(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103281564 A
(43)申请公布日 2013.09.04

(21)申请号 201210599357.7

(22)申请日 2012.12.28

(30)优先权数据
11306804.3 2011.12.29 EP

(71)申请人 汤姆森特许公司
地址 法国伊西莱穆利诺

(72)发明人 A·罗伯特 F·勒费布弗里
B·丘佩奥

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 史新宏

(51)Int.Cl.
H04N 21/2347(2011.01)
H04N 21/4405(2011.01)

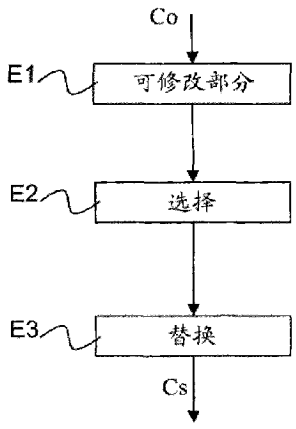
权利要求书2页 说明书6页 附图3页

(54)发明名称

选择性加扰比特流的方法

(57)摘要

本发明涉及一种选择性加扰编码比特流的方法，该方法包括：在该编码比特流中确定至少一个可修改部分的步骤，其中包含选择性可修改部分的已修改编码比特流关于编码标准的符合性不受影响；选择至少一个可修改部分的步骤，其中与该编码比特流的呈现相比，包含已选选择性可修改部分的符合的已修改编码比特流的呈现在感知上受影响；对于该至少一个已选可修改部分的每一个，用选择性可修改部分替换编码比特流中的初始可修改部分导出符合的选择性加扰比特流的步骤。本发明还涉及相关的解扰方法。



CN 103281564 A

1. 一种选择性加扰编码比特流 (C_0) 的方法，其特征在于，该方法包括：

在该编码比特流中确定至少一个可修改部分的步骤 (E1)，其中，包含选择性可修改部分的已修改编码比特流关于编码标准的符合性不受影响；

选择该至少一个可修改部分的步骤 (E2)，其中，与该编码比特流 (C_0) 的呈现相比，包含该选择性可修改部分的符合的已修改编码比特流的呈现在感知上受影响；

对于该至少一个已选可修改部分的每一个，用该选择性可修改部分替换编码比特流中的初始可修改部分导出符合的选择性加扰比特流 (C_S) 的步骤 (E3)。

2. 根据权利要求 1 的方法，其中，选择该至少一个可修改部分的步骤 (E2) 包括计算表示呈现后在符合的选择性加扰比特流 (C_S) 和编码比特流 (C_0) 之间的失真的感知性的度量。

3. 根据权利要求 2 的方法，其中，根据在一组函数中的至少一个函数计算该度量，该组函数包括 PSNR、SSIM、MSE。

4. 根据权利要求 1 的方法，其中，选择该至少一个可修改部分的步骤 (E2) 进一步被一种确定标准控制，所述确定标准专用于一个应用。

5. 根据权利要求 1 的方法，其中，在该编码比特流中确定至少一个可修改部分的步骤 (E1) 进一步包括对该编码比特流使用水印算法。

6. 根据权利要求 1 的方法，其中，该编码比特流 (C_0) 的长度与该符合的选择性加扰比特流 (C_S) 的长度相同。

7. 根据权利要求 1 的方法，其中，该方法进一步包括传送元数据的步骤，所述元数据包括该编码比特流的初始可修改部分和该至少一个已选可修改部分的每一个在该编码比特流中的位置。

8. 根据权利要求 7 的方法，其中，传送元数据的步骤进一步包括加密元数据的步骤 (E4)。

9. 根据权利要求 8 的方法，其中，使用第一密钥加密第一组元数据和使用第二密钥加密第二组元数据。

10. 根据权利要求 7 的方法，其特征在于，传送元数据的步骤包括将元数据复用到符合的已修改比特流 (C'_S) 的步骤 (E5)。

11. 根据权利要求 10 的方法，其特征在于，该比特流是 H.264 编码比特流，并且复用步骤 (E5) 包括将加密的元数据插入到符合的已修改比特流的 SEI 消息。

12. 根据权利要求 1 到 11 中任一项的方法，其特征在于，该比特流是 H.264CABAC 编码比特流，以及该比特流的可修改部分是语法元素。

13. 根据权利要求 1 到 11 中任一项的方法，其特征在于，该比特流是 H.264CAVLC 编码比特流，以及该比特流的可修改部分是语法元素。

14. 一种用于解扰选择性加扰比特流的方法，其特征在于，该选择性加扰比特流包括至少一个已修改部分，其中，所述选择性加扰比特流是符合有关编码标准的，并且其中，与解扰的比特流的呈现相比，该选择性加扰比特流的呈现在感知上受影响，该解扰方法包括：

接收元数据的步骤 (D1)，所述元数据包括该比特流的初始部分和该选择性加扰比特流中的该至少一个已修改部分的每一个在比特流中的位置；

根据接收的位置确定该选择性加扰比特流的该至少一个已修改部分的步骤 (D2)；

用接收的初始部分替换该至少一个已修改部分导出解扰比特流的步骤 (D3)。

15. 一种选择性加扰编码比特流 (C_0) 的设备，其特征在于，该设备包括：

在该编码比特流中确定至少一个可修改部分的装置，其中，包含选择性可修改部分的已修改编码比特流关于编码标准的符合性不受影响；

选择该至少一个可修改部分的装置，其中，与该编码比特流 (C_0) 的呈现相比，包含该选择性可修改部分的符合的已修改编码比特流的呈现在感知上受影响；

对于该至少一个已选可修改部分的每一个，用该选择性可修改部分替换编码比特流中的初始可修改部分导出符合的选择性加扰比特流 (C_S) 的装置。

16. 一种表示选择性加扰编码比特流 (C_S) 的数据结构，其特征在于，该数据结构相较于初始编码比特流 (C_0) 包括至少一个已修改部分，

其中，该选择性加扰编码比特流的关于编码标准的符合性不受影响；

以及其中，相较于该初始编码比特流 (C_0) 的呈现，所述选择性加扰编码比特流的呈现在感知上受影响；

并且进一步包括为该至少已修改部分的每一个替换元数据，所述替换元数据包括该初始编码比特流的初始部分和在该选择性加扰编码比特流中的位置。

选择性加扰比特流的方法

技术领域

[0001] 本发明涉及内容保护。更具体地，本发明涉及一种选择性加扰编码比特流的方法。

背景技术

[0002] 这一部分的目的是向读者介绍各个方面的技术，这些技术可能涉及下文描述的和/或声称的本发明的各个方面。相信这种讨论有助于向读者提供背景信息来帮助其更好地理解本发明的各个方面。据此，应该理解的是这些将被读到的陈述内容应该从这个角度看，而不是承认其是现有技术。

[0003] 人们早就知道通过加密来保护内容，尤其是在条件接收电视系统或者在数字版权管理 (DRM) 系统中。因而，使用一个或多个加密密钥来加密内容。

[0004] 最近，已经设计了选择性加密来应对标准加密的性能问题。选择性加密内容的一部分，这样为了将内容全部呈现给用户，解密那部分内容对于解码内容来说是绝对强制的。2008 年 6 月 30 日以 Thomson Licensing 的名义提交的名称为“Methods and apparatuses for selective data encryption(选择性数据加密的方法和系统)”的专利申请EP2141923描述了一种提出与标准加密具有同样安全等级的选择性加密算法。选择性加密算法的一个优点在于允许使用专用于每个用户的密钥进行加密，这比标准加密方法在服务器实时资源方面具有低得多的成本。然而，选择部分内容来加密的算法可能会改变压缩流的符合性(compliance)，从而禁止任何呈现 (rendering) 并导致视频解码器崩溃的。

[0005] 因此需要一种生成具有选择性加密算法性能的被保护比特流的方法，其中作为结果的被保护比特流通过仅仅影响呈现的方式依然符合译码进程。

发明内容

[0006] 本发明的目的是通过提供一种不会修改比特流的符合性地加扰编码比特流的方法来克服现有技术的至少一个不足。本发明的理念是修改编码比特流的初始部分，例如感知地影响修改内容的呈现，但是并不会影响关于编码格式的符合性。为解扰修改的比特流，提供通过标准加密算法加密的比特流的初始部分。

[0007] 加扰是呈现难以理解的声音、图像和数据的过程。在解扰后，不应感觉到声音、图像或数据的任何瑕疵或失真。因此，通过加扰内容，人们应该大体上理解，相较于初始内容，生成在感知上受影响的呈现的内容，这样用户不能忍受。因此为了欣赏解扰内容的呈现，为了解扰过程用户需要初始部分和当初始部分被加密时的有利解密密钥。

[0008] 为了这个目的，本发明涉及一种选择性加扰编码比特流的方法，包括：在编码比特流中确定至少一个可修改部分的步骤，其中，包含选择性可修改部分的已修改编码比特流关于编码标准的符合性不受影响；选择至少一个可修改部分的步骤，其中，与初始编码比特流的呈现，包含选择性可修改部分的符合的已修改编码比特流的呈现在感知上受影响；对于至少一个已选择的可修改部分的每一个，用选择性可修改部分替换编码比特流中的初始可修改部分，导出一个符合的选择性加扰比特流的步骤。

[0009] 本发明非常有利地适用于生成不会破坏解码器的符合的加扰比特流。

[0010] 根据本发明的一个特别有利地特性，选择至少一个可修改部分的步骤包括计算代表呈现后在符合的已修改编码比特流和初始编码比特流之间的失真的感知性的度量。根据在一组函数中的至少一个函数计算该度量，该组函数包括 PSNR、SSIM、MSE。

[0011] 根据本发明的一个特别有利地特性，选择至少一个可修改部分的步骤进一步被确定的标准控制，该标准专用于一个应用。本发明的这个特性提供一种用于生成例如被应用需求控制的比特流的解决方案，该方案只加扰图像的较高部分。从而能够控制加扰的空间和时间延伸以及归因于加扰的退化强度。

[0012] 在第一个优选的实施例中，在编码比特流中确定至少一个可修改部分的步骤进一步包括对初始编码比特流采用水印算法。根据本发明的一个特别有利地特性，编码比特流的长度和符合的选择性加扰比特流的长度相同。

[0013] 在第二个优选的实施例中，该方法进一步包括传送元数据的步骤，该元数据包括编码比特流的初始可修改部分和至少一个选择的可修改部分的每一个在比特流中的位置。根据本发明的一个特别有利地特性，传送元数据的步骤进一步包括加密元数据的步骤。根据本发明的其他特别有利地特性，采用第一密钥加密第一组元数据以及采用第二密钥加密第二组元数据。该特性有利地提供了某种程度的加扰可伸缩性。

[0014] 根据其他特别有利地特性，传送元数据的步骤包括复用元数据至符合的已修改比特流的步骤。在一种变形中，其中该比特流是 H.264 编码比特流，复用步骤包括将已加密元数据插入符合的已修改编码比特流的 SEI 消息中。

[0015] 在第三优选实施例中，该比特流是 H.264CABAC 编码比特流并且该比特流的该可修改部分是语法元素。

[0016] 在第四优选实施例中，该比特流是 H.264CAVLC 编码比特流并且该比特流的该可修改部分是语法元素。

[0017] 根据另一个方面，本发明还涉及用于解扰选择性加扰比特流的方法，其中该选择性加扰比特流包括至少一个已修改部分；其中该选择性加扰比特流是符合有关编码标准的，并且其中选择性加扰比特流的呈现与解扰的比特流的呈现相比在感知上受影响。该解扰方法包括接收元数据的步骤，该元数据包括比特流的初始部分和该选择性加扰比特流中的至少一个已修改部分的每一个在比特流中的位置；根据接收的位置确定该选择性加扰比特流的该至少一个已修改部分的步骤；用接收到的初始部分替换该至少一个已修改部分导出解扰比特流的步骤。

[0018] 为加扰方法描述的任何特性或实施例也与解扰方法兼容。

附图说明

[0019] 在所包含附图的帮助下，通过将被说明的对本发明非限制性实施例的描述，本发明的其他特性和优点将会显现。

[0020] 图 1 表示根据第一实施例的加扰编码比特流的方法，

[0021] 图 2 表示根据第二实施例的加扰编码比特流的方法，

[0022] 图 3A 和 3B 表示根据一个特定实施例的初始编码比特流和被保护 / 加扰的编码比特流，

[0023] 图 4 表示根据一个特定实施例的解扰比特流的方法，以及

[0024] 图 5 表示根据特定实施例的加扰 / 解扰比特流的设备。

具体实施方式

[0025] 作为说明性示例，接下来的描述将致力于电子内容（如为优化分配而压缩的那些内容）的保护。至于内容，可以被理解为任何电影、音乐、文本或视频游戏。

[0026] 图 1 表示根据一个特定实施例的加扰编码比特流的方法。

[0027] 根据描述实施例的本方法修改编码比特流。通过编码压缩载有电子内容的流得到编码比特流。在编码标准中，本发明符合包括压缩音频内容、压缩 3D 数据的 MPEG-2、MPEG-4、H.264/AVC 或 VC-1 比特流。

[0028] 在步骤 E1 中，确定编码比特流中潜在的可修改部分，这样对于已修改的比特流不会影响解码进程。其中对于比特流中可修改部分的值被替换值取代的这种已修改比特流仍然符合编码标准。根据一种变形，2007 年 11 月 2 日以 Thomson Licensing 的名义提交的名称为“Modifying a coded bitstream（修改编码比特流）”的专利申请 WO2008/118145 描述了一种修改熵编码比特流的方法。该方法包括一些部分解码和重编码级来确定适用于承载水印信息的编码比特流的潜在的可修改部分。在 H.264 视频流的情况中，该方法包括搜索可修改的 CABAC 语法元素。从而该方法包括搜索预测图像间的一些块的运动矢量差的可修改的旁路部分。编码比特流被部分译码直到找到可接受的语法元素。修改的语法元素然后被 CABAC 重编码来选择不影响比特流的符合性的那些元素。根据另一种变形，为了检查比特流的符合性，一种包括一些任意的已修改比特流的部分解码级的方法与本发明兼容。在这种变形中，比特流的长度被自然地保留。

[0029] 在步骤 E2 中，为每一个潜在的可修改部分评估对已解码的符合的已修改比特流的视觉效果。测量在呈现的初始比特流和呈现的已修改比特流之间的视觉效果或失真。图像处理领域的技术人员会了解测量两幅图像之间的相似性的已知算法，至少包括峰值信噪比 (PSNR)、均方差 (MSE) 和结构相似性 (SSIM) 指数。该 SSIM 指数是全参考度量，换句话说，图像质量的测量是基于初始的未压缩或无失真图像作为参考。SSIM 被设计来改进传统方法，例如峰值信噪比 (PSNR) 和均方差 (MSE)，这些传统方法被证明与人眼感知并不一致。基于这种变形，为比特流的每一个图像计算基于已解压缩比特流的像素值的测量。在这种 PNSR 和 MSE 的变形中，为初始的和已修改比特流两者的图像中的每一块计算确定的块的亮度。根据另一种变形，测量是基于亮度和色度两者的。采用引用的算法计算代表呈现后在符合的已修改编码比特流和初始编码比特流之间的失真的感知性的度量。人们应该注意到这些函数中的一个或几个被用于度量计算以及一些结果的聚合被完成以定义一个特定的度量。然后基于应用的已确定标准允许选择具有想要的视觉效果的可修改部分，即保存通道标识或者广告，但是隐藏图像的其它部分。可采用应用的其他变形来改变图像的较高或较低部分，来只改变图像中的人物。选择可修改的部分可在于选择具有最高视觉效果的部分，即改变呈现最多的部分。可在应用到已压缩比特流的水印算法中执行这样的算法，其中在一组水印中选择涉及最大视觉失真的水印作为适用于选择性加扰的比特流的可修改的部分。在步骤 E2 的输出部分，在 H.264 比特流的变形中，为初始比特流确定与编码比特流的初始部分相关和与可修改部分在比特流中的位置相关的一组初始语法元素。此外，进一

步确定与比特流的已选择性修改的部分有关的一组可替换语法元素。当在初始比特流中的已确定位置插入时，已选择性修改的部分高度改变在通过语法元素的修改解码后的内容的呈现，同时并不会影响解码过程的符合性。人们应该注意到，对每一个可修改部分，可能有多个不会影响比特流的符合性但是会改变它的呈现的可选部分。对于确定的可修改部分的每一个可选部分在可变级别的感知上影响呈现。通过对于确定的可修改部分的每一个替换部分引起的感知力级别可能不够高。然后不选择可修改部分，因为没有一个可选部分符合选择标准。相反，当几个可选部分导致的感知力级别足够高时，在这几个满足选择标准的可选部分中选择一个可选部分。因此选择步骤包括确定可修改部分和与可修改部分相关的可选部分。

[0030] 在步骤 E3 中，对于每一个已选择的可修改部分执行可选部分对初始部分的替换。将可选部分直接插入在 H.264 输出流中而不是在确定位置的初始部分。

[0031] 图 2 表示根据第二实施例的加扰编码比特流的方法。前几个步骤 E1、E2 和 E3 等同于第一实施例。第二实施例进一步包括为解扰加密和复用初始数据的步骤。

[0032] 在增补的步骤 E4 中，通过一些加密方法加密可修改部分的初始值和位置。每一个可修改部分的初始值和位置是从步骤 E3 中输出的并且与修改的比特流相关的元数据。有利地，只有初始比特流中非常小的部分被加密，同时没有恢复已加密元数据的流的解码严重地影响了感知的呈现。本领域技术人员会了解到初始值和位置是级联的且被块加密的。从而满足了为保证数据安全性的密码长度要求。精细地讲，用第一密钥加密初始值和用第二密钥加密比修改部分值引起的更少可感知的失真的可选值。进一步细讲，对于确定一部分比特流的位置，元数据包括通过一个密钥加密的初始值和每一个都被一个不同的密钥加密的几个可选值。这个变形通过提供具有不同的呈现质量级别的内容以允许一些加扰可伸缩性，每个级别通过专用密钥保护。基于他的凭证，用户会通过确定的用户凭证的密钥函数来享有一个确定的级别。这种变形也允许为不同目标提供内容。根据他的身份，例如成年人或孩子，用户会有权去观看限制成年人观看的呈现性或暴力的场景，同时内容的其他场景被全部解扰。

[0033] 在步骤 E4 中，基于解扰的目的，将加密的元数据与已修改比特流传送给用户。根据不同的实施例，在运送流级别或直接在比特流级别复用加密的元数据，通过安全通道直接发送加密的元数据给用户。在一种变形中，元数据被打包进 SEI 消息并且加入到 H.264 输出流 C'_S 中。有利地，当直接存储在流中时，这些加密的元数据不会修改比特流的符合性。

[0034] 图 3A 和图 3B 表示根据特定实施例的初始编码比特流 300 和被保护 / 加扰的编码比特流 310，其中元数据在带内或带外被发送。

[0035] 在图 3A 中，初始比特流 300 的序列被表示。初始比特流 300 包括头部 301 及随后的帧部 302，在帧部 302 中标识出可修改部分 303。在已修改比特流 310 中，初始可修改部分 303 的值被可选值 313 代替，同时头部 301 和帧部 302 的其他部分 304 保持不变。在图 3A 表示的变形中，将加密的元数据 314 插入到编码比特流的消息中。在图 3B 上示的变形中，加密的元数据 314 在比特流 310 的外部。例如，在单独的文件中传送元数据 314。

[0036] 在一个特定实施例中，熵码是一个算术码，并且更具体地，采用已知为基于上下文的适应性二元算术编码 (CABAC) 的算术编码方案。CABAC 广泛用于 H.264/AVC 标准。在这个特定实施例中，元数据 314 被插入到 H.264 编码比特流的 SEI 消息中。

[0037] 图 4 表示根据特定实施例的解扰比特流的方法。

[0038] 在步骤 D1 中，接收包括编码比特流的初始部分和可选择性修改部分在流中的位置的元数据。人们应该注意到元数据或者从 SEI 消息中、或者从一个安全通道或者从一个单独的文件中恢复。根据优选的实施例，那里元数据被加密，接收元数据的步骤进一步包括元数据的解密。

[0039] 在步骤 D2 中，根据接收的位置确定每一个已选择性修改部分在流中的位置。

[0040] 在步骤 D3 中，通过接收的初始部分替换编码比特流中的每一个可替换部分，从而产生符合的初始比特流。

[0041] 从而在解码级，没有加密密钥，跳过被复用的或者外部的加密元数据，读出影响视觉质量但不会危害解码过程的已修改比特流。当有加密密钥时，解密被复用的或者外部的元数据，根据本消息完成替换；有利地，所呈现的比特流是初始比特流。在一种变形中，不是初始部分，而是其他一些可选部分用来替换，从而不是导出初始比特流的质量，而是一些中间退化级。

[0042] 不像在选择性加密算法中，那里编码比特流的部分被加密和被直接插入到比特流中从而移除信息，在选择性加扰方法中，一些信息（可选部分）还在比特流中，这可使得在没有解密密钥的情况下更容易重建初始比特流。然而，不知道已加密元数据中的位置，可选部分在比特流中的位置是真正的挑战。因此选择性加扰方法的安全级别是令人满意的。此外，密码学领域的技术人员会认识到类 (class) 攻击对本发明的选择性加扰的比特流是不可能的，这是因为黑客会失去用于比较的参考比特流。确实是因为该流是符合的，在没有参考流的情况下隔离所有的已修改部分（位置，大小）是很困难的。此外这些修改取决于比特流，然后不遵守例如关于周期性修改的精确规则。最后，对于每一个可修改部分不得不重复进行黑客行为。

[0043] 图 5 示出了根据特定实施例的用于或加扰或解绕比特流的设备。用于加扰编码比特流的设备例如是内容提供商或者服务提供商处的计算机。在一种变形中，加扰设备是意欲处理初始压缩比特流的任何设备。该设备 500 包括意欲实现本发明的实施例的物理装置，在一个非限制性示例中，包括处理器 501(CPU)、数据存储器 502(RAM，HDD)、程序存储器 503(ROM) 和处理压缩比特流的编码器 / 解码器 505。处理器 505 被配置用于评估在比特流中的可修改部分的视觉影响。处理器 505 被进一步配置用于确定在编码比特流中的潜在的可修改部分，执行选择和替换步骤。在一种变形中，处理器 505 被配置用于加密元数据，在另一种变形中，加扰设备进一步包括用于这种任务的安全处理器。在一种变形中，该设备包括数个编码器 / 解码器 505，用于同时处理初始比特流、确定在编码比特流中的潜在的可修改部分和数个已修改比特流。数据存储器 502 可进一步存储比特流 C_s、C_0。从而该设备被适配成实现前面描述的方法的第一和第二实施例。

[0044] 用于解扰比特流的设备是例如个人计算机、机顶盒 (STB)、解码器或家用网关。解扰设备 500 包括意欲实现本发明的实施例的物理装置，在一个非限制性的例子中，包括处理器 501(CPU)、数据存储器 502(RAM，HDD)、程序存储器 503(ROM)、接收比特流的接口 (504) 和处理压缩比特流的解码器 505。处理器 505 被配置为确定比特流中的可选位置并执行逆替换 (back-substitution)。在一种变形中，该设备包括同时处理已修改比特流并执行逆替换的解码器 505。数据存储器 502 可进一步存储比特流 C_s、C_0。在一种变形中，处理器 505

被适配用于解密元数据。

[0045] 本质上，本发明并不局限于先前描述的实施例。

[0046] 尤其是，本发明兼容任何搜索编码比特流中的一些可选部分来修改解码的精确部分的任何方法，并且本发明可被普及到包括压缩音频内容、压缩 3D 数据的所有其他压缩内容（例如 MPEG-2，MPEG-4，VC-1 比特流）。

[0047] 最终，本发明兼容任何标准加密方法和密钥管理过程。

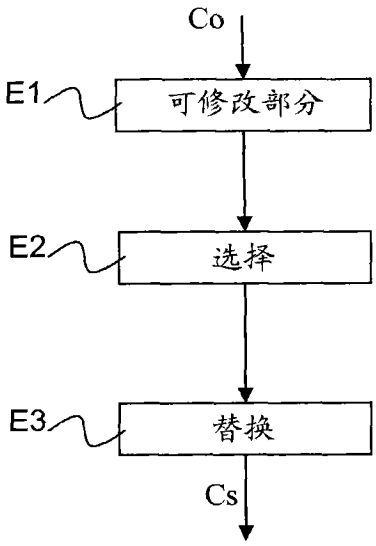

Co
E1
可修改部分
E2
选择
E3
替换
Cs

图 1

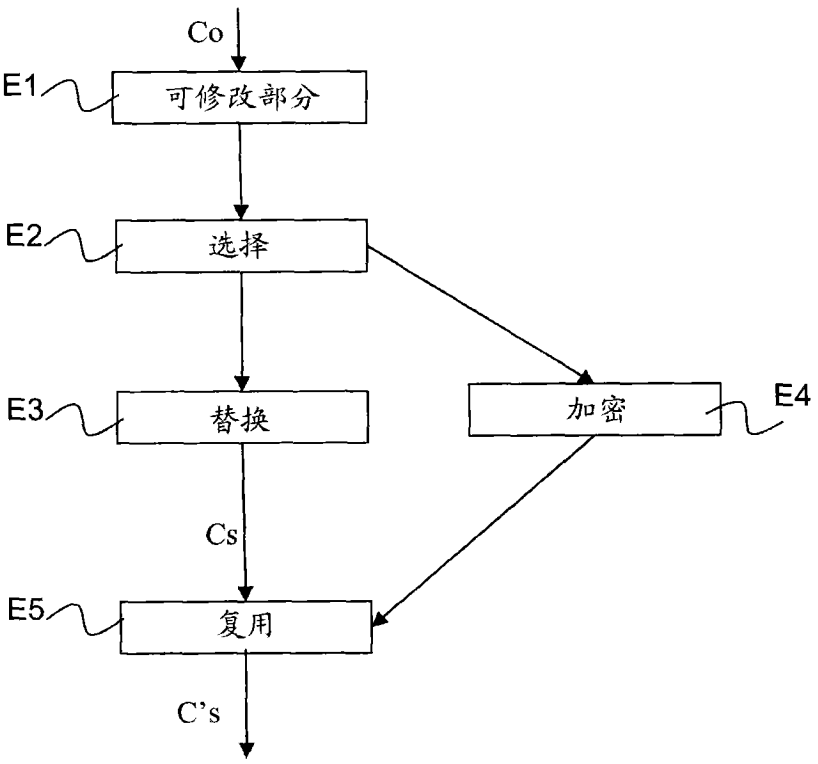

Co
E1
可修改部分
E2
选择
E3
替换
加密
E4
Cs
E5
复用
C's

图 2

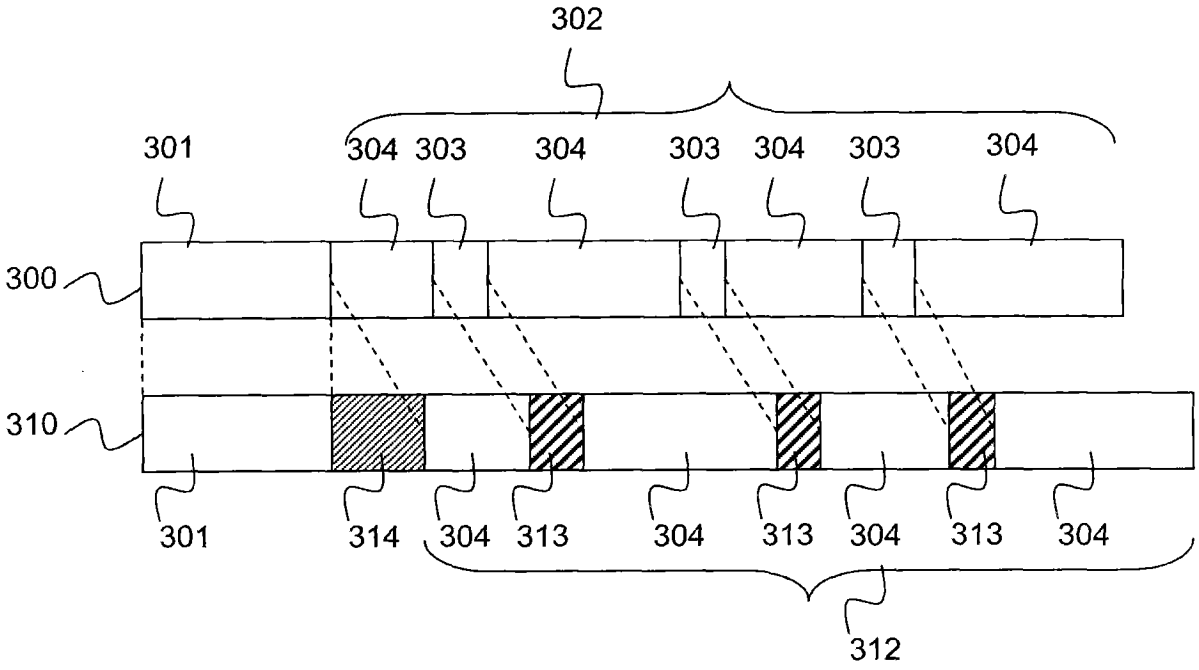

302
301
304
303
304
303
304
303
304
300
310
301
314
304
313
304
313
304
313
304
312

图 3A

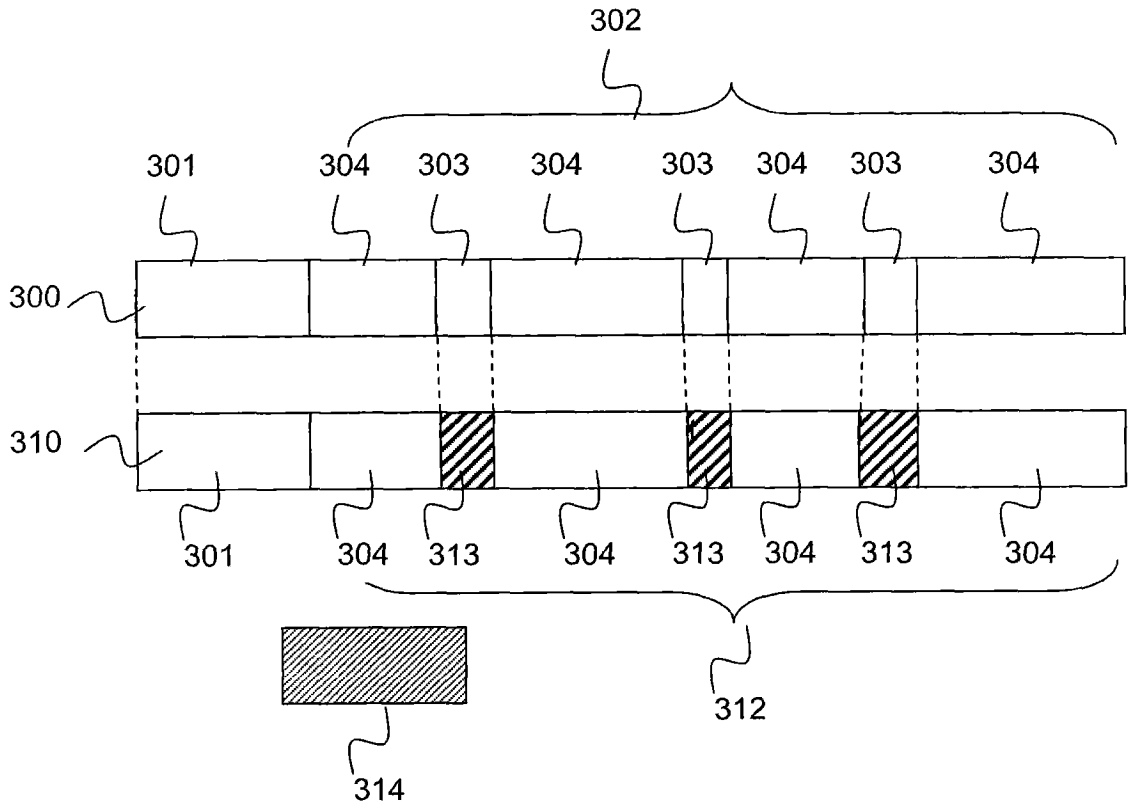

302
301
304
303
304
303
304
303
304
300
310
301
304
313
304
313
304
313
304
312
314

图 3B

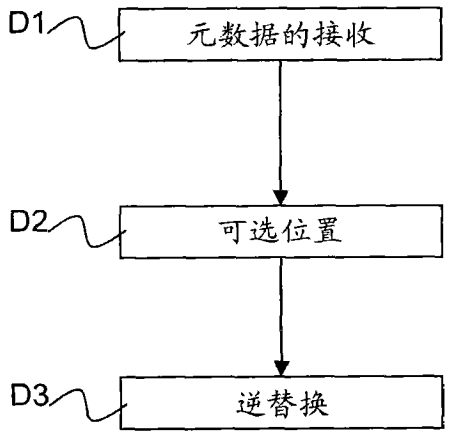

D1
元数据的接收
D2
可选位置
D3
逆替换

图 4

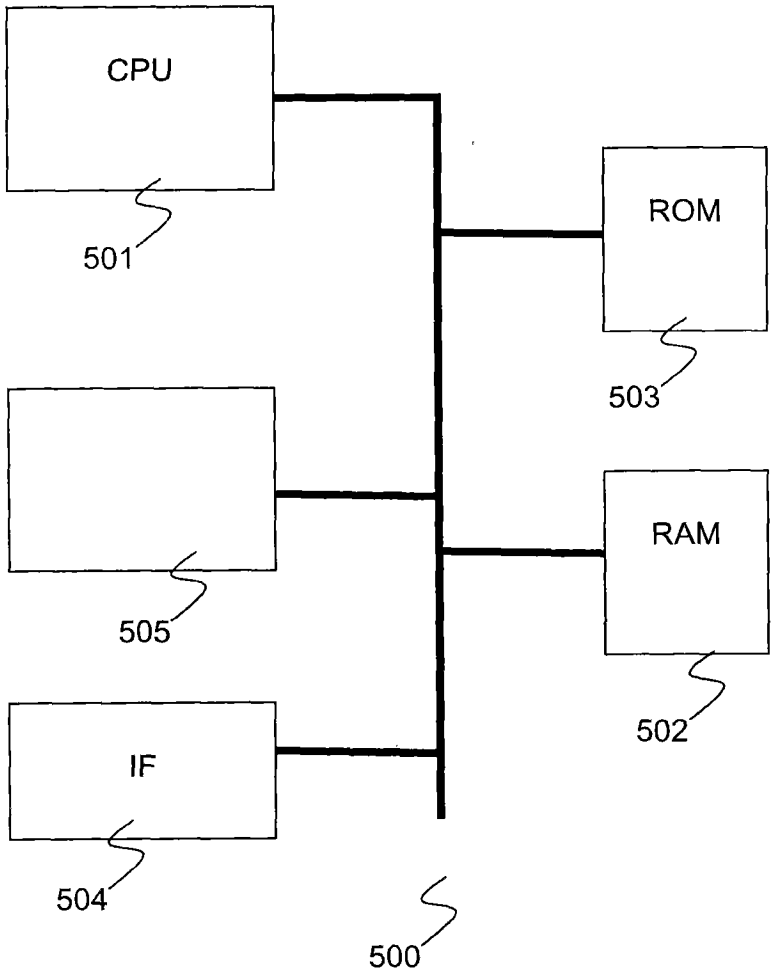


图 5