[19]中华人民共和国专利局

[51]Int.Cl[6]
H04L 9/00

[12] 发明专利申请公开说明书

[21] 申请号 96111260.3

[43]公开日 1997 年 7 月 23 日

[11] 公开号 CN 1155196A

[22]申请日 96.8.30

[30]优先权

[32]95.12.7 [33]JP[31]319421 / 95

[71]申请人 富士通株式会社

地址 日本神奈川

[72]发明人 小川清隆 小桧山清之 秋山良太 饭岛清克

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

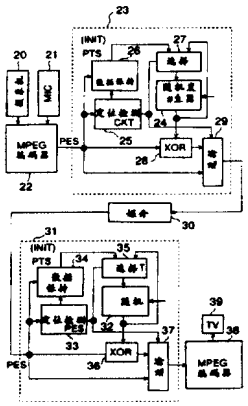
代理人 陆立英

权利要求书 6 页 说明书 37 页 附图页数 13 页

[54]发明名称 高保密性的数据加密与解密

[57]摘要

一个由一串连续数据流单元的数据流构成的数据流加密方法，数据流单元包括一个第一数据流和一个位于第一数据流之后的第二数据流。该加密方法是使用一个随机数发生器对第二数据流加密，并且包括以下步骤，即对每个待加密的第二数据流，加密方法把第一数据流中包含的一个预置不定值数据，提供给随机数发生器作为初始值。还有加密设备，解密方法和解密设备已公开。



权 利 要 求 书

1、一个包含一串连续单元数据流的数据流的加密方法，单元数据流包括一个第一数据流和一个位于第一数据流之后的第二数据流，利用一个随机数发生器（24，45，71，122）对第二数据流加密的加密方法，包括下面这个步骤：

对每个待加密的第二数据流，把第一数据流中所包含的并具有一个不定值的预置数据，提供给随机数发生器作为初始值。

2、权利要求1中的加密方法，特征在于：当第一数据流中不存在预置的数据时，将相应于此不存在预置数据的第一数据流之前的上一个第一数据流的数据的数据提供给随机数发生器作为初始值。

3、权利要求1中的加密方法，特征在于：包含一串连续单元数据流的数据流是由MPEG标准规定的，其第一数据流包含形成数据组标题的数据流，第二数据流包含形成数据组的数据流，以及其中，预置的数据包含了放象时间标记（PTS）。

4、权利要求1中的加密方法，特征在于：包含一串连续单元数据流的数据流是由MPEG标准规定的，其第一数据流包含形成数据组标题的数据流，第二数据流包含形成数据组的数据流，预置的数据包含了程序时钟基准（PCR）。

5、权利要求1中的加密方法，还包含并行转换步骤，用于至少将数据流中单元数据流部分转换成多元数据流，此方法可对每一种多元数据流加密。

6、加密设备提供了包含一串连续单元数据流的数据流，单元数据流包括一个第一数据流和一个位于第一数据流之后的第二数据流，加密设备对第二数据流加密，包括：

一个随机数发生器（24，45，71，122），用于产生随机数；

一个初始值提供电路（25，26，27；46，47，48；72，74，76；125，126，127），对于每个待加密的第二数据流，把包含在第一数据流中的预置不定值数据提供给随机数发生器作为初始值；

一个逻辑操作电路（28，49，77，129），用于将待加密的第二数据流和由随机数发生器产生的随机数进行逻辑操作，以便对第二数据流加密。

7、权利要求6中的加密设备，特征在于：其中，初始值供给电路（25，26，27；46，47，48；72，74，76；125，126，127）当第一数据流中不存在预置的不定值数据时，将相应于此不存在预置的不定值数据的第一数据流之前的上一个第一数据流的预置的不定值数据的数据提供给随机数发生器（24，45，71，122）作为初始值。

8、权利要求6中的加密设备，特征在于：包含一串连续单元数据流的数据流是由MPEG标准规定的，其第一数据流包含形成数据组标题的数据流，第二数据流包含形成数据组的数据流，以及其中，预置的不定数据包含了放象时间标记（PTS）。

9、权利要求6中的加密设备，特征在于：包含一串连续单元数据流的数据流是由MPEG标准规定的，其第一数据流包含形成数据组标题的数据流，第二数据流包含形成数据组的数据流，以及其中，预置的不定数据包含了程序时钟基准（PCR）。

10、权利要求6中的加密设备，其初始值供给电路包含定位检测电路（25，46，72，123），用于检测预置的不定值数据的位置和第二数据流的起始位置；数据保持电路（26，47，74，125）用来保持预置的不定值数据，在定位检测电路检测到预置的不定值数据时，该数据保持电路就保存预置的不定值数据。

11、权利要求6中的加密设备，其加密设备还包含串－并转换器（73），用于将一串连续单元数据流的数据流转换成多元数据流，每个单元数据流包括一个第一数据流和一个位于第一数据流之后的第二数据流；包含随机数发生器，初始值供给电路和将每个多元数据流加密成多元加密数据流的逻辑操作电路。加密设备中还包含并－串转换器（79），用于将多元加密数据流转换成简单的加密数据流。

12、权利要求10中的加密设备，其定位检测电路包含微处理器（123）和存有微处理器控制程序的程序存储器（124），使得定位检

测电路能够对不同格式的多元数据流中任选一个进行加密，如同对数据流加密一样。

13、一个包含一串连续单元数据流的数据流的解密方法，单元数据流包括一个第一数据流和一个位于第一数据流之后的第二数据流，该解密方法利用一个随机数发生器（32，58，83，107，136）对第二数据流解密，包括下面这个步骤：

对每个待加密的第二数据流，把第一数据流中包含的预置的一个不定值数据，提供给随机数发生器作为初始值，以便对第二数据流解密。

14、权利要求13中的解密方法，当第一数据流中不存在预置的不定的数据时，将相应于此不存在预置不定数据的第一数据流之前的上一个第一数据流中的预置不定的数据的数据提供给随机数发生器作为初始值。

15、权利要求13中的解密方法，其中，包含一串连续单元数据流的数据流是由MPEG标准规定的，其第一数据流包含一个形成数据组标题的数据流，第二数据流包含一个形成数据组的数据流，预置的不定的数据包含一个放象时间标记（PTS）。

16、权利要求13中的解密方法，其中，包含一串连续单元数据流的数据流是由MPEG标准规定的，其第一数据流包含一个形成数据组标题的数据流，第二数据流包含一个形成数据组的数据流，预置的不定数据包含一个程序参考时钟（PCR）。

17、权利要求13中的解密方法，包含了并行转换步骤，用于至少将由单元数据流形成的部分数据流转换成多元数据流，此方法可对每一种多元数据流加密。

18、解密设备提供了包含一串连续单元数据流的数据流，单元数据流包括一个第一数据流和一个位于第一数据流之后的第二数据流，解密设备包括：

一个随机数发生器（32，58，83，107，136），用于产生随机数；

一个初始值提供电路（33，34，35；59，60，61；84，86，

88； 137， 139， 140），对每个待解密的第二数据流，把第一数据流中包含的预置的不定值数据提供给随机数发生器作为初始值；

一个逻辑操作电路（36， 62， 89， 110， 143），用于对待解密的第二数据流和由随机数发生器产生的随机数进行操作，以便对第二数据流解密。

19、权利要求18中的解密设备，其中的初始值供给电路（33，34， 35； 59， 60， 61； 84， 86， 88； 137， 139， 140）当第一数据流中不存在预置的不定值数据时，将相应于此不存在预置不定值数据的第一数据流之前的上一个第一数据流的预置不定值数据的数据提供给随机数发生器（32， 58， 83， 107， 136）作为初始值。

20、权利要求18中的解密设备，其中包含一串连续单元数据流的数据流是由MPEG标准规定的，其第一数据流包含一个形成数据组标题的数据流，第二数据流包含一个形成数据组的数据流，预置的数据组包含了放象时间标记（PTS）。

21、权利要求18中的解密设备，包含一串连续单元数据流的数据流是由MPEG标准规定的，其第一数据流包含一个形成数据组标题的数据流，第二数据流包含一个形成数据组的数据流，预置的数据组包含了程序参考时钟（PCR）。

22、权利要求18中的解密设备，其初始值供给电路包含定位检测电路（33， 59， 84， 106， 137），用于检测预置的不定值数据的位置和第二数据流的起始位置；数据保持电路（34， 60， 86， 108， 139），在定位检测电路检测到预置的不定值数据时，该数据保持电路就保存预置的不定值数据。

23、权利要求18中的解密设备，其解密设备中还包含串－并转换器（85），用于将一串连续单元数据流的数据流转换成多元数据流，每个单元数据流包括第一数据流和位于第一数据流之后的第二数据流；包含随机数发生器，初始值供给电路和将每个多元数据流解密成多元解密数据流的逻辑操作电路。解密设备中还包含一个并－串转换器（79），用于将多元解密数据流转换成简单的解密数据流。

24、权利要求22中的解密设备，其定位检测电路包含微处理器（137）和存有微处理器控制程序的程序存储器（138），使得定位检测电路能够对从多元不同格式的数据流中任选一个数据流进行解密，如同对数据流一样进行解密。

25、权利要求18中的解密设备，其解密设备构成一个带有用于存储个人识别数据的存储电路的IC卡（98），此IC卡适合于可分离安装在一个外部设备中，只有当IC卡的识别数据由外部设备认可时，解密设备才允许随机数发生器动作。

26、一种数据传输方法，包括以下若干步骤：

提供一个包含一串连续单元数据流的数据流的加密方法，单元数据流包括一个第一数据流和一个位于第一数据流之后的第二数据流。对每个待加密的第二数据流，加密方法包含一个步骤，把第一数据流中包含的预置的一个不定值数据，提供给随机数发生器（24，45，71，122）作为初始值；

在加密步骤中经由一个媒介将加密数据流传输到终端；

在终端中，对经由一个媒介传递的数据流提供一个解密方法，对每个待解密的第二数据流，解密方法包含一个步骤，把第一数据流中包含的预置的一个不定值数据，提供给随机数发生器（32，58，83，107，136）作为初始值，以便对第二数据解密；

27、一个数据传输系统，用于传输包含一串连续单元数据流的数据流，单元数据流包括一个第一数据流和一个位于第一数据流之后的第二数据流。上述数据传输系统包括：

一个包含加密设备的传输源（23，44，70，118），加密设备包括：一个随机数发生器产生随机数；一个初始值提供电路，对每个待加密的第二数据流，把第一数据流中包含的预置的不定值数据提供给随机数发生器作为初始值；一个逻辑操作电路，用于对待加密的第二数据流和由随机数发生器产生的随机数进行操作，以便对第二数据流加密。传输源将加密设备产生的加密数据流提供给一个媒介；

一个包含解密设备的终端（31，57，82，98，132），对经由

一个媒介传递的加密数据流解密，解密设备包括：一个随机数发生器产生随机数；一个初始值提供电路，对每个包含经由媒介提供的已加密数据流中的待解密的第二数据流，把包含在由一个媒介传递的加密数据流的第一数据流中的预置不定值数据提供给随机数发生器作为初始值；一个逻辑操作电路，用于对待解密的第二数据流和由随机数发生器产生的随机数进行操作，以便对第二数据流解密。

说　明　书

高保密性的数据加密与解密

本发明涉及一种加密（ scrambling ）方法及其装置，一种解密（ descrambling ）方法及其装置和一个数据传输方法及其系统，该系统适合传输符合 MPEG (动态图象专家组) 规定的数据位流(或简化流)。MPEG 标准(后面简称为 MPEG)是数字动态图象编码(压缩)和声音信号编码的一个国际标准，同样也是多路复用与信号分离的国际标准。

图 1.显示了一个传统的数据传输系统。

参照图 1，数据传输系统包括一个摄像机 1 用于获得图象数据，一个麦克风 2 用于获得声音数据。还有一个 MPEG 编码器 3，它把通过摄像机 1 获得的图象数据和通过麦克风 2 获得的声音数据，按时分复用处理过程进行编码以产生符合 MPEG 规格的数据位流。这里产生的数据位流包括一个数据组标题，它包含附加数据；数据位流还包含一个分组数据（ packet data part ），它包含了图象数据和声音数据。

图 1 的传输信息还包含一个加密电路 4，用于对 MPEG 编码器 3 输出的数据流进行加密，这样的数据流就成为一个分组数据已加密流。

加密电路 4 包括一个随机数发生器 5，用于依照一个密钥信号的规定来产生一串随机数；还包括一个异或电路 6，它对 MPEG 编码器 3 输出的分组数据数据流与随机数发生器 5 产生的随机数两者进行异或操作。

加密电路 4 还包括一个选择电路 7，用于对 MPEG 编码器 3 输出的分组数据数据流和异或电路 6 输出的数据流进行有选择的输出，选择电路 7 输出加密电路 4 在传输媒介 8 上的数据流，传输媒介 8 可能是一个物理媒介如一个磁盘或磁带，或者是一个非物理媒介如卫星广播或有线电视广播。

图 1 的系统中还包括一个解密电路 9，它对传输媒介 8 传送的，由加密电路 4 输出的数据流进行解密，使数据流成为其中的分组数据已解密的数据流。

需要注明的是，解密电路 9 包括一个与随机数发生器 5 结构相同的随机数发生器 10，在随机数发生器 5 中使用的密钥信号也同样用于随机数发生器 10。

解密电路 9 还包括一个异或电路 11，它对传输媒介传送的，由加密电路 4 输出的分组数据流和随机数发生器 10 产生的随机数进行异或操作。

解密电路 9 还包括一个选择电路 12，它在传输媒介 8 传送的，由加密电路 4 输出的数据流的组标题和异或电路 11 输出的数据流两者之中有选择地输出其中之一。

解密电路 9 输出的数据流送入一个 MPEG 解码器 13，用来对其中的图象数据和声音数据进行分离，这样解密后的图象数据和声音数据便送入电视接收机 14。

通过利用图 1 的数据传输系统，在传输过程中 MPEG 流的分组数据被加密，这就可以保护数据组不被非法拷贝。

图 1 的系统在图 2 所示的情况下会产生问题。MPEG 编码器 3 输出了包括数据 a1,a2,a3 …… 的一个数据流，同时随机数发生器 5 和 10 输出了随机数 c1,c2,c3 ……。这种情况下，异或电路 6 产生输出为：

$a1 \oplus c1$，$a2 \oplus c2$，$a3 \oplus c3$ ……

上述结果经由选择电路 7 选择后输出到异或电路 11。这样，异或电路 11 产生包括 a1,a2,a3 …… 的数据流。

这种情况下，要想恢复随机数 c1,c2,c3 ……，只需加入另一个异或电路 15，对输入异或电路 11 的数据流与异或电路 11 输出的数据流 a1,a2,a3 …… 两者进行异或操作 $a1 \oplus c1$，$a2 \oplus c2$，$a3 \oplus c3$ …… 即可。

这意味着即便密钥信号秘密保存，图 1 的传输系统仍很容易被非法拷贝随机数发生器 10 产生的随机数。这样，加密的数据组很容易被解

密。

相应地，本发明的总体目标就是提供一个新型有效的数据传输系统和传输方法，从而可以消除前述问题。

本发明的另一个更具体的目标是提供一个加密方法及其装置，一个解密方法及其装置，还有一个数据传输方法和传输系统，在该系统中提高了数据传输的安全性。

本发明的另一个目标是提供一个数据流加密方法，适用于包括一串连续的单元数据流的数据流，单元数据流包括一个第一数据流和一个位于第一数据流之后的第二数据流。第二数据流的加密方法是利用一个随机数发生器，该方法包括下面这个步骤：

把第一数据流中包含的有一个不定数值的预置的数据提供给每个第二数据流用于对其加密，同时也提供给随机数发生器作为初始值。

使用本发明的加密方法时，第一数据流中包含的有一个不定数值的预置的数据作为初始值提供给解密装置中的随机数发生器，以便解密使用。

相应于这一过程，解密一方的随机数发生器使用一个不确定的初始值对第二数据流的每一个解密。这样，分析随机数发生器产生的随机数模式就变得很困难，数据传输的安全性有了很大的提高。

本发明的另一个目标是提供一个加密装置，它适用于包括一串连续的单元数据流的数据流，单元数据流包括一个第一数据流和第一数据流之后的一个第二数据流，加密装置对第二数据流加密，加密装置由以下部分组成：

一个随机数发生器，用于产生随机数；

一个初始值提供电路，为每个第二数据流的加密，把第一数据流中包含的预置不定值数据提供给随机数发生器作为初始值；

还有一个逻辑操作电路，用于对待加密的第二数据流和由随机数发生器产生的随机数进行逻辑操作，以便对第二数据流加密。

使用本发明的加密装置时，使用的解密装置中包括有：一个随机数发生器用于产生随机数；一个初始值提供电路用于提供第一数据流中

包含的有一个不定数值的预置的数据提供给随机数发生器作为初始值；还有一个逻辑操作电路，用于对已加密的第二数据流和由随机数发生器的随机数进行逻辑操作，从而对已加密的第二数据流进行解密。

本发明中，各个第二数据流加密时使用的不定初始值提供给解密一方的随机数发生器，作为解密时的初始值来使用。这样，分析随机数发生器产生的随机数模式就变得很困难，数据传输的安全性有了很大提高。

本发明的另一个目标是提供一个数据流解密方法，这里的数据流包含有一串连续的单元数据流，单元数据流又包含一个第一数据流和紧跟其后的一个第二数据流，第二数据流的解密方法是利用一个随机数发生器，该方法包括下面这个步骤：

对每个待解密的第二数据流，把各个第一数据流中包含的预置的不定的数据值提供给随机数发生器作初始值，以便对每个待解密的第二数据流进行解密。

本发明中，需要注意的是：第二数据流加密时使用的不定初始值提供给解密装置的随机数发生器。这样，分析随机数发生器产生的随机数模式就变得很困难，数据传输的安全性有了很大提高。

本发明的另一个目标是提供一个数据流解密装置，数据流包括一个数据流和紧跟其后的第二数据流两部分。解密装置由以下部分组成：

一个随机数发生器用于产生随机数；

一个初始值提供电路，为了每个待解密的第二数据流，把各个第一数据流中预置的不定值数据提供给随机数发生器作为初始值；

还有一个逻辑操作电路，用于对待解密的第二数据流和随机数发生器产生的随机数进行逻辑操作，以便对第二数据流解密。

本发明中，需要注意的是：各个第二数据流加密时的不定的初始值被提供给解密装置中的随机数发生器。这样，分析随机数发生器产生的随机数模式就变得很困难，数据传输的安全性有很大提高。

本发明的另一个目标是提供数据传输的方法，包括下面的步骤：

对包括一串连续单元数据流的数据流使用加密方法。其中单元数据流包括一个第一数据流和紧跟其后的一个第二数据流。加密方法包括的一个步骤就是提供各个第一数据流中的具有不定数值的预置的数据，为了对各个第二数据流加密，提供给随机数发生器作为初始值；

经过加密步骤后已加密的数据流通过媒介被传送至目的地；

经媒介传送到目的地的数据流被运用解密方法解密。该方法的一个步骤就是对每个待解密的第二数据流，把各个第一数据流中预置的不定数据值提供给随机数发生器作为初始值，以便对各个第二数据流解密。

本发明的数据传输方法中，每个第二数据流各有一个加密用的不定的初始值提供给加密装置的随机数发生器和解密装置的随机数发生器。这样，分析随机数发生器产生的随机数模式就变得很困难，数据传输的安全性有很大提高。

本发明的另一个目的是提供数据传输系统，用于传输包括一串连续单元数据流在内的数据流，单元数据流包括一个第一数据流和紧跟其后的一个第二数据流，上述的数据传输系统由以下部分组成：

一个包括了加密装置的传输源。加密装置包括：一个随机数发生器用于产生随机数；一个初始值提供电路，把各个第一数据流中包含的预置的不同数据提供给随机数发生器作为初始值，用于为各个第二数据流加密；还有一个逻辑操作电路，用于对待加密的第二数据流和由随机数发生器产生的随机数进行逻辑操作，以便对第二数据流加密。传输源把加密装置产生的已加密数据流传送到媒介上；

一个包括了解密装置的目的地。解密装置对通过媒介传送来的已加密数据流解密。解密装置包括：一个随机数发生器用于产生随机数；一个初始值提供电路，把由媒介传送来的已加密流中各个第一数据流包含的预置的不定数据，提供给随机数发生器作为初始值，用于为媒介传送来的各个已加密的第二数据流解密；还有一个逻辑操作电路，用于对已加密的第二数据流和由随机数发生器产生的随机数进行逻辑操作，以便对第二数据流解密。

本发明的传输系统中，每个第二数据流各有一个加密用的不定的初始值提供给加密装置的随机数发生器和解密装置的随机数发生器。这样，分析随机数发生器产生的随机数类型就变得很困难，数据传输的安全性有很大提高。

随后的详细描述和所附图表会使本发明的其它目标和进一步的特点更加清晰明确。

图 1.显示了常规数据传输系统的结构；

图 2.显示了图 1 中常规数据传输系统的操作；

图 3.显示了依照本发明的实施例一的数据传输系统的结构；

图 4.是解释了 MPEG2 - PS 中使用的 PES 数据组的构造的视图；

图 5.是一个流程图，它解释了图 3 的数据传输系统中的加密电路的操作；

图 6.是一个流程图，它解释了图 3 的数据传输系统中的解密电路的操作；

图 7.显示了依照本发明的实施例二的数据传输系统的结构；

图 8.是解释了 MPEG2 - TS 中使用的传输数据组的构造的视图；

图 9.是一个流程图，它解释了图 7 的数据传输系统中的加密电路的操作；

图 10.是一个流程图，它解释了图 7 的数据传输系统中的解密电路的操作；

图 11.显示了依照本发明的实施例三的数据传输系统的结构；

图 12.显示了依照本发明的实施例四的数据传输系统的结构；

图 13.显示了依照本发明的实施例五的数据传输系统的结构。

〖实施例一〗

图 3.显示了依照本发明的实施例一的数据传输系统的结构；

参照图 3，系统包括一个摄像机 20 用于获得图象数据，一个麦克风 21 用于获得声音数据。还有一个 MPEG 编码器 22，它利用时分多路复用技术把通过摄像机 20 得到的图象数据和通过麦克风 21 得到的声音数据多路复合为依照 MPEG2 － PS(程序流)规定的数据位流。

图4.显示了一个按照MPEG2 － PS规定的PES(分组基本数据流)数据组。

参照图4，PES数据组包括一系列PES数据组，每个PES数据组包括一个数据标题和分组数据，数据组标题包括一个32位的数据组启动码，一个16位的数据组长度代码，一个2位代码指定为“10”，一个14位代码用于标志位和控制位，一个8位的PES头长度代码和一个40位的代码用于标志和控制，一个8位码长的PES标题，一个40位的码PTS和DTS数据。另一方面，数据组内的数据可能包含有图象数据和声音数据。

图4中，PTS(放像时间标记)数据代表了再现输出时使用的时间管理信息，每隔700ms加入一条PTS数据。另一方面，DTS(解码时间标记)是解码时使用的时间管理信息。14位的“标志和控制”域中有两位作为“PES加密控制”的代码，它是代表是否有加密控制存在的数据，而一个PTS&DTS标志位则是代表PTS数据是否存在的标志。

重回到图3，系统中还包括一个加密电路23，它通过加密分组数据数据流对MPEG编码器22输出的数据流进行加密。

加密电路23包括一个随机数发生器24和一个定位检测电路25。其中随机数发生器24是一个DES(数据加密标准)型的随机数发生器，它由一个密钥信号指定产生一系列随机数。另一方面，MPEG编码器22输出的数据流提供给定位检测电路25，由定位检测电路25进行各种不同的操作，如检测数据组启动码，确认PES加密控制中的内容，确认PTS&DTS标志位，定位检测DTS，检测分组数据的起始位置等等。

加密电路23还包括有一个数据保持电路26用于保存PTS数据，在加密电路23中数据保持电路26受到控制，当电路25发现PTS的位置，便保留已经定位的PTS数据。

加密电路23还包括一个选择电路27，它把数据保持电路26得到的PTS数据或随机数发生器24产生的随机数有选择地提供给随机数发生器本身。这样，当定位检测电路25发现了待加密的分组数据的起始

位置时，选择电路27就把数据保持电路中的PTS数据提供给随机数发生器24作为初始值。之后，选择电路27受定位检测电路25控制直到分组数据结束，这样随机数发生器24产生的随机数又被反馈到随机数发生器24自身。

需要注意的是，定位检测电路25，数据保持电路26和选择电路27一起在加密电路23中组成了初始值提供电路。

加密电路23还包括一个异或电路28，它为了对分组数据加密，对MPEG编码器22输出的数据流以及随机数发生器24产生的随机数进行异或操作。异或操作的结果是分组数据被加密。

加密电路23还包括一个选择电路29，它有选择地输出由MPEG编码器22输出的数据流和由异或电路28输出的数据流。选择电路29受控于定位检测电路25，这样就可以输出已加密数据流。在已加密数据流中，MPEG编码器22输出的分组数据流已经被加密。

选择电路29输出的数据流提供给媒介30，该媒介可能是一张磁盘，其中存放加密电路23输出的数据流。存于媒介30中的加密电路23输出的数据流随后被解密电路31解密。特别指出的是，解密电路31把从媒介30中读出的数据流转换为已解密流，在已解密流中，被加密流中的加密分组数据已经被解密。

解密电路31也组成了本发明实施例一的一个部分。

需要注意的是，解密电路包括一个与随机数发生器24相同的随机数发生器32，后者使用与前者相同的密钥信号。

解密电路31还包括一个定位检测电路33，通过媒介30传送的加密电路23的输出数据流被提供给定位检测电路33，由它进行各种不同操作，如检测数据组启动码，确认PES加密控制中的内容，确认PTS&DTS标志位，对DTS检测定位，检测分组数据的起始位置等等。

解密电路31还包括有一个数据保持电路34用于保存PTS数据，在解密电路31中数据保持电路34受到控制，当电路33发现PTS的位置，便保持已被定位的PTS数据。

解密电路31还包括一个选择电路35，它把数据保持电路34保持

的PTS数据或随机数发生器32产生的随机数有选择地提供给随机数发生器32本身。这样，当定位检测电路33发现了待解密的分组数据的起始位置时，选择电路35就把数据保持电路34中保持的的PTS数据提供给随机数发生器32作为初始值。之后，直到分组数据结束，选择电路35受定位检测电路33控制，使得随机数发生器32产生的随机数又反馈给随机数发生器32自身。

需要注意的是，定位检测电路33，数据保持电路34和选择电路35一起在解密电路31中组成了初始值提供电路。

解密电路31还包括一个异或电路36，它对经媒介30传送来的已加密的分组数据流以及随机数发生器32产生的随机数进行异或操作。异或操作的结果就是使分组数据被解密。

解密电路31还包括一个选择电路37，它有选择地输出经媒介30传送的数据流或由异或电路36输出的数据流。选择电路37受控于定位检测电路33，这样就可以输出已解密数据流。在已解密数据流中，媒介30提供的分组数据流已被解密。

通过解密电路31解密的数据流和来自选择电路37的输出被送到一个MPEG解码器38中，分离并解码为图象数据流和声音数据流，其中解码后的图象数据和声音数据被送至电视接收机39。

综上所述，由摄像机20获得的图象数据和由麦克风21获得的声音数据通过MPEG编码器22，编码为按照MPEG2 - PS的规定形式的数据流，然后提供给加密电路23。在加密电路23中，数据流被提供给定位检测电路25，数据保持电路26，异或电路28和选择电路29。

图5.显示了参照本发明实施例一的加密电路23的操作流程图，在加密电路23中，同样的操作被重复数次。这样，随后的描述将从选择电路29完成了待加密数据流的输出这一状态开始。

参照图5，定位检测电路25控制了选择电路29，这样从MPEG编码器22传输的数据流就可以被连续输出（第S1步）。这样，加密电路23改变了状态，等待数据组起始代码的输入(第S2步)。

当发现了数据组起始代码的时候，定位检测电路25接下来检查数

据组标题的加密控制信息的内容，辨别该分组数据流是否应被加密(第S3步)。当相关的数据流不是应加密时，操作转回第S2步，定位检测电路25等待下一个数据组起始代码的输入。

当分组数据流应被加密时（第S3步结果为“是”），定位检测电路25辨别数据组标题的PTS&DTS标志位是否是“10”或“11”（第S3步）。换句话说，这一步中检查是否存在PTS数据。

当确认PTS&DTS标志位是“10”或“11”，也就是说PTS数据存在的时候，定位检测电路25发现PTS的位置并使数据保持电路26保留该PTS数据(第S5步)。之后，定位检测电路25等待找到分组数据的起始位置（第S6步)。

相反地，当PTS&DTS标志位不是“10”或“11”，也就是说PTS数据不存在的时候，定位检测电路25等待找到分组数据的起始位置(第S6步)。

在发现了分组数据起始位置的情况下，定位检测电路25控制选择电路27，这样由数据保持电路26保留的PTS数据被提供给随机数发生器24作为初始值。当待加密的数据组标题不存在PTS数据时，此数据组在加密之前的上一个数据组的PTS数据被提供给随机数发生器22作为初始值（第S7步)。当再次出现数据组不存在PTS数据时，则选择更前面的一个数据组的PTS数据，直到数据组含有PTS数据为止。

异或电路28对MPEG编码器22输出流中的待加密分组数据流部分和随机数发生器24产生的随机数进行异或操作。这样，包含有待加密数据的数据流就被加密。

定位检测电路25控制选择电路29，这样异或电路28产生的已加密流就被连续地输出（第S8步)，直到分组数据流结束（第S9步)。这以后，处理过程重返第S1步。

MPEG编码器22的数据流就这样转换为一个已加密数据流，其中的成组数据流已被加密。然后已加密流被存储在媒介30中，必要时提供给解密电路31。

图6.显示了参照本发明实施例一的解密电路31的操作流程图。在

解密电路31中，同样的操作被重复数次。因此，随后的描述将从选择电路37完成了待解密分组数据流输出的状态开始。

参照图6.，定位检测电路33控制选择电路37，这样从媒介30传送来的数据流就被连续地输出（第P1步）。这之后，解密电路31改变了状态，等待数据组启动码的输入（第P2步）。

当发现了数据组启动码的时候，定位检测电路33根据数据组标题的加密控制信息的内容，辨别该分组数据是否应被解密（第P3步）。当相关数据流并未被加密时，操作转回第P2步，定位检测电路33等待下一个数据组启动码的输入。

当分组数据流已被加密而又必须解密时（第P3步结果为“是”），定位检测电路25辨别数据组标题的PTS&DTS标志位是否为“10”或“11”（第P4步）。换句话说，这一步检查是否存在PTS数据。

当确认PTS&DTS标志位是“10”或“11”，也就是说PTS数据存在的时候，定位检测电路33发现PTS的位置并使数据保持电路34保留该PTS数据（第P5步）。之后，解密电路31等待找到分组数据的起始位置（第P6步）。

相反地，当PTS&DTS标志位不是“10”或“11”，也就是说PTS数据不存在的时候，定位检测电路33等待找到分组数据的起始位置（第P6步）。

在发现了分组数据起始位置的情况下，定位检测电路33控制选择电路35，这样由数据保持电路34保留的PTS数据被提供给随机数发生器32作为初始值。当待解密的数据组标题中不存在PTS数据时，此待解密数据组之前的上一个数据组的PTS数据被提供给随机数发生器32作为初始值（第P7步）。当再次出现数据组标题不存在PTS数据时，则选择更前面的一个数据组的PTS数据，直到数据组含有PTS数据为止。

异或电路36对媒介30输出的待解密分组数据流和随机数发生器32产生的随机数进行异或操作。这样，包含有待解密数据的数据流就被解密。

定位检测电路33控制选择电路37，这样异或电路36产生的已解密输出流就被连续地输出(第P8步)，直到分组数据流结束(第P9步)。这以后，处理过程重返第P1步。

由媒介30提供的数据流便转换为一个已解密数据流，其中的成组数据流已被解密。然后，已解密数据流被传输至MPEG解码器38。

在MPEG解码器38中，由解密电路31提供的数据流被分为图象数据流和声音数据流，并且由MPEG解码器38对已分离的图象数据流和声音数据流进一步解码。由MPEG解码器38解码后的图象数据和声音数据被传输至电视接收机39。

在本发明的实施例一中，MPEG编码器22输出的符合MPEG2－PS规格的数据流由加密电路23转换为已加密数据流，数据流中待加密的分组数据被加密。已加密数据流随后经由媒介30提供给解密电路31，解密电路31在数据流解密后把它传送至MPEG解码器38。

这里需要注意的是，为了对各个分组数据加密，加密电路23把包含于各待加密数据组标题的PTS数提供给随机数发生器24作为初始值。当待加密数据组标题不存在PTS数据时，此待解密数据组之前的上一个数据组的PTS数据被提供给随机数发生器24作为初始值。当再次出现数据组标题不存在PTS数据时，则选择更前面的一个数据组的PTS数据，直到数据组含有PTS数据为止。

与上述情况相同，解密电路31为了对各个数据解密，解密电路31把包含于各待解密数据组标题的PTS数据提供给随机数发生器32作为初始值。当待解密数据组标题不存在PTS数据时，此数据组之前的上一个数据组的PTS数据被提供给随机数发生器32作为初始值。当再次出现数据组标题不存在PTS数据时，则选择更前面的一个数据组的PTS数据，直到数据组含有PTS数据为止。

本发明实施例一中的数据传输方法及系统中，为了对各个待加密数据流加密，把其中的数值非常数或不定值的PTS提供给随机数发生器32作为初始值。这样，分析随机数发生器32产生的随机数形式就变得很困难，数据传输的安全性有很大提高。

〖实施例二〗

图 7.表示依照本发明实施例二的数据传输系统的结构。

参照图 7，数据传输系统包括一个摄像机 41 用于获得图象数据，一个麦克风 42 用于获得声音数据。还有一个 MPEG 编码器 43，它对通过摄像机 41 得到的图象数据和通过麦克风 42 得到的声音数据进行编码，并利用时分复用技术把它们多路复用为符合 MPEG2 － TS(传输流)规定的数据位流。

图 8.表示一个符合 MPEG2 － TS 规定的传输数据组。

参照图 8.，传输数据包包括一个标题和一个负载。标题中包括一个 8 位同步代码域，一个 3 位标志域，一个 13 位 PTD 域，一个加密控制代码域，一个适配域控制标志域，一个 4 位循环计数器域，和一个 8 位的适配域长度代码域。其中适配域控制标志可以包括 1 位适配标志或 1 位负载标志。适配标志标明了适配域的存在，而负载标志标明了负载的存在。

另一方面，负载中装有如 A1， B1， A2……的图象数据或声音数据。并包括一个 1 位的标志域，如一个 PCR 标志或一个 OPCR 标志；还包括一个 48 位的 PCR（程序参考时钟）数据域。PCR 数据用于对 STC 信号复位。负载中还包括一个同步信号，它用作 MPEG 编码器 43 的指定时间参考值。通常， PCR 数据每隔 100ms 插入一个。还有，PCR 标志标明 PCR 是否存在。

重回到图 7.，数据传输系统中包括一个加密电路 44，它把 MPEG 编码器 43 中的数据流转换为已加密流，其中数据流中的负载被加密。

加密电路 44 包括一个 DES 型的随机数发生器 45，它依照密钥信号的指令产生一系列随机数；还包括一个定位检测电路 46，它进行各种不同的操作，如检测包括在 MPEG 编码器 45 输出的数据流中的同步字节或代码，确认适配标志位的内容，确认负载标志位的内容，确认 PCR 标志位的内容，检测 PCR 的位置，以及检测负载的起始位置。

数据传输系统还包括一个数据保持电路 47，用来保留 PCR 数据，

当定位检测电路46检测PCR的位置时，数据保持电路47是由定位检测电路46控制的。以便把位置被检测到的PCR数据保存下来。

传输系统还包括一个选择电路48，它有选择地将由数据保持电路47所保持的PCR数据或由随机数发生器45所产生的随机数提供给随机数发生器45本身。应该注意的是，当由位置检测电路46检测待加密的负载的起始位置时，选择电路48将由数据保持电路47所保持的PCR数提供给随机数发生器45作为初始值。其后，选择电路48受位置检测电路46控制，这样使得从随机数发生器45输出的随机数反馈到随机数发生器45，直到负载流的输出结束。

定位检测电路46，数据保持电路47和选择电路48一起组成了加密电路44中的初始值提供电路。

传输系统还包括一个异或电路49，它为了对相应的负载加密，对MPEG编码器43输出的数据流和随机数发生器45产生的随机数进行异或操作。这样，异或电路49对负载数据流进行了加密。

传输系统还包括一个选择电路50，它有选择地输出MPEG编码器43输出的数据流或异或电路49输出的数据流。选择电路50受定位检测电路46控制，这样选择电路输出了已加密数据流，其中MPEG编码器43输出的负载数据流已被加密。

传输系统还包括一个数字调制器51，它用于对选择电路50输出的数据流以及此处加密电路44的输出流进行数字调制；还包括一个上变频器52用于传输数字调制器51的输出；还包括一个传输天线53。

图7.中的传输系统还包括一个接收天线54和一个用于调谐的调谐器55，还有一个数字解调器56用于对调谐器55进行数字解调。

传输系统中还包括一个解密电路57，它对数字解调器56输出的已加密流进行解密，从而使已加密的负载数据流被解密。

解密电路57同样也包括一个与随机数发生器45结构相同的随机数发生器58，它使用的密钥信号与随机数发生器45使用的一样。

解密电路57还包括一个定位检测电路59，它进行各种不同的操作，如检测包含在数字解调器56输出的数据流中的同步字节或代码，

确认适配标志位的内容，确认负载标志位的内容，确认PCR标志位的内容，检测PCR的位置，以及检测负载的起始位置。

解密电路57还包括一个数据保持电路60，用来保留PCR数据，数据保持电路60是由定位检测电路59控制的。一旦定位检测电路59发现PCR的位置，就把被检测到的PCR数据保存下来。

解密电路57还包括一个选择电路61，它有选择地提供数据保持电路60保留的PCR数据或随机数发生器58产生的随机数，当定位检测电路59发现了已加密负载的位置时，选择电路61把数据保持电路60保留的PCR数据提供给随机数发生器58作为初始值。之后，选择电路61受定位检测电路59的控制，这样使得随机数发生器58产生的随机数又反馈给随机数发生器58。

需要注意的是，定位检测电路59，数据保持电路60和选择电路61一起组成了解密电路57的初始值提供电路。

解密电路57还包括一个异或电路62，它对从数字解调器56传送来的已加密负载数据流和随机数发生器58产生的随机数进行异或操作，异或操作的结果是，在异或电路62中已加密流被解密。

解密电路57还包括一个选择电路63，它有选择地输出数字解调器56输出的数据流或异或电路62输出的数据流，选择电路63受定位检测电路59的控制，这样选择电路63输出了已解密数据流，其中数字解调器56输出的已加密负载流被解密。

从选择电路63输出的解密电路57的输出流随后被提供给MPEG解码器64以便对图象数据流和声音数据流进行分离和解码，然后被分离和解调的图象数据和声音数据被送至电视接收机65。

在数据传输系统中，需要注意的是，由摄像机41得到的图象数据和由麦克风42得到的声音数据通过MPEG编码器43，被编码为符合MPEG2－TS规定的数据流，然后被提供给加密电路44。在加密电路44中，数据流被提供给定位检测电路46，数据保持电路47，异或电路49和选择电路50。

图9.表示按照本发明实施例二的加密电路44的操作流程图，在加

密电路 44 中，同样的操作被重复数次。这样，随后的描述将从选择电路 50 完成了待加密负载数据流的输出这一状态开始。

参照图 9，定位检测电路 46 控制选择电路 50，这样从 MPEG 编码器 43 传输过来的数据流就可以被连续输出。这样，定位检测电路 46 处于检测同步字节的状态(第 N1 步)。

当发现了同步字节的时候，在数据组标题所描述的加密控制信息的内容基础上，定位检测电路 46 同样也辨别该负载数据流是否应被加密(第 N2 步)。当相关的数据流不是应加密流时，操作转回第 N1 步，定位检测电路 25 等待下一个同步代码的输入。

当分组数据流应被加密时（第 N2 步结果为“是”），定位检测电路从适配标志上辨别是否有适配域存在（第 N3 步）。

当确认有适配域存在（第 N3 步结果为“是”），定位检测电路通过 PCR 标志位辨别是否有 PCR 存在(第 N4 步)。当有 PCR 存在(第 N4 步结果为“是”)，定位检测电路找到 PCR 的位置并使数据保持电路 47 保留 PCR 数据(第 N5 步)。

定位检测电路 46 还需要从负载标志位辨别是否有负载存在。如果有负载存在（第 N6 步结果为“是”），定位检测电路 46 就等待直到发现负载的起始位置（第 N7 步）。当没有负载时（第 N7 步结果为“否”），定位检测电路 46 的操作转回第 N1 步。

当第 N3 步中经辨别没有适配域存在或第 N4 步中没有 PCR 存在，操作过程转到第 N6 步。

在发现了负载起始位置的情况下，定位检测电路 46 控制选择电路 48，使得数据保持电路 47 保持 PCR 数据，也就是说，待加密负载的数据组标题中的 PCR 数据直接被提供给随机数发生器 48 作为初始值（第 N8 步）。当待加密的数据组标题不存在 PCR 数据时，此数据组之前的上一个数据组的 PCR 数据被提供给随机数发生器 45 作为初始值（第 N8 步）。当再次出现被选择的分组数据中不存在 PCR 数据时，则选择更前面的一个负载的 PCR 数据，直到负载含有 PCR 数据为止。

异或电路 49 对待加密分组数据流部分的 MPEG 编码器 43 输出流

和随机数发生器45产生的随机数进行异或操作。这样，包含有待加密的负载的数据流就被加密。

定位检测电路46控制选择电路50，这样异或电路49产生的已加密流就被连续地输出（第N9步），直到负载输出结束（第N10步）。这以后，处理过程重返第N1步。

MPEG编码器43产生的输出数据流就这样转换为一个已加密数据流，其中的成组数据流已被加密。然后已加密流通过数字调制器51，上变频器52，天线53和54，和数字解调器56被传送至解密电路57。

图10.显示了参照本发明实施例二的解密电路57的操作流程图，在解密电路57中，同样的操作被重复数次。这样，随后的描述将从选择电路63完成了待解密分组数据流的输出这一状态开始。

参照图10，定位检测电路59控制了选择电路63，这样从数字解调器56传输过来的数据流就可以被连续输出(第Q1步)。这样，定位检测电路53被置为监测同步字节的状态。

当发现了同步字节的时候，在数据组标题所描述的加密控制信息的内容的基础上，定位检测电路59同样也辨别该负载数据流是否应被解密(第Q2步)。当相关的数据流不是应解密流时，操作转回第Q1步，定位检测电路59等待下一个同步字节的输入。

当负载数据流应被解密时（第Q2步结果为“是”），定位检测电路59从适配标志上辨别是否有适配域存在（第Q3步）。

当确认有适配域存在（第Q3步结果为“是”），定位检测电路59通过PCR标志位辨别是否有PCR存在(第Q4步)。当有PCR存在(第Q4步结果为“是”），定位检测电路59找到PCR的位置并使数据保持电路60保留PCR数据(第Q5步)。

之后，定位检测电路59还需要从负载标志位判断是否有负载存在（第Q6步），如果有负载存在（第Q6步结果为“是”），定位检测电路59等待直到发现负载的起始位置（第Q7步）。当没有负载时（第Q7步结果为“否”），处理过程转回第Q1步。

当第Q3步中经辨别没有适配域存在（第Q3步结果为“否”），或

第 Q4 步中没有 PCR 存在（第 Q4 步结果为“否”)时，操作过程转到第 Q6 步。

在第 Q7 步后发现了负载起始位置的情况下，定位检测电路 59 控制选择电路 61，使得数据保持电路 60 保持 PCR 数据，也就是说，待解密负载中的 PCR 数据被提供给随机数发生器 58 作为初始值。当待解密的负载数据组标题不存在 PCR 数据时，此数据组之前的上一个负载的 PCR 数据被直接提供给随机数发生器 58 作为初始值（第 Q8 步）。当再次出现分组数据标题中不存在 PCR 数据时，则选择更前面的一个负载，直到碰到含有 PCR 数据的负载为止。

异或电路 62 对待解密负载数据流部分的数字解调器 56 的输出流和随机数发生器 58 产生的随机数进行异或操作。这样，包含有负载的数据流就被解密。

因此，位检测电路 59 控制选择电路 63，这样异或电路 62 产生的已解密流就被连续地输出（第 Q9 步），直到负载输出结束（第 Q10 步）。这以后，处理过程重返第 Q1 步。

由解调器 56 输出的数据流便通过解密电路 57 转换为一个已解密数据流，这样负载数据流在解密电路 57 中已被解密。然后，已解密数据流被传输至 MPEG 解码器 64。

在 MPEG 解码器 64 中，图象数据流和声音数据流从解码数据流中分离出来并被解码，解码后的图象数据和声音数据被传输至电视接收机 65。

在本发明的实施例二的数据传输系统和方法中，MPEG 编码器 43 输出的符合 MPEG2 － TS 规格的数据流由加密电路 44 转换为已加密数据流，数据流中的负载流被加密。已加密数据流随后被提供给解密电路 57，数据流解密后把它传送至 MPEG 解码器 64。

在加密电路 44 中，把包含于待加密负载数据组标题的 PCR 数提供给随机数发生器 45 作为初始值。当待加密负载数据组标题不存在 PCR 数据时，在待加密负载之前的负载分组数据标题中的 PCR 数据被提供给随机数发生器 45 作为初始值。当选择的负载分组数据标题中仍不存

在 PCR 数据时，选择更前面一个负载，直到遇到包含 PCR 数据的负载。

解密电路 57 为了对各个数据解密，把包含于各待解密负载数据组标题的 PCR 数据提供给随机数发生器 58 作为初始值。当待解密负载数据组标题不存在 PCR 时，此数据组之前的上一个负载的 PCR 数据立即被提供给随机数发生器 58 作为初始值。当再次出现数据组标题不存在 PCR 数据时，则选择更前面的一个负载的 PCR 数据，直到负载含有 PCR 数据为止。

本发明实施例二中的数据传输方法及系统中，为了对各负载流解密，提供给解密电路 57 中的随机数发生器 58 的 PCR 的数据不是常数。这样，分析随机数发生器 58 产生的随机数型式就变得很困难，数据传输的安全性有很大提高。

本实施例中，可以用循环计数器的值代替 PCR 数据作为初始值提供给随机数发生器 45 和 58，还可以使用将 PCR 与循环计数器值组合起来所产生的数据。另一种选择是，通过对包含 PCR 数据与循环计数器值进行的操作来得到初始值。

〖实施例三〗

图 11.显示了依照本发明实施例三的数据传输系统的结构。

参照图 11，数据传输系统包括一个摄像机 67 用于获得图象数据，一个麦克风 68 用于获得声音数据。还有一个 MPEG 编码器 69，它对通过摄像机 67 得到的图象数据和通过麦克风 68 得到的声音数据进行编码，并利用时分多路复用技术把它们多路复合为依照 MPEG2 - PS 规定的数据位流。

在图 11.中，数据传输系统中包括一个加密电路 70，它把 MPEG 编码器 69 中的数据流转换为已加密流，数据流中的分组数据被加密。

加密电路 70 包括一个随机数发生器 71 和一个定位检测电路 72，随机数发生器 71 是一个 DES（数据加密标准）型的随机数发生器，它依照密钥信号的指令产生一系列随机数。另一方面 MPEG 编码器 69 输出的数据流提供给定位检测电路 72，定位检测电路 72 还进行各种

不同的操作，如发现数据组起始代码，确认PES加密控制的内容，确认PTS&DTS标志位，定位检测PTS，发现分组数据的起始位置等等。

加密电路70包括一个串－并转换器73，它对MPEG编码器69输出的数据流进行并行转换后变为64位并行数据流。加密电路70还包括一个40位的寄存器74用于保存PTS数据。当定位检测电路72检测PTS的位置时寄存器74受定位检测电路72控制，这样使得寄存器74保存由串－并转换器73输出的PTS数据。

加密电路70还包括一个64位的寄存器75，寄存器75受控于定位检测电路72并保存待加密的分组数据流。

加密电路70还包括一个选择电路76，它把寄存器74保留的PTS数据或随机数发生器71产生的随机数有选择地提供给随机数发生器71本身。这样，当定位检测电路72发现了待加密的分组数据的起始位置时，选择电路76就把寄存器74中的PTS数据提供给随机数发生器71作为初始值。之后，选择电路76受定位检测电路72控制直到分组数据结束，这样随机数发生器71产生的随机数又被重输入随机数发生器71自身。

需要注意的是，定位检测电路72，寄存器74和选择电路76一起在加密电路70中组成了初始值提供电路。

加密电路70还包括一个异或电路77，它对寄存器75输出的并行数据流及随机数发生器71产生的随机数进行异或操作。异或操作的结果就是使分组数据被加密。

加密电路70还包括一个64位寄存器用于在定位检测电路72的控制下存储异或电路77输出的并行数据流。加密电路70还包括一个并－串转换器79用于把寄存器78输出的并行数据流转换为串行数据流。

加密电路70还包括一个选择电路80，它有选择地输出由MPEG编码器69输出的数据流或由并－串转换器79输出的数据流。选择电路80受控于定位检测电路72，这样就可以输出已加密数据流。在已加密流中，MPEG编码器69输出的分组数据流已经被加密。

选择电路 80 输出的数据流提供给媒介 81，该媒介可能是一张磁盘，其中存有加密电路 70 输出的数据流。存于媒介 81 中的加密电路 70 输出的数据流随后被解密电路 82 解密。特别指出的是，解密电路 82 把从媒介 81 中读出的数据流转换为已解密流，在已解密流中，被加密流中的加密分组数据已经被解密。

需要注意的是，解密电路 82 包括与随机数发生器 71 相同的一个随机数发生器 83，并使用与随机数发生器 71 相同的密钥信号。

解密电路 82 还包括一个定位检测电路 84，通过媒介 81 传送来的加密电路 70 的输出数据流被提供给定位检测电路 84，由它进行各种不同操作，如检测数据组启动码，确认 PES 加密控制中的内容，确认 PTS&DTS 标志位，对 PTS 定位检测，检测分组数据的起始位置等等。

解密电路 82 还包括一个串－并转换器 85，它对媒介 81 输出的串行数据流进行串－并转换，使之成为 64 位宽的并行数据流。解密电路 82 还包括一个 40 位宽的寄存器 86 用于保存 PTS 数据。当定位检测电路 84 发现并定位了 PTS 时寄存器 86 受控于定位检测电路 84，这样使得寄存器 86 保存串－并转换器 85 输出的 PTS 数据。

解密电路 82 还包括一个另一个 64 位的寄存器 87，它受控于定位检测电路 84 并保存待解密的分组数据。

解密电路 82 还包括一个选择电路 88，它把寄存器 86 保存的 PTS 数据或随机数发生器 83 产生的随机数有选择地提供给随机数发生器 83 本身。这样，当定位检测电路 84 发现了待加密的分组数据的起始位置时，选择电路 88 就把寄存器 86 中的 PTS 数据提供给随机数发生器 83 作为初始值。之后，选择电路 88 受定位检测电路 84 控制直到分组数据结束，这样随机数发生器 83 产生的随机数又被反馈到随机数发生器 83 自身。

需要注意的是，定位检测电路 84，寄存器 86 和选择电路 88 一起在解密电路 82 中组成了初始值提供电路。

解密电路 82 还包括一个异或电路 89，它对寄存器 87 提供的待解密分组数据流以及随机数发生器 83 产生的随机数进行异或操作。异或

操作的结果就是使分组数据被解密。

解密电路82还包括一个64位结构的寄存器90用于在定位检测电路84的控制下存储异或电路89输出的并行数据流。解密电路82还包括一个并－串转换器91用于把寄存器90输出的并行数据流转换为串行数据流。

解密电路82还包括一个选择电路92，它有选择地输出媒介81输出的数据流或由并－串转换电路91输出的数据流。选择电路92受控于定位检测电路84，这样就可以输出已解密数据流。在已解密流中，媒介81输出的分组数据流已经被解密。

通过解密电路82解密的数据流从选择电路92输出到一个MPEG解码器93中，经过分离解码为图象数据流和声音数据流，其中解码后的图象数据和声音数据被送至电视接收机94。

在该数据传输系统中，由摄像机67获得的图象数据和由麦克风68获得的声音数据通过MPEG编码器69，编码为按照MPEG2 - PS的规定形式的数据流，然后提供给加密电路70。在加密电路70中，数据流被提供给定位检测电路72，串－并转换器73和选择电路80。

操作中，当发现了数据组起始代码的时候，定位检测电路72就在数据组标题所描述的加密控制信息的内容基础上，辨别该分组数据的数据流是否应被加密。当相关的数据流不是应加密流时，操作返回等待数据组起始代码输入的状态。

当分组数据流应被加密时，定位检测电路72辨别数据组标题的PTS&DTS标志位是“10”还是“11”。换句话说，这一步中检查是否存在PTS数据。

当确认PTS&DTS标志位是“10”或“11”，也就是说确认PTS数据存在的时候，定位检测电路72发现PTS的位置并使寄存器74保留该PTS数据。之后，加密电路70等待找到分组数据的起始位置。

相反地，当PTS&DTS标志位不是“10”或“11”，也就是说PTS数据不存在的时候，定位检测电路72继续检测分组数据的起始位置。

在发现了分组数据起始位置的情况下，定位检测电路72控制选择

电路 76，这样由寄存器 74 保留的 PTS 数据被提供给随机数发生器 71 作为初始值。当待加密的数据组标题不存在 PTS 数据时，此数据组之前的上一个数据组的 PTS 数据立即被提供给随机数发生器 71 作为初始值。当再次出现数据组标题不存在 PTS 数据时，则选择更前面的一个数据组的 PTS 数据，直到数据组含有 PTS 数据为止。然后，由串－并转换器 73 输出的数据流被寄存器 75 保存。

异或电路 77 对寄存器 75 输出流中的待加密分组数据流部分和随机数发生器 71 产生的随机数进行异或操作。这样，包含有待加密数据的数据流就被加密。加密后的数据流被存入寄存器 78，寄存器 78 输出的并行数据流又通过并－串转换器 79 转换为串行数据流。

定位检测电路 72 控制选择电路 80，使得连续地输出并－串转换器 79 的加密输出数据流，直到分组数据结束。也可以在加密数据流输出结束之后输出 MPEG 编码器 69 的输出。

因此，MPEG 编码器 69 的输出数据流被转换成加密数据流，流中分组数据流被加密，随后加密数据流被存储在媒介 81 内。在需要的时候存储在媒介 81 中的数据流提供给解密电路 82。

在解密电路 82 中，媒介 81 来的数据流传送给定位检测电路 84，串－并转换器 85 和选择电路 92。

在解密电路中，当数据启动码被检测到时，根据数据组标题加密控制信息的内容，由定位检测电路 84 确定是否对分组数据流进行解密操作。当相关的数据流不需解密时，操作回到等待数据组启动码输入的状态。

当分组数据流已被加密时，定位检测电路 84 辨别数据组标题的 PTS&DTS 标志位是不是“10”或“11”。换句话说，在这一步骤中检测 PTS 数据的存在。

当确定了 PTS&DTS 标志位是“10”或“11”，或者说，当确定了 PTS 数据存在，定位检测电路 84 检测 PTS 的位置，并使寄存器 86 保持 PTS 数据。之后，解码电路 82 等待检测数据组起始位置。

反之，当 PTS&DTS 标志并非“10”或“11”，或者说，当 PTS

数据不存在，定位检测电路84就继续检测分组数据起始位置。

当检测分组数据起始位置时，定位检测电路84控制选择电路88使得寄存器86保持的PTS数据供给随机数发生器83作为初始值。当需要解密的数据组标题不存在PTS数据时，此数据组之前的上一个数据组的PTS数据立即被提供给随机数发生器83作为初始值。当再次出现数据组标题不存在PTS数据时，则选择更前面的一个数据组的PTS数据，直到数据组含有PTS数据为止。此外，串－并转换器85的输出数据流由寄存器87保持。

异或电路89对含有加密数据组部分的寄存器87的输出数据和随机数发生器83输出的随机数进行异或操作。于是，包含数据组的加密数据流被解密。

定位检测电路84控制选择电路92，使得并－串转换器91连续输出解密数据流，直到分组数据的数据流结束。随后，选择电路92可被控制为使得来自媒介81的数据流按原样输出。

于是，由媒介81提供的数据被转换成解密数据流，流中数据组被解密，解密数据流传送到MPEG解码器93。在MPEG解码器93内，从解密电路82送来的数据流中，图象数据流和声音数据流被分离，并由MPEG解码器93进一步将分离的图象数据流和声音数据流解码。被MPEG解码器93解码的图象数据和声音数据被传送给电视接收机94。

根据本发明实施例一，MPEG编码器69以MPEG2-PS-规定的格式输出的数据流由加密电路70转换成加密数据流，使得含有待加密数据组的数据流被加密。加密数据流经媒介81提供给解密电路82，由解密电路82在解密后传送给MPEG解码器93。

这里，需要注意的是对于每个待加密数据组，加密电路70提供包含在待加密数据组标题内的PTS数据，作为随机数发生器71的初始值。当待加密的数据组标题不存在PTS数据时，此数据组之前的上一个数据组的PTS数据被立即提供给随机数发生器83作为初始值。当再次出现数据组标题不存在PTS数据时，则选择更前面的一个数据组的

PTS 数据，直到数据组含有 PTS 数据为止。

为适应上述事项，解密电路 82 实现解密操作，对于每个待解密数据组数据，解密电路 82 提供包含在待解密数据组标题的 PTS 数据，作为随机数发生器 83 的初始值。当待解密的数据组标题不存在 PTS 时，此数据组之前的上一个数据组的 PTS 数据被立即提供给随机数发生器 83 作为初始值。当再次出现数据组标题不存在 PTS 数据时，则选择更前面的一个数据组的 PTS 数据，直到数据组含有 PTS 数据为止。

根据本发明实施例三中的数据传输方法和系统，对于每个数据组已加密的数据流，提供给解密电路 82 的随机数发生器 83 的 PTS 的数据的值不固定，也不是常数。因此，分析由随机数发生器 83 生成的随机数模式明显变得困难，数据传输的保密性有显著改进。

实施例四

图 12 展示了本发明实施例四的实现数据传输方法的数据传输系统。

参考图 12，数据传输系统包括一台个人电脑 97 和一块符合 PCMCIA2.0 标准的 PCMCIA（个人电脑存储卡国际联盟）卡。

个人电脑 97 包括一个 CPU（中央处理单元）99，一个存储器 100，一条总线 101 和一个 PCMCIA 接口 102。

详细来讲，个人电脑 97 包含了带有一张磁盘 104 的磁盘驱动器 103。磁盘 104 存有数据组被加密的加密状态中的 MPEG2-PS 数据流。

图 12 的系统还包括了定位检测电路 106，磁头机构读出的数据流提供给它和进行其它一些操作。例如，检测数据组启动码，确定 PES 加密控制的内容，确定 PTS&DTS 标志位，定位检测 PTS，以及检测数据组起始位置等等。

PCMCIA 卡 98 还包括用来通过密钥信号产生随机数序列的随机数发生器 107 和保持 PTS 数据的数据保持电路 108。数据保持电路 108 用于当定位检测电路 106 检测出 PTS 数据时，保持其位置被检测到的 PTS 数据。

PCMCIA 卡 98 还包含选择电路 109，以便有选择地将由数据保持电路 108 所保持的 PTS 数据或随机数发生器 107 输出的随机数，提供给随机数发生器 107 本身。因此，选择电路 109 在定位检测电路 106 检测到待加密数据组起始位置时将数据保持电路 108 的 PTS 数据作为初始值提供给随机数发生器 107 。此后，由定位检测电路 106 控制选择电路 109，直到数据组结束。使得随机数发生器 107 产生的随机数被反馈给随机数发生器 107，

PCMCIA 卡 98 还包含一个异或电路 110，该电路对来自磁头机构的待加密的数据组的输出数据流和随机数发生器 107 产生的随机数进行异或操作。异或操作的结果是数据组的数据流被解密。

PCMCIA 卡 98 还包含在磁头机构 105 输出数据流和异或电路 110 输出数据流之间进行有选择的输出的选择电路 111 。由定位检测电路 106 控制选择电路 110 使得输出为解密数据流。在解密流中，由磁头机构输出数据流的加密数据被解密。

此外， PCMCIA 卡还包括存储用于识别用户的 ID 数据的存储设备 112，以及与存储装置 112 协同操作、阅读并输出 ID 数据的处理电路 113 等等。

需注意的是，根据本发明实施例四，定位检测电路 106 和 PCMCIA 卡 98 一起构成了解密电路。

还需注意的是，定位检测电路 106，数据保持电路 108 和选择电路 109 一起构成了解密电路的初始值供给电路。

定位检测电路 106 可装在 PCMCIA 卡 98 内，但最好装入个人电脑 97 中以便减少 PCMCIA 卡 98 的输入输出管脚。

应注意的是，个人电脑 97 包含 MPEG 解码器 114，它从选择电路 111 的数据流输出中分离并解码图象数据流和声音数据流，以便恢复图象数据和声音数据。

个人电脑还包含从 MPEG 解码器 114 接受图象数据的显示装置和从 MPEG 解码器 114 接受声音数据的扬声器。

在图 12 数据传输系统中，当 PCMCIA 卡 98 被插入个人电脑后，

无论CPU99是否决定接受ID数据，它都驱动PCMCIA卡98输出ID数据。如果结果是“是”，则CPU99使处理单元113产生一个密钥，此密钥与磁盘104中数据加密时使用的密钥相同。随后，随机数发生器107产生一串与加密时一样的随机数序列。

在磁盘驱动器103动作时，存于磁盘104中的数据流被磁头机构105读出并传送给定位检测电路106、PCMCIA卡98的数据保持电路108、异或电路110和选择电路111。

在解密电路中，当数据启动码被检测到时，根据数据组标题加密控制信息的内容，由定位检测电路106确定是否对分组数据流进行解密操作。当相关的数据流不需解密时，操作回到等待输入数据组启动码的状态。

另一方面，当数据组的数据流需解密时，定位检测电路106辨别数据组标题的PTS&DTS标志位是不是“10”或“11”。换句话说，即在这一步骤中检查PTS数据的存在性。

当确定了PTS&DTS标志位是“10”或“11”，或者说，当确定了PTS数据存在，定位检测电路106就检测PTS的位置，并使数据保持电路108保持PTS数据。之后，定位检测电路106处于等待检测数据组起始位置的状态。

反之，当PTS&DTS标志并非“10”或“11”，或者说，当PTS数据不存在时，定位检测电路106就继续检测分组数据起始位置。

当检测分组数据起始位置时，定位检测电路106控制选择电路109使得数据保持电路108保持的PTS数据供给随机数发生器107作为初始值。当需要解密的数据组标题不存在PTS数据时，此数据组之前的上一个数据组的PTS数据被立即提供给随机数发生器107作为初始值。当再次出现数据组标题不存在PTS数据时，则选择更前面的一个数据组的PTS数据，直到数据组含有PTS数据为止。

异或电路110对含有解密数据组部分的磁头机构105的输出数据和随机数发生器107输出的随机数进行异或操作。于是，包含待解密的数据组的数据流被解密。

定位检测电路106控制选择电路111，使得异或电路110连续输出解密数据流，直到分组数据的数据流结束。随后，来自磁头机构105的数据流按原样输出。

于是，由磁头机构105提供的加密数据被转换成解密数据流，流中数据组被解密，解密数据流传送到MPEG解码器114。

在MPEG解码器114内，从PCMCIA卡98送来的数据流中，图象数据流和声音数据流被分离，并由MPEG解码器114进一步将分离的图象数据流和声音数据流解码。被解码的图象数据和声音数据被传送给显示装置115和扬声器116。

于是，根据本发明实施例四的数据传输系统和方法，从磁盘104读出的以MPEG2-PS-规定为格式的加密数据流被包含定位检测电路106和PCMCIA卡98的解密电路解密。

这里，需要注意的是对于每个待解密数据组，包含定位检测电路106和PCMCIA卡98的解密电路通过提供包含在待加密数据组标题的PTS数据作为随机数发生器107的初始值来解密。当待解密的数据组标题不存在PTS数据时，此数据组之前的上一个数据组的PTS数据被立即提供给随机数发生器107作为初始值。当再次出现数据组标题不存在PTS数据时，则选择更前面的一个数据组的PTS数据，直到数据组含有PTS数据为止。

根据本发明实施例四的数据传输方法和系统，对于每个数据组加密的数据流，提供给PCMCIA卡98中随机数发生器107的PTS的数据的值不固定，也不是常数。因此，分析由随机数发生器107生成的随机数模式明显变得困难，数据传输的保密性有显著改进。

进一步地，可以制造含有记帐信息的PCMCIA卡。这样，就可以为读出磁盘104的信息计费。

〖实施例五〗

图13表示根据本发明实施例五，实现一种数据传输方法的数据传输系统。

参考图 13，该系统包含一个 MPEG 编码器 117，通过按时分复用处理，对摄像机获得的图象数据和麦克风获得的声音数据进行编码以产生符合 MPEG2-PS 或 MPEG2-TS 规格的数据位流。

图 13 的传输系统还包含一个加密电路 118，用于将 MPEG 编码器 117 输出的数据流转换成加密数据流，其中分组数据的数据流被加密。

请注意，在前面的实施例中，加密电路 118 用于加密数据流。

加密电路 118 包含缓冲存储器 119 用于存储 MPEG 解码器 117 的输出数据流，一个存储器控制器 120，用于控制缓冲存储器 119 和总线 121。

加密电路 118 还包括一个随机数发生器 122 和一个定位检测电路 123，其中 DES（数据加密标准）型随机数发生器 122 用于产生依照一个密钥信号规定的一串随机数。另外，定位检测电路 123 由封装成集成电路形式的 CPU 构成，CPU123 执行了一系列操作，例如检测数据组启动码，确定 PES 加密控制的内容，确定 PTS&DTS 标志位，定位检测 PTS，以及对 MPEG2-PS 数据流检测数据组起始位置。对于 MPEG2-TS 数据流，定位检测电路 123 执行的操作有检测同步位，确定适配标志位内容，确定负载标志位内容，确定 PCR 标志位内容，检测 PCR 位置，检测负载起始位置等等。

加密电路 118 还包含存有程序的程序存储器 124，它依靠 MPEG 解码器 117 的数据流是否是 MPEG-PS 或 MPEG-TS 来切换 CPU123 的操作。

加密电路 118 还包含数据寄存器 125，用来保存供给随机数发生器 122 用的初始值。因此，当 MPEG 编码器 117 输出数据流是 MPEG2-PS 时数据寄存器 125 保存 PTS 数据，当 MPEG 编码器 117 输出数据流是 MPEG2-TS 时数据寄存器 125 保存 PCR 数据，

加密电路 118 还包含选择电路 126 和控制选择电路 126 操作的控制寄存器 127，选择电路 126 从数据寄存器 125 保存的数据或随机数发生器 122 输出的随机数中进行选择并供给随机数发生器 122 自身。

因此，当 CPU123 检测到待加密的数据组或负载的起始位置时，

将数据寄存器 125 保存的数据作为初始值提供给随机数发生器 122。随后，直到数据组或负载结束，选择电路 126 由控制寄存器 127 的输出控制，使得随机数发生器 122 产生的随机数反馈给随机数发生器 122。

加密电路 118 还包含存放缓冲存储器 119 输出数据流的数据寄存器 128 和异或电路 129，后者对数据寄存器 128 输出的待加密数据流和随机数发生器 122 产生的随机数提供异或操作。异或操作的结果是数据组的数据流被加密。

加密电路还包含选择电路 130，它对数据寄存器 128 和异或电路 129 的输出数据流有选择地输出。受控的选择电路 130 使数据组或负载的加密数据流被输出。在加密数据流中，从数据寄存器 128 来的数据组或负载数据流被加密。

选择电路 130 的输出数据流被送入媒介 131，它也许是一张磁盘。在媒介中存储了加密电路 118 的输出数据流。

存储在媒介 131 中的加密电路 118 的输出数据流被解密电路 132 解密。

尤其是，解密电路 132 包含缓冲存储器 133，用于存储媒介 131 的输出数据流，一个存储器控制器 134，用于控制缓冲存储器 133 和总线 135。

解密电路 132 还包括与随机数发生器 122 结构相同的随机数发生器 136，并且使用了与随机数发生器 136 中完全相同的密钥信号。

解密电路 132 还包括了定位检测电路 137。定位检测电路 137 中提供了 CPU 并执行一系列操作。例如对于 MPEG2-PS 数据流，检测数据组启动码，确定 PES 加密控制的内容，确定 PTS&DTS 标志位，定位检测 PTS，以及检测数据组起始位置等等。另一方面，若提供给定位检测电路 137 的是 MPEG2-TS 数据流，定位检测电路 137 就执行以下操作，例如检测同步位，确定适配标志位内容，确定负载标志位内容，确定 PCR 标志位内容，检测 PCR 位置，检测负载起始位置等等。

解密电路 132 还包含了依靠 MPEG 解码器 117 的数据流是否是

MPEG-PS 或 MPEG-TS 来切换 CPU123 的操作的程序存储器 138。

加密电路 118 还包含数据寄存器 139，用来保存供给随机数发生器 136 使用的初始值。当媒介 131 来的数据流是 MPEG2-PS 数据流时，数据寄存器 125 保存 PTS 数据，当 MPEG 编码器 117 输出数据流是 MPEG2-TS 数据流时，数据寄存器 125 保存 PCR 数据。

解密电路 132 还包含选择电路 140，在控制选择电路 140 操作的选择控制寄存器 141 控制下，选择电路 126 从数据寄存器 139 保存的数据或随机数发生器 136 输出的随机数中进行选择并供给随机数发生器 136 自身。

这里要注意的是，选择电路 140 使得数据寄存器 139 将初始值送入随机数发生器 136 来响应由 CPU137 对加密数据组或负载的检测。选择电路 140 由选择控制寄存器 141 的输出来控制，使得随机数发生器 136 产生的随机数反馈给随机数发生器 136 自身，直到数据组或负载数据流结束。

解密电路 132 还包含一个存放缓冲存储器 133 输出数据流的数据寄存器 142 和一个异或电路 143，后者对数据寄存器 142 输出的数据流和随机数发生器 122 产生的随机数提供异或操作。异或操作的结果是数据组的加密数据流被解密。

解密电路 132 还包含一个选择电路 144，它对数据寄存器 142 和异或电路 143 的输出数据流进行选择输出。选择电路 144 被控制使得解密数据流被输出，即从数据寄存器 142 来的数据流中数据组或负载被解密。

由解密电路 132 解密的数据流输入 MPEG 卡 145 进行图象数据和声音数据的解码和分离。解码后的图象和声音数据送入电视接收机 145。

在这样的数据传输系统中，摄像机来的图象数据和麦克风来的声音数据由 MPEG 编码器 117 编码成为 MPEG2-PS 或 MPEG2-TS 形式，其中被编码的数据流被送入加密电路 118。

在加密电路 118 中，数据流存入缓冲存储器 119 并由 CPU123 读

出。

当 MPEG 编码器 117 的输出是 MPEG2-PS 数据流，CPU123 执行一系列操作。例如检测数据组启动码，确定 PES 加密控制的内容，确定 PTS&DTS 标志位，定位检测 PTS，以及检测数据组起始位置等等。

当 CPU123 检测到数据启动码时，根据数据组标题加密控制信息的内容，辨别分组数据流是否被加密。当数据流不需加密时，CPU123 回到检测数据组启动码的状态。

当分组数据流待加密时，CPU123 辨别数据组标题的 PTS&DTS 标志位是不是“10”或“11”。换句话说，在这一步骤中检测 PTS 数据的存在。

当确定了 PTS&DTS 标志位是“10”或“11”，或者说，当确定了 PTS 数据存在，CPU123 检测 PTS 的位置，并使寄存器 125 保持 PTS 数据。之后，CPU123 设定为等待检测数据组起始位置的状态。

反之，当 PTS&DTS 标志并非“10”或“11”，或者说，当 PTS 数据不存在，CPU123 就继续检测分组数据起始位置。

当检测分组数据起始位置时，CPU123 重写选择控制寄存器 127 的内容，使得数据寄存器 125 保持的 PTS 数据供给随机数发生器 122 作为初始值。当需要解密的数据组标题不存在 PTS 数据时，此数据组之前的上一个数据组的 PTS 数据被立即提供给随机数发生器作为初始值。当被选择的数据组标题不存在 PTS 数据时，则选择更前面的一个数据组的 PTS 数据，直到数据组含有 PTS 数据为止。

因此，异或电路 129 对含有待加密数据组部分的寄存器 128 的输出数据和随机数发生器 122 输出的随机数进行异或操作。于是，包含待加密的数据组的数据流被加密。

CPU123 控制选择电路 130，使得异或电路 129 连续输出解密数据流，直到分组数据的数据流结束。随后，处理回到检测数据组启动码的状态。

MPEG 编码器 117 的输出数据流被转换成分组数据被加密的加密数据流。加密数据流被存入存储媒介 131，在需要的时候将存入存储

媒介 131 的数据流提供给解密电路 132。

提供给解密电路 132 的数据流存入缓冲存储器 133。存入缓冲存储器 133 的数据流又被 CPU137 读出。

另一方面，当检测数据组启动码时，CPU137 依靠数据组标题的加密控制信息来辨别数据组是否被加密。若没加密，CPU137 回到检测分组数据起始位置的状态。

当分组数据流是加密的（步骤 P3 判定“是”），CPU137 辨别 PTS&DS 标志位是不是“10”或“11”。换句话说，即在这一步骤中检查 PTS 数据的存在性。

当确定了 PTS&DTS 标志位是“10”或“11”，或者说，当确定了 PTS 数据存在，CPU137 检测 PTS 的位置，并使数据保持电路 134 保持 PTS 数据。之后，CPU137 等待数据组起始位置的检测。

反之，当 PTS&DTS 标志并非“10”或“11”，或者说，当 PTS 数据不存在，CPU137 就继续检测分组数据起始位置。

当检测分组数据起始位置时，CPU137 重写选择控制寄存器 141 的内容，使得寄存器 139 保持的 PTS 数据供给随机数发生器 136 作为初始值。当需要解密的数据组标题不存在 PTS 数据时，此数据组之前的上一个数据组的 PTS 数据被立即提供给随机数发生器 136 作为初始值。当被选择的数据组标题不存在 PTS 数据时，则选择更前面的一个数据组的 PTS 数据，直到数据组含有 PTS 数据为止。

异或电路 143 对数据寄存器 142 输出的待解密数据流和随机数发生器 136 产生的随机数提供异或操作。异或操作的结果是待解密的数据组的数据流被解密。

因此，CPU123 控制选择电路 144 使得异或电路 143 输出的解密数据流连续的输出，直到分组数据流结束为止。之后，过程回到检测数据组起始码的状态。

于是，从媒介 131 来的输出数据流被转换成分组数据被解密的解密数据流。解密数据流被传送到 MPEG 解码器 145。

在 MPEG 解码器 117 产生的是 MPEG2-TS 数据流的情况下，

CPU123 检测同步位并根据数据组标题加密控制域的内容辨别负载数据流是不是被加密的。当数据流是未加密的，CPU123 回到检测同步位的状态。

当负载数据流被加密，CPU123 从适配标志位判断是否存在适配域。若无适配域，CPU 依靠负载标志位判断是否存在负载。

当确认适配域存在，CPU123 从 PCR 标志位判断是否存在 PCR。若无 PCR，CPU 依靠负载标志位判断是否存在负载。

当 PCR 存在，CPU123 检测 PCR 位置，并使数据寄存器 125 保持 PCR 数据，CPU123 进一步依靠负载标志位判断是否存在负载。

当负载不存在，CPU123 处于检测同步字节的状态。当负载存在时，CPU123 就取检测负载起始位置的状态。

当检测负载起始位置时，CPU123 重写选择控制寄存器 127 的内容，使得寄存器 125 保持 PCR 数据，或者说，加密负载的数据组标题的 PCR 数据，供给随机数发生器 122 作为初始值。当需要解密的数据组标题不存在 PCR 数据时，此数据组之前的上一个数据组的 PCR 数据被立即提供给随机数发生器 122 作为初始值。当被选择的数据组标题不存在 PCR 数据时，则选择更前面的一个数据组的 PCR 数据，直到数据组含有 PCR 数据为止。

因此，异或电路 129 对数据寄存器 128 输出的待解密数据流和随机数发生器 122 产生的随机数提供异或操作。异或操作的结果是包含待解密的负载的数据组的数据流被解密。

定位检测电路 123 控制选择电路 130 使得异或电路 129 输出的解密数据流连续的输出，直到负载输出结束为止。之后，CPU123 回到检测同步位的状态。

MPEG117 的输出数据流被转换成数据组被加密的加密数据流。然后加密数据流被存入媒介 131 并在需要的时候再送入解密电路 132。

应注意的是送入解密电路的数据流被存入缓冲存储器 133，再从缓冲存储器 133 被 CPU137 读出。

CPU137 检测同步位并根据数据组标题加密控制信息的内容辨别

数据流或负载是不是被加密的。当负载数据流是未加密的，CPU123就回到检测同步位的状态。

反之，当负载数据流被加密，CPU123从适配标志位判断是否存在适配域。

当适配域存在，CPU123从PCR标志位判断是否存在PCR。若无PCR，CPU依靠负载标志位判断是否存在负载。

当PCR存在，CPU123检测PCR位置，并使数据寄存器139保持PCR数据，CPU进一步依靠负载标志位判断是否存在负载。当负载不存在，CPU123处理回到检测同步位的状态。另一方面，当负载存在，CPU137处于检测负载起始位置的状态。

当检测负载起始位置时，CPU137重写选择控制寄存器141的内容，使得寄存器139保持PCR数据,或者说，待解密负载的数据组标题的PCR数据，供给随机数发生器136作为初始值。当需要解密的数据组标题不存在PCR数据时，此数据组之前的上一个数据组的PCR数据被立即提供给随机数发生器136作为初始值。当被选择的数据组标题仍不存在PCR数据时，则选择更前面的一个数据组的PCR数据，直到数据组含有PCR数据为止。

因此，异或电路143对数据寄存器142输出的待解密数据流和随机数发生器122产生的随机数提供异或操作。从而，包含数据组的待解密数据流的解密操作被完成。

CPU137控制选择电路144使得异或电路143输出的加密数据流连续的输出，直到分组数据流结束为止。之后，CPU137回到检测同步位的状态。

于是，从媒介131读出的数据流被解密电路132转换成解密数据流，使得负载的加密数据流被解密。解密数据流被送入MPEG解码器145。

因此，在根据本发明第5实施例的数据传输系统和方法中，MPEG117的MPEG2－PS或MPEG2－TS格式的输出数据流由加密电路118被转换成加密的数据流，这样使得分组数据或负载的数据

流被加密。然后，被加密的数据流提供给解密电路 132 以便经媒介 131 解密。然后被解密的数据流传输给 MPEG 解码器 145。

在加密电路 118 中，通过提供待加密的分组数据的数据组标题的 PTS 数据或负载的数据组标题的 PCR 数据给随机数发生器 122 作为初始值，来完成加密。当需要加密的数据组标题不存在 PTS 数据时，此数据组之前的上一个数据组的 PTS 数据被立即提供给随机数发生器 122 作为初始值。当再次发生数据组标题不存在 PTS 数据时，则选择更前面的一个数据组的 PTS 数据，直到数据组含有 PTS 数据为止。当需要加密的负载数据组标题不存在 PCR 数据时，此数据组之前的上一个数据组的 PCR 数据被提供给随机数发生器 122 作为初始值。当再次发生负载的数据组标题不存在 PCR 数据时，则选择更前面的一个负载的 PCR 数据，直到负载含有 PCR 数据为止。

另一方面，在解密电路 132 中，对于每一个待解密数据组或负载，通过提供待加密的分组数据的数据组标题的 PTS 数据或负载的数据组标题的 PCR 数据给随机数发生器 136 作为初始值，来完成加密。当需要加密的数据组标题不存在 PTS 数据时，此数据组之前的上一个数据组的 PTS 数据被立即提供给随机数发生器 136 作为初始值。当再次发生数据组标题不存在 PTS 数据时，则选择更前面的一个数据组的 PTS 数据，直到数据组含有 PTS 数据为止。当需要加密的负载数据组标题不存在 PCR 数据时，此数据组之前的上一个数据组的 PCR 数据被提供给随机数发生器 136 作为初始值。当再次发生负载数据组标题不存在 PCR 数据时，则选择更前面的一个负载的 PCR 数据，直到负载含有 PCR 数据为止。

根据本发明实施例五的数据传输方法和系统，对于每个被解密的数据组或负载的数据流，提供给解密电路 132 中随机数发生器 136 的 PTS 数据或 PCR 数据的值不是常数。因此，分析由随机数发生器 107 生成的随机数模式明显变得困难，数据传输的保密性有显著改进。而且，本发明中的数据传输系统可用于 MPEG2-PS 和 MPEG2-TS 两种系统。

在上面的任何实施例中，供给加密或解密设备中的随机数发生器的预定的不定值并不局限于 PTS 数据或 PCR 数据，而是可由另外的数据，如包含在数据组标题的其它数据，对 PTS 数据或 PCR 数据的操作来形成。例如，预定数据可以通过组合，或者将 PTS 数据作用于 DTS 数据或具有 MPEG2 - PS 格式的循环计数器数据上来形成。而且，预定的数据也可通过组合，或者将 PCR 数据作用于循环计数器数据来获了。

本发明并不局限于这里描述的实施例，可以有不遵循本发明范围的各种各样的变化和修改。

图 .1

现有技术

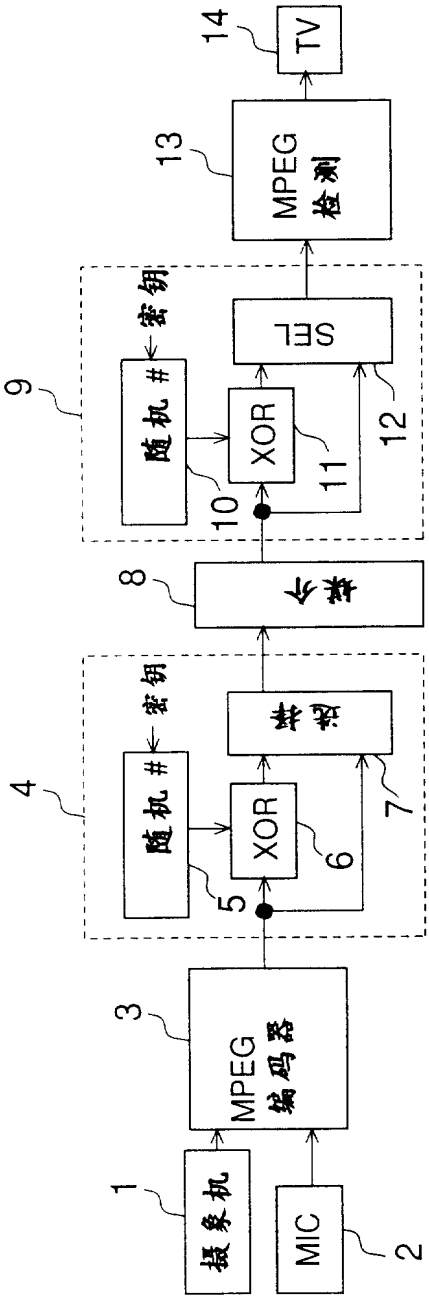

摄象机
MIC
MPEG 编码器
随机 #
密钥
XOR
禁用
卡券
随机 #
密钥
XOR
SEL
MPEG 检测
TV
1
2
3
4
5
6
7
8
9
10
11
12
13
14

图.2

现有技术

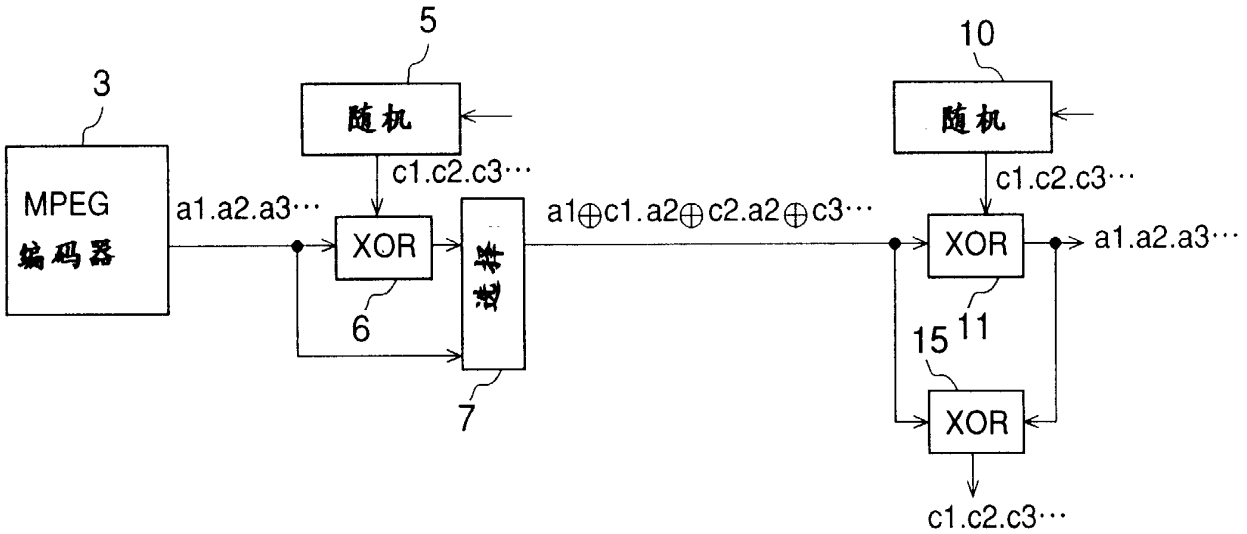

3
MPEG
编码器
a1.a2.a3…
5
随机
c1.c2.c3…
XOR
6
选择
7
a1⊕c1.a2⊕c2.a2⊕c3…
10
随机
c1.c2.c3…
XOR
a1.a2.a3…
11
15
XOR
c1.c2.c3…

图 .3

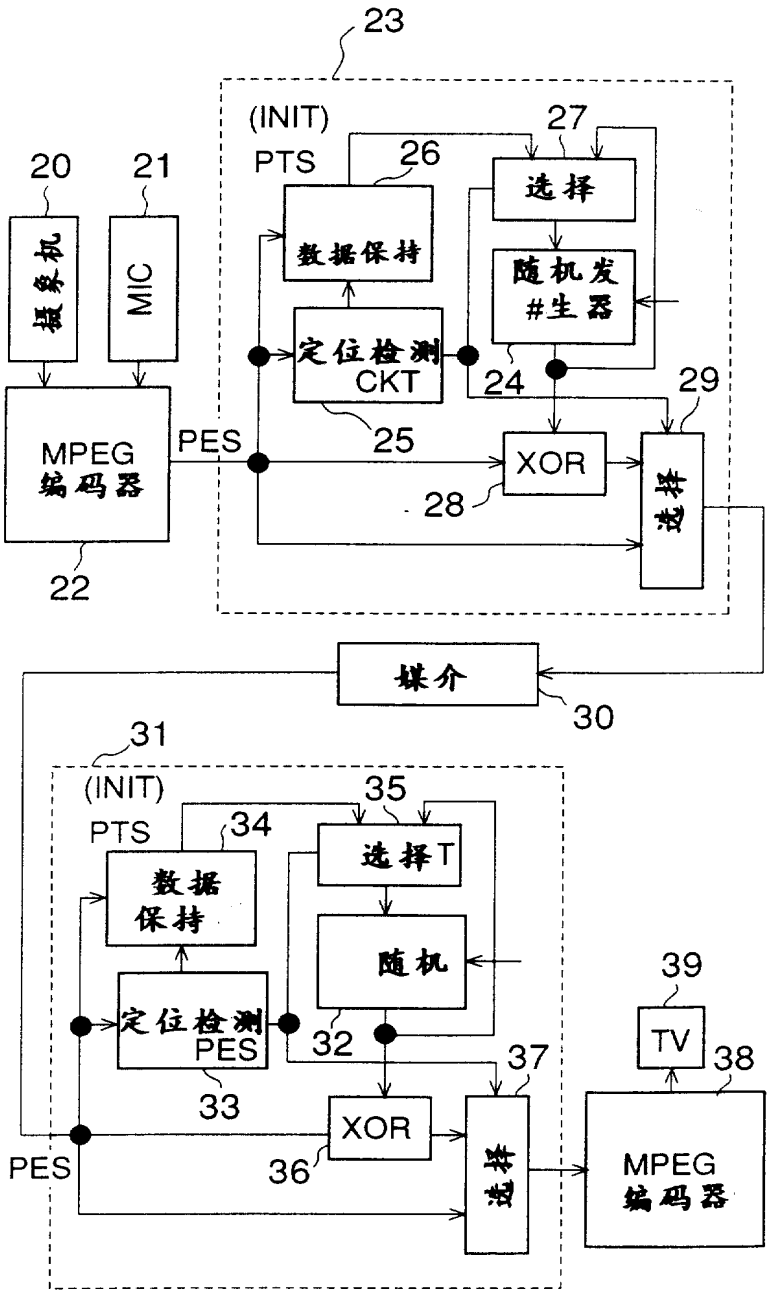

23
(INIT)
PTS
26
27
选择
数据保持
随机发
#生器
20
21
摄象机
MIC
定位检测
CKT
24
29
MPEG
编码器
PES
25
XOR
28
选择
22
媒介
30
31
(INIT)
35
PTS
34
选择T
数据
保持
随机
39
定位检测
PES
32
TV
38
37
33
XOR
PES
36
MPEG
编码器

图.4

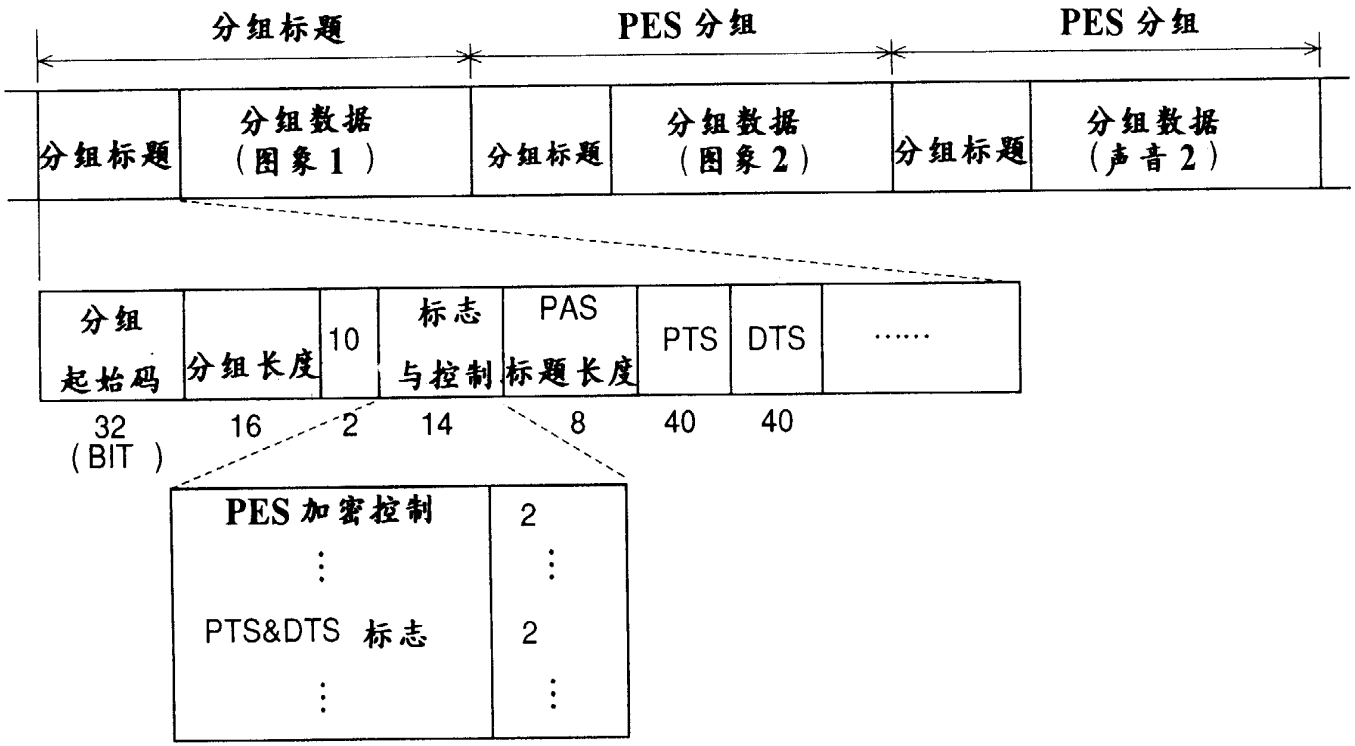

分组标题
PES 分组
PES 分组
分组标题
分组数据
（图象 1）
分组标题
分组数据
（图象 2）
分组标题
分组数据
（声音 2）
分组
起始码
分组长度
10
标志
与控制
PAS
标题长度
PTS
DTS
……
32
（BIT）
16
2
14
8
40
40
PES 加密控制
2
PTS&DTS 标志
2

图.5

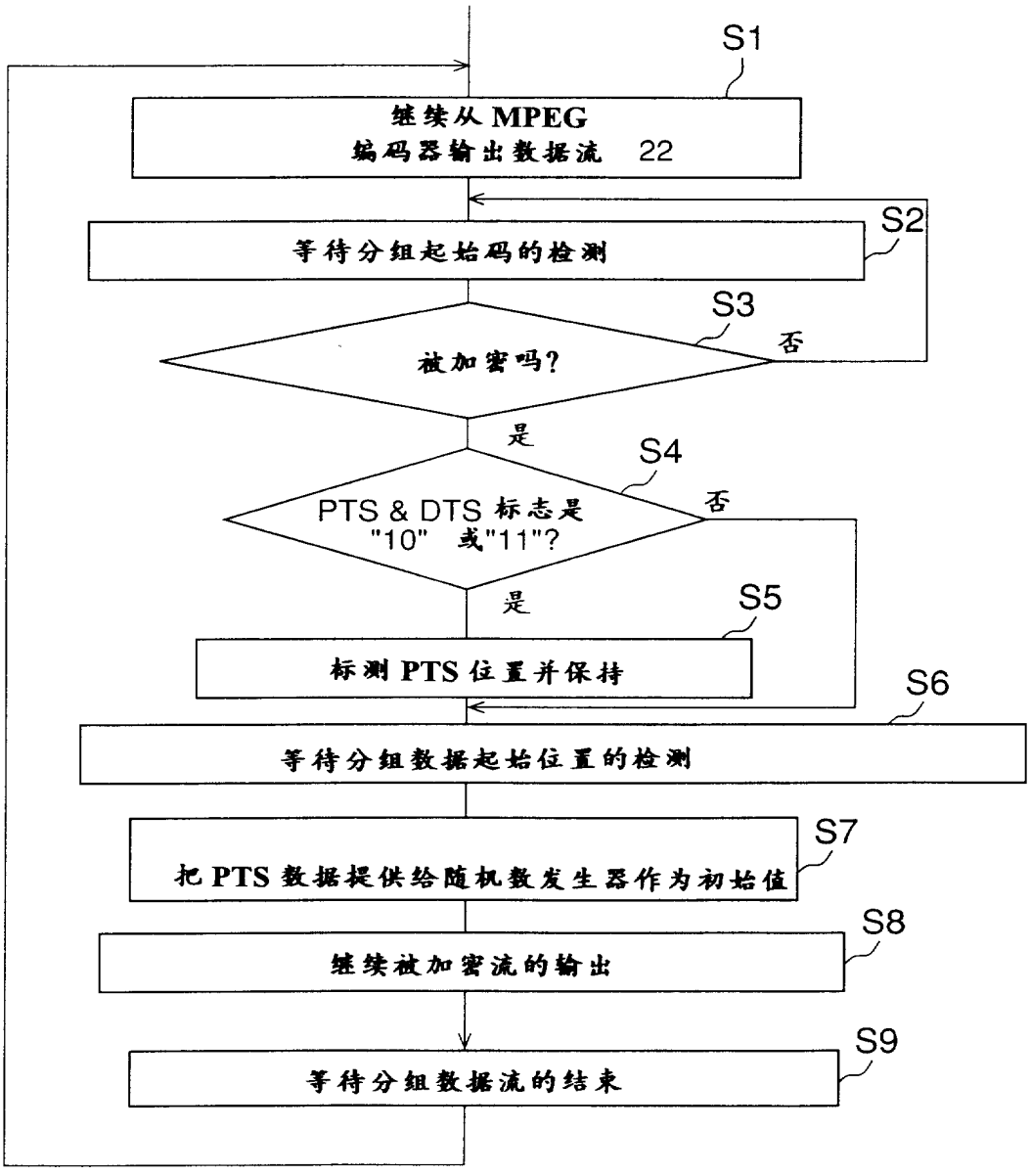

S1
继续从 MPEG
编码器输出数据流 22
S2
等待分组起始码的检测
S3
被加密吗?
否
是
S4
PTS & DTS 标志是
"10" 或"11"?
否
是
S5
标测 PTS 位置并保持
S6
等待分组数据起始位置的检测
S7
把 PTS 数据提供给随机数发生器作为初始值
S8
继续被加密流的输出
S9
等待分组数据流的结束

图.6

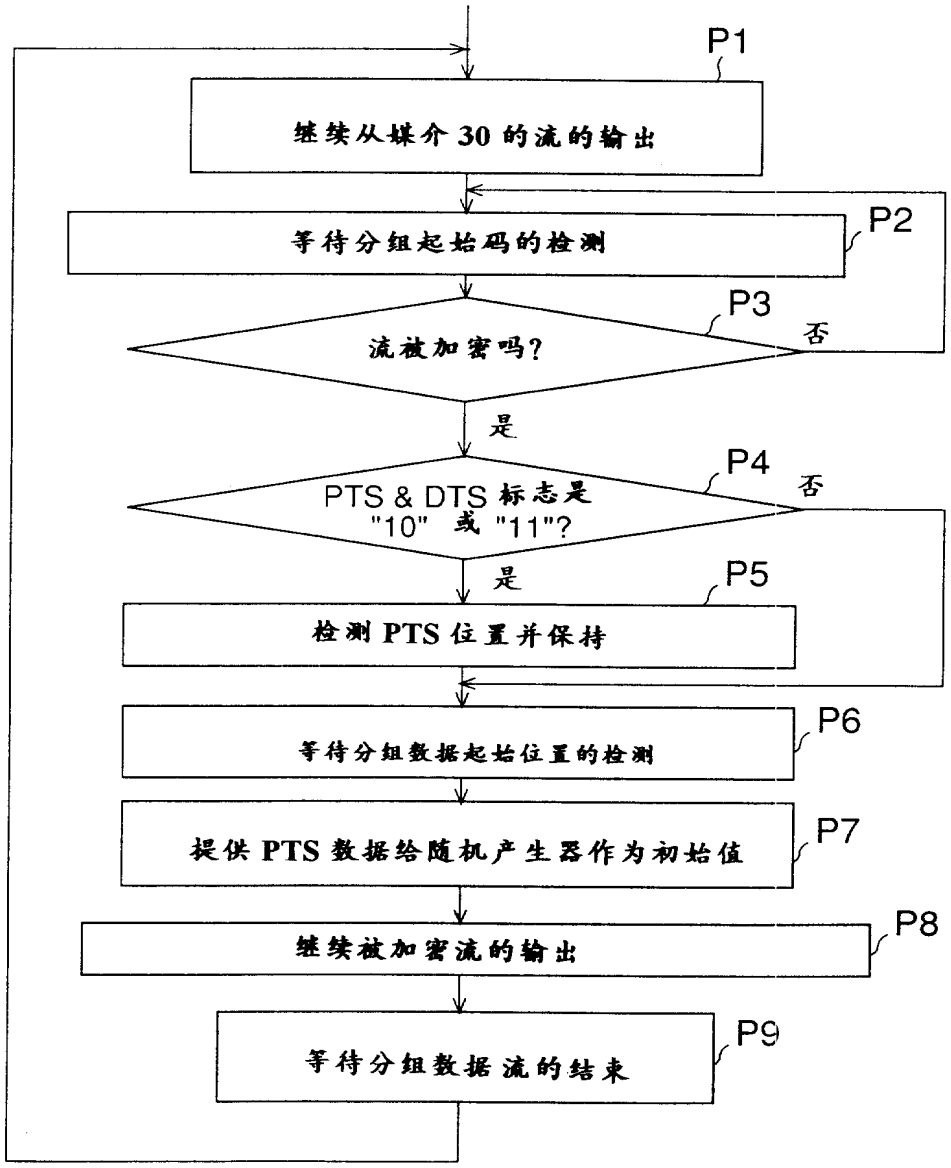

P1
继续从媒介 30 的流的输出
等待分组起始码的检测
P2
P3
流被加密吗?
否
是
P4
PTS & DTS 标志是
"10" 或 "11"?
否
是
P5
检测 PTS 位置并保持
等待分组数据起始位置的检测
P6
提供 PTS 数据给随机产生器作为初始值
P7
继续被加密流的输出
P8
等待分组数据流的结束
P9

图.7

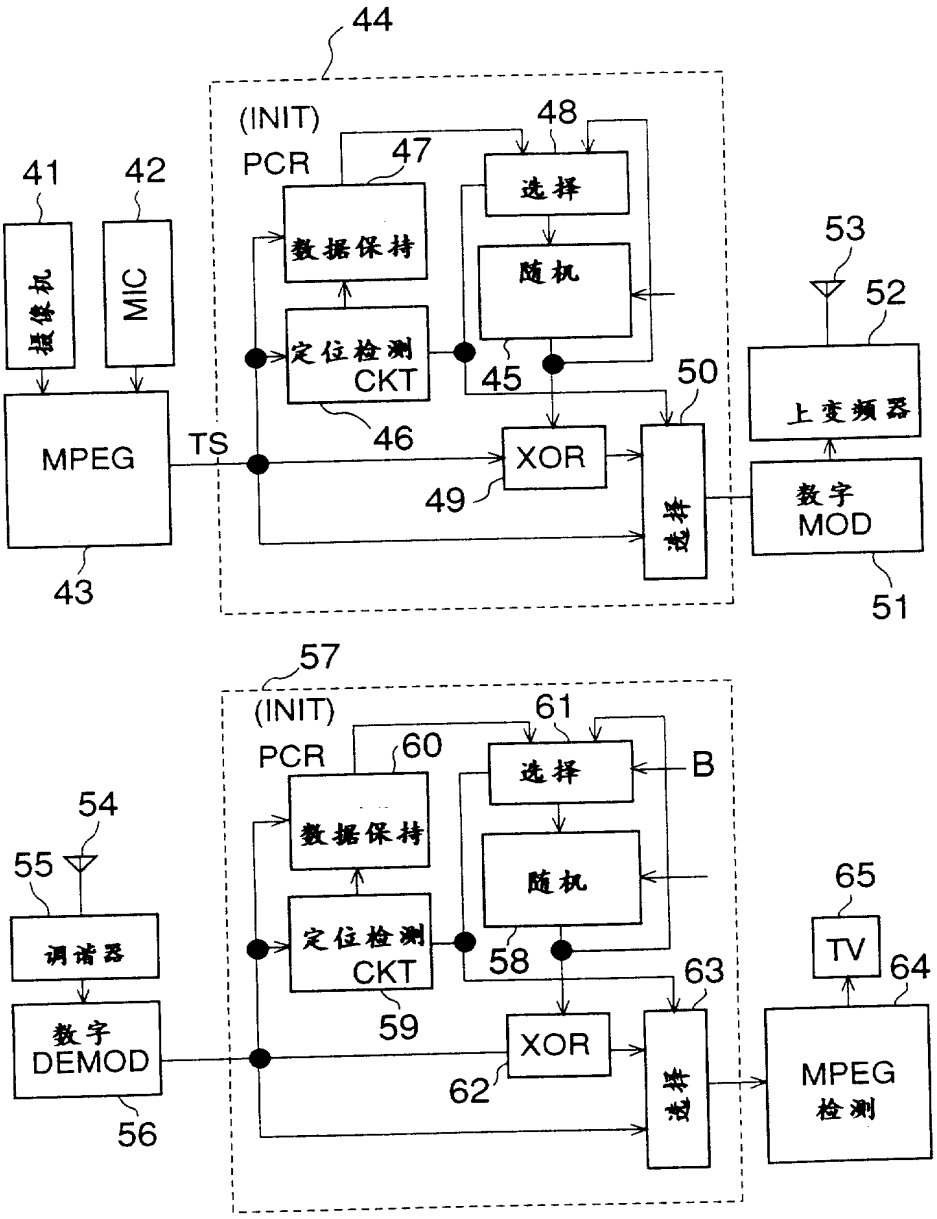

44
(INIT)
PCR
47
48
选择
数据保持
随机
41
42
摄像机
MIC
定位检测
CKT
45
50
53
52
上变频器
MPEG
TS
46
XOR
49
选择
数字
MOD
43
51
57
(INIT)
61
PCR
60
选择
B
数据保持
随机
54
55
调谐器
定位检测
CKT
58
63
65
TV
64
数字
DEMOD
59
XOR
62
选择
MPEG
检测
56

图.8

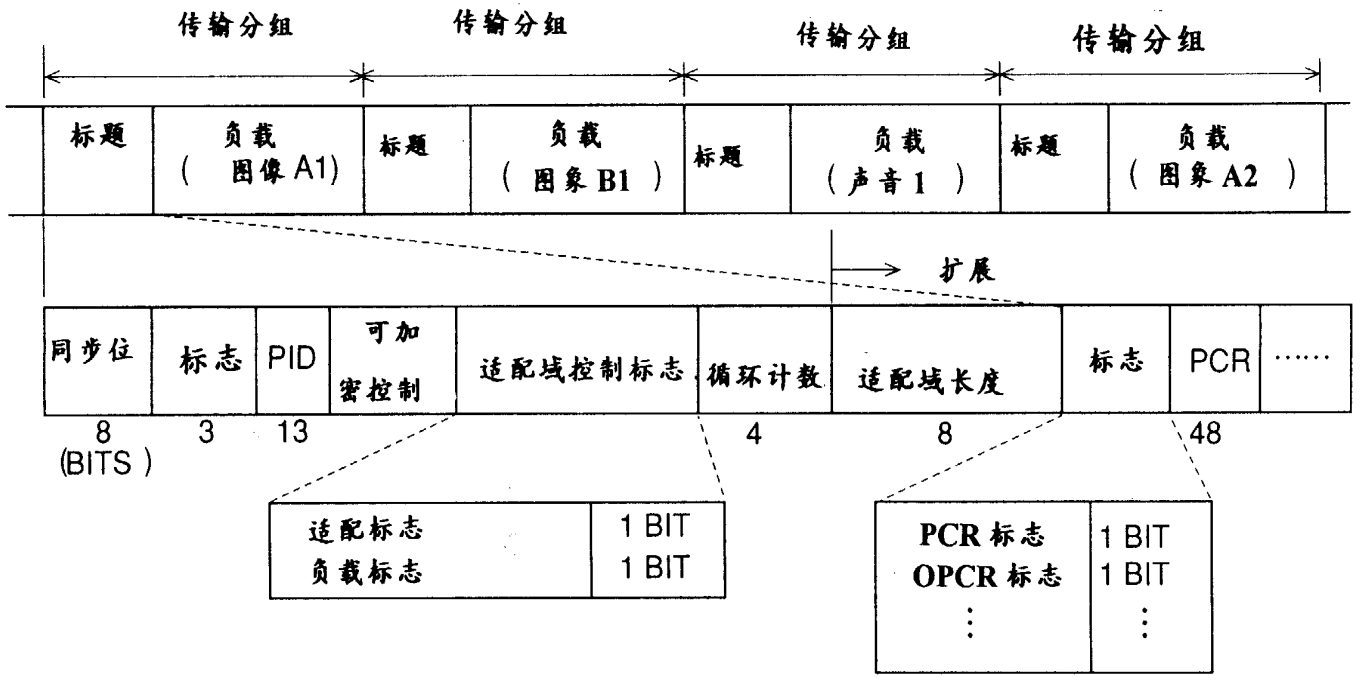

传输分组
传输分组
传输分组
传输分组
标题
负载
(图像 A1)
标题
负载
(图象 B1)
标题
负载
(声音 1)
标题
负载
(图象 A2)
扩展
同步位
标志
PID
可加
密控制
适配域控制标志
循环计数
适配域长度
标志
PCR
.....
8
(BITS)
3
13
4
8
48
适配标志
负载标志
1 BIT
1 BIT
PCR 标志
OPCR 标志
1 BIT
1 BIT

图 9

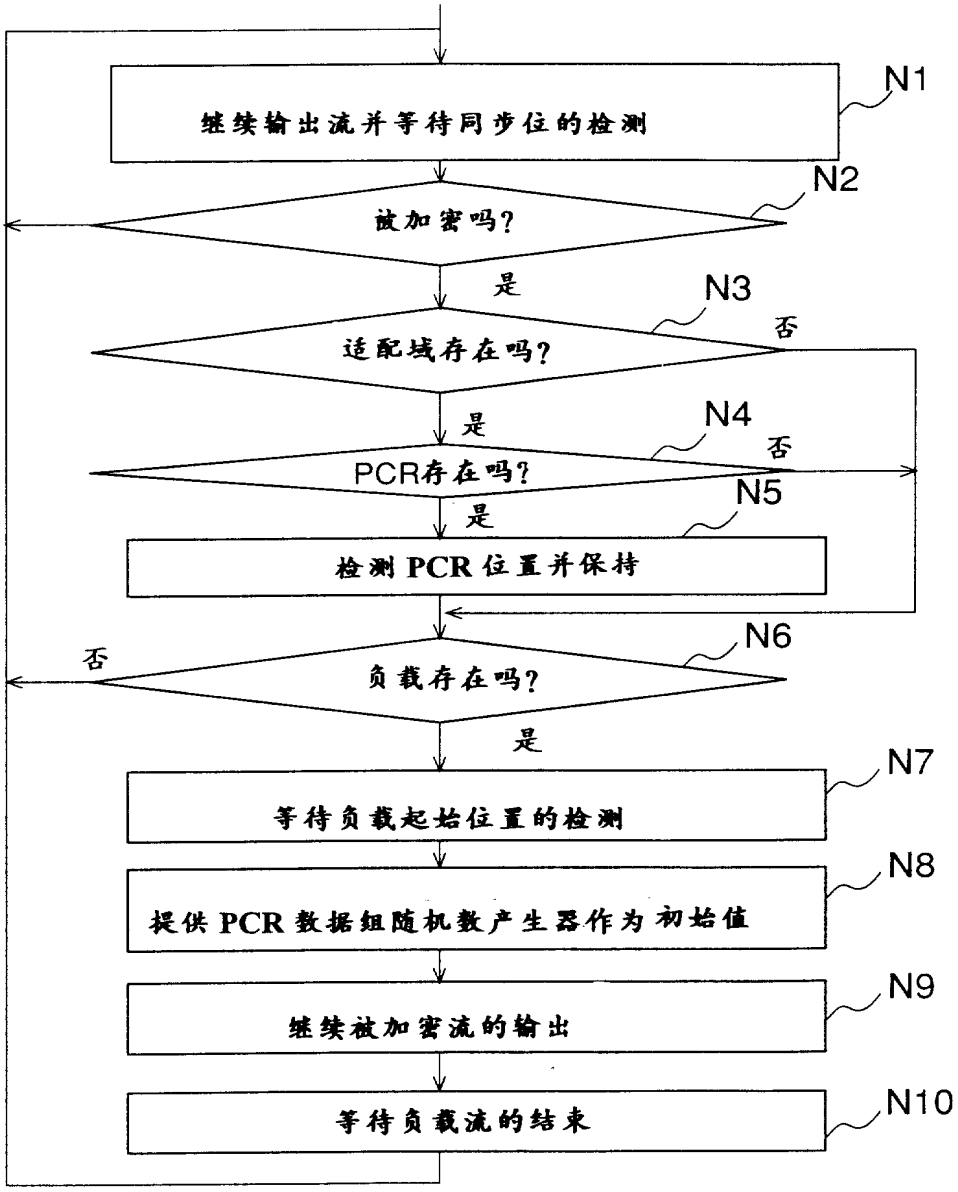

继续输出流并等待同步位的检测
N1
被加密吗?
N2
是
适配域存在吗?
N3
否
是
PCR存在吗?
N4
否
是
检测 PCR 位置并保持
N5
否
负载存在吗?
N6
是
等待负载起始位置的检测
N7
提供 PCR 数据组随机数产生器作为初始值
N8
继续被加密流的输出
N9
等待负载流的结束
N10

图 10

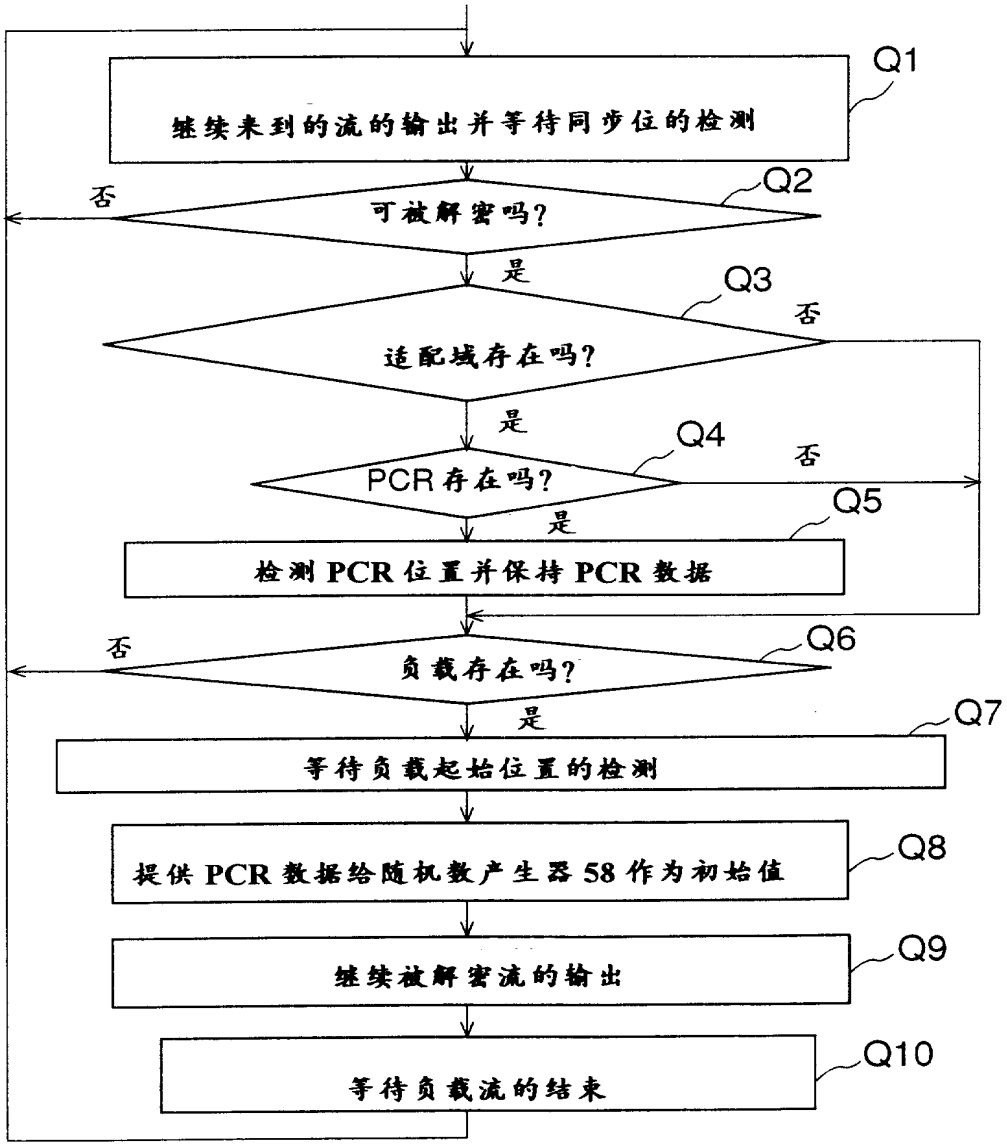

Q1
继续来到的流的输出并等待同步位的检测
Q2
否
可被解密吗?
是
Q3
否
适配域存在吗?
是
Q4
否
PCR存在吗?
是
Q5
检测 PCR 位置并保持 PCR 数据
Q6
否
负载存在吗?
是
Q7
等待负载起始位置的检测
Q8
提供 PCR 数据给随机数产生器 58 作为初始值
Q9
继续被解密流的输出
Q10
等待负载流的结束

图 11

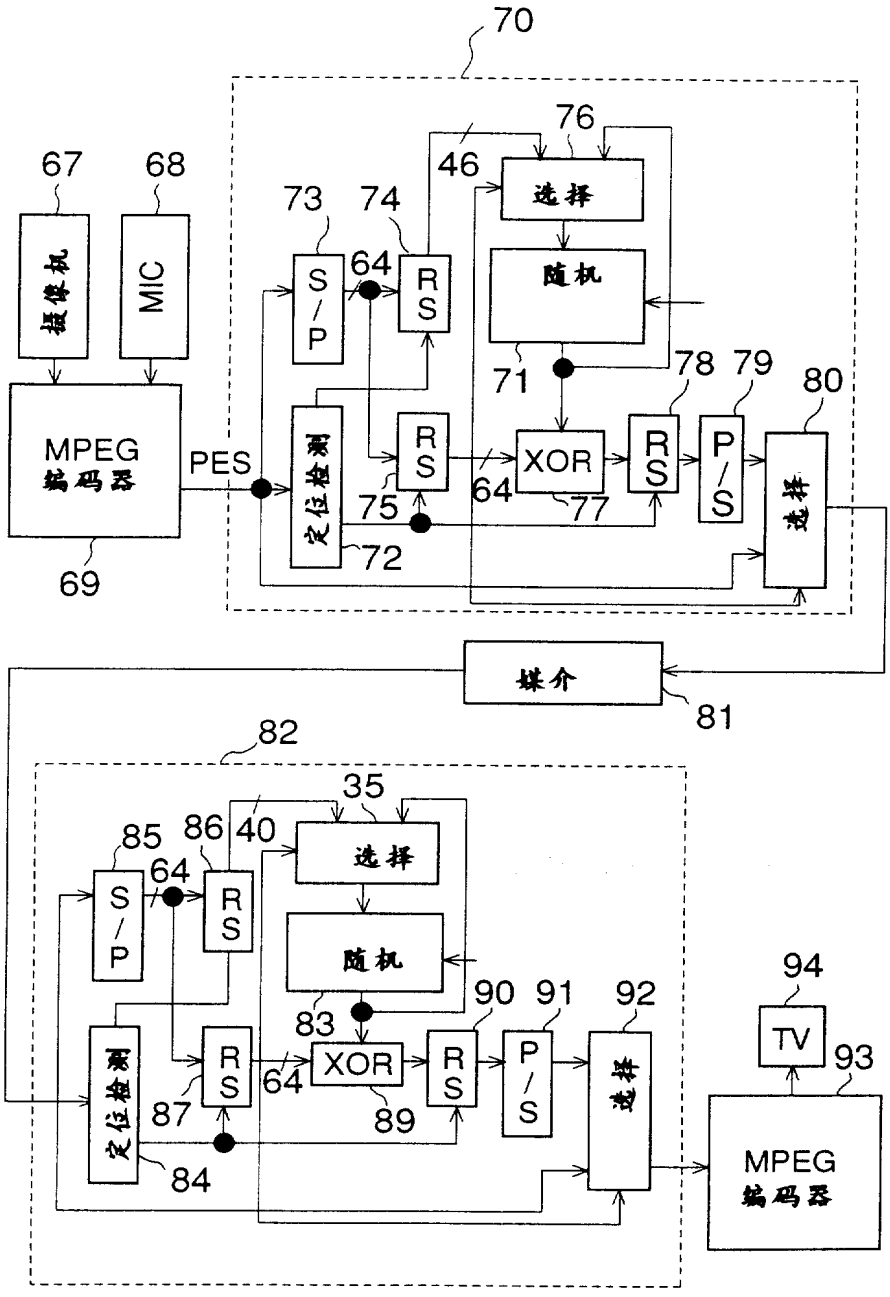

70
67
68
摄像机
MIC
MPEG
编码器
PES
69
73
74
S/P
64
RS
46
76
选择
随机
71
78
79
80
RS
XOR
RS
P/S
选择
75
64
77
72
定位检测
媒介
81
82
35
85
86
40
选择
64
S/P
RS
随机
83
90
91
92
94
TV
93
RS
64
XOR
RS
P/S
选择
87
89
84
定位检测
MPEG
编码器

图.12

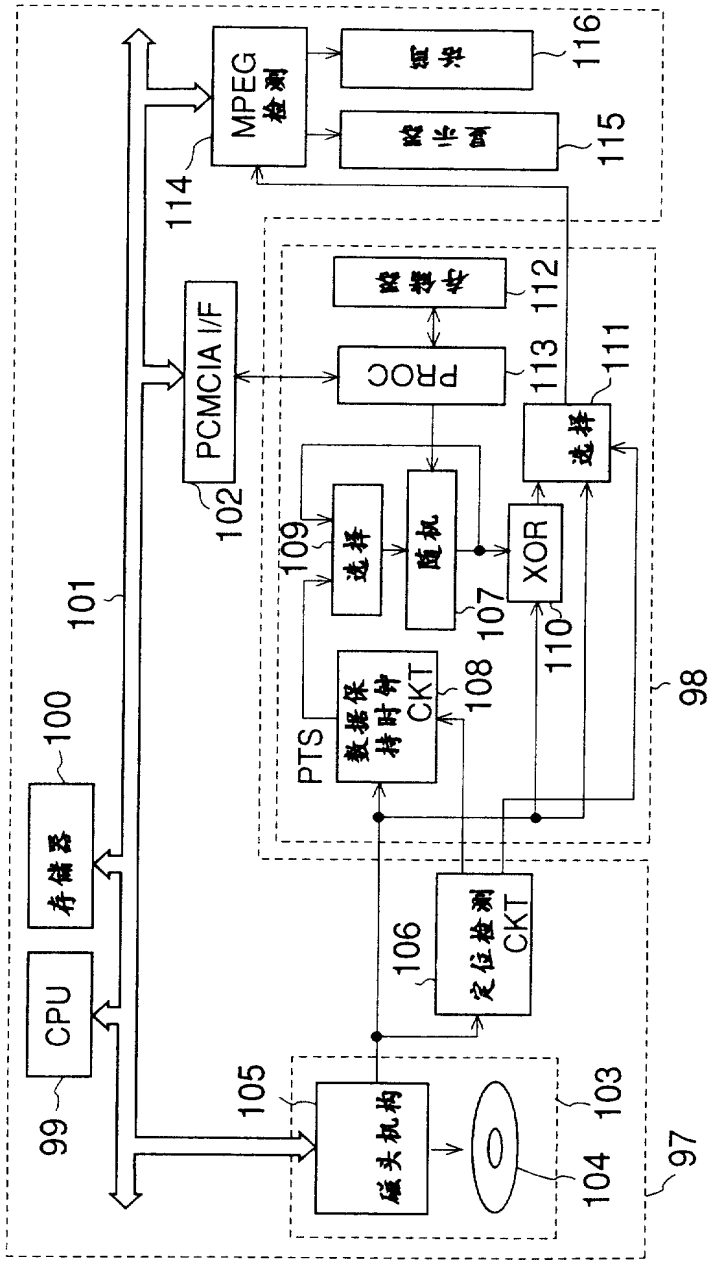
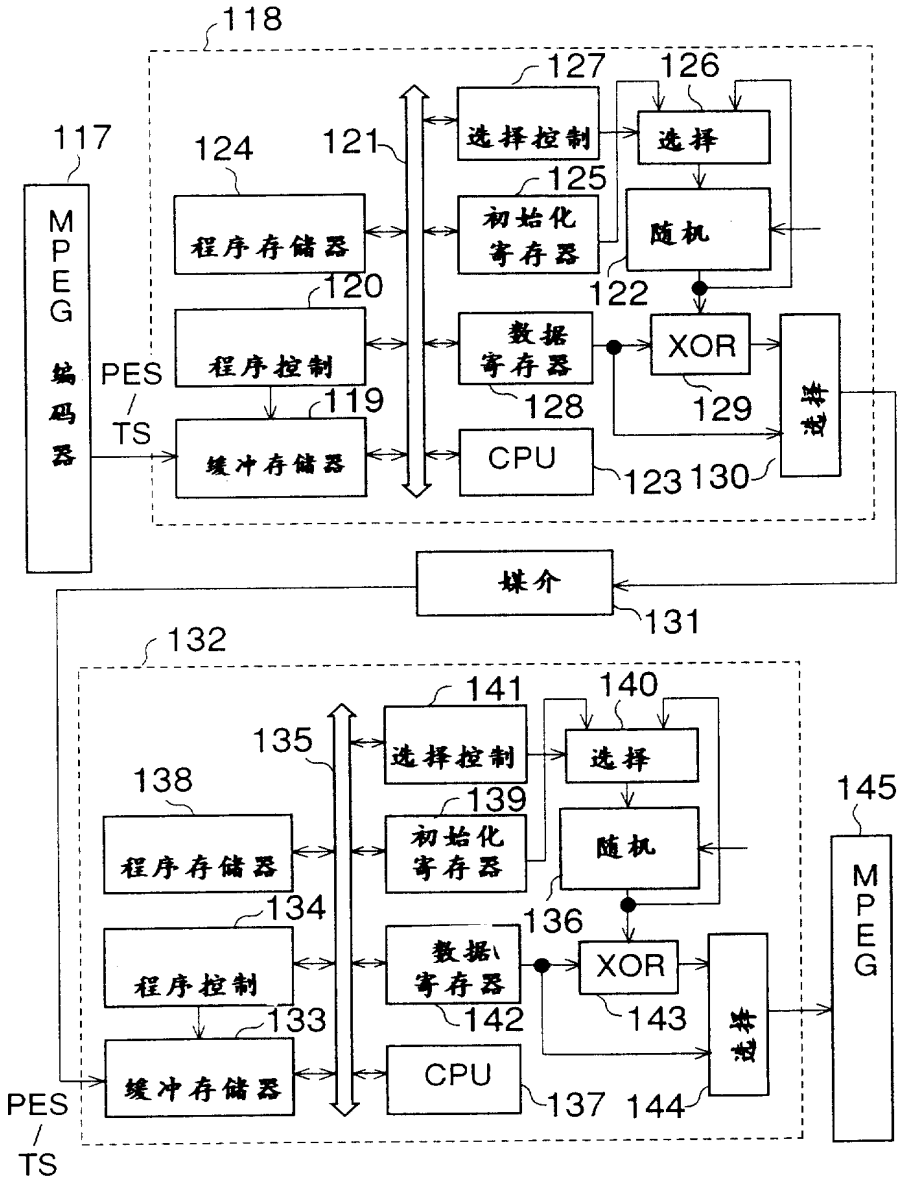

MPEG 检测
显示
输出
116
115
114
PCMCIA I/F
102
缓冲器
112
PROC
113
111
选择
109
随机
107
XOR
110
选择
数据保持时钟 CKT
108
PTS
98
CPU
99
存储器
100
101
定位检测 CKT
106
磁头机构
105
103
104
97

图 13


118
127
126
选择控制
选择
117
124
121
125
MPEG 编码器
程序存储器
初始化寄存器
随机
122
120
程序控制
数据寄存器
XOR
PES / TS
119
128
129
缓冲存储器
CPU
123
130
媒介
131
132
141
140
135
选择控制
选择
138
139
145
程序存储器
初始化寄存器
随机
MPEG
134
136
程序控制
数据寄存器
XOR
133
142
143
缓冲存储器
CPU
137
144
PES / TS