(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106664203 B
(45)授权公告日 2021.02.12

(21)申请号 201580033127.6
(22)申请日 2015.08.07
(65)同一申请的已公布的文献号
申请公布号 CN 106664203 A
(43)申请公布日 2017.05.10
(30)优先权数据
62/034,714 2014.08.07 US
(85)PCT国际申请进入国家阶段日
2016.12.20
(86)PCT国际申请的申请数据
PCT/US2015/044325 2015.08.07
(87)PCT国际申请的公布数据
WO2016/022979 EN 2016.02.11

(73)专利权人 帝威视有限公司
地址 美国加利福尼亚
(72)发明人 J·布兰尼斯 W·D·阿米德 M·斯瑞尼瓦桑
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 鲍进

(51)Int.Cl.
H04L 9/18(2006.01)
审查员 郑红萍

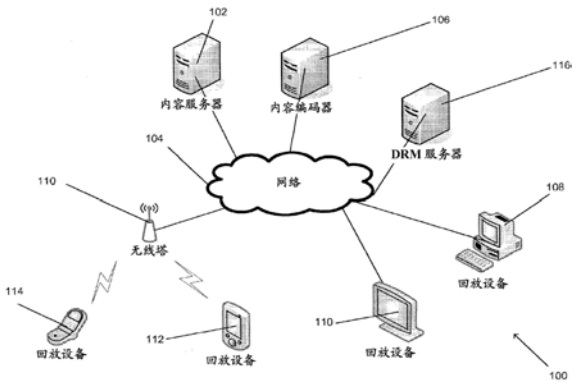
权利要求书2页 说明书10页 附图7页

(54)发明名称

用于保护结合独立编码的方格的单元位流的系统和方法

(57)摘要

本公开涉及用于保护结合独立编码的方格的单元位流的系统和方法。公开了根据本发明实施例的用于部分帧加密的系统和方法。在一个实施例中，该方法接收包括若干帧的视频位流，每个帧包括在该帧内的若干独立编码的压缩单元，加密若干帧中的若干压缩单元中每一个压缩单元的一部分，并且生成包括其中包括压缩单元的加密部分的若干独立编码的压缩单元的输出位流。



CN 106664203 B

1.一种包含处理器指令的非临时性机器可读介质,其中处理器对所述指令的执行使得所述处理器执行包括以下的过程:

接收包括多个帧的视频位流,每个帧包括将该帧分割为矩形区域的多个方格,其中每个方格是在不依赖另一方格中的信息的情况下被编码的独立编码的压缩单元;

基于由与视频帧相关联的至少一个元数据头部提供的信息,确定多个方格在视频位流中的位置;

基于所确定的位置,加密该视频帧内的多个方格中每个方格的一部分;及

生成包括包含方格的加密部分的多个方格的输出位流。

2.如权利要求1所述的非临时性机器可读介质,其中每个方格是特定视频帧的可独立解码部分,使得所述方格不依赖于所述特定视频帧内的另一压缩单元以被解码。

3.如权利要求1所述的非临时性机器可读介质,其中加密多个方格中每个方格的一部分包括:基于与视频位流相关联的头部内的信息确定方格被启用。

4.如权利要求1所述的非临时性机器可读介质,还包括:

加密视频帧中每个方格的一部分。

5.如权利要求4所述的非临时性机器可读介质,其中所述一部分选自包括以下项的组:i)方格的前N个字节,ii)方格的最后N个字节,iii)方格内中间部分的N个字节,以及iv)压缩单元内的N字节的模式。

6.如权利要求1所述的非临时性机器可读介质,其中所述方格是高效视频编码(HEVC)标准内的方格并且视频位流是基于HEVC标准编码的,并且还包括:

解析HEVC视频位流的图片参数集(PPS)以识别所述视频位流内的所述方格的结构;及

基于所述结构加密所述方格的部分。

7.如权利要求1所述的非临时性机器可读介质,其中加密多个方格中每个方格的一部分包括:使用公共加密格式(CENC)来加密所述部分。

8.一种内容编码器,包括:

存储器;以及

处理器,被配置为与存储器通信,其中所述存储器包含编码器应用;

其中所述编码器应用指示所述处理器:

接收包括多个帧的视频位流,每个帧包括该帧内的多个独立编码的压缩单元,其中所述压缩单元是高效视频编码(HEVC)标准内的方格并且视频位流是基于HEVC标准编码的;

解析HEVC视频位流的图片参数集(PPS)以识别所述视频位流内的方格的结构;

基于所述结构加密多个帧内的多个方格中每个方格的一部分;及

生成包括包含压缩单元的加密部分的多个独立编码的压缩单元的输出位流。

9.如权利要求8所述的内容编码器,其中每个方格是特定视频帧的可独立解码部分,使得所述方格不依赖于所述特定视频帧内的另一压缩单元以被解码。

10.如权利要求8所述的内容编码器,其中所述编码器应用还指示所述处理器:

解析元数据头部以识别压缩单元在视频帧内的位置;及

基于所述压缩单元的位置加密视频位流的一部分。

11.如权利要求8所述的内容编码器,其中加密多个方格中每个方格的一部分包括:基于与视频位流相关联的头部内的信息确定方格被启用。

12.如权利要求8所述的内容编码器,其中所述编码器应用还指示所述处理器加密视频帧中每个方格的一部分。

13.如权利要求12所述的内容编码器,其中所述一部分选自包括以下项的组:i)方格的前N个字节,ii)方格的最后N个字节,iii)压缩单元内中间部分的N个字节,以及iv)方格内的N字节的模式。

14.如权利要求8所述的内容编码器,其中加密多个方格中每个方格的一部分包括:使用公共加密格式(CENC)来加密所述部分。

15.一种内容解码器,包括:

存储器;以及

处理器,被配置为与存储器通信,其中所述存储器包含解码器应用;

其中所述解码器应用指示所述处理器:

接收包括多个帧的视频位流,每个帧包括将该帧分割为矩形区域的多个方格,其中每个方格是在不依赖另一方格中的信息的情况下被编码的独立编码的压缩单元;

基于由与视频帧相关联的至少一个元数据头部提供的信息,确定多个方格的加密部分在视频位流中的位置;

基于所确定的位置,加密该视频帧内的多个方格中每个方格的一部分;及

生成输出解码视频以供回放。

用于保护结合独立编码的方格的单元位流的系统和方法

技术领域

[0001] 本发明涉及视频信息的加密和解密领域。更具体而言，本发明针对用于利用部分帧加密来生成压缩数字视频的受保护流的方法和系统。

背景技术

[0002] 现有的数字视频压缩技术是依赖于将未压缩的视频数据单元变换(即，“编码”)为编码形式的各种技术的复杂过程。这种编码允许在表示原始未压缩视频数据的内容中使用较少的位。所得到的编码数据能够利用反向处理(即，“解码”)进行变换，从而产生在视觉上与原始数据相似或完全相同的数据的数字视频单元。数字视频压缩的现代技术可以实现非常高水平的压缩。

[0003] 运动图像专家组(MPEG)和国际标准组织(ISO)已经产生了指定用于视频编码的视频压缩和解压缩算法的各种国际标准。这些标准包括MPEG-1、MPEG-2、MPEG-4、H.261、H.264和更新的高效视频编码(HEVC)标准，相对于其前身，HEVC标准具有显著改进的压缩效率。具体而言，与先前H.264标准相比，HEVC能够以相同的主观质量实现2x压缩比。为了实现这些压缩优化，HEVC标准已经引入了为在多核处理器体系架构上的视频内容的并行处理而专门设计的几个新工具。具体而言，市场上可用的许多智能手机和平板电脑体系架构现在使用多核处理器并且因此能够利用其多核体系架构回放HEVC内容。此外，随着经网络的视频流量的增长，HEVC标准提供了减轻用于分发高质量内容的一些带宽要求的某些工具。

[0004] 保护数字内容的分发免于盗版和其它类型的非法分发是内容提供商的另一个关注点。术语数字版权管理(DRM)被用来描述用于控制对数字内容的访问和/或复制的访问控制技术。DRM系统通常涉及使用密码信息来控制对一条内容的访问或保护一条内容。内容保护通常是利用诸如(但不限于)加密内容的一个或多个加密密钥的密码信息来实现的。

[0005] 当前存在可被用来保护数据的各种类型的加密方案。在数字世界中，加密常常是通过利用称为“密钥”的某种长度的位的集合对数据单元执行可预测的变换来实现的。这产生在不知道用于执行变换的密钥的情况下不能被“读取”的另一个数据单元。加密过程只有在加密密钥或其对应物(例如，“公共”密钥)可用于将加密数据变换或“解密”回原始形式的情况下是容易可逆的。视频数据常常利用符合例如数据加密标准(DES)或高级加密标准(AES)的对称块密码来加密。用来加密数字内容的特定技术可能仍然消耗进一步的处理资源，对于跨网络的内容的编码和分布，这些处理资源需要被考虑在内。

发明内容

[0006] 公开了根据本发明实施例的用于部分帧加密的系统和方法。在一个实施例中，该方法接收包括若干帧的视频位流，其中每个帧在该帧内包括若干独立编码的压缩单元，加密若干帧中的若干压缩单元中每一个压缩单元的一部分，并且生成包括其中包括压缩单元的加密部分的若干独立编码的压缩单元的输出位流。

[0007] 在本发明的另一实施例中，压缩单元是特定视频帧的可独立解码部分，使得其不

依赖于该特定帧内的另一压缩单元以便被解码。

[0008] 在本发明的又一个实施例中，该方法还解析元数据头，以识别压缩单元在视频帧内的位置，并且基于压缩单元的位置加密视频位流的一部分。

[0009] 在本发明的另一实施例中，该方法通过基于与视频位流相关联的头部内的信息确定压缩单元被启用来加密多个压缩单元中每一个压缩单元的所述部分。

[0010] 在本发明的又一实施例中，该方法还包括加密视频帧中的每个压缩单元的一部分。

[0011] 在本发明的又一实施例中，所述部分选自包括以下项的组：i)压缩单元的前N个字节，ii)压缩单元的最后N个字节，iii)压缩单元内中间部分的N个字节，以及iv)压缩单元内的N字节的模式。

[0012] 在本发明的又一实施例中，压缩单元是高效视频编码(HEVC)标准内的方格并且视频位流是基于HEVC标准编码的。

[0013] 在本发明的又一实施例中，更进一步，该方法还包括解析HEVC视频位流的图片参数集(PPS)，以识别视频位流内的方格的结构，并且基于该结构加密方格的各部分。

[0014] 在本发明的另一实施例中，再次，该方法还利用公共加密格式(CENC)来加密若干压缩单元中每一个压缩单元的所述部分，以加密这些部分。

[0015] 本发明的又一实施例包括一种内容编码器，其包括：被配置为与存储器通信的处理器，其中存储器包含编码器应用，其中编码器应用指示处理器：接收包括若干帧的视频位流，其中每个帧在该帧内包括若干独立编码的压缩单元，加密若干帧中的若干压缩单元中每一个的一部分，并且生成包括其中包括压缩单元的加密部分的若干独立编码的压缩单元的输出位流。

[0016] 在本发明的另一实施例中，压缩单元是特定视频帧的可独立解码部分，使得其不依赖于该特定帧内的另一压缩单元以便被解码。

[0017] 在本发明的又一个实施例中，编码器应用还指示处理器解析元数据头，以识别压缩单元在视频帧内的位置，并且基于压缩单元的位置加密视频位流的一部分。

[0018] 在本发明的又一实施例中，加密若干压缩单元中每一个压缩单元的部分包括基于与视频位流相关联的头部内的信息来确定压缩单元被启用。

[0019] 在又一个实施例中，再次，编码器应用还指示处理器加密视频帧中每个压缩单元的一部分。

[0020] 在本发明的另一个实施例中，再次，所述部分选自包括以下项的组：i)压缩单元的前N个字节，ii)压缩单元的最后N个字节，iii)压缩单元内中间部分的N个字节，以及iv)压缩单元内的N字节的模式。

[0021] 在本发明的另一实施例中，压缩单元是高效视频编码(HEVC)标准内的方格并且视频位流是基于HEVC标准编码的。

[0022] 在本发明的又一实施例中，再次，编码器应用还指示处理器解析HEVC视频位流的图片参数集(PPS)，以识别视频位流内的方格的结构，并且基于该结构加密方格的各部分。

[0023] 在本发明的又一个实施例中，再次，加密多个压缩单元中每一个压缩单元的部分包括利用公共加密格式(CENC)来加密这些部分。

[0024] 在本发明的另一实施例中，一种内容解码器包括：被配置为与存储器通信的处理

器,其中存储器包含解码器应用,其中解码器应用指示处理器接收包括若干帧的视频位流,其中每一帧在该帧内包括若干独立编码的压缩单元,解密若干帧中的若干压缩单元中每一个压缩单元的一部分,并且生成用于回放的输出解码视频。

[0025] 在本发明的又一实施例中,压缩单元是特定视频帧的可独立解码部分,使得其不依赖于该特定帧内的另一压缩单元以便被解码。

[0026] 在本发明的又一实施例中,再次,解码器应用还指示处理器解析元数据头,以识别压缩单元在视频帧内的位置,并且基于压缩单元的位置来解密视频位流的一部分。

[0027] 在本发明的又一个实施例中,再次,解密若干压缩单元中每一个压缩单元的部分包括基于与视频位流相关联的头部内的信息确定压缩单元被启用。

[0028] 在本发明的另一个进一步的实施例中,解码器应用还指示处理器解密视频帧中的每个压缩单元的一部分。

[0029] 在本发明的又一个实施例中,再次,所述部分选自包括以下项的组:i)压缩单元的前N个字节,ii)压缩单元的最后N个字节,iii)压缩单元内中间部分的N个字节,以及iv)压缩单元内的N字节的模式。

[0030] 在本发明的另一实施例中,压缩单元是高效视频编码(HEVC)标准内的方格并且视频位流是基于HEVC标准解码的。

[0031] 在本发明的另一实施例中,解码器应用还指示处理器解析HEVC视频位流的图片参数集(PPS),以识别视频位流内的方格的结构,并且基于该结构解密方格的各部分。

[0032] 在本发明的又一实施例中,解密多个压缩单元中每一个压缩单元的部分包括利用公共加密格式(CENC)来解密这些部分。

附图说明

[0033] 图1是根据本发明实施例的视频编码和输送系统的系统图。

[0034] 图2A概念性地示出了根据本发明实施例的、被配置为生成部分加密的内容的内容编码器。

[0035] 图2B概念性地示出了根据本发明实施例的、被配置为管理和分发部分加密的内容的内容服务器。

[0036] 图2C概念性地示出了根据本发明实施例的、被配置为接收和回放部分加密的内容的回放设备。

[0037] 图3示出了根据本发明实施例的用于部分加密内容的过程。

[0038] 图4示出了根据本发明实施例的用于部分加密内容的过程。

[0039] 图5示出了根据本发明实施例的用于解码和回放部分加密的内容的过程。

[0040] 图6示出了根据本发明实施例的视频帧内的方格的例子。

[0041] 图7示出了根据本发明实施例的、用于HEVC视频中的方格的语法结构的例子。

具体实施方式

[0042] 如上所述,不同的技术可被用来加密内容,并且除了与用来压缩或编码视频内容的压缩技术(例如,H.264或HEVC)相关联的处理成本之外,每种技术还会消耗不同量的处理资源。因而,本发明的许多实施例能够通过仅加密帧的部分而不是整个帧而在生成具有加

密帧的受保护压缩视频序列时实现效率。这些技术一般可以被称为“部分帧加密”，因为它们仅加密帧的部分。视频帧内被加密的一个或多个部分可以通过开始位置和长度在帧内指定。通常，这种信息可以在与帧相关联的头部内提供并且被解码器用来定位帧的加密部分以用于解密。

[0043] 在诸如H.264/MPEG-4AVC(高级视频编码)的许多视频压缩格式中，在帧内和跨多个帧存在依赖性(由于压缩算法)。由于依赖性，当被加密的部分不能被解密并且因此不能被正确回放时，该帧内或其它帧中依赖于该加密部分的其它部分也不能被回放。因此，在AVC编码的位流中，加密帧或单元序列的开始x个字节常常足以防止帧或其它单元的许多其它部分的解码。

[0044] 许多实施例可以利用用于加密的ISO/IEC 23001-7:2012公共加密方案(CENC)标准，这是指定可以由一个或多个数字版权和密钥管理系统(DRM系统)使用的标准加密和密钥映射方法的行业加密标准，以使得能够利用不同的DRM系统对相同文件进行解密。该方案允许加密帧的多个不连续部分。

[0045] 诸如高效视频编码(HEVC)的一些视频压缩格式允许帧的各部分被独立地编码和解码，而不参考或依赖于其它部分中的信息，这使得能够同时并行处理视频帧的不同部分。被设计为启用并行处理的一个此类特征是HEVC中的“tile(方格)”。具体而言，通过将图片分成矩形区域(方格)，其中每个方格由多个编码树单元(CTU)组成，方格可被用于由不同处理器同时编码和解码帧的各部分。

[0046] 方格可以包含在单个NAL(网络抽象层)单元或片段内。帧的类似的可独立解码部分可以跨不同的编码格式被称为压缩单元(即，HEVC中的方格)。压缩单元在解码位流时启用并行性，因为它们可以被彼此独立地处理。在启用了方格的HEVC编码流中，如果仅仅视频NAL单元或帧的前x个字节被加密，则其它部分(方格)可以在不必解密加密的(一个或多个)部分的情况下是完全可解码的，因为它们独立于加密的(一个或多个)部分。

[0047] 因此，在许多实施例中，可以通过加密帧内的多个方格的至少一部分来提高具有方格(或其它压缩单元)的编码位流的安全性，以便使更多的帧在不解密加密部分的情况下不可恢复。在若干实施例中，编码器和/或编码过程可被设计为对位流的至少一部分进行解码，以确定方格位于何处并加密方格的部分。编码器可以获取关于方格的结构和/或位置的信息，以便加密多个方格内的信息并且保护更多的位流在不被解密的情况下不能被解码。用于获取关于方格(或其它可独立解码的单元)的这种信息的方法可以包括解析NAL单元头部，以确定一个或多个方格的开始位置。下面进一步讨论根据本发明实施例的用于压缩单元的部分帧加密的系统和方法。

[0048] 用于利用部分帧加密来部分编码和回放视频的系统体系架构

[0049] 如上所述，许多新的压缩标准提供了允许在多核体系架构上对视频内容进行并行处理(即，编码和解码)的新工具。这些工具包括，例如，在HEVC标准中“方格”的使用，以及可用来将视频内容的帧分割成单独的可解码单元的其它类型的类似的可独立解码的压缩单元。如将贯穿本申请所描述的，压缩单元(例如，HEVC中的方格)一般可以指，对于给定的编码标准，单个视频帧的经分割和/或可独立解码的部分。此外，“方格”是已经在HEVC标准中引入的一种类型的压缩单元。虽然下面的许多例子描述了基于根据HEVC标准压缩的视频的方格的部分帧加密，但是，根据本发明的实施例，部分帧加密可被用来加密已经根据适于具

体应用的需求的任何其它标准压缩的视频，所述任何其它标准使用类似类型的压缩单元分割视频帧。

[0050] 此外，为了保护已经利用可独立解码的压缩单元压缩的数字内容，可以使用对视频帧内的压缩单元(即，方格)的一个或多个部分应用部分帧加密的某些加密技术。具体而言，在已被设计为允许对视频帧内的压缩单元进行独立解码的较新标准(例如，HEVC)中，基于其它部分将具有需要对加密帧进行正确解密的帧间依赖性的压缩标准设计，仅加密整个视频帧的一部分(即，视频图片)可能不再足够。如上所述，在这些较旧的压缩标准中，由于单个视频帧的不同部分之间的依赖性，当加密的部分不能被解密并且因此不能被正确回放时，该帧内或其它帧中依赖于该加密部分的其它部分也不能被回放。因此，在许多实施例中，部分帧加密可以应用于视频帧内的一个或多个压缩单元的部分。根据本发明实施例的用于利用部分帧加密来编码视频内容的系统在图1中示出。

[0051] 系统100包括被配置为将源媒体编码成编码视频的内容编码器102。在若干实施例中，通过在视频的每一帧内生成例如允许帧的部分的独立编码/解码而无需参照视频帧的其它部分的压缩单元(例如，方格)，内容编码器可以利用允许内容的并行处理的压缩标准(例如，HEVC标准)来编码内容。具体而言，在若干实施例中，内容编码器可以利用HEVC标准来编码内容，以编码视频内容的帧。HEVC标准还可以为视频的每一帧生成一个或多个可独立解码的方格。

[0052] 除了基于压缩标准(例如，HEVC)编码视频帧之外，在许多实施例中，内容编码器106还可以加密视频内容的部分，以保护内容免受非法分发。为了减少与加密视频内容相关联的开销成本，在许多实施例中，内容编码器106利用部分帧加密来编码视频内容，借此视频帧内的一个或多个压缩单元(即，方格)的仅一部分被加密(而不是加密视频内容的整个帧)。在一些实施例中，内容编码器加密视频帧内的每个方格的起始x个字节。其它实施例可以加密方格的不同部分，包括位于位流内某处的x个字节、结尾的x个字节或者适于特定应用的需求的方格内的字节的任何其它组合。在某些实施例中，内容编码器可以加密帧中的每个方格的相同部分。在其它实施例中，内容编码器可以加密不同方格的不同部分。在若干实施例中，内容编码器可以加密视频帧内的仅某些方格(例如，少于所有方格)的部分。如可以容易地认识到的，包含加密视频的容器文件可以包括单独的DRM轨道，其包含关于帧内的方格的加密部分的位置的信息和/或用来加密全部或每个加密部分的密码信息。

[0053] 在一些实施例中，内容编码器106将内容存储在Matroska(MKV)容器文件中。Matroska容器是由位于法国Aussonne的Matroska非营利组织作为开放标准项目开发的媒体容器。Matroska容器基于可扩展二进制元语言(Extensible Binary Meta Language，EBML)，它是可扩展标记语言(XML)的二进制衍生物。Matroska容器的解码被许多消费电子(CE)设备支持。在其它实施例中，可以利用适于具体应用的需求的各种容器文件格式中的任何一种，所述容器文件格式包括(但不限于)由运动图像专家组指定为MPEG-4部分14的MP4容器文件格式。

[0054] 在一些实施例中，在内容编码器106已经压缩和/或加密视频序列之后，内容编码器106将编码视频上传到内容服务器102。

[0055] 在许多实施例中，内容服务器102便于源媒体向一个或多个回放设备108-114的分发。根据本发明若干实施例的内容服务器102可以负责存储受保护内容以分发到回放设备。

在许多实施例中，内容服务器接收并处理来自寻求下载编码视频的各种回放设备108-114的下载请求。在一些实施例中，设备可以请求(i)下载整个文件，或(ii)接收用于以渐进(progressive)或自适应(adaptive)流传输模式回放的流传输视频。当分发服务器从回放设备接收到下载请求时，它可以向回放设备提供编码视频用于存储和/或回放。

[0056] 下载的视频文件可以包括包含描述视频帧内的压缩单元(例如，HEVC编码视频中的方格)的结构的数据的一个或多个头部。头部可以包括指向一个或多个方格的开始位置的指针。在一些实施例中，编码的HEVC视频序列内的方格的位置可以在提供关于一个或多个视频帧内的方格结构的信息的图片参数结构(PPS)中指定。在一些实施例中，方格在帧内的某些位置可以是固定的，而在其它实施例中，方格可以对于不同的视频帧位于不同的位置。回放设备上的解码器可以使用这个信息来确定需要被解密以便回放视频文件的帧的部分。

[0057] 在一些实施例中，内容服务器102从各种回放设备接收流请求，并且随后将编码视频流传输到回放设备，用于渐进式回放和/或作为自适应位速率流传输系统的一部分。在若干实施例中，各种回放设备可以使用HTTP或另一种适当的无状态协议来经由诸如互联网的网络104请求流。在若干实施例中，各种回放设备可以使用RTSP，借此分发服务器记录每个回放设备的状态并且基于从回放设备接收的指令和描述回放设备的状态的所存储数据来确定要流传输的视频。

[0058] 在若干实施例中，DRM服务器116(数字版权管理)便于对源媒体的授权和访问，包括管理加密/解密源媒体所需的密钥。

[0059] 根据本发明某些实施例的DRM服务器116可以负责存储用于向回放设备分发(例如，流传输和/或下载)的内容的受保护的流和/或文件。DRM服务器还可以存储用来保护内容的公共密码信息。在若干实施例中，公共密码信息是利用与公共密码信息相关联的标识符和一条内容来识别的。

[0060] 在所示实施例中，回放设备包括个人计算机108-110和移动电话112-114。在其它实施例中，回放设备可以包括消费者电子设备，诸如DVD播放器、蓝光播放器、电视，机顶盒、视频游戏控制台、平板电脑以及能够经由HTTP连接到服务器并回放编码视频的其它设备。

[0061] 在所示实施例中，内容编码器、内容服务器和DRM服务器是被配置为在服务器计算机硬件上执行的服务器应用。在其它实施例中，内容编码器、内容服务器和DRM服务器可以是包括处理器并具有足够资源来执行源媒体的加密、分发和数字版权管理的任何处理设备，其中源媒体包括(但不限于)视频、音频和/或字幕。虽然在图1中示出了具体的体系架构，但是，根据本发明的实施例，可以使用适于具体应用的需求的启用回放设备以请求具有部分帧加密的编码视频的各种体系架构中的任何一种。

[0062] 根据本发明实施例的内容编码器202的基本体系架构在图2A中示出。内容编码器202包括与非易失性存储器208、易失性存储器206和网络接口214通信的处理器204。在所示实施例中，非易失性存储器包括配置处理器以编码内容212的内容编码器应用210。在若干实施例中，内容编码器应用210利用部分帧加密来加密内容，使得仅视频帧内的一个或多个压缩单元(例如，方格)的部分而不是整个帧被加密，以减少与压缩视频的加密相关联的开销。

[0063] 在若干实施例中，网络接口214可以与处理器204、易失性存储器206和/或非易失

性存储器208通信。虽然在图2A中示出了具体的内容编码器体系架构，但是，根据本发明的实施例，可以使用其中包括内容编码器应用位于盘或某种其它形式的储存器上并在运行时被加载到易失性存储器中的体系架构在内的各种体系架构中任何一种来实现内容编码器。

[0064] 根据本发明实施例的内容服务器222的基本体系架构在图2B中示出。内容服务器222包括与非易失性存储器228、易失性存储器226和网络接口234通信的处理器224。在所示实施例中，非易失性存储器包括配置处理器以分发内容232的内容分发应用230。在若干实施例中，网络接口234可以与处理器224、易失性存储器226和/或非易失性存储器228通信。虽然在图2B中示出了具体的内容服务器体系架构，但是，根据本发明的实施例，可以使用包括其中内容分发应用位于盘或某种其它形式的储存器上并在运行时被加载到易失性存储器中的体系架构在内的各种体系架构中任何一种来实现内容服务器。

[0065] 根据本发明实施例的回放设备的基本体系架构在图2C中示出。回放设备252包括与非易失性存储器258、易失性存储器256和网络接口240通信的处理器254。在所示实施例中，非易失性存储器包括配置处理器以解码内容262的解码器应用260。在一些实施例中，解码器应用260使用在视频容器文件和/或视频流内提供的信息来识别视频帧内的压缩单元的位置，并且仅解密压缩单元的某些部分，以便解码视频。

[0066] 在若干实施例中，网络接口264可以与处理器254、易失性存储器256和/或非易失性存储器258通信。虽然在图2C中示出了具体的回放设备体系架构，但是，根据本发明的实施例，可以使用包括其中解码器应用位于盘或某种其它形式的储存器上并在运行时被加载到易失性存储器中的体系架构在内的各种体系架构中任何一种来实现回放设备。

[0067] 用于部分帧加密的系统和方法

[0068] 如上所述，一些视频压缩格式(例如，HEVC)允许帧的部分(例如，压缩单元或方格)被独立地编码和解码，而不参考或依赖于该帧(或其它帧)的其它部分中的信息。帧的这些可独立解码的部分可以跨不同的编码格式被称为压缩单元。因此，在利用独立的压缩单元对流进行加密期间，如果仅仅帧的前x个字节被加密，则其它部分(压缩单元或方格)可以在不必解密压缩单元的加密部分的情况下是完全可解码的，这是因为它们独立于加密的压缩单元。因此，具有方格(或其它压缩单元)的编码位流的安全性可以通过加密帧内的多个方格的至少一部分以使帧的更多部分在不解密加密部分的情况下不可恢复来提高。根据本发明实施例的用于视频位流的压缩单元的部分帧加密的过程在图3中示出。

[0069] 该过程(在302)接收视频数据。在一些实施例中，该过程可以从一个或多个内容分发器下载视频数据。在其它实施例中，该过程可以在视频回放期间流传输视频数据。

[0070] 该过程(在304)确定多个压缩单元在视频数据内的位置。位置可以基于由与视频帧相关联的一个或多个头部提供的信息来确定。在一些实施例中，头部可以提供关于帧内的每个压缩单元的开始位置的信息。在一些实施例中，每个压缩单元的位置在每个视频帧内可以是固定的并且因此可以不需要由头部来识别。例如，编码器可以利用关于视频序列的结构的信息预编程。

[0071] 该过程(在306)确定要加密的视频帧内的每个压缩单元的一部分。在一些实施例中，该过程确定每个压缩单元的固定x字节应当被加密。在若干实施例中，该过程基于压缩单元的特点来确定不同压缩单元的不同部分。在其它实施例中，该过程可以编码视频帧的一个或多个压缩单元中的中间或最后x个字节。在某些实施例中，该过程可以不加密视频的

某些帧，而仅加密其它视频帧的部分。如可以容易地认识到的，被加密的特定帧的具体部分以及加密的方式通常取决于应用的需求。

[0072] 该过程(在308)加密压缩单元的部分。在一些实施例中，该过程利用标准DES和/或AES密码来加密这些部分。其它实施例可以使用适于具体应用的需求的其它加密机制。

[0073] 该过程(在310)生成包含具有已被加密的部分的压缩单元的输出位流。然后，该过程结束。

[0074] 虽然在图3中描述了用于加密压缩单元的部分的具体过程，但是，根据本发明的实施例，可以使用适于具体应用的需求的各种过程中的任何一种来加密压缩单元的部分。

[0075] HEVC标准的概述

[0076] 如上所述，HEVC视频压缩标准包括被设计为用于利用支持并行处理的多核体系架构来回放视频内容的几个新工具。除了切片结构之外，这些工具还包括波前并行处理(WPP)和方格。当使用WPP和/或方格时，对应于一个图片的视频位流可被封包为可独立解码的位流子集。具体而言，HEVC包括将视频帧分割为某些尺寸的矩形区域的可独立解码的方格。根据本发明实施例的视频帧内方格的例子在图6中示出。具体而言，图6是示出在水平和垂直维度中将帧均匀地分割为九个方格——从位于左上角的方格1到位于右下角的方格9——的图。每个方格包括编码树单元。

[0077] 方格相关的参数可以在HEVC中的图片参数集(PPS)中被发信号通知。在视频序列中，可以允许不同的图片使用不同的PPS。方格参数可以在相同的视频序列中从图片到图片改变。在大多数视频应用中，方格的数目和方格的位置有可能在视频序列(例如，一系列图片)中保持相同，但是，可能出现这样的情况，其中不仅可以允许方格的配置在相同的视频序列中从图片到图片改变，而且可以允许方格的分组从图片到图片改变。

[0078] 图7示出了HEVC视频中的图片参数集(PPS)中用于方格的语法结构的例子。如果tiles_enabled_flag被开启，则可以发信号通知每个维度中方格的数量。如果方格是均匀尺寸的(例如，如果uniform_spacing_flag是1)，则没有附加信息可以被发信号通知。方格的宽度和高度可以被发信号通知。例如，如图7中所示，num_tile_columns_minus1和num_tile_rows_minus1可以被设置为2，并且uniform_spacing_flag可以被设置为1。

[0079] 编码器可以通过由编码器发信号通知具有新的方格分区参数的新PPS来从一个帧到另一个帧改变方格如何被分割。在许多实施例中，方格不需要彼此相比保持相等的尺寸，或者与较早情况下的相同方格相比具有相同的尺寸。具体而言，编码器可以发信号通知具有新的方格分区参数的新PPS，所述新的方格分区参数将应用于一个或多个帧的新集合。

[0080] HEVC中的部分帧加密

[0081] 如上所述，HEVC标准引入了支持高级并行处理的某些工具。具体而言，HEVC包括方格，其允许将帧切分成矩形区域，然后可将其独立地编码和解码。帧可以被均匀地或非均匀地切分成方格。每个方格的入口点可以在切片头部中指定。为了允许利用HEVC标准部分加密视频文件，本发明的许多实施例可以部分地加密多个方格，以便加密视频内容。根据本发明实施例的用于HEVC方格的部分加密的过程在图4中示出。

[0082] 该过程(在402)确定方格是否被启用。在许多实施例中，当方格被启用时，位流可以包含指示每个图片分区的开始位置的入口点偏移，这是让每个核心立即访问该分区所必需的。

[0083] 该过程(在404)确定帧和/或位流内的NAL单元的结构。

[0084] 该过程(在406)确定NAL单元内的方格的结构。在一些实施例中,该过程解析NAL头部,以确定视频帧内每个方格的开始位置。在一些实施例中,HEVC方格可以将图片分割成某些尺寸的矩形区域。用于方格的参数结构可以在HEVC中在图片参数集(PPS)、视频可用性信息(VUI)和/或补充增强信息(SEI)消息中指定。HEVC中的PPS的例子在图7中示出。如果tile_enabled_flag被开启,则每个维度中方格的数量可以被发信号通知。在一些实施例中,如果方格是均匀尺寸的(例如,如果uniform_spacing_flag是1),则没有附加信息可以被发信号通知。PPS还可以发信号通知方格的宽度和高度。

[0085] 该过程(在408)选择多个NAL单元。在一些实施例中,该过程可以选择所有NAL单元。在某些实施例中,该过程可以选择一个或多个NAL单元。

[0086] 该过程(在410)选择在被选的每一个NAL单元中方格的数量。在一些实施例中,通过编码器发信号通知具有新的方格分区参数的新PPS,编码器可以从图片到图片改变如何分割方格。图7示出了在PPS中发信号通知方格的例子。在一些实施例中,方格可以彼此相比具有不同的尺寸,或者与较早情况下的相同方格相比具有不同的尺寸。在一些实施例中,编码器可以发信号通知具有用于每个新图片的新方格分区参数的新PPS或者何时方格分区从前一图片改变。

[0087] 该过程加密所选择的方格的至少一部分。在一些实施例中,该过程可以加密前x个字节、结尾的x字节或者位于方格的位流的某个部分中的某个x个字节。在若干实施例中,该过程可以加密方格内的多个块。其它实施例可以根据具体应用的需求加密方格的其它部分。在许多实施例中,该过程利用使用关于如何加密位流的公共规范的公共加密格式(CENC)来加密方格的部分。CENC指定可以由DRM系统用来启用文件的解密的行业标准加密和密钥映射方法。该方案通过定义解密受保护流所必需的加密相关的元数据的公共格式来操作。该方案把版权映射、密钥获取和存储、DRM顺应性规则以及各种其它考虑的细节留给支持CENC方案的DRM系统。此外,在许多实施例中,加密信息可以存储在MKV容器内。

[0088] 然后,该过程结束。虽然在图4中描述了用于加密HEVC视频内容中的方格的一部分的具体过程,但是,根据本发明的实施例,可以使用适于具体应用的需求的各种过程中的任何一种来加密方格的部分。

[0089] 解码部分加密的视频

[0090] 根据本发明实施例的用于解码部分加密的视频的过程在图5中示出。

[0091] 该过程(在502)接收加密的视频数据。在一些实施例中,该过程可以从内容提供商下载、流传输和/或流传输以下载视频内容。在其它实施例中,视频数据可以存储在盘上或通过适于具体应用的需求的任何其它机制来获得。

[0092] 该过程(在504)确定多个压缩单元(例如,HEVC中的方格)在视频数据内的位置。在一些实施例中,方格的位置在一个或多个视频帧内可以是固定的。在其它实施例中,方格的位置可以在帧之间或帧集合之间改变。方格的位置可以基于包含在对应于帧的PPS内的信息来确定。具体而言,该过程可以解析PPS,以识别在已经加密的方格中的特定字节。

[0093] 该过程(在506)确定压缩单元是否是加密的并解密加密的压缩单元。在一些实施例中,该过程可以获得用于解密加密内容的解密密钥。解密密钥可以基于从与内容相关联的DRM服务接收的授权来获得。

[0094] 该过程(在508)解码压缩单元。在许多实施例中,该过程基于用来编码视频(例如,HEVC视频)的特定压缩标准来解码内容。

[0095] 该过程(在510)生成用于回放的输出解码视频。然后,该过程结束。

[0096] 虽然在图5中描述了用于解密视频内容中的压缩单元的部分的具体过程,但是,根据本发明的实施例,可以使用适于具体应用的需求的各种过程中的任何一种来解密视频内容中的压缩单元的部分。

[0097] 虽然已经在某些具体方面描述了本发明,但是许多附加的修改和变化对于本领域技术人员将是显而易见的。因此,应当理解,本发明可以以与具体描述不同的其它方式实践。因此,本发明的实施例在所有方面都应当被认为是说明性而不是限制性的。

[0098] 此外,前面的讨论仅仅公开和描述了本发明的示例性实施例。本领域技术人员将容易地从这种讨论和从附图中认识到,在不背离本发明的精神和范围的情况下,可以在其中进行各种改变、修改和变化。因此,本发明意在不限于所公开的特定实施例,而是本发明将包括落入所附权利要求的范围内的所有实施例。

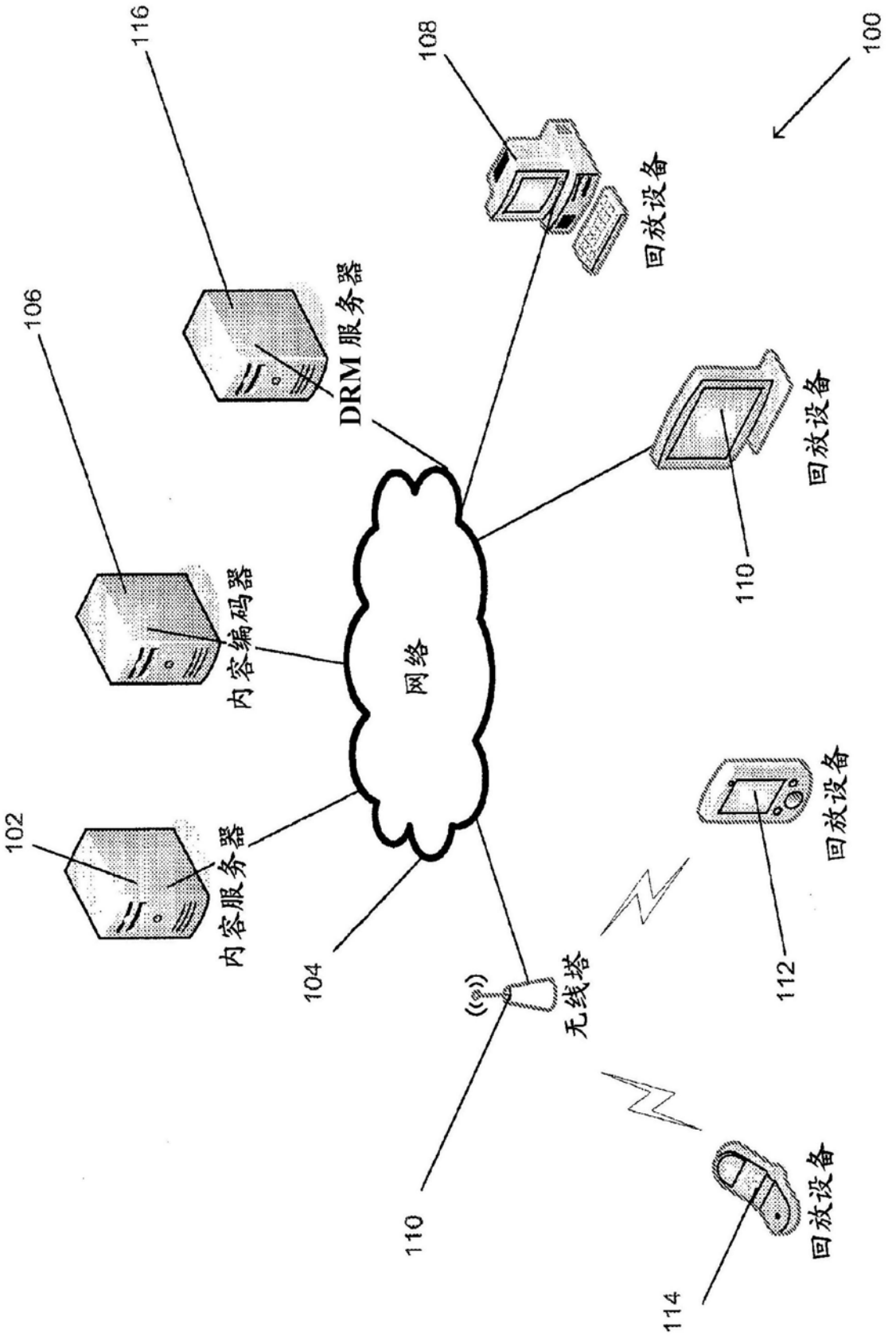

116
108
100
DRM 服务器
回放设备
106
内容编码器
网络
110
回放设备
102
内容服务器
104
无线塔
112
回放设备
110
114
回放设备

图1

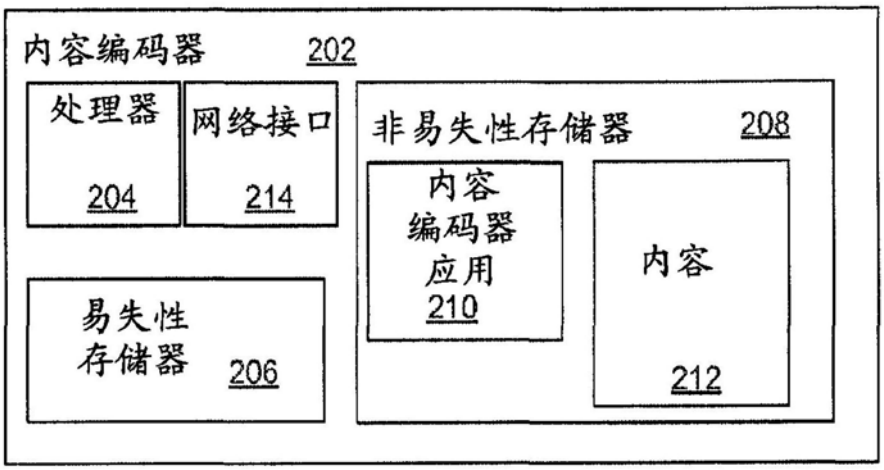

内容编码器 202
处理器 204
网络接口 214
非易失性存储器 208
内容编码器应用 210
内容 212
易失性存储器 206

图2A

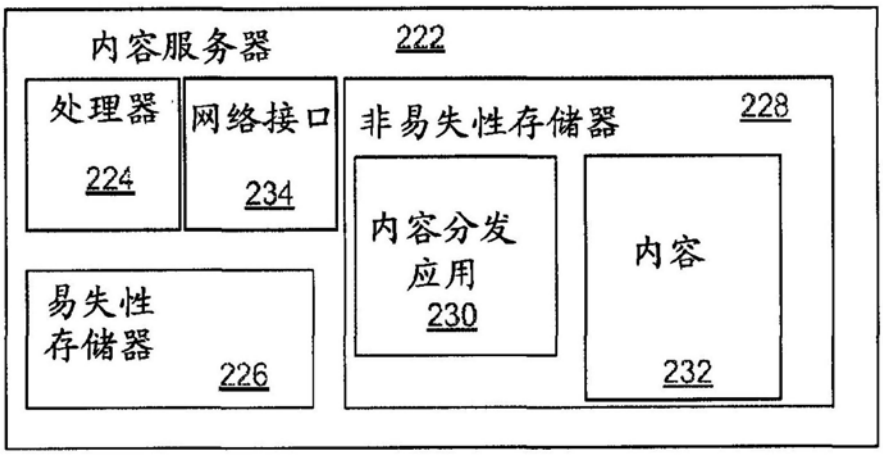

内容服务器 222
处理器 224
网络接口 234
非易失性存储器 228
内容分发应用 230
内容 232
易失性存储器 226

图2B

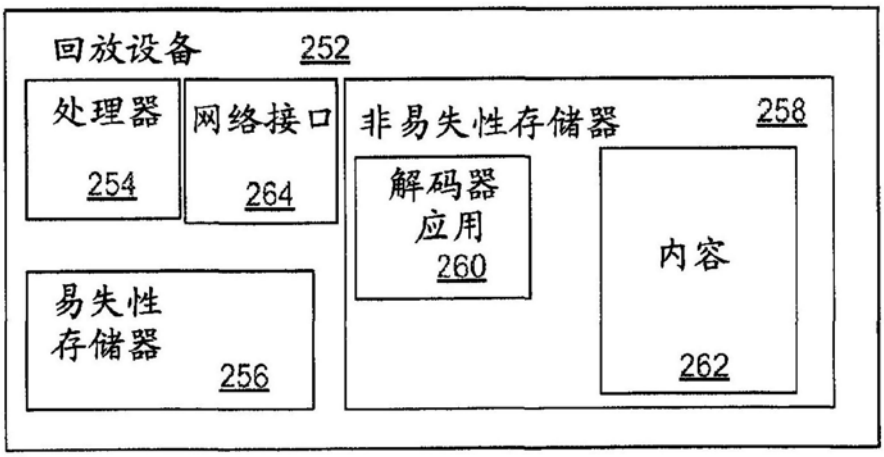

回放设备 252
处理器 254
网络接口 264
非易失性存储器 258
解码器应用 260
内容 262
易失性存储器 256

图2C

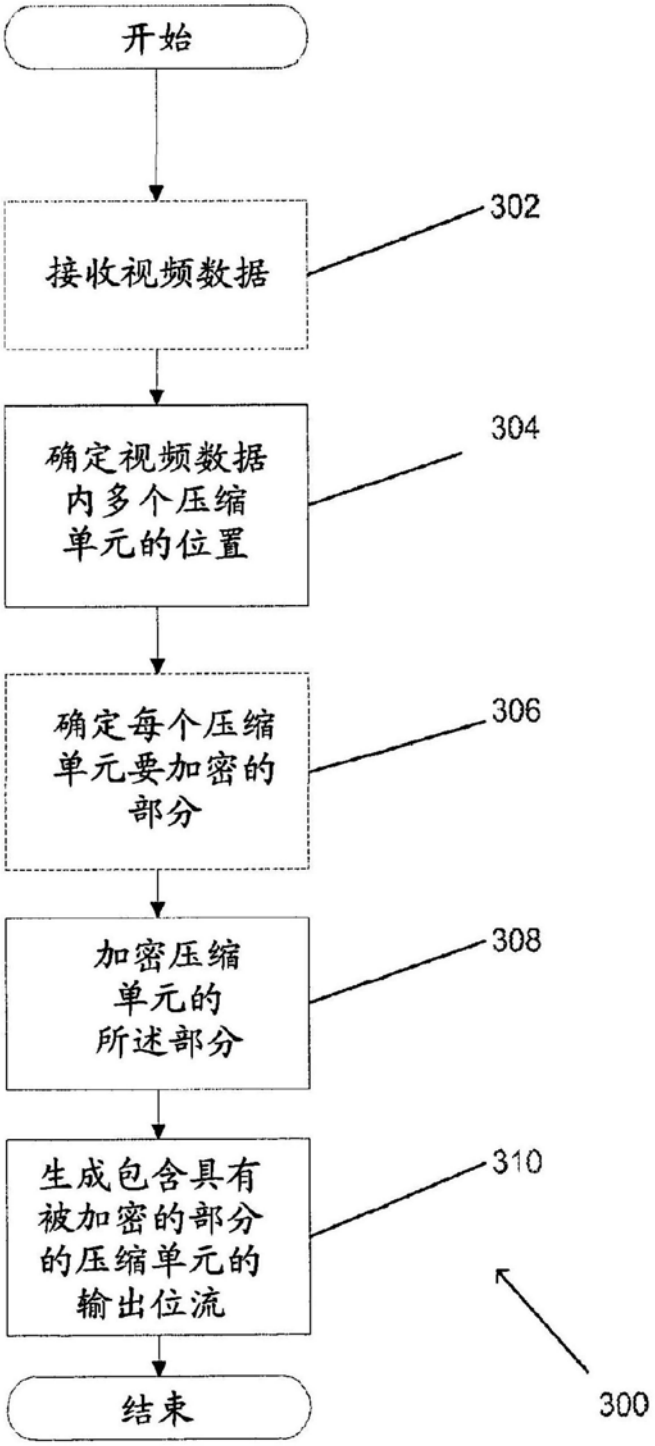

开始
接收视频数据
302
确定视频数据内多个压缩单元的位置
304
确定每个压缩单元要加密的部分
306
加密压缩单元的所述部分
308
生成包含具有被加密的部分的压缩单元的输出位流
310
结束
300

图3

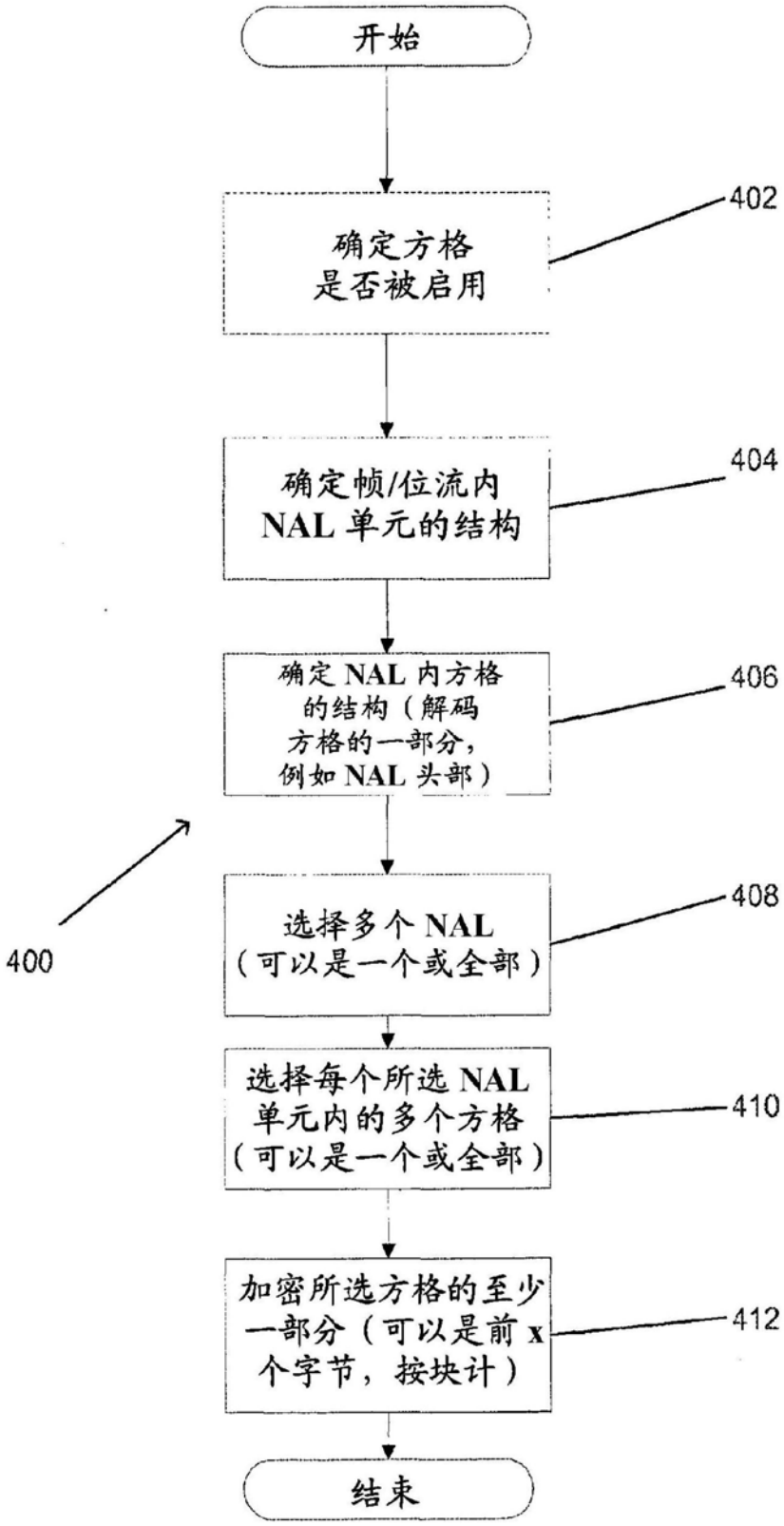

开始
确定方格是否被启用
402
确定帧/位流内NAL单元的结构
404
确定NAL内方格的结构（解码方格的一部分，例如NAL头部）
406
400
选择多个NAL（可以是一个或全部）
408
选择每个所选NAL单元内的多个方格（可以是一个或全部）
410
加密所选方格的至少一部分（可以是前x个字节，按块计）
412
结束

图4

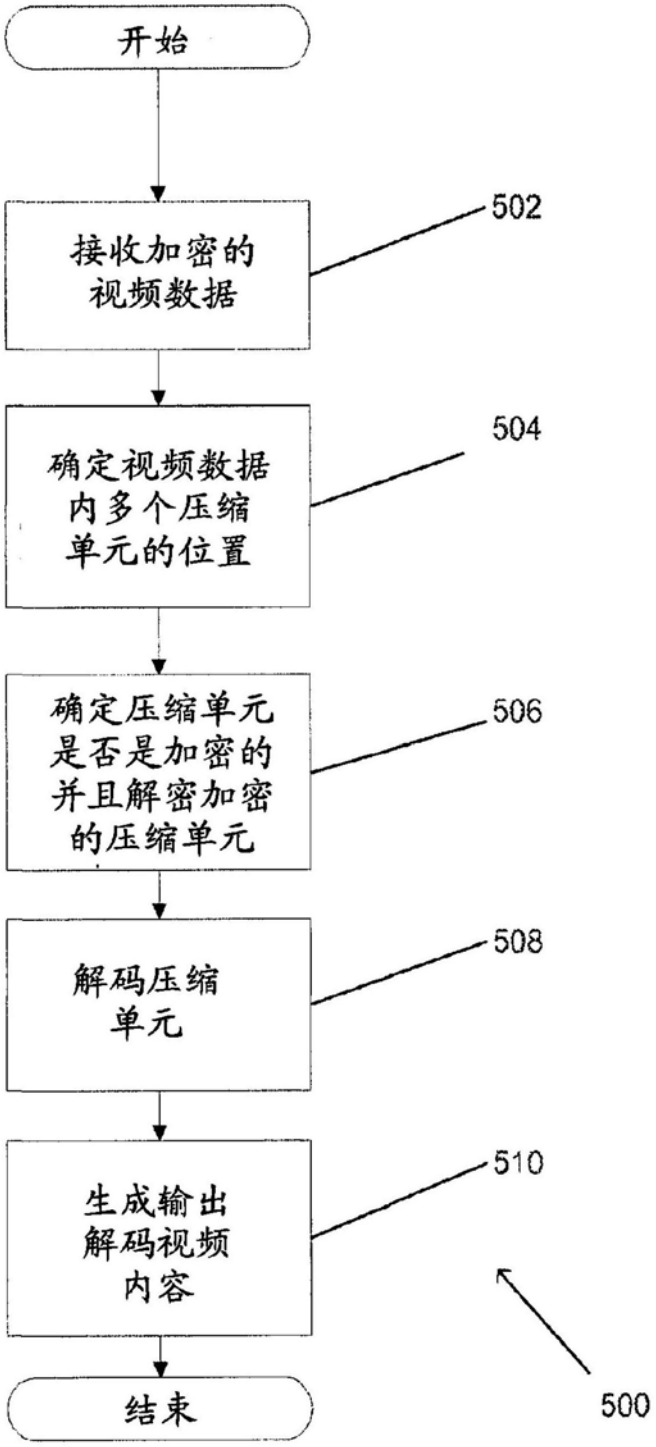

开始
接收加密的视频数据
502
确定视频数据内多个压缩单元的位置
504
确定压缩单元是否是加密的并且解密加密的压缩单元
506
解码压缩单元
508
生成输出解码视频内容
510
结束
500

图5

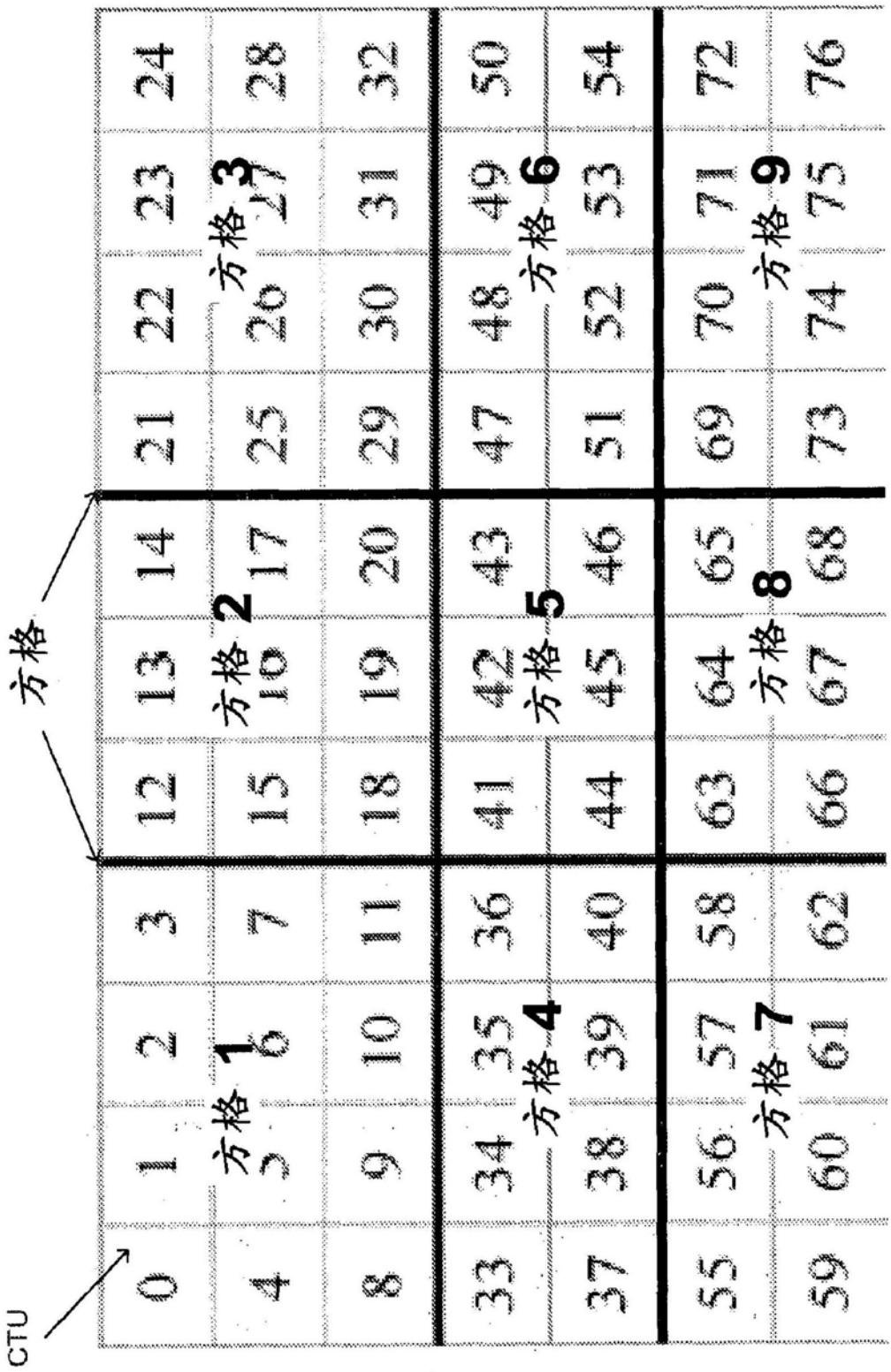

CTU
方格
方格 1
方格 2
方格 3
方格 4
方格 5
方格 6
方格 7
方格 8
方格 9
0 1 2 3 12 13 14 21 22 23 24
4 5 6 7 15 10 17 25 20 27 28
8 9 10 11 18 19 20 29 30 31 32
33 34 35 36 41 42 43 47 48 49 50
37 38 39 40 44 45 46 51 52 53 54
55 56 57 58 63 64 65 69 70 71 72
59 60 61 62 66 67 68 73 74 75 76

图6

在 PPS 中发信号通知方格的例子

pic_parameter_set_rbsp( ){	描述符
...	
tiles_enabled_flag	u(1)
entropy_coding_sync_enabled_flag	u(1)
entropy_slice_enabled_flag	u(1)
if(tiles_enabled_flag){	
num_tile_columns_minus1	ue(v)
num_tile_rows_minus1	ue(v)
uniform_spacing_flag	u(1)
if(!uniform_spacing_flag) {	
for (i = 0; i < num_tile_columns_minus1; i++)	
column_width_minus1[i]	ue(v)
for(i = 0; i < num_tile_columns_minus1; i++)	
row_height_minus1[i]	ue(v)
}	
loop_filter_across_tiles_enabled_flag	u(1)
}	
...	
}	

图7