[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
H04N 7/50
H04N 7/08 H04N 5/913
G11B 20/00

[12]发明专利申请公开说明书

[21]申请号 98800368.6

[43]公开日 1999年6月23日

[11]公开号 CN 1220805A

[22]申请日 98.1.22 [21]申请号 98800368.6
[30]优先权
[32]97.1.27 [33]EP [31]97200165.5
[32]97.4.25 [33]EP [31]97201237.1
[32]97.5.15 [33]EP [31]97201470.8
[86]国际申请 PCT/IB98/00087 98.1.22
[87]国际公布 WO98/33325 英 98.7.30
[85]进入国家阶段日期 98.11.26
[71]申请人 皇家菲利浦电子有限公司
地址 荷兰艾恩德霍芬
[72]发明人 J·P·M·G·林纳茨

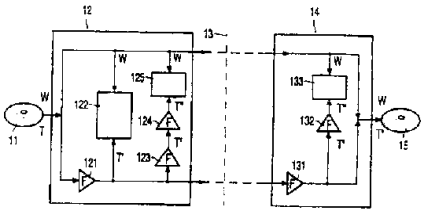
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 李亚非

权利要求书4页 说明书14页 附图页数3页

[54]发明名称 传递内容信息和与其相关的附加信息的方法和系统

[57]摘要

描述了一种用于经过光盘传递内容信息和与其相关的附加信息(例如音频、视 频和附加的作者或复制控制的状态)的系统。产生一个编码信号,它包括表示 附加信息的水印模式。除非在严重影响重放后的内容信息的质量的情况下水印 模式是不能改变的。按照本发明在对控制模式施加一个单向函数以产生水印时 ,控制模式也被传递。这具有下列优点,即可以很容易检测出对水印或控制模 式的任何改变,因为从计算角度上是不可能对改变了的水印计算出新的控制模 式的。因此附加信息受到良好保护而免遭篡改。或者,盗版者将被迫全部替换水 印模式,从而极大地影响重放内容的质量。在允许第一代复本("复制一次")的复制控制方法中原始的控制模式由单向函数处理3次以产生水印,而每个 重放或记录装置则在输出/记录它之前对控制模式处理一次,从而形成加密保 护的减数计数器。



ISSN1008-4274

权 利 要 求 书

1. 一种传递内容信息和与其相关的附加信息的方法，其中：

被传递的是表示内容信息和表示附加信息的水印模式的编码信号，其特征在于，传递一个表示控制模式的控制信号，该水印模式和控制模式的组合表示该附加信息，并且水印模式包括把一个单向函数加到控制模式上所产生的结果。

2. 一种对内容信息和与其相关的附加信息进行编码的方法，在其中：

通过对内容信息按照表示附加信息的水印模式进行编码来产生一个编码信号，其特征在于，产生一个表示控制模式的控制信号，该水印模式和控制模式组合起来表示附加信息，并且水印模式是通过把一个单向函数加到控制模式上而产生的。

3. 一种恢复与内容信息相关的附加信息的方法，其中：

表示附加信息的水印模式是从一个表示内容信息和水印模式的编码信号中恢复的，其特征在于，该水印模式和控制模式的组合表示附加信息，并且控制模式由一个单向函数来处理，同时附加信息是通过把水印模式和处理过的控制模式进行比较而验证的。

4. 一种通过一个包括编码信号的传递信号来传递内容信息和相关的附加信息的系统，该系统包括一个发送该传递信号的发射机，该发射机包含一个编码单元，该编码单元通过根据表示附加信息的水印模式对内容信息进行编码来产生编码信号，该系统还包括一个用于接收该传递信号的接收机，该接收机含有一个用于恢复水印模式的恢复单元，该系统的特征在于，传递信号还包括表示控制模式的控制信号，该水印模式和控制模式的组合表示附加信息，并且该发射机包含一个用于根据控制模式产生水印模式的单向函数单元，并且该接收机包括另外一个用于产生经过处理的控制模式的单向函数单元，并包括一个用于通过比较水印模式和经处理的控制模式以验证该附加信息的比较器。

5. 一种用于产生编码信号的装置，该装置包括一个编码单元，用于根据表示附加信息的水印模式对内容信息进行编码以产生编码信号，其特征在于，该装置包括一个用于产生表示控制模式的控制信号的控制单元，该水印模式和控制模式的组合表示该附加信息，还包括一个用于根据控制模式产生水印模式的单向函数单元。

6. 如权利要求 5 所述的装置，其特征在于该装置包括一个传递单元，用于产生一个包括编码信号和控制信号的传递信号。

7. 如权利要求 5 所要求的装置，其特征在于该单向函数单元设计成可通过把控制模式 n 次通过一个加密的单向函数来产生经过 n 次处理的控制模式，其中 n 是大于零的整数。

8. 如权利要求 7 所要求的装置，其特征在于 n=3 表明可允许有一代的复本。

9. 如权利要求 5 所要求的装置，其特征在于该装置包括一个识别单元，用于在附加信息中包含一个记录装置识别码。

10. 一种用于处理表示内容信息和表示附加信息的水印模式的编码信号的装置，该装置包括一个用于恢复水印模式的恢复单元，其特征在于，该装置包括一个用于接收表示控制模式的控制信号的控制单元，该水印模式和控制模式的组合表示附加信息，还包括用于产生经过处理的控制模式的单向函数单元，和用于通过比较水印模式和经过处理的控制模式以验证附加信息的比较器。

11. 如权利要求 10 所要求的装置，其特征在于，该单向函数单元设计成可通过把控制模式 n 次通过一个加密的单向函数而产生经过 n 次处理的控制模式，其中 n 是大于零的整数。

12. 如权利要求 11 所要求的装置，其特征在于，控制模式包括第一部分和第二部分，并且该装置包括一个组合单元，用于把经 n 次处理的控制模式和经（n－1）次处理的控制模式的第二部分组合起来，该组合单元的输出则耦合到单向单元的输入。

13. 如权利要求 11 所要求的装置，其特征在于，该装置包括一个控制单元，用于输出另外一个表示经 n 次处理的控制模式的控制信号，其中 n 等于 1。

14. 如权利要求 11 所要求的装置，其特征在于该比较器设计用来确定一个 m 值，即先在 n=1 时首先比较水印模式和经 n 次处理的控制模式、然后在 n>1 时再至少比较一次水印模式和经 n 次处理的控制模式，其中 m 是得到一个成功的比较时的 n 值。

15. 如权利要求 10 所要求的装置，其特征在于，该装置包括一个输出单元，用于输出表示与附加信息有关的内容信息的输出信号。

16. 如权利要求 15 所要求的装置，其特征在于，该输出单元是记录

单元，用于把输出信号记录在记录载体上。

17. 如权利要求 13 和 16 所要求的装置，其特征在于，该记录单元设计成用于记录另外的控制信号。

18. 如权利要求 14 和 15 所要求的装置，其特征在于该输出单元设计成当 m=1 或 m=3 时则输出输出信号。

19. 如权利要求 14 和 16 所要求的装置，其特征在于，该记录单元设计成当 m=2 时则进行记录。

20. 如权利要求 10 所要求的装置，其特征在于，该装置包括一个重放单元，用于从记录载体输入编码信号。

21. 如权利要求 10 所要求的装置，其特征在于该装置包括一个载体模式读出单元，用于从记录载体恢复载体模式，还包括一个用于产生经处理的载体模式的单向函数单元，和一个用于比较水印模式和经处理的载体模式的比较器。

22. 一种用于权利要求 5 的系统中的编码信号，该编码信号表示内容信息和一个表示附加信息的水印模式，其特征在于，该水印模式包括由单向函数处理过的控制模式的结果，该水印模式和控制模式的组合表示附加信息。

23. 用于权利要求 5 的系统中的控制信号，其特征在于，该控制信号表示一个控制模式，该模式用于控制一个表示内容信息和水印模式的编码信号，该控制模式和水印模式的组合表示附加信息，该水印模式包含由单向函数处理过的控制模式的结果。

24. 一种在其上载有如权利要求 22 所要求的编码信号和/或如权利要求 23 所要求的控制信号的记录载体。

25. 如权利要求 24 所要求的记录载体，其特征在于，该水印是 n 次控制模式的指示，该 n 次控制在经 n 次通过加密单向函数的处理之后对应于该水印，其中 n 是大于零的整数。

26. 如权利要求 24 或 25 所要求的记录载体，其特征在于，该记录载体包括一个载体模式，该水印模式含有由单向函数处理过的载体模式的结果。

27. 如权利要求 26 所要求的记录载体，在其中编码信号是由一个物理参数的变化的调制模式所表示的，其特征在于，该记录载体包括另外一个物理参数变化的另外一种模式，它以表示编码信号的另外一种不同

方式来表示该载体模式。

28. 如权利要求 24 所要求的记录载体，其特征在于上述的记录载体是一种可用光学方式读出的类型，该编码信号是以在循迹上可用光学方式检测到的标记的调制模式来表示的。

说　明　书

传递内容信息和与其相关的附加信息的方法和系统

本发明涉及传递内容信息和与其相关的附加信息的一种方法，在该方法中被传递的是表示内容信息和表示附加信息的水印（watermark）模式的编码信号。

本发明还涉及对内容信息和与其相关的附加信息进行编码的一种方法，其中编码信号是把内容信息按照表示附加信息的水印模式经编码而产生的。

本发明进一步涉及恢复与内容信息相关的附加信息的一种方法，其中表示附加信息的水印模式是从表示内容信息和水印模式的编码信号中恢复的。

本发明还涉及传递内容信息和相关的附加信息的系统、产生编码信号的装置、处理编码信号的装置、编码信号、控制信号和记录载体。

这样的方法和这样的传递系统在专利申请 WO 97/13248（PHN 15391）即相关文件表中的文件 D1 中有说明。该文件说明，视频和音频内容正越来越多地用数字编码形式，例如 MPEG 比特流的形式来发送和记录。对于传递在逻辑上和内容信息相关的附加信息存在着日益增长的需求，这种附加信息是用来控制对内容信息的处理的。附加信息应受保护不被扰动以便它仍然能掌握其控制功能。附加信息对用于防止复制是特别有用的。

在音乐出版中复制保护已有长时间的历史。目前已安装的设备基础（包括带有声卡的 PC 机在内）对防止非法复制几乎没有提供保护。在防止复制方案中，最困难的问题在于盗版人总是可以试图重放一张原版盘，他可以把这种盘当作家庭录制的模拟盘一样来处理其内容并将它记录下。人们希望做到这样，即消费者的记录装置能够毫无限制地录下消费者自己创作的材料，但却禁止录下有版权的材料。因此，防止复制机制必须能够在消费者自己的创作和从专业音乐出版人所得来的原版内容之间加以区分。这种设备必须仅仅根据音频或视频信号本身来实现这种区别，因为任何打算参考内容的物理来源（例如盘或微音器）以进行区别都是不可靠的。对于数字存储介质，如 DCC，已经规定了“复制比特”，

这些比特表示一种版权状态，例如“不允许复制”、“自由复制”或“允许复制一次”。其余的复制比特可能表明含有信息的介质必须是通过压制而生产的“专业”介质而不是一张“可录制”的盘。

给数字内容信号加标记称作为加水印，例如在这样一种编码信号中插进一个标记以便把该编码信号归类为真正的节目材料。在我们的系统中水印具有多比特水印模式的形式，它表示某种附加信息，例如表明该编码信号构成了防止复制的内容和/或表明内容的出处。水印通常具有固定部分以识别该比特模式为有效的水印和/或用来同步恢复过程，同时也可能包括可变部分以表示上述的附加信息。在 D1 中公开了一种把水印模式嵌在编码信号中的方法，从而使它易于检测，但却难于擦除或修改，除非在解码后使音响或视频内容的质量严重变劣。此外，水印模式必须相当长以防止一个未加标记的编码信号偶而被认为是加了标记的。同时，水印应该能在相对较短的时间内（例如 1 到 10 秒内）被检测到，以便在区分信号时有一个较快的响应。已知的水印都有缺点，即它们只能表示有限数量的附加信息。蓄意地篡改（一部分）水印而对解码后的内容仅有少量劣化的情况仍是有可能的。

本发明的一个目的是提供一种用于传递与内容信息相关的附加信息以便更加有效地对抗对该附加信息的改动的装置。

为此目的，按照本发明的传递方法的特征在于：传递一个表示控制模式的控制信号，该水印模式和控制模式的组合表示该附加信息，并且水印模式包括把一个单向函数加到控制模式上所产生的结果。按照本发明的编码方法的特征在于产生一个表示控制模式的控制信号，该水印模式和控制模式的组合表示附加信息，并且水印模式是通过把一个单向函数加到控制模式上而产生的。用于恢复信息的方法的特征在于：将水印模式和控制模式的组合表示附加信息，并且控制模式由一个单向函数来处理，同时附加信息是通过把水印模式和处理过的控制模式进行比较而验证的。为此目的，用于处理表示内容信息和表示附加信息的水印模式的编码信号的装置包括一个按照本发明恢复水印模式的信息恢复单元，该装置的特征在于：它包括一个控制单元，用于接收表示控制模式的控制信号、表示附加信息的水印模式和控制模式的组合，还包括一个单向函数单元，用于产生一个经过处理的控制模式，并包括一个比较器，用于通过对水印模式和处理后的控制模式进行比较以验证附加信息。按照

本发明的记录载体含有编码信号和/或控制信号作为其记录下的信息。

按照本发明的上述措施具有这样的效果，即控制模式的小量变动将由于单向函数的性质而导致完全不同的处理后的控制模式。当恶意的用户改动控制模式时，水印就不再和改变了的控制模式相对应，或者它需要全部被取代。因此控制模式的改动在记录或重放装置中验证水印时可以很容易地被检测出来。同样，由于单向函数的性质，对水印模式的少量改变不能通过也对控制模式进行修改而得以匹配，这就阻止了从一个给定的输出值“往回”计算输入数据。这样做的好处在于对控制模式或水印的任何改变都可以被容易地检测到。如果恶意的用户想要改动由水印和/或附带的控制信号所表示的附加信息，他就不得不全部更换水印模式，而这将导致重放内容的质量严重下降，而且即使少量的水印修改也不能通过计算相应的控制模式来获得匹配，同时也会被检测出来。

应该指出，从 EP－0545472（文件 D2）中已经知道了一种防止记录信号被复制的系统、信息载体、和读出设备。该已知系统利用一个表示附加信息的物理标记来控制信息的再生。如果信息被复制到一个可写入的信息载体上，则这个复制的信息不能再生，因为在写入过程中记录下的只是信息而该复制件本身并不包含该物理标记。这种已知系统的问题在于它不可能做到复制一个不能进一步复制的复本。按照本发明的系统的一个实施例中，上述的控制模式具有一个允许复制标记的功能，它是和从原始记录所再生的信号一起分发的。该实施例的记录装置确实要针对该允许复制标记来验证信号中的水印。如果两个标记相对应，其内容就可录制在可记录的记录载体上，因而可以制成第一代的复本，但是允许标记本身是不允转录到复本上的。因此，当再生该复本的信号时，它不会再包含允许复制标记。记录装置就不会再从第一代复本上制成另外一个记录。因此，可以制成一代也仅仅就一代复本。

按照本发明来产生和/或处理编码信号的装置的一个实施例的特征在于：设计了一个单向函数单元，它使控制模式 n 次经过一个加密的单向函数来产生一个经 n 次处理的控制模式，这里的 n 是大于零的整数。它具有这样的效果：即编码信号含有水印模式而控制信号含有作为加密的可控计数器的控制模式。由控制模式隐含地表示的计数器值是这样来确定的，即：对经 n 次处理的控制模式和水印模式进行比较，直到找到匹配为止（或者在预定的最大计数范围内不可能有匹配）。在重放装置

中在把经处理的控制模式输出到记录装置之前，计数器值以加密的方式减少。记录装置检验计数器，如果计数允许，就再次减少计数值并对包括经处理的控制模式在内进行录制。这具有下列优点，即可以允许进行有限代数的复制，而且复制控制是在重放装置和记录装置中实现的。这种减少是由加密的单向函数实现的，它在没有巨大而且代价极高的计算努力的情况下是不能逆向进行的，因而要增加上述的计数器的值实际上是不可能的。一旦计数器的值减少得过多，经处理的控制模式就不能再和水印相匹配。重放装置和记录装置就会阻止再生和/或录制信息。

更多的优点、按照本发明的系统和装置的优选实施例在各从属权利要求中给出。

本发明的这些和其它特点可参考在下面的叙述中作为例子而说明的实施例并结合下列附图而变得明显并被进一步阐明，这些附图是：

图 1 表示一种复制控制系统；

图 2 表示包括两个部分的复制控制模式的单向处理过程；

图 3 表示一种单向函数；

图 4 表示利用介质标记 P 的复制控制系统；

图 5 表示处理编码信号的一种装置；和

图 6 表示一种记录装置。

本发明的总体概念是给带水印的编码信号加上一个控制模式，同时使用一个单向函数以便从控制模式产生水印。这样就可以在带水印信号的最终地点检查水印和相伴的控制模式的完整性。这有若干种优点，例如，水印可以相对比较短而且不需要它本身的完整性校验比特，它可以在信号中每隔几秒钟就重复一次从而可以在编辑后区分信号的各个部分，等等。由于水印必须和一个由使用单向函数而产生的经处理的控制模式相匹配，因而就不可能通过计算来从一个水印“反向”算出这个控制模式。篡改控制模式和水印只有在把两者都被完全取代的情况下才有可能，而这样做会导致再生的内容质量严重下降。如果得不到有效的控制模式，那么在重放装置和/或记录装置中再生或记录编码信号将根据防止复制的规定而可能受到控制或阻止。最好是所有消费者可用的设备都要检查水印模式且在没有控制信号时不接收任何信号。许多应用可以从这种控制中受益，例如复制控制、版权费支付、音乐和影视的租借等。复制控制可以类似于上述的 DCC 复制比特。可能要求呈现一个控制模式

以允许重放，和/或指明版权状态，例如允许有一代的复制品等。另外通过在某一日期之后发布不同的控制模式而实现在该日期之后的版本。此外，任何有关的信息可以被分开地附加进去，例如作者、歌词、名称、表演者或使用期限等都可以包含在这个控制模式中。

本发明的一个实施例是一个允许有一代复本的复制保护系统（这也叫做复制一次）。专业的音频流（audio stream）中含有内嵌的版权数据，它授权允许作一次复制。这是通过在音频流中内嵌一个水印 Yco 而实现的。此外，专业盘片含有一个特殊的允许标记 Xco，此外 Yco = H(Xco) 而 H( )是一个加密单向函数。在重放期间标记 Yco 保留在音频中（可能是内嵌的）。但它被消费者的记录装置除去了。由记录装置制成的复本因此就不再含有允许标记也就不能再复制。

对于系统的实施例，表示比特图形 Y 的水印和控制模式 X 之间的一个合适的关系是一个单向函数。单向函数的一种实施方案可以是 $Y = X^2 \bmod N$，此处 N 是公开模（Public modulus）。这里的 N 是两个保密的大素数的乘积（N = pq）。实际上 N 可以是内嵌在水印中的数据的一部分，即它是连接到 Y 上的。另一种可能是 Diffie 和 Hellman[1976]推测的离散对数单向函数（见文件 D4）：即在 GF（P）中 $F(x)=\alpha^x$，此处 α是 GF（P）的一个素元（Primitive element）。这里 P 是一个大素数，并要使 P－1 具有一个大的质因数。上述两种实施方案具有下述缺点，即自变量的大小或为了安全所需的比特数是相当大的。基于较少比特数的实际系统可以应用一个适当的安全密钥加密算法，例如 DES（数据加密标准），并使 Y = F(X) = X⊗DES(X)。这在图 3 的线路中作了说明。图 3 表示根据安全密钥加密算法的单向函数发生器的实施方案。在输入端 31 加上控制模式 X 并在加密器 32 中使用从密钥输入端 33 得到的一个密钥来加以处理。加密器 32 的输出由逻辑单元 34 与输入 X 作按位的异或运算，其结果出现是在输出端 35 上的比特模式 Y。在这个电路中，密钥可以做成是公开的或包含在水印中，即连接到 Y 上。

对于具有 DSD 格式（见文件 D3）的音频信号用的合适的水印是通过迫使一小部分（0.01％到 1％）的比特具有由 W 确定的特定值而嵌入的。这能使检测得以简化，因为重放装置或记录装置只需在预定位置检测预定比特的值就可以了。由那些为了表示水印而被迫形成的比特所引起的人为干扰可通过噪声整形而被减到最小。我们发现，对于 DSD 而言

涉及到 1% 比特的水印在信噪比超过 110 分贝时信号－噪声/失真比将减少 1 分贝。相反，如果盗版人改变这些比特的值，则信噪比将剧烈地变坏数十个分贝。对于视频信号，合适的水印是内嵌在压缩的 MPEG 中，例如在图象类型中（D1 中说明的 PTY 水印）。

本发明的另外一种实施例是允许复制 n 代的防止复制系统，也叫做具有复制 n 次的复制控制。这个实施例在防止录制信号被复制方面允许有限数量的复制。在我们的概念中，专业发布的标题至少包括两种类型的复制控制标记：内嵌于内容中的水印，和附加在内容上但可由记录装置去除和修改的复制控制（认证/授权）控制模式。上述控制模式叫做复制控制票证。在数字信号流中的该票证在信号每次通过记录设备或重放设备时被修改。在每次重放和每次记录期间就验证水印和票证之间的加密关系。一个可选的第三种类型的复制控制标记，表示识别介质（盘/带/等等）的介质标记的载体模式，可以单独使用或者也可以和同一个水印相关。介质标记可以用例如偏心的槽或凹坑跳动调制来表示，而且最好它是肉眼可见到的。可记录的介质可能带一个固定的预先确定的介质标记以识别该介质是可记录的，或者它是从已知来源得到的专业盘。可以对介质标记单独进行一次检查，这个标记可以是一个预定的值或者是通过加密函数而与水印和/或票证相关的一个值。在整体的系统概念中，我们区分：

· 种子 U：由内容拥有者产生的一个随机数。

· 介质标记 P，它出现在专业发布的盘/存储介质上；可记录的介质上带一个预先确定的值 P。

· 水印 W，它内嵌于内容中。W 能够同时存在于所有以数字表示的格式中（音频中的 DSD 格式、比特流、PCM，或视频的 MPEG 等）以及模拟版本中。如果这种概念用于视频影像中，模拟的水印可以例如和在垂直消隐间隔中所表示的票证相结合。数字的水印则可以在 MPEG PTY（图象类型）序列和可以在象素区域中表示，票证可以存放在 GOP（图象组）标题的用户数据区中。用户的家庭录音（像）（不受版权限制）可通过不存在预先确定的 W 的值而得到区别。

· 复制控制票证 T，它起到加密计数器的作用。T 是存在于数据标题中的一个小数据区，例如它可以像上面所说的 DCC 复制控制比特的类似方式加到信号中。T 一般包括 40 到 4000 个比特。

在整体系统概念中，在该流中的票证 T 在每次记录或重放操作时被 $T'=F(T)$ 所取代，这里的 F 是一个公开而周知的加密单向函数，这就是说，不论重放装置或记录装置都不是透明地通过 T 的，而是要把它通过函数 F。我们的方案发挥本发明的作用，使 T 可以认为是加密计数器，它可以轻易地增量而不能减量，除非盗版者能够使 F 逆转。从加密的观点来看，没有必要把 F 对潜在的盗版者保密。这里我们的目标是限制复制途径的长度，例如限制复本的复本的复本的代数，即限制复制的代数。只有在数据流中的水印与 $F^m(T)$ 相匹配时重放才被许可，此外 m 是仍然被允许的顺序记录或重放操作的次数。一般情况下 m 是奇数。只有在数据流中的水印与 $F^m(T)$ 相匹配时记录才被许可，此处 m 是仍然被允许的顺序记录或重放操作的次数。一般情况下 m 是偶然。在上面的叙述中，m 可以是明确地提供的，也可以在 m 相当小的情况下（例如当不论如何最大允许复制的次数是一次的情况下 $m<4$）由设备来检查所有的 m。可能的加密单向函数的一个例子在上面结合图 3 而作了说明。

在一个实施例中限制了从一个原件所得到的并行的复本数。上面的概念被延伸并应用于限制从一个盘所作的并行复本的数量，例如，顾客被允许只能用他从出版商那里买来的原版盘进行复制，而且这样的复本的数量是受限制的。为此我们需要在每个专业发布的标题中有一个小的记录区域以存放和修改 T。基本概念是，每次当重放装置核准记录装置进行一次复制时重放装置把 T 修改成 $F(T)$。在这种情况下由出版商出售的原始盘在生产时最初要产生一个种子 U。根据这个种子计算下列各变量：$P=F(U)$ 和 $T=F(F(U))$，后者我们用 $F^2(U)$ 来表示。对于允许让顾客并行复制 n 次的盘，要产生一个水印 W，这里 $W=F^{n+1}(U)$。重放装置在正常操作时输出其内容，但不输出 T。在记录时记录装置要求重放装置提供一个票证 T 使 $W=F(T)$，这个 T 也要记录在可录制的盘上。重放装置读出 T 并用 $F(T)$ 取代它。如果重放装置从原始盘读出，即盘上有一个与 T 匹配的有效 T，则重放装置只向记录装置提供 $F(T)$。记录装置反复地用 $F(T)$ 取代 T 直到 $W=F(T)$。带有内嵌 W 和相应 T 的内容记录在盘上。如果记录装置读的是可记录的盘，则永远不会把 T 发布到外面。

公开了一种复制控制概念，它依赖于介质上的物理记录，隐嵌于内容中的水印和用一个数字量表示的复制控制票证。应该指出，这个概念

体现了两种独立的机理：带水印的内容和控制票证 T 及介质标记 P 两者相结合。很明显，利用控制票证和带水印的信号相结合的概念可以单独地用于传递内容的系统中，例如，在广播系统中或在因特网上。从原理上说，控制票证提供一个只能增量但不能减量的计数器。控制票证概念特别适合于对 DSD 音频加水印，如文件 D3 所述。把数据嵌入最低位比特并利用噪声整形来减少它们的人为因素的概念也能用于脉码调制音频。这个概念也能用于 DVD 的 MPEG 视频存储。水印可以通过修改 PTY 序列而存放在 GOP 结构中。此外，记录装置的识别码可以包括在 W 中或一个独立的水印 Wi 中。最好是每个家用记录装置在对未加标记的资料进行录制时包括这样一个识别符。这种识别符可以仅仅只是该记录装置的制造厂代码、型号和串号。

图 1 表示按照本发明的一个复制控制系统。在记录载体 11 上的音乐内容用一个水印模式 W 加上水印，同时记录载体 11 上还含有一个控制模式，即复制控制票证 T。重放装置 12 包括通常的用于从例如已知的 CD 播放机的记录载体上再生音乐的部件和验证装置，验证装置包括由一个单向函数 F（见参考图 3 的说明）组成的三个单向函数单元 121、123、124 和两个比较器 122、125，它可以由一个单个的计算单元来实现，例如一个微处理器和一个程序。水印 W 和票证 T 是从原始的记录载体 11 导出的。票证 T 耦合到单向函数单元 121 而得到 T′，该 T′耦合到第一比较单元 122 和一个第二单向单元 123，它的输出是 T″，T″耦合到第三单向单元而得到 T‴，它耦合到第二比较单元 125。两个比较单元都在其第二输入端接收水印 W 以供比较。如果第一比较器 122 发现两者相等，则允许重放，但不允许（进一步）复制。如果第二比较器 125 也发现两者相等，则允许重放并且可以再进行一次复制。如果两个比较器都未找到相等的情况，则不允许重放，重放装置有一个接到数字接口 13 的输出，例如 IEC 958 和 P1394 数字接口，以便输出包括水印 W 和处理过的票证 T′在内的内容信息。记录装置 14 具有接收从该数字接口 13 来的上述信号的输入端。水印 W 耦合到第三比较单元 133。票证 T′耦合到第四个单向函数单元 131，得到处理后的票证 T″，该 T″耦合到第五个单向函数单元 132，其结果 T‴耦合到第三比较单元 133。如果第三比较单元 133 发现 T‴和 W 之间相等，则允许复制，包括水印 W 和经两次处理的票证 T″在内的音乐内容被录制在可录制的记录载体 15 上。这样，当经过三次

处理的控制模式等于 W 时就允许复制一代。所得到的复本含有经二次处理的控制模式 T″，它允许这种第一代复本进行重放，因为重放装置将首先产生一个处理过一次的模式，即（T″）′，而这和水印 W 现在是匹配的。对音乐内容的进一步复制则会被记录装置阻止，因为经过 5 次处理的票证和水印不再匹配。即使盗版者使用一种篡改过的记录装置，所得到的复本也会含有在记录装置上出现经过 4 次处理的票证 T″″。这样的复本不能在兼容的记录装置上重放，因为第一和第二比较器找不到相等性。所以为了要建立和使用非法的复本，记录装置和重放装置都要经过篡改。

在一个传递系统的实施例中经过 n 次处理的控制模式构成了加密保护的计数器。这个计数器可以用于对某个编码信号被允许在例如音频或视频租借系统中重放的次数进行计数，或者例如对所谓的并行复本的录制次数进行计数。在这类应用中控制信号最好在记录介质本身上面存放或修改。但是也可以另外单独存放，例如放在重放和/或记录装置中或在芯片板卡上。另外还可以存储若干个控制信号，而且对于每一种要被控制的作用，可通过例如加上或去除在光盘上相应区域上的墨水，从而使控制信号之一被损毁或使之不能读出。

图 2 表示含有两个部分的对控制模式 T^{n-1} 的单向处理。第一部分 21 是一个种子而第二部分是信息部分，包括附加信息，例如作者名、拥有者、发布日期等。这两个部分 21、22 在组合单元 23 中被合并，例如通过串接、相加或异或运算，其结果耦合到第一单向函数单元 24。控制模式 T^n 也包括两部分，第一部分 25 是第一个单向函数单元 24 的输出，而第二部分 26 是和信息部分 22 相同的。在下一个单向处理周期中使用了同一个函数，即另一个组合单元 27 和另一个单向函数单元 28，结果得到另外一个含有两部分的控制模式 T^{n+1}。在经过预定次数的单向周期之后从单向单元的输出得来的模式的第一部分和前面所叙述的实施例一样地和水印相匹配。这具有这样的优点，即每一个控制模式的信息部分 22、26 是可直接读出的并且也受到保护而免遭处置修改，因为信息部分的任何一点小修改都会使验证时在单向单元的输出端所得的模式被完全改变。在加密的编码信号的情况下，信息部分可以包含解密密钥。信息部分 22 也可能包括一个明显的计数器值，在处理以后的（n+1）次经处理的控制模式之前该值必须减少。这样，明显的计数器值就表示单向单元

的处理周期。这有这样的优点，即只有处理过 P 次的控制模式需要和水印模式相比较。当然，一个预定的变化，例如包括在信息部分中的明显的计数器值在产生和验证时必须以同样的方式予以改变。因此对这样的预先确定的变化值的篡改可以被有效地防止。

图 4 表示利用介质标记 P 的复制控制系统。介质标记允许在得到重放以前对于原盘可以验证两种独立的情况。记录载体 41，例如一张光盘，含有另外的一个物理参数变化的调制模式，这个物理参数表示与水印 W 相关的记录介质标记 P，这另一个调制模式是和原调制模式不同的另一种类型。在 D2 中可以找到这另一种调制模式，例如是一条偏心摆动的循迹。按照本发明，介质标记 P 耦合到一个单向单元 421，它的输出连接到第一比较器 423 和/或第二比较器 424。每个单向单元包括一个加密的单向函数，例如参照图 3 所说明的那样。第一比较器 423 还接收水印 W，在相等时就检测到无复制的原始盘的第一条件。第二比较器接收控制票证 T，在相等时就检测到允许复制一次的盘的第一条件。票证 T 同时还耦合到第二单向单元 425 而得到 T′，这个 T′耦合到第三比较器 426，它同时还接收水印 W，在相等时就检测到无复制的原始盘的第二条件，或者检测到合适的第一代复本（在这种情况下可能不存在介质标记 P 或者它有一个预先确定的值）。经过 1 次处理的票证 T′还耦合到数字接口 43 上的记录装置的一个输出端，并接到第三单向单元 427，后者再接到第 4 单向单元 428，得到一个经过 3 次处理的票证 T″，而它又接到第 4 比较器 429，该比较器还接收水印 W。在相等时就检测到允许复制一次的盘的第二条件。当重放的诸条件满足时，包括水印 W 在内的音乐内容就从重放装置 42 输出到数字接口 43。可以在数字接口 43 上连接一台记录装置 44 以便录制音乐。从接口来的水印 W 和票证 T′是以参考图 1 所说明的记录装置相同的方式来验证的。

在一个实施例中重放装置 42 和记录装置 44 具有用于家用水印 W_H 的输入端 431、441。在重放装置中家用水印 W_H 耦合到第五比较器 430，它同时还接收水印。在相等时就检测到家庭个人的创作。输入 431 最好经过另一个单向单元耦合到上述的第五比较器 431，在这种情况下家用的种子值要加到另外一个单向单元的输入端。家用种子值或水印可以存放在记录/重放装置的存储器内，或者在一个单独的存储模块上，例如芯片板卡上，或者可以写在纸上并由用户用键盘输入，就像个人身份识别

码（PIN）一样。另外的方案是消费者个人的音频创作的记录可以被认识和区别，因为他们的水印是一个固定的水印，例如全为零的一个字。

在系统的一个实施例中，编码信号是加密的，而 P 则用于解密，表示为连接在读出信号和带有包括 W 和票证 T 在内的明码内容的各信号之间的任选的解密单元 422。这对防止盘片免受未加控制的数据恢复或比特到比特的复制是有利的，例如在计算机上的复制。载体模式 P 可以由制造主盘的设备中的单向函数来产生，这种主盘是用来复制盘片的。然后主设备可以在载体模式上使用一个另外的单向函数来产生和输出水印模式。这有这样的好处，即载体模式 P 不可能在主设备之外被利用，而主设备则不能被控制来产生带有预先确定的载体模式的盘片（例如由盗版者从要加以复制的源盘中取出的模式）。

控制模式和票证可以和内容信息一起录制，或者另外的方式是记录在单独的地点，对盗版者而言是不可直接访问的地方，例如位于文件的标题或 CD 或 DVD 的导入段。复制控制票证可以隐藏在 MPEG 视频流中。在一个实施例中这一数据位于 GOP 标题中，在扩展和用户数据区中（见 MPEG 视频压缩标准）。

图 5 表示处理编码信号用的一种装置。所示的装置是用于重放光盘 51 的重放装置 52。重放装置备有读出装置，它包括一个读出头和伺服/控制单元 58 以便从盘 51 上读出信息。重放装置有一个到数字总线的数字输出 53 用于输出包括水印 W 和经过处理的控制票证 T 在内的被恢复的内容信号。还可以提供另外一个模拟输出 54 以便连接耳机或其它音响设备以便在经过数/模变换器（任选品，未示出）处理后输出音乐内容。从盘片 51 读出的信号由读出单元 55 处理，该单元可以具有参考图 4 所说明的解密功能。读出单元 55 耦合到恢复单元 61 以便恢复水印模式 W，还耦合到另一个恢复单元 60 以恢复控制模式 T。水印 W 和控制模式 T 连接到控制单元 62。控制单元 62 具有一个包括加密的单向函数 F（上面参考图 3 所说明的）的单向单元，该函数可以应用 n 次以产生一个 n 次的控制模式 T^n，还具有一个比较器单元，用于比较处理过的控制模式 T^n 和水印。在控制单元 62 的输出端 57 上的经过 1 次处理的控制票证 T′和加上水印的内容信号一起经过开关 56 而切换到数字输出 53 上，这个开关 56 是由控制单元 62 根据验证过程而操作的。因此，表示内容信息的输出信号只能根据由水印以及控制票证的组合所代表的附加信息

而可以在输出端 53 上获得。在验证时进行下列检查：W = F（T）或 W = F^3（T）表示允许重放，或者也有可能进一步重复测试到 W = F^{2n+1}（T）。经过 n 次处理的控制模式 T^m 与水印 W 相等的第一次成功测试表明了控制模式的计数器值 m。计数器值 m 可以用来验证在允许做 n 代复本的系统中的复本的代数，或者某一被允许进行的动作的作用次数（例如在软件程序中每次付费的使用），或者任何需要一个加密计数器的应用。在重放装置的一个实施例中提供了一个载体模式读出单元 59，用来从记录载体上恢复介质标记 P，例如在 D2 中所叙述的从伺服单元 58 的伺服信号读出偏心摆动模式。介质标记 P 连接到控制单元 62，在其中实施一个进一步的检查 T = F（P）以便验证控制模式 T 和物理标记 P。介质标记 P 可以耦合到读出单元 55 中的一个任选的解密单元。如果对盘片内容已作了加密，则重放装置利用 P 来对信息流解密。

图 6 显示一个记录装置。该装置是用于对可录写盘片 66 进行录制的记录装置 65。该记录装置具有从数字总线来的数字输入 72 以便接收需要录制的包括水印 W 和控制票证 T 在内的信号。输入端 72 耦合到用于恢复水印模式 W 的恢复单元 69，还耦合到另一个用于恢复控制模式 T 的恢复单元 70。水印 W 和控制模式 T 连接到控制单元 71。控制单元 71 具有一个包括加密单向函数 F 的单向单元（上面参考图 3 所作的说明），该函数 F 可以使用 n 次以产生一个 n 次的控制模式 T^n，并具有一个用来比较处理后的控制模式 T^n 和水印的比较器单元。在控制单元 71 的输出 67 上的经过 1 次处理的控制票证 T'和加上水印的内容信号一起经过开关 68 而切换到记录装置 73 上，该开关 68 是由控制单元 71 根据验证过程而操作的。因此表示内容信息的记录装置的输出只有在验证过程表示肯定而且表明可以进行复制的情况下才可以在可录制的盘片 66 上得到它。记录装置在把复制控制票证 T 传递到盘片之前总是把它先通过控制单元 71 中的单向函数。如果在信息流中的水印和 W = F^2（T）相匹配，则允许记录版权所有的音频。在允许更多代数的复本的实施例中，要检查 W = F^{2n}（T）。如果盗版者想要修改他的记录装置以便即使在不存在相应的 T 的情况下记录音频。那么正常的重放装置会拒绝重放这样的盘片。在专业出版时，专业标题是要在最初产生一个种子 U 而生产的。根据这个种子来计算下列变量：P = G（U）和 T =（F（F（U））），后者我们用 F^2（U）来表示。对于允许用户复制 n 次的盘片来说，水印 W 是按 W

$= F^{2n+1}(T)$ 而产生的。单向函数 G 和变量 P 可以这样规定，即 P 也含有出版人的识别码或制造主盘的机器的串号。如果盗版的出版商企图写一个特定的 P 以便对一张版权所有的盘片进行完全按比特的复制，那么盗版者必须修改他的制造主盘的机器。专业发布的盘片含有利用上述加密关系的 P、T、W 以及可能还有 n。专业发布的（版权所有的）内容的合法复本在可记录的介质上含有水印 W 和票证 T，使得 $W = F^m(T)$，此处 $m = 1, 3, 5, 7\cdots$。在 m=1 的情况下，盘片/介质的内容不能进一步复制。送到记录装置去的专业发布的（版权所有的）内容的数据流含有水印 W 和票证 T，使得 $W = F^m(T)$，此处 $m = 2, 4, 6\cdots$。在 m=2 的情况下，内容可以再有一次记录和重放。

虽然本发明是用盘片作为记录介质的实施例来说明的，但是很清楚，本发明也可以用别的系统来传递信息。例如，编码信号和控制信号可以通过像因特网这样的数据网络来传递。

尽管本发明是参考它的优选实施例来说明的，但应该理解，这些不是限制性的例子。因此，对那些熟悉本技术的人而言，各种修正可以变得很明显而不会背离由权利要求所规定的本发明的范围。例如，编码信号可以在只读盘片或磁带上分发，而控制信号可以分开地分发。另外，也可以使用在模拟域中的水印，不过一般说来这样的水印更难于恢复。通过使用一个只被目标方所了解的密钥，例如在特定的再生设备中内藏的密钥，或者使用一个由目标方利用公开密钥系统（例如 RSA）提供的公开密钥来对控制信号加密，可以防止无限制地使用控制信号。另外，编码信号和/或控制信号可以通过扰码或加密的方法得到外加的保护，或者可以外加一个数字签名。可以利用一个自由复制票证 R，它是在内容和/或水印（或其一部分）上的一个数字签名。另外，本发明是每个和各个新特征或各特征的组合，包括那些在引用或相关文件中所叙述的内容。

相关文件清单

（D1）WO 97/13248-A1(PHN 15391)

水印编码的信号。

(D2)EP－0545472（PHN 13922）

带有物理拷贝防护的闭合信息系统。

（D3）EP－A 97200197.8，提交日 27.01.97（申请人参见 PHN 16209）

比特流或 DSD 信号的水印（A. A. M. Bruekers 等人）

（D4）加密的新方向（Diffie 和 Hellman），IEEE Transaction on information theory, vol IT-22, No. 6, Nov. 1976, P. 644-654

说　明　书　附　图

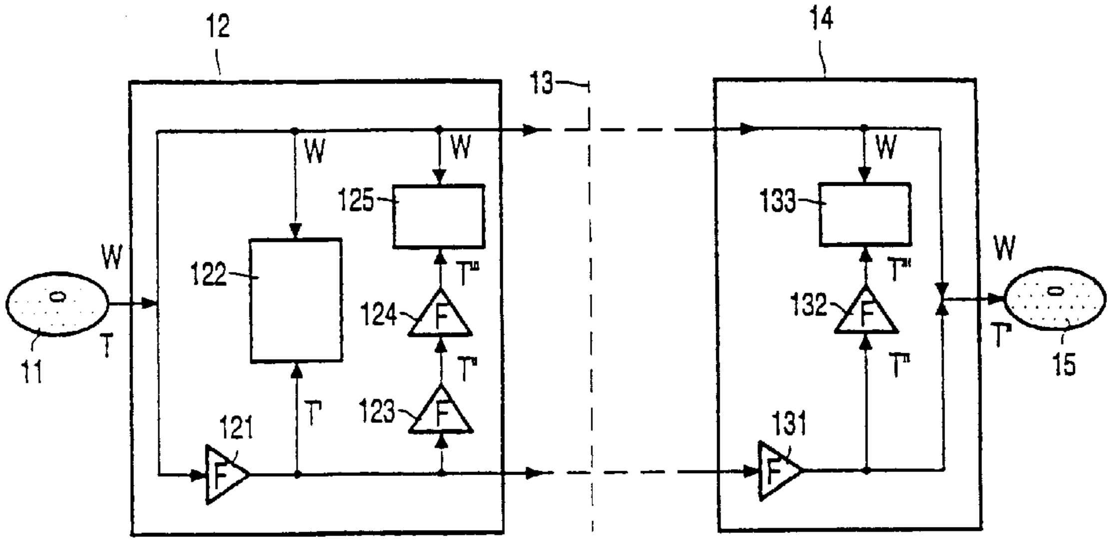

12
13
14
W
125
122
124
123
121
T
T'
T''
T'''
11
F
133
132
131
15

图 1

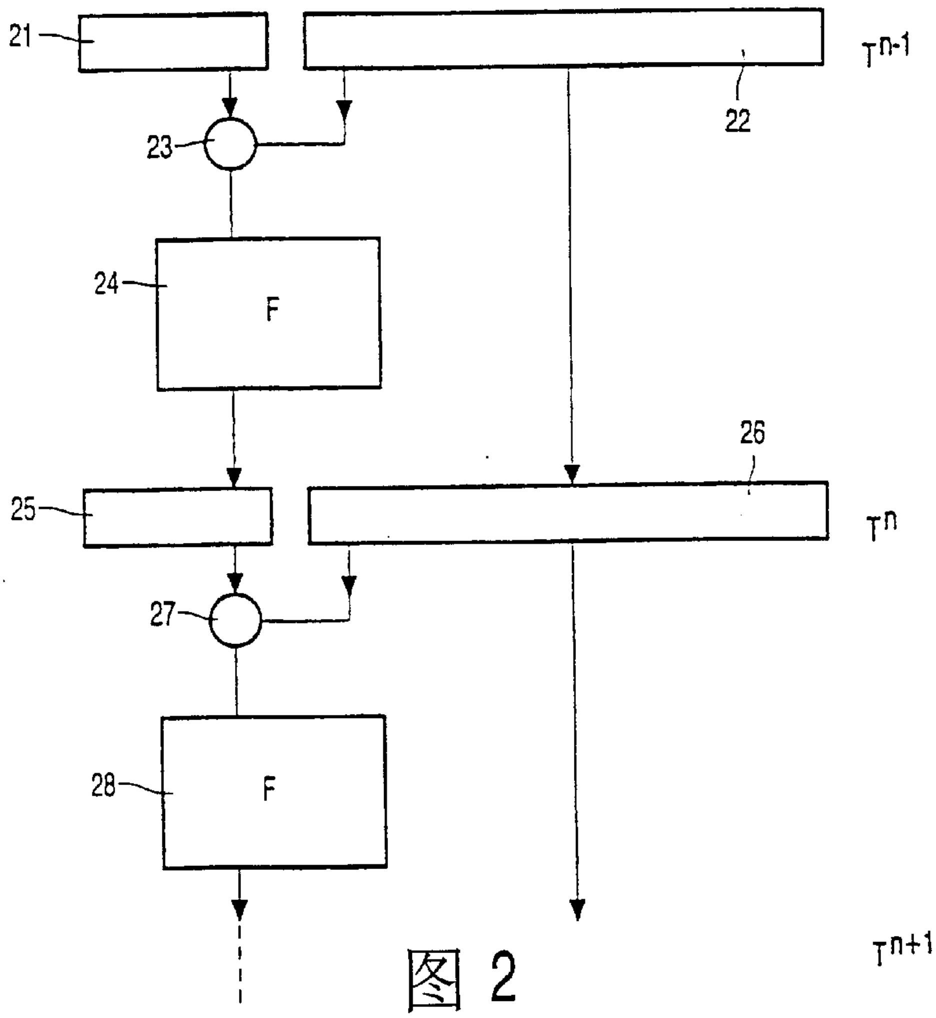

21
22
T^{n-1}
23
24
F
25
26
T^n
27
28
F
T^{n+1}

图 2

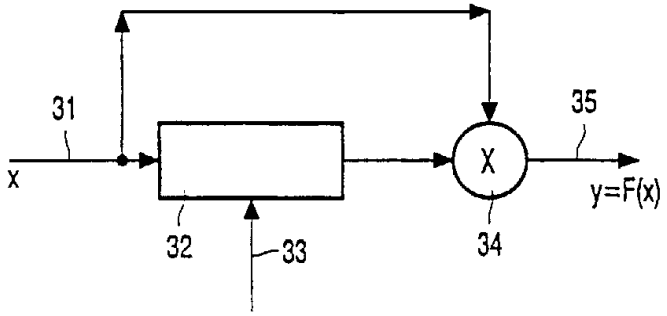

31
35
x
X
y=F(x)
32
33
34

图 3

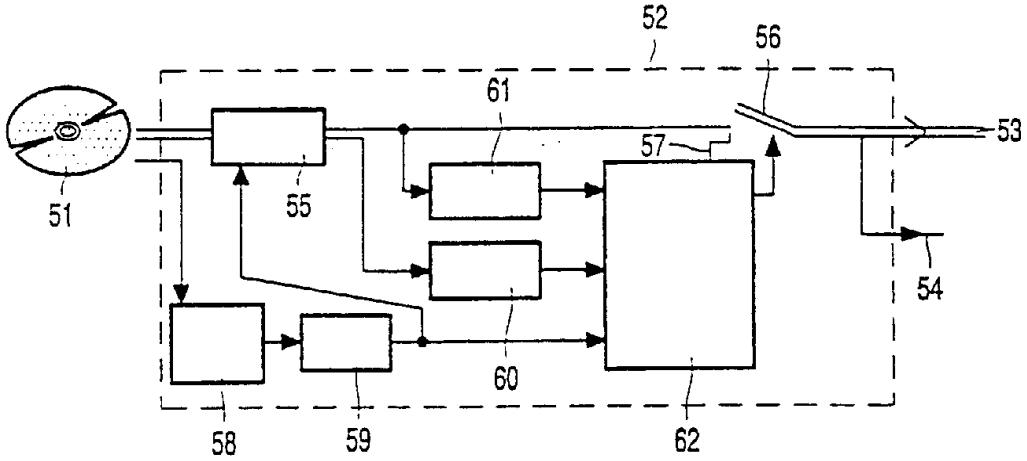

52
56
61
57
53
51
55
54
60
58
59
62

图 5

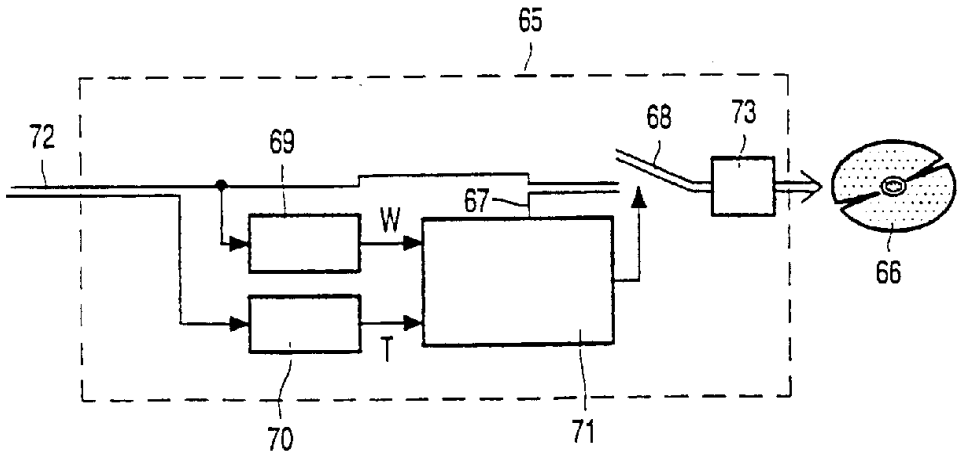

65
72
69
68
73
67
W
66
T
70
71

图 6

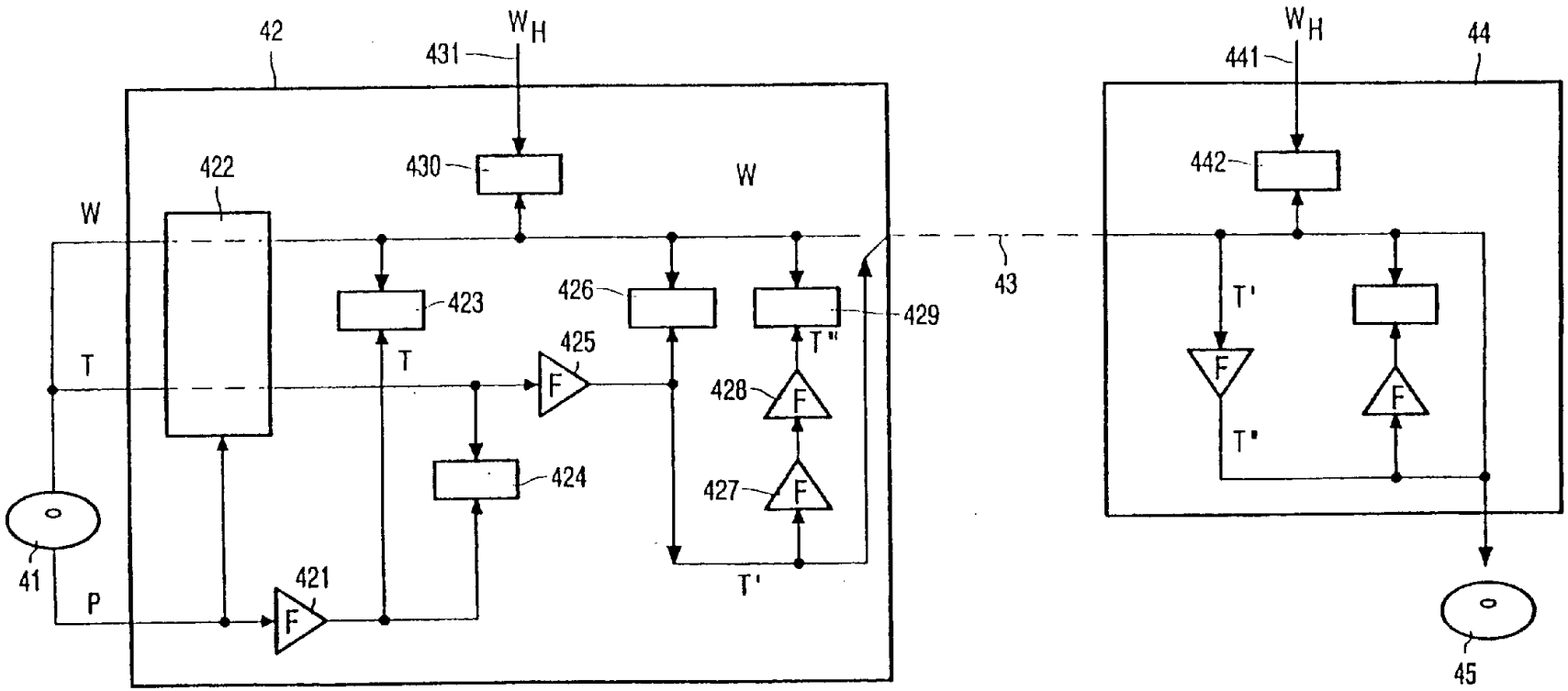

42
W_H
431
430
W
422
W
423
426
429
T"
T
425
T
F
428
F
424
427
F
41
P
421
F
T'
43
44
W_H
441
442
T'
F
T"
F
45

图 4