(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 108174207 A
(43)申请公布日 2018.06.15

(21)申请号 201711478565.0

(22)申请日 2017.12.29

(71)申请人 重庆邮电大学
地址 400065 重庆市南岸区黄桷垭崇文路2号

(72)发明人 曾浩 纪磊

(74)专利代理机构 北京同恒源知识产权代理有限公司 11275
代理人 赵荣之

(51)Int.Cl.
H04N 19/13(2014.01)
H04N 19/91(2014.01)
H04N 19/46(2014.01)
H04N 21/2347(2011.01)
H04N 21/4408(2011.01)
H04L 9/00(2006.01)

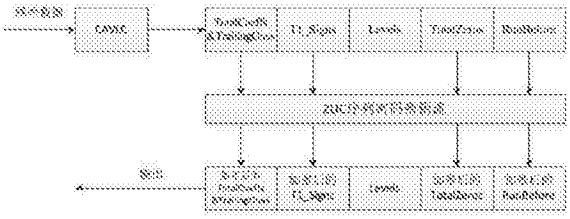
权利要求书1页 说明书4页 附图1页

(54)发明名称

基于ZUC算法的H.264熵编码视频加密方法

(57)摘要

本发明涉及一种基于ZUC算法的H.264熵编码视频加密方法，属于移动通信技术领域。该方法为：在H.264视频压缩编码的CAVLC编码过程中，采用ZUC算法生成随机密钥流，与非零系数个数、拖尾系数个数、拖尾系数符号、最后一个非零系数前零的个数、每个非零系数前零的个数编码后的码流相异或，得到新的码流，然后与其余非零系数幅值编码后的码流合并输出，实现加密；本发明增加了加密参数的数量，提高了安全性；与索引得到的明文相异或，复杂度低，并未增加太多的开销；采用ZUC算法，运算速度快，易于实现，性能上可以替代现有加密方法中所用的国外加密算法，实现了加密算法的国产化。



CN 108174207 A

1.基于ZUC算法的H.264熵编码视频加密方法，其特征在于：该方法为：在H.264视频压缩编码的CAVLC编码过程中，采用ZUC算法生成随机密钥流，与非零系数个数、拖尾系数个数、拖尾系数符号、最后一个非零系数前零的个数、每个非零系数前零的个数编码后的码流相异或，得到新的码流，然后与其余非零系数幅值编码后的码流合并输出，实现加密；

具体步骤为：

S1：在H.264视频压缩编码的CAVLC编码过程中，对参数进行编码，得到原码流；

S2：根据ZUC序列密码算法产生密钥流并分发；

S3：利用密钥流加密重要参数编码后的原码流，得到密文码流；

S4：将密文码流与未进行加密的原码流合并、输出。

2.根据权利要求1所述的基于ZUC算法的H.264熵编码视频加密方法，其特征在于：所述对参数进行编码包括对非零系数个数Total Coeffs编码、对拖尾系数个数Trailing Ones编码、对拖尾系数符号T1_Signs编码、对其余非零系数幅值Levels编码、对最后一个非零系数前零的个数Total Zeros编码和对每个非零系数前零的个数Run Before编码。

3.根据权利要求1所述的基于ZUC算法的H.264熵编码视频加密方法，其特征在于：所述重要参数编码后的原码流包括非零系数个数、拖尾系数个数、拖尾系数符号、最后一个非零系数前零的个数和每个非零系数前零的个数五个参数编码后的码流。

4.根据权利要求1所述的基于ZUC算法的H.264熵编码视频加密方法，其特征在于：所述未进行加密的原码流为其余非零系数幅值编码后的码流。

基于ZUC算法的H.264熵编码视频加密方法

技术领域

[0001] 本发明属于移动通信技术领域，涉及基于ZUC算法的H.264熵编码视频加密方法。

背景技术

[0002] ①H.264是新一代视频编码标准，它着重于解决压缩的高效率和传输的高可靠性，其优异的压缩性能及良好的网络性能使其在视频实时通信、网络流媒体等各个领域广泛应用。熵编码是无损压缩编码方法，普遍应用于H.264及其他视频压缩标准。②对熵编码加密方法已有一定的研究。Wen等人提出了直接置乱编码码表或加密码字序号的加密方法。Tosun和Feng提出了基于前向纠错编码的加密方法。李晓举等提出基于CAVLC熵编码的可分级视频加密方案，提高了加密算法的灵活性。

[0003] ③目前，对H.264熵编码进行加密的构想已经有了一定的研究与实现，主要可分为加密码字索引和直接加密明文。对于加密码字索引，要对加密后的索引号是否落在有效区域进行判断，增大了计算开销；对于加密明文，现有的加密方案较少，不同方案间的差异多为加密算法的变更，且加密算法多为国外加密算法，尚无国密算法应用于H.264熵编码加密过程的研究。

[0004] ④H.264熵编码采用CAVLC方法，根据CAVLC编码特点和国密算法中的ZUC算法，设计一种新的基于ZUC算法的H.264熵编码视频加密方法是本发明要解决的技术问题。

[0005] 图1为H.264视频压缩编码流程图。

[0006] H.264熵编码提供了两种编码方法，分别为基于上下文自适应的可变长编码(CAVLC)和基于上下文自适应的二进制算术编码(CABAC)。其中，CAVLC易于实现，计算简单，主要应用于视频会议、可视电话和无线通信等对实时性要求高的通信中，H.264编解码标准的四个档次均包含此编码方法。CABAC具有很高的编码效率，但编码过程复杂，主要应用于多媒体数字通信。本发明仅针对应用广泛的CAVLC进行研究，而较为复杂的CABAC暂不考虑。

[0007] H.264视频压缩编码中，CAVLC编码过程中的参数有六个，为非零系数个数、拖尾系数个数、拖尾系数符号、其余非零系数幅值、最后一个非零系数前零的个数、每个非零系数前零的个数。每个参数都有相关编码码表，根据编码索引查表输出码流。

发明内容

[0008] 有鉴于此，本发明的目的在于提供一种基于ZUC算法的H.264熵编码视频加密方法，将对非零系数个数、拖尾系数个数、拖尾系数符号、最后一个非零系数前零的个数、每个非零系数前零的个数五个参数进行加密，其余非零系数幅值的编码涉及前缀编码和后缀编码，有一定的复杂度，所以不对此部分进行加密。

[0009] 为达到上述目的，本发明提供如下技术方案：

[0010] 基于ZUC算法的H.264熵编码视频加密方法，该方法为：在H.264视频压缩编码的CAVLC编码过程中，采用ZUC算法生成随机密钥流，与非零系数个数、拖尾系数个数、拖尾系数符号、最后一个非零系数前零的个数、每个非零系数前零的个数编码后的码流相异或，得

到新的码流，然后与其余非零系数幅值编码后的码流合并输出，实现加密；

[0011] 具体步骤为：

[0012] S1：在H.264视频压缩编码的CAVLC编码过程中，对参数进行编码，得到原码流；

[0013] S2：根据ZUC序列密码算法产生密钥流并分发；

[0014] S3：利用密钥流加密重要参数编码后的原码流，得到密文码流；

[0015] S4：将密文码流与未进行加密的原码流合并、输出。

[0016] 进一步，所述对参数进行编码包括对非零系数个数Total Coeffs编码、对拖尾系数个数Trailing Ones编码、对拖尾系数符号T1_Signs编码、对其余非零系数幅值Levels编码、对最后一个非零系数前零的个数Total Zeros编码和对每个非零系数前零的个数Run Before编码。

[0017] 进一步，所述重要参数编码后的原码流包括非零系数个数、拖尾系数个数、拖尾系数符号、最后一个非零系数前零的个数和每个非零系数前零的个数五个参数编码后的码流。

[0018] 进一步，所述未进行加密的原码流为其余非零系数幅值编码后的码流。

[0019] 本发明的有益效果在于：本发明是一种针对CAVLC方法，基于ZUC算法的H.264熵编码视频加密方法。在H.264压缩编码的CAVLC过程中，采用ZUC算法产生密钥流，与非零系数个数、拖尾系数个数、拖尾系数符号、最后一个非零系数前零的个数、每个非零系数前零的个数编码后的码流相异或得到新的码流，然后与其余非零系数幅值编码后的码流合并输出，实现加密。

[0020] (1)与现有加密方法相比，本发明增加了加密参数的数量，提高了安全性；与索引得到的明文相异或，复杂度低，并未增加太多的开销；采用ZUC算法，运算速度快，易于实现，性能上可以替代现有加密方法中所用的国外加密算法，实现了加密算法的国产化。

[0021] (2)在安全性方面，本发明加密了非零系数个数、拖尾系数个数、拖尾系数符号、最后一个非零系数前零的个数、每个非零系数前零的个数。这些参数主要集中在低频位置，在块中占有极大的比重，且没有明显统计特征，不容易被破译。相较于现有方案中只加密拖尾系数符号、其余非零系数幅值、每个非零系数前零的个数，增大了加密数据量大，提高了安全性。ZUC算法在逻辑上采用三层结构设计，极大地增强了抗攻击的能力，安全性高。

[0022] (3)在复杂度方面，相较于加密码字索引的方法，本发明采用密钥流直接加密明文的方法，码流与密钥流逐位异或，省去了对加密后的索引号是否落在有效区域进行判断的时间，操作简单，对整个编码过程所需的时间影响很小，复杂度主要由序列密码所决定。而ZUC算法每次产生的密钥流为32bit，运算速度快，密钥流生成和分发所需的时间少。所以本方法的计算开销很小。

[0023] (4)在加密算法的选择方面，ZUC算法由我国自主研发，结构简单，易于软硬件实现，加解密速度快。同时因ZUC在结构上采用的一些特殊设计，提高了它的抗攻击能力，具有可靠的高安全性能和低复杂度，目前已被批准为第4代移动通信加密标准。因此采用ZUC算法对视频图像进行加密，既可以很好地保证安全性，又能实现加密算法的国产化，进一步推动我国密码算法的发展和应用。

附图说明

[0024] 为了使本发明的目的、技术方案和有益效果更加清楚，本发明提供如下附图进行说明：

[0025] 图1为H.264视频压缩编码流程图；

[0026] 图2为CAVLC编码流程图；

[0027] 图3为本发明加密流程图。

具体实施方式

[0028] 下面将结合附图，对本发明的优选实施例进行详细的描述。

[0029] H.264视频压缩编码的过程如图1所示，视频经过帧内和帧间预测、变换、量化、熵编码实现压缩编码。图2为CAVLC编码流程图；图3为本发明加密流程图。

[0030] H.264的CAVLC编码过程主要为：(1)对非零系数个数(TotalCoeffs)和拖尾系数个数(TrailingOnes)进行编码；(2)对拖尾系数符号(T1_Signs)进行编码；(3)对其余非零系数幅值(Levels)进行编码；(4)对最后一个非零系数前零的个数(TotalZeros)进行编码；(5)对每个非零系数前零的个数(RunBefore)进行编码。

[0031] 在H.264视频压缩编码的CAVLC编码过程中，采用ZUC算法生成随机密钥流，与非零系数个数、拖尾系数个数、拖尾系数符号、最后一个非零系数前零的个数、每个非零系数前零的个数编码后的码流相异或，得到新的码流，然后与其余非零系数幅值编码后的码流合并输出，实现加密。

[0032] 在步骤2中，ZUC序列密码算法产生密钥流，主要可分为三个步骤：初始密钥的加载，初始化阶段和工作阶段。主要处理为初始秘钥的加载，在128bit种子密钥和128bit初始向量的控制下，可产生32bit的密钥流。

[0033] 将上述产生的密钥流分发入需要加密的码流中，用密钥流与码流进行异或操作，实现加密。

[0034] 结合实例对本加密方法进行说明：

[0035] 假设4*4块数据为：

[0036]

0	0	-1	0
5	2	0	0
3	0	0	0
1	0	0	0

[0037] 经过数据重排序，Zigzag扫描系数输入为：0,0,5,3,2,-1,0,0,0,1,……

[0038] 经过编码得到CAVLC编码输出的的码流：000010110001001010101010111。设加密本块数据的密钥流为0,0,1,1,,1,0,0,1,……

[0039] 加密过程：

[0040]

编码参数	原码流	密钥流	加密后的密文码流
TotalCoeffs& TrailingOnes	0000101	0	0000101
T1_Signs	1	0	1
	0	1	0
Levels	001	不加密	001
	0010	不加密	0010
TotalZeros	101	1	010
RunBefore	010	1	101
	1	0	1
	1	0	1
	1	1	0
	Last_RunBefore		

[0041] 由加密过程可见，对非零系数个数(TotalCoeffs)和拖尾系数个数(TrailingOnes)、拖尾系数符号(T1_Signs)、最后一个非零系数前零的个数(TotalZeros)、每个非零系数前零的个数(RunBefore)编码后的原码流进行异或操作，得到密文码流，与其余非零系数幅值(Levels)编码后的码流合并输出，实现加密。最终的密文码流为00001011000100100101011110。

[0042] 最后说明的是，以上优选实施例仅用以说明本发明的技术方案而非限制，尽管通过上述优选实施例已经对本发明进行了详细的描述，但本领域技术人员应当理解，可以在形式上和细节上对其作出各种各样的改变，而不偏离本发明权利要求书所限定的范围。

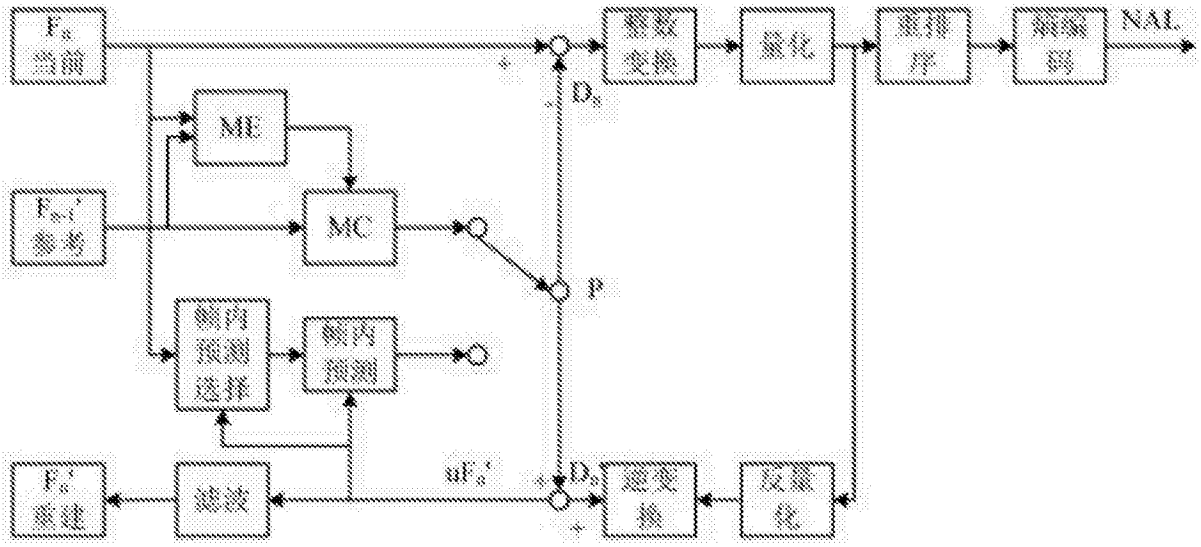

ME
MC
P
NAL

图1

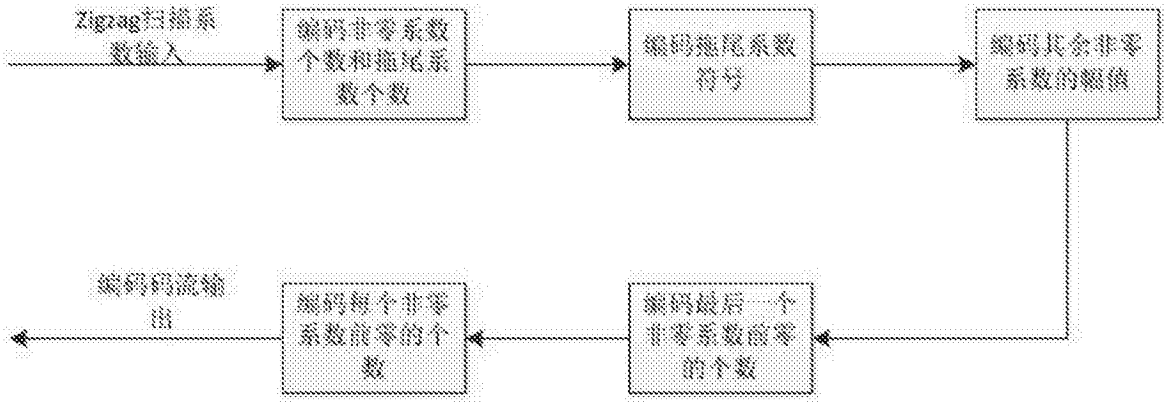

Zigzag扫描系数输入
编码非零系数个数和拖尾系数个数
编码拖尾系数符号
编码其余非零系数的幅值
编码每个非零系数前零的个数
编码最后一个非零系数前零的个数

图2

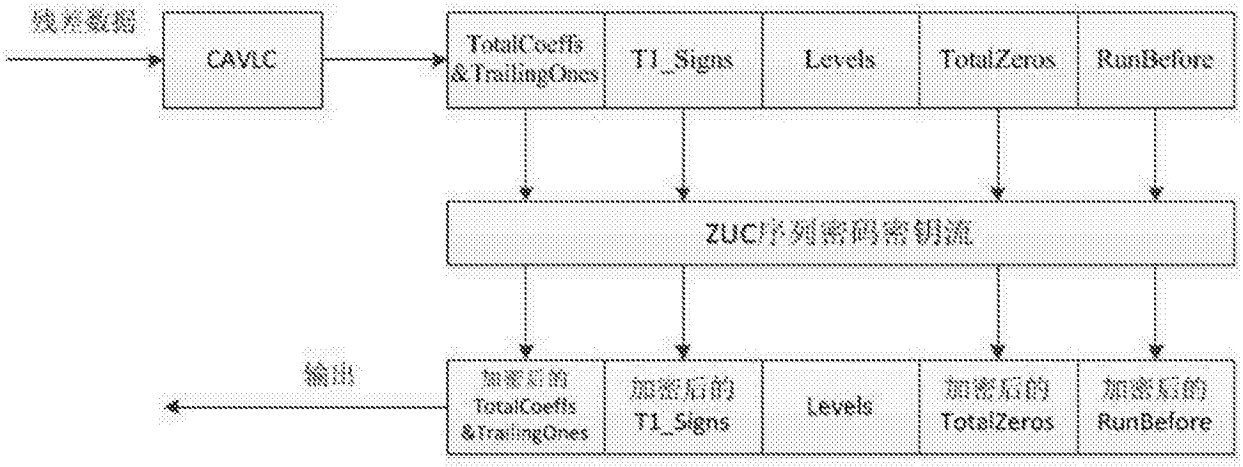

残差数据
CAVLC
TotalCoeffs &TrailingOnes
T1_Signs
Levels
TotalZeros
RunBefore
ZUC序列密码密钥流
输出
加密后的TotalCoeffs &TrailingOnes
加密后的T1_Signs
Levels
加密后的TotalZeros
加密后的RunBefore

图3