[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G11B 7/00
G11B 20/10 G11B 7/26
G11B 20/12

[12] 发明专利说明书

[21] ZL 专利号 95191218.6

[45] 授权公告日 2003 年 10 月 29 日

[11] 授权公告号 CN 1126079C

[22] 申请日 1995.11.16 [21] 申请号 95191218.6
[30] 优先权
[32] 1994.11.17 [33] JP [31] 283,415/1994
[32] 1995.2.2 [33] JP [31] 016,153/1995
[32] 1995.10.9 [33] JP [31] 261,247/1995
[86] 国际申请 PCT/JP95/02339 1995.11.16
[87] 国际公布 WO96/16401 日 1996.5.30
[85] 进入国家阶段日期 1996.7.15
[71] 专利权人 松下电器产业株式会社
地址 日本国大阪府门真市
[72] 发明人 大嶋光昭 後藤芳稔
审查员 周 滨

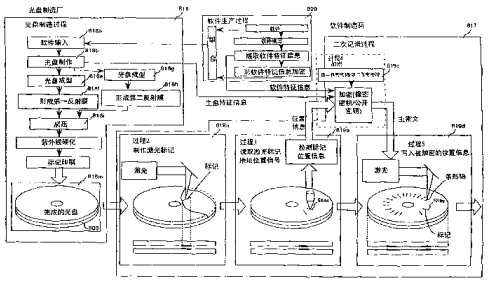
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 汪惠民

权利要求书 6 页 说明书 43 页 附图 42 页

[54] 发明名称 光盘标记形成设备及方法、再现设备、光盘及其制造方法

[57] 摘要

本发明的目的是提供一种标记形成设备、一种在光盘上形成激光标记的方法、一种再现设备、一种光盘和一种制造光盘的方法。与现有技术相比，本发明大大提高了防止复制的能力。为了达到该目的，例如在本发明的光盘中，用激光器在保持所写数据的光盘的反射膜上形成标记，并以加密的形式或用添加数字签名，至少将标记的位置信息或与位置信息有关的信息写到光盘上。



ISSN1008-4274

1. 一种标记形成设备，其特征在于，包括：

激光标记形成装置(813)，用于至少将一个标记(584)加至在盘上形成的至少一层反射膜上；

标记位置检测装置(600)，用于至少检测所述标记的一个位置；和

位置信息输出装置(596)，用于输出所述检测到的位置，作为所述标记的位置信息。

2. 如权利要求 1 所述的标记形成设备，其特征在于，还包括位置信息写入装置(813)，用于至少把所述输出位置信息或与所述位置信息有关的信息写至所述盘或不同的媒体上。

3. 如权利要求 2 所述的标记形成设备，其特征在于，所述位置信息写入装置(813)包括至少对所述输出位置信息或与所述位置信息有关的信息加密的加密装置(830)，并将如此加密后的内容写到所述盘上。

4. 如权利要求 3 所述的标记形成设备，其特征在于，当加密装置(830)进行加密时，它使用公开密钥加密函数的保密密钥或保密密钥加密函数的保密密钥。

5. 如权利要求 3 所述的标记形成设备，其特征在于，所述加密装置(830)包括：

第一加密装置(831)，它用公开密钥加密函数的主保密密钥对写在所述盘上的与软件内容特征有关的软件特征信息和所述公开密钥加密函数的副公开密钥进行加密；和

第二加密装置(832)，它用对应于所述副公开密钥的副保密密钥对所述位置信息或与所述位置信息有关的信息加密，并且

用于至少写入所述输出位置信息或与所述位置信息有关的信息的装置(845)，将所述第一加密装置加密的内容和所述第二加密装置加密的内容写到所述盘上。

6. 如权利要求 2 所述的标记形成设备，其特征在于，所述位置信息写入装置(813)包括数字签名装置，所述数字签名装置用于将数字签名至

少加至所述输出位置信息或与所述位置信息有关的信息中，并且

用于至少写入所述输出位置信息或与所述位置信息有关的信息装置(845)，将与所述数字签名的应用结果有关的信息写至所述盘上。

7. 如权利要求 6 所述的标记形成设备，其特征在于，当所述数字签名装置施加所述数字签名时，它使用公开密钥加密函数的保密密钥。

8. 如权利要求 6 所述的标记形成设备，其特征在于，所述数字签名装置包括：

第一数字签名装置(866b)，它用一公开密钥加密函数的主保密密钥将数字签名加至与写在所述盘上的软件内容特征有关的软件特征信息和所述公开密钥加密函数的副公开密钥上，和

第二数字签名装置(866f)，它用对应于所述副公开密钥的副保密密钥将数字签名加至所述位置信息或与所述位置信息有关的信息上，并且

用于至少写入所述输出位置信息或与所述位置信息有关的信息的装置(845)，将所述第一数字签名装置施加所述数字签名的结果和所述第二数字签名装置施加所述数字签名的结果写到所述盘上。

9. 如权利要求 2 所述的标记形成设备，其特征在于，位置信息写入装置(813)并存地写入通过对同一位置信息使用多种加密技术或数字签名技术而处理的信息。

10. 如权利要求 4、5、7 或 8 所述的标记形成设备，其特征在于，所述公开密钥加密函数是 RSA 函数或椭圆函数。

11. 如权利要求 1 至 9 中任何一项所述的标记形成设备，其特征在于，通过将两个盘层压在一起来构成所述盘。

12. 如权利要求 10 所述的标记形成设备，其特征在于，通过将两个盘层压在一起来构成所述盘。

13. 一种在光盘上形成激光标记的方法，其特征在于该方法包括下列步骤：

在盘上形成表示可通过光照射读取的数据信号的凹坑；

在所述盘上形成反射膜；

将所述盘与另一个盘层压在一起；和

用激光在所述反射膜上至少形成一个标记。

14. 一种再现设备（9004），其特征在于，包括：

位置信息读出装置（9101），它用于读出至少一个标记的位置信息或与所述位置信息有关的信息，所述标记位于在盘上形成的至少一层反射膜上，并且检测所述标记的位置，至少将如此检测得到的位置作为所述标记的所述位置信息输出；

标记读出装置（9106），用于读取至少与所述标记的一个实际位置有关的信息；

比较／判定装置（9107），它利用所述位置信息读出装置的读出结果和所述标记读出装置的读出结果进行比较和判断；和

光盘再现装置，它根据所述比较／判定装置所进行的比较和判断结果，再现被记录在所述光盘上的数据。

15. 如权利要求 14 所述的再现设备，其特征在于，用位置信息写入装置(813)至少将所述输出位置信息或与所述位置信息有关的信息写到所述盘上。

16. 如权利要求 15 所述的再现设备，其特征在于，

所述位置信息写入装置(813)包括加密装置(830)，所述加密装置至少对所述输出位置信息或与所述位置信息有关的信息加密，并且

所述位置信息读出装置包括与所述加密装置对应的解密装置(9105)，并且用所述解密装置对所述加密的位置信息或与所述位置信息有关的信息解密。

17. 如权利要求 16 所述的再现设备，其特征在于，当加密装置(830)进行加密时它使用公开密钥加密函数的保密密钥，并且

所述解密装置(9105)用对应于所述保密密钥的公开密钥进行解密。

18. 如权利要求 16 所述的再现设备，其特征在于，

所述加密装置(830)包括：

第一加密装置(831)，它用一公开密钥加密函数的主保密密钥对与写在所述盘上的软件内容特征有关的软件特征信息和所述公开密钥加密函数的副公开密钥进行加密，和

第二加密装置(832)，它用对应于所述副公开密钥的副保密密钥对所述位置信息或与所述位置信息有关的信息加密，并且所述解密装置(9105)

包括：

第一解密装置(534)，它用对应于所述主保密密钥的主公开密钥对所述被加密的软件特征信息和所述公开密钥加密函数的被加密的副公开密钥解密，和

第二解密装置(718)，它用如此解密的副公开密钥对所述被加密的位置信息和与所述位置信息有关的信息解密。

19. 如权利要求 15 所述的再现设备，其特征在于，

所述位置信息写入装置(813)包括用于将数字签名至少加至所述输出位置信息或与所述位置信息有关的信息中的数字签名装置，并将与所述数字签名施加结果有关的信息写到所述盘上，

并且所述位置信息读出装置(9101)包括：

认证装置，它与所述数字签名装置相对应，和

位置信息提取装置(964)，它通过所述认证装置所进行的认证过程和/或从与所述数字签名施加结果有关的信息中获得所述位置信息，

当所述认证装置产生表示所述认证结果正确性的输出时，所述比较/判定装置(9107)用所述位置信息提取装置(964)获得的位置信息和所述标记读出装置读出的结果进比较和判定，并且当不产生所述表示正确性的输出时，不进行再现。

20. 如权利要求 19 所述的再现设备，其特征在于，

当所述数字签名装置施加所述数字签名时，它使用公开密钥加密函数的保密密钥，并且

所述认证装置用对应于所述保密密钥的公开密钥进行所述认证。

21. 如权利要求 19 所述的再现设备，其特征在于，

所述数字签名装置包括：

第一数字签名装置(866b)，它用一公开密钥加密函数的主保密密钥将数字签名加至与写在所述盘上的软件内容特征有关的软件特征信息和所述公开密钥加密函数的副公开密钥上，和

第二数字签名装置(866f)，它用对应于所述副公开密钥的副保密密钥将数字签名加至所述位置信息或与所述位置信息有关的信息上，

并且用于至少写入所述输出位置信息或与所述位置信息有关的信息

的装置(845)，将所述第一数字签名装置施加所述数字签名的结果和所述第二数字签名装置施加所述数字签名的结果写到所述盘上，

并且，所述位置信息读出装置包括：

认证装置，它用对应于所述主保密密钥的主公开密钥认证所述加有数字签名的软件特征信息和所述公开密钥加密函数的副公开密钥，和

位置信息提取装置(964)，它由所述认证过程和／或从用所述认证过程所获得的副公开密钥施加所述数字签名的结果中和／或从施加所述数字签名的结果中获得所述位置信息，

并且，当所述认证装置产生表示所述认证结果正确性的输出时，所述比较／判定装置(9107)用所述位置信息提取装置获得的位置信息和所述标记读出装置读出的结果进行比较和判定，并且当不产生所述表示正确性的输出时，不进行再现。

22. 如权利要求 14 至 21 中任何一项所述的再现设备，其特征在于，当所述比较和判定的结果是，所述位置信息读出装置(9101)读出的结果与所述标记读出装置读出的结果相互不一致时，不进行再现。

23. 如权利要求 17、18、19 或 21 所述的再现设备，其特征在于，所述公开密钥加密函数是 RSA 函数或椭圆函数。

24. 一种制造光盘的方法，其特征在于，该方法包括下列步骤：

至少形成一个盘；

在所述形成的盘上形成反射膜；

至少将一个标记加至所述反射膜上；

至少检测所述标记的一个位置；并且

将所述检测到的位置作为所述标记的位置信息输出，并对所述信息加密，以写到所述盘上。

25. 一种制造光盘的方法，其特征在于，该方法包括下列步骤：

至少形成一个盘；

在所述形成的盘上形成反射膜；

至少将一个标记加至所述反射膜上；

至少检测所述标记的一个位置；并且

将所述检测到的位置作为所述标记的位置信息输出，并施加与所述

位置信息有关的数字签名，以写到所述盘上。

26. 一种光盘，其特征在于，用激光在保持所写数据的盘的至少一层反射膜（802）上形成表示至少一个标记的凹坑（584）；并以加密的形式或用所加的数字签名，至少将所述标记的位置信息或与所述位置信息有关的信息写到所述盘上。

27. 一种光盘，其具有的结构是至少一层反射膜（802）被直接或间接地夹在由耐激光材料形成的两组件之间，包括：

表示可通过光照射读取的数据信号的凹坑，

形成在凹坑上的反射膜，和

用激光在所述反射膜上形成的至少一个标记。

光盘标记形成设备及方法、再现设备、光盘及其制造方法

技术领域

本发明涉及一种形成标记的设备，在光盘上形成激光标记的方法，一种再现设备，一种光盘、和制造光盘的方法，例如可用它们防止光盘复制。

背景技术

近年来，随着只读存储器（ROM）型光盘的广泛使用，盗版光盘也泛滥成灾，侵犯了版权人的权利。

这是因为 ROM 盘的制造设备容易买到，并且很容易操作。

盗版者只要从小型光盘（CD）所包含的软件中提取逻辑数据，将其复制在磁带上，再把磁带放在主盘制作设备上，便可制作 CD 主盘。从该单个主盘可以压制出成千上万的盗版盘。由于盗版者不付版税，所以他们通过低价出售盗版盘来获得利润。这必然给版权人造成经济损失。

对于现用的 CD 规范，只有从 CD 上读取逻辑数据的功能，而没有检查光盘物理特征的功能，因此，通过对逻辑数据的按比特复制很容易制作盗版 CD。

现有技术揭示了一种通过增加光盘物理特征的识别功能来防止盗版的方法。

该方法包括建立一种新的规范，新规范规定，在原版盘上包括一个物理标记，以防止按该规范制作的光盘被盗版。作为现有技术的一个例子，日本未审查专利公报第 5－325193 号揭示了一种防盗版的方法。根据该方法，在切割过程中，当记录某一指定区域时，故意沿光道（tracking）方向摆动记录光束，以在主盘上形成一摆动线（wobbling）。当在装有摆动线检测电路的再现设备上重放光盘时，检查光盘，观察在上述指定区域中是否形成有摆动线。如果在指定区域中检测到有指定摆动线频率的

摆动线，则判定该光盘是合法光盘；否则，判定该光盘为盗版光盘。

具体他说就是，根据预定的物理标记设计数据，用具有制作摆动线功能的特殊的主盘制作设备在主盘上形成一物理标记。由于盗版者既没有这种特殊的主盘制作设备，也没有物理标记设计数据，所以可以防止盗版者制作盗版光盘。在每个按该规范制作的光盘上都需要形成这样一个防盗版标记，但是，由于通过对合法光盘的检查可以提取此物理标记，所以现有技术存在这样的问题，即如果这种特殊的主盘制作设备落入非法人员的手中，就可以制造盗版盘了，在本专利说明书中，在主盘上形成物理标记的防盗版方法将被称为主盘级方法。

除了上述方法外，已出现一种更成熟的主盘级方法，该方法包括形成一个更复杂的物理标记。另一方面，还已知一种复制方法，无论在主盘级上制作的物理标记有多复杂，该方法可以通过熔化合法盘的树脂，来制作具有完全相同物理特征的复制品。该方法需要大量的时间和资金来制造一个主盘，但由于可从一个盗版的主盘制作成千上万的光盘，所以每个盗版盘的成本很低。因此，产生这样一个问题，即随着将来复制方法的普及，防盗版技术在主盘级上的效力会被破坏。

如上所述，现有的防盗版技术存在一些问题需要克服。

这些问题概括如下。

问题 1：由于可以复制物理标记，所以现有技术中主盘级防盗版技术的效力较低。

向题 2：在根据物理标记设计数据形成物理标记的现有方法中，如果获得了与合法光盘制造商使用的设备同样精密的制造设备，便很容易制造非法光盘。

问题 3：由于现有防盗版方法所提供的安全级是固定的，因此其效力会相对不断提高的盗版技术而下降。

问题 4：如果允许无复制保护的光盘格式与有复制保护的光盘格式共存，则可用无复制保护的光盘格式制作盗版光盘。因此，必须制造都有复制保护的光盘。因此，复制保护的使用局限于诸如游戏盘等详细规范。

问题 5：根据现有的方法，只有有限数量的许可公司拥有特殊的制

造设备，并且不能使设备公开。因此除了在这些许可公司，软件制造商不能制造光盘。

问题 6：在主盘作标记的方法中，由同一主盘压制的所有光盘都具有相同的光盘标识符 ID。这意味着，使用同一口令便能运行所有的光盘。因此，不能保持口令的保密性，除非与软盘或通讯线结合起来使用。另外，由于不可能进行二次记录，所以每次使用光盘时都必须输入口令。

发明内容

从以上概括的现有技术中的问题来看，本发明的一个目的是，获得一种与现有技术相比有很大提高的防复制能力。

具体他说，本发明提供了下列装置，以克服上述现有技术中防盗版方法的六个问题。

为了克服问题 1，提供了一种防盗版方法，该方法包括在反射膜等级上使用物理标记，而不是如现有技术中在主盘等级上使用物理标记，在该方法中，在光盘反射膜上形成物理标记。如果在主盘等级上进行复制，则该方法可防止生产盗版盘。

为了克服问题 2，使用一种新的 ROM 记录装置，它用激光器对两盘层压的 ROM 光盘进行二次记录，第一步，随机形成物理标记，而第二步，用高达 0.13 微米的测量精度来测量物理标记。第三步，用二次记录装置对它们的位置信息进行加密，用数十微米的常用处理精度将一条形码记录至 ROM 盘上。由此，可用比常规设备的处里精度高得多的精度例如 0.1 微米的精度来获得光学标记位置信息。由于用市场可买到的设备不能以 0.1 微米的精度形成光学标记，所以可以防止生产盗版盘。

为了克服问题 3，将安全度低的第一代密码和安全度高的第二代密码都预先记录在一媒质上，其中每种密码都用一数字化的签名对位置信息进行加密，并且如果再现设备的设计更新换代，则可通过使用这种媒质，用与应用代相应的安全度防止盗版。

为了克服问题 4，将表示软件产品是否具有版权防盗版功能的防盗版功能识别符记录在主盘上。为了防止识别符被变更，当把软件内容记录在主盘上时，将压缩的软件内容信息和防盗版功能识别符一起混合编码和加密。由于不能变更识别符，所以盗版者不能用无防盗版措施的光

盘格式生产光盘。这防止了盗版盘的生产。

为了克服问题 5，由主密钥生成副密钥，作为制造光盘不可缺少的进行数字签名的保密密钥，并且把副密钥交给每个软件制造商，从而允许软件制造商在其自己的工厂制造合法盘。

为了克服问题 6，将每个光盘都不同的本发明防盗版标记的位置信息用作光盘标识符。将位置信息和光盘序号即光盘 ID 合并并与数字签名一起加密，从而给每个盘增加一个不可更改的光盘 ID。由于每个完成的盘都具有不同的 ID，所以口令也是不同的。口令在其他盘上不会有效。这增加了口令的安全度。

另外，用本发明的二次记录将口令二次记录在光盘上，使该光盘永远成为可操作盘。

以下通过实施例描述用于克服上述六个问题的具体方法。

本发明提供了一种标记形成设备，该设备包括：激光标记形成装置，用于至少将一个标记加至在盘上形成的至少一层反射膜上；标记位置检测装置，用于至少检测所述标记的一个位置；和 位置信息输出装置，用于输出所述检测到的位置，作为所述标记的位置信息。

本发明还提供一种标记形成设备，它还包括：位置信息写入装置，用于至少把所述输出位置信息或与所述位置信息有关的信息写至所述光盘或不同的媒质上。

本发明还提供一种在光盘上形成激光标记的方法，该方法包括下列步骤：在盘上形成表示可通过光照射读取的数据信号的凹坑；在所述盘上形成反射膜；将所述盘与另一个盘层压在一起；和用激光在所述反射膜上至少形成一个标记。

本发明还提供一种再现设备。该设备包括：位置信息读出装置，用于读出至少一个标记的位置信息或与所述位置信息有关的信息，所述标记位于形成在光盘上的至少一层反射膜上，并且对其位置进行检测，至少将如此检测得到的位置作为所述标记的所述位置信息输出；标记读出装置，用于读取与所述标记的至少一个实际位置有关的信息；比较 / 判定装置，它利用所述位置信息读出装置的读出结果和所述标记读出装置的读出结果进行比较和判断；以及光盘再现装置，它根据所述标记 / 判

断装置所进行的比较和判断，再现被记录在所述光盘上的数据。

本发明还提供了一种制造光盘的方法，该方法包括下列步骤：至少成型一个盘；在所述成型的盘上形成反射膜；至少将一个标记加至所述反射膜上；至少检测所述标记的一个位置；并将所述检测到的位置作为所述标记的位置信息输出，并对所述信息加密，以写到所述光盘上。

本发明还提供一种制造光盘的方法，该方法包括下列步骤：至少成型一个盘；在所述成型的盘上形成反射膜；至少将一个标记加至所述反射膜上；至少检测所述标记的一个位置；并将所述检测到的位置作为所述标记的位置信息输出，并施加与所述位置信息有关的数字签名，以写到所述光盘上。

本发明还提供了一种光盘，在该光盘中，用激光在保持所写数据的盘的至少一层反射膜上形成表示至少一个标记的凹坑；并以加密的形式或用所加的数字签名，至少将所述标记的位置信息或与所述位置信息有关的信息写到所述盘上。

本发明还提供了一种光盘，其具有的结构是至少一层反射膜被直接或间接地夹在由耐激光材料形成的两组件之间，包括表示可通过光照射读取的数据信号的凹坑，形成在凹坑上的反射膜，和用激光在所述反射膜上形成的至少一个标记。

附图说明

图 1 示出了本实施例中光盘制造过程和二次记录过程的示意图；

图 2（a）是实施例中光盘的俯视图，（b）是实施例中光盘的俯视图，（c）是实施例中光盘的俯视图，（d）是实施例中光盘的横向截面图，而（e）是本实施例中再现信号的波形图；

图 3 是一流程图，示出了依照本实施例以条形码的形式在光盘上记录被加密位置信息的过程；

图 4 示出了本实施例的光盘制造过程和二次记录过程（部分 1）的示意图；

图 5 示出了本实施例的光盘制造过程和二次记录过程（部分 2）的示意图；

图 6 示出了本实施例的双层光盘制造过程（部分 1）的示意图；

图 7 示出了本实施例的双层光盘制造过程（部分 2）的示意图；

图 8（a）是本实施例的层压型非反射部分的放大图，而（b）是本实施例的单板型非反射部分的放大图；

图 9（a）是本实施例中一非反射部分的再现波形图，（b）是本实施例中一非反射部分的再现波形图，而（c）是本实施例中一非反射部分的再现波形图；

图 10（a）是本实施例中层压型非反射部分的截面图，而（b）是本实施例中单板型非反射部分的截面图；

图 11 是一示意图，它根据在透射电子显微镜下的观察，示出了本实施例中非反射部分的截面；

图 12（a）是本实施例中一光盘的截面图，而（b）是本实施例中该光盘非反射部分的截面图；

图 13（a）一示意图，示出了实施例中合法 CD 上地址的物理配置，而（b）示出了实施例中非法复制的 CD 上地址的物理配置；

图 14 是实施例中光盘制造的方框图；

图 15 是实施例中低反射位置检测器的方框图；

图 16 是实施例中检测低反射部分之地址 / 时钟位置的原理图；

图 17 是合法光盘与复制光盘的低反射部分地址表的对照图；

图 18 是实施例中用一个方向函数的光盘检查过程的流程图；

图 19 是实施例中不同主盘上地址坐标位置的比较图；

图 20 是实施例中低反射位置检测程序的流程图；

图 21 是实施例中磁记录设备的方框图；

图 22 是实施例中用 RSA 函数进行加密等过程的流程图；

图 23 是实施例中用椭圆函数进行数字签名等过程的流程图；

图 24 是实施例中位置信息检查过程的流程图；

图 25 是实施例中信息处理设备的方框图；

图 26 是实施例中第二低反射部分的俯视图；

图 27 是本实施例中第一层标记信号的检测波形图；

图 28 是本实施例中第二层标记信号的检测波形图；

图 29 是本实施例中一光盘制造设备的方框图；

图 30 是本实施例中非反射部分的代码图；

图 31 是本实施例中来自非反射部分的检测波形图；

图 32 是说明本实施例中条形码记录的信息内容及其相互关系的说明图；

图 33 是依照本实施例在双层光盘中形成的非反射部分的透视图；

图 34 说明了本实施例中光盘分布的数据流程；

图 35 示出了本实施例的光盘分布过程；

图 36 是一方框图，说明了依照本实施例当用主密钥、副密钥等对位置信息进行复杂加密时的一种制造过程；

图 37 是一方框图，说明了依照本实施例当用主密钥、副密钥等对位置信息复杂加密时的制造过程；

图 38 是本实施例中一再现设备的流程图；

图 39 是本实施例中在光盘上联合使用的保密密钥加密和公开密钥加密，及其与再现设备关系的示意图；

图 40 是一方框示意图，示出了依照本实施例在光盘上记录用主密钥、副密钥等加密的位置信息的过程和再现这种信息的过程；

图 41 是本实施例中一光盘再现设备的方框图；

图 42 是一流程图，示出了本实施例中扰码标识符的功能和程序安装过程中驱动 ID 与光盘 ID 之间的切换。

具体实施方式

以下结合本发明的一个实施例描述标记形成设备的构造和工作情况、在光盘上形成激光标记的方法、再现设备、和制造光盘的方法。

在这里所给的本实施例的描述中，前半部分（1）叙述这样一些操作，如制造光盘，用激光形成标记，读取标记的位置信息，为对光盘进行写操作而对位信息等进行加密和其他处理，以及在一播放机上重放光盘。在第一部分（1）中主要描述加密和再现操作。

接着，在后半部分（2）中，将进一步详细描述已在第一部分（1）中作简要描述的，对光盘上标记位置信息的加密和其他处理等，以及对

位置信息的解密和再现等，第二部分（2）还叙述了各种防盗版技术。

在本专利说明书中，激光熔蚀（laser trimming）被称为激光制标，同时非反射的光学标记部分被简称为标记或光学标记，或者有时被称为光盘独有的物理标识符。

（1）图 1 是一流程图，示上了光盘从制造至完成的一般过程的流程。

首先，软件公司在软件生产过程 820 中进行软件创作。完成后的软件从软件公司送到光盘制造厂。在光盘制造厂，在光盘制造过程 816 中，在步骤 818a 输入完成的软件，（在步骤 818b）生产主盘，（在步骤 818e、818g）压制光盘，（在步骤 818f、818h）在各光盘上形成反射膜，（在步骤 818i）将两个盘层压在一起，并（在步骤 818m 等）完成诸如 DVD 或 CD 的 ROM 光盘。

将如此完成的光盘 800 交给软件制造商，或者软件制造商控制的一个工厂，在这里，在二次记录保持 817 中，（在步骤 819a）形成如图 2 所示的防盗版标记 584，并在（步骤 819b）用测量装置读取该标记的准确位置信息，以获得起光盘物理特征信息作用的位置信息。在步骤 819c，对光盘的这个物理特征信息加密。将加密后的信息转换成脉冲宽度调制（PWM）的信号，然后在步骤 819d，用激光将其作为条形码信号记录在光盘上。在步骤 819c 中，将光盘物理特征信息与软件特征信息结合在一起，用于加密。

现将进一步详细地描述上述过程。即，将参照图 4、图 5 和图 8 至 12，详细描述本发明中有关光盘的制造过程、标记制作过程、标记位置读取过程、和加密信息写入过程。还将参照图 6 和图 7 补充说明具有双层反射层的光盘。在以下的描述中，标记制作过程和标记位置读取过程被统称为二次记录过程。

（A）首先，将描述光盘制造过程。在图 4 所示的光盘制造过程 806 中，首先在步骤（1）压制透明衬底 801。在步骤（2），溅射诸如铝或金等金属，以形成反射层 802。通过旋压涂覆，将由紫外线固化树脂形成的粘着层 804 施加到在不同处理步骤中形成的衬底 803 上，而且将衬底 803 与具有反射层 802 的透明衬底 801 胶合，并使其高速旋转，从而使胶合间隔均匀。在外界紫外射线的曝光下，树脂硬化，从而将两片衬底

牢固地胶合在一起。在步骤（4），通过丝网印刷或胶版印刷，印刷一层印刷层805，该印刷层上将印刷CD或DVD的标题。由此，在步骤（4），完成了普通的层压型ROM光盘。

（B）接着，将参照图4或图5描述标记形成过程。在图4中，使钇铝拓榴石（YAG）脉冲式激光器813发出的激光束通过凸透镜814聚焦在反射层802上，以形成图5中步骤（6）所示的非反射部分815，即，从图5中步骤（6）形成的非反射部分815中再产生出一区别波形，例如步骤（7）所示的波形（A）。通过对该波形的限幅，可获得波形（B）所示的标记检测信号，由该标记检测信号可以测得分层标记位置信息，它包含信号（d）中所示的地址以及信号（e）中所示的地址、帧同步信号编号和再现时钟计数。

如前所述，以下将参照图6和图7补充说明另一种类型的光盘（双层层压盘）。

图4和图5示出了一般称作单层层压盘的光重，它只在一个衬底801上有反射层。另一方面，图6和图7示出了一般称为双层层压盘的光盘，它在两个衬底801和803上都有反射层。对于激光熔蚀，步骤（5）和步骤（6）对两种类型的光盘都基本相同，明显的不同将在下文中作简要描述，首先，单层光盘使用反射率高达或超过70%的铝膜所形成的反射层，而在双层光盘中，读出面衬底801上形成的反射层825是反射率为30%的半透明金（Au）膜，印刷面衬底803上形成的反射层802与单层光盘中使用的相同，其次，与单层光盘相比，双层光盘需要较高的光学精度，例如，粘着层804必须光学透明且厚度均匀，并且光学透明度不能因激光熔蚀而受损失。图7的步骤（7）、（8）和（9）示出了双面记录层光盘第一层的波形。第二层的波形类似于第一层的波形，但其信号电平低于第一层的信号电平。然而，由于第一和第二层被胶合在一起，所以它们之间相对位置的准确度是随机的，并且只能控制在凡百微米的精度内。如以下将要描述的，由于激光束要通过两层反射膜，所以例如要制作非法光盘，则必须使第一和第二层上第一标记的位置信息与合法光盘上的数值相同。但是使它们匹配要求在层压时具有近亚微米的精度，因此，制作双层类型的非法光盘是不可行的。

以下参照图 8 至 12，用段落（a）至（d）进一步详细地描述形成非反射光学标记部分的技术，与单层类型作比较，叙述层压型。图 8（a）和（b）是两张显微相片，示出了非反射光学标记部分的平面图，而图 10 是双层层压盘非反射部分的截面简化示意图。

（a）用 5 微焦耳 / 脉冲的 YAG 激光器，将激光束照射在 500 埃厚的铝层上，铝层位于由两片 0.6 毫米厚的光盘层压构成的 1.2 毫米厚 ROM 光盘表面以下 0.6 毫米处，结果形成了图 8（a）中放大 750 倍的 12 微米宽的缝状非反射部分 815。在该放大 750 倍的显微相片中，非反射部分 815 上观察不到铝的残留物。沿非反射部分 815 和反射部分间的边界可观察到增厚的铝层，厚 2000 埃，宽 2 微米。如图 10（a）所示，可以确定内部没有发生重大的破损。在这种情况下，估计脉冲式激光器的作用熔化了铝反射层，并因表面张力，产生了熔化的铝沿两侧边界堆积的现象。我们称此为热熔表面张力（hot melt surface tension）（HMST）记录法。这是在层压盘 800 上才能观察到的特征现象。图 11 是一示意图，它根据透射电子显微镜（TEM）下的观察，示出了上述激光熔浊过程所形成的非反射部分的截面图。在图中，如果铝膜增厚部分宽 1.3 微米，厚 0.20 微米，则该部分中增加的铝的数量为 1.3×（0.20－0.05）＝0.195 微米 ^{2}，原先沉积在激光瀑光区（10 微米）一半部分（5 微未）中铝的数量为 5×0.05=0.250 微米 ^{2}，其差算得为 0.250－0.195=0.055 微米 ^{2}，就长度而言，它等于 0.055 / 0.05=1.1 微米。这表示保留下来的铝层 0.05 微米厚，1.1 微米长，因此可以说几乎所有的铝都被移到膜增厚的部分，因此，该图的分析结果还证明了对上述特征现象的解释。

（b）接下来将叙述单板光盘（光盘包含单个盘）。用相同功率的激光脉冲进行实验，曝光在单侧模压盘上形成的厚度为 0.05 微米的铝反射层，其结果如图 8（b）所示。如图中所示，可观察到铝的残留物，并且由于铝的残留物会引起重放噪音，因此可见，单板型不适于进行光盘信息的二次记录，它要求高密度和低差错率，另外，与层压盘不同，对单板盘的情况，如图 10（b）所示，当非反射部分经激光熔蚀时，保护层 862 会不可避免地发生破损。破损程度依赖于激光功率，但即使精确控制激光功率，破损也不可避免。再有，根据我们的实验，对于用丝网印刷在

保护层 862 上形成数百微米厚的印刷层 805，当其热吸收高时会被损坏。对于单板盘的情况，为了解决保护层破损的问题，或者必须再加一层保护层，或者在沉积保护层之前进行激光切割工序。在任何情况下，单板型都有这样的问题，即必须将激光切割过程合并到压制过程中。尽管单板盘可用，但这限制了它的应用。

（c）以上用一个双层层压盘作为例子，讨论了单板盘与层压盘的对比。由上述讨论可知，用单层层压盘可以获得与双层层压盘相同的效果。参照图 12（a）和图 12（b）等，将进一步描述单层型的情况。如图 12（a）所示，反射层 802 一侧是透明的聚碳酸酯衬底 801，另一侧是硬化的粘着层 804 和一衬底，因此反射层 802 被密封其间。在这种情况下，将脉冲式激光聚焦加热；在我们的实验中，将 5 微焦耳 / 脉冲的热量加至反射层 802 上 10 至 20 微米直径的圆点上，持续 70 纳秒的时间。结果，温度马上升至熔点 600℃，导致熔化状态。通过热量传递，小部分靠近圆点的透明衬底 801 被熔化，并且一部分粘着层 804 也被熔化。表面张力向两侧加力，使该状态下熔化的铝沿边界 821a 和 821b 聚集起来，从而形成硬化的铝的聚集部 822a 和 822b，参见图 12（b）。由此形成没有铝残留物的非反射部分 584。这表明，如图 10（a）所示用激光熔蚀层压盘可以获得清楚明确的一非反射层部分 584。即使将激光功率增大超过最佳值的 10 倍，也不会观察到单板盘时因保护层破损使反射层外露的情况。激光熔浊后，非反射层 584 的结构如图 12（b）所示，它被夹在两个透明衬底 801 之间，并且粘着层 804 在两侧将其密封与外界隔绝，从而产生保护该结构免受外界影响的效果。

（d）接下来将描述把两盘层压在一起的另一好处。如图 10（b）所示，在单板盘的情况下，当以条形码形式进行二次记录时，非法制造商可通过清除保护层来曝光铝层。这就有可能通过在合法盘的条形码部分处再沉积一层铝层，然后激光熔蚀一不同的条形码，来篡改未加密的数据。例如，如果标识号被记录在明文中或者与主密文分开放，则在单板盘的情况下，可以改变标识号，用不同的密码非法使用软件。但是，如果如图 10（a）所示，在层压盘上进行二次记录，那么很难将层压盘分成两部分。另外，当把一部分与另一部分分开时，会使铝反射层部分受

损。当防盗版标记被破坏时，光盘将被判定为盗版盘，从而不能工作。因此，当对层压盘进行非法变更时，成功率是很低的，从而因经济原因抑制了非法变更。特别是，对于双层层压盘的情况，由于聚碳酸酯材料具有温度／湿度膨胀系数，所以一旦分离，就几乎不可能以数微米精度来对准第一和第二层上的防盗版标记，压合两盘，而大量生产光盘。因此，双层类型在盗版防御方面提供了更好的效果。由此发现，通过激光熔蚀层压盘 800 可以获得缝隙清晰明确的非反射部分 584。

上述段落（a）至（d）描述了形成非反射光学标记部分的技术。

（C）接下来，将描述读出由此形成的标记的位置的过程。

图 15 是一方框图，示出了光盘制造过程中用于检测非反射光学标记部分的低反射率光量检测器 586 以及与之相连的电路。图 16 示出了检测低反射率部分之地址／时钟位置的原理。为了便于说明，下文叙述当在单个盘构成的光盘上所形成的非反射部分上进行读操作时的操作原理。将会看到，同样的原理也适用于两盘层压所构成的光盘。

如图 15 所示，将光盘 800 放入装有低反射率位置检测器 600 的标记读取设备中，以读出标记，并且如图 9（a）的波形图所示，在该情况下，由于因有无凹坑所产生的信号波形和因存在非反射部分 584 所产生的信号波形在信号电平上有明显的差异，所以用一简单的电路便能将它们清楚地区分开。

用图 15 方框图中所示的低反射率光量检测器 586 可容易地检测到具有上述波形的非反射部分 564 的起始位置和终止位置。在低反射率位置信息输出部分 596，将再现的时钟信号用作参考信号，可获得位置信息。

如图 15 所示，低反射率光量检测器 586 中的比较器 587 通过检测信号电平比光量参考值 588 低的模拟光再现信号来检测低反射率光部分。在检测期间，输出图 16（5）所示波形的低反射率部分检测信号，测量该信号起始位置和终止位置的地址和时钟位置。

为了转换成数字信号，用具有 AGC 590a 的波形整形电路 590 对再现光信号进行整形。时钟再生器 38a 从整形的信号中再生时钟信号。解调装置 591 中的 EFM 解调器 592 对信号解调，并且 ECC 纠正差错并输出数字信号。经 EFM 解调的信号还被送至物理地址输出装置 593，在该

装置中，地址输出装置 594 输出 MSF 的地址，它来自 CD 中子码的 Q 个位，并且同步信号输出装置 595 输出诸如帧同步信号的同步信号。时钟再生器 38a 输出解调后的时钟。

在低反射率部分地址／时钟信号位置信号输出装置 596 中，低反射率部分起始／终止位置检测器 599 通过使用（n－1）地址输出装置 597 和地址信号以及时钟计数器（clock counter）598 和同步时钟信号或解调后的时钟，对低反射率部分 584 的起始位置和终止装置进行精确的测量。以下借助图 16 所示的波形图详细描述该方法。如图 16（1）中光盘的截面图所示，局部形成了标记号为 1 的低反射率部分 584。输出图 16（3）所示的反射包络信号，其中来自反射部分的信号电平低于光量参考电平 588。用光电平比较器 587 对此进行检测，并由低反射率光量检测器 586 输出如图 16（5）所示的低反射率光检测信号。如图 16（4）中再现的数字信号所示，由于它没有反射层，所以标记区不输出数字信号。

接着，为了获得低反射率光检测信号的起始和终止位置，将图 16（6）所示的解调后的时钟或同步时钟与地址信息联用。首先，测量图 16（7）中地址 n 处的参考时钟 605。当（n－1）地址输出装置 597 检测到紧挨在地址 n 前的地址时，发现下一个同步信号 604 是地址 n 处的同步信号，用时钟计数器 598 对同步信号 604 至参考时钟 605 的时钟数进行计数，它是低反射率光检测信号的起始位置。该时钟计数被定义为参考延迟时间 TD，由参考延迟时间 TD 测量装置 608 对其进行测量并存储起来。

电路延迟时间会随用于读操作的再现设备而变化，即参考延迟时间 TD 依赖于所用的再现设备。因此，使用 TD 时，用时间延迟校正器 607 进行时间校正，并且所得效果是，如果用设计不同的再现设备进行读操作，可以精确测量低反射率部分的起始时钟计数。接着，如图 16（8）所示，通过在下一光道中寻找光学标记 1 的起始和终止地址，可获得地址 n＋12 处的时钟 m＋14。由于 TD＝2，所以将时钟计数校正为 12，但为了便于说明，使用 n＋14。我们将描述另一种方法，该方法不必获取用于读取的再现设备中的参考延迟时间 TD，便可消除延迟时间变化的影响。该方法通过检查图 16（8）中地址 n 处的标记 1 相当于另一标记 2 的位置关系是否一致，来检查光盘是否是合法盘。即不把 TD 视作一个

变量，并获得所测标记 1 的位置 A1＝a1＋TD 与所测标记 2 的位置 A2=a2＋TD 之间的差，差值为 A1－A2=a1－a2。同时，检查该差值是否与解密标记 1 的位置 a1 和标记 2 的位置信息 a2 之间的差值 a1－a2 相一致，从而判定光盘是否是合法光盘。该方法的效果是，可以在补偿了参考延迟时间 TD 的变化之后，通过使用一较简单的结构检查各位置。

（D）接下来得描述加密信息的写入过程。如下一部分（2）中将要详细描述的那样，对过程（C）中读取的位置信息进行加密，并用条形码或其他方法将其写在光盘上。图 3 指出了该如何来做。在图 3（1）中，用脉冲式激光熔蚀反射层，并形成图 3（2）所示的条形码式的熔蚀图案。在再现设备（播放机）处获得图 3（3）所示的包络波形，其中有一些部分消失。这些消失的部分产生一与普通凹坑产生的信号不同的低电平信号，并且用第二限幅电平比较器对该信号限幅，以获得图 3（4）所示的低反射率部分检测信号。根据该低反射率部分检测信号，图 3（5）中的 PWM 解调器 621 对包含加密信息的信号进行解调。

以上描述了光盘制造过程中的各个处理步骤。下面将参照图 41，描述把如此完成的光盘放在播放机上再现的再现设备（播放机）的构造和工作情况。

首先将描述图中光盘 9102 的构造。在沉积于光盘 9102 上的反射层（未示出）上形成一标记 9103。在光盘的制造过程中，用位置检测装置检测标记 9103 的位置，并将检测到的位置加密成为标记位置信息，且用条形码 9104 的方式将信息写在光盘上。

位置信息读出装置 9101 读取条形码 9104，并且包括在其中的解密装置 9105 对条形码内容进行解密，用以输出。标记读出装置 9106 读取标记 9103 的实际位置，并输出结果。比较 / 判定装置 9107 将来自位置信息读出装置 9101 中的解密装置 9105 的解密结果与标记读出装置 9106 读出的结果进行比较，并判断两者是否在一预定的许可范围内一致。如果两者一致，则输出用于再现光盘的再现信号 9108；如果两者不一致，则输出再现停止信号 9109。控制装置（未示出）根据这些信号控制光盘的再现操作；当输出再现停止信号时，并将该光盘是非法复制盘的表示显示在显示器（未示出）上，并且停止再现操作。在上述操作中，可以

看到，当标记读出装置 9106 还可以在读取标记 9103 实际位置时使用来自解密装置 9105 的解密结果。

因此，上述构造的再现设备能检测非法复制的光盘并停止光盘再现，并且能实际防止非法复制品。

上述内容叙述了从光盘制造到播放机再现操作的过程，而下面我们将描述与上述过程的细节有关的事项。

（A）将说明一低反射率部分地址表，该表列出了低反射率部分的位置信息。

（a）在工厂的防盗版标记形成过程中激光标记是随机形成的。用这种方式形成的激光标记的物理特征都不相同。在下一过程步骤中，对于 DVD，用 0.13 微米的分辨率测量每个光盘上形成的低反射率部分 584，以构成图 13（a）中所示的低反射率部分地址表 609。这里，图 13（a）示出了依照本实施例制造的合法 CD 的低反射率部分地址表，而图 13（b）与非法复制的 CD 有关。用诸如图 18 所示的单向函数（one－direction function）对低反射率部分地址表 609 进行加密，并且在第二反射层形成步骤中，如图 2 所示，将清除了反射层的一系列低反射率部分 584c 至 584e 记录在光盘最里面部分上的条形码状图案中，另一种方法如图 14 所示，可将其记录在 CD－ROM 的磁记录部分 67 上。图 18 是一流程图，示出了用单向函数进行加密的光盘检查过程，而图 14 是光盘制造设备和特殊记录／再现设备的方框图。如图 13 所示，合法 CD 和非法复制的 CD 分别具有低反射率部分地址表 609 和 609x，它们相互有本质的不同。如前所述，造成这种差别的一个原因是无法使激光标记的物理特征相同。另一原因是，如果主盘不同，那么预先分配给光盘的扇区地址（sector address）会不同。

现参照图 13，我们将描述合法盘和盗版盘的标记位置信息是如何不同的。图示的例子综合了上述两个因素。在示例中，在一个光盘上形成两个标记。在合法 CD 中，如地址表 609 所示，标记号为 1 的第一标记位于从逻辑地址扇区 A1 的起始点开始的第 262 时钟位置。在 DVD 的情况下，一个时钟等于 0.13 微米，并用此精度进行测量。另一方面，对于盗版的 CD，如地址表 609x 所示，第一标记位于地址扇区 A2 的第 81 时

钟位置。通过检测合法盘和盗版盘第一标记位置之间的差，可分辨出盗版盘。同样，第二标记位置也是不同的。要使位置信息与合法盘的相符，必须用一个时钟单位即 0.13 微米的精度形成地址扇区 A1 中第 262 位置上的反射膜；否则，盗版盘便无法使用。

由此，如图 14 所示，在再现设备中，对加密表解密，以重新建立合法表，然后用检查程序 535 对其检查，将合法盘和非法复制盘区分开，并对复制盘停止其再现操作。在图 16 的例子中，合法盘和非法复制盘分别具有低反射率部分地址表 609 和 609x，如图 17 所示，它们的值是不同的。对于合法盘的情况，如图 16（8）所示，在标记 1 之后的光道中，起始和终止位置分别是 m＋14 和 m＋267，而对于非法复制盘的情况，如图 16（9）所示，它们分别是 m＋24 和 m＋277。因此，如图 17 所示，低反射率部分地址表 609 和 609x 中的相应值不同，从而能够分辨复制盘。如果合法制造商想复制具有低反射率部分地址表 609 的光盘，他们必须用图 16（8）所示的再现的时钟信号分辨率进行精确的激光溶蚀操作。对于 DVD 盘的情况，如图 27（5）所示，当把再现的时钟脉冲周期 T 转化为光盘上的某一距离时，它为 0.13 微米，因此，要进行非法复制，必须以 0.1 微米的亚微米分辨率来清除反射膜。以下情况是真实的，即当使用为光盘而设计的光头时，可用亚微米分辨率在诸如 CD－R 等记录膜上进行记录。但在这种情况下，再现的波形将如图 9（c）所示，并且不能获得图 9（a）所示的特征波形 824，除非将反射膜清除掉。

（b）通过清除反射膜来大量生产盗版盘的第一种方法是用诸如 YAG 激光器等高输出激光器进行激光熔蚀。在当前的技术状况下，即使是最高精度加工的激光熔蚀也只能获得数微米的处理精度。在用于半导体掩模校正的激光熔蚀中，据说 1 微米是处理精度的极限。这意味着，在大量生产的级别上，很难获得 0.1 微米的处理精度。

（c）目前所知的第二种方法是用于处理 VLSI 半导体掩模的 X 射线曝光设备和离子束处理设备，它们能获得亚微米量级的处理精度，但是这种设备非常昂贵，而且处理一张光盘要化很长的时间，并且如果用这种设备处理每一张盘，那么每张光盘的成本会很高，因此，目前该成本要比多数合法盘的零售价高，从而制造盗版盘就不会划算而且是无意义

的。

（d）如上所述，用包括激光熔蚀的第一种方法很难进行亚微米精度的处理，因此很难大量生产盗版盘。另一方面，利用诸如 X 射线曝光等亚微米处理技术的第二种方法。每张光盘的成本很高，以致从经济的角度看，制造盗版盘是无意义的。因此，可防止制造非法复制品，直至将来某一天可用成本低的亚微米处理技术进行大批量的生产。由于这种技术的实际实施将是将来许多年之后的事，所以可以防止生产盗版盘。如图 33 所示，对于在每层上形成一低反射率部分的双层光盘，不能制造非法复制盘，除非在层压时以良好的精度使顶片和底片上的凹抗对准，这在防止盗版方面提高了有效性。

（B）接下来，我们将描述如何规定低反射率部分在光盘上的角度安排。

在本发明中，是通过反射层级别的机械方式来提供防盗版中足够的有效性的，即只制作低反射率的标记。在这种情况下，即使主盘是复制品，防止也是有效的。然而，将其与主盘级别上的防盗版技术并用可提高有效性。如果如图 13（a）中表 532a 和表 609 所示规定低反射率部分在光盘上的角度安排，则非法制造商连每个凹坑在主盘上的角度安排也精确复制。这便会增加盗版盘的成本，并因此提高防止盗版的能力。

（C）以下将综述本发明的要点。在本发明中，合法制造商可以通过使用具有数十微米处理精度的一般用途的激光熔浊设备处理光盘，来制造合法盘。尽管需要 0.13 微米的测量精度，但用消费者 DVD 播放机中所包括的常规电路便能达到。通过用一保密的加密密钥对测得的结果进行加密，可以制造合法盘。也就是说，合法制造商只需要一保密密钥和一具有 0.13 微米测量精度的测量设备，同时所需的处理精度可低二或三个数量级，即为数十微米。这意味着，可以使用常规的激光处理设备。另一方面，没有保密密钥的非法制造商必须直接复制记录在合法盘上的加密信息。这意味着，必须用 0.13 微米的处理精度形成与加密位置信息对应的物理标记，即合法盘上的位置信息。也就是说，必须用处理精度比合法制造商所用处理设备的精度高两个数量级的处理设备形成低反射的标记。即使在可预见的将来，进行精度高出两个数量级即 0.1 微米精

度的大批量生产在技术和经济上都是很困难的。这意味着，在 DVD 标准的使用期中，可以防止生产盗版盘。本发明的一个重点是利用了这样一个事实，即测量精度一般要比处理精度高数个数量级。

对于 CLV 的情况，上述方法利用了这样一个事实、即如前所述，一个主盘的地址坐标安排与另一个的不同。图 19 示出了对实际 CD 上地址位置的测量结果。一般，有两种类型的主盘，一种（CAV）是通过以恒定转速即恒定的角速度旋转电动机来记录的，而另一种（CLV）是通过以恒定的线速度旋转光盘来记录的。对于 CAV 光盘的情况，由于逻辑位置位于光盘上某预定的角位置，所以无论制造多少主盘，光盘上的逻辑地址及其物理角位置是完全相同的。另一方面，对于 CLV 光盘的情况，由于只控制线速度，所以主盘上逻辑地址的角位置是随机的。从图 19 中实际的 CD 上逻辑地址位置的测量结果可知，即使用相同的制作主盘的设备来记录完全相同的数据，盘与盘之间的光道间距、起始点和线速度会略有不同，并且这些误差会累积，导致不同的物理位置。在图 19 中，白圆圈表示第一主盘上每个逻辑地址的位置，而黑圆圈和三角形分别表示第二和第三主盘上的位置。可见，每次制作主盘时逻辑地址的物理位置都会不同。图 17 示出了合法盘和非法复制盘的低反射率部分地址表，以作比较。

以上描述了在主盘级别上防止盗版的方法。这就是说，如图 19 所示，当用制作主盘的设备根据相同的逻辑数据制造诸如 CD 或 DVD 等 CLV 记录的主盘时，各主盘间即合法盘与盗版盘间，盘上每个凹坑的物理位置是不同的。该方法利用这一特点来识别盗版盘和合法盘。主盘级别上的防盗版技术可通过只从合法盘上的数据进行简单复制，便能在逻辑级别上防止盗版盘。但近年发现盗版制造商已具有更先进的技术，他们通过熔化合法盘的聚碳酸酯衬底来制造物理特征与合法盘相同的主盘复制品。在这种情况下，主盘级别上的防盗版方法宣告失败。为了防止这一新的生产盗版盘的迹象，本发明已在反射层级别上发明了防盗版的方法，在该方法中，在反射膜上形成标记。

根据本发明的方法，通过在反射膜形成过程中清除一部分反射膜要在由主盘压制的每一张盘上形成标记，即使这些盘是用同一张主盘压制

也如此。结果，各盘所获低反射标记的位置和形状相互不同。在通常的处理中，以亚微米的精度部分地除去反射膜是近于不可能的。由于复制本发明光盘的成本将证明是不合算的，因此可以提高防复制的有效性。

图 20 示出了用低反射率部分地址表检测被复制 CD 的流程图。由于所用再现设备的光头和电路设计，检测光学标记所需的延迟时间咯有变化。可在设计阶段或大批量生产时预测该电路延迟时间 TD。通过测量时钟数即从帧同步信号开始的时间，来获得光学标记位置信息。由于电路延迟时间的影响，所测的光学标记位置信息数据会产生误差。结果，会错误地将合法盘判定为盗版盘，给合法用户带来不便。以下将描述用于减少电路延迟时间 TD 的措施。另外，光盘出售后在盘上造成的擦痕会中断再现后的时钟信号，使光学标记位置信息的测量结果产生几个时钟的误差。为了解决这一问题，将容差 866 和合格计数 867 记录在光盘上，并且当根据再现时的实际情况允许测量值有一定程度的容差时，在到达合格计数 867 时允许进行再现操作；在装运光盘之前版权人可以控制因光盘上的表面擦痕而允许的误差范围。这将参照图 20 进行描述。

在图 20 中，在步骤 865a 中再现光盘，以从本发明的条形码记录部分或凹坑记录部分中恢复出加密的位置信息，在步骤 865b 进行解密或签名验证，并在步骤 865c，恢复光学标记位置信息的列表。接着，如果再现电路的延迟时间 TD 被存储在图 15 的再现设备中的电路延迟时间存储装置 608a 中，则在步骤 865h 读出 TD，过程进入步骤 865x。如果 TD 未被存储在再现设备中，或者如光盘上记录了测量指令，那么过程进入步骤 865d，进入参考延迟时间的测量过程。当检测到地址 Ns－1 时，便可找到下个地址 Ns 的起始位置。对帧同步信号和再现后的时钟进行计数，并在步骤 865f，对参考光学标记进行检测。在步骤 865g，测量并存储电路延迟时间 TD。该操作与以后将参照 16（7）描述的操作相同，在步骤 865x，测量位于地址 Nm 旁边的光学标记。在步骤 865i、865j、865k 和 865m 中，与步骤 865d、865y、865f 和 865g 相同，用一个时钟单位的分辨率检测光学标记位置信息。接着，在步骤 865n，进入盗版盘的检测过程。首先，校正电路延迟时间。在步骤 865p，读取图 27 所示的、记录在光盘上的容差 866，即 tA 和合格计数 867，以检查在步骤 865g 中测得

的位置信息是否落在容差 tA 的范围内。如果步骤 865r 中的结论是肯定的，则在步骤 865s 中检查被检查的标记计数是否已达到合格计数。如果结论为肯定的，则在步骤 865u 中将光盘判定为合法盘，并允许再现，如果还没有达到合格计数，则过程返回步骤 865z。如果在步骤 865r 中结论是否定的，则在步骤 865f 中检查误差检测计数是否小于 NA，并且只有当结论为肯定时，过程才返回步骤 865s。如果不是肯定的，则在步骤 865v 中将光盘判定为非法盘，并且停止操作。

如上所述，由于再现设备的电路延迟时间 TD 被存储在 IC ROM 中，所以可用增大的精度获得光学标记位置信息。另外，根据允许光盘出售后在盘上产生擦痕的实际情况，通过给每个盘上的软件设定容差 866 和合格计数，可改变盗版盘检测用的判定标准。这能降低把合法盘错判成非法盘的概率。

（D）以下将进一步描述关于读取两盘层压光盘非反射光学标记部分的工作情况。重点放在上述操作原理的描述中尚未涉及的部分。

也就是说，如图 16 所示，可用常规的播放机，以 1T 单位的分辨率即 DVD 标准下的 0.13 微米分辨率，精确地测量起始位置地址数、帧数和时钟数，从而精确地测量本发明的光学标记。图 27 和图 28 示出了适用于 DVD 标准的图 16 的光学标记地址读出方法。由于操作原理与图 16 所示的相同，所以此处不再对图 27 和 28 中的信号（1）、（2）、（3）、（4）和（5）加以说明。

以下将给出图 16 与图 27 和 28 之间的对应关系，其中图 16 说明了用于检测 CD 上低反射率部分位置的检测操作原理，而图 27 和 28 与 DVD 有关。

图 16（5）与图 27（1）和图 28（1）对应。图 16（6）中再现的时钟信号与图 27（5）和图 28（5）中所示的对应。图 16（7）中的地址 603 与图 27（2）和图 28（2）中所示的对应。

图 16（7）中的帧同步 604 与图 27（4）和图 28（4）所示的对应。图 16（8）中的起始时钟数 605a 与图 27（6）中再现的通道时钟数对应。在图 27（7）和图 28（7）中用 6 位的标记长度压缩数据，以代替图 16（7）中的终止时钟数 606。

如上所述，CD 和 DVD 的检测操作基本相同。第一个差别是，如图 27（7）中所示加入了的 1 比特的标记层识别符 603a 用来识别低反射率部分是单层类型的还是双层类型的。如前所述，双层的 DVD 结构具有更好的防盗版效果。第二个差别是，由于线记录密度几乎为两倍，所以 1T 的再现时钟与 0.13 微米一样短，这提高了检测位置信息的分辨率，并由此提供了更好的防盗版效果。

图 27 所示的是来自具有两层反射层的双层光盘中第一层的信号。信号示（1）出了检测到第一层上光学标记起始位置时的状态。图 28 示出了来自第二层的信号的状态。

为了读出第二层，图 15 中的第一 / 第二层切换装置 827 将一切换信号发送给聚焦控制装置 828，然后聚焦控制装置 828 控制聚焦驱动装置 829，将焦点从第一层切换至第二层。由图 27 可知，标记位于地址（n），并且用计数器对帧同步信号（4）进行计数，得知标记处于帧 4。从信号（5），可找到 PLL 再现的时钟数并且可获得信号（6）所示的光学标记位置数据。利用该位置数据，可在常规的消费者 DVD 播放机上以 0.13 微米的分辨率测量光学标记。

（E）以下将进一步描述与两盘层压的光盘有关的附加事项。

图 28 示出了与第二层上所形成的光学标记有关的地址位置信息。如图 7 中过程步骤（6）所示，激光通过同一孔穿透第一和第二层，第一反射层 802 上形成的非反射部分 815 和第二反射层 825 上形成的非反射部分 826 在形状上相同，图 33 的透视图对此作了描绘。在本发明中，当透明衬底 801 和第二衬底 803 被层压在一起后，使激光穿透到第二层，以在其上形成相同的标记。在这种情况下，由于第一和第二层上凹坑的坐标安排是不同的，并且由于当将它们层压在一起时，第一和第二层之间的位置关系是随机的，所以第一和第二层上形成标记的凹坑位置是不同的，并且从每层上会获得完全不同的位置信息。将这两种位置信息加密，以生产防盗版盘。如果企图非法复制该盘，则必须以大约 0.13 微米的分辨率使两层上的光学标记对准。如前所述，在目前的技术状况下，通过用 0.13 微米的精度即 0.1 微未量级的精度使具有凹坑的光学标记对准的方法来复制光盘是不可能的，但是将来有可能在商业上实现大批量生产

的技术，它能以低成本，用 0.1 微米的处理精度大量熔蚀单层的光盘。即使在上述情况下，由于对于双层层压盘 800 的情况，顶盘和底盘是同时熔蚀的，所以必须以数微米的精度使凹坑位置和光学标记对准，从而将两盘层压在一起。但是，由于聚碳酸酯衬底的温度系数等的影响，用该精度层压所述盘是近于不可能的。当通过施加激光使其透过双层光盘 800 来形成光学标记时，所得的防盗版标记很难复制。这大大提高了防盗版的效果。由此完成了具有防盗版机制的光盘。关于防盗版的用途，在诸如单板型等情况下，光盘制造过程和激光切割过程是不可分的，在这类场合中，作为激光切割过程之整体部分的加密过程和包含保密密钥的过程必须在光盘制造厂中进行。这意味着，对于单板型的情况，必须将软件公司保留的保密密钥交给光盘制造工厂。这大大降低了密码的机密性。另一方面，依照构成本发明一个方面的包括用激光处理层压盘的方法，可将激光熔蚀构成完全与光盘制造过程分离开来。由此，激光熔蚀和加密操作可在软件制造商的工厂中进行。由于软件制造商持有的保密密钥不必送交光盘制造商，所以加密用的保密密钥在软件制造商的安金保管之中。这大大地提高了加密的机密性。

（2）（A）在（1）中简要描述了对标记位置信息的加密（数字签名）和对光盘位置信息的解密和再现，现将作更详细的描述，（B）以下还将描述防盗版的各种机理。

（A）描述加密（数字签名）及其再现。

（a）简单加密（数字签名）

（使用 RSA 函数）

首先，参照图 22 和 24 所述的流程图，描述用信息恢复型签名方法的函数，譬如 RSA 函数等进行加密的一个例子。

如图 22 所示，过程包括以下主要程序：在步骤 735a，由光盘制造商测量标记位置信息；在步骤 695，对位置信息加密（或增加一数字签名）；在步骤 698，在再现识别中将位置信息解密（或者验证或认证签名）；并且在步骤 735w，进行检查，确定光盘是否为合法光盘。

首先，在步骤 735a 中，在步骤 735b，测量光盘上的标记位置信息。然后在步骤 735d，压缩位置信息，并在步骤 735e，获得压缩后的位置信

息 H。

在步骤 695 中，构成压缩位置信息 H 的密文。首先，在步骤 695g，设定 512 比特或 1024 比特的保密密钥 d 和 256 比特或 512 比特的保密密钥 p 和 q，并在步骤 695b，用 RSA 函数进行加密。当用 M 表示位置信息时，将 M 增大至 d 次幂，并且计算模 n，产生密文 C。在步骤 695d，将密文 C 记录在光盘上。由此完成光盘并（在步骤 735k）发货。

在再现设备中，在步骤 735m，装入光盘，并在步骤 698，将密文 C 解密。具体地说，在步骤 698e，恢复密文 C，并在步骤 698f，设定公开密钥 e 和 n；然后在步骤 698b 为了对密文 C 解密，将密文 C 增大至 e 次幂，并计算该结果的模 n，从而获得明文 M。明文 M 是压缩后的位置信息 H。可在步骤 698g 中进行差错检查。如果没有差错，则确定位置信息没有变化，并且过程行进至图 24 所示光盘检查程序 735w。如果检测到差错，则确定数据不合法，并且停止操作。

在下一步骤 736a，扩展被压缩的位置信息 H，以恢复原始的位置信息。在步骤 736c，进行测量，以检查标记是否实际位于位置信息所表示的光盘上的位置中。在步骤 736d，检查解密后的位置信息与实际测得的位置信息之间的差是否落在容差范围内。如果在步骤 736e 中检查是肯定的，那么过程行进至步骤 736b，输出软件或数据，或者执行存储在光盘中的程序。如果检查结果落在容差范围外，也就是说，如果两则位置信息不一致，那么显示该光盘是一非法复制盘的信息，并且在步骤 736g 停止操作。由于只需要记录密文，所以 RSA 具有减少所需容量的效果。

（使用椭圆函数）

接下来，参照图 23 和 24 所示的流程图，描述另一种类型的签名系统，即用椭圆函数进行加密的印码型（imprint type）签名系统。

如图 23 所示，过程包括以下主要程序：在步骤 735a，由光盘制造商测量标记位置信息；在步骤 735f，计算位置信息的认证密文（即签名）；在步骤 735n，在再现设备中进行位置信息的认证（签名验证）；并在步骤 735w，进行检查，以确定该光盘是否为合法光盘。

从步骤 735a 至步骤 735e 的过程与 RSA 函数的过程相同。

在步骤 735f，构建压缩位置信息 H 的认证密文。首先，在步骤 735g，

设定保密密钥 X（128 比特或更多）和 K，并在步骤 735h，确定一公开的系统参数 G，它是椭圆曲线上的点，并使用单向函数 f（x），首先获得 R＝f（K×G）、然后获得 R'＝f（R）；然后由方程 S=（K×R'－H）X_1 mod Q，生成 R 和 S，作为认证密文。在步骤 735j，将认证密文 R 和 S 以及压缩的位置信息的明文 H 记录在光盘上，并在步骤 735k，发运完成的光盘。

在再现设备中，在步骤 735，装入光盘，并在步骤 735n，进行认证操作，以认证位置信息。

首先，在步骤 735p，从装入的光盘中恢复出认证密文 R 和 S 以及压缩的位置信息 H。在步骤 735r，设定公开密钥 Y、G 和 Q，并在步骤 735s，进行认证操作，从而由 A=SR_1 mod Q 和 B=HR_1 mod Q 获得 f（A×Y＋B×G）。在步骤 735t，检测上述值是否与 R 一致。如果两种一致，则确定位置信息没有改变，并且过程行进至图 24 所示的光盘检查程序 735w。如果两种不一致，则确定数据不合法，并停止操作。

接下来从步骤 736a 至步骤 736g 的过程与 RSA 函数的过程相同。也就是说，如果光盘被判定为非法复制盘，则显示上述信息，并在步骤 736g，停止操作。与 RSA 函数相比，椭圆函数具有计算时间短的优点，它能缩短再现开始前的时间。因此，该系统适于消费者再现设备的应用。

（b）使用主密钥、副密钥的复杂加密（数字签名）

不仅标记位置信息，而且与存诸在光盘上的软件内容特征有关的信息。以及防盗版标识符都要进行加密（时间签名）。另外，使用两种保密密钥，即主密钥和副密钥，以下将描述一具体例子，在该例中，保密密钥加密函数与公开密钥加密函数联合使用。在对具体例子进详细描述之前，为便于理解该系统的基本部件，首先参照图 40 描述其基本功能。

在以下基本说明所论述的例子中，用一公开密钥加密函数进行加密，并且此处不处理用保密密钥加密函数进行加密的情况。因此，将用于公开密钥加密的主保密密钥和用于公开密钥加密的副保密密钥分别简称为主保密密钥和副保密密钥。同样，将用于公开密钥加密的主公开密钥和用于公开密钥加密的副公开密钥分别简称为主公开密钥和副公开密钥。

如图 40 所示，密钥管理中心 9001 严格管理主保密密钥，以保持其

机容性，并且通过通信线 9003 与软件制造商 9002 联接，下文将对此加以描述。当软件制造商 9002 请求加密时，为了加密，密钥管理中心通过网络 9003 接收数据，并用主保密密钥对数据加密。

为了便于说明，这里假设软件制造商 9002 也包括光盘制造厂家。因此，这里的软件制造商 9002 除了生产软件之外，还是在图 1 所示的光盘制造工厂中进行制造过程的一个部门。也就是说，当制造电影软件光盘时，还进行防止非法复制的加密。为了实现加密，软件制造商 9002 从密钥管理中心 9001 获得专用的副保密密钥。以上描述了光盘制造商一方的结构。

另一方面，在使用光盘的用户方有一播放机 9004。播放机 9004 是一台用于再现光盘的设备，它包括 ROM，ROM 中预先存有与密钥管理中心保留的主保密密钥相对应的主公开密钥。还具有停止非法复制光盘再现的功能。

描述了总体结构后，我们将描述工作情况。

（b－1）首先，将描述软件制造商 9002 进行加密的处理步骤。

首先进行的加密步骤（第一加密步骤）包括在压模盘制造阶段的加密，并且加密信息反映在压模盘的形状中。最终进行的加密步骤（第二加密步骤）是在用激光熔蚀形成标记之后的阶段进行加密。

（1－1）在第一加密步骤中，用一副公开密钥并用软件特征信息和防盗版标识符进行加密，所述副公开密钥与将在第二加密步骤中使用的副保密密钥对应。通过通信线 9003 将信息传送给密钥管理中心 9001。软件特征信息是指描述写于光盘上的电影软件内容的信息，并且它对每个电影软件是唯一的，软件之间相互不同。提供防盗版标识符可检测制造完成的光盘是否经过防盗版处理。使用第二密文进行光盘防盗版处理的光盘标识符为“1”；否则标识符为“0”。在该例子中，不用说，标识符为“1”。

（1－2）密钥管理中心 9001 用中心持有的主保密密钥对从软件制造商 9002 那里传送来信息进行加密，并且将加密后的信息送返给软件制造商 9002。由此产生的密文被称为第一密文。

（1－3）软件制造商 9002 将第一密文和电影软件一同记录在盘的模

具（或母版盘）上。

（1－4）软件制造商 9002 用如此完成的压模模压各盘。

（1－5）接着，软件制造商 9002 用模压好的盘制造光盘，并如前所述进行激光熔蚀，以在每张光盘上形成标记。

（1－6）接着，软件制造商 9002 标记位置并用制造商持有的副保密密钥对获得的位置信息进行加密。如此加密后的信息被称为第二密文。由于它是通过对位置信息加密而产生的，所以即使它们是用同一压模压制而成的，光盘的第二密文互不相同，这与第一密文的情况不同。

（1－7）最好，软件制造商 9002 将第二密文作为条形码记录在光盘上，从而完成了光盘。

（b－2）接下来，我们将描述当购买了如此完成的光盘的用户将其放在播放机 9004 上播放时的工作情况。

（2－1）首先，播放机 9004 读出记录在光盘上的第一密文，并用存储在 ROM 中的主公开密钥对第一密文解密，第一密文以加密的形式包含与副保密密钥对应的副公开密钥、软件特征信息和防盗版识别符。

（2－2）同时，播放机 9004 从记录在光盘上的电影软件内容中提取软件特征信息。将提取得到的软件特征信息与通过（2－1）中的解密获得的软件特征信息作比较；如果它们不一致，则该光盘被判定为非法复制盘，并停止后续的再现操作。如果，它们一致，则过程行进至下一步骤。

（2－3）检测在（2－1）中解密获得的防盗版标识符是否为“1”或“0”。如果它为“0”，则立即开始再现操作，跳过下文描述的过程。如果为“1”，则过程继续进行。

用这种方式，如果光盘恰是未用第二密文进行防盗版处理的盘，那么只要用合法的方法将其标识符设定为“0”，便能在播放机 9004 上再现光盘。如果盗版者企图把标识符改成“0”，以进行非法复制，那么由于如前所述，在将标识符与软件特征信息组合后用主保密密钥对其进行了加密，所以他的努力将遭挫折。

（2－4）首先，读出记录在光盘上的第二密文。然后，用（2－1）中解密获得的副公开密钥对第二密文解密，所述第二密文是位置信息的

加密形式。

（2－5）利用解密后的位置信息，检查标记是否真正形成在位置信息所表示的光盘的位置上。然后，将实际测得的标记位置信息与（2－4）中解密获得的位置信息进行比较。如果它们不一致，则该光盘被判定为非法复制盘，并停止再现操作。如果它们一致，则该光盘被判定为合法盘，并开始再现操作。

以上是对系统的概述。现将作更具体的描述。

如图 32 所示，软件特征提取装置 864 从软件内容中提取软件专用的软件参数，譬如表示视屏软件各章（chapter）的时间结构的 TOC 信息、压缩参数和标题名称等，并且通过计算检验和（checksum），在 Galois 域内计算以及利用诸如 SHA 和 MD5 等单向散列（hash）函数 864a，将提取到的信息压缩到 128 位至 256 位，以产生软件特征信息 863。然后，将软件特征信息 863 与软件制造商特有的副公开密钥 861 和作为版权标识符的防盗版标识符 865 组合，形成一个数据块，然后在步骤 866a 和 866b，用对公开密钥加密的主保密密钥对该数据块加密，并在步骤 866e，将其与软件正文一起记录在主盘 867 上。

当使用的系统将保密密钥加密与公开密钥加密联合使用时，在步骤 866c，使用用于保密密钥加密的主密钥，并在步骤 866d 进行加密，而且在步骤 866e，将数据记录在主盘 867 上。

由此完成了主盘的制作过程。记录在主盘上防盗版标识符 865 规定了如何保护软件的版权，标识符至少包括 4 个版权保护标志位，其中一个标志位表示软件是否具有防盗版的机制，一个标志位表示它是否具有低反射率的条形码播放，一个标志位作为擦痕标识符 965a，表示软件是否被擦伤，而另一个标志位表示是否防止软件翻录（dubbing）。由于防盗版标识符 865 和副公开密钥 861 与软件专用的软件特征信息组合在一起，并且用用于公开密钥加密的主保密密钥将其一起加密，所以不可能改变它们。

将防盗版标识符 865 和副公开密钥 861 与软件专用的软件特征信息组合，形成一数据块，然后用保密密钥对其加密。

如果软件特征信息 863 包括 256 比特，那么就有 2^{256} 种变化。这意

味着，当从通过创作某特定电影软件产品所获得的数据中提取软件特征信息时，它与其他软件的软件特征信息相吻合的概率为 $1 / 2^{256}$；因此，发生这种吻合的概率几乎为零，当使用诸如 MD5 或 SHA 等单向散列函数时，如果散列值即软件特征信息 963 包括 256 位，那么用目前已有的大型计算机寻找两段具有相同散列值的软件内容将需要 1018 年的计算时间，结果，几乎不可能替换软件。对于被创作的某特定软件产品的软件特征信息，只存在一个值，并且其他软件不具有相同的值。

由于将软件特征信息同防盗版标识符 865 和副公开密钥 861 一起加密，所以这两个值中没有一个能够更换，因此，创作完成后，特定软件产品的防盗版标识符 865 和副公开密钥 861 是唯一标识的。

将进一步详细描述将防盗版标识符 865 记录在主盘上的过程。

如何将防盗版标识符 865 真正添加到软件上是由软件版权人决定的。为光盘软件施加防盗版的措施需要花费资金和劳力。因此，不是所有的光盘都具有防盗版的机制；一些光盘包含本发明的防盗版机制或条形码，但其他的则没有。如果允许无防盗版机制或条形码的合法盘存在，则要求再现设备具有使两种都能适当再现的功能。在这种情况下，当再现不防盗版的光盘时，必须考虑两种可能：一种可能是，光盘是一合法盘，软件公司已用合法的方式对其解除了盗版保护，另一种可能是，软件公司原先对光盘加有盗版保护，但盗版者非法更换了防盗版标识符。

因此，用于识别防盗版标识符是否合法的装置是很重要的。

在本发明中，用保密密钥对包括防盗版标识符的防盗版标识符 865 连同软件特征信息一起加密，将其记录在主盘上的密文记录部分中。再现识别用先前描述的公开密钥对密文解密。这防止了对任何一种数据的非法变更。

盗版者唯一可行的方法只剩下用另一部分替换第一密文的整个部分，该部分包含软件特征信息 863 和防盗版标识符 865。

为了区别软件特征信息 863 和从真正写在光盘上的电影软件中提取出来的软件特征信息（将在以后描述），有时将前者称为第一软件特征信息，而将后者称为第二软件特征信息。两种信息的相同之处在于，它们都涉及同一电影软件的内容，但不同之处在于，前者是在制造光盘上以

加密的形式写入的，而后者是在再现时通过检查实际记录的电影软件的内容而提取得到的。

由于第一软件信息 863 的值是已完成创作的软件所专有的，所以如前所述，其他软件获得相同值的概率为 $1/2^{256}$，即近似为零。如果替换第一软件信息 863，则信息不再会与从光盘实际提取的第二软件特征信息 885 相同，第二软件特征信息 885 的提取可参见图 38 中通过步骤 876a、876c、876e 和 876f 进行的检查程序中的步骤 876e。这使具有变更信息的光盘不能播放。用这种方式，可保护软件的防盗版标识符 865 和下文将作描述的副公开密钥不被非法更换。因此，想通过对合法盘复制软件来制造非法盘的非法制造商会想到制造那些既没有防盗版标识符也没有条形码的光盘。在这种情况下，必须将防盗版标识符 865 中的防盗版标识符从开（“1”）设置转变为关（“0”）设置。但是，为了改变设置，必须使密钥管理中心用图 36 中步骤 866a 所示的主保密密钥发出第一密文，但一般有措施可防止密钥管理中心将其发送给未被许可的人，从而防止了对防盗版识别符 865 的非法变更。

这就是说，将第一软件特征信息 863 和防盗版标识符 865 一起加密成第一密文 886，以便记录在主盘上。这能有效地制止盗版者以没有防盗版标记或机制的不防盗版的光盘格式对受盗版保护的软件进行非法复制的任何企图。用这一构成本发明一个方面的方法，如果制定了盘的标准，允许没有盗版保护的光盘与有盗版保护的光盘共存，如果新的标准代替了该标准，则新一代的再现设备能对所有的光盘防止盗版。这是一个很大的实用的优点。另外，在上述实施例中，作为保护版权标志（标识符）的例子，已描述了使用防盗版标识符 865 的例子，其中防盗版标识符表示软件内容是否为防盗版软件。除了上述实施例外，通过使用表示软件内容是否为防复制软件的防复制标识符，可以保护具有防复制软件的光盘在消除了防复制标识符的情况下不被出售。

以下将详细描述在公开密钥加密的保密密钥中主保密密钥和副保密密钥的必要性，和这些保密密钥的结构和功能。

在本发明的防盗版方法中，由于进行二次记录，所以不必将保密密钥送给光盘制造厂。但是，由一个加密中心为全世界每张生产出的光盘

产生密文并且通过网络接收密文是不现实的，因为这会使通信业务量大幅度增长。另一方面，从保密的角度看，将保密密钥分配给每个软件制造商和光盘制造厂是不可能的。因此，需要一个能解决这一问题的方法。

作为克服上述问题的方法，本发明提供了主密钥／副密钥系统，依照本发明，密钥管理中心（密钥发放中心）保管不对外公开的主保密密钥。另一方面，软件公司保管副保密密钥，公司负责用副保密密钥保持其软件的机密性。如已参照图 32 所描述的，用主保密密钥将软件特征信息和软件公司保管的副公开密钥一同加密，形成第一密文。再现设备用主公开密钥将第一密文解密，并从解密后的文本中提取副公开密钥。这防止了对副公开密钥的非法变更，对第二密文（即标记位置信息的加密形式）的解密是必要的。

这意味着，只能用特定的保密密钥对特定的软件产品加密，也就是用软件制造商拥有的对应于副公开密钥的保密密钥。软件制造商可用副保密密钥随意对加锁或未加锁的软件上设置密钥。

因此，这意味着，盗版者不能生产盗版盘，除非他们从软件制造商那里窃取了软件专用的副保密密钥信息。

在图 32 中，软件制造商将光盘的物理位置信息 868 和光盘 ID869 组合，先在步骤 866f 用副保密密钥 876 将它们一起加密、以构成按条形码形式记录在光盘 800 上的公开密钥密码 859。这使得软件制造商不必非有主保密密钥 866a 才能生产防盗版的光盘，其效果是保护了主保密密钥的机密性。如果副保密密钥被盗，并制造了盗版盘，则损失仅局限于被发给该副保密密钥的软件。当软件制造商发放新的副保密密钥和新的公开密钥时，便可防止此后软件盗版盘的生产，图 36 和图 37 是表示数据流程的一般系统图。

在操作方面，图 36 与图 32 相同，并将在此不作详细说明，在图 36 中，软件公司 871a 首先设定它自己的副保密密钥 876，并计算副公开密钥 861。将副公开密钥 861 与将被记录的软件的软件特征信息 861 组合，并通过诸如 Internet 之类的网络发送给密钥发放中心 872。密钥发放中心 872 用主保密密钥 866a 对组合后的信号加密，并把加密后的主公开密钥 858 发送回软件公司。软件公司将其与软件组合，并将组合后的信号发

送给光盘制造厂 873，在制造厂 873，把信号记录在生产盘 800 的主盘上，接下来参考图 37，软件公司 871b 在盘 800 上形成一标记，读出标记位置信息，用对应于副公开密钥的副加密密钥 876 对位置信息进行加密，并且用脉冲式激光器 813 将加密后的信息按条形码形式记录在盘 800b 上。已详细描述了记录的操作情况，这里不再重复。

接下来，将参照图 38 进一步详细地描述当再现如此完成的光盘时，再现设备中防盗版操作的过程。

操作基本上包括软件检查步骤 874 和光盘检查步骤 875。在软件检查步骤 874 中，首先在步骤 876a，从光盘 800 中再现出第一密文，然后在步骤 876b，用步骤 876c 中存储在再现设备 ROM 中的主公开密钥，将第一密文解密成为明文。在步骤 876d，获得第一软件特征信息 863 的明文和副公开密钥 861，并在步骤 876f，检查用单向散列函数提取的第二软件特征信息。如果在步骤 876g，检查结果为否定，则停止操作；如果检查结果为肯定，则在步骤 876h 输出副公开密钥，如果盗版者更换了副公开密钥或软件特征，则两种信息会不一致，从而防止了对非法盘的再现。由此，在再现设备处获得了合法的副公开密钥。

在光盘检查步骤 875 中，在步骤 876k 输入副公开密钥，并在步骤 876m 再现第二密文即公开密钥密码 859（见图 32）。在步骤 876n，用副公开密钥将第二密文解密成明文，并在步骤 876p 获取标记位置信息。在这种情况下，不能非法变更标记位置信息，除非泄露了与副公开密钥对应的副保密密钥 876（见图 32）。在步骤 876p，读出由激光实际在光盘上形成的标记位置，并在步骤 876r 检查该位置。如果在步骤 876s 检查结果为否定，则在步骤 876t 停止操作，产生“盗版盘”的显示，如果检查结果为肯定，则在步骤 876u 允许再现操作继续。

利用上述构造，在再现设备上不能再现非法复制的光盘，除非软件制造商持有的副保密密钥被盗，或者以亚微米的精度，例如 0.13 微米激光熔蚀了无反射标记部分，并以数微米量级的精度将两盘层压在一起。这使得实际上不可能制造盗版盘。它具有防止光盘盗版的效果。

（c）以下将详细描述一例将公开密钥加密函数与保密密钥加密函数联用的情况。

本发明加密系统的第一特征是在对每张光盘上的标记位置信息进行加密时，使用两种加密函数，公开密钥加密函数和保密密钥加密函数。以下论述的是当实际实施使用公开密钥密码的防盗版方法时所遇到的问题，以及方法的实施。这里的公开密钥密码是指用公开密钥加密函数加密的位置信息（例如 RSA 函数）

从保密的角度看，希望所有的再现设备都装有公开密钥密码解码器，以对本发明的防盗版公开密钥密码进行解码。但是，用 32 位 50 兆赫兹的 CPU 处理 512 位的公开密钥密码需要 0.3 秒。另一方面，当今消费者设备中的 DVD 播放机控制 IC 主要是 8 位的单片微机。用这种 CPU 处理公开密钥，所化时间将大于数分钟。这意味着，在 DVD 再现出图像之前，用户必须等待数分钟，这在消费品中使用公开密钥密码系统方面提出了一个问题。

由于，在目前的水平，还不能用消费品中使用的 CPU 来处理公开密钥密码，所以目前没有其他选择，消费者再现设备只能使用保密密钥密码解码器，因为所需的处理时间少。但是，对于保密密钥密码，由于从密码解码器信息中很容易解出保密密钥，所以保密密钥密码一旦被解密，则将失去其防盗版的效果。因此将来，转化成难以解密的公开密钥密码是绝对必要的。

保密密钥密码和公开密钥密码是相互不兼容的。如果将来简单地把系统从保密密钥密码切换至公开密钥密码，则将不能对具有公开密钥密码第二代光盘进行解码，并在具有保密密钥密码解码器的第一代播放机上再现。另外，具有保密密钥密码的第一代光盘将不能在未来的播放机上再现。如果本发明的构造允许这类光盘再现，那么将允许盗版者对保密密钥密码的保密密钥解密，并用解密后的密钥产生保密密钥密码，从而引发在市场上出现大量盗版盘的可能，如果允许用保密密钥加密的光盘在将来的播放机上再现，那么即使使用公开密钥密码也不能防止盗版。

因此，需要一种机制，如果将来把再现设备的密码解码器从保密密钥变换为公开密钥系统，它能保持兼容，以允许早先的光盘在具有新的公开密钥密码解码器的再现设备上适当再现，同时防止盗版盘的再现。

以下揭示本发明的满足这种兼容需求的方法。如图 39 所示，本发明

的光盘具有保密密钥密码记录部分 879 和公开密钥密文记录部分 880 两者。制造方法将在后文中参照图 29 描述。首先，当把图 39 的光盘放在装有保密密钥密码解码器 881 的第一代再现设备上再现时，从盘上的保密密钥密码记录部分 879 中读出合法盘专用的第一物理特征信息（对应于位置信息的加密形式），并用保密密钥加密解码器 881 将其解密成明文。另外，测量光盘的第二物理特征信息（对应于测得的位置信息），并比较两种物理信息。

对于合法盘的情况，如步骤 878a 所示，由于两种物理特征信息一致，所以通常可以再现光盘。

对于盗版盘的情况，如步骤 878c 所示，由于它们不一致，所以防止了光盘的再现。也就是说，只要保密密钥密码不被破坏，就能防止再现。如果盗版者在未来的某时破坏了密码，则如前所述，盗版者能通过非法产生保密密钥密码而大量生产非法盘。

在上述情况下，如步骤 878d 所示，由于第一代再现设备中的保密密钥解码器 881 只检查保密密钥密码，所以会通过比较检查，从而允许再现非法盗版盘，但是，在将来，具有公开密钥密码解码器 882 的第二代再现设备已成为主要类型；因此以非法方式在第一代再现设备上再现盗版盘将不会有重大的冲击。

如步骤 878b 所示，由于本发明的合法盘具有公开密钥密码，所以通常可第二代再现设备上再现光盘。另一方面，如步骤 878e 所示，当插入盗版盘进行再现时，无论保密密钥密码是否被解密，再现设备都只检查公开密钥密码。结果，如步骤 878e 所示，公开密钥密码的防盗版功能起作用，从而几乎完全防止了盗版盘在第二代再现设备上再现。

依照本发明，从第一代再现设备进入商界起，就用预先写上的保密密钥密码 879 和公开密钥密码 880 制造所有的光盘。因此，在第一阶段，由于能用装在第一代再现设备中的 8 位微机处理密文，所以提供了保密密钥密码等级上的防盗版，在第二阶段，即将来当保密密钥密码被破坏时，那时已成主要类型的第二代设备中所包括的公开密钥密码解码器可更成熟地防止盗版。通过这种方式，如果一代被下一代替代，则可继续保持与旱先媒体的良好兼容，第二代再现设备几乎将彻底地防止盗版。

以上描述了一例低反射率标记方法的应用，即反射层等级上的防盗版方法。但是，希望在应用主盘等级上的防盗版方法时，同样也能在换代时保持兼容，其中如图 13 所示，主盘等级上的防盗版方法使用主盘的物特征信息。

上例具有这样的特点，即当进行加密时，用公开密钥加密函数和保密密钥加密函数对同一信息分开加密，并且分别将信息的加密形式记录在光盘上。

因此，当将来从现用的播放机向未来的播放机过渡时，可在任何一种类型的播放机上有效地使用上例中描述的光盘，其中现用的播放机具有解码器，基于 8 位的微机，它用保密密钥加密函数对产生的密文解码，而未来的播放机具有解码器，基于 32 位微机，它用公开密钥解码函数对产生的密文解码。

（B）以下将描述其他机制。

（a）我们将描述另一个具体的公开密钥 / 保密密钥组合型的例子，在该例中，对软件特征信息、ID 数码和标记位置信息进行加密（参见图 29）。ID 数码是指分配给每个盘的数码，用以识别光盘，下文将描述的光盘 ID（也称为光盘 ID 数码），其含义与 ID 数码相同。本例与上例的主要区别在于（参见图 32、36 和 37）：（1）在上文具体的例子中，软件特征信息作为第一密文写在主盘上的，而标记位置信息作为第二密文写在被压制的盘上，但是在本例中，将软件特征信息、ID 数码和标记位置信息全都组合在一起加密，并且将加密后的文本写在早已压制好的盘上；（2）在上例中，用主保密密钥和副保密密钥进行两个阶段的加密操作，但在本例中，只用主保密密钥而不用与副保密密钥对应的密钥进行为加密。

具体地说，如图 29 所示，在保密密钥加密装置 832 中用保密密钥加密用的保密密钥 834 对上述组合的信号偏码。还在公开密钥加密装置 831 中用公开密钥加密用的保密密钥 833 对同一组合的信号编码。通过这种方式，联合使用公开密钥密码和保密密钥密码。这克服了这样的问题，即由于现用再现设备的微机处理速度慢，所以它只能对保密密钥密码解码。未来的再现设备将使用速度较快的微机，例如 32 位结构的微机，并

通过只对具有较高安全度公开密钥密码解码来进行盗版检查；因此，几乎能彻底防止盗版。如果将来某时，保密密钥密码被破坏，则由于那时公开密钥类型的播放机将是主要类型，所以能基本防止盗版。如果发生从现用播放机向下一代播放机的过渡，那么通过把公开密钥密码和保密密钥密码同时记录在媒体上，可在老一代的再现设备上再现该媒体，同时基本上防止了盗版。

（b）接下来，将参照同一附图详细描述条形码的调制记录方法。

在图 29 中，用条形码记录设备（PWM 记录设备）845 将加密后的信息写在光盘上。

首先，用光学标记位置检测装置 600 检测在反射层 802 或在第二反射层 825 上形成的有关非反射部分 815 的位置信息。检测方法已参照图 15 作了描述，因此这里不再重复。用组合装置 835 将光学标记位置信息、软件特征信息和 ID 发生器 546 产生的 ID 数码组合。通过用诸如 SHA 等单向散列函数从一部分软件内容中提取特征，和通过获取 128 比特或 160 比特的散列值，来获取软件特征信息。ID 数码发生器 546 已参照图 14 描述过了，因此这里不再重说明，在加密装置 830 中，在公开密钥加密装置 831，譬如 RSA 中，用公开密钥加密用的保密密钥 833 对物理特征信息的组合信号编码。

在组合装置 835 中组合上述公开密钥密码和保密密钥密码，并在记录电路 836 的误差校正编码器 837 中，用里德一索罗门（Reed-Solomon）编码器 838 和交织器 839 对其进行交织 / Reed-Solomon 纠错。如此设定该情形下的交织长度，以便能够校正因 2.38 毫米或更长的光盘擦痕（与 CD 同一等级）引起的突发差错，从而产生这样的效果，即针对消费者使用情况最差的条件下引起的光盘擦痕，为本发明中条形码记录的数据中的差错提供纠错。

以下将参照同一附图描述脉冲宽度调制方法的原理。该方法不需要用主保密密钥产生第一密文，用副保密密钥产生第二密文。在该方法中，将软件特征信息、位置信息和 ID 数码组合在一起进行加密。每年生产亿万张 ROM 光盘。因此，很可能碰巧产生出一张其标记位置图案很容易复制的光盘。通过使用该容易复制标记位置信息和该位置信息的合法密

文的组合信息，可生产盗版盘。在图 29 中，将位置信息与软件特征信息组合，以进行加密或用签名进行认证。由此，位置信息与软件特征信息不可分离。这意味着，如果碰巧生产了容易复制的标记，那么只可能生产具有相应软件内容的盗版盘，从而大大限制了潜在的损失。这里应当认识到，可将该密文记录在主盘上。

用脉冲间隔调制器 840 将经误差校正编码的信号调制成 PWM 信号。当用激光器描线时，很难通过对线宽的精确控制来构成条形码。因此，在本发明中，如图 30 所示，将脉冲间隔分为四个值：1T、2T、3T 和 4T，并且例如通过将标记 843b、843c、843d 和 843e 编码为 00、01、10 和 11，用一条条形码发送 2 比特数据。如图 30 中表示线宽和记录速率之间关系的表 842 所示，当用 10 微米的线宽将 PIM 条形码记录在 ROM 光盘 800 的引入区（lead-in）中时，可以看到，可在一圈内在完成的光盘上附加写上 5.6kbits 的信息。

图 31 的部分（1）示出了非反射部分的检测信号。

信号具有一同步信号区 858，该区由三个脉冲 857a、857b 和 857c 组成，间隔为 T；该区表示起始位置。接着是 4T 的空白，它是用于测量参考时间 T 的参考时间区。当线宽为 10 微米时，T＝20 微米。接着是用于保持二次记录数据的大约为 1k 比特的第一记录区 860。然后在 100 微米或更长的空白 861a 之后是用于第三次记录数据的第二记录区 862a。由制造商记录解扰用的口令。

（c）以下描述能通过使用 HMST 方法进行第二次和第三次记录的条形码使用方法。

如图 35 所示，在过程（2）中，软件制造商生产具有专用 ID 数码的盘 844b，并记录与用户秘密通信用的私人密钥。不需要任何特殊的过程就能再现光盘 844c 和 844d。

如以下将要描述的图 21 所示，可以用 PWM（PIM）调制／解调激光器代替磁记录／再现电路中的 MFM 调制／解调磁头，来构成实施本发明 HMST 方法的记录／再现电路。

（d）图 35 示出了另一个制造光盘的具体例子。在表示光盘另一种应用的图 35 过程（3）中，将经扰码的 MPEG 视频信号的信息或类似信

息记录在光盘 844e。以下将对 MPEG 扰码操作作简要描述。MPEG 的视屏压缩信号在 AC 分量的长度可变的编码器和长度固定的编码器之间分开，每个编码器包括一随机数加法器，用于扰码。在本发明中，加密编码器用单向函数对解扰信号进行加密。另外，加密编码器对图像压缩控制器中的压缩程序部分进行压缩。这使复制公司很难用非法的产品替换加密编码器。因此，副公开密钥只对合法盘解密。

再参照图 35，接下来我们将描述如何在下一过程（4）和以后的过程中处理上述过程（3）中制造的光盘 844e。

在图 35 的过程（4）中，软件公司用主保密密钥对光盘 ID 数码和用于对解扰信号进行解码的副公开密钥进行加密，并将加密的文本通过条形码二次记录在光盘上，从而完成光盘 844f。由于光盘 844f 被扰码，所以不能接原样再现光盘。这里所述光盘 ID 数码的含义与上述 ID 数码的含义相同。在过程（5）中，销售商从消费者那里收到光盘的钱后，用使用对应于副公开密钥的副保密密钥的光盘 ID 数码产生口令，并第三次将口令记录在光盘上。一旦记录了口令，则通过对数据解扰可在再现设备上再现光盘 844g。对于计算机程序，可安装程序。利用这种方法，如果有人行窃光盘，那么由于图像扰码和密文未被解开，所以不能再现光盘上的图像或软件。这就打击了行窃者的努力，从而获得防止行窃的效果。

（e）现在我们中断对图 35 的说明，而回头参考图 21，以描述再现设备的操作和构造，如图所示，再现设备包括集中体现为磁记录和再现电路的记录电路，它与一光学再现设备组合，构成一个记录 / 再现电路，在图 21 中，示出和再现电路与光学再现设备的组合，但也可用普通光学再现设备与软盘的组合来代替。

在该图中，磁再现电路含有两个解调器，MFM 解调器 30d 和第二解调器 662，其中第二解调器是 MFM 的另一种类型，由选择器 661 选择使用哪个解调器。相应的调制器只由工厂保管，致使尽管有可能再现，但没有提供完整的记录能力。因此，当在工厂记录了特殊调制的区域时，没有记录特殊调制的信号。驱动方的 CPU 665 进行控制，致使不能进行记录，除非从该区域中再现出特殊调制的信号。因此可以认为，该区域是逻辑的只写一次的区域，只允许记录一次。因此，一旦在光盘或软盘

上磁记录部分的这个只写一次区域中记录了机器 ID，例如记录在再现设备中 ROM 699 中的诸如驱动器 ID 699a，那么用户驱动器就不能改变被记录的内容，从而防止在超过被允许的机器数量的机器上非法安装。这里驱动器 ID 是分配给每个再现设备的一个数码，用于识别该设备。机器 ID 可以是分配给个人计算机的 ID。网络接口装置 14 检查接至网络 664 的第二台个人计算机上的 HDD，并监督操作情况，以便不起动或运作同一驱动器 ID 或同一机器 ID 的程序，从而防止了非法复制软件的使用。

本发明的激光标记记录方法同磁记录方法一样，允许进行二次记录，譬如销售商记录销售代码。但这并不构成本发明的一个特征，因此这里将不作详细说明。

对于影像产品出租店，如果将口令永久记录在光盘上，并且如果该光盘被盗，那么窃贼便能播放该光盘。为防止这点，如过程（6）所示，影像产品出租店交给租借者一张扰码盘 844j。在步骤 851g，用副保密密钥从下文将作描述的光盘 ID 或驱动器 ID 中计算出解扰用的口令。在步骤 851j，将口令印在交给用户的收据上，如步骤 851u 所示，也可用电话通知用户该口令。

如步骤 851r 所示，用户在家中在其再现设备上进行解码再现，首先，在步骤 851s，用副公开密钥对密文解码，解出扰码标识符（scramble identifier）和软件特征信息，将解密获得的软件特征信息与用单向散列函数从软件内容中实际提取的软件特征信息比较，验证它们是否一致，如果不能作出证实，则把光盘认定为非法光盘，并停止再现。如果在步骤 851x，扰码标识符为“关”，则允许在步骤 851p 中进行再现操作。如果编码标识符为“开”，则用户在步骤 851k，通过数字键盘输入口令，并用副公开密钥计算口令。在步骤 851t，用光盘 ID 和 / 驱动器 ID 作进一步的计算，并只有当口令计算结果与光盘 ID 或驱动器 ID 一致时，才打开扰码或密文，准许再现或操作预先说定的天数，当租给用户光盘时，所给的口令只能使用一部分软件，这时如果用户希望列览软件的其他内容，他可以用电话请求密钥发放中心发给所需软件内容的口令；随后在步骤 851u 将口令通知用户，并在步骤 851 输入口令，使光盘上所需的软件再现。

现将参照图 34 进一步详细地描述在图 35 的过程（5）和（6）中由影像产品零售店或影像产品出租店所进行的操作。影像产品零售店收到扰码或加密的盘 844f，并在用户付款后，通过 POS 终端 846 将光盘 844f 的光盘 ID 数码和副公开密钥数据从条形码记录 / 再现设备 845 发送到口令发放中心 852。对于一个小规模的店铺系统，口令发放中心（即包括副公开密钥之副保密密钥的系统）可以包括在 POS 终端中。在步骤 851q，口令发放中心输入光盘 ID 数码和时间信息，在步骤 851s 进行计算，在步骤 851t 用副保密密钥进行加密，并在步骤 851g 发出口令。然后，如果网络 848 和 POS 终端将口令发送给条形码记录设备 845，并将记录有口令的光盘 844g 交给客户。该光盘便能接原样再现。

接下来，将详细描述出租店进行的操作。首先，将通过扰码锁定的 ROM 盘 844f 陈列在货架上。当客户指定特殊的 ROM 盘 844f 时，店员手持一个圆形的条形码阅读器 850，该阅读器装有一个能产生螺旋扫描图案的旋转型光头 853，并且店员将阅读器压在容纳于透明盒中的光盘 800 的中心，以读出由光盘 844f 中反射层上非反射部分 815 形成的条形码，从而读出光盘 ID 数码。产品代码可以从本发明中由非反射部分 815 形成的条形码读出，也可以从用现有的记录方法预先记录或压制在主盘凹坑记录区内侧内环部分上的圆形条形码读出。用 POS 终端 846 处理这些信息项，并结算租借费用；同时，如前所述，在步骤 851g，发出与光盘 ID 数码对应的口令。对于出租的情况，如步骤 851r 中所做的，要将限制视听天数的时间信息加到光盘 ID 数码中，用以加密，并由此产生口令。在预先设定的天数里该口令有效，其效果是，例如可在口令中设定某租赁盘的租赁期为 3 天。

在步骤 851i，将如此发行的用于打开扰码的口令、租赁时期、希望归还的日期和名称的租赁费用印在连同光盘一起交给客户的收据 849 上。用户将光盘 844j 和收据 849 拿回家。当在步骤 851k，用图 25 所示信息处理设备 676 上的诸如数字键盘等输入装置 854 输入口令时，用光盘 ID 数码计算口令，并将其输入到主密码解码器 534，在主密码解码器 534 处，用公开密钥将加密的数据解码成为明文。在明文数据检查装置 715 中检查该明文，确定它是否满足预定的条件；只有当口令正确时，才用

副密码解码器 718 对程序数据解扰，并输出视频图像。

在这种情况下，如果口令包含数据信息，则检查来自时钟装置 855 的日期数据，并且只要日期数据与数据信息相符就允许进行解扰。持口令及其对应的 ID 数码存储在存储器 755 的固定存储器 755a 中。一旦输入了口令，用户就不必再输入它来进行解扰操作。用这种方式，可用电子装置开闭光盘上的密钥，这为商业销售带来好处。

以上主要借助将光盘 ID 加至光盘的光盘 ID 方法描述了上述实施例。但是，对于没有光盘 ID 的光盘，就有必要使用驱动器的驱动器 ID。以下的描述详细论述了当只用驱动器 ID 和当驱动器 ID 和光盘 ID 都使用时的解扰操作，口令产生和检查操作。

在图 35 中，当用与驱动器 ID 相关的口令对软件解扰时，用电话或通过个人计算机的通信将存储在再现设备的 ROM 中的驱动器 ID 699a 从图 34 中的信号装置 851z 发送至口令发放中心。在口令发放中心，在步骤 851q，使用驱动器 ID 和软件 ID，在步骤 851s 进行计算，并在步骤 851t，用副保密密钥对结果加密，从而在步骤 851g 产生口令。在步骤 851u，用电话或通过个人计算机通信将口令发送给包括用户个人计算机的再现设备中的通信装置 85z。在步骤 851k，用户输入口令，并在步骤 851m，用副公开密钥进行解密计算。在步骤 851t，将驱动器 ID 与计算结果作比较，如果它们不一致，则通知操作。如果它们一致，则在步骤 851p，进行再现或操作。

以下将描述驱动器 ID 方法和光盘 ID 方法的优点和缺点。当使用光盘 ID 时，口令只对一个特定的光盘有效。该光盘可以在任何驱动器上运行。因此，该方法适用于电影软件和类似软件。但是，对于个人计算机用的商业软件，如果软件可以在任何驱动器上安装，那么光盘上的软件就可以被非法复制到不止一个计算机上。

对于电影软件，光盘只能在一个驱动器上运行是驱动器 ID 方法的一个缺点。但是，对于个人计算机软件，这却是个优点。对于只需要安装一次的商业软件，驱动器 ID 方法的好处在于，其口令保护的解锁特征防止软件通过使用其他非指定驱动器被非法安装在个人计算机上。

但是，驱动器 ID 被写在机器的 EPROM 中，并且容易被变更，如果

具有相同驱动器 ID 的驱动器被出售，那么就可以在许多机器上进行非法安装。另一方面，如已经所述的，很难变更本发明的光盘 ID。在图 34 中，如果准备在步骤 851q 产生关于光盘 ID 和驱动器 ID 两者的口令，并在步骤 851t 中检查两种 ID，则可防止光盘 ID 的变更。所得的效果是，如果大量销售驱动器 ID 相同的驱动器，那么由于光盘 ID 只对一个特定的光盘有效，所以可以制止在许多机器上非法安装。

如上所述，驱动器 ID 方法和光盘 ID 方法具有它们自己的优点和缺点，并且对于不同的应用，优点是不同的，希望将来驱动器 ID 方法能用于只安装一次的计算机软件，光盘 ID 方法能用于多次再现的电影或音乐软件。这要求再现设备的设计能支持两种方法。利用图 42 的流程图，我们将描述处理驱动器 ID 和光盘 ID 两者的操作过程。当开始安装时，首先在步骤 901a，检查扰码标识符是否为“开”。如果软件被扰码并且标识符为“关”，则意味着是非法操作，并停止安装。如果标识符为“开”但软件没有扰码，则也停止安装。如已经描述的，该扰码标识符不能变更，因此能有效防止非法安装。在步骤 901c，通过一网络将个人计算机接至口令发放中心。在步骤 901d，输入用户 ID，并在步骤 901e，如果再现设备具有驱动器 ID，则把驱动器 ID 发送给口令发放中心。确认付款后，口令发放中心用副保密密钥对驱动器 ID 和软件 ID 进行加密和计算，从而产生口令。用户端的个人计算机用副公开密钥进行计算，对口令解码，并将其与个人计算机的机器 ID 或驱动器的驱动器 ID 作比较。如果它们不一致，则停止操作；如果它们一致，则在步骤 901n，运行安装程序。也就是说，在上例中，当在步骤 901k 用驱动器 ID 计算口令时，可以输出程序解密密钥，以完成解密或解扰。

回到步骤 901e，如果不存在驱动器 ID，那么在步骤 901h 检查光盘 ID 是否被记录在光盘上，并且如果不存在光盘 ID，则停止安装。如果记录了光盘 ID，则将光盘 ID 和软件 ID 发送给口令发放中心，口令发放中心与信贷公司通信，并在确认通过信贷联机付款后，在步骤 901j 用副保密密钥从光盘 ID 和软件 ID 中产生口令。在步骤 901m，用户端的个人计算机用副公开密钥对口令解密，并且如果检查结果为肯定，则完成程序安装或软件再现。

用这种方法，可以处理驱动器 ID 和光盘 ID 两者，它具有防止安装的效果，同时允许合法安装具有各种 ID 的软件产品。

由此，通过用单向加密的编码器对光盘物里 ID 加密，可以增强复制保护的安全性。

如上所述，依照本发明，在由两盘层压在一起而构成的光盘的反射层上形成一非反射部分，并至少对其位置信息加密且将其写在同一光盘上。与现有技术相比，这使得更难进行复制。从而真正不可能生产非法复制品，即所谓的盗版盘。

从到此为止所给的说明可见，本发明与现有技术相比，具有大大提高防复制能力的优点。

另外，依照本发明，如参照图 32 所述的，通过将公开密钥数据和软件特征信息与格式化的主盘物理特征信息 876 结合在一起加密，可使盗版检查机构包含在主盘中。这进一步提高了保密性。

在图 26 中，揭示了一种方法，该方法为联网的购物公司提供了更大的安全度。依照该方法，联网的购物公司将秘密通信用的私人密钥二次记录在所有的光盘上，并将其分配给用户，不必通过邮寄把私人密钥送给用户，并且用户还省去了要键入包含许多数字的私人密钥的麻烦。另外，由于用户不必自己使用私人密钥，所以由 100 个或更多个数字组成的大数值可用作私人密钥。这大大地提高了网络的安全度。

在上述实施例中，将本发明的标记位置信息写在了同一光盘上，但本发明不局限于所述的实施例。例如，可将信息写在作为不同媒体的软盘上。

另外，在上述实施例中，描述了一些实施例，在这些例子中，将椭圆函数或 RSA 函数应用于数字签名或数字签名类技术或者加密技术中。但是，本发明不局限于所述的例子，例如可以使用诸如 DES 等保密密钥加密函数，或者任何其他的加密技术。

此外，在上述实施例中，对位置信息加密或为其提供了数字签名，但也可将位置信息本身直接写在光盘上，以作替代。同样，在该情况下，本发明能有效防止通过复制标记及其位置信息来制造盗版盘。

本发明的光盘具有这样的结构，即将反射膜直接或间接夹在两个能

耐激光的部件之间，并且用激光器在反射膜上形成标记。上述实施例已经描述了将该结构用于防盗版技术的例子，但希望这种结构还能应用于其他技术。在上述实施例中，描述了通过将两层衬底与位于中间的粘着层层压在一起来制造本发明的光盘。但是，可以省去粘着层，或者用不同材料制成的部件譬如保护层来替代；也就是说，只要将反射膜直接或间接夹在两个能耐激光的部件之间，就可使用任何合适的结构。另外，在上述实施例中，描述了本发明的光盘包含作为被层压在一起的部件的衬底，但可以使用诸如保护层等其他部件；也就是说，可以使用任何耐激光的部件。

在上述实施例中，描述了对保密密钥密码和公开密钥密码两者密码的组合，将其作为不同代多种密码组合的一个代表性例子，但本发明不局限于该特殊的例子。例如，作为不同代的另一种组合，可以使用具有256 比特保密密钥的公开密钥密码，它的保密性较差但可用慢的 CPU 处理，已经具有 1024 比特保密密钥的公开密钥密码，它提供较好的保密性但只能用高速 CPU 处理。用这种方法，通过组合具有不同安全等级的公开密钥密码，可以获得在不同代间同样保持兼容的效果。另外，还可使用三种不同代的密码的组合，例如保密密钥密码、保密性差的公开密钥密码和保密性好的公开密钥密码。

工业应用性

如上所述，在本发明中，例如用激光器在写有数据的光盘的反射膜上形成一标记，并以加密的形式或用所加的数字签名，至少将标记的位置信息或与该位置信息有关的信息写在光盘上，从而与现有结构相比，大大提高了防复制的能力。

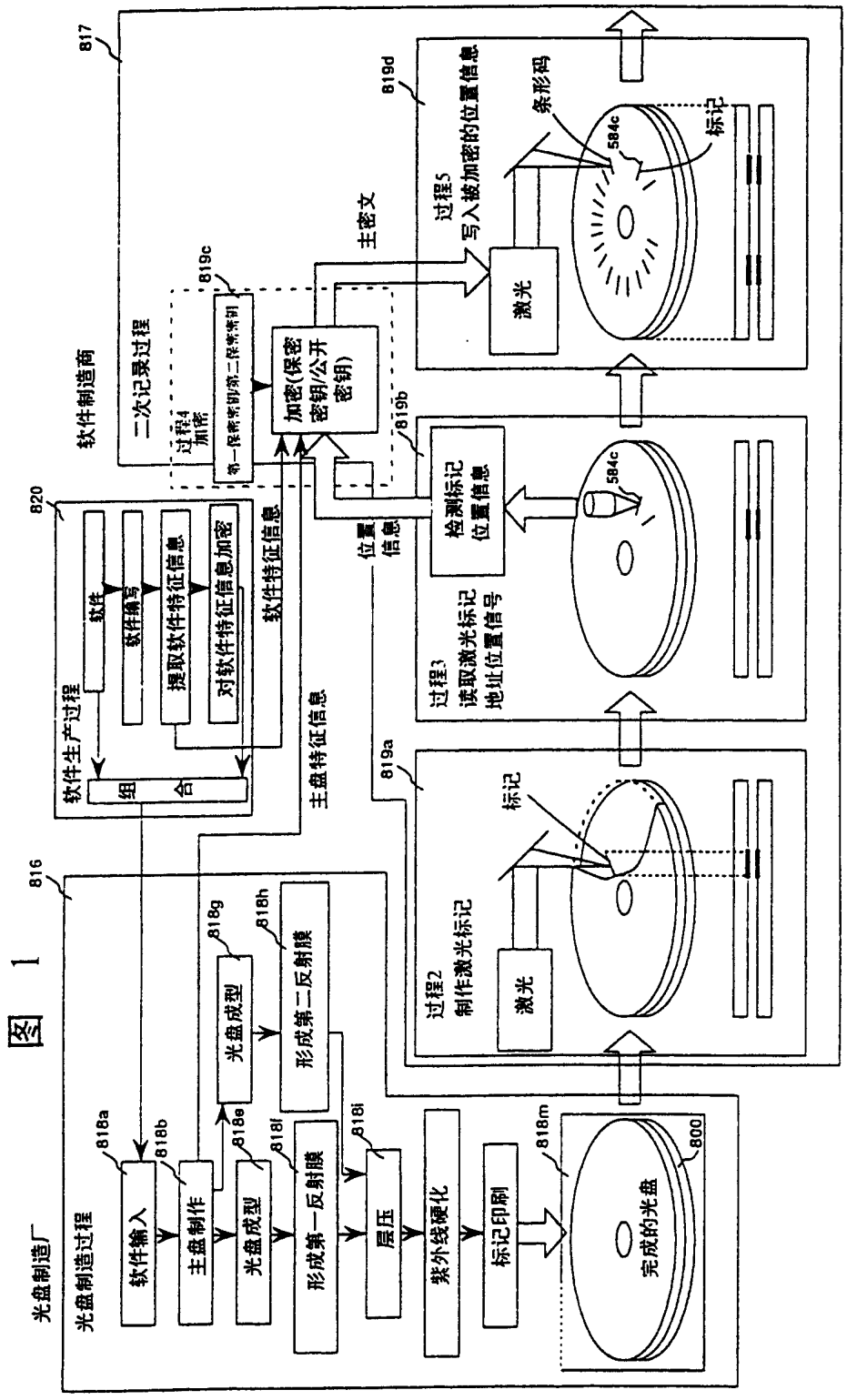

光盘制造厂
816
光盘制造过程
818a 软件输入
818b 主盘制作
818e 光盘成型
818f 形成第一反射膜
818i 层压
紫外线硬化
818m 标记印刷
800 完成的光盘
818g 光盘成型
818h 形成第二反射膜
主盘特征信息
软件制造商
817
二次记录过程
过程4 加密
819c
加密(保密密钥/公开密钥)
主密文
819d
过程5 写入被加密的位置信息
激光
584c
标记
条形码
820
软件生产过程
软件
软件编写
提取软件特征信息
对软件特征信息加密
软件特征信息
组 合
位置信息
819b
检测标记位置信息
过程3 读取激光标记地址位置信号
819a
过程2 制作激光标记

图 1

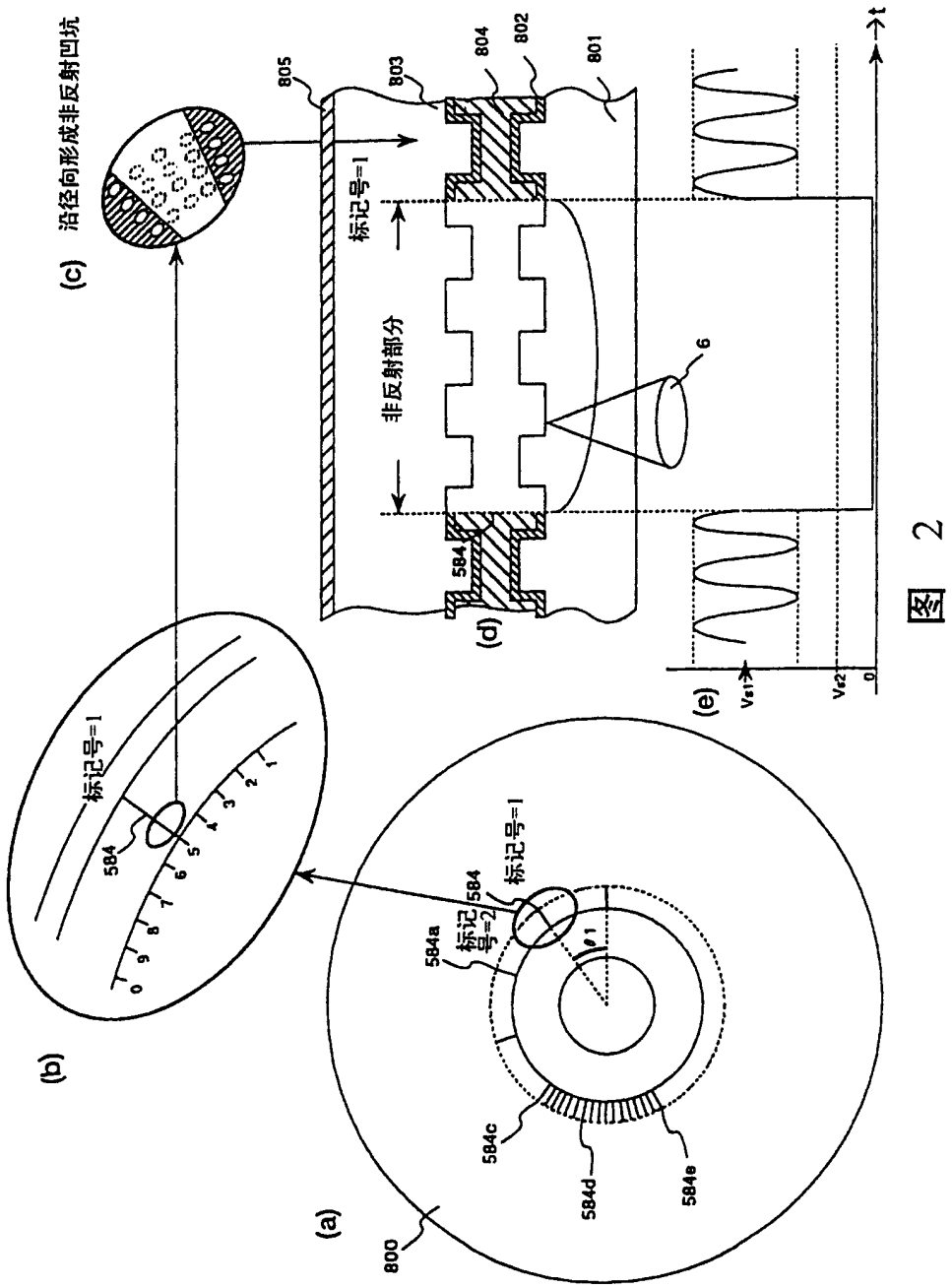

(a)
800
584a
标记号=2
584
标记号=1
584c
584d
584e
(b)
标记号=1
584
(c) 沿径向形成非反射凹坑
(d)
805
803
804
802
801
标记号=1
非反射部分
584
6
(e)
Vs1
Vs2
0
t

图 2

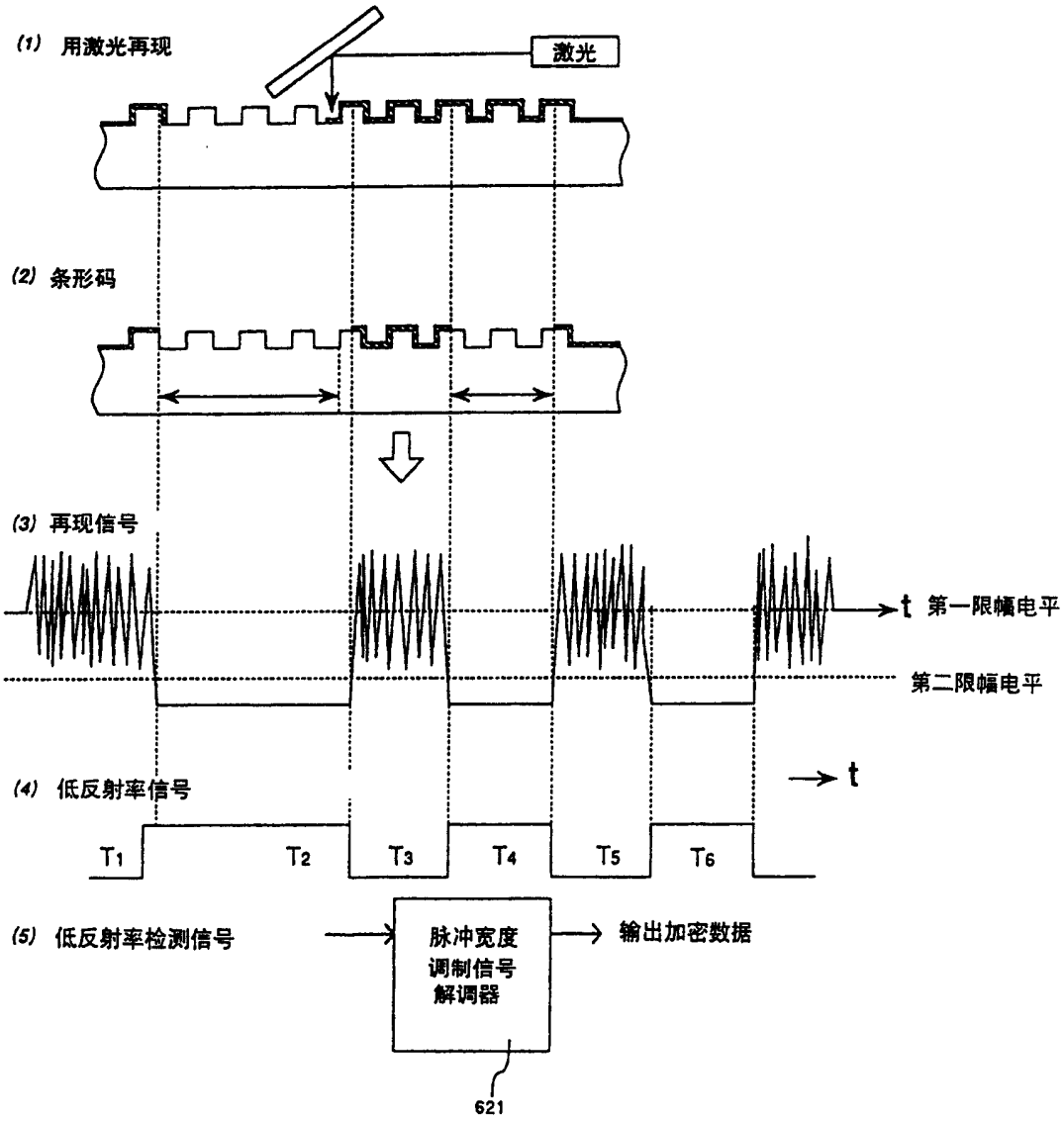

(1) 用激光再现
激光
(2) 条形码
(3) 再现信号
t 第一限幅电平
第二限幅电平
(4) 低反射率信号
t
T1
T2
T3
T4
T5
T6
(5) 低反射率检测信号
脉冲宽度
调制信号
解调器
输出加密数据
621

图 3

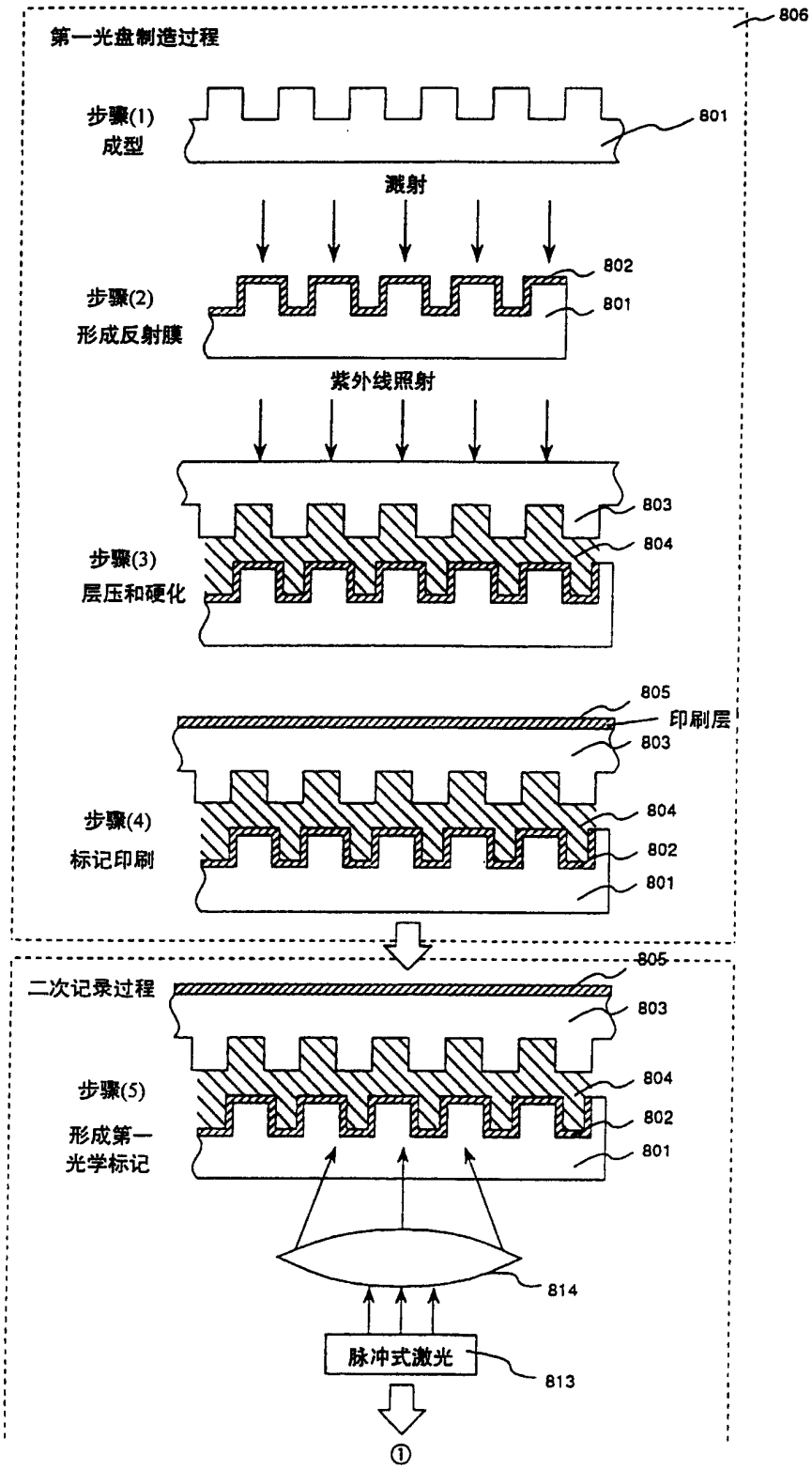

806
第一光盘制造过程
步骤(1)
成型
801
溅射
802
步骤(2)
形成反射膜
801
紫外线照射
803
804
步骤(3)
层压和硬化
805
印刷层
803
804
步骤(4)
标记印刷
802
801
二次记录过程
805
803
804
步骤(5)
形成第一
光学标记
802
801
814
脉冲式激光
813
①

图 4

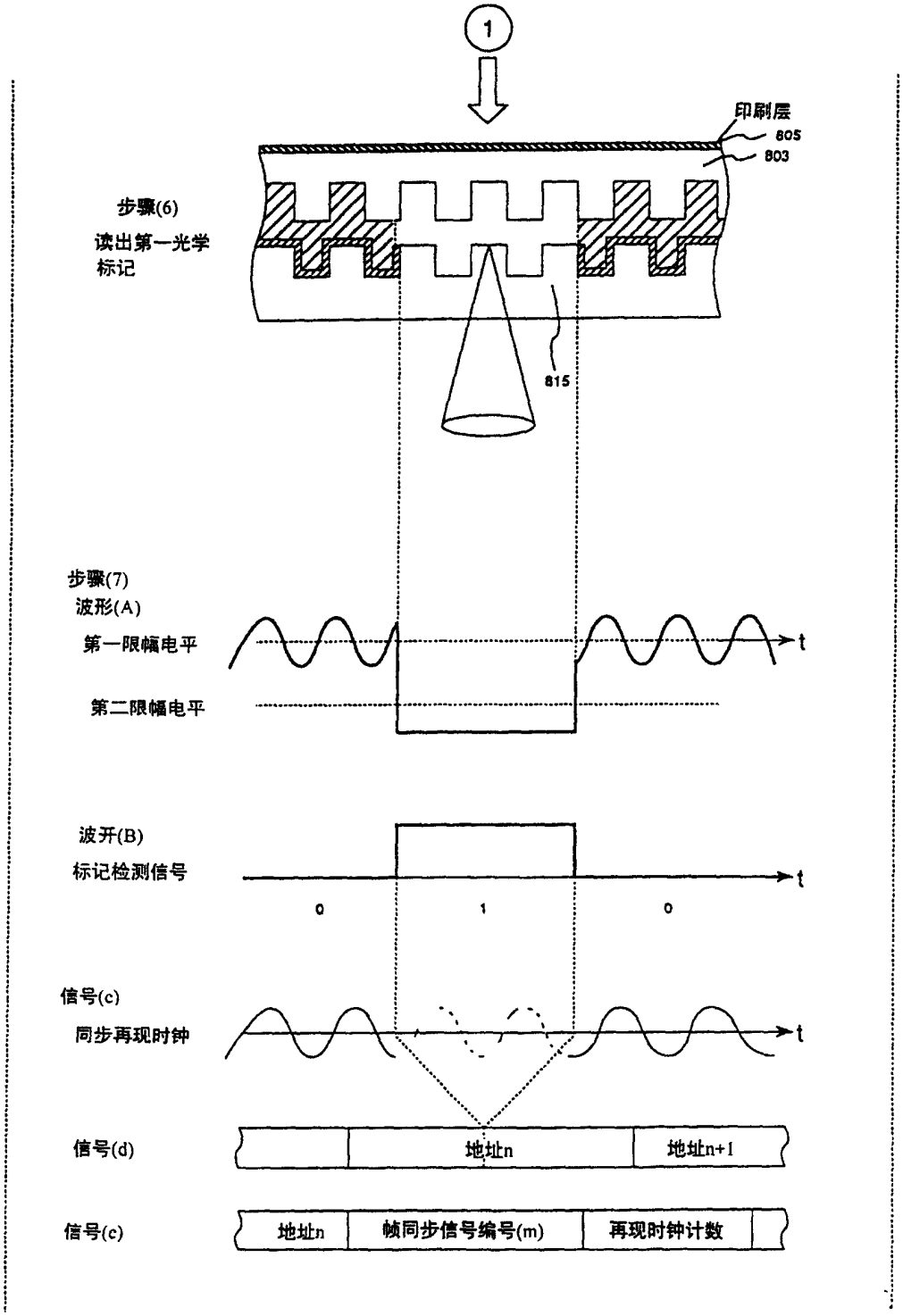

1
印刷层
805
803
步骤(6)
读出第一光学标记
815
步骤(7)
波形(A)
第一限幅电平
t
第二限幅电平
波开(B)
标记检测信号
t
0
1
0
信号(c)
同步再现时钟
t
信号(d)
地址n
地址n+1
信号(c)
地址n
帧同步信号编号(m)
再现时钟计数

图 5

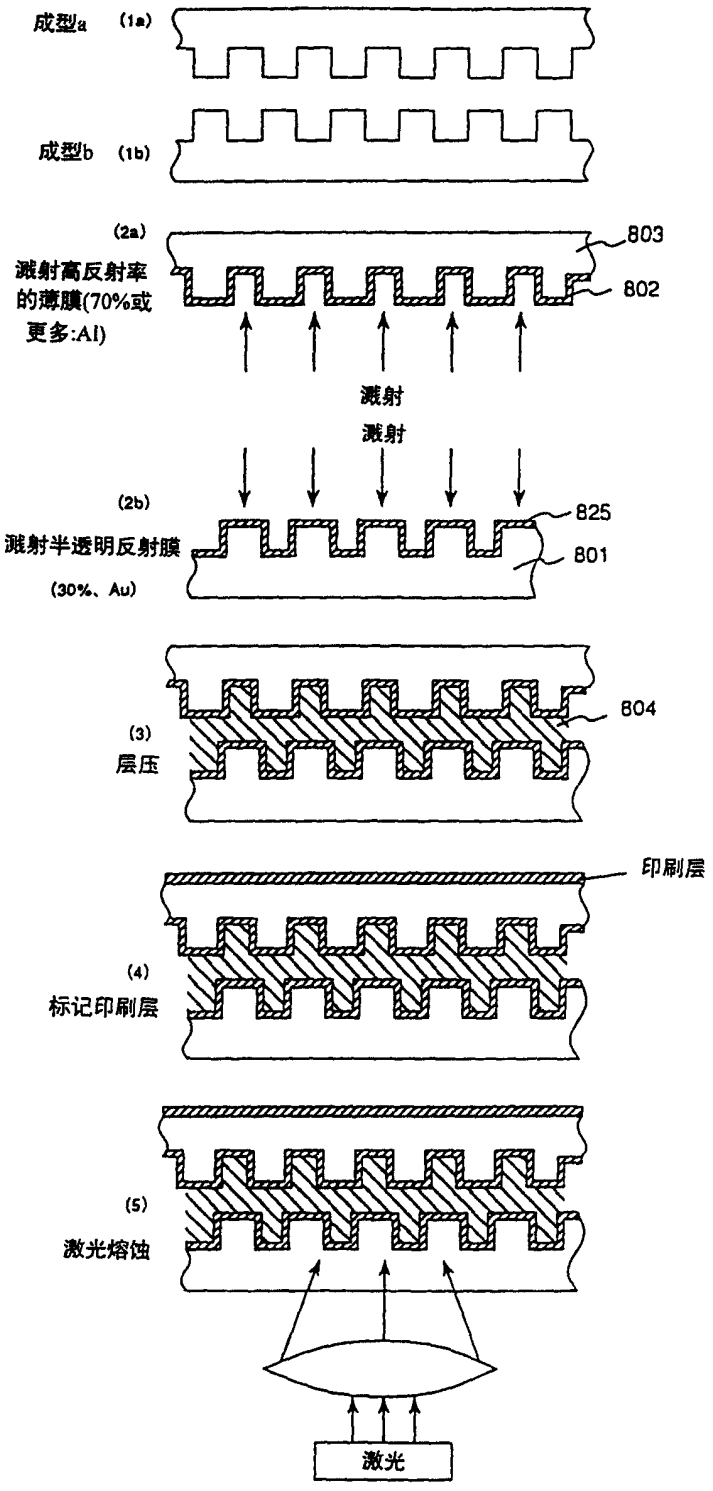

成型a (1a)
成型b (1b)
(2a)
溅射高反射率的薄膜(70%或更多:Al)
803
802
溅射
溅射
(2b)
溅射半透明反射膜
(30%、Au)
825
801
(3)
层压
804
印刷层
(4)
标记印刷层
(5)
激光熔蚀
激光

图 6

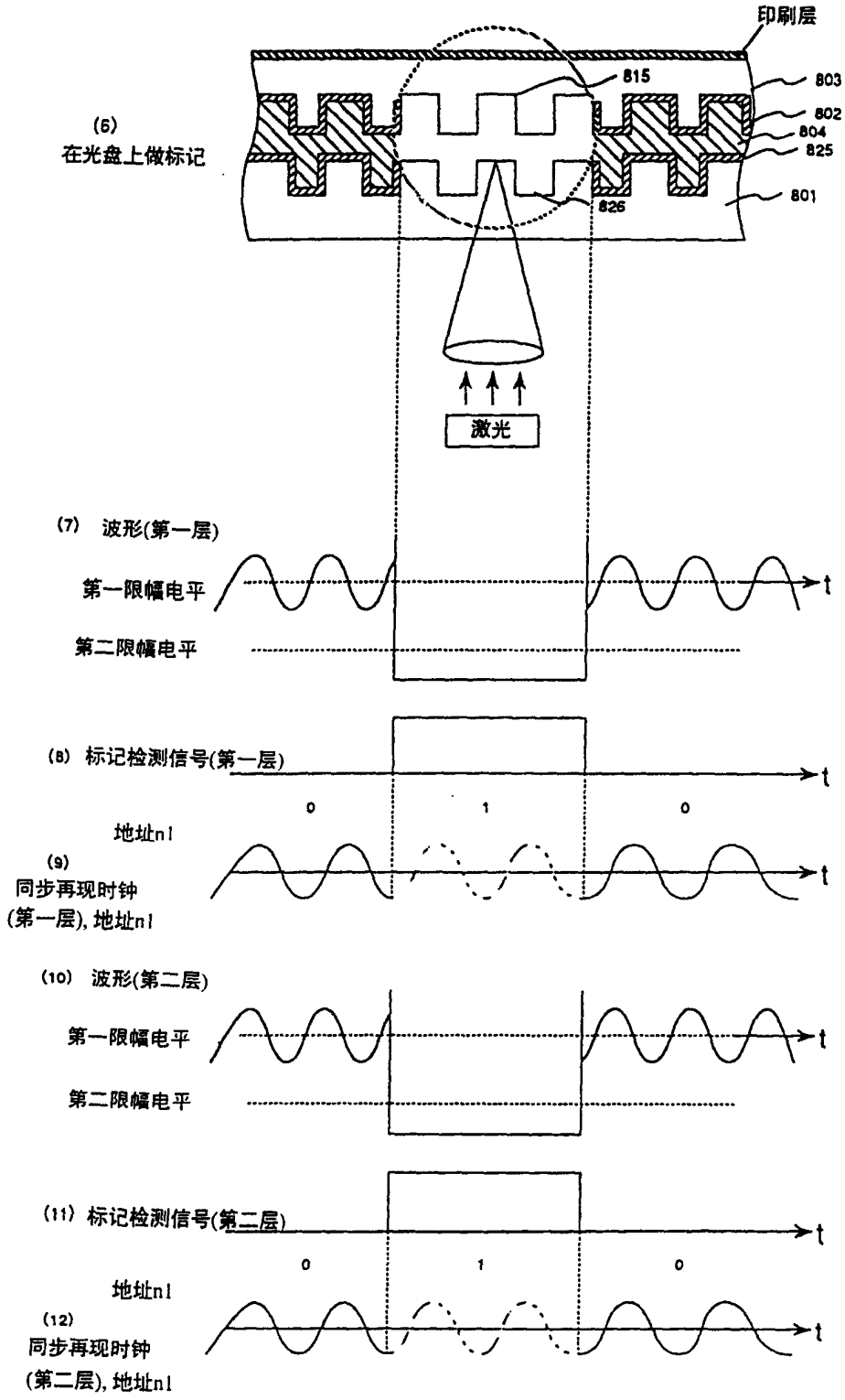
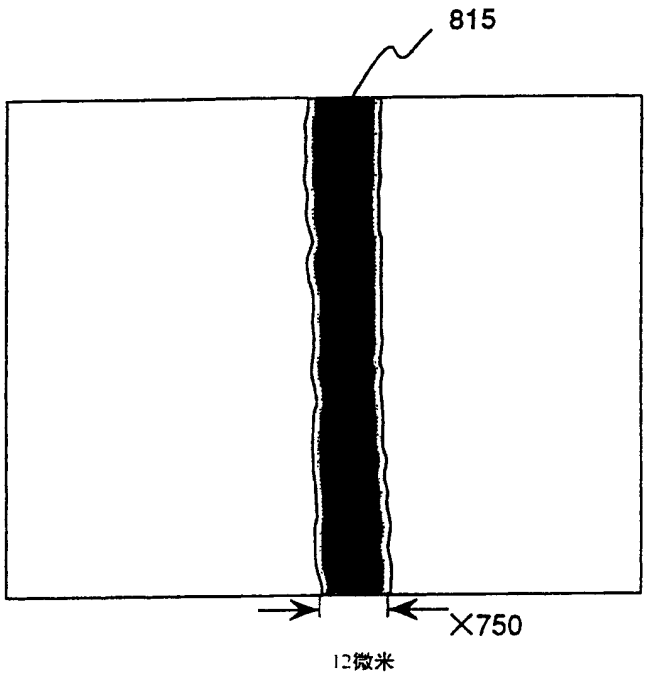

印刷层
815
803
802
804
825
826
801
(6)
在光盘上做标记
激光
(7) 波形(第一层)
第一限幅电平
第二限幅电平
t
(8) 标记检测信号(第一层)
0
1
0
地址n1
(9)
同步再现时钟
(第一层), 地址n1
(10) 波形(第二层)
第一限幅电平
第二限幅电平
(11) 标记检测信号(第二层)
0
1
0
地址n1
(12)
同步再现时钟
(第二层), 地址n1

图 7

(a)



(b)

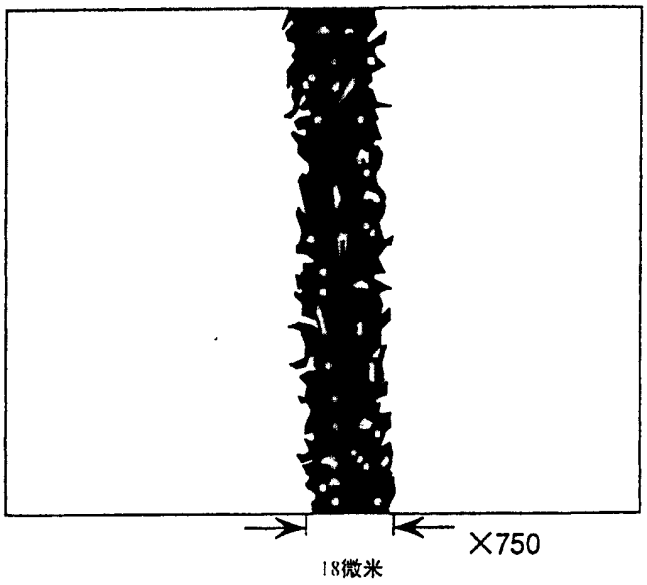


图 8

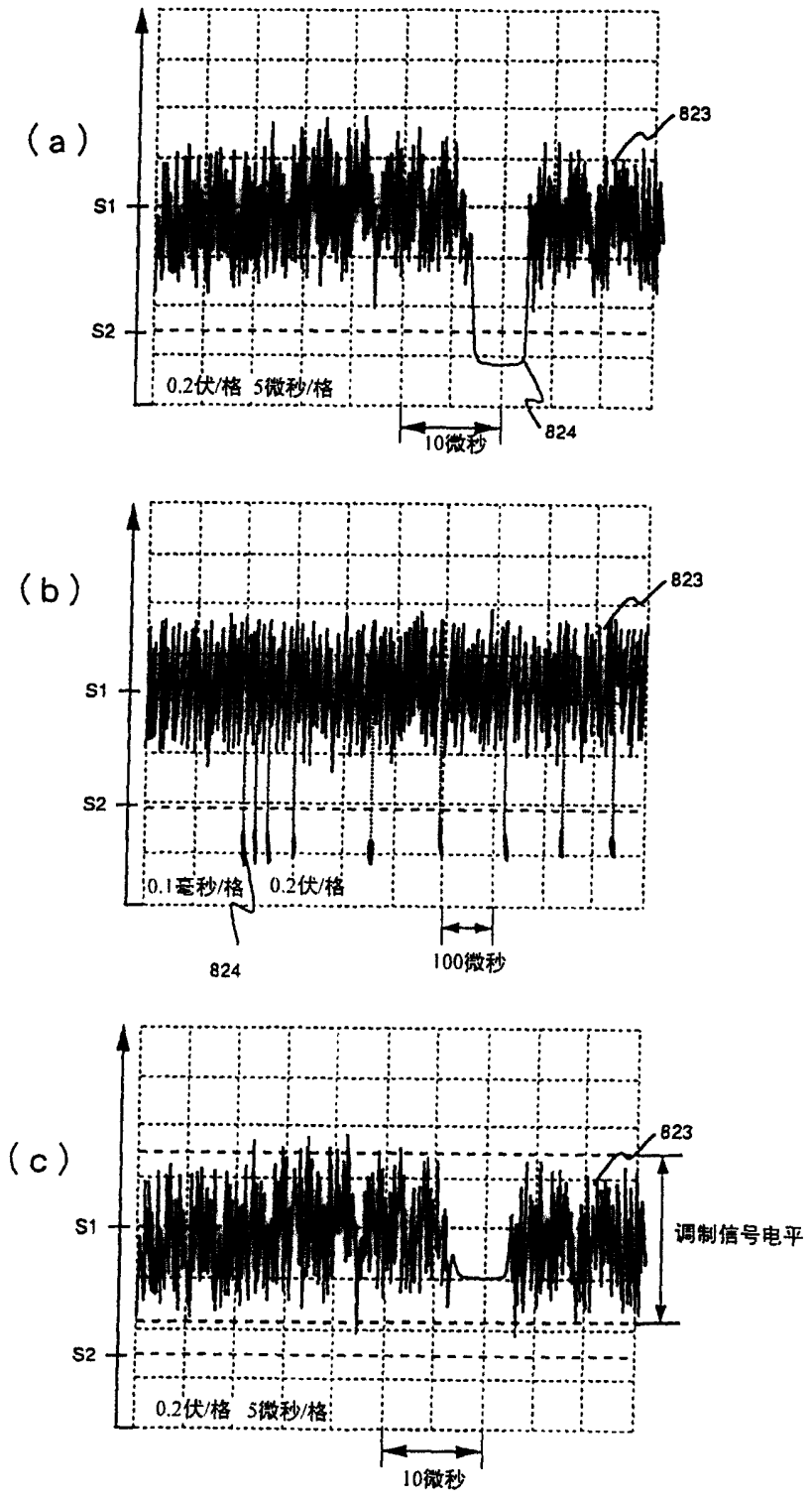

(a)
S1
S2
823
824
0.2伏/格 5微秒/格
10微秒
(b)
S1
S2
823
824
0.1毫秒/格
0.2伏/格
100微秒
(c)
S1
S2
823
调制信号电平
0.2伏/格 5微秒/格
10微秒

图 9

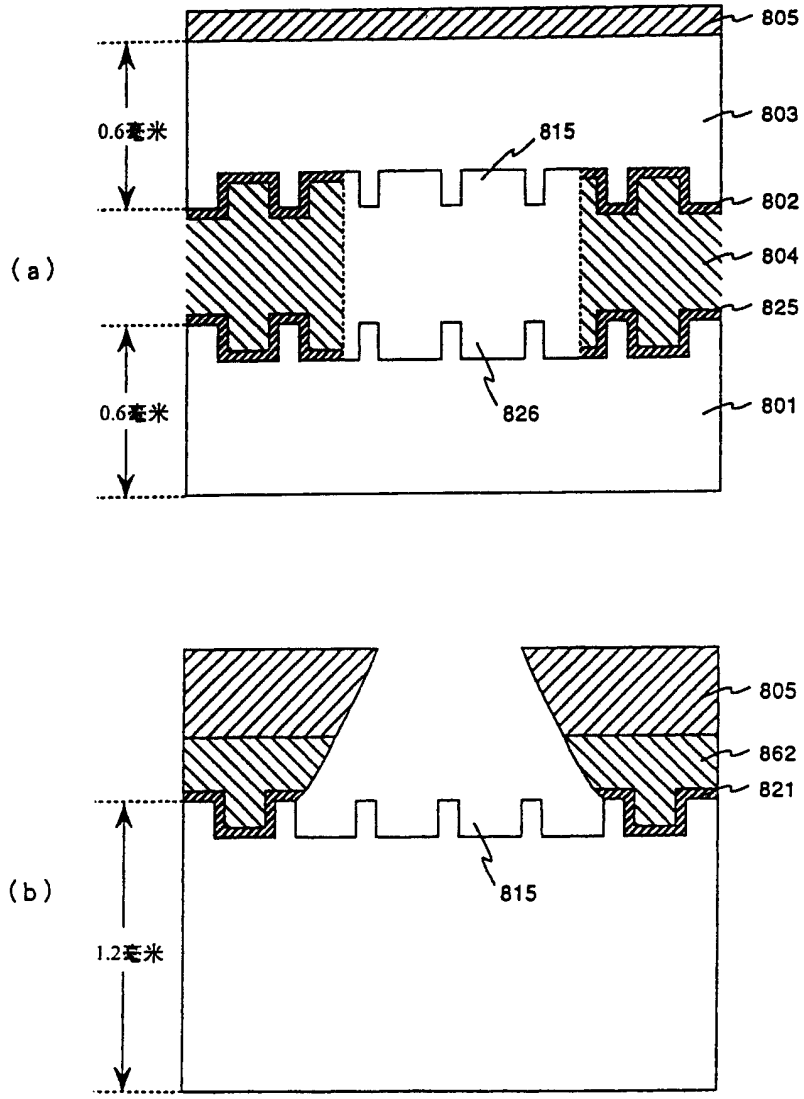

(a)
805
803
815
802
804
825
826
801
0.6毫米
0.6毫米
(b)
805
862
821
815
1.2毫米

图 10

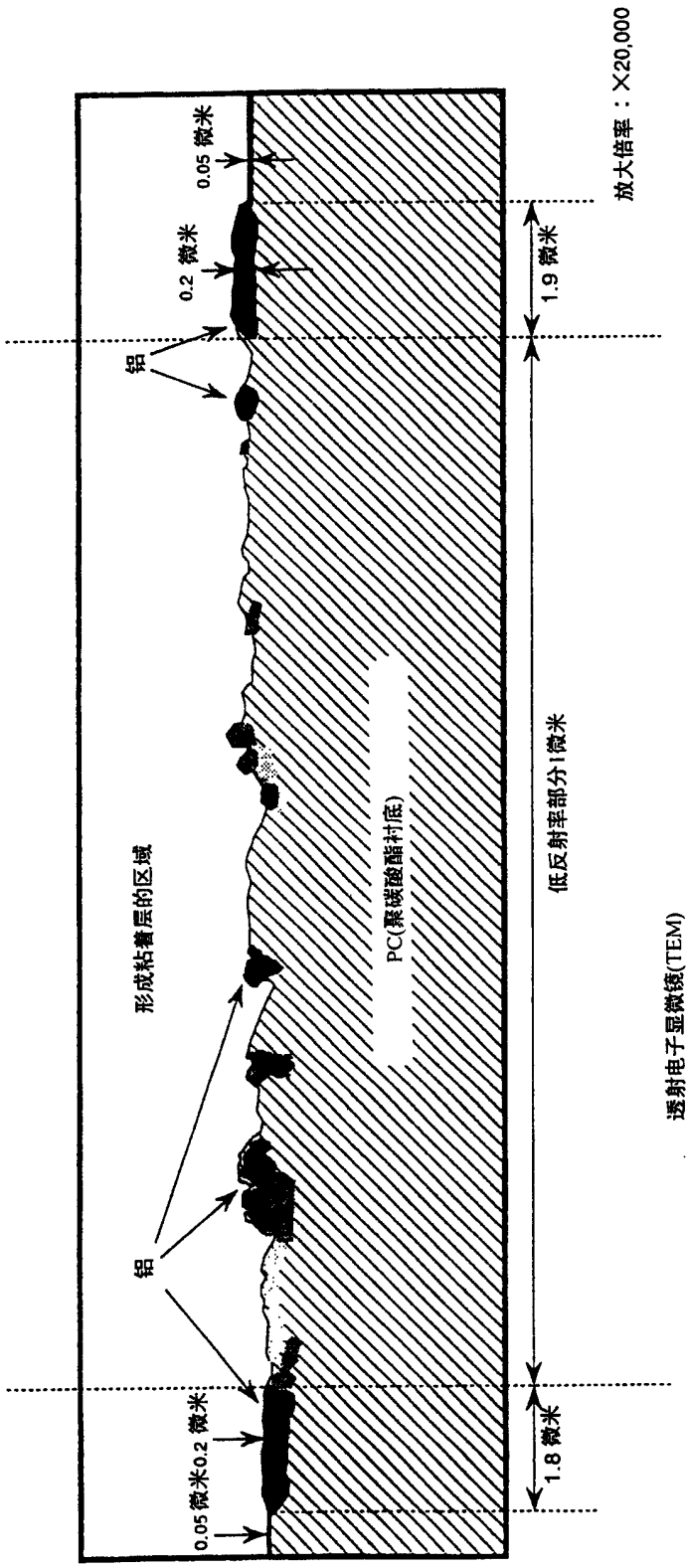

放大倍率：×20,000
0.05 微米
0.2 微米
铝
1.9 微米
形成粘着层的区域
PC(聚碳酸酯衬底)
低反射率部分1微米
铝
0.05 微米0.2 微米
1.8 微米
透射电子显微镜(TEM)

图 11

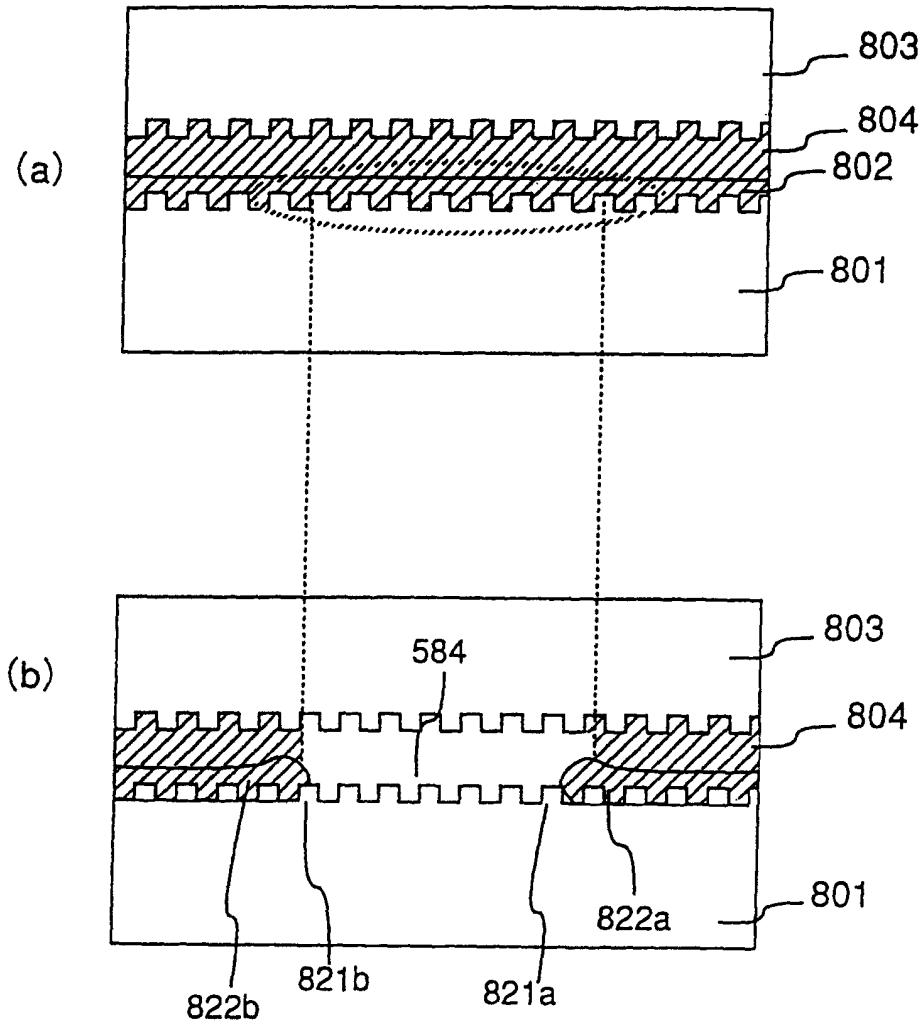


图 12

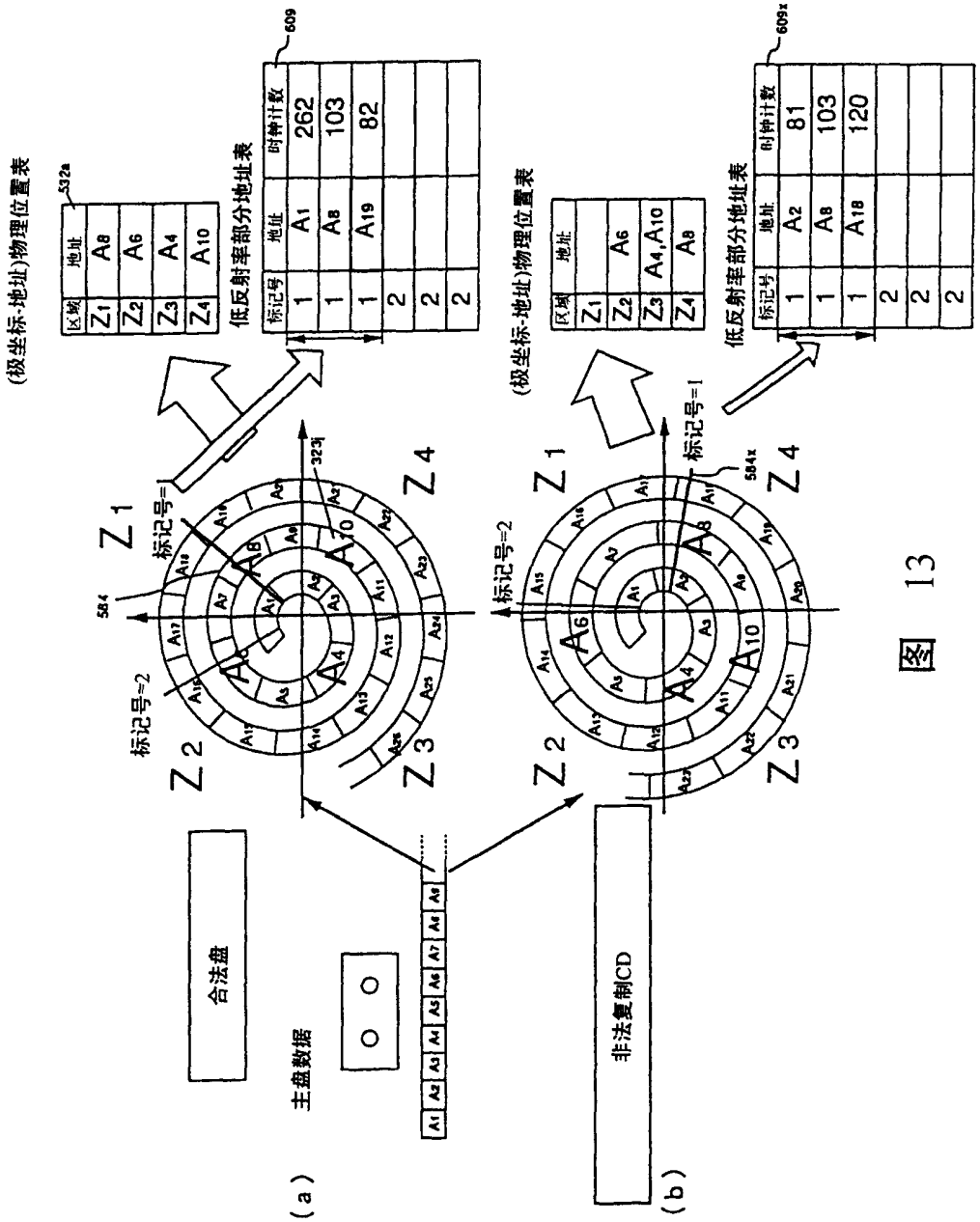

(极坐标-地址)物理位置表
区域 地址
Z1 A8
Z2 A6
Z3 A4
Z4 A10
532a
低反射率部分地址表
标记号 地址 时钟计数
1 A1 262
1 A8 103
1 A19 82
2
2
2
609
标记号=1
标记号=2
Z1
Z2
Z3
Z4
584
323
合法盘
主盘数据
(a)
非法复制CD
(b)
(极坐标-地址)物理位置表
区域 地址
Z1
Z2 A6
Z3 A4,A10
Z4 A8
低反射率部分地址表
标记号 地址 时钟计数
1 A2 81
1 A8 103
1 A18 120
2
2
2
609a
584a

图 13

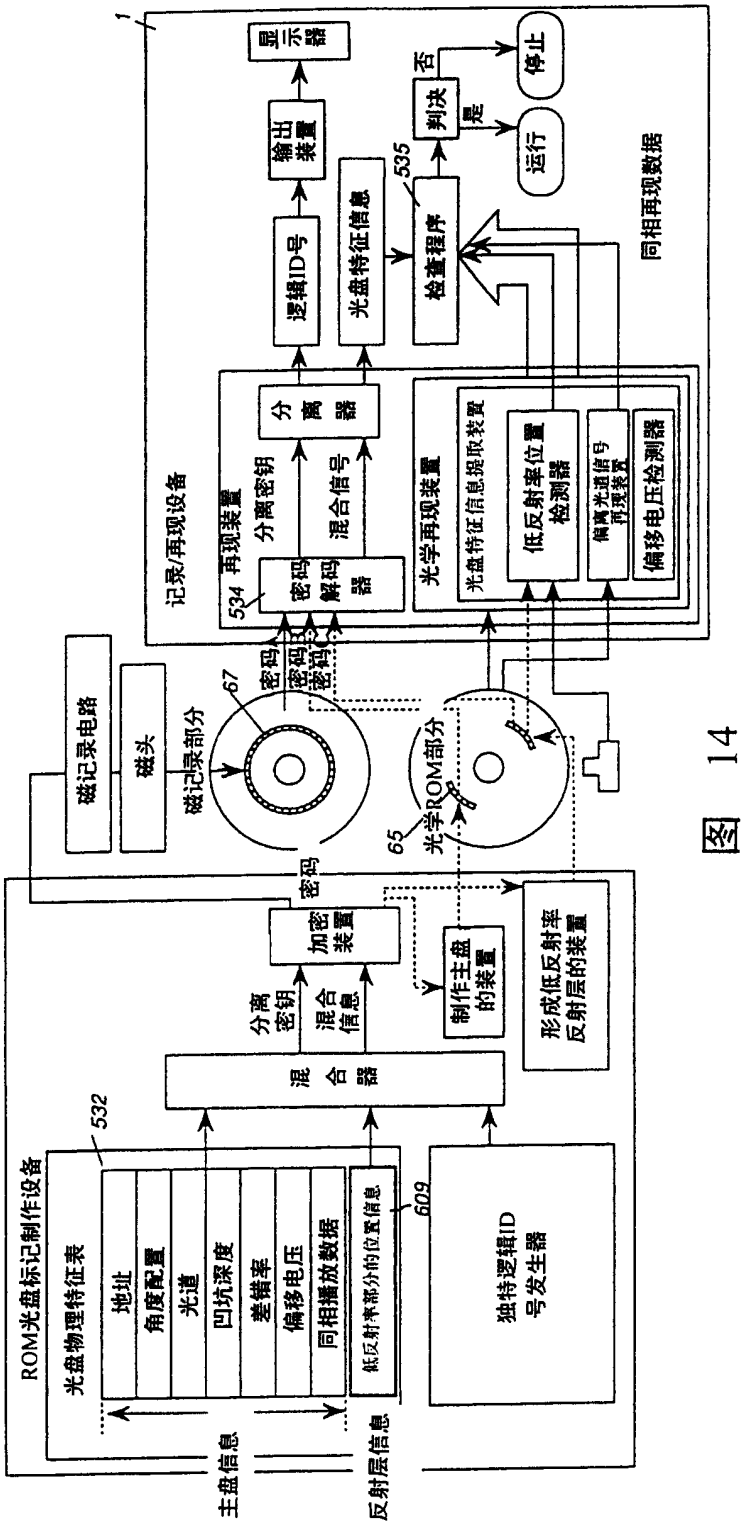

ROM光盘标记制作设备
光盘物理特征表
地址
角度配置
光道
凹坑深度
差错率
偏移电压
同相播放数据
低反射率部分的位置信息
532
609
主盘信息
反射层信息
混合器
分离密钥
混合信息
加密装置
密码
制作主盘的装置
形成低反射率反射层的装置
独特逻辑ID号发生器
磁记录电路
磁头
磁记录部分
67
密码
密码
密码
65
光学ROM部分
记录/再现设备
1
再现装置
534
密码解码器
分离密钥
分离器
混合信号
逻辑ID号
光盘特征信息
535
检查程序
输出装置
显示器
光学再现装置
光盘特征信息提取装置
低反射率位置检测器
偏离光通信号再现装置
偏移电压检测器
同相再现数据
判决
是
否
运行
停止

图 14

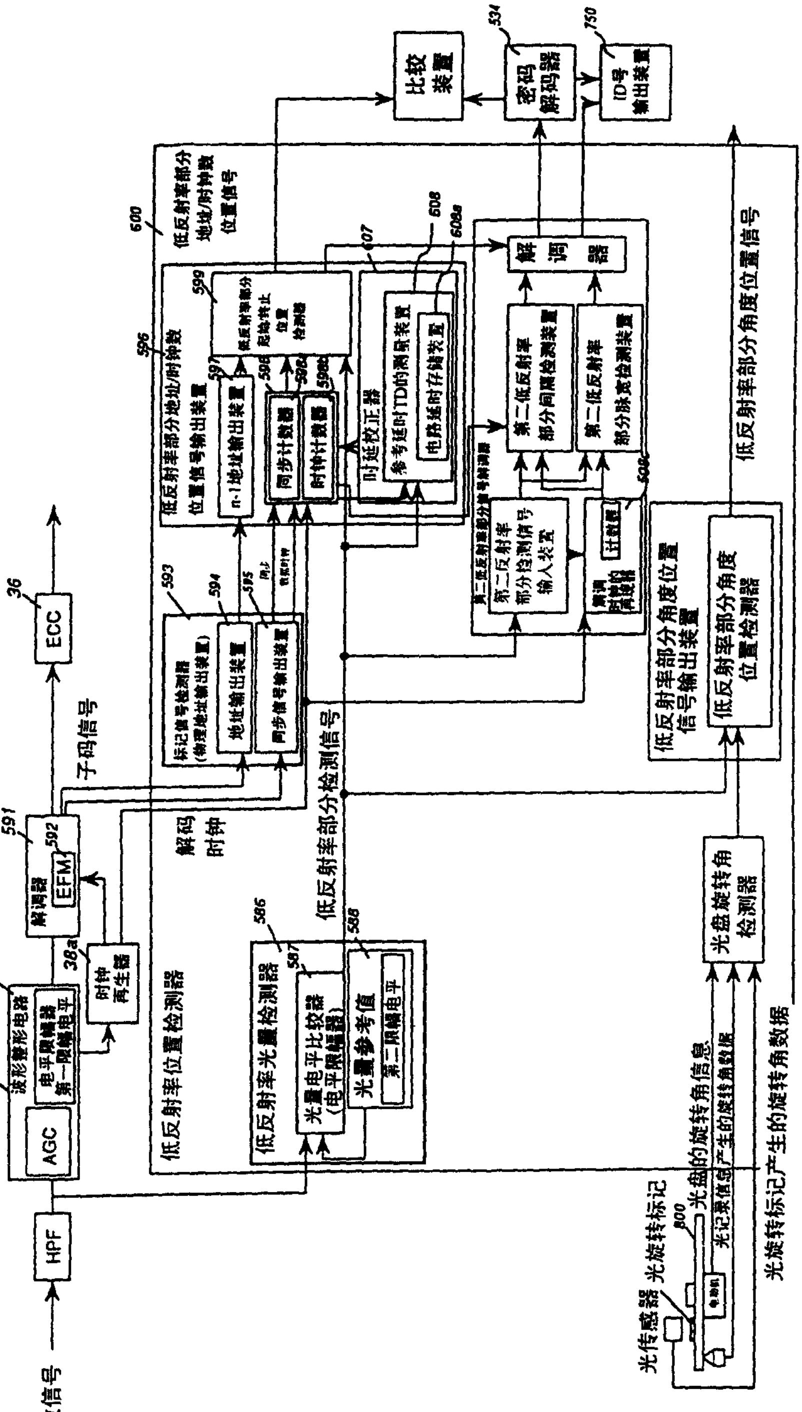

光学播放信号
HPF
AGC
590a
590
波形整形电路
电平限幅器
第一限幅电平
591
解调器
592
EFM
38a
时钟再生器
36
ECC
子码信号
解码时钟
低反射率位置检测器
586
低反射率光量检测器
587
光量电平比较器（电平限幅器）
588
光量参考值
第二限幅电平
低反射率部分检测信号
593
标记信号检测器（物理地址输出装置）
594
地址输出装置
595
同步信号输出装置
596
低反射率部分地址/时钟数位置信号输出装置
597
n-1地址输出装置
同步计数器
时钟计数器
599
低反射率部分起始/终止位置检测器
600
低反射率部分地址/时钟数位置信号
607
时延校正器
608
608a
参考延时TD的测量装置
电路延时存储装置
第二低反射率部分信号解调器
第二反射率部分检测信号输入装置
解调时钟的再生器
计数器
第二低反射率部分间隔检测装置
第二低反射率部分脉宽检测装置
解调器
比较装置
534
密码解码器
750
ID号输出装置
低反射率部分角度位置信号输出装置
低反射率部分角度位置检测器
低反射率部分角度位置信号
光盘旋转角检测器
光传感器
光旋转标记
800
光盘的旋转角信息
光记录信息产生的旋转角数据
光旋转标记产生的旋转角数据

图 15

图 16

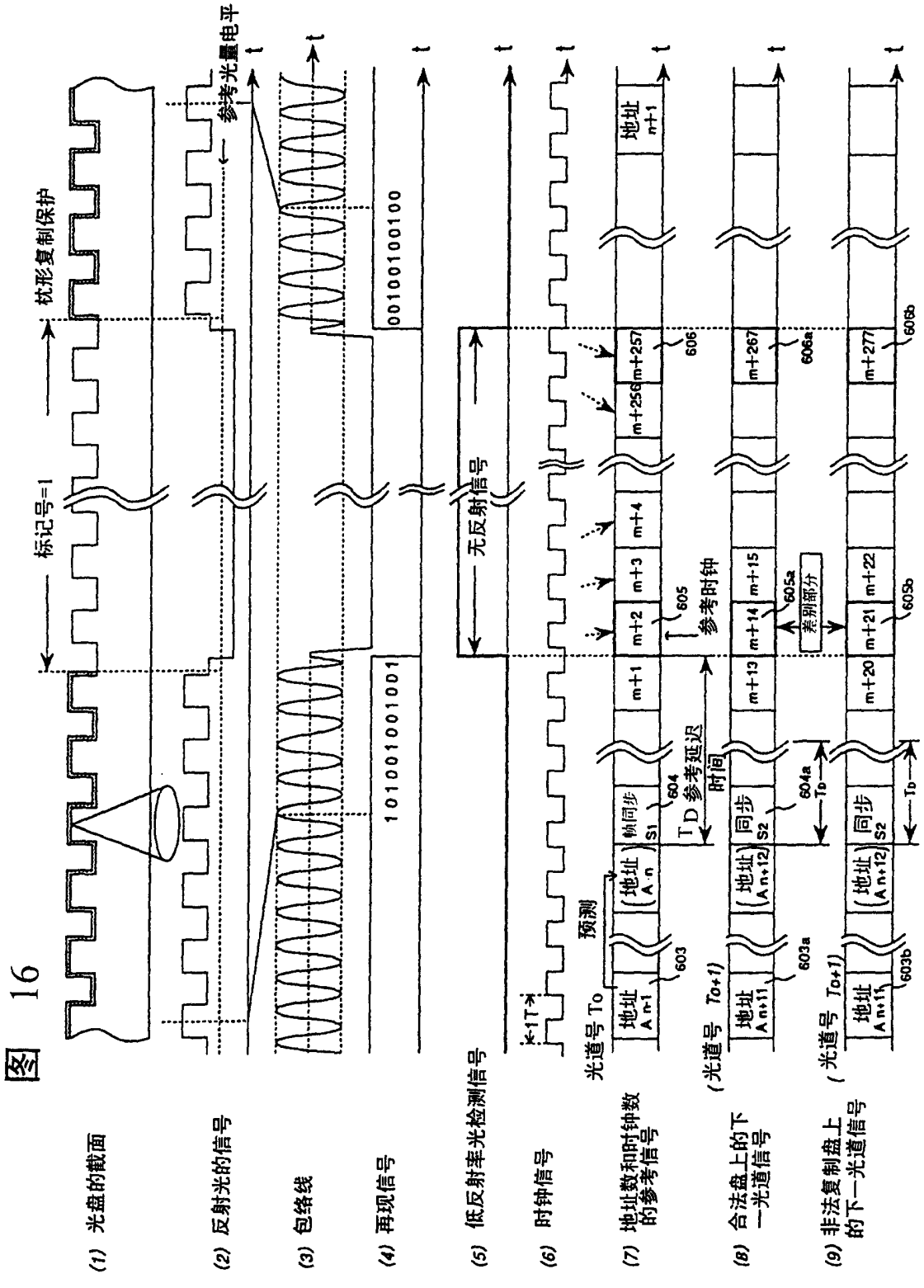
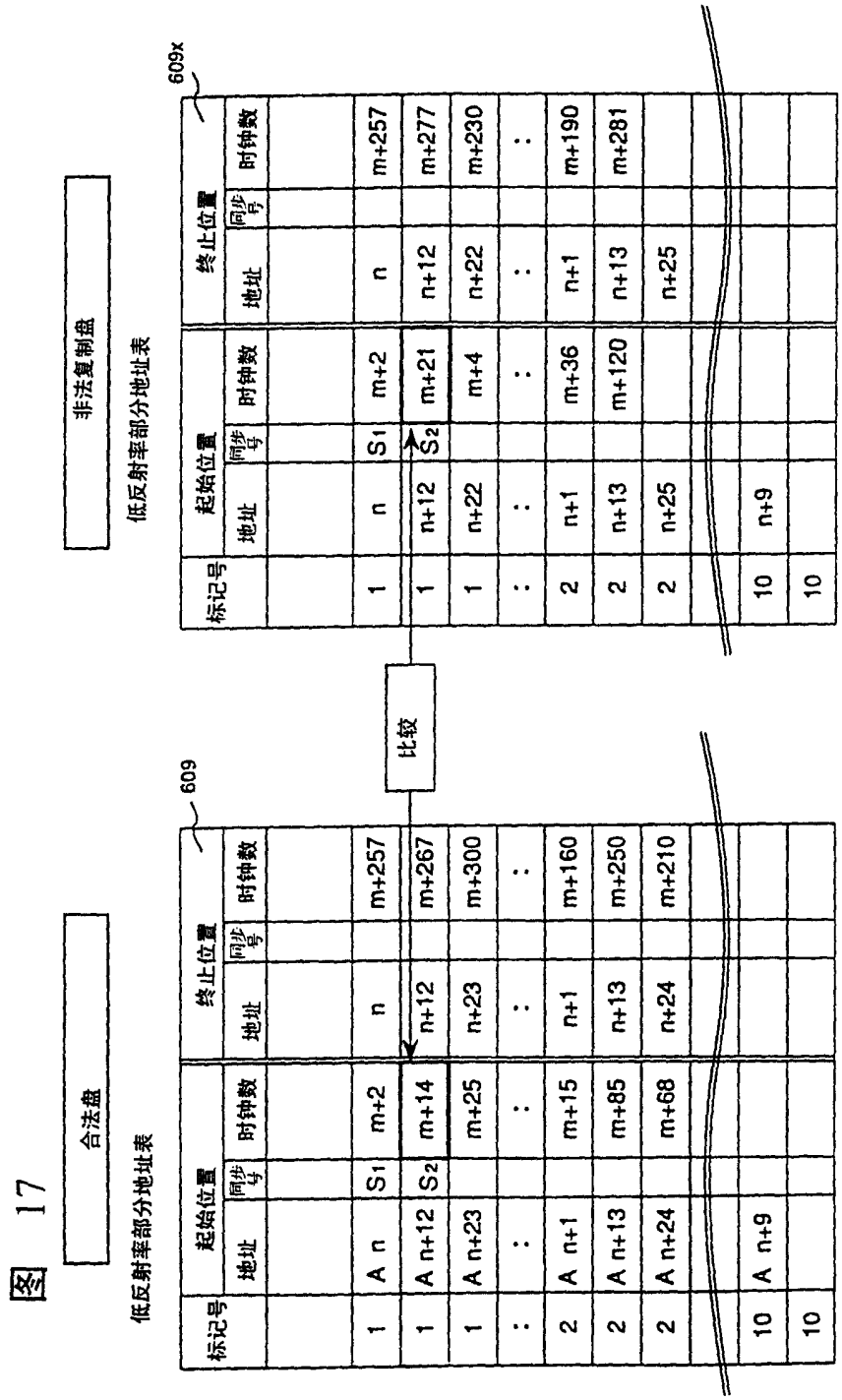

(1) 光盘的截面
标记号=1
枕形复制保护
(2) 反射光的信号
参考光量电平
(3) 包络线
(4) 再现信号
1010010010001
00100100100
(5) 低反射率光检测信号
无反射信号
(6) 时钟信号
(7) 地址数和时钟数的参考信号
预测
光道号 To
地址 An-1
603
地址 An
协同步 S1
604
TD 参考延迟时间
m+1
m+2
m+3
m+4
605
参考时钟
m+256
m+257
606
地址 n+1
(8) 合法盘上的下一光道信号
(光道号 To+1)
地址 An+11
603a
地址 An+12
同步 S2
604a
To
m+13
m+14
m+15
605a
差别部分
m+267
606a
(9) 非法复制盘上的下一光道信号
(光道号 To+1)
地址 An+11
603b
地址 An+12
同步 S2
To
m+20
m+21
m+22
605b
m+277
606b

图 17


合法盘
非法复制盘
低反射率部分地址表
低反射率部分地址表
609
609x
比较
标记号
起始位置
地址
同步号
时钟数
终止位置
地址
同步号
时钟数

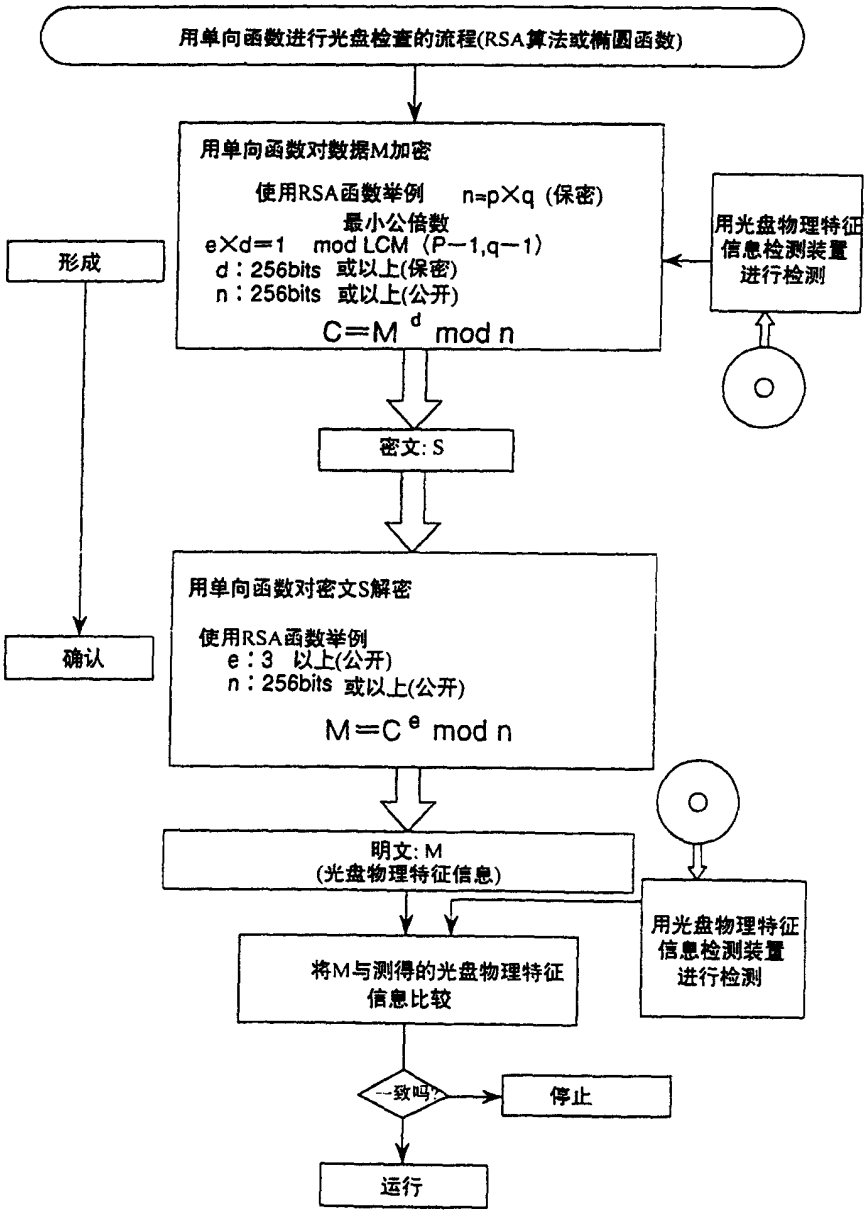

用单向函数进行光盘检查的流程(RSA算法或椭圆函数)
用单向函数对数据M加密
使用RSA函数举例 n=p×q (保密)
最小公倍数
e×d=1 mod LCM (P−1,q−1)
d：256bits 或以上(保密)
n：256bits 或以上(公开)
C=M d mod n
用光盘物理特征信息检测装置进行检测
形成
密文: S
用单向函数对密文S解密
使用RSA函数举例
e：3 以上(公开)
n：256bits 或以上(公开)
M=C e mod n
确认
明文: M
(光盘物理特征信息)
用光盘物理特征信息检测装置进行检测
将M与测得的光盘物理特征信息比较
一致吗?
停止
运行

图 18

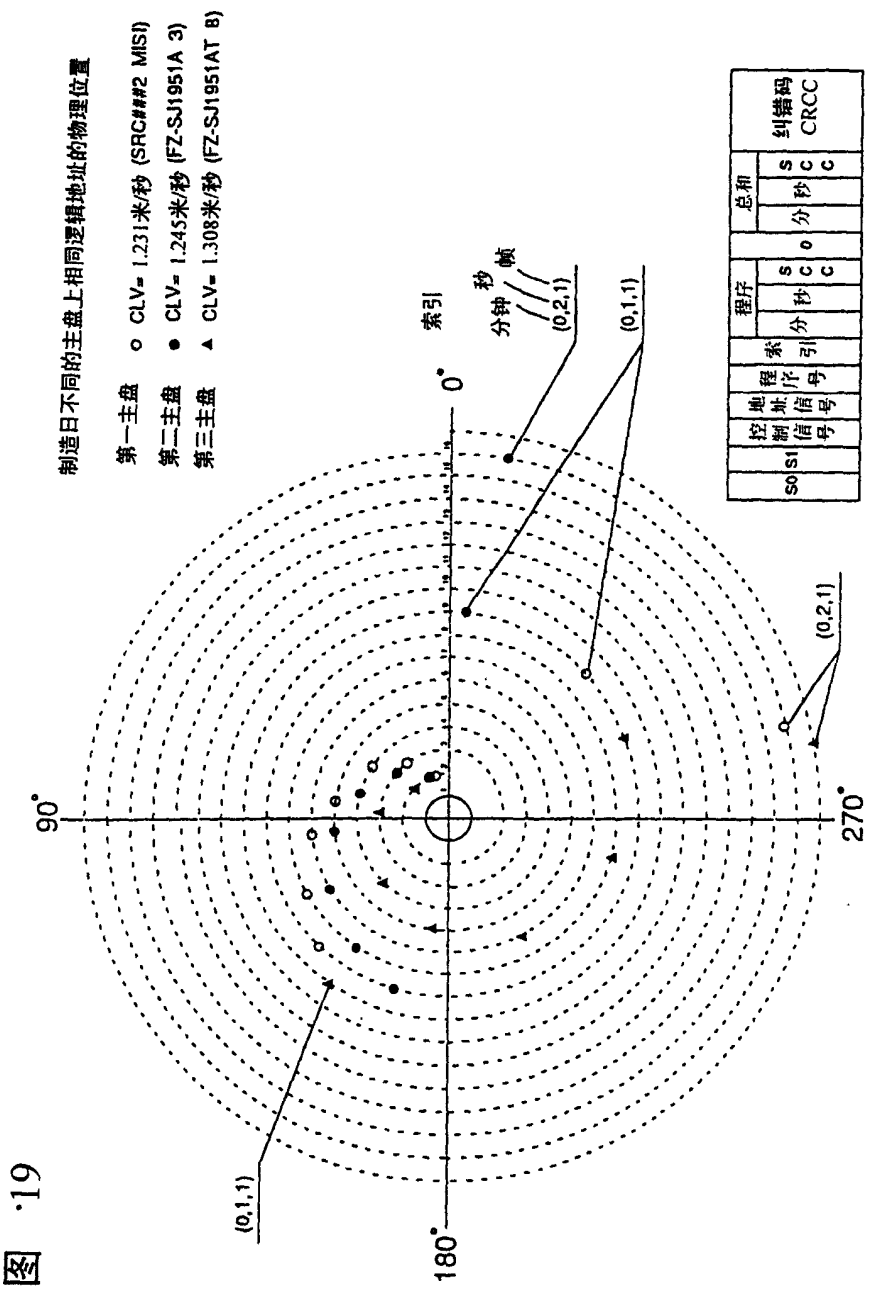

制造日不同的主盘上相同逻辑地址的物理位置
第一主盘 ○ CLV= 1.231米/秒 (SRC###2 MISI)
第二主盘 ● CLV= 1.245米/秒 (FZ-SJ1951A 3)
第三主盘 ▲ CLV= 1.308米/秒 (FZ-SJ1951AT 8)
0°
90°
180°
270°
索引
分钟
秒
帧
(0,2,1)
(0,1,1)
(0,2,1)
(0,1,1)
SOSI
控制信号
地址信号
程序号
索引
程序
分
秒
总和
分
秒
纠错码 CRCC

图 19

图 20

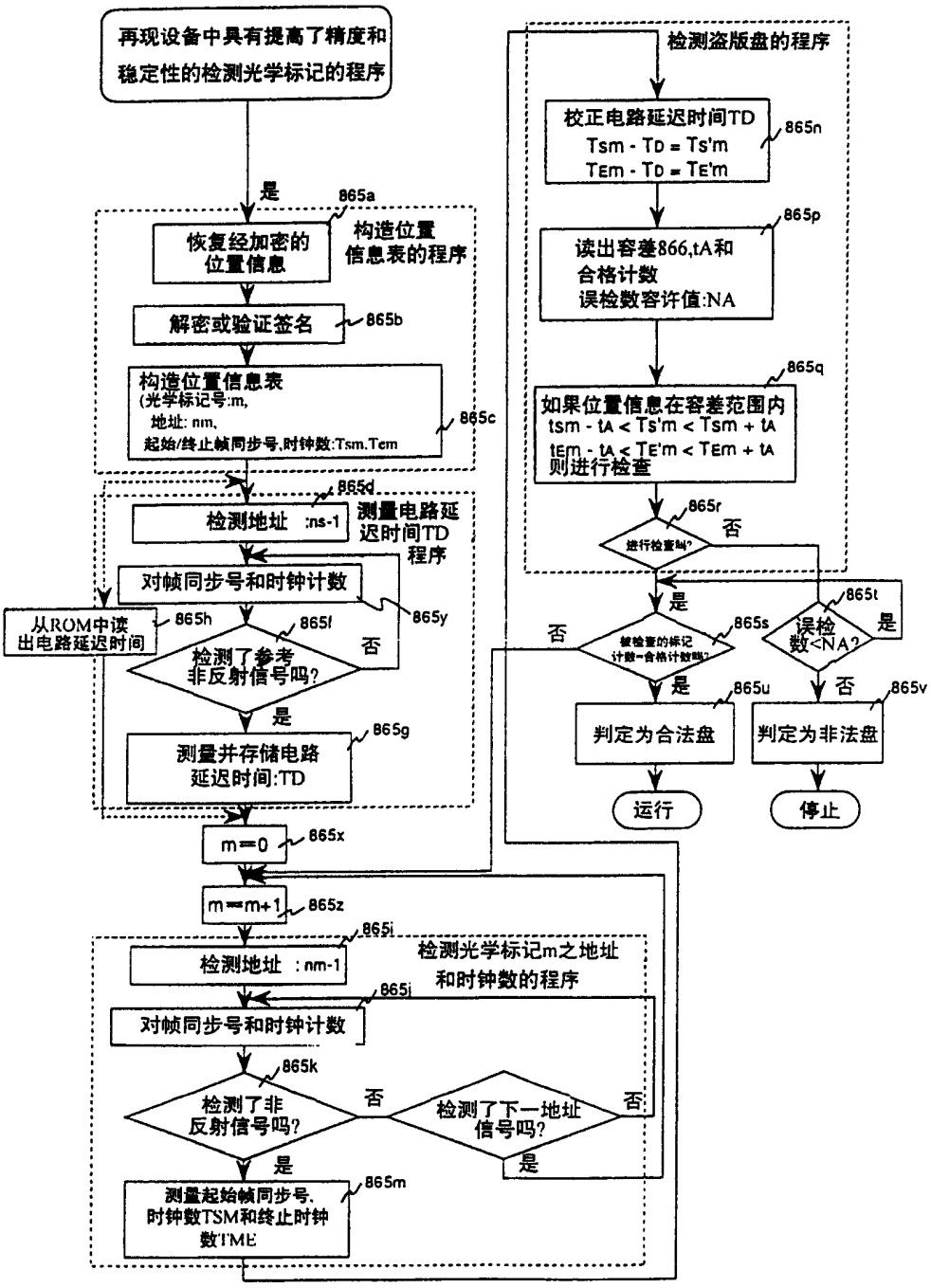

再现设备中具有提高了精度和稳定性的检测光学标记的程序
是
865a
恢复经加密的位置信息
构造位置信息表的程序
解密或验证签名
865b
构造位置信息表
(光学标记号:m,
地址: nm,
起始/终止帧同步号,时钟数:Tsm.Tem
865c
865d
检测地址 :ns-1
测量电路延迟时间TD程序
对帧同步号和时钟计数
865y
从ROM中读出电路延迟时间
865h
865f
检测了参考非反射信号吗?
否
是
测量并存储电路延迟时间:TD
865g
m=0
865x
m=m+1
865z
865i
检测地址 :nm-1
检测光学标记m之地址和时钟数的程序
865j
对帧同步号和时钟计数
865k
检测了非反射信号吗?
否
检测了下一地址信号吗?
否
是
测量起始帧同步号,时钟数TSM和终止时钟数TME
865m
检测盗版盘的程序
校正电路延迟时间TD
Tsm - TD = Ts'm
TEm - TD = TE'm
865n
读出容差866,tA和合格计数
误检数容许值:NA
865p
如果位置信息在容差范围内
tsm - tA < Ts'm < Tsm + tA
tEm - tA < TE'm < TEm + tA
则进行检查
865q
进行检查吗?
865r
否
是
被检查的标记计数=合格计数吗?
865s
否
是
误检数<NA?
865t
是
否
判定为合法盘
865u
判定为非法盘
865v
运行
停止

图 21

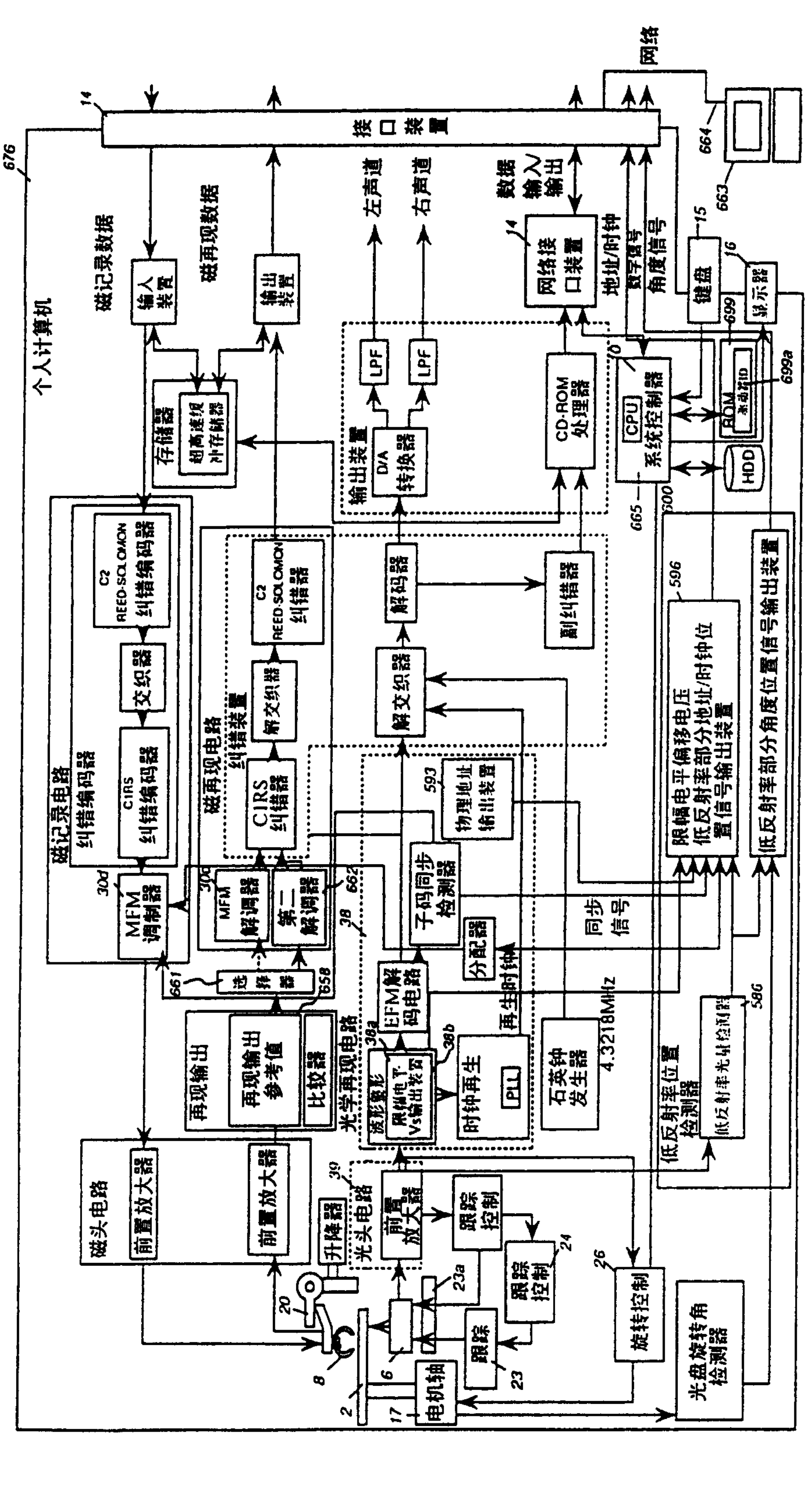

个人计算机
676
14
接口装置
网络
664
663
磁记录数据
磁再现数据
输入装置
输出装置
左声道
右声道
数据输入/输出
网络接口装置
地址/时钟
数字信号
角度信号
15
键盘
16
显示器
699
699a
ROM
CPU
系统控制器
HDD
665
600
存储器
超高速缓冲存储器
输出装置
D/A转换器
LPF
CD-ROM处理器
磁记录电路
纠错编码器
C2 REED-SOLOMON纠错编码器
交织器
C1RS纠错编码器
MFM调制器
30d
磁再现电路
纠错装置
C2 REED-SOLOMON纠错器
解交织器
C1RS纠错器
30c
MFM解调器
第二解调器
662
选择器
661
658
解码器
副纠错器
解交织器
593
物理地址输出装置
子码同步检测器
同步信号
分配器
再生时钟
EFM解码电路
38
38a
38b
光学再现电路
波形整形
限幅电平Vs输出装置
时钟再生
PLL
石英钟发生器
4.3218MHz
596
限幅电平偏移电压
低反射率部分地址/时钟位置信号输出装置
低反射率部分角度位置信号输出装置
低反射率位置检测器
低反射率光量检测器
586
再现输出
再现输出参考值
比较器
磁头电路
前置放大器
升降器
39
光头电路
前置放大器
跟踪控制
24
23a
跟踪
23
26
旋转控制
光盘旋转角检测器
20
8
6
2
17
电机轴

图 22

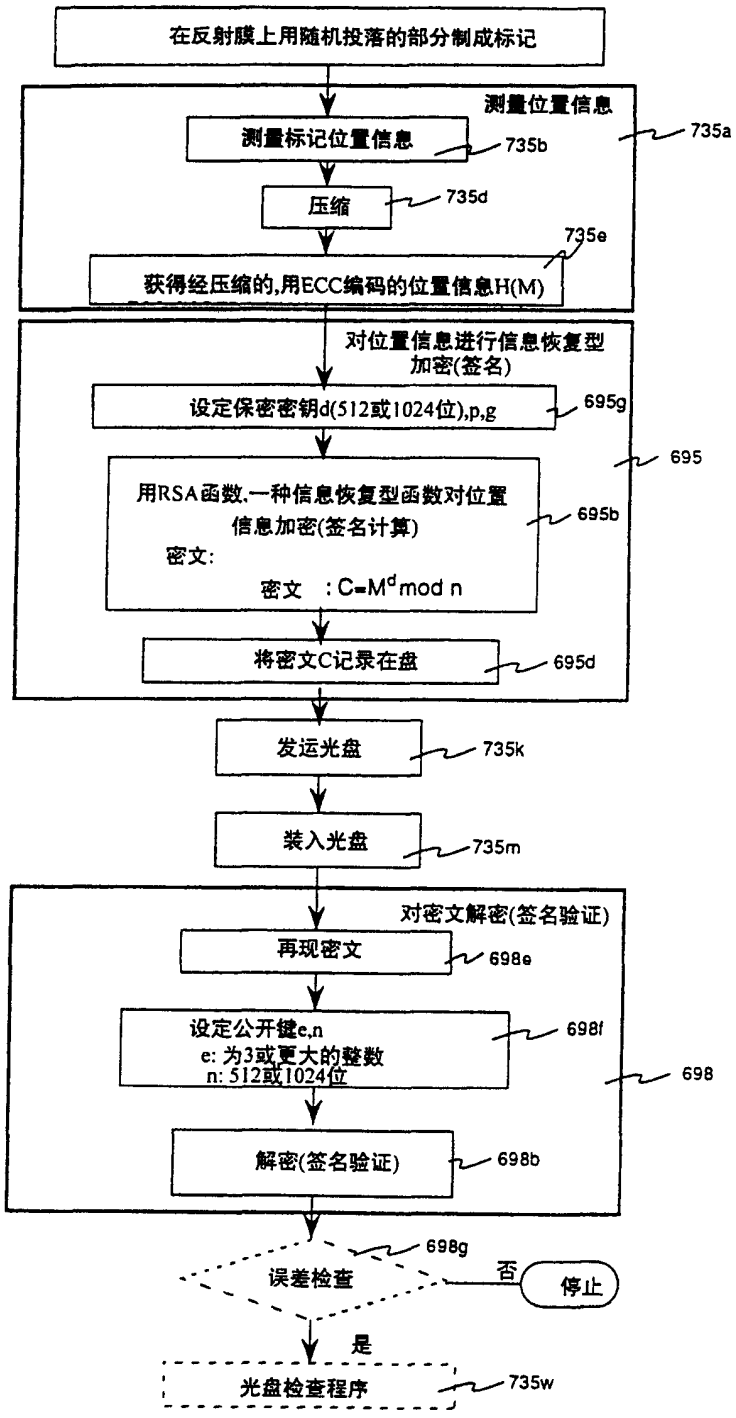

在反射膜上用随机投落的部分制成标记
测量位置信息
测量标记位置信息
735b
735a
压缩
735d
735e
获得经压缩的,用ECC编码的位置信息H(M)
对位置信息进行信息恢复型加密(签名)
设定保密密钥d(512或1024位),p,g
695g
695
用RSA函数,一种信息恢复型函数对位置信息加密(签名计算)
密文:
密文 : C=M^d mod n
695b
将密文C记录在盘
695d
发运光盘
735k
装入光盘
735m
对密文解密(签名验证)
再现密文
698e
设定公开键e,n
e: 为3或更大的整数
n: 512或1024位
698f
698
解密(签名验证)
698b
698g
误差检查
否
停止
是
光盘检查程序
735w

图 23

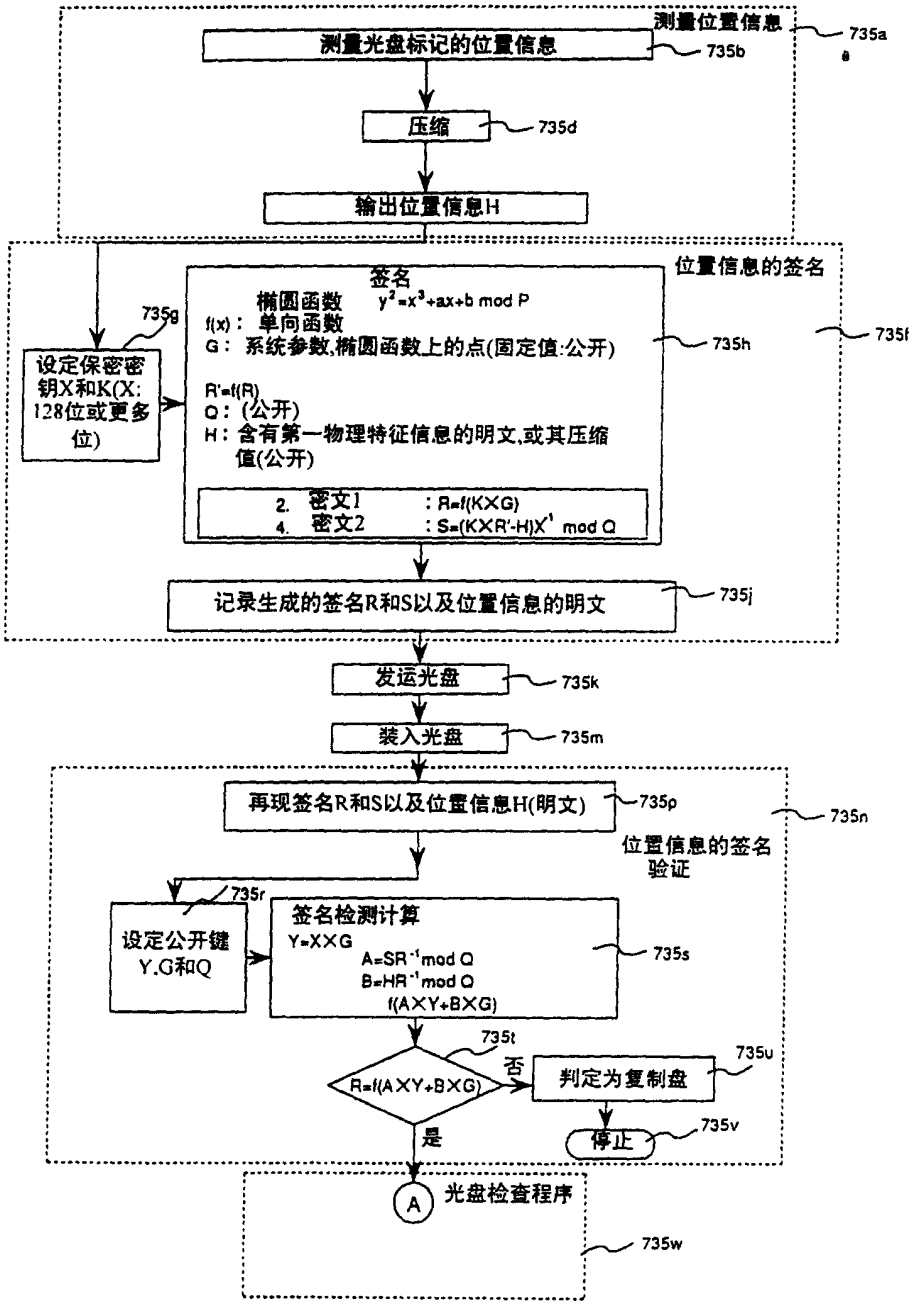

测量位置信息
735a
测量光盘标记的位置信息
735b
压缩
735d
输出位置信息H
位置信息的签名
735f
签名
椭圆函数 $y^2=x^3+ax+b \bmod P$
f(x)： 单向函数
G： 系统参数,椭圆函数上的点(固定值:公开)
735h
R'=f(R)
Q： (公开)
H： 含有第一物理特征信息的明文,或其压缩值(公开)
2. 密文1 ：R=f(K×G)
4. 密文2 ：$S=(K\times R'-H)X^{-1} \bmod Q$
735g
设定保密密钥X和K(X:128位或更多位)
记录生成的签名R和S以及位置信息的明文
735j
发运光盘
735k
装入光盘
735m
再现签名R和S以及位置信息H(明文)
735p
735n
位置信息的签名验证
735r
设定公开键Y.G和Q
签名检测计算
Y=X×G
$A=SR^{-1} \bmod Q$
$B=HR^{-1} \bmod Q$
f(A×Y+B×G)
735s
735t
R=f(A×Y+B×G)
否
判定为复制盘
735u
是
停止
735v
A
光盘检查程序
735w

图 24

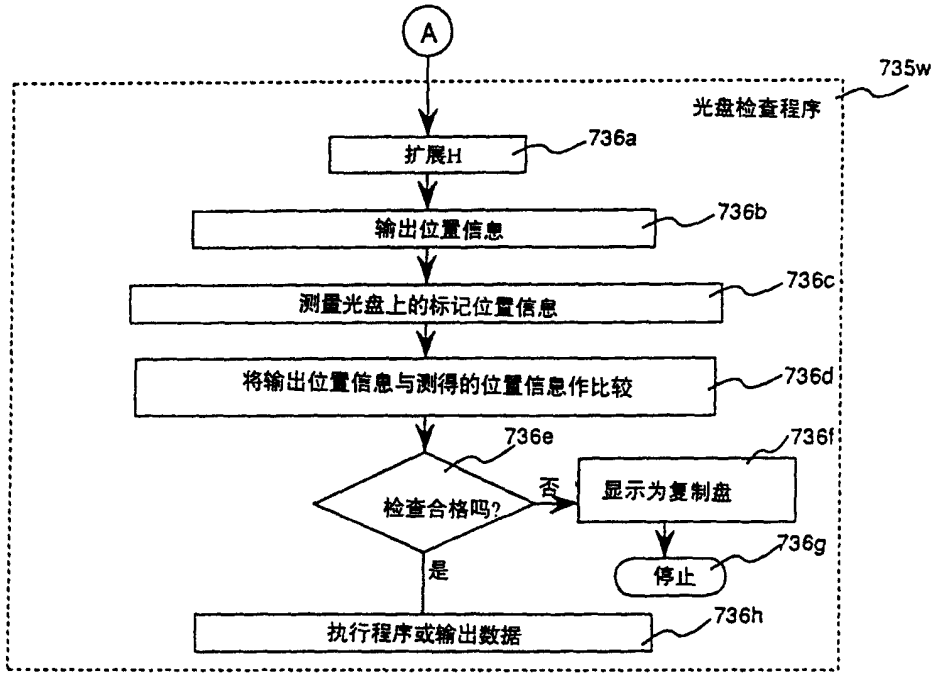
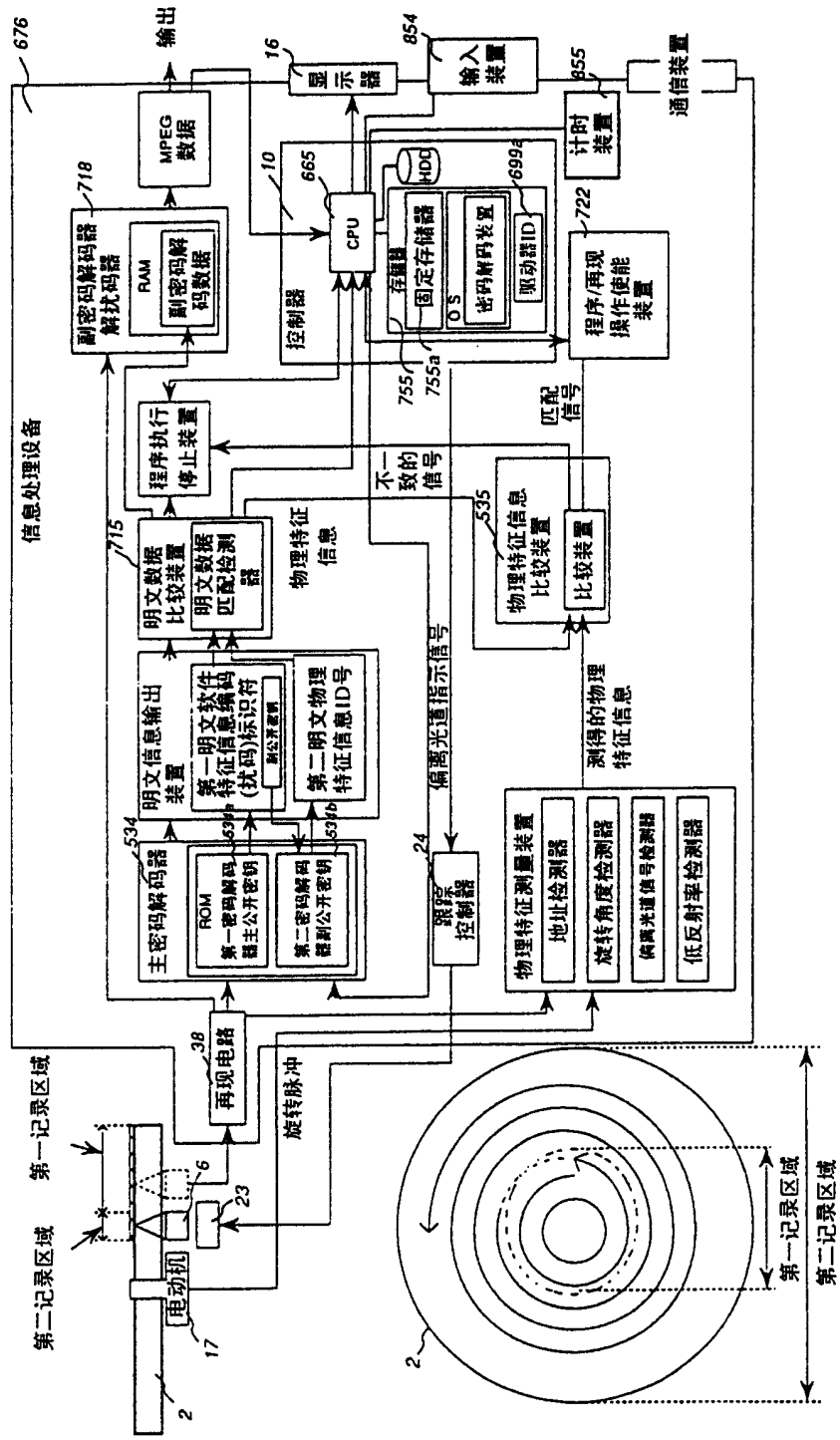

A
735w
光盘检查程序
扩展H
736a
输出位置信息
736b
测量光盘上的标记位置信息
736c
将输出位置信息与测得的位置信息作比较
736d
736e
检查合格吗?
否
736f
显示为复制盘
736g
停止
是
执行程序或输出数据
736h

图 25


676
信息处理设备
输出
MPEG数据
显示器
输入装置
通信装置
计时装置
副密码解码器解扰码器
RAM
副密码解码数据
718
控制器
CPU
HDD
存储器
固定存储器
OS
密码解码装置
驱动器ID
699a
程序/再现操作使能装置
722
程序执行停止装置
明文数据比较装置
明文数据匹配检测器
715
物理特征信息
755
755a
不一致的信号
匹配信号
物理特征信息比较装置
比较装置
535
明文信息输出装置
第一明文软件特征信息编码(扰码)标识符
第二明文物理特征信息ID号
639a
639b
主密码解码器
534
ROM
第一密码解码器主公开密钥
第二密码解码器副公开密钥
跟踪控制器
24
偏离光道指示信号
测得的物理特征信息
物理特征测量装置
地址检测器
旋转角度检测器
偏离光道信号检测器
低反射率检测器
再现电路
38
旋转脉冲
电动机
17
2
6
23
第一记录区域
第二记录区域
第一记录区域
第二记录区域

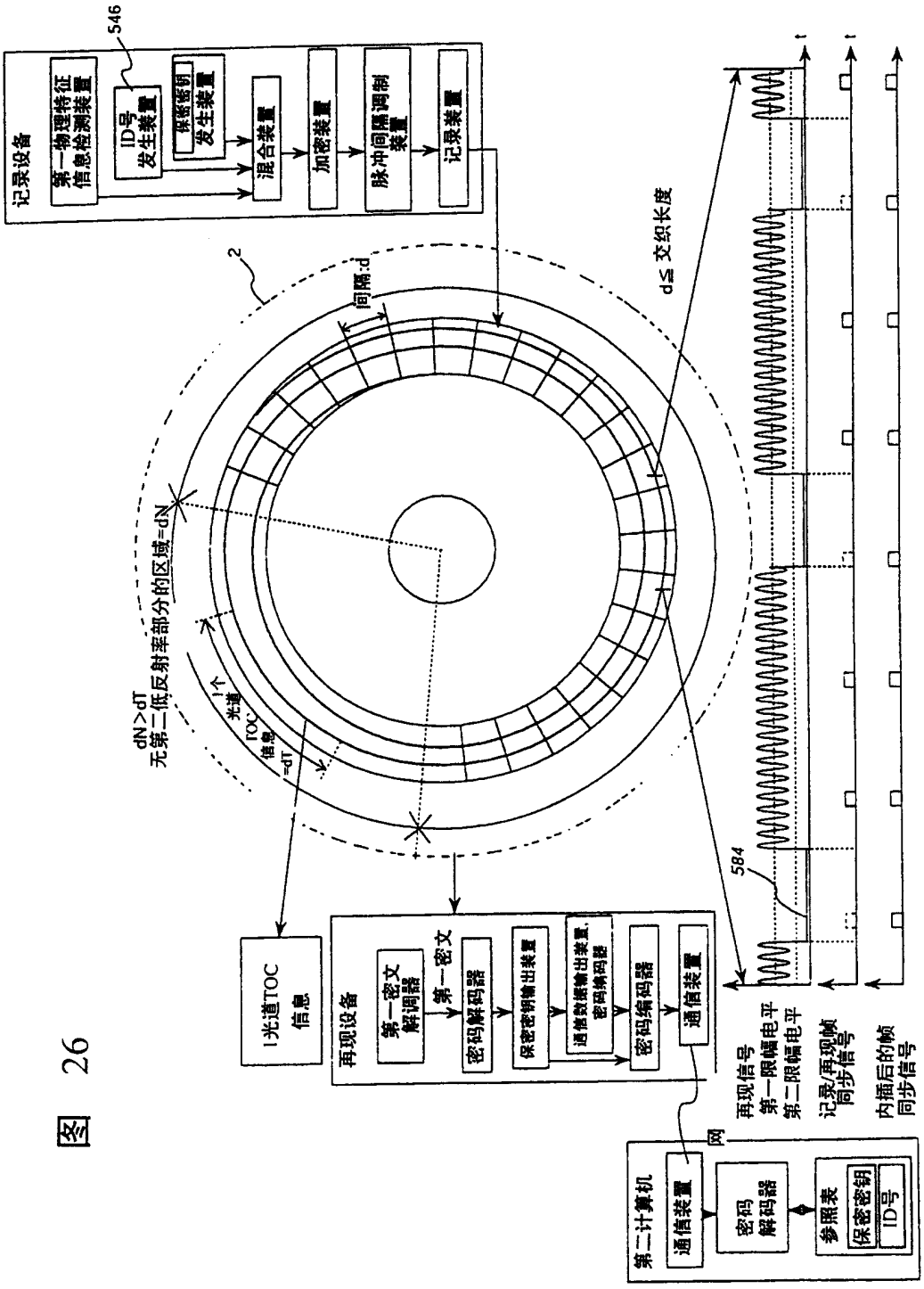

记录设备
第一物理特征信息检测装置
546
ID号发生装置
保密密钥发生装置
混合装置
加密装置
脉冲间隔调制装置
记录装置
2
间隔:d
d≤交织长度
dN>dT
无第二低反射率部分的区域=dN
1个光道TOC信息=dT
1光道TOC信息
再现设备
第一密文解调器
第一密文
密码解码器
保密密钥输出装置
通信数据输出装置,密码编码器
密码编码器
通信装置
584
网
第二计算机
通信装置
密码解码器
参照表
保密密钥
ID号
再现信号
第一限幅电平
第二限幅电平
记录/再现帧同步信号
内插后的帧同步信号

图 26

图 27

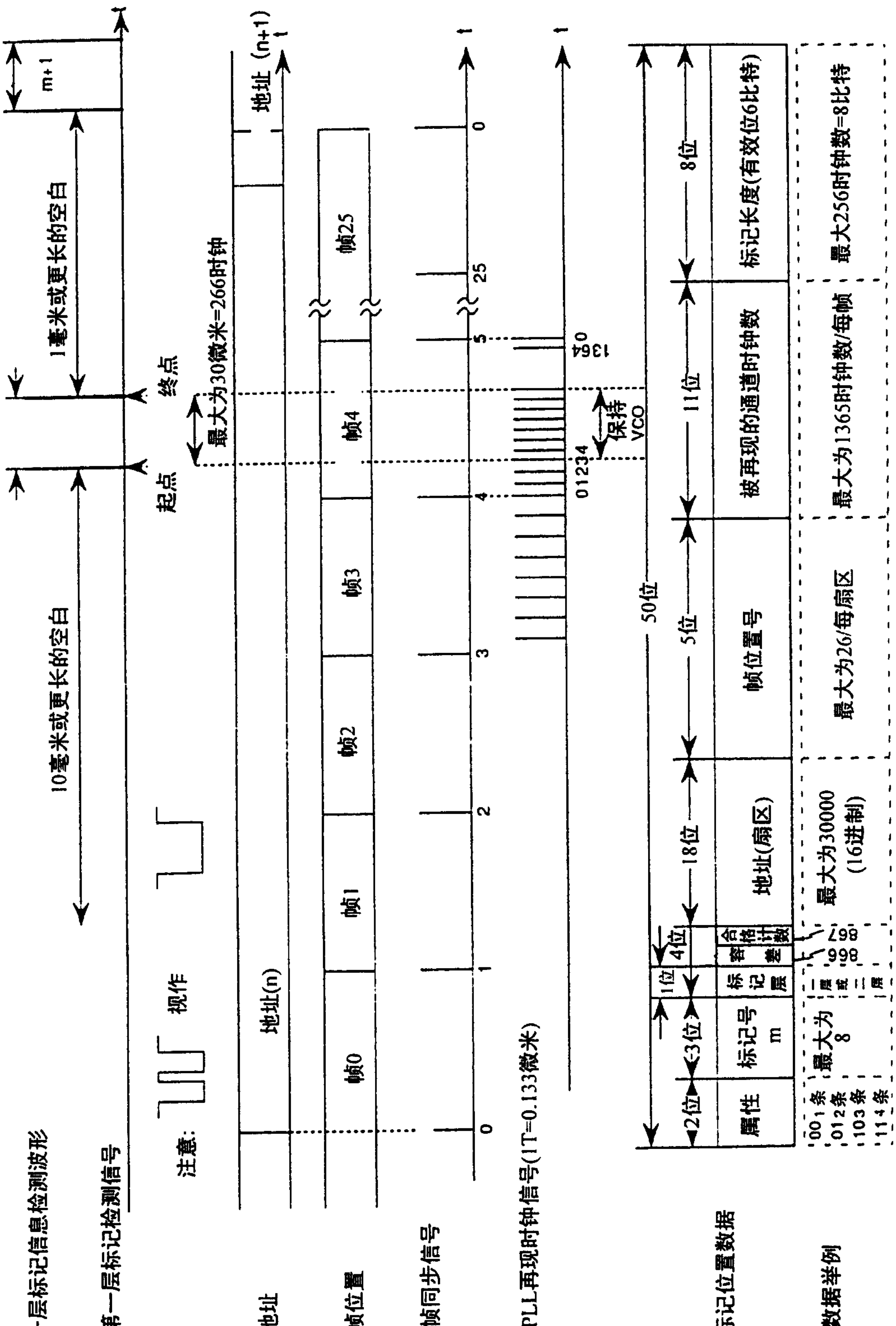

第一层标记信息检测波形
(1) 第一层标记检测信号
(2) 地址
(3) 帧位置
(4) 帧同步信号
(5) PLL再现时钟信号(1T=0.133微米)
(6) 标记位置数据
(7) 数据举例
标记号:m
下一标记
m+1
10毫米或更长的空白
1毫米或更长的空白
起点
终点
注意:
规作
地址(n)
地址(n+1)
最大为30微米=266时钟
帧0
帧1
帧2
帧3
帧4
帧25
0
1
2
3
4
5
25
01234
1364
保持
VCO
50位
2位
3位
1位
4位
18位
5位
11位
8位
属性
标记号 m
标记层
合格计数
地址(扇区)
帧位置号
被再现的通道时钟数
标记长度(有效位6比特)
最大为8
最大为30000 (16进制)
最大为26/每扇区
最大为1365时钟数/每帧
最大256时钟数=8比特

图 28

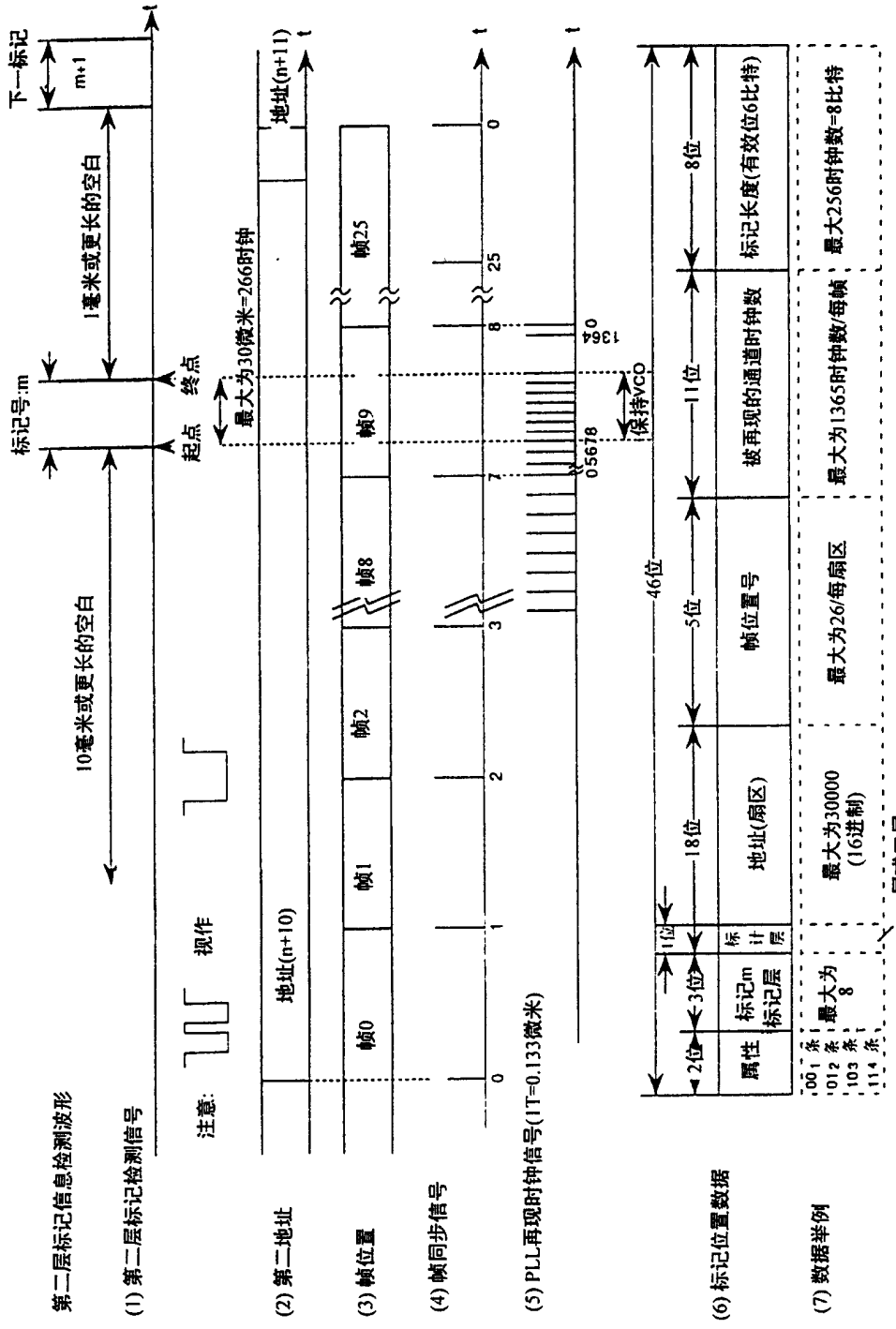

第二层标记信息检测波形
(1) 第二层标记检测信号
下一标记
m+1
1毫米或更长的空白
标记号:m
起点
终点
10毫米或更长的空白
注意:
现作
最大为30微米=266时钟
(2) 第二地址
地址(n+10)
地址(n+11)
(3) 帧位置
帧0
帧1
帧2
帧8
帧9
帧25
(4) 帧同步信号
(5) PLL再现时钟信号(1T=0.133微米)
保持VCO
46位
(6) 标记位置数据
2位
3位
1位
18位
5位
11位
8位
属性
标记m
标记层
标记层
地址(扇区)
帧位置号
被再现的通道时钟数
标记长度(有效位6比特)
(7) 数据举例
最大为8
最大为30000
(16进制)
最大为26/每扇区
最大为1365时钟数/每帧
最大256时钟数=8比特
一层或二层

图 29

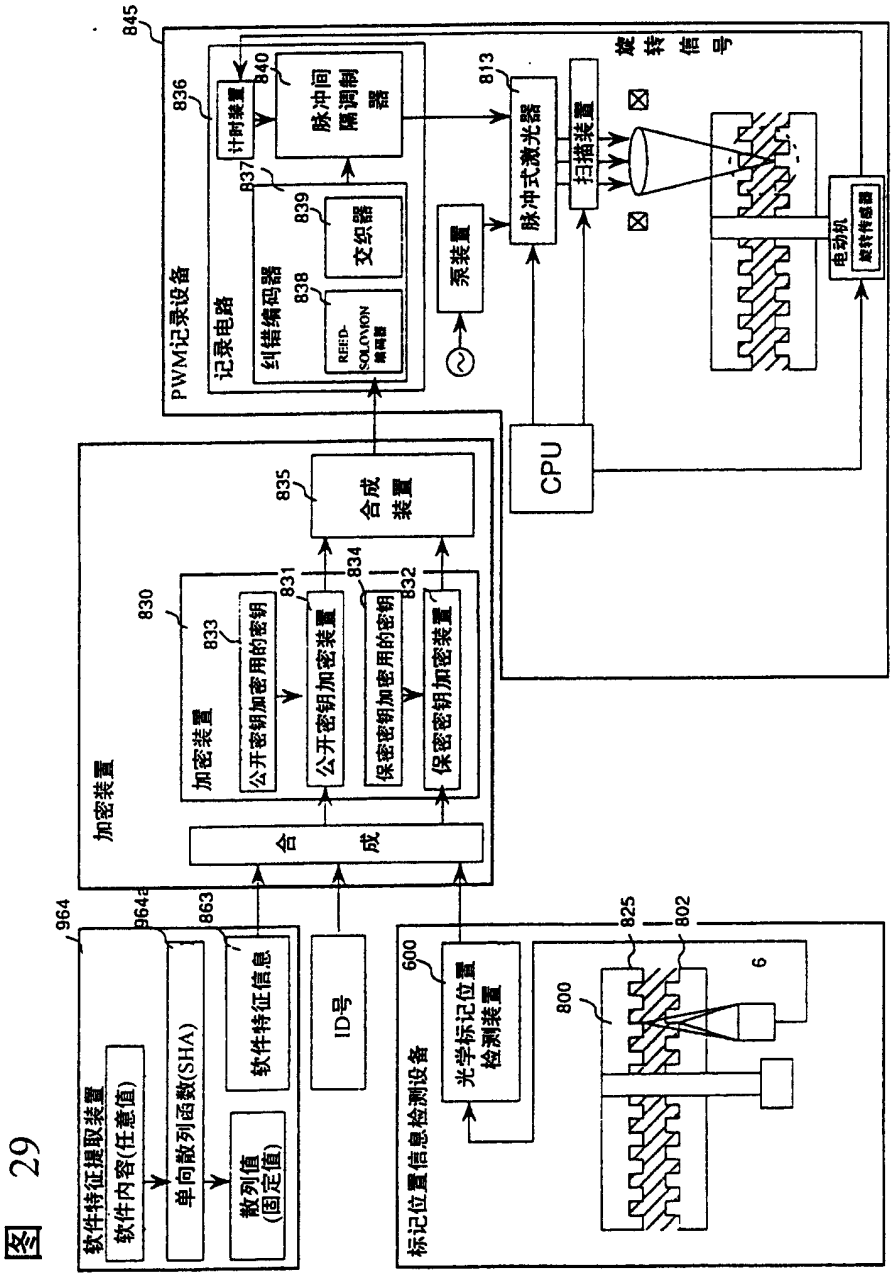

软件特征提取装置
软件内容(任意值)
单向散列函数(SHA)
散列值(固定值)
软件特征信息
ID号
964
964a
863
加密装置
合 成
加密装置
公开密钥加密用的密钥
公开密钥加密装置
保密密钥加密用的密钥
保密密钥加密装置
830
831
832
833
834
合成装置
835
PWM记录设备
记录电路
纠错编码器
REED-SOLOMON
交织器
计时装置
脉冲间隔调制器
836
837
838
839
840
845
泵装置
CPU
脉冲式激光器
扫描装置
旋转信号
电动机
旋转传感器
813
标记位置信息检测设备
光学标记位置检测装置
600
800
825
802
6

图 30

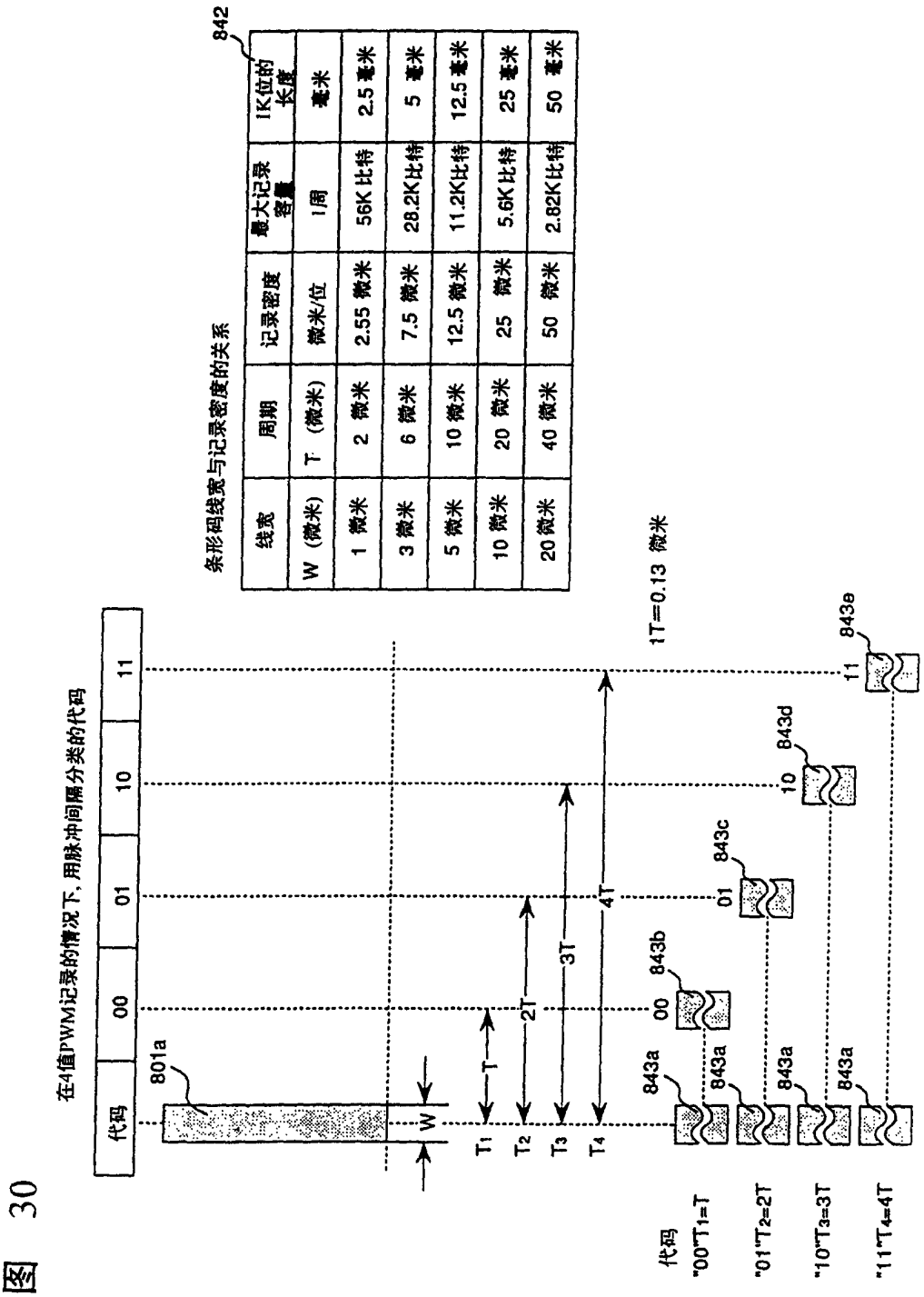
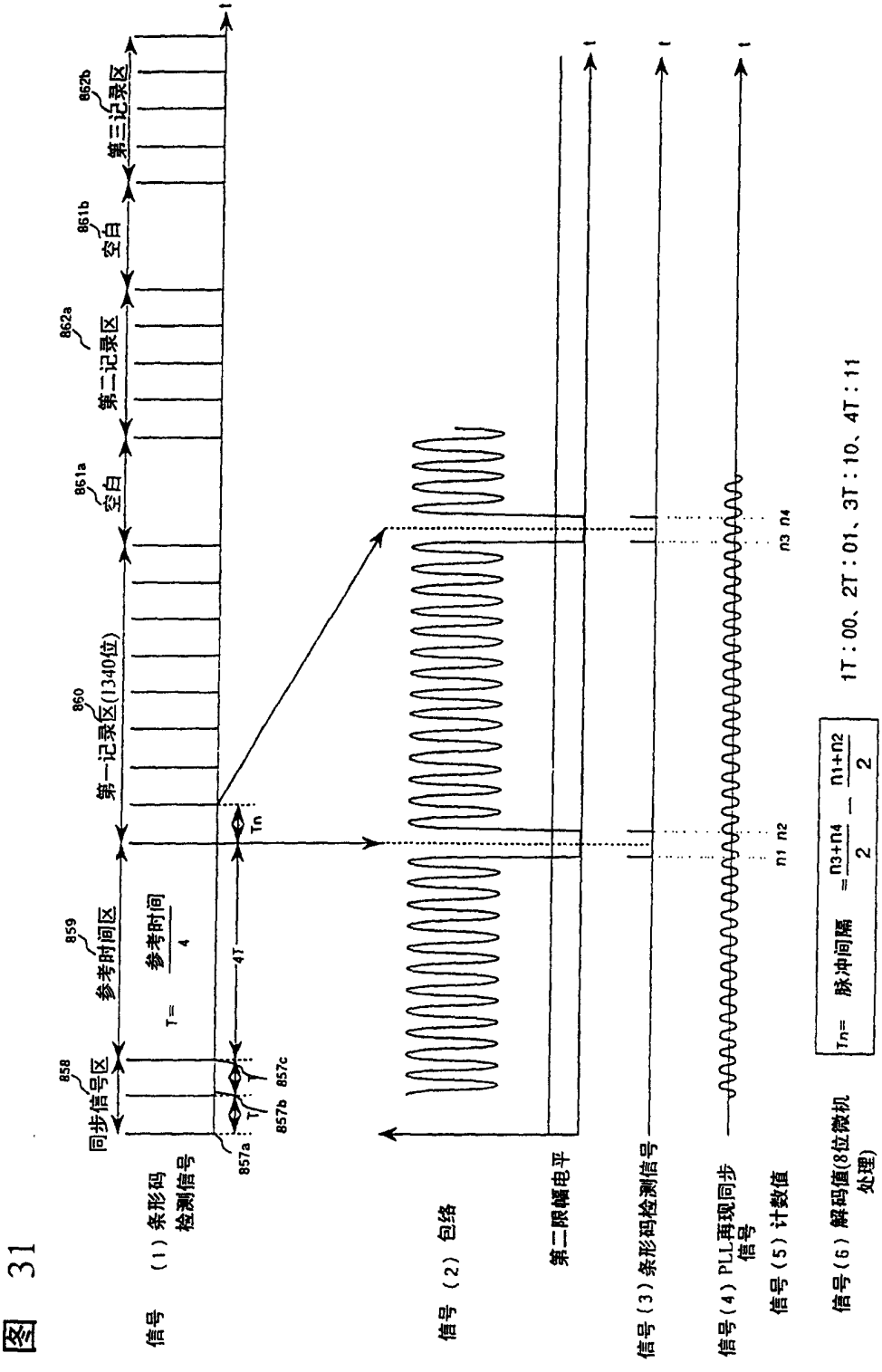

842
条形码线宽与记录密度的关系
线宽 W（微米）
周期 T（微米）
记录密度 微米/位
最大记录容量 1周
1K位的长度 毫米
1 微米 2 微米 2.55 微米 56K 比特 2.5 毫米
3 微米 6 微米 7.5 微米 28.2K比特 5 毫米
5 微米 10 微米 12.5 微米 11.2K比特 12.5 毫米
10 微米 20 微米 25 微米 5.6K比特 25 毫米
20 微米 40 微米 50 微米 2.82K比特 50 毫米
在4值PWM记录的情况下，用脉冲间隔分类的代码
代码
00
01
10
11
801a
W
T
2T
3T
4T
T1
T2
T3
T4
1T=0.13 微米
843a
843b
843c
843d
843e
代码
"00"T1=T
"01"T2=2T
"10"T3=3T
"11"T4=4T

图 31


信号 (1) 条形码检测信号
同步信号区
858
参考时间区
859
T= 参考时间 / 4
4T
第一记录区(1340位)
860
空白
861a
第二记录区
862a
空白
861b
第三记录区
862b
Tn
857a
857b
857c
信号 (2) 包络
第二限幅电平
信号(3)条形码检测信号
信号(4) PLL再现同步信号
信号(5)计数值
n1 n2
n3 n4
信号(6)解码值(8位微机处理)
Tn= 脉冲间隔 = (n3+n4)/2 − (n1+n2)/2
1T : 00、2T : 01、3T : 10、4T : 11
t

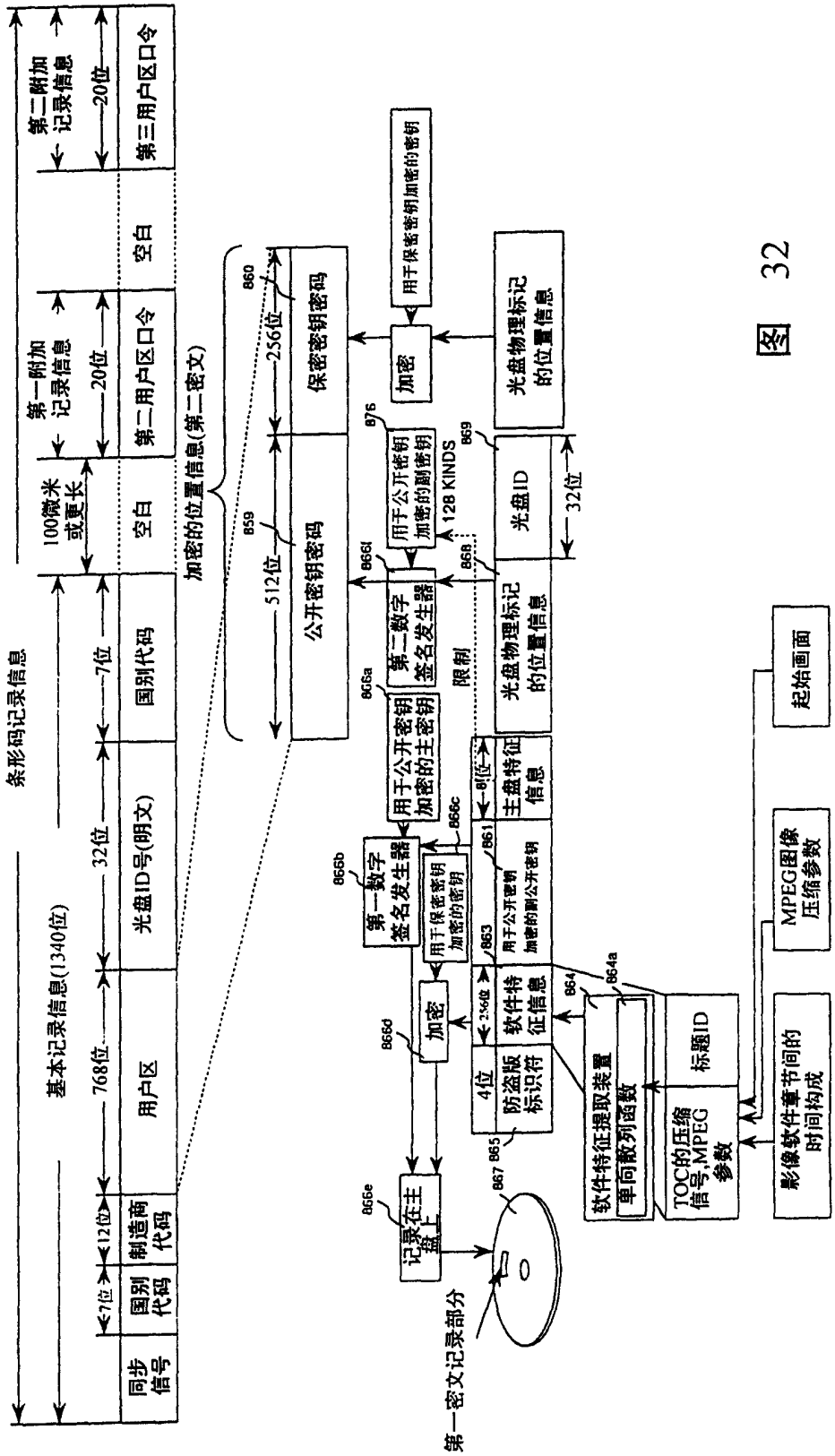

条形码记录信息
基本记录信息(1340位)
同步信号
7位
国别代码
制造商代码
12位
用户区
768位
光盘ID号(明文)
32位
国别代码
7位
空白
100微米或更长
第一附加记录信息
20位
第二用户区口令
空白
第二附加记录信息
20位
第三用户区口令
加密的位置信息(第二密文)
860
256位
保密密钥密码
859
512位
公开密钥密码
866l
用于公开密钥加密的副密钥
876
用于保密密钥加密的密钥
加密
光盘物理标记的位置信息
128 KINDS
869
光盘ID
32位
868
光盘物理标记的位置信息
限制
866a
用于公开密钥加密的主密钥
第二数字签名发生器
866b
第一数字签名发生器
866c
用于保密密钥加密的密钥
加密
866d
866e
记录在主盘上
867
865
防盗版标识符
4位
256位
863
软件特征信息
用于公开密钥加密的副公开密钥
861
主盘特征信息
81位
864
软件特征提取装置
单向散列函数
TOC的压缩信号,MPEG参数
标题ID
影像软件章节间的时间构成
MPEG图像压缩参数
起始画面
第一密文记录部分

图 32

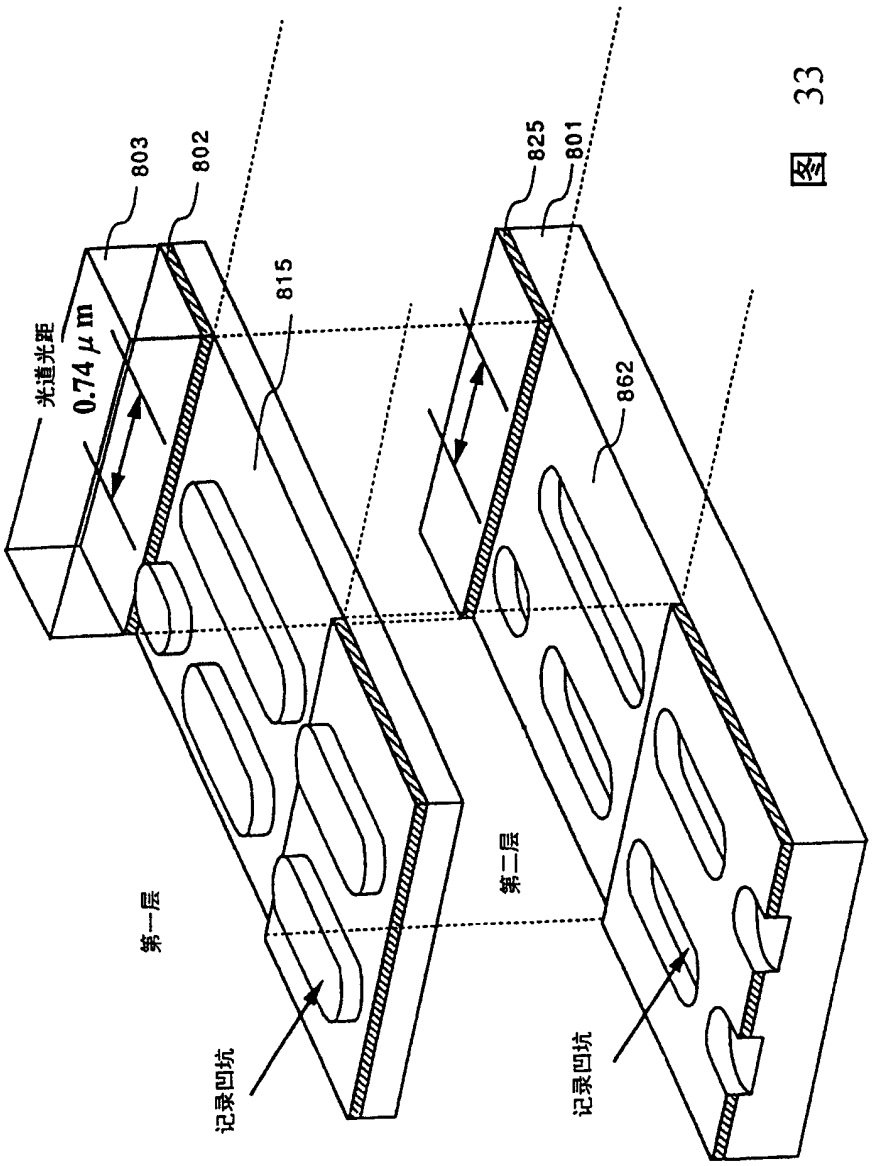


图 33

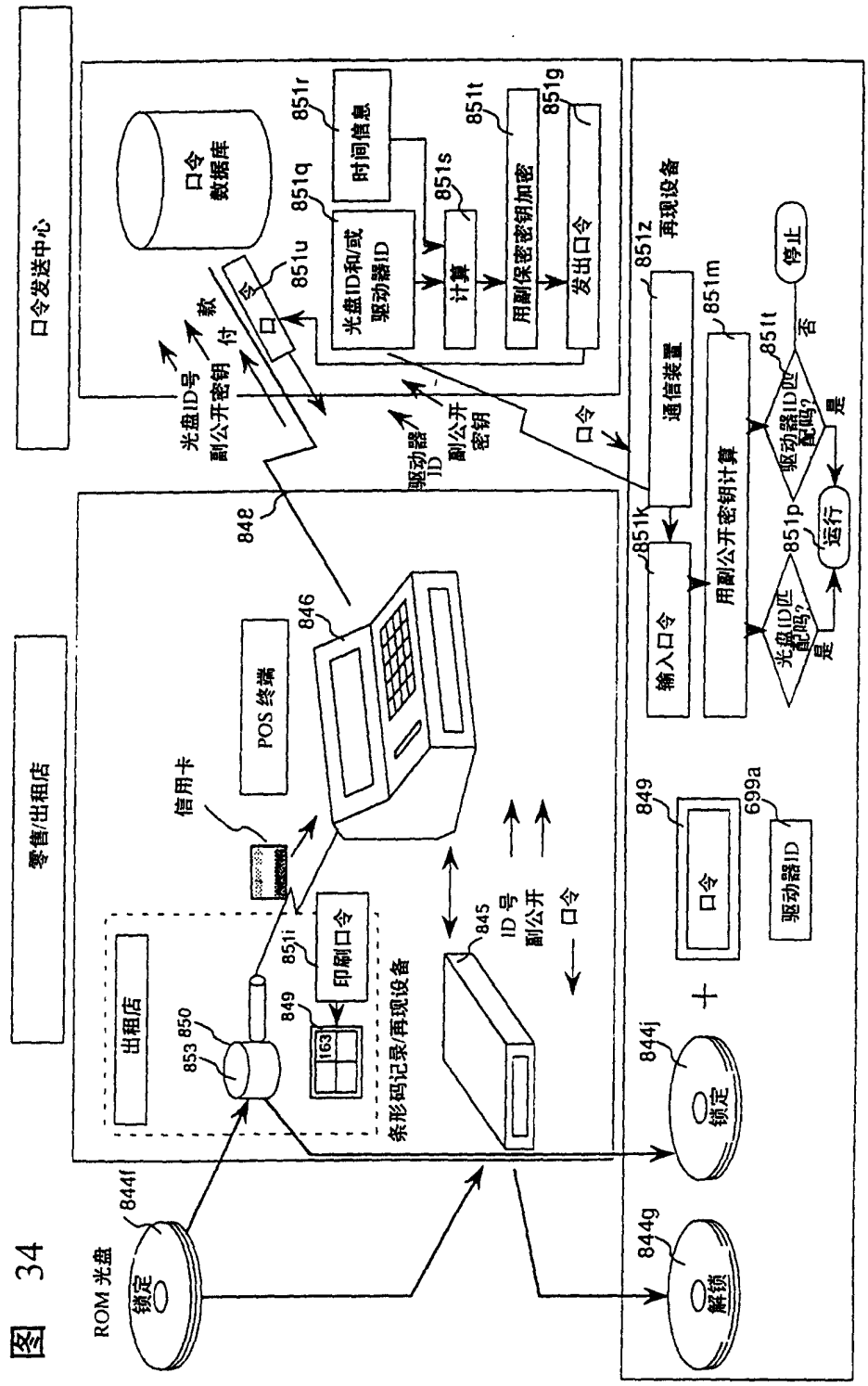

口令发送中心
口令数据库
851r
时间信息
851q
光盘ID和/或驱动器ID
851s
计算
851t
用副保密密钥加密
851g
发出口令
851u
口令
光盘ID号
副公开密钥
款
付
驱动器ID
副公开密钥
口令
848
零售/出租店
POS 终端
846
信用卡
出租店
853
850
849
851i
印刷口令
163
条形码记录/再现设备
845
ID号
副公开
口令
849
口令
699a
驱动器ID
844j
锁定
844l
ROM 光盘
锁定
844g
解锁
851z
再现设备
通信装置
851m
用副公开密钥计算
851k
输入口令
851p
光盘ID匹配吗?
是
运行
851t
驱动器ID匹配吗?
否
停止
是

图 34

图 35

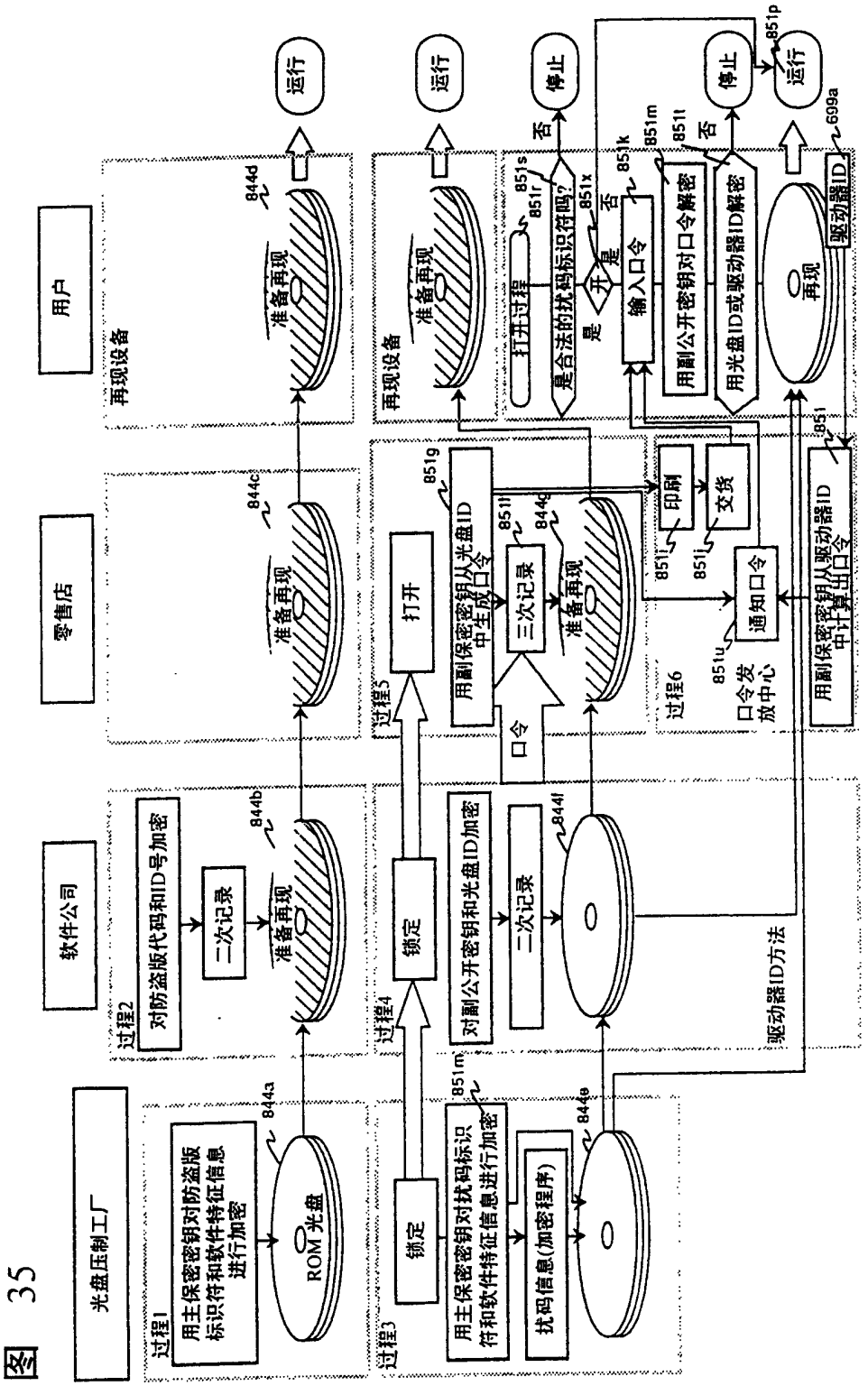
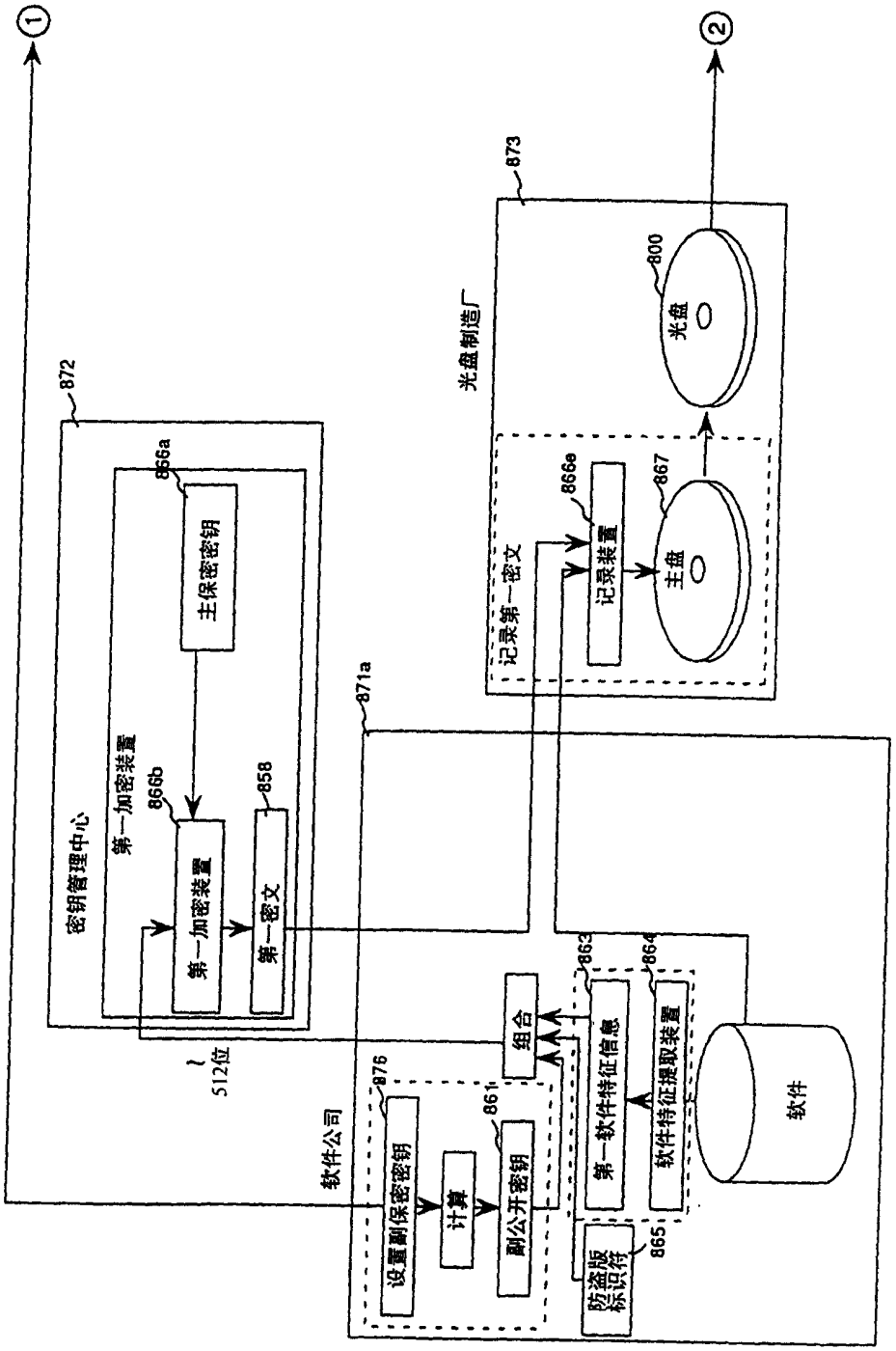

光盘压制工厂
软件公司
零售店
用户
过程1
用主保密密钥对防盗版标识符和软件特征信息进行加密
ROM光盘
844a
过程2
对防盗版代码和ID号加密
二次记录
准备再现
844b
844c
844d
再现设备
运行
过程3
锁定
用主保密密钥对扰码标识符和软件特征信息进行加密
扰码信息(加密程序)
851m
844e
过程4
锁定
打开
对副公开密钥和光盘ID加密
二次记录
844f
过程5
用副保密密钥从光盘ID中生成口令
851g
三次记录
851l
844g
准备再现
口令
打开过程
851r
851s
是合法的扰码标识符吗?
851x
开
是
否
停止
输入口令
851k
用副公开密钥对口令解密
851m
用光盘ID或驱动器ID解密
851l
过程6
印刷
851t
交货
851i
通知口令
851u
口令发放中心
再现
851p
运行
驱动器ID
699a
用副保密密钥从驱动器ID中计算出口令
851l
驱动器ID方法

图 36


①
②
872
密钥管理中心
第一加密装置
866a
主保密密钥
866b
第一加密装置
858
第一密文
512位
871a
软件公司
876
设置副保密密钥
计算
861
副公开密钥
组合
863
第一软件特征信息
864
软件特征提取装置
865
防盗版标识符
软件
873
光盘制造厂
记录第一密文
866e
记录装置
867
主盘
800
光盘

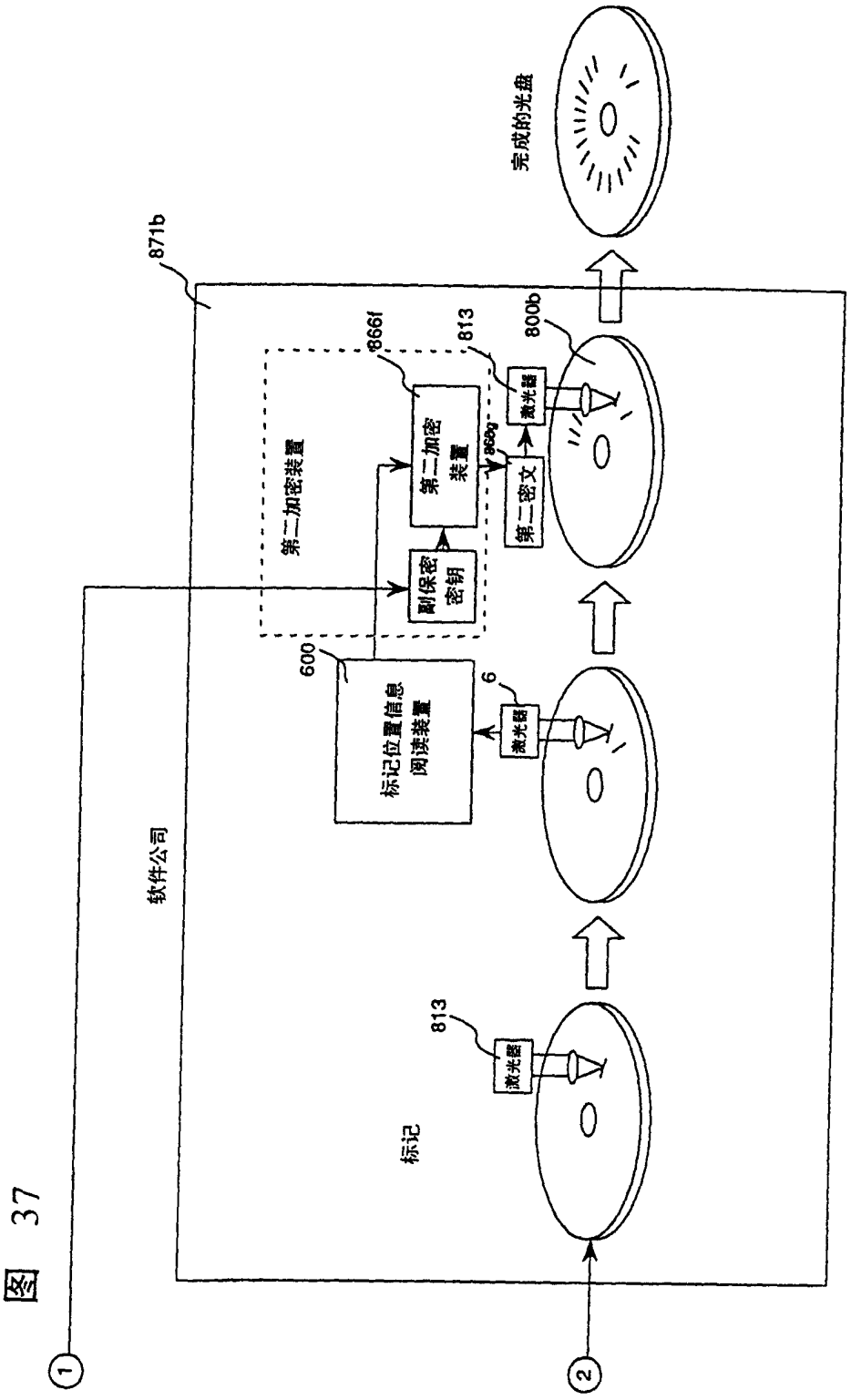

完成的光盘
871b
800b
813
866f
第二加密装置
第二加密装置
激光器
第二密文
866g
副保密密钥
600
标记位置信息阅读装置
6
激光器
813
激光器
软件公司
标记
1
2

图 37

图 38

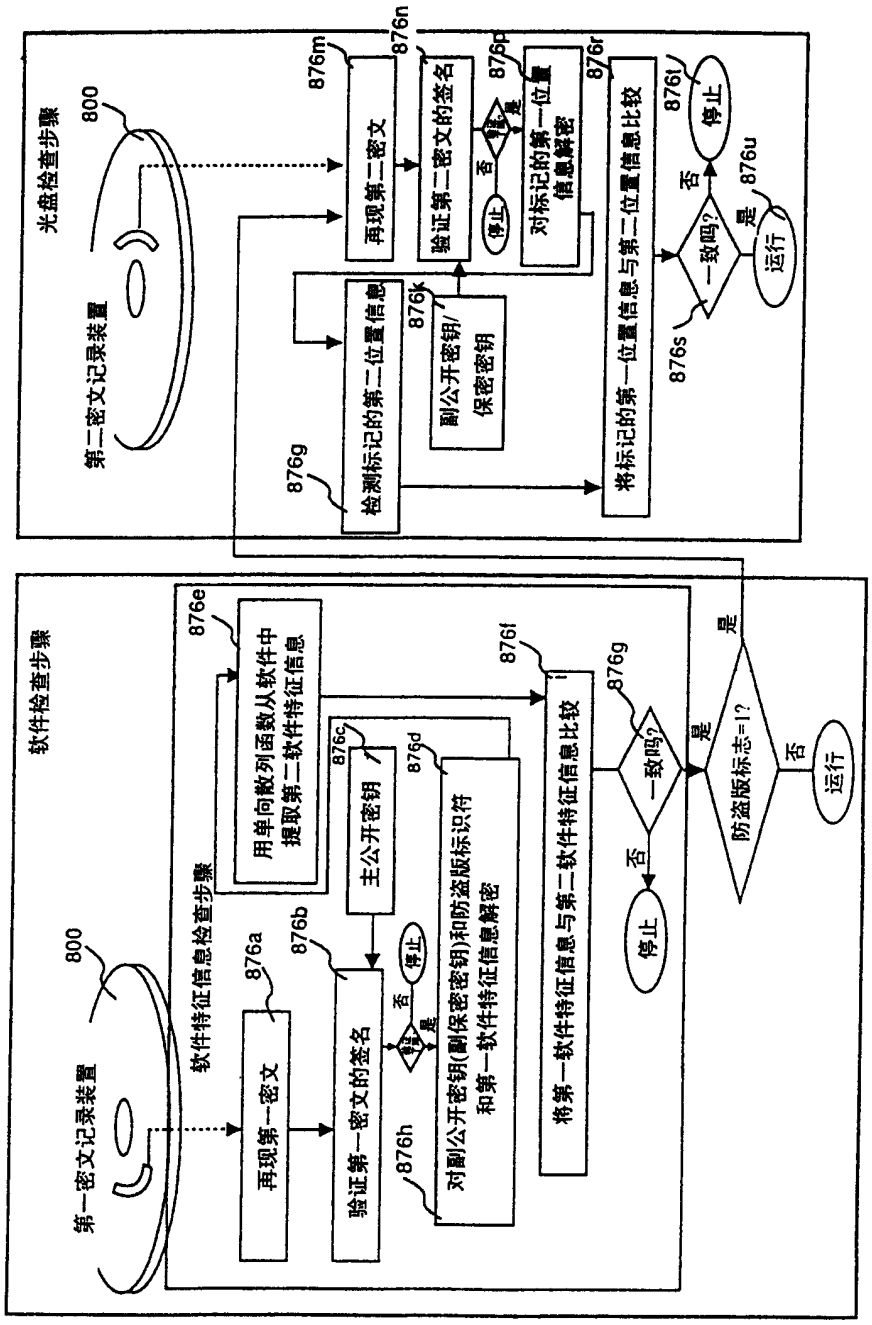

光盘检查步骤
800
第二密文记录装置
876m
再现第二密文
876n
验证第二密文的签名
876p
对标记的第一位置信息解密
876r
将标记的第一位置信息与第二位置信息比较
876l
停止
876u
运行
876s
一致吗?
否
是
停止
876k
副公开密钥/保密密钥
876g
检测标记的第二位置信息
软件检查步骤
800
第一密文记录装置
软件特征信息检查步骤
876a
再现第一密文
876b
验证第一密文的签名
否
是
停止
876h
对副公开密钥(副保密密钥)和防盗版标识符和第一软件特征信息解密
876c
主公开密钥
876e
用单向散列函数从软件中提取第二软件特征信息
876f
将第一软件特征信息与第二软件特征信息比较
876g
一致吗?
否
停止
是
防盗版标志=1?
是
否
运行

图 39

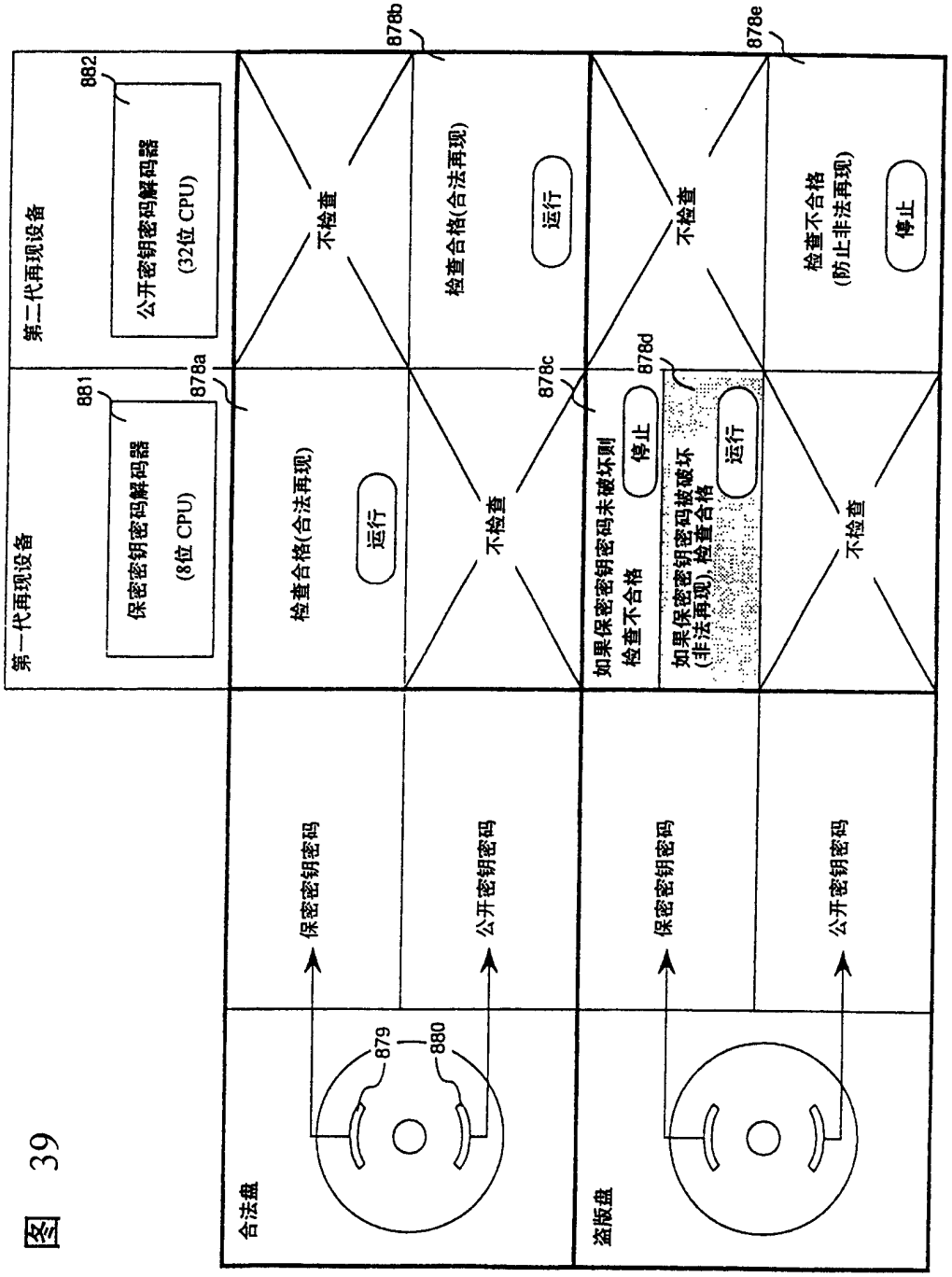

第一代再现设备
第二代再现设备
保密密钥密码解码器
(8位 CPU)
881
公开密钥密码解码器
(32位 CPU)
882
878a
878b
878c
878d
878e
检查合格(合法再现)
运行
不检查
检查合格(合法再现)
运行
如果保密密钥密码未被坏则
检查不合格
停止
如果保密密钥密码被破坏
(非法再现),检查合格
运行
不检查
检查不合格
(防止非法再现)
停止
不检查
合法盘
盗版盘
879
880
保密密钥密码
公开密钥密码
保密密钥密码
公开密钥密码

图 40

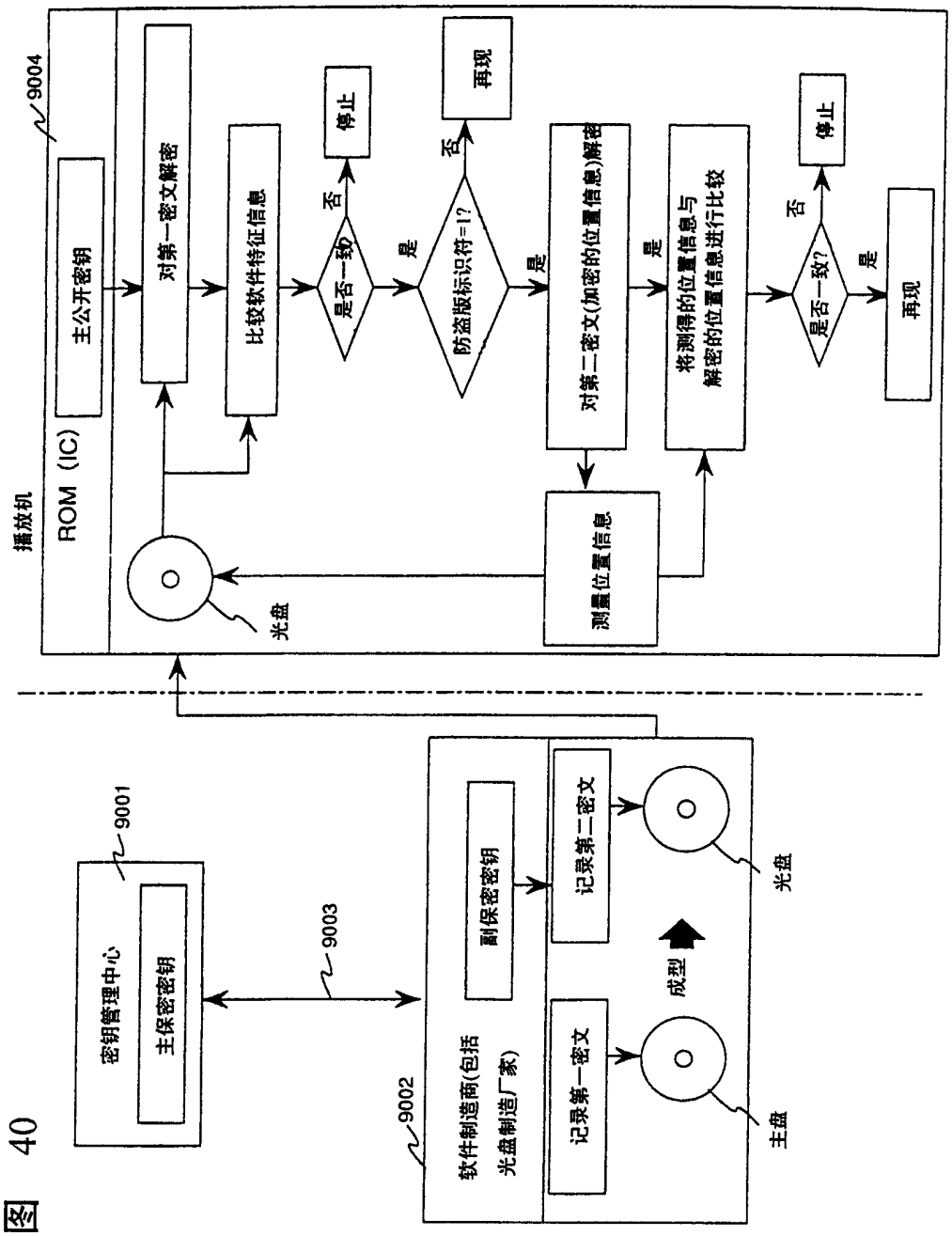
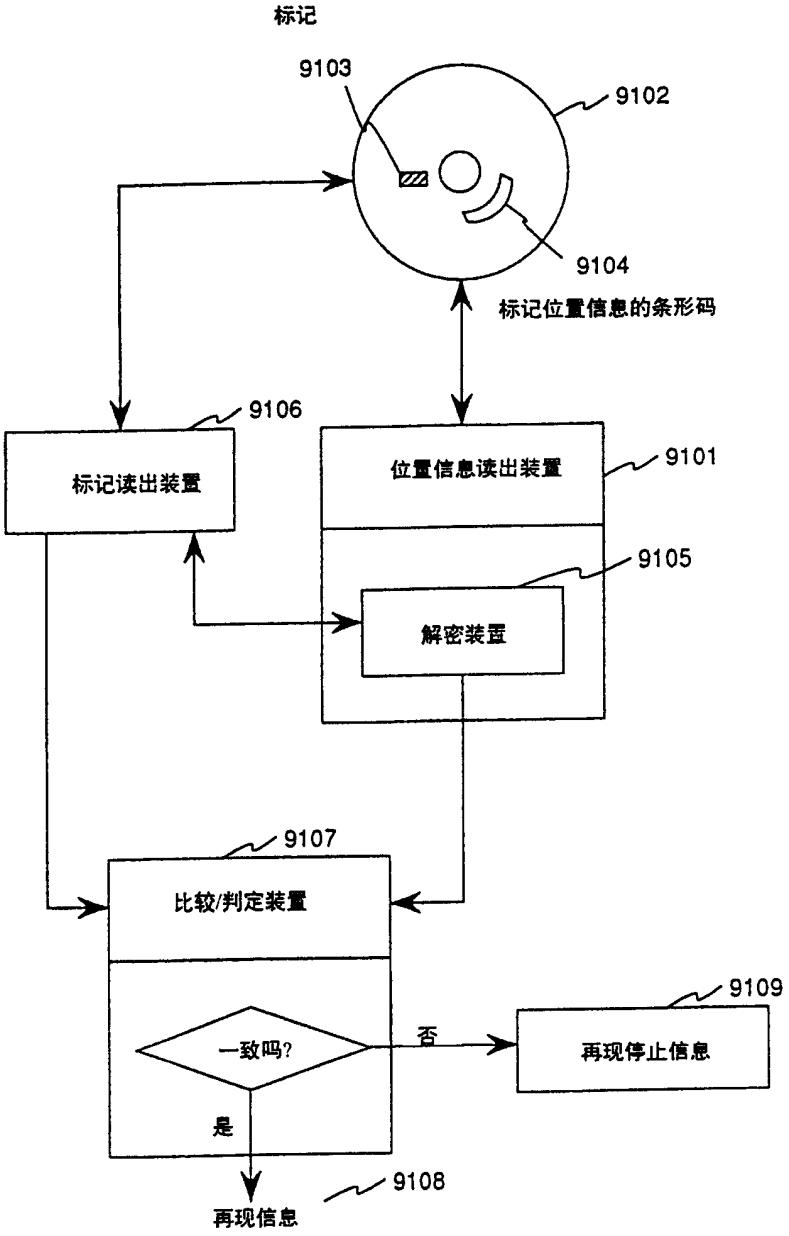

播放机
ROM (IC)
9004
主公开密钥
对第一密文解密
比较软件特征信息
是否一致
否
停止
是
防盗版标识符=1?
否
再现
是
对第二密文(加密的位置信息)解密
是
将测得的位置信息与
解密的位置信息进行比较
是否一致?
否
停止
是
再现
光盘
测量位置信息
密钥管理中心
9001
主保密密钥
9003
软件制造商(包括
光盘制造厂家)
9002
副保密密钥
记录第一密文
记录第二密文
成型
主盘
光盘

图 41


标记
9103
9102
9104
标记位置信息的条形码
9106
标记读出装置
位置信息读出装置
9101
9105
解密装置
9107
比较/判定装置
一致吗?
否
9109
再现停止信息
是
9108
再现信息

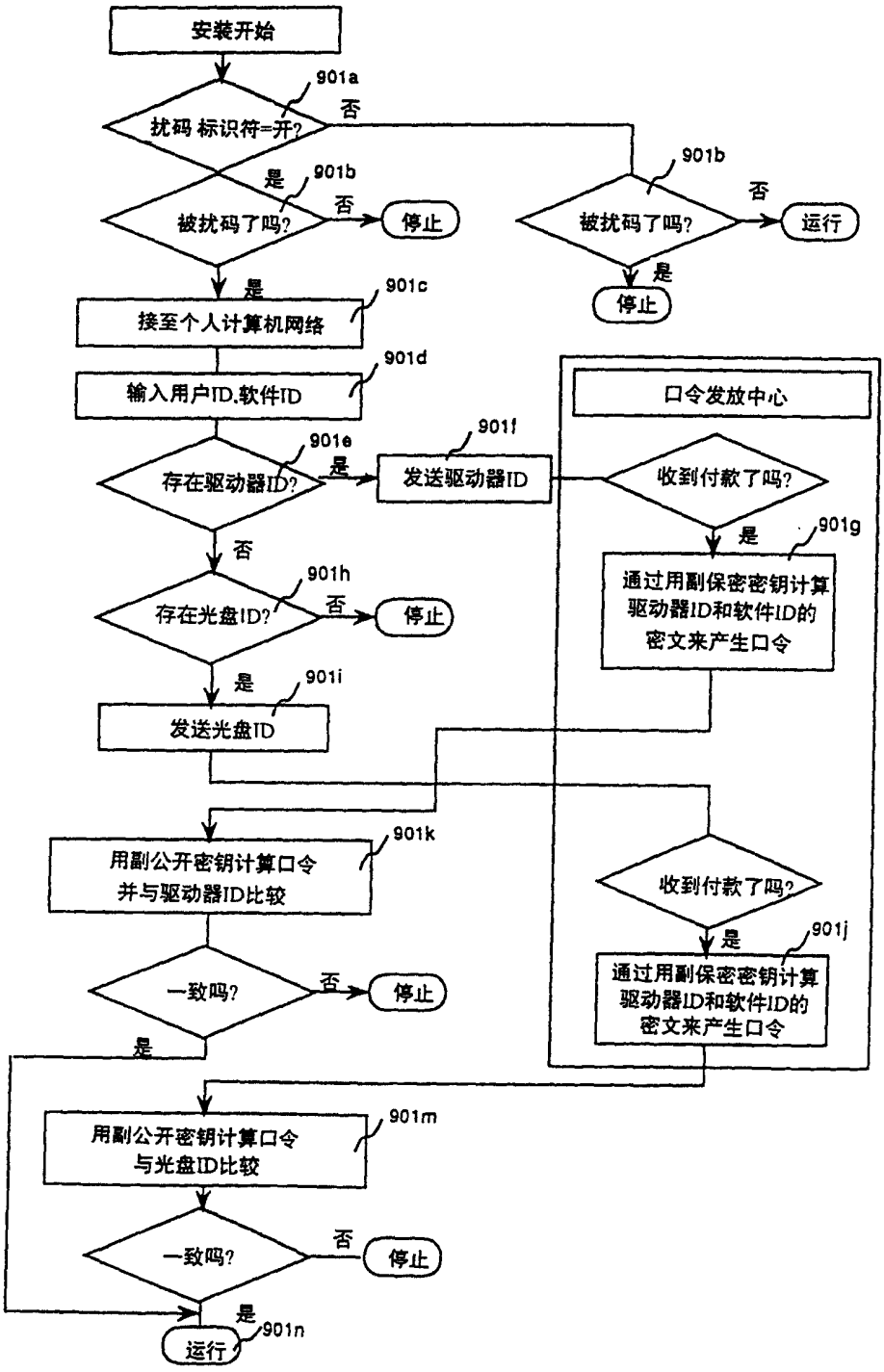

安装开始
901a
扰码 标识符=开?
否
是
901b
被扰码了吗?
否
停止
是
901c
接至个人计算机网络
901d
输入用户ID,软件ID
901e
存在驱动器ID?
是
901f
发送驱动器ID
否
901h
存在光盘ID?
否
停止
是
901i
发送光盘ID
901k
用副公开密钥计算口令
并与驱动器ID比较
一致吗?
否
停止
是
901m
用副公开密钥计算口令
与光盘ID比较
一致吗?
否
停止
是
运行
901n
901b
被扰码了吗?
否
运行
是
停止
口令发放中心
收到付款了吗?
是
901g
通过用副保密密钥计算
驱动器ID和软件ID的
密文来产生口令
收到付款了吗?
是
901j
通过用副保密密钥计算
驱动器ID和软件ID的
密文来产生口令

图 42