(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 107078901 A
(43)申请公布日 2017.08.18

(21)申请号 201580050177.5

(22)申请日 2015.09.21

(30)优先权数据
1416631.8 2014.09.19 GB

(85)PCT国际申请进入国家阶段日
2017.03.17

(86)PCT国际申请的申请数据
PCT/EP2015/025065 2015.09.21

(87)PCT国际申请的公布数据
WO2016/041641 EN 2016.03.24

(71)申请人 古鲁洛吉克微系统公司
地址 芬兰图尔库

(72)发明人 托马斯·卡开宁 奥西·卡雷沃

(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
代理人 王达佐 王艳春

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/12(2006.01)
H04N 21/2347(2011.01)
H04N 21/2389(2011.01)
H04N 21/4385(2011.01)
H04N 21/4405(2011.01)

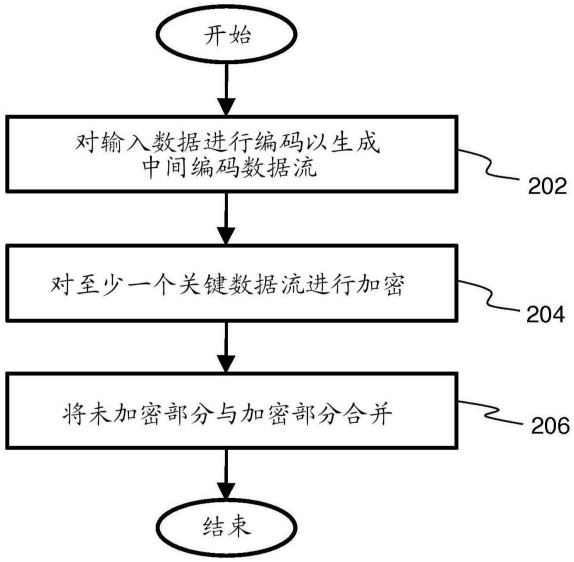
权利要求书4页 说明书20页 附图5页

(54)发明名称

采用部分数据加密的编码器、解码器和方法

(57)摘要

提供了对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的方法。输入数据(D1)被编码以生成中间编码数据流。中间编码数据流包括至少一个关键数据流，关键数据流对于中间编码数据流的一个或多个其余数据流的后续解码是关键的和必要的。使用一个或多个加密算法对至少一个关键数据流进行加密，以生成至少一个中间加密数据流。随后，中间编码数据流的未加密部分与至少一个中间加密数据流被合并在一起以生成编码和加密数据(E2)。



CN 107078901 A

1.用于对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的编码器(110),其中,所述编码器(110)包括用于处理所述输入数据(D1)的数据处理配置,其特征在于:

(a)所述数据处理配置能够操作成对所述输入数据(D1)进行编码,从而生成多个中间编码数据流,其中,所述多个中间编码数据流包括至少一个关键数据流,所述至少一个关键数据流对于所述多个中间编码数据流的一个或多个其余数据流的后续解码是关键和必要的,其中,所述至少一个关键数据流仅表示所述多个中间编码数据流的一部分;

(b)所述数据处理配置能够操作成使用一个或多个加密算法来对所述至少一个关键数据流进行加密,从而生成至少一个中间加密数据流;以及

(c)所述数据处理配置能够操作成将所述多个中间编码数据流的未加密部分与所述至少一个中间加密数据流合并在一起以生成所述编码和加密数据(E2)。

2.如权利要求1所述的编码器(110),其特征在于,所述至少一个关键数据流包括指示以下各项中的至少一项的信息:用于将所述输入数据(D1)划分和/或组合成多个数据块和/或数据包的多个分割操作和/或组合操作;用于对所述多个数据块和/或数据包的信息进行编码的一个或多个编码方法;用于将所述多个数据块和/或数据包熵编码为多个熵编码数据块和/或数据包的一个或多个熵编码方法;和/或熵编码数据流中的所述多个熵编码数据块和/或数据包的长度;和/或所述多个数据块和/或数据包在熵编码之前的长度。

3.如权利要求2所述的编码器(110),其特征在于,所述数据处理配置能够操作成执行对所述多个数据块和/或数据包的统计分析和/或迭代分析,以确定指示所述多个数据块和/或数据包中的相应的数据块和/或数据包内的统计变化的多个参数,以及其中,所述数据处理配置能够操作成采用所述多个参数来选择用于对所述多个数据块和/或数据包的信息进行编码以生成所述多个中间编码数据流的一个或多个编码方法。

4.如权利要求1、2或3所述的编码器(110),其特征在于,所述数据处理配置能够操作成处理以下列形式中的至少一种形式提供的输入数据(D1):一维数据、多维数据、文本数据、二进制数据、传感器数据、音频数据、图像数据、视频数据、编码数据。

5.如权利要求1、2、3或4所述的编码器(110),其特征在于,所述数据处理配置能够操作成在对所述至少一个关键数据流进行加密之前将所述至少一个关键数据流压缩成至少一个压缩数据流。

6.如权利要求5所述的编码器(110),其特征在于,所述数据处理配置能够操作成计算所述至少一个压缩数据流的第一字节,所述第一字节描述用于压缩所述至少一个关键数据流的熵编码方法。

7.如权利要求1至6中任一项所述的编码器(110),其特征在于,所述数据处理配置能够操作成通过使用以下各项中的至少一项来限定加密:在加密数据流的开始处写入的新字节、在熵编码方法字节和/或熵编码方法字中的最高有效位、未加密数据流和加密数据流被包括在所述编码和加密数据(E2)中的顺序、标志位。

8.通过编码器(110)对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的方法,其中,所述编码器(110)包括用于处理所述输入数据(D1)的数据处理配置,其特征在于,所述方法包括:

(a)操作所述数据处理配置以对所述输入数据(D1)进行编码,从而生成多个中间编码

数据流，其中，所述多个中间编码数据流包括至少一个关键数据流，所述至少一个关键数据流对于所述多个中间编码数据流的一个或多个其余数据流的后续解码是关键和必要的，其中，所述至少一个关键数据流仅表示所述多个中间编码数据流的一部分；

(b)操作所述数据处理配置以使用一个或多个加密算法来对所述至少一个关键数据流进行加密，从而生成至少一个中间加密数据流；以及

(c)操作所述数据处理配置以将所述多个中间编码数据流的未加密部分与所述至少一个中间加密数据流合并在一起以生成所述编码和加密数据(E2)。

9.如权利要求8所述的方法，其特征在于，所述至少一个关键数据流包括指示以下各项中的至少一项的信息：用于将所述输入数据(D1)划分和/或组合成多个数据块和/或数据包的多个分割操作和/或组合操作；用于对所述多个数据块和/或数据包的信息进行编码的一个或多个编码方法；用于将所述多个数据块和/或数据包熵编码为多个熵编码数据块和/或数据包的一个或多个熵编码方法；和/或熵编码数据流中的所述多个熵编码数据块和/或数据包的长度；和/或所述多个数据块和/或数据包在熵编码之前的长度。

10.如权利要求9所述的方法，其特征在于，所述方法包括：

(d)操作所述数据处理配置以执行对所述多个数据块和/或数据包的统计分析和/或迭代分析，以确定指示所述多个数据块和/或数据包中的相应的数据块和/或数据包内的统计变化的多个参数；以及

(e)操作所述数据处理配置以采用所述多个参数来选择用于对所述多个数据块和/或数据包的信息进行编码以生成所述多个中间编码数据流的一个或多个编码方法。

11.如权利要求8、9或10所述的方法，其特征在于，所述方法包括操作所述数据处理配置以处理以下列形式中的至少一种形式提供的输入数据(D1)：一维数据、多维数据、文本数据、二进制数据、传感器数据、音频数据、图像数据、视频数据、编码数据。

12.如权利要求8、9、10或11所述的方法，其特征在于，所述方法包括操作所述数据处理配置以在对所述至少一个关键数据流进行加密之前将所述至少一个关键数据流压缩成至少一个压缩数据流。

13.如权利要求12所述的方法，其特征在于，所述方法包括操作所述数据处理配置以计算所述至少一个压缩数据流的第一字节，所述第一字节描述用于压缩所述至少一个关键数据流的熵编码方法。

14.如权利要求8至13中任一项所述的方法，其特征在于，所述方法包括操作所述数据处理配置以通过使用以下各项中的至少一项来限定加密：在加密数据流的开始处写入的新字节、在熵编码方法字节和/或熵编码方法字中的最高有效位、未加密数据流和加密数据流被包括在所述编码和加密数据(E2)中的顺序、标志位。

15.用于对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的解码器(120)，其中，所述解码器(120)包括用于处理所述编码和加密数据(E2)的数据处理配置，其特征在于：

(i)所述数据处理配置能够操作成处理所述编码和加密数据(E2)以确定所述编码和加密数据(E2)中的一个或多个加密子部分以及一个或多个未加密子部分，其中，所述编码和加密数据(E2)中的所述一个或多个未加密子部分包括被编码的多个数据块和/或数据包的信息；

(ii)所述数据处理配置能够操作成对所述一个或多个加密子部分进行解密,以确定与所述多个数据块和/或数据包相关联的尺寸和/或相对位置和/或一个或多个编码方法;

(iii)所述数据处理配置能够操作成将所述一个或多个编码方法的逆过程应用于被编码的多个数据块和/或数据包的信息以对被编码的多个数据块和/或数据包的信息进行解码,从而生成多个解码数据块和/或数据包;以及

(iv)所述数据处理配置能够操作成基于与所述多个数据块和/或数据包相关联的尺寸和/或相对位置来组合所述多个解码数据块和/或数据包以生成所述解密和解码数据(D3)。

16.如权利要求15所述的解码器(120),其特征在于,所述一个或多个加密子部分以至少一个压缩数据流的形式提供,以及所述数据处理配置能够操作成从所述至少一个压缩数据流的第一字节确定与所述至少一个压缩数据流相关联的熵编码方法。

17.如权利要求15或16所述的解码器(120),其特征在于,所述数据处理配置能够操作成使用以下各项中的至少一项来确定所述一个或多个加密子部分以及所述一个或多个未加密子部分:在加密数据流的开始处写入的新字节、在熵编码方法字节和/或熵编码方法字中的最高有效位、包括在所述编码和加密数据(E2)中的未加密数据流和加密数据流的顺序信息、标志位。

18.如权利要求15、16或17所述的解码器(120),其特征在于,所述数据处理配置能够操作成对以下列形式中的至少一种形式提供的所述编码和加密数据(E2)进行解密和解码:编码和加密的一维数据、编码和加密的多维数据、编码和加密的文本数据、编码和加密的二进制数据、编码和加密的传感器数据、编码和加密的音频数据、编码和加密的图像数据、编码和加密的视频数据。

19.通过解码器(120)对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的方法,其中,所述解码器(120)包括用于处理所述编码和加密数据(E2)的数据处理配置,其特征在于,所述方法包括:

(i)操作所述数据处理配置以处理所述编码和加密数据(E2)以确定所述编码和加密数据(E2)中的一个或多个加密子部分以及一个或多个未加密子部分,其中,所述编码和加密数据(E2)中的所述一个或多个未加密子部分包括被编码的多个数据块和/或数据包的信息;

(ii)操作所述数据处理配置以对所述一个或多个加密子部分进行解密,以确定与所述多个数据块和/或数据包相关联的尺寸和/或相对位置和/或一个或多个编码方法;

(iii)操作所述数据处理配置以将所述一个或多个编码方法的逆过程应用于被编码的多个数据块和/或数据包的信息以对被编码的多个数据块和/或数据包的信息进行解码,从而生成多个解码数据块和/或数据包;以及

(iv)操作所述数据处理配置以基于与所述多个数据块和/或数据包相关联的尺寸和/或相对位置来组合所述多个解码数据块和/或数据包以生成所述解密和解码数据(D3)。

20.根据权利要求19所述的方法,其特征在于,所述一个或多个加密子部分以至少一个压缩数据流的形式提供,以及所述方法包括操作所述数据处理配置以从所述至少一个压缩数据流的第一字节确定与所述至少一个压缩数据流相关联的熵编码方法。

21.根据权利要求19或20所述的方法,其特征在于,所述方法包括操作所述数据处理配置以使用以下各项中的至少一项来确定所述一个或多个加密子部分以及所述一个或多个

未加密子部分:在加密数据流的开始处写入的新字节、在熵编码方法字节和/或熵编码方法字中的最高有效位、包括在所述编码和加密数据(E2)中的未加密数据流和加密数据流的顺序信息、标志位。

22.如权利要求19、20或21所述的方法,其特征在于,所述方法包括操作所述数据处理配置以对以下列形式中的至少一种形式提供的所述编码和加密数据(E2)进行解密和解码:编码和加密的一维数据、编码和加密的多维数据、编码和加密的文本数据、编码和加密的二进制数据、编码和加密的传感器数据、编码和加密的音频数据、编码和加密的图像数据、编码和加密的视频数据。

23.编解码器(130),包括:至少一个如权利要求1所述的编码器(110)以对输入数据(D1)进行编码和加密从而生成相应的编码和加密数据(E2);以及至少一个如权利要求15所述的解码器(120)以对所述编码和加密数据(E2)进行解密和解码从而生成相应的解密和解码数据(D3)。

24.计算机程序产品,包括存储有计算机可读指令的非暂时性计算机可读存储介质,所述计算机可读指令能够由包括处理硬件的计算装置执行,从而执行如权利要求8或19所述的方法。

采用部分数据加密的编码器、解码器和方法

技术领域

[0001] 本公开涉及用于对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的编码器以及对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的相应方法。此外，本公开涉及用于对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的解码器以及对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的相应方法。此外，本公开涉及包括存储有计算机可读指令的非暂时性计算机可读存储介质的计算机程序产品，计算机可读指令可由包括处理硬件的计算装置执行以执行前述方法。另外，本公开涉及包括至少一个上述编码器和至少一个上述解码器的编解码器。

背景技术

[0002] 通常，术语“加密(encryption)”是指以这样的方式对消息或信息进行编码的过程，即，只有授权方可以读取消息或信息。处理加密的科学领域称为密码学。对信息进行加密在历史上早已有之，并且众所周知，每个加密算法具有其自身相关的弱点。密码分析是密码学的一个分支，用于发现加密算法的弱点。

[0003] 加密算法可以分为对称算法(即对称密钥算法)和非对称算法(即非对称密钥算法)。对称算法和非对称算法以使用和处理加密密钥的方式相互不同。对称加密算法使用共享公共密钥在发送端加密数据，并在相应的接收端解密加密数据。另一方面，非对称加密算法使用两个不同的密钥，其中一个密钥是用于加密数据的公钥，而另一个密钥是用于对加密数据进行解密的私钥。只有公钥在各方之间共享。

[0004] 此外，存在单向消息摘要函数(Digest Function)，即散列函数(Hash Function)，其不是数据加密技术，因为它们表示的数据难以复原或无法复原。然而，单向消息摘要函数用于验证数据和密码的真实性，并且还用于生成用于加密算法的加密密钥。

[0005] 众所周知，数据加密是需要相当多的计算资源的高技术要求的操作。因此，为了节省计算资源并减少计算时间，经常使用不对称加密算法和对称加密算法的混合组合。这种组合提供足够强的保护，使得未授权的第三方解密在当前计算资源情况下不能实时地执行。这种类型的方法通常用在各种不同的数据传输协议中，例如，诸如安全套接层(SSL)/传输层安全(TLS)和安全壳(SSH)，以及在签名和加密电子邮件消息的应用中，例如，完美隐私(PGP)。

[0006] 已经确定的是：密码学，即加密和密码分析的科学研究，是一个不断发展的科学领域，其中，密码分析的方法试图找到加密算法的弱点。为此，必须能够最大程度地保护信息，但是相应地需要针对实现加密的计算资源的使用进行折衷。此外，可用的计算资源通常是有限的，尤其是在最大程度节省电池电量的移动装置中。

[0007] 此外，电子邮件应用通常能够对以下项目进行加密：

[0008] (i)仅电子邮件消息，而不是电子邮件消息的电子邮件附件，或

[0009] (ii)仅电子邮件消息的电子邮件附件，而不是电子邮件消息。

[0010] 这意味着包括电子邮件附件的整个电子邮件未被加密。然而，这种类型的操作的采用是基于使用场景或客户端软件之间的不兼容性，而不是作为可用于执行加密的适度处理能力的结果。

[0011] 在过去几年中，已经对图像和视频信息的部分加密进行了大量研究，主要是因为在互联网上的数据传输量逐年呈指数增长。常规地，“部分图像加密(Partial Image Encryption)”技术通常用于基于离散余弦变换(DCT)和小波的图像和视频编解码器。然而，该技术在速度方面效率较低，并且在可实现的保护程度方面较弱。

[0012] 在一种常规技术中，给定图像的像素值被加密。在另一种常规技术中，给定图像块中的像素的顺序通过加密来加扰。在另一种常规技术中，对DCT编码的非零AC系数进行加密。在另一种常规技术中，图像的细节，即亮度、颜色对比度等被加密，而图像中的图案的形状和轮廓被保持未加密并且对于人类观察者是可见的。

[0013] 然而，上述常规技术不能高效地工作，因为当前的现有技术使用这样的方法来对不固有地产生部分数据流的图像进行编码。因此，上述常规技术不能在不对速度和加密强度之间进行妥协的情况下，进行高效部分图像加密。

发明内容

[0014] 本公开寻求提供用于对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的改进的编码器。

[0015] 此外，本公开寻求提供用于对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的改进的解码器。

[0016] 在第一方面，本公开的实施方式提供了用于对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的编码器，其中，该编码器包括用于处理输入数据(D1)的数据处理配置，其特征在于：

[0017] (a)数据处理配置能够操作成对输入数据(D1)进行编码，从而生成多个中间编码数据流，其中，多个中间编码数据流包括至少一个关键数据流，至少一个关键数据流对于多个中间编码数据流的一个或多个其余数据流的后续解码是关键和必要的，其中，至少一个关键数据流仅表示多个中间编码数据流的一部分；

[0018] (b)数据处理配置能够操作成使用一个或多个加密算法来对至少一个关键数据流进行加密，从而生成至少一个中间加密数据流；以及

[0019] (c)数据处理配置能够操作成将多个中间编码数据流的未加密部分与至少一个中间加密数据流合并在一起以生成编码和加密数据(E2)。

[0020] 可选地，编码器的数据处理配置能够操作成对以下列述形式中的至少一种形式提供的输入数据(D1)进行编码和加密：一维数据、多维数据、文本数据、二进制数据、传感器数据、音频数据、图像数据、视频数据、编码数据，但不限于此。

[0021] 编码器的数据处理配置能够操作成对输入数据(D1)进行编码，从而生成多个中间编码数据流。可选地，为此目的，编码器的数据处理配置能够操作成采用多个分割操作和/或组合操作来将输入数据(D1)划分和/或组合成多个数据块和/或数据包。

[0022] 可选地，编码器的数据处理配置能够操作成对多个数据块和/或数据包执行统计分析和/或迭代分析，以确定指示相应数据块和/或数据包内的统计变化的多个参数。编码

器的数据处理配置然后可选地能够操作成采用多个参数来选择待用于对多个数据块和/或数据包的信息进行编码，从而生成多个中间编码数据流的一个或多个编码方法。

[0023] 随后，编码器的数据处理配置能够操作成采用用于将多个数据块和/或数据包的信息编码成多个中间编码数据流的一个或多个编码方法。

[0024] 可选地，编码器的数据处理配置能够操作成采用一个或多个熵编码方法将多个数据块和/或数据包压缩成多个熵编码数据块和/或数据包，以包括在多个中间编码数据流中。这样的熵编码可选地在使用上述编码方法对一个或多个数据块和/或数据包进行编码之后执行。

[0025] 多个中间编码数据流包括至少一个关键数据流，该至少一个关键数据流对于多个中间编码数据流的一个或多个其余数据流的后续解码是关键的和必要的。可选地，该至少一个关键数据流包括指示以下各项中的至少一项的信息：

[0026] (i)用于将输入数据(D1)划分和/或组合成多个数据块和/或数据包的多个分割操作和/或组合操作，

[0027] (ii)用于对多个数据块和/或数据包的信息进行编码的一个或多个编码方法，

[0028] (iii)用于对多个数据块和/或数据包进行熵编码的一个或多个熵编码方法，和/或

[0029] (iv)该熵编码数据流中的多个熵编码数据块和/或数据包的长度；可选地，熵编码前的原始数据长度也可以用作待加密到至少一个关键数据流中的关键信息；和/或

[0030] (v)该多个数据块和/或数据包在被熵编码之前的长度。

[0031] 因此，至少一个关键数据流仅表示多个中间编码数据流的一部分。

[0032] 此外，编码器的数据处理配置能够操作成使用一个或多个加密算法来对至少一个关键数据流进行加密，从而生成至少一个中间加密数据流。

[0033] 随后，编码器的数据处理配置能够操作成将多个中间编码数据流的未加密部分(即被编码的多个数据块和/或数据包的信息)与至少一个中间加密数据流合并在一起以生成编码和加密数据(E2)。

[0034] 此外，可选地，编码器的数据处理配置能够操作成在对至少一个关键数据流进行加密之前将至少一个关键数据流压缩成至少一个压缩数据流。可选地，编码器的数据处理配置能够操作成计算至少一个压缩数据流的第一字节，该第一字节描述用于压缩至少一个关键数据流的熵编码方法。

[0035] 可选地，指示该至少一个压缩数据流的长度的信息提供在该至少一个压缩数据流的开始处，例如在前述的第一字节之后。

[0036] 此外，可选地，编码器的数据处理配置能够操作成通过使用以下各项中的至少一项来限定加密：在加密数据流的开始处写入的新字节、在熵编码方法字节和/或熵编码方法字中的最高有效位(MSB)、未加密数据流和加密数据流被包括在编码和加密数据(E2)中的顺序、和/或标志位。

[0037] 在第二方面，本公开的实施方式提供了通过编码器对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的方法，其中编码器包括用于处理输入数据(D1)的数据处理配置，其特征在于，该方法包括：

[0038] (a)操作数据处理配置以对输入数据(D1)进行编码，从而生成多个中间编码数据

流，其中，多个中间编码数据流包括至少一个关键数据流，至少一个关键数据流对于多个中间编码数据流的一个或多个其余数据流的后续解码是关键和必要的，其中，至少一个关键数据流仅表示多个中间编码数据流的一部分；

[0039] (b)操作数据处理配置以使用一个或多个加密算法来对至少一个关键数据流进行加密，从而生成至少一个中间加密数据流；以及

[0040] (c)操作数据处理配置以将多个中间编码数据流的未加密部分与至少一个中间加密数据流合并在一起以生成编码和加密数据(E2)。

[0041] 在第三方面，本公开的实施方式提供了计算机程序产品，其包括存储有计算机可读指令的非暂时性(即非瞬态)计算机可读存储介质，该计算机可读指令可由包括处理硬件的计算装置执行以执行前述方法。

[0042] 在第四方面，本公开的实施方式提供了用于对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的解码器，其中解码器包括用于处理编码和加密数据(E2)的数据处理配置，其特征在于：

[0043] (i)数据处理配置能够操作成处理编码和加密数据(E2)以确定编码和加密数据(E2)中的一个或多个加密子部分以及一个或多个未加密子部分，其中，编码和加密数据(E2)中的一个或多个未加密子部分包括被编码的多个数据块和/或数据包的信息；

[0044] (ii)数据处理配置能够操作成对一个或多个加密子部分进行解密，以确定与多个数据块和/或数据包相关联的尺寸和/或相对位置和/或一个或多个编码方法；

[0045] (iii)数据处理配置能够操作成将一个或多个编码方法的逆过程应用于被编码的多个数据块和/或数据包的信息以对被编码的多个数据块和/或数据包的信息进行解码，从而生成多个解码数据块和/或数据包；以及

[0046] (iv)数据处理配置能够操作成基于与多个数据块和/或数据包相关联的尺寸和/或相对位置来组合多个解码数据块和/或数据包以生成解密和解码数据(D3)。

[0047] 可选地，解码器的数据处理配置能够操作成对以下列形式中的至少一种形式提供的编码和加密数据(E2)进行解密和解码：编码和加密的一维数据、编码和加密的多维数据、编码和加密的文本数据、编码和加密的二进制数据、编码和加密的传感器数据、编码和加密的音频数据、编码和加密的图像数据、编码和加密的视频数据、编码数据，但不限于此。

[0048] 解码器的数据处理配置能够操作成处理编码和加密数据(E2)，以确定编码和加密数据(E2)中的一个或多个加密子部分以及一个或多个未加密子部分。编码和加密数据(E2)中的一个或多个未加密子部分包括被编码的多个数据块和/或数据包的信息。

[0049] 解码器的数据处理配置能够操作成对一个或多个加密子部分进行解密，以确定与多个数据块和/或数据包相关联的尺寸、相对位置和/或一个或多个编码方法。可选地，解码器的数据处理配置还能够操作成确定与多个数据块和/或数据包相关联的一个或多个熵编码方法。

[0050] 此外，可选地，以至少一个压缩数据流的形式提供一个或多个加密子部分。在这种情况下，解码器的数据处理配置可选地能够操作成从至少一个压缩数据流的第一字节确定与至少一个压缩数据流相关联的熵编码方法。

[0051] 可选地，指示该至少一个压缩数据流的长度的信息提供在该至少一个压缩数据流的开始处，例如在前述的第一字节之后。

[0052] 此外，可选地，解码器的数据处理配置能够操作成使用以下各项中的至少一项来确定一个或多个加密子部分以及一个或多个未加密子部分：在加密数据流的开始处写入的新字节、在熵编码方法字节和/或熵编码方法字中的最高有效位(MSB)、未加密数据流和加密数据流被包括在编码和加密数据(E2)中的顺序信息、和/或标志位。

[0053] 随后，解码器的数据处理配置可选地能够操作成应用熵编码方法的逆过程，以解压缩至少一个压缩流，以确定与多个数据块和/或数据包相关联的尺寸、相对位置和/或一个或多个编码方法。解码器的数据处理配置然后能够操作成将一个或多个编码方法的逆过程应用于被编码的多个数据块和/或数据包的信息，以对该被编码的多个数据块和/或数据包的信息进行解码，从而生成多个解码数据块和/或数据包。可选地，解码器的数据处理配置还能够操作成在应用一个或多个编码方法的逆过程之前，将一个或多个熵编码方法的逆过程应用于包括在编码和加密数据(E2)的一个或多个未加密子部分中的多个熵编码数据块和/或数据包。

[0054] 随后，解码器的数据处理配置能够操作成基于尺寸和/或相对位置来组合多个解码数据块和/或数据包，从而生成解密和解码数据(D3)。

[0055] 在第五方面，本公开的实施方式提供了通过解码器对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的方法，其中，解码器包括用于处理编码和加密数据(E2)的数据处理配置，其特征在于，该方法包括：

[0056] (i)操作数据处理配置以处理编码和加密数据(E2)以确定编码和加密数据(E2)中的一个或多个加密子部分以及一个或多个未加密子部分，其中，编码和加密数据(E2)中的一个或多个未加密子部分包括被编码的多个数据块和/或数据包的信息；

[0057] (ii)操作数据处理配置以对一个或多个加密子部分进行解密，以确定与多个数据块和/或数据包相关联的尺寸和/或相对位置和/或一个或多个编码方法；

[0058] (iii)操作数据处理配置以将一个或多个编码方法的逆过程应用于被编码的多个数据块和/或数据包的信息以对被编码的多个数据块和/或数据包的信息进行解码，从而生成多个解码数据块和/或数据包；以及

[0059] (iv)操作数据处理配置以基于与多个数据块和/或数据包相关联的尺寸和/或相对位置来组合多个解码数据块和/或数据包以生成解密和解码数据(D3)。

[0060] 在第六方面，本公开的实施方式提供了计算机程序产品，其包括存储有计算机可读指令的非暂时性(即非瞬态)计算机可读存储介质，该计算机可读指令可由包括处理硬件的计算装置执行以执行前述方法。

[0061] 在第七方面，本公开的实施方式提供了包括上述编码器和上述解码器的编解码器。

[0062] 依据本公开的实施方式的前述方法可以利用任何合适的编码布置来实现，而与使用哪种加密算法无关。在这种情况下，前述方法不改变加密算法的行为，这意味着由加密算法提供的保护不会受到妥协。

[0063] 前述方法使得可以使用很快速高效的加密算法。在这点上，前述方法可以以高效的方式与加密算法结合使用，而不会干扰加密算法本身的内部操作。适合于用前述方法实现的加密算法的示例包括但不限于AES、RSA、Twofish、Blowfish、数据加密标准(DES)、三重DES(3-DES)、Serpent、国际数据加密算法(IDEA)、MARS、Rivest Cipher6(RC6)、Camellia、

CAST-128、Skipjack、扩展微型加密算法(XTEA)等,这些示例名称包括注册商标。

[0064] 根据本公开的实施方式的前述方法提供了与已知的现有技术方法相比很快速并且相当高效的保护数据的方式。值得注意的是,仅对编码数据的一个或多个必要和关键部分进行加密。例如,当使用Gurulogic多变量编解码器(GMVC®)编码解决方案对图像或视频进行编码时,只有整个编码数据的1/100部分至1/1000部分被加密保护,但没有对数据安全性进行妥协的风险。因此,可以得出结论,以这种方式使用加密对实时视频的传输速率没有任何显著影响,也不以任何显著的方式增加计算资源的消耗。

[0065] 此外,该加密过程的附加优点是,编码和加密数据(E2)不需要通过具有受保护的安全网络连接的网络(例如采用虚拟专用网络(VPN)隧道、安全壳(SSH)或SSL/TLS协议)来传输。因此,前述方法提供了用于例如在公共互联网网络中或在网站服务和云服务中传输文本、二进制、音频、图像、视频和其它类型的数据的有利模型。

[0066] 根据结合所附权利要求解释的说明性实施方式的附图和详细描述,本公开的附加方面、有益效果、特征和目的将变得显而易见。

[0067] 应当理解,在不脱离由所附权利要求限定的本公开的范围的情况下,本公开的特征易于以各种组合方式进行组合。

附图说明

[0068] 当结合附图阅读时,将更好地理解上面的概述以及说明性实施方式的以下详细描述。为了说明本公开的目的,在附图中示出了本公开的示例性构造。然而,本公开不限于本文公开的特定方法和设备。此外,本领域技术人员将理解,附图不是按比例绘制的。在可行的情况下,相同的元件由相同的附图标记表示。

[0069] 现在将仅通过示例的方式参考以下附图来描述本公开的实施方式,其中:

[0070] 图1是根据本公开的实施方式的用于对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的编码器和用于对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的解码器的示意图,其中该编码器和该解码器共同形成编解码器;

[0071] 图2是描述根据本公开的实施方式的对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的第一方法的步骤的流程图的示意图;

[0072] 图3是根据本公开的实施方式的加密过程的步骤的示意图;

[0073] 图4是描述根据本公开的实施方式的对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的第二方法的步骤的流程图的示意图;以及

[0074] 图5是根据本公开的实施方式的解密过程的步骤的示意图。

[0075] 在附图中,带下划线的附图标记用于表示带下划线的附图标记所在的项目或带下划线的附图标记相邻的项目。不带下划线的附图标记涉及由将不带下划线的附图标记与项目链接的线标识的项目。

具体实施方式

[0076] 在以下详细描述中,阐明了本公开的说明性实施方式及其可以实现的方式。虽然描述了执行本公开的一些模式,但是本领域技术人员将认识到,用于执行或实践本公开的

其它实施方式也是可行的。

[0077] 总而言之，本公开的实施方式涉及用于部分数据加密的加密方法以及对应的解密方法。前述方法能够实现很快速的加密过程，并且提供很强的保护以防止未经授权的访问。

[0078] 前述方法有利地对已经压缩或以其它方式编码的一维或多维文本、二进制、音频、图像、视频或其它类型的数据使用已知的加密算法。然而，该方法还可选地使用迄今未知的加密算法，例如未来设计的加密算法，因为该方法的功能能够适用于各种加密算法。

[0079] 本公开中描述的部分数据加密结合各种压缩算法很高效地工作，该压缩算法基于数据的内容、属性和成分对数据进行编码。这种压缩算法通常产生多于一个数据流作为输出，其中至少一个数据流就数据的内容而言是极为重要的。

[0080] 本公开的实施方式尝试通过仅加密数据的一个或多个最重要部分来提供用于对数据加密的低成本的方式。这节省了由数据处理器消耗的计算资源和处理能量，并且减少了加密所需的时间，而不削弱对加密所需的保护程度。这种能量消耗的节省在便携式计算装置(例如智能电话)上是很有利的，其使得能够采用更小的可充电电池，或者能够延长在需要再次对电池充电之前的操作时间。

[0081] 本公开全文中，未加密信息被称为“明文(Plaintext)”，而相应地，加密信息被称为“密文(Ciphertext)”。

[0082] 参考图1，本公开的实施方式涉及：

[0083] (i)用于对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的编码器110以及对输入数据(D1)进行编码和加密以生成编码和加密数据(E2)的相应方法；

[0084] (ii)用于对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的解码器120以及对编码和加密数据(E2)进行解密和解码以生成解密和解码数据(D3)的相应方法；以及

[0085] (iii)包括至少一个编码器和至少一个解码器的组合的编解码器130，例如编码器110和解码器120的组合。

[0086] 可选地，解密和解码数据(D3)与输入数据(D1)完全相似，如在无损操作模式中。或者，可选地，解密和解码数据(D3)大致类似于输入数据(D1)，如在有损操作模式中。或者，可选地，解密和解码数据(D3)与输入数据(D1)不同，例如通过变换，例如在对数据进行代码转换时使用，但是保留存在于输入数据(D1)中的基本相似的信息；例如，当还需要对解密和解码数据(D3)进行重新格式化时，解密和解码数据(D3)与输入数据(D1)不同是有用的，例如以与不同类型的通信平台、软件层、通信装置等兼容。

[0087] 编码器110包括用于处理输入数据(D1)以生成相应的编码和加密数据(E2)的数据处理配置。可选地，编码器110的数据处理配置通过采用可操作成执行程序指令的至少一个精简指令集计算(RISC)处理器来实现，如下面将详细描述的。

[0088] 可选地，编码器110的数据处理配置可操作成对以下述形式中的至少一种形式提供的输入数据(D1)进行编码和加密：一维数据、多维数据、文本数据、二进制数据、传感器数据、音频数据、图像数据、视频数据、编码数据，但不限于此。可选地，输入数据(D1)作为流或文件被接收。

[0089] 编码器110的数据处理配置可操作成对输入数据(D1)进行编码，从而生成多个中间编码数据流。

[0090] 可选地，为了对输入数据(D1)进行编码，编码器110的数据处理配置可操作成采用多个分割操作和/或组合操作来将输入数据(D1)划分和/或组合成多个数据块和/或数据包。在第一示例中，输入数据(D1)是一维的，并且可以使用扫描线来分割。在第二示例中，输入数据(D1)是多维的，并且可以根据数据块具有的维度的数量被分割为数据块。

[0091] 在这点上，编码器110可有利地与其它已知的编码器一起使用；例如，结合在授权的英国专利GB2503295B中描述的块编码器，该英国专利通过引用并入本文。块编码器可以用于以优化的方式将输入数据(D1)分割和/或组合成多个数据块和/或数据包。

[0092] 在输入数据(D1)是一维的第一示例中，通过将输入流(即字节串)分割为更短的流来从输入数据(D1)提取数据块。例如，在常规扫描之后获得的6×4图像中的像素的索引，即，首先从左到右扫描然后从上到下扫描，可以表示如下：

[0093] 01 02 03 04 05 06

[0094] 07 08 09 10 11 12

[0095] 13 14 15 16 17 18

[0096] 19 20 21 22 23 24

[0097] 这些索引当以一维形式传输以用于编码时，产生行组合的字节串，其可以表示如下：

[0098] 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

[0099] 字节串可以例如被分割为四个字节的较短字节串，其可以表示如下：

[0100] (01 02 03 04)

[0101] (05 06 07 08)

[0102] (09 10 11 12)

[0103] (13 14 15 16)

[0104] (17 18 19 20)

[0105] (21 22 23 24)

[0106] 在第二示例中，为了说明的目的，输入数据(D1)是二维(2D)图像。在该示例中，2D图像可选地被分割为较小的2×2区域，并且可以通过在2D图像的2×2区域上使用常规扫描顺序来将2D图像中的像素的索引重新组织为四字节的字节串。这些字节串可以表示如下：

[0107] (01 02 07 08)

[0108] (03 04 09 10)

[0109] (05 06 11 12)

[0110] (13 14 19 20)

[0111] (15 16 21 22)

[0112] (17 18 23 24)

[0113] 此外，在一些示例中，输入数据(D1)可以是三维(3D)的，例如在3D视频内容中。在其它示例中，在输入数据(D1)中可以存在更多维度，例如，诸如视频中的时间。

[0114] 同样，当输入数据(D1)是音频数据时，可以执行类似的分割过程。在示例中，音频数据可选地包括来自多个麦克风的音频信号。在这种情况下，音频数据可以以单独的音频信号被分离并且然后被进一步分割成数据包的方式被分割。

[0115] 一旦输入数据(D1)被分割成多个数据块和/或数据包,则编码器110的数据处理配置可选地可操作成执行多个数据块和/或数据包的统计分析和/或迭代分析以确定指示相应的数据块和/或数据包内的统计变化的多个参数。编码器110的数据处理配置然后可选地可操作成采用多个参数来选择待用于对多个数据块和/或数据包的信息进行编码的一个或多个编码方法。

[0116] 随后,编码器110的数据处理配置可操作成采用一个或多个编码方法以将多个数据块和/或数据包的信息编码成多个中间编码数据流中的至少一个中间编码数据流。

[0117] 可选地,编码器的数据处理配置可操作成采用一个或多个熵编码方法将多个数据块和/或数据包压缩成多个熵编码数据块和/或数据包,以包括在多个中间编码数据流中的至少一个中间编码数据流中。这样的熵编码可选地在使用上述编码方法对多个数据块和/或数据包进行编码之后执行。关于这种压缩,将理解的是,当生成编码数据(E2)时,前述熵编码方法的目的是压缩数据(D1),并且这些方法在实现这样的数据压缩时通常是成功的,但是不总是成功的。在任一情况下,在本公开的实施方式中应用的给定熵编码方法需要被包括在中间编码数据流中,通常具有被熵编码的数据的长度,并且有时还具有在执行其熵编码之前的数据的长度。

[0118] 应当理解,多个中间编码数据流中的一个或多个中间编码数据流对于对多个中间编码数据流中的一个或多个其余数据流的正确解码是关键的和必要的。以下将多个中间编码数据流中的关键的和必要的一个或多个中间编码数据流称为“关键数据流”。以下将多个中间编码数据流的一个或多个其余数据流称为“非关键数据流”。

[0119] 可选地,多个中间编码数据流的关键数据流包括指示以下各项中的至少一项的信息:

[0120] (i)用于将输入数据(D1)划分和/或组合成多个数据块和/或数据包的多个分割操作和/或组合操作,

[0121] (ii)用于对多个数据块和/或数据包的信息进行编码的一个或多个编码方法,

[0122] (iii)用于对多个数据块和/或数据包进行熵编码的一个或多个熵编码方法,和/或

[0123] (iv)该熵编码数据流中的多个熵编码数据块和/或数据包的长度,和/或

[0124] (v)在应用熵编码之前该多个数据块和/或数据包的长度。

[0125] 因此,关键数据流仅表示多个中间编码数据流的一部分。关键数据流通常占整个中间编码数据流的1/100部分到1/1000部分的范围内。

[0126] 可选地,非关键数据流包括指示以下各项中的至少一项的信息:数据库参考值、离散余弦变换(DCT)参数的值、DC系数的值、滑动值、行值、比例值、多级值和/或掩码,但不限于此。

[0127] 此外,如前所述,关键数据流是多个中间编码数据流的必要部分,如果没有该关键数据流,则不可能正确地解码多个中间编码数据流的非关键数据流。因此,为了保护多个中间编码数据流免受未经授权的访问,关键数据流中的至少一个关键数据流被有利地加密,如下面更详细地阐述的。

[0128] 此外,可选地,编码器110的数据处理配置可操作成生成或接收用于对关键数据流中的至少一个关键数据流进行加密的至少一个密钥。

[0129] 可选地，在一个实现中，编码器110的数据处理配置在操作中被提供有至少一个密钥。

[0130] 或者，在另一实现中，编码器110的数据处理配置可选地可操作成使用适当的密钥生成算法来生成至少一个密钥。为此目的，编码器110的数据处理配置可选地可操作成应用密钥扩展来生成至少一个密钥。可选地，密钥扩展包括通过单向摘要算法(即，散列算法)多次重复地提供相关联的密码。

[0131] 此外，可选地，编码器110的数据处理配置可操作成使用至少一个密钥利用一个或多个加密算法来对关键数据流中的至少一个关键数据流进行加密，从而生成至少一个中间加密数据流。可选地，编码器110的数据处理配置可操作成在对关键数据流中的至少一个关键数据流进行加密时，结合至少一个密钥应用至少一个初始化向量(“Init Vector”;IV)。

[0132] 随后，编码器110的数据处理配置可操作成将包括未加密的非关键数据流的多个中间编码数据流中的未加密部分与至少一个中间加密数据流合并，从而生成编码和加密数据(E2)。

[0133] 此外，可选地，编码器110的数据处理配置可操作成在加密之前将关键数据流中的至少一个关键数据流压缩为至少一个压缩数据流。同样，可选地，编码器110的数据处理配置可操作成将非关键数据流压缩成一个或多个其它压缩数据流，以包括在编码和加密数据(E2)中。

[0134] 可选地，编码器110的数据处理配置可操作成计算至少一个压缩数据流的第一字节，使得第一字节描述用于压缩关键数据流中的至少一个关键数据流的熵编码方法。同样，可选地，编码器110的数据处理配置可操作成计算一个或多个其它压缩数据流的第一字节，使得这些第一字节描述用于压缩非关键数据流的熵编码方法。

[0135] 可选地，当对关键数据流中的至少一个关键数据流(即至少一个压缩数据流)进行加密以生成加密数据流时，将加密限定为一种熵编码方法的新字节被写入在加密数据流的开始处。当在解码器120的随后的解密和解码期间读取新字节时，解码器120注意到数据流被加密。因此，解码器120将加密数据流解密为至少一个压缩数据流，并从该至少一个压缩数据流的第一字节读取实际熵编码方法。这使得能够对至少一个压缩数据流进行解压缩。

[0136] 或者，可选地，代替传输限定加密的新字节，关于所采用的加密的信息，例如通过在熵编码方法字节和/或熵编码方法字中使用最高有效位(MSB)来将新字节与关于所采用的熵编码方法的信息组合。

[0137] 或者，可选地，编码器110可操作成向解码器120传送未加密的数据流和加密的数据流被包括在编码和加密数据(E2)中的顺序，以及关于所加密的关键数据流中的至少一个关键数据流的信息。

[0138] 或者，可选地，使用一个或多个标志位来指示哪些数据流包含被编码的信息(即，非关键数据流)，以及哪些数据流不包含被编码的信息(即，关键数据流)。

[0139] 可选地，在第一字节之后提供指示至少一个压缩数据流的长度的信息。这使得解码器120能够读取至少一个压缩数据流的长度，可将其内容复制到解码器120自身的缓冲器，并且跳转到读取下一个数据流。可选地，指示长度的信息保持未加密。或者，可选地，在新字节之后写入加密数据流的新长度。或者，可选地，第一字节在编码器110中加密，并且随后在解码器120中解密，并且然后可以在不对整个编码和加密数据(E2)进行解密和解码的

情况下在解码器120中读取至少一个压缩数据流的长度。

[0140] 在可替代的实现中，关键数据流中的至少一个关键数据流可以首先被加密，然后被压缩。然而，应当理解，在加密之前执行对关键数据流中的至少一个关键数据流的压缩是有利的，因为关键数据流中的至少一个关键数据流通常包括相当多的冗余数据。因此，编码器110的数据处理配置可操作成采用合适的熵编码方法来压缩关键数据流中的至少一个关键数据流。在这种情况下，编码和加密数据(E2)的熵和数据尺寸小于当在压缩之前对关键数据流中的至少一个关键数据流进行加密时的熵和数据尺寸。一个或多个加密算法通常倾向于在编码和加密数据(E2)中产生最大数据熵，这在数学上意味着存在如理论上可行的数量的用于对编码和加密数据(E2)进行解密的选择。

[0141] 作为示例，可从Gurulogic Microsystems Oy获得的Gurulogic多变量编解码器(GMVC®)编码解决方案与本公开的实施方式的结合可以是有益的。GMVC®编码解决方案能够对不同类型的数据进行高效编码，同时以熵编码的方式高效地产生包含原始输入的整个信息(即输入数据(D1))的若干不同数据流。例如，在前述专有GMVC®编码解决方案中，根据输入数据(D1)的格式和内容，图像数据或视频数据的编码采用相互不同的编码方法来产生各种不同的数据流。因此，有利的是，在考虑输入数据(D1)的比特计数和熵的同时，用针对那些类型的数据优化的不同的编码和熵编码方法来高效地编码和压缩不同类型的数据。压缩减小了数据尺寸。这意味着更少量的数据需要被加密，并且加密过程因此更快。

[0142] 此外，当对图像数据或视频数据进行编码时，GMVC®编码解决解决方案产生例如对于块编码器典型的数据流，其包括指示用于将输入数据(D1)分割和/或组合成多个数据块和/或数据包的多个分割和/或组合的信息(即，分割和/或组合决定)。该数据流在下文中被称为“分割/组合信息数据流(Split/Combine-Information Data Stream)”。在数据尺寸方面，分割/组合信息数据流通常在整个中间编码数据流的1/200部分到1/2000的部分的范围。分割/组合信息数据流是中间编码数据流的最重要部分之一，因为它限定了多个数据块和/或数据包的尺寸和/或相对位置。在一些实施方式中，非关键数据流的解码通常仅在已知多个数据块和/或数据包的尺寸之后才可能执行。在不同数据流中分别提供不同尺寸的数据块和/或数据包的被编码的信息的其它实施方式中，非关键数据流的解码仅在已知这些数据块和/或数据包的相对位置之后才可行。

[0143] 此外，随着GMVC®编码解决方案对多个数据块和/或数据包执行一个或多个编码方法，GMVC®编码解决方案产生另一数据流，该另一数据流包括指示用于编码多个数据块和/或数据包的信息的一个或多个编码方法的信息。该数据流在下文中被称为“编码方法数据流”。在尺寸方面，编码方法数据流通常也在整个中间编码数据流的1/100部分到1/1000部分的范围，并且是中间编码数据流的最重要部分之一。

[0144] 可选地，为不同尺寸的数据块和/或数据包产生不同的编码方法数据流。

[0145] 此外，可选地，例如基于输入数据(D1)的内容和期望的编码质量，将输入数据(D1)划分为不同尺寸的数据块和/或数据包。通常，为了更好的编码质量，将输入数据(D1)划分为较小尺寸的数据块和/或数据包，反之亦然。

[0146] 除了分割/组合信息数据流和编码方法数据流之外，GMVC®编码解决方案产生例如与图像数据或视频数据中的数据块和/或数据包的至少部分重现有关的其它数据流。

其它数据流通常包括多个数据块和/或数据包中的数据元素的数据值。然而，这些其它数据流不提供关于数据块和/或数据包的尺寸和相对位置的信息，以及用于对数据块和/或数据包的信息进行编码的编码方法。

[0147] 因此，分割/组合信息数据流和编码方法数据流对于由编码器110执行的编码处理是关键的和必要的，并且通过加密过程一起或单独保护。因此，当与所有数据流都将被加密的已知现有技术解决方案相比时，仅消耗计算资源和处理能量的从1/100部分到1/1000的部分。因此，加密过程很快，而与是否有可用的专用加密电路无关。

[0148] 此外，当分割/组合信息数据流和/或编码方法数据流被加密时，未经授权的窃听第三方不能理解如何使用其它数据流，以及数据块和/或数据包应当如何定位以及在何处定位。

[0149] 然而，可能出现数据块和/或数据包具有相等尺寸的情况，因此，在对数据块和/或数据包进行编码时不使用多种编码方法。也可能发生数据块和/或数据包根本未分割和/或组合，因为数据块和/或数据包已经具有预定的最小/最大尺寸，因此不存在要加密的分割/组合信息。在这些类型的情况下，恶意第三方有可能对数据块和/或数据包应当如何定位以及在何处定位进行解密。因此，在本公开的实施方式中可选地采用替代选项。待加密的可选流涉及一个或多个熵编码方法以及多个熵编码数据块和/或数据包的长度，其长度不同于在应用熵编码之前的多个数据块和/或数据包的长度。

[0150] 实际上，由于GMVC®编码解决方案对多个数据块和/或数据包执行一个或多个熵编码方法，GMVC®编码解码产生包括指示一个或多个熵编码方法的信息的另一数据流，该熵编码方法用于将多个数据块和/或数据包熵编码为多个熵编码的数据块和/或数据包。该数据流在下文中被称为“熵编码方法数据流”。熵编码方法数据流通常在尺寸方面包括小于整个中间编码数据流的1/1000部分，因此可以高效地用于根据本公开的实施方式的前述方法中。

[0151] 此外，由于GMVC®编码解决方案对多个数据块和/或数据包执行一个或多个熵编码方法，GMVC®编码解决方案产生另一个数据流，该另一个数据流包括指示熵编码的数据流中的多个熵编码的数据块和/或数据包的长度的信息。该数据流在下文中被称为“熵编码数据长度流”。由于熵编码数据的长度通常不同于原始数据的长度，所以第三方不可能尝试重建未加密的数据。此外，与实际数据相比，长度信息的尺寸通常很小，因此有利的是仅将长度信息与指示已经采用的一个或多个熵编码方法的信息一起加密，而不是加密整个数据。

[0152] 应当理解，在熵编码之前的数据长度通常已经是已知的，但是有时不是已知的，因而该数据长度需要被传输到解码器，例如通过将信息包括到待加密的中间编码数据流，使得可以执行解码而与其它数据及其内容无关。此外，即使熵编码数据的长度也可以被表示/传输为原始数据(即，在熵编码之前)的长度和熵编码数据的长度之间的差，但是这样做通常不是有利的。相反，为了简化和保持数据量低，将该信息作为实际长度信息传输通常是有益的。仅为了说明的目的，现在描述一个例子，其中图像数据(D1)已经用前述GMVC®编码解决方案编码，并且从整个中间编码数据流中，仅使用用RSA创建的很强的加密密钥对分割/组合信息数据流和编码方法数据流进行加密，以生成编码和加密数据(E2)。RSA是一种众所周知的公钥加密算法。此外，假设在该示例中，对编码和加密数据(E2)进行访问的未经

授权的窃听第三方尝试对加密的数据流以及编码和加密数据(E2)的其它数据流进行解密。此外,假设未授权的第三方知道图像数据(D1)的格式,因为图像数据(D1)是用GMVC®编码解决方案来编码的。因此,未授权的第三方能够解压缩所有其它数据流,其在编码和加密数据(E2)的99/100部分到999/1000部分的范围。然而,未授权的第三方不能对加密的数据流进行解密,因此,不能对编码和加密数据(E2)进行解密。

[0153] 恶意第三方理论上可能尝试以用所有可能的编码方法尝试所有可能的分割/组合的方式对编码和加密数据(E2)进行解密。然而,在这种情况下,试图破解加密并对编码和加密数据(E2)进行解密所需的计算资源量和时间将是相当大的,并且将对密码分析器提出新的挑战。

[0154] 此外,可选地,编码器110可操作成将编码和加密数据(E2)传送到数据服务器和/或数据存储器(图1中未示出)以存储在数据库(图1中未示出)中。数据服务器和/或数据存储器被布置为可由解码器120访问,解码器120有利地与编码器110兼容,用于随后对编码和加密数据(E2)进行解密和解码。

[0155] 此外,可选地,编码器110可操作成将至少一个密钥和/或IV传送到数据服务器和/或数据存储器以存储在数据库中。

[0156] 在一些示例中,解码器120可选地可操作成从数据服务器和/或数据存储器访问编码和加密数据(E2)。另外,可选地,解码器120可操作成从数据服务器和/或数据存储器和/或另一数据服务器访问至少一个密钥和/或IV。

[0157] 在替代示例中,编码器110可选地可操作成经由通信网络或经由直接连接将编码和加密数据(E2)流送到解码器120。此外,应注意,配备有基于硬件的编码器或基于软件的编码器的装置还可以直接与配备有基于硬件的编码器或基于软件的解码器的另一装置通信。虽然本公开的实施方式被描述为利用可操作成执行计算指令的计算硬件,但是可以在专用硬件中实现本公开的实施方式,例如经由专用集成电路(ASIC)和/或经由使用现场可编程门阵列(FPGA)。这样的硬件实现方式是有用的,例如,用于在可能受到电离辐射暴露的装置中实现很鲁棒的加密,例如在诸如卫星的基于空间的设备中。

[0158] 在其它替换示例中,解码器120可选地被实现为从诸如硬盘驱动器和固态驱动器(SSD)之类的非暂时性(即非瞬态)计算机可读存储介质中检索编码和加密数据(E2)。

[0159] 此外,可选地,编码器110的数据处理配置可操作成安排将至少一个密钥从编码器110传输到解码器120,以用于随后对编码和加密数据(E2)的解密和解码。可选地,在相应用户之间手动地将至少一个密钥从编码器110传输到解码器120。或者,可选地,通过加密电子邮件将至少一个密钥从编码器110传输到解码器120,例如,诸如通过使用完美隐私(PGP)、GNU隐私保护(GnuPG)等加密的电子邮件。或者,可选地,通过加密的通信连接将至少一个密钥从编码器110传输到解码器120。可选地,加密通信连接通过安全套接字层(SSL)/传输层安全(TLS)实现。

[0160] 解码器120包括用于处理编码和加密数据(E2)的数据处理配置以生成相应的解密和解码数据(D3)。可选地,解码器120的数据处理配置通过采用至少一个RISC处理器来实现,该RISC处理器可操作成执行将在后面详细阐述的程序指令;这样的RISC处理器能够以很高的速度执行相对更简单的级联操作,并且适合于例如实时地对以流传输格式提供的数据进行解码。以流传输格式提供的这样的数据包括例如视频信息、远程监视视频信息和/或

视频会议信息。

[0161] 可选地，解码器120的数据处理配置可操作成对以下述形式中的至少一种形式提供的编码和加密数据(E2)进行解密和解码：编码和加密的一维数据、编码和加密的多维数据、编码和加密的文本数据、编码和加密的二进制数据、编码和加密的传感器数据、编码和加密的音频数据、编码和加密的图像数据、编码和加密的视频数据，但不限于此。

[0162] 解码器120的数据处理配置可操作成处理编码和加密数据(E2)，以确定一个或多个加密子部分及其一个或多个未加密子部分。编码和加密数据(E2)的一个或多个未加密子部分包括非关键数据流，即被编码的多个数据块和/或数据包的信息。

[0163] 可选地，基于前述第一字节确定加密子部分。或者，可选地，可以基于在包括与加密和所采用的熵编码方法有关的信息的熵编码方法字节和/或熵编码方法字中的前述MSB进行确定。或者，可选地，基于对未加密的数据流和加密的数据流包括在编码和加密数据(E2)中的顺序进行确定。或者，可选地，基于指示哪些数据流包含被编码的信息以及哪些数据流不包含被编码的信息的前述标志位进行确定。

[0164] 可选地，解码器120的数据处理配置在操作中被提供有用于生成解密和解码数据(D3)的至少一个密钥。可选地，使用至少一个密钥，解码器120的数据处理配置可操作成对一个或多个加密子部分进行解密，以确定与多个数据块和/或数据包相关联的尺寸、相对位置和/或一个或多个编码方法。可选地，解码器120的数据处理配置还可操作成确定与多个数据块和/或数据包相关联的一个或多个熵编码方法。

[0165] 可选地，解码器120的数据处理配置可操作成使用与至少一个秘钥组合的至少一个初始化向量(“Init Vector”；IV)来对一个或多个加密子部分进行解密。如前所述，在操作中将至少一个初始化向量提供给解码器120。

[0166] 此外，可选地，以至少一个压缩数据流的形式提供一个或多个加密子部分。在这种情况下，解码器120的数据处理配置可选地可操作成从至少一个压缩数据流的第一字节确定与至少一个压缩数据流相关联的熵编码方法。

[0167] 此外，可选地，在至少一个压缩数据流的开始处，例如在其第一字节之后，提供指示至少一个压缩数据流的长度的信息。因此，解码器120的数据处理通过仅对至少一个压缩数据流的开始进行解密来提供与将要解码的数据量有关的信息，而不必对其进行全部解密。这对于并行处理(即数据流的并行解码)尤其有利。

[0168] 解码器120的数据处理配置然后可选地可操作成应用熵编码方法的逆过程，以解压缩至少一个压缩流，以确定与多个数据块和/或数据包相关联的前述尺寸、前述相对位置和一个或多个编码方法。

[0169] 解码器120的数据处理配置然后可操作成将一个或多个编码方法的逆过程应用于被编码的多个数据块和/或数据包的信息，以对被编码的多个数据块和/或数据包的信息进行解码以生成多个解码的数据块和/或数据包。可选地，解码器120的数据处理配置还可操作成在应用一个或多个编码方法的逆过程之前，将一个或多个熵编码方法的逆过程应用于包括在编码和加密数据(E2)的一个或多个未加密子部分中的多个熵编码数据块和/或数据包。

[0170] 随后，解码器120的数据处理配置可操作成基于尺寸和/或相对位置来组合多个解码数据块和/或数据包，以生成解密和解码数据(D3)。

[0171] 应当理解，指示与多个数据块和/或数据包相关联的前述尺寸、前述相对位置和/或一个或多个编码方法的信息以加密的方式被包括在加密子部分中。因此，对被编码的多个数据块和/或数据包的信息进行解码以生成解密和解码数据(D3)需要对编码和加密数据(E2)的加密子部分进行正确地解密。

[0172] 图1仅仅是示例，其不会不适当地限制本文的权利要求的范围。应当理解，编解码器130的具体设计作为示例提供，并且不应被解释为将编解码器130限制为编码器和解码器的具体数字、类型或布置。本领域技术人员将认识到本公开的实施方式的许多变化、替代和修改。

[0173] 可选地，编解码器130在单个装置内实现。或者，可选地，编解码器130在多个装置之间有效地实现。可选地，编解码器130例如通过使用一个或多个专用集成电路(ASIC)被实现为定制设计数字硬件。或者或另外地，编解码器130在可在计算硬件上执行的计算机软件指令中实现。

[0174] 编解码器130可以实现为数据编解码器、音频编解码器、图像编解码器和/或视频编解码器中的至少一项，但不限于此。

[0175] 此外，编解码器130可以被实现为提供发送方与接收方之间的安全通信，同时显著地节省数据传输所需的网络带宽，并且不需要用于数据传输的加密通信连接，诸如SSL/TLS。在示例中，编解码器130可以在基于请求-响应类型通信的系统中实现，诸如在网站浏览器和万维网(www)服务器中用于数据传输的超文本传输协议(HTTP)。

[0176] 尽管今天加密的数据可能在将来通过使用“暴力攻击(Brute Force Attack)”技术被破解和解密，但是设想未来的加密算法将相应地生成比当前加密算法更强的加密密钥，从而仍然确保数据的强加密。

[0177] 除了“暴力攻击”技术之外，还存在诸如“Biclique攻击”、“相关密钥攻击(Related-Key Attack)”、“Padding Oracle攻击”、“长度扩展攻击(Length Extension Attack)”技术等其它公知的攻击技术，但是这些技术基本上不能破坏由编码器110执行的加密。

[0178] 仅仅为了说明的目的，下面提供了在编码器110内执行的加密过程的技术示例。在该示例中，提出了一个通常有效的模型，用于通过使用对称高级加密标准(AES)加密算法在具有扩展的加密密钥的密码块链接(CBC)模式中执行以下步骤来对未加密的明文数据流进行加密：

[0179] 1.获取或生成两个加密密钥，即Key1和Key2；

[0180] 2.为AES CBC生成加密伪随机初始化向量(IV)字节；

[0181] 3.使用具有Key1和IV的AES CBC函数将明文字节(即，关键数据流中的至少一个关键数据流)加密为密文字节(即，至少一个中间加密数据流)；

[0182] 4.合并IV和密文字节；

[0183] 5.使用具有Key2和密文的HMAC函数创建消息认证码(MAC)字节；以及

[0184] 6.将MAC和密文字节写入数据流，即编码和加密数据(E2)的一个或多个加密子部分。

[0185] 此外，上述算法的伪码如下：

[0186] Key1＝KeyStretch(GetKey())

[0187] Key2＝KeyStretch(GetKey())

[0188] IV＝Random()

[0189] Ciphertext＝IV+AES(Key1,IV,Plaintext)

[0190] MAC＝HMAC(Key2,Ciphertext)

[0191] DATA＝MAC+Ciphertext

[0192] 在上面的示例中，使用“密钥拉伸(Key Stretching)”技术创建了两个加强的密钥。“密钥拉伸”技术通常通过运行用于通过单向摘要算法(即散列算法)加密数千次的密码来实现。这创建了足够多的排列以保护密码免受攻击，例如，密钥相关攻击。

[0193] 此后，为CBC模式创建相应的随机初始化向量(IV)字节。然后将这些IV字节加扰并混合到明文字节的一个或多个第一字节中，即关键数据流中的待加密的至少一个关键数据流。然后使用具有乘法扩展的密钥和IV字节的CBC模式中的对称AES加密算法来对关键数据流中的至少一个关键数据流进行加密。

[0194] 使用IV字节对于提高由此获得的加密的保护程度地目的是特别有利的，例如在关键数据流中的至少一个关键数据流包含大量冗余数据的情况下。因此，在整个信息序列从开始到结束被破坏之前，入侵攻击者不能对关键数据流中的至少一个关键数据流进行解密。

[0195] 最后，消息认证码(MAC)字节被插入到密文字节中，即插入到至少一个中间加密数据流中。这防止了由在关键数据流中的至少一个关键数据流中可能出现的冗余明文引起的可能相同的密文，并且还防止加密被通过例如“Padding Oracle攻击”技术被破解。这还确保了编码和加密数据(E2)的一个或多个加密子部分的完整性是完整的。

[0196] 现在参考图2，提供了描述根据本公开的实施方式的对输入数据(D1)进行编码和加密以生成相应的编码和加密数据(E2)的第一方法的步骤的流程图。该方法被描述为逻辑流程图中的步骤的集合，其表示可以在硬件、软件或其组合(例如，如上所述)中实现的步骤序列。

[0197] 仅出于说明的目的，接下来将参考图1中所描绘的编码器110来说明第一方法。

[0198] 在步骤202，编码器110的数据处理配置对输入数据(D1)进行编码，从而生成多个中间编码数据流。

[0199] 可选地，步骤202包括这样的子步骤，在该子步骤处编码器110的数据处理配置采用多个分割操作和/或组合操作来将输入数据(D1)划分和/组合成多个数据块和/或数据包，并且采用一个或多个编码方法将该多个数据块和/或数据包的信息编码到该多个中间编码数据流中的至少一个中间编码数据流中。

[0200] 可选地，步骤202包括这样的子步骤，在该子步骤处编码器110的数据处理配置采用一个或多个熵编码方法将多个数据块和/或数据包压缩成多个熵编码数据块和/或数据包，其中指示熵编码方法的信息或熵编码方法的实现与熵编码数据的长度以及(可选地)原始数据的长度一起被包括在多个中间编码数据流中的至少一个中间编码数据流中；指示熵编码方法的信息或熵编码方法的实现以及长度信息有利地包括在它们自己的中间数据流中。这样的熵编码可选地在使用上述编码方法对一个或多个数据块和/或数据包进行编码之后执行。可选地，在该阶段，所生成的中间编码数据流可以在被加密之前被进一步压缩。接下来，在步骤204，编码器110的数据处理配置使用一个或多个加密算法对多个中间编码

数据流中的至少一个关键数据流进行加密，以生成至少一个中间加密数据流。可选地，该至少一个关键数据流包括指示以下各项中的至少一项的信息：多个分割操作和/或组合操作、一个或多个编码方法、一个或多个熵编码方法和/多个熵编码数据块和/或数据包的长度，和/或在应用熵编码之前的数据块和/或包的长度。

[0201] 可选地，在步骤204，编码器110的数据处理配置在对至少一个关键数据流进行加密时结合至少一个密钥应用至少一个初始化向量(“Init Vector”;IV)。

[0202] 结合图3描述了步骤204的加密过程。

[0203] 随后，在步骤206，编码器110的数据处理配置将多个中间编码数据流的未加密部分(即被编码的多个数据块和/或数据包的信息)与至少一个中间加密数据流合并在一起以生成编码和加密数据(E2)。

[0204] 步骤202至步骤206仅是说明性的，并且在不脱离本文权利要求的范围的情况下还可以提供其它替代方案，其中添加一个或多个步骤、移除一个或多个步骤，或者以不同顺序提供一个或多个步骤。例如，可选地，该方法包括这样的附加步骤，其中编码器110的数据处理配置在加密之前将至少一个关键数据流压缩为至少一个压缩数据流。可选地，在附加步骤中，编码器110的数据处理配置计算至少一个压缩数据流的第一字节，使得第一字节描述用于压缩至少一个关键数据流的熵编码方法。

[0205] 此外，可选地，使用对称AES加密算法的CBC模式来执行步骤204。可选地，使用与至少一个密钥合并的随机生成的IV来执行步骤204。应当理解，可以使用其它加密算法来执行步骤204，而不管IV是否用于对至少一个关键数据流进行加密，并且不管是否使用CBC模式。

[0206] 或者，可选地，输入数据(D1)已经被编码。在这种情况下，该方法开始于这样的替代步骤，其中至少一个关键数据流被识别然后加密。可选地，通过逐个流处理输入数据(D1)并识别其中的一个或多个关键数据流来执行这种识别。当输入数据(D1)的每个数据流包括所采用的编码方法的信息以及该数据流的长度时，该过程是快速和高效的。

[0207] 图3是根据本公开的实施方式的加密过程的步骤的示意图。

[0208] 在步骤302，编码器110的数据处理配置读取或接收多个中间编码数据流的内容。

[0209] 在步骤304，编码器110的数据处理配置处理多个中间编码数据流的第一数据流或下一数据流。

[0210] 在步骤306，编码器110的数据处理配置确定在步骤304处理的第一数据流或下一数据流是否需要被加密。

[0211] 如果在步骤306确定需要对第一数据流或下一数据流进行加密，则执行步骤308。否则，如果确定不需要对第一数据流或下一数据流进行加密，则执行步骤310。

[0212] 在步骤308，编码器110的数据处理配置对第一数据流或下一数据流进行加密。根据步骤308，编码器110的数据处理配置可选地写入或发送加密信息，即指示在步骤308处采用的一个或多个加密算法的信息。

[0213] 此后，在步骤310，编码器110的数据处理配置写入或发送加密数据流以包括在编码和加密数据(E2)中。

[0214] 当第一数据流或下一数据流未被加密时，编码器110的数据处理配置在步骤310处原样地写入或发送第一数据流或下一数据流。

[0215] 接下来，在步骤312，编码器110的数据处理配置确定输入数据(D1)中是否存在下

一数据流。如果确定存在下一数据流，则加密过程在步骤302重新开始。否则，如果确定输入数据(D1)中不存在下一数据流，则加密过程结束。

[0216] 步骤302至步骤312仅是说明性的，并且在不脱离本文权利要求的范围的情况下还可以提供其它替代方案，其中添加一个或多个步骤、移除一个或多个步骤，或者以不同顺序提供一个或多个步骤。

[0217] 本公开的实施方式提供了计算机程序产品，其包括存储有计算机可读指令的非暂时性(即非瞬态)计算机可读存储介质，该计算机可读指令可由包括处理硬件的计算装置执行以执行结合图2和图3描述的第一方法。计算机可读指令可选地可从软件应用商店下载，例如从“App Store”下载到计算装置。

[0218] 图4是描述根据本公开的实施方式的对编码和加密数据(E2)进行解密和解码以生成相应的解密和解码数据(D3)的第二方法的步骤的流程图的示意图。该方法被描述为逻辑流程图中的步骤的集合，其表示可以在硬件、软件或其组合中实现的步骤序列。

[0219] 仅出于说明的目的，接下来将参考图1中所描绘的解码器120来说明第二方法。

[0220] 在步骤402，解码器120的数据处理配置处理编码和加密数据(E2)以确定一个或多个加密子部分及一个或多个未加密子部分。编码和加密数据(E2)的一个或多个未加密子部分包括非关键数据流，即被编码的多个数据块和/或数据包的信息。

[0221] 在步骤404，解码器120的数据处理配置对编码和加密数据(E2)的一个或多个加密子部分进行解密，以确定与多个数据块和/或数据包相关联的尺寸、相对位置和/或一个或多个编码方法。可选地，在步骤404，解码器120的数据处理配置还确定与多个数据块和/或数据包相关联的一个或多个熵编码方法。

[0222] 可选地，在步骤404，解码器120的数据处理配置使用至少一个初始化向量(“Init Vector”;IV)以及至少一个密钥对一个或多个加密子部分进行解密。

[0223] 可选地，在操作中将至少一个密钥和/或至少一个初始化向量提供给解码器120。

[0224] 结合图5描述了步骤404的解密过程。

[0225] 接下来，在步骤406，解码器120的数据处理配置将在步骤404确定的一个或多个编码方法的逆过程应用于被编码的多个数据块和/或数据包的信息，以对被编码的多个数据块和/或数据包的信息进行解码，从而生成多个解码的数据块和/或数据包。可选地，在步骤406，解码器120的数据处理配置还提取应用的熵编码方法的信息以及熵编码的数据块和/或包的长度信息，并且在应用一个或多个编码方法的逆过程之前，将一个或多个熵编码方法的逆过程应用于包括在编码和加密数据(E2)的一个或多个未加密子部分中的多个熵编码的数据块和/或数据包。在中间编码数据流在采用加密之前被进一步压缩的情况下，解码器120应用一个或多个相应的逆过程数据解压缩方法。

[0226] 随后，在步骤408，解码器120的数据处理配置基于在步骤404确定的尺寸和/或相对位置组合多个解码数据块和/或数据包，以生成解密和解码数据(D3)。

[0227] 步骤402至步骤408仅是说明性的，并且在不脱离本文权利要求的范围的情况下还可以提供其它替代方案，其中添加一个或多个步骤、移除一个或多个步骤，或者以不同顺序提供一个或多个步骤。例如，可选地，该方法包括这样的附加步骤，在该附加步骤，解码器120的数据处理配置从一个或多个加密子部分的至少一个压缩数据流的第一字节确定与至少一个压缩数据流相关联的熵编码方法。可选地，在附加步骤中，解码器120的数据处理配

置将熵编码方法的逆过程应用于解压缩至少一个压缩流以确定与多个数据块和/或数据包相关联的尺寸、相对位置和一个或多个编码方法。

[0228] 此外，可选地，使用对称AES加密算法的CBC模式来执行步骤404。可选地，使用与至少一个密钥合并的随机生成的IV来执行步骤404。应当理解，可以使用其它解密算法来执行步骤404，而不管IV是否用于对一个或多个加密子部分进行解密，并且不管是否使用CBC模式。

[0229] 图5是根据本公开的实施方式的解密过程的步骤的示意图。

[0230] 在步骤502，解码器120的数据处理配置读取或接收编码和加密数据(E2)的内容。

[0231] 在步骤504，解码器120的数据处理配置处理包括在编码和加密数据(E2)内的第一数据流或下一数据流。

[0232] 在步骤506，解码器120的数据处理配置确定第一数据流或下一数据流是否被加密。可选地，在步骤506，基于以下各项中的至少一项进行确定：前述第一字节、在熵编码方法字节和/或熵编码方法字中的最高有效位(MSB)、未加密数据流和加密数据流的顺序，和/或前述标志位。

[0233] 如果在步骤506确定第一数据流或下一数据流被加密，则执行步骤508。否则，如果确定第一数据流或下一数据流未加密，则执行步骤510。

[0234] 在步骤508，解码器120的数据处理配置对第一数据流或下一数据流进行解密。根据步骤508，解码器120的数据处理配置可选地读取或接收加密信息，即指示与第一数据流或下一数据流相关联的一个或多个加密算法的信息。

[0235] 此后，在步骤510，解码器120的数据处理配置写入或发送解密的数据流。

[0236] 当第一数据流或下一数据流未加密时，解码器120的数据处理配置在步骤510处原样地写入或发送第一数据流或下一数据流。

[0237] 接下来，在步骤512，解码器120的数据处理配置确定在编码和加密数据(E2)中是否存在下一个数据流。如果确定存在下一数据流，则解密过程在步骤502重新开始。否则，如果确定在编码和加密数据(E2)中不存在下一数据流，则解密过程结束。

[0238] 步骤502至512仅是说明性的，并且在不脱离本文权利要求的范围的情况下还可以提供其它替代方案，其中添加一个或多个步骤、移除一个或多个步骤，或者以不同顺序提供一个或多个步骤。

[0239] 本公开的实施方式提供了计算机程序产品，其包括存储有计算机可读指令的非暂时性(即非瞬态)计算机可读存储介质，该计算机可读指令可由包括处理硬件的计算装置执行以执行结合图4和图5描述的第二方法。计算机可读指令可选地可从软件应用商店下载，例如从“App Store”下载到计算装置。

[0240] 前述加密方法和加密过程适合于实现到编码器或另一相应的预处理器中。类似地，上述解密方法和解密过程适合于实现到解码器或另一相应的预处理器中。上述方法可以在软件中实现和/或通过使用硬件逻辑(例如ASIC)来实现。众所周知，许多系统具有用于加密的专用微芯片，例如当前的AES，其高效地实现加密，同时比纯软件方法使用更少的电力。与使用具有对抗第三方攻击的相应强度的加密(例如对抗监视组织)的现有技术方法相比，前述方法可以实现相当大的电力和能量节省。

[0241] 在根据本公开的实施方式的加密方法作为软件实现执行的情况下，有益的是完全

或部分地在受保护的存储器空间中执行该软件处理。这样的预防有助于尝试防止可能的恶意软件读取待加密的信息或在加密过程中使用的加密密钥。相应地，在这种情况下，解密有利地也在受保护的存储器空间中执行。即使许多当前的装置包括用于加密的专用微芯片，或者存在可用于加密的单独指令集，如在前述AES中，仍然有益的是，根据本公开的加密解决方案确保加密的明文数据完全在受保护的存储器空间中或在部分受保护的存储器空间中处理；在后一种情况下，如果例如所使用的加密密钥在受保护的存储器空间中被处理，则可以在受保护的存储器空间外部处理待加密的明文数据。最有益的是，总是仅在受保护的存储器中存在未加密的形式的明文信息。然而，如果这不可能，则有利的是确保在加密之后不会在未受保护的存储器中就此结束。例如，有益的是，根据本公开的实施方式加密的数据的部分总是仅存储在受保护的存储器中。存储器保护是可以在大多数操作系统(例如现有的操作系统)中实现的一种保护，但是技术和访问机制可能有所不同。

[0242] 根据本公开的实施方式的方法可以利用任何合适的编码解决方案来实现，而不管使用哪种加密算法。在这种情况下，前述方法不改变加密算法的行为，这意味着由加密算法提供的保护不会受到妥协。

[0243] 前述方法使得可以使用很快速高效的加密算法。在这点上，前述方法高效地使用加密算法，而不干扰加密算法本身的内部操作。适合于用前述方法实现的加密算法的示例包括但不限于AES、RSA、Twofish、Blowfish、数据加密标准(DES)、三重DES(3-DES)、Serpent、国际数据加密算法(IDEA)、MARS、Rivest Cipher 6(RC6)、Camellia、CAST-128、Skipjack、扩展微型加密算法(XTEA)等，这些示例名称包括注册商标。

[0244] 根据本公开的实施方式的前述方法提供了与已知的现有技术方法相比很快速并且相当高效的保护数据的方式。值得注意的是，仅对编码数据的一个或多个必要和关键部分进行加密。例如，当使用渐进式GMVC®编码解决方案对图像或视频进行编码时，如先前所阐述的，通常只有整个编码数据的1/100部分至1/1000部分被加密保护。因此，可以得出结论，以这种方式使用加密对实时视频的传输速率没有任何显著影响，也不以任何显著的方式增加计算资源的消耗。

[0245] 此外，该加密过程的附加优点是，编码和加密数据(E2)不需要通过具有受保护的安全网络连接的网络(例如采用虚拟专用网络(VPN)隧道、安全壳(SSH)或SSL/TLS协议)来传输。因此，前述方法提供了用于例如在公共互联网网络中或在网站服务和云服务中传输文本、二进制、音频、图像、视频和其它类型的数据的有利模型。

[0246] 本公开的实施方式易于在很大范围的系统和装置中使用，例如智能电话、个人计算机(PC)、视听设备、照相机、通信网络、数据存储装置、监视系统、视频会议系统、医疗设备、地震设备、测量设备、“黑盒子”飞行记录器、使用采样技术的数字乐器，但不限于此。

[0247] 在不脱离由所附权利要求限定的本发明的范围的情况下，可以对前述的本发明的实施方式进行修改。用于描述本发明和对本发明要求保护的诸如“包含”、“包括”、“含有”、“涵盖”、“具有”、“是”的表述旨在以非排他性的方式解释，即允许未明确描述的项目、组件或元件的存在。对单数形式的引述也应解释为涉及复数形式。所附权利要求中括号内所包括的数字旨在帮助理解权利要求，而不应以任何方式解释为限制这些权利要求所要求保护的主题。

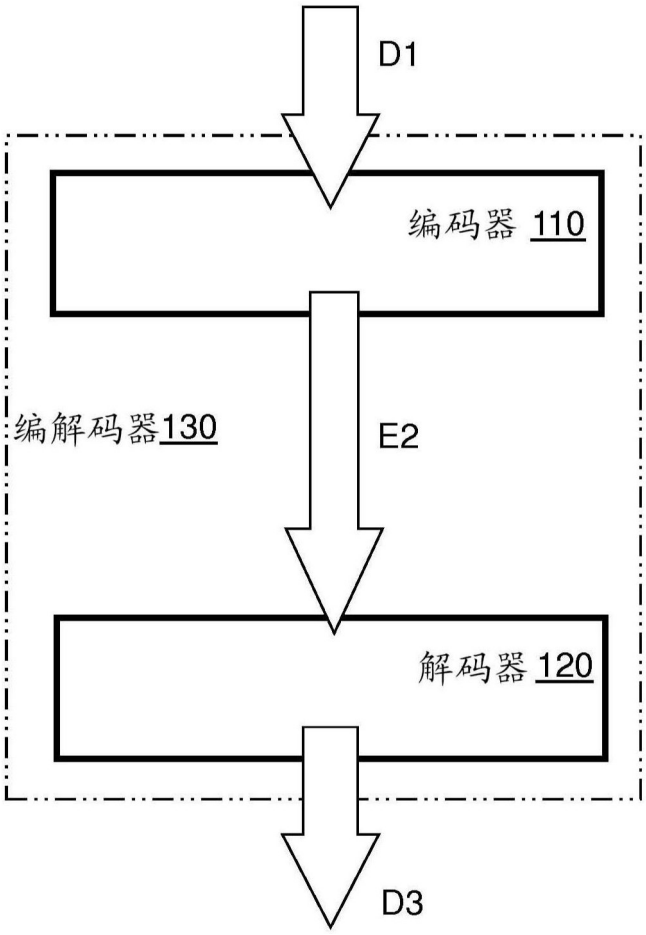


图1

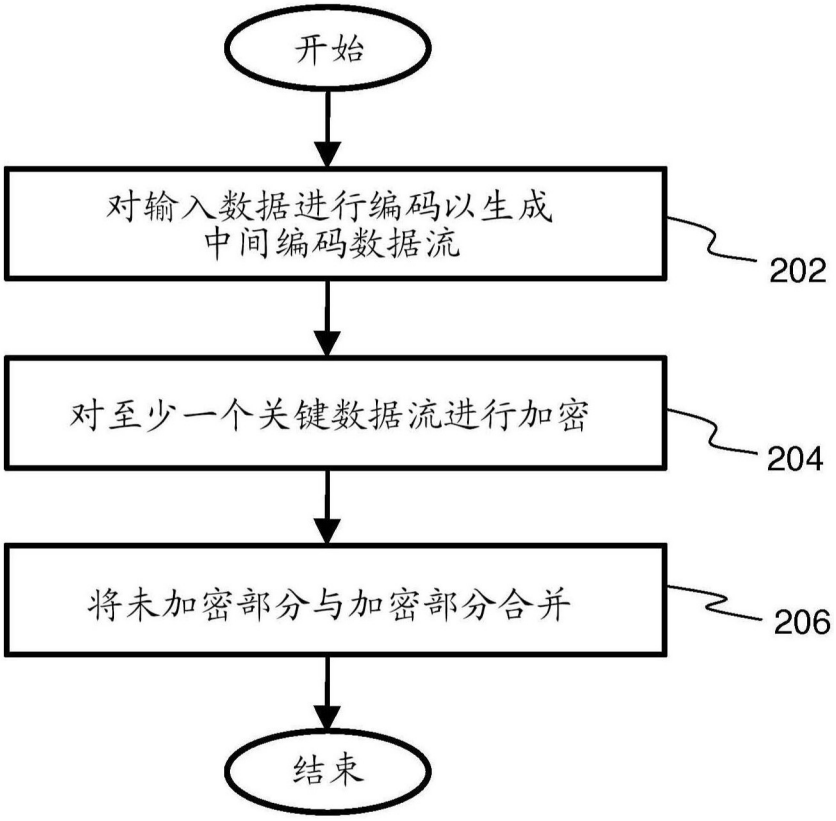

开始
对输入数据进行编码以生成
中间编码数据流
202
对至少一个关键数据流进行加密
204
将未加密部分与加密部分合并
206
结束

图2

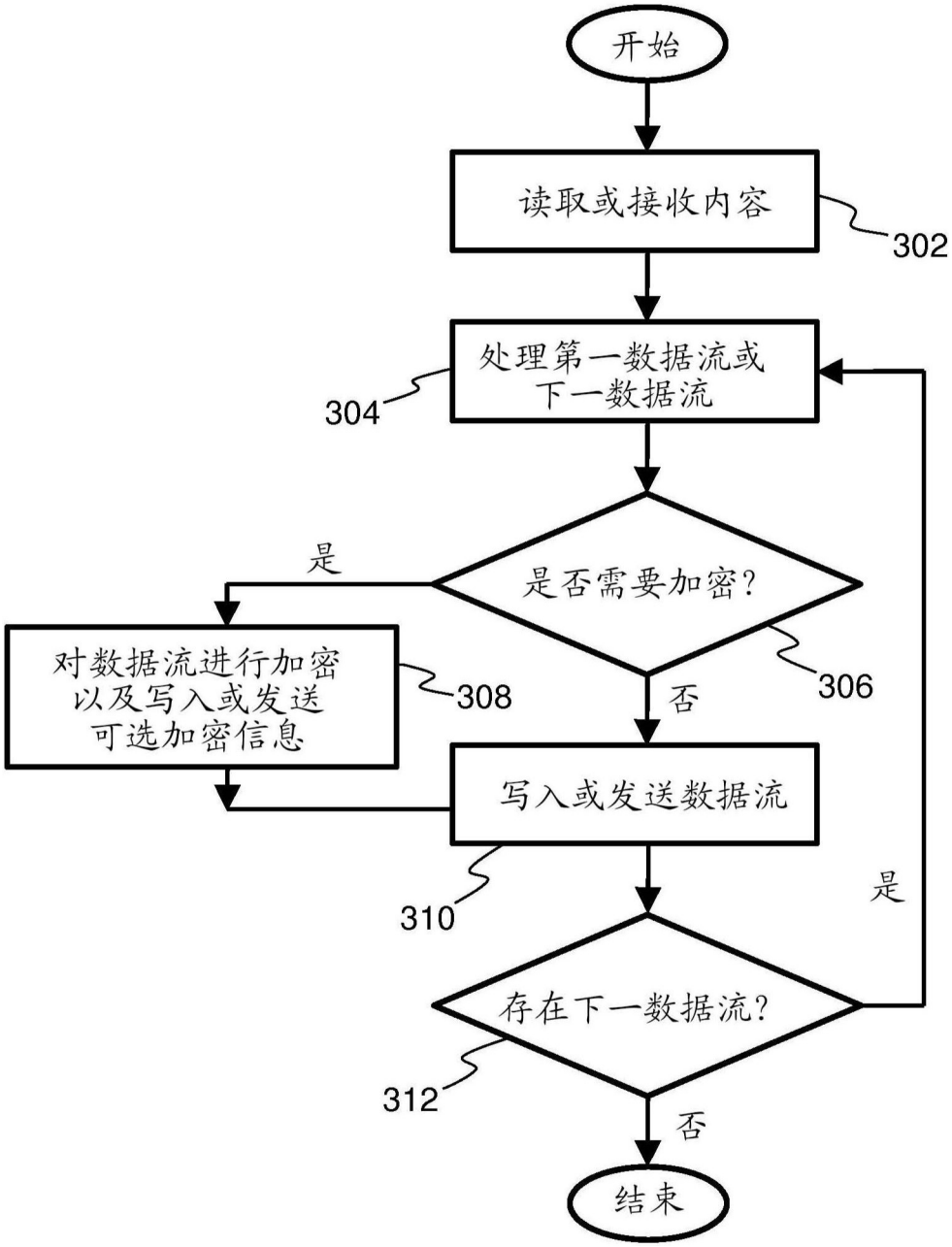

开始
读取或接收内容
302
处理第一数据流或
下一数据流
304
是否需要加密?
306
是
否
对数据流进行加密
以及写入或发送
可选加密信息
308
写入或发送数据流
310
存在下一数据流?
312
是
否
结束

图3

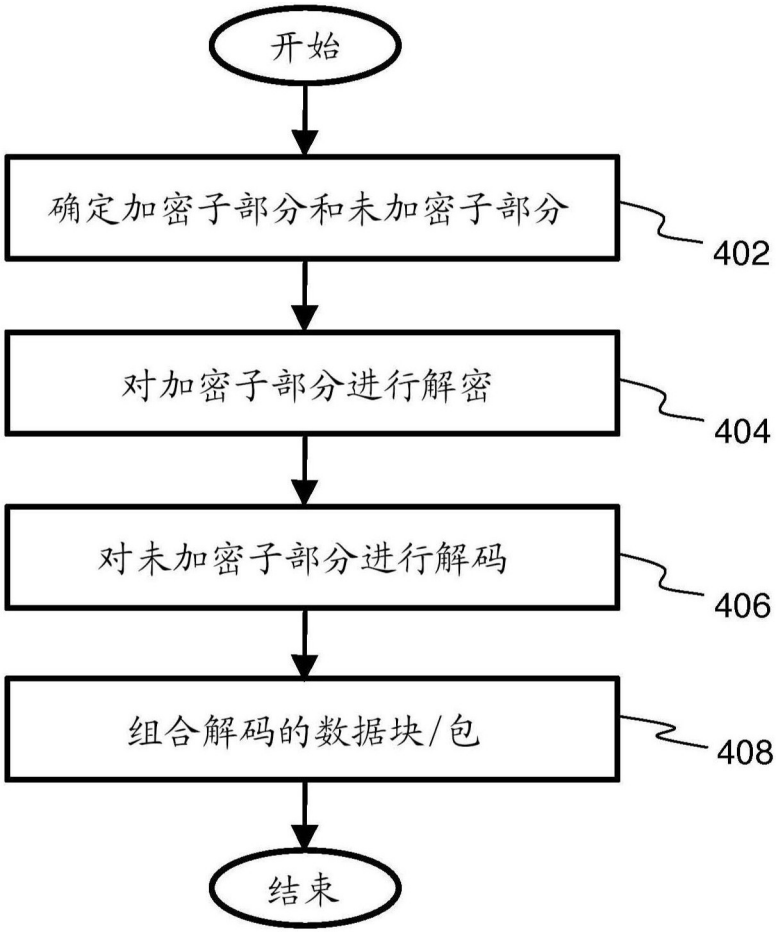

开始
确定加密子部分和未加密子部分
402
对加密子部分进行解密
404
对未加密子部分进行解码
406
组合解码的数据块/包
408
结束

图4

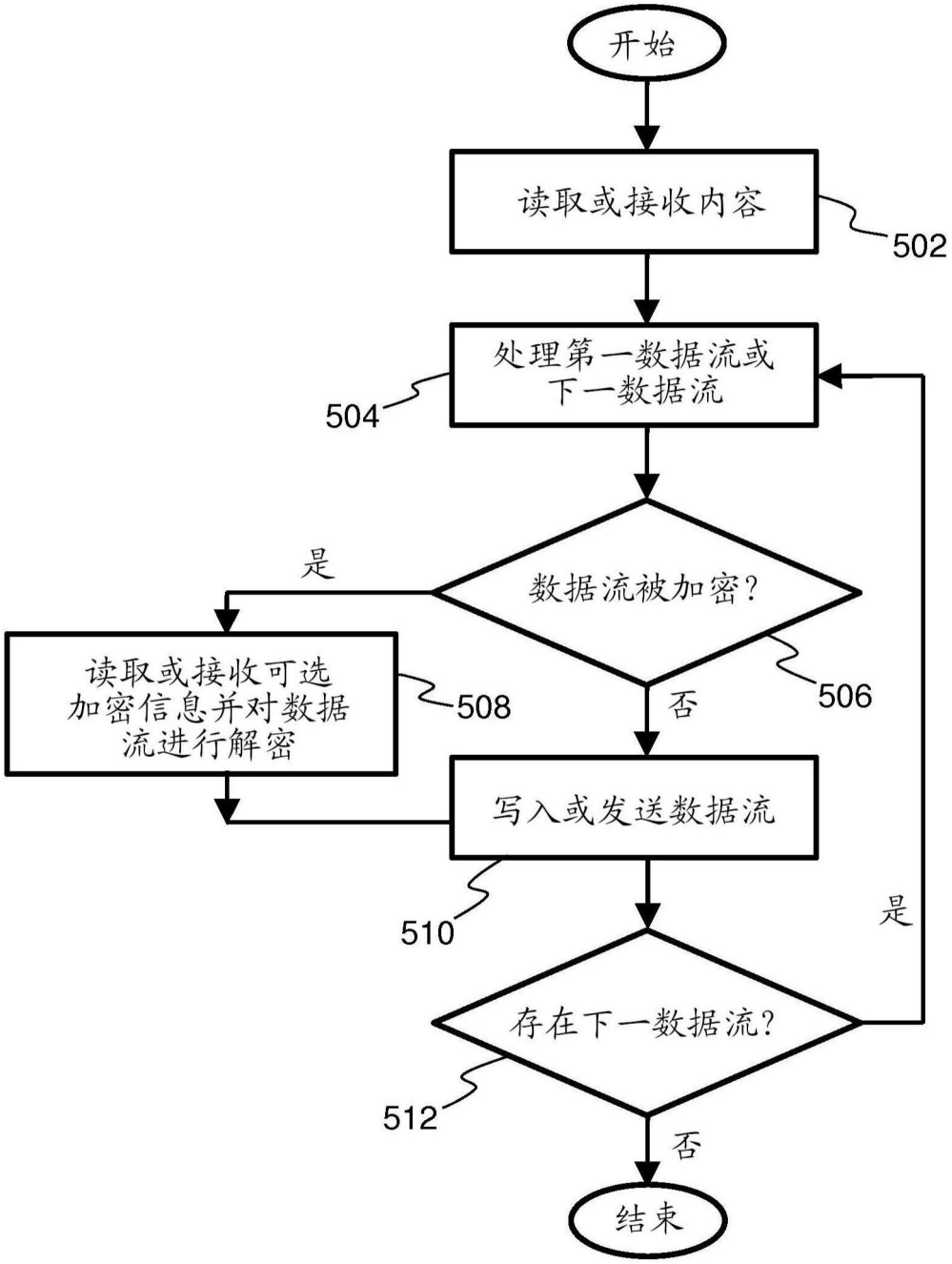

开始
读取或接收内容
502
处理第一数据流或下一数据流
504
数据流被加密？
506
是
否
读取或接收可选加密信息并对数据流进行解密
508
写入或发送数据流
510
存在下一数据流？
512
是
否
结束

图5