[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 9/00

[12]发明专利申请公开说明书

[21]申请号 01145473.3

[43]公开日 2002年7月10日

[11]公开号 CN 1357992A

[22]申请日 2001.12.5 [21]申请号 01145473.3
[30]优先权
[32]2000.12.5 [33]JP [31]374698/00
[71]申请人 索尼公司
地址 日本东京都
[72]发明人 阿部三树 吉田忠雄

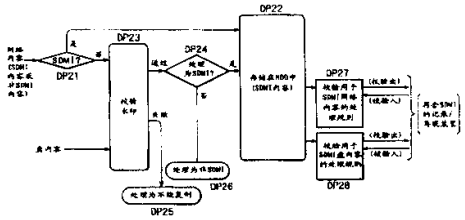
[74]专利代理机构 北京市柳沈律师事务所
代理人 马 莹 邵亚丽

权利要求书6页 说明书27页 附图页数9页

[54]发明名称 数据传输系统、装置和方法及数据记录装置和记录介质

[57]摘要

符合SDMI的可移动介质和非符合SDMI的可移动介质能有选择地连接到被许可的相符组件。当从许可的相符组件传输受版权保护的加密内容数据时，确定传输的目标是符合SDMI的可移动介质还是非符合SDMI的可移动介质。当发现该目标是符合SDMI的可移动介质时，加密内容数据可传输的次数被限制。当发现该目标是非符合SDMI的可移动介质时，加密内容数据从非符合SDMI的可移动介质向许可的相符组件的返回(或校验入)被禁止。



ISSN1008-4274

01.12.31

权 利 要 求 书

1. 一个数据传输装置，包括：

传输元件，它将以预定形式加密的内容数据从能够储存加密内容数据的第一记录元件传输到外部装置；

鉴别元件，它用于在第一外部装置和第二外部装置之间进行鉴别，第一外部装置只能将加密内容数据记录到与所述的数据传输装置连接的所述外部装置中的第二记录元件，第二外部装置只能将解密内容数据记录到所述第二记录元件；和

控制元件，如果所述第一外部装置被所述鉴别元件鉴别，该控制元件在所述加密内容数据从所述第一记录元件传输到所述外部装置时、用于减小加密内容数据的传输计数，该控制元件在加密内容数据从所述第一外部装置返回时增加所述传输计数，如果传输计数超过预定的限制值，则中止所述内容数据从所述第一记录元件向所述外部装置的传输，和

如果所述第二外部装置被所述鉴别元件鉴别，则所述控制元件中止该加密内容数据从所述第二外部装置返回。

2. 如权利要求 1 的数据传输装置，其特征在于，位于所述第一外部装置内的所述第二记录元件是快速擦写存储器。

3. 如权利要求 1 的数据传输装置，其特征在于，位于所述第一外部装置内的所述第二记录元件是磁光盘。

4. 如权利要求 1 的数据传输装置，其特征在于，所述第一记录元件是硬盘。

5. 如权利要求 1 的数据传输装置，其特征在于，所述第二外部装置具有解密元件，用于对从所述数据传输装置传输的加密内容数据进行解密，并将所述解密元件解密的内容数据记录到所述第二记录元件。

6. 如权利要求 1 的数据传输装置，还包括：

第一接收元件，用于从内容服务器接收加密的内容数据和控制信号；

第二接收元件，用于接收来自封装介质的非加密内容数据；和

确定元件，如果所述第二外部装置被所述鉴别元件鉴别，则根据附加到所述内容服务器提供的所述内容数据上的所述控制信号确定是否从所述内容服务器传输所述的内容数据。

7. 如权利要求 6 的数据传输装置，其特征在于，所述控制元件限制从所述内容服务器提供的所述内容数据的传输计数，所述内容数据从所述第一记录元件传输到所述第二外部装置。

8. 如权利要求 1 的数据传输装置，还包括:

第一接收元件，用于接收从内容服务器提供的加密内容数据和控制信号；

第二接收元件，用于接收来自封装介质的非加密内容数据；和

加密元件，用于对从所述封装介质提供的并被所述第二接收元件接收的非加密内容数据进行加密；

如果所述第二外部装置被所述鉴别元件鉴别，则被所述加密元件加密的内容数据被提供到所述第二外部装置。

9. 一个具有数据传输装置和至少一个能选择地连接到所述数据传输装置的第一外部装置和第二外部装置的数据传输系统，所述的数据传输装置包括:

传输元件，它将以预定形式加密的内容数据从能够储存加密内容数据的第一记录元件传输到外部装置；

鉴别元件，它用于在第一外部装置和第二外部装置之间进行鉴别，第一外部装置只能将加密内容数据记录到与所述的数据传输装置连接的所述外部装置中的第二记录元件，第二外部装置只能将解密内容数据记录到所述第二记录元件；和

控制元件，如果所述第一外部装置被所述鉴别元件鉴别，该控制元件在所述加密内容数据从所述第一记录元件传输到所述外部装置时、用于减小加

密内容数据的传输计数，该控制元件在加密内容数据从所述第一外部装置返回时，用于增加所述传输计数，如果传输计数超过预定的限制值，则中止所述内容数据从所述第一记录元件向所述外部装置的传输，和

如果所述第二外部装置被所述鉴别元件鉴别，则所述控制元件中止加密内容数据从所述第二外部装置返回；

所述第二外部装置包括：

接收元件，用于从所述传输元件接收以预定方式加密的内容数据；

解密元件，用于对所述接收元件接收的所述以预定方式加密的内容数据进行解密；和

记录元件，用于将所述解密元件解密的所述内容数据记录到所述第二记录元件。

10. 如权利要求 9 的数据传输系统，其特征在于，位于所述第一外部装置内的所述第二记录元件是快速擦写存储器。

11. 如权利要求 9 的数据传输系统，其特征在于，位于所述第二外部装置内的所述第二记录元件是磁光盘。

12. 如权利要求 9 的数据传输系统，其特征在于，所述第一记录元件是硬盘。

13. 如权利要求 9 的数据传输系统，其特征在于，所述第二外部装置具有解密元件，用于对从所述数据传输装置传输的加密内容数据进行解密，并将由所述解密元件解密的内容数据记录到所述第二记录元件。

14. 如权利要求 9 的数据传输系统，还包括：

第一接收元件，用于从内容服务器接收加密的内容数据和控制信号；

第二接收元件，用于接收来自封装介质的非加密内容数据；和

确定元件，如果所述第二外部装置被所述鉴别元件鉴别，则根据附加到所述内容服务器提供的所述内容数据上的所述控制信号确定是否从所述内容服务器传输所述的内容数据。

01.12.31

15. 如权利要求 14 的数据传输系统，其特征在于，所述控制元件限制从所述内容服务器提供的所述内容数据传输计数、所述内容数据从所述第一记录元件传输到所述第二外部装置。

16. 如权利要求 9 的数据传输系统，其中所述数据传输装置还包括：

第一接收元件，用于接收从内容服务器提供的加密内容数据和控制信号；

第二接收元件，用于接收来自封装介质的非加密内容数据；和

加密元件，用于对从所述封装介质提供的并被所述第二接收元件接收的非加密内容数据进行加密；

如果所述第二外部装置被所述鉴别元件鉴别，则被所述加密元件加密的内容数据被提供到所述第二外部装置。

17. 一种数据传输方法，用于将加密数据从具有能储存加密内容数据的第一存储器的数据传输装置传输到位于连接到所述数据传输装置的外部装置中的第二存储器，所述数据传输方法包括：

鉴别步骤，它用于在第一外部装置和第二外部装置之间进行鉴别，第一外部装置只能将加密内容数据记录到与所述的数据传输装置连接的所述外部装置中的第二存储器，第二外部装置只能将解密内容数据记录到所述第二存储器；和

第一控制步骤，如果所述第一外部装置被所述鉴别步骤鉴别，该控制步骤在所述加密内容数据从所述第一存储器传输到所述外部装置时，用于减小加密内容数据的传输计数，该控制元件在加密内容数据从所述第一外部装置返回时，用于增加所述传输计数，如果所述传输计数超过预定的限制值，则中止所述内容数据从所述第一存储器向所述外部装置的传输，和

第二控制步骤，如果所述第二外部装置被所述鉴别步骤鉴别、则所述第二控制步骤中止加密内容数据从所述第二外部装置返回。

18. 如权利要求 17 的数据传输方法，其特征在于，位于所述第一外部装置内的所述第二存储器是快速擦写存储器。

19. 如权利要求 17 的数据传输方法，其特征在于，位于所述第二外部装置内的所述第二存储器是磁光盘。

20. 如权利要求 17 的数据传输方法，其特征在于，所述第一存储器是硬盘。

21. 如权利要求 17 的数据传输方法，其特征在于，如果储存在所述第一存储器中的加密内容数据经网络被提供，则控制信息被附加到所述加密内容数据并储存在所述第一存储器，所述数据传输方法还包括：

判断步骤，用于当所述加密内容数据从所述第一存储器传输到所述第二外部装置时判断是否存在所述控制信息；和

确定步骤，当如果所述第二外部装置已经在所述鉴别步骤中被鉴别时、该确定步骤用于确定是否根据所述控制信息的存在传输从所述内容服务器提供的所述的内容数据。

22. 如权利要求 21 的数据传输方法，还包括：

限制步骤，用于限制传输计数，在该传输计数中、从所述内容服务器提供的所述内容数据可从所述数据传输装置的所述第一存储器传输到所述第二外部装置。

23. 如权利要求 17 的数据传输方法，其特征在于，如果储存在所述第一存储器中的加密内容数据从封装介质被提供、并且所述第二外部装置已经在鉴别步骤中被鉴别，则所述的加密内容数据被提供到所述第二外部装置。

24. 一个数据记录装置，该数据记录装置接收来自数据传输装置的加密内容数据、并将接收的加密内容数据记录到第二记录介质，该数据传输装置具有储存所述加密内容数据的第一记录介质，所述的数据记录装置包括：

通信元件，用于与所述数据传输装置进行双向通信；

验证处理元件，用于借助所述通信元件与所述数据传输装置进行验证；

解密元件，用于对通过所述通信元件从所述数据传输装置提供的加密内容数据进行解密；

记录元件，用于将借助所述解密元件解密的所述内容数据记录到所述第二记录介质；和

控制元件，用于禁止所述内容数据从所述第二记录介质经所述通信元件返回到所述数据传输装置。

25. 一种储存计算机可读程序的记录介质，该计算机可读程序用于将加密的内容数据从具有储存所述加密内容数据的第一存储器的数据传输装置传输到位于连接到所述数据传输装置的外部装置内的第二存储器，所述计算机可读程序包括:

鉴别步骤，它用于在第一外部装置和第二外部装置之间进行鉴别，第一外部装置只能将加密内容数据记录到与所述的数据传输装置连接的所述外部装置中的第二存储器，第二外部装置只能将解密内容数据记录到所述第二存储器;

第一控制步骤，如果所述第一外部装置在所述鉴别步骤中被鉴别，该控制步骤在所述加密内容数据从所述第一存储器传输到所述外部装置时用于减小加密内容数据的传输计数，该控制步骤在所述加密内容数据从所述第一外部装置返回时用于增加所述传输计数，如果所述传输计数超过预定的限制值，则中止所述内容数据从所述第一存储器向所述外部装置的传输，和

第二控制步骤，如果所述第二外部装置被所述鉴别步骤鉴别、则所述第二控制步骤中止加密内容数据从所述第二外部装置返回。

01.12.31

说　明　书

数据传输系统、装置和方法及数据记录装置和记录介质

技术领域

本发明涉及适于传输和记录诸如受版权保护的音乐的内容数据的数据传输系统、数据传输装置、数据记录装置、数据传输方法和记录介质。

背景技术

例如，诸如音乐的内容数据被储存在作为记录介质的个人计算机的硬盘驱动器（以下称作“HDD”）中，储存的内容数据传输到另一记录介质（辅助记录介质），内容数据从这个辅助记录介质中再现。

在这种情况下，HDD 储存从诸如 CD－DA（数字音频光盘）和 DVD（数字多用途光盘）等封装介质再现的诸如音乐的内容数据或储存经个人计算机连接的通信网从例如外部音乐服务器下载的内容数据。个人计算机用户将用于辅助记录介质的记录装置连接到个人计算机、将内容数据从 HDD 向辅助记录介质复制或移动，并通过与辅助记录介质兼容的再现装置再现诸如音乐的内容数据。

辅助记录介质可以是基于半导体存储器的存储卡，例如，快速擦写存储器、微型盘（Mini Disc，商标）、CD－R（可记录 CD）、CD－RW（可重写 CD）、DVD－RAM、DVD－R、或 DVD－RW，它是磁光盘。

能够记录和/或播放这些记录介质的记录器/播放器被广泛地用作与辅助记录介质兼容的记录/再现装置。这些记录器/播放器具有多种形式:固定式、便携式等等。用户可根据他们的嗜好和他们的设备记录/回放内容数据。

鉴于上述内容数据的使用形式，必须考虑对这些内容数据的版权保护。例如，如果用户能通过内容数据分配服务器或从购买的封装介质下载内容数

据而将内容数据存储到其个人计算机的 HDD 中、而后不加限制地将存储的内容数据复制到辅助记录介质，则会产生侵权问题。为了克服这个问题以维护作为数字数据的内容数据处理的版权保护，已提出各种技术和数据处理标准。其中之一是 SDMI（安全数字音乐创制权）。

图 1 表示由 SDMI 确定的数据路径。应注意，在具有作为主记录介质的 HDD 的个人计算机中，这一数据路径将音乐内容存储和传输到外部装置（在辅助记录介质侧）。换言之，这一路径由安装的用于存储和/或传输音乐内容的软件程序实现。图 1 所示数据路径中的过程和处理由标号 DP21－DP28 表示。在下文中，这些标号用于相应的描述。

安装在具有 HDD 的个人计算机中的软件确定经网络由外部服务器分配的内容数据（以下称作“网络内容”）是否基于用于版权保护的 SDMI（DP21）。

被分配的网络内容包括由服务器侧传输的作为符合 SDMI 内容的内容数据（以下称作“符合 SDMI 的内容”）和不与 SDMI 相关的内容数据（以下称作“非 SDMI 内容”）。

对于符合 SDMI 的内容，内容数据基于例如 DES（数据加密标准）由内容密钥 CK 加密。内容数据本身借助诸如 ATRAC3 或 MP3（活动图像专家组 1/2 层 3）的压缩算法进行初始编码，而后进行加密用于分发。

应注意，为了说明方便，由密钥 x 加密的数据 y 表示为 E（x，y）。

对于加密的数据 E（x，y），由密钥 x 解密后的数据表示为 D{x，E（x，y）}。

所以，如果基于 ATRAC3 的压缩数据表示为 A3D，则由密钥 CK 加密的用于分配的符合 SDMI 的内容表示为 E（CK，A3D）。

如果分配的网络内容为符合 SDMI，则该内容作为 SDMI 内容存储在诸如 HDD 的主记录介质（DP21 和 DP22）。

在这种情况下，内容数据以加密的 E（CK，A3D）状态写入 HDD。另一种方式是，内容数据被解密，而后以另一个密钥 CK'加密、即密钥被改变，

然后将新加密的内容数据以 E（CK'，A3D）状态写入 HDD。

另一方面，如果网络内容是非 SDMI 内容，则进行水印校验、即用电子水印进行筛选（DP21－DP23）。

再有，对从诸如 CD－DA 和 DVD 等封装介质阅读的内容数据（以下称作“盘内容”）进行直接水印校验（DP23），所述封闭介质在诸如安装在个人计算机的 CD－ROM 驱动器的盘驱动器装置或连接到个人计算机的盘驱动器装置上进行再现。

即，在不基于 SDMI 的内容数据上进行水印校验。

如果发现经水印校验的内容数据不好，则该内容数据不能在 SDMI 数据路径上复制（DP23－DP25）。不能复制禁止的具体处理基于软件设计。例如，内容数据可存储在 HDD，但不能传输用于复制或移动到其它记录介质、或该内容数据不能在符合 SDMI 内容的处理中存储到 HDD。

如果内容数据通过了水印校验，即如果在内容数据中发现了水印且控制位指示复制许可，则可知该内容数据能合法地复制。而后，确定该内容数据是否根据 SDMI 进行处理（DP24）。是否将这些内容数据处理成符合 SDMI 可由软件设计或用户设置来确定。

如果内容数据不处理成符合 SDMI，则内容数据被看作非 SDMI 内容、并从符合 SDMI 的内容数据路径排除（DP26）。例如，这些内容数据可传输到非符合 SDMI 的记录装置。

另一方面，如果内容数据被处理成符合 SDMI，则这些内容数据被加密并作为 SDMI 内容存储在 HDD 中（DP24－DP22）。例如，这些内容数据以 E（CK，A3D）或 E（CK'，A3D）的形式被存储。

在诸如 HDD 的主记录介质中，上述数据路径储存经网络得到的处理为符合 SDMI 的内容（以下称作“SDMI 网络内容”）和从诸如 CD－DA 提取的处理为符合 SDMI 的内容（以下称作“SDMI 盘内容”）。

储存在 HDD 中的 SDMI 内容（SDMI 网络内容或 SDMI 盘内容）传输到

符合 SDMI 的记录/再现装置、可复制到符合 SDMI 的辅助记录介质。符合 SDMI 的记录/再现装置是基于例如存储卡的可移动记录器/播放器，它与基于 SDMI 的加密兼容。

在 SDMI 盘内容的情况下，与 SDMI 盘内容对应的传输处理规则（或使用规则）被限定，根据该规则，用于复制到符合 SDMI 的记录/再现装置的传输被授权（DP28）。

应注意，从主记录介质（HDD）复制到被符合 SDMI 的记录/再现装置记录和再现的辅助记录介质（例如，存储卡）的传输被称作“校验出”。从辅助记录介质移动到主记录介质的传输被称作“校验入”。应注意，从辅助记录介质到主记录介质的移动删除在辅助记录介质的被传输内容数据。

传输 SDMI 盘内容的规则可限定校验出上限计数，每段内容数据可被校验出最多三次。所以，SDMI 盘内容可被复制到例如三个符合 SDMI 的辅助记录介质。如果校验出发生，在具有 HDD 的个人计算机中管理的内容数据的校验出计数被减小。于是，即使复制到三个符合 SDMI 辅助记录介质之后，如果内容数据从一个辅助记录介质到主记录介质（HDD）被校验入，则在个人计算机中管理的内容数据的校验出计数被加 1。结果，内容可再一次从主记录介质（HDD）向符合 SDMI 的辅助记录介质复制。即，内容数据被允许总是存在于最多三个符合 SDMI 的辅助记录介质。

在 SDMI 网络内容的情况下，与 SDMI 网络内容对应的传输处理规则（使用规则）也被限定，根据该处理规则，用于复制到符合 SDMI 记录/再现装置的传输被授权（DP27）。

与例如用于 SDMI 盘内容的规则一样，这个传输处理规则规定校验出计数的上限。该上限计数可与用于 SDMI 盘内容的规则相同或不相同。例如，该上限校验出计数可以是 1。在这种情况下，一个内容数据段只能复制到另一个符合 SDMI 辅助记录介质；但是，如果内容数据从那个辅助记录介质校验入，则该内容数据可再次进行复制传输。

当 SDMI 内容根据这些处理规则被传输以复制到符合 SDMI 的辅助记录介质时，该内容数据在传输路径上被加密传输。即，该内容数据以上述的 E（CK，A3D）或 E（CK'，A3D）的状态传输。

另外，在接收加密的 SDMI 内容的符合 SDMI 的记录/再现装置上，被接收的 SDMI 内容加密地复制到辅助记录介质。

如果符合 SDMI 的记录/再现装置从辅助记录介质再现 SDMI 内容，从该辅助记录介质读取的内容数据被解密。即，以 E（CK，A3D）或 E（CK'，A3D）的状态复制到辅助记录介质的内容数据被密钥 CK 或 CK'解密。

更具体地，原始内容数据被恢复成解密为 D{CK，E(CK，A3D)} = A3D 或 D{CK'，E(CK'，A3D)} = A3D 的 ATRAC3 数据（A3D）。而后，解密的内容数据从 ATRAC3 压缩状态解压缩、以便解调为例如用于再现音乐的音频数据。

根据符合 SDMI 的数据路径，加密的内容数据从网络上的服务器传输到辅助记录介质，这些内容数据的复制由预定规则控制，所以该内容数据的版权可有效地被保护。

但是，当内容数据复制到符合 SDMI 的辅助记录介质时可能出现下述问题。

这里假定目前广泛地使用的微型盘（一种磁光盘）用作辅助记录介质。

例如，如果使用符合 SDMI 的微型盘记录装置，这个微型盘记录装置以 E(CK，A3D)或 E(CK'，A3D 的加密状态记录校验出到微型盘的 SDMI 内容。

当再现时，解密为 D{CK，E(CK，A3D)} = A3D 或 D{CK'，E(CK'，A3D)} = A3D 的 ATRAC3 数据（A3D）必须以预定形式被解码，例如音乐的结果被输出供再现。

目前流行的微型盘系统不能将加密数据记录到微型盘。显然，没有微型盘再现装置具有用于解密加密数据的解码器。

如果将来符合 SDMI 的微型盘记录装置进一步发展且加密的内容数据可

记录到微型盘，但记录到微型盘的加密内容数据不能被许多非符合 SDMI 的微型盘播放器再现。即，这种系统不能提供再现兼容性。

最终，这将限制由普通用户购买的 SDMI 内容的正常使用，明显降低 SDMI 内容的价值和普通用户对 SDMI 内容提供服务的满意程度。

鉴于上述问题，可提出一种系统，该系统能以解密状态将 SDMI 内容传输到例如非 SDMI 的微型盘记录设备以被复制到诸如微型盘的辅助记录介质。

然而，如果这种复制形式被许可，则内容数据可方便地复制、包括非授权复制。这将会妨碍执行 SDMI 版权保护的原有意图的实现。

发明内容

因此，本发明的一个目的是在不限制用户正确使用例如需要版权保护的音乐的内容数据的前提下保持版权保护能力。为了实现这一目的，本发明提供：数据传输装置、数据记录装置和包括这些装置的数据传输系统，在数据传输装置中使用的数据传输方法和储存操作数据传输装置的操作程序的记录介质。

在实施本发明中，根据本发明的一个方面，提供了数据传输装置，包括：传输器，它将以预定形式加密的内容数据从能够储存加密内容数据的第一存储器传输到外部装置；鉴别器，它用于在第一外部装置和第二外部装置之间进行鉴别，第一外部装置只能将加密内容数据记录到与数据传输装置连接的外部装置中的第二存储器，第二外部装置只能将解密内容数据记录到该第二存储器；控制器，如果第一外部装置被该鉴别器鉴别，则该控制器在加密内容数据从第一存储器传输到外部装置时、用于减小加密内容数据的传输计数，该控制器在加密内容数据从第一外部装置返回时、用于增加传输计数，如果传输计数超过预定的限制值、则中止内容数据从第一存储器向外部装置的传输，如果第二外部装置被鉴别器鉴别、则控制器中止加密内容数据从第二外

部装置返回。

在实施本发明中，根据本发明的另一个方面，提供了数据传输系统，具有数据传输装置和至少一个可选择地连接到所述数据传输装置的第一外部装置和第二外部装置，所述的数据传输装置包括：传输器，它将以预定形式加密的内容数据从能够储存加密内容数据的第一存储器传输到外部装置；鉴别器，它用于在第一外部装置和第二外部装置之间进行鉴别，第一外部装置只能将加密内容数据记录到与数据传输装置连接的外部装置中的第二存储器，第二外部装置只能将解密内容数据记录到该第二存储器；控制器，如果第一外部装置被该鉴别器鉴别，则该控制器当加密内容数据从第一存储器传输到外部装置时、用于减小加密内容数据的传输计数，该控制器当加密内容数据从第一外部装置返回时、用于增加传输计数，如果传输计数超过预定的限制值、则中止内容数据从第一存储器向外部装置的传输，如果第二外部装置被鉴别器鉴别、则控制器中止加密内容数据从第二外部装置返回。第二外部装置包括：接收器，用于从所述传输器接收以预定形式加密的内容数据；解密元件，对接收器接收的以预定形式加密的内容数据进行解密；记录元件，将解密元件解密的内容数据记录到第二存储器。

在实施本发明中，根据本发明的又一个方面，提供了数据记录装置，它从具有存储加密内容数据的第一记录介质的数据传输装置接收加密内容数据并将接收的加密内容数据记录到第二记录介质，所述的数据记录装置包括：通信线，用于与数据传输装置进行双向通信；授权处理器，通过通信线与数据传输装置执行验证；解密元件，对通过通信线从数据传输装置提供的加密内容数据解密；记录元件，将解密元件解密的内容数据记录到第二存储器；和控制器，用于中止来自第二记录介质的内容数据经通信线返回到数据传输装置。

附图说明

通过结合附图对本发明所作的说明将使本发明的这些和其它目的更为清楚，在附图中：

图 1 是表示由 SDMI 制定的内容流程和使用规则的示意图；

图 2 是表示可用于本发明的整体系统的框图；

图 3 是表示可用于本发明的主记录介质侧装置的框图；

图 4 是表示可用于本发明的辅助记录介质侧装置的框图；

图 5 是表示主记录介质侧装置与辅助记录介质侧装置之间的验证处理程序的交互图；

图 6 表示作为本发明第一实施例执行的内容流程和使用规则；

图 7 表示作为本发明第二实施例执行的内容流程和使用规则；

图 8 表示作为本发明第三实施例执行的内容流程和使用规则；和

图 9 表示作为本发明第四实施例执行的内容流程和使用规则。

具体实施方式

下面将结合附图通过示例按以下顺序进一步详细说明本发明：

1. 系统结构
2. 数据传输装置的示例结构（主记录介质侧装置 = PC）
3. 数据记录装置的示例结构（辅助记录介质侧装置 = 记录/再现装置）
4. 验证处理
5. SDMI 内容传输处理的实例

1. 系统结构

图 2 示出一个系统结构的示例。主记录介质侧装置 1 与本发明的数据传输装置对应。辅助记录介质侧装置 20A 与本发明的数据记录装置对应。所以，由图 2 所示的主记录介质侧装置 1 与辅助记录介质侧装置 20A 组成的结构与本发明的数据传输系统对应。

主记录介质侧装置 1 由例如个人计算机构成。在以下的说明中，为简便起见，主记录介质侧装置 1 也称作个人计算机（PC）1。但是，主记录介质侧装置 1 不总是由个人计算机构成；它可以是安装有软件并具有高容量存储装置的任何设备。

主记录介质侧装置 1 通过执行软件而起到这里所称的数据传输装置的功能，它在例如计算机上被启动、用于存储和/或传输 SDMI 内容数据。

包含在（或外附在）个人计算机 1 中的 HDD 5 用作主记录介质（和主记录介质驱动装置）。应注意，在本实施例的说明中，HDD 5 是主记录介质；但是，显然主记录介质也可以例如是诸如光盘或磁光盘的盘介质、或是例如内置的或可拆卸的（例如，存储卡）半导体存储器。

主记录介质侧装置 1 可经通信网络 110 与内容服务器 91 通信、可从内容服务器 91 下载诸如音乐的内容数据。显然，有许多内容服务器 91，个人计算机 1 的用户可利用内容服务器 91 使用各种需要的下载服务。

从内容服务器 91 下载到个人计算机 1 的内容数据包括符合 SDMI 的内容数据和非符合 SDMI 的内容数据。

构成通信网络 110 的传输路径可以是有线或无线的公共交换线网或设置在个人计算机 1 与内容服务器 91 之间的专用线路。通信网络 110 可以是例如通信卫星线、ISDN（综合业务数字网）、模拟电话线、或蓝牙。

个人计算机 1 的 HDD 5 也能通过内置或外附的盘驱动器储存从诸如 CD－DA 和 DVD 的封装介质 90（以下也称作“盘 90”）再现的诸如音乐的内容数据。

个人计算机 1 连接到辅助记录介质侧装置 20A 或 20B，内容数据从 HDD 5 传输到设备 20A 或 20B。辅助记录介质侧装置 20A 或 20B 是用于辅助记录介质的记录装置或记录和再现装置。辅助记录介质侧装置 20A 或 20B 能复制从个人计算机 1 传输到辅助记录介质的内容数据。

辅助记录介质侧装置 20A 或 20B 具有不同的具体形式。这里的辅助记录

介质侧装置 20B 是符合 SDMI 的记录介质。即，图 1 所示的符合 SDMI 的记录/再现装置与辅助记录介质侧装置 20B 对应。在这种情况下，辅助记录介质是基于例如诸如快速擦写存储器的半导体存储器的符合 SDMI 的存储卡。因此，辅助记录介质侧装置 20B 是与例如符合 SDMI 存储卡兼容的记录/再现装置。在这种情况下，SDMI 内容被加密地记录到辅助记录介质。

另一方面，辅助记录介质侧装置 20A 与这里涉及的数据记录装置对应。辅助记录介质侧装置 20A 将在辅助记录介质中储存下面将详细说明的版权保护的解密的 SDMI 内容。这里的辅助记录介质的一个实例是微型盘。因此辅助记录介质侧装置 20A 是微型盘记录/再现装置。在下文中，辅助记录介质侧装置 20A 也可称作记录/再现装置 20A。

除了微型盘之外，借助辅助记录介质侧装置 20A 记录或再现的介质包括例如基于半导体存储器的存储卡，如快速擦写存储器、作为磁光盘的微型盘、CD－R（可记录 CD）、CD－RW（可重写 CD）、DVD－RAM、DVD－R、和 DVD－RW。因此，辅助记录介质侧装置 20A 可以是任何与这些记录介质兼容的装置。

个人计算机 1 根据诸如 USB（通用串行总线）或 IEEE1394 的传输协议而连接到辅助记录介质侧装置 20A 或 20B。显然，控制信号和内容数据也可根据诸如蓝牙或 DS－SS（符合 IEEE 802.11b）的其它传输协议通过有线或无线传输路径在其间传输。

2. 数据传输装置的示例结构（主记录介质侧装置＝PC）

图 3 示出了提供数据传输装置的主记录介质侧装置 1 的结构。应注意，在这个实例中，主记录介质侧装置 1 由个人计算机构成；显然，主记录介质侧装置 1 也可由基于具有相同效力的专用软件的只传送数据的装置构成。

在这个实例中，当用于执行作为数据传输装置的功能的软件程序安装在个人计算机 1 时，则用于提供数据传输装置的主记录介质侧装置被实现。应注意，“个人计算机”或“计算机”在这里是指所谓通用计算机。

这个软件程序可预先储存在作为记录介质的安装在计算机内的硬盘（HDD）5 或 ROM 3 中。

作为替代方式，这个软件也可暂时或永久地储存（或记录）在诸如软盘、CD－ROM（只读光盘存储器）、MO（磁光）盘、DVD（数字多用途光盘）、磁盘、或半导体存储器的可移动记录介质中。可移动记录介质 90 可被提供为所谓的套装软件。

应注意，除了从可移动记录介质 90 安装到计算机之外，该程序也能以无线方式经数字卫星网或以有线方式经诸如 LAN（局域网）或因特网的网络从下载网站下载。计算机在其通信部件 8 接收下载程序、并将它储存到内装的 HDD 5。

图 3 所示的计算机 1 包括 CPU（中央处理单元）2。CPU 2 经总线 12 连接到输入/输出接口 10。当用户借助操作例如由键盘、鼠标、和话筒构成的输入部件 7 而输入指令时，CPU 2 执行储存在 ROM（只读存储器）3 中的程序。另外，CPU 2 通过将其装入 RAM（随机存储器）4 执行储存在 HDD 5 中的程序、由通信卫星或网络传输、被通信部件 8 接收并储存在 HDD 5 中的程序，或者从诸如装入驱动器 9 和装入 HDD 5 的光盘的可移动记录介质 90 读取的程序。于是，CPU 2 执行作为数据传输装置的对 SDMI 内容的处理，下文将说明。

之后，CPU 2 经过输入/输出接口 10、从例如由 LCD（液晶显示器）和扬声器构成的输出部件 6 输出得到的处理结果，并将它们从通信部件 8 传输、或记录到 HDD 5。

在这个实例中，通信部件 8 可经图 2 所示的网络 110 与各种服务器通信。即，计算机 1 可从外部服务器 91 下载诸如音乐的网络内容。下载的网络内容被下文所述的程序处理成符合 SDMI 的内容或非符合 SDMI 的内容，对于 SDMI 处理而言，处理的 SDMI 内容储存在 HDD 5 中。储存在 HDD 5 中的 SDMI 内容变成被传输到符合 SDMI 的辅助记录介质侧装置 20B 或特许类型

的辅助记录介质侧装置（记录/再现装置）20A，设备 20B 或 20A 是与本发明相关的数据记录装置。

连接部件 11 提供主记录介质侧装置 1 与辅助记录介质侧装置 20A 或 20B 之间的连接。连接部件 11 是例如 USB 接口或 IEEE1394 接口。显然，可使用其它基于红外或射频的有线或无线的标准接口。

下面将说明由这个实例的数据传输装置执行的验证处理和数据传输处理。应注意，这些处理操作不需按下述的程序以时间相关方式执行；它们可用并行或离散方式执行（例如，并行处理或目标处理）。

上述程序可由单个计算机或由两个或多个计算机以分布方式进行处理。此外，这些程序可传输到远端计算机来执行。

3. 数据记录装置的示例结构（辅助记录介质侧装置 = 记录/再现装置）

图 4 示出与本发明的数据记录装置对应的辅助记录介质侧装置（记录/再现装置）20A 的示例结构。

在这个实例中，辅助记录介质侧装置 20A 被配置成例如微型盘记录器。所以，辅助记录介质 100 是微型盘（一种磁光盘）的实例，且被称作微型盘 100。

应注意，图 4 只示出用于在作为辅助记录介质 100 的微型盘上记录/再现数据的处理系统和用于通过上述主记录介质侧装置 1 进行鉴别和数据传输的处理系统，而略去了对微型盘 100 驱动系统、伺服系统和再现输出系统的详细表示，因为这些系统一般与普通微型盘记录/再现装置相同。

CPU 21 是用于控制整个记录/再现装置 20A 的系统控制器。更具体地，CPU 21 执行用于控制旋转驱动、主轴伺服、焦点伺服、跟踪伺服、滑轨伺服的操作，执行用于控制光学头激光束和磁头磁力施加的操作和执行用于控制被记录和再现数据的编码和解码、从而在微型盘 100 上记录和再现该数据的操作。另外，CPU 21 控制与个人计算机 1 关于验证的通信和数据产生的指示、发自个人计算机 1 的各种指令的传输和所接收内容数据处理的通信。

虽然没有示出，但是操作员面板和显示区被设置为用户接口。CPU 21 也执行诸如监测用户在操作面板上的操作和显示区控制的处理。

记录/再现部件 25 具有光学头、磁头、盘旋转驱动系统、伺服系统等，所以实际上在微型盘 100 上记录和再现数据。

编码器/解码器 24 对记录到微型盘 100 的数据进行编码、对从微型盘 100 再现的数据进行解码。如已知的，在微型盘系统的情况下，要记录的数据通过 ACIRC（高级交叉交织里德-所罗门码（Advanced Cross Interleave Reed Solomon Coding））和 EFM（八对十四的调制）。于是，编码器/解码器 24 对记录数据进行 ACIRC 和 EFM 处理、并将结果数据提供到记录/再现部件 25。

当再现时，编码器/解码器 24 对从记录/再现部件 25 提供的数据执行诸如二值化、EFM 和 ACIRC 的解码。

编解码器 23 根据 ATRAC/ATRAC3 算法执行数据压缩和解压缩。

如上所述，记录到微型盘 100 的数据由 ATRAC（自适应变换声音编码）压缩并然后编码。所以，如果数据不被压缩，例如 PCM 音频数据作为记录数据输入记录/再现装置辅助记录介质侧装置 20A，则编解码器 23 根据 ATRAC 对输入的数据进行压缩，压缩数据并被提供给编码器/解码器 24。

应注意，存在两个音频数据压缩方案；即，ATRAC 和 ATRAC3，后者的压缩效率高于前者。与 ATRAC 的 292 Kbps 的位速率相比，ATRAC3 提供可选择的 132 Kbps 和 66 Kbps 两个位速率。公认的符合 SDMI 的辅助记录介质的存储棒(MS)加密被 ATRAC3 压缩的数据并储存该加密数据。目前，一些市售的非符合 SDMI 的辅助记录介质的微型盘装置具有 ATRAC 编码器/解码器和 ATRAC3 编码器/解码器，以便储存未加密的 ATRAC 和 ATRAC3 数据。

当再现时，由记录/再现部件 25 阅读并被编码器/解码器 24 解码的数据是根据 ATRAC 压缩的数据。所以，该压缩数据由编解码器 23 解压缩。于是，例如 44.1KHz 和 16 位数值转换的数字音频数据被解调制。解调制数字音频数据由未示出的输出电路进行 D/A 转换、模拟信号处理和放大，以变成再现为

例如音乐的扬声器输出信号。

作为替代方式，数字音频数据可不用改变而输出到另一设备。

上述结构也应用到普通微型盘系统的记录/再现装置。本实施例的记录/再现装置辅助记录介质侧装置 20A 具有与作为主记录介质侧装置 1 的个人计算机相对应的接口 26 和解密部件 29。

接口 26 连接到图 3 所示个人计算机 1 的连接部件 11，与个人计算机 1 进行数据通信。所以，接口 26 具有用于缓冲发送/接收数据的缓冲器 27 和用于在接口进行信号处理的发送/接收处理器 28。例如，接口 26 根据 USB 或 IEEE1394 通信协议进行信号处理。

通过接口 26 与个人计算机 1 的通信包括从个人计算机 1 接收各种指令、下文所述验证处理所需的数据的传输和接收、和 SDMI 内容的接收。

解密部件 29 对 SDMI 内容进行解密、并具有密钥储存部件 30 和解密处理器 31。

密钥储存部件储存用于解密所加密 SDMI 内容的密钥（例如，密钥 CK 和密钥 CK'）。这些密钥可在预定时间预先储存到或从个人计算机 1 传输到记录/再现装置 20A。当个人计算机 1 传输这些密钥时，它们可由另一密钥 CCK 加密，接收的密钥在记录/再现装置 20A 由密钥 CCK 解密，解密的密钥被储存在密钥储存部件 30。

储存用于解密 SDMI 内容的诸如密钥 CK 等的密钥，可使解密处理器 31 对通过例如密钥 CK 加密而接收的 SDMI 内容、即对例如 E（CK，A3D）状态的内容进行解密。即，可得到由解密为 D{CK，E（CK，A3D）} = A3D 的由 ATRAC3 压缩的数据。而后，解密的 ATRAC3 数据由编码器/解码器 24 编码以便经记录/再现部件 25 记录到微型盘 100。

应注意，SDMI 内容不总是被加密的 ATRAC3 压缩数据。例如，SDMI 内容可以是由密钥 CK 加密的线性 PCM 数据。即，内容可以例如 E（CK，PCM）状态输入。在这种情况下，显然在解密处理器 31 中、可得到解密为

D{CK，E（CK，PCM）}＝PCM 的线性 PCM 数据。在这种情况下，PCM 数据由编解码器 23 进行 ATRAC3 压缩、由编码器/解码器 24 编码、并经记录/再现部件 25 记录到微型盘 100。

密钥储存部件 30 也可储存用于验证处理的密钥。下文所述的示例性验证处理使用储存在记录再现设备 20A 内的公用密钥 P 和私用密钥 S。在这种情况下，公用密钥 P 和私用密钥 S 均储存在密钥储存部件 30 内。

4. 验证处理

这里所说的记录/再现装置 20A 是指具有图 4 所示结构并被个人计算机 1 成功验证的记录/再现装置。记录/再现装置 20A 将来自个人计算机 1 的 SDMI 内容解密记录到微型盘 100，下文详细说明。验证校验该记录/再现装置是否是用于记录操作的有效装置。

当与符合 SDMI 的记录/再现装置 20B 不同的记录/再现装置被连接时，这个验证处理被执行。应注意，如果符合 SDMI 的记录/再现装置 20B 被连接，则校验这个装置是否是这里所指的符合 SDMI 的装置。即，如果发现连接的装置不是 SDMI 兼容的记录/再现装置 20B，则进行随后的验证处理、以校验连接的装置是否是记录/再现装置 20A。

本实例中的验证处理使用基于不对称密码术（或公用密钥密码术）的验证方案。在不对称密码术中，加密密钥与解密密钥不同。使加密前的数据是 Db、加密密钥是 CKe、解密密钥是 CKd，则加密数据 C 由 C＝E（CKe，Db）加密、数据 Db 由 D（CKd，C）＝Db 解密。

加密密钥 CKe 和解密密钥 CKd 被称作密钥对，其中一个被公开制作为公用密钥，另一个作为私用密钥保持在预定部分。

在以下的验证处理中，在密钥对 CKe 和 CKd 中，公用密钥由 P 表示，私用密钥由 S 表示。如上所述，在这种情况下，记录/再现装置 20A 将提供加密密钥 CKe 和解密密钥 CKd 的公用密钥 P 和私用密钥 S 储存在密钥储存部件 30 中。

当进行验证处理时，主记录介质侧装置（个人计算机）1 的 CPU 2 向辅助记录介质侧装置 20A（记录/再现装置）的 CPU 21 例如发出验证请求的指令，于是在 CPU 2（主记录介质侧装置 1 = 个人计算机 1）与 CPU 21（辅助记录介质侧装置 20A = 记录/再现装置 20A）之间产生下面的处理，如图 5 所示。

当验证处理开始时，在步骤 S1 中，辅助记录介质侧装置 20A 的 CPU 21 将公用密钥 P 从密钥储存部件 30 经接口 26 传输到主记录介质侧装置 1。应注意，公用密钥 P 也被主记录介质侧装置 1 获知。

在步骤 S2 中，接收了公用密钥 P，主记录介质侧装置 1 的 CPU 2 产生随机数 r。在步骤 S3 中，CPU 2 将产生的随机数 r 传输到辅助记录介质侧装置 20A。

之后，在步骤 S4 中，辅助记录介质侧装置 20A 的 CPU 21 利用储存在密钥储存部件 30 中的私用密钥 S 加密接收的随机数 r。在步骤 S5 中，CPU 21 将加密数据 E（S，r）传输到主记录介质侧装置 1。

在步骤 S6 中，接收了加密数据 E（S，r），主记录介质侧装置 1 的 CPU 2 利用公用密钥 P 解密接收的加密数据 E（S，r）。即，CPU 2 执行 D{P，E（S，r）}的处理。

在步骤 S7 中，CPU 2 将步骤 S2 中产生的随机数 r 与步骤 S6 中得到的解密结果 D{P，E（S，r）}进行比较。

如果公用密钥 P 和私用密钥 S 是正确的密钥对，则可得到结果 r = D{P，E（S，r）}。

如果发现匹配，则表示辅助记录介质侧装置 20A 持有用于公用密钥 P 的私用密钥 S，并基于此使程序从 S8 进行到 S9，其中，辅助记录介质侧装置 20A 被验证为授权的连接配对。

另一方面，如果未发现匹配，则程序从 S8 到 S10，其中，连接的辅助记录介质侧装置不被看作是授权的连接配对（即，可传输 SDMI 内容的装置），

因此验证失败。

如果利用上述验证处理使连接的装置被成功地验证为本实例的辅助记录介质侧装置，则主记录介质侧装置 1 认可已经满足了允许传输 SDMI 内容到连接设备的条件之一。

5. SDMI 内容传输处理的实例

下面借助第一到第四实例说明作为本发明的一个实施例的从主记录介质侧装置（个人计算机）1 向辅助记录介质侧装置 20ASDMI 内容的传输。这些实例将利用如图 1 所示的数据路径、并结合图 6 到图 9 进行说明。图 6－9 中每个图所示的数据路径利用个人计算机 1 的 CPU 2 的处理被执行。更具体地，CPU 2 基于从例如可移动记录介质 90 安装的传输处理程序执行下述数据路径。

应注意，图 6－9 所示的数据路径的程序/处理由 DP1－DP11 表示。在下文中，这些标号用于对应的部分。

传输处理的第一实例:

下面利用图 6 所示的数据路径说明传输处理的第一实例。

从图 1 所示内容服务器 91 经网络 110 分发到计算机 1 的网络内容被确认是否将根据 SDMI 而受到版权保护（DP1）。

要被分发的网络内容包括从服务器传输的作为与 SDM I 相符的内容的符合 SDMI 的内容和非符合 SDMI 的内容。

在符合 SDMI 内容的情况中，其数据由基于诸如 DES 的密钥密码术的内容密钥 CK 而加密。如果内容数据本身是用诸如 ATRAC3 的压缩方案编码的数据，则符合 SDMI 的内容以 E（CK，A3D）的状态进行分发。

如果分发的内容是符合 SDMI 的内容，则它作为 SDMI 内容被储存在作为主记录介质的 HDD 5 中（DP1－DP2）。

在这种情况中，内容数据以 E（CK，A3D）的分发状态写入 HDD 5。另外，该内容数据被解密，并由另一密钥 CK'（即，加密密钥被改变）加密，

而后以 E（CK'，A3D）状态写入 HDD 5。

另一方面，如果网络内容是非 SDMI 内容，则对其校验水印，即用水印进行筛选（DP1－DP3）。

此外，对利用诸如个人计算机 1 的 CD－ROM 或连接到个人计算机 1 的盘驱动器的驱动器 9 进行再现的、从诸如 CD－DA 或 DVD 等封装介质读出的内容数据（盘内容）直接进行水印校验（DP3）。

即，与 SDMI 不一致的内容数据被水印校验。

如果发现该内容数据未通过水印校验，则该数据内容被处理为不能在 SDMI 数据路径上复制（DP3－DP5）。虽然具体处理依赖于所用的软件设计，然而失败的内容数据被储存在 HDD 5 中而不传输到另一用于复制或移动的记录介质，或不在与 SDMI 符合的内容处理中储存在 HDD 5 中。

如果内容数据通过了水印校验，即如果在内容数据中发现了水印并且控制位指示许可复制，则说明该内容数据能合法复制。而后，确认该数据内容是否基于 SDMI 进行处理（DP4）。可以通过软件设计或用户设置确认是否将这些内容数据按照与 SDMI 相符来处理。

如果内容数据未处理为与 SDMI 相符，则该内容数据被看作非 SDMI 内容、并从符合 SDMI 的内容数据路径中排除（DP6）。例如，这些内容数据可传输到与 SDMI 不兼容的记录装置。

另一方面，如果内容数据的处理为与 SDMI 相符，则这些内容数据作为 SDMI 内容被加密并储存在 HDD 5 中（DP4－DP2）。例如，这些内容数据以 E（CK，A3D）或 E（CK'，A3D）的形式储存在 HDD 5 中。

上述数据路径在 HDD 5 中储存经网络得到的处理成符合 SDMI 的内容（SDMI 网络内容）合从诸如 CD－DA 的盘检索到的处理成符合 SDMI 的内容（SDMI 盘内容）。

储存在 HDD 5 中的 SDMI 内容（SDMI 网络内容或 SDMI 盘内容）被传输到能复制到符合 SDMI 的辅助记录介质的符合 SDMI 的记录/再现装置 20B。

在本实例中，除了 SDMI 兼容的记录/再现装置 20B 之外，SDMI 内容在预定条件下可传输到成功验证的记录/再现装置 20A。

首先，如果符合 SDMI 的记录/再现装置 20B 连接到连接部件 11，则下述操作发生。

在 SDMI 盘内容的情况下，确立对应于 SDMI 盘内容的传输处理规则（使用规则）。因此，在这个处理规则下，到达符合 SDMI 记录/再现装置 20B 的传输以用于复制被许可（DP8）。

传输 SDMI 盘内容的规则可限定校验出上限计数，其中，内容数据的每段可被校验出最多三次。因此，SDMI 盘内容可被复制到例如最多三个符合 SDMI 的辅助记录介质。如果发生校验入，则内容数据的校验出计数减少。所以，既使在复制到三个符合 SDMI 的辅助记录介质后，如果内容数据从这些辅助记录介质之一校验入，则该内容可再次复制到符合 SDMI 的介质。即，允许内容数据总是一起存在到最多三个符合 SDMI 的辅助记录介质。

在 SDMI 网络内容的情况下，与 SDMI 网络内容对应的传输处理规则（使用规则）也被限定，根据该规则，复制到符合 SDMI 的记录/再现装置 20B 的传输被授权（DP7）。

这个传输处理规则与用于 SDMI 盘内容的规则相同地规定例如校验出计数的上限。该上限计数可与用于 SDMI 盘内容的规则相同或不同。例如，该上限校验出计数可以是一。在这种情况下，内容数据的一段可只复制到另一个符合 SDMI 的辅助记录介质；不过，如果内容数据从该辅助记录介质校验入，则该内容数据可被再次传输以便复制。

当基于这些处理规则 SDMI 内容被传输以复制到符合 SDMI 的辅助记录介质时，内容数据可在传输路径上加密地传输。即，内容数据以上述的 E（CK，A3D）或 E（CK'，A3D）状态进行传输。

另外，在接收加密 SDMI 内容的符合 SDMI 的记录/再现装置 20B 上，接收的 SDMI 内容被加密复制到辅助记录介质。

如果符合SDMI的记录/再现装置20B从辅助记录介质上再现SDMI内容，则从辅助记录介质读出的内容数据被解密。即，以E（CK，A3D）或E（CK'，A3D）状态复制到辅助记录介质的内容数据被密钥CK或CK'解密。

更具体地，原始内容数据被恢复为解密为D{CK，E（CK，A3D）} = A3D或D{CK'，E（CK'，A3D）} = A3D的ATRAC3数据（A3D）。而后，解密内容数据从ATRAC3压缩状态解压缩以便例如被解调为再现为音乐的音频数据。

如上所述，符合SDMI的内容数据在数据路径上保持加密直到内容数据被校验出并到辅助记录介质的点，复制控制由上述传输处理规则校验执行，因此能保护内容数据版权。

以上所述的处理通常与参考图1所述的常规SDMI数据路径相同。

以下说明由图6中虚线所示的部分，这是与图1所示的结构不同的部分（这一差别构成本发明的一个特征）。

如果如上所述成功验证的记录/再现装置20A被连接到连接部件11，则执行以下处理。

如果请求将某一储存在HDD 5中的SDMI网络内容传输到记录/再现装置20A的处理，则附加到这个SDMI网络内容的控制信号被校验以查看“MDOK”标志是否有效（DP9）。

这个MDOK标志提供控制信息指示内容服务器91或版权持有者是否允许将某些内容以解密状态复制和记录到作为辅助记录介质的微型盘的信息。即，MDOK标志是预置在内容服务器91侧的控制信息。

应注意，“MDOK”是一个标志名，它的提供是为了方便与用于例如记录/再现装置20A中的微型盘的情况相一致的说明。如果辅助记录介质100与微型盘不同，则它并不意味这个标志处理将不适用。

如果MDOK标志有效，则SDMI网络内容可以传输到记录/再现装置20A。

但是，作为进一步的条件，一旦被传输且而后复制和记录到微型盘100

的内容数据不能被校验入。

当在这些条件下将SDMI网络内容传输到记录/再现装置20A时，数据传输以加密状态在传输路径上进行。即，SDMI网络内容以上述的E（CK，A3D）或E（CK'，A3D）状态进行传输。

这个加密的SDMI网络内容在图4所示的记录/再现装置20A的接口26被接收、并且在解密部件29被解密成例如原始ATRAC3压缩数据（A3D）。而后，解密的内容数据由编码器/解码器24编码，编码的内容数据被提供到记录/再现部件25以便复制和记录到微型盘100。

因此，为再现记录/再现装置20A记录到微型盘100的SDMI内容，从微型盘100读出的数据可只在微型盘系统中以常规方式解码；即，EFM、ACIRC、和ATRAC解压缩可只在从微型盘100读出的数据上进行。

这表示复制和记录有内容数据的微型盘100在装入常规微型盘播放器时也可以再现该内容数据。即，使用常规的非符合SDMI的微型盘播放器，用户可回放复制和记录到微型盘100的SDMI网络内容以便例如欣赏音乐。

应注意，如果被传输的SDMI网络内容的MDOK标志无效，则不允许传输；这个SDMI网络内容被处理为不可复制的（DP10）。

对传输到除符合SDMI的记录/再现装置20B的其它记录/再现装置的处理被概括如下。

在下述条件都被满足时，SDMI网络内容可传输到记录/再现装置20A，即以不加密状态复制和记录到微型盘100，这些条件是：（1）记录/再现装置20A已经被成功地验证，（2）被传输的内容数据的MDOK标志有效（该传输由版权持有者授权），和（3）禁止校验入。

于是，用户能有效地使用记录到微型盘100的SDMI网络内容，因而提高了对用户的服务能力。同时，虽然在上述三个条件下允许该传输，SDMI网络内容数据不能以无条件的方式传输到除记录/再现装置20B外的其它装置，而且由于SDMI网络内容以加密状态进行传输，所以版权保护能力得到

保障。

传输处理的第二实例:

下面结合图 7 所示的数据路径说明传输处理的第二实例。应注意，将跳过对与图 6 所示步骤基本相同的 DP1－DP8 的说明；只说明被验证的记录/再现装置 20A 连接到个人计算机 1 的情况。与第一实施例不同的部分由图 7 中的虚线标出。

当经验证的记录/再现装置 20A 连接到连接部件 11 时执行后续处理。

如果请求将储存在 HDD 5 中的某一 SDMI 网络内容传输到记录/再现装置 20A 的处理，则传输处理规则校验首先在 SDMI 网络内容上执行（DP7）。即，不论连接的装置是符合 SDMI 的记录/再现装置 20B 还是验证的记录/再现装置 20A，校验出计数的上限被校验。

例如，如果 SDMI 网络内容的传输处理规则只允许有一个校验出、并且发现所述该 SDMI 网络内容在过去已经校验出到符合 SDMI 的记录/再现装置 20B（除非这个内容已经校验入），则这个内容到验证的记录/再现装置 20A 的传输被禁止。

如果用于 SDMI 网络内容的传输处理规则被清除，则附加到该 SDMI 网络内容的控制信号被校验以查看 MDOK 标志是否有效（DP7－DP9）。

如果发现 MDOK 标志无效，则禁止这个内容的传输（DP10）。

如果发现 MDOK 标志有效，则表明这个 SDMI 网络内容可以传输到辅助记录介质侧装置 20A。在这种情况下，该内容数据在传输路径上以加密状态进行传输。在记录/再现装置 20A 中，这个网络内容以解密状态复制和记录到微型盘 100。

在这个情况下，任何已经传输一次并随后复制和记录到微型盘 100 的内容数据也不能被校验入。

在这个传输处理实例中，当下述条件被满足时、允许 SDMI 网络内容向记录/再现装置 20A 传输。这些条件是:（1）记录/再现装置 20A 已经成功验

证，（2）被传输的内容数据的 MDOK 标志有效（该传输由版权持有者授权），（3）禁止校验入，和（4）不识别 SDMI 网络内容的目标装置的传输处理规则已经清除。于是，向记录/再现装置 20A 的传输被允许，SDMI 网络内容可以解密状态复制和记录到微型盘 100。

因此，可得到与上述传输处理第一实例相同的效果。同时，被允许的复制计数的上限不会因不识别连接装置的常规传输处理规则而超出，所以版权保护能力强于传输处理的第一实例。

在上述第一实施例中，从主记录介质（HDD）到辅助记录介质（微型盘）的 SDMI 网络内容的允许复制计数（可执行的校验出次数）不被限制。在上述第二实施例中，MDOK 标志通过校验 SDMI 网络内容的处理规则而确定，于是从主记录介质到辅助记录介质的 SDMI 网络内容的允许复制计数可被限制。因此，可执行比第一实施例更严格的版权保护控制。

传输处理的第三实例：

下面结合图 8 所示的数据路径说明传输处理的第三实例。应注意，将跳过与图 6 所示步骤基本相同的 DP1－DP8 的说明；只说明被验证的记录/再现装置 20A 连接到个人计算机 1 的情况。

当验证的记录/再现装置 20A 连接到连接部件 11 时执行后续处理。

如果请求储存在 HDD 5 中的某一 SDMI 网络内容向记录/再现装置 20A 的传输，则附加到这个 SDMI 网络内容的控制信号被校验以查看 MDOK 标志是否有效（DP9）。

如果发现 MDOK 标志无效，则这一内容传输不允许（DP9－DP10）。

如果发现 MDOK 标志有效，则校验用于 SDMI 网络内容的传输处理规则（DP11）。这个校验的执行独立于当连接目的地是符合 SDMI 的记录/再现装置 20B 时所执行的 DP7 的传输处理校验。即，不管到达符合 SDMI 的记录/再现装置 20B 的校验出，允许复制计数的上限被预定、并且如果在预定上限之内则请求的传输被校验。

如果发现请求的传输在上限计数之内，则这个传输处理规则校验被清除；否则，该校验不良，于是禁止该请求的传输（DP11－DP10）。

当对于该SDMI网络内容的记录/再现装置20A的传输处理规则校验被清除时，这个SDMI网络内容可传输到记录/再现装置20A。在这种情况下，内容数据以加密状态在传输路径上传输。在记录/再现装置20A中，内容数据以解密状态复制和记录到微型盘100。

在这个情况下，任何已经传输一次并随后复制和记录到微型盘100的内容数据也不能被校验入。

在这个传输处理实例中，当下述条件被满足时、允许SDMI网络内容向记录/再现装置20A传输。这些条件是:（1）记录/再现装置20A已经成功验证，（2）被传输的内容数据的MDOK标志有效（该传输由版权持有者授权），（3）禁止校验入，和（4）SDMI网络内容数据的目的地是记录/再现装置20A的情况下的传输处理规则已经清除。于是，向记录/再现装置20A的传输被允许，SDMI网络内容可以解密状态复制和记录到微型盘100。

于是，得到与连接装置是记录/再现装置20A时相同的效果。同时，用于连接装置是记录/再现装置20A的传输处理规则作为一个传输许可条件被校验，使得版权保护能力强于传输处理的第一实例、但弱于传输处理的第二实例。这里所用的“弱于”表示用户的授权使用范围扩展到某一程度、而不表示非授权复制活动被便利（至少，传输处理第一实例的版权保护能力使得更难进行这些活动）。

传输处理的第四实例:

下面结合图9所示的数据路径说明传输处理的第四实例。应注意，与图6所示步骤基本相同的DP1－DP8R 的说明被跳过。当验证的记录/再现装置20A连接到个人计算机1时的用于传输SDMI网络内容的处理（DP9和 DP10）与图5所示的处理相同。

下面，将说明SDMI盘内容的处理。

当上述验证的记录/再现装置20A被连接到连接部件11、且请求储存在HDD 5中的某一SDMI盘内容向记录/再现装置20A传输的处理时，这个SDMI盘内容向记录/再现装置20A的传输被许可。在传输路径上，内容数据以加密状态传输。在记录/再现装置20A中，内容数据以解密状态复制和记录到微型盘100。

在这种情况下，任何已经传输一次并随后复制和记录到微型盘100的内容数据也不能被校验入。

在这个传输处理实例中，当下述条件被满足时，允许SDMI网络内容向记录/再现装置20A传输，内容数据可复制和记录到微型盘100。这些条件是：（1）记录/再现装置20A已经成功验证，（2）禁止校验入。

于是，复制到微型盘100的SDMI盘内容的使用范围也可扩展。同时，通过传输目的装置的确认、禁止校验入、和以加密状态进行传输可保障该版权保护能力。

在这个实例中，MDOK标志校验不像前述实例那样进行。这是因为诸如MDOK标志的控制信息不记录到广泛使用的CD－DA和其它介质。因此，版权持有者的意向不被反映。但这并不意味传输处理的第四实例的版权保护能力不充分，这是因为对于数字复制而言，复制计数是由常规SCMS（串行复制管理系统）控制。

另外，SDMI盘内容的版权保护能力可通过执行未识别的传输目标的传输处理规则校验或执行以记录/再现装置20A作为传输目标的传输处理规则校验而进一步提高。

以上通过实例说明了本发明的优选实施例。显然，本发明不被限制在这些实例中。

例如，上述的数据传输处理操作不但可应用于SDMI内容、而且还可应用于需要版权保护的各种其它数据。

主记录介质不仅可以是HDD，也可以是许多其它储存装置。

也很明显的是，辅助记录介质和辅助记录介质侧装置 20A 不仅可以是微型盘和微型盘播放器，也可以是各种其它装置。辅助记录介质 100 也可以是 CD－R、CD－RW、DVD－RAW、DVD－R、DVD－RW 或存储卡。所以，辅助记录介质侧装置 20A 可以是与这些记录介质兼容的任何记录装置。

在上述说明中，辅助记录介质侧装置以有线或无线方式连接到作为主记录介质侧设备的个人计算机，获得版权的内容数据在这个结构中传输。显然，作为主记录介质侧装置的个人计算机可设置用于安装不符合 SDMI 的辅助记录介质（MD，CD－R 或其它介质）的槽，因此不使用辅助记录介质侧装置即可复制受版权保护的数据。

在上述实施例中，从辅助记录介质到主记录介质的校验入由个人计算机禁止。显然，这一禁止可由辅助记录介质记录/再现装置进行控制。

如上所述，根据本发明，如果满足诸如连接到数据传输装置的数据记录装置的成功校验和禁止从数据记录装置的校验入的条件，则例如储存在数据传输装置的主记录介质中、作为受版权保护的诸如 SDMI 内容的内容数据的传输被许可。另外，如果 SDMI 内容提供者（版权持有者或服务器）许可传输，则向数据记录装置的传输被许可。再有，如果规定许可复制传输计数上限的传输许可条件被满足。数据记录装置以解密状态记录接收的内容数据到达辅助记录介质。

因而，记录有内容数据的辅助记录介质（例如，微型盘）可由常规播放器回放，所以可除去对内容使用的不必要的限制。这最终将提高对于普通用户的服务能力。

在这些条件下的内容传输和复制的许可避免了出现无条件和非授权的内容复制。传输路径上的所有内容数据均被加密。这些新颖的结构对内容版权的保护作出了贡献。

虽然已借助具体形式对本发明的优选实施例作了说明，但这种说明只是示意性的，应该理解，在不脱离附权利要求书的宗旨和范围的前提下可作出

种种改进和变化。

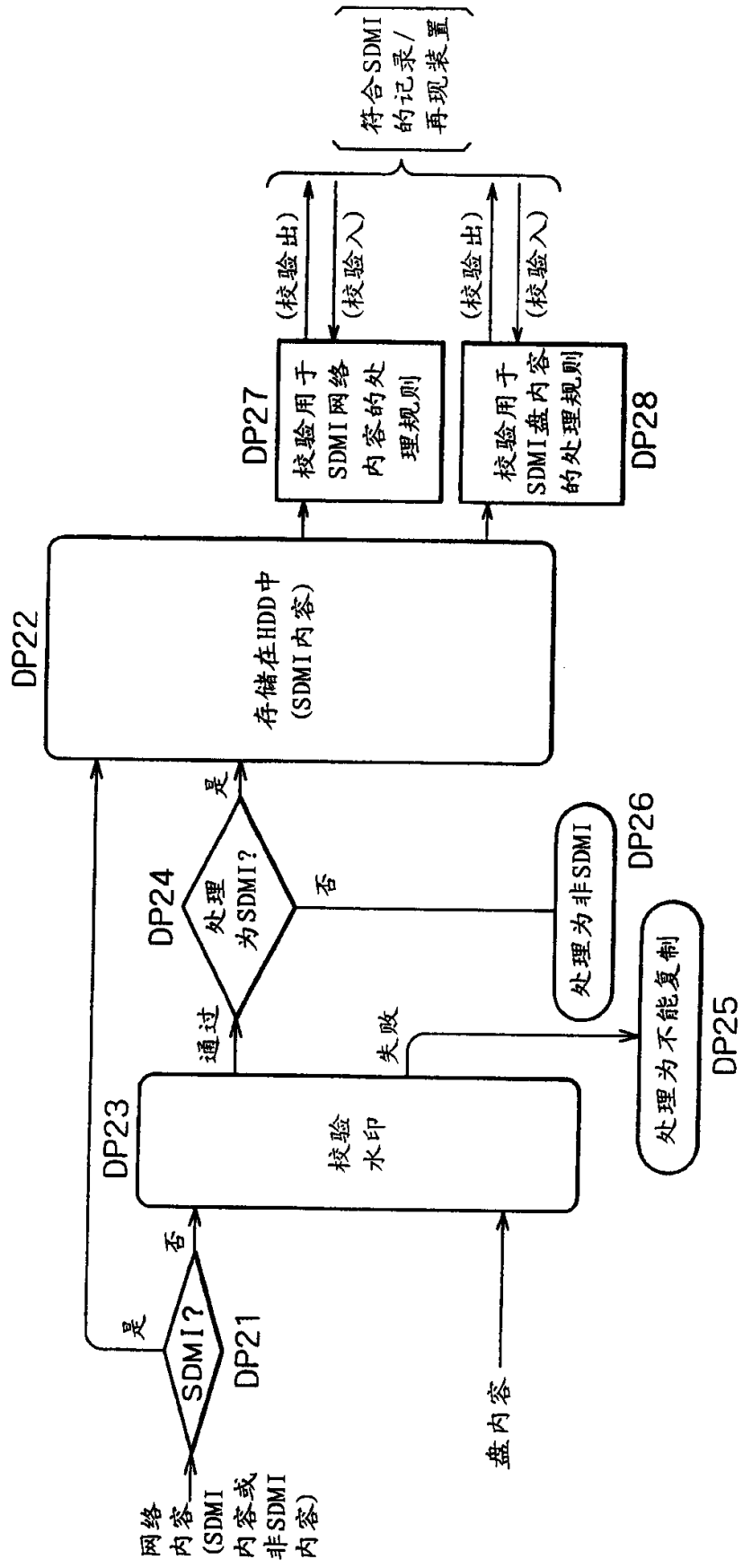

网络内容(SDMI内容或非SDMI内容)
SDMI?
DP21
是
否
盘内容
校验水印
DP23
通过
失败
处理为SDMI?
DP24
是
否
处理为非SDMI
DP26
处理为不能复制
DP25
存储在HDD中(SDMI内容)
DP22
校验用于SDMI网络内容的处理规则
DP27
校验用于SDMI盘内容的处理规则
DP28
(校验出)
(校验入)
(校验出)
(校验入)
符合SDMI的记录/再现装置

图 1

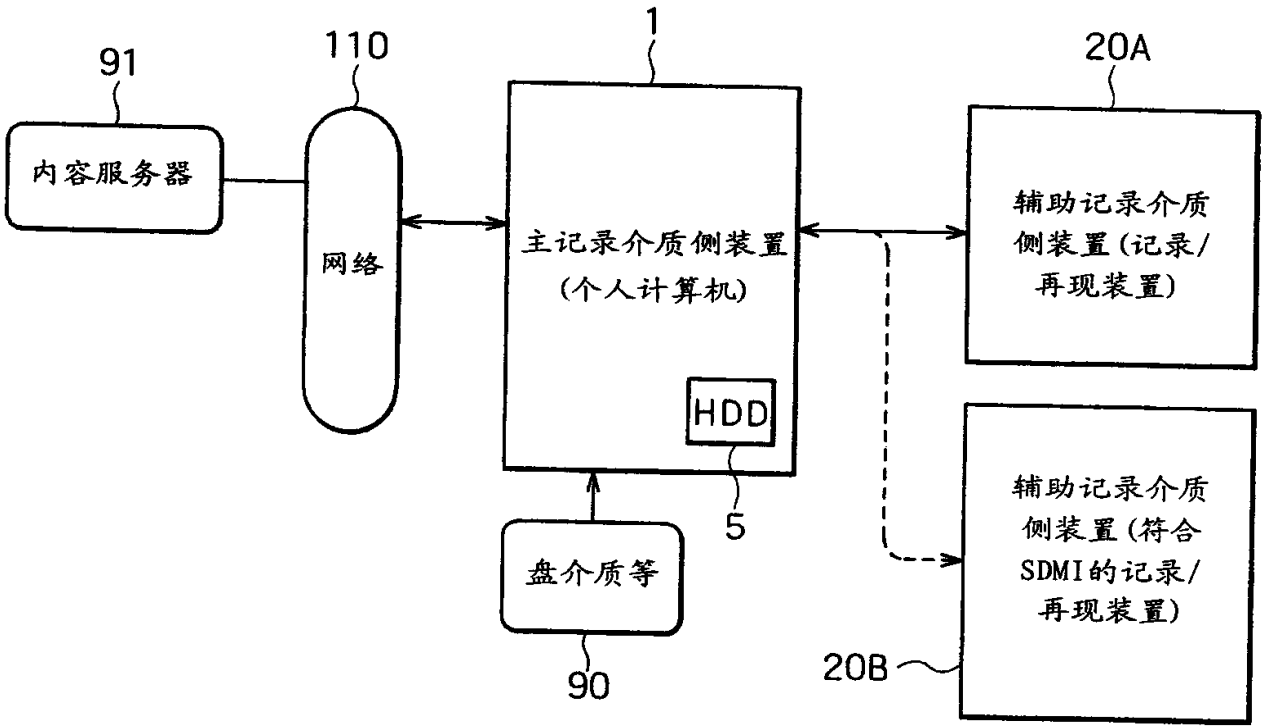

91
内容服务器
110
网络
1
主记录介质侧装置
(个人计算机)
HDD
5
盘介质等
90
20A
辅助记录介质
侧装置(记录/
再现装置)
辅助记录介质
侧装置(符合
SDMI的记录/
再现装置)
20B

图 2

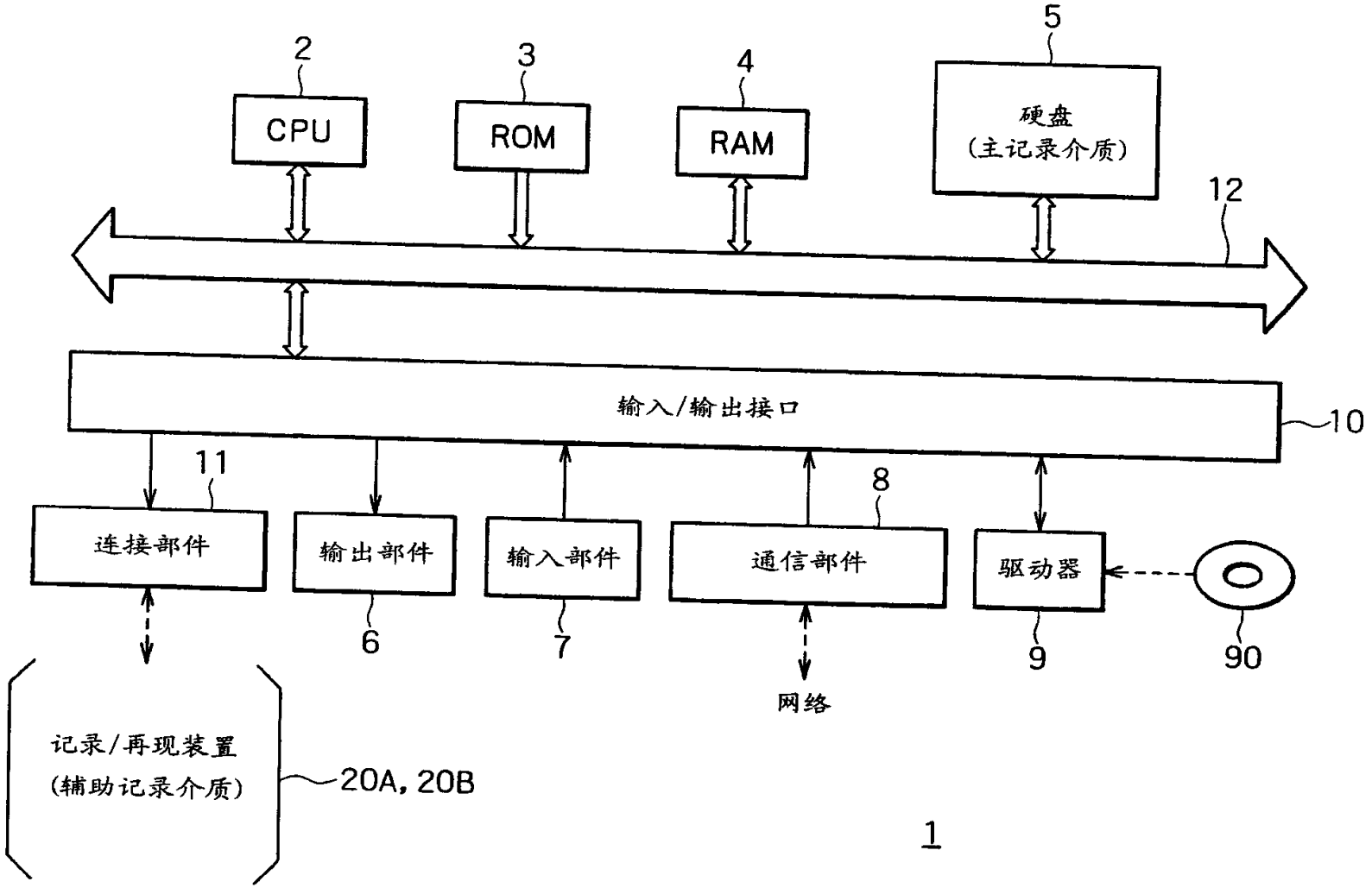

2
CPU
3
ROM
4
RAM
5
硬盘
(主记录介质)
12
输入/输出接口
10
11
连接部件
输出部件
6
输入部件
7
8
通信部件
网络
驱动器
9
90
记录/再现装置
(辅助记录介质)
20A, 20B
1

图 3

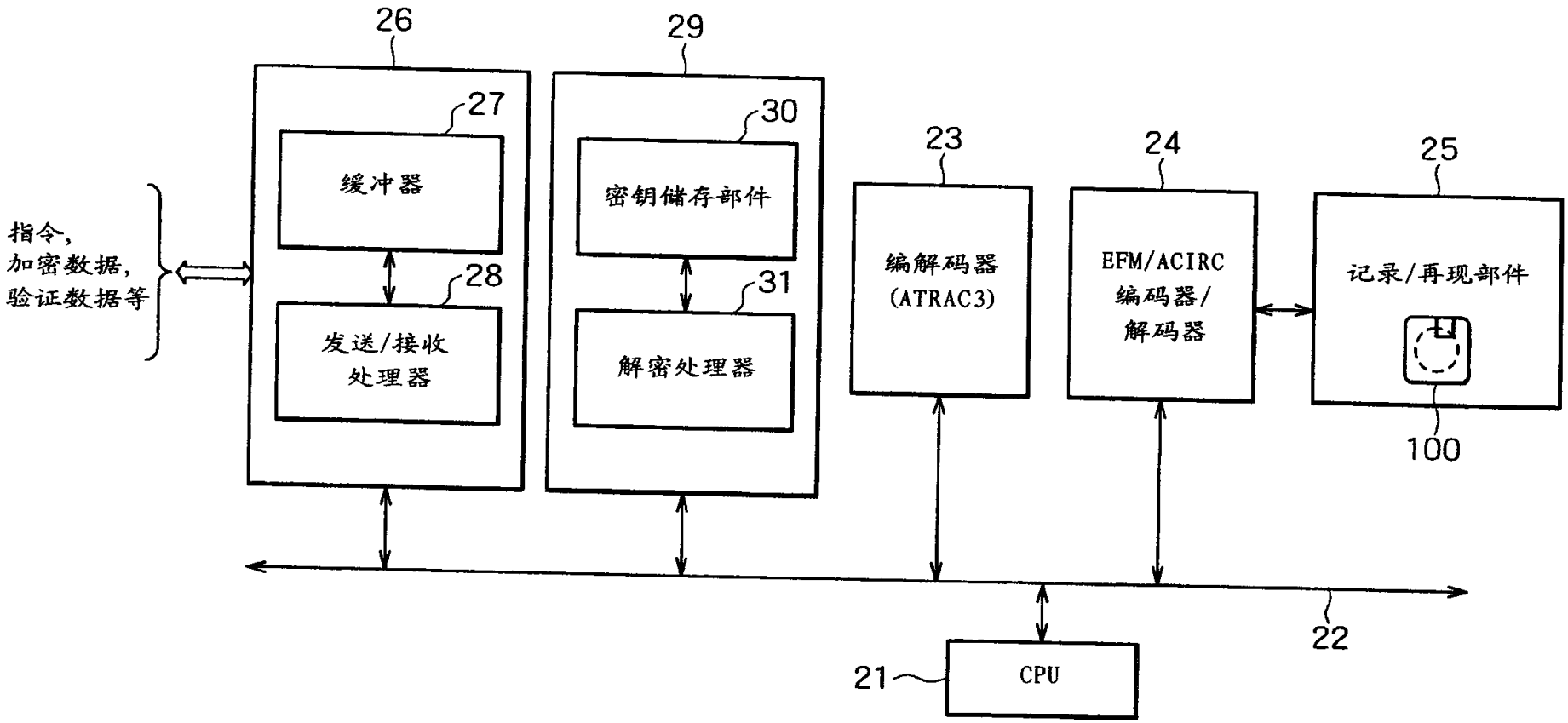

26
29
27
30
缓冲器
密钥储存部件
23
24
25
指令，
加密数据，
验证数据等
28
31
编解码器
(ATRAC3)
EFM/ACIRC
编码器/
解码器
记录/再现部件
发送/接收
处理器
解密处理器
100
22
21
CPU
20A

图 4

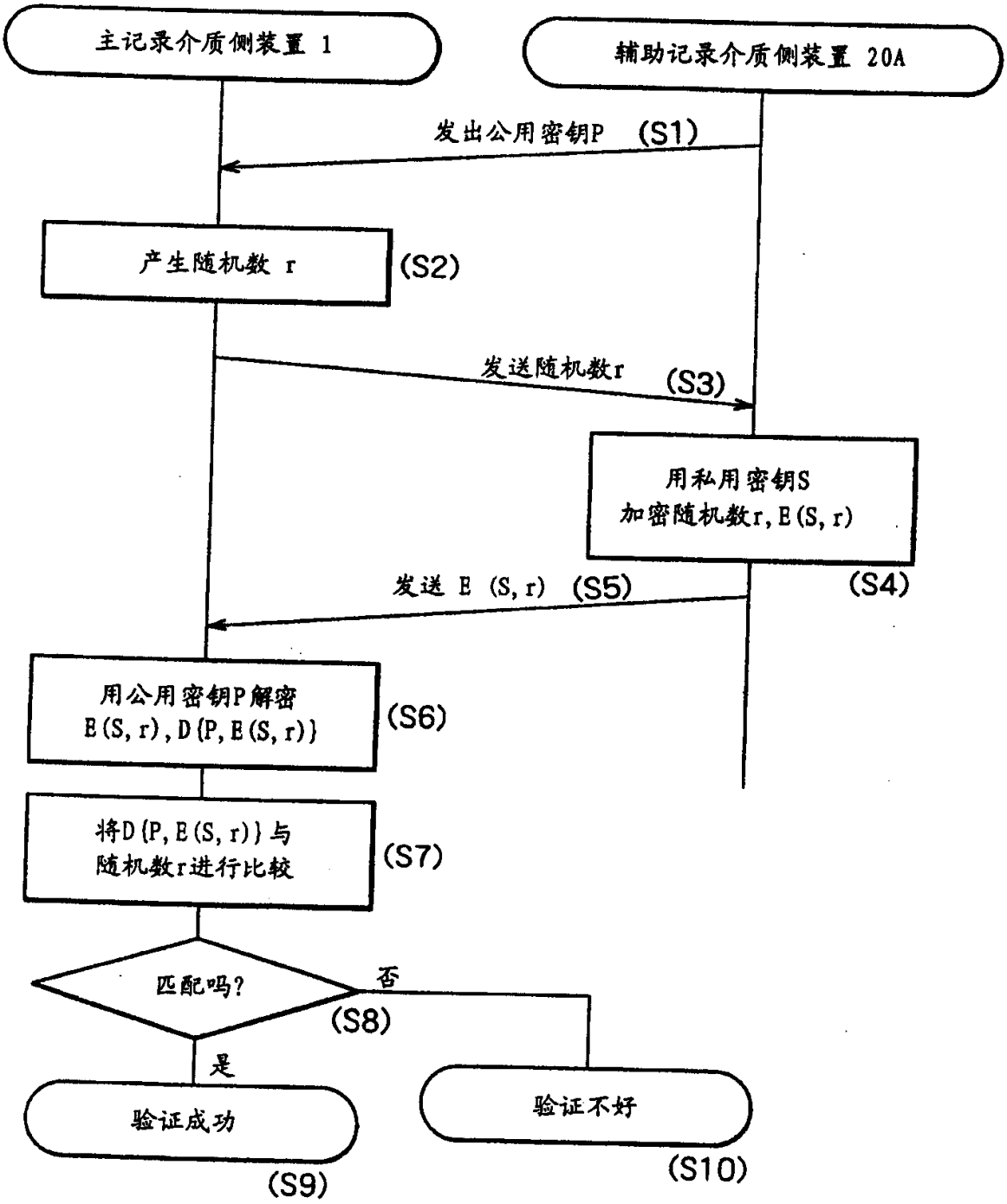

主记录介质侧装置 1
辅助记录介质侧装置 20A
发出公用密钥P (S1)
产生随机数 r
(S2)
发送随机数r
(S3)
用私用密钥S
加密随机数r, E(S, r)
(S4)
发送 E (S, r) (S5)
用公用密钥P解密
E(S, r), D{P, E(S, r)}
(S6)
将D{P, E(S, r)}与
随机数r进行比较
(S7)
匹配吗?
否
(S8)
是
验证成功
(S9)
验证不好
(S10)

图 5

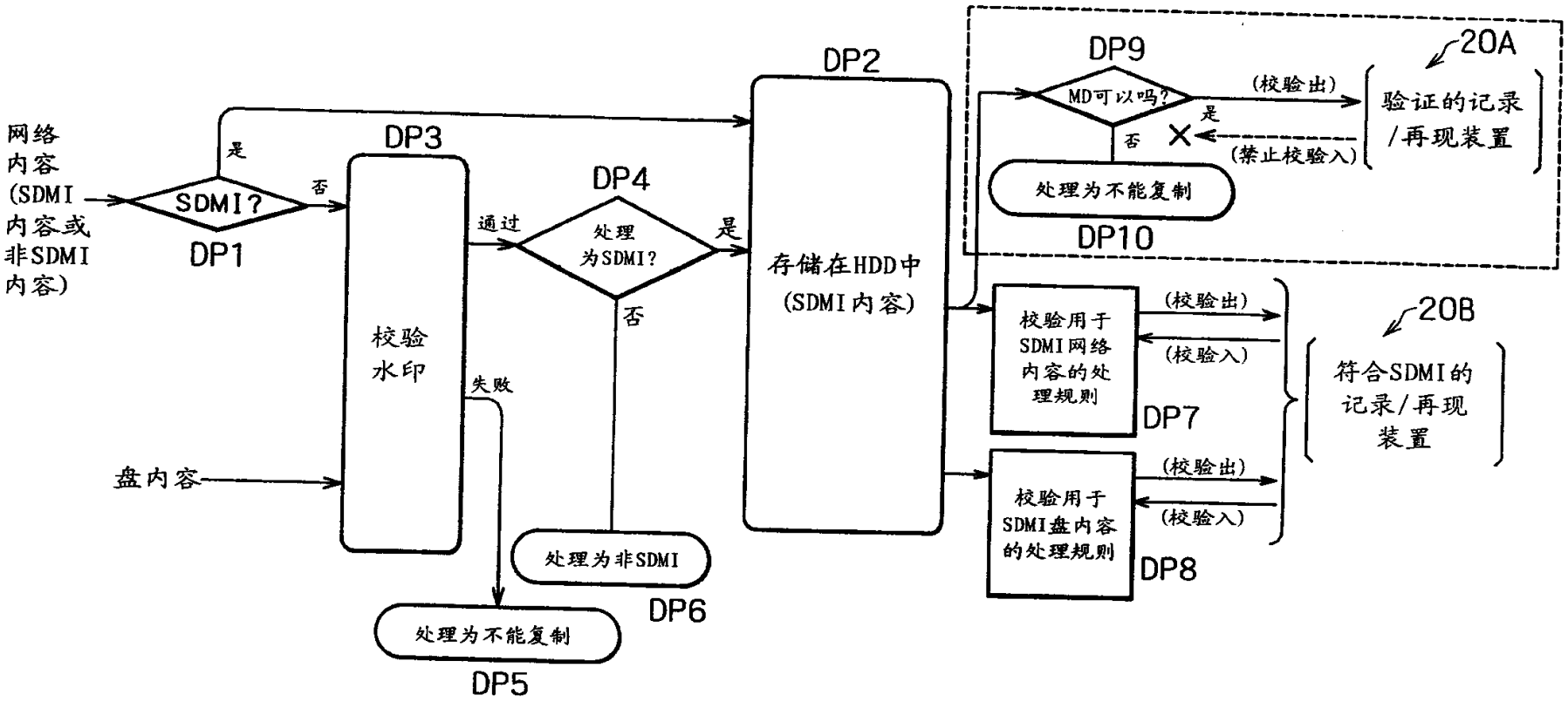

网络内容(SDMI内容或非SDMI内容)
SDMI?
DP1
是
否
DP3
校验水印
盘内容
失败
处理为不能复制
DP5
通过
处理为SDMI?
DP4
是
否
处理为非SDMI
DP6
DP2
存储在HDD中(SDMI内容)
DP9
MD可以吗?
是
否
(校验出)
(禁止校验入)
验证的记录/再现装置
20A
处理为不能复制
DP10
校验用于SDMI网络内容的处理规则
DP7
校验用于SDMI盘内容的处理规则
DP8
(校验出)
(校验入)
(校验出)
(校验入)
符合SDMI的记录/再现装置
20B

图 6

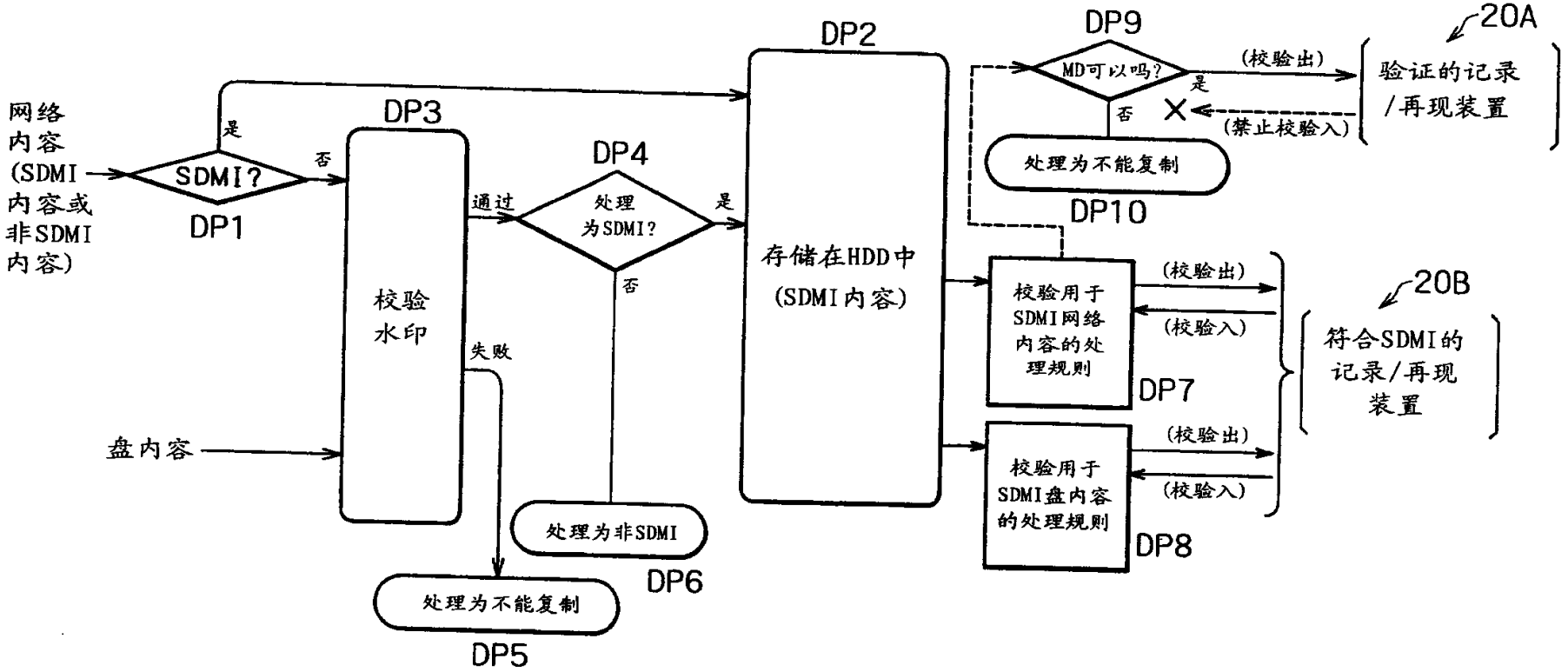

网络内容(SDMI内容或非SDMI内容)
SDMI?
DP1
是
否
DP3
校验水印
盘内容
通过
失败
处理为SDMI?
DP4
是
否
处理为非SDMI
DP6
处理为不能复制
DP5
DP2
存储在HDD中(SDMI内容)
DP9
MD可以吗?
是
否
(校验出)
(禁止校验入)
处理为不能复制
DP10
20A
验证的记录/再现装置
校验用于SDMI网络内容的处理规则
DP7
校验用于SDMI盘内容的处理规则
DP8
(校验出)
(校验入)
(校验出)
(校验入)
20B
符合SDMI的记录/再现装置

图 7

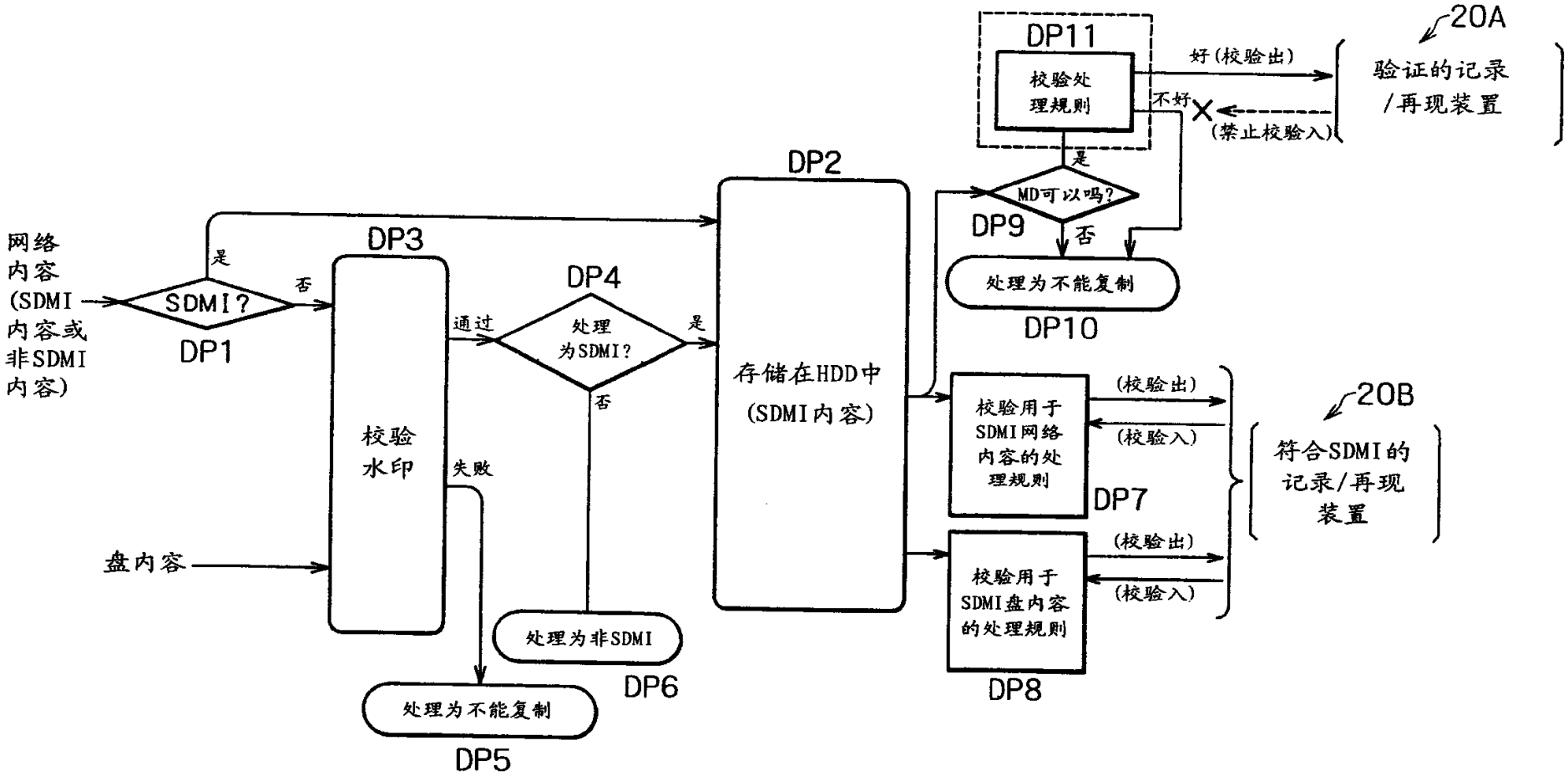

网络内容(SDMI内容或非SDMI内容)
SDMI?
DP1
是
否
DP3
校验水印
通过
失败
DP4
处理为SDMI?
是
否
盘内容
处理为非SDMI
DP6
处理为不能复制
DP5
DP2
存储在HDD中(SDMI内容)
DP11
校验处理规则
好(校验出)
不好
(禁止校验入)
20A
验证的记录/再现装置
是
MD可以吗?
DP9
否
处理为不能复制
DP10
校验用于SDMI网络内容的处理规则
DP7
(校验出)
(校验入)
校验用于SDMI盘内容的处理规则
DP8
(校验出)
(校验入)
20B
符合SDMI的记录/再现装置

图 8

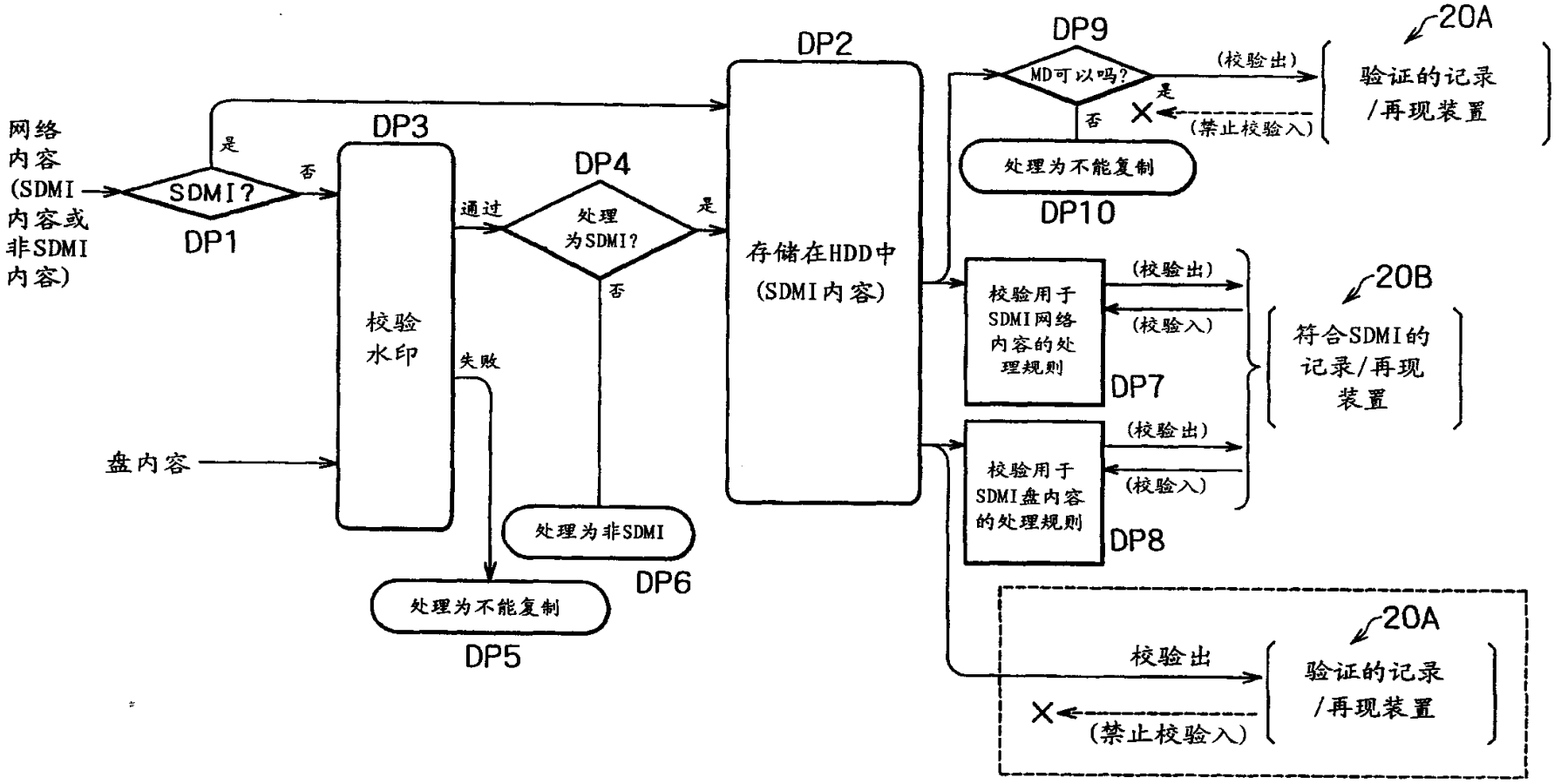

网络内容(SDMI内容或非SDMI内容)
SDMI?
DP1
是
否
DP3
校验水印
通过
失败
DP4
处理为SDMI?
是
否
盘内容
处理为非SDMI
DP6
处理为不能复制
DP5
DP2
存储在HDD中(SDMI内容)
DP9
MD可以吗?
(校验出)
是
否
(禁止校验入)
处理为不能复制
DP10
20A
验证的记录/再现装置
校验用于SDMI网络内容的处理规则
(校验出)
(校验入)
DP7
20B
符合SDMI的记录/再现装置
校验用于SDMI盘内容的处理规则
(校验出)
(校验入)
DP8
20A
校验出
(禁止校验入)
验证的记录/再现装置

图 9