



研究与开发

基于幻方变换的 HEVC 熵编码加密方案

徐博文, 王晓东, 郭磊, 王健

(宁波大学信息科学与工程学院, 浙江 宁波 315211)

摘要: 针对多媒体信息安全问题, 基于高效视频编码标准 (HEVC/H.265) 的熵编码模块, 结合幻方变换矩阵, 设计了一种具有实时性和高效性的面向高清视频流的加密算法。该算法有效利用变换系数的分布稀疏性, 置乱变换块 (TB) 的系数组 (CG), 并对 CG 熵编码的语法元素进行了选择性加密。实验结果表明, 本文的加密方案具有高安全性, 保证格式兼容性并仅对编码比特率造成很小的影响, 满足视频加密保护的需求。

关键词: HEVC; 幻方矩阵; 熵编码; 变换系数; 选择性加密

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018015

A video encryption in HEVC entropy coding based on magic square

XU Bowen, WANG Xiaodong, GUO Lei, WANG Jian

Institute of Communication Technology, Ningbo University, Ningbo 315211, China

Abstract: In view of the multimedia information security, based on the entropy module on high efficiency video coding (HEVC/H.265), combined with the magic square, a real time and high efficiency encryption technique for high-definition video streaming was proposed. The algorithm which had an effective use of transform coefficient sparsity enabled coefficient group (CG) of transform block (TB) scrambling, and used a selective encryption on syntax elements in CG's entropy. The experiments prove that the investigated scheme has high security, which can guarantee the standard compliance and the demand of video encryption while having a low impact on encoding-rate performance.

Key words: high efficiency video coding, magic square matrix, entropy coding, transform coefficient, selective encryption

收稿日期: 2017-09-22; 修回日期: 2017-11-10

基金项目: 国家科技支撑计划基金资助项目 (No.2012BAH67F01); 国家自然科学基金资助项目 (No.U1301257); 浙江省教育厅科研计划基金资助项目 (No.Y201327703); 浙江省自然科学基金资助项目 (No.Y1110161); 宁波市科技创新团队研究计划基金资助项目 (No.2011B81002)

Foundation Items: National Science and Technology Program (No.2012BAH67F01), The National Natural Science Foundation of China (No.U1301257), Research Project of Zhejiang Provincial Education Department (No.Y201327703), Zhejiang Provincial Natural Science Foundation of China (No.Y1110161), Science and Technology Innovation Team Research Project of Ningbo (No.2011B81002)



1 引言

随着多媒体信息时代的迅猛发展,视频流量高速增长,智能终端带来视频应用多样化的同时也对视频编码技术提出更加高效的要求。在这种背景下,催生出了新一代视频编码标准(high efficiency video coding, HEVC/H.265),在同等的主观视频质量下,HEVC 的压缩效率比前代 H.264/AVC 提升了 50%^[1]。另一方面,诸如安防监控的相关文件、视频会议的重要内容,当运用 HEVC 的编码框架时,如何保证这些视频的安全实时传输已经成为视频编码应用中的热点课题。

许多学者及相关研究机构都提出了基于 H.264 的视频加密方案,现有的加密算法都是在熵编码过程中对语法元素进行合适的加密,如 Ashgar 等人^[2]针对 DCT 变换过程采取一种无损加密方案,并且提出了一种新的密钥管理机制。由于新的 HEVC 编码标准采用了递归的四叉树编码结构,宏块具有可伸错性,使得熵编码的语法元素设计不同于 H.264,因而不能在 HEVC 上应用。譬如, Ahn 等人^[3]选择对帧内预测模式进行加密,对于不同大小的 PU,针对加密兼容性要求,但是其密钥空间的选择只有 1 bit 密钥流,因而安全性不高。朱文斌等人^[4]利用混沌映射生成伪随机置乱群,置乱变换单元(transform unit, TU),结合 RSA 密文传输混沌映射参数,实现了 HEVC 编码框架下的视频安全传输。Boyadjis 等人^[5]针对 HEVC 新的 CABAC 熵编码模式,选择了沿用前代 H.264/AVC 的旁路模式下的语法元素,使得该加密算法可以适用于 H.264/AVC 和 HEVC。对视频质量显著下降与额外的码流开销进行折中,并分析了 H.265 熵编码常规模式下的加密安全性能。Ouamri 等人^[6]在熵编码的二值化中引入一个 CBC 模式,对 K 阶哥伦布指数编码以及莱斯截断码的后缀采用经典的 AES 加密,后缀的加密空间十分可观,加密后的图像视觉质量下降显著,并且具

有良好的可靠性和顽健性。

一个优秀的视频加密方案需要保证加密安全性,满足码流格式兼容性,并且对编码效率造成的影响要在可接受范围内。幻方变换是一种十分经典的图像置乱方法,丁伟等人^[7]利用标准幻方改变数字图像的空间位值,但是仅对图像进行幻方加密,安全性较低,易遭受攻击。Zhong 等人^[8]引入了基于 GLP 的全新幻方矩阵加密方法,对这种经典方法进行了改进,它通过提供不同的加密周期实现了更好的加密效果。当加密整个视频流,比如使用标准加密方案(data encryption scheme, DES),时间复杂度很高,难以保证视频传输的时效性,并且这种加密方式往往破坏了视频码流格式,即无法满足视频兼容性。因此在 H.265 中,选择性加密是加密算法的主流方向,根据编码标准选择合适的加密位置和合理的加密元素十分关键。本文将重点讨论如何最大可能地在视频加密方案中获得安全、高效以及兼容性之间的折中。

2 算法思路和步骤

本文的视频加密算法包含以下几个步骤,以采用对角扫描模式的 8×8 像素 TB 为例,算法流程如图 1 所示。

步骤 1 构造四阶全幻方矩阵,生成变换系数置乱的密钥空间。

步骤 2 对于 $N \times N$ 的 TB,使用基于 4×4 像素的子块扫描技术,将 TB 分割为 $n \times n$ 的 CG($n=N/4$)。

步骤 3 在步骤 2 的基础上,利用步骤 1 中生成的幻方矩阵置乱 CG,得到 CG'。

步骤 4 对变换系数中的语法元素,当 HEVC 采用上下文模型进行算术编码,选择 CG 中对应的语法元素;当 HEVC 采用旁路编码模式,则选择 CG'中对应的语法元素。

3 基于幻方变换的视频加密算法

HEVC 采用更为灵活多变的四叉树编码结构

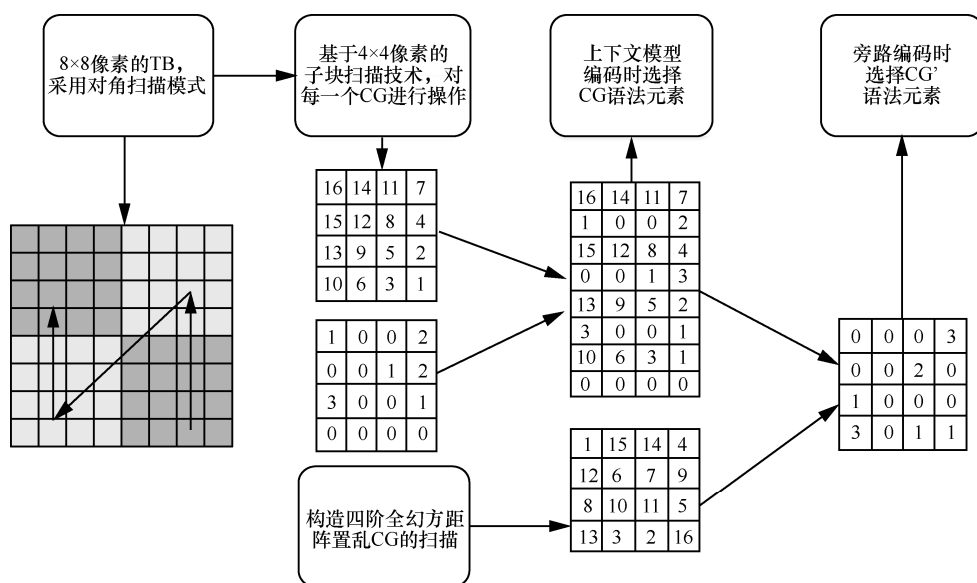


图1 基于幻方变换的熵编码加密算法的结构

替代 H.264 中的宏块结构, 大大提升了编码效率。CU (coding unit, CU) 是基本编码单元, 分为 4 种不同层次: 64×64 像素、32×32 像素、16×16 像素、8×8 像素。在预测编码中, 依据率失真代价遍历所有可能的预测模式^[9], CU 将被划分为一个或多个预测单元 (prediction unit, PU), 根据预测编码生成的预测残差的差异性, TU 可以自适应地选择最佳的划分深度, 有 4 种尺寸选择: 4×4 像素、8×8 像素、16×16 像素、32×32 像素。编码器通过变换、量化, 最后对变换系数进行熵编码。

3.1 变换系数熵编码

3.1.1 变换系数的特征

熵编码按照信息熵原理, 去除表征视频序列的元素和符号的统计冗余, 是保证视频码流压缩效率的关键模块之一。预测残差经过变换量化得到变换系数是视频码流中的主要组成部分, 该部分的熵编码在整个熵编码中举足轻重。图 2 给出 OP=32 时标准测试序列的码流组成, 可以看出变换系数在编码比特流中的开销一般需要占到 80% 以上。在 HEVC 中, 色度和亮度的变换系数都是通过 TB 来处理, 判断 TB 中是否存在非零系数, 并编码这些非零系数的位置

信息和幅值信息。图 3 中统计了 Johnny 序列中非零系数个数的分布情况, 绝大部分的 CG 内很少甚至没有非零系数, 充分说明了其分布具有稀疏性, 这种稀疏性保证了本文加密算法的计算复杂度。

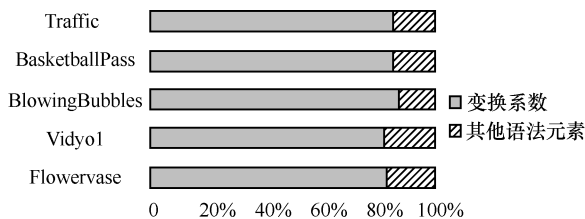


图2 不同序列的变换系数占码流比率

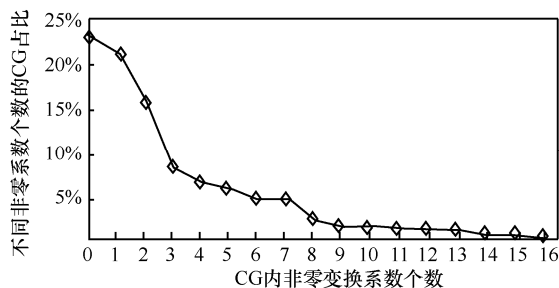


图3 Johnny 序列中不同 CG 的非零变换系数组成

3.1.2 变换系数熵编码规则

在对变换系数熵编码前, 需先确定 TB 中所有系数的扫描顺序。HEVC 为了使不同 TB



的熵编码具有同一性, 采用了基于 CG (coefficient group, CG) 的扫描技术, CG 表示每个 4×4 像素大小的子块, 譬如 8×8 像素的 TB 被分为 4 个 CG, TB 中 CG 有 3 种扫描方式: 分别为垂直扫描、水平扫描以及对角扫描, 具体如图 4 所示。每个子块内的扫描顺序如图 5 所示, 4 个 CG 的先后顺序同样按照图 5 的 3 种扫描方式来确定。经过系数扫描, 二维的变换系数矩阵降维排列成一维序列。

一个 TB 中变换系数的熵编码具体流程如下。

步骤 1 确定 TB 内的 CG 个数 numCG, 从 $i = 1$ 开始编码每一个 CG。

步骤 2 判断当前 CG 是否存在非零系数, CSBF(Coded Sub_Block_Flag)=1 表示当前 CG 内存在非零系数, CSBF=0 表示 CG 系数全为零。当 CSBF=1, 转至步骤 3; CSBF = 0, $i = i + 1$, 转至步骤 2。

步骤 3 扫描至最后一个非零系数, 编码该系数的 x 和 y 的坐标信息: last_posX 和 last_posY。

步骤 4 在 CG 内编码所有非零系数的标识位 sig_flag。

步骤 5 编码所有非零系数的幅值信息:

coeff_flag、g1flag、g2flag、coeff_remain。

步骤 6 当 $i = \text{numCG}$ 时, TB 的变换系数编码结束。

coeff_flag=1 表示非零系数为正值, 否则为负值; g1flag 和 g2flag 分别表示非零系数绝对值是否大于 1 和 2。

coeff_remain 表示幅值信息绝对值的剩余部分, 计算方法如式 (1) 所示, 其中, abscoeff 表示幅值的绝对值。

$$\text{coeff_remain} = \text{abscoeff} - \text{coeff_flag} - \text{g1flag} - \text{g2flag} \quad (1)$$

3.2 幻方矩阵置乱变换系数

3.2.1 全四阶幻方的构造

如式 (2) 所示, 幻方是一个 N 阶矩阵 ($N \geq 3$), 其中, $1 \leq a_{ij} \leq N^2$ ($i \leq N, j \leq N$)。

$$A = \begin{bmatrix} a_{11} & L & a_{1N} \\ M & O & M \\ a_{N1} & L & a_{NN} \end{bmatrix} \quad (2)$$

幻方具有如下重要特征^[10]。

- 令 $S = (N^2 + 1)N/2$, 幻方的行和、列和、两条对角线之和均为 S ;
- 对于本文中采用的四阶幻方 $\{a_1, a_2, a_3, \dots, a_{15}, a_{16}\}$, $S = 34$, 同时还满足式 (3):

16	12	8	4
15	11	7	3
14	10	6	2
13	9	5	1

(a) 垂直扫描

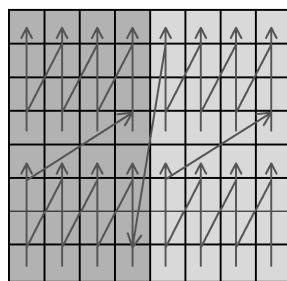
16	15	14	13
12	11	10	9
8	7	6	5
4	3	2	1

(b) 水平扫描

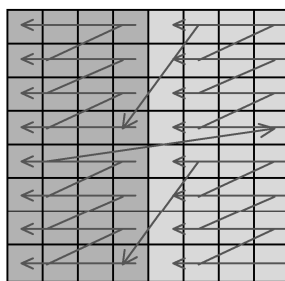
16	14	11	7
15	12	8	4
13	9	5	2
10	6	3	1

(c) 对角扫描

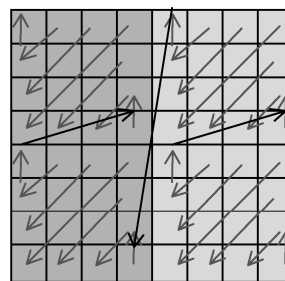
图 4 CG 的扫描顺序



(a) 垂直扫描



(b) 水平扫描



(c) 对角扫描

图 5 8×8 像素的 TB 扫描顺序

$$\begin{cases} a_6 + a_7 + a_{10} + a_{11} = 34 \\ a_1 + a_{16} + a_4 + a_{13} = 34 \\ a_5 + a_9 + a_8 + a_{12} = 34 \\ a_2 + a_3 + a_{14} + a_{15} = 34 \end{cases} \quad (3)$$

- 所有形式的四阶幻方共有 7 040 个。

利用上述性质并考虑到加密算法对时间复杂度的要求, 本文采用回溯法构造出全部的四阶幻方。充分利用上述性质构造出全部 7 040 个四阶幻方作为密钥空间。在编码开始阶段便生成该密钥空间表, 对于每一个 CG, 只需随机选择一个表中索引, 利用相应的幻方矩阵作为 CG 新的扫描顺序。全四阶幻方的构造耗时在 10 s 内, 伪代码如下所示:

```

initialization  $i \leftarrow 1, a[17], b[17]$ 
function MagicFunction( $i$ )
 $n \leftarrow 0$ 
 $j \leftarrow 1$ 
while  $j < 17$ 
do  $b[i] \leftarrow j$ 
 $a[j] \leftarrow 1$ 
if  $i=1$  or  $2$  or  $3$  or  $5$  or  $6$  or  $7$  or  $9$  or  $10$ 
then MagicFunction( $i+1$ )
else if  $i=11$  and  $b[6] + b[7]+b[10]+b[11]=34$ 
then MagicSquare(12)
else if  $i=4$  or  $8$  or  $12$  and  $b[i-3]+b[i-2]+$ 

```

```

 $b[i-1] + b[i] == 34$ 
then MagicSquare( $i+1$ )
else if  $i=13$  and  $b[1]+b[5]+b[9]+b[13]=34$ 
and  $b[4]+b[7]+b[10]+b[13]=34$ 
then MagicSquare(14)
else if  $i=14$  or  $15$  and  $b[i-12]+b[i-8]+b[i-4]+b[i]==34$ 
then MagicSquare( $i+1$ )
end if
 $a[j] \leftarrow 0$ 
end

```

3.2.2 变换系数的置乱过程

由于 CG 的大小为 4×4 像素, 并且 TB 以 CG 作为子块扫描的基本单位, 这使得利用四阶幻方矩阵改变 CG 中非零系数的位置非常合适。CG 的变换系数具有稀疏性, 往往集中于扫描系数的后 8 位, 在需要加密的语法元素中利用幻方矩阵代替 CG 矩阵, 可以有效地改变变换系数的空间位置, 达到置乱效果。图 6(a) 中左上的矩阵为 CG 的对角扫描, 变换系数矩阵的位置和幅值信息如图 6(a) 中左下矩阵所示, 规定 TB 中系数位置由右下角向左上角 Z 字扫描, 显然经过对角扫描, 非零系数集中于扫描的后 8 位。图 6(b) 和图 6(c) 中用两种不同的四阶幻方矩阵, 改变了图 6(a) 中的变换系数扫描顺序。CG 中非零系数绝大部分分布在

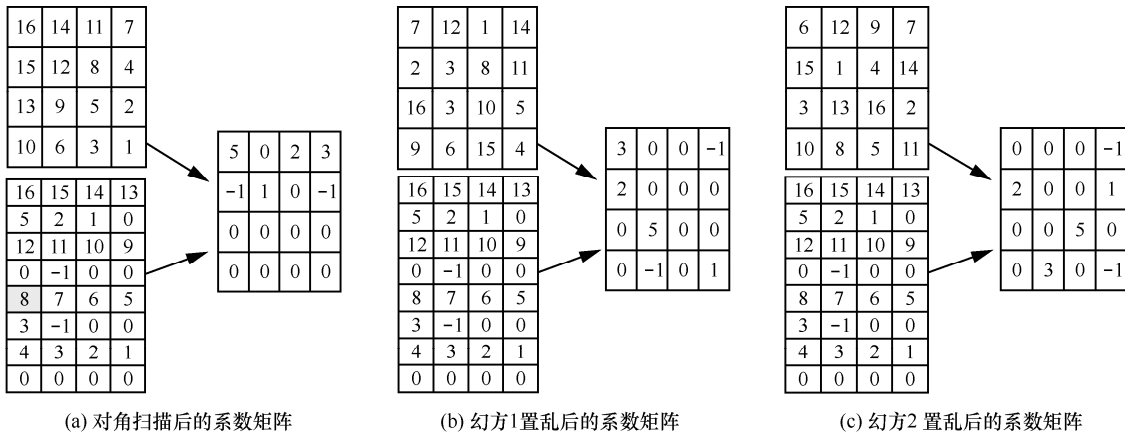


图 6 不同四阶幻方置乱变换系数



左上角区域,从图 6 (b) 和图 6 (c) 可以看出,经过幻方置乱后预测残差的能量均匀地分布在 CG 之中而不再只是后 8 位,原先 CG 位置上的系数基本都发生了变换。经过扫描后的变换系数,将按照上述 Z 扫描的方式对每个变换系数的位置信息和幅值信息进行熵编码。

3.3 语法元素选择性加密

在 HEVC 中,绝大部分语法元素的熵编码模式是基于上下文的自适应二进制算术编码 (context adaptive binary arithmetic coding, CABAC)^[11],这种方法将自适应性二元算数编码与上下文模型结合起来。变换系数中语法元素的上下文模型,利用邻近系数之间的相关性以提高编码效率。因此改变非零系数的值破坏了原本的上下文模型,不仅会显著提升码流增益,更有可能丢失解码端的兼容性。如图 7 所示,熵编码中还存在旁路编码模式,该编码模式无需更新上下文模型,只进行常规的二元算数编码。

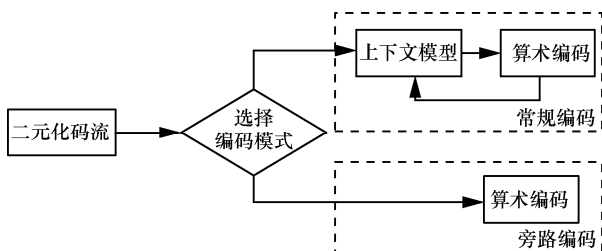


图 7 HEVC 两种熵编码模式

HEVC 对图 7 中的变换系数按照 Z 扫描的方式逐一编码,将一个二维矩阵转化成了一组一维序列。通过扫描到的最后一个非零系数区分不同 TB,因此最后一个非零系数的位置不可以改变,

在 HEVC 熵编码模块中需要先确定最后一个非零系数,采用正确的扫描顺序使解码器能正确地定位不同 TB。图 8 列出了所有需要进行熵编码的语法元素,对 TB 中的最后一个非零系数的位置信息熵编码后,以 CG 作为子块单位编码剩余的语法元素,其中灰色部分表示该语法元素采用了旁路编码模式。第 3 行和第 4 行分别为正常扫描方式下的 CG 序列 pcCoeff1 和四阶幻方置乱后的 CG 序列 pcCoeff2,对比 pcCoeff1 和 pcCoeff2 可以看出,幻方矩阵下变换系数的扫描顺序发生了改变,非零系数不再集中分布于后 8 位。当 pcCoeff1 对 coeff_flag 和 coeff_remain 两个语法元素熵编码时,以 pcCoeff2 中相同位置的语法元素替换,从而置乱了码流中非零系数。本文的加密方案结合了四阶幻方与熵编码的特点,保证了视频加密兼容性。

3.4 加密的抗攻击能力

视频加密的防攻击性十分关键,从破解概率角度分析本文加密方案的性能。在变换系数的加密过程中,本文加密了 coeff_flag 以及 coeff_remain。针对这两个语法元素,在每个 CG 中,令可置乱的语法元素个数为 n ($1 \leq n \leq 16$),正确破解 CG 的概率为 P_n ,用于置乱 CG 的扫描顺序个数为 7040。对于一帧视频而言,用穷举法正确破解的概率为 P_{FRAME} ,那么可以得到式 (4) 的结果。其中, P_n 表示每个 CG 被正确破解的可能性,假设整帧视频中存在 m 个待加密 CG,CG 单元的个数则达到了数千级别,想要正确破解的可能性微乎其微。

TB扫描	last_posX	last_posY													
CG	CSBF	sig_flag										coeff_flag	g1flag	g2flag	coeff_remain
子块扫描	0 0 0 0 0 0 0 0 -1 0 1 -1 3 2 0 5										pcCoeff1				
	1 0 -1 0 0 0 5 0 0 0 0 2 -1 0 0 2										pcCoeff2				

图 8 不同扫描方式下的变换系数组合熵编码

$$P_{\text{FRAME}} = (Pn)^m = \left(\frac{1}{7\,040} \right)^m \quad (4)$$

4 实验结果与对比分析

本文的实验平台选择 HM12.02 版本, 首先对不同等级的序列编码并解码得到一系列原始视频码流。为说明该加密方法对不同序列具有普适性, 选择的视频序列见表 1, 包括 7 个像素深度为 8 bit 的测试序列, 分辨率从 416 dpi×240 dpi 到 2 560 dpi×1 600 dpi。在同样条件下, 采用四阶幻方置乱变换系数, 并将置乱后的视频码流送入标准解码器, 通过比较原始视频码流和置乱后码流来评估本方案的加密效果以及加密带来的比特率影响。编码的参数配置选择全 I 帧编码, 图像组 (group of picture, GOP) 的大小为 8, 选择 4 种 QP 值 (22、27、32、37) 以分析不同 QP 下测试序列的加密表现。

表 1 本文视频加密选择的测试序列

序列	帧数	帧率(f·s ⁻¹)	分辨率
Traffic	60	30	2 560 dpi×1 600 dpi
Kimono	60	24	1 920 dpi×1 080 dpi
Johnny	60	60	1 280 dpi×720 dpi
ChinaSpeed	60	30	1 024 dpi×768 dpi
BaksetballDrill	60	50	832 dpi×480 dpi
BasketballPass	60	50	416 dpi×240 dpi
BlowingBubbles	60	50	416 dpi×240 dpi

在图 9 中, 选取了第 8、9、10 帧以展示 Johnny 序列加密前后的对比, 表明了在不同 QP 下的加密均使得视频的主观质量很差。图 9 (a) 是未加密的原始序列, 可以清晰地看出画面中的人物以及背景; 图 9 (b) ~ 图 9 (e) 是标准解码器下解码得到, 从而验证了本文加密方案的兼容性, 同时整图中的内容均已无可辨认, 主要是因为变换系数的非零幅值信息 `coeff_remain` 被加密所致。为了分析视频加密的客观质量, 本文首先使用 PSNR 比较序列加密前后的置乱效果, 见表 2。HM 平台中利用重建帧和原始帧计算 PSNR, 由于本文的加密方法是发生在重建之后的熵编码阶段, 因此利用解码帧和原始帧统计出 PSNR。可以发现增加 QP 会使标准编码下的 PSNR 越来越低, 不同 QP 条件下加密序列的 PSNR 均严重下降。`deltaPSNR` 表示相比标准编码的 PSNR, 加密后的 PSNR 下降比例, 本文所用测试序列中 `deltaPSNR` 平均值达到 77.432%。`SSIM` 是一种基于人眼视觉特性的图像质量客观评价准则, 图 10 利用 `SSIM` 分别比较原始序列与标准编码模式以及加密模式下的结构相似性。可以直观地看出加密前后 `SSIM` 巨大的变化, 未加密时所有序列在不同 QP 下的 `SSIM` 均维持在 0.9 附近, 而加密后视频序列结构相似性的平均值仅为 0.172。

表 2 不同测试序列加密前后的 PSNR 对比

序列	QP22/dB		QP27/dB		QP32/dB		QP37/dB	
	未加密	加密	未加密	加密	未加密	加密	未加密	加密
Traffic	43.35	9.96	40.16	8.03	37.12	9.08	34.10	7.55
Kimono	43.01	8.35	41.66	9.30	39.82	7.02	37.40	6.33
Johnny	44.04	10.70	41.88	10.38	39.59	10.97	37.00	10.20
ChinaSpeed	45.18	6.11	41.31	5.20	37.52	3.77	33.82	3.71
BaksetballDrill	41.77	12.15	38.41	7.60	35.46	9.28	32.83	9.60
BasketballPass	42.86	9.54	39.34	11.82	35.91	9.58	32.78	10.47
BlowingBubbles	42.71	10.41	37.55	10.45	33.52	9.23	29.33	6.81
平均	43.28	9.60	40.04	8.97	36.99	8.42	33.89	7.81

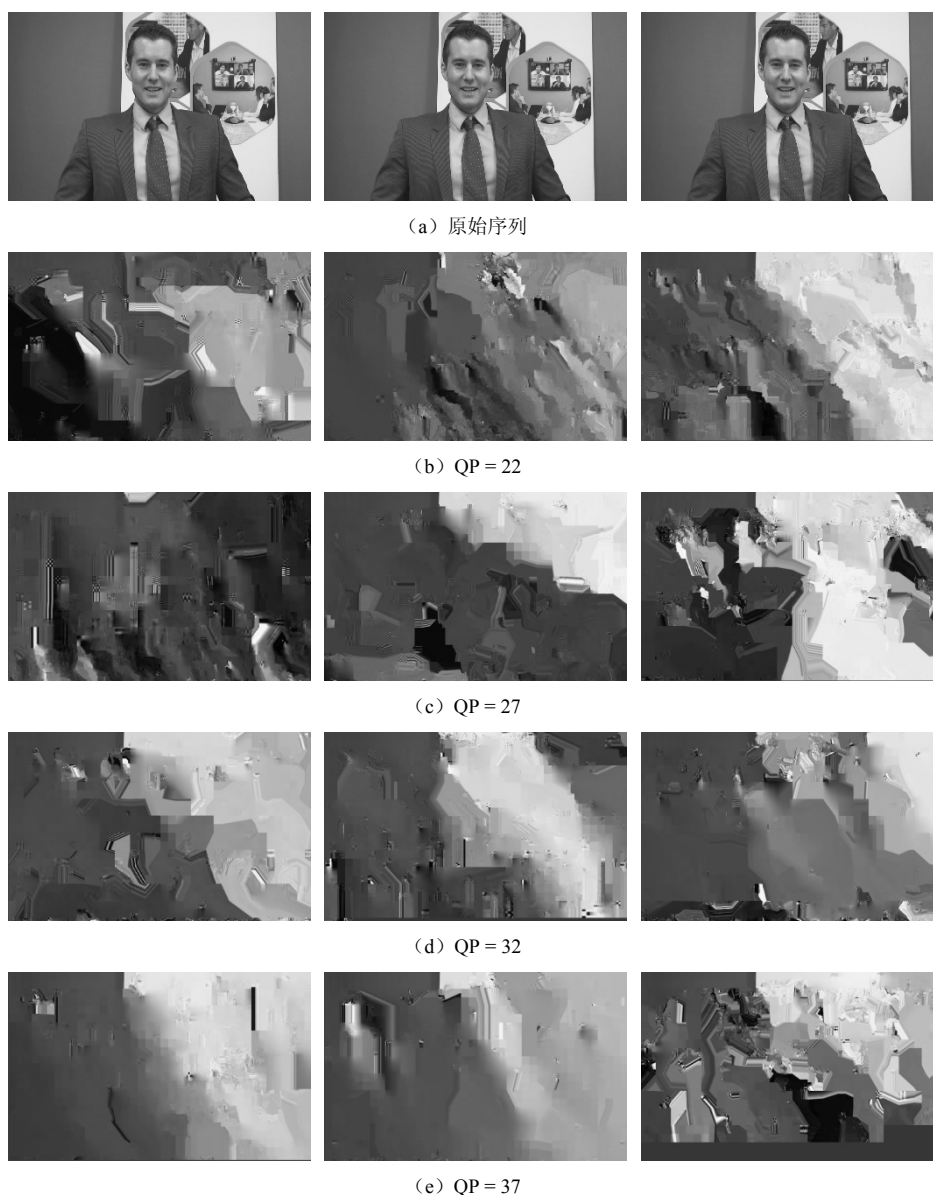


图9 Johnny序列加密前后主观质量对比

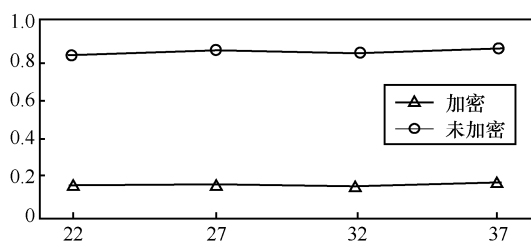


图10 加密前后不同QP下SSIM对比

为说明加密变换系数对码率的影响,表3分别对各个序列做了测试,可以看出,随着QP愈

来愈大,码率变化幅度也略微升高。因为在标准编码模式下非零系数往往集中在左上角区域,因此HEVC熵编码中会将CG的后8位的g2flag默认置1,置乱后的非零系数发生了改变,显然造成了g2flag以及coeff_remain的变化。但是总体而言加密后的序列码率增长都很小,因此本文加密方法带来的额外码率开销是很小的。

目前面向HEVC的视频加密应用并不多,表4给出了本文的加密方案和现有加密算法的综合比

表3 不同测试序列的码率增长情况

序列	QP22	QP27	QP32	QP37	平均
Traffic	+0.76%	+1.14%	+1.43%	+1.69%	+1.25%
Kimono	+1.89%	+2.36%	+2.42%	+2.52%	+2.30%
Johnny	+0.92%	+0.90%	+1.10%	+1.24%	+1.04%
ChinaSpeed	+3.46%	+2.74%	+1.82%	+0.44%	+2.11%
BaksetballDrill	+0.83%	+1.04%	+1.02%	+1.01%	+0.97%
BasketballPass	+0.37%	+0.65%	+0.87%	+1.11%	+0.75%
BlowingBubbles	+0.09%	+2.65%	+1.32%	+0.99%	+1.26%

表4 各加密方案综合比较

方案	加密元素	加密方式	Δ PSNR/dB	Δ SSIM	兼容性
参考文献[11]方案	HEVC 标准头信息	混沌密钥	--	--	否
参考文献[12]方案	mvd_sign+residual sign	AES	-22.1	-0.680%	是
参考文献[13]方案	帧内预测模式和运动残差以及量化变换符号	AES	-30.05	-0.610%	是
参考文献[14]方案	coeff_remain 的 TR 后缀码和 k 阶指数哥伦布的后缀码	混沌序列	-19.785	0.285%	是
本文方案	coeff_flag+coeff_remain	幻方置乱	-29.85	-0.701%	是

较。在熵编码过程中,部分 HEVC 标准的头信息采用指数哥伦布编码的方式二值化,参考文献[12]中利用混沌密钥流改变了指数哥伦布编码方式,这样的暴力加密方法会使得标准解码器无法正常解码。参考文献[13]采用 AES 加密运动矢量残差(mvd_sign)以及预测残差符号位(residual sign),参考文献[14]加密了帧内预测模式(rem_intra_luma_pred_mode)、mvd_sign、量化参数变化符号(cu_qp_delta_sign)、非零系数符号(coeff_sign_flag);参考文献[15]改变了 coeff_remain 的截断莱斯码以及指数哥伦布后缀码的编码方式,这几种加密方案均可以满足加密兼容性。从表4中可以看出,本文的加密方案在 SSIM 以及 PSNR 的下降率上具有一定优势,因此本文的加密方案在保证视频兼容性的同时具有更优秀的安全性能。

5 结束语

针对当今多媒体信息安全的需求,本文依据 H.265/HEVC 的熵编码特性,置乱了变换系数组的

扫描顺序。实验结果表明,在视频码率增长很小的情况下,本文加密方案有效降低了 PSNR 以及 SSIM,同时可以满足视频兼容性,这种高安全性的加密方案有着广阔的应用前景。今后将继续研究面向 H.265/HEVC 的视频加密应用,主要包括:结合感兴趣区域提取,设计出一种用于加密视频关键区域的加密方案,如新闻采访中受访者隐私的保护;基于 HEVC 的可分层视频编码,针对不同的分辨率需求,进行不同的加密设计。

参考文献:

- [1] SULLIVAN G J, OHM J, HAN W J, et al. Overview of the high efficiency video coding (HEVC) standard[J]. IEEE Transactions on Circuits & Systems for Video Technology, 2012, 22(12): 1649-1668.
- [2] ASGHAR M N, GHANBARI M. An efficient security system for CABAC bin-strings of H.264/SVC[J]. IEEE Transactions on Circuits & Systems for Video Technology, 2013, 23(3): 425-437.
- [3] AHN J, SHIM H J, JEON B, et al. Digital video scrambling method using intra prediction mode[J]. Lecture Notes in Computer Science, 2004(3333): 386-393.
- [4] 朱文斌. 基于 H.265 的视频信息安全传输的研究[J]. 网络安全



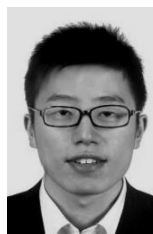
- 全技术与应用, 2016(10): 47-49.
- ZHU W B. Research on secure transmission of video information based on H.265[J]. Network Security Technology and Application, 2016(10): 47-49.
- [5] BOYADJIS B, BERGERON C, PESQUET-POPESCU B, et al. Extended selective encryption of H.264/AVC (CABAC) and HEVC encoded video streams[J]. IEEE Transactions on Circuits & Systems for Video Technology, 2016: 1.
- [6] OUAMRI M, FARAOUN K M. Robust and fast selective encryption for HEVC videos[J]. Journal of Communications Software & Systems, 2014, 10(4): 221-229.
- [7] 丁玮, 齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报, 1998, 21(9): 838-843.
- DING W, QI D X. Digital image transformation and information hiding and masking technology[J]. Journal of Computer Science, 1998, 21(9): 838-843.
- [8] ZHONG W, DENG Y H, FANG K T. Image encryption by using magic squares[C]//International Congress on Image and Signal Processing, Biomedical Engineering and Informatics, October 14-16, 2017, Shanghai, China. Piscataway: IEEE Press, 2017: 771-775.
- [9] 姚英彪, 李晓娟. 基于图像空间相关性与纹理的 HEVC 块划分快速算法[J]. 电信科学, 2015, 31(1): 32-40.
- YAO Y B, LI X J. Fast algorithm for HEVC block partitioning based on image spatial correlation and texture[J]. Telecommunications Science, 2015, 31(1): 32-40.
- [10] OLLERENSHAW D K, BONDI H. Magic squares of order four[J]. Philosophical Transactions of the Royal Society A Mathematical Physical & Engineering Sciences, 1982, 306(1495): 443-494.
- [11] ZHOU M, GAO W, JIANG M, et al. HEVC lossless coding and improvements[J]. IEEE Transactions on Circuits & Systems for Video Technology, 2012, 22(12): 1839-1843.
- [12] 郭芳, 张家树. 基于 H.265 的安全高效的指数哥伦布编解码方案[J]. 计算机应用与软件, 2013(10): 85-86.
- GUO F, ZHANG J S. A safe and efficient index Columbo encoding and decoding scheme based on H.265[J]. Computer Applications and Software, 2013(10): 85-86.
- [13] BOHO A, WALLENDIAEL G V, DOOMS A, et al. End-to-end security for video distribution: the combination of encryption, watermarking, and video adaptation[J]. IEEE Signal Processing Magazine, 2013, 30(2): 97-107.
- [14] YANG M, ZHUO L, ZHANG J, et al. An efficient format compliant video encryption scheme for HEVC bitstream[C]// IEEE

International Conference on Progress in Informatics and Computing, October 5, 2016, Austin, TX, USA. Piscataway: IEEE Press, 2016: 374-378.

- [15] 陈谢. 基于 H.265 的视频加密算法研究与实现[D]. 杭州: 杭州电子科技大学, 2016.

CHEN X. Research and implementation of video encryption algorithm based on H.265[D]. Hangzhou: Hangzhou Dianzi University, 2016.

[作者简介]



徐博文 (1993-), 男, 宁波大学信息科学与工程学院硕士生, 主要研究方向为视频图像处理、多媒体信息安全技术。



王晓东 (1970-), 男, 宁波大学信息科学与工程学院教授、硕士生导师, 主要研究方向为图像及视频信息处理、多媒体通信、信息安全。近年来在核心刊物和国际会议上发表论文 30 余篇, 其中 SCI/EI 检索论文 20 篇, 主持和参与国家科技支撑计划项目 1 项、国家自然科学基金项目 4 项、浙江省自然科学基金项目 7 项、浙江省科技计划项目 1 项。



郭磊 (1993-), 男, 宁波大学信息科学与工程学院硕士生, 主要研究方向为视频编码、视频图像处理。



王健 (1993-), 男, 宁波大学信息科学与工程学院硕士生, 主要研究方向为图像显著性区域检测、多媒体通信技术。