

[12] 发明专利申请公开说明书

[21] 申请号 00800506.0

[43] 公开日 2001 年 6 月 20 日

[11] 公开号 CN 1300398A

[22] 申请日 2000.2.17 [21] 申请号 00800506.0

[30] 优先权

[32] 1999.2.17 [33] JP [31] 39218/1999

[86] 国际申请 PCT/JPOO/00904 2000.2.17

[87] 国际公布 WO00/49510 日 2000.8.24

[85] 进入国家阶段日期 2000.12.5

[71] 申请人 索尼公司

地址 日本东京都

[72] 发明人 河上达 石黑隆二

田边充 江面裕一

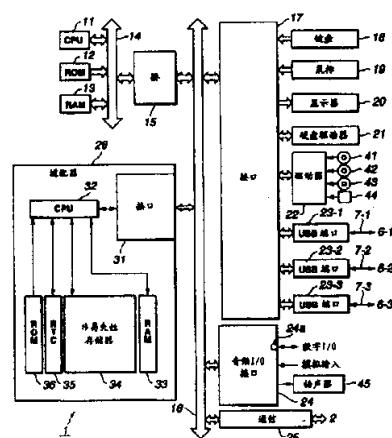
[74] 专利代理机构 柳沈知识产权律师事务所
代理人 宋军

权利要求书 15 页 说明书 47 页 附图页数 36 页

[54] 发明名称 信息处理设备和方法, 以及程序存储介质

[57] 摘要

个人计算机(1)的 CPU(11)指令控制由半导体 IC 组成的适配器(26)的 CPU(32), 以计算用于管理记录在 HDD(21)中的内容的音调数据库的哈希值, 并将该哈希值保存到非易失性存储器(34)中。当回放记录在 HDD(21)中的内容时, CPU(11)计算所述音调数据库的哈希值, 将它同保存在非易失性存储器(34)中的哈希值进行比较, 并根据比较的结果控制从 HDD(21)中回放内容。



I S S N 1 0 0 8 - 4 2 7 4

权 利 要 求 书

1、一种信息处理设备，包括：

用于储存内容数据的装置；

5 具有软件的控制装置，该软件控制在内容数据存储装置中保存或从该内
容数据存储装置中读取内容数据；以及

提供的在硬件上独立于控制装置的装置，用以解密和执行从控制装置提
供的加密程序，并将程序执行的结果提供给控制装置；

10 所述控制装置根据所述程序执行装置提供的程序执行结果，控制在内容
数据存储装置中保存或从内容数据存储装置中读取内容数据。

2、如权利要求1所述的设备，其中：

所述内容数据存储装置还保存管理信息，利用所述管理信息来管理保存
在该装置中的内容数据；以及

15 所述控制装置使程序执行装置根据所述管理信息执行预先确定的计
算。

3、如权利要求1所述的设备，其中：

所述控制装置是CPU；

所述内容数据存储装置是硬盘；以及

20 所述程序执行装置是包含在半导体IC中的CPU，而不是作为控制装置
的CPU。

4、一种由信息处理设备所使用的信息处理方法，所述信息处理设备包
括：

用于保存内容数据的装置；

具有软件的控制装置，控制将内容数据保存在存储装置中或从该内容数

25 据存储装置中读取内容数据；以及

提供的在硬件上独立于控制装置的装置，用以解密和执行从控制装置提
供的加密程序，并将程序执行的结果提供给控制装置；

所述信息处理方法包括步骤：

根据程序执行装置的程序执行结果，控制在所述内容数据存储装置中保

30 存或从所述内容数据存储装置中读取内容数据。

5、一种由信息处理设备所使用的程序存储介质，所述信息处理设备包

括：

用于保存内容数据的装置；

具有软件的控制装置，用于控制在内容数据存储装置中保存或从该内容数据存储装置中读取内容数据；以及

5 提供的在硬件上独立于控制装置的装置，用以解密和执行从控制装置提供的加密程序，并将程序执行的结果提供给控制装置；

所述程序存储介质，设计成在控制装置中使用，且在其中记录有计算机可读程序的介质，该程序包括步骤：根据程序执行装置的程序执行结果，控制在所述内容数据存储装置中存储内容数据或从该内容数据存储装置中读取内容数据。

6、一种信息处理设备，包括：

用于输入内容数据的装置；

用于保存从输入装置提供的内容数据的装置；

15 用于以预先确定的方式、压缩保存在内容数据存储装置中的内容数据的装置；

用于以预先确定的方式加密保存在内容数据存储装置中的内容数据的装置；以及

用于控制在内容数据存储装置中保存或从内容数据存储装置中读取内容数据的装置，该内容数据是由压缩装置压缩和由加密装置加密的内容数据。

20 7、如权利要求 6 所述的设备，其中，以同样的方式，压缩装置压缩或加密装置加密从输入装置提供的不同的数据。

8、如权利要求 6 所述的设备，其中，以同样的方式，压缩装置压缩或加密装置加密从输入装置提供的不同的数据，并且采用预先确定的公共压缩或加密方式将从内容数据存储装置读取的数据输出到预先确定的设备。

9、一种信息处理方法，包括步骤：

输入数据；

保存从数据输入步骤提供的数据；

以预先确定的方式压缩在数据存储步骤保存的数据；

30 以预先确定的方式加密在数据存储步骤保存的数据；以及

控制在压缩步骤压缩和在加密步骤加密的数据的存储或读取。

10、一种程序存储介质，在其中记录有由信息处理设备执行和由计算机可读的程序，所述程序包括步骤：

输入数据；

保存从数据输入步骤提供的数据；

5 以预先确定的方式压缩在数据存储步骤保存的数据；

以预先确定的方式加密在数据存储步骤保存的数据；以及

控制在压缩步骤压缩和在加密步骤加密的数据的存储或读取。

11、一种信息处理设备，包括：

用于输入内容数据的装置；

10 用于保存从内容数据输入装置提供的内容数据的装置；

用于持有保存在内容数据存储装置中的内容数据的管理信息的装置；

用于根据在管理信息持有装置中持有的管理信息进行预先确定的计算的装置；以及

依据对于计算装置的计算结果与保存在内容数据存储装置中的以前计

15 算结果的比较，用于控制保存在内容数据存储装置中的内容数据的使用的装置。

12、如权利要求 11 所述的设备，其中计算装置使用作为管理信息的哈希函数进行计算。

13、如权利要求 11 所述的设备，其中所述数据是音乐数据，并且所述

20 管理信息包括用于识别音乐数据的识别信息。

14、一种信息处理方法，包括步骤：

输入数据；

保存在数据输入步骤提供的数据；

持有在数据存储步骤保存的数据的管理信息；

25 根据在管理信息持有步骤所持有的管理信息进行预先确定的计算；

保存在计算步骤所做的计算结果；以及

比较在计算步骤所做的计算结果与在数据存储步骤中保存的以前的计算结果，以控制在数据存储步骤所保存的数据的使用。

15、一种程序存储介质，在其中记录有信息处理设备要执行和计算机可

30 读的程序，所述程序包括步骤：

输入数据；

- 保存从数据输入步骤提供的数据；
持有在数据存储步骤中所保存的数据的管理信息；
根据在管理信息持有步骤所持有的管理信息进行预先确定的计算；
保存在计算步骤所做的计算结果；以及
5 依据对于在计算步骤的计算结果与在数据存储步骤中保存的以前计算结果的比较的结果，控制在数据存储步骤中所保存的数据的使用。
- 16、一种信息处理设备，包括：
用于向其它设备发送数据，和从其它设备接收数据的装置；
用于持有预先确定的锁密钥和副本密钥的装置；
10 使用持有装置持有的锁密钥的认证装置，当向其它设备发送数据和从其它设备接收数据时，与其它设备进行相互认证，以产生通信密钥；
用于使用副本密钥加密通信密钥的装置；以及
用于保存在数据发送和接收装置中接收的数据的装置，该数据已由与加密装置加密的通信密钥相对应的通信密钥加过密。
- 15 17、如权利要求 16 所述的设备，还包括：
加密密钥解密装置，使用副本密钥解密保存在存储装置中的通信密钥；
以及
用于解密在存储装置中保存的数据的装置。
- 18、一种信息处理方法，包括步骤：
20 向其它设备发送数据，和从其它设备接收数据；
持有预先确定的锁密钥和副本密钥；
使用在持有步骤持有的锁密钥，当向其它设备发送数据和从其它设备接收数据时，与其它设备进行相互认证，以产生通信密钥；
使用副本密钥加密通信密钥；以及
25 保存在数据发送和接收步骤中接收的数据，该数据已由与加密步骤中加密的通信密钥相对应的通信密钥加过密。
- 19、一种程序存储介质，在其中记录有信息处理装置要执行和计算机可读的程序，所述程序包括步骤：
向其它设备发送数据，和从其它设备接收数据；
30 持有预先确定的锁密钥和副本密钥；
使用在持有步骤持有的锁密钥，当向其它设备发送数据和从其它设备接

收数据时，与其它设备进行相互认证，以产生通信密钥；

使用副本密钥加密通信密钥；以及

保存数据发送和接收步骤中接收的数据，所述数据已由与与加密步骤中加密的通信密钥相对应的通信密钥加过密。

5 20、一种信息处理设备，包括：

存储装置，用于保存数据；

持有装置，用于持有保存在数据存储装置中数据的使用规则；

判断装置，当将保存在数据存储装置中的数据移动到其它设备时，用于判断保存在数据存储装置中的数据的使用规则是否可由其它设备复制；以及

10 移动装置，根据判断装置的判断结果，将保存在存储装置中的数据以及保存在数据存储装置中的数据的使用规则移动到其它设备，所述数据的使用规则由持有装置持有。

21、如权利要求 20 所述的设备，其中数据的使用规则包括：

回放限制条件；

15 回放计帐条件；或

复制限制条件。

22、一种信息处理方法，包括步骤：

保存数据；

持有在数据存储步骤保存的数据的使用规则；

20 当将在数据存储步骤中保存的数据移动到其它设备时，判断在数据存储步骤中保存的数据的使用规则是否可由其它设备复制；以及

根据判断步骤的判断结果，将保存在存储装置中的数据以及在数据存储步骤中保存的数据的使用规则移动到其它设备，所述数据的使用规则在持有步骤中持有。

25 23、一种程序存储介质，在其中记录有信息处理装置要执行和计算机可读的程序，该程序包括步骤：

保存数据；

持有在数据存储步骤中保存的数据的使用规则；

当将在数据存储步骤中保存的数据移动到其它设备时，判断在数据存储步骤中保存的数据的使用规则是否可由其它设备复制；以及

30 根据判断步骤的判断结果，将保存在存储装置中的数据以及在数据存储

000.10.05

步骤中保存的数据的使用规则移动到其它设备，所述数据的使用规则在持有
步骤中持有。

说 明 书

信息处理设备和方法，以及程序存储介质

5 技术领域

本发明涉及信息处理设备和方法，以及程序存储介质，特别涉及适合于阻止伪造使用数据的软件，以防止欺诈性地复制这些数据的信息处理设备和方法，以及涉及程序存储介质，在其中记录了用于阻止欺诈性复制的信息处理程序。

10

背景技术

目前，随着数字技术的进展和广泛应用，在记录介质上数字地记录多种音乐数据、图像数据等，或从记录介质上回放多种音乐数据、图像数据等已成为可能。结果，甚至重复复制数据多次也可能获得在图像或声音质量上不15 低于原始数据的数据。

但是，随着数字技术的发展，出现了下述问题：

(1) 例如，当数字音乐数据从紧凑盘(compact disk, CD)复制到个人计算机的硬盘上时，CD 上的音乐数据就可被原样地记录或压缩到硬盘上，这样，该音乐数据通过例如因特网的网络被欺诈地大量散发了。

20 (2) 当数字音乐数据从 CD 复制到个人计算机的硬盘上时，由于复制的次数没有限制，所以音乐数据将被大量地散发。

(3) 当数字音乐数据从个人计算机的硬盘复制到外部设备，如便携设备时，在复制后，由于原始的数字音乐数据仍将保留在硬盘上，这样将可能大量地复制和散发。

25 (4) 为阻止上述问题(3)，应设计个人计算机的软件，以使在数字音乐数据复制到外部设备后，删除作为数据源的硬盘中的数据 (移走音乐数据)。但是，如果硬盘中的内容在移走之前被备份在另一个记录介质上，备份的数据在移走之后就能重新恢复到硬盘上，已经移走的数据仍将保留在硬盘上。

(5) 当个人计算机硬盘上的数字音乐数据复制到外部设备，如便携设备30 时，由于不确认是哪种类型的外部设备，就可能传递给非法设备。

当数字音乐数据从外部设备如便携设备传递到个人计算机时，由于不确

认控制个人计算机软件的类型，就可能传递给非法软件。

- (6) 当在个人计算机上处理从 CD 复制的音乐数据时，包含在音乐数据中的 ISRC(International Standard Recording Code, 国际标准记录代码)可用于判别一首音乐是否与其音乐它的相同。但是 CD 中可能不包含 ISRC 数据。
- 5 在这种情况下，就不可能判别这些音乐是否彼此相同。

(7) 在个人计算机软件的控制下可以执行上述功能。但是，如果软件本身被改变了，那么将可能产生系统设计者不希望的操作。

本发明的说明

10 因此，本发明的一个目的，就是通过提供信息处理设备和方法，积极地防止别人通过分析和伪造使用这些数据的软件，将数据大量地欺诈性地复制，并且通过提供其中记录了信息处理程序的程序存储介质，来克服上述现有技术的缺点。

15 依据本发明的信息处理设备包括：存储内容数据的装置，具有软件的控制装置，控制将内容数据保存到内容数据存储装置，或从内容数据存储装置读取内容数据，以及在硬件上独立于控制装置的装置，用于解密和执行控制装置提供的加密程序，并将程序执行的结果提供给控制装置；控制装置根据程序执行装置提供的程序执行结果，控制将内容数据保存到内容数据存储装置，或从内容数据存储装置读取内容数据。在信息处理装置中，内容数据存储装置还保存管理信息，利用管理信息管理它自己保存的内容数据，并且控制装置根据管理信息使程序执行装置执行预先确定的计算。控制装置也可以是 CPU，内容数据存储装置可以是硬盘，程序执行装置可以是包含在半导体 IC 中的 CPU，而不是构成控制装置的 CPU。

20 上述目的还可通过提供一种信息处理方法来达到，依据本发明，该信息处理方法包括：根据程序执行装置的程序执行结果，控制将内容数据保存到内容数据存储装置，或从内容数据存储装置读取内容数据的步骤。

25 上述目的还可通过提供一种在其中记录有程序的程序存储介质来达到，依据本发明，包括根据程序执行装置的程序执行结果，控制将内容数据保存到内容数据存储装置，或从内容数据存储装置读取内容数据的步骤。

30 上述目的还可通过提供一种信息处理设备来达到，依据本发明，该设备包括：输入内容数据的装置；存储输入装置提供的内容数据的装置；以预先

确定的方式压缩存储在内容数据存储装置中的内容数据的装置；以预先确定的方式加密保存在内容数据存储装置中数据的装置；控制在内容数据存储装置中存储或从内容数据存储装置中读取数据，以及控制保存和读取由压缩装置压缩和由加密装置加密的数据的装置。

5 上述目的还可通过提供一种信息处理方法来达到，依据本发明，该方法包括步骤：输入数据；保存由输入数据步骤提供的数据；以预先确定的方式压缩在数据存储步骤中保存的数据；以预先确定的方式加密在数据存储步骤中保存的数据；以及控制在压缩步骤压缩数据的存储或读取和控制在加密步骤加密数据的存储或读取。

10 上述目的还可通过提供一种程序存储介质来达到，该程序存储介质中记录有希望由信息处理设备执行和计算机可读的程序，依据本发明，该程序包括步骤：输入数据；保存由输入数据步骤提供的数据；以预先确定的方式压缩在数据存储步骤中保存的数据；以预先确定的方式加密在数据存储步骤中保存的数据；以及控制在压缩步骤压缩数据的存储或读取和控制在加密步骤
15 加密数据的存储或读取。

上述目的还可通过提供一种信息处理设备来达到，依据本发明，该设备包括：输入内容数据的装置；存储内容数据输入装置提供的内容数据的装置；持有保存在内容数据存储器装置中的内容数据管理信息的装置，根据管理信息持有装置中持有的管理信息，进行预先确定的计算的装置；依据计算装置计算的结果和保存在内容数据存储装置中的过去的计算结果的比较结果，控制保存在内容数据存储装置中的内容数据的使用的装置。
20

上述目的还可通过提供一种信息处理方法来达到，依据本发明，该方法包括步骤：输入数据；存储数据输入步骤中提供的数据；持有在数据存储步骤中保存的数据的管理信息，根据在管理信息持有步骤中持有的管理信息，
25 进行预先确定的计算；保存计算步骤中的计算结果，依据计算步骤中的计算结果和在数据存储步骤中保存的过去的计算结果的比较结果，控制在数据存储步骤中保存的数据的使用。

上述目的还可通过提供一种程序存储介质来达到，该程序存储介质中记录有希望由信息处理设备执行和计算机可读的程序，依据本发明，该程序包括步骤：输入数据；存储数据输入步骤中提供的数据；持有在数据存储步骤中保存的数据的管理信息，根据在管理信息持有步骤中持有的管理信息，进
30

行预先确定的计算；保存计算步骤中的计算结果，依据计算步骤中的计算结果和在数据存储步骤中保存的过去的计算结果的比较结果，控制在数据存储步骤中保存的数据的使用。

上述目的还可通过提供一种信息处理设备来达到，依据本发明，该设备
5 包括：向其它设备发送和从其它设备接收数据的装置；持有预先确定的锁密
钥和副本密钥的装置；使用持有装置中的锁密钥的认证装置，当向其它装置
发送和从其它装置接收数据时，与其它设备进行相互认证以产生通信密钥；
使用副本密钥加密通信密钥的装置；以及保存由数据发送和接收装置接收
10 的，并使用通信密钥加过密的数据的装置，而该通信密钥相应于加密装置加
密的通信密钥。

上述目的还可通过提供一种信息处理方法来获得，依据本发明，该方法
包括步骤：向其它设备发送和从其它设备接收数据；持有预先确定的锁密钥
和副本密钥；当向其它装置发送和从其它装置接收数据时，使用持有步骤中
的锁密钥，与其它设备进行相互认证以产生通信密钥；使用副本密钥加密通
信密钥；以及保存在数据发送和接收步骤中接收的，并使用通信密钥加过密
15 的数据，而该通信密钥相应于加密步骤中加密的通信密钥。

上述目的还可通过提供一种程序存储介质来达到，该程序存储介质中记
录有希望由信息处理设备执行和计算机可读的程序，依据本发明，该程序包
括步骤：向其它设备发送和从其它设备接收数据；持有预先确定的锁密钥和
20 副本密钥；当向其它装置发送和从其它装置接收数据时，使用持有步骤中的
锁密钥，与其它设备进行相互认证以产生通信密钥；使用副本密钥加密通
信密钥；以及保存在数据发送和接收步骤中接收的，并使用通信密钥加过密
的数据，而该通信密钥相应于加密步骤中加密的通信密钥。

上述目的还可通过提供一种信息处理设备来达到，依据本发明，该设备
25 包括：存储数据的装置；持有保存在数据存储装置中数据的使用规则的装
置，判断当将保存在数据存储装置中的数据移动到其它设备时，保存在数据
存储装置中的数据使用规则可否由其它设备复制的装置；以及根据判断装置
的判断结果，将保存在数据存储装置中的数据，连同保存在数据存储装置中
数据的使用规则移动到其它设备的装置，数据的使用规则由持有装置持有。

30 上述目的还可通过提供一种信息处理方法来达到，依据本发明，该方法
包括步骤：存储数据；持有在数据存储步骤中保存的数据的使用规则，判断

当将在数据存储步骤中保存的数据移动到其它设备时，在数据存储步骤中保存的数据使用规则可否由其它设备复制；以及根据在判断步骤中的判断结果，将保存在数据存储装置中的数据，连同在数据存储步骤中保存的数据的使用规则移动到其它设备的装置，数据的使用规则在持有步骤中持有。

5 上述目的还可通过提供一种程序存储介质来达到，该程序存储介质中记录有希望由信息处理设备执行和计算机可读的程序，依据本发明，该程序包括步骤：存储数据；持有在数据存储步骤中保存的数据的使用规则，判断当将在数据存储步骤中保存的数据移动到其它设备时，在数据存储步骤中保存的数据使用规则可否由其它设备复制；以及根据在判断步骤中的判断结果，
10 将保存在数据存储装置中的数据，连同在数据存储步骤中保存的数据的使用规则移动到其它设备的装置，数据的使用规则在持有步骤中持有。

附图的简要说明

图 1 表示依据本发明的一个内容数据管理系统的实施例。

15 图 2 说明在内容数据管理系统中使用的个人计算机的结构。

图 3 说明包括在内容数据管理系统中的便携设备的结构。

图 4 是用于说明个人计算机功能的个人计算机的方框图。

图 5 表示一个显示/操作指导窗口的例子。

图 6 表示一个记录程序使得显示单元显示的窗口的例子。

20 图 7 是在将内容从紧凑盘复制到 HDD 所产生的操作的流程图。

图 8 是在图 7 流程图的步骤 S12 中检查时间限制数据库所产生的操作的流程图。

图 9 是一个时间限制数据库的例子。

图 10 说明了水印(water mark)。

25 图 11 表示一个音乐数据库的例子。

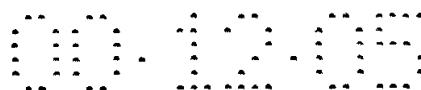
图 12 是将内容从 HDD 移动到便携设备所产生的操作的流程图。

图 13 是将内容从 HDD 移动到便携设备所产生的操作的流程图。

图 14 是将内容从 HDD 移动到便携设备所产生的操作的流程图。

30 图 15 是在图 12 流程图的步骤 S55 中检查所选择内容回放条件而产生的操作的流程图。

图 16 说明便携设备管理的回放条件。



- 图 17 是在图 12 流程图的步骤 S58 中进行格式转换所产生的操作的流程图。
- 图 18 是将内容从 HDD 复制到便携设备所产生的操作的流程图。
- 图 19 是将内容从 HDD 复制到便携设备所产生的操作的流程图。
- 5 图 20 是将内容从 HDD 复制到便携设备所产生的操作的流程图。
- 图 21 是将内容从 HDD 复制到便携设备所产生的操作的流程图。
- 图 22 是将内容从便携设备复制到 HDD 所产生的操作的流程图。
- 图 23 是将内容从 EMD 服务器复制到 HDD 所产生的操作的流程图。
- 图 24 是在图 23 流程图的步骤 S58 中记帐所产生的操作的流程图。
- 10 图 25 说明记帐日志。
- 图 26 是将内容从个人计算机的 IEC60958 终端复制到 HDD 所产生的操作的流程图。
- 图 27 是将内容从个人计算机的 IEC60958 终端复制到 HDD 所产生的操作的流程图。
- 15 图 28 是将内容从个人计算机的 IEC60958 终端复制到 HDD 所产生的操作的流程图。
- 图 29 是将内容从个人计算机的 IEC60958 终端复制到 HDD 所产生的操作的流程图。
- 图 30 在图 28 流程图的步骤 S275 中检查回放条件操作的流程图。
- 20 图 31 是内容从 HDD 输出给便携设备将所产生的操作的流程图。
- 图 32 是内容从 HDD 输出给便携设备将所产生的操作的流程图。
- 图 33 说明非易失性存储器的功能。
- 图 34 是适配器操作的流程图。
- 图 35 表示适配器的内部结构。
- 25 图 36A 和 36B 分别是表示非易失性存储器内部结构的例子。
- 图 37 是一个表示非易失性存储器内部结构的例子。

实施本发明的最好模式

下面将参考附图进一步详细说明实施本发明的最好模式。

- 30 图 1 表示依据本发明的一个内容数据管理系统的实施例。内容数据管理系统包括个人计算机 1，连接到包括局域网或因特网的网络 2。个人计算机 1

以预先确定的方式压缩从 EMC(Electrical Music Distribution, 电子音乐分配)服务器 4-1 到 4-3 接收的或从 CD(紧凑盘)读取的音乐数据(以下称为“内容”),这些将在后面进一步说明,并且通过诸如 DES(Data Encryption Standard, 数据加密标准)等加密方法加密压缩的内容,进行记录。

5 个人计算机 1 还记录使用该内容的使用规则,作为一项被加密和记录的内容。

使用规则表明,例如,多个便携设备(象可能的情况那样缩写为“PD”)能按照规则同时使用内容。PD 的数量这里称为能登出内容的多个 PD, 将在对它们进一步说明。即使已经登出包含在使用规则中的多项内容之后, 10 个人计算机 1 也能回放该内容。

否则, 使用规则可能表明该内容可以被复制。当该内容被复制到便携设备 6-1 到 6-3 中时, 个人计算机 1 可以回放所记录的内容。该内容被保存到便携设备 6-1 到 6-3 中多次, 该次数象可能的情况那样, 是有限制的。在这种情况下, 该内容可以被复制多次, 该次数将不再增加。

15 另一种选择是, 使用规则可能表明该内容可以被移动到其它的计算机中。在该内容被移动到便携设备 6-1 到 6-3 之后, 记录在计算机 1 中的内容就不能使用了(该内容被删除了或使用规则改变了)。

使用规则将在后面详细说明。

20 个人计算机 1 将所加密和记录的内容及与内容有关的数据(例如, 每首音乐的标题或回放条件等)一起通过 USB(Universal Serial Bus, 通用串行总线)电缆 7-1 保存到所连接的便携设备 6-1 中, 并将所保存内容的使用规则更新到便携设备 6-1 中(这种操作将在下面称为“登出(check-out)”), 以作为对内容存储的响应。更具体地说, 当内容被登出后, 包含在内容使用规则中和记录在个人计算机中的内容可以被登出的次数就减 1。因此, 当一项内容可以被登出的次数变为零时, 按照使用规则, 该内容就再也不能被登出了。

30 个人计算机 1 也将加密的和记录的内容及与内容有关的数据一起通过 USB 电缆 7-2 保存到所连接的便携设备 6-2, 并将所保存内容的使用规则更新到便携设备 6-2 中, 以作为对内容存储的响应。而且, 个人计算机 1 也将所加密和记录的内容及与内容有关的数据一起通过 USB 电缆 7-3 保存到所连接的便携设备 6-3 中, 并将所保存内容的使用规则更新到便携设备 6-3 中, 以作为对内容存储的响应。

计算机 1 通过 USB 电缆 7-1 也将使与其连接的便携备 6-1 删 5 去个人计算机 1 已经登出的内容，或禁止便携设备 6-1 使用个人计算机 1 已经登出的内容，因此更新所删除内容的使用规则(该操作以下称为登入(check-in))。更具体地说，当内容被登入之后，包含在内容使用规则并记录在个人计算机 1 中的内容可以被登入的次数就增加 1。

计算机 1 通过 USB 电缆 7-2 也将使与其连接的便携备 6-2 删 10 去个人计算机 1 已经登出的内容，或禁止便携设备 6-2 使用个人计算机 1 已经登出的内容，因此更新所删除内容的使用规则。而且，计算机 1 通过 USB 电缆 7-3 也将使与其连接的便携备 6-3 删 15 去个人计算机 1 已经登出的内容，或禁止便携设备 6-3 使用个人计算机 1 已经登出的内容，因此更新所删除内容的使用规则。

个人计算机 1 不能登入其它计算机(未表示出)登出到便携设备 6-1 的内 20 容。个人计算机 1 也不能登入其它计算机登出到便携设备 6-2 的内容。而且个人计算机 1 还不能登入其它计算机登出到便携设备 6-3 的内容。

如图所示，依据本发明的内容数据管理系统还包括 EMD 注册服务器 3。当个人计算机 1 开始从 EMD 服务器 4-1 到 4-3 获得内容时，EMD 注册服务 25 器 3 响应来自个人计算机 1 的请求，并通过网络 2 向个人计算机 1 发送个人计算机和 EMD 服务器 4-1 到 4-3 之间相互认证的认证密钥，并发送给个人计算机 1 连接到 EMD 服务器 4-1 到 4-3 的程序。

作为对来自个人计算机 1 请求的响应，EMD 服务器 4-1 将通过网络 2 向个人计算机 1 提供一项内容及与内容有关的数据(例如每首音乐的标题或回放限制等)。作为对来自个人计算机 1 请求的响应，EMD 服务器 4-2 也将通过网络 2 向个人计算机 1 提供一项内容及与内容有关的数据。而且，作为对来自个人计算机 1 请求的响应，EMD 服务器 4-3 也将通过网络 2 向个人计算机 1 提供一项内容及与内容有关的数据。

从 EMD 服务器 4-1 到 4-3 提供的内容以相同的方式或分别以不同的方式进行压缩。而且，从 EMD 服务器 4-1 到 4-3 提供的内容以相同的方式或分别以不同的方式进行加密。

如图所示，依据本发明的内容数据管理系统还包括 WWW(world wide web, 全球网)服务器 5-1 和 5-2。WWW 服务器 5-1 响应来自个人计算机的请 30 求，通过网络 2 提供给个人计算机 1 一张 CD，从该 CD 读取了一项内容(如

CD 专辑的名称或 CD 提供商等), 并提供相应于所读取内容的数据(如每首音乐的标题或作曲者姓名等)。作为对来自个人计算机 1 请求的相应, WWW 服务器 5-2 通过网络 2 提供给个人计算机 1 一张 CD, 从该 CD 读取了一项内容, 并提供相应于所读取内容的数据。

5 便携设备 6-1 保存由个人计算机 1 提供的内容(即登出的内容), 以及与该内容有关的数据(如每首音乐的标题或回放限制等)。基于相关内容的数据, 便携设备 6-1 将所保存的内容进行回放并输出到诸如耳机中(未表示出)。

例如, 当试图回放内容的次数超过保存的作为相关内容数据的回放次数限制时, 便携设备 6-1 将停止回放相应的内容。而且, 当已经超过保存的作为相关内容数据的回放次数限制时, 再试图回放, 携设备 6-1 将停止回放相应的内容。
10

用户由于携带的原因, 可以断开携带便携设备 6-1 与个人计算机 1 的连接, 而便携设备 6-1 中保存了内容, 并且, 这样回放保存在便携设备 6-1 中的内容, 以通过耳机等欣赏相应于内容的音乐片段。

15 便携设备 6-2 保存由个人计算机 1 提供的内容, 以及与内容有关的数据。根据相关内容的数据, 便携设备 6-2 将所保存的内容进行回放并输出到耳机等中(未表示出)。用户由于携带的原因, 可以断开携带便携设备 6-2 与个人计算机 1 的连接, 而便携设备 6-2 中保存了内容, 并且, 回放保存在便携设备 6-2 中的内容, 以通过耳机等欣赏相应于内容的音乐片段。

20 便携设备 6-3 保存由个人计算机 1 提供的内容, 以及与内容有关的数据。根据相关内容的数据, 便携设备 6-3 将所保存的内容进行回放并输出到耳机等中(未表示出)。用户由于携带的原因, 可以断开携带便携设备 6-3 与个人计算机 1 的连接, 而便携设备 6-3 中保存了内容, 并且, 回放保存在便携设备 6-3 中的内容, 以通过耳机等欣赏相应于内容的音乐片段。

25 便携设备 6-1 到 6-3 在不需要单独指定的场合, 下面将简称为“便携设备 6”。

图 2 说明个人计算机 1 的组成。如图所示, 个人计算机 1 包括 CPU(中央处理单元)11。CPU 11 实际上执行多种应用程序(将在后面进一步说明)和 OS(操作系统)。在个人计算机 1 中也提供 ROM(只读存储器)12, ROM 一般用于保存 CPU 11 使用的程序和计算的参数这些基本固定的数据。在个人计算机 1 中包含的 RAM(随机存取存储器)13 用于保存 CPU 11 执行应用程序和

OS 的程序，以及在执行应用程序和 OS 中的适当的变量。CPU 11，ROM12 和 RAM13 通过包括 CPU 总线的主总线 14 等互相连接。

主总线 14 通过桥 15 连接到外部总线 16 如 PCI 总线(外围设备互连/接口)。

5 个人计算机 1 还设有键盘 18，用户通过键盘 18 将各种命令输入到 CPU 11，以及设有鼠标 19，用户使用鼠标 19 在显示单元 20 上指定和选择一个点。显示单元 20 是液晶显示器或 CRT(阴极射线管)，以文本和/或图形方式显示各种信息。进一步，个人计算机 1 提供 HDD(硬盘驱动器)21，它通过驱动硬盘写或读 CPU 11 执行的程序，以及向硬盘写入或从硬盘读出信息。

10 个人计算机 1 还设有驱动器 22。驱动器 22 读取记录在磁盘 41、光盘 42(包括 CD)、磁光盘 43、半导体存储器 44 等连接在驱动器 22 上的任一种设备中的数据或程序，并通过接口 17、外部总线 16、桥 15 和主总线 14 向相连接的 RAM 13 提供所读取的数据或程序。

15 个人计算机 1 还设有 USB 端口 23-1，23-2 和 23-3。USB 端口 23-1 通过 USB 电缆 7-1 连接便携设备 6-1，并通过接口 17、外部总线 16、桥 15 或主总线 14，向便携设备 6-1 输出由 HDD 21、CPU 11 或 RAM 13 提供的数据(例如：包括给便携设备 6-1 的内容或命令)。

20 USB 端口 23-2 通过 USB 电缆 7-2 连接便携设备 6-2，并通过接口 17、外部总线 16、桥 15 或主总线 14，向便携设备 6-2 输出由 HDD 21、CPU 11 或 RAM 13 提供的数据(例如：包括给便携设备 6-2 的内容或命令)。

USB 端口 23-3 通过 USB 电缆 7-3 连接便携设备 6-3，并通过接口 17、外部总线 16、桥 15 或主总线 14，向便携设备 6-3 输出由 HDD 21、CPU 11 或 RAM 13 提供的数据(例如：包括给便携设备 6-3 的内容或命令)。

25 个人计算机 1 还设有具有 IEC(International Electrotechnical Commission, 国际电工技术委员会)60958 终端 24a 的音频输入/输出接口 24。该音频输入/输出接口 24 是数字音频输入/输出或模拟音频输入/输出接口。个人计算机 1 还有扬声器 45，它根据由音频输入/输出接口 24 提供的音频信号，可提供相应于每个内容的预先确定声音。

30 包括键盘 18 的附件和相邻的音频输入/输出接口 24 连接到接口 17 上，接口 17 依次通过外部总线 16、桥 15 和主总线 14 与 CPU 11 连接。

而且，个人计算机 1 有连接到网络 2 的通信块 25。通信块 25 通过网络 2，

以预先确定的方式发送由 CPU 11 或 HDD 21 提供的作为包形式保存的数据(如：请求注册或请求发送内容等)，同时，将在接收包中保存的数据(如：认证密钥或内容等)通过网络 2 输出到 CPU 11、RAM 13 或 HDD 21 中。

半导体 IC 集成的适配器 26 也被提供与个人计算机 1 的连接。它具有 CPU 5 32、RAM 33、非易失性存储器 34、RCT(real-time clock, 实时时钟)35、ROM 36。CPU 32 通过外部总线 16、桥 15 和主总线 14 连接到个人计算机 1 的 CPU 11 上，并与 CPU 11 一起协同实现多种处理。RAM 33 保存 CPU 32 执行各种处理所必须的数据和程序。非易失性存储器 34 保存个人计算机 1 关机后仍然必须保存的数据。ROM 36 保存用于对个人计算机 1 传递的被加密的程序 10 进行解密的程序。RTC 35 保证能提供时间信息。

通信块 25 和适配器 26 通过外部总线 16、桥 15 和主总线 14 连接到 CPU 11 上。

若没有单独指出，以下将 USB 端口 23-1 至 23-3 简称为“USB 端口 23”。而且若没有单独说明，以下将 USB 电缆 7-1 至 7-3 简称为“USB 电缆 7”。

参考图 3，是方框图形式表示的便携设备 6 的示意图。便携设备 6 包括将干电池 51 提供的电压转换成内部电源的预确定电压的电源电路 52。给 CPU 53 到显示单元 67 的部件提供电源，这样电源电路 52 将驱动整个便携设备 6。

便携设备 6 提供 USB 控制器 57。当通过 USB 连接器 56 和 USB 电缆 7 20 连接到个人计算机 1 时，USB 控制器 57 将通过内部总线 58，将从个人计算机 1 传递来的数据提供给 CPU 53。

从个人计算机 1 传递来的数据包括每个包的 64 字节的数据，并且数据以 12M 比特/秒的传输率从个人计算机 1 传递。

被传递给便携设备 6 的数据包括报头和内容。报头保存一项内容的 ID、文件名称、报头大小、内容密钥、文件大小、编解码器(codec)ID、文件信息等，还有回放限制所必须的回放限制数据、开始日期、结束日期、回放限制、回放计数器等。这里应注意术语“date(日期)”在此是指日期和时间。内容通过如 ATRAC3 的编码方式编码并进行加密。

报头大小表示报头的数据长度(如：33 字节等)，文件大小表示内容的数据长度(如：33,636,138 字节等)。

内容密钥是用于解密加密内容的密钥，并且根据由个人计算机 1 和便携

设备 6 之间的相互认证而产生的会话密钥(临时的), 以加密的形式从个人计算机 1 发送给便携设备 6。

当便携设备 6 通过 USB 电缆 7 与个人计算机 1 的 USB 端口 23 连接时, 在便携设备 6 和个人计算机 1 之间将进行相互认证。例如这种相互认证是应答式的。应注意到, 在便携设备 6 中还提供 DSP(数字信号处理器)59, 在进行应答式的认证时解密加密的内容。

上述的应答式的相互认证是这样的, 例如, 在响应由个人计算机产生的特定值(要求)时, 由便携设备 6 通过使用便携设备 6 与个人计算机 1 公用的私人密钥产生一个值(回复)。在应答式相互认证中, 在每次认证中个人计算机 1 产生的值是不同的。因此, 例如, 即使读取了用私人密钥产生并从便携设备 6 输出的值, 即发生所谓的伪装攻击, 个人计算机 1 也能检测出欺诈, 因为在下一个相互认证中将使用不同的值。

一项内容的 ID 是用于识别该内容的 ID。

编解码器 ID 是相应于一项内容的编码方法的 ID。例如, 编解码器 ID 是“1”时相应的编码方法是 ATRAC3, 而编解码器 ID 是“0”时相应的编码方法是 MP3(MPEG(移动图像专家组)音频层 3)。

文件名是将相应于一项内容的内容文件(将在后面说明)转换为 ASCII 码(信息交换的美国国家标准码)所得到的数据, 并且记录在个人计算机 1 中。文件信息是音乐标题(内容名)、艺术家演奏的音乐名称、音乐词作者名或音乐曲作者名转换成的 ASCII 码数据。

回放限制数据指示是否设置了一项内容可以回放(即开始日期或结束日期等)的回放时间段, 或一项内容可以回放的回放限制(限定的次数)。当设置回放限制时, 回放限制数据指定为“1”。当设置一项内容可以回放的时间段时, 回放限制数据指定为“2”。当既没有回放限制也没有回放时间端时(即, 当内容被购买)时, 回放限制数据指定为“0”。

当回放限制数据指定为“2”时, 开始日期和结束日期是指示一项内容可以回放的时间段范围的数据。例如, 当开始日期是“00040F”, 而结束日期是“00070F”时, 相应的内容可以回放的时间段为从 2000 年 4 月 15 日到 2000 年 7 月 15 日。

相似地, 回放限制和回放计数器如下: 即, 当回放限制数据指定为“1”或“2”时, 回放限制是一项内容可以回放的预先确定的次数, 回放计数器

是该内容已经回放的次数，并且由 CPU53 在完成回放时更新。例如，当回放限制是“02”时，该内容可以回放两次。当回放计数器是“01”时，意味着该内容已经回放了一次。

例如，当回放限制数据指定为“2”，开始日期为“00040F”，结束日期 5 为“00070F”，并且回放限制为“02”时，便携设备 6 在 2000 年 4 月 15 日到 2000 年 7 月 15 这段时间允许一天回放两次相应的内容。

还例如，当回放限制数据指定为“1”，开始日期为“000000”，结束日期为“000000”，并且回放限制为“0”，回放计数器为“05”时，相应的内容可以在不限定的时间段内回放，可以回放 10 次，并且已经回放了 5 次。

10 当便携设备 6 从个人计算机 1 接收一项内容和一项内容的写命令时，CPU 53 执行从 ROM 55 读到 RAM 54 的主程序，将接收该写命令，控制快闪存储器 60，并且将从个人计算机 1 接收的内容写到快闪存储器 61 中。

快闪存储器 61 有大约 64M 字节的存储容量来保存内容。而且，快闪存储器之中已经提前保存了按预先确定的方式压缩了的内容扩展回放码。

15 注意到快闪存储器 61 可以组成存储卡，可连接到便携设备 6，也可从便携设备 6 上移开。

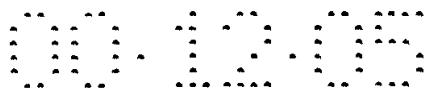
当 CPU 53 通过操作键控制器 62 被提供了相应于回放/停止按钮(未示出)按下操作的回放命令时，它将使快闪存储器控制器 60 从快闪存储器 61 读取回放码和内容，并且传递给便携设备 6 的 DSP 59。

20 当依据从快闪存储器 61 传递的回放码，检测出内容的 CRC(循环冗余码)校验错误时，DSP 59 将回放该内容及回放数据(参考图 3 的 D 所指示的)到数字/模拟转换电路 63 中。

DSP 59 在便携设备 6 中集成了发送电路(未示出)，根据来自外部晶体振荡器 59A 的主时钟 MCLK 回放一项内容，并且给数字/模拟转换电路 63 提供 25 主时钟 MCLK、依据主时钟 MCLK 由内部振荡电路产生的并且有预先确定的频率的一比特时钟 BCLK、以及在帧单元中包括左声道时钟 LCLK 和右声道时钟 RCLK 的操作时钟 LRCLK。

为了回放一项内容，DSP 59 将依据回放码向数字/模拟转换电路 63 提供上述操作时钟。当不回放内容时，DSP 59 将依据回放码停止提供操作时钟以 30 关掉数字/模拟转换电路 63，因此降低了整个便携设备 6 的功耗。

相似地，CPU 53 和 USB 控制器 57 分别具有与其相连接的外部晶体振



荡器 53 A 和 57 A，并基于振荡器 53 A 和 57 A 提供的主时钟 MCLK，分别产生预先确定的操作。

由于上述的结构，便携设备 6 不需要时钟产生模块为 CPU 53，DSP 59 和 USB 控制器 57 中的每个提供时钟，因而可以采用更简单和更紧凑的电路
5 结构。

数字/模拟转换电路 63 将回放内容转换为模拟音频信号并提供给放大电
路 64。放大电路 64 放大音频信号并通过耳机插座 65 提供给耳机(未示出)。

这样，当按下回放/停止按钮时，便携设备 6 在 CPU 53 的控制下回放保
存在快闪存储器 61 中的一项内容。当在回放一项内容的过程中按下回放/停
10 止按钮时，便携设备 6 将停止回放该内容。

当在停止内容回放的操作之后按下回放/停止按钮时，便携设备 6 在 CPU
53 的控制下将在回放操作停止的位置上恢复该内容的回放。在通过按下回放/
停止按钮停止回放操作之后，当几秒之后无附加的操作，则便携设备 6 将自
动关断电源，因而降低了功耗。

15 这里应该注意到，在关断电源之后按下回放/停止按钮时，便携设备 6 将
在第一首或 No.1 音乐的位置恢复回放，而不是在先前回放时停止的位置上回
放该内容。

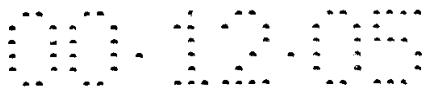
而且，便携设备 6 的 CPU 53 使 LCD 控制器 68 在显示单元 67 上显示回
放模式(如重复回放、引入回放等)、均衡调节(即音频信号频带的增益调节)
20 音乐的序号、回放时间、回放的操作模式，如回放、停止、快进和快倒，以
及例如声音音量及干电池中电量的信息。

而且，便携设备 6 向 EEPROM 68 中分别存入在快闪存储器 80 中写入
的内容的次数，内容写入快闪存储器 61 中块的位置，以及保存在该存储器
中各种信息的所谓的 FAT(文件分配表)。

25 应该注意到在这个实施例中，一项内容占用一个 64 k 字节的块，并且每
首音乐内容所占用块的位置保存在 FAT 中。

一旦 FAT 保存在快闪存储器 61 中，当第一首音乐在 CPU 53 的控制下写
入快闪存储器 61 时，相应于第一首音乐内容的块的位置将作为 FAT 写入快
30 闪存储器 61 中，相应于第二首音乐的内容的块的位置也将作为 FAT 写入快
闪存储器 61(在第一首音乐写入的相同的位置)中。

采用这种方法，每当将内容写到快闪存储器 61 中时，就重写 FAT，而且



为了保护数据，相同的数据为了保留还再写一次。

当将 FAT 写进快闪存储器 61 时，相应于第一次内容的写入将在相同的快闪存储器的位置上重写两次。为此，当内容只被写了较少的次数时，重写快闪存储器 61 的次数将达到一个特定的次数，使得快闪存储器 61 再也不能 5 重写了。

为了避免上述问题，便携设备 6 用 EEPROM 68 来保存 FAT，以使在向快闪存储器 61 写每项内容时，重写 FAT 的次数能减少。

通过将被写多次的 FAT 保存到 EEPROM 68，便携设备 6 就可以使得将内容写到快闪存储器 61 的次数与将 FAT 直接保存到快闪存储器 61 相比，可 10 以将内容写到快闪存储器 61 的次数多数十倍。而且，由于 CPU 53 使得 EEPROM 附加地保存了 FAT，EEPROM 中相同的位置被重写的频率就会降低，从而阻止 EEPROM 很快不能重写。

当便携设备 6 通过 USB 电缆 7 连接到个人计算机 1(下面称为“USB 连接”)时，根据从 USB 控制器提供给 CPU 53 的中断信号就可识别出已经进 15 行了 USB 连接。

当便携设备 6 识别出 USB 连接时，它通过 USB 电缆 7 从个人计算机 1 提供具有特定电流值的外部电源，并使电源电路 52 停止从干电池 51 取得电源。

当建立了 USB 连接时，CPU 53 将停止 DSP 59 回放内容。这样，CPU 53 20 将阻止来自个人计算机 1 的外部电源超过特定的电流值，这样使得总能提供特定电流值的外部电源。

这样，当建立了 USB 连接时，CPU 53 在来自干电池的电源和来自个人计算机 1 的电源之间作出选择。也就是说，可以使来自个人计算机 1 的廉价的外部电源，这样就能消耗较少的来自干电池 51 的价格较贵的电源。并且也能使干电池 51 具有较长的使用寿命。

注意当通过 USB 电缆 7 从个人计算机 1 提供外部电源时，CPU 53 将使 DSP 59 停止回放内容以减少从 DSP 59 的发热，于是，整个系统包括个人计算机 1 的发热能进一步减少。

参考图 4，表示个人计算机 1 的方框图，说明由 CPU 11 执行预先确定的程序来实现个人计算机 1 的功能。如图所示，个人计算机 1 使用内容管理程 30 序 111，内容管理程序 111 由多个程序组成，包括：EMD 选择程序 131、登

入/登出管理程序 132、复制管理程序 133、移动管理程序 134、加密方法转换程序 135、压缩方法转换程序 136、加密程序 137、压缩/展开程序 138、使用规则转换程序 139、使用规则管理程序 140、认证程序 141、解密程序 142、PD 驱动程序 143、购买程序 144 和 145。

5 在上述程序中，内容管理程序 111 由混洗(shuffled)或加密指令组成，目的是为了例如对外隐藏指令操作，使很难解释该指令(例如，即使用户能直接读取内容管理程序 111，他或她也不能识别这些指令)。

当内容管理程序 111 安装在个人计算机 1 中时，EMD 选择程序 131 不包括在内容管理程序 111 中，但它可通过网络 2 在 EMD 注册时从 EMD 注册服务器 3 接收 EMD 选择程序 131，这将在后面进一步说明。EMD 选择程序 131 选择同任何 EMD 服务器 4-1 到 4-3 的连接，以使购买应用程序 115、购买程序 144 或 142 能与任何 EMD 服务器 4-1 到 4-3 通信(例如购买一项内容的下载)。

根据登入或登出之一的设置和保存在内容数据库 114 中的使用规则文件 162-1 到 162-N，登入/登出管理程序 132 登出保存在内容文件 161-1 到 161-N 中的内容到任何便携设备 6-1 到 6-3 中，或登入保存在便携设备 6-1 到 6-3 中的内容。

为响应所进行的登入/登出，登入/登出管理程序 132 更新保存在使用规则文件 162-1 到 162-N 中的使用规则，而使用规则文件 162-1 到 162-N 记录在内容数据库 114 中。

根据记录在内容数据库 114 中的使用规则文件 162-1 到 162-N，复制管理程序 133 将保存在内容文件 161-1 到 161-N 中的内容移动到任何便携设备 6-1 到 6-3 中，或将内容从便携设备 6-1 到 6-3 移动到内容数据库 114 中。

25 加密方法转换程序 135 转换为如下的加密方法：与记录在内容数据库 114 中、保存在内容文件 161-1 到 161-N 的内容所使用的相同加密方法；通过网络 2 从 EMD 服务器 4-1 接收的购买应用程序 115 的内容、通过网络 2 从 EMD 服务器 4-2 接收的购买程序 144 的内容或通过网络 2 从 EMD 服务器 4-3 接收的购买程序 145 的内容所使用的加密方法。

另外，为将一项内容登出到便携设备 6-1 或 6-3 中，加密方法转换程序 30 135 将要登出内容的加密方法转换为在便携设备 6-1 或 6-3 中使用的加密方法。

压缩方法转换程序 135 转换为如下的压缩方法：记录在内容数据库 114 中、保存在内容文件 161-1 到 161-N 的内容所使用的相同压缩方法；通过网络 2 从 EMD 服务器 4-1 接收的购买应用程序 115 的内容、通过网络 2 从 EMD 服务器 4-2 接收的购买程序 144 的内容或通过网络 2 从 EMD 服务器 4-3 接收 5 的购买程序 145 的内容所使用的压缩方法。

另外，为将一项内容登出到便携设备 6-1 或 6-3 中，压缩方法转换程序 135 将要登出内容的压缩方法转换为在便携设备 6-1 或 6-3 中使用的压缩方法。

10 加密程序 137 用于加密从 CD 读取和由记录程序 113 提供的内容(未加密)，例如，按照记录在内容数据库 114 中、保存在内容文件 161-1 到 161-N 的内容所使用的相同加密方法。

15 所述压缩/展开程序 138，按照记录在内容数据库 114 中、保存在内容文件 161-1 到 161-N 的内容所使用的相同编码方法，对从 CD 读取和由记录程序 113 提供的内容(未压缩)进行编码。另外，压缩/展开程序 138 将展开(解密)编码内容。

20 使用规则变换程序 139 转换为如下格式：记录在内容数据库 114 中、保
存在使用规则文件 162-1 到 162-N 的内容的使用规则的相同格式；通过网络 2 从 EMD 服务器 4-1 接收的购买应用程序 115 的内容、通过网络 2 从 EMD 服务器 4-2 接收的购买程序 144 的内容或通过网络 2 从 EMD 服务器 4-3 接收
的购买程序 145 的内容的使用规则格式。

另外，为将一项内容登出到便携设备 6-1 或 6-3 中，使用规则转换程序 139 将要登出内容的使用规则转换为在便携设备 6-1 或 6-3 中使用的使用规则。

25 在执行内容复制、移动、登入或登出之前，使用规则管理程序 140 根据 满足记录在内容数据库 114 中、保存在使用规则文件 161-1 到 161-N 中使用 规则的哈希(hash)值(将在后面说明)，检测使用规则的篡改或变化。随着记 录 在 内 容 数据 库 114 中、保 存 在 使用 规 则 文 件 161-1 到 161-N 中 使用 规 则 的 更 新，以 及 内 容 复 制、移 动、登 入 或 登 出 的更 新，使 用 规 则 管 理 程 序 140 更新 满 足 使用 规 则 的 哈 希 值。

30 认证程序 141 执行内容管理程序 111 和购买应用程序 111 之间的相互认 证，以及内容管理程序 115 和购买应用程序 144 之间的相互认证。同样，认

证程序 141 将保存 EMD 服务器 4-1 和购买应用程序 115 之间相互认证使用的认证密钥，EMD 服务器 4-2 和购买程序 144 之间相互认证使用的认证密钥，EMD 服务器 4-3 和购买程序 145 之间相互认证使用的认证密钥。

应注意当内容管理程序 111 安装在个人计算机 1 中时，认证程序 141 在 5 相互认证时使用的认证密钥没有保存在认证程序 141 中，但当显示/操作指导程序 112 成功注册认证密钥时，该密钥将由 EMD 注册服务器 3 提供并保存在认证程序 141 中。

当个人计算机 1 回放记录在内容数据库 114 中、保存在内容文件 161-1 到 161-N 中的内容时，解密程序 142 解密该内容。

10 当登出(管理程序)向便携设备 6-2 输入一项预先确定的内容或从便携设备 6-2 中登入一项预先确定的内容时，PD 驱动器 143 给便携设备 6-2 提供该内容或命令，使便携设备 6-2 进行预先确定的操作。

15 当登出(管理程序)向便携设备 6-1 输入一项预先确定的内容或从便携设备 6-1 中登入一项预先确定的内容时，PD 驱动器 143 给便携设备 6-1 提供该内容或命令，使设备驱动器 116-1 进行预先确定的操作。

当登出(管理程序)向便携设备 6-3 输入一项预先确定的内容或从便携设备 6-3 中登入一项预先确定的内容时，PD 驱动器 143 给便携设备 6-2 提供该内容或命令，使设备驱动器 116-1 便携设备 6-2 进行预先确定的操作。

20 购买程序 144 是所谓的插件程序。与内容管理程序 11 一起安装到个人计算机 1 中，通过网络 2 由 EMD 注册服务器 3 提供，或提供成记录在预先确定的 CD 中。当安装在个人计算机 1 中时，购买程序 144 将通过内容管理程序 111 具有的预先确定形式的接口，发送或接收内容管理程序 111 和数据。

25 购买程序 144 由混淆或加密指令组成，目的是为了例如对外隐藏指令操作，使很难解释该指令(例如，即使用户能直接读取购买程序 144，他或她也不能识别这些指令)。

购买程序 144 通过网络 2，请求 EMD 服务器 4-2 发送预先确定的内容，然后从 EMD 服务器 4-2 接收该内容。当从 EMD 服务器 4-2 接收该内容时，购买程序 144 将对该内容记帐。

30 购买程序 145 将与内容管理程序 111 一起安装。它要求通过 EMD 服务器 4-3 发送预先确定的内容，然后从 EMD 服务器 4-3 接收该内容，当从 EMD 服务器 4-3 接收到该内容时，购买程序 145 将对该内容记帐。

依据过滤(filter)数据文件 181、显示数据文件 182、图像文件 183-1 至 183-K 或历史数据文件 184，显示/操作指导程序 112 在显示单元 20 上显示预先确定的窗口图像，并给内容管理程序 111 发出登入和登出指令。作为对用户键盘 18 或鼠标 19 操作的响应。

5 过滤数据文件 181 保存记录在内容数据库 114 中、保存在使用规则文件 161-1 到 161-N 中加权内容的数据，并且被记录在 HDD 21 中。

显示数据文件 182 保存相应于记录在内容数据库 114 中、保存在使用规则文件 161-1 到 161-N 中的内容的数据，并且被记录在 HDD 21 中。

10 图像文件 183-1 至 183-N 保存相应于内容文件 161-1 至 161-N 的数据，记录在内容数据库 114 中，并且被记录在 HDD 21 中。

图像文件 183-1 至 183-K 在不单个指定的情况下，将在后面简称为“图像文件 183”。

15 历史库数据文件 184 保存历史库数据，包括已经登出的记录在内容数据库 114 中、保存在使用规则文件 161-1 到 161-N 中内容的次数、该内容已经登入的次数，以及登出登入的日期。历史库数据文件 184 记录在 HDD 21 中。

为了注册，显示/操作指导程序 112 通过网络向 EMD 注册服务器 3 发送预先保存内容管理程序 111 的 ID 号，当接收时，通过网络 2，接收 EMD 注册服务器 3 中的认证密钥和 EMD 选择程序 131，并提供给内容管理程序 111。

20 记录程序 113 用于显示预先确定窗口的图像，并读取数据如来自 CD 的内容的记录时间，在该实施例中 CD 作为放入驱动器 22 中的光盘 42，以作为对用户键盘 18 或鼠标 19 操作的响应。

25 根据记录在 CD 中内容的记录时间，记录程序 113 通过网络 2 要求 WWW 服务器 5-1 或 5-2 发送相应于 CD 的数据，例如专辑的名称或艺术家的名称或相应于记录在 CD 中内容的数据如一首音乐的标题，从而通过网络 2，从 WWW 服务器 5-1 或 5-2 中接收相应于 CD 的数据或记录在 CD 中内容。

而且，记录程序 113 给显示/操作指导程序 112 提供相应于 CD 所接收的数据或相应记录在 CD 中的内容的数据。

30 进一步，当提供记录指令时，记录程序 113 读取并输出给内容管理程序 111 一项 CD 中的内容，CD 在该实施例中作为放入驱动器 22 的光盘 42。

内容数据库 114 向内容文件 161-1 至 161-N 任何一个中保存由内容管理

程序 111 提供的内容，并且以预先确定的方式被压缩，以预先确定的方式被加密(将该内容记录在 HDD 21)中。内容数据库 114 将保存在内容文件 161-1 至 161-N 中的内容的使用规则保存到相应于内容文件 161-1 至 161-N 的任何一个使用规则文件 161-1 至 161-N 中，在内容文件 161-1 至 161-N 中保存了 5 内容(将该使用规则记录到 HDD21 中)。

内容数据库 114 作为记录，可以记录内容文件 161-1 至 161-N 或使用规则文件 161-1 至 161-N。

例如，保存在内容文件 161-1 中的内容的使用规则被保存在使用规则文件 162-1 中。保存在内容文件 161-N 中内容的使用规则被保存在使用规则文件 162-N 中。 10

注意到记录在使用规则文件 162-1 至 162-N 中的数据相应于记录在时间限制数据库或音乐数据库中的数据，将在后面作详细说明。即，内容数据库 114 包括时间限制数据库和音乐数据库。

在不单独指定的情况下，内容文件 161-1 至 161-N 在后面将简称为“内容文件 161”。而且，在不单独指定的情况下，使用规则文件 162-1 至 162-N 在后面将简称为“使用规则文件 162”。 15

购买应用程序 115 通过网络 2 由 EMD 注册服务器 3 提供，并记录在预先确定的 CD-ROM 中。购买应用程序 115 通过网络 2 请求 EMD 服务器 4-1 发送一项预先确定的内容，而从 EMD 服务器 4-1 接收该内容并提供给内容 20 管理程序 111。而且，当从 EMD 服务器 4-1 接收到该内容时，购买应用程序 115 将为该内容记帐。

接下来将在下面说明保存在显示数据文件 82 中的数据和保存在内容数据库 114 中的内容文件 161-1 到 161-N 之间的对应。

首先，保存在任何一个内容文件 161-1 到 161-N 中的内容属于一个预先 25 确定的包，更具体地说，该包是原始包、我所选择的包(my selected package) 和过滤包中的任意一个。

在上述的包中，原始包具有属于它的多于一项的内容。该包相应于 EMD 服务器 4-1 到 4-3 或一个 CD 中的内容的分类(即所谓的专辑)。一项内容属于 30 任意一个原始包并且不可能属于多个原始包。而且，不能修改一项内容属于的原始包。用户可以编辑相应于原始包(例如，附加的信息或附加信息的变化) 的一部分信息。

用户自由选择的多于一项的内容属于我所选择的包。用户可以任意编辑分配给我所选择的包的内容。一项内容可以同时属于多个我所选择的包。而且，一项内容可能不属于任意一个我所选择的包。

基于保存在过滤数据文件 181 中的过滤数据所选择的内容属于过滤包。

5 过滤数据通过网络 2 由 EMD 服务器 4-1 到 4-3 或 WWW 服务器 5-1 或 5-3 提供，或记录在预先确定的 CD 中。用户可以编辑保存在过滤数据文件 181 中的过滤数据。

10 过滤数据作为选择预先确定内容的参考或作为计算相应于该内容加权的参考。例如，个人计算机 1 可以使用相应于每周 J-POP(日本流行歌曲)前十位的过滤数据，以识别每周日本流行歌曲的第 1 到第 10 位的内容。

15 过滤数据文件 181 包括按照时间长度减少的顺序排列的选择内容的过滤数据，在这段时间该过滤数据文件被登出过去一个月的情况，或者，过滤数据文件 181 包括按照它们在过去的半年中被登出的次数减少的顺序排列的选择内容的过滤数据，或者，过滤数据文件 181 包括音乐的标题(内容名称)中包含字符“AI(love)”的选择内容的过滤数据。

这样，通过将过滤数据与内容显示数据 221(包括用户已经设置的数据)、历史数据 184 等比较，选择过滤包中的内容。

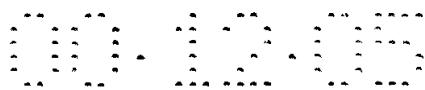
20 驱动器 117 在内容管理程序 111 等的控制下驱动音频输入/输出接口 24 以输入一项内容作为由外部提供的数字数据，并提供给内容管理程序 111，并且经过内容管理程序 111，作为数字数据输出由内容数据库 114 提供的内容，或者通过内容管理程序 111，输出相应于由内容数据库 114 提供内容的一个模拟信号。

图 5 显示/操作指导程序 112 使显示单元 20 显示的显示/操作指导窗口的例子。

25 在显示/操作指导窗口中显示有几个按钮，按钮 201 用于启动记录程序 113，按钮 202 用于启动 EMD 选择程序 131，按钮 203 用于显示登入或登出设置的区域，按钮 204 由于选择将要编辑的、我所选择的包的区域，等等。

当选择按钮 205 时，相应于原始包的数据显示在窗口的 211 区域。当选择按钮 206 时，相应于我所选择包的数据显示在窗口的 211 区域。当选择按钮 207 时，相应于过滤包的数据显示在窗口的 211 区域。

在区域 211 中显示的数据涉及一个包。例如，该数据是包的名称或音乐



家的姓名。

如图 5 所示，在区域 211 中显示包的名称“FIRST(第一个)”和艺术家姓名“A TARO”，显示包的名称“SECOND(第二个)”和艺术家的姓名“A TARO”，等。

5 显示/操作指导窗口还有一个区域 212，在其中显示有数据，该数据相应于属于在区域 211 中所选择包的内容。显示在该区域的数据是一首音乐的标题，回放时间或该内容可以被登出的次数。

10 在图 5 中，选择相应于包名称为“SECOND(第二个)”的包。这样，在区域 212 中显示音乐的标题(内容名称)“MINAMI-NO-SAKABA”，相应于属
15 于包名称为“SECOND(第二个)”包的内容，内容可以被登出的次数(例如，八分之一的注释是一次登出，八分之二的注释是两次登出)，还显示音乐的标
20 题(内容名称)“KITA-NO-HAKABA”和内容可以被登出的次数(例如，八分之一的注释相应于一次登出)

这样，八分之一的注释作为表示一项内容可以被登出的次数显示在区域
15 212 中，指示相应的内容可以登出一次。

一个“休止符(rest)”作为表示一项内容可以被登出的次数显示在区域 212 中，指示相应的内容不能被登出(登出的次数是零；但是，个人计算机 1 可以回放该内容)。一个“中音谱号(C clef)”作为一项内容可以登出的次数显示在区域 212 中，指示登出相应内容登出的次数是无限的(该内容可以被登出任意的次数)。

注意到一项内容可以被登出的次数，可以用如图 5 中所示那样带有预先确定的图样(figure)(例如，可以是圆形、星形、月牙形等)以及数字的相应音乐片段数目进行指示。

25 在显示/操作指导窗口还有一个区域 208，其中显示相应于所选包或内容(相应于图 4 中图像文件 183-183K 中的任意一个)的图像等。在该区域，当回放所选内容(将相应于内容的声音输出到扬声器 45)时，点击按钮 209。

当选择显示在区域 212 中预先确定内容(内容名称)的音乐标题，并进行删除操作时，在选择了按钮 205 且在在区域 211 中正在显示相应于原始包的数据时，显示/操作指导程序 112 将使内容管理程序 111 删除相应于所选音乐
30 标题、保存在内容数据库 114 中的预先确定的内容。

当从 CD 读取的内容被记录在数据库 114 中时，在记录程序 113 的控制

下选择(激活)窗口中的按钮 255(后面进一步说明)时, 显示/操作指导程序 112 将使显示/操作指导窗口显示区域 213, 在显示区域 213 中显示保存在任意一个预先指定的便携设备 6-1 到 6-3 中的一项内容的音乐标题(内容名称)。

当从 CD 读取的内容被记录在数据库 114 中时, 在记录程序 113 的控制
5 下选择(激活)窗口中的按钮 255(后面进一步说明)时, 显示/操作指导程序 112 将使内容管理程序 111 登出记录在内容数据库 114 中的内容, 并且从 CD 读到任意一个预先指定的便携设备 6-1 到 6-3 中。

在区域 213 中, 在其最左的相应于一项内容的音乐标题(内容名称)的位置上, 显示有一个符号, 指示该内容能否登入到个人计算机 1 中。例如, 在
10 区域 213 的最左的位置上的符号“o”指示一项内容的音乐标题(内容名称)所对应的内容可以登入到个人计算机 1 中(即, 它已经从个人计算机 1 中登出)。在区域 213 的最左的位置上的符号“x”指示一项内容的音乐标题(内容名称)所对应的内容不能登入到个人计算机 1 中(即, 它还没有从个人计算机 1 中登出; 例如它已经从其它任何一台个人计算机 1 中登出)。

15 当显示/操作指导程序 112 已经在显示/操作指导窗口显示区域 213 时, 显示/操作指导程序 112 将在显示/操作指导窗口中显示区域 214, 在该区域显示便携包的名称(保存在任意一个指定的便携设备 6-1 到 6-3 中的内容属于该便携包), 和关闭区域 213 的按钮 213, 以及执行登入或登出操作的按钮 215。

进一步, 当显示/操作指导程序 112 已经在显示/操作指导窗口显示区域
20 213 时, 显示/操作指导程序 112 将在显示/操作指导窗口中显示按钮 216, 来设置在区域 212 中所选音乐标题对应内容的登出操作, 还将在显示/操作指导窗口中显示按钮 217 来设置在区域 212 中所选音乐标题对应内容的登入操作, 还将在显示/操作指导窗口中显示按钮 218 来设置显示在区域 212 中内容名称对应所有内容的登入操作, 以及按钮 219 来取消登入或登出设置。

25 即使使用按钮 216 到 219 进行了登入或登出的设置, 个人计算机 1 也将不执行登入或登出的操作。

在使用按钮 216 到 219 进行了登入或登出的设置后, 当点击按钮 215 时,
显示/操作指导程序 112 将使内容管理程序 111 执行登入或登出。也就是说,
当点击按钮 215 时, 显示/操作指导程序 112 将根据登入或登出设置, 使内容
30 管理程序 111 向便携设备 6-1 到 6-3 中的任意一个发送一项内容, 或一个删除
相应于登入设置(如删除保存在便携设备 6-1 到 6-3 中的任意一个中的预先

确定的内容)预先确定内容的命令，并更新保存在使用规则文件 162 中、相应于所发送内容或命令的使用规则。

当执行登入或登出时，显示/操作指导程序 112 将响应所发送的内容或命令，以更新保存在历史数据文件 84 中的历史数据。历史数据包括该已经被 5 登入或校验的内容的识别信息，还包括一项内容已经被登入或登出的日期，还包括该内容从中被登出的便携设备 6-1 到 6-3 中的一个的名称。

由于登入或登出可以被很快设置，用户在执行登入或登出操作之后可以很快知道该状态，而登入或登出操作的次数可以减小，使得进行登入或登出过程的总的时间(包括登入或登出操作的设置和执行)最小。

10 图 6 表示记录程序 113 使显示单元 20 显示的窗口的例子。例如根据从 WWW 服务器 5-2 中接收的 CD 信息，记录程序 113 将在区域 251 中显示 CD 的标题例如“ACYNCHRONIZED”。而且，根据从 WWW 服务器 5-2 中接收的 CD 信息，记录程序 113 将在区域 252 中显示艺术家的姓名例如“KUWAI”。

15 根据从 WWW 服务器 5-2 中接收的 CD 信息，记录程序 113 将在多首音乐标题被显示的区域 253 中显示其标题，例如“HEAT(炽热)”、“PLANET(行星)”“BLACK(黑的)”“SOUL(心灵)”等。相似地，记录程序 113 将在显示艺术家姓名的区域 253 中显示艺术家的姓名例如“KUWAI”。

20 在接收到预先确定的 CD 信息之后，记录管理程序 113 将它保存到 HDD21 的预先确定的目录中。

当通过点击按钮 254 接收到获得 CD 信息的指令时，记录程序 113 将首先搜索 HDD21 中预先确定的目录。当在该目录下找到该 CD 信息时，记录程序 113 将显示对话框(未示出)以提示用户选择他或她是否将使用保存在该目录下的 CD 信息。

25 记录程序 113 在窗口中显示按钮 256，该按钮执行开始记录一项内容的操作，当点击该按钮时，记录程序 113 将从驱动器 22 中的 CD 装置中读取一项内容并将它连同该 CD 信息提供给内容管理程序 111。内容管理程序 111 的压缩/展开程序 138 以预先确定的方式压缩由记录程序 113 提供的内容，并且加密程序 137 加密所压缩的内容。而且，使用规则转换程序 139 产生所压缩和加密内容的使用规则。

30 内容管理程序 111 将向内容数据库 114 提供所压缩和加密的内容，以及

使用规则。

内容数据库 114 将产生内容文件 161 和从内容管理程序 111 接收的内容的使用规则文件 162，并将该内容保存到内容文件 161 中，将该使用规则保存到使用规则文件 162 中。

5 当该内容和该内容的使用规则被保存到数据库 114 中时，内容管理程序 111 将向显示/操作指导程序 112 提供 CD 信息和从记录程序 113 接收的使用规则。

显示/操作指导程序 112 将通过记录和 CD 信息，依据保存在内容数据库 114 中的内容的使用规则显示保存到显示数据文件 182 中的数据。

10 当从 CD 中读取的内容被记录到内容数据库 114 中时，通过记录程序 113 显示的窗口已经在其中显示一个按钮 255，以自动设置是否使便携设备 6-1 到 6-3 中的任意一个登出从 CD 中读取的一项内容。

15 例如，当点击按钮 255 时，记录程序 133 将显示一个下拉菜单，显示便携设备 6-1 到 6-3 的列表。当用户从下拉菜单中选择便携设备 6-1 到 6-3 中的任意一个时，个人计算机 1 将登出 CD 中记录的内容到任意所选的一个便携设备 6-1 到 6-3 中。当用户从下拉菜单中选择“不登出”时，个人计算机 1 将不登出在 CD 中记录的内容。

20 这样，当通过将记录程序 113 设置为激活，从 CD 中读取的内容被记录在内容数据库 114 中，并显示只有一个按钮 255 的窗口时，个人计算机 1 可以使得任何预先指定的便携设备 6-1 到 6-3 登出从 CD 中读取的内容。

参考图 7，表示将一项回放的内容从驱动器 22 中的 CD 装置传递到 HDD 21 中，并将该内容从 CD 复制到 HDD 21 中操作的流程图，这些操作受到执行管理程序、显示/操作指导程序 112、记录程序 113 和内容数据库 114 的 CPU 11 的影响。当用户操作键盘 18 和鼠标 19 通过接口 17 向 CPU 11 提供一条传递命令，用于复制来自驱动器 22 的 CD 装置中(未表示出)回放内容时，记录程序 113 将在步骤 S11 中显示例如图 6 中的 GUI(图形用户接口)，用于通过接口 17 选择将被复制到显示单元 20 中的内容。

30 更具体地说，记录程序 113 将读取驱动器 22 中 CD 装置的 TOC(内容表)，从 CD 中获得内容信息，并显示在显示单元 20 中。可选择地，记录程序 113 将读取包含在 CD 中的每项内容的 ISRC(国际标准记录码)，获得内容信息，并显示在显示单元 20 中。还可选择的是，当点击按钮 254 时，记录程序 113

将通过网络 2 访问 WWW 服务器 5-1 或 5-2，通过使用 TOC 获得 CD 中的内容信息，并在区域 253 中显示内容的音乐名称。

使用显示在显示单元 20 上的 GUI，用户操作键盘 18 或鼠标 19，并点击显示在区域 253 中每首音乐标题的校验框来选择一项要复制的内容。

5 接着步骤 S12 中，记录程序 113 使得使用规则管理程序 140 检查保存在 HDD 21 中的时间限制数据库(相应于图 4 的内容数据库 114 中的使用规则文件 162-1 到 162-N)。有关检查时间限制数据库的细节将在后面参考图 8 中的流程图进行说明。

10 在步骤 S31 中，使用规则管理程序 140 结合适配器 26 的 CPU 32 计算整个时间限制数据库的哈希值，并且在步骤 S32 中，它将比较该计算的哈希值和先前保存的哈希值。

注意到当在时间限制数据库中没有记录时，使用规则管理程序 140 将不计算任何哈希值。

15 更具体地说，时间限制数据库在 HDD 21 中组成，并且保存成对的 IISR 和已经记录的内容的复制日期，作为内容管理的信息记录在 HDD 21 中，如图 9 所示。在图 9 的例子中，是三个项目 1 到 3 中每个项目的 ISRC 和复制日期区域。在步骤 S38 中，根据记录在时间限制数据库中的所有内容的 ISRC 和复制日期，由适配器 26 的 CPU 32 计算整个时间限制数据库的哈希值并保存在非易失性存储器 34 中。哈希值是将哈希函数作用到这些数据上得到的值。哈希函数通常是单向函数，它将可变长度的较长数据映射为固定长度的较短的数据并且具有这样的特性即哈希值不会轻易地互相冲突。哈希函数包括 SHA(安全哈希算法)，MD(信息摘要)5 等。在步骤 S31 中，象 CPU 32 计算的那样，使用规则管理程序 140 计算哈希值。在步骤 S32 中，使用规则管理程序 140 将要求 CPU32 读取保存在非易失性存储器 34 中的哈希值，并且在步骤 S31 中，它将比较所传递的哈希值和它已经计算出的哈希值。

20 在步骤 S33 中，使用规则管理程序 140 判断在步骤 S31 中计算的哈希值是否与保存在非易失性存储器 34 中先前时间限制数据库的哈希值相一致。当发现两个哈希值之间不一致时，使用规则管理程序 140 将确定出时间限制数据库已经被篡改或改变了。并且使记录程序 113 产生一条消息，例如“由于时间限制数据库已经改变了，不能进行复制”，并通过接口 17 将消息输出给显示单元 20，在显示单元 20 上显示该消息。之后，禁止复制。即在这种

情况下，禁止回放记录在 CD 中用于复制到 HDD 21 中的内容。

当发现在步骤 S31 计算的哈希值与前述的值相一致时，使用规则管理程序 140 转移到步骤 S35，在此，它将使记录程序 113 从 CD 中获得在步骤 S11 中指定并且将被选择作为复制的一项内容的 ISRC。如果在 CD 中没有记录 5 ISRC，那么使用规则管理程序 140 将使记录程序 113 从 CD 中读取 TOC 数据，并且将哈希函数作用在该数据上以获得适当长度的数据，如用于 ISRC 的 58 比特的数据。

在步骤 S36 中，使用规则管理程序 140 判断在步骤 S35 中获得的 ISRC(所选择的内容)是否在时间限制数据库(在图 9)中注册。如果 ISRC 没有在时间 10 限制数据库中注册，那么意味着该内容还没有记录在 HDD 21 中。这样，使用规则管理程序 140 转移到步骤 S37 中，在该步骤它将向时间限制数据库中注册该内容和当前日期。注意到使用规则管理程序 140 使用从 CPU 32 传递并从适配器 26 的 RTC 35 输出的值作为当前的日期。在步骤 S38 中，使用规则管理程序 140 于是从时间限制数据库读取数据并传递到适配器 26 的 CPU 15 32 中。CPU 32 计算所传递数据的哈希值并将它保存到非易失性存储器 34 中。如上所述，该保存的哈希值将用作在步骤 S32 中先前保存的哈希值。

接下来在步骤 S39 中，使用规则管理程序 140 将设置未注册标志来指示出所选择的内容没有在时间限制数据库中注册。该标志用在图 7 的步骤 S13 中以判断所选择的内容是否在时间限制数据库注册了。

如果在步骤 S36 中已经确定所选内容的 ISRC 在时间限制数据库中注册了，那么它意味着所选的内容是已经在 HDD21 中至少注册了一次的内容。在这种情况下，使用规则管理程序 140 转移到步骤 S40 中，在该步骤将判断当前的日期(从适配器 26 的 RTC 35 中输出)距在时间限制数据库注册的所选内容的最后一次注册日期是否大于 48 个小时。当当前的时间距该注册日期 20 已经大于 48 个小时时，意味着该内容已经在 HDD 21 中至少记录过一次。但是，由于当前的时间距该内容记录的时间大于 48 个小时，该内容即使再复制实际上也不能大规模地复制了。在这种情况下，允许将该内容复制到 HDD 21 中。然后，使用规则管理程序 140 将转移到步骤 S41 中，在该步骤，它将时间限制数据库中的日期，从过去的注册日期改变为当前的日期(从 RTC 35 30 输出)。然后，使用规则管理程序 140 将返回步骤 S38，在该步骤中，它将使 CPU 32 计算整个时间限制数据库的哈希值并保存到非易失性存储器 34 中。

在步骤 S39 中，使用规则管理存储器 140 将为该内容设置未注册的标志。
另一方面，如果在步骤 S40 中确定出当前的日期距注册日期不超过 48
小时，那么禁止将所选的内容复制到 HDD 21 中。在这种情况下，使用规则
5 管理程序将转移到步骤 S42 中，在该步骤中，它将为所选的内容设置注册标
志。

如果在步骤 S40 中不判断预先确定的时间，没用超过预先确定的时间，
那么该内容不能重新复制，这样，例如假冒销售或分销所要求的大量复制该
内容实际上就不可能了，而并不会无故地禁止普通的合法使用者对内容的复
制。注意到，在步骤 S40 所做的评价标准是时间延迟 48 个小时，而不限制
10 为 48 个小时。例如，该标准可以是从 12 到 168 小时间的任何时间。

如上所述，通过检查时间限制数据库，就设置了指示所选内容是否已在
HDD 21 中注册的标志。

再参考图 7 作进一步说明。在步骤 S13 中，复制管理程序 133 根据上面
提到的标志判断出所选内容已经在时间限制数据库中注册。如果所选内容已
15 经注册，那么复制管理程序 133 将转移到步骤 S14，在此，它将使记录程序
113 在显示单元 20 上显示一个消息，例如“这首音乐不能复制，因为该音乐
已经复制一次，而且未超过 48 个小时”。于是，用户能知道该内容不能复制
到 HDD 21 的原因。

如果在步骤 S13 确定所选内容还没有在时间限制数据库注册，那么复制
20 管理程序 133 将转移到步骤 S15，在此，记录程序 113 将从驱动器 22 的 CD
装置中读取内容。如图 10 所示，该内容已经在预先确定的位置插入水印码。
在步骤 S16 中，记录程序 113 将提取出包含在该内容中的水印码，并在步骤
S17 中判断该水印码是否指示禁止复制该内容。如果该水印码指示禁止复
制，那么，复制管理程序 133 将转移到步骤 S18，在此，它将使记录程序 113
25 通过接口 17 在显示单元 20 上显示例如这样的消息“复制被禁止”，并中断
该复制操作。

另一方面，在步骤 S17 判断出水印码指示复制不被禁止，那么，复制管
理程序 133 将转移到步骤 S19，在此，记录程序 113 将使压缩/展开程序 138
通过软件操作，使用如 ATRAC(Adaptive Transform Acoustic Coding, 自适应
30 变换语音编码)3(商标)的方法压缩该内容。在步骤 S20，记录程序 113 将使加
密程序 137 通过如 DES(Data Encryption Standard, 数据加密标准)、FEAL(Fast

Encipherment Algorithm, 快速加密运算算法)等使用已经预先设置并保存在存储器 13 中的加密密钥加密该内容。所述加密密钥可以是根据由软件操作产生的随机数或由适配器 26 的 CPU 32 产生的随机数形成的密钥。通过使个人计算机和作为计算机 1 辅助硬件的适配器 26, 以联合的方式加密该加密密钥, 能获得的加密将使解密该加密的加密密钥非常困难。

接着在步骤 S21 中, 记录程序 113 将加密的数据传递到内容数据库 114, 给该数据指定文件名并使 HDD 21 将它保存为一个文件(如内容文件 161)。可选择地, 记录程序 113 可以在保存 HDD 21 之前, 给定加密数据的位置信息(即从顶开始的字节数)作为一个文件的一部分。

10 数据的保存可以与前述的压缩和加密独立进行或同时进行。

再接着在步骤 S22 中, 记录程序 113 将使用预先确定的存在非易失性存储器 34 中的副本密钥(save key)和前述的 DES 方法、FEAL 方法或其它方法, 使加密程序 137 加密已用于加密该内容的加密密钥, 将加密的加密密钥保存在 HDD 21 的音乐数据库中(相应于如图 4 所示的内容数据库 114 的使用规则文件 161-1 到 162-N)。

20 在步骤 S23 中, 记录程序 113 将设置所保存的有关该文件的信息, 加密的加密密钥、该内容的信息和由用户通过 GUI 提供的音乐标题信息的元素, 并将它注册在 HDD 21 的音乐数据库中(如使用规则文件 162-1 到 162-N)。在步骤 S24, 记录程序 113 将使 CPU 32 计算整个音乐数据库的哈希值并将它保存在非易失性存储器 34 中。

25 这样, 例如如图 11 所示的音乐数据库就注册到 HDD 21 中。在该音乐数据库例子中, 有每个项目 1 到 3 中每个项目的所记录的文件名、加密的加密密钥、音乐题目、播放时间长度、回放条件(开始日期、结束日期和回放限制), 回放计数器、回放记帐条件、复制条件(复制数), 复制计数器和复制条件(SCMS)。

例如, 在由 SDMI(Secure Digital Music Initiative, 安全数字音乐倡导)定义的方法中, 一项内容从可以被登出(或登出限制)的 CD 中复制的次数设置为 3。

30 一方面, 由于当将一项内容从 CD 复制到 HDD 21 的时间已经过了预先确定的时间段时, 该内容可被再次复制, 并且仅仅出于用户私人的使用, 允许将该内容复制多次。在另一方面, 如果试图复制的次数远远大于用户私人

使用的允许次数，例如，大规模地的复制，那么复制将花费很长时间而实际上是不可能的。还有，如果个人计算机 1 没有复制，并且记录在 HDD 21 中的内容已经被删除，当预先确定时间过去了，所删除的内容也被再次复制并记录到 HDD 21 中。

5 还有，记录在 HDD 21 中的时间限制数据库的内容通过网络 2 能被共享。

上述解释的例子中，复制的日期相应地保存到 ISRC 中。但是除 ISRC 之外，可以使用任何其它可被识别的内容和 CD 的信息(如音标题目、专辑名或它们的组合)。

接着将在以下参考图 12 到 14 的流程图说明由执行显示/操作指导程序
10 112 和内容管理程序 111 的 CPU 11，以及执行主程序的 CPU 52 所产生的，
将一项内容从 HDD 21 移动到便携设备 6 的快闪存储器 61(即：存储器戳
(memory stick)(商标))和内容登出的操作。

首先，在下文说明内容的移动。在步骤 S51 中，移动管理程序 134 使用规则管理程序 140 计算整个音乐数据库的哈希值，并且在步骤 S52 中，将
15 计算的哈希值与由 CPU 32 先前计算并保存在非易失性存储器 34 中的哈希值进行比较。当这两个哈希值不一致时，移动管理程序 134 将转移到步骤 S53，在此步骤中，它将使显示/操作指导程序 112 在显示单元 20 上显示这样的消息“音乐数据库可能被篡改或改变了”，并终止该操作。这些操作与图 8 的
20 步骤 S31 到 S34 的操作相似。在此情况下，该内容将不会从 HDD 21 移动到便携设备 6 上。

接着，在步骤 S54 中，移动管理程序 134 读取在 HDD 21 形成的、记录在音乐数据库(包含在内容数据库 114 内)的有关内容的信息，并使显示/操作指导程序 112 在显示单元 20 上显示该信息作为选择使用的 GUI。用户点击一首音乐标题(内容名)和显示在图 5 区域 212 中的按钮 216，来选择将从 HDD
25 21 移动到便携设备 6 的内容。接着在步骤 S55 中，移动管理程序 134 检查在步骤 S54 中已选内容的回放条件、复制条件、回放记帐条件等。将参考图 15 的流程图在后面对该操作进一步说明。

接下来在步骤 S56 中，在个人计算机 1 的认证程序 141 和便携设备 6 的 CPU 53 之间进行互相认证，并且在两者之间共享通信密钥。

30 例如，在此假定便携设备 6 的快闪存储器 61(或 EEPROM 68)具有一个预先保存的主密钥 KM，个人计算机 1(或 HDD 21 中预先确定的文件)的 RAM

具有预先保存的一个个人密钥 KP 和 ID。CPU 53 被提供了从认证程序 141 来的先前保存在 RAM 13 中的 ID，并且将哈希函数作用到 ID 和它自己的主密钥 MK 上，以产生与个人计算机 1 的个人密钥相同的密钥，并保存在 RAM13 中。这样，个人计算机 1 和便携设备 6 将共享用于产生临时通信密钥的公共个人密钥。

可选择地，ID 和主密钥 KMM 被预先保存在个人计算机 1 的 RAM13 中，并且 ID 和主密钥 KMP 被预先保存在便携设备 6 的快闪存储器 61 中。RAM 13 将它的 ID 和主密钥发送到快闪存储器 61 中，而快闪存储器 61 又将它的 ID 和主密钥发送到 RAM 13 中，并且 RAM 13 将哈希函数作用到从快闪存储器 61 中接收的 ID 和主密钥上，而后者将哈希函数作用到从 RAM 13 中接收的 ID 和主密钥上。这样，RAM 13 产生快闪存储器 61 的个人密钥，而后者产生 RAM 13 的个人密钥。临时通信密钥将进一步从该个人密钥中产生。

应该注意到对于认证方法，例如可以使用 ISO(国际标准化组织)9798-2。

当没用正确地互相认证时，操作就终止了。当成功地进行了相互认证时，移动管理程序 134 将使内容数据库 114 在步骤 S57 中从音乐数据库中读取所选内容的文件名称，并且从 HDD 21 中读取具有该文件名的一项内容(例如，在图 7 的步骤 S20 中该文件名已经被加密了)。在步骤 S58 中，移动管理程序 134 将压缩方法(用于在步骤 S19 中实施的压缩)、加密方法(用于在步骤 S20 中实施的加密)，格式(例如报头的格式)，等等在步骤 S57 中读取的作为数字数据的内容转换为用在便携设备 6 中的形式。该转换将在后面参考图 17 中的流程图进一步说明。

在步骤 S59 中，移动管理程序 134 将使 PD 驱动器 143 将在步骤 S58 中所转换的内容通过 USB 端口 23 传递给便携设备 6。在步骤 S60 中，便携设备的 CPU 53 通过 USB 连接器 56 接收所传递的内容并且原样保存到快闪存储器 61 中。

在步骤 S61 中，移动管理程序 134 将进一步使使用规则转换程序 139 将所选内容的回放条件(开始日期、结束日期，回放限制等)转化为在便携设备 6 中使用的回放条件，并在音乐数据库中注册。在步骤 S62 中，移动管理程序 134 将进一步使使用规则转换程序 139 将用于选择内容复制条件中的 SCMS 信息转换为便携设备 6 管理的格式，并在音乐数据库中注册。然后在步骤 S63 中，移动管理程序 134 使 PD 驱动器 143 向便携设备 6 传递在步骤

S61 所转换的回放条件和在步骤 S62 中已经转换的 SCMS 信息。便携设备 6 的 CPU 53 将所传递的回放条件和 SCMS 信息传递给快闪存储器 61 中。

在步骤 S64 中，移动管理程序 134 使 PD 驱动器 143 向便携设备 6 传递所选内容的回放条件、回放记帐条件、复制条件等等，并在音乐数据库中注册，象 CPU 11 在音乐数据库中处理的格式中的那样，并且将它们保存在快闪存储器 61 中。

在步骤 S65 中，移动管理程序 134 使内容数据库 114 从音乐数据库读取所选内容的加密的加密密钥，然后在步骤 S66 中，移动管理程序 134 将使解密程序 142 利用保存在 RAM 13 中的副本密钥来解密加密密钥，并且，加密程序 137 利用通信密钥加密已解密的加密密钥。然后，移动管理程序 134 使 PD 驱动器 143 利用通信密钥将加密的加密密钥传递给便携设备 6。

在步骤 S67 中，便携设备 6 的 CPU 53 将使用由相互认证产生的公共通信密钥，解密从个人计算机 1 传递来的加密密钥，并用自己的副本密钥加密该加密密钥，使该加密密钥与已经保存的数据相关联，并将它保存到快闪存储器 61 中。

当完成了加密密钥的保存后，在步骤 S68 中，CPU 53 将通知个人计算机 1 加密密钥已经保存。当从便携设备 6 接收到该信息时，在步骤 S69 中，个人计算机 1 的移动管理程序 134 将使内容数据库 114 删除相应于该内容的内容文件 161，以及从音乐数据库中删除该内容元素的设置(即：使用规则文件 162)。这样该内容将被移动，而不是被复制。在步骤 S70 中，所述移动管理程序 134 将音乐数据库中的数据传递给适配器 26 的 CPU 32，并使 CPU 32 计算整个音乐数据库的哈希值，且将该哈希值保存在非易失性存储器 34 中。该哈希值在上面步骤 S52 中的作为先前保存的哈希值使用。

接着，下面将说明将个人计算机 1 中的一项内容登出到便携设备 6 中。这个操作与在前面参考图 12 到 14 所说明的将内容从个人计算机 1 移动到便携设备 6 的操作相似。也就是说，登出操作基本相似于内容移动操作，只是登出操作由登入/登出管理程序 132 在个人计算机 1 中执行，且在图 14 的步骤 S 69 中只是更新在音乐数据库中所登出和记录内容的已经登出(或能被登出)的次数，因此，对登出操作将不再加以说明。

执行内容管理程序 111 的 CPU 11 检查图 12 的步骤 S55 中所选内容的回放条件等。下面将参考图 15 对这种检查操作进行说明。在步骤 S81 中，移

动管理程序 134 使内容数据库 114 从音乐数据库读取各种条件。然后，在步骤 S82 中，移动管理程序 134 将判断步骤 S81 中的那些条件下读取的复制计数器是否已超出复制极限。当复制计数器已超出复制极限时，不允许进一步的复制，于是，移动管理程序 134 将转移到步骤 S83，在该步骤中移动管理
5 程序 134 将使显示/运行指导程序 112 在显示单元 20 上显示如“复制计数器
已经超出了复制极限”的消息，并终止操作。如果在步骤 S82 中确定该复制计数器没有超出复制极限时，移动管理程序 134 转移到步骤 S84，在该步骤中
10 移动管理程序 134 将判断当前日期是否超过回放的结束日期。当前日期是从适配器 26 的 RTC 35 输出的日期。由于这种操作，用户不能使用个人计算机
11 中的任何当前时间，该当前时间可采用有意地修改为过去时间而获得。移动管理程序 134 由 CPU32 提供当前时间，并且在步骤 S84 中自己进行判断，或在步骤 S81 中，将从音乐数据库读取的回放条件提供给适配器 26 的 CPU
32，这样使 CPU 32 在步骤 S84 中进行判断。

如果当前的日期超过了回放的结束日期，那么移动管理程序 134 转移到
15 步骤 S85 中，在该步骤中，它将使内容数据库 114 从 HDD 21 中删除所选择的内容，从音乐数据库中删除关于所选择内容的信息。在步骤 S86 中，移动管理程序 134 使 CPU 32 计算整个音乐数据库的哈希值并将它保存到非易失性存储器 34 中。到这里操作就结束了。因此，在这种情况下将不移动任何
16 内容。

如果在步骤 S84 中确定出当前日期还没有超过回放的结束日期，那么移动管理程序 134 将转移到步骤 S87 中，在该步骤中它将判断所选内容的回放记帐条件(例如每次回放的费用)是否在音乐数据库中注册。如果发现回放记帐条件注册了，则移动管理程序 134 将在步骤 S88 中，使 PD 驱动器 143 与便携设备 6 通信以判别便携设备 6 是否有记帐功能。如果便携设备 6 没有记
20 帐功能，则所选择的内容不能被传递到便携设备 6 中。因此，移动管理程序 134 将在步骤 S89 中使显示/操作指导程序 112 在显示单元 20 上显示一条消息“目标没有记帐功能”，并终止操作。

如果在步骤 S87 中确定出注册了没有回放记帐条件，或在步骤 S88 中便
25 携设备 6 具有记帐功能，那么移动管理程序 134 将转移到步骤 S90 中，在该步骤中它将判断出是否为所选择的内容注册了其它的回放条件例如回放限制。如果发现注册了其它回放条件，那么移动管理程序 134 就转移到步骤

S91，在该步骤它将判断便携设备 6 是否具有符合回放条件的功能。如果便携设备 6 没用这样的功能，则移动管理程序 134 转移到步骤 S92，在该步骤中它将使显示/操作指导程序 112 在显示单元 20 上显示一条消息“目标没有记帐功能”，并终止操作。

5 如果在步骤 S90 中确定注册了没有回放条件，或者，如果在步骤 S91 中确定出便携设备 6 具有符合回放条件的功能，将结束回放条件的检查，并且移动管理程序 134 将返回到图 12 的步骤 S56 中。

10 图 16 表示便携设备 6 管理的(可以符合(follow)的)回放条件的例子。图 16 所示的回放条件保存在 EEPROM68 中。在这个例子中，为项目 1 到 3 的每项内容注册回放的开始日期和结束日期。但是，只为项目 2，不为项目 1 和 3 注册回放限制。因此当项目 2 的内容作为选择的内容时，就可能符合回放的限制如回放条件(一项内容可以被回放的次数)，但当项目 1 或 3 的内容作为选择的内容时，就不可能符合回放限制。

15 接下来，将在下面参考图 17 中的流程图，详细说明由执行内容管理程序 111 的 CPU 11 在图 12 的步骤 S58 中产生的格式转换。在步骤 S101 中，移动管理程序 134 检查所选内容的格式(如包括回放条件的报头、使用规则、复制条件等)，并记录在内容数据库 114 中。在步骤 S102 中，移动管理程序 134 将检查可以在目标中设定的条件(在这种情况下的便携设备 6)，即移动管理程序 134 查询这种可设定条件的便携设备的 CPU 53，并从 CPU53 获得回答。在 20 步骤 S103 中，移动管理程序 134 将根据在步骤 S102 中检查的条件，以在音乐数据库中登入的格式，确定出一些可以在目标中设置的条件。

25 在步骤 S104 中，移动管理程序 134 判断是否有一些在目标中可以设定的条件。如果没有这样的条件，移动管理程序 134 就转移到步骤 S105，在该步骤中将禁止将内容移动到便携设备 6 中。也就是说，在这种情况下，由于在音乐数据库中注册的条件不能符合便携设备 6 的条件，所以禁止将内容移动到便携设备 6 中。

30 如果在步骤 S104 中确定出存在这样的可设定的条件，那么移动管理程序 134 就转移到步骤 S106，在该步骤中，它将使使用规则转换程序 139 将这些条件转换为目标功能格式的条件(例如当所选的内容被传递到便携设备时，被保存在报头中的条件)。然后在步骤 S107 中，移动管理程序 134 将在目标中设定所转换的条件。结果，便携设备 6 将能依据设定的条件(或符合的

条件)回放该内容。

接下来，在下面将参考图 18 至 20 的流程图说明从 HDD 21 到便携设备 6 的内容复制，该复制由执行内容管理程序 111 的 CPU 11 和执行主程序的 CPU 53 实施。复制内容管理程序 133 实施图 18 到 20 中步骤 S111 到 S127
5 的操作。这些操作与步骤 51 到 67 中将内容从 HDD 21 复制到便携设备 6 相似，如图 12 到 14 所示。而且在这种情况下，检查音乐数据库以确定它是否被伪造或改变，然后用记录在音乐数据库中的条件检查所选内容的回放条件。进一步，在进行了便携设备 6 和个人计算机 1 之间的相互认证后，该内
10 容被从个人计算机 1 的 HDD 21 中传递到便携设备 6 的快闪存储器 61 中，并在那里保存起来。然后在步骤 S128 中，复制管理程序 133 将在音乐数据库中将复制计数器的值加 1。在步骤 S129 中，复制管理程序 133 将使 CPU 32
15 计算整个音乐数据库的哈希值，并将它保存到非易失性存储器 34 中。

接下来，在下面将参考图 21 中的流程图，说明从便携设备 6 到 HDD 21 的内容移动和登入操作，该移动和登入操作由执行内容管理程序 111 的 CPU
11 和执行主程序的 CPU 53 实施。

首先解释内容移动。在步骤 S161 中，移动管理程序 134 要求便携设备 6 的 CPU 53 读取保存在快闪存储器 61 中的内容信息。当从移动管理程序 134
接收到请求时，CPU 53 将向个人计算机 1 传递保存在快闪存储器 61 中的内
容信息。根据该信息，移动管理程序 134 使显示单元 20 显示保存在快闪存
20 储器 61 中的所选内容的 GUI。根据显示在显示单元 20 上的 GUI，用户将操
作键盘 18 或鼠标 19 指定一项内容，该内容将从便携设备 6 移动到 HDD 21
中(内容数据库 114)。

在步骤 S162 中，移动管理程序 134 使认证程序 141 执行与 CPU 53 的相
互认证，以产生它们之间公共使用的通信密钥。该操作与图 12 的步骤 S56
25 中的操作相似。

接着，在步骤 S163 中，CPU 53 将读取保存在快闪存储器 61 中的加密的、所选的内容，并将它传递给个人计算机 1。在步骤 S164 中，移动管理程序 134 将从便携设备 6 传递的内容当作一个文件，给它一个文件名，并且
30 将它保存到内容数据库 114 中(在 HDD 21 中)。这种保存是利用给定为一个文件的一部分的位置信息(如从顶端开始的字节数)来完成的。

在步骤 S165 中，CPU 53 将读取所选内容的加密的加密密钥，记录在快

闪存储器 61 中，并且用它自己的副本密钥对其解密，进一步用通信密钥对其加密，并传递给个人计算机 1。加密密钥可以是例如在图 14 的步骤 S67 的操作中，已经被保存在快闪存储器 61 中的密钥。

当接收从便携设备 6 传递的加密密钥时，移动管理程序 134 将在步骤 5 S166 中使解密程序 142 用通信密钥解密加密密钥，并使加密密钥 137 用它自己的副本密钥对该加密密钥进行加密。在步骤 S167 中，移动程序管理 134 将使内容数据库 114 将内容文件名和在步骤 S164 中保存的内容信息，以及由用户通过 GUI 输入的音乐名(内容名称)，还有在步骤 S166 中加密的加密密钥等注册到音乐数据库中。然后在步骤 S168 中，移动管理程序 134 使使 10 用规则管理程序 140 通过 CPU 32 计算整个音乐数据库的哈希值，并且非易失性存储器 34 保存该哈希值。

在步骤 S169 中，移动管理程序 134 通知便携设备 6 该加密密钥已经保存了，并要求它删除该内容。当要求从个人计算机 1 中删除该内容时，CPU 53 就在步骤 S170 中删除保存在快闪存储器 61 中的该内容。

接着，下面将说明将一项内容从便携设备 6 登入到个人计算机 1 的操作。将内容从便携设备 6 登入到个人计算机 1 的操作与图 21 所示的将内容从便携设备 6 移动到个人计算机 1 的操作相似。也就是说，由个人计算机 1 中的登入/登出管理程序 132 实施登入操作，而省略在图 21 的步骤 S162 到 S166 的操作。还有，在图 21 的步骤 S167 中，个人计算机 1 将更新登出的限制，即所登入的内容可以被登出的次数，记录在音乐数据库中，并且在完成步骤 20 S170 的操作后，其后的操作，除将实施该内容文件的删除确定外，与内容移动的操作基本相同。对该操作将不再作进一步说明。

应注意到当便携设备 6 的快闪存储器 61 采用可移动的存储卡时，个人计算机 1 将在图 21 的步骤 S162 中产生登入过程的相互认证。

接着，下面将参考图 22 的流程图说明将内容从便携设备 6 复制到 HDD 21 的操作，该操作由执行内容管理程序 111 的 CPU 11 以及执行主程序的 CPU 53 实施。在将内容从便携设备 6 移动到 HDD 21 方面，图 22 的步骤 S181 到 S188 中的操作与(在图 21 中)步骤 S161 到 S168 的操作相似。也就是说，该复制由复制管理程序 133 实施，并且该复制操作除省略了图 21 的步骤 S169 到 S170 中的操作外，与移动操作基本相似。因此，对该复制运行将不作进一步说明。

接着，下面将参考图 23 的流程图说明将从 EMD 服务器 4 传递来的内容复制到 HDD 21 的操作，该操作由 EMD 服务器 4 和 执行内容管理程序 111 的 CPU 11 实施。当用户点击图 5 中的按钮 202 以产生访问 EMD 服务器 4 的指令时，在步骤 S201 中，购买程序 144 将使通信块 25 通过网络 2 访问
5 EMD 服务器 4 中。作为对此访问的响应，EMD 服务器 4 将如音乐数量、标题信息及一项内容所持有的信息通过网络 2 传递给个人计算机 1。当获得该信息时，购买程序 144 使显示/运行指导程序 112 通过接口 17 在显示单元 20 上显示该信息。利用在显示单元 20 上显示的 GUI，在步骤 S202 中，用户可指定他要复制的内容。所指定信息通过网络 2 传递给 EMD 服务器 4。在步
10 骤 S203，购买程序 144 将通过网络 2 实现它自己与 EMD 服务器 4 之间的相互认证，以产生它们共用的通信密钥。

个人计算机 1 与 EMD 服务器 4 之间实施的相互认证可通过使用如 ISO 9798-3 所定义的公开密钥和私人密钥实现。在此情况下，个人计算机 1 有它自己的私人密钥和预先持有的用于 EMD 服务器 4 的公开密钥，且 EMD 服务
15 器 4 有它自己的私人密钥。个人计算机 1 与 EMD 服务器 4 之间相互认证可使用这些密钥来实现。通过从 EMD 服务器 4 传递公开密钥的方式，或预先已经分配给个人计算机 1 证书的方式，而该证书由 EMD 服务器 4 确认，个人计算机 1 就可以获得个人计算机 1 的公开密钥。进一步在步骤 S204 中，
20 购买程序 144 将在它自己与 EMD 服务器 4 之间进行记帐操作。记帐操作将在后面参考图 24 的流程图作进一步说明。

接着，在步骤 S205 中，EMD 服务器 4 通过网络 2 将在步骤 S202 指定的加密内容传递给个人计算机 1。此时，它在任何时间都给个人计算机 1 传递时间信息。在步骤 S206，购买程序 144 将给所传递的内容指定一个文件名，并使内容数据库 114 将该内容作为一个内容文件 161 保存在 HDD 21 中。
25 在步骤 S207，EMD 服务器 4 将进一步使用在步骤 S203 产生的、它自己与个人计算机 1 共用的通信密钥，加密该内容的加密密钥，并且将该加密的加密密钥传递给个人计算机 1。

在步骤 S208，购买程序 144 使解密程序 142 单独使用通信密钥或与适配器 26 的 CPU 32 协同一起解密从 EMD 服务器 4 传递来的加密密钥，并使加密程序 137 用它自己的副本密钥加密所解密的加密密钥。在步骤 S209 中，
30 购买程序 144 将使内容数据库 114 把由用户输入的一系列的内容的文件名

称、内容信息、音乐标题，以及加密的加密密钥注册在 HDD 21 的音乐数据库中。进一步在步骤 S210 中，购买程序 144 使 CPU 32 计算全部音乐数据库的哈希值，并将它存入非易失性存储器 34 中。

注意在步骤 S205 中，EMD 服务器 4 将该内容连同时间数据一起发送给 5 个人计算机 1。时间数据从个人计算机 1 传递到适配器 26。当接收到从个人计算机 1 传递来的时间数据时，在步骤 S211，适配器 26 的 CPU 32 将修正 RTC 35 的时间。这样，根据从已经识别为正确设备的外部设备提供的时间信息作为相互认证的结果，对适配器 26 的 RTC 35 的时间信息进行改正，这样使得适配器 26 总能保持正确的时间信息。

10 接下来，将参考图 24 的流程图说明由 EMD 服务器 4 和执行内容管理程序 111 的 CPU 11 在图 23 的步骤 S204 中实施的记帐操作。在步骤 S221 中，购买程序 144 从步骤 S201 的 EMD 服务器 4 传递的价格信息中读取步骤 S202 指定的所选内容的价格信息，并将它写到 HDD 21 中的记帐日志中。图 25 表示一个这样记帐日志的例子。在该例子中，用户从 EMD 服务器 4 中复制 15 项目 1 到 3，项目 1 和 2 的价格为 50 日元，而项目 3 的价格为 60 日元。该记帐日志的哈希值已经由 CPU 32 计算出，并且注册在非易失性存储器 34 中。

接着在步骤 S222 中，购买程序 144 将从 HDD 21 中读取在步骤 S221 中写的记帐日志，并将它通过网络 2 传递到 EMD 服务器 4 中。在步骤 S223 中，
20 EMD 服务器 4 根据从个人计算机 1 传递的记帐日志进行记帐计算。也就是说，EMD 服务器 4 将个人计算机 1 的用户传递的记帐日志添加到其所提供的数据库中，并更新数据库。在步骤 S224 中，EMD 服务器 4 判断是否立即处理记帐日志。当确定立即处理记帐日志时，EMD 服务器 4 就转移到步骤 S225 中，在该步骤中，它将传递给处理服务器(未表示出)交易名称，现金数量等处理所需要的信息。然后在步骤 S226 中，处理服务器将对个人计算机 1
25 的用户实施处理。如果在步骤 S224 中确定记帐日志不被立即处理，那么将跳过步骤 S225 和 S226 的操作。即将周期性地执行这些操作，例如一个月一次。

接着，参考图 26 和 27 的流程图，说明执行内容管理程序 111 的 CPU 11 30 所产生的将 CD 播放机(未表示出)回放的、并从音频输入/输出终端 24 的 IEC60958 终端 24a 输入的内容复制到 HDD 21 中的操作。在步骤 S241 中，

用户将 CD 播放机的 IEC60958 输出终端连接到个人计算机 1 的音频输入/输出接口 24 的 IEC60958 终端 24a 上。在步骤 S242 中，用户操作键盘 18 或鼠标 19 以输入将从 CD 播放机(或内容的序号)复制的一项内容的音乐标题。然后在步骤 S243 中，用户操作 CD 播放机上的按钮以开始播放 CD 播放机。

5 如果在 CD 播放机和个人计算机 1 之间连接有一个控制信号发送/接收线，那么用户可以操作个人计算机 1 的键盘 18 或鼠标 19，以输入回放开始指令，从而使 CD 播放机开始播放 CD。

当 CD 播放机开始播放 CD 时，在步骤 S242 中，从 CD 读出的内容通过 IEC 60958 终端 24a 被传递到个人计算机 1 中。在步骤 S245 中，复制管理程序 133 从通过 IEC 60958 终端 24a 输入的数据中读取 SCMS(串行复制管理系统)数据。SCMS 数据包括复制条件信息如禁止复制、允许进行一次复制、允许免费复制等。在步骤 S246 中，CPU 11 判断 SCMS 数据是否指示禁止复制，如果 SCMS 数据指示禁止复制，那么复制管理程序 133 就转移到 S247，在该步骤中它将使显示/操作指导程序 112 在显示单元 20 上显示如“复制被禁止”的消息，并终止复制操作。在这种情况下，禁止向 HDD21 中复制。

在步骤 S246 中，当由 CPU 11 确定出在步骤 S245 中读取的 SCMS 信息没有指示任何复制禁止时，那么复制管理程序 133 将转移到步骤 S248 中，在该步骤它读取一个水印码，并且在步骤 S249 中，它将判断水印码是否指示禁止复制。当水印码指示禁止复制时，那么复制管理程序 133 就转移到步骤 20 S247，在该步骤中它将使显示/操作指导程序 112 在显示单元 20 上显示上述预先确定的消息，并终止复制操作。

如果在步骤 S249 中确定出水印不指示任何复制禁止，那么复制管理程序 133 将转移到步骤 S250，在该步骤中它将检查时间限制数据库。如果发现所选的内容已经注册，作为时间限制数据库检查的结果，那么，该操作就以在步骤 S251 和 S252 中的操作而结束。这些操作与在图 7 的步骤 S13 和 S14 中的操作相似。

如果所选的内容不是尚未在 HDD 21 中注册的内容，它将在步骤 S253 到 S258 中登入。在步骤 S253 到 S258 的操作与在图 7 步骤 S19 到 S24 的操作相似，除了从 IEC 60958 终端 24a 提供的 SCMS 信息在步骤 30 7 中还在音乐数据库中之中注册了之外。因此，对这些操作不作进一步的说明了。

接着将参考图 28 和 29 的流程图说明执行内容管理程序 111 的 CPU 11

所实施的将一项内容从 HDD 21 中输出(回放)到 IEC 60958 终端 24a 的操作。在步骤 S271 到 S273 中，象图 18 的步骤 S111 到 S113 中那样计算整个音乐数据库的哈希值，并判断该哈希值是否与先前保存的相一致，以检查音乐数据库是否被伪造或改动过。如果音乐数据库没有被伪造，那么显示/操作指导
5 程序 112 转移到步骤 S274，在该步骤中，它将通过内容管理程序 111 使内容
数据库 114 访问 HDD 21 中的音乐数据库，读取关于在音乐数据库中注册的
音乐的信息，并显示在显示单元 20 上。观测该显示，用户以适当的方式操
作键盘 18 或鼠标 19 来选择用户想要回放的内容。在步骤 S275 中，显示/操
作指导程序 112 检查所选内容的回放条件。后面将参考如 30 中的流程图进
10 一步说明回放条件的检查。

接着在步骤 S276 中，显示/操作指导程序 112，通过内容管理程序 111，使内容数据库 114 从音乐数据库中读取在步骤 S274 所选内容的加密密钥，并且解密程序 142 使用副本密钥解密加密的密钥。在步骤 S277 中，显示/操
作指导程序 112，通过内容管理程序 111，使内容数据库 114 从音乐数据库中
15 读取所选内容的 SCMS 信息，并且依据 SCMS 系统的规则决定将从 IEC60958
终端 24a 输出的 SCMS 信息。例如：如果内容可被回放的次数是有限的(即：
作为回放限制)，那么回放计数器加 1。因此增加的回放计数被当作新的 SCMS
信息。在步骤 S278 中，显示/操作指导程序 112，通过内容管理程序 111，将
进一步使内容数据库 114 从音乐数据库读取所选内容的 ISRC。

20 接着在步骤 S279 中，显示/操作指导程序 112，通过内容管理程序 111，使内容数据库 114 从音乐数据库读取所选内容的文件名，然后，根据该文件名从 HDD 21 读取该内容。进一步，显示/操作指导程序 112，通过内容管理程序 111，使内容数据库 114 从音乐数据库读取所该内容的加密密钥，并且解密程序 142 使用副本密钥解密该加密密钥，然后使用解密的加密密钥解密
25 加密的内容。压缩/展开程序 138 将进一步解密(展开)该内容的压缩码。在步
骤 S280 中，显示/操作指导程序 112 使驱动器 117，在 IEC60958 24a 上，输出在步骤 S279 读取的解密的内容(数字数据)，还有在步骤 S277 确定的 SCMS
信息，以及在步骤 S278 依据 IEC60958 规则读取的 ISRC 信息。更进一步，
显示/操作指导程序 112 将使如实时播放器(商标；未示出)的程序进入运行以
30 将数字数据内容转化为模拟数据，且在音频输入/输出接口 24 的模拟输出端
输出。

在步骤 S281 中，显示/操作指导程序 112，通过内容管理程序 111，使内容数据库 114 将音乐数据库中的回放计数器加 1。在步骤 S282，判断所选内容是否有加在其中的回放记帐条件。如果所选内容有加在其中的记帐条件，那么显示/操作指导程序 112 就转移到步骤 S283，在该步骤中它将使内容数据库 114 通过内容管理程序 111 向记帐日志中写入相应的费用。在步骤 S284 中，显示/操作指导程序 112 将通过使用规则管理程序 140，使 CPU 32 计算整个音乐数据库的哈希值并将它保存到非易失性存储器 34 中。如果在步骤 S282 中确定出所选内容没有加在其中的回放记帐条件，那么显示/操作指导程序 112 将跳过在步骤 S283 和 S284 中的操作。

接着将参考图 30 所示的流程图详细说明由执行内容管理程序 111 的 CPU 11 所实施的在图 28 的步骤 S275 中回放条件的检查。在步骤 S301 中，显示/操作指导程序 112 将通过内容管理程序 111 使内容数据库 114 读取在音乐数据库中的各种条件。在步骤 S302 中，使用规则管理程序 140 判断从音乐数据库中读取的条件中的回放计数是否超过回放限制。如果回放计数超过了回放限制，那么使用规则管理程序 140 转移到步骤 S303，在该步骤中它将通过内容管理程序 111 使内容数据库 114 从 HDD 21 中删除所选内容，从音乐数据库中删除关于所选内容的信息。在步骤 S304 中，显示/操作指导程序 112 将进一步通过使用规则管理程序 140 使 CPU 32 计算音乐数据库的新的哈希值并将它保存到非易失性存储器 34 中。在这种情况下，禁止回放(输出)。

如果在步骤 S302 中，确定出回放计数没有超过回放限制，那么使用规则管理程序 140 就转移到步骤 S305，在该步骤中它将判断回放的结束日期是否超过当前日期。如果回放的结束日期超过当前日期，那么显示/操作指导程序 112 在步骤 S303 中将使使用规则管理程序 140 从 HDD 21 中并从上述的音乐数据库中删除所选的日期。在步骤 S304 中，计算并保存音乐数据库的新的哈希值。在这种情况下，也禁止回放(输出)。

如果在步骤 S305 中确定出回放的结束日期没有超过当前日期，那么 CPU 32 转移到步骤 S306，在该步骤中，它将判断所选内容是否有加在其中的回放记帐条件。如果所选内容有加在其中的记帐条件，那么显示/操作指导程序 112 就转移到步骤 S307，在该步骤它将使显示单元 20 显示回放记帐条件加上费用的消息。如果在步骤 S306 中确定出所选内容没有加在其中的记帐条件，那么就跳过步骤 307 的操作。

接着将参考图 31 和 32 所示的流程图说明由执行内容管理程序 111 的 CPU 11 所实施的，通过便携设备 6 从 HDD 21 中进行内容回放(输出)的操作。在步骤 S321 到 S325 中，检查音乐数据库是否伪造或改动了，指定所选内容并检查所选内容的回放条件。这些操作与图 28 的步骤 S271 到 S275 中的操作相似，将不再说明。

在步骤 S326 中，在便携设备 6 和个人计算机 1 之间产生相互认证以产生它们之间共用的通信密钥。在步骤 S327 中，显示/操作指导程序 112 命令便携设备 6 回放将被提供的加密内容。在步骤 S328 中，显示/操作指导程序 112 将通过内容管理程序 111，使内容数据库 114 从音乐数据库中读取步骤 S324 中指定的所述内容的文件名称，并从 HDD21 中读取具有该文件名称的内容。在步骤 S329 中，显示/操作指导程序 112 将使内容管理程序 111 将内容压缩方法、加密方法和格式转换为便携设备 6 中使用的方法和格式。而且在步骤 S330 中，显示/操作指导程序 112 将使加密程序 137 使用通信密钥加密在步骤 S329 中所转换的内容，并将它传递给便携设备 6。

在步骤 S331 中，便携设备 6 的 CPU 53 对步骤 S327 中个人计算机 1 所传递的指令作出响应，以便用通信密钥解密所传递的数据并将它回放。在步骤 S332 中，显示/操作指导程序 112 将通过内容数据库 114，使内容管理程序 111 将在音乐数据库中的回放计数器加 1。而且在步骤 S333 中，显示/操作指导程序 112 将判断所选内容是否有加在其中的回放记帐条件。如果所选内容有加在其中的记帐条件，那么显示/操作指导程序 112 就在步骤 S334 中，通过内容管理程序 111，使内容管理数据库 114 向记帐日志中写入回放的费用。在步骤 S335 中，显示/操作指导程序 112 将使 CPU 32 计算整个音乐数据库的新的哈希值。如果所选内容没有加在其中的回放记帐条件，那么就跳过在步骤 S334 和 S445 中的操作。

本发明提供了各种方法防止内容欺诈性的复制。例如，操作 CPU 11 的程序是所谓的阻止篡改软件，该软件的执行顺序在 CPU 11 的每个操作中是不同的。

而且，CPU 11 的功能由采用硬件的适配器 26 共同承担，以使 CPU 11 和适配器一起工作才能执行各种操作。因此就保证了很高的数据安全。

例如，音乐数据库的哈希值没有象以上所述那样保存在音乐数据库本身中，而是保存在适配器 26 的非易失性存储器 34 中。即，例如与先前在步骤

S32 和 S33 中保存的哈希值相比，先前的用于比较的哈希值保存在非易失性存储器 34 中。因此，在所有的记录包括保存在 HDD 21 中的内容被复制或移动到任何其它记录介质之前，都可以备份。在保存在 HDD 21 的内容被从 HDD 21 复制或移动到任何其它记录介质之后，包含在所述记录中、备份到 5 HDD 21 中的内容可以被重新恢复，这样就能阻止不顾使用规则无限制地复制或移动内容。

例如，当内容 A 和 B 被保存到 HDD 21 时，如图 33 所示，内容 A 和 B 的哈希值就被保存在非易失性存储器 34 中。这里假定在这种情况下，包含在 HDD 21 中的内容 A 和 B 的一部分或所有记录数据被备份到另一个记录介质 271 上。当 HDD 21 上的内容 A 被移动到另一个记录介质 272 后，就只有 10 内容 B 将保留于在 HDD 21 记录的内容中，这样非易失性存储器 34 中的哈希值也变为内容 B 的哈希值。

如果记录在 HDD 21 中的部分或全部数据，已备份在记录介质 271 中，其后被恢复到 HDD 21 中，且内容 A 和 B 被再次保存在 HDD 21 中，则将发现从内容 B 的信息计算的哈希值保存在非易失性存储器 34 中，同时，将发现从内容 A 和 B 的信息计算的哈希值没有保存在非易失性存储器 34 中。因此，根据保存在 HDD 21 中的内容 A 和 B 计算的哈希值将与先前保存在非易失性存储器 34 中的哈希值不一致，这就检测出音乐数据库已经被伪造了。结果，之后使用保存在 HDD 21 中的内容 A 和 B 将受到限制。

进一步，如上述已经说明的，适配器 26 包含 RTC 35。根据从可被正确认证的任何其它设备(如：EDM 服务器 4)传递来的时间数据，修正 RTC 35 的时间信息。使用从 RTC 35 输出的当前日期，而不是由个人计算机 1 管理的任何日期。因此，用户不能故意地在个人计算机 1 上将当前日期编辑为任何过去的日期，这样，就避免了将当前日期判定为超过回放条件中的回放结束日期。

根据预先保存在 ROM 36 中的程序，适配器 26 还被指定解密所传递的加密程序，并执行该程序，这样，能保证了较高的数据安全性。将在下面参考图 34 的流程图对此作进一步说明。

更具体地说，当个人计算机 1 将去执行适配器 26 需要的预先确定的操作时，在步骤 S351，将使用预先保存在 RAM 13 中的加密密钥，加密要由适配器 26 执行的程序，并将它传递给适配器 26。适配器 26 的 RAM 13 先前已

经在其中保存了从个人计算机 1 传递来的程序并希望解密和执行该加密的程序。CPU 32 遵循保存在 RAM 36 中的该程序，以在步骤 S352 中解密保存在 RAM 36 中的该加密的程序。在步骤 S313，CPU 32 把解密的程序展开在 RAM 33 中，并在步骤 S354 执行该程序。

5 如前面所说明的，例如，当适配器 26 计算在 HDD 21 中的音乐数据库的哈希值时，个人计算机 1 的 CPU 11 将使用加密密钥加密音乐数据库中的数据，并将它传递给适配器 26 的 CPU 32。CPU 32 将哈希函数作用到音乐数据库中所传递的数据上，计算其哈希值。于是，计算的哈希值将保存在非易失性存储器 34 中。可选择地，CPU 32 将该哈希值与先前已预先保存的哈希值进行比较，并将计算结果传递到个人计算机 1 的 CPU 11 中。
10

15 图 35 详细表示了适配器 26 的内部结构。适配器 26 由半导体 IC 组成。如图 35 所示，适配器 26 包括：除图 2 所示的接口 31、CPU 32、RAM 33、非易失性存储器 34、RTC 35、ROM 36 外，还有：RAM 控制器 301，控制从 RAM 33 读和写操作，以及逻辑电路 302，使用它，从适配器 26 直接输出如上所述已经解密的加密内容。

从接口 31 到 ROM 36、RAM 控制器 301 和逻辑电路 302 的功能块集成在半导体 IC 中，按照这种方式，以它们就不可能被从外部拆开。

而且，提供晶体振荡器 311 为由适配器 26 执行的各种操作产生参考时钟。还提供振荡电路 312 以使 RTC 35 进行操作。适配器 26 还包括为振荡电路 312、非易失性存储器 34 和 RTC 35 提供后备电源的电池 313。另外，适配器 26 的元件电路由个人计算机 1 的电源电路 321 提供电源。
20

25 非易失性存储器 34 可由可擦除 ROM 组成。例如如图 36A 和 36B 所示，假如非易失性存储器 34 由从电池 313 提供备用电源的 RAM 组成，但是，保护性铝层 351 可在非易失性存储器 34 上形成，并且由电池 313 给非易失性存储器 34 提供电源的电源模型(pattern)352，可以与保护性铝层 351 同高形成。于是，如果用户试图移去保护性铝层 351 以改变非易失性存储器 34，与非易失性存储器 34 同高的电源模型也将被移去，为非易失性存储器 34 提供的电源也将被断掉，而且保存在存储器 34 中的数据将被擦除。这样，进一步提高了抵抗篡改能力。

30 进一步，适配器 26 被提供有连线 401-1 到 401-3，用于从非易失性存储器 34 读出日期或将日期写入非易失性存储器 34 中。如图 37 所示，连线 401-1

到 401-3 相互垂直交叠。因此，为从最低的连线 401-3 读取数据，不得不移开连线 401-3 上面的连线 401-1 和 401-2。因此，不能同时从 401-1 到 401-3 读取数据。

还有，非易失性存储器 34 的连线 401-1 到 401-3 可以形成冗余的形式。

5 例如，当在非易失性存储器 34 内部形成的连线 401-1 到 401-3 用于连接一些元件如形成非易失性存储器 34 的晶体管时，这些元件之间的连线不是直线形式的，即使可以通过连线以直线形式连接，但它们之间的连线具有预先确定的长度。这样，401-1 到 401-3 的连线将比所要求的长度要长，并且与连线为必需的最短长度时相比，具有较大的寄生电容。

10 为从非易失性存储器 34 中读取数据而设计的专用电路(作为半导体 IC 包含在适配器 26 中)，当该专用电路的阻抗与寄生电容相匹配时，它可以正常地读取保存在非易失性存储器 34 中的数据。但是，当探头连接到接线 401-1 到 401-3 以从非易失性存储器 34 中读取数据时，由于寄生电容和探头电容的结合，将使得不能正常地从非易失性存储器 34 中读取数据。

15 在前面的说明中，使用便携设备 6 来解释记录介质，但应注意的是，本发明可应用于将数据移动或复制到任何其它记录介质。

所述的内容除了是音乐声音数据如音乐或音频数据外，还可以是图像或其它数据。

如上所述，本发明具有下述优点：

20 (1) 依据本发明，数据被加密并记录在 HDD 21 中，并且加密密钥用副本密钥加密，记录在 HDD 21。这样，即使记录在 HDD 21 中的内容被复制了，该内容也不能被解密，这就使得不能大规模地复制散发。

(2) 依据本发明，当预先确定的音乐被复制一次时，其标题和记录数据就被注册在音乐数据库中，以阻止该音乐在预先确定的时间段内(如上述的 25 48 个小时)被复制。这样，可以限制该音乐被复制的次数，以阻止该音乐被大规模地复制散发。

而且依据本发明，每当更新数据库时，就计算数据库中数据的哈希值并且保存起来。这样很容易地阻止数据库被伪造或篡改。

(3) 依据本发明，一旦内容被传递到外部设备，相应的在 HDD 21 中 30 的内容就被删除了。这样，作为原始数字数据的内容将不再保留在 HDD 21 中，并且不能被大规模地复制散发。

(4) 依据本发明，在 HDD 21 中提供音乐数据库，以便每次检查整个音乐数据库的哈希值。这样，即使在 HDD 21 中的内容在移去之前已经备份了，并且在内容移去之后备份的数据又恢复到 HDD21 中，也肯定能擦除内容源中的数据。

5 (5) 依据本发明，在数据被从个人计算机 1 传递到外部设备之前，在个人计算机 1 和外部设备之间要进行相互认证。这样，就能阻止数据被传递到任何错误的设备中。

10 (6) 依据本发明，在数据被从外部设备传递到个人计算机 1 之前，通过在该外部设备和个人计算机 1 之间进行的相互认证，确定个人计算机 1 的软件是否合法。这样就能阻止数据被传递到任何错误的软件中。

(7) 依据本发明，IRSC 用于识别一首音乐，并且如果没有 ISRC 时，就使用 TOC，这样即使当一首音乐没有 ISRC 时，也能识别该音乐。

15 (8) 依据本发明，作为连接到个人计算机 1 上的外部设备，适配器 26 执行个人计算机 1 中一部分预先确定的软件的功能。这样，仅仅通过分析个人计算机 1 上的软件，不可能知道整个软件是如何工作的。因此，就不能通过伪造或篡改该软件，加上另有意谋的功能。

注意到将由适配器 26 执行的操作可以由 CPU 11 依据安全程序执行。在这种情况下，例如，当需要副本密钥时，由内容管理程序 111 产生具有相同值的多个副本密钥。相似地，由内容管理程序 111 将哈希值隐藏保存起来。

20 并且，当 CPU 11 依据安全程序执行由适配器 26 执行的操作时，个人计算机 1 从连接到网络 2 的预先确定的服务器(如 EMD 注册服务器 3 等)中下载当前时间数据，代替从适配器 26 的 RTC35 提供的当前时间，并且根据当前时间数据进行判断。而且，为此目的，可以设计个人计算机 1 以预先确定的时间间隔保存当前的时间，并且当时间被设置在保存的当前时间之前时，就显示错误，因此接受任何有意图的时间设置。

上述的一系列操作可以由硬件也可由软件完成。在后一种情况下，组成软件的程序将从程序存储介质安装到包含在专用硬件或通用个人计算机的计算机中，例如，在该计算机中依据其中安装的各种程序，就可以执行各种功能。

30 如图 2 所示，用于保存安装在计算机中的程序并使计算机可执行该程序的程序存储介质，包括磁盘 41(包括软盘)、光盘 42(CD-ROM(=紧凑只读存储

器盘))、DVD(数字多功能盘)、磁光盘 43(MD(=小型盘))、从半导体存储器 44 形成的包介质、程序临时保存或永久保存的 ROM 12、或硬盘 21。程序通过 接口如必要的通信块 25，并使用网络 2 保存到程序存储介质中，网络 2 比如 是局域网(LAN)或因特网，电缆或象数字卫星广播等无线通信介质。

5 注意，描述将程序保存到存储介质的操作，在这里包括根据描述的序列 按时间顺序进行的操作，以及不受时间顺序影响而并行或单独进行的操作。

也应该注意，在此“系统”是指多个设备的集合。

如上所述，依据本发明的信息处理设备、方法和程序存储介质，适于根 据硬件中程序执行装置的操作结果，通过由软件组成的控制方法，控制将内 10 容数据累积到存储装置或从存储装置读出，因此完全能阻止通过分析和伪造 软件的方式来进行数据的欺诈性复制。

说 明 书 附 图

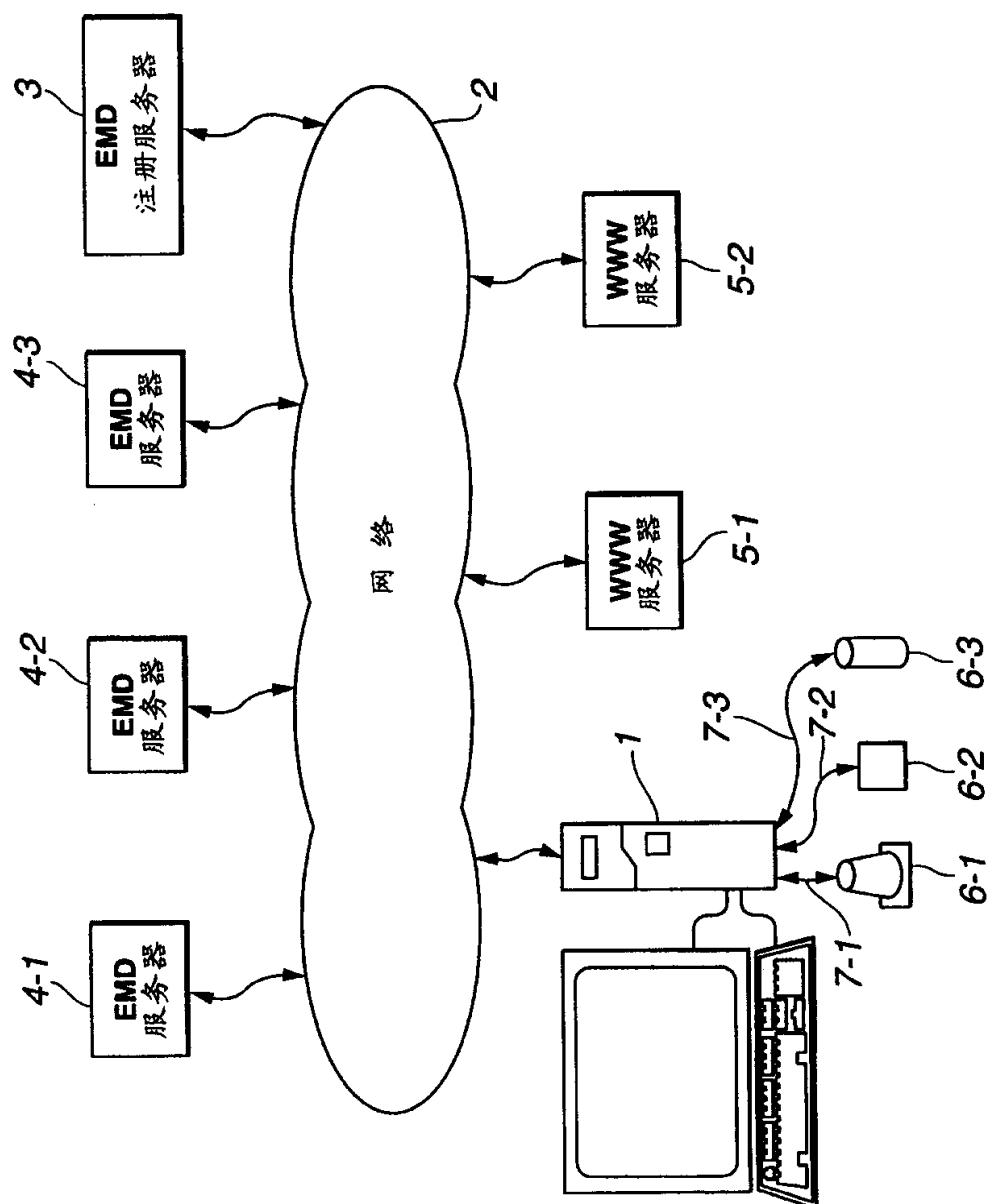


图 1

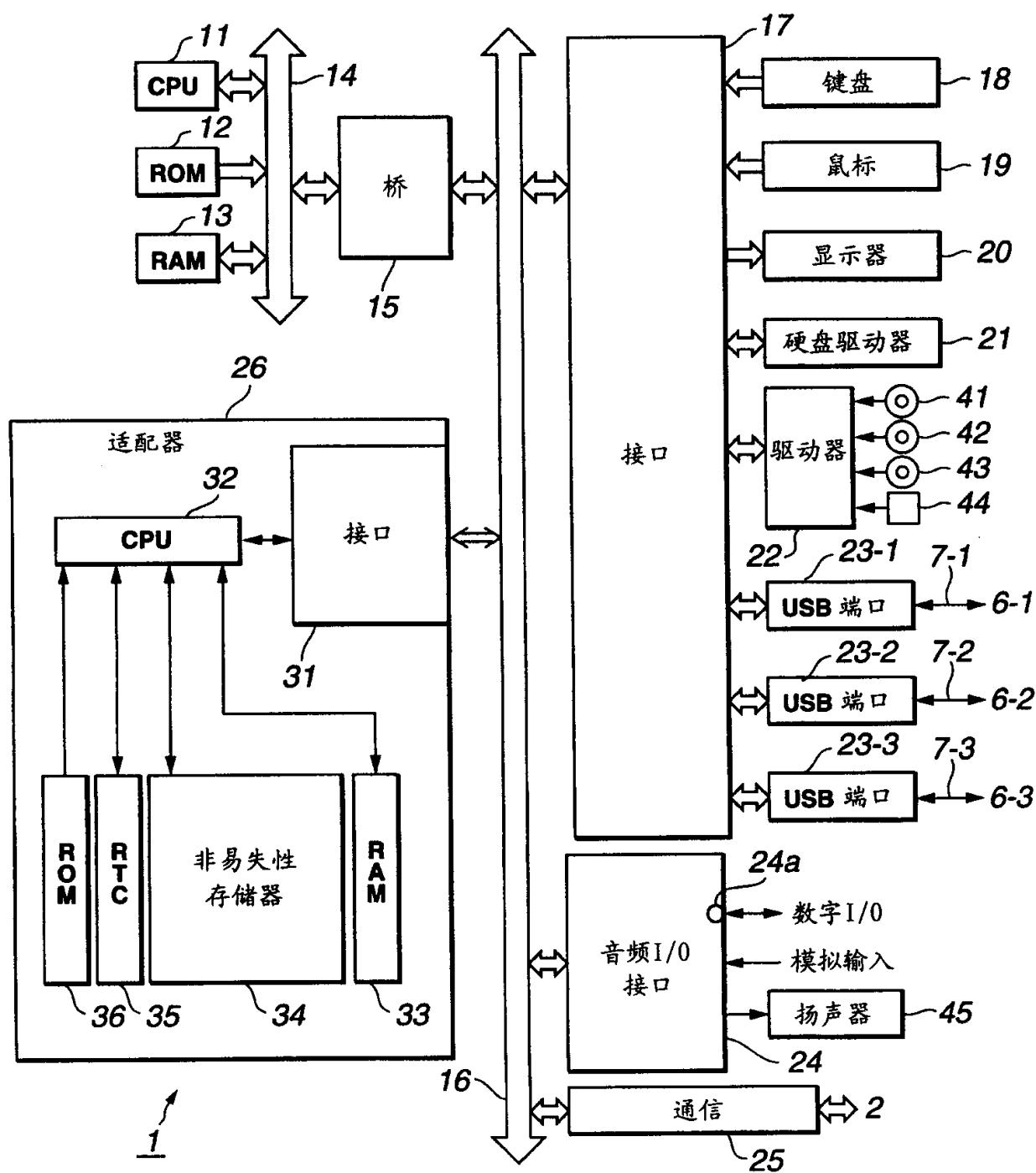


图 2

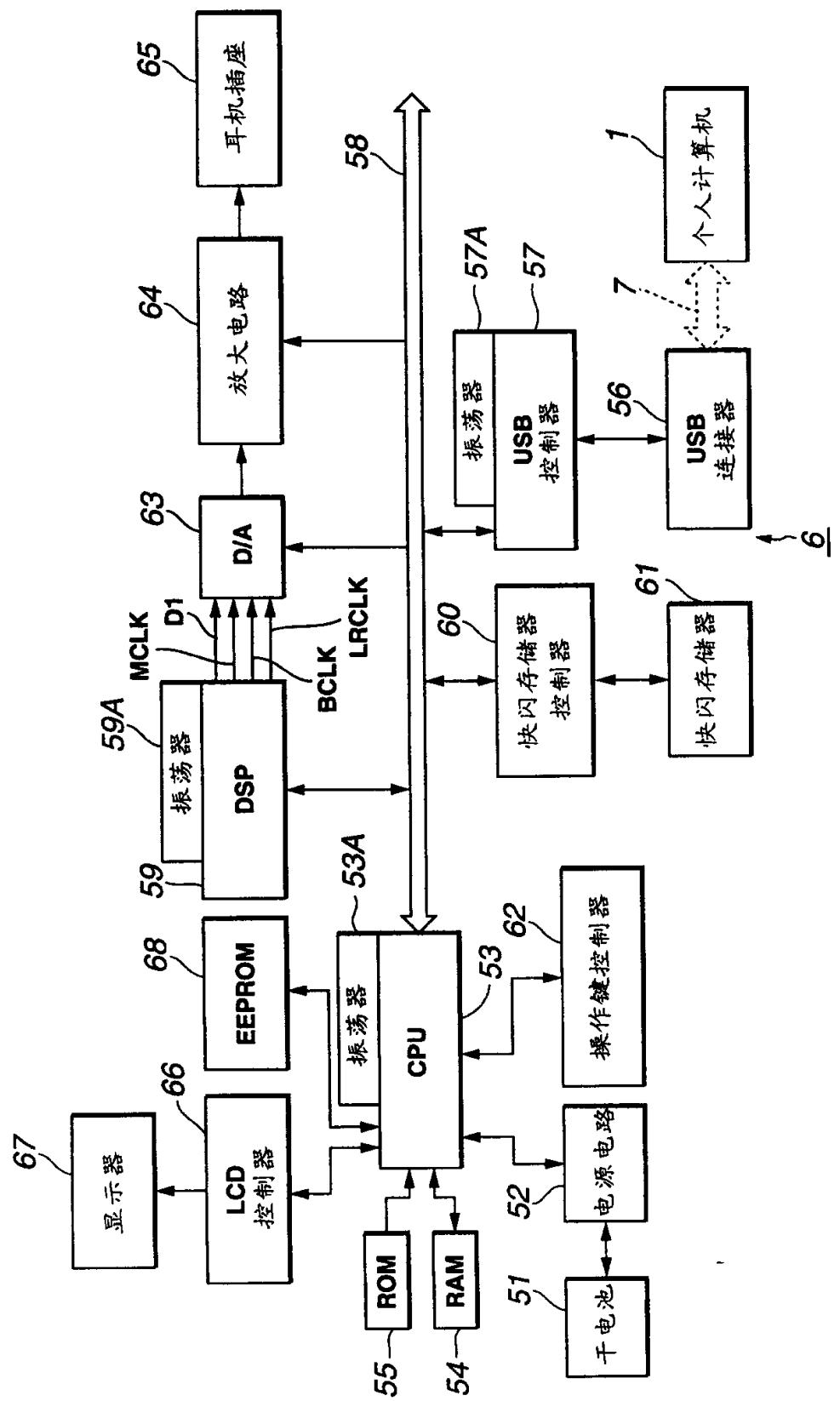


图 3

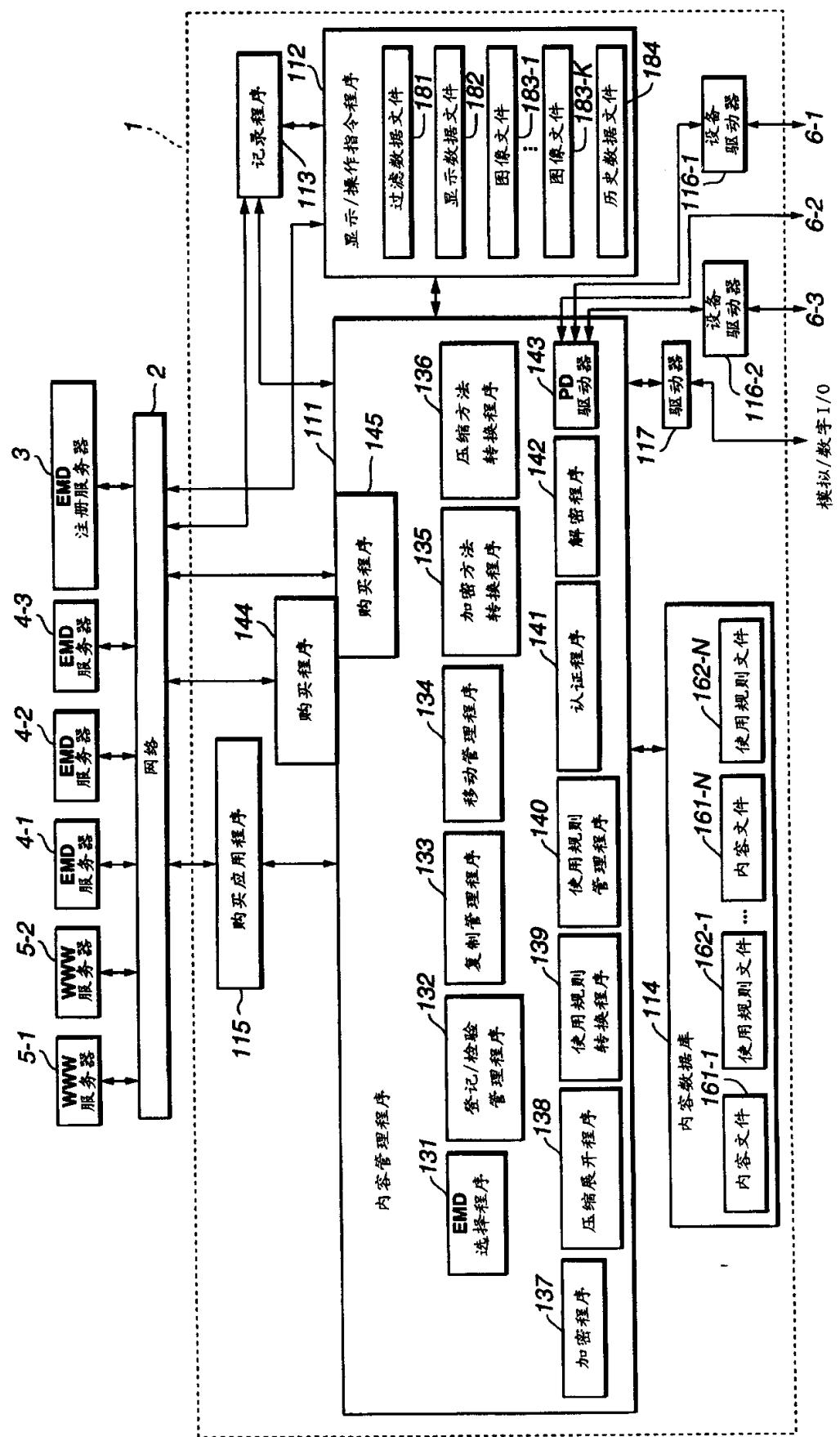
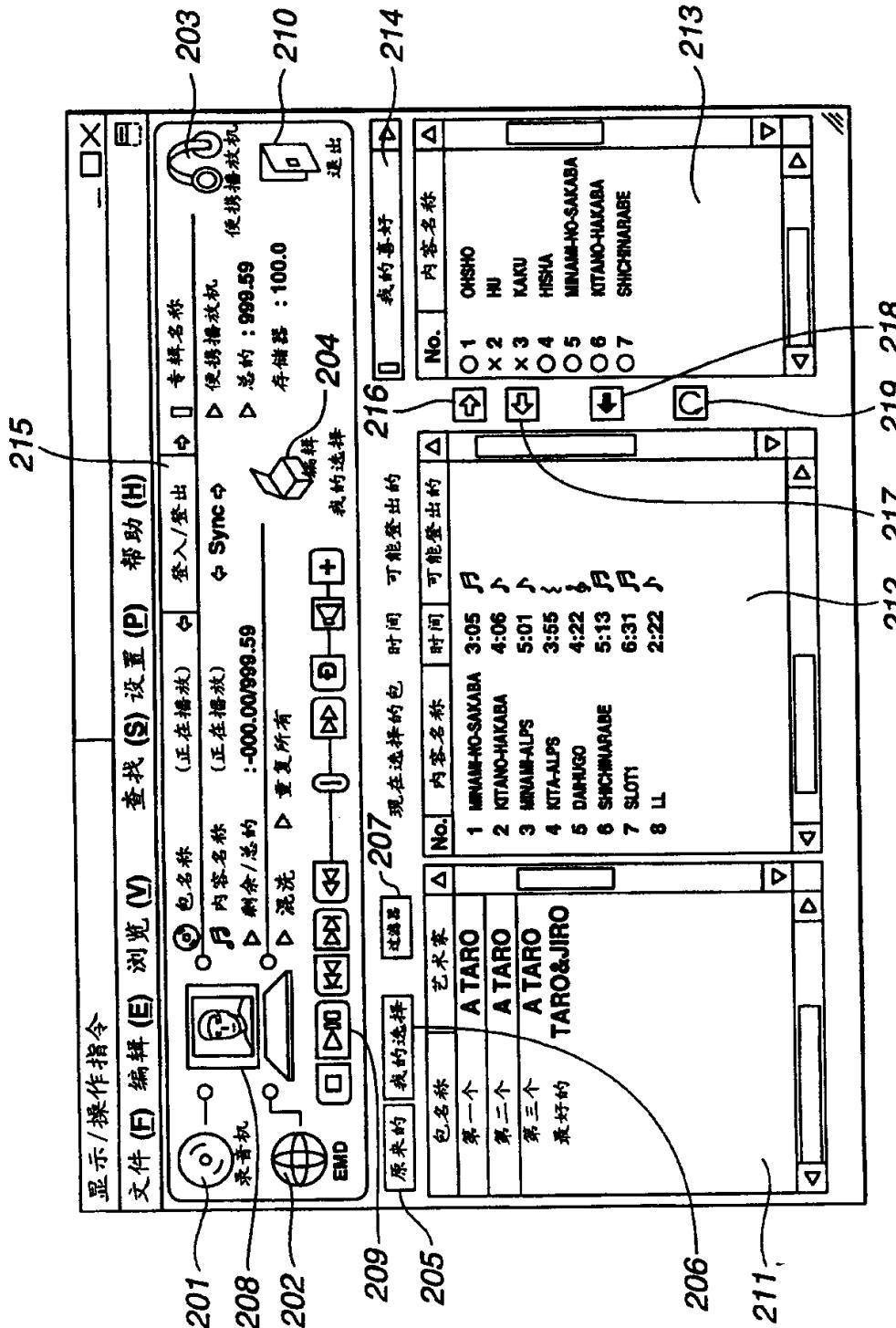


图 4

图 5



00.10.05

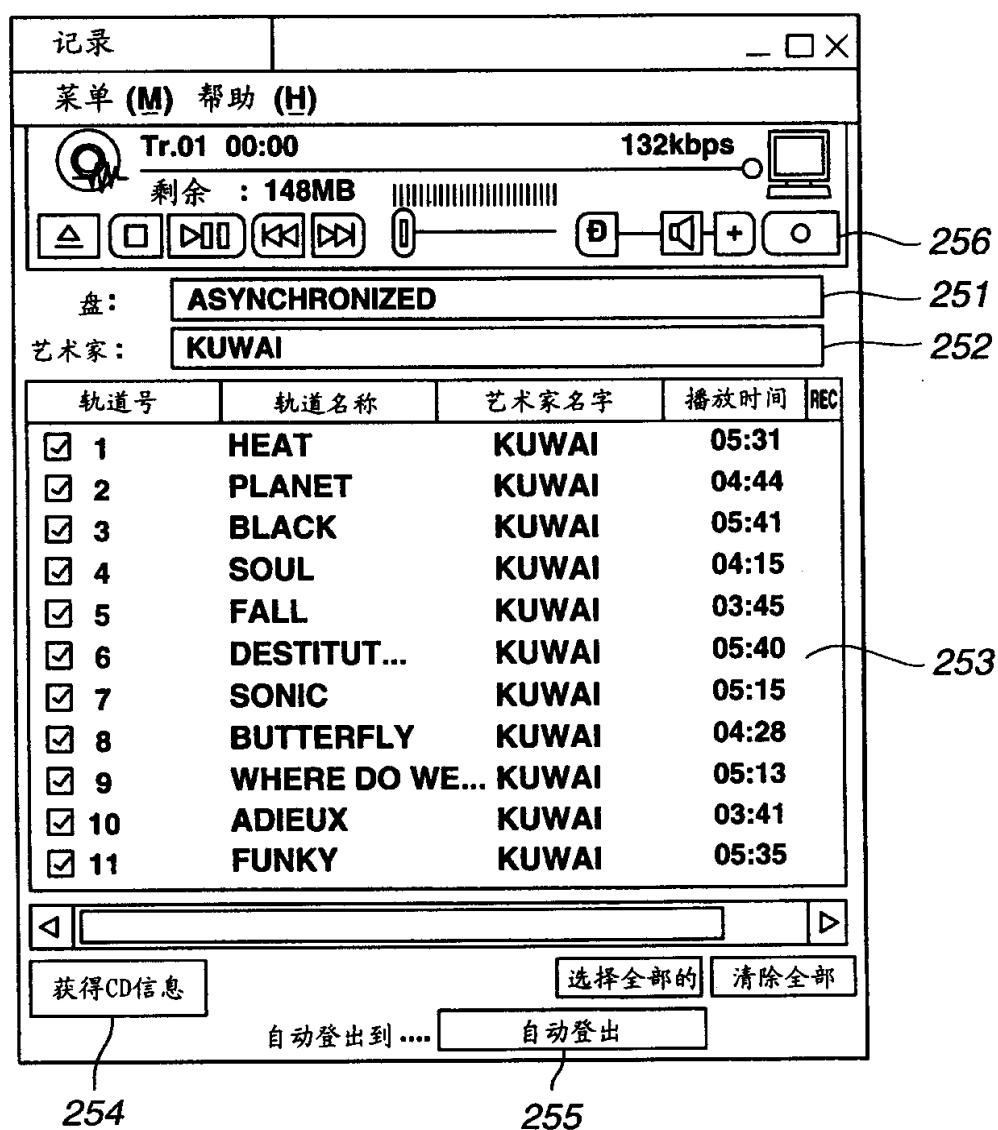


图 6

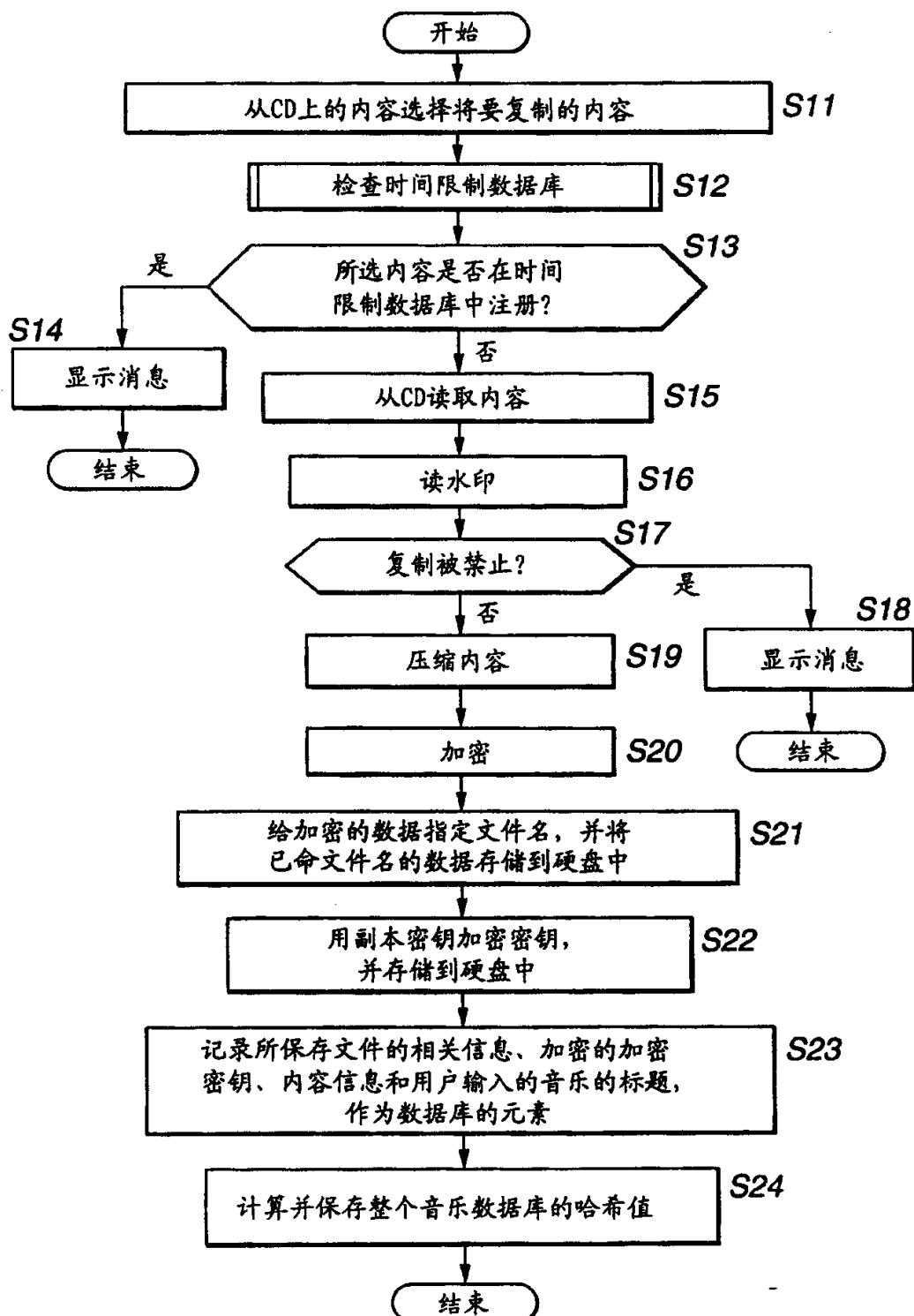


图 7

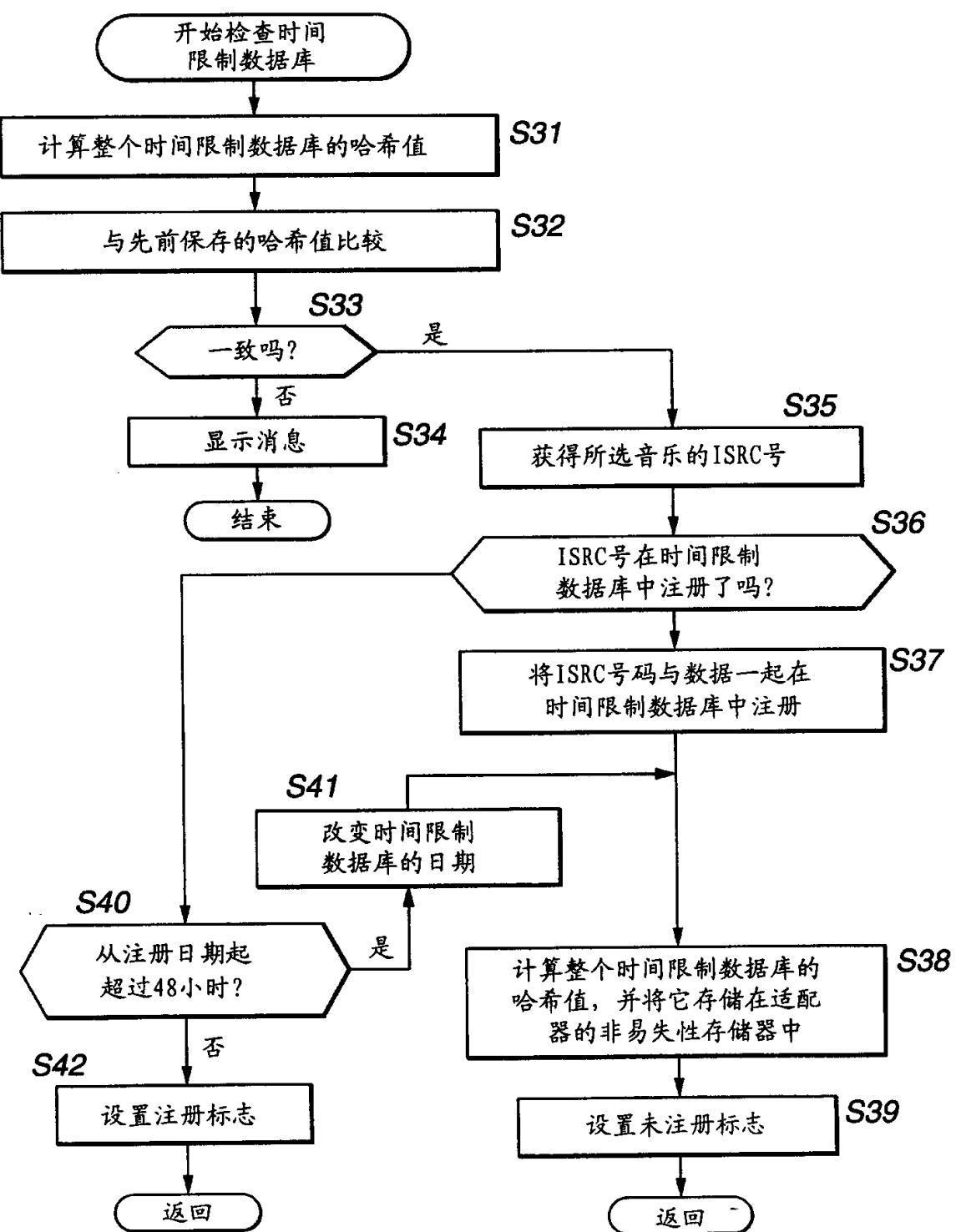


图 8

00-12-05

时间限制数据库

	项目 1	项目 2	项目 3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
复制日期	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

哈希值	0xf3352e125934
-----	----------------

图 9

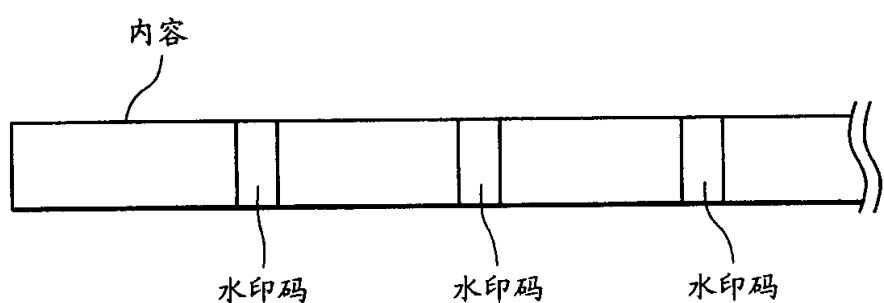


图 10

音乐数据库

	项目 1	项目 2	项目 3
文件名	xd000110.at2	px92341234.at2	aa0234287034.at2
加密的加密密钥	0xabbabababab	0x9898989898989899	0x123456789012
音乐名	HARU-NO-OGAWA	UNMEI(DESTINY)	KOUJOU-NO-TSUKI
播放时间长度	180	190	200
回放条件：开始日期	-	2001.01.01.00:00	-
回放条件：结束日期	1999.07.31.23:59	-	-
回放条件：回放限制	-	20	-
回放计数器	-	12	-
回放计帐条件	-	-	*5
复制条件：复制份数	2	0	0
复制计数器	1	0	0
复制条件：SCMS	0b01	0b10	0b00

哈希值	0xf9951e566321
-----	----------------

图 11

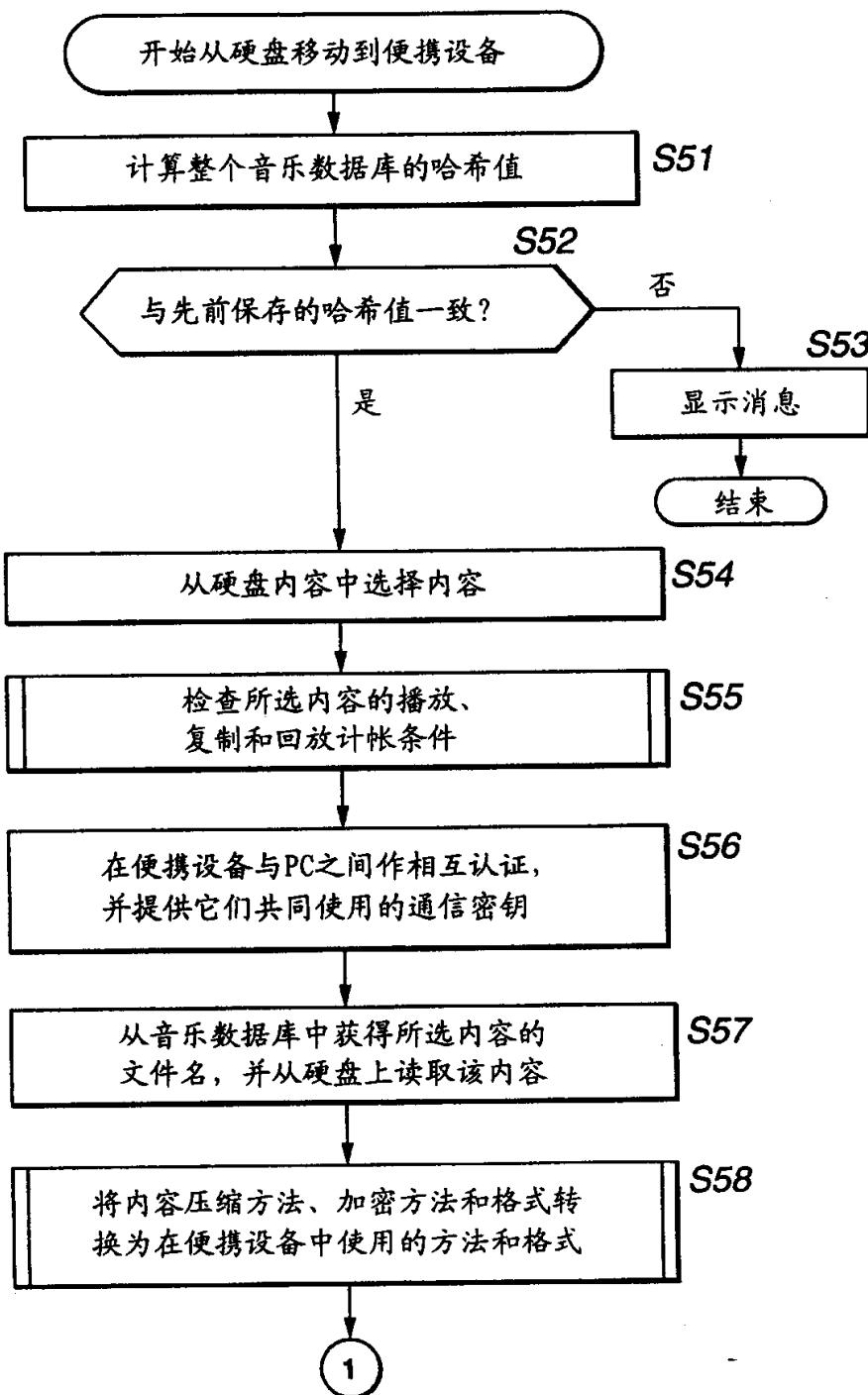


图 12

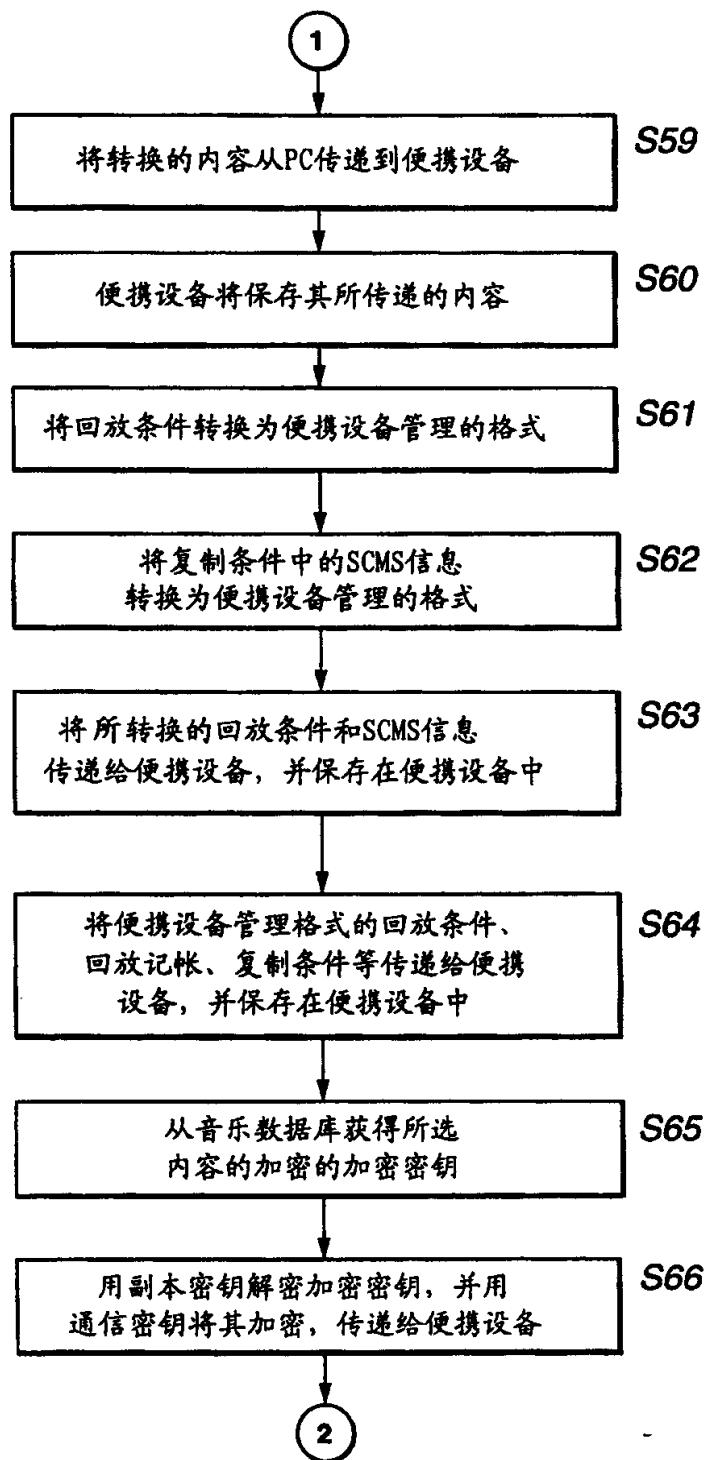


图 13

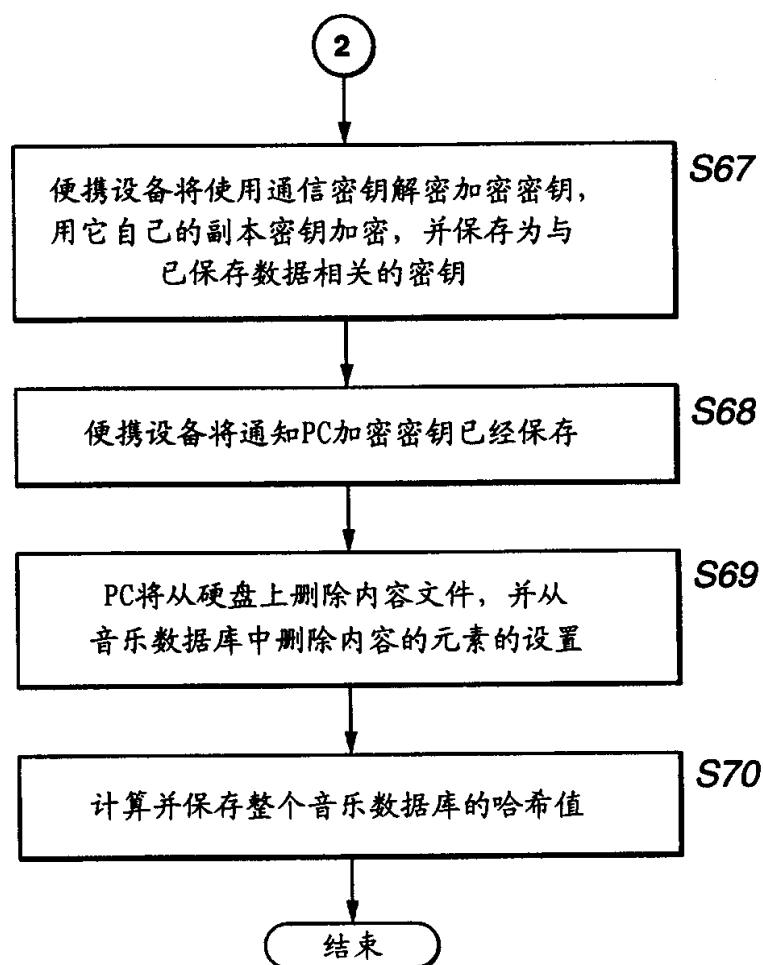


图 14

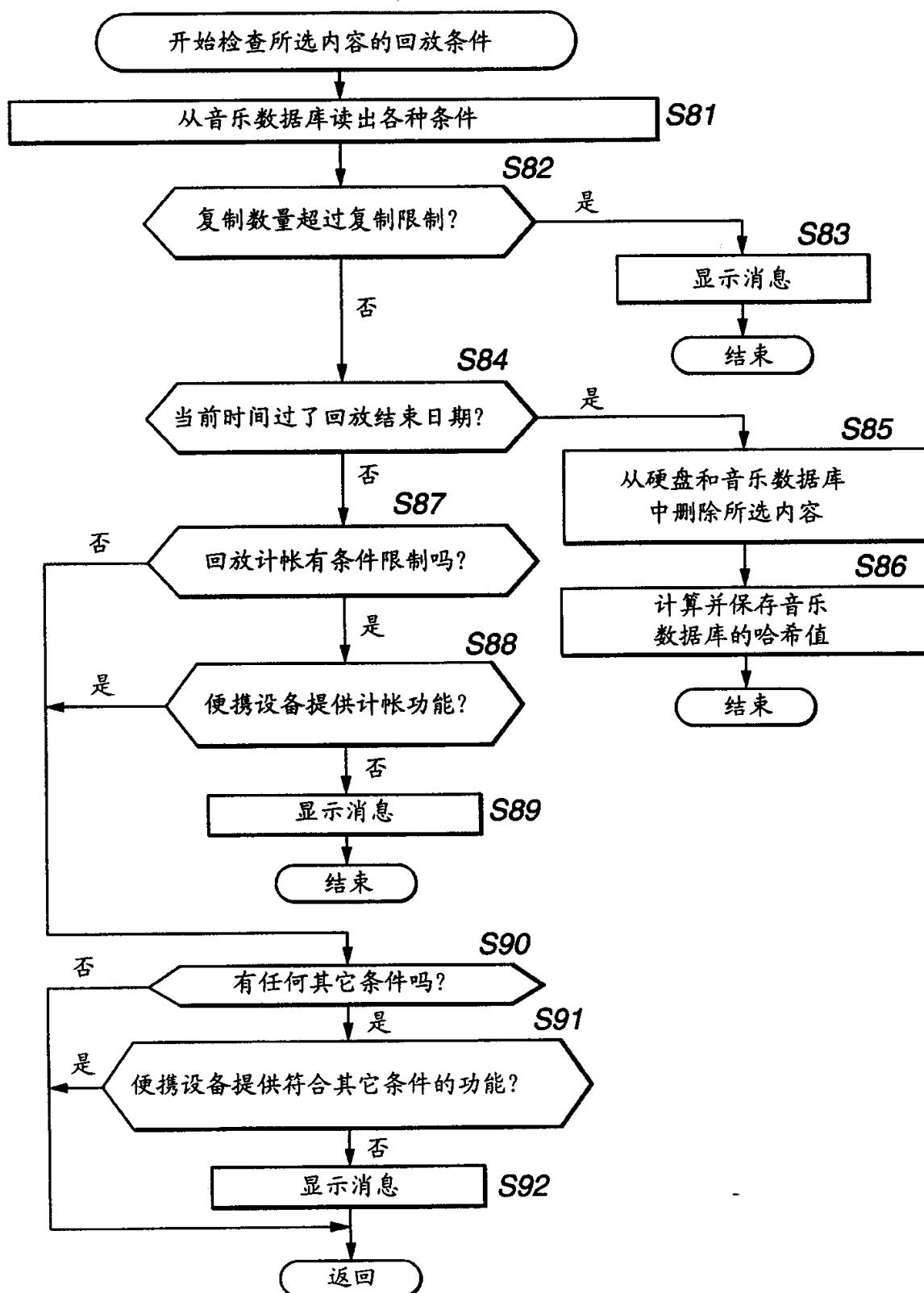


图 15

便携设备管理的回放条件

	项目 1	项目 2	项目 3
内容ID	00001	00002	00003
播放开始日期	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
播放结束日期	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
回放限制	-	15	-

图 16

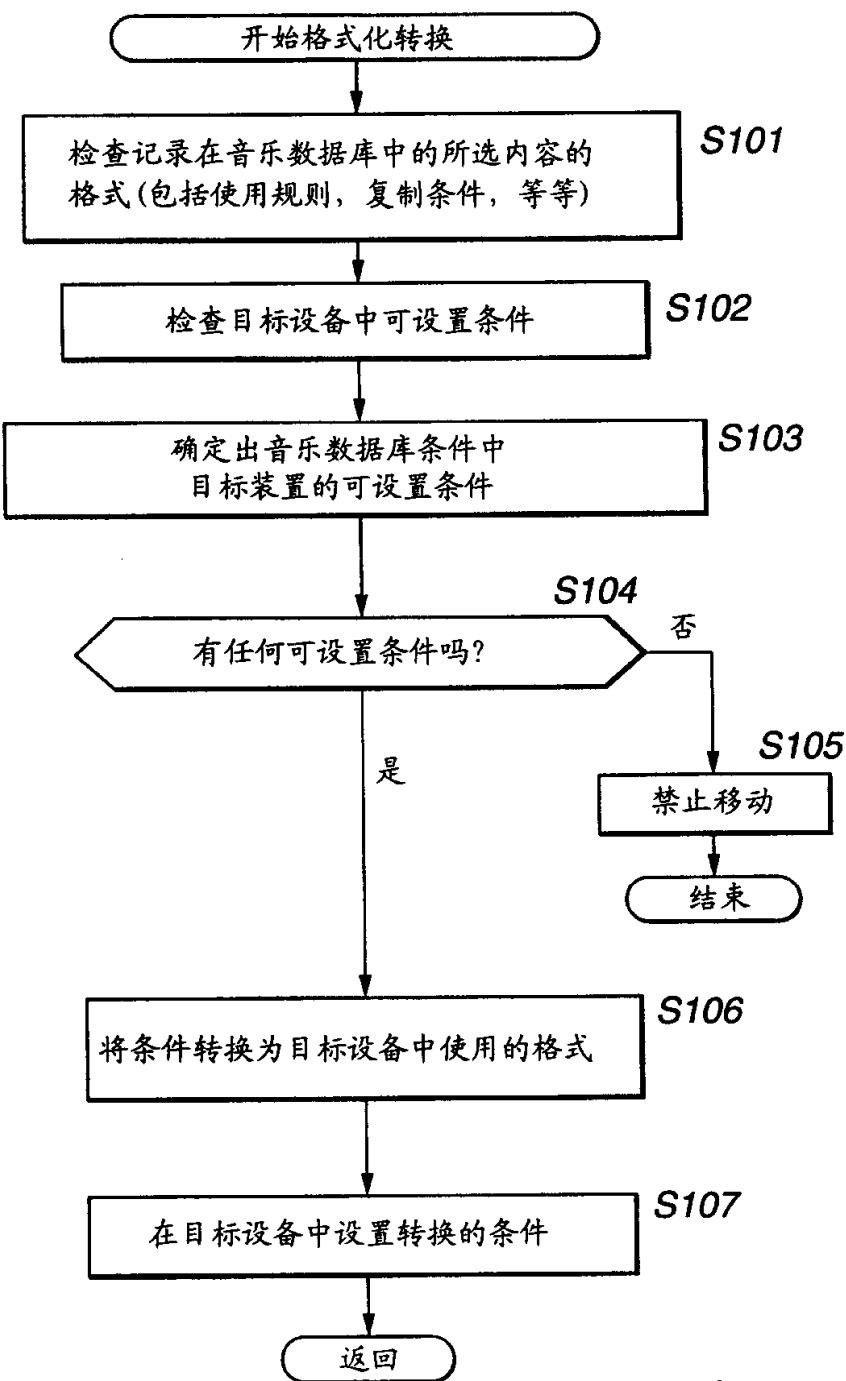


图 17

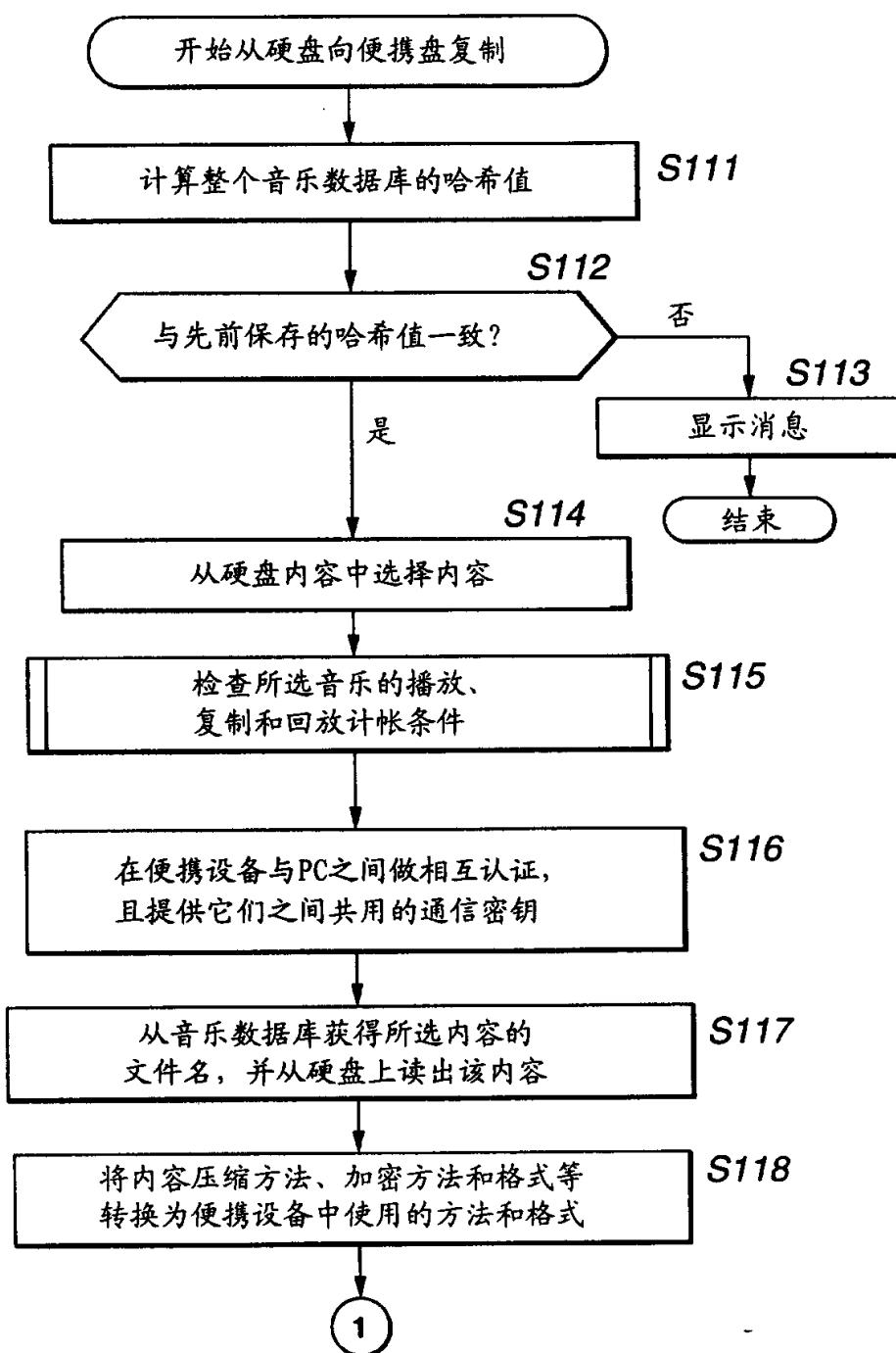


图 18

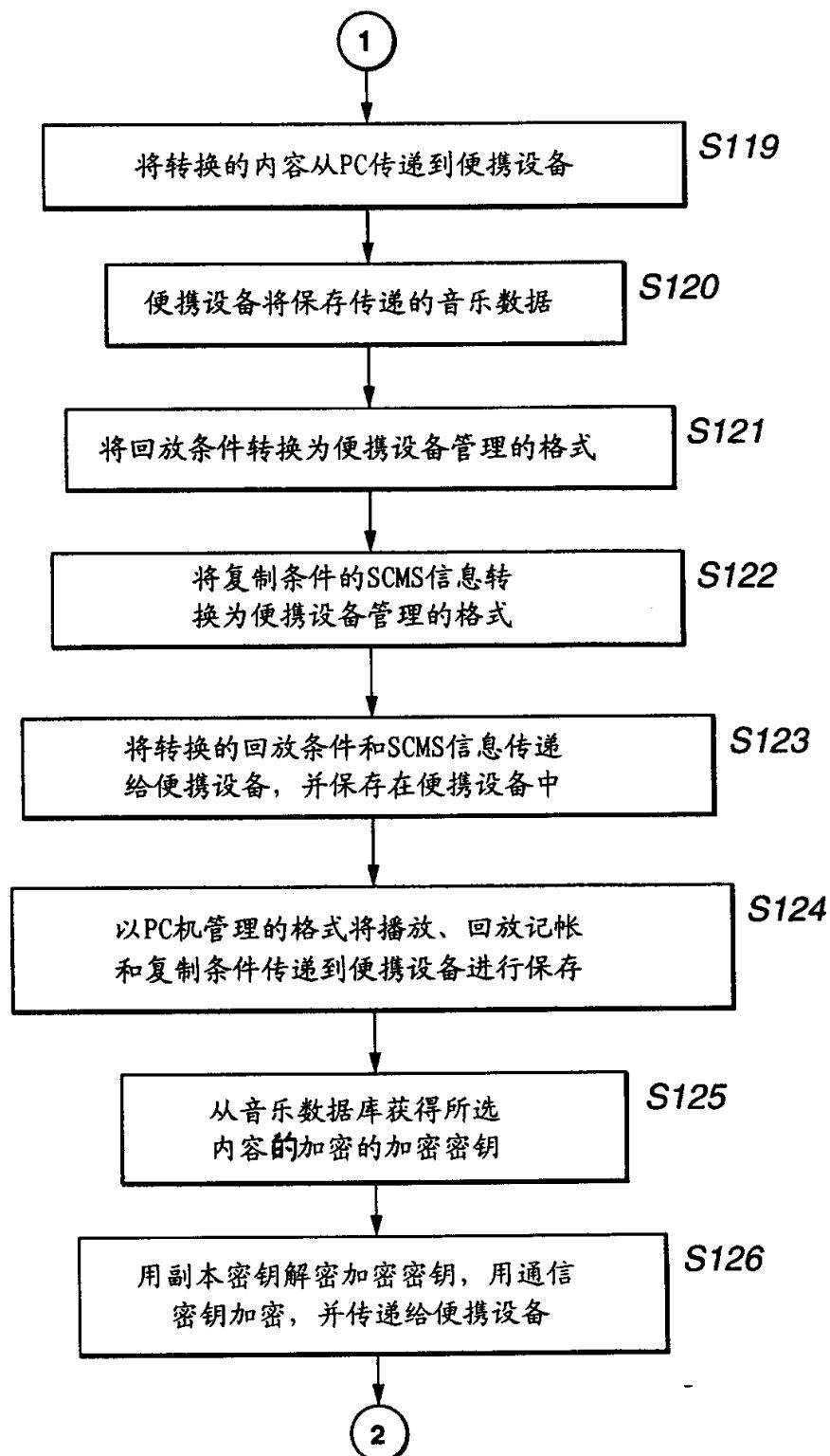


图 19

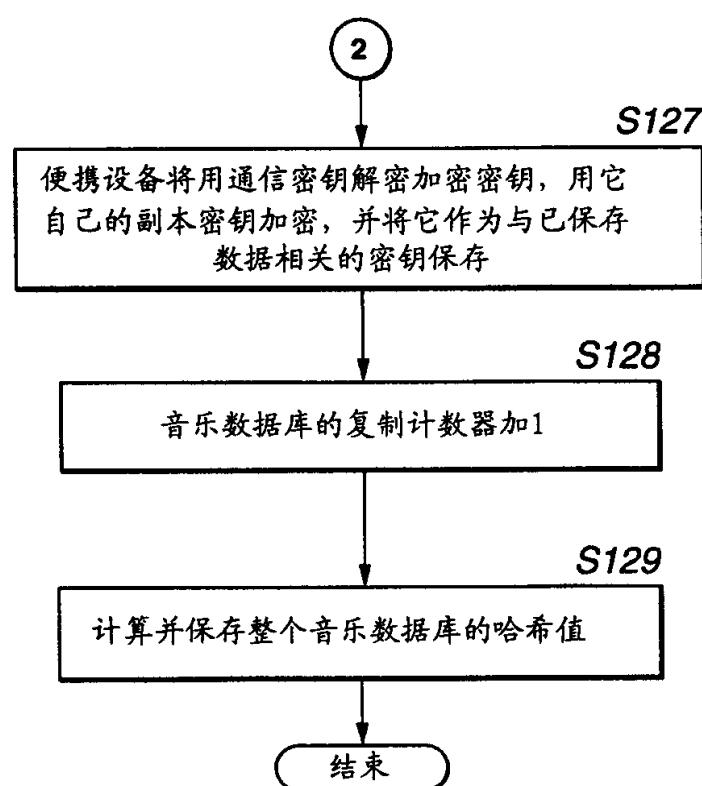


图 20

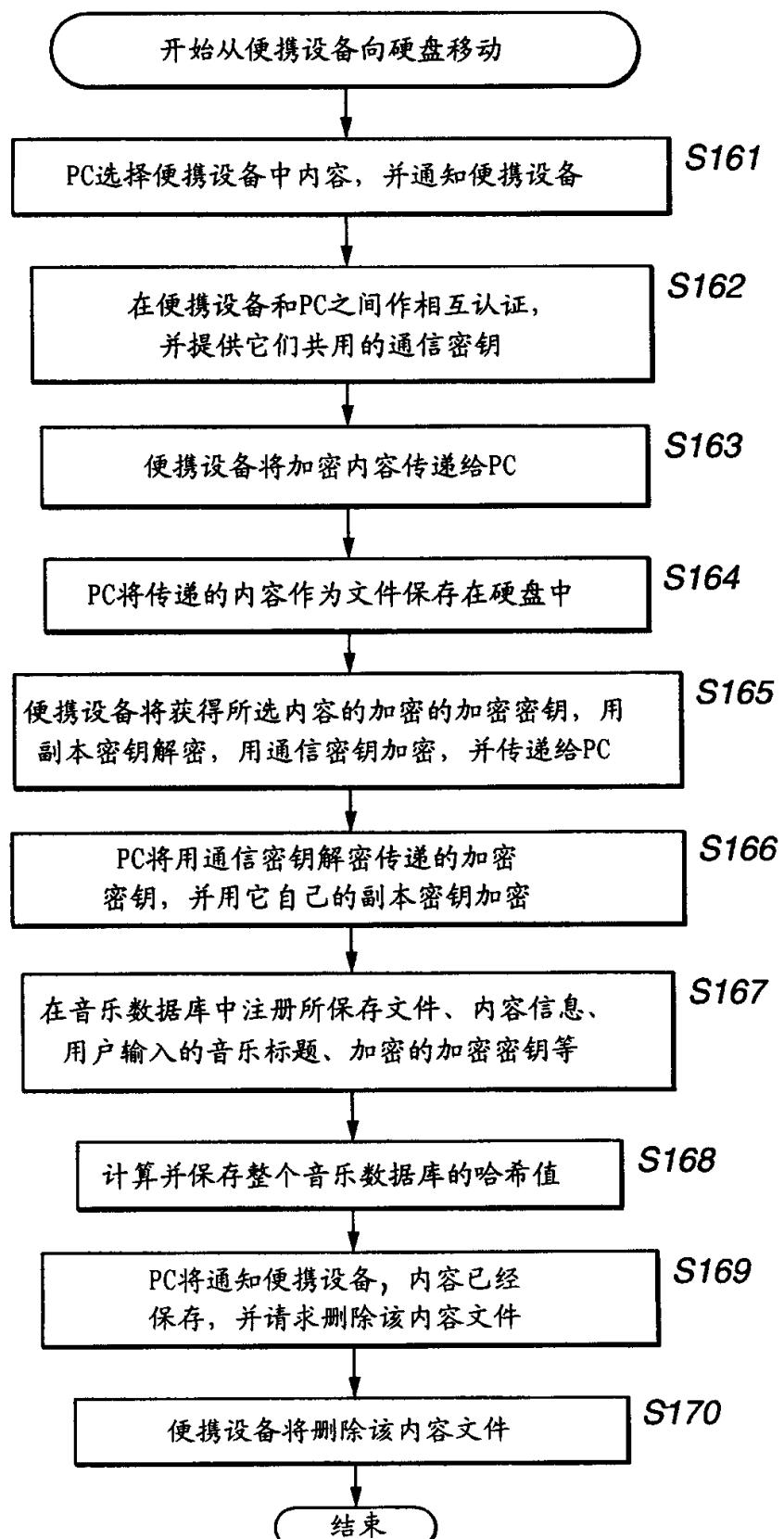


图 21

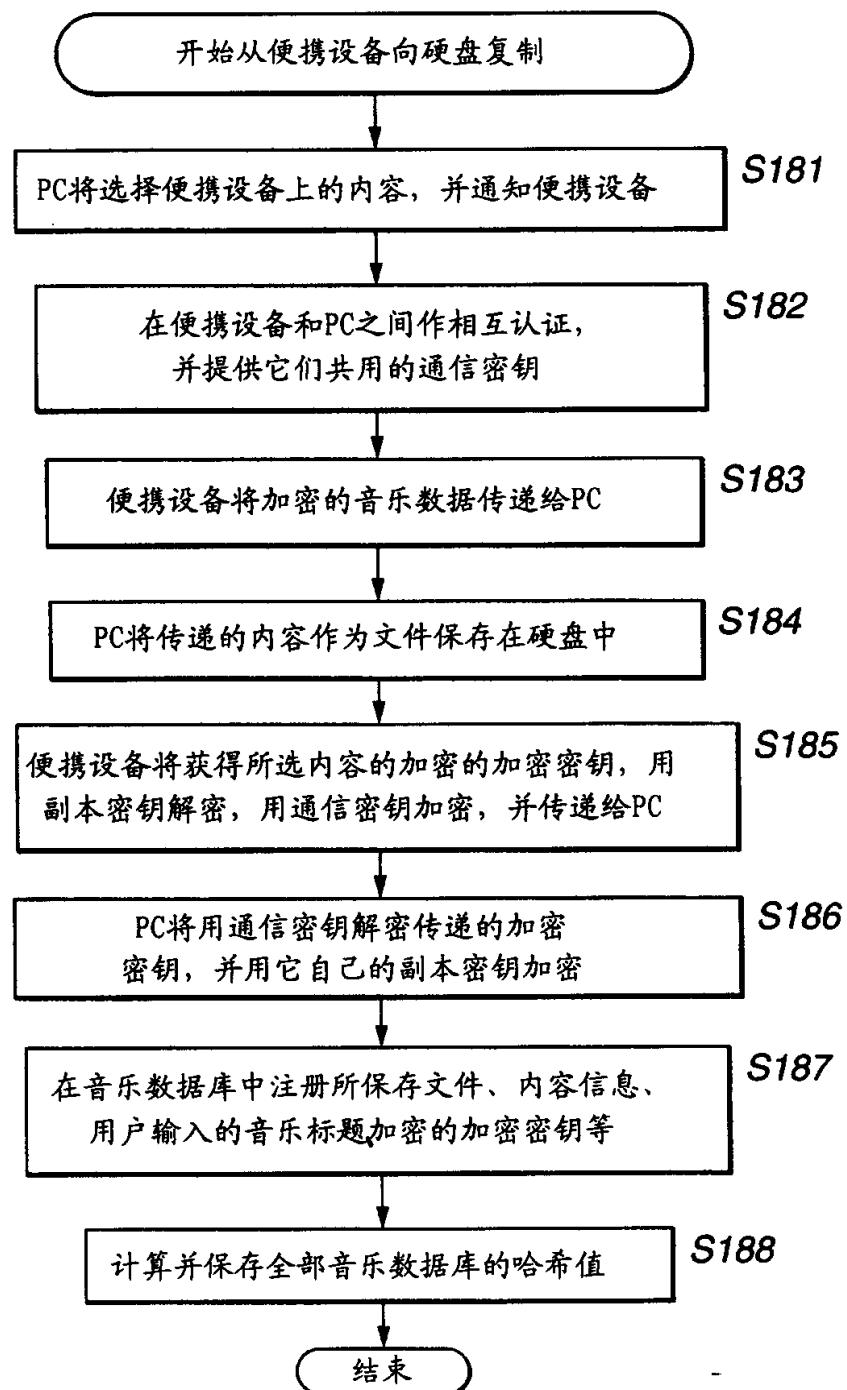


图 22

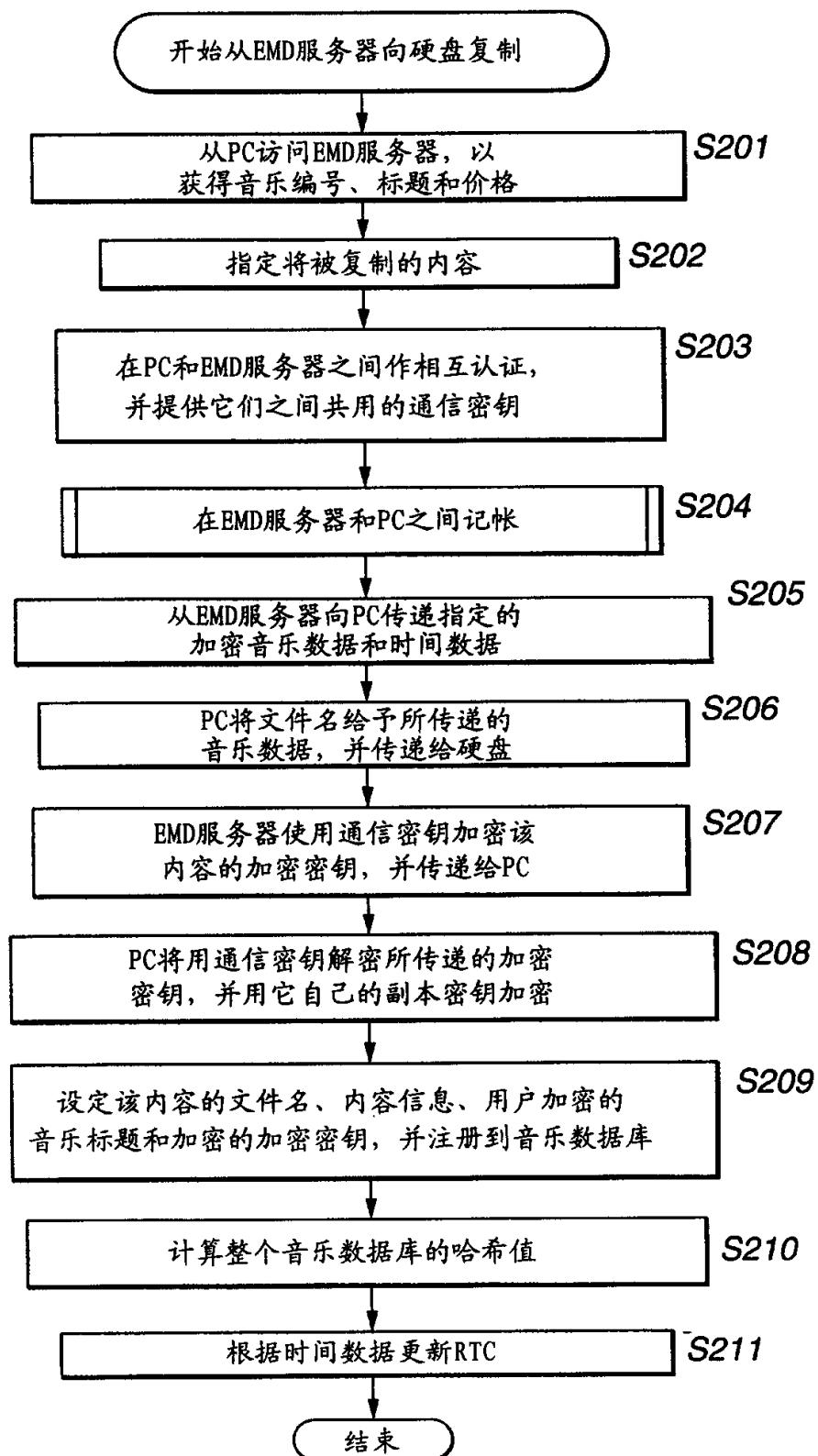


图 23

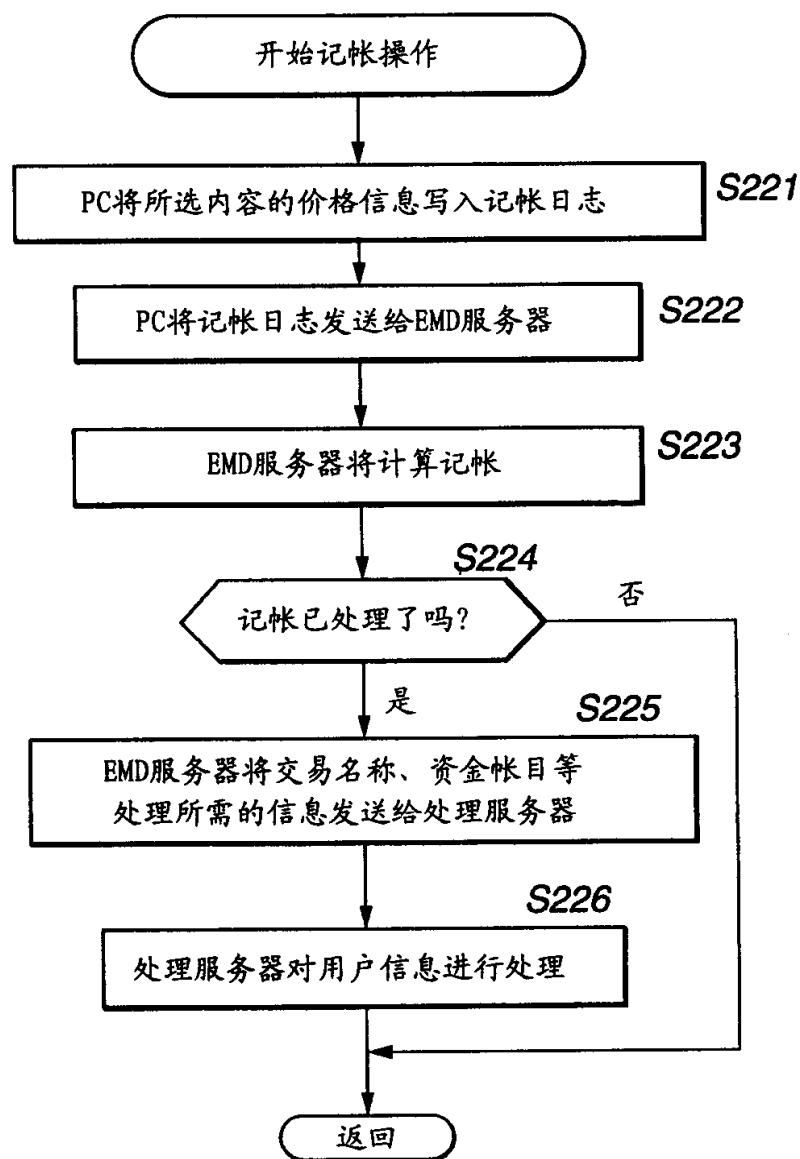


图 24

00.10.00

计帐日志

	项目 1	项目 2	项目 3	
费用	50	50	60	

哈希值	0xf8783e263517
-----	----------------

图 25

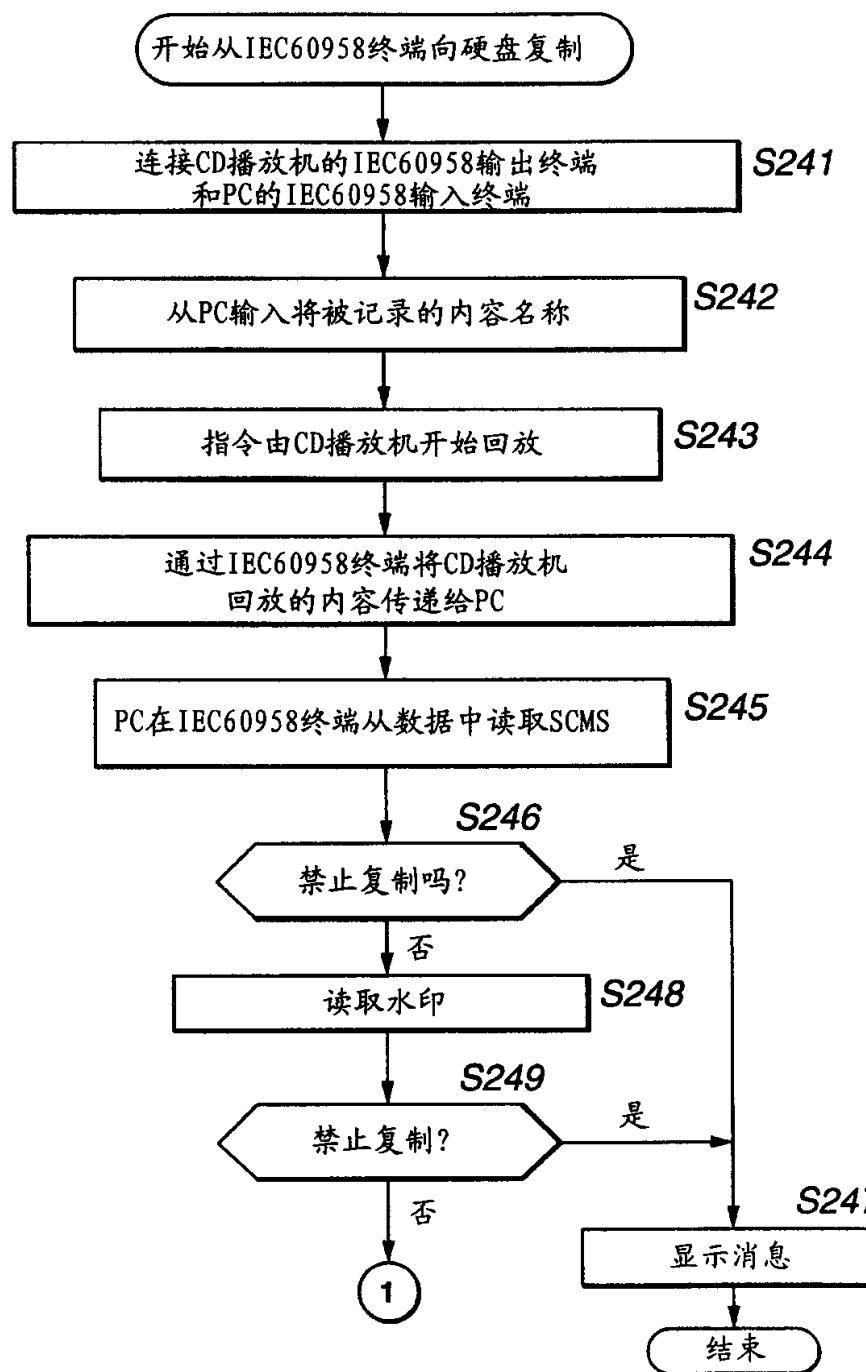


图 26

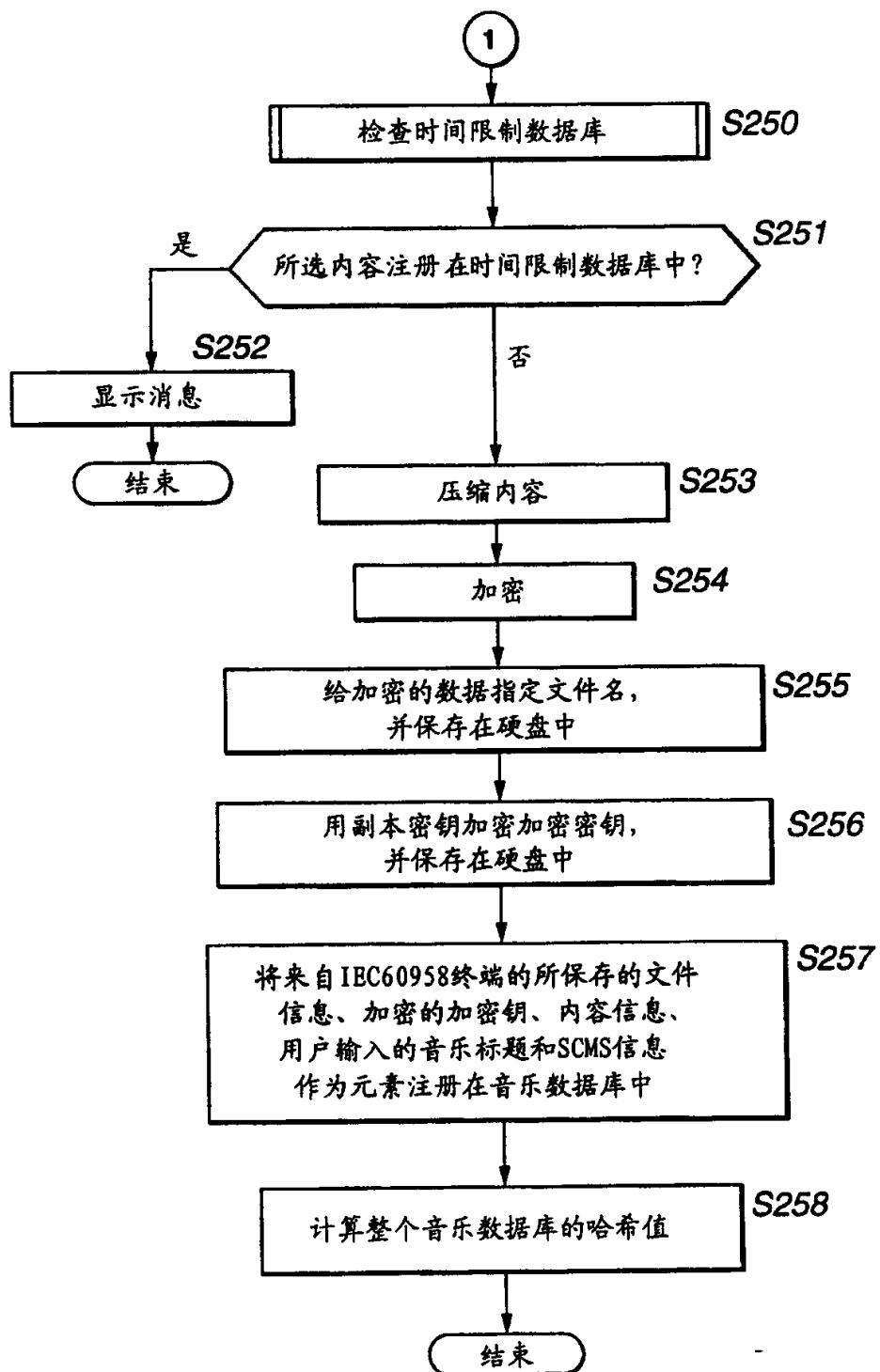


图 27

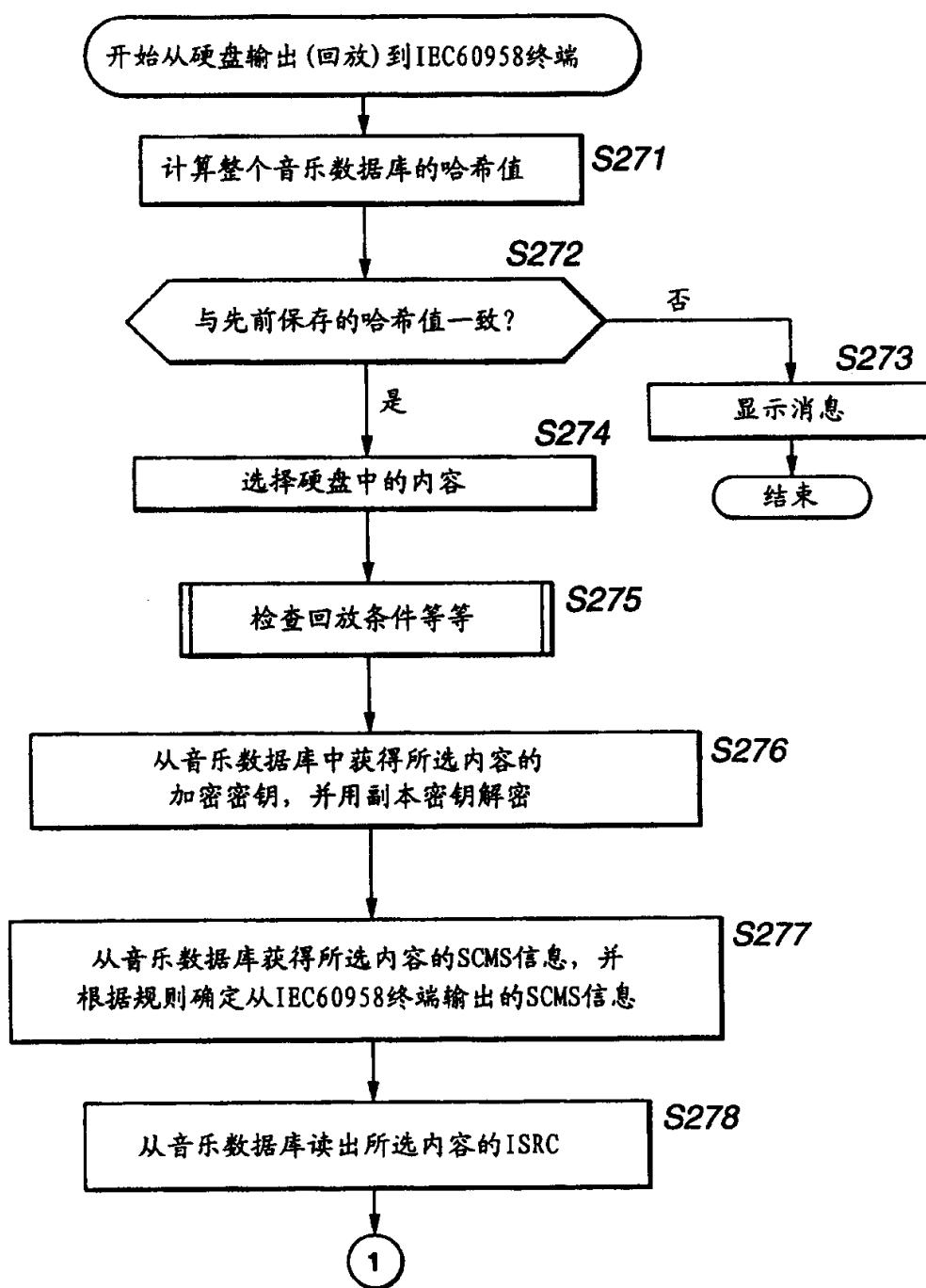


图 28

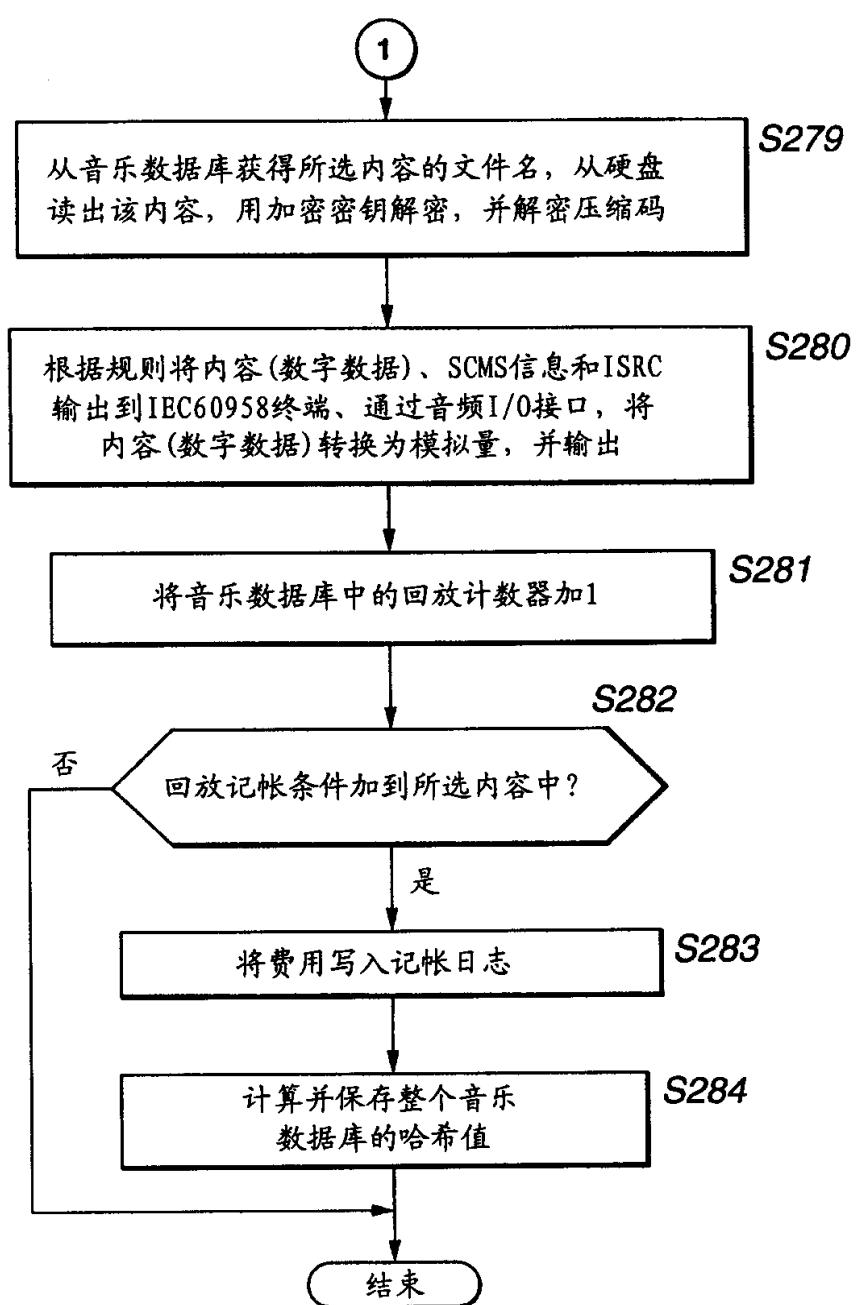


图 29

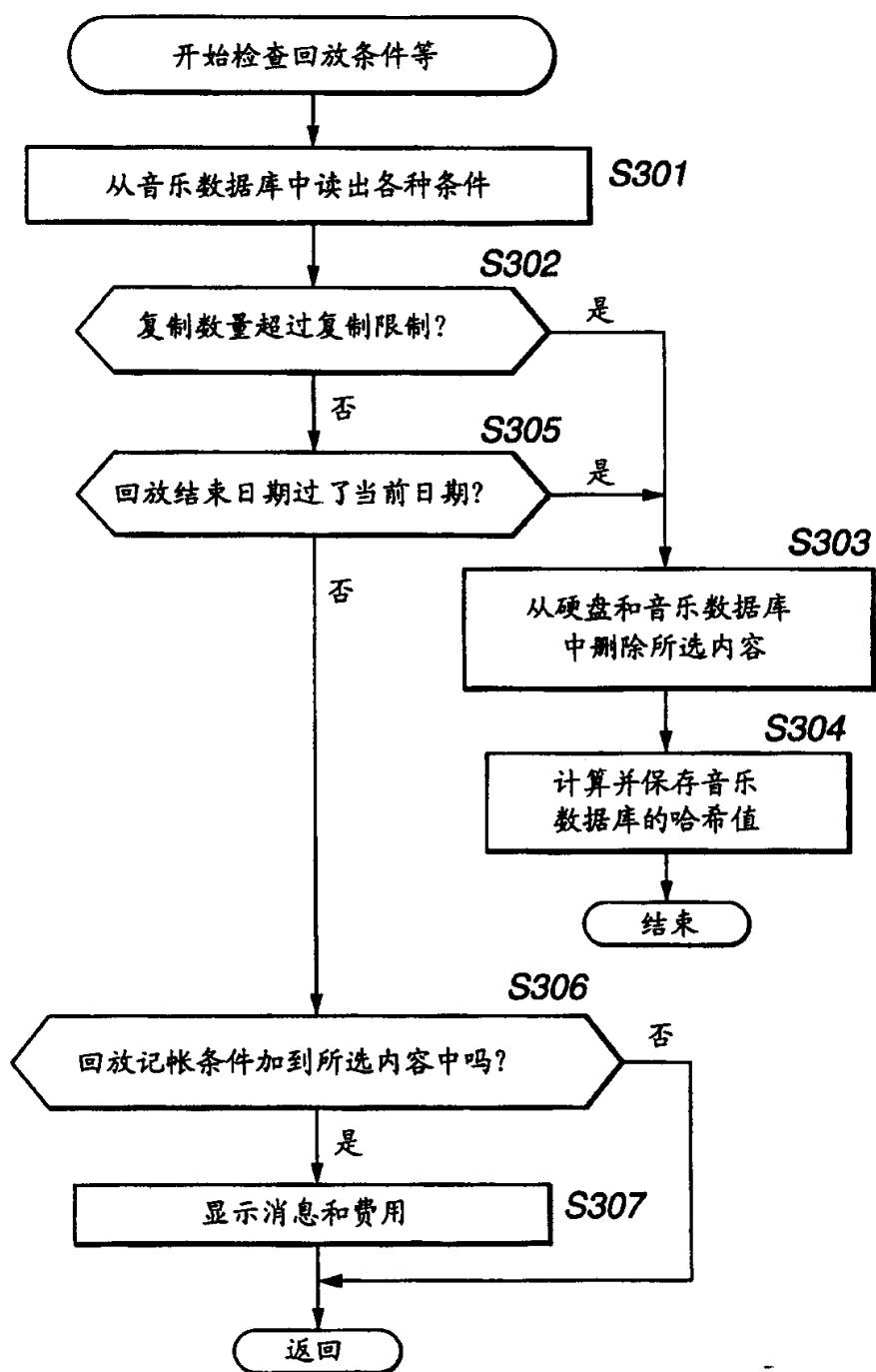


图 30

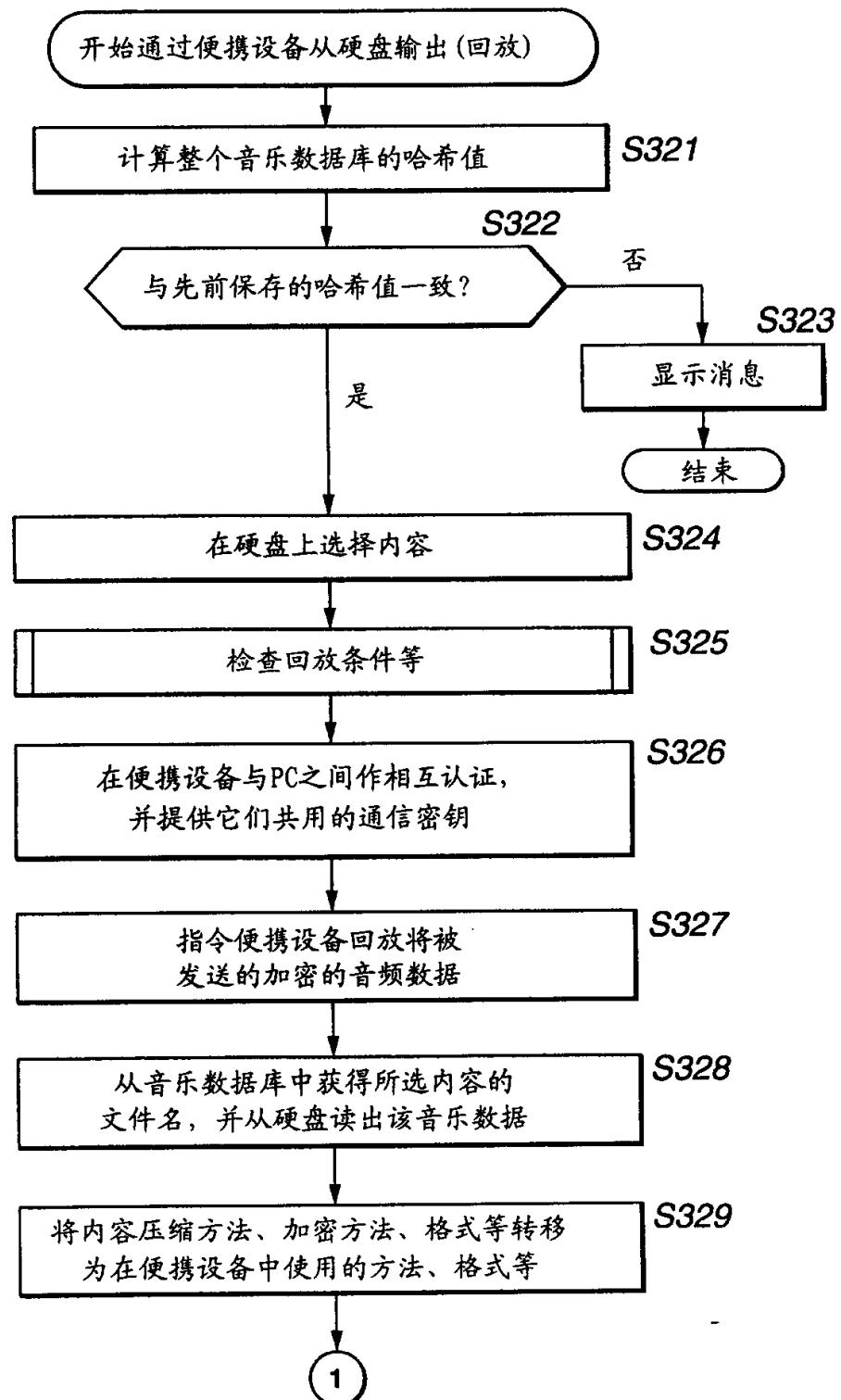


图 31

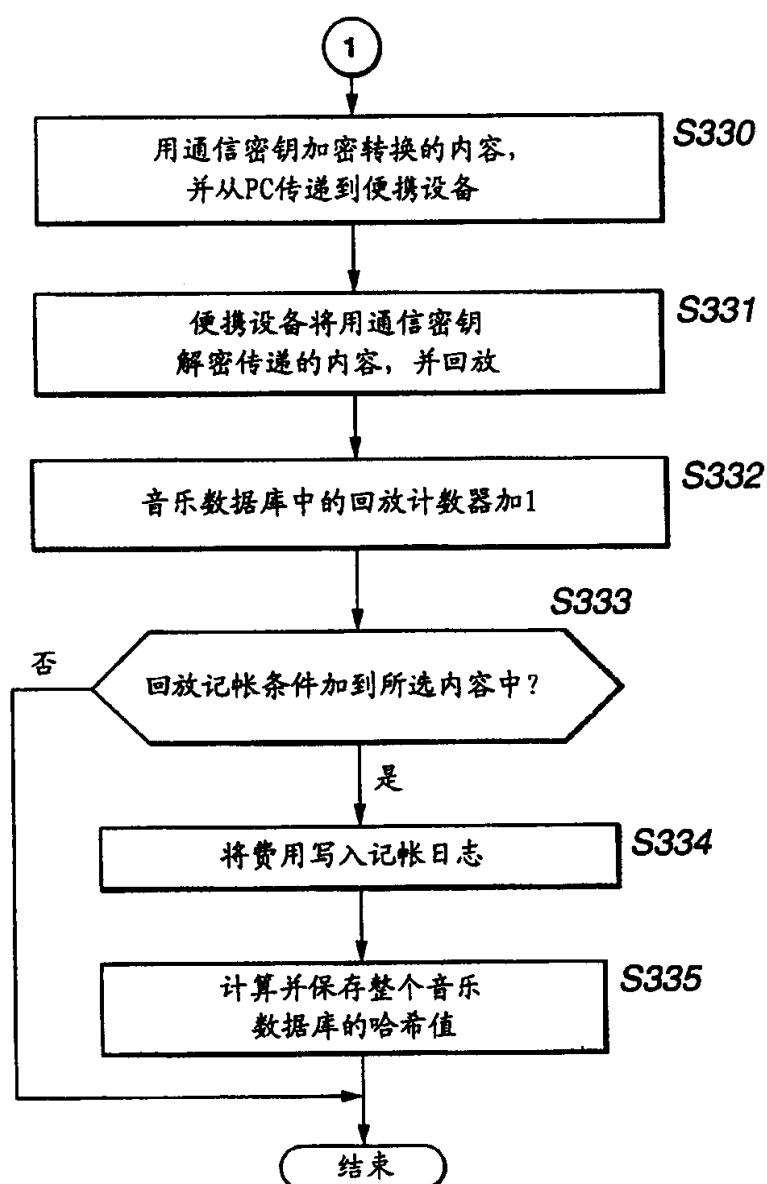


图 32

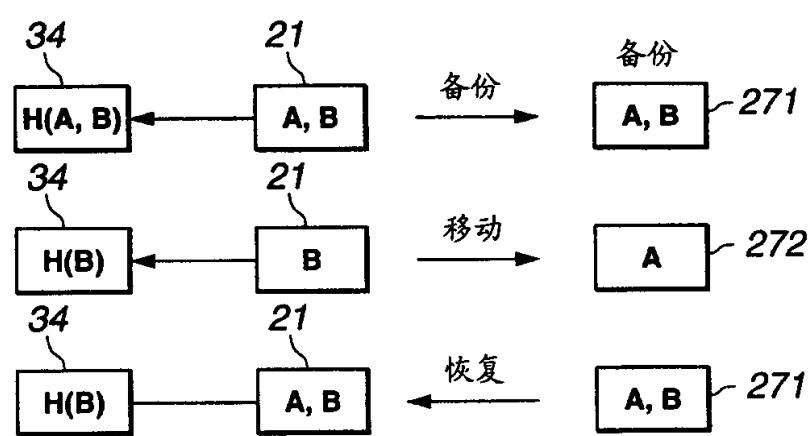


图 33

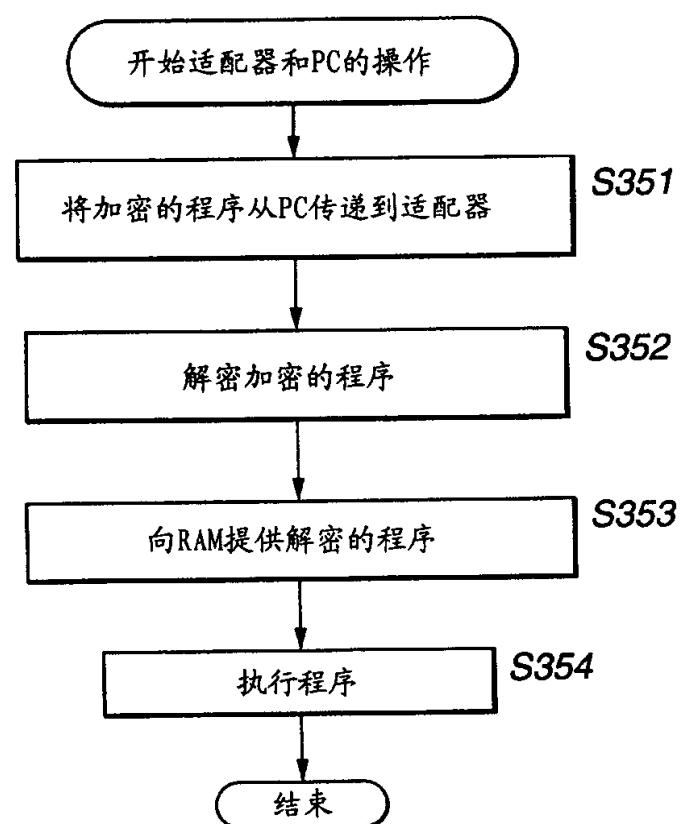


图 34

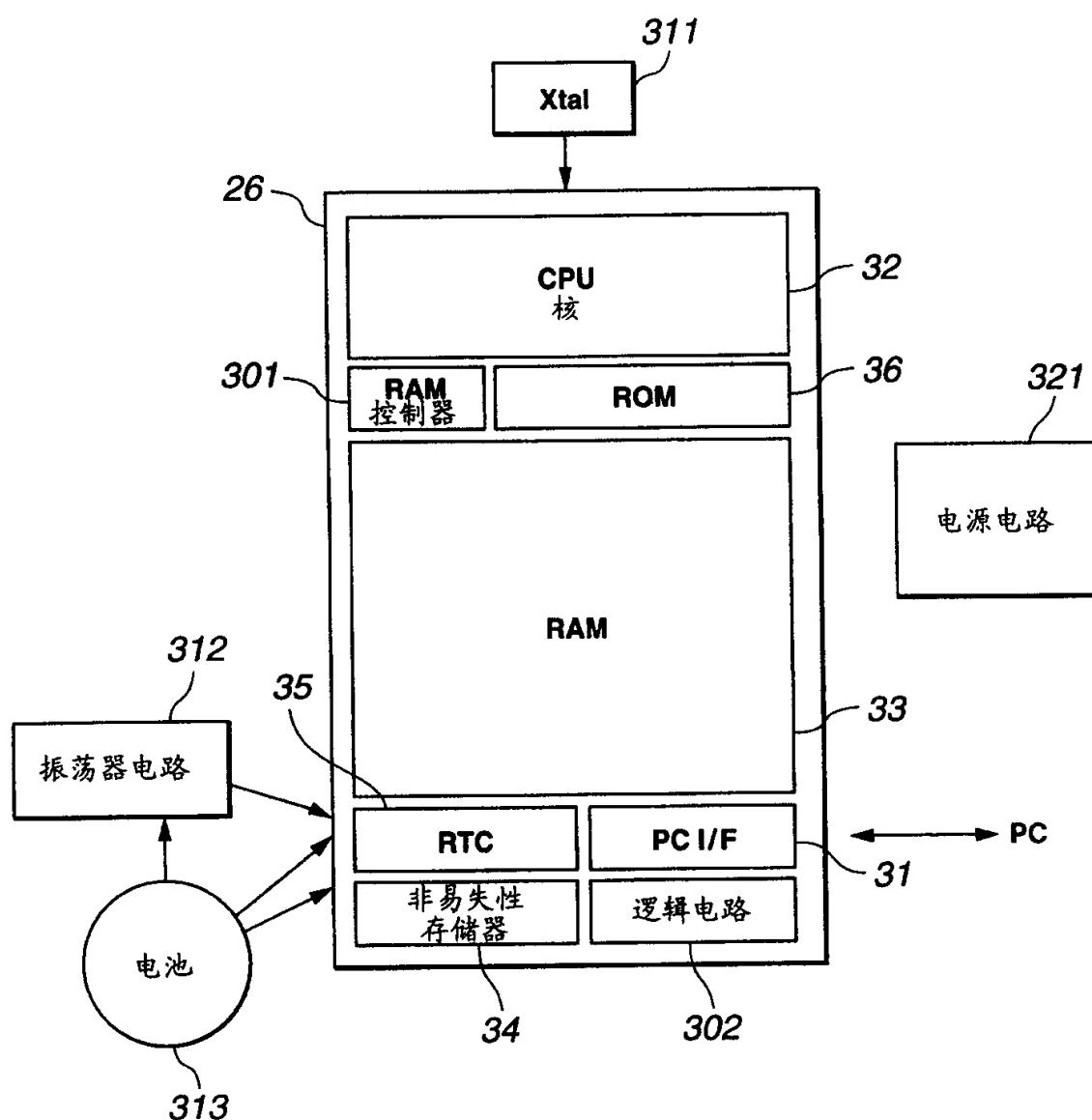


图 35

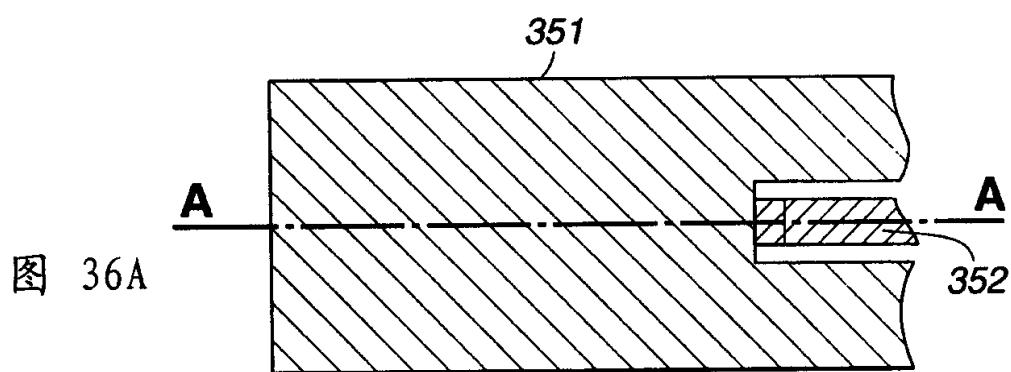


图 36A

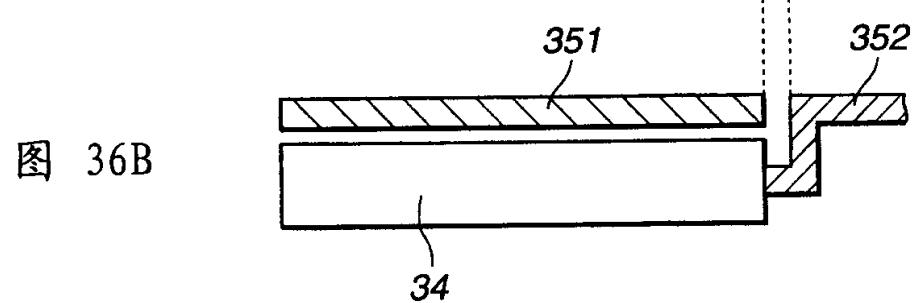


图 36B

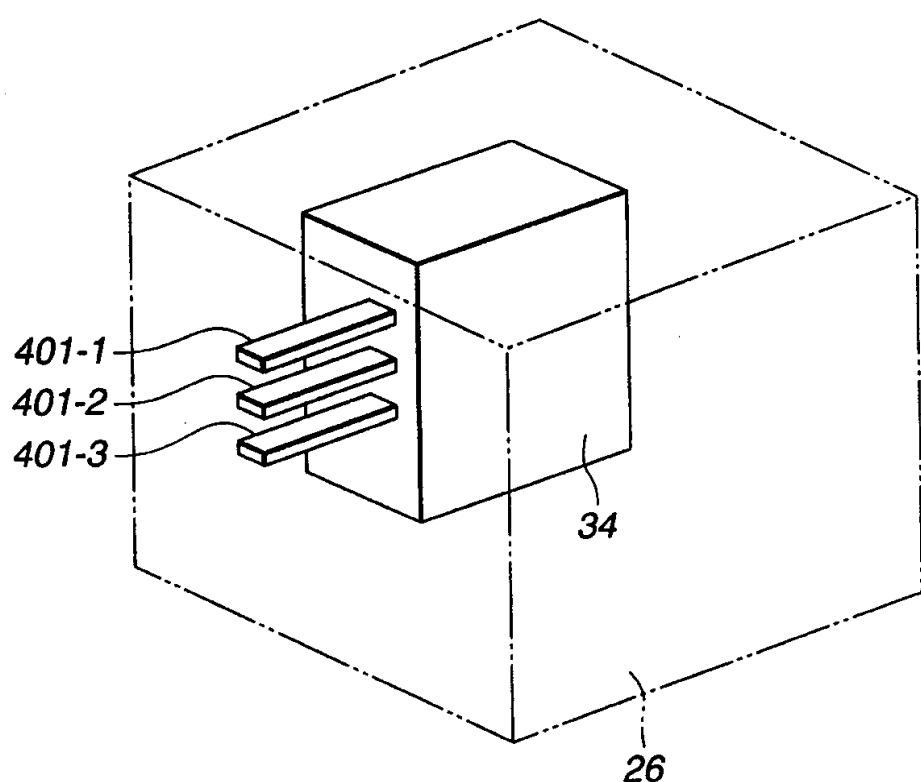


图 37

权 利 要 求 书
按照条约第 19 条的修改

1、一种信息处理设备，包括：

用于储存内容数据的装置；

5 具有软件的控制装置，该软件控制在内容数据存储装置中保存或从该内
容数据存储装置中读取内容数据；以及

提供的在硬件上独立于控制装置的装置，用以解密和执行从控制装置提
供的加密程序，并将程序执行的结果提供给控制装置；

10 所述控制装置根据所述程序执行装置提供的程序执行结果，控制在内容
数据存储装置中保存或从内容数据存储装置中读取内容数据。

2、如权利要求 1 所述的设备，其中：

所述内容数据存储装置还保存管理信息，利用所述管理信息来管理保存
在该装置中的内容数据；以及

15 所述控制装置使程序执行装置根据所述管理信息执行预先确定的计
算。

3、如权利要求 1 所述的设备，其中：

所述控制装置是 CPU；

所述内容数据存储装置是硬盘；以及

20 所述程序执行装置是包含在半导体 IC 中的 CPU，而不是作为控制装置
的 CPU。

4、一种信息处理设备，包括：

存储介质，用于保存内容数据和内容数据的内容管理信息；

以软件形成的处理控制器，控制将内容数据保存到存储介质，或从存储
介质中读取内容数据；以及

25 程序执行控制器，以独立于处理控制器的半导体芯片形式提供，所述程
序执行控制器被提供有来自处理控制器提的密程序，并且，解密所述程序并
将程序执行结果提供给处理控制器；

根据所述程序执行控制器的程序执行结果，所述处理控制器控制将内容
数据保存到存储介质，或从存储介质中读取内容数据；以及

30 使程序执行控制器设计成使它内部的操作不能从半导体芯片外部确
定，以及进行计算来检查对所述内容管理信息所做的任何篡改。

- 5、一种由信息处理设备所使用的信息处理方法，所述信息处理设备包括：
- 用于保存内容数据的装置；
- 具有软件的控制装置，控制将内容数据保存在存储装置中或从该内容数
5 据存储装置中读取内容数据；以及
- 提供的在硬件上独立于控制装置的装置，用以解密和执行从控制装置提
供的加密程序，并将程序执行的结果提供给控制装置；
- 所述信息处理方法包括步骤：
- 根据程序执行装置的程序执行结果，控制在所述内容数据存储装置中保
10 存或从所述内容数据存储装置中读取内容数据。
- 6、一种由在信息处理设备使用的信息处理方法，所述信息处理设备包
括：
- 存储介质，用于保存内容数据和内容数据的内容管理信息；
- 以软件形成的处理控制器，控制将内容数据保存到存储介质，或从存储
15 介质中读取内容数据；以及
- 程序执行控制器，以独立于处理控制器的半导体芯片形式提供，所述程
序执行控制器被提供有来自处理控制器提的密程序，并且，解密所述程序并
将程序执行结果提供给处理控制器；
- 根据所述程序执行控制器的程序执行结果，所述处理控制器控制将内容
20 数据保存到存储介质，或从存储介质中读取内容数据；以及
- 使程序执行控制器设计成使它内部的操作不能从半导体芯片外部确定，
以及进行计算来检查对所述内容管理信息所做的任何篡改。
- 7、一种在信息处理设备中所使用的信息处理方法，所述信息处理设备
包括：
- 25 用于保存内容数据的装置；
- 具有软件的控制装置，控制将内容数据保存在存储装置中或从该内容数
据存储装置中读取内容数据；以及
- 提供的在硬件上独立于控制装置的装置，用以解密和执行从控制装置提
供的加密程序，并将程序执行的结果提供给控制装置；
- 30 在其中记录有计算机可读程序的控制装置，该程序包括步骤：根据所述
程序执行装置中提供的程序执行结果，控制将内容数据保存在所述内容数据

存储装置中或从所述内容数据存储装置中读取内容数据。

8、一种信息处理设备，包括：

用于输入内容数据的装置；

用于保存从输入装置提供的内容数据的装置；

5 用于以预先确定的方式、压缩保存在内容数据存储装置中的内容数据的装置；

用于以预先确定的方式加密保存在内容数据存储装置中的内容数据的装置；以及

10 用于控制在内容数据存储装置中保存或从内容数据存储装置中读取内容数据的装置，该内容数据是由压缩装置压缩和由加密装置加密的内容数据。

9、如权利要求 8 所述的设备，其中以同样的方式，压缩装置压缩或加密装置加密从输入装置提供的不同的数据。

15 10、如权利要求 8 所述的设备，其中，分别以不同的方式，压缩装置压缩或加密装置加密从输入装置提供的不同的数据，并且采用预先确定的公共压缩或加密方式将从内容数据存储装置读取的数据输出到预先确定的设备。

11、一种信息处理设备，包括：

接口，通过该接口，从预先确定的记录介质或服务器提供内容数据；

20 存储介质，用于保存通过所述接口提供的内容数据；

压缩程序，用于以预先确定的方式压缩保存到所述存储介质中的内容数据；

加密程序，用于以预先确定的方式加密保存到存储介质中的内容数据；

25 控制器，用于控制内容数据在存储介质中的存储或读取，所述内容数据已经由压缩程序压缩和由加密程序加密；

30 分别以相同或不同的方式，所述压缩程序压缩或所述加密程序加密通过接口提供并且被以不同方式处理过的内数据，将所述内数据保存到存储介质中，并进行转换，当从存储介质中读出以不同的方式压缩了或加密了的所述内数据时，将所述内数据传递给预先确定的便携设备，使得所述内数据可以以公共的方式被压缩或加密到所述信息处理设备和便携设备中。

- 12、一种信息处理方法，包括步骤：
输入数据；
保存从数据输入步骤提供的数据；
以预先确定的方式压缩在数据存储步骤保存的数据；
5 以预先确定的方式加密在数据存储步骤保存的数据；以及
控制在压缩步骤压缩和在加密步骤加密的数据的存储或读取。
- 13、一种信息处理方法，包括步骤：
从预先确定的记录介质或服务器输入内容数据；
保存在数据输入步骤提供的数据；
10 以预先确定的方式压缩在数据存储步骤保存的数据；
以预先确定的方式加密在数据压缩步骤保存的数据；以及
控制将在压缩步骤压缩和在加密步骤加密的数据保存在存储介质中或
者从存储介质中读取该数据；
分别以相同或不同的方式，所述压缩步骤压缩或所述加密步骤加密在数
15 据输入步骤中提供并且已被以不同方式处理过的内容数据，将所述内容数据
保存到存储介质中，并进行转换，当从存储介质中读出以不同的方式压缩了
或加密了的所述内容数据时，将所述内容数据传递给预先确定的便携设备，
使得所述内容数据可以以公共的方式被压缩或加密到这台设备和便携设备
中。
- 20 14、一种程序存储介质，在其中记录有由信息处理设备执行和由计算机
可读的程序，所述序包括步骤：
输入数据；
保存从数据输入步骤提供的数据；
以预先确定的方式压缩在数据存储步骤保存的数据；
25 以预先确定的方式加密在数据存储步骤保存的数据；以及
控制在压缩步骤压缩和在加密步骤加密的数据的存储或读取。
- 15、一种信息处理设备，包括：
用于输入内容数据的装置；
用于保存从内容数据输入装置提供的内容数据的装置；
30 用于持有保存在内容数据存储装置中的内容数据的管理信息的装置；
用于根据在管理信息持有装置中持有的管理信息进行预先确定的计算

的装置；以及

依据对于计算装置的计算结果与保存在内容数据存储装置中的以前计算结果的比较，用于控制保存在内容数据存储装置中的内容数据的使用的装置。

5 16、如权利要求 15 所述的设备，其中计算装置使用作为管理信息的哈希函数进行计算。

17、如权利要求 15 所述的设备，其中所述数据是音乐数据，并且所述管理信息包括用于识别音乐数据的识别信息。

18、一种信息处理设备，包括：

10 接口，用于输入内容数据和该内容数据的识别信息；

存储介质，用于保存通过所述接口提供的内容数据；

第一存储器，象使用规则文件一样，用于持有在存储介质中保存的内容数据的识别信息；

15 管理程序，用于计算，将哈希函数作用在第一存储器持有的识别信息上；

第二存储器，用于保存由管理程序计算的结果；以及

控制器，用于将管理程序的计算结果与保存在第二存储器中的以前的计算结果比较，当两种计算结果不一致时，禁止复制或移动保存在存储介质中的内容数据。

20 19、一种信息处理方法，包括步骤：

输入数据；

保存从数据输入步骤提供的数据；

持有在数据存储步骤中保存的数据的管理信息；

根据在管理信息持有步骤所持有的管理信息进行预先确定的计算；

25 保存在计算步骤所做的计算结果；以及

比较计算结果，将在计算步骤所做的计算结果与在数据存储步骤中保存的以前的计算结果进行比较，以控制在数据存储步骤保存的数据的使用。

20、一种信息处理方法，包括步骤：

输入内容数据和该内容数据的识别信息；

30 将在输入步骤提供的内容数据保存在存储介质中；

象使用规则文件一样，持有在存储步骤中保存的内容数据的识别信息；

进行计算，将哈希函数作用到在持有步骤持有的识别信息上；

保存计算步骤所做的计算结果；以及

将计算步骤的计算结果与在存储步骤保存的过去计算结果进行比较，当两种计算结果不一致时，禁止复制或移动保存在存储介质中的内容数据。

5 21、一种程序存储介质，在其中记录有信息处理设备要执行和计算机可读的程序，所述程序包括步骤：

输入数据；

保存从数据输入步骤提供的数据；

持有在数据存储步骤中所保存的数据的管理信息；

10 根据在管理信息持有步骤所持有的管理信息进行预先确定的计算；

保存在计算步骤所做的计算结果；以及

依据对于在计算步骤的计算结果与在数据存储步骤中保存的以前计算结果的比较的结果，控制在数据存储步骤中所保存的数据的使用。

22、一种信息处理设备，包括：

15 用于向其它设备发送数据，和从其它设备接收数据的装置；

用于持有预先确定的锁密钥和副本密钥的装置；

使用持有装置持有的锁密钥的认证装置，当向其它设备发送数据和从其它设备接收数据时，与其它设备进行相互认证，以产生通信密钥；

用于使用副本密钥加密通信密钥的装置；以及

20 用于保存在数据发送和接收装置中接收的数据的装置，该数据已由与加密装置加密的通信密钥相对应的通信密钥加过密。

23、如权利要求 22 所述的设备，还包括：

加密密钥解密装置，使用副本密钥解密保存在存储装置中的通信密钥；

以及

25 用于解密在存储装置中保存的数据的装置。

24、一种信息处理设备，包括：

接口，通过它可以在所述信息处理设备与连接到所述信息处理设备的便携设备或服务器之间进行数据传递；

存储器，用于持有预先确定的主密钥和副本密钥；

30 认证程序，当数据将传递给便携设备或服务器或从便携设备或服务器传递来时，所述认证程序利用保存在存储器中的主密钥与便携设备或服务器相

互认证以产生通信密钥；

加密解密的程序，使用通信密钥对加密密钥解密，从便携设备或服务器传递来的内容数据由所述加密密钥加密过，并使用副本密钥对加密密钥加密；

5 存储介质，用于保存通过所述接口接收并使用所述通信密钥加密的内容数据，所述通信密钥相应于使用副本密钥加密的加密密钥；

加密密钥解密程序，用副本密钥解密保存在存储介质中的加密密钥；以及

10 数据解密程序，用由所述加密解密程序解密的加密密钥，将保存在存储介质中的内容数据解密。

25、一种信息处理方法，包括步骤：

向其它设备发送数据，和从其它设备接收数据；

持有预先确定的锁密钥和副本密钥；

15 使用在持有步骤持有的锁密钥，当向其它设备发送数据和从其它设备接收数据时，与其它设备进行相互认证，以产生通信密钥；

使用副本密钥加密通信密钥；以及

保存在数据发送和接收步骤中接收的数据，该数据已由与加密步骤中加密的通信密钥相对应的通信密钥加过密。

26、一种信息处理方法，包括步骤：

20 在所述设备与连接到所述设备的便携设备或服务器之间传递数据；

持有预先确定的主密钥和副本密钥；

当数据被传递到所述便携设备或服务器，或从所述便携设备或服务器传递来数据时，使用在持有步骤中的主密钥与所述便携设备或服务器进行相互认证，以产生通信密钥；

25 使用所述通信密钥，解密对从所述便携设备或服务器发送的内容数据进行加密的加密密钥，并用所述副本密钥加密所述的加密密钥；

存储内容数据，所述内容数据是通过所述接口接收、并使用相应于用所述副本密钥加密的加密密钥的通信密钥加密的；

30 使用所述副本密钥，解密在所述存储步骤中在存储介质中保存的加密密钥；

使用在加密解密步骤中解密的加密密钥，解密保存在所述存储介质中的

内容数据。

27、一种程序存储介质，在其中记录有信息处理装置要执行和计算机可读的程序，所述程序包括步骤：

向其它设备发送数据，和从其它设备接收数据；

5 持有预先确定的锁密钥和副本密钥；

使用在持有步骤持有的锁密钥，当向其它设备发送数据和从其它设备接收数据时，与其它设备进行相互认证，以产生通信密钥；

使用副本密钥加密通信密钥；以及

10 保存数据发送和接收步骤中接收的数据，所述数据已由与与加密步骤中加密的通信密钥相对应的通信密钥加过密。

28、一种信息处理设备，包括：

存储装置，用于保存数据；

持有装置，用于持有保存在数据存储装置中数据的使用规则；

15 判断装置，当将保存在数据存储装置中的数据移动到其它设备时，用于判断保存在数据存储装置中的数据的使用规则是否可由其它设备复制；以及

移动装置，根据判断装置的判断结果，将保存在存储装置中的数据以及保存在数据存储装置中的数据的使用规则移动到其它设备，所述数据的使用规则由持有装置持有。

29、如权利要求 28 所述的设备，其中数据的使用规则包括：

20 回放限制条件；

回放计帐条件；或

复制限制条件。

30、一种信息处理设备，包括：

存储内容数据的存储装置；

25 存储器，持有保存在存储装置中的内容数据的使用规则；以及

移动管理程序，当保存在存储装置中的内容数据将被移动到便携设备时，判断所述便携设备是否适合所述使用规则；

当由移动管理程序的判断结果确定出所述便携设备不满足所述使用规则时，禁止将保存在存储装置中的内容数据移动到便携设备。

30 31、如权利要求 30 所所述的设备，其中所述移动包括复制、移动或登出，而所述使用规则包括回放限制条件、回放记帐条件或复制限制条件。

32、一种信息处理方法，包括步骤：

保存数据；

持有在数据存储步骤中保存的数据的使用规则；

当将在数据存储步骤中保存的数据移动到其它设备时，判断在数据存储

5 步骤中保存的数据的使用规则是否可由其它设备复制；以及

根据判断步骤的判断结果，将保存在存储装置中的数据以及在数据存储步骤中保存的数据的使用规则移动到其它设备，所述数据的使用规则在持有步骤中持有。

33、一种信息处理方法，包括步骤：

10 将内容数据保存在存储装置中；

在存储器中，持有用于保存在存储装置中的内容数据的使用规则；以及

当保存在存储装置中的内容数据将被移动到便携设备时，判断所述便携设备是否满足所述使用规则；

当确定出便携设备不满足所述使用规则时，禁止把保存在存储装置中的

15 内容数据移动到所述便携设备。

34、如权利要求33所述的方法，其中所述移动包括复制、移动或登出，而所述使用规则包括回放限制条件、回放记帐条件或复制限制条件。

35、一种程序存储介质，在其中记录有信息处理装置要执行和计算机可读的程序，该程序包括步骤：

20 保存数据；

持有在数据存储步骤中保存的数据的使用规则；

当将在数据存储步骤中保存的数据移动到其它设备时，判断在数据存储步骤中保存的数据的使用规则是否可由其它设备复制；以及

根据判断步骤的判断结果，将保存在存储装置中的数据以及在数据存储步骤中保存的数据的使用规则移动到其它设备，所述数据的使用规则在持有步骤中持有。