基于块参考比重模型的 H.264/AVC 视频选择性加密

黄梦蝶， 杨成， 张远

中国传媒大学，信息与通信工程学院，北京

摘要：4K 和 8K 技术的兴起导致了视频数据流的发展。因此，选择性加密（SE）对加密效率和信息泄漏的挑战越来越大，因此有必要尽可能降低加密率。本文从抵抗加密攻击和素描攻击的角度出发，设计了一种基于 H.264/AVC 视频的选择性加密方案，实现了低加密率和高安全性之间的折衷。首先，我们提出了一种新的计算模型，称为块权重模型，它可以利用视频序列的参考结构来定量分析每个块对其他块的运动补偿的影响。该计算模型有助于准确选择压缩比特流中的密钥字节进行加密，大大保留了网络的友好性，提高了加密效率。此外，我们的方案通过提供一个可调整的加密参数来满足不同的安全级别，从而支持可伸缩的加密粒度。实验结果表明，该方案计算简单，对保密视频内容的保护效率较高。

关键词 选择性加密；H.264/AVC；压缩比特流；素描攻击

Abstract

The rise of 4K and 8K techniques has led to the growth of video data streaming. Consequently, the greater challenges of encryption efficiency and information leakage facing selective encryption (SE) makes it necessary to reduce the encryption ratio as much as possible. In this paper, we design a SE scheme for H.264/AVC video which achieves a trade-off between low encryption ratio and high safety, for both cryptographic attack and sketch attack point of view. As a starting point, we propose a novel calculation model, called block weight model that can take advantage of reference structure of a video sequence to quantitatively analyze the impact of each block on the motion compensation of other blocks. This calculation model can conduce to accurately select the key bytes in the compressed bitstream for encryption, which greatly retains the network friendliness and improves the efficiency compared to previous work. In addition, our scheme supports scalable encryption granularity by providing an adjustable encryption parameter to meet different security levels. Experimental results verified that our solution is highly efficient in protecting confidential video content with simple computation.

Keywords: selective encryption; H.264/AVC; compressed bitstream; sketch attack

一 介绍

根据思科在 2017 发布的最新“视觉网络指数”报告，到 2021 年，移动视频将产生超过四分之三的数据流量。丰富的视频服务所带来的是一个具有挑战性的视频安全研究课题。由于 H.264/AVC 在压缩比和网络友好性方面具有突出的性能，因此成为常用的视频编码标准。选择性加密已经被提出和实践了几十年，通过结合密码技术和视频编码技术来保护视频。与完全加密比特流相比，选择性加密的优势在于降低了加密/解密过程的计算成本。

目前，用于 H.264/AVC 的 SE 技术可分为三类：压缩编码前的加密、压缩编码过程中的加密和压缩后比特流上的加密。将加密嵌入到编码过程中的方案通常会干扰语法元素的统计特性，从而导致压缩比降低。虽然 Asghar[1]研究了一种对语法元素统计没有影响的加密方法，但该方案不支持基于上下文模型的规则熵编码引擎。在[2]中，在选择性加密方案中考虑了熵编码的正规模式和旁路模式，但作者指出比特率确实增加了。此外，编码过程中加密会增加信息泄漏的风险。语法元素的精确选择为编码中的加密提供了极好的加密率，但是为满足格式兼容性而保留的语法元素也给了对手一个机会。[3]给出了 H.264 视频的最新的素描攻击，通过对宏块头的分析，可以生成视频的轮廓。在这里，我们将一个选择性加密算法应用于压缩域数据。它对编码效率和压缩比没有任何影响。

选择策略的设计是基于对一组图片中帧间参考结构的分析。在 H.264 中，帧间重构过程依赖于运动补偿。一些重建的块将经常被后面的块引用。因此，重建过程中产生的误差将沿着后续的块组成的路径累积。相反，一些块将很少被引用，因此错误不会影响其他块太多。显然，选择加密的目标应该集中在最常被引用的块上。

本文提出了一种 H.264/AVC 的安全选择性加密方案。首先，提出了一种计算 GOP 重建过程中各区块权重的模型，并对该模型进行了扩展，以计算宏块权重。其次，根据权重值，选择少量宏块进行 AES 加密。特别是，我们提供了一个加密参数来定制安全级别。本文的其余部分组织如下。第二节简要介绍了 H.264 码流选择性加密方法的研究现状。第三节详细介绍了建议的块权重模型和选择性加密方案。第四节介绍了在提出的 SE 之后视频显示的实验结果，并详细分析了安全性和计算开销。最后，在第五节中得出结论。

二 相关工作

1. H.264/AVC 视频安全的研究现状

对 H.264 压缩比特流的码字进行选择性加密已经有了一些相关的工作。Andreas[4]提出了一种 H.264/AVC 的 SE 方法，通过改变 NAL 报头中的 nut 值并加密 NAL 单元有效载荷。该方法通过独立加密每个 NAL 单元来保留 H.264 的网络友好特性。然而，由于没有有效负载数据的选择，加密率很高。[5]中的作者设计了一种适合 DRM 的加密方案。通过对算法参数的定制，可以控制 SE 的粒度。然而，在加密效率方面，基于切片层的选择策略有点粗糙，对于每一个视频，加密位置都是固定的，没有对视频内容进行统计分析。蒋[6]应用 CAVLC 后选择内部预测模式（IPM）加密的思想。它可以保持视频数据格式，但是码字的长度会增加。此外，所有的预测宏块（P-MB）和 B 预测宏块（B-MB）都缺乏保护，因为语法元素 IPM 仅存在于帧内宏块（I-MB）中。显然，该方案不足以保证视频内容的安全性。在[7]中也存在类似的问题，即使用 AES 加密 I 帧中的所有位。孔[8]建议对从 H.264 比特流中提取的 I 帧和部分 P 帧中的整个帧数据进行加密。它在稳健性方面表现良好，但计算开销过大。王[9]研究了 H.264 块层上的 SE 算法，通过改变 4x4 块在每个 MB 中的位置来提供多级视频安全，但最高的加密率可达 60%，压缩率下降了 2%。

考虑到从加密的 MB 中解码出来的 MB 会严重失真，在[10]中的工作描述了一种决策方法，其中 Dubois 对 CAVLC 模式下编码的每一帧的部分 MB 进行加密，以将此错误扩展到视频序列的每一帧。根据计算 PSNR 得到的保密性来选择 MB。在这种方法中，由于需要一次以上的预测，需要对编码器帧和解码器进行重新设计。Khlif[11]提出了运动矢量符号的加密，他认为对第一个 P 帧的 MV 进行加密的误差是可以扩散的。然而，当 P 帧中的所有 MV 都被选中时，加密率太高，接近 50%。研究[12]显示了 H.264 视频的运动参考结构。定义了一个称为 MRR（运动参考比）的比率，用于测量 MBS 之间的依赖关系，用于选择 MB。对于动作幅度小的视频，只加密 I 帧。对于运动密集的视频，I 帧的所有 MB 和 P 帧的部分 MBS 都将被加密。如果以这种方式加密视频，则仅选择 I 帧时，运动轨迹将泄漏。在这里，通过对 MBS 的进一步分析，还可以减少在 I 帧和 P 帧中选择的 MB 的数量。

2. H.264/AVC 选择加密存在的问题

我们总结了 H.264 的 SE 技术中的以下问题。随着越来越多的互联网流量被加密以保护用户的隐私，对加密媒体流的攻击越来越严重。除了传统的密码攻击

之外，近年来出现了一些新的感知攻击[13]。毫无疑问地，安全性必须是视频 SE 首先考虑的问题。此外，NAL 单元有助于 H.264/AVC 比特流对异构网络的适应性。因此，也应保留 NAL 单元的封装格式，以便解码器正确地解码它。计算开销是设计方案的一个普遍问题，在低延迟的视频业务中，计算开销的重要性将得到提高。大部分的计算开销都花在加密上，而不是选择上，因此加密率至关重要。通常，当有选择地加密变换系数、内部编码模式或压缩中的运动矢量差异时，可以获得较低的加密率。但同时也伴随着实现的复杂性和对压缩比的影响。由于 H.264/AVC 中 SE 的问题不是相互独立的，所以我们综合考虑了这些问题。

三 提出的选择性加密方案

1. 块参考比重计算模型

在 H.264 译码器中，当前重构块的失真将扩展到需要当前重构块参考的后续块。在我们提出的方案中，我们充分利用这一特性来对视频内容进行加扰。块权重（BW）被定义为直观地描述每个块对一组图片（GOP）中的相互预测的重要性。当我们重建一个 4x4 块时，参考帧中的匹配区域可能对应于一个完整的块，或者两个或四个块（见图 1）。

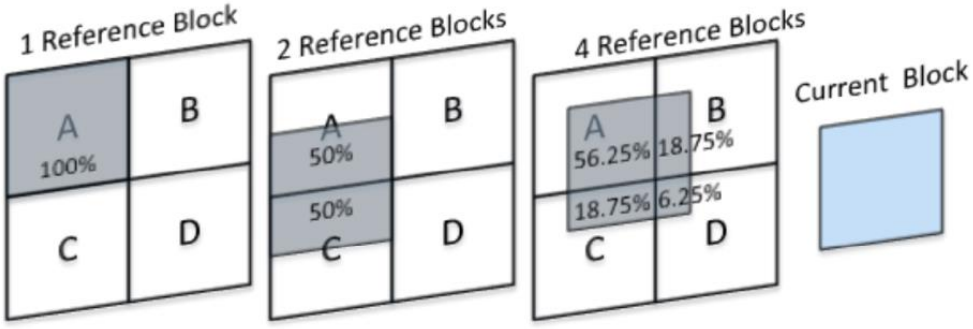


图 1 三种块匹配状态

显然，每个参考块重建当前块的比例并不总是相等的。将参考区块覆盖面积的大小定义为测度时，A 区块在最后一个参考状态中扮演着更重要的角色，因为它在四个区块中所占的比例最大。此外，引用每个块的次数也不相同。有些块经常用作参考块，有些则很少被引用。为了通过尽可能少的加密来保护视频内容，我们设计了以下模型来挑选 GOP 中具有高 BW 的块。

$$P_{(x,i)} = \frac{S_{(x,i)}}{16} \tag{1}$$

$$W_b(x) = \begin{cases} 1 + \sum_{i=1}^{n} P_{(x,i)} W_b(i), & n \neq 0 \\ 1, & n = 0 \end{cases} \tag{2}$$

本文提出以块参考比重 Block Impact 来评估 H.264 中 4x4 像素块的误差传播影响力。具体以参考面积衡量块的参考比重，块参考比重计算模型以一个 GOP 组为单位进行抽象，如图 2 所示。虚线标注的是假设的参考比例，块内标注的是计算得到的当前块参考比重。从 GOP 组的最后一帧开始，根据 Block i 的运动向量和参考帧信息匹配到参考块 Block x，然后按照公式（1）求出 Block x 在重建 Block i 时所占的面积比重 P(x,i)。Block x 在 GOP 组中可能不止一次作为参考块，根据公式（2）用参考比重 Wb(x)定量的表示 Block x 对正确解码一个 GOP 组的重要意义。块的参考比重被初始化为 1，块不被任何块引作参考区域时，其比重值 Wb 不会被更新。从模型的计算结果可以发现，当递推到 IDR 帧时，即所有块的参考比重均被更新完后，每一帧块的 Wb 值都有高低之分。面积比重高、参考频率高的块对应的综合参考比重值也高，本文据此将此类块定义为重建 GOP 组时误差传播影响力较高的块。

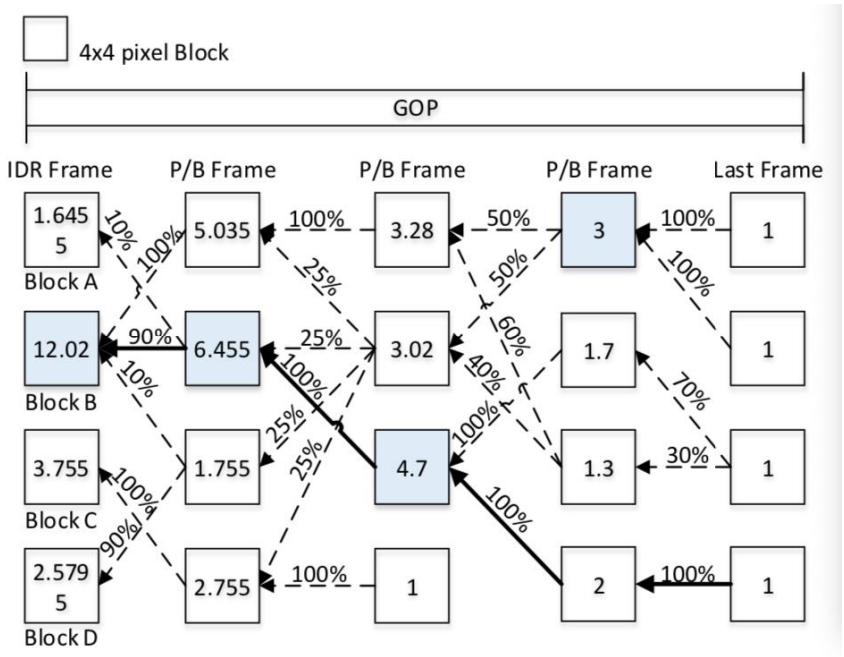


图 2 块参考比重计算图示

根据计算结果，我们可以得出如下结论：后续区块越多，参考比例越大，其 BW 值越高。同时，根据 IDR 帧中的最高 BW，可以从模型中得到从 IDR 帧到最后一帧的一条相互预测路径。这意味着 B 块的畸变将扩展到最后一帧，在某种程度上，与同一帧中的其他三个块相比，它对预测 GOP 的影响最大。当然，并非路径上的每个块在其对应的帧中都有最大的 BW。随着运动的改变，帧间的某些块在短路径上会得到较高的 BW。为了避免信息泄漏，只加密 I 帧中的块显然是不够的。因此，我们随后提出了一种基于块参考比重模型的 H.264 视频选择

性加密方案。

2. 选择策略和加密规则

为了应对越来越多的感知攻击，如[3]中依赖于视频加密前后宏块数据中保持完整的信息的素描攻击，这些信息主要是在宏块头中，我们决定将宏块层作为视频加密的粒度。因为块层加密将不可避免地暴露宏块头，使更多的黑客利用它。根据 BW 模型计算后，对 BW 值进行进一步处理。我们将 MBx 的权重（mbw）定义为（3）。Wb（x，i）是属于 MBx 的块 i 的 BW 值。由于 skip 块不会在 h.264 中编码，因此 skip 块的块权重在 BW 模型中定义为不更新，保留初始值。基于此初始设置，通过计算非 skip 的宏块（非 skip 的 P 类宏块和 I 类宏块）的 BW，可以清楚地观察到 GOP 中物体的运动轨迹。

$$W_{mb}(x) = (\sum_{i=1}^{16} W_{b(x,i)})/16 \tag{3}$$

$$m_n = \alpha N_n = \alpha \cdot (wh/(16 \times 16)), 0 < \alpha \leq 1 \tag{4}$$

$$m_n = \sum_{i=1}^{q} l_i \tag{5}$$

$$P_s = \sum_{i=0}^{l_s-1} MB_{(s,i)}, s\ from\ 1\ to\ q \tag{6}$$

$$C_s = Enc(P_s), s\ from\ 1\ to\ q \tag{7}$$

$$F_n = \sum_{i=0}^{q-1} C_i \tag{8}$$

在获取 GOP 中每个 MB 的参考权重后，决定和加密步骤如下。

第 1 步：将每个帧的宏块（MBS）重新组织成一个有序的序列{MB0，MB1，…，MBNn-1 }通过 MBW 从高到低对宏块进行排序。Nn 是属于第 n 帧的非 skip 类型宏块的总和。

第 2 步：在第 n 帧中，{MB0，MB1，…，MBmn-1 }被挑选出来进行加密。mn 是第 n 帧中选定宏块的数目，定义为公式（4）。W 和 H 分别以像素表示压缩视频的宽度和高度。α 被定义为选择比例，这是算法中支持调整的参数。

第 3 步：拆分序列{MB0，MB1，…，MBmn-1 }根据宏块所属的 NAL 单元（NALU）分成若干个子序列。然后用一个特定的密钥独立地加密每个子序列。这样，解码器可以在接收到 NALU 后立即进行检索和解密，而无需等待 GOP 完全被接受。假设 n 帧对应的 NAL 单元数为 q，则由所选宏块组成的序列将被拆

分为子序列{S1，S2，…，Sq}，长度为{l1，l2，…，lq}，满足公式（5）。然后，从 H.264 比特流中提取子序列中的宏块，并将其合并为明文，如公式（6）。MB（s，i）表示子序列 SS 中包含的 MBi。lS 是 SS 的长度，它是 NALU 中选定的宏块的数量。加密 SS 生成的密文定义为公式（7）。AES 作为经典的对称加密算法，被选为加密算法，用 128 位长的密钥对明文进行加密。为了确保加密前后子序列的长度不变，指定不对长度小于 16 字节的明文中的最后一个块执行填充加密。

步骤 4：在完成 PS 的加密后，根据提取的 MBS 长度将 CS 分成段。最后，将它们放回 NALU 比特流中提取的宏块的位置。第 n 帧的 SE 表示为公式（8）。

当视频以 CACLC 模式编码时，GOP 中没有 B 帧。因此，最后一帧不会被任何帧引用。最后一帧中每个块的 BW 在计算过程中将保持初始值。按 MBW 对最后一帧中的宏块进行排序的尝试无疑将失败，因为它们具有相同的 MBW。因此，我们在最后一帧中设置一个选定的 MBS 的恒定比例，以降低信息泄漏的风险，即 0.5。

我们的选择性加密方法总结如下。首先，根据重建过程中的运动参考，计算出 GOP 内各区块的权重和各宏块的权重。其次，从所有帧中选择高权重的宏块，选定的宏块从其所属的切片中提取，然后拼接、加密并放回比特流。总而言之，我们针对 H.264 提出的选择性加密算法以宏块层作为选择和加密的粒度。通过适当调整选择性加密算法的参数，可以定制加密视频的感知度。

四 实验结果和分析

视频内容可以通过固定机位或者移动镜头来获取。于前者而言相机的位置和焦距都是不变的，而后者则拍摄主体和相机都会移动，这也就意味着需要编码更多的运动信息。本文中我们用了五个移动镜头拍摄的 CIF 格式标准测试序列：Mobile,Stefan,Coastguard,Basketball pass and Foreman 来研究我们提出的 SE 算法的性能。我们在 JM18.6 中设定 IDR 帧的周期为 50，并用该框架将这些测试序列编码为 H.264 格式。这个部分详细分析了方案的安全性和计算复杂度来证明其可行性。

1. 感知安全性

鉴于选择性加密的主要缺点在于可能有信息泄露，其中包括运动信息、主题信息、背景信息。我们首先证明我们的选择性加密算法的感知安全性。

(a)

(b)

图 3 α=0.05 时用我们的方法加密视频后的感知效果

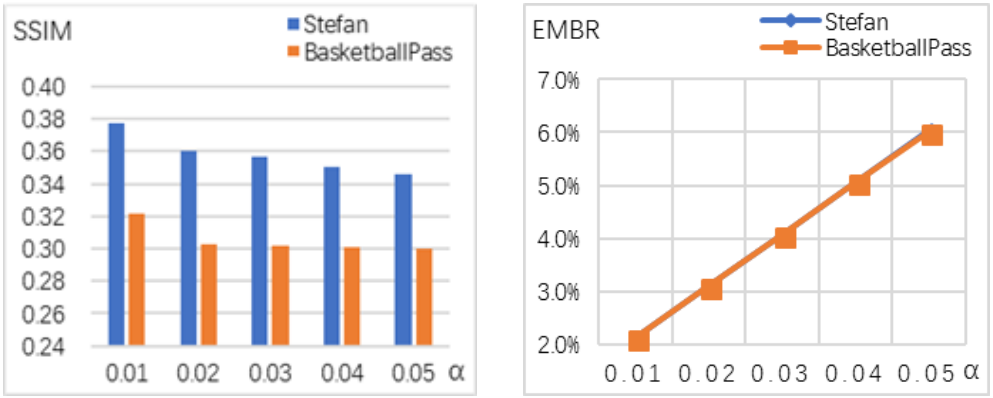
(a) 原视频中的 IDR 帧、第 20 帧、第 25 帧和最后一帧

(b) 加密视频的 IDR 帧、第 20 帧、第 25 帧和最后一帧

图 3 展示了我们的 SE 算法中的参数 α 设为 0.05 时加密视频的感知结果。为

了直观的观测视频运动特征，图 3 中的（a）显示了没有加密 IDR 帧时的 SE 加密效果，图 b 则为正常加密的效果。由于对运动补偿过程有很大影响的运动特征信息被基于宏块的加密方法破坏，加密视频中的运动主体从第一帧到最后一帧都保持静止状态。而当 IDR 帧也被加密时，解码器无法从码流获取任何信息，最终解码结果如图（b）所示。即使只加密了 5%的帧内编码块和前向预测编码块，视频内容也很难被视频攻击方获取。

图 4 是我们在 α 分别为 0.01、0.02、0.03、0.04、0.05 时对两个具有明显运动特征的标准视频 Stefan 和 Basketball Pass 加密的结果。SSIM（structural similarity index）是用来评估原始 YUV 格式视频与由加密后的 H.264 比特流解码得到的 YUV 格式视频之间结构相似性的指标。EMBR 是编码的宏块中加密的宏块所占比例，它反映了计算开销。从图 4 的（a）图可以看出，随着 α 值的下降，SSIM 值不断增大，加密效果有所减弱，但从 SSIM 值中可以看出，仍然是符合加密视频的视觉安全需求的。图 5 展示了将 α 值设定为 0.02 时的视频质量。由于 IDR 帧中加密的宏块数减少，所以在 GOP 的最后一帧中会泄露少量背景信息，但是运动痕迹以及运动主体依旧很难辨识，同时 EMBR 从 6%降到 3%（见图 4（b））也意味着计算复杂度锐减。

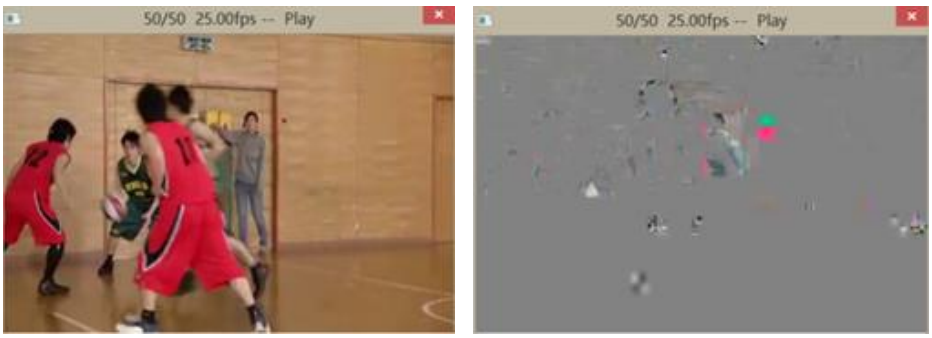


(a) (b)

图 4 不同 α 值下加密视频的 SSIM 和加密比例

（a）不同 α 下 SSIM 表现

（b）不同 α 下 EDR 表现



（a）

（b）

图 5 α=0.02 时,Basketball Pass 和 Stefan 加密的感知效果

（a）α=0.02 时，Basketball Pass 原始视频和加密视频的最后一帧对比

（b）α=0.02 时，Stefan 原始视频和加密视频的最后一帧对比

2. 密钥空间分析

为抵御暴力攻击，我们的 SE 算法扩展了密钥空间。BSE 算法采用了 AES CTR 模式加密，单次加密的密钥长度为 128 比特， 对应一个 NAL 单元的密钥空间为 2^{128}。当帧被划分成片时，假设片的数目为 q， 则对应一帧的密钥空间为2^{128*q}。当一个 GOP 组中包含 n 个帧时，加密视频序列 的密钥空间就达到了$2^{128*q*n}$，即密钥的猜测范围多大$2^{128*q*n}$，可见攻击者很难在有限的资源下猜测出正确密钥。

3. 素描攻击

[3]提出了一种针对 H.264 编码视频的素描攻击，它可以利用宏块头部暴露出的宏块比特流大小来产生原始视频的轮廓线。在我们提出的 SE 方法中，所选的宏块头部信息和宏块数据部分都会被加密。因此，除非密钥被破解，否则我们的加密方法是足以抵挡素描攻击的。如果一些视频服务商想要吸引用户购买更高质量的视频服务，那么可以降低视频加密水平。如果可以接受素描攻击，那么我

们的 SE 算法唯一需要改变的就是在加密所选宏块时不加密宏块的头部，这样编码的视频在解码时具有格式兼容性。

4. 计算复杂度

我们的 H.264 视频选择性加密方法独立于编码器，它对熵编码效率和压缩率并没有影响。主要的计算开销产生于加密数据的过程中，而非计算 BW 或者选择加密宏块的过程中。接下来，我们将用加密宏块率（EMBR）和加密比特率（EDR）来衡量加密算法的计算复杂度。，码流加密比例越小，执行 AES 加密时消耗的计算开销也会相应减少。

H.264 标准提供了官方测试视频，我们选取五个具有丰富运动信息和复杂结构特征的视频序列用作测试序列，SE 算法设定在没有信息泄露的最高安全等级，即 α 等于 0.05。图一的实验结果显示，加密前后 Mobile 视频的 SSIM 值大幅下降，降幅达 0.782，这表明视频的结构已被严重破坏。EDR 低至 6.07%，这说明运用该算法只加密了少量数据，计算开销少。与此同时 EMBR 始终在 6%左右浮动，这是因为除了最后一帧 α =0.5 之外其它所有帧 α 均为 0.05，最后一帧中宏块数的不同带来了 EMBR 的轻微浮动。

我们进一步比较了我们的算法同其它针对 H.264 视频加密的选择性算法的性能。在[12]中运动参考结构也被用来选取加密的宏块，但是其选择不具备灵活性，加密的宏块数远远超过我们的方案（见表 2）。由于选取宏块中特定的语法元素来加密，所以 EDR 的值有所下降， 但暴露出来的宏块头信息正是素描攻击所需的关键信息。与[12]中的方案相比，我们的方案在将 EMBR 降低了 5-10 倍的同时只带来 EDR 的微小增幅。这也表明我们的方案能更精确地找到包含关键信息的宏块。[11]中提出的是针对运动矢量的 SE 方案，由于缺乏运动矢量的选择策略，导致 EDR 相当高，几乎有一半的比特均被加密（见表 3）。对比之下，我们的方案显现了在加密效率上的优势，在保证保密性的前提下，Mobile 和 Foreman 中分别只有 6.07%和 9.94%的字节被加密，并且用我们的方案对这两个测试序列加密前后的 PSNR 差值比[11]对应差值大，这表明我们的方案达到更高的感知安全性和更低的计算复杂度。

表 1 原始视频和加密视频的数值比较

测试序列	EMBR (%)	EDR (%)	原始 SSIM	原始 PSNR	加密后 SSIM	加密后 PSNR
Mobile	5.97	6.07	0.975	35.264	0.193	12.003
Stefan	6.03	7.03	0.979	36.509	0.335	15.210
Coastguard	6.04	7.47	0.941	35.023	0.247	14.313
Basketball	6.01	8.08	0.937	38.337	0.300	15.557
Foreman	6.10	9.94	0.942	37.603	0.353	12.019

表 2 文献[12]和本文加密方法的比较

测试序列	[12]		本文 SE	
	EMBR (%)	EDR (%)	EMBR (%)	EDR (%)
Mobile	54.0	5.30	5.97	6.07
Foreman	42.7	8.86	6.10	9.94
Stefan	33.0	5.15	6.03	7.03

表 3 文献[6]和本文加密方法的比较

测试序列	[6]				本文 SE			
	原始 PSNR	加密后 PSNR	PSNR 差值	EDR (%)	原始 PSNR	加密后 PSNR	PSNR 差值	EDR (%)
Mobile	29.84	8.99	20.850	49.640	35.264	12.003	23.261	6.07
Foreman	35.92	10.67	25.250	49.175	37.603	12.109	25.584	9.94

五 结论

本篇论文提出了 H.264/AVC 压缩领域的一种新的选择性加密方案。在一个 GOP 中，我们选取了被参考得更多的宏块来加密，通过改变加密宏块的比例，可以达到不同等级的安全性，根据实验结果分析可知，我们的方案能高效地加密视频，最多只需要加密比特流中 10%的字节便可以保证不泄露任何有效信息。总结而言，首先我们的方法能够抵抗暴力攻击和素描攻击，并且有很大的密钥空间。

并且它在保证网络友好性的同时通过用独立的密钥加密NALU提高了解码效率。最后精确选择加密宏块有效地降低了计算开销。

六 致谢

感谢杨成老师对实验设计和论文撰写的悉心指导， 杨成老师提出的许多深刻见解和宝贵建议也使我的课题研究和论文撰写工作能够顺利完成，在此对恩师付出的关怀和心血表示深深的感激。其次，感谢实验室安全课题组同学在论文实验中对我的支持和帮助，不管是研究上的合作还是生活中的相处都使我受益良多。感谢中国传媒大学中央高校基本科研业务费项目专项资金资助。

参考文献

[1] Asghar, Mamoona Naveed, and M. Ghanbari. "An Efficient Security System for CABAC Bin-Strings of H.264/SVC." IEEE Transactions on Circuits & Systems for Video Technology 23.3(2013):425-437.

[2] Boyadjis, Benoit, et al. "Extended Selective Encryption of H.264/AVC (CABAC)- and HEVC-Encoded Video Streams." IEEE Transactions on Circuits & Systems for Video Technology 27.4(2017):892-906.

[3] Minemura, Kazuki, et al. "A Novel Sketch Attack for H.264/AVC Format-Compliant Encrypted Video." IEEE Transactions on Circuits & Systems for Video Technology PP.99(2016):1-1.

[4] Uhl, Andreas. "Format-Compliant Encryption of H.264/AVC and SVC." Tenth IEEE International Symposium on Multimedia IEEE Computer Society, 2008:446-451.

[5] Zou, Yuanzhi, et al. "H.264 video encryption scheme adaptive to DRM." IEEE Transactions on Consumer Electronics 52.4(2006):1289-1297.

[6] Jiang, Jianguo, S. Xing, and M. Qi. "An Intra Prediction Mode-Based Video Encryption Algorithm in H.264." International Conference on Multimedia Information NETWORKING and Security IEEE Computer Society, 2009:478-482.

[7] Abomhara, Mohamed, et al. "Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard." International Journal of Computer Theory & Engineering 2.2(2010):223-229.

[8] Hole, Rupali N., and M. Kolhekar. "Robust video encryption and decryption using selective encryption." International Conference on Nascent Technologies in Engineering IEEE, 2017:1-4.

[9] Wang, Qiuhua, and X. Wang. "A new selective video encryption algorithm for the H.264 standard." International Conference on Progress in Informatics and Computing IEEE, 2014:275-279.

[10] Dubois, Loic, J. Blanc-Talon, and J. Blanc-Talon. "Smart selective encryption of CAVLC for H.264/AVC video." IEEE International Workshop on Information Forensics and Security IEEE Computer Society, 2011:1-6.

[11] Khlif, N., et al. "Motion vectors signs encryption for H.264/AVC." International Conference on Advanced Technologies for Signal and Image Processing IEEE, 2014:1-6.

[12] Shen, Haojie, L. Zhuo, and Y. Zhao. "An efficient motion reference structure based selective encryption algorithm for H.264 videos." Iet Information Security 8.3(2014):199-206.

[13] Ran, Dubin, et al. "I Know What You Saw Last Minute—Encrypted HTTP Adaptive Video Streaming Title Classification." IEEE Transactions on Information Forensics & Security 12.12(2017):3039-3049.