

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.⁷
H04N 7/167



[12] 发明专利说明书

[21] ZL 专利号 98122600.0

[45] 授权公告日 2004 年 9 月 29 日

[11] 授权公告号 CN 1169367C

[22] 申请日 1998.11.25 [21] 申请号 98122600.0

[30] 优先权

[32] 1997.11.26 [33] FR [31] 9714844

[71] 专利权人 汤姆森多媒体公司

地址 法国布洛涅

[72] 发明人 马里奥·德维托

让-伯纳德·费希尔

维罗尼克·普拉

审查员 韩 岳

[74] 专利代理机构 北京市柳沈律师事务所

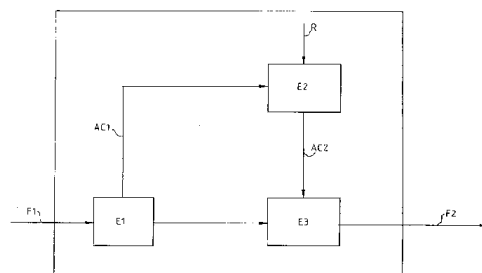
代理人 吕晓章

权利要求书 1 页 说明书 6 页 附图 2 页

[54] 发明名称 加扰和解扰数字视频数据的方法

[57] 摘要

本发明涉及一种对 MPEG2 视频格式的视频数据加扰的方法以及解扰根据本发明的方法加扰的数据的方法。加扰的视频数据是从“离散余弦变换”操作(DCT)产生的系数 AC 和/或 DC, 它们与以“内部”模式编码的至少一个图像的至少一个块有关。本发明应用于条件访问系统例如付费电视系统。



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

1. 一种用于对 MPEG2 视频格式的视频数据加扰的方法，视频数据表示以“内部”模式编码的至少一个图像的至少一个块并且包括从离散余弦变换操作产生的数据，以及对于每一块包括表示块的像素的平均强度的第一系数和表示块的像素之间强度变化的系数，其特征在于所述方法包括在至少一个相同的块内的置换步骤，该置换步骤在于根据置换顺序、在表示块的像素之间强度变化的系数其自身中进行置换以构成一组新的系数。

2. 一种用于对 MPEG2 视频格式的视频数据加扰的方法，视频数据表示以“内部”模式编码的至少一个图像的至少一个块并且包括从离散余弦变换操作产生的数据，以及对于每一块包括表示块的像素的平均强度的第一系数和表示块的像素之间强度变化的系数，其特征在于所述方法包括在命令的作用下，将选择的系数代替表示块的像素平均强度的系数的步骤。

3. 根据权利要求 2 所述的方法，其特征在于随机地选择命令。

4. 一种用于在解扰密钥的作用下解扰加扰的视频数据的方法，其中所述视频数据是根据权利要求 1 的方法加扰的数据以及，其中所述方法包括接收解扰密钥和用该解扰密钥解扰的步骤，所述解扰密钥包括表示块的像素之间的强度变化的系数的置换顺序。

5. 根据权利要求 4 的方法，其特征在于所述接收的解扰密钥是被密钥加密的。

6. 一种用于在解扰密钥的作用下解扰加扰的视频数据的方法，其中视频数据是根据权利要求 2 的方法加扰的数据以及其中所述方法包括接收解扰密钥和用该解扰密钥解扰的步骤，所述解扰密钥是表示块的像素之间的平均强度的系数。

7. 根据权利要求 6 的方法，其特征在于所述接收的解扰密钥是被密钥加密的。

加扰和解扰数字视频数据的方法

5 技术领域

本发明涉及加扰数字视频数据的方法以及解扰根据本发明的加扰方法加扰的数字视频数据的方法。

本发明特别应用于条件访问系统，对于该系统视频数据根据 MPEG2 视频标准格式化并且根据 MPEG2 系统传送标准传输。

10

背景技术

通过非限定的例子，如一个上述的条件访问系统可以是一个广播加扰节目的付费电视系统。

如本领域的技术人员所公知的，在根据 MPEG2 标准操作的条件访问系统的范围内，以这样一种方式加扰视频数据使得在加扰后，它们不再遵守 MPEG2 视频标准。

在接收加扰节目的用户已经获得对节目解扰的资格的情况下，解扰加扰的视频数据使得恢复到 MPEG2 视频标准。然后用户的 MPEG2 译码器能够译码它接收的解扰视频数据。

20 在用户没有获得解扰加扰的节目的资格的情况下，不解扰视频数据。然后用户的 MPEG2 译码器完全不能识别视频数据。没有任何图像出现在屏幕上：屏幕是黑的。

完全没有图像甚至阻止瞥见广播节目，因此使得不可能吸引任何潜在的未来用户对于分配节目的供应商的注意。

25 本发明没有这个缺点。

发明内容

这样，本发明涉及加扰 MPEG2 视频格式的视频数据的方法，视频数据表示以“内部(INTRA)”模式编码的至少一个图像的至少一个块，并且包括从“离散余弦变换”操作产生的数据(AC, DC)，以及对于每一块包括表示该块的像素的平均强度的第一系数(DC)和表示该块的像素之间强度变化的至

少一个第二系数(AC)。通过用于处理从兼容于 MPEG2 视频标准的“离散余弦变换”操作产生的数据(AC, DC)的操作执行视频数据的加扰。

本发明还涉及解扰加扰的视频数据的方法，在解扰密钥的作用下完成视频数据的解扰。视频数据是根据本发明的上述解扰方法加扰的数据，并且解扰密钥包括从用于处理从“离散余弦变换”操作产生的数据的操作中产生的至少一个数据。

本发明还涉及加扰 MPEG2 视频格式的视频数据的装置，视频数据表示以“内部(INTRA)”模式(I)编码的至少一个图像的至少一个块，并且包括从“离散余弦变换”操作产生的数据(AC, DC)，以及对于每一块包括表示该块的像素的平均强度的第一系数(DC)和表示该块的像素之间强度变化的至少一个第二系数(AC)，其特征在于它包括通过用于处理从兼容于 MPEG2 视频标准的“离散余弦变换”操作产生的数据(AC, DC)的操作执行视频数据的加扰的机构。

本发明还涉及解扰根据本发明的上述加扰方法加扰的视频数据的装置，视频数据的解扰在解扰密钥的作用下完成，其特征在于它包括在解扰密钥的作用下解扰视频数据的装置，解扰密钥包括从用于处理从“离散余弦变换”操作产生的数据的操作产生的至少一个数据。

本发明还涉及一种根据 MPEG2 视频标准编码的视频数据的译码器，包括用于解扰加扰的视频数据的装置，其特征在于解扰装置是一个根据本发明如上述装置的解扰装置。

本发明的一个优点是它实现加扰和解扰与 MPEG2 视频标准兼容的视频数据的方法。

具体地，本发明提供一种用于对 MPEG2 视频格式的视频数据加扰的方法，视频数据表示以“内部”模式编码的至少一个图像的至少一个块并且包括从离散余弦变换操作产生的数据，以及对于每一块包括表示块的像素的平均强度的第一系数和表示块的像素之间强度变化的系数，其特征在于所述方法包括在至少一个相同的块内的置换步骤，该置换步骤在于根据置换顺序、在表示块的像素之间强度变化的系数其自身中进行置换以构成一组新的系数。

一种用于对 MPEG2 视频格式的视频数据加扰的方法，视频数据表示以“内部”模式编码的至少一个图像的至少一个块并且包括从离散余弦变换

操作产生的数据，以及对于每一块包括表示块的像素的平均强度的第一系数和表示块的像素之间强度变化的系数，其特征在于所述方法包括在命令的作用下，将选择的系数代替表示块的像素平均强度的系数的步骤。

一种用于在解扰密钥的作用下解扰加扰的视频数据的方法，其中所述
5 视频数据是上述加扰方法加扰的数据以及，其中所述方法包括接收解扰密钥和用该解扰密钥解扰的步骤，所述解扰密钥包括表示块的像素之间的强度变化的系数的置换顺序。

一种用于在解扰密钥的作用下解扰加扰的视频数据的方法，其中视频数据是根据上述加扰方法加扰的数据以及其中所述方法包括接收解扰
10 密钥和用该解扰密钥解扰的步骤，所述解扰密钥是表示块的像素之间的平均强度的系数。

附图说明

阅读参照附图所给出的优选实施例将可以看出本发明的其他特征和优
15 点，其中

- 图 1 表示本发明第一实施例的用于加扰视频数据的方法；
- 图 2 表示本发明第二实施例的用于加扰视频数据的方法；

具体实施方式

20 图 1 表示本发明第一实施例的用于加扰视频数据的方法。

根据本发明的方法处理的数据流 F1 包括根据 MPEG2 视频标准编码的一系列视频数据包。

根据 MPEG2 视频标准的编码利用信号的特性减少它的比特率。

实现的编码算法利用要被编码图像的空间冗余度和时间冗余度描述了
25 按块的图像。

空间冗余度主要借助于一系列的三种操作估计：一种通常称为“离散余弦变换”并且表示为 DCT 的操作，一种量化从 DCT 产生的系数的操作以及一种描述从 DCT 产生的量化系数的可变长度编码的操作。

时间冗余度通过运动补偿操作分析，该操作包括经过当前图像每一块
30 的转换操作，寻找位于参考图像中的最类似的块。时间冗余度的分析导致转换矢量、即通常称为运动矢量的字段以及预测误差的确定，该误差是当

前图像的信号和通过运动补偿预测的图像信号之间的差值。随后根据空间冗余度原理分析预测误差。

根据MPEG2视频标准的编码是预测类型的编码。因此与它有关的译码过程必须有规则地重新初始化，使得保护信号免于例如由于译码器从一个节目到另一个节目反转的传输误差或任何信号中断。

为此，MPEG2视频标准规定图像必须周期性地以空间模式，也就是说根据单独利用空间冗余度的模式编码。以空间模式编码的图像通常称为“内部”图像或I图像。

本发明的加扰方法应用于相应至少一个I图像的至少一个块的视频数据的加扰。

表征一个I图像块的视频数据包含通常表示为系数DC(DC代表“直流”)的系数和若干通常表示为系数AC(缩写AC代表“交流”)的系数。系数DC代表图像块的像素的平均强度而系数AC代表块的像素之间的强度变化。

根据本发明的第一实施例，对于至少一个I图像的至少一个块，包含在流F1中并且在图1中表示为AC1的系数AC从流F1中提取出来。从流F1中系数AC1的提取由图1中操作E1符号表示。

随后将提取的系数AC1以这样一种方式在它们中间置换，使得构成系数AC的一个新组AC2。各种系数AC1最好根据置换顺序(permutation rank)R置换，该置换顺序R从系数AC的置换中包含的第一组连续块到另一组块不同。然而，本发明也涉及置换顺序R对于系数AC的置换中包含的所有连续块是相同的情况。系数AC1的置换由图1中操作E2符号表示。

在上述置换后，在流F1内系数AC2代替系数AC1以便构成数据流F2。

提取和置换系数AC1的操作以及用系数AC2代替系数AC1的操作通过例如编程微处理器完成。

在代替系数AC1之后获得的数据流F2构成根据本发明第一实施例的加扰的数据流。为了构成根据MPEG2系统标准的数据流，加扰形式的视频数据与根据MPEG2音频标准的音频数据和涉及关于所分配节目的各项信息的数据以一种公知的方式被多路复用。

本发明的一个优点是它使得容易调制接收的非解扰图像的失真。这是因为块的各种系数AC的置换不仅能够大些或小些，而且完成系数置换的I图像数也能够自己改变。

图2表示本发明第二实施例的用于加扰视频数据的方法。

根据图2表示的实施例，对于至少一个I图像的至少一个块，包含在流F1中并且在图2中表示为DC1的系数DC从流F1中提取。各种系数DC1的提取由图2中的操作E4符号表示。

- 5 然后，在命令C的作用下，从流提取的系数DC1中产生新的系数DC2。命令C最好是一个随机命令。随后在流F1内用新的系数DC2代替系数DC1。

从系数DC1产生系数DC2以及在流F1中用系数DC2代替系数DC1分别地由图2中操作E5和E6符号表示。

- 10 用于提取系数DC1、在命令C的作用下产生系数DC2以及将产生的系数DC2代替系数DC1的操作由例如微处理器完成。

在代替系数DC1之后获得的数据流F3构成加扰的数据流。为了根据MPEG2系统标准构成数据流，加扰形式的视频数据与根据MPEG2音频标准的音频数据以及涉及关于所分配节目的各项信息的数据一起被多路复用。

- 15 根据本发明的这个第二实施例，同样有益的是能容易地调制接收的非解扰图像的失真。这同样是因为完成系数DC替代的I图像数越大，接收的图像的失真越严重。

- 20 有益的是，图1和2中描述的两种加扰方法相互之间不是排斥的。因此，根据本发明的第三种加扰方法涉及到实现图1中描述的方法和图2中描述的方法的过程。根据本发明的这个第三实施例，对于置换系数AC的同一个块可以或不可以具有代替系数DC的另一个系数。

如前面提到的，本发明还涉及一种用于解扰根据图1中描述的加扰方法和/或图2中描述的加扰方法加扰的视频数据的方法。

- 25 为了实现根据图1描述的方法加扰的视频数据的解扰，把在置换中包含的各个块的系数AC1的连续的置换顺序R传送到解扰装置。连续的置换顺序R则是用于解扰加扰的数据的密钥。

最好在根据具有密钥K的算法被加密后把连续的置换顺序R传送到解扰装置。置换顺序R的传输最好在包含加扰的视频数据的流中完成。

为了实现根据图2描述的方法加扰的视频数据的解扰，作为解扰密钥传送到解扰装置的是系数DC1。

- 30 最好在用具有密钥K的算法加密后，各种系数DC1传送到解扰装置。系数DC1的传输最好在包含加扰的视频数据的数据流中完成。

如上所述，在加扰方法实现根据图1的方法和根据图2的方法的情况下，解扰密钥包括置换顺序R或系数DC1，或者置换顺序R和系数DC1的组合。

不管数据加扰的方式，即根据图1的方法，根据图2的方法，或者根据图1和2的另外一种方法，通过用于加扰数据的操作的逆操作，在解扰密钥5的作用下，对数据解扰。这些逆操作通过例如编程微处理器完成。

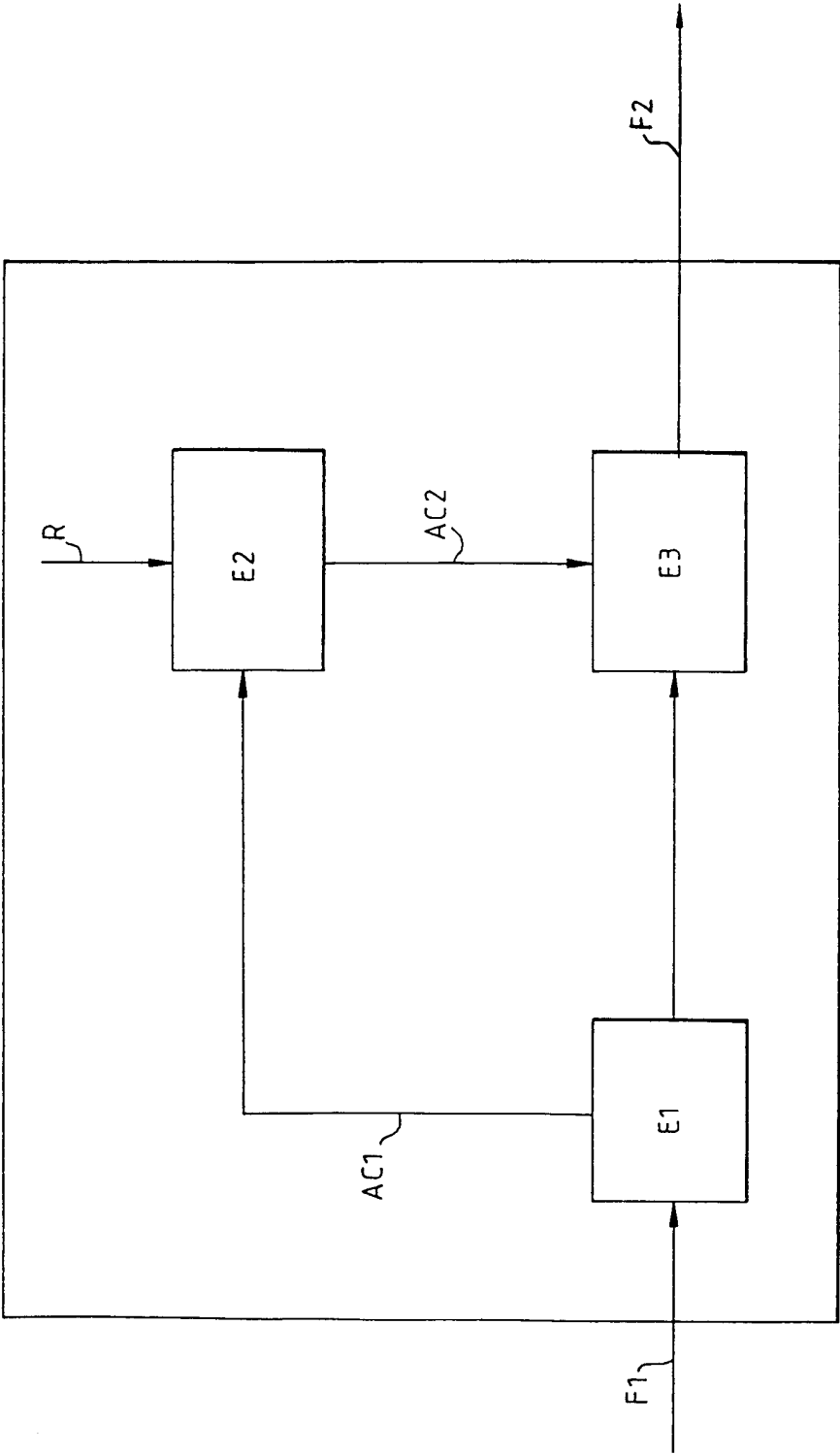


图 1

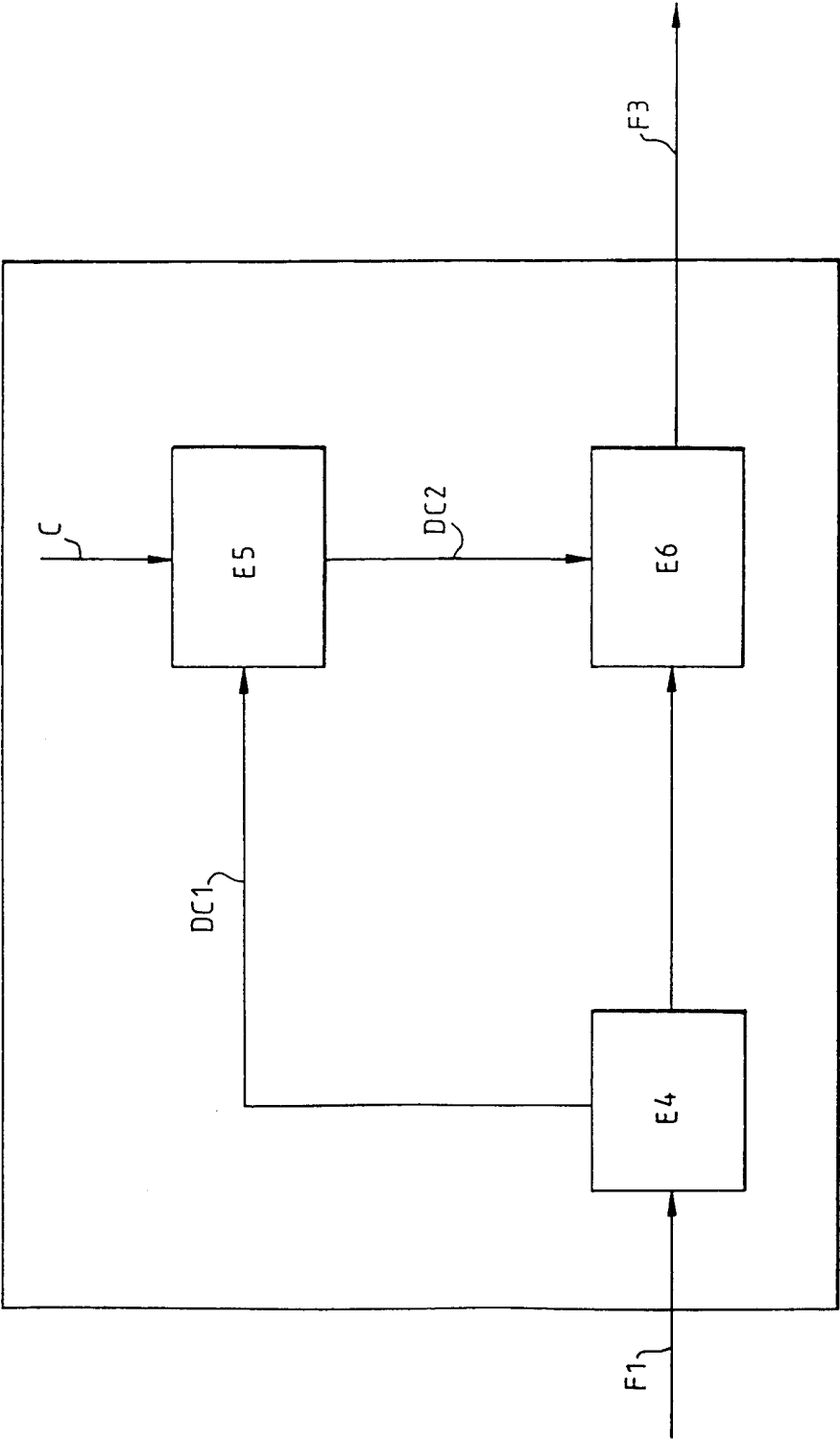


图 2