

[19] 中华人民共和国国家知识产权局



## [12] 发明专利申请公开说明书

[21] 申请号 200610007133.7

[51] Int. Cl.

C11B 20/00 (2006.01)

H04N 5/913 (2006.01)

[43] 公开日 2006 年 8 月 23 日

[11] 公开号 CN 1822167A

[22] 申请日 1995.11.26

[21] 申请号 200610007133.7

分案原申请号 03107336.0

[30] 优先权

[32] 1994.11.26 [33] KR [31] 31373/94

[71] 申请人 LG 电子株式会社

地址 韩国首尔市

[72] 发明人 朴兑浚

[74] 专利代理机构 北京市柳沈律师事务所

代理人 黄小临 王志森

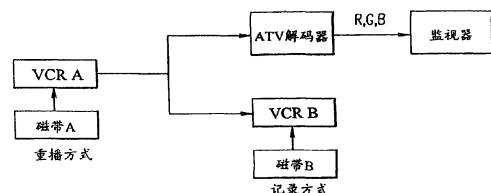
权利要求书 2 页 说明书 12 页 附图 7 页

[54] 发明名称

用于数字数据处理和记录系统的防复制方法  
和防复制设备

[57] 摘要

本发明公开了用于数字数据处理和记录系统的防复制方法和防复制设备。用于数字数据处理系统的防复制方法包括步骤：(a)接收第一密钥信息；(b)利用所述第一密钥信息加密第二密钥信息；(c)利用所述第二密钥信息加密数字数据流；以及(d)记录至少所加密的第二密钥信息和所加密的数字数据流到数字介质上。由于密码信息记录在数字介质上，以致于只有能检测到密码信息的再生装置可以正常地再生该数字介质，由此防止非法复制。



1. 一种用于数字数据系统的防复制方法，包含步骤：
  - (a) 接收第一密钥信息；
  - (b) 利用所述第一密钥信息加密第二密钥信息；
  - (c) 利用所述第二密钥信息加密数字数据流；以及
  - (d) 记录至少所加密的第二密钥信息和所加密的数字数据流到数字介质上。
2. 根据权利要求 1 所述的方法，其中，所述步骤(b)随机地选择所述第二密钥信息。
3. 根据权利要求 1 所述的方法，其中，所述步骤(c)以块为单位加密所述数字数据流。
4. 一种用于数字数据系统的防复制设备，包含：

加密单元，用以接收第一密钥信息，利用所述第一密钥信息加密第二密钥信息，并且利用所述第二密钥信息加密数字数据流；以及

控制器，用以控制至少所加密的第二密钥信息和所加密的数字数据流在数字介质上的记录。
5. 根据权利要求 4 所述的设备，其中，所述加密单元随机地选择所述第二密钥信息。
6. 根据权利要求 4 所述的设备，其中，所述加密单元以块为单元加密所述数字数据流。
7. 一种用于数字数据系统的防复制方法，包括：

接收第一密钥信息，所述第一密钥信息用于加密数字数据；

利用第二信息加密所述第一密钥信息；以及

传送所加密的第一密钥信息。
8. 根据权利要求 7 所述的方法，其中，所述加密步骤利用公用密钥加密所述第一密钥信息。
9. 根据权利要求 7 所述的方法，其中，所述传送步骤在数字介质上记录所加密的第一密钥信息。
10. 根据权利要求 7 所述的方法，其中，所述传送步骤传送所加密的第一密钥信息。

11. 一种用于数字数据系统的防复制设备，包括：

加密单元，用于接收第一密钥信息并利用第二密钥信息加密所述第一密钥信息，所述第一密钥信息用于加密数字数据；以及

控制器，用于控制所加密的第一密钥信息的传送。

12. 根据权利要求 11 所述的设备，其中，所述加密单元利用公用密钥加密所述第一密钥信息。

13. 根据权利要求 11 所述的设备，其中，所述控制器控制在数字介质上记录所加密的第一密钥信息。

14. 根据权利要求 11 所述的设备，其中，所述控制器控制传送所加密的第一密钥信息。

---

用于数字数据处理和记录系统的  
防复制方法和防复制设备

本申请是申请日为 1995 年 11 月 26 日、申请号为 03107336.0、发明名称为“用于数字数据处理和记录系统的防复制方法和记录装置”的发明专利申请的分案申请。

#### 发明领域

本发明涉及一种用于数字数据处理和记录系统的防复制技术以及在该系统中用于记录数字数据的记录装置。特别涉及一种用于数字 VCR 的防复制方法，其中加密码被引入到 VCR 中以便仅在内部包括一个相应加密码的 VCR 中显示一个图像，由此防止磁带被复制；还涉及一种具有用于在数字数据处理装置中控制防复制功能的操作的信息的记录介质。

#### 背景技术

用于模拟 VCR 的普通防复制方法被公开在美国专利号为 4819098, 4571642 和 4577216 的文献中。

首先，美国专利 4819098 公开了一种方法，在该方法中一个干扰信号在 VCR 的一个自动增益控制电路(AGC)中被插入到一个视频波形中。这里，插入的信号不影响其监视器的 AGC，但影响了 VCR 在一个视频带上记录一个信号精确电平的 AGC。

在美国专利 4571642 中公开了一种方法，在该方法中一个相位噪声或其它校正信号被插入到一个视频波形的彩色同步信号中。

然而，所有公知技术都是利用在一个监视器的电路和 VCR 的一个相应的电路之间的区别把分布信号插入到模拟信号中。一些 VCR 可以进行正常复制而不管防复制。一些监视器不能显示原始视频磁带的图像。通常引入到一个模拟 VCR 系统中的防复制很难应用到一个数字存储介质(DSM)上。

特别是在一个卫星接收器或高清晰度 TV 解码器中，如在图 2 中所示，由一个数字 VCR 接收的 MPEG 比特数据流被构成以便分别地或同时传送一

个传送标题、信息包化单元比特数据流(PES)标题和音频和视频数据。

PES 标题包括一个 14 位的 PES 标题特征位区域和一个具有可变长度的 PES 标题域，其中 14 位是一个用于像数字 VCR 这样的 DSM 的域。该 PES 标题特征位区域包括：1 位版权(CR)特征位，1 位原始或复制(OC)特征位，2 位 PD 特征位，1 位 TM 特征位和 1 位 AC 特征位。

PES 标题域在长度上变化，并且其部分上设置有 PD、TM 和 AC 特征位，如果 PD 特征位的值是“00”，那么不存在一个 PTS/DTS 区域。如果该值是“10”，那么它是 40 位。如果该值是“11”，那么该区域是 80 位。如果 TM 特征位是“0”，那么不存在 DSM 策略方式域。如果该 TM 特征位是“1”，那么该域是 8 位。如果 AC 特征位是“1”，那么一个附加复制信息域是 8 位。

当利用卫星接收器或高清晰度 TV 解码器进行记录和被压缩的视频数据在编码器 101 中被编码时，它在信息包处理部分 102 中被转换成一个信息包形式，如在图 1 中所示。如果压缩的音频数据在音频编码器 103 中被编码，那么该数据在信息包处理部分 104 中被转换成一种信息包形式。

当信息包处理部分 102 和 104 的输出在传送多路调制器 105 中被多路调制时，在图 2 中所示的一个固定传送流输出给一个数字 VCR。在这种情况下，为了防复制，在美国专利 4200770 中建议应用一个公用密码加密码。它解决了当像数据的密标准(DES)这样的常规单元密码或流密码算法仅用一个保密密码来加密或解密时在密码管理或密码分布中的缺陷。

这种公用密码加密系统使所有用户  $U$  持有专门的加密算法  $E^{PK}_u$  和解密算法  $D^{PK}_u$ 。在此，用于公用密码的加密算法  $E^{PK}_u$  被公开为一个对密码提供部分 107 的公用密码。用于保密密码的解密算法  $D^{PK}_u$  保持为保密。 $E^{PK}_u$  和  $D^{PK}_u$  的特征如下。

首先，根据所有用户  $U$  和传送的信息  $m$ ,  $D^{PK}_u(E^{PK}_u(m))=m$ 。

第二，加密算法  $E^{PK}_u$  和解密算法  $D^{PK}_u$  不需要复杂的计算。

第三，从加密算法  $E^{PK}_u$  中求出  $D^{PK*}_u$  来满足  $D^{PK*}_u(E^{PK}_u(m))=m$  是不可能的。

在具有上述特征的加密系统中，如在图 3 中所示，当用户 A 传送信息  $m$  给用户 B 时，从密码提供部分 107 接收的用于用户 B' 的公用密码的公用密码算法  $E^{PK}_B$  的加密器 106 对信息  $m(E^{PK}_B(m)=c)$  加密并且借助于一个公用信道把结果传送给解密 109。在此，公用信道代表一个在其中传送的数据不

是保密的信道。

从密码提供部分 107 接收密码信息的密码解码器 108 输出与加密算法  $E^{PK}_B$  相对应的一个算法  $D^{PK}_B$ ，解密器 109 用解密算法  $D^{PK}_B$  对加密器 106 输出解密( $D^{PK}_B(c)=m$ )，并且然后传送给用户 B。换言之，仅有用户 B 能够对与加密算法  $E^{PK}_B$  相对应的解码算法  $D^{PK}_B$  解密。

在美国专利 4405829 中公开了一种由公用密码加密改进的原理。这种公用密码加密系统被称为 RSA 系统。在美国专利 4964164 中公开了一种利用分批处理来有效计算 RSA 公用密码加密的方法。

然而，这种公用密码加密不适用高速加密。一个 CA 系统是为了防止非法复制。然而，没有办法能够保护通过一个数字 VCR 中的数字存储介质提供的节目。

### 发明内容

因此，本发明的一个目的是提供一种用于数字视频系统的非法复制防止单元，其中，在复制带中已加密的密码信息被传送和被记录，以致于一个被复制的磁带仅能在一个具有相应加密密码信息的 VCR 中被再生，由此防制了复制。

为了实现本发明的上述目的，提供一种用于数字数据处理系统的防复制方法，包含步骤：(a)从数字介质中检测加密密钥；(b)利用密钥信息解密所述加密密钥；(c)基于所解密的加密密钥来解密记录在数字介质上的主数字数据；以及(d)将所解密的主数字数据流传送到监视器和数字记录器至少之一。

为了实现本发明的上述目的，还提供一种用于数字数据处理系统的防复制设备，包含：密钥检测器，用以从数字介质中检测加密密钥；解密单元，用以利用密钥信息解密所述加密密钥并且基于所解密的加密密钥来解密主数字数据；以及控制器，用以控制所解密的主数字数据流向监视器和数字记录器至少之一的传送。

为了实现本发明的上述目的，还提供一种用于数字数据处理系统的防复制方法，包含步骤：(a)从数字介质中检测加密密钥；(b)利用密钥信息解密所述加密密钥；(c)基于所解密的加密密钥来解密主数字数据流。

为了实现本发明的上述目的，还提供一种用于数字数据处理系统的防

---

复制设备，包含：密钥检测器，用以从数字介质中检测加密密钥；解密单元，用以利用密钥信息解密所述加密密钥并且基于所解密的加密密钥来解密主数字数据流。

为了实现本发明的上述目的，还提供一种用于数字数据处理系统的防复制方法，包含步骤：(a)从数字介质中检测加密密钥；(b)利用预定密钥信息解密所述加密密钥；(c)基于所解密的加密密钥来解密主数字数据流。

为了实现本发明的上述目的，还提供一种用于数字数据处理系统的防复制设备，包含：密钥检测器，用以从数字介质中检测加密密钥；解密单元，用以利用预定密钥信息解密所述加密密钥并且基于所述解密的加密密钥来解密主数字数据流。

为了实现本发明的上述目的，还提供一种用于数字数据处理系统的防复制方法，包含步骤：(a)接收第一密钥信息；(b)利用所述第一密钥信息加密第二密钥信息；(c)利用所述第二密钥信息加密数字数据流；以及(d)记录至少所加密的第二密钥信息和所加密的数字数据流到数字介质上。

为了实现本发明的上述目的，还提供一种用于数字数据处理系统的防复制设备，包含：加密单元，用以接收第一密钥信息，利用所述第一密钥信息加密第二密钥信息，并且利用所述第二密钥信息加密数字数据流；以及控制器，用以控制至少所加密的第二密钥信息和所加密的数字数据流在数字介质上的记录。

为了实现本发明的上述目的，还提供一种具有用于控制数字数据处理装置中的防复制功能的操作的数据结构的记录介质，包括：数字数据区域，用于存储利用第一密钥信息加密的数字数据；密钥信息区域，用于存储利用第二密钥信息加密的所述第一密钥信息，所述第一密钥信息在数字数据处理装置中操作来控制所加密的数字数据的解密。

为了实现本发明的上述目的，还提供一种用于数字数据系统的防复制方法，包括：接收第一密钥信息，所述第一密钥信息用于加密数字数据；利用第二信息加密所述第一密钥信息；以及传送所加密的第一密钥信息。

为了实现本发明的上述目的，还提供一种用于数字数据系统的防复制设备，包括：加密单元，用于接收第一密钥信息并利用第二信息加密所述第一密钥信息，所述第一密钥信息用于加密数字数据；以及控制器，用于控制所加密的第一密钥信息的传送。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：基于密钥信息加密数字内容，该密钥信息是解密要再现的数字内容所必需的；以及在数字记录介质上记录所加密的数据和该密钥信息。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：(a)提供加密的密钥信息，该密钥信息用于控制要再现的数字内容的至少解密；以及(b)在数字记录介质上记录所述加密的密钥信息和该数字内容。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：(a)产生密钥信息，该密钥信息用以控制要再现的数字内容的至少解密；以及(b)加密该密钥信息和要再现的数字内容；以及(c)在数字记录介质上记录所加密的密钥信息和所加密的数字内容。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：(a)检测密钥信息以解密记录在数字记录介质上的、加密的用户数据；(b)基于所检测到的密钥信息解密所述加密的用户数据；以及(c)输出所解密的用户数据以恢复原始数据。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：(a)接收加密的数字内容和加密密钥，该加密密钥用于解密该加密的数字内容；(b)提取该加密密钥；以及(c)基于所述加密密钥解密所接收到的数字数据。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：(a)从再现自数字记录介质的信号中检测密钥信息，该密钥信息用于解密记录在该数字记录介质上的至少用户数据，该用户数据划分为多个第一数据单元，而第一数据单元分别划分为第二数据单元，第二数据单元包括标题部分和用户数据部分，标题部分包含用于指示用户数据部分被加密的分类信息；以及(b)基于该密钥信息控制解密过程。

为了实现本发明的上述目的，还提供一种记录介质，包括：数据区域，包含加密的数字数据；以及控制信息区域，包含密钥信息，所述密钥信息用于操作来控制所述加密的数字数据的解密。

为了实现本发明的上述目的，还提供一种记录介质，包括：数据区域，用于存储加密或未加密的用户数据；以及控制信息区域，包含用于指示所存储的用户数据是否被加密的状态信息。

为了实现本发明的上述目的，还提供一种记录介质，包含：数据区域，用于存储加密的用户数据；以及密钥信息区域，用于存储解密所述加密的

用户数据所需要的密钥信息，其中，数据区域划分为多个 GOP (图像组) 单元，每个 GOP 单元划分为多个信息包单元，每个信息包单元包含标题部分和数据部分，其中数据部分包括至少加密的用户数据而密钥信息存储在由数据区域跟随的密钥信息区域中。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：产生加密的数字内容；以及传送该加密的数字内容和用于加密该数字内容的密钥信息，其中该密钥信息是在接收部件中解密所述加密的数字内容所需要的。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：接收加密的数字内容以及用以指示数字内容被加密的分类信息；基于分类信息识别所接收到的数字内容被加密；以及基于解密所述加密的数字内容所需要的密钥信息来解密所述加密的数字内容。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：(a) 对要传送的用户数据产生密钥信息；(b) 基于该密钥信息加密该用户数据；以及(c) 输出所述加密的用户数据和该密钥信息。

为了实现本发明的上述目的，还提供一种防复制设备，包括：接收单元，用以接收从数字介质中再现的信号；密钥检测器，用以从所接收到的信号中检测加密密钥；解密单元，用以基于所述加密密钥解密数字内容；以及连接到所述解密单元的控制器，用于控制所述数字内容的解密。

为了实现本发明的上述目的，还提供一种防复制设备，包括：接收单元，用以接收数字数据流；密钥检测器，用以检测包含在所述接收到的数字数据流中的加密密钥；以及控制器，用以基于所述检测到的密钥信息控制用户数据的解密过程，其中该控制器基于从所述接收单元中接收到的分类信息来确定包含在数字数据流上的用户数据是否被加密，并且如果所述分类信息指示用户数据是加密的，则利用所述密钥信息解密所述用户数据。

为了实现本发明的上述目的，还提供一种防复制方法，包括步骤：(a) 读取密钥信息以再现记录在数字介质上的用户数据；(b) 解码密钥信息以解密所述用户数据；以及(c) 基于所述解码的密钥信息来解密所述用户数据。

## 附图说明

图 1 是常规信息包处理装置的一个方框图；

图 2 是表示一般的传送比特数据流的一个例子；  
 图 3 是常规公用密码加密系统的方框图；  
 图 4 是表示在本发明的系统连接图；  
 图 5 是本发明的用于数字视频系统的防复制装置的方框图；  
 图 6 是图 5 的防复制信息检测器的方框图；  
 图 7 是图 6 的 PES 标题检测器的电路图；  
 图 8a - 8f 是在图 7 的各个部分上输入/输出的波形图；  
 图 9 是图 6 的防复制信息分离器的电路图；  
 图 10a-10g 是在图 9 的对应部分上输入/输出的波形图；和  
 图 11a-d 表示本发明的一个比特数据流的例子。

#### 具体实施方式

此后将参照附图来描述本发明的优选实施例。

参照图 5，本发明的一种防止复制装置包含：一个再生部分 1，用于再生在磁带上记录的数据；一个密码插入部分 2，用于在再生部分 1 的比特数据流前面加上一个磁带标题起始码和密码信息组；一个解码部分 3，用于把密码插入部分 2 的输出解码并把它作为并行数据传送；一个密码检查/校正部分 4，用于检测来自解码部分 3 传送的并行数据的密码信息组；一个防止复制信息检测部分 5，用于检测从被检测的密码信息组来的一个 PES 标题并分离出防止复制信息；一个防止复制信息校正部分 6，用于如果需要，校正防止复制信息检测部分 5 的输出；一个加密部分 7，用于把防止复制信息校正部分 6 的输出加密；和一个记录部分 8，用于在磁带上记录加密部分 7 的输出。

如在图 6 中所示，防止复制信息检测部分 5 包含：一个 PES 标题检测部分 10，用于与一个时钟 c1k 同步地搜索并行数据以便检测 PES 标题，和一个防止复制信息分离器 20，它由 PES 标题检测部分 10 的 PES 标题信号起动以便检测防止复制信息域。

参照图 7，PES 标题检测部分 10 包含：第一和第二触发器 11 和 12，用于根据时钟 c1k 顺序地使并行数据延迟；一个信息包起始码检测器 13，用于检索并行数据和第一和第二触发器 11 和 12 的输出，以便检测 PES 标题的信息包起始码；一个比特数据流 ID 检测器 14，用于检索第二触发器

12 的输出以便检测 PES 标题的比特数据流 ID; 一个延迟器 15, 用于根据时钟 c1k 顺序地使信息包起始码检测器 13 的输出 is-pscp 延迟, 和一检测信号发生器 16, 用于把延迟器 15 的输出和比特数据流 ID 检测器 14 的输出逻辑地相乘并且输出一个 PES 标题检测信号 is-PES-标题。

如在图 9 中所示, 防止复制信息分离器 20 包含: 一个 D-触发器 21, 用于保持从 PES 标题检测器 10 输出的并行数据; 一个 D-触发器 22, 用于保持 PES 标题检测器 10 的 PES 标题检测信号 is-PES 标题; 一个由 D-触发器 22 的输出清零的 D-触发器 23, 用于通过 D-触发器 21 输出的一个 CR 信号来保持电压(+5V)并且输出一个信号 LCR; 一个由 D-触发器 22 的输出清零的 D-触发器 24, 用于通过 D-触发器 21 输出的一个 OC 信号来保持电压(+5V)并且输出一个信号 LOR, 一个防止复制信息位置操作器 25, 用于检索 PES 标题检测器 10 的并行数据和计算一个附加复制信息域的位置; 一个计数器 26, 用于对复制信息位置操作器 25 的输出进行计数, 和一个 D-触发器 27, 用于保持 D-触发器 21 的输出的附加复制信息域。

下面将描述本发明的操作和效果。一般在磁带上再生或复制记录的数据的情况下, 要进行在两个系统之间的连接, 如在图 4 中所示。

通过这些连接, 由 VCR A 再生的一个 MPEG 比特数据流输入给一个卫星接收器或高清晰度 TV, 以致于不能够识别该比特数据流是否在一个屏上被显示, 或输入给 VCR B 并被记录在另一个视频带上。

为此, 根据本发明, 在由 VCR A 再生的比特数据流由 VCR B 被复制的情况下, 防止复制的信息从 VCR A 传送给 VCR B。VCR B 分析这个用比特数据流记录的信息。

在此, 包含在一个 GA 比特数据流中的防止复制信息的插入位置是非常受限制的, 因为它不应影响卫星接收器或高清晰度 TV 的解码器的解码, 以致于在一个监视器上正常地显示一个图像。该防止复制信息可以被插入到 MPEG 比特数据流的前端或插入到 PES 标题里面。

当 MPEG 比特数据流在图像组(GOP)的单元中被解码时, 使用它们的 GOP 起始码使对应的 GOPS 被分类。这在把初始化数据传送给一记录侧 VCR 时是有用的, 这是因为甚至当少量的数据被加到 MPEG 比特数据流的前端时也不会影响解码。

在重复传送信息中把防止复制信息插入到 PES 标题中是有用的, 这是

因为像 DSM 这样的记录介质的防止复制是利用 PES 标题和附加复制信息域的 CR 和 OC 特征位来决定的。在这种情况下，具有各种防复制方法。

首先，当从 PES 标题的附加复制信息域中检测出“不能复制”(“No Copy”)的一种方式时，VCR B 不能进入到它的记录方式中。

第二，当为了进行象 DAT 方式这样的防复制而检测出“允许复制”(“Copy permitted”)的一种方式时，VCR B 开始记录，但“不能复制”方式被记录在附加复制信息域以便中断从一个复制带上的再复制。这就意味着：由原始带，即第一源带可以形成第二源带，但是不能形成第三源带。

第三，用于“备用复制”(“Back-up Copy”)，由 VCR B 复制的带 B 仅能在 VCR A 中正常再生。根据该方法，再生侧 VCR A 用其自己固有的密码给比特数据流加密，并且将它记录在磁带上，以致于仅有再生侧 VCR A 能够把记录在磁带上的 MPEG 比特数据流解密。对于每个 VCR 装置，设置有由 VCR 的密码加密并记录在磁带 B 上的专门的密码。然而，用于记录磁带 B 的 VCR 装置是 VCR B 并且磁带 B 由 VCR A 的密码来加密，以致于 VCR A 的密码需要利用 GA 比特数据流待传送给 VCR B。

因此，当 VCR A 的密码信息作为在“备用复制”中的比特数据流之前一个标题被传送时，它被记录在磁带 B 的前端，这就满足了上述的防复制信息的插入位置。

这里，如在图 2 中所示，根据指示时间标记(PTS)/解码时间标记(PTS)和 DSM 策略方式域是否出现，附加复制信息域位置在 PES 标题中被变化。这种变化的位置必须被补偿。在此，通过附加复制信息传送的信息是一种由记录侧 VCR B 待进行的防复制方法。

在“备用复制”的方法中记录在图 11A 中所示的比特数据流情况下，在磁带上记录的比特数据流格式被确定，如在图 11B 中所示。

在此，加到 MPEG 比特数据流前面的一个标题区域被形成有一个磁带标题起始码，即标题识别码，和一个用于存储密码信息的密码信息组。在把 GOP 的单元中的 MPEG 比特数据流加密的情况下，利用信息包起始码首标和 PES 标题的比特数据流 ID 把加密单元分类。该加密单元是加密的一个基本单元，并且不管在加密单元，和加密算法以及密码选择的单元中是否进行加密，加密单元能够改变。在此，加密单元不必被加密直到 PES 标题的附加复制信息域。在附加复制信息域之后直到加密单元的结束为止进行

加密。第一“传送标题”不被加密。

下面将描述通过加标题来进行“备用复制”的操作。

首先，在复制中，当磁带 A 的记录数据被加密时，再生侧 VCR A 利用密码信息组的密码信息对其进行解密以产生信息 m。它的密码信息被加到标题并以图 11C 的格式被传送。

记录侧 VCR B 把从再生侧 VCR A 传送的密码信息记录在复制磁带 B 的标题，然后记录被加密的比特数据流。在此，当密码信息从再生侧传递到记录侧时，为了可靠，一个公用的密码加密可以用于该系统，因为该信息可以对非法翻录者公开。

即使该公用密码被公开，但由于大量的计算不能实时被处理，所以这样的公用密码加密系统确保了数据的保密。因此，当 MPEG 比特数据流直接地被加密时，这个系统是不适应的。当利用一个像 DES 这样的单元密码算法或比特数据流密码算法使 MPEG 比特数据流被加密并且在公用密码加密中使一个已使用的密码被加密时，能够完成“备用复制”。

在这种情况下，每个 VCR u 包括与公用密码相对应的加密算法  $E^{PK}_u$  和与保密密码相对应的解密算法  $D^{PK}_u$ 。加密算法  $E^{PK}_u$  采用了 VCR u 的一个有效密码(a power key)，而解密算法  $D^{PK}_u$  采用了 VCR u 的一个内部密码。

在此，内部密码可以对公众公开。由于其它的 VCR 利用内部密码来加密，所以再生侧 VCR A 传递在标题的密码信息组上的内部密码。记录侧 VCR B 随机地选择一个像 DES 这样的单元密码算法中使用的密码 Y 并且利用使用一个外部密码  $E^{PK}_A$  的公用密码加密系统给它加密。其结果被记录在复制磁带 B 的密码信息组上。

数据顺序地被分成加密单元并且被加密以及利用密码 Y 以单元密码算法被记录。用这种方法图 11D 的比特数据流被记录在复制带 B 上。

当在再生侧 VCR A 中再生复制带 B 时，利用其中数据被适当地解密的解密码  $D^{PK}_A[E^{PK}_A(Y)]$  能够恢复密码 Y。在其它的 VCRs 中，不能发现密码 Y，这就不能使比特数据流解码。

下面将描述用于进行这种操作的在图 5 中所示的本发明的一种实施例。

当用于磁带复制的再生开始时，再生部分 1 检测如在图 11A 中所示的磁带上记录的数据并且将该数据放大一个预定的电平。如在图 11B 中所示，密码插入部分 2 把一个具有磁带标题起始码的标题和一个密码信息组加到

在图 11A 中所示的再生部分 1 的 GA 比特数据流上。防复制信息被加到 PES 标题的附加复制信息域上以便形成在图 11C 中所示的格式。在此，解码部分 3 把在密码插入部分 2 中形成的比特数据流解码并且借助于一个接口把它作为并行数据传送给记录侧 VCR。

当图 11C 的比特数据流借助于接口被传送给记录侧 VCR 时，密码检测/校正部分 4 检测加到比特数据流上的密码信息组，且如果需要，校正该密码信息组。

防复制信息检测部分 5 搜索 PES 标题区域以便检测附加复制信息域。在此，虽然少量的信息被记录在附加复制信息域中，但是多余的信息被记录在比特数据流的几个区域中以便增加信息传送的可靠性。

防复制信息检测部分 5 从 PES 标题特征位中分离出 AC 特征位的值，以便计算附加复制信息域的位置，因为该位置在 PES 标题中变化。在此，当防复制信息校正部分 6 校正防复制信息检测部分 5 的输出时，加密部分 7 利用像 DES 这样的单元密码算法进行加密。在此，防复制信息校正部分 6 进行校正而输入数据被存储在一个 RAM 中。因此，加密部分 7 在记录部分 8 中的磁带上记录已加密的比特数据流。由于再生侧 VCR 的密码信息被加在复制带上，仅具有这种密码信息的 VCR 能够正常地再生磁带。

如在图 6 中所示，在防复制信息检测部分 5 中，PES 标题检测部分 10 检索密码检测/校正部分 4 的输出并输出一个标题检测信号 is-PES-标题。在标题检测信号 is-PES-标题输入时，防复制信息分离器 20 检测出附加复制信息域和 OC 和 CR 特征位。

用于检测 PES 标题的 PES 标题检测器 10 被形成如在图 7 中所示。当比特数据流 data-in 如在图 8A 中所示被输入时，与时钟 clk 同步的第一触发器 11 延迟一个预定时间以便输出如在图 8B 中所示的已延迟的比特数据流。第二触发器 12 把第一触发器 11 的输出延迟一个预定时间并且输出如在图 8C 中所示已延迟的比特数据流。

在此，信息包起始码检测部分 13 检索在图 8A 中所示比特数据流和在图 8B 和 8C 中所示的第一和第二触发器 11 和 12 的输出，以便检测 PES 标题的信息包起始码。当检测信号 is-pscp 输出为在图 8D 中所示的时，在其中连接为多级触发器的延迟器 15 根据时钟 clk 把检测信号 is-pscp 顺序地延迟。

同时，比特数据流 ID 码检测器 14 检索第二触发器 12 的输出并且检测 PES 标题的比特数据流 ID 区域。然后，在图 8E 中所示的检测信号 is-sid 输出给检测信号产生器 16。检测信号产生器 16 把延迟器 15 和比特数据流 ID 码检测器 14 的输出进行逻辑相乘，并且触发器根据时钟 clk 保持 AND 门的输出，以致于 PES 标题检测信号 is-PES-标题如在图 8F 中所示输出给防复制信息分离器 20。

在此，用于检测防复制信息的防复制信息分离器 20 被形成，如在图 9 中所示。当从 PES 标题检测器 10 输出的并在图 10A 中所示的并行数据被保持并且输出为在图 10B 中所示时，与在图 8F 中所示的 PES 标题检测器 10 的 PES 标题检测信号 is-PES-标题同步的 D-触发器 22 保持+5V 电压，以致于一个 HIGH 信号输出给 D-触发器 23、24 和 27 的清除端以便解除清除状态。

D-触发器 23 与在图 10B 中所示的 D-触发器 21 的输出的 CR 特征位相同步以保持电压 Vcc，以致于一个 HIGH 信号 LCR 被输出，如在图 10C 中所示。D-触发器 24 与 D-触发器 21 的输出的 OC 特征位相同步以保持电压 Vcc，以致于一个 HIGH 信号 LOC 被输出，如在图 10D 中所示。

防复制位置检测器 25 检索在图 10A 中所示 PES 标题检测器 10 的并行数据的 PD、TM 和 AC 的特征位，以便计算附加复制信息域的位置，其结果被输出给计数器 26，如在图 10E 中所示。接收 4 位值的计算器 26 进行计数以致于一个 HIGH 信号以一个预定计数值输出，如在图 10F 中所示。

与计数器 26 的 HIGH 输出 rco 同步的 D-触发器 27 保持来自在图 10B 所示的 D-触发器 21 的并行数据的附加复制信息域。该信息域如在图 10G 中所示地被输出。

如上面所述，在用于本发明的数字视频系统的防复制方法和装置中，一个密码信息被记录有一个比特数据流，以致于一个具有密码信息的 VCR 正常地再生磁带，由此防止磁带的非法复制。此外，对于密码信息传送，引入了公用密码加密码以便使非法复制者不能解除防复制，由此增加了防复制的可靠性。

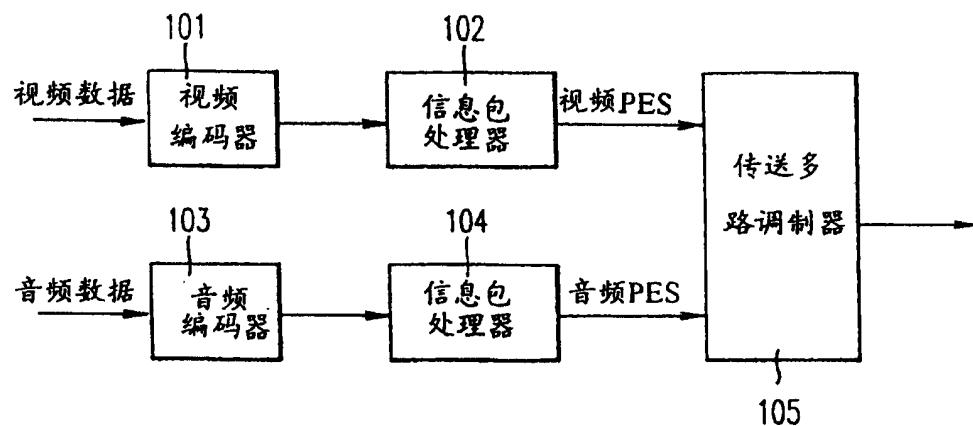


图 1

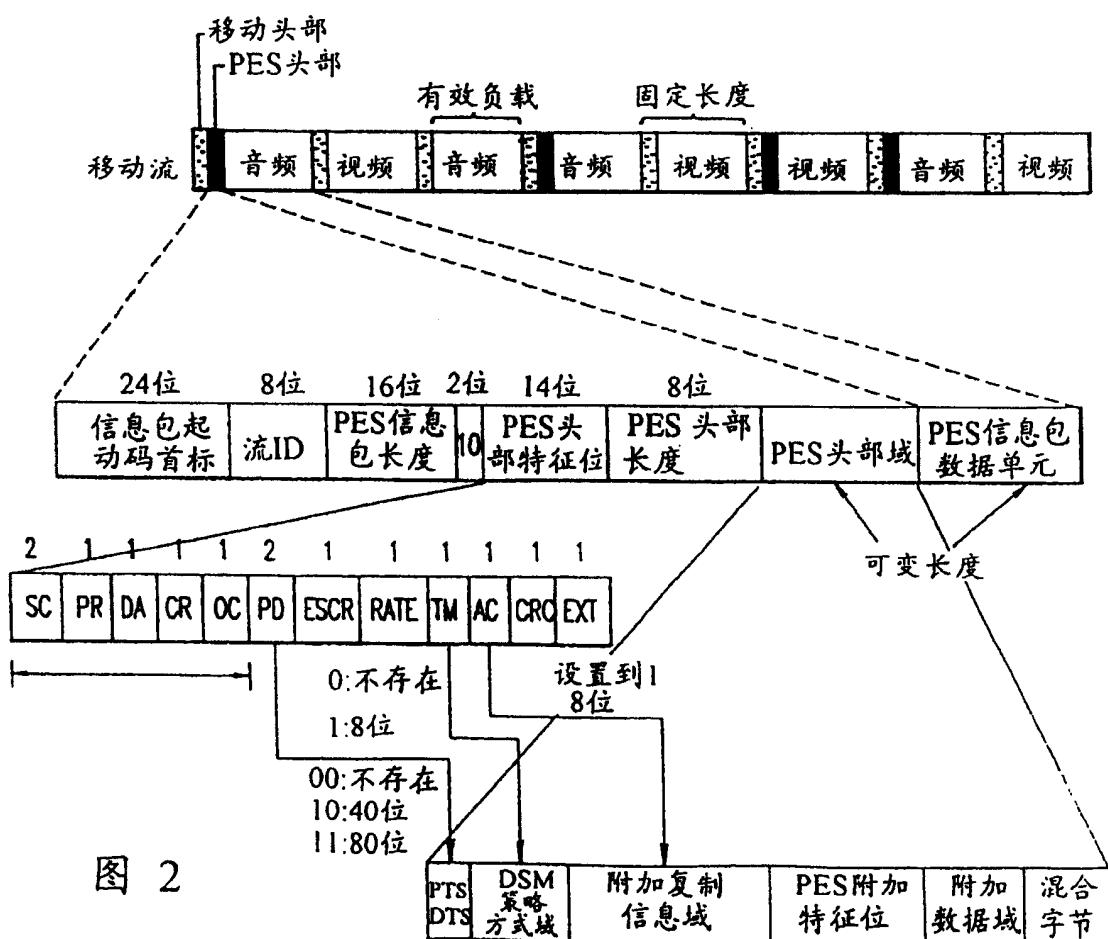


图 2

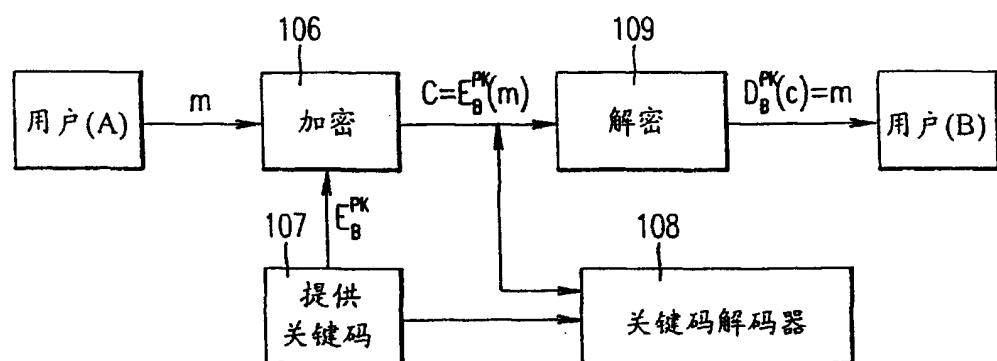


图 3

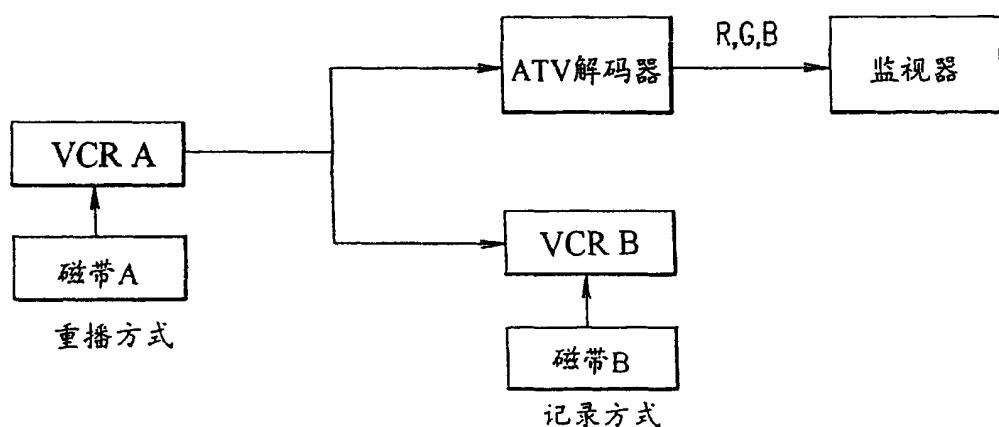


图 4

图 5

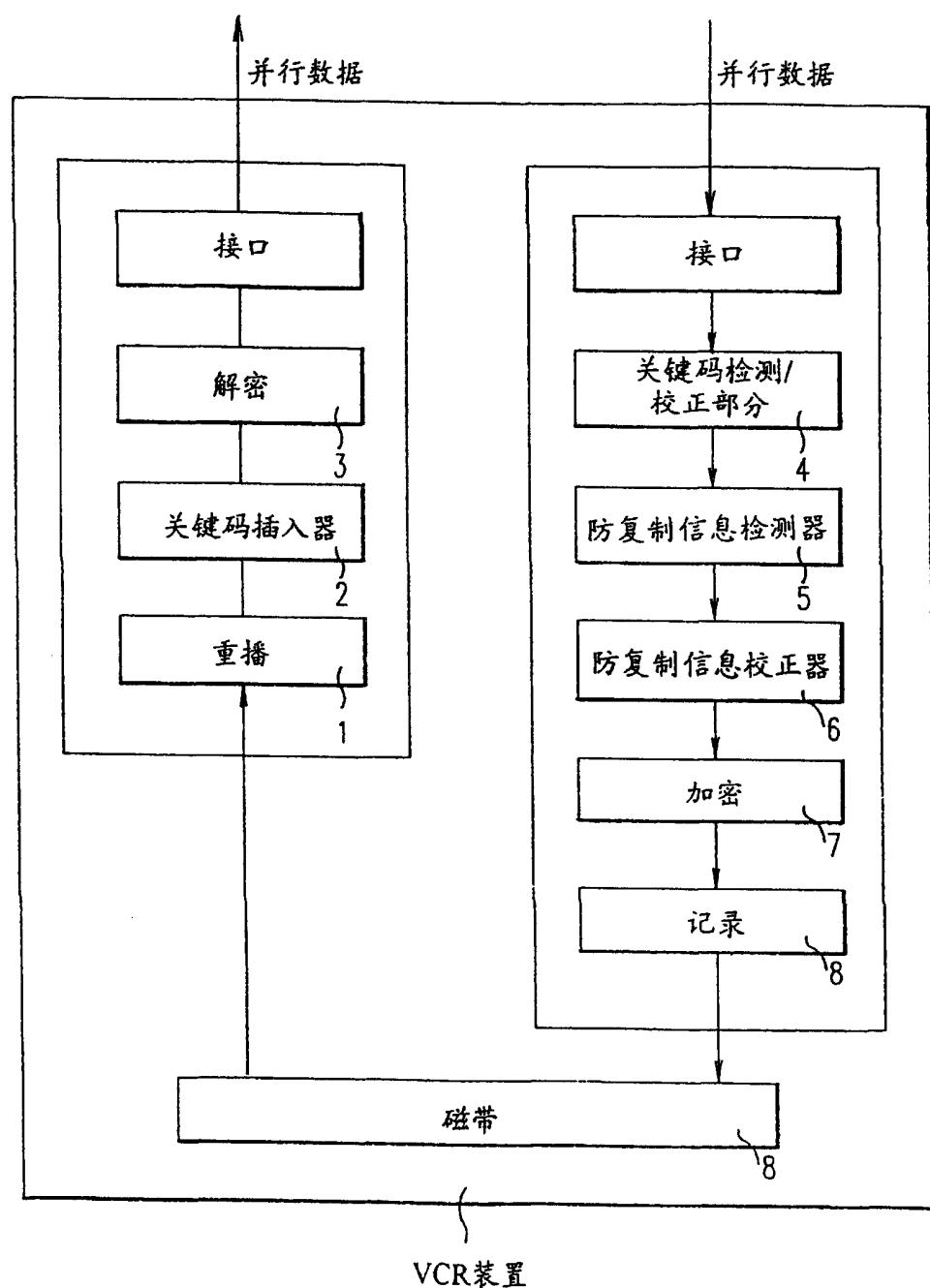


图 6

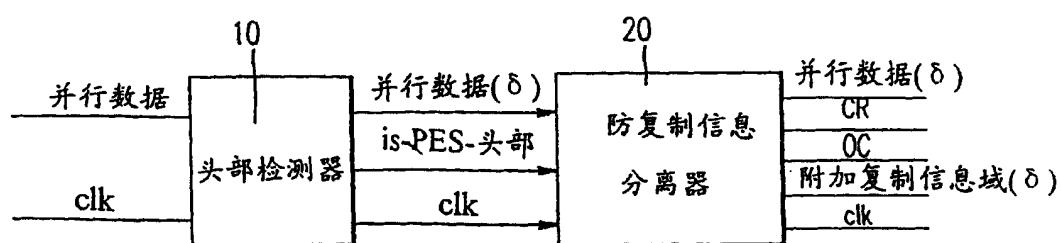
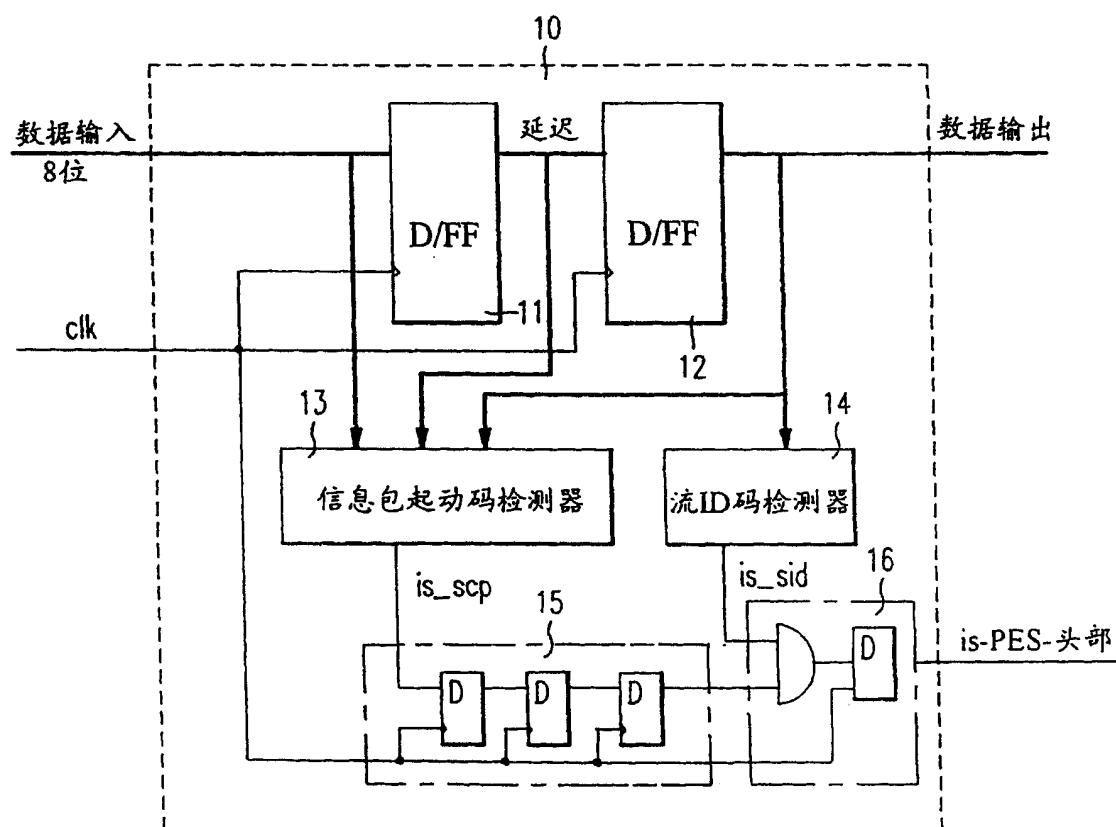


图 7



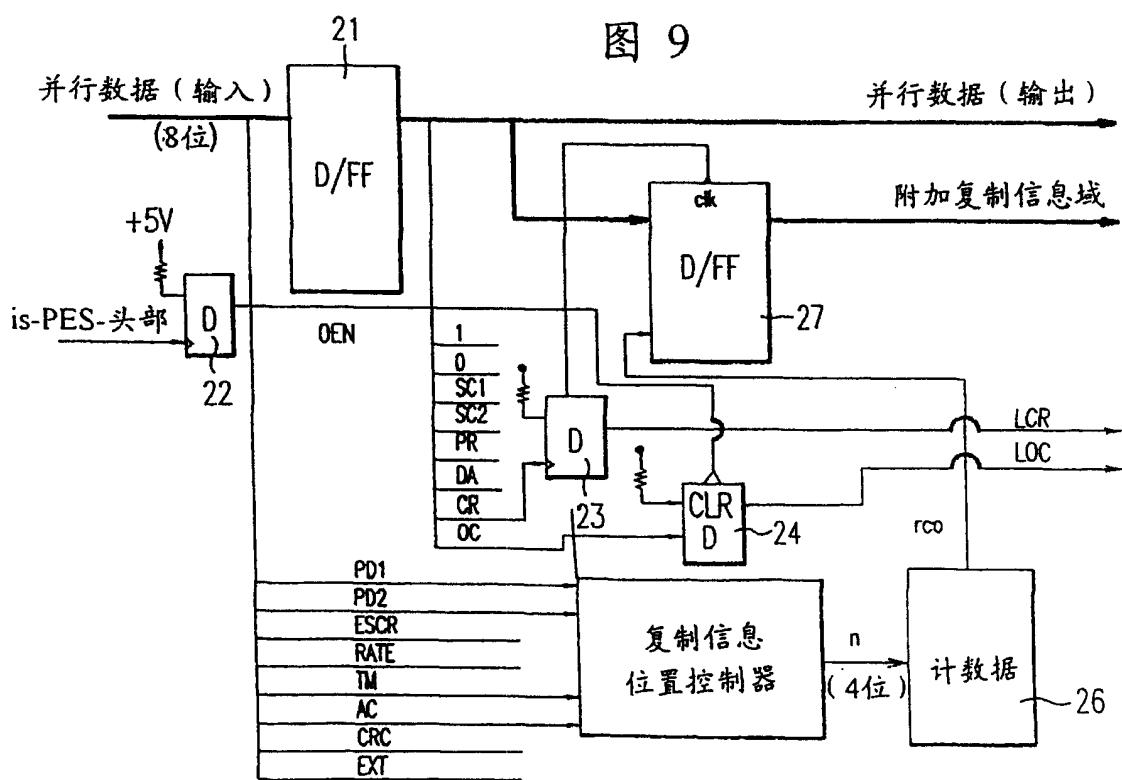
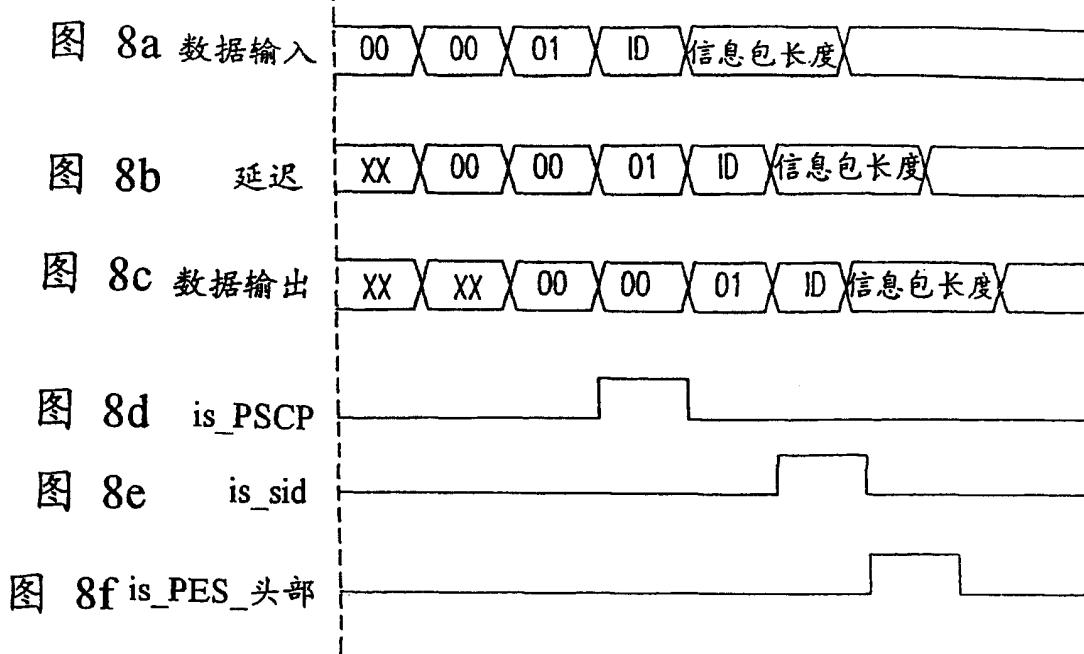


图 10a

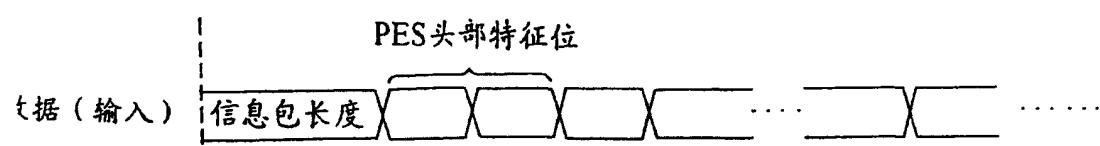


图 10b

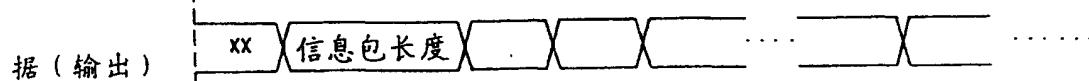


图 10c



图 10d



图 10e

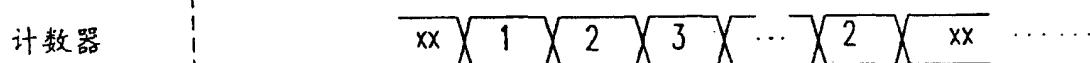


图 10f



图 10g

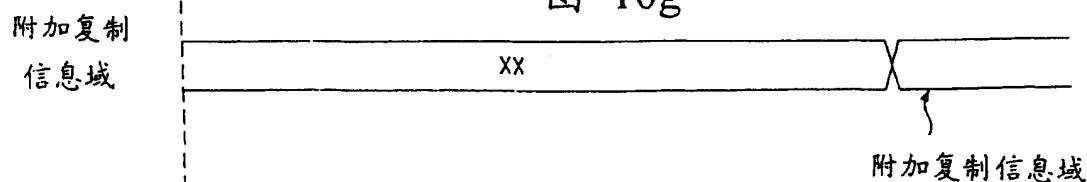
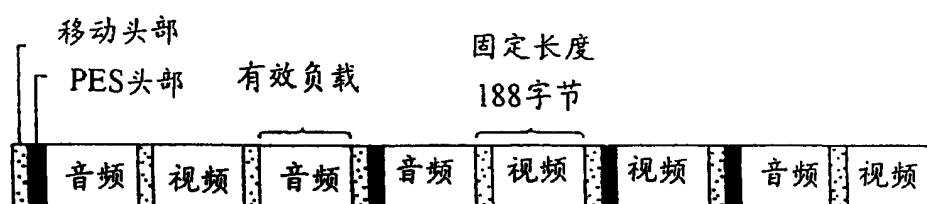


图 11a



磁带头部起动域

关键码  
信息组

头部区域

加密单元  
(可变长度)

图 11b

图 11c



图 11d

