(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 102077592 A
(43)申请公布日 2011.05.25

(21)申请号 200980125105.7

(22)申请日 2009.06.30

(30)优先权数据
08305364.5 2008.06.30 EP

(85)PCT申请进入国家阶段日
2010.12.29

(86)PCT申请的申请数据
PCT/EP2009/058161 2009.06.30

(87)PCT申请的公布数据
WO2010/000727 EN 2010.01.07

(71)申请人 汤姆森许可贸易公司
地址 法国伊西莱穆利诺

(72)发明人 阿尤布·马苏迪
弗雷德里克·勒菲弗

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王波波

(51)Int.Cl.
H04N 7/26(2006.01)
H04N 21/2347(2011.01)
H04L 9/06(2006.01)

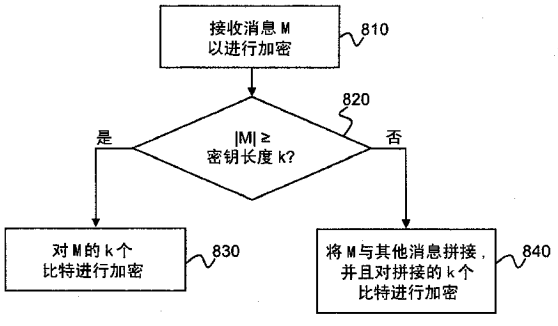
权利要求书 1 页 说明书 7 页 附图 5 页

(54)发明名称

选择性数据加密的方法和装置

(57)摘要

一种使用密钥长度为 k 的加密密钥 K 对至少一个包括均匀分布的符号的消息 M 进行加密的方法，对至少 k 比特长的消息 M 的 k 个比特进行加密 (830)，而对于较短的消息进行延长，例如通过填充或拼接以获得在加密之前至少 k 比特长的延长消息。因此，优化了加密的效率而保持加密的安全性。此加密方法特别适合于包括消息 M 的 JPEG2000 编码的分组。还提出了一种加密装置 (710)，一种解密方法以及一种解密装置 (910)。



CN 102077592 A

1. 一种使用密钥长度为 k 的加密密钥 K 对均匀分布的符号的至少一个消息 M 进行加密的方法，在加密设备 (710) 处，该方法包括以下步骤：

- 对所述至少一个消息 M 中长度为 k 比特的每一个消息 M 的 k 个比特进行加密；

其特征在于，该方法还包括以下步骤：

- 对所述至少一个消息 M 中长度大于 k 比特的每一个消息 M 的小于消息 M 总长度的至少 k 个比特进行加密。

2. 根据权利要求 1 所述的方法，还包括以下步骤：

- 延长短于 k 比特的至少一个消息 M，以获得至少 k 比特长的延长的消息；

- 如果延长的消息 M 为 k 比特长，则对延长的消息的 k 个比特进行加密；以及

- 如果延长的消息 M 长于 k 比特，则对延长的消息的小于延长消息总长度的至少 k 个比特进行加密。

3. 根据权利要求 2 所述的方法，其中，通过填充对至少一个消息 M 进行延长。

4. 根据权利要求 2 所述的方法，其中，通过与至少一个其他消息相拼接来延长至少一个消息 M。

5. 根据权利要求 1 所述的方法，其中，对长于 k 比特的消息的正好 k 个比特进行加密。

6. 根据权利要求 5 所述的方法，其中，均匀分布的符号也是有因果关系的。

7. 根据权利要求 1 所述的方法，其中，至少一个消息 M 是 JPEG2000 编码的。

8. 一种使用密钥长度为 k 的加密密钥 K 对均匀分布的符号的至少一个消息 M 进行加密的装置 (710)，该装置包括处理器 (730)，所述处理器 (730) 适于：

- 对所述至少一个消息 M 中长度为 k 比特的每一个消息 M 的 k 个比特进行加密；

其特征在于，所述处理器 (730) 还适于：

- 对所述至少一个消息 M 中长度大于 k 比特的每一个消息 M 的小于消息 M 总长度的至少 k 个比特进行加密。

9. 一种使用密钥长度为 k 的解密密钥 K 对至少一个已加密消息 [M] 进行解密的方法，在解密设备 (930) 处，该方法包括以下步骤：

- 对所述至少一个已加密消息 [M] 中长度为 k 比特的每一个已加密消息 [M] 的 k 个比特进行解密；

其特征在于，该方法还包括以下步骤：

- 对所述至少一个消息 M 中长度大于 k 比特的每一个消息 M 的小于消息 M 总长度的至少 k 个比特进行解密。

10. 一种使用密钥长度为 k 的解密密钥 K 对至少一个已加密消息 [M] 进行解密的装置 (910)，该装置包括处理器 (930)，所述处理器 (930) 适于：

- 对所述至少一个消息 M 中长度为 k 比特的每一个消息 M 的 k 个比特进行解密；

其特征在于，所述处理器 (930) 还适于：

- 对所述至少一个消息 M 中长度大于 k 比特的每一个消息 M 的小于消息 M 总长度的至少 k 个比特进行解密。

选择性数据加密的方法和装置

技术领域

[0001] 本发明总体上涉及数据加密，具体涉及以分组化比特流形式组织的图像数据的加密。

背景技术

[0002] 本节旨在向读者介绍与以下描述和 / 或要求保护的本发明的各方面有关的现有技术的各方面。相信此处的讨论有助于向读者提供背景知识，以便更好地理解本发明的各个方面。因此，应当理解的是应该据此阅读这些说明，而不应将这些说明视为对现有技术的认可。

[0003] 作为示意示例，下面的描述涉及分组化视频数据流的保护，诸如那些通过例如 JPEG2000 编码而获得的视频数据流。然而，技术人员将认识到本发明的数据保护也可以用于在具有必要属性的分组中传输数据的类似领域。

[0004] 一直以来已知通过加密来对数据进行保护，特别是在条件访问电视系统中。图 1 示出了内容访问控制的传统现有技术方法。首先使用标准压缩编码器对视频信号 CNT 进行编码 110，并且然后通过对称加密标准（例如 DES、AES、或 IDEA）对所产生的比特流 CNT’进行加密 120。然后通过接收器接收已加密比特流 [CNT’]，该接收器对已加密数据进行解密 130 以获得编码比特流 CNT’，对此编码比特流 CNT’进行解码 140 从而获得至少从理论上来说与原始视频信号一样的视频信号 CNT。在这种方法中，所谓的完全分层、压缩以及加密是完全独立的过程。假设明文中的所有符号或比特是具有同等重要性的，即，符号是均匀分布的，该媒体比特流作为传统的明文数据进行处理。

[0005] 当内容的传输不受约束时，这种方案是适当的，但是，在资源（例如存储器、功率或计算能力）有限的情况下看起来就不适当了。例如，另一种方式是有时希望提高例如处理器处理已加密数据的能力。

[0006] 此外，许多研究表明了图像和视频内容的具体特征（高传输速率和有限的允许带宽），判定针对这样的内容的标准密码技术的不足。这已经使得研究者探索一种新的保护内容安全的方案（命名为“选择性加密”、“部分加密”、“软加密”或“感知加密”），通过比特流的子集应用加密，以期望在没有对已加密子集进行解密的情况下所得到的部分加密的比特流是无用的。一般方法是将内容分成两个部分 :第一部分是信号的基本部分（例如离散余弦变换 DCT 分解中的直流 DC 系数，或离散小波变换 DWT 分解中的低频率层），这允许重构原始信号的清晰但是低质量的版本 ;以及第二部分，可以被称作“增强”部分（例如，图像的 DCT 分解中的交流 AC 系数，或 DWT 中的高频层），这允许恢复图像的精细细节并重构原始信号的高质量版本。根据这种新方案，仅加密基本部分，而以未加密的形式来发送增强部分，或在一些情况中以具有轻量加扰的形式发送增强部分。目的在于保护内容而不是二进制流本身。

[0007] 图 2 示出了根据现有技术的选择性加密。如图 1 所示来执行编码和解码。在选择性加密中，根据选择性加密参数 240 对编码比特流 CNT’进行加密 220。如上所述，例如，这

些参数可以表明仅应对 DC 系数或低频层进行加密，而应保持编码比特流 CNT' 的其余部分未加密。然后根据选择性加密参数 240 来（部分地）解密 230 部分加密的比特流 [CNT']。

[0008] T.Kunkelmann 和 R.Reinema 在“A Scalable Security Architecture for Multimedia Communication Standards”;Multimedia Computing and Systems ′ 97。Proceedings,IEEE International Conference on Ottawa,Ont.,Canada,3-6 June 1997,Los Alamitos,CA,USA,IEEE Comput.Soc,US,3 June 1997,pages 660-661,XP010239268,ISBN:978-0-8186-7819-6 中描述了示例性的选择性加密方案。为了加密 8×8 块，选择两个小于 64 的整数值；一个值用于 DC 分量，另一个值用于 AC 分量。然后加密各个单独块，例如使用具有密钥长度为 64 比特的 DES（例如 Scheier B:“Applied Cryptography,Description of DES”Applied Cryptography,Second Edition,Protocols,Algorithms and Source Code in C,John Wiley & Sons,Inc,New York,1 January 1996,pages 270-277,XP002237575,ISBN:978-0-471-11709-4 所描述的）。显然，也可以使用其他诸如 US 2001/0033656 中所描述的适当的块加密方法。将该过程进行迭代，直到已经对多个 AC 和 / 或 DC 分量进行加密为止。换句话来说，不是对所有分量进行加密，而是对每一个分量进行完全加密。

[0009] 由于本发明特别适合于 JPEG2000，JPEG2000 也用作本发明的非限制性实施例，现在将给出这个标准的相关部分的简要介绍，例如它的码流结构。

[0010] 将 JPEG2000 码流组织到分组中，码流分组是传送来自称作分辨率、层、分量和区的实体特定组合的数据的基本单元。压缩图像具有 R 个分辨率、L 个层、P 个分区以及 C 个分量，因此产生 R×L×C×P 个分组。

[0011] JPEG2000 利用嵌入的比特流：可以在分组的任意给出的结尾处截去码流，不会对先前已编码的码流有不良的影响。

[0012] 图 3 示出了主码流结构，包括：

[0013] •主报头 310，包括码流起始 (SOC = 0xFF4F) 标记段 312 和主报头标记段 314。SOC 标记指示码流的起始并且用作第一标记。主报头标记段指示多个用户定义的压缩参数，例如，进行顺序、主编码类型、分量编码类型以及拼接块 (tile) 大小。

[0014] • 一个或多个拼接块部分报头 320a、320b，每个拼接块部分报头包括拼接块部分标记起始 (SOT = 0xFF90)322、拼接块部分信息 324a、424b 以及数据标记起始 (SOD = 0xFF93)326。将认识到，SOT 322 和 SOD 326 具有标准值，而拼接块部分信息 324a、324b 包括与拼接块有关的信息；例如，拼接块部分信息 324a 指示该拼接块属于拼接块 0，而拼接块部分信息 324b 指示该拼接块属于拼接块 1。在每个拼接块部分的起始处需要至少一个拼接块部分报头 320a、320b，所述拼接块部分包括拼接块部分报头 320a、320b 以及通常包括随其后的比特流 330a、330b，其中 SOD 标记指示包含压缩数据在内的比特流 330a、330b 的起始。

[0015] • 码流结束 340：该标记 (EOC = 0xFFD9) 指示码流的结束。

[0016] 可以看出，比特流主要由分组报头以及形成分组的分组数据构成。图 4 示出了包括分组报头 420 以及分组数据 440 在内的示例性 JPEG2000 分组。根据用户定义的选项，分组报头可以用在比特流中或用在主报头中。图 4 示出了比特流内这种报头的使用：分组报头起始 410(SOP = 0xFF91) 和分组报头结束 430(EPH = 0xFF92) 分别指示分组报头 420 的

起始和结束。

[0017] 应注意，对于分组数据，在 JPEG2000 中保留了一些码字（在范围 [0xFF90 ; 0xFFFF] 内的码字）。这种保留的码字用作为流的主构建块定界的标记或标记段。例如，SOT(0xFF90)、SOD(0xFF93) 和 EOC(0xFFD9) 是这种保留的码字。当对码流进行加密时，重要的是确保‘正常’（即，非保留的）码字不会导致其值被保留的加密码字。对分组数据进行熵编码，并且这个特征使得他们非常适合后面所描述的密码安全选择性加密。

[0018] 分组报头 420 包括解码器正确解析和解码分组数据所需的信息 :

[0019] • 零长度分组 :指示当前分组是否为空。

[0020] • 码块包含 :针对每个分区，使用标签树对所包含的码块的包含信息进行编码。

[0021] • 零比特平面信息 :针对每个分区，标签树对第一非零比特平面进行编码。

[0022] • 编码通道的数目 :使用霍夫曼型码字对针对每个码块而包含的编码通道的数目进行编码。

[0023] • 来自每个码块的压缩数据的长度。

[0024] M.Van Droogenbroeck 和 R.Benedett 在“Techniques for a Selective Encryption of Uncompressed and Compressed Images”，Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS)2002，Ghent，Belgium，September 9-11，2002，提出了将选择性加密应用于哈夫曼编码器。实际上，JPEG 哈夫曼编码器使用码字 / 符号终止零的运行以近似于熵。将附加比特添加至这些码字，来充分指定非零系数的幅度和符号，仅使用 DES 或 IDEA 对这些附加比特进行加密。

[0025] 在“Selective Encryption of Wavelet-Packet Encoded Image Data”，ACM Multimedia Systems Journal，Special Issue on Multimedia Security in 2003 中，A.Pommer 和 A.Uhl 提出了基于图像编码的小波分组的报头信息的 AES 加密的算法，该报头指定子带树结构。

[0026] 在“Compliant Encryption of JPEG2000 Codestreams”，IEEE International Conference on Image Processing(ICIP 2004)，Singapore，October 2004 中，Y.Wu 和 R.H.Deng 提出了符合 JPEG2000 的加密算法，该加密算法迭代地加密对分组的码块贡献 (CCP)。加密过程使用流密码或块密码（优选地，采用算数模加法的流密码）作用于（分组数据中的）CCP 上。使用 Rivest 密码 4(CR4) 来产生密钥流。迭代地加密每个 CCP，直到该 CCP 不具有禁用码字（即，在 [0xFF90，0xFFFF] 范围内的任何码字）为止。

[0027] 在“Selective Encryption of the JPEG2000 Bitstream”，in A.Lioy and D.Mazzocchi，editors，Communications and Multimedia Security.Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security，CMS ′ 03，volume 2828 of Lecture Notes on Computer Science，pages 194-204，Turin，Italy，Oct.2003.Springer-Verlag 中，R.Norcen 和 A.Uhl 观察到 JPEG2000 是一种嵌入式比特流，按照 JPEG2000 压缩图像的进行顺序，在比特流的起始发送最重要的数据。基于这一点，所提出的方案在于对所选分组数据的 AES 加密。该算法使用两个可选标记 SOP 和 EPH（如图 5 所示）来标识分组数据。然后在 CFB 模式下使用 AES 来加密该分组数据，这是因为该分组数据具有可变的长度。以不同的进行顺序（分辨率和层进行顺序）对两种图像（有损压缩和无损压缩的图像）进行实验。评估准则是针对给定量的加密数据

而得到的视觉退化。发现对于有损压缩的图像，层进行给出更好的结果。对于无损压缩的图像，分辨率进行给出较好的结果。

[0028] 欧洲专利申请 EP 08300093.5 提供了一种改进的解决方案，该方案针对每一个分组使用失真率比值，以按照递减比值对分组进行排序，并且加密分组，直到实现预定累加的失真。

[0029] 然而，该申请人已经发现当对分组数据进行加密时仍然有改进的空间。

[0030] 因此，应当理解，需要一种允许进一步改进加密而不会不可接受地降低加密内容的安全性的解决方案。本发明提供了这样的解决方案。

发明内容

[0031] 在第一方面中，本发明涉及一种使用密钥长度 k 的加密密钥 K 对均匀分布的符号的至少一个消息 M 进行加密的方法。对至少一个消息 M 中 k 比特长度的每一个消息 M 的 k 个比特进行加密，并且对至少一个消息 M 中长度大于 k 比特的每一个消息 M 的小于消息 M 总长度的至少 k 个比特进行加密。

[0032] 在第一优选实施例中，延长长度小于 k 比特的至少一个消息 M，以获得至少 k 比特长的延长的消息。如果延长的消息为 k 比特长，则对延长的消息的 k 个比特进行加密；以及如果延长的消息长于 k 比特，则对延长的消息的小于总长度的至少 k 个比特进行加密。有利的是，通过填充或与至少一个其他消息拼接，来延长至少一个消息 M。

[0033] 在第二优选实施例中，对长度大于 k 比特的消息的正好 k 个比特进行加密。有利的是，均匀分布的符号进一步是有因果关系的。

[0034] 在第三优选实施例中，对至少一个消息 M 进行 JPEG2000 编码。

[0035] 在第二方面中，本发明涉及一种使用密钥长度为 k 的加密密钥 K 对对均匀分布的符号的至少一个消息 M 进行加密的装置。该装置包括处理器，适于对至少一个消息 M 中长度为 k 比特的每一个消息 M 的 k 个比特进行加密，以及对至少一个消息 M 中长度大于 k 比特的每一个消息 M 的小于消息 M 总长度的至少 k 个比特进行加密。

[0036] 在第三方面中，本发明涉及一种使用密钥长度为 k 的解密密钥 K 对至少一个已加密消息 [M] 进行解密的方法。解密设备对至少一个已加密消息 [M] 中长度为 k 比特的每一个已加密消息 [M] 的 k 个比特进行解密；并且对至少一个消息 M 中长度大于 k 比特的每一个消息 M 的小于消息 M 总长度的至少 k 个比特进行解密。

[0037] 在第四方面中，本发明涉及一种使用密钥长度为 k 的加密密钥 K 对至少一个已加密消息 [M] 进行解密的装置。该装置包括：处理器，适于对至少一个消息 M 中长度为 k 比特的每一个消息 M 的 k 个比特进行解密；并且对至少一个消息 M 中长度大于 k 比特的每一个消息 M 的小于消息 M 总长度的至少 k 个比特进行解密。

附图说明

[0038] 现在参考附图，作为非限制示例，对本发明的优选特征进行描述，其中：

[0039] 图 1 示出了内容访问控制的传统现有技术方法；

[0040] 图 2 示出了根据现有技术的选择性加密；

[0041] 图 3 示出了现有技术的 JPEG2000 主码流结构；

[0042] 图 4 示出了示例现有技术 JPEG2000 分组；

[0043] 图 5 示出了根据现有技术从图像编码中发出的 JPEG2000 分组；

[0044] 图 6 示意性示出了使用本发明实施例的构思已加密消息 M；

[0045] 图 7 示出了根据本发明优选实施例的选择性加密的加密装置；

[0046] 图 8 示出了根据本发明优选实施例的选择性加密方法；以及

[0047] 图 9 示出了根据本发明优选实施例的解密设备。

具体实施方式

[0048] 本发明使用 JEPG2000 编码的固有特征作为开始点以达到令人惊讶的目的。在 JPEG2000 中，对分组的码块贡献 (CCP) 是有因果关系的。实际上，通过基于上下文的 CABAC（上下文自适应二进制算数编码）编码器对码块进行编码。换句话讲，不访问数据的开头对 CCP 进行正确的解码是不可能的，数据的开头使得对比整个分组少的数据进行加密以保证加密安全性成为可能。

[0049] 图 5 示出了根据现有技术与编码图像相对应的多个 JPEG2000 编码分组。对这些分组进行排列，使得与特定质量层 (L) 相对应的分组在同一行。

[0050] 图 6 示出了 n 个字节的消息 M，其中要对 n_e 个字节进行加密。例如在 JPEG2000 的情况下，M 由多个可能有因果关系的均匀分布符号组成。应该注意的是，将消息 M 认为是有效载荷，例如，它不包括任何报头，然而整个消息 M 用于接收器。为了确定消息 M 中要加密的数据量（即，n_e），考虑使用以下加密比 ER 进行已加密消息 M（代表 CCP）：

[0051] $$ER = \frac{n_e}{n} = \frac{n_e}{|M|}$$

[0052] 其中 |M| 是 M 的比特数。

[0053] 为了找到保证加密安全性的最小加密比，使用一个度量来测量已加密消息的不可预知性。

[0054] 本发明的主要构思是考虑优化的穷举 (brute attack) 攻击，攻击者具有语言符号可能性分布的全部的知识。设 X 为在语言中使用其值的离散随机变量。

[0055] $$L^{n_e}, X \in \left\{X_1, X_2 \ldots X_{|L^{n_e}|}\right\}$$

[0056] 攻击者通过按所有可能值的概率的降序排列尝试这些可能值，以试图猜测 X 的值：

[0057] $$P_1 \geq P_2 \ldots \geq P_{|L^{n_e}|}$$

[0058] 这里给出猜测 (guesswork)W：

[0059] $$W(X) = \sum_{i=1}^{L^{n_e}} i \cdot p_i$$

[0060] 其中，W(X) 是攻击者在找到正确值消息之前必须尝试的猜测的期望数目。

[0061] 注意，因此使用输出均匀分布数据的算数编码对码块贡献进行编码：

[0062] $$P_i = 1/|L^{n_e}| = 1/|\Sigma|^{n_e}$$

[0063] 其中，Σ是码块贡献的字母表示。这里给出猜测值：

[0064] $$W(X)=\frac{1}{|\Sigma|^{n_e}}\sum_{i=1}^{|\Sigma|^{n_e}} i=\frac{|\Sigma|^{n_e}+1}{2}$$

[0065] 另一方面，如果攻击者使用密钥猜测，给出必须进行猜测（或尝试）以找到正确密钥的密钥 W(K) 的期望数目针对 k 比特密钥，通过下面给出：

[0066] $$W(X)=\sum_{i=1}^{2^k}\frac{i}{2^k}=\frac{2^k+1}{2}$$

[0067] 从后面的两个等式中，可以得出结论，如果 W(X) ≥ W(K)，消息空间的穷举攻击比密钥猜测要困难，还可以表示为：

[0068] $$|\Sigma|^{n_e}\geq 2^k$$

[0069] 因此，加密部分的大小具有由以下公式确定较低的界限：

[0070] $$n^e\geq\frac{k}{\log_2(|\Sigma|)}$$

[0071] 在 JPEG2000 选择性加密算法的示例性实施例中，典型值包括：

[0072] ●深入研究的加密算法 AES-128，k = 128

[0073] ● | Σ | = 256

[0074] 这里给出：

[0075] $n^e \geq 16$

[0076] 概括来讲，给定这些参数的情况下，建议加密的部分至少与加密密钥（128 比特 = 16 字节）一样长；否则，可以绕过加密算法，并且对于攻击者而言明文空间的穷举攻击变得更容易。因此，如果加密的比特数目在 k 和 M-1 之间，则提高加密效率，而同时保持加密安全性。

[0077] 在一般 JPEG2000 情况下，根据本发明，考虑属于 $Pack_e$ 的并且包括来自于 p 个编码块 $\{m_1, m_2, \cdots, m_p\}$ 的贡献的分组数据，以确保加密安全性，应当对来自每个码块贡献的至少$\frac{k}{\log_2(|\Sigma|)}$个字节进行加密。技术人员将理解这个结果将被概括为由其他适合的编码方法产生的数据。

[0078] 然而，为了优化加密，优选对正好该数目的字节进行加密。为了这个目的，在编码处理期间，针对 $Pack_e$ 中的每个分组，产生给出每个码块贡献的长度的元数据。如果码块贡献小于$\frac{k}{\log_2(|\Sigma|)}$，对整个码块贡献进行加密。针对目标应用要求，该方法允许实现保证密码安全性的最低加密比。

[0079] 在此示例 JPEG2000 实施例中，如所述，加密 128 比特（例如使用 AES-128）是足够的。

[0080] 如果针对加密仅选择 L_e 中最重要的层，则实现最小加密比。然后针对密码安全加密实现相同的视觉失真。

[0081] 图 7 示出了根据本发明的优选实施例的用于选择性加密的加密设备。加密设备 710 包括至少一个处理器（下文中称为“处理器”）720、用于接收至少一个消息 M 来进行加

密的输入 730、以及用于输出已加密消息 [M] 的输出 740。

[0082] 此外参考图 8，处理器 720 适于接收消息 M 进行加密（步骤 810）。在步骤 820 中，处理器确定消息长度 |M| 是否大于或等于加密密钥 K 的长度 k。如果是，则在步骤 830 中，处理器 720 使用加密密钥 K 对消息 M 的 k 个比特（优选地，前 k 个比特）进行加密。另一方面，如果消息长度 |M| 比加密密钥长度 k 短，则处理器 720 将消息 M 与其他消息进行拼接 840，来获得至少 k 比特长的消息，并且然后使用加密密钥 K 对拼接的消息的 k 个比特进行加密。应该注意，有利地拼接仅用于加密目的，也就是说加密的拼接消息随后被分成其相应的已加密消息。应该注意的是，还能够填充长度太短的消息 M，使得所填充的消息 M 包括 k 个比特。在这种情况下，可能有必要增加填充信息，以便接收器能够移除填充。

[0083] 在 JPEG2000 中，有利地，只要需要，就将消息 M 与来自最近下层的质量层 (L) 的具有相同分辨率 (R)、分量 (C) 以及分区 (P) 消息进行拼接。换句话讲，将与 $R_iC_iP_iL_i$ 相对应的消息和与 $R_iC_iP_iL_{i+1}$（其中 L_0 是最重要的层）相对应的消息进行拼接，直到拼接的长度等于所需长度。

[0084] 应该理解在大多数的情况下，消息 M 是分组的有效载荷部分。自然，还可能的是，消息 M 是分组的有效载荷的一部分。在这些情况下，不对报头部分进行加密。

[0085] 图 9 示出了根据本发明优选实施例的解密装置。解密装置 910 包括至少一个处理器（下文中称为“处理器”）、用于接收至少一个消息 [M] 进行解密的输入 930、以及用于输出解密后的消息 M 的输出 940。

[0086] 尽管在图中没有示出，解密方法反映了图 8 中示出的加密方法。处理器 920 适于接收消息 [M] 来进行解密。处理器 920 确定消息长度 |M| 是否大于或等于解密密钥 K 的长度 k。如果是，则处理器 920 使用解密密钥 K 对消息 [M] 的 k 个比特进行解密（通过加密装置进行加密的 k 个比特）。另一方面，如果消息长度 |M| 比加密密钥长度 k 短，则处理器 920 拼接已加密消息 |M|，以获得至少与加密密钥一样长拼接消息，并且使用解密密钥 K 对拼接的消息的 k 个比特进行解密。在加密期间使用的填充的情况下，没有短于 k 个比特的消息，因此可以使用解密密钥 K 对每个消息进行解密，并且如果需要可以移除（可能使用发送器提供的信息）填充。

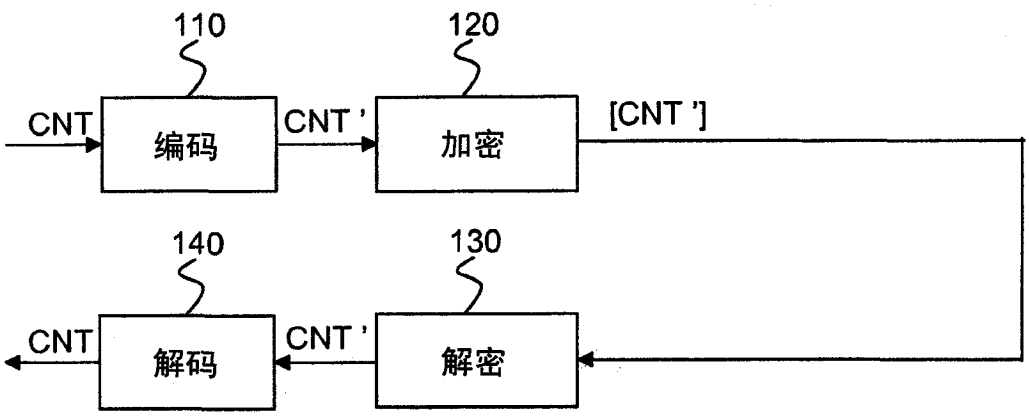
[0087] 有利的是，消息 M 是分组的有效载荷的至少一部分，因为这使得对于解密设备而言分离任意拼接消息变得更容易。

[0088] 如将要理解的，在优选实施例中，密钥 K 是对称的密钥，例即，加密密钥和解密密钥是相同的。然而，也能够使用非对称的密钥方案，例如基于椭圆曲线的方案。在这种情况下，解密密钥的长度用于确定要已加密消息的比特数。

[0089] 在说明书和权利要求（适当的地方）以及附图中所公开的每个特征都可以独立提供或以任何适当组合的形式来提供。以在硬件中实现的方式描述的特征也可以以软件形式实现，反之亦然。在适当情况下，连接可以被实现为无线连接或有线连接（不必须是直接连接或专用连接）。

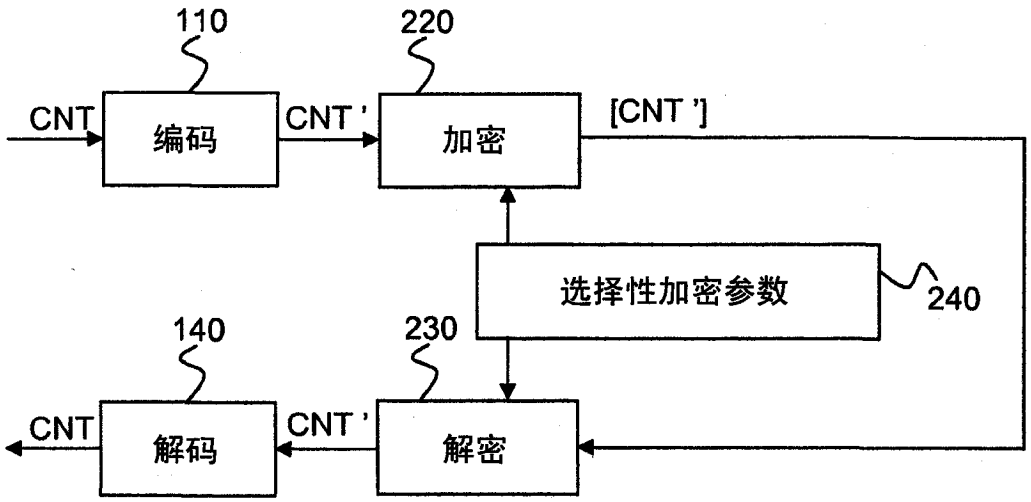
[0090] 将认识到，本发明不限于优选实施例 JPEG2000，然而可以等效地应用于其他系统中，所述其他系统具有类似的压缩图像分层结构。

[0091] 权利要求中出现的参考数字仅仅是说明性的，不应对权利要求的范围起到任何限制作用。



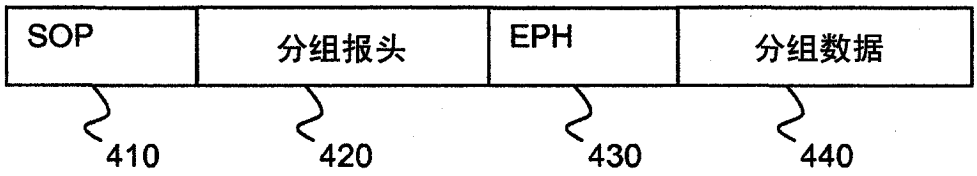
（现有技术）

图 1



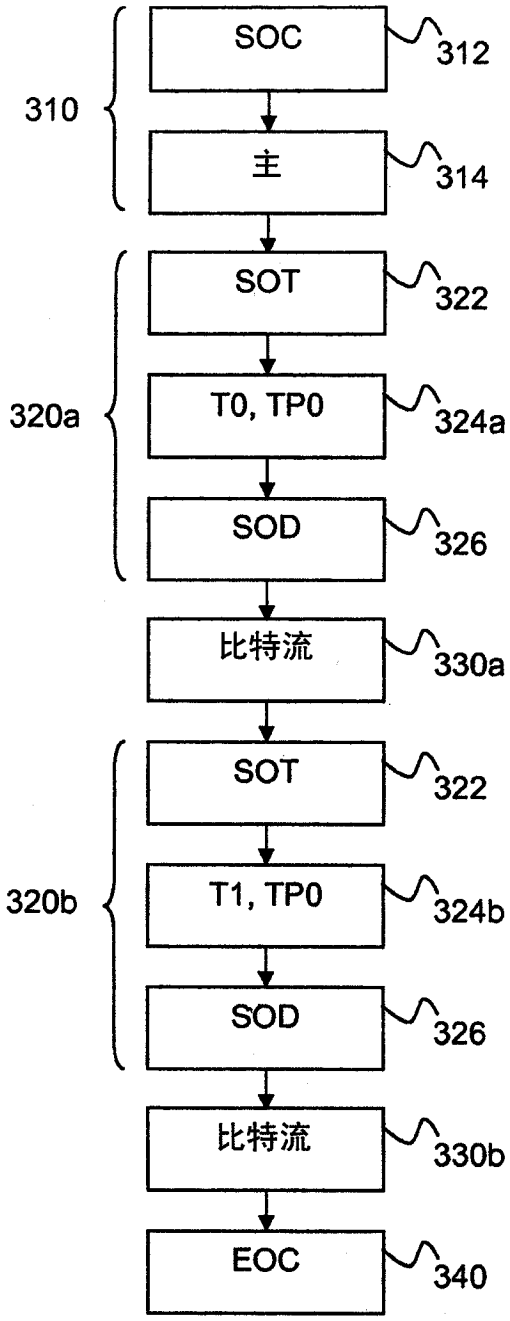
（现有技术）

图 2



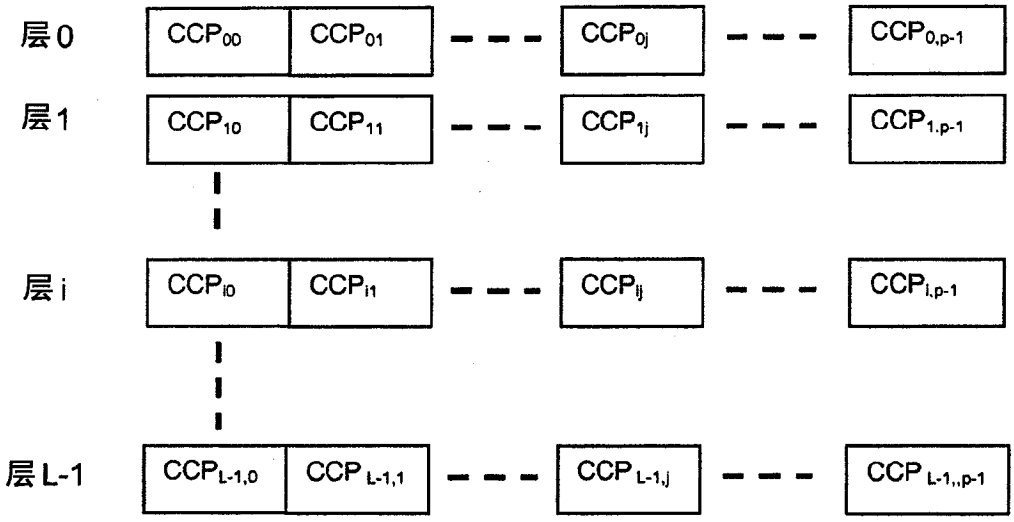
（现有技术）

图 4


SOC
312
310
主
314
SOT
322
320a
T0, TP0
324a
SOD
326
比特流
330a
SOT
322
320b
T1, TP0
324b
SOD
326
比特流
330b
EOC
340

（现有技术）

图 3


层 0
CCP00
CCP01
CCP0j
CCP0,p-1
层 1
CCP10
CCP11
CCP1j
CCP1,p-1
层 i
CCPi0
CCPi1
CCPij
CCPi,p-1
层 L-1
CCPL-1,0
CCP L-1,1
CCP L-1,j
CCP L-1,,p-1

（现有技术）

图 5

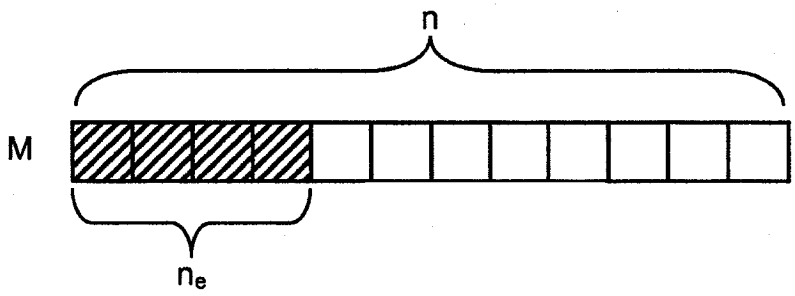

n
M
ne

图 6

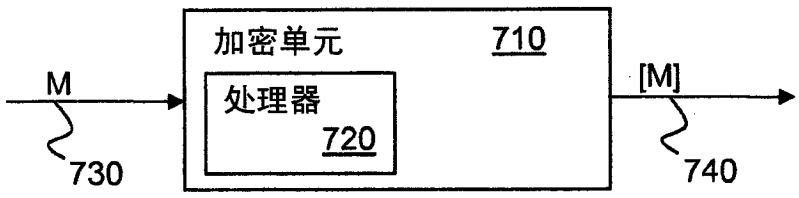

加密单元
710
处理器
720
M
730
[M]
740

图 7

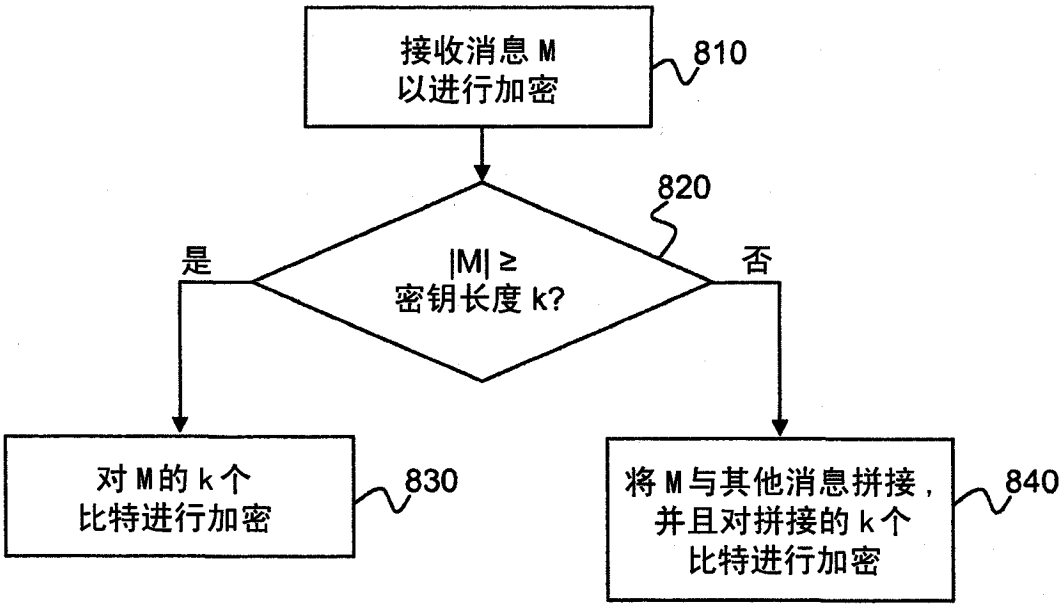

接收消息 M
以进行加密
810
820
|M| ≥
密钥长度 k?
是
否
对 M 的 k 个
比特进行加密
830
将 M 与其他消息拼接，
并且对拼接的 k 个
比特进行加密
840

图 8

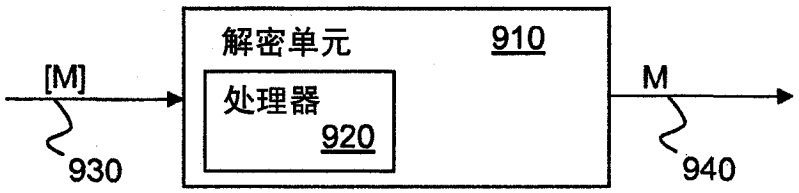

解密单元
910
[M]
处理器
920
M
930
940

图 9