HEVC视频加密技术综述

叶清[1]，刘小兵[1]，荣里[2]，何俊霏[1]，张乔嘉[1]
（1. 海军工程大学信息安全全系，湖北 武汉 430033；2. 海军工程大学舰船综合试验训练基地，湖北 武汉 430033）

摘　要：针对视频数据在传输和存储过程中存在被非法获取和恶意破坏的问题，从高效视频编码（HEVC）标准和加密技术出发，对HEVC视频编码标准下的加密技术进行综述。回顾了视频编码技术的发展历程，介绍了HEVC视频编码标准，讨论了视频加密技术常见攻击方法及性能评估指标，全面梳理与详细分析了不同视频加密技术性能及其优缺点，展望了视频加密技术的发展趋势，旨在为视频加密技术的研究和应用提供参考。

关键词：高效视频编码；加密；感兴趣区域；帧内预测模式；运动矢量差；熵编码
中图分类号：TP391
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024113

Review of HEVC video encryption technology

YE Qing[1], LIU Xiaobing[1], RONG Li[2], HE Junfei[1], ZHANG Qiaojia[1]
1. Department of Information Security, Naval University of Engineering, Wuhan 430033, China
2. Base of Warship Testing and Training, Naval University of Engineering, Wuhan 430033, China

Abstract: Concerning the issue of illegal access and malicious destruction of video data during transmission and storage, a review on encryption techniques under the high efficiency video coding (HEVC) standard was conducted, starting with the HEVC standard and encryption technology. The development history of video coding technology was reviewed, and the HEVC standard was introduced. Common attack methods on video encryption technology and performance evaluation indicators were discussed. The performance, advantages, and disadvantages of different video encryption technologies were comprehensively analyzed and detailed. The development trends of video encryption technology was summarized and anticipated in order to provide reference for the research and application of video encryption technology.

Keywords: HEVC, encryption, region of interesting, intra prediction mode, motion prediction difference, entropy coding robustness

0　引言

随着多媒体技术服务的日益多样化、高清视频的逐渐普及以及超高清视频格式的出现，对早期高级视频编码（AVC, advanced video coding）[1]的编码效率产生了更高的要求，视频编码技术面临着严峻的挑战。高效视频编码（HEVC, high efficiency video coding）[2]也称为H.265，是由视频编码专家组和国际标准组织/国际电工委员会运动图像专家组发布的视频编码标准，旨在解决AVC（H.264）所面临的困境，并特别关注2个关键问题：提高视频分辨率和增加并行处理架构的使用。HEVC的语法是通用的，通常情况下也适用于视频编码领域的其他应用。HEVC在AVC框架的基础上，引入了大量新的编码技术，在实现视频相同编码质量的情况下，压缩效率大约提高了一倍，并且还可以处理高达8 K的分辨

收稿日期：2023–11–22；**修回日期：**2024–05–24
通信作者：刘小兵，d23381007@nue.edu.cn
基金项目：国家自然科学基金资助项目（No.61672531）；国防科技173计划基金资助项目（No.2021-JCJQ-JJ1267）
Foundation Items: The National Natural Science Foundation of China (No.61672531), Defense Technology 173 Program (No.2021-JCJQ-JJ1267)

率。最新的视频编码标准——通用视频编码（VVC, versatile video coding）于2020年7月定稿[3]，但由于其编码复杂度远大于HEVC，因此在存储、计算能力和传输带宽受限的场景中，主要采用HEVC视频编码技术。视频编码技术的发展如图1所示。

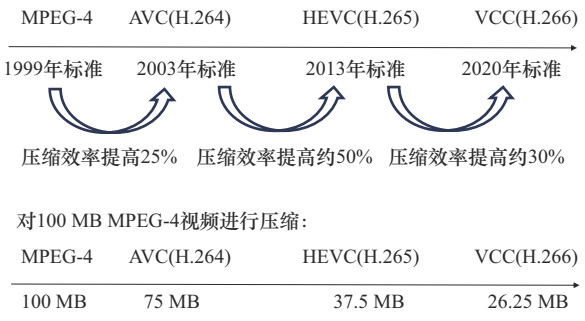


图1　视频编码技术的发展

目前，国内外学者对于HEVC视频提出了许多不同类型的加密技术。然而，目前的视频加密技术综述还没有对HEVC视频编码标准下的加密技术进行全面且详细的分析。因此，本文对HEVC视频编码标准下的加密技术进行了全面的综述，总结了不同HEVC视频加密技术的性能及其优缺点，归纳了各视频加密算法的研究思路，为视频加密技术的研究和应用提供了依据。

本文的主要贡献总结如下。

1) 介绍了HEVC视频编码标准的技术架构，给出了HEVC视频加密技术的常见攻击手段及性能评估指标。

2) 根据应用加密算法的区域和加密元素不同，提出了HEVC视频加密技术的分类方法，并对每类视频加密技术进行了综述，全面梳理与详细分析了不同视频加密技术的性能及其优缺点。

3) 讨论了HEVC视频加密技术面临的挑战以及未来的发展趋势。

1　HEVC视频编码标准

1.1　HEVC编码框架

HEVC是一种用于压缩高清视频的技术，可以在相同画质下显著减小视频文件的大小，或者在相同文件大小的前提下提供更高质量的视频。HEVC视频编码标准的出现使视频传输和存储变得更加高效，因此被广泛应用于数字电视、视频会议、视频存储和在线视频等领域。HEVC视频编码标准旨在实现多方面的改进，包括编码效率、传输系统集成、数据丢失恢复能力以及使用并行处理结构的可行性。HEVC的编码原理和基本结构与AVC基本一致，即预测加变换的分块编码方式，如图2所示。HEVC编码主要包括帧内预测、帧间预测（运动估计与补偿）、变换量化、去方块滤波&SAO滤波、熵编码等编解码模块。HEVC编码器的工作步骤如下。

步骤 1　视频编码器将输入视频帧划分为互不重叠的编码树单元（CTU, coding tree unit）。

步骤 2　利用视频的空间相关性和时间相关性进行预测编码，分别采用帧内预测和帧间预测去除时空域冗余信息，从而得到预测图像块。

步骤 3　将预测图像块与原始图像块作差得到预测残差块，再对预测残差块进行离散余弦变换和

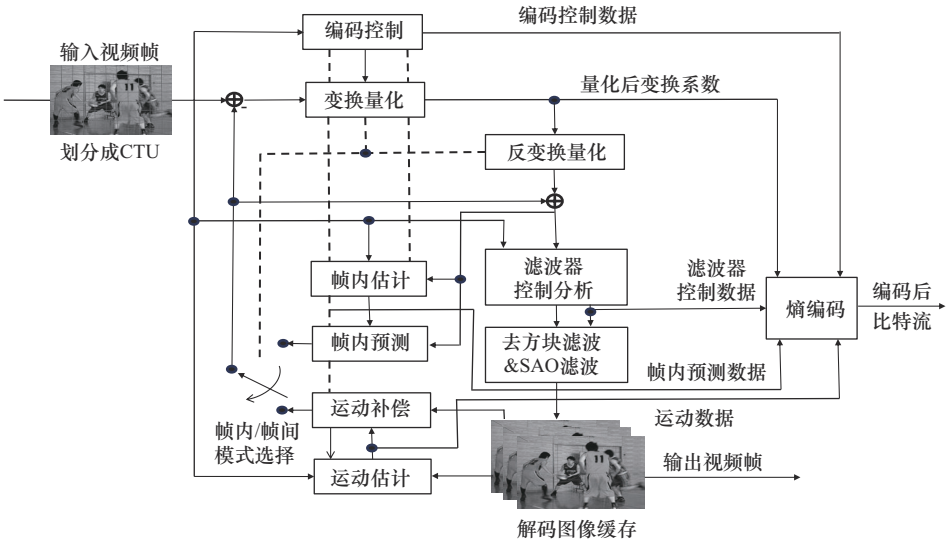


图2　HEVC编码原理和基本结构

量化，获得量化后的离散余弦变换系数。

步骤4 对量化后的离散余弦变换系数进行熵编码，得到压缩码流。

1.2 HEVC编码主要特征

有学者研究表明，若对HEVC的每个环节的编码进行有效改进，就可以节省大约50%的比特率，而且可获得同等质量的视频[2]（特别是对于高分辨率视频）。下面介绍HEVC视频编码所涉及的主要特征。

1) 编码树单元。HEVC引入了编码树单元，其大小由编码器选择，可以大于传统的宏块。CTU由亮度编码块、色度编码块和语法元素组成。亮度编码块尺寸可以为16×16、32×32和64×64，较大的尺寸通常可以实现更好的压缩。HEVC支持使用树形结构将编码块分割成更小的块，以提高编码效率[4]。

2) 编码单元（CU, coding unit）。根据CTU的四叉树语法规定，确定亮度和色度编码块的大小和位置。四叉树的根与CTU相关联，因此亮度编码块的尺寸取决于亮度编码块能够支持的最大尺寸。CTU可以分解成亮度和色度编码块的联合信号，一个亮度编码块和2个色度编码块以及相关的语法组成了一个编码单元。一个编码块可能只包含一个CU，也可能被分割成多个CU，每个CU划分为相关的预测单元和变换单元[5]。

3) 预测单元（PU, prediction unit）。作为进行预测运算的基本单元，其包括帧内预测和帧间预测两类。一个编码单元可以包含一个或多个预测单元，CU到PU仅允许划分一层，最小的PU为4×4。划分可以是对称的或不对称的。一个2*N*×2*N*（*N*可以是4、8、16和32）的CU可划分为8种包含PU的方式。在帧间预测时可以在这8种方式中任意选择，在帧内预测时只允许选择2*N*×2*N*或*N*×*N*种方式。

4) 变换单元（TU, transform unit）。TU是在CU的基础上进行变换和量化的基本单元，同时受所在的PU的限制。如果PU是正方形，则TU也必须是正方形，尺寸大小为4×4、8×8、16×16和32×32。在帧内编码模式中，变换单元的尺寸需小于或等于预测单元；在帧间编码模式中，变换单元的尺寸可以大于预测单元，但不能超过编码单元。一个编码单元中多个变换单元也是按照四叉树的结构排列，即依次将下一层划分为4个小的正方形。如果PU为非正方形，TU也必须为非正方形，其尺寸大小为32×8、8×32、16×4和4×16，可用于亮度分量，其中只有32×8、8×32可用于色度分量。HEVC中允许使用的变换包括4×4、8×8、16×16和32×32整数离散余弦变换以及对帧内预测中4×4亮度块使用的整数离散正弦变换。

5) 运动矢量信号（MVS, motion vector signaling）。使用高级运动矢量预测，根据相邻预测块的数据和参考图片推导出几个最可能的候选运动矢量。除此之外，还可以使用MV编码的合并模式，允许MV从时间或空间上相邻的预测块中继承。因此，相较于AVC，HEVC提出了改进的跳跃和直接运动推断。

6) 运动赔偿。对MVS采用四分之一采样精度，并使用7抽头或8抽头滤波器对分数采样位置进行插值（相比于半样本位置的6抽头滤波），然后对四分之一采样位置进行线性插值。与AVC类似，HEVC采用多参考图像，对于每个预测单元，可以传输一个或2个运动矢量信号，分别产生单预测或双预测编码。

7) 帧内预测。帧内预测是指对未进行帧间预测的区域使用解码得到的相邻块边界样本作为空间预测的参考数据。帧内图像预测支持33种预测模式，加上水平和垂直方向在内共35种预测模式。所选择的帧内预测模式通过基于先前解码相邻预测块的最大可能模式进行编码。与AVC相比，HEVC的帧内图像预测模式数量更多。

8) 量化控制。与AVC一样，HEVC采用了均匀重建量化（URQ, uniform reconstruction quantization），支持不同变换块大小的量化缩放矩阵。

9) 熵编码。HEVC采用了上下文自适应二进制算术编码（CABAC, context adaptive binary arithmetic coding），类似于AVC中的CABAC方案，经过多次改进，提高了吞吐率和压缩性能，并降低了上下文内存需求，特别是对于负载均衡的结构。

10) 环内去方块滤波。为了简化硬件设计和并行处理，HEVC采用环内去方块滤波方法，只对8×8的边界进行滤波，且定义了3个边界强度等级。在滤波前，需要判断每个边界是否需要进行滤波，以及进行强滤波还是弱滤波。这一判决根据穿越边界像素的梯度值和由该块的量化参数导出的门限值

共同决定。HEVC 的环内去方块滤波对所有边界进行统一处理，先对整个图像的所有垂直边界进行水平方向滤波，再对所有的水平边界进行垂直方向滤波。

11) 样值自适应偏移（SAO, sample adaptive offset）。HEVC 在帧间预测环路中引入非线性幅度映射，旨在通过使用查找表更好地重建原始信号的幅值。该查找表由一些额外的参数构成，这些参数可以通过编码器端的直方图分析来确定。

2　常见攻击方法及性能评估指标

攻击者可以尝试各种安全漏洞来破坏加密技术并破译密钥。性能评估指标用于衡量加密技术的有效性[6]。常见视频加密技术的密码攻击方法如下。

差分攻击。该方法用于评估加密对视频图像中细微变化的脆弱性。攻击者稍微更改原始数据，然后对已修改和未修改的图像应用相同的加密方法，以查找这两者之间的关系。

统计分析。该方法将加密数据和原始数据统计信息进行比较，所需的工具为直方图，并对相关系数进行统计分析。

暴力攻击。该方法涉及尝试所有可能的密钥组合，直到找到正确的密钥来破解加密过程中使用的密钥。

明文攻击。在这种攻击中，攻击者掌握了部分或全部的明文及其对应的密文，可以对密码进行更深入的分析和破解。

噪声攻击。在这种攻击中，攻击者向加密的普通多媒体添加噪声，以破坏普通多媒体的可用信息，从而阻止预期的接收者在解密后取回原始数据。

目前，学术界已出现大量的HEVC视频加密方案，不同的HEVC视频加密方案的性能优劣是人们关注的焦点，对其进行比较分析显得极其重要。解密过程中的明文和密钥统计信息至关重要，通过对加密技术的安全性和质量进行分析来检查其稳健性。统计分析、差分攻击、噪声攻击等攻击方法都是安全性分析的类型。质量分析使用峰值信噪比（PSNR, peak signal-to-noise ratio）、计算成本、格式兼容性和比特增幅等性能指标来衡量加密技术的性能[7-8]。常见视频加密技术攻击方法和性能指标如图3所示。

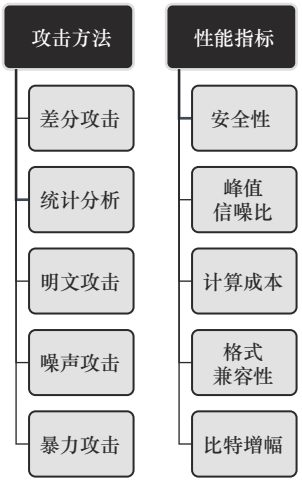


图3　视频加密技术攻击方法和性能指标

视频加密技术性能评估指标详细描述如下。

1) 安全性

加密方案的安全性取决于视频加密过程所采用的密码算法和加密技术。如果采用的视频加密方案不受不同类型密码攻击的影响，则方案安全性更高。视频加密技术的安全性主要通过密钥长度、PSNR、结构相似性（SSIM, structure similarity index measure）、信息熵、算法复杂度、密钥敏感性等性能指标进行评估。信息熵表示视频数据经过加密处理后的随机性和不确定性程度。信息熵越高，表示加密后视频数据的不确定性和随机性越大，加密视频被破解的难度也越大。因此，视频加密后的信息熵越接近理想值8，说明加密算法的安全性越高，对视频数据的保护程度也越高。信息熵可表示为

$$H(I)=-\sum P(i)\mathrm{lb}^{P(i)} \tag{1}$$

其中，$H(I)$表示图像I的信息熵，$P(i)$表示图像I中灰度级别为i的像素点的概率。

2) 峰值信噪比

峰值信噪比是一种衡量图像或视频质量的指标，主要用于评估经过加密后的视频重构质量。通过比较加密视频与原始视频的质量，评估加密算法对视频的保护效果。如果PSNR较小，则说明加密后的视频是具有高度安全性的。PSNR可表示为

$$\mathrm{PSNR}=20\lg\left(\frac{255}{\sqrt{\mathrm{MSE}}}\right) \tag{2}$$

其中，MSE（mean squared error）是视频帧加密前后在每个像素点上差异的平方的平均值，其计算式为

$$\mathrm{MSN}=\frac{1}{hw}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left\|I(i,j)-K(i,j)\right\|^2 \tag{3}$$

其中，I和K分别表示原始视频帧和加密后视频帧，h和w分别表示图像的长和宽。

结构相似性从亮度、对比度和结构3个方面对图像的相似性进行衡量，常与PSNR一起使用来衡量两帧图像间的相似性。这2个指标的值越小，表明两帧图像间变化程度越显著。SSIM可表示为

$$\mathrm{SSIM}=\frac{(2\mu_I\mu_K+c_1)(2\sigma_{IK}+c_2)}{(\mu_I^2+\mu_K^2+c_1)(\sigma_I^2+\sigma_K^2+c_2)} \tag{4}$$

其中，μ_I和σ_I^2分别为原始图像的均值和方差，μ_K和σ_K^2分别为加密图像的均值和方差，σ_{IK}是原始图像和加密图像的协方差，c_1和c_2分别为常数且取值为c_1=0.000 4，c_2=0.003 6。

3) 计算成本

加密方案不应严重影响视频编码的计算处理效率，而应保持较低的计算成本和计算复杂度，处理HEVC视频编解码所耗费的时间不应超过未加密处理太多。

4) 格式兼容性

如果加密后视频的格式被破坏，导致其不能被HEVC解码器解码，无法还原播放，那么加密也就失去了意义。因此加密方案应该保证HEVC格式的兼容性。

5) 比特增幅

视频本身就是一种传输开销较大的数据，加密方案不应大幅度增加视频的数据流量和比特数。比特增幅表示加密处理后视频文件大小相对于加密前视频文件大小的增加百分比。

3　HEVC视频加密研究现状

对于HEVC视频加密技术，国内外学者提出了许多不同类型的加密技术，根据应用加密算法的区域不同，大致可以分为两类[9]。一类是完全加密方法，即使用加密技术对整个视频数据进行完全加密，该方法提供高安全性的加密，但其复杂性很高，一般应用于重要领域，如医学和军事领域；另一类是选择性加密方法，只加密部分区域或者重要语法元素，这样既可以节省计算成本，又可以保证格式兼容性，视频内容在加密操作过程中会略有损坏，但仍可部分恢复，一般用于复杂度较小的系统。

3.1　完全加密方法

完全加密方法是对整个视频进行加密，使得未经授权的用户无法获取任何视频内容。这种加密技术可以保护视频的所有部分，包括图像、声音、元数据等，确保视频内容的安全性和隐私性。

文献[10]提出了一种基于ChaCha20流密码和混合混沌映射的轻量级视频加密方法。该方法旨在利用密码学技术和混沌理论，通过结合ChaCha20流密码和混合混沌映射，对视频进行高效加密处理。在实验过程中，该方法使用动态参考帧分离序列帧之间的变化，然后对生成的视频进行2次加密来缩小视频的大小。实验结果表明，与现有的加密方法相比，所提轻量级加密方法具有更高的安全性和更短的计算时间。

文献[11]提出了一种基于改进高级加密标准（AES, advanced encryption standard）的视频加密算法，克服了传统AES在安全视频存储和传输方面的缺点，降低了加密和解密的复杂度，提高了加密视频的熵，并增强了扩散和混淆操作。算法通过第三代安全散列算法（SHA-3, secure hash algorithm-3）生成混沌映射的初始条件，使用Henon混沌映射生成更具随机性的密钥。实验结果表明，与标准算法相比，混沌与AES相结合的新算法使加密视频的熵增加了15%，降低了视频加密和解密的复杂度，且在安全级别和加密速度之间取得了平衡，为视频安全传输提供了保障。

文献[12]提出了一种基于超混沌和脱氧核糖核酸（DNA, deoxyribonucleic acid）编码的视频加密方案，结合基于稀疏表示的视频数据空间压缩方法，提供了更高的安全性。该HEVC加密方案通过在视频帧上引入稀疏编码帧来提高压缩效率，在稀疏编码帧上采用基于5维超混沌和DNA编码的加密模块，使用全局位加扰方法降低了加密视频帧中相邻块之间的相关性。经过大量实验结果表明，该方案相比其他视频加密算法在效率、质量和安全性方面具备优势，表现出更好的安全性能和混沌性能，同时具备抵御各种攻击的能力。

文献[13]提出了一种基于混沌的多媒体加密系统，使用二维修改模型进行数据的安全传输。该系统采用基于扰动的数据加密技术进行混淆和扩散，使用混合混沌结构进行多媒体数据加密，保证了高水平的加密质量，并具有降低残余清晰度和密钥敏

感度的优点，适用于所有多媒体格式的数据加密。

文献[14]提出了一种在物联网多媒体应用中安全高效地传输 HEVC 压缩视频的新型混合加密系统。该系统结合改进的 Mandelbrot 集、Arnold 混沌映射和 DNA 编码技术，改进了压缩 HEVC 帧的安全功能，可以加密任何大小的 HEVC 帧，具有宽阔的密钥空间，能够承受多种多媒体攻击并抵抗暴力攻击，对提高物联网多媒体应用中视频传输的安全性和隐私性具有重要意义。

文献[15]提出了一种基于混沌映射和 Ikeda 时延微分方程的视频加解密方法。该方法使用混沌映射和 Ikeda 时延系统生成混沌序列，然后将该混沌序列与视频像素进行异或运算，以实现数据加密。另外，该方法结合了一种基于像素置换的视频加密方法，使用离散混沌映射生成的伪随机序列作为置换序列，并将其应用于视频像素置换。通过安全性分析和实验验证，证明了该加密方法的有效性和可靠性。

文献[16]提出了一种基于 Arnold 映射和离散余弦变换的 HEVC 视频编码网络安全框架。该框架采用一种新颖的加密方法将视频帧分为不同的块，然后对每个块进行 Arnold 映射和离散余弦变换，最后将加密后的块合并成完整的视频帧。实验结果表明，该框架在保证视频质量的同时，具有很高的安全性和鲁棒性，可以有效地防止网络攻击和数据泄露。

表 1 总结了上述完全加密方法采用的密码技术、主要特征和不足。从表 1 中可以看到，每种完全加密方法都有其不同的优缺点和性能表现，没有一种完全加密方法能解决所有的视频加密问题，在实际应用中应根据应用场景和加密需求，选择满足需求的视频加密方法。

3.2　选择性加密方法

选择性加密是指在视频加密技术中，对视频内容进行选择性加密，即只对视频中的部分内容进行加密，而其他部分内容保持明文。这种加密方式根据选择加密内容的不同，可以分为基于感兴趣区域的视频加密技术和基于语法元素的视频加密技术，以此满足不同的安全和隐私需求。

3.2.1　基于感兴趣区域的视频加密技术

对视频内容中的特定感兴趣区域进行选择性加密，即基于感兴趣区域（ROI, region of interesting）的视频加密技术。该技术可将视频分为多个单元，通常是图像或视频帧，用户选择性地对其中的某些单元进行加密，保持其他单元为明文。这种加密技术通常应用于对视频内容的特定区域进行保护，如在视频监控系统中，可以对包含敏感信息的区域进行加密，以保护个人隐私。同时，对于一般的视频内容，可以保持为明文，以提高视频的传输效率和解码效率。

文献[17]介绍了一种基于 YOLOv3 和块混淆的监控视频隐私加密技术。该技术可以检测视频中的人脸，使用不同的密钥加密每个 ROI，以保护检测到的人脸边缘，防止关键信息泄露。实验研究表明，这种技术可以有效地保护监控视频中的个人隐私信息，并且表现出良好的性能。因此，该技术有

表 1　　**完全加密方法对比**

文献	密码技术	主要特征	不足
文献[10]	混沌	一种轻量级的流密码视频加密方法，适用于资源受限场合，具有较高的安全性和较短的计算时间	出现噪声和数据丢失时，性能需要进一步分析
文献[11]	混沌 改进 AES	改进的 AES 方法增强了视频加密中的扩散和混淆，使用 Henon 混沌映射生成密钥，缩短了运行时间，提高了系统的适用性和安全性	多轮 Feistel 结构的使用增加了加密时间，不利于嵌入式系统的实时传输
文献[12]	混沌 DNA 压缩感知	结合了 5D 超混沌、DNA 编码和压缩感知的优点，提高了压缩效率和安全性能，表现出更好的混沌特性，具有抵御各种攻击的能力	由于使用了基于块的变换，在重建帧上会出现块效应
文献[13]	混沌	使用混合混沌结构产生置换和扩散的控制参数，提出了一种基于扰动的数据加密技术，保证了高水平的加密质量	在对视频帧加密时没有考虑时间冗余
文献[14]	混沌 DNA	结合了改进的 Mandelbrot 集、Arnold 混沌映射和 DNA 编码技术，可以加密任何大小的 HEVC 帧，具有宽阔的密钥空间，能够抵抗各种攻击	处理时间较长，无法满足实时应用需求
文献[15]	混沌	一种基于 12D 混沌映射和 Ikeda 时延微分方程的视频加解密方法，在随机性、混合性、遍历性和对初值敏感性表现良好，对各种威胁均有鲁棒性	加密时间较长和格式不兼容
文献[16]	混沌	一种基于 Arnold 映射和离散余弦变换的 HEVC 视频编码网络安全框架，具有很高的安全性和鲁棒性，可以有效地防止网络攻击和数据泄露	有待进一步分析在抗噪声和统计攻击上的性能

望在监控视频处理领域得到广泛应用。

文献[18]提出了一种基于HEVC压缩的ROI加密方案，能够在保持视频质量的同时对ROI进行有效加密。该方案对ROI内所有的HEVC语法元素使用AES算法进行比特层面的加密，在压缩域中对ROI进行选择性加密，并且在实验中证明了该方案的有效性和性能优势。该方案ROI的PSNR平均值不超过11.5 dB，加密后ROI内视觉质量急剧下降，无法识别内容细节。但同时加密会导致ROI内的解码器不同步，破坏格式的兼容性。

文献[19]提出了一种在HEVC压缩视频中进行感兴趣区域选择性加密的方法。该方法首先将整个视频分成多个块，并根据块的重要性进行分类。然后，对于ROI中的块，采用一种基于混沌理论的加密算法进行加密，能够提供较高的安全性和抗攻击性。实验结果表明，该方法能够在保证视频质量的同时，有效地保护ROI的安全性，但是会降低高分辨率视频的视频质量，也可能导致生成的视频格式不兼容HEVC。

文献[20]提出了一种基于HEVC中ROI的端到端实时加密方案。首先采用符合HEVC语法元素格式的方式对一组HEVC参数进行加密，保持加密后视频的比特率不变。然后对帧内预测模式进行加密，帧内预测模式分为3组，每组包含相同扫描方向的预测模式。最后使用循环移位操作执行加密过程，利用混沌伪随机数生成器生成加密过程所需的5位比特流。该方案加密后视频质量明显下降，ROI内的平均PSNR保持在11.4 dB以下，但相应的帧间编码速度下降明显，平均速率损失达到9.81%。

文献[21]提出了一种基于编码单元的HEVC视频ROI加密方法。该方法通过选择性加密具有显著视觉影响的参数，如帧内预测模式、运动矢量、运动矢量符号、变换系数和变换系数符号等，实现选择性视频加密，提高加密速度并保持编码效率，且通过限制参考区域来保留ROI周围的内容。然而在实际应用中，需要根据具体性能指标来评估加密方法的性能。

文献[22]提出了一种基于混沌流密码的选择性加密方案，用于高效视频编码中感兴趣区域的安全加密。该方案通过对感兴趣区域内的一组HEVC语法元素进行规范加密，使得比特流可以通过标准的HEVC解码器解码，而ROI解密只需要一个密钥。实验结果表明，该选择性加密方案在实时环境下能够实现安全的视频加密，并且具有较小的比特率和较低的计算复杂度。

以上基于感兴趣区域的视频加密技术在加密后的ROI内视频信息模糊性高，计算成本低，能满足实时应用场景的需求，但是整体安全性低，可能会导致格式不兼容。基于感兴趣区域的视频加密技术对比如表2所示。

表2 基于感兴趣区域的视频加密技术对比

文献	密码技术	安全性	PSNR	计算成本	格式兼容性	比特增幅
文献[17]	混沌	高	高	中	是	高
文献[18]	AES	高	高	中	否	低
文献[19]	混沌	高	高	低	否	低
文献[20]	混沌	高	高	低	是	中
文献[21]	AES	高	低	中	是	低
文献[22]	混沌	高	低	低	是	低

3.2.2 基于语法元素的视频加密技术

选择性加密方法对编码过程中一些重要的语法元素进行加密，即基于语法元素的视频加密技术。该技术通常能保持格式兼容性，确保能由标准HEVC解码器解码。加密后解码的视频会产生失真，非授权访问用户无法从中获取有效信息。根据目前加密方案中主要加密语法元素的不同，可将基于语法元素的视频加密技术大致分为3类，即基于帧内预测模式、基于运动矢量差和基于熵编码过程的视频加密方案[23]。

当然，选择基于某一种语法元素的加密方案通常无法满足视频加密性能的需求，因此不少学者对HEVC编码视频中的不同阶段、不同类型语法元素进行了加密。文献[24]为了在保持相同比特率的情况下提高安全性，选择运动矢量参数、残差信息、量化参数、合并模式索引、参考帧索引和边缘滤波参数组合进行加密，能保持格式兼容性并取得了很好的安全性能。文献[25]采用AES加密算法对语法元素运动矢量差的符号和值、合并模式索引、参考帧索引、运动矢量预测索引进行加密，在符合HEVC编解码标准的前提下，保证了一定的加密安全性，但比特率有所增加。

基于语法元素的视频加密技术[26-61]通常需要结合实际应用场景有针对性地对视频内容进行加密，

在加密复杂度和安全性能之间达到一定的平衡，如表 3 所示，其中，—表示原文未提及或未证实，下面将详细介绍。

方案 1　基于帧内预测模式的视频加密方案

帧内预测是根据转换块的大小进行操作，并使用之前从空间相邻的多个转换块中解码的边界样本来形成预测信号。如图 4 所示，对于从 4×4 到 32×32 的转换块大小，总共定义了 35 个不同的帧内预测模式方向。除图 4 中给出的 33 个不同方向的帧内预测模式外，还包括平面预测模式 0 与直流预测模式 1。每个帧内编码对亮度都会有一个帧内预测模式，对色度则有另一个帧内预测模式。

一个预测单元内所有的变换单元会对每个分量使用相同的预测模式。编码器会从 35 个方向中选

表 3　　基于语法元素的视频加密技术对比

文献	加密方案	加密元素	密码技术	安全性	PSNR	计算成本	格式兼容性	比特增幅
文献[27]	基于帧内预测模式	帧内预测模式、运动矢量差、合并模式索引、参考帧索引、运动矢量预测索引、残差值和样点自适应偏移参数	AES	高	高	高	是	低
文献[29]		帧内预测模式、空间信息和运动矢量信息	AES/RSA	高	—	高	是	低
文献[30]		帧内预测模式和交流系数符号	AES	高	—	高	否	高
文献[31]		帧内预测模式	秘密共享	中	低	低	否	低
文献[32]		帧内预测模式、运动矢量差和量化变换系数	AES	中	高	高	否	中
文献[33]		帧内预测模式、运动矢量差和量化变换系数	RC4	高	低	高	是	中
文献[34]		亮度帧内预测模式和离散余弦变换系数符号	AES	高	低	低	是	低
文献[38]	基于运动矢量差	运动矢量差、量化参数变化量和变换系数	AES	中	高	低	是	低
文献[39]		运动矢量差	AES	高	低	低	是	低
文献[40]		运动矢量差符号、量化变换系数符号和帧内预测模式	Rabbit	中	高	低	是	高
文献[41]		运动矢量差符号、运动矢量差幅值、亮度残差系数符号和色度残差系数符号	RC4	高	低	低	是	低
文献[42]		运动矢量差和离散余弦变换系数符号	RC6	低	中	高	是	低
文献[43]		运动矢量差符号、运动矢量差绝对值的后缀、变化系数符号和量化参数绝对值增量	AES	高	中	中	是	低
文献[44]		运动矢量差符号和残差系数符号	RC4	低	高	中	是	中
文献[45]		运动矢量差和残差值	AES	中	中	低	是	低
文献[46]		运动矢量差符号和交流系数符号	哈希	中	高	低	是	低
文献[47]		运动矢量差的符号和值,离散余弦变换系数的符号和后缀、量化系数的符号和后缀	混沌	高	高	中	是	低
文献[48]		运动矢量差符号和离散余弦变换系数符号	混沌	高	高	中	是	低
文献[49]		量化变换符号、运动矢量差符号和运动矢量差	RC4	高	高	中	是	低
文献[51]	基于熵编码过程	运动矢量差符号、非零变换系数和纹理值符号	流密码	中	中	中	是	低
文献[53]		变换系数、变换系数符号、运动矢量差、运动矢量差符号和量化参数符号	混沌	高	高	低	是	低
文献[56]		量化变换系数符号、前缀和后缀	AES	高	低	中	是	低
文献[57]		运动矢量差和离散余弦变换系数的符号	混沌	高	中	中	是	低
文献[58]		运动矢量差符号、非零变换系数的符号及其绝对值后缀	SLEPX	高	低	低	是	低
文献[59]		运动矢量差的符号和值、离散余弦变换系数的符号和值、量化参数的变化量、样点自适应偏移参数、参考帧索引和残差值	RC6	高	高	低	是	低
文献[60]		亮度帧内预测模式、运动矢量差符号和值、运动矢量预测索引、样点自适应偏移参数、参考帧索引、合并模式索引、残差符号和值	AES	高	高	高	是	低
文献[61]		运动矢量差符号位、变换系数符号位量化参数后缀以及变换系数后缀	Blowfish	中	高	低	是	低

择最优的亮度帧内预测模式。对于帧内编码预测单元的色度分量，编码器直接在平面、直流、水平、垂直和亮度帧内预测这5种预测模式内选择最优的色度帧内预测模式[26]。

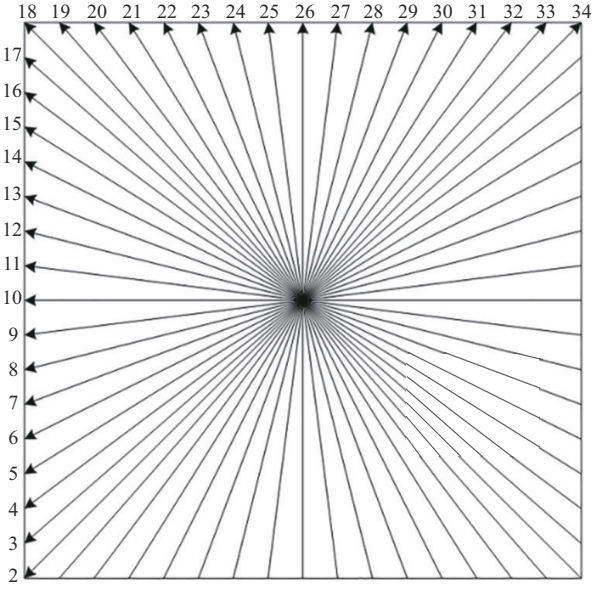


图4　帧内预测模式的方向

文献[27]提出了一种基于色度帧内预测模式和置乱系数的加密方案。首先利用AES算法生成伪随机序列，然后用生成伪随机序列对HEVC编码过程中的预测、残差和重构信息进行加密。通过旁路模式对CABAC的语法元素进行加密。同时常规模式下的一些色度帧内预测语法元素也被加密。采用置乱系数提取每一帧的边缘信息，对包含变换单元的系数进行置乱。最后，将用于标记每个变换单元类型的符号嵌入置乱系数中。该方案的优点是在加密的语法元素较多的情况下，加密后的视频帧产生高度失真，同时加密视频比特增幅较小，平均值为8.978%。并且使用AES算法的安全性较高，加密空间大，能保持良好的格式兼容性；缺点是加密较多的语法元素，增加了数据量，导致加密时间增加。

文献[28]提出了一种基于帧内预测的视频加密和隐写技术。首先结合编码单元和预测单元的编码信息提出了一种覆盖选择规则，将所有4×4预测单元分为两类，分别为均匀的4×4预测单元和非均匀的4×4预测单元。如果一个8×8的编码单元中包含的4个4×4预测单元具有相同的帧内预测模式，则将这4个预测单元归类为均匀的4×4预测单元；否则，归类为非均匀的4×4预测单元。通过实验对比，均匀的4×4预测单元只占很小部分，最高不超过8%，这意味着忽略均匀的4×4预测单元的帧内预测模式对该规则的容量没有显著影响。具体步骤如下。

步骤1　从原始视频流中读取一帧，然后执行HEVC编码器的默认压缩过程以压缩当前帧。

步骤2　获取编码单元深度信息、预测单元分区模式和帧内预测模式，选取合适的块作为候选嵌入块。

步骤3　通过由私钥控制的伪随机序列来选择候选嵌入块的位置。

步骤4　获取秘密信息，并将每2 bit组合在一起，秘密信息被另一个私钥置乱。

步骤5　使用矩阵编码将秘密信息W_1和W_2嵌入每组候选嵌入块中，并记录需要修改帧内预测模式块的位置。

步骤6　重复执行步骤5，直到所有组将信息嵌入其中。

步骤7　获取步骤5中块的修改模式的记录，并使用修改后的帧内预测模式重新编码当前帧。

步骤8　返回步骤1，直到最后一帧结束。

该加密方案可以保证视频格式兼容性和安全性，缺点是作者没有给出用于加密的密码技术，这对于加密方案的计算成本来说非常重要。另外，修改预测单元的帧内预测模式也会造成一定程度的比特增幅。

文献[29]使用了改进的AES-256和RSA（Rivest Shamir Adleman）算法，对帧内预测模式、空间信息和运动矢量按顺序进行加密操作。该方案保证了HEVC视频编码格式的兼容性，改进AES和RSA算法的加密处理时间缩短4.76%，同时视频比特增幅控制在0.72%，适用于移动用户与云平台之间进行安全的数据交换。但是缺点在于对I帧压缩率较低，使得加密和解密的计算时间和网络时延增加，同时增大了计算成本。

文献[30]提出了一种使用AES-256密码算法对HEVC帧内编码信息进行加密，允许在大范围的量化参数下进行透明加密，并对直流系数符号进行加密。该方案使用的AES-256密码算法能保证视频内容的安全性，通过评估质量退化和对攻击的鲁棒性评估算法适用性，但同时计算开销大，耗费时间

较长。

文献[31]结合帧内和帧间数据的加密提出了一种基于秘密共享的视频加密方法，利用 Shamir 秘密共享方案对离散余弦块和运动矢量块进行加密，通过与随机生成的伪随机序列进行异或运算的方式加密。实验结果表明，该视频加密算法具有扩展性，适用于对视频数据进行加密。

文献[32]提出了一种用于在能量受限的物联网多媒体中的低开销 HEVC 加密方案。该方案根据每一帧的结构、纹理和运动能量来调整要加密的语法元素的选择。首先计算量化变换系数和运动矢量差的能量级，并与自适应阈值进行比较，对每个视频帧的能量级进行分类。当出现高能量帧时，所有的语法元素会被加密；当出现低能量帧时，将对替代语法元素进行加密，实现低加密开销。此外，在变换系数中，为了抵御变换系数插值攻击，将帧与其相邻系数关联后对交替系数进行加密。最后，在熵编码阶段，对每一帧的编码单元结构进行组合加密置换。该方案能有效抵御蛮力攻击、变换系数插值攻击和替换攻击，但计算成本高，影响格式兼容性并且比特率略有增加。

文献[33]提出了一种鲁棒的选择性加密方案。该方案将视频编码分为多个切片，使用 RC4（Rivest cipher 4）流密码对每个切片进行独立加密，设计了 2 轮移位算法对变换单元的非零系数进行置乱，然后选择帧内预测模式、运动矢量差和量化变换系数进行加密。这种加密方案能够在丢包情况下正常解密，并支持在线实时交互。通过实验证明，该方案具有格式兼容性、高安全性和低计算复杂度，因此被认为是一种非常有前景的视频加密方法。

文献[34]提出了一种多级加密方案，包括轻量级、中量级和重量级加密。该方案使用 AES-CTR（AES-counter）模式生成伪随机序列，对 HEVC 编码过程中的主要语法元素进行加密。在轻量级加密层面，选择亮度帧内预测模式进行加密；在中量级加密层面，利用离散余弦变换系数符号进行置乱加密；在重量级加密层面，亮度帧内预测模式和离散余弦变换系数符号同时被伪随机序列加密。实验结果表明，在每个加密级别中都存在不同数量的视觉信息，用户可以根据需求灵活地选择加密级别。

文献[35]提出了一种基于 4 种适配算法和 HEVC 内部编码器的完全并行硬件架构，支持 35 种帧内预测模式，所有编码树单元分区在 4 个预测引擎中独立处理，以实现高并行性。该架构为每个预测引擎分配了一组适当的内部预测模式、远程数据对象候选项和 CABAC 速率估计实例，最大限度地提高处理吞吐量。与其他设计方案相比，该设计方案在计算复杂度、比特率、视频质量、吞吐量、可靠性和灵活性方面表现出优势。

林志坚等[36]设计了一种新的基于帧内率失真优化预测模式的并行流水线硬件架构方案，支持最大 64×64 编码树单元的帧内预测编码。该方案包含 9 路并行预测模式，按照 Z 型扫描顺序实现以 4×4 块为基本处理单元的流水线硬件架构，并复用 32×32 预测单元的预测数据，代替 64×64 预测单元的预测数据，减少运算量。为实现高效的流水线处理，该方案提出了一种新的哈达玛变换电路，与已有设计方案相比，能够用更小的电路面积实现更高帧率的 1 080P 实时视频编码。

公衍超等[37]提出了一种帧内码率控制算法，能够有效提高视频感知率失真性能。通过结合空时域复杂度设计视频主观观测实验，度量视频的空时域复杂度，结合人类视觉系统相关感知特性，构建能够有效衡量人眼对视频不同区域感知差异性的视频内容空时域感知敏感因子，将空时域感知敏感因子运用到帧内图像最大编码单元层目标比特分配中，实现感知帧内码率控制。实验结果表明，在比特预测准确度和感知率失真性能 2 个核心指标上，所提算法均明显优于 HEVC 采用的码率控制算法。

方案 2　基于运动矢量差的视频加密方案

在大多数视频序列中，相邻图像帧内容非常相似，其背景画面变化极小，一次不需要对每幅图像帧的全部信息进行编码，而是将当前图像帧中运动物体的运动信息传给解码器，利用运动矢量差就可以恢复当前图像帧，这样可以有效减少比特率。HEVC 中提出了自适应运动矢量预测技术，利用空域和时域上运动矢量的相关性，为当前预测单元建立候选预测运动矢量列表，编码器从中选择最优的预测运动矢量。为了进一步减少编码比特数，采用残差编码，即只对当前运动矢量和预测运动矢量的差值进行编码，这个差值就是运动矢量差。当加密运动矢量差时，如果采用的方案不合适，将会导致视频格式被破坏，影响格式兼容性。因此，大多数

加密方案通过将运动矢量差的符号与其他语法元素相结合进行加密。

文献[38]提出了一种基于HEVC选择性加密方法的格式兼容加密框架，根据格式兼容加密的有效性原则和独立性原则，采用比特翻转和比特插入删除方法，用AES算法对运动矢量差、量化参数变化量和变换系数进行加密，实现了对编码比特流的格式兼容加密，保证了基本性能和安全需求，所提格式兼容加密框架在实际应用中具有较高的价值。

文献[39]提出了一种在HEVC中对运动目标进行加密的方案。该方案对视频内容中的移动对象进行了选择性加密，选取运动矢量差的垂直数据，采用AES算法进行加密。该方案仅对视频序列中的运动对象进行保护，会跳过静止对象，如果待加密视频中的运动对象在时域和空域上联系不紧密，则加密效果就会大打折扣。如果加密数据很小，如只有运动矢量差的标志位或者变换系数的符号，则加密数据容易受到蛮力攻击。但同时，该方案在计算成本、时间消耗、格式兼容性和比特增幅方面表现良好，对不同分辨率视频均能使用。

文献[40]提出了一种HEVC视频交换加密和数据隐藏方案。该方案对量化变换系数符号和运动矢量差符号使用基于Rabbit的流密码进行加密，对帧内预测模式的符号分4种情况进行取模运算操作，并根据莱斯参数的值分5种情况对残差绝对值的二进制串进行数据嵌入。该方案能使视频内容在加密后被极大扭曲，有较高的安全性；将产生符合HEVC视频格式的比特流，确保了格式兼容性；在加密过程中只使用异或运算和模运算，保证了较低的计算成本。缺点在于加密后的视频比特增幅较大。

文献[41]提出了一种基于RC4算法的HEVC感知加密方案。该方案基于RC4构造了一种密钥流生成方法，可以调节密钥流中“1”和“0”的比例，对运动矢量差符号、运动矢量差幅值、亮度残差系数符号和色度残差系数符号4种语法元素进行了选定密钥流的加密。该方案具有加密空间大、计算成本低、不增加比特率和保证格式兼容性的优点，但在加密比例不高时，视频加密效果不佳。

文献[42]提出了一种基于RC6分组密码的HEVC部分加密技术，主要加密了离散余弦变换系数符号和运动矢量差，与使用高级加密标准的HEVC部分加密算法进行了比较，并介绍了其安全性分析，包括加密质量测试、密钥空间测试、统计分析和密钥敏感性分析等实验。实验结果证实了该技术的安全性、可靠性和稳健性。该技术能保证与不加密视频的编码时间几乎相同，同时在比特增幅和格式兼容性方面表现良好，缺点是计算成本较高。

文献[43]提出了一种高效的格式兼容的加密方案。该方案选择视频重构中最重要的语法元素进行加密，并保证加密后的比特流能与HEVC编码标准相互兼容，对运动矢量差符号、运动矢量差绝对值的后缀、变化系数符号与量化参数绝对值增量使用AES进行加密。该加密方案不用修改HEVC标准解码器的结构，便能保证加密后视频的格式兼容性。但需要在安全性和计算成本之间进行权衡，当安全性作为首要考虑因素时，计算成本就要相应地增加。

文献[44]提出了一种用于HEVC的可分离可逆数据隐藏加密方案。在编码阶段，利用RC4密钥流对运动矢量差符号和残差系数符号进行加密，并将数据隐藏到非零的交流剩余系数中。该加密方案具有良好的感知安全性，且加密空间足够大，可以有效抵挡对视频内容进行暴力攻击。在保证视频内容得到保护的同时还可以完成数据嵌入，并且能保证格式兼容性。缺点是需要完成加密和嵌入数据，增加了计算成本和复杂度。

文献[45]提出了一种在恒定比特率下的HEVC视频选择性加密方案。该方案加密算法使用密码反馈模式下的AES，加密了一组HEVC语法元素，包括运动矢量差和残差值。加密是在CABAC熵编码之后进行。此外，该文还提出只加密变换系数后缀的算法，加密后不影响自适应参数，满足恒定比特率和格式兼容性。该方案可以以较低的计算成本实现所需安全性，能保证格式兼容性和很小的比特增幅。

文献[46]提出了一种利用HEVC编码结构中的变换跳跃信号、运动矢量差和剩余系数符号进行选择性加密的方案。该方案中截断莱斯码上下文保持不变，采用此方法生成的加密比特流能保证格式兼容性。同时计算成本低，但加密的效果在不同视频帧中存在差异，部分加密性不能达到要求，加扰效果有限。

文献[47]提出了一种基于耦合映像格子混沌系统的HEVC算法，利用耦合映像格子混沌系统生成流密码，并对HEVC种的不同语法元素进行加密操作，包括运动矢量残差的符号和值、离散余弦变换系数的符号和后缀、量化系数的符号和后缀等。实验结果表明，系统生成的流密码通过了SP800-22Revla测试，具有较强的随机性。与其他混沌系统加密方案相比，该加密方案具有更优的安全性、加密时间和加密效率。

文献[48]提出了一种基于水印和选择性加密鲁棒混合技术的选择性网络安全HEVC框架。该框架利用离散小波变换中的同态变换和奇异值分解来提高嵌入水印的HEVC码流对攻击的免疫能力。同时，采用Logistic混沌映射对运动矢量差符号和离散余弦变换系数符号位进行加密，以较低的加密开销提供符合HEVC格式的特性。对该框架进行了广泛的安全性调查，结果显示选择性网络安全HEVC框架对HEVC序列传输的有效性令人满意。然而，该框架并未实现对HEVC安全算法认证工具的构建。

文献[49]提出了一种改进的交换加密和数据隐藏方案，该方案可以完全保持HEVC视频的码率。为了实现交换属性，将一组语法元素用于加密，另一组语法元素用于数据隐藏。选择性加密的目标是加密量化变换符号、运动矢量差符号和运动矢量差，对HEVC视频的格式兼容性和码率没有影响。为数据嵌入设计了一种改进的系数修正技术，从而提高了数据嵌入能力。此外，无论视频是在加密还是在解密中，都可以执行数据提取操作。安全性分析结果表明，该方案能够实现感知安全和密码安全。然而，该方案的嵌入率和失真性能有待提高。

方案3　基于熵编码过程的视频加密方案

HEVC视频编码标准中只采用一种熵编码器，即基于上下文的自适应二进制算数编码器。HEVC的CABAC熵编码流程与H.264基本类似，主要包括二进制化、文本模型选择、概率估计和二进制算术编码，但HEVC在概率估计精确度和自适应速度加快等方面进行了改进。它基于统计模型和上下文信息，将视频数据转换为二进制码流，并根据上下文信息来自适应地调整编码概率，以提高编码效率。在视频加密中，CABAC可以用于对视频数据进行加密，以保护视频内容的安全性和隐私性。HEVC-CABAC包括以下4个步骤[50]。

步骤1　二值化。非二进制形式语法元素将被转换成二进制形式，用于转换的有5种基本编码树结构，分别为一元码、截断一元码、截断莱斯码、k阶指数哥伦布编码和定长编码。

步骤2　上下文模型。上下文模型是二值化符号的一个或多个比特的概率模型，它依据最近编码的数据符号的统计分布从可用的模型中进行选择。

步骤3　算术编码。算术编码器按照所选的概率模型对每个bin进行编码。

步骤4　概率更新。所选的上下文模型基于实际编码值进行更新。

文献[51]提出了一种基于CABAC的透明加密和可伸缩视频通信方案。在确保格式兼容性和压缩视频比特流的前提下，选择性加密熵编码过程中的参数。该加密方案提出了2种方法：方法1选择运动矢量差符号、非零变换系数和纹理值符号3个语法元素的二进制串和伪随机数生成器生成的随机序列进行异或加密[52]；方法2使用相同的选择性加密，但不加密I帧和P帧，只加密B帧。该方案的2种方法在格式兼容性和计算复杂度上都表现良好，但在安全性方面表现不佳，能够明显识别加密视频的部分内容。

文献[53]提出了一种基于可扩展HEVC的选择性加密方案。该方案对包括变换系数、变换系数符号、运动矢量差、运动矢量差符号以及量化参数符号在内的5种语法元素进行加密，在CABAC编码后的二进制串层面进行加密，并使用混沌加密系统作为流密码使用的序列生成器，可以动态地对重要语法元素进行加解密，不用额外占用内存和增加时延[54-55]。

文献[56]提出了一种在CABAC熵编码模块中对截断莱斯码和k阶指数哥伦布编码进行加密的方案。采取在HEVC的CABAC熵编码模块中进行结构保持的选择性加密，使用AES密码算法在密码反馈模式下，以上下文感知的方式对二进制串的明文进行加密，加密后具有相同的比特增幅和格式兼容性。

文献[57]提出了一种利用低复杂度混沌映射对视频熵编码阶段的运动矢量差和离散余弦变换系数的符号进行加密的方案。该方案利用给定密钥生成逻辑混沌的随机参数值，利用逻辑混沌映射加密系

统生成伪随机比特流，将离散余弦变换系数的符号和运动矢量差分别与生成的伪随机比特流进行XOR操作。实验表明，该加密方案具有计算复杂度低、编码时间快、比特率恒定和格式兼容性的优点。

文献[58]提出了一种基于置换和异或的轻量级对称密码（SLEPX, symmetric cipher for lightweight encryption based on permutation and XOR）方案，简称可扩展HEVC标准，通过选择CABAC编码器的非零值-总量级别符号和后缀的绝对值进行选择性加密。实验结果表明，该方案在视觉保护方面与AES一样安全，而计算效率与基本的异或加密相当。视觉质量评估和安全性分析表明，该HEVC视觉保护方案相对于以前使用的密码技术更具有效性。

文献[59]在HEVC的CABAC编码过程中，使用低计算量的RC6算法对非零离散余弦变换系数的符号、运动矢量差的符号、离散余弦变换剩余绝对值后缀、运动矢量差绝对值后缀、样本自适应偏移参数、残差值、参考帧索引等语法元素进行加密。直方图分析、相关系数测试和密钥敏感性测试等安全性分析结果证明，HEVC-CABAC选择加密算法能够抵御暴力破解和统计攻击，具有较高的安全性，可用于实时HEVC视频应用中。

文献[60]提出了一种针对HEVC中CABAC码流的选择性加密方法，选择对解码视频数据的视频质量影响较大的亮度帧内预测模式作为加密对象，改善了I帧的失真，但没有考虑边缘区域的保护，视频中物体的轮廓仍然可以被识别，主要解决了内容保护的安全问题，改善了视觉的失真。但基于正则模式处理语法元素的加密，显示出压缩效率的损失，同时增加了一定的系统性能开销。

叶清等[61]提出了一种基于HEVC视频编码标准的视频选择性加密方案，防止实时视频信息被非法获取，选择熵编码过程中对运动加密影响较大的运动矢量差符号位、变换系数符号位量化参数后缀以及变换系数后缀等语法元素，在此基础上，运用Blowfish加密算法对视频图像进行选择性加密。实验结果表明，该方案在对视频视觉信息产生极大扰乱的同时，能保证视频的格式兼容性、加密视频的安全性和视频编码的高效性。

基于语法元素的不同视频加密方案性能分析是评估视频加密方案在保护视频内容安全的同时对性能的影响程度。为说明不同视频加密方案安全性能，选取部分文献加密方案的PSNR、SSIM、密钥长度和信息熵4个指标进行数值比较，如表4所示。

通过对选择性视频加密方案的性能分析，可以帮助用户选择适合自己需求的加密方案，平衡安全性和性能之间的关系，提高视频内容的安全性和用

表4 基于语法元素的视频加密方案数值对比

文献	加密技术	PSNR/dB	SSIM	密钥长度	信息熵	序列
文献[27]	基于帧内预测模式	12.24	0.118	2^{128}	7.839	PartyScene
文献[32]	基于帧内预测模式	10.21	0.341	2^{128}	—	ParkScene
文献[33]	基于帧内预测模式	11.911 8	0.105 4	2^{256}	7.862 1	PartyScene
文献[34]	基于帧内预测模式	11.493 8	0.504	2^{256}	7.544 8	Akiyo
文献[39]	基于运动矢量差	20.76	0.47	2^{256}	7.277 1	ParkScene
文献[40]	基于运动矢量差	12.836 5	0.932 3	2^{128}	—	Football
文献[42]	基于运动矢量差	8.69	0.044	2^{128}	7.288 8	Fourpeople
文献[44]	基于运动矢量差	9.92	0.116	2^{128}	—	PartyScene
文献[47]	基于运动矢量差	12.49	0.574 1	2^{256}	—	FourPeople
文献[48]	基于运动矢量差	10.59	0.236	—	6.930 3	Bospharous
文献[49]	基于运动矢量差	12.887 7	0.328 8	2^{128}	—	Football
文献[51]	基于熵编码过程	16.651 8	0.377 7	2^{128}	—	Football
文献[57]	基于熵编码过程	8.25	0.011 1	2^{256}	7.563	FourPeople
文献[58]	基于熵编码过程	13.693 7	0.423 2	2^{128}	—	FourPeople
文献[59]	基于熵编码过程	12.606 7	0.011 08	2^{128}	7.308 7	FourPeople
文献[60]	基于熵编码过程	11	0.45	2^{128}	—	Vidyo1

户体验。综上所述，选择性视频加密方案性能分析如图5所示，有以下特点。

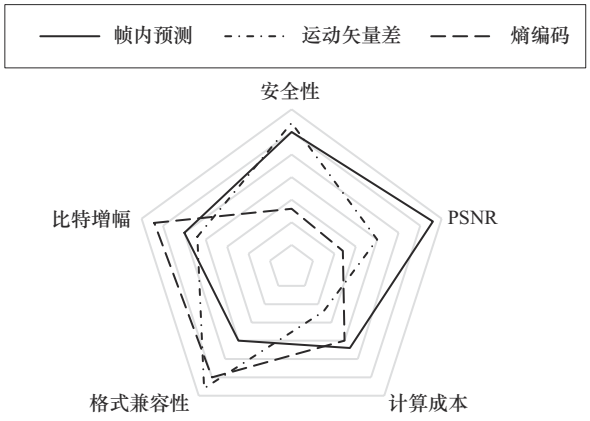


图5　选择性视频加密方案性能分析

1) 基于帧内预测模式的加密方案在安全性和PSNR上表现良好。由于加密的数据量较少，比特增幅低，但同时该类方案对替换攻击敏感。

2) 基于运动矢量差的加密方案不影响比特增幅，安全性高且能保证格式兼容性。但在应用场景需要更高视频信息模糊性时，比特增幅和计算成本均会增高。

3) 基于熵编码的加密方案是在CABAC二进制串中进行的，加密后的二进制串跟未加密的二进制串长度相同。因此，比特增幅不发生改变，格式兼容性也能够保持，但部分方案在PSNR和安全性上表现不佳。

4　HEVC视频加密技术发展趋势

上述基于HEVC标准的加密技术各有优缺点，单个方案很难满足所有性能参数要求。因此目前提出的加密方案都根据实际应用的需求，在各项性能参数上采取折中和有所取舍。未来视频加密技术将着重于视频编码技术和加密算法，包括以下几个方面。

1) 采取压缩率更高、性能更好的视频编码技术。目前，新一代H.266/VVC的视频编码标准已经公布[62-63]，快速、简易地实现从HEVC到VVC转码将成为一个新的研究热点[64-65]。

2) 目前，视频加密领域使用较多的加密算法有AES、RC4和混沌系统伪随机数等。由于视频文件数据量大，故采用加密算法运算速度极为重要，神经网络与深度学习等加密算法在运算速度和安全性方面均表现突出，具有良好的应用前景[66-67]。

3) 将更加先进的视频编码技术和加密算法高效结合，根据应用场景设计出具备实时性、智能化和轻量级的加密方案，将是未来视频加密研究的主要方向[68-69]。

4) 人工智能和5G不仅增强了数据计算和分析，还为新产品和新服务提供了数据互联。因此，能够反映真实场景三维信息的沉浸式视频应运而生，作为高效视频编码标准的扩展，3D-HEVC愈发引起广大学者的注意[70-71]。

5　结束语

本文综述了基于HEVC视频加密标准的加密方案，重点介绍了基于重要语法元素的选择性视频加密技术，并从安全性、峰值信噪比、计算成本、格式兼容性以及比特增幅5个方面进行了评估和比较。结果表明，单个方案难以做到面面俱到，不能在所有性能指标上令人满意。因此，HEVC视频加密算法的选择应该取决于需要应用的场景，通过牺牲部分指标来满足整体的需求是当下最好的选择。对于研究人员而言，设计一种能在这5个性能指标上同时表现良好的加密方案是未来的研究方向。

参考文献：

[1] WIEGAND T, SULLIVAN G J, BJONTEGAARD G, et al. Overview of the H.264/AVC video coding standard[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(7): 560-576.

[2] SULLIVAN G J, OHM J R, HAN W J, et al. Overview of the high efficiency video coding (HEVC) standard[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2012, 22(12): 1649-1668.

[3] BROSS B, WANG Y K, YE Y, et al. Overview of the versatile video coding (VVC) standard and its applications[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 31(10): 3736-3764.

[4] SAMET H. The quadtree and related hierarchical data structures[J]. ACM Computing Surveys, 1984, 16(2): 187-260.

[5] NI C T, HUANG Y C, CHEN P Y. A hardware-friendlyand high-efficiency H.265/HEVC encoder for visual sensor networks[J]. Sensors, 2023, 23(5): 2625.

[6] MUSTAFA A, HENDRAWAN. Secure HEVC video by encrypting header of wavefront parallel processing[C]//Proceedings of the 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). Piscataway: IEEE Press, 2017: 1-4.

[7] HOSNY K M, ZAKI M A, LASHIN N A, et al. Multimedia security using encryption: a survey[J]. IEEE Access, 2023, 11: 63027-63056.

[8] QIAO L, NAHRSTEDT K. A new algorithm for MPEG video encryption[C]//Proceedings of the First International Conference on Imaging

Science System and Technology. Piscataway: IEEE Press, 1997: 21-29.

[9] SHAH J, SAXENA V. Video encryption: a survey[J]. arXiv Preprint, arXiv: 1104.0800, 2011.

[10] MAOLOOD A T, GBASHI E K, MAHMOOD E S. Novel lightweight video encryption method based on ChaCha20 stream cipher and hybrid chaotic map[J]. International Journal of Electrical and Computer Engineering (IJECE), 2022, 12(5): 4988.

[11] HAFSA A, FRADI M, SGHAIER A, et al. Real-time video security system using chaos-improved advanced encryption standard (IAES)[J]. Multimedia Tools and Applications, 2022, 81(2): 2275-2298.

[12] KARMAKAR J, PATHAK A, NANDI D, et al. Sparse representation based compressive video encryption using hyper-chaos and DNA coding[J]. Digital Signal Processing, 2021, 117: 103143.

[13] SETHI J, BHAUMIK J, CHOWDHURY A S. Chaos-based uncompressed frame level video encryption[C]//Proceedings of the Seventh International Conference on Mathematics and Computing. Berlin: Springer, 2022: 201-217.

[14] ALARIFI A, SANKAR S, ALTAMEEM T, et al. A novel hybrid cryptosystem for secure streaming of high efficiency H. 265 compressed videos in IoT multimedia applications[J]. IEEE Access, 2020, 8: 128548-128573.

[15] VALLI D, GANESAN K. Chaos based video encryption using maps and Ikeda time delay system[J]. The European Physical Journal Plus, 2017, 132(12): 542.

[16] FARAGALLAH O S, EL-SAYED H S, EL-SHAFAI W. Efficient opto MVC/HEVC cybersecurity framework based on Arnold map and discrete cosine transform[J]. Journal of Ambient Intelligence and Humanized Computing, 2023, 14(3): 1591-1606.

[17] SHENG Q X, FU C, SONG W, et al. A chaotic selective encryption scheme for H.265/HEVC video with zero bit rate increment[J]. Nonlinear Dynamics, 2024, 112(9): 7631-7648.

[18] WALLENDAEL G V, BOHO A, COCK J D, et al. Encryption for high efficiency video coding with video adaptation capabilities[J]. IEEE Transactions on Consumer Electronics, 2013, 59(3): 634-642.

[19] TEW Y, WONG K, PHAN R C W. Region-of-interest encryption in HEVC compressed video[C]//Proceedings of the 2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). Piscataway: IEEE Press, 2016: 1-2.

[20] TAHA M A, SIDATY N, HAMIDOUCHE W, et al. End-to-end real-time ROI-based encryption in HEVC videos[C]//Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO). Piscataway: IEEE Press, 2018: 171-175.

[21] YU J Y, KIM Y G. Coding unit-based region of interest encryption in HEVC/H.265 video[J]. IEEE Access, 2023, 11: 47967-47978.

[22] TAHA M A, HAMIDOUCHE W, SIDATY N, et al. Privacy protection in real time HEVC standard using chaotic system[J]. Cryptography, 2020, 4(2): 18.

[23] XU D W. Data hiding in partially encrypted HEVC video[J]. ETRI Journal, 2020, 42(3): 446-458.

[24] HOSNY K M, ZAKI M A, HAMZA H M, et al. Privacy protection in surveillance videos using block scrambling-based encryption and DCNN-based face detection[J]. IEEE Access, 2022, 10: 106750-106769.

[25] FARAJALLAH M, HAMIDOUCHE W, DÉFORGES O, et al. ROI encryption for the HEVC coded video contents[C]//Proceedings of the 2015 IEEE International Conference on Image Processing (ICIP). Piscataway: IEEE Press, 2015: 3096-3100.

[26] BROSS B. High efficiency video coding (HEVC) text specification draft 9 (SoDIS)[C]//Proceedings of the 2012 11th Joint Collaborative Team on Video Coding Meeting(JCT-VC). Piscataway: IEEE Press, 2012: 1-7.

[27] PENG F, ZHANG X, LIN Z X, et al. A tunable selective encryption scheme for H.265/HEVC based on chroma IPM and coefficient scrambling[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2020, 30(8): 2765-2780.

[28] WANG J, JIA X Q, KANG X G, et al. A cover selection HEVC video steganography based on intra prediction mode[J]. IEEE Access, 2019, 7: 119393-119402.

[29] USMAN M, AHMAD JAN M, HE X J. Cryptography-based secure data storage and sharing using HEVC and public clouds[J]. Information Sciences, 2017, 387: 90-102.

[30] HOFBAUER H, UHL A, UNTERWEGER A. Transparent encryption for HEVC using bit-stream-based selective coefficient sign encryption[C]//Proceedings of the 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Piscataway: IEEE Press, 2014: 1986-1990.

[31] VIJAYALAKSHMI V, VARALAKSHMI L M, SUDHA G F. Efficient encryption of intra and inter frames in MPEG video[C]//International Conference on Network Security and Applications. Berlin: Springer, 2010: 93-104.

[32] THIYAGARAJAN K, LU R X, EL-SANKARY K, et al. Energy-aware encryption for securing video transmission in Internet of multimedia things[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(3): 610-624.

[33] CHEN C, WANG X J, LIU G N, et al. A robust selective encryption scheme for H. 265/HEVC video[J]. IEEE Access, 2023, 11: 17252-17264.

[34] WEN W Y, TU R X, ZHANG Y S, et al. A multi-level approach with visual information for encrypted H. 265/HEVC videos[J]. Multimedia Systems, 2023, 29(3): 1073-1087.

[35] ZHANG Y Z, LU C. Efficient algorithm adaptations and fully parallel hardware architecture of H.265/HEVC intra encoder[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(11): 3415-3429.

[36] 林志坚, 丁永强, 杨秀芝, 等. HEVC帧内率失真优化预测模式的并行流水线硬件设计[J]. 华南理工大学学报(自然科学版), 2023, 51(5): 95-103.
LIN Z J, DING Y Q, YANG X Z, et al. Parallel pipeline hardware design of intra rate-distortion optimization prediction mode in HEVC[J]. Journal of South China University of Technology (Natural Science Edition), 2023, 51(5): 95-103.

[37] 公衍超, 王玲, 刘颖, 等. 视频主观观测实验启发的HEVC感知帧内码率控制[J]. 通信学报, 2021, 42(8): 90-102.

GONG Y C, WANG L, LIU Y, et al. HEVC perceptual intra-frame rate control inspired by video subjective observation experiment[J]. Journal on Communications, 2021, 42(8): 90-102.

[38] LIN J L, CHEN Y W, HUANG Y W, et al. Motion vector coding in the HEVC standard[J]. IEEE Journal of Selected Topics in Signal Processing, 2013, 7(6): 957-968.

[39] SALEH M A, TAHIR N M, HASHIM H. Moving objects encryption of high efficiency video coding (HEVC) using AES algorithm[J]. Journal of Telecommunication, Electronic and Computer Engineering, 2016, 8: 31-36.

[40] XU D W. Commutative encryption and data hiding in HEVC video compression[J]. IEEE Access, 2019, 7: 66028-66041.

[41] CHEN J, PENG F. A perceptual encryption scheme for HEVC video with lossless compression[J]. International Journal of Digital Crime and Forensics, 2018, 10(1): 67-78.

[42] SALLAM A I, FARAGALLAH O S, EL-RABAIE E S M. HEVC selective encryption using RC6 block cipher technique[J]. IEEE Transactions on Multimedia, 2018, 20(7): 1636-1644.

[43] YANG M X, ZHUO L, ZHANG J, et al. An efficient format compliant video encryption scheme for HEVC bitstream[C]//Proceedings of the 2015 IEEE International Conference on Progress in Informatics and Computing (PIC). Piscataway: IEEE Press, 2015: 374-378.

[44] LONG M, PENG F, LI H Y. Separable reversible data hiding and encryption for HEVC video[J]. Journal of Real-Time Image Processing, 2018, 14(1): 171-182.

[45] SHAHID Z, PUECH W. Visual protection of HEVC video by selective encryption of CABAC binstrings[J]. IEEE Transactions on Multimedia, 2014, 16(1): 24-36.

[46] TEW Y, MINEMURA K, WONG K. HEVC selective encryption using transform skip signal and sign bin[C]//Proceedings of the 2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA). Piscataway: IEEE Press, 2015: 963-970.

[47] YE Q, ZHANG Q J, LIU S J, et al. A novel chaotic system based on coupled map lattice and its application in HEVC encryption[J]. Mathematical Biosciences and Engineering, 2021, 18(6): 9410-9429.

[48] FARAGALLAH O S, EL-SHAFAI W, SALLAM A I, et al. Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication[J]. Journal of Ambient Intelligence and Humanized Computing, 2022, 13(2): 1215-1239.

[49] GUAN B, XU D W, LI Q. An efficient commutative encryption and data hiding scheme for HEVC video[J]. IEEE Access, 2020, 8: 60232-60245.

[50] 卡米塞提·拉姆莫汉·饶, 金道年, 黄在静,等. 视频编码全角度详解: AVS China、H.264/MPEG-4 PART10、HEVC、VP6、DIRAC、VC-1[M]. 北京: 机械工业出版社, 2017.
KAMISETTI R R, KIM D N, HWANG J J, et al. Video coding standards: AVS China、H.264/MPEG-4 PART10、HEVC、VP6、DIRAC、VC-1[M]. Beijing: Machinery Industry Press, 2017.

[51] ASGHAR M N, KOUSAR R, MAJID H, et al. Transparent encryption with scalable video communication: lower-latency, CABAC-based schemes[J]. Journal of Visual Communication and Image Representation, 2017, 45: 122-136.

[52] KELSEY J, SCHNEIER B, FERGUSON N. Yarrow-160: notes on the design and analysis of the yarrow cryptographic pseudorandom number generator[C]//Selected Areas in Cryptography. Berlin: Springer 2000: 13-33.

[53] HAMIDOUCHE W, FARAJALLAH M, RAULET M, et al. Selective video encryption using chaotic system in the SHVC extension[C]//Proceedings of the 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Piscataway: IEEE Press, 2015: 1762-1766.

[54] LI S L, LIU Y Z, REN F Y, et al. Design of a high throughput pseudorandom number generator based on discrete hyper-chaotic system[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 70(2): 806-810.

[55] DONG E Z, YUAN M F, DU S Z, et al. A new class of Hamiltonian conservative chaotic systems with multistability and design of pseudo-random number generator[J]. Applied Mathematical Modelling, 2019, 73: 40-71.

[56] SHAHID Z, PUECH W. Investigating the structure preserving encryption of high efficiency video coding (HEVC) [C]//Proceedings of the Real-Time Image and Video Processing. Bellingham: SPIE Press, 2013, 8656: 191-200.

[57] SALLAM A I, EL-RABAIE E S M, FARAGALLAH O S. Efficient HEVC selective stream encryption using chaotic logistic map[J]. Multimedia Systems, 2018, 24(4): 419-437.

[58] ALI SHAH R, ASGHAR M N, ABDULLAH S, et al. SLEPX: an efficient lightweight cipher for visual protection of scalable HEVC extension[J]. IEEE Access, 2020, 8: 187784-187807.

[59] SALLAM A I, EL-RABAIE E S M, FARAGALLAH O S. CABAC-based selective encryption for HEVC using RC6 in different operation modes[J]. Multimedia Tools and Applications, 2018, 77(21): 28395-28416.

[60] 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 and Systems for Video Technology, 2017, 27(4): 892-906.

[61] 叶清, 张乔嘉, 袁志民. 基于Blowfish的HEVC高效选择性加密方案[J]. 海军工程大学学报, 2022, 34(1): 7-12, 19.
YE Q, ZHANG Q J, YUAN Z M. High-efficiency and selective encryption scheme of HEVC based on Blowfish[J]. Journal of Naval University of Engineering, 2022, 34(1): 7-12, 19.

[62] DOMINGUEZ H O, RAO K R. Versatile video coding[M]. New York: River Publishers, 2022.

[63] VIITANEN M, SAINIO J, MERCAT A, et al. From HEVC to VVC: the first development steps of a practical intra video encoder[J]. IEEE Transactions on Consumer Electronics, 2022, 68(2): 139-148.

[64] XIE X, ZHANG K, ZHANG L, et al. Low complexity transcoding from HEVC to VVC[C]//Proceedings of the 2023 IEEE International Conference on Multimedia and Expo (ICME). Piscataway: IEEE Press, 2023: 2573-2578.

[65] GARCÍA-LUCAS D, CEBRIÁN-MÁRQUEZ G, DÍAZ-HONRUBIA

A J, et al. A fast full partitioning algorithm for HEVC-to-VVC video transcoding using Bayesian classifiers[J]. Journal of Visual Communication and Image Representation, 2023, 94: 103829.

[66] UDDIN K, YANG Y, OH B T. Deep learning-based counter anti-forensic of GAN-based attack in HEVC compressed domain using coding pattern analysis[J]. Expert Systems with Applications, 2023, 233: 120912.

[67] HE S H, XU D W, YANG L, et al. Adaptive HEVC video steganography with high performance based on attention-net and PU partition modes[J]. IEEE Transactions on Multimedia, 2023, 26: 687-700.

[68] NICCOLO C, ANDREA T, CARLO D, et al. Secure real-time multimedia data transmission from low-cost UAVs with a lightweight AES encryption[J]. IEEE Communications Magazine, 2023, 61(5): 160-165.

[69] FARAGALLAH O S, SALLAM A I, EL-SAYED H S. Visual protection using RC5 selective encryption in telemedicine[J]. Intelligent Automation & Soft Computing, 2022, 31(1): 177-190.

[70] TANG B, YANG C, ZHANG Y N. A format compliant framework for HEVC selective encryption after encoding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2023, 33(3): 1140-1156.

[71] LIU C, JIA K B, LIU P Y. Fast depth intra coding based on depth edge classification network in 3D-HEVC[J]. IEEE Transactions on Broadcasting, 2022, 68(1): 97-109.

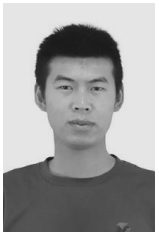
[作者简介]

叶清（1978– ），男，湖北蕲春人，博士，海军工程大学教授、博士生导师，主要研究方向为网络空间安全、密码理论及应用等。

刘小兵（1989– ），男，湖南永州人，海军工程大学博士生，主要研究方向为视频加密、信息隐藏等。

荣里（1980– ），男，湖北石首人，海军工程大学讲师，主要研究方向为舰艇安全。

何俊霏（1997– ），女，河南新乡人，海军工程大学硕士生，主要研究方向为公钥密码理论、格公钥密码。



张乔嘉（1993– ），男，湖北潜江人，海军工程大学硕士生，主要研究方向为视频编码及加密。