 CD 播放器或 DVD 唱片播放器认出和再现为音乐，超发行内容和超发行标题不是由这个管理信息来管理的。这是为了阻止 CD 播放器或 DVD 唱片播放器把超发行内容认作音乐和不解密超发行内容时就再现它。在这种情况下，超发行内容会被再现为噪音。因此，超发行内容和超发行标题是由独特的管理信息来管理的，以把它们从零售内容中识别出来。这个管理信息由专用设备用来检测记录媒体上的超发行标题和超发行内容的记录区的开始和结束的，当从该记录媒体读取超发行标题和超发行内容时。这里注意术语 CD 播放器和 DVD 唱片播放器不是指后面要描述的数字数据回放设备 400。

下面参考图 6 来说明零售内容 3 是如何发行给用户的，以及超发行内容 10 是如何超发行给用户的。

如图 6 中的箭头 y1 所示，安装于工厂内由音乐公司操作的数字数据录制设备 100 把零售内容 3，回放控制命令表 4，静态图象数据 5，和容器 6 录制到零售记录媒体 200 上。零售记录媒体 200 接着如

箭头 y2 所示由卡车运输到, 例如, 零售商店, 正如传统 CD 的发行那样, 这样用户就能在零售商店中买到零售记录媒体 200, 如箭头 y3 所示。

5 购买零售记录媒体 200 的用户以播放普通 CD 或 DVD 唱片同样的方式播放零售内容 3。例如, 用户可能在走路时用便携式回放设备听零售内容 3, 如箭头 y4 所示。

10 假定购买了零售记录媒体 200 的用户在他屋里有数字数据录制设备 300 和数字数据回放设备 400, 正是前面提到的连接到通信网络的专用设备。数字数据录制设备 300 把超发行内容 10 从零售记录媒体 200 录制到另一记录媒体上, 同时由音乐公司收取费用。数字数据回放设备 400 播放零售记录媒体 200 上的超发行内容 10, 也是收费的。

15 零售记录媒体 200 中的回放控制命令表 4 令数字数据录制设备 300 和数字数据回放设备 400 显示一个交互屏幕, 上面包含再现的静态图象数据 5。图 8 示出了交互屏幕的一个例子。在图 8 中, 图象 m1 是超发行内容 10 的介绍图象, 例如, 演奏超发行内容 10 的相关发行唱片的乐队的照片。消息 m2 提示用户再现超发行内容 10, 按钮 m3 和 m13 用来指出对消息 m2 的肯定和否定的响应。回放费 m4 示出超发行内容 10 的再现费用。消息 m5 提示用户购买超发行内容 10, 按钮 m6 和 m16 用来指出对消息 m5 的肯定和否定的响应。购买费 m7 示出超发行内容 10 的购买价格。该交互屏幕允许用户在零售记录媒体 200 中获知超发行内容 10, 而且如果感兴趣的话, 用户能令数字数据回放设备 400 再现超发行内容 10 或者通过数字数据录制设备 300 购买超发行内容 10。当用户购买或再现超发行内容 10 时, 数字数据录制设备 300 或数字数据回放设备 400 发送费用信息来指出购买或回放的费  
20 用, 通过通信网络 500, 到安装在音乐公司的帐单办公室的主机 600。  
25

30 图 7A-7D 显示了数字录制设备 300 把超发行内容 10 从零售记录媒体 200 录制到另一记录媒体来购买该超发行内容 10 的过程。然后, 从零售记录媒体录制了超发行内容 10 以购买它的记录媒体被称为买来拷贝的记录媒体。这里, 假定买来拷贝的记录媒体是 DVD-RAM。

如图 7A 所示, 当用户把零售记录媒体 200 和作为买来拷贝的记录媒体 DVD-RAM 650 装入数字数据录制设备 300 时, 数字数据录制设备 300 把超发行内容 10 录制到 DVD-RAM 650 上, 如图 7B 所示。当用户取出 DVD-RAM 650 时, 如图 7C 所示, 超发行内容 10 的购买就完成了。为了播放 DVD-RAM 650, 用户把 DVD-RAM 650 从其盒中取出, 并把 DVD-RAM 650 装入与 DVD-RAM 兼容的, 可播放 DVD 唱片和 DVD-RAM 的 DVD 唱片播放器。

注意数字录制设备 300 可能把超发行内容 10 录制到存储卡上, 来代替 DVD-RAM。

在本实施方案中阐明的超发行中, 超发行内容 10 的价格可设得低于零售内容 3 的零售价格。这是因为零售内容 3 的零售价格包含增强 CD 或 DVD 唱片的各种发行成本, 比如运输成本, 而超发行内容 10 的价格不包含任何发行成本, 因为它只需通过解密密码就能被购买。

本实施方案使得用户能够以交互的方式购买相关的内容, 类似于电子商务, 却不用高速通信线, 而成功的通过互联网的电子发行却要求高速通信线, 举个例子来说。

注意当增强 CD 和 DVD 唱片被用作记录媒体来存储本实施方案的音乐内容时, 混合型的 DVD 唱片同时充当 DVD 唱片和 DVD-ROM。

现在完成了适于超发行的一种数据结构的描述, 即本发明的第一实施方案。

## **第二实施方案**

第二实施方案涉及数字数据录制设备 100, 它产生一种记录媒体, 其包含的数据格式适于超发行。图 9 显示了本实施方案的数字数据录制设备 100。数字数据录制设备 100 的实现是通过把专用的应用程序安装到通用的个人计算机上, 它包含输入单元 101, 控制单元 102, 编码单元 103, 内容存储单元 104, 获取单元 105, 超发行内容加密单元 106, 超发行标题加密单元 107, 零售内容加密单元 108, 录制单元 109, 和唯一信息获取单元 110。数字数据录制设备 100 把超发行内容录制到零售记录媒体 200 上。

注意尽管本实施方案的数字数据录制设备 100 把音乐内容录制到一种零售记录媒体上, 要被录制到零售记录媒体上的数据并不局

限于此,也就是说,其它数据,比如图形数据,字符数据,或图形数据和字符数据的组合,可以被录制到该零售记录媒体上。

5 输入单元 101 被连接到一台指向设备,比如鼠标或键盘,接收来自操作者的指令来对一段音乐进行编码以获得一段编码数据,等等。

控制单元 102 翻译来自输入单元 101 的请求,并命令编码单元 103 对一段音乐进行编码,或者命令获取单元 105 获取一段存储在内容存储单元 104 中的音乐内容。

10 编码单元 103 对录制在主带等的原音乐进行编码,并压缩编码后的音乐来产生音乐内容。例如,编码单元 103 产生 LPCM 格式的数字数据,并压缩所产生的 LPCM 数字数据来产生 AAC 格式的音乐内容。产生该音乐内容后,编码单元 103 生成所产生的音乐内容的内容标识,这已在第一实施方案中描述过。注意数字数据录制设备 100 不一定必须包含编码单元 103,因为这样的编码可由,例如一台不同的设备预先进行,已被编码的音乐内容可存储在内容存储单元 104 中。

15 内容存储单元 104 是大容量的硬盘设备,存储由编码单元 103 进行编码的音乐内容和其内容标识。

按照来自控制单元 102 的指令,获取单元 105 从内容存储单元 104 获取已被编码的音乐内容和其内容标识。

20 超发行内容加密单元 106 加密超发行内容。这里,假定数字数据录制设备 100 要产生零售记录媒体 200,它拥有如图 1 或图 2 所示的相同的存储内容。这样,超发行内容加密单元 106 采用解密密钥 13 作为加密密钥来加密超发行内容 10,以产生加密内容 8。解密密钥 13 的设定可由操作者任意决定。

25 超发行标题加密单元 107 产生超发行标题 9,通过合并操作者用适于超发行的格式所写的购买条件 12,内容标识 11,和解密密钥 13。超发行标题加密单元 107 接着加密所产生的超发行标题 9 以产生加密标题 7,它被附于加密内容 8 以产生容器 6。

30 如果零售记录媒体 200 是 DVD 唱片,并且零售内容 3 需要基于对该 DVD 唱片唯一的标识信息来被加密,唯一信息获取单元 110 便获取该 DVD 唱片在制造时被录制在该 DVD 唱片上的标识信息。唯一信息获取单元 110 接着输出获取的标识信息给零售内容加密单元

108。如果零售记录媒体 200 是增强 CD，零售内容 3 不需被加密，唯一信息获取单元 110 的处理便不执行。

5 如果零售记录媒体 200 是 DVD 唱片，零售内容加密单元 108 便基于所获取的对该 DVD 唱片唯一的标识信息来加密零售内容 3。如果零售记录媒体 200 是增强 CD，零售内容 3 不需被加密，因此零售内容加密单元 108 不加密零售内容 3。基于对记录媒体唯一的标识信息的密码体制已由日本的公开专利申请号 5-257816 所公开，因而不

10 再给出其详细说明。  
录制单元 109 把容器 6 录制到零售记录媒体 200 上，容器 6 由超发行标题加密单元 107 和零售内容 3 产生，零售内容 3 可由零售内容加密单元 108 加密。

下面参考图 10 的流程图说明数字数据录制设备 100 的处理过程。下面提供的说明假定原音乐已被编码和压缩为音乐内容，并且多个这样的音乐内容已存储在内容存储单元 104 中。

15 在 S1 步中，控制单元 102 在被激活后，等待内容存储单元 104 中的多个音乐内容中的一个音乐内容指定被录制到零售记录媒体 200 上。如果一个音乐内容已被指定，控制单元 102 便在 S2 步中等待来自操作者的指令来把被指定的音乐内容录制到零售记录媒体 200 上，作为零售内容或者超发行内容。接收到指令后，控制单元 102 在 S3 步中判断所接收的指令示意应该把指定的音乐内容录制为零售内容  
20 还是超发行内容。

这里，假定控制单元 102 在 S3 步中判定指令示意音乐内容应该被录制成零售内容（零售内容 3）。因此，流程从 S3 步转到 S8 步，在 S8 步中控制单元 102 判断零售记录媒体 200 是 DVD 唱片还是增强  
25 CD。如果控制单元 102 判定零售记录媒体 200 是增强 CD，流程便从 S8 步转到 S6 步，在 S6 步中控制单元 102 命令获取单元 105 从内容存储单元 104 获取指定的音乐内容，然后录制单元 109 将其录制到零售记录媒体 200 上。另一方面，如果控制单元 102 在 S8 步中判定零售记录媒体 200 是 DVD 唱片，流程便转到 S9 步，其中控制单元 102  
30 命令获取单元 105 从内容存储单元 104 获取指定的音乐内容，然后将其发送给零售内容加密单元 108。零售内容加密单元 108 接着命令唯一信息获取单元 110 从零售记录媒体 200 获取唯一标识信息。流

程接着从 S9 步转到 S10 步，在 S10 步中零售内容加密单元 108 采用获取的标识信息作为加密密钥来加密零售内容 3，然后到 S6 步，其中录制单元 109 把加密的零售内容 3 录制到零售记录媒体 200 上。上面从 S1 到 S3，S8 到 S10，和 S6 步的流程使得零售内容 3 被录制到零售记录媒体 200 上。下面说明当控制单元 102 在 S3 步中判定所接收的指令示意指定的音乐内容应该被录制成超发行内容（超发行内容 10）时所执行的处理过程。

当判定所指定的音乐内容应该被录制成超发行内容时，控制单元 102 便在 S3 步中命令获取单元 105 去获取该音乐内容，并输出获取的音乐内容（超发行内容 10）到超发行内容加密单元 106。在 S4 步中，超发行内容加密单元 106 加密输出的超发行内容 10 以产生加密内容 8。

在 S5 步中，控制单元 102 命令超发行标题加密单元 107 合并内容标识 11，购买条件 12，和解密密钥 13，并加密合并结果以产生加密标题 7。控制单元 102 接着把加密标题 7 附于加密内容 8 以产生容器 6。在 S6 步中，录制单元 109 把容器 6 录制到零售记录媒体 200 上。在 S7 步中，数字数据录制设备 100 询问操作者是否结束录制。如果是，本流程图所示的处理过程便结束，或者如果否，流程从 S7 步转到 S1 步。

如上所述，本实施方案中的数字数据录制设备 100 从多个要被录制到零售记录媒体 200 上的音乐内容中选择一个音乐内容，其再现和录制到另一记录媒体是作为超发行内容来进行收费。数字数据录制设备 100 接着加密该超发行内容以防止该超发行内容在未收费时被再现或录制到另一记录媒体。

由于超发行标题 9 被附于加密的超发行内容 10，而前者中包含解密密钥 13 和费用信息 12 供专用设备在超发行内容 10 被再现或/和购买时采用，因此音乐公司在每次用户播放超发行内容 10 或者当用户购买超发行内容 10 时能够被付款。

### **第三实施方案**

下面阐明第三实施方案。

图 11 显示了第三实施方案的数字数据录制设备 300 的内部结构。数字数据录制设备 300 基本上与用于传统电子音乐发行的数字

数据录制设备相同，因此含有电子音乐发行的下载功能以通过互联网接收音乐内容，并把该音乐内容录制到买来拷贝的记录媒体上，并且收费。更具体地，数字数据录制设备 300 包括通信单元 313，用于通过互联网传送数据，和记帐单元 310，用于通过通信网络进行收费，当使用电子商务时。图 11 用于功能性地显示涉及超发行内容购买的数字数据录制设备 300 的内部结构。

数字数据录制设备 300 由已安装了专用应用程序的个人计算机实现，包含输入单元 301，显示单元 302，控制单元 303，获取单元 304，超发行标题解密单元 305，超发行内容解密单元 306，唯一信息获取单元 307，超发行内容重新加密单元 308，录制单元 309，记帐单元 310，费用信息存储单元 312，通信单元 313，和录制计数管理单元 314。下面的说明假定零售记录媒体 200 含有图 1 或图 2 所示的存储内容，并且买来拷贝的记录媒体 650 是 DVD - RAM。

输入单元 301 被连接到一台指向设备，比如鼠标或键盘，接收来自用户的指令来购买一段超发行内容。注意超发行内容通过超发行的“购买”可以这样实现，通过把超发行内容中的数据录制到另一记录媒体上，或者通过数字数据录制或回放设备提供的数字输出终端输出超发行内容中的数据。后面一种情况是可能的，因为它使得超发行内容 10 中的数据能够被录制到已被装入另一驱动设备的另一记录媒体上。这里，注意数字数据录制设备 300 被假定含有这样的数字输出终端，并与一台驱动设备相连，如图 7A 所示。

显示单元 302 显示一个交互屏幕，基于回放控制命令表 4 和静态图象数据 5，它们被录制在零售记录媒体 200 上，以在视觉上提供用户关于超发行内容 10 的信息，比如超发行内容 10 的回放和购买费用。

控制单元 303 翻译通过输入单元 301 输入的来自用户的指令，并按该指令命令其它功能单元。例如，接收到来自用户的指令要购买超发行内容 10 时，控制单元 303 便命令获取单元 304 从零售记录媒体 200 中获取超发行内容 10 和超发行标题 9。控制单元 303 还控制此后的处理过程，按照另一功能单元的输出。

获取单元 304 从零售记录媒体 200 获取容器 6。

超发行标题解密单元 305 利用解密密钥对由获取单元 304 获取

的容器 6 中的加密标题 7 解密, 以获得超发行标题 9。当超发行标题 9 被获得, 就可把购买条件 12 显示给用户。这里, 用来解密加密标题 7 的解密密钥可以预先包含于安装到数字数据录制设备 300 上的应用程序中, 或者可以通过通信网络从帐单办公室发送来。

- 5           当超发行标题解密单元 305 解密超发行标题 9 后, 超发行内容解密单元 306 利用包含在超发行标题 9 中的解密密钥 13 对加密内容 8 解密。从而获取超发行内容 10。

10           唯一信息获取单元 307 获取对买来拷贝的记录媒体 650 唯一的标识信息, 其中买来拷贝的记录媒体 650 是 DVD-RAM。对于 DVD-RAM, 用分段分割区 (burst cutting area) (BCA) 写成的信息被用作 DVD-RAM 上的标识信息。不同的标识信息在每个 DVD-RAM 被制造时被录制到该 DVD-RAM 上, 并且标识信息不能被改变。当超发行内容 10 用对 DVD-RAM 唯一的标识信息作为加密密钥被加密, 用于解密超发行内容 10 的解密密钥也将基于同一标识信息, 因此如果加  
15           密的超发行内容从一个 DVD-RAM 被复制到另一个上, 标识信息是不同的, 从而防止了复制的超发行内容被解密。因此超发行内容 10 的版权可以被安全地保护。

20           基于由唯一信息获取单元 307 获取的标识信息, 超发行内容重新加密单元 308 加密已被超发行内容解密单元 306 解密的超发行内容 10。

          录制单元 309 把重新加密的超发行内容 10 录制到买来拷贝的记录媒体 650 上, 并输出录制结束通知给记帐单元 310。

25           接收到来自录制单元 309 的录制结束通知时, 记帐单元 310 从解密的超发行标题 9 中的购买条件 12 读取费用信息, 并基于所读取的费用信息为此次购买计算费用。记帐单元 310 然后把计算出来的购买费用加入所读取的费用信息中。

30           费用信息存储单元 312 是由个人计算机中的硬盘实现的, 保存包含了所计算费用的费用信息。这样做是可取的, 费用信息存储单元 312 以加密状态保存费用信息, 或者把费用信息保存在用户通过标准处理所不能访问的“安全区域”中, 以防止该费用信息被篡改。

          通信单元 313 包括连接到通信网络的调制解调器设备和控制该调制解调器设备的软件, 并在适当时机通过通信网络把用户标识和

费用信息存储单元 312 中的费用信息发送给安装在音乐公司的帐单办公室的主机 600。这里，适当时机可能是费用达到预定量时，或者是预定的一天到来。当然可能每次用户把超发行内容录制到买来拷贝的记录媒体 650 上时都与主机 600 通信。

- 5            录制计数管理单元 314 保存录制单元 309 迄今为止把超发行内容 10 录制到买来拷贝的记录媒体 650 上的次数，每次录制单元 309 把超发行内容 10 录制到买来拷贝的记录媒体 650 上时将此数加一。

下面参考图 12 的流程图说明有上述结构的数字数据录制设备 300 的处理过程。

- 10           这张流程图的流程始于当零售记录媒体 200 被装入数字数据录制设备 300 时。在 S20 步中，等待来自用户的、请求介绍相关音乐的超发行内容 10 的输入。接收到该输入时，在 S21 步中控制单元 303 令获取单元 304 从零售记录媒体 200 的增值区 2 读取回放控制命令表 4 和静态图象数据 5。控制单元 303 然后令显示单元 302 显示如图
- 15           8 所示的交互屏幕。在 S22 步中，等待来自用户的要购买超发行内容 10 的指令。如果指示用户执行了取消操作的输入被接收到，流程则被终止，或者如果购买指令被接收到，流程便从 S22 步转到 S23 步，在 S23 步中控制单元 303 令获取单元 304 从零售记录媒体 200 获取包含了加密标题 9 的容器 6。在 S24 步中，超发行标题解密单元 305
- 20           对加密标题 7 解密以获得超发行内容 9。在 S25 步中，控制单元 303 从录制计数管理单元 314 读取迄今为止录制单元 309 已经录制超发行内容 10 的次数。在 S26 步中，控制单元从超发行标题 9 读取数字输出的次数限制。在 S27 步中，控制单元 303 判断从录制计数管理单元 314 读出的次数是否低于读取的次数限制。如果否，超发行内容 10 的录制则不再被允许，本流程图的流程被终止。如果是，在 S28
- 25           步中控制单元 303 便令超发行内容解密单元 306 利用超发行标题 9 中的解密密钥 13 对加密内容 8 进行解密，以获得超发行内容 10。

- 30           超发行内容 10 解密后，在 S29 步中控制单元 303 便令唯一信息获取单元 307 从买来拷贝的记录媒体 650 获取标识信息，并令超发行内容重新加密单元 308 利用获取的标识信息作为加密密钥来对超发行内容 10 加密。在 S30 步中，控制单元 303 令录制单元 309 把重新加密的超发行内容 10 录制到买来拷贝的记录媒体 650 上。

录制单元 309 的录制完成后, 控制单元 303 使记帐单元 310 从超发行标题 9 读取购买条件 12 中的费用信息, 并基于所读取的费用信息计算购买费用。在 S31 步中, 控制单元 303 使记帐单元 310 把计算出来的购买费用加入读取的费用信息中, 并把添加后的费用信息置于费用信息存储单元 312 中。在 S32 步中, 控制单元 303 等待适当的时机发送保存在费用信息存储单元 312 中的费用信息, 当这样的时机到来时, 在 S33 步中控制单元 303 令通信单元 313 获取和发送费用信息, 连同用户标识, 到帐单办公室的主机 600。这就完成了整个处理过程。

如上所述, 只有当用户同意购买该用户已经购买了的零售记录媒体 200 中的超发行内容 10 时, 数字数据录制设备 300 才把超发行内容 10 录制到买来拷贝的零售记录媒体 650 上, 并且通过通信网络发送该录制的费用信息到帐单办公室。由于用户不需要通过通信网络下载超发行内容 10, 因而向用户收取的通信费用可减到最少, 在电子音乐发行所要求的基础结构还未被充分实现, 因而通信网络的传输速度较低的情况下。这样, 超发行内容 10 可以很少的成本售出。

#### **第四实施方案**

第四实施方案涉及数字数据回放设备 400, 用于再现已被收费的超发行内容。不同于第三实施方案中把超发行内容 10 从零售记录媒体录制到另一记录媒体上的数字数据录制设备 300, 本数字数据回放设备 400 直接再现来自零售记录媒体 200 的超发行内容, 这是上述两种设备的主要区别。两种设备均有通过互联网的电子音乐发行的下载音乐内容的功能, 因此包含用于实现这样下载的共同功能单元。

图 13 显示了本实施方案的数字数据回放设备 400 的结构。在图 13 中, 数字数据录制设备 300 与数字数据回放设备 400 共同的功能单元被给予了与图 11 中相同的标号, 这里就不再说明了。下面仅说明在 400 中分配标号的功能单元, 它们是数字数据回放设备 400 独有的。这些是回放单元 401 和回放计数管理单元 402。

回放单元 401 再现已被超发行内容解密单元 306 解密的超发行内容 10。当开始再现超发行内容 10 时, 回放单元 401 便通知记帐单元 310 再现的开始, 于是记帐单元 310 向用户收取再现费用。

回放计数管理单元 402 记录回放单元 401 已经再现超发行内容 10

的次数，每次回放单元 401 再现时便将此数加一。

下面参考图 14 的流程图具体说明数字数据回放设备 400 的处理过程。在这张流程图中，S20 步到 S24 步，S28 步，和 S31 步到 S33 步与图 12 中相同，因此不会再被说明。下面的说明集中于第四实施方案所独有的 S41 到 S46 步。

在加密标题 7 被解密以获得超发行标题 9 的 S24 步之后，在 S41 步中控制单元 303 从回放计数管理单元 402 读取回放单元 401 已再现超发行内容 10 的次数。在同一步中，控制单元 303 从超发行标题 9 读取允许的播放次数。在 S42 步中，控制单元 303 判断从回放计数管理单元 402 读出的次数是否低于允许的播放次数。如果否，即意味着再现不再被允许，本流程图的流程被终止，或者如果是，控制单元 303 便在 S43 步中读取当前的时间和日期，并在 S44 步中从超发行标题 9 读取回放允许的到期时间和日期。在 S45 步中，控制单元 303 判断所读取的当前时间是否已经超过所读取的回放允许到期时间和回放允许到期日期。如果是，本流程图的流程被终止，或者如果否，流程便从 S45 步转到 S28 步，在 S28 步中控制单元 303 令超发行内容解密单元 306 利用解密密钥 13 对加密内容 8 进行解密，以产生超发行内容 10。在 S46 步中，控制单元 303 令回放单元 401 再现超发行内容 10。

采用本实施方案的数字数据回放设备 400，回放单元 401 每次开始再现超发行内容 10 时便通知记帐单元 310。这样使得音乐公司在每次超发行内容 10 被再现时都能够向用户收费。

注意上述的再现超发行内容 10 的功能可与在第三实施方案中描述的购买超发行内容 10 的功能合并，以实现这两个功能均被提供的数字数据录制设备。

### **第五实施方案**

尽管第一到第四实施方案被描述时均假定音乐内容是利用一种记录媒体被发行的，本实施方案的描述前提是内容的发行不仅利用一种记录媒体，还有互联网或卫星广播的广播波，CATV 电缆，等等。

图 15 显示了多种发行内容包的方法，其中的内容包是由本实施方案的内容打包设备 700 产生的。内容包包含多个内容，以后会说明。如图 15 所示，内容包的发行是通过 DVD 唱片 701，CD 702，互

联网 703, CATV 电缆 704, 以及通信卫星 705。内容回放设备 801 - 809 是用于再现内容包的设备。设备 801 是专用于再现内容的高级设备, 而设备 802 和 803 是内容的低级专用设备。设备 804 和 805 是内容的专用便携式设备, 而设备 806 和 807 是通用的个人计算机, 装备了专用于内容再现的硬件。设备 808 和 809 是机顶盒, 用于通过通信卫星或 CATV 电缆接收广播波。

这样, 内容包被分发给各种类型的内容回放设备。在内容回放设备 801 - 809 中, 用户设备, 比如设备 801 和 802 包括专用于解密加密内容的硬件, 而设备 806 和 807 是通用的个人计算机, 不包括这样的用于解密的专用硬件, 只能通过通用硬件上运行解密软件来解密加密内容。相应地, 可能认为通用个人计算机 806 和 807 没有版权保护系统, 而认为用户设备 801 - 805 含有这样的系统。这样安排是因为用户回放设备可以高质量再现内容, 而通用个人计算机只能以低质量再现内容。

图 16 显示了内容打包设备 700 和内容回放设备 801 - 809 的内部结构, 按第五实施方案。内容打包设备 700 包括内容编码单元 706, 质量等级/加密对应表存储单元 707, 内容加密单元 708, 和内容打包单元 709。

内容编码单元 706 利用不同方法对将要发行的产品编码, 以产生多个内容, 每个内容都有不同的再现质量, 但基于同一产品。这里, 假定所产生的多个内容是零售内容 710 和再现质量低于零售内容 710 的样品内容 711。

内容等级/加密对应表存储单元 707 存储第一对应表和第二对应表。第一对应表存储多个对, 每对包含量化位数和采样频率, 供内容编码单元 706 在加密内容时使用, 同时存储分配给每个内容的多个内容等级, 内容等级的产生是编码的结果。在该表中, 每对与不同的内容等级对应。第二对应表存储与第一对应表相同的内容等级和多个对, 每对包含加密密钥位数和加密算法名称。每个内容等级对应于不同的对。

图 17A 显示了第一对应表的一个例子。如图中所示, 1 级对应于量化位数为 24 位和采样频率为 96 KHz 的对, 2 级对应于量化位数为 16 位和采样频率为 44.1 KHz 的对, 3 级对应于量化位数为 16 位和

采样频率为 22.05 KHz 的对，其中级数越低表示内容等级越高。这样，较高量化位数和较高采样频率的对与较高的内容等级对应。

图 17B 显示了第二对应表的一个例子。如图 17B 所示，1 级对应于 1024 位的加密密钥和 RSA 加密算法的对，2 级对应于 512 位的加密密钥和 RSA 加密算法的对，3 级对应于 56 位的加密密钥和 DES 算法的对。这里，RSA 加密算法是公开密钥体制，提供比是共用密钥体制的 DES 加密算法更高的安全性。位数较高的加密密钥保证更高的安全性。这样，较高的内容等级对应于保证较高安全性的加密密钥和加密算法。

内容加密单元 708 参考第一对应表，并对由内容编码单元 706 编码和产生的每个内容分配 1-3 级中的一个内容等级。内容加密单元 708 然后参考第二对应表和加密内容，该内容的内容等级的分配是利用与所分配的内容等级对应的加密密钥和加密算法。例如，当加密已由内容编码单元 706 以 24 位量化和 96KHz 采样来进行编码的零售内容 710 时，内容加密单元 708 参考第一对应表，并把 1 级分配给零售内容 710。内容加密单元 708 然后参考第二对应表，产生一个与 1 级对应的 1024 位的加密密钥（会话密钥），并利用与 1 级对应的、所产生的 1024 位的加密密钥和 RSA 算法来加密零售内容 710。内容加密单元 708 然后把该 1024 位的加密密钥附于已被执行了上述编码的零售内容 710。

另一方面，当加密已由内容编码单元 706 用 16 位的量化位数和 44.1KHz 的采样频率来进行编码的样品内容 711 时，内容加密单元 708 把 2 级分配给样品内容 711，产生与 2 级对应的 512 位的加密密钥（会话密钥），并利用与 2 级对应的、所产生的 512 位的加密密钥和 RSA 加密算法来加密样品内容 711。内容加密单元 708 然后把该 512 位的加密密钥附于已被执行了上述编码的样品内容 711。

内容打包设备 709 把已由内容加密单元 708 进行加密的零售内容 710 和样品内容 711 打包以产生一个内容包，并将其转化为适于一种发行方法的格式。更具体地，如果该内容包要通过互联网，卫星广播，或 CATV 电缆发行，内容打包单元 709 便把该内容包转化为传输控制协议（TCP）包或传输包，并输出所产生的包。如果该内容包要通过一种记录媒体来发行，比如 CD-ROM 或 DVD-ROM，内容打

包单元 709 便把该内容包转化为通用磁盘格式 (UDF) 等的文件, 并将转化后的文件录制到 CD-ROM 或 DVD-ROM 上。图 18 示出已被打包的内容包的一个例子, 但还未被内容打包单元 709 转化。如图中所示, 内容包包含多个内容, 并被分发给内容回放设备 801-809。

5           下面说明内容回放设备 801-809。尽管内容回放设备 801-809 拥有不同的总体结构, 如图 15 所示, 这些设备含有共同的功能单元, 如图 16 所示, 即, 硬件等级/解密对应表存储单元 810, 硬件性能评估单元 811, 内容开包单元 812, 内容解密单元 813, 内容存储单元 814, 和内容回放单元 815。

10           硬件等级/解密对应表存储单元 810 存储硬件等级/解密对应表, 把多个硬件等级和多个对对应起来, 每个对包括解密密钥位数和解密算法名称。每个硬件等级对应于不同的对, 表示内容回放设备的硬件性能。更具体地, 这张表中的每个硬件等级的确定是通过硬件是否专用于加密内容的解密, 即, 版权保护系统是否被提供给内容回放设备, 而且如果是, 该版权保护系统的解密能力。这些硬件等级是用降序表示为 A, B, 和 C 级。例如, A 级表示版权保护系统被提供

15           给内容回放设备, 而 B 和 C 级表示版权保护系统不被提供给内容回放设备。图 17C 示出了保存在硬件等级/解密对应表存储单元 810 中的表。在表中, A 级对应于 1024 位的解密密钥和 RSA 解密算法的对, B 级对应于 512 位的解密密钥和 RSA 解密算法的对, C 级对应于 56 位的解密密钥和 DES 解密算法的对。

20           

          硬件性能评估单元 811 评估该内容回放设备的硬件性能, 在内容回放设备中这个单元被提供来计算其等级, 通过检测该内容回放设备是否包含专用于加密内容的解密的硬件和计算该硬件能够用于解密的内存大小。

25           

          内容开包单元 812 接收来自内容打包单元 700 的内容包, 并打开该内容包以获得零售内容 710 和样品内容 711。

          内容解密单元 813 首先参考硬件等级/解密对应表, 选择对应于由硬件性能评估单元 811 所计算出来的等级的解密密钥和解密算法。

30           然后, 内容解密单元 813 从由内容开包单元 812 所打开的内容中仅分离出能够被所选的解密密钥和解密算法解密的内容。最后, 内容解密单元 813 利用解密密钥和解密算法对分离出的内容解密。

下面具体阐明由内容回放设备 801 的内容解密单元 813 实现的解密过程，其中内容回放设备 801 是一台高级用户回放设备。当该内容回放设备 801 含有用于解密的专用硬件时，硬件性能评估单元 811 把与硬件等级/解密表存储单元 810 中的表中的 A 级相应的等级分配给该回放设备 801。然后，内容解密单元 813 参考该表以选择对应于 A 级的对。由于 A 级对应于 1024 位的解密密钥和 RSA 解密算法的对，内容解密单元 813 便选择该对。在发现零售内容 710 是由 1024 位的加密密钥和 RSA 加密算法来进行加密的之后，内容解密单元 813 从由内容开包单元 812 所打开的内容中仅分离出零售内容 710。然后，内容解密单元 813 利用预先已被提供的 RSA 解密算法和解密密钥来解密所分离出来的零售内容 710。

另一方面，如果回放设备是内容回放设备 806，它是一台个人计算机，通过在通用硬件上运行解密软件来解密内容，硬件性能评估单元 811 分配与硬件等级/解密表存储单元 810 中的表中的 C 级相应的等级。然后，内容解密单元 813 参考该表以选择对应于 C 级的对。由于 C 级对应于 56 位的解密密钥和 DES 解密算法的对，内容解密单元 813 便选择该对。在发现样品内容 711 是由 56 位的加密密钥和 DES 加密算法来进行加密的之后，内容解密单元 813 从由内容开包单元 812 所打开的内容中仅分离出样品内容 711。然后，内容解密单元 813 从内容包中提取附于样品内容 711 的加密密钥以获得该加密密钥来作为解密密钥，这是可能的，因为 DES 算法是共用密钥体制。内容解密单元 813 利用提取的加密密钥作为解密密钥和 RSA 解密算法来解密所分离出来的样品内容 711。

内容存储单元 814 存储由内容解密单元 813 解密的内容。

内容回放单元 815 再现已被临时存放在内容存储单元 814 中的内容。

如前所述，本实施方案的内容打包设备产生零售内容 710 和样品内容 711，其中样品内容 711 的再现质量低于零售内容 710，并用有着不同安全等级的不同加密方法来加密零售内容 710 和样品内容 711。内容打包设备然后把零售内容 710 和样品内容 711 打包成一个内容包，并把该内容包发送给不同类型的内容回放设备。因此，每个内容回放设备能够根据该内容回放设备的硬件性能来从发送来的

内容包中选择一个内容。相应地，内容供应商能够发送不同质量的内容，而不需考虑目标内容回放设备的不同再现条件，同时内容的版权被保护。

### **第六实施方案**

5       第六实施方案涉及内容打包设备，它是第五实施方案的内容打包设备的变型。两者的主要区别在于本实施方案中的内容编码单元 706 把要被发行的产品的起始部分编码以产生样品内容，并把该发行主题的其余部分编码以产生主内容。内容打包单元 709 将编码的主内容和样品内容打包以产生内容包。

10       图 19 显示了内容打包设备 700 和内容回放设备 801 - 809 的结构。

内容加密单元 708 分配一个预定的等级给样品内容和一个比预定等级更高的等级给主内容。内容加密单元 708 然后参考一个类似于第五实施方案的第二对应表的表，并利用与所分配的等级对应的加密密钥和加密算法来加密分级后的内容。如上所述，内容打包单元 709 然后把加密的主内容和样品内容打包以产生内容包。图 20 示出了由本实施方案的内容打包单元 709 打包的内容包。

按照本实施方案，比第五实施方案中的内容包更小的内容包能够通过每种发行方法被传播，以及在被录制到一种记录媒体，比如硬盘或 CD - ROM 上时占用较小的存储区域。

20       尽管本发明已在第一到第六实施方案的基础上被描述，这些实施方案仅仅是一些例子，通过这些例子能够获得本发明的最佳效果。本发明因此能够在不改变其本质的情况下被修改。下面描述被认为具有代表性的修改。

25       (a)   在第一到第四实施方案中，买来拷贝的记录媒体 650 被描述为光存储盘，比如 DVD - RAM，尽管买来拷贝的记录媒体 650 可替换为硬盘或半导体存储器。

30       (b)   第三和第四实施方案声明费用信息存储单元 312 由个人计算机的硬盘实现，尽管费用信息存储单元 312 并不局限于此，也可由一种记录媒体，比如 IC (集成电路) 卡来实现。

(c)   在第一到第四实施方案中描述的数字数据录制设备 500 被描述为通过家用的个人计算机来实现，尽管数字数据录制设备 500

也可安装在商店里，比如唱片店。

5 (d) 尽管第一到第四实施方案已在假定供应商发行的信息是音乐内容的情况下被描述，要被发行的信息并不局限于音乐内容。当然可能发行图象内容，文本数据，或是图象内容与文本数据的组合。

(e) 在第五实施方案中，零售内容 710 和样品内容 711 被产生和发行，它们是有着不同再现质量的两种类型的内容，尽管也可能产生和发行有着不同再现质量的三种或更多类型的内容。

10 (f) 在第一到第六实施方案中描述的处理过程，如图 10，12，和 14 中的流程图所示，可以用机器语言写成程序，并录制到要被发行和出售的记录媒体上。这样的记录媒体可以是 IC 卡，光存储盘，软盘，等等。通过安装上述程序到通用计算机和令该通用计算机执行所安装的程序，可以实现本发明的数字数据录制设备和数字回放设备的功能。

15 尽管本发明已通过例子参考附图被全面描述，应该注意各种变化和修改对于那些本领域的专业人士来说会是明显的。因此，除非这样的变化和修改脱离本发明的范围，否则应该认为它们已被包括在这里了。

### 行业适用性

20 本发明的记录媒体有利于方便和低价地售出内容，因此在制造和销售这种内容的音乐业和电影业中有行业适用性。

25 本发明的数字数据录制设备和数字数据回放设备在生产下述设备的制造业中有行业适用性：把上述内容录制到一种记录媒体上的设备，再现被录制在一种记录媒体上的内容的设备，以及把内容从一种记录媒体录制到另一种记录媒体上的设备。

图 1A

零售记录媒体 (类型1)

增强光盘

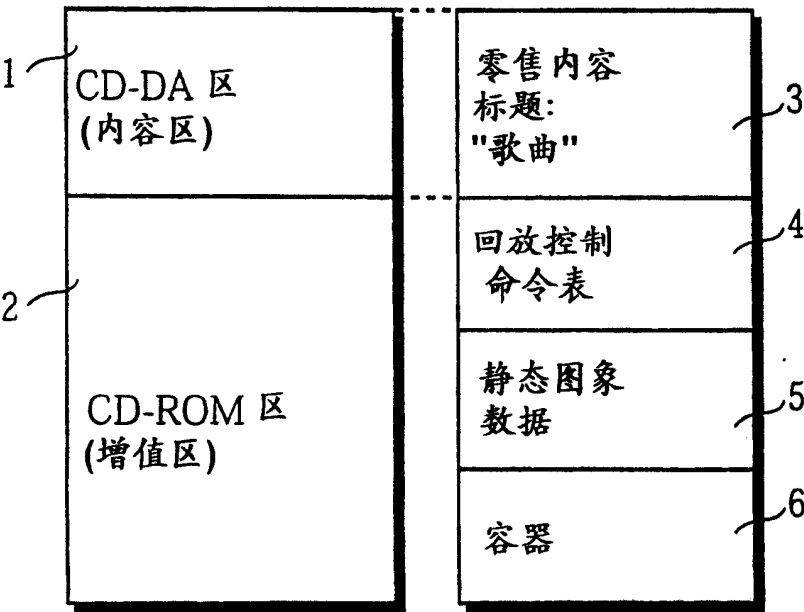
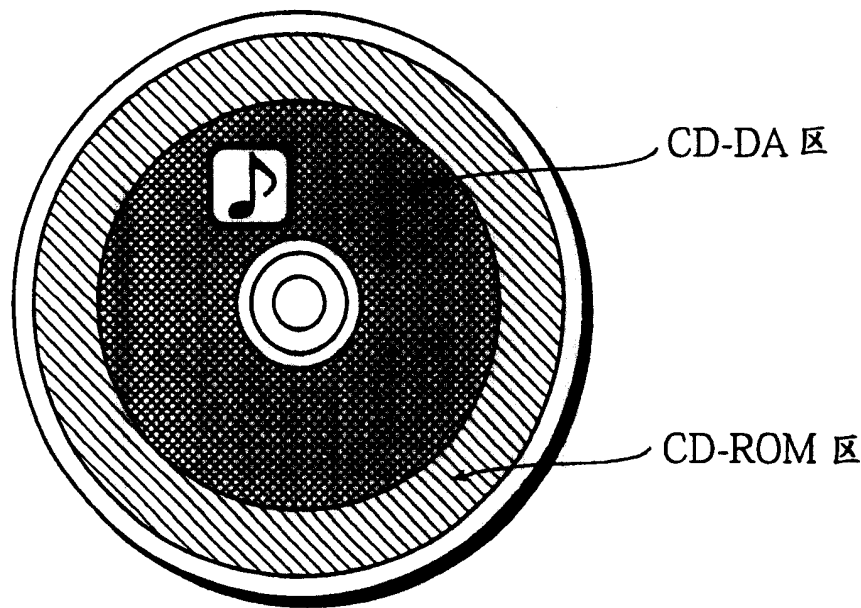


图 1B

图 2A  
零售记录媒体 (类型2)  
DVD-唱片

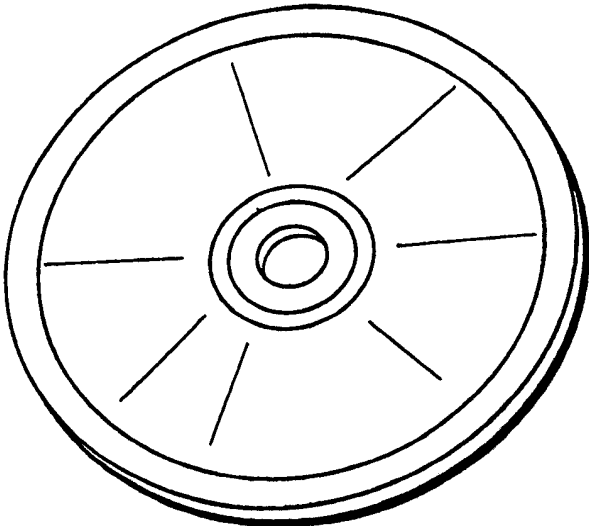


图 2B

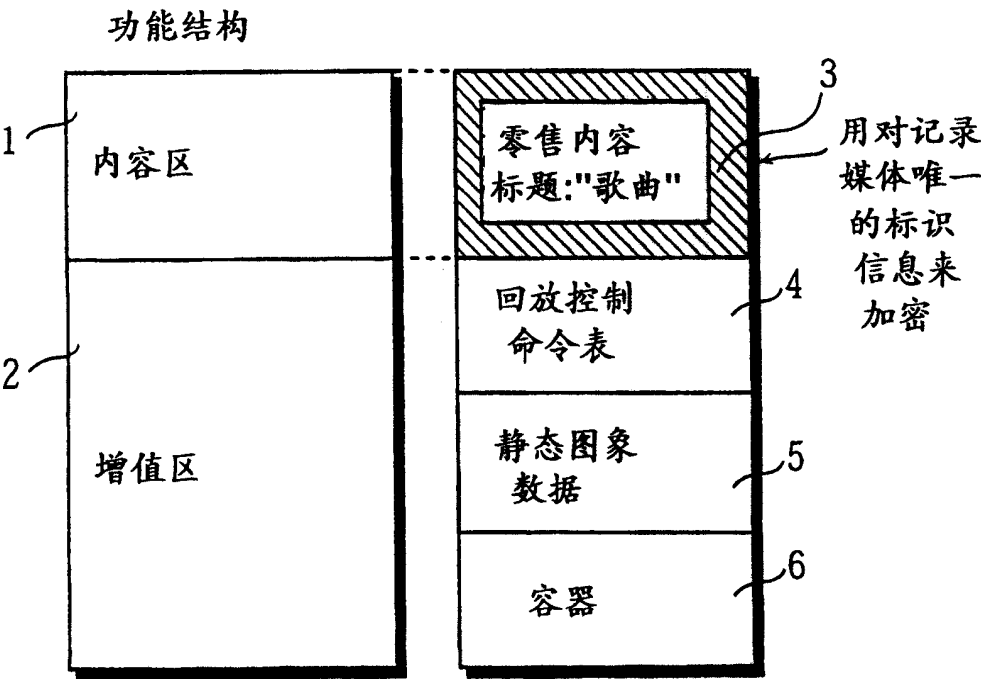




图 3

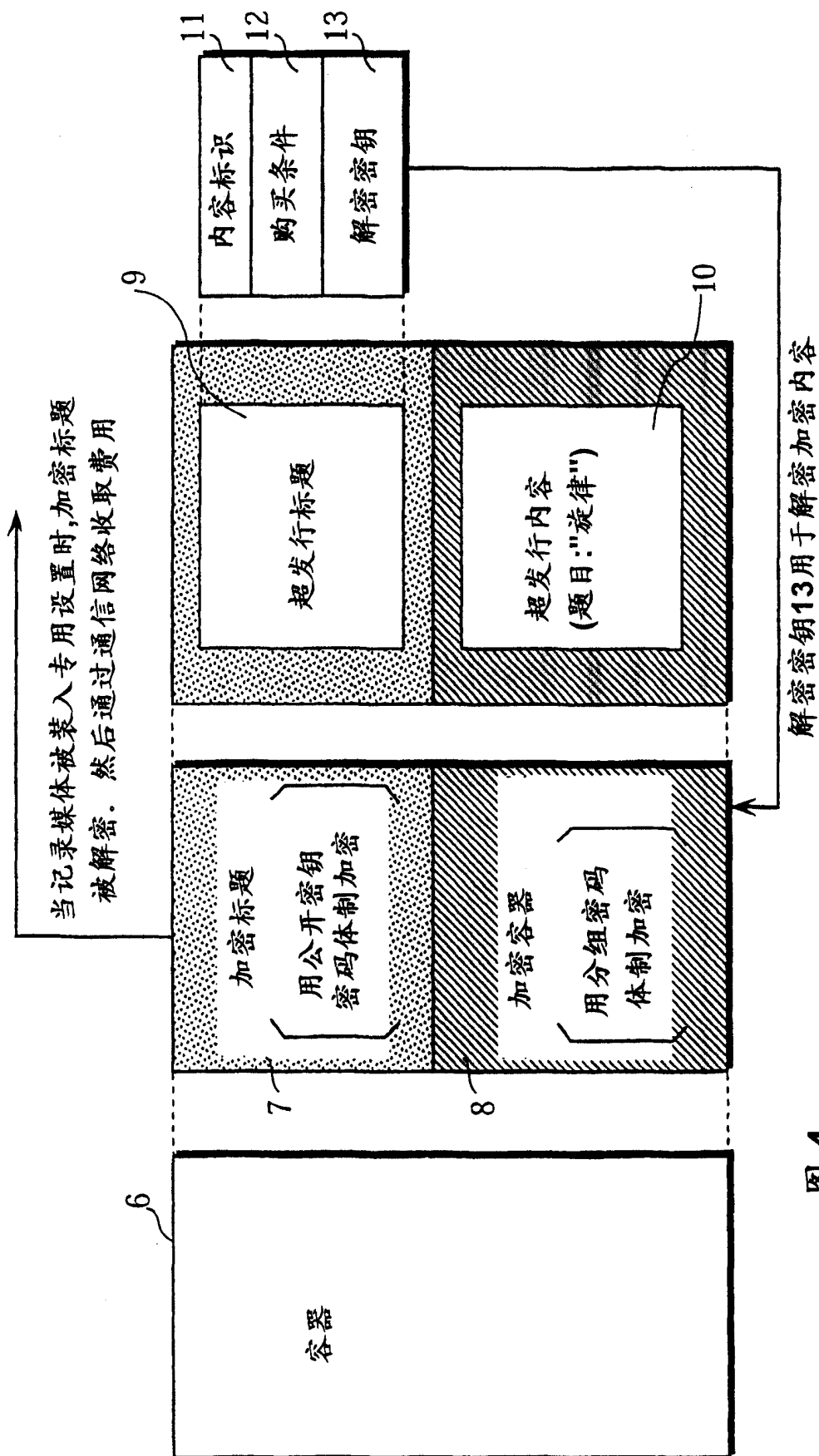


图4

| 信息       | 内容                             |
|----------|--------------------------------|
| 允许播放次数   | 播放超发行内容的次数限制                   |
| 数字输出允许   | 超发行内容10是否能被数字输出,及如果能,数字输出的次数限制 |
| 回放允许到期时间 | 回放允许到期的时间                      |
| 回放允许到期日期 | 回放允许到期的日期                      |
| 费用信息     | 超发行内容的购买价格和回放价格                |

图 5

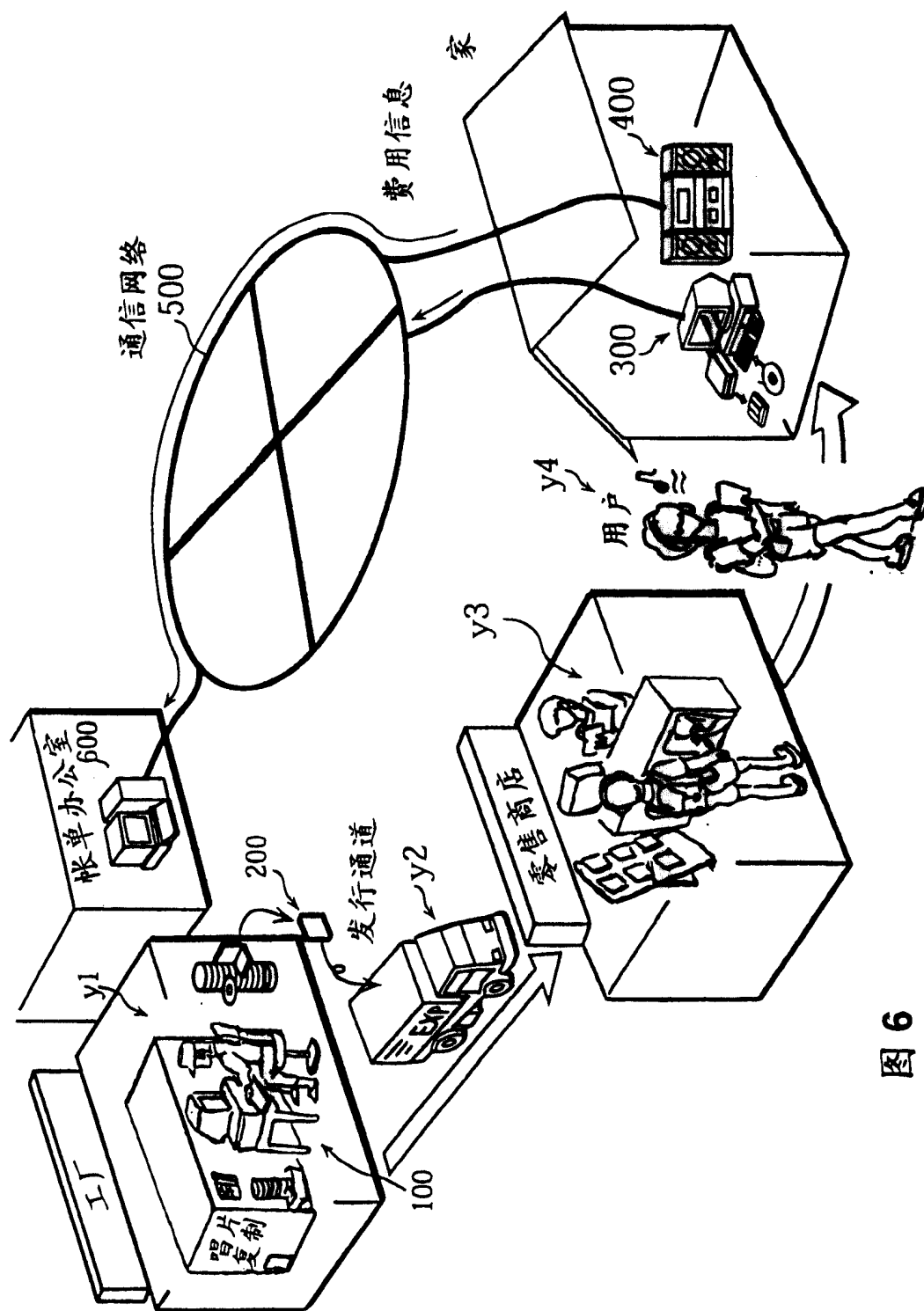


图6

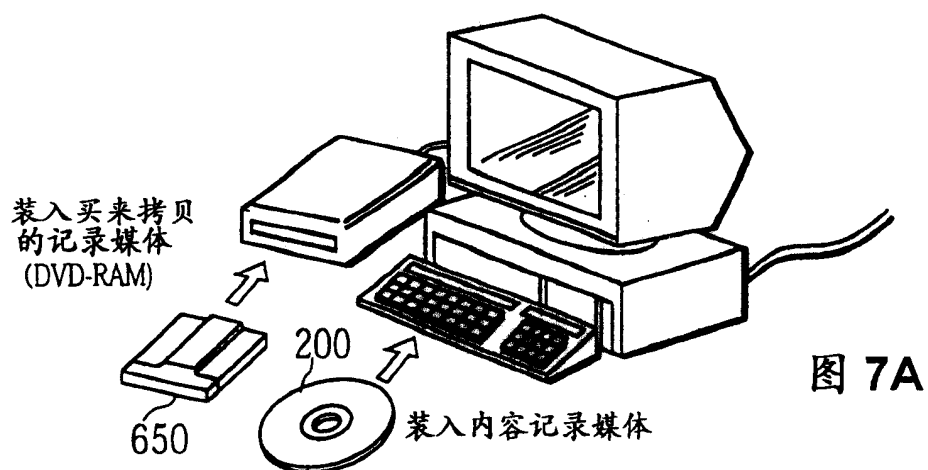


图 7A

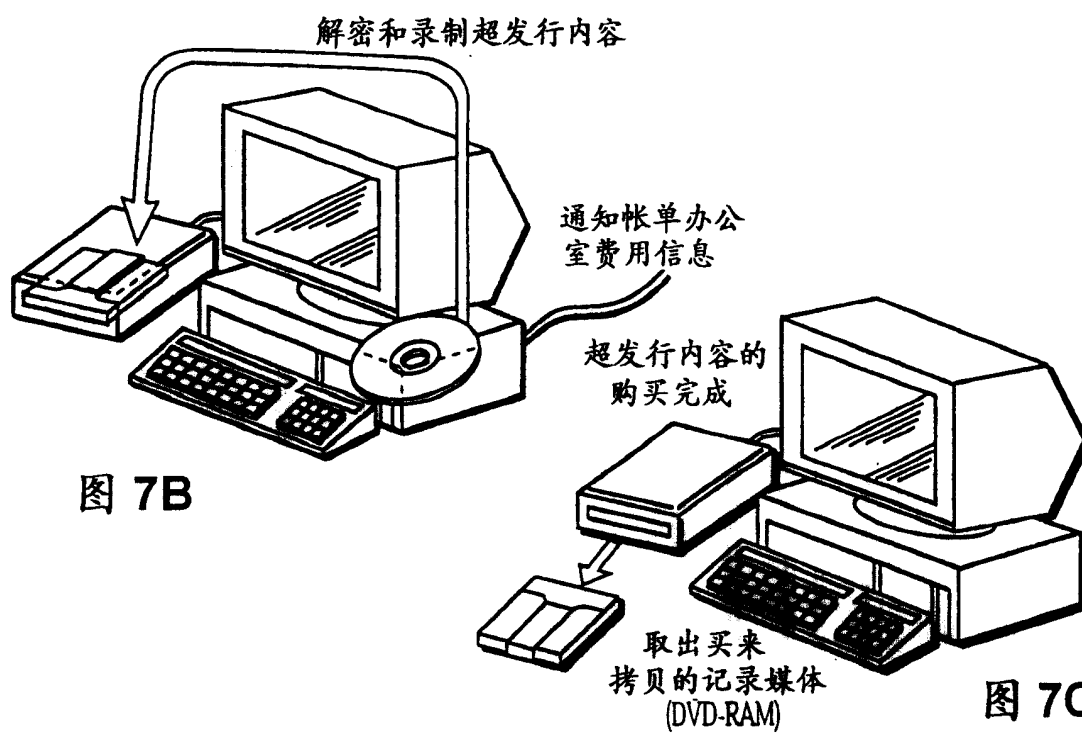


图 7B

图 7C

到RAM准备好的DVD唱片播放器

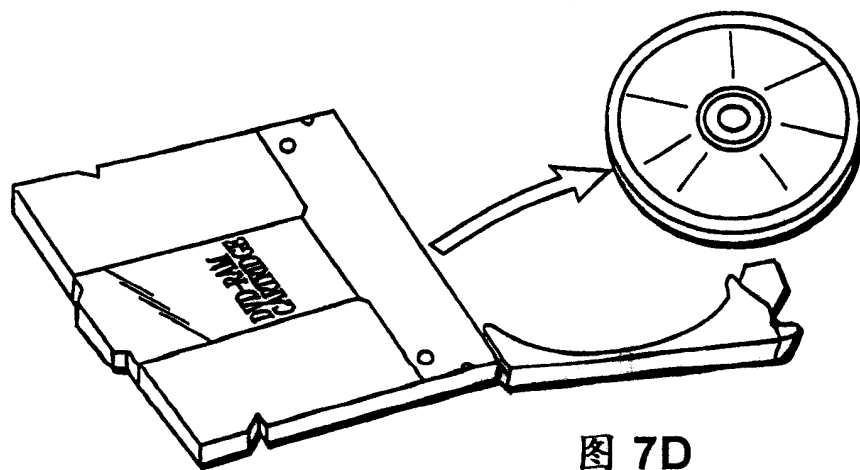


图 7D

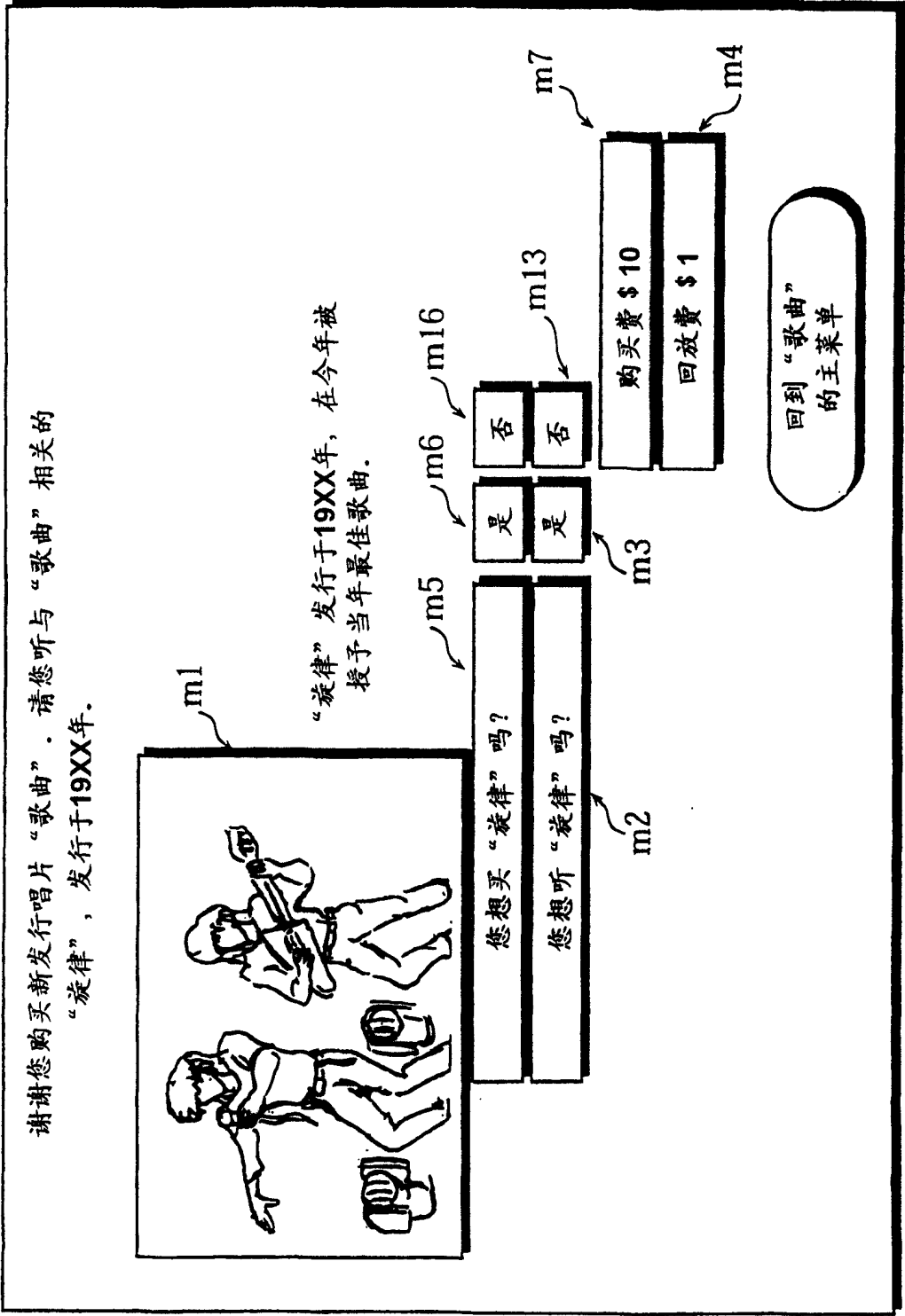
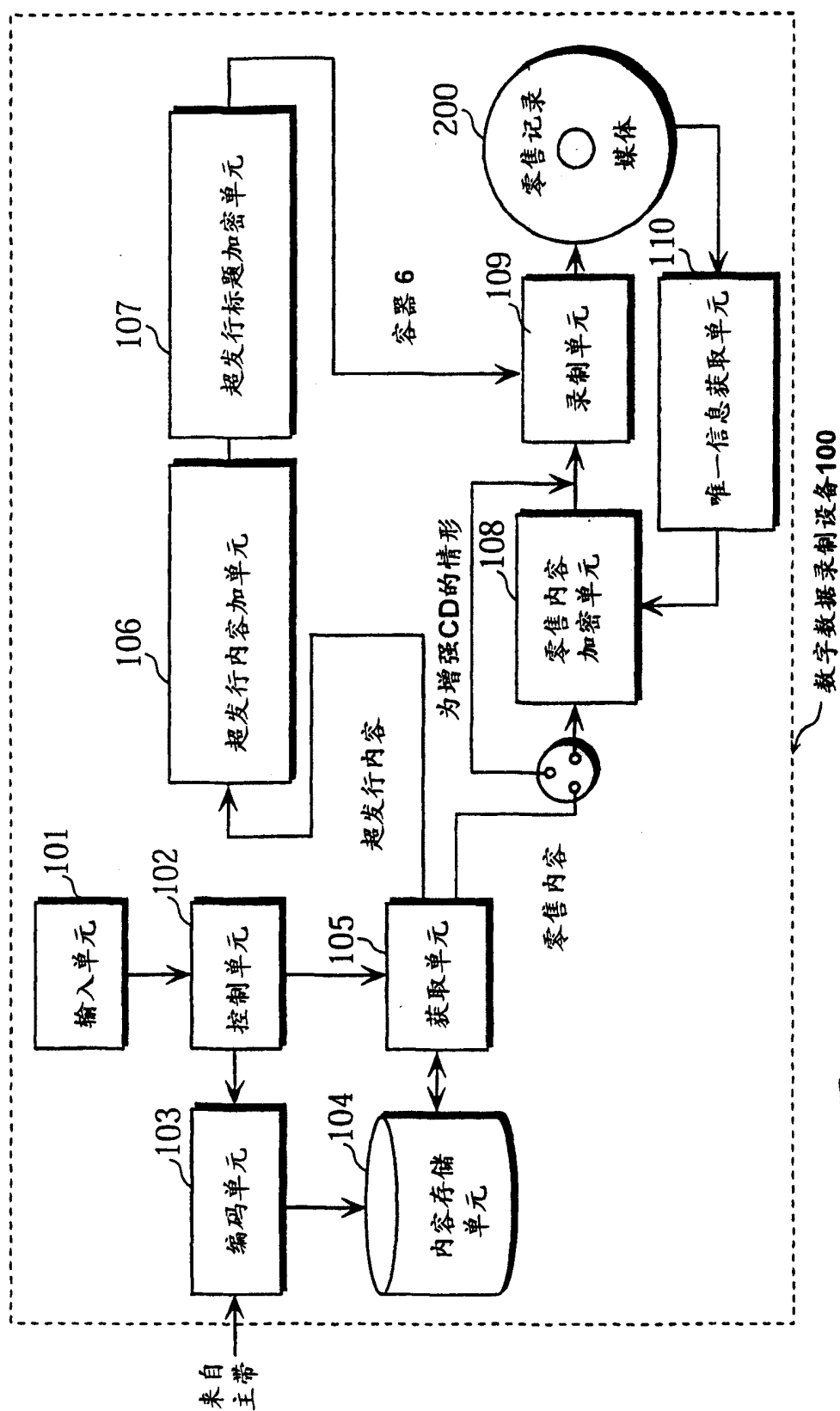


图 8



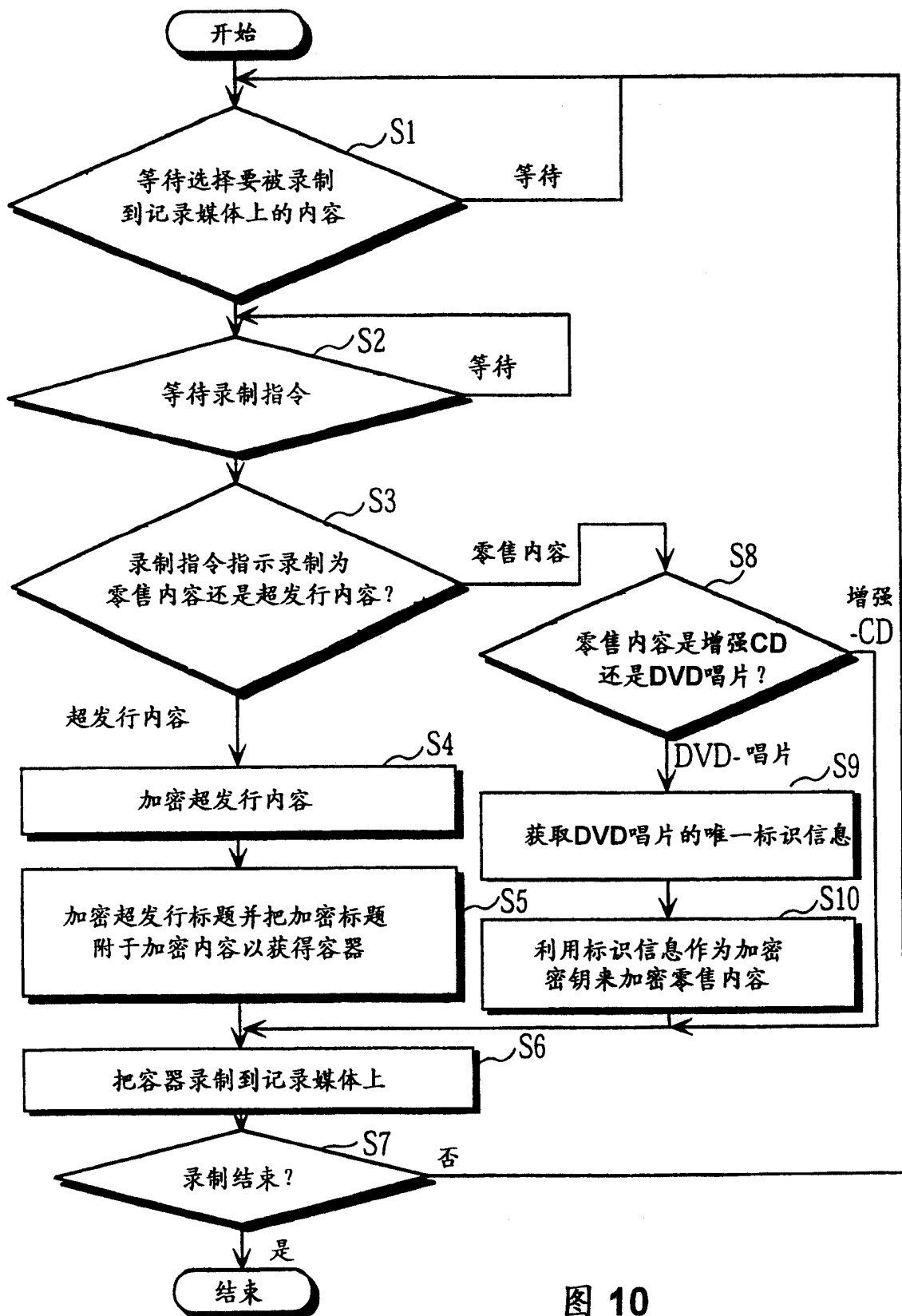
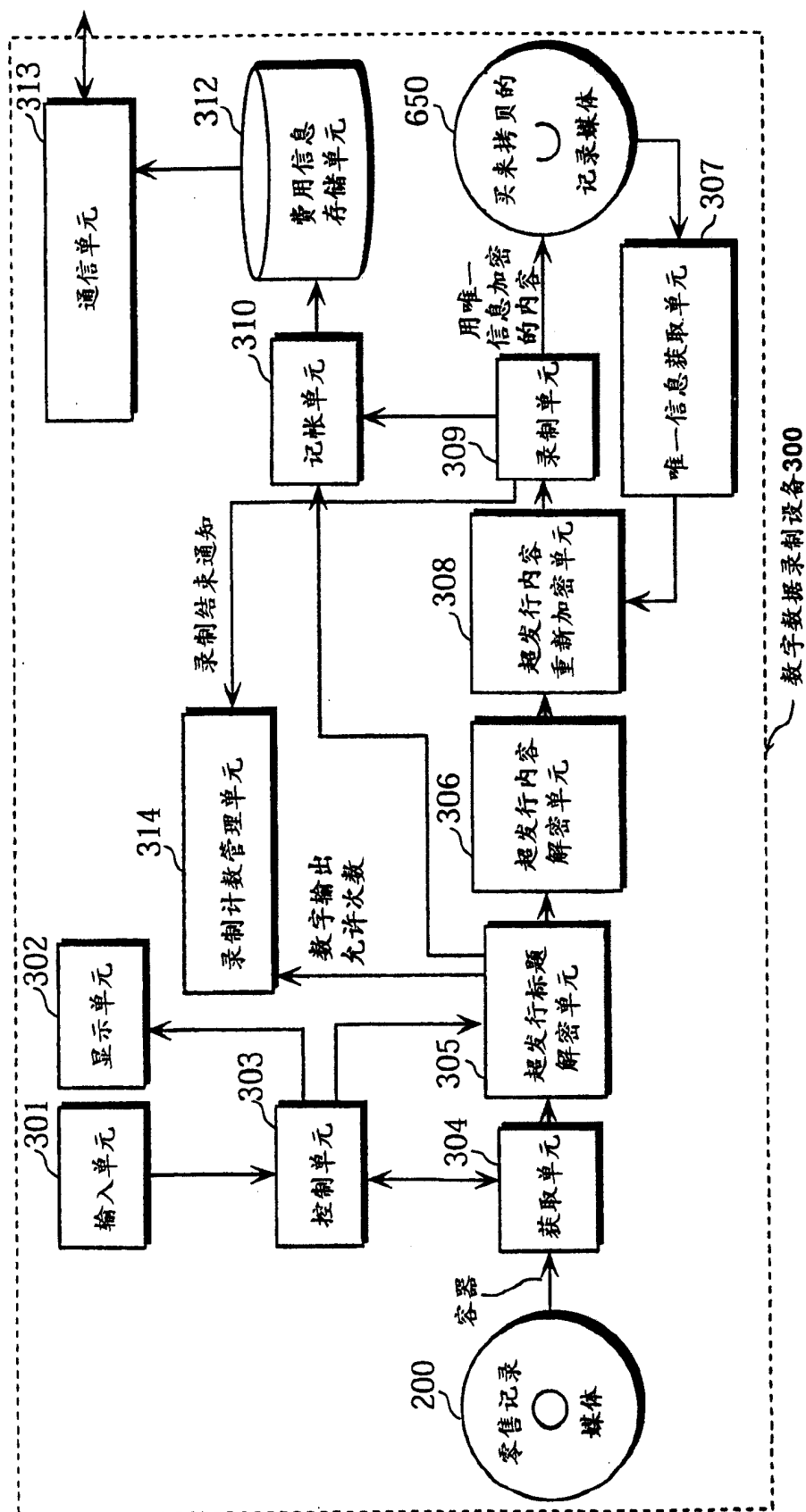


图 10



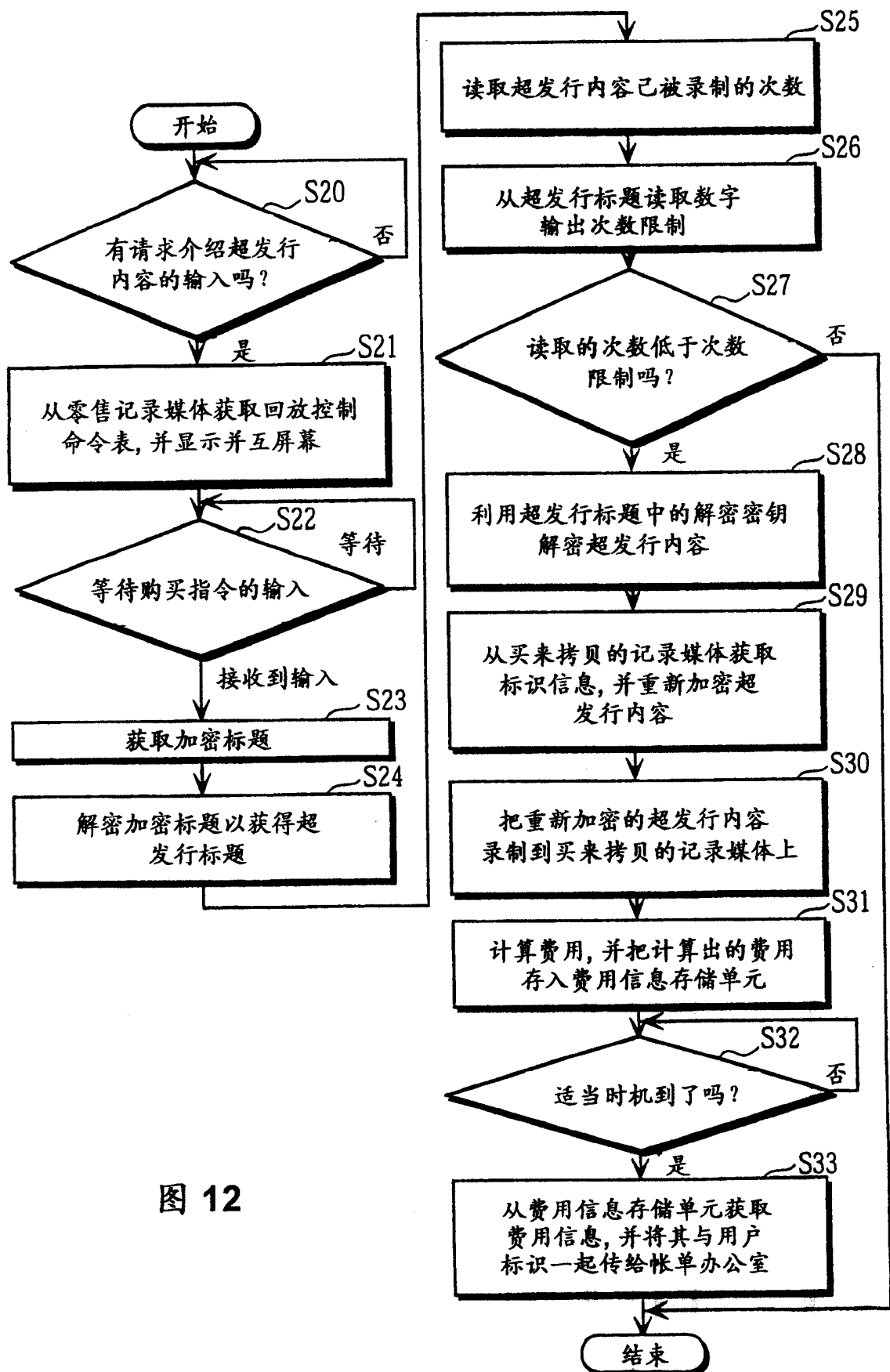


图 12

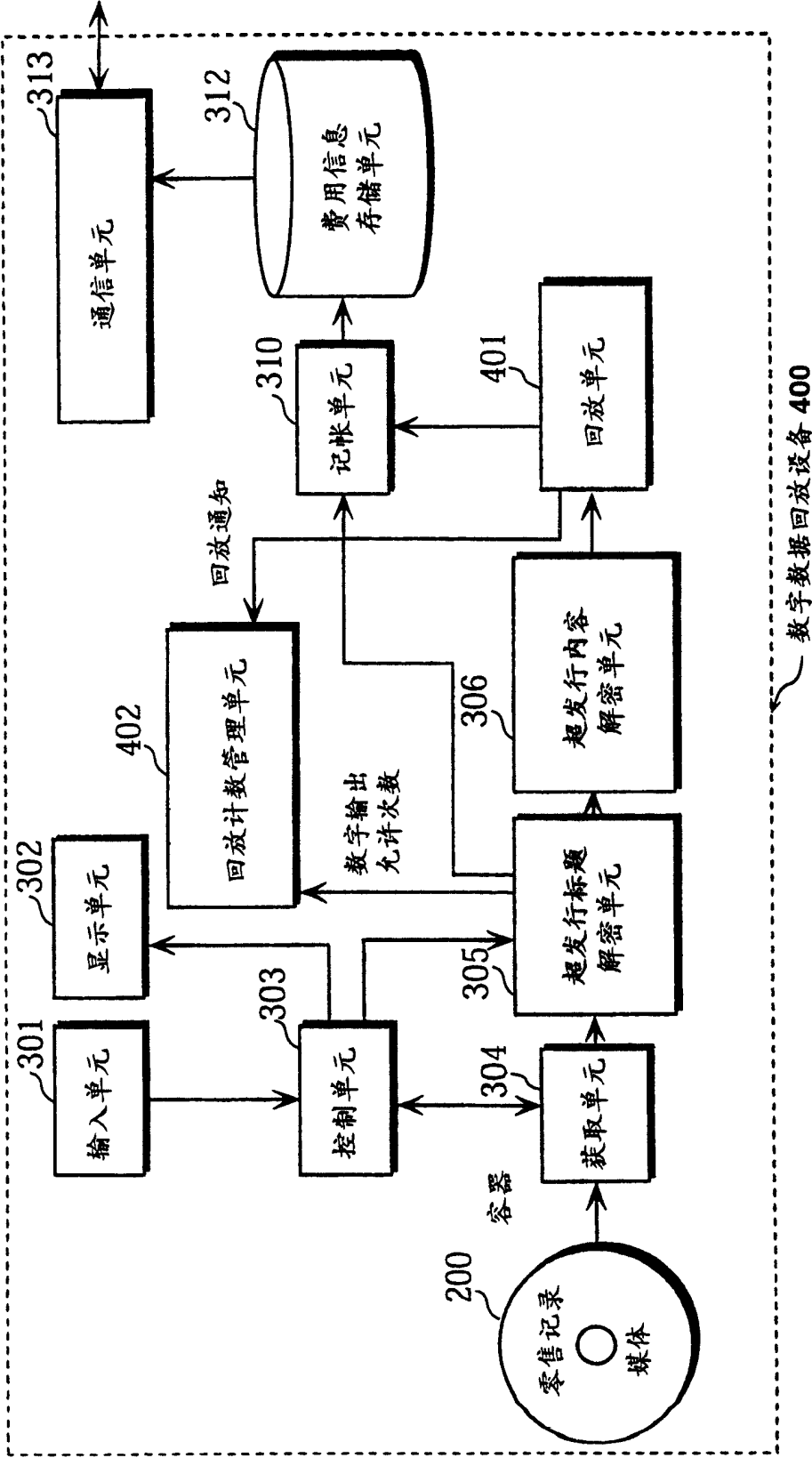


图 13

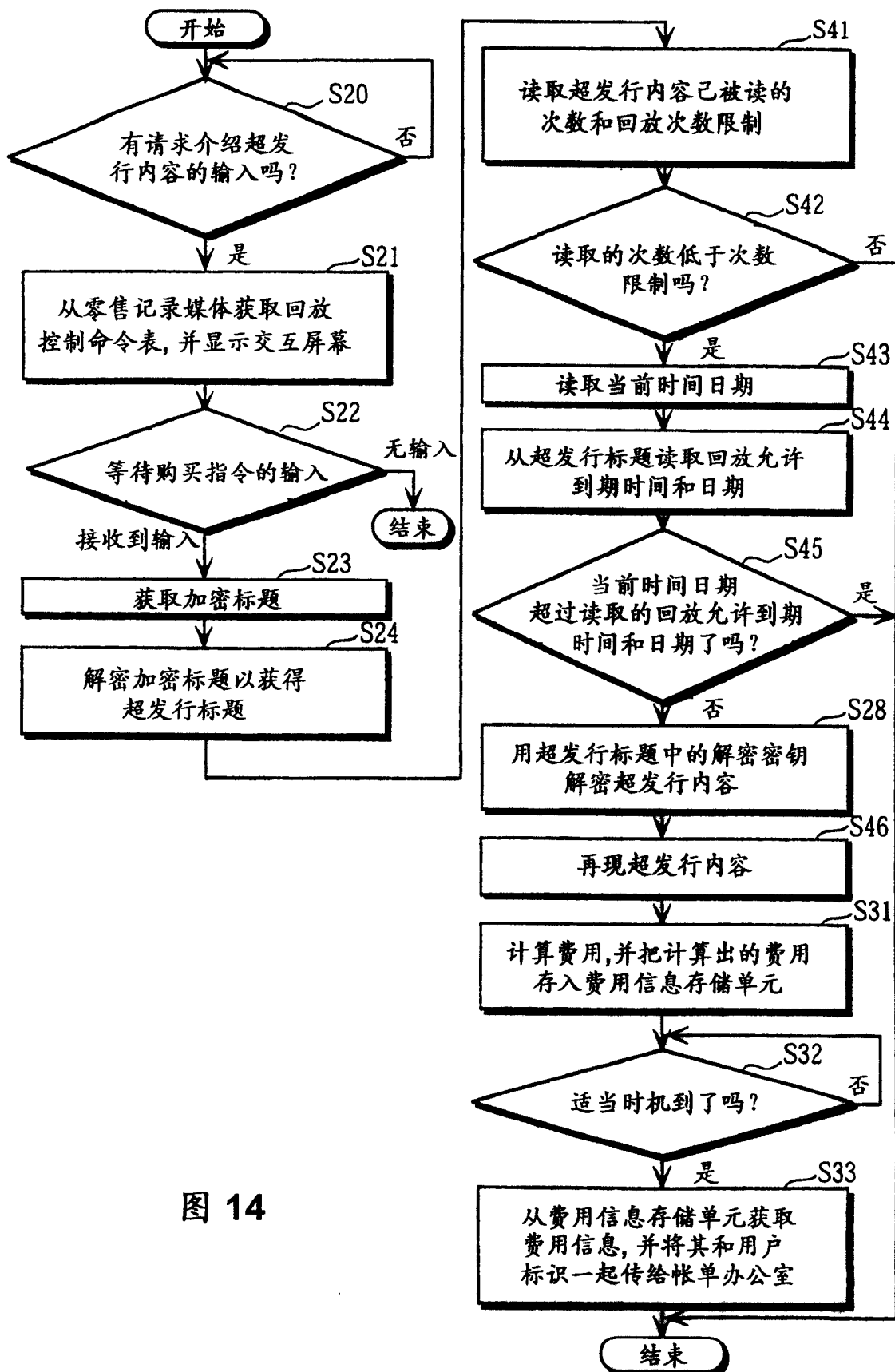


图 14

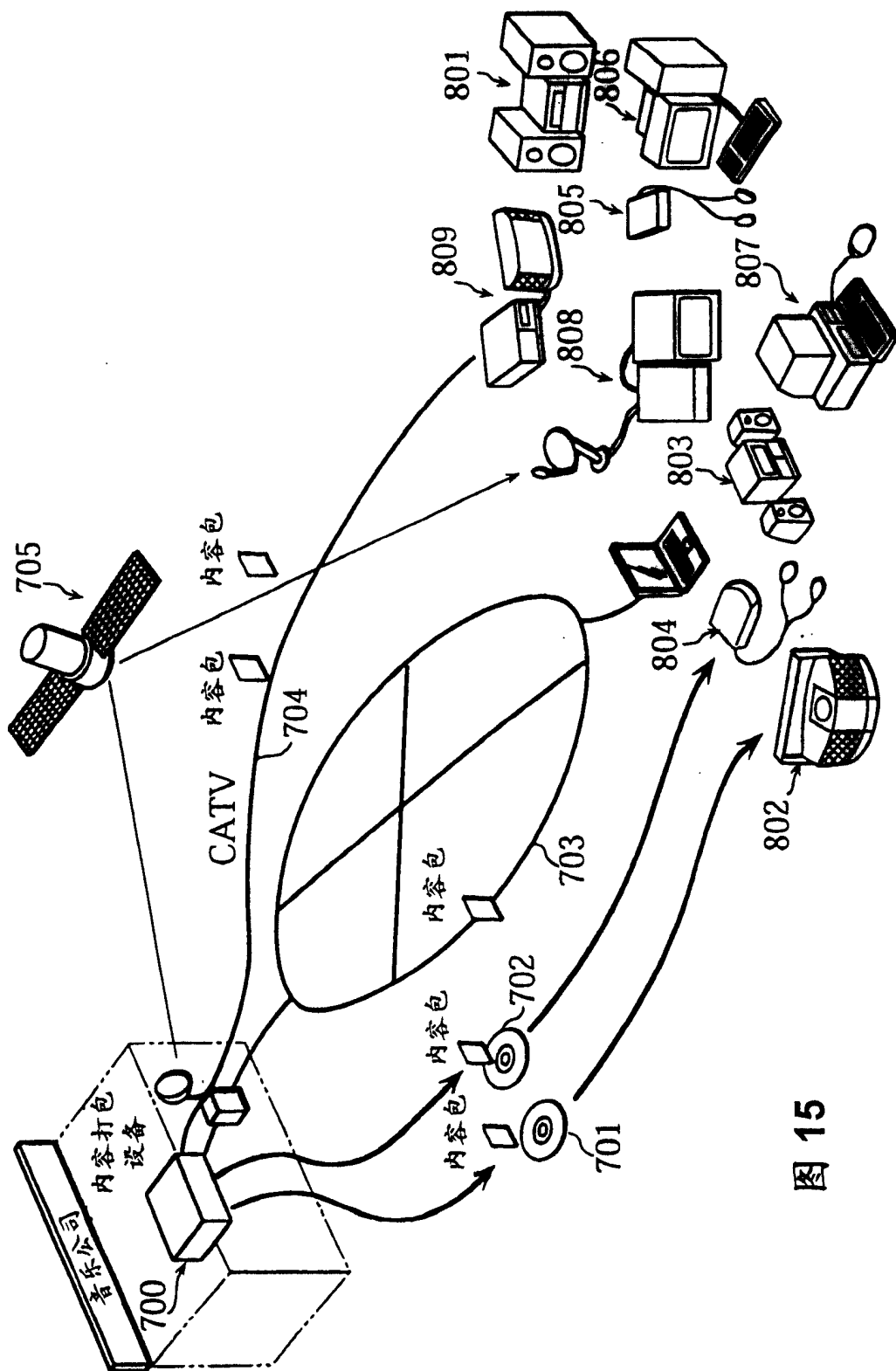


图 15

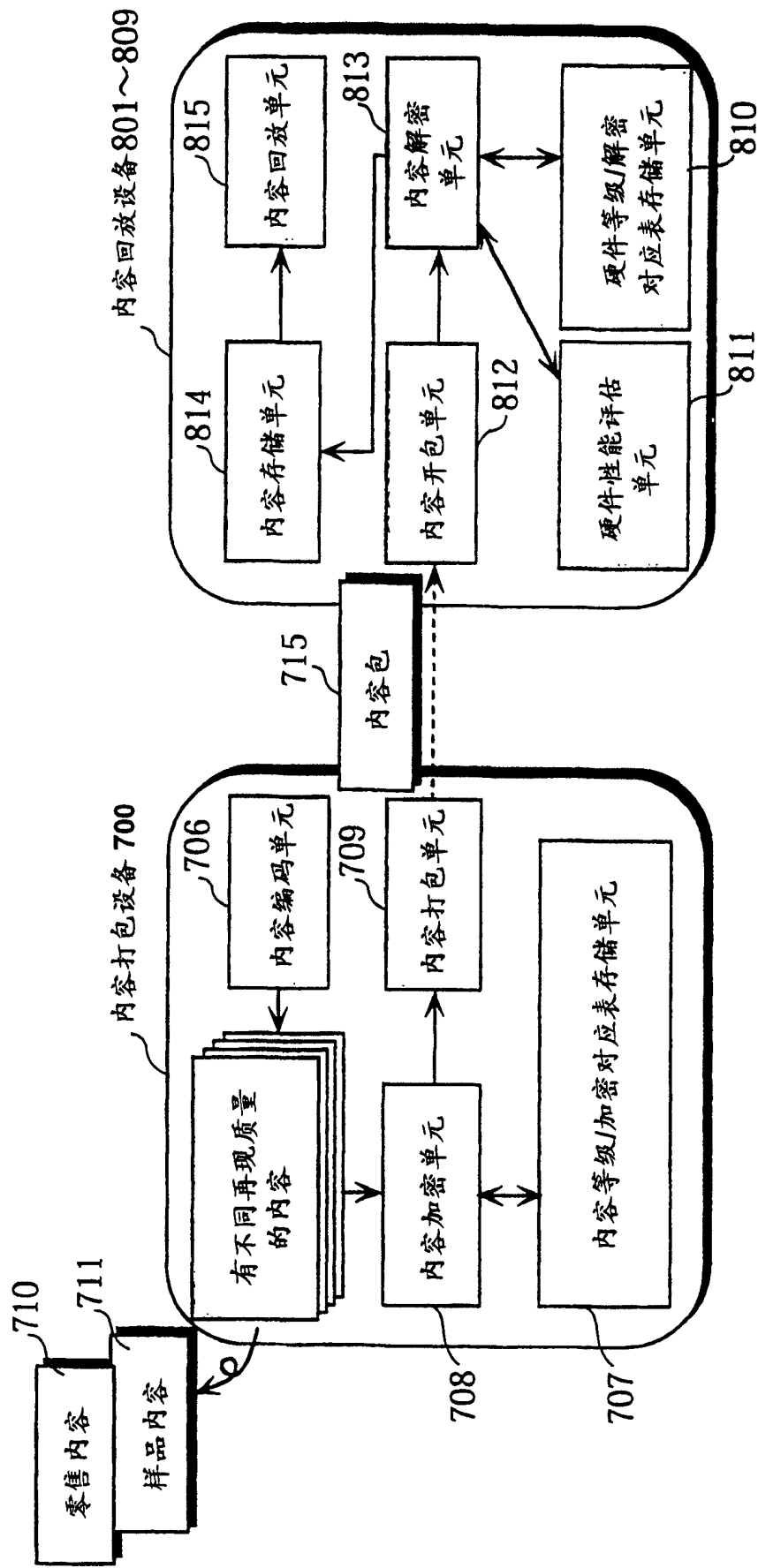


图 16

| 内容等级 | 量化位数 | 采样频率      |
|------|------|-----------|
| 1 级  | 24 位 | 96 KHz    |
| 2 级  | 16 位 | 44.1 KHz  |
| 3 级  | 16 位 | 22.05 KHz |

图 17A

| 内容等级 | 加密密钥位数 | 加密算法 |
|------|--------|------|
| 1 级  | 1024 位 | RSA  |
| 2 级  | 512 位  | RSA  |
| 3 级  | 56 位   | DES  |

图 17B

| 硬件等级 | 解密密钥位数 | 解密算法 |
|------|--------|------|
| A 级  | 1024 位 | RSA  |
| B 级  | 512 位  | RSA  |
| C 级  | 56 位   | DES  |

图 17C

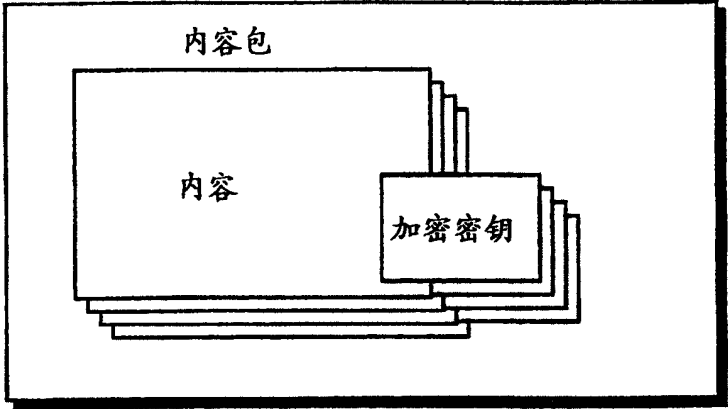


图 18

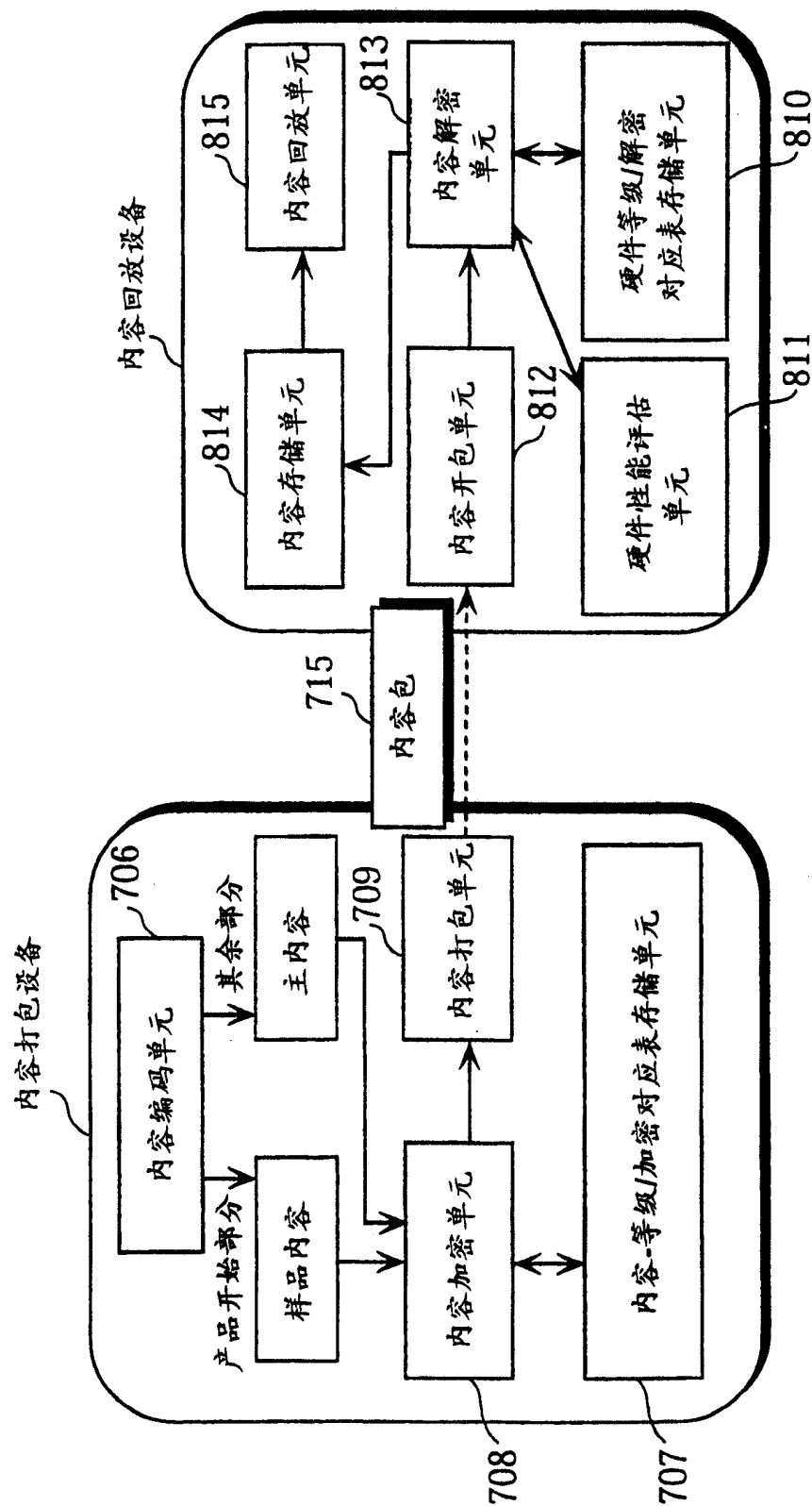


图 19

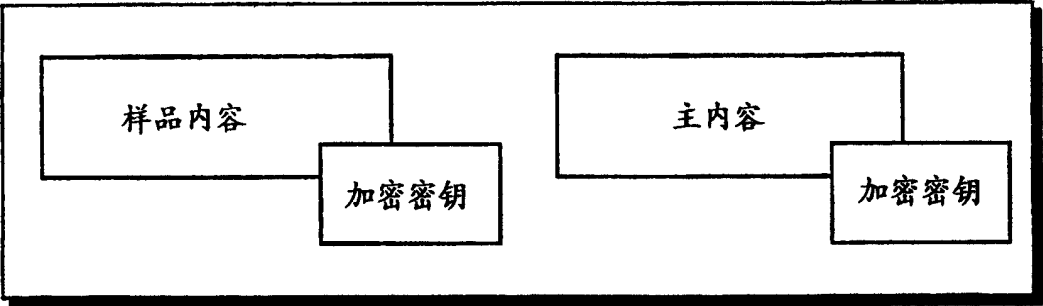


图 20