# 基于宏块复杂度的自适应视频运动矢量隐写算法

王丽娜 徐一波 翟黎明 任延珍

(武汉大学空天信息安全与可信计算教育部重点实验室 武汉 430072) (武汉大学计算机学院 武汉 430072)

信息隐藏是一种将秘密信息嵌入常见的载体中以实现信息秘密传递的技术.然而,隐写改动都会不可避 摘 要 免地造成各种失真.视频运动矢量隐写则会造成画面质量下降、比特率增加、概率分布改变等变化.这些由隐写造 成的影响可能会被已有的或者潜在的隐写分析方法所检测.已有的运动矢量隐写分析特征大致可以分为两类:--类基于局部最优性特征,另一类基于时域和空域相关性特征.为了尽可能降低运动矢量的隐写失真,该文对视频编 解码过程中运动矢量相关内容给出形式化描述方法.进一步地,理论分析了关于运动矢量的局部最优性以及相邻 相关性两个因素.此外,文中研究了运动矢量隐写造成的最优概率下降的原因,指出了隐写纹理简单宏块的运动矢 量不容易造成显著的局部最优性异常.该文讨论了运动矢量分量的分布规律,认为使得分量更靠近分布均值的修 改,可以较好保持相关性. 通过这些理论研究,提出基于宏块复杂度的视频运动矢量自适应隐写算法(Adaptive Macroblock Complexity, AMC), 其可以分开处理运动矢量局部最优性和相邻相关性两个因素. 该算法可以不使用 编码实现秘密信息在最低代价路径上的嵌入和提取,而且每个运动矢量可以嵌入2比特秘密信息.算法包括两步: 首先,压缩 cover 视频,不做任何嵌入,记录所有宏块压缩后的复杂度,同时依据分布统计设定一个复杂度阈值.然 后,在第2次进行的视频压缩过程中,通过自适应阈值选择低复杂度宏块,将其运动矢量用于 LSB(最低有效位)匹 配嵌入.对于运动矢量来说,低复杂度宏块较容易保持局部最优,而 LSB 匹配嵌入可以保持相邻相关性.在实验部 分,将不同隐写算法但相同嵌入率的 stego 样本在不可见性、码率增长、反检测能力等方面分别进行了对比.实验结 果表明, cover 的 PSNR 值最高, 而 AMC 排在第二, 与之相差不超过 0. 05 dB. 对比比特率增长, AMC 算法比特率 增长量只有其他算法的1%至50%左右.此外,该文使用两种隐写分析特征评估这些算法的安全性.检测的错误率 表明 AMC 隐写算法和已有算法相比安全性更均衡. 总体看来, AMC 隐写算法能够较好抵抗隐写分析, 特别是隐写 后视频码率得到了控制,画面质量得到了很好保证.

关键词 运动矢量;信息隐藏;复杂度;隐写分析;反隐写分析 中图法分类号 TP391 **DOI**号 10.11897/SP.J.1016.2017.01044

# An Adaptive Video Motion Vector Steganography Based on Macroblock Complexity

WANG Li-Na XU Yi-Bo ZHAI Li-Ming REN Yan-Zhen

(Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan 430072) (Computer School, Wuhan University, Wuhan 430072)

**Abstract** Modern steganography is the art of covert communication which sends secret messages under the regular-looking cover media. However, different distortions will be introduced inevitably by the embedding modification of steganography. The modification of video motion vectors can also result in many distortions, such as poor image quality, bitrate increase and the changes of probability distribution. All of these impacts caused by embedding may be detected by existing or potential steganalysis methods. The established features of motion vector steganalysis can be

收稿日期:2016-06-28;在线出版日期:2017-02-24.本课题得到国家自然科学基金重点项目(U1536204)、国家科技支撑计划项目 (2014BAH41B00)、国家自然科学基金(61373169)、国家"八六三"高技术研究发展计划项目基金(2015AA016004)资助.王丽娜,女,1964年 生,博士,教授,主要研究领域为信息隐藏和云计算安全.E-mail: lnwang@whu.edu.cn.徐一波,男,1986年生,博士研究生,主要研究方向 为信息隐藏.翟黎明,男,1989年生,博士研究生,主要研究方向为信息隐藏.任延珍,女,1973年生,博士,副教授,主要研究方向为信息隐藏. broadly separated into two categories: one is based on local optimality, and the other is based on spatial and temporal correlation. In order to stay the distortions of motion vector steganography as low as possible, the formal description regarding motion vectors in the process of video coding and decoding is provided in this paper. Moreover, the local optimality and the correlation of adjacent motion vectors have been analyzed theoretically. Furthermore, we study the causes of the local optimal probability decrease due to motion vector modification, and point out that the embedding, in the motion vector of simple texture macroblocks, is not likely to cause significant distortion of local optimality. This paper discusses the distribution rule of motion vector components. The rule reveals that the modification, making the component become more close to the distribution mean value than before, can protect the correlation better. With the aid of theoretical study, we propose a novel adaptive steganography algorithm based on macroblock complexity (Adaptive Macroblock Complexity, AMC), which can deal with local optimality and adjacent correlation of motion vectors separately. This algorithm can embed and extract secret information on the minimum distortion path without using any coding method, and every motion vector can be embedded into 2 bits. There are two stages in this algorithm, firstly it compresses the cover video without any embedding, records the complexity of all macroblocks after the compression, and sets the threshold of complexity according to the complexity distribution. And then, the motion vectors of the low complexity macroblocks which are chosen by the adaptively adjusting threshold, are used for LSB (Lest Significant Bit) match embedding in the second compression. For motion vectors, the low complexity macroblocks can preserve local optimality easily, and the adjacent correlation can be protected by LSB match embedding. In the experiment, we made comparisons among stego samples, different algorithms but same payload, in invisibility, bitrate increase and anti-steganalysis respectively. The experimental results show that, the cover samples enjoyed the highest PSNR value, and the AMC ranked second with difference no more than 0.05 dB. In comparison with bitrate growth, the AMC algorithm only accounts for about 1% to 50% of other ones. In addition, two steganalysis features have been used to evaluate the security of the embedding algorithms in this paper. The detection error indicates that the AMC algorithm have a more relatively balanced security than existing ones. In general, the AMC algorithm has a better performance on anti-steganalysis against the classic steganalysis algorithm, especially the bitrate of embedding video is controlled and the quality of the video image maintains very well.

Keywords motion vector; steganography; complexity; steganalysis; anti-steganalysis

# 1 引 言

信息隐藏是一种将秘密信息嵌入数据载体借助 载体掩蔽作用实现信息秘密传递的技术.近年来,基 于数字图像和数字视频等主流网络媒体的信息隐藏 技术得到了广泛研究<sup>[1-3]</sup>.视频信息隐藏作为一个新 兴研究领域,基于帧内预测<sup>[4]</sup>、频域<sup>[5]</sup>和运动矢量的 隐写算法<sup>[6-9]</sup>纷纷出现.众多信息隐藏方法中,运动 矢量隐写具有隐藏容量大,画面失真小等优势,是目 前视频信息隐藏领域中的一个研究热点.

在运动矢量隐写方面,Xu等人<sup>[6]</sup>提出选择绝对

值较大的分量进行隐写,可以保持较小的失真. Aly<sup>[7]</sup>提出通过选择重建块和参考块差异较大的运动 矢量隐写能够降低视觉失真控制码率增长.Cao等人 在文献[8]中通过次优运动矢量结合湿纸编码选择干 通道进行信息嵌入进一步提升了算法安全性.此后, Cao等人在文献[9]中,使用 STC<sup>[10]</sup> (Syndrome-Tellis Codes)和湿纸的双层编码以保持运动矢量局 部最优性.另外,Yao等人<sup>[11]</sup>同样使用 STC 编码控 制运动矢量隐写在残差和相关性方面的失真.这两 类失真互相制约,未取得各自最优.Zhang 等人<sup>[12]</sup> 提出一种局部最优保持算法,其使用奇偶性相反且 具备局部最优特性的候选运动矢量进行隐写替换, 结合 STC 编码保证了运动矢量的局部最优. 该算法 是目前众多运动矢量隐写算法中安全性最高的一种.

隐写分析作为信息隐藏的对抗技术,特征的性 能极大地影响隐写分析的检测效果.目前的运动矢 量隐写分析特征大致可以分为两类:一类是运动矢 量的相关性特征,主要利用运动矢量在空域或时域 上的相似性构造;另一类则是运动矢量的局部最优 性特征,主要利用运动矢量在其周围邻域内一般具 有最小残差代价的特性构造.基于相关性的特征包 括: Zhang 和 Su 等人<sup>[13-14]</sup>的运动矢量空域和时域相 关性特征. Wang 等人<sup>[15]</sup>的单个帧内宏块在空域 4个方向上相邻差值共生矩阵的隐写分析特征,以及 Ye 等人<sup>[16]</sup>的空域和时域相关性特征. 基于最优性 的特征有:Cao等人[17]提出的重压缩视频的残差特 征. Ren 等人<sup>[18]</sup>提出的基于局部区域运动矢量最优 概率的 SPOM(Subtractive Probability of Optimal Matching)特征以及 Wang 等人<sup>[19]</sup>的运动矢量在其 加减1(Add or Subtract One, AoSO)局部范围最优 概率分布的特征.这两大类特征中,目前基于运动矢 量局部最优构造的隐写分析特征更加有效一些.而 AoSO 是现在运动矢量隐写分析领域公认最为有效 的特征.

早期运动矢量隐写算法(如 Xu 等人<sup>[6]</sup>和 Aly<sup>[7]</sup>) 大多注重视频画面质量保真,对于运动矢量相关性 和局部最优性较少关注.近期隐写算法(如 Cao 等 人<sup>[8-9]</sup>,Yao 等人<sup>[11]</sup>,Zhang 等人<sup>[12]</sup>)更加关注隐写 算法安全性,使用 STC 编码和湿纸编码控制隐写风 险.特别是 STC 编码的出现,极大提升了隐写算法 的安全性:一方面,隐写算法可以借助 STC 极高的 编码效率,大大降低其对于载体比特的修改率;另一 方面,STC 编码可以提供一条近似最低代价的嵌入 路径.这两点使得隐写算法代价失真最小.因此,基 于 STC 编码的隐写算法一般都具有较强的反检测 能力,安全性较高.

事实上,隐写造成的任何失真均可能带来潜在 被检测的风险,而不仅是特定一类已有算法的检测. 目前隐写研究更多针对特定隐写算法,较关注单一 统计特性的保持,不利于隐写算法安全性的全面提 升.同时,隐写失真的定义较依赖于发现规律和总结 经验,欠缺一定的理论证明.目前基于单层甚至双层 编码的隐写算法<sup>[9,11-12]</sup>构造相对复杂,运行效率较低,而代价函数可能依赖大量统计,难以实现.针对以 上问题,本文对于运动矢量特性进行了详细的理论分 析,提出一种基于宏块复杂度的自适应(Adaptive Macroblock Complexity, AMC)隐写算法.该算法可 不使用编码实现最小化失真嵌入路径,将局部最优 性和相邻相关性相互分离分别进行控制:通过选取 低复杂度宏块隐写保持运动矢量局部最优,以及通 过加减1方法保持运动矢量相互间的相关性.基于 以上策略,达到既可以抵抗最优性特征检测,也可以 抵抗相关性特征检测的效果.实验结果表明该算法 具有隐写和提取简单、抵抗隐写分析的特点,相比 于目前已有算法具有好的画面质量和更低的码率增 长.此外,若将复杂度作为代价函数,该算法也可以 借助 STC 编码进一步降低修改率,提升算法安 全性.

本文第2节介绍本文相关工作;本文在第3节 对运动矢量局部最优性以及相邻相关性进行理论分析;第4节是本文的隐藏方法;第5节通过实验验证 隐藏算法的不可见性、比特率、抗隐写分析能力、隐 藏容量等内容;最后是本文的总结.

# 2 视频编码与运动矢量隐写相关工作

在视频编码过程中,视频预测帧主要通过存储 宏块运动矢量和运动残差实现宏块的压缩存储.为 了方便描述本文隐写算法,本节首先对视频编码和 运动矢量隐写相关工作加以说明,并给出本文统一 的形式化描述方法.

#### 2.1 当前块

一个待编码视频帧,在编码压缩前会被分割为 特定大小的宏块.设需要编码的宏块大小为 *m×n* 像素,则其亮度信息是由 *m×n* 个像素组成的矩阵. 该亮度宏块称为当前块,可表示为

 $\mathbf{B}_{m \times n} = (b_{i,i})_{m \times n}, \ 0 \le i < m, \ 0 \le j < n \ (1)$ 

当前块是编码压缩之前的无失真宏块,由于视频编码过程会造成宏块的信号损失,因此当前块仅存在于编码开始之前.一般彩色视频宏块由亮度和 色度组成,为了方便研究,本文代价计算和视频分析 均在亮度宏块上进行,文中的宏块也是指亮度宏块, 后面不再说明.

#### 2.2 运动矢量与参考块

编码时,编码器需要在参考帧(该帧一般与当前 块所在的帧相邻)中搜索与当前块尽可能相同的参 考块,并进行两者残差计算以消除冗余.编码器使用 运动矢量(*H*,*V*)表示参考块与当前块的相对位置, 不同的运动矢量会对应不同的参考块.其中*H*和*V* 分量分别表示参考块和当前块在水平和垂直方向上 的相对偏移.本文用  $\mathbf{R}_{m\times n}^{(H,V)}$ 表示运动矢量(H,V)所指向的参考块矩阵,如式(2)所示:

 $\mathbf{R}_{m \times n}^{(H,V)} = (r_{i,j}^{(H,V)})_{m \times n}, 0 \le i < m, 0 \le j < n$  (2) 为了便于理解,图 1 给出了当前块  $\mathbf{B}_{m \times n}$ 、参考 块  $\mathbf{R}_{m \times n}^{(H,V)}$ 与运动矢量(H,V)三者之间的关系.



图 1 运动矢量指向的参考块

为了提高运动矢量的预测精度,编码器选择运动矢量偏移的单位可以是整数像素,也可以是二分之一像素或者四分之一像素.非整数像素精度下运动矢量对应的参考块可以通过对参考帧像素插值得到.



图 2 运动矢量(H,V)与(H+1,V+1)对应的参考块

简单地,假设运动矢量为整像素精度,以图 2 为 例,实线 8×8 区域为参考块  $R_{8\times8}^{(H,V)}$ . 当运动矢量变 为(H+1,V+1)时,得到调整后即虚线参考块  $R_{8\times8}^{(H+1,V+1)}$ ,其表示参考块位置与当前位置在水平和 垂直方向上各相差 1 个像素.

#### 2.3 宏块残差与 SAD

编码时,编码器将当前块减去参考块,获得的残差矩阵  $D_{m\times n}^{(H,V)}$ 可描述如下:

 $\boldsymbol{D}_{m \times n}^{(H,V)} = (d_{i,j}^{(H,V)})_{m \times n}, 0 \leq i < m, 0 \leq j < n \quad (3)$ 该矩阵也可写成当前块  $\boldsymbol{B}_{m \times n}$ 与参考块  $\boldsymbol{R}_{m \times n}^{(H,V)}$ 差值的表达式,即

$$\boldsymbol{D}_{m \times n}^{(H,V)} = \boldsymbol{B}_{m \times n} - \boldsymbol{R}_{m \times n}^{(H,V)} = (b_{i,j} - r_{i,j}^{(H,V)})_{m \times n},$$
  
$$0 \le i \le m, \ 0 \le i \le n$$
(4)

编码器对宏块的编码主要通过存储运动矢量 和残差实现.为了进一步降低存储开销,编码器会将 残差矩阵进行有损压缩.残差矩阵 **D**<sub>m×n</sub><sup>(H,V)</sup> 会依次经 过 DCT、量化、反量化以及逆 DCT 变为量化残差 **D**'<sub>m×n</sub><sup>(H,V)</sup>,该过程可用式(5)表示:

 $D'_{m \times n}^{(H,V)} = iDCT(iQ(Q(DCT(D_{m \times n}^{(H,V)}))))$ (5) 其中,  $DCT(\cdot)$ 为 DCT 变换;  $iDCT(\cdot)$ 为 DCT 逆变 换;  $Q(\cdot)$ 为 DCT 系数矩阵量化操作;  $iQ(\cdot)$ 为反量 化操作. 通过残差量化, 宏块被存储为运动矢量 (H,V)和量化残差  $D'_{m \times n}^{(H,V)}$ . 这里  $D_{m \times n}^{(H,V)}$ 为编码量化 前残差, 即编码端的残差,  $D'_{m \times n}^{(H,V)}$ 为有损量化的残 差, 即解码端的残差.

显然,残差矩阵非零数值越多,绝对值越大,越 不利于视频的压缩存储.为了度量残差代价大小,编 码器一般使用残差矩阵各元素绝对值之和,即误差 绝对和 SAD(Sum of Absolute Difference)评价运 动矢量代价. SAD 数值代表了编码代价的大小,编 码器选用的运动矢量一般会对应较小的 SAD.

#### 2.4 重建块

在编码端,当前块  $B_{m \times n}$ 最终会被编码为运动矢量(H,V)和量化后的残差  $D'^{(H,V)}_{m \times n}$ .这样编码后可得到  $B_{m \times n}$ 的重建块  $B'^{(H,V)}_{m \times n}$ .

$$\boldsymbol{B}_{m \times n}^{\prime(H,V)} = \boldsymbol{R}_{m \times n}^{(H,V)} + \boldsymbol{D}_{m \times n}^{\prime(H,V)}$$
(6)

由于重建块的残差经过了有损量化处理,故重 建块 **B**<sup>'(H,V)</sup>与当前块 **B**<sub>m×n</sub>存在一定失真,这些差异 也就是视频压缩的失真.

进一步地,本文将重建块描述为式(7):

 $\boldsymbol{B}_{m \times n}^{\prime (H,V)} = (b_{i,j}^{\prime (H,V)})_{m \times n}, \ 0 \le i < m, \ 0 \le j < n \ (7)$ 

依据之前描述, $B_{m\times n}$ 为当前块(编码端量化失 真前的宏块), $B'^{(H,V)}_{m\times n}$ 为重建块(有损量化后宏块).

#### 2.5 运动矢量隐写

视频在正常编码时,运动矢量(H,V)指向参考 块 $R_{m\times n}^{(H,V)}$ ,因此 $B_{m\times n}$ 经量化压缩后成为重建块  $B'_{m\times n}^{(H,V)}$ ,整个过程可用式(8)描述:

 $\boldsymbol{B}_{m \times n}^{\prime(H,V)} = \boldsymbol{R}_{m \times n}^{(H,V)} + \boldsymbol{D}_{m \times n}^{\prime(H,V)}$ 

 $= \mathbf{R}_{m \times n}^{(H,V)} + iDCT(iQ(Q(DCT(\mathbf{D}_{m \times n}^{(H,V)})))) (8)$ 

图 3 是式(8)的具体流程,当前块  $B_{m\times n}$ 被编码 为重建块运动矢量(H,V)和量化残差  $D'_{m\times n}^{(H,V)}$ .

视频运动矢量隐写算法在隐写时,运动矢量 (*H*,*V*)会在残差计算前通过一种嵌入方法(假设为 Emb(•))嵌入秘密信息变为(*Ĥ*,*V*):



图 3 宏块重建过程

 $(\hat{H}, \hat{V}) = \operatorname{Emb}(H, V) \tag{9}$ 

然后,编码器计算改动的运动矢量对应的残差 及其量化残差,并进行宏块编码.即隐写后,( $\hat{H},\hat{V}$ ) 指向新的参考块  $R_{m\times n}^{(\hat{H},\hat{V})}$ ,当前块  $B_{m\times n}$ 也会编码得到 新的重建块  $B'_{m\times n}^{(\hat{H},\hat{V})}$ :

 $\boldsymbol{B}_{m \times n}^{\prime(\hat{H},\hat{V})} = \boldsymbol{R}_{m \times n}^{(\hat{H},\hat{V})} + \boldsymbol{D}_{m \times n}^{\prime(\hat{H},\hat{V})}$ 

 $= \mathbf{R}_{m \times n}^{(\hat{H}, \hat{V})} + iDCT(iQ(Q(DCT(\mathbf{D}_{m \times n}^{(\hat{H}, \hat{V})})))) (10)$ 

运动矢量变化后,残差和参考块会随着改变,由于  $B'_{m\times n}^{(\hat{H},\hat{V})}$  与 $B'_{m\times n}^{(H,V)}$ 都与 $B_{m\times n}$ 十分接近,因此隐写前后视频画面变化一般不可察觉.

# 3 运动矢量局部最优性与相邻相关性

目前已有的运动矢量隐写分析主要依赖运动矢 量局部最优性和相邻相关性进行特征构造.前者特 征需要借助运动矢量残差进行特征提取,较少研究 各运动矢量相互关系.后者特征则借助运动矢量本 身相关性进行提取,不关心运动矢量残差代价.为了 能够控制这两种隐写分析带来的被检测风险.本部 分对于运动矢量局部最优性和相邻相关性分别进行 分析,讨论控制两种失真的方法.

#### 3.1 本文对运动矢量局部最优性的分析

运动矢量局部最优性:在编码器端,由于编码器 会让运动矢量(H,V)尽可能指向与当前块 $B_{m\times n}$ 相 同的参考块 $R_{m\times n}^{(H,V)}$ ,即他们之间的残差 SAD 最小. 一般来说,此时处于(H,V)周围的运动矢量对应的 残差代价 SAD 都会大于(H,V)对应的 SAD,这种 局部最低代价的性质即运动矢量的局部最优.

如图 4,最优运动矢量(H,V)相邻有 8 个运动 矢量,记为( $H\pm\Delta1,V\pm\Delta2$ ).这里  $\Delta1$  与  $\Delta2$  均为变 量,取 0 或 1,且不同时为 0.由于一般运动矢量(H,V) 对应代价不高于周围 8 个邻域中的任何 1 个,则 (H,V)为局部最优运动矢量.

这种局部最优性在编码端显然存在,然而由于 编码量化的影响,处于解码端的隐写分析者所研究 的局部最优性已遭受了编码过程所带来的破坏.但

(H-1,V-1)	( <i>H</i> , <i>V</i> -1)	(H+1,V-1)
(H-1,V)	(H <b>,</b> V)	( <i>H</i> +1, <i>V</i> )
(H-1,V+1)	( <i>H</i> , <i>V</i> +1)	(H+1,V+1)

图 4 运动矢量及其周围 8 个相邻矢量

文献[19]中已证明该局部最优性依然很好保持,并 且隐写会降低这种最优性概率.于是,无论在编码端 还是解码端,一个预测帧内的运动矢量满足局部最 优的概率代表了该帧运动矢量的局部最优性.若该 帧内的运动矢量被改写过,一般都会造成代价增大, 引起最优概率下降的异常.

在编码器端,运动矢量(H,V)指向参考块,于 是残差由当前块减去参考块得到,对应 SAD 可以 用式(11)表示:

$$SAD(\boldsymbol{B}_{m \times n} - \boldsymbol{R}_{m \times n}^{(H,V)}) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} |b_{i,j} - \boldsymbol{r}_{i,j}^{(H,V)}| \quad (11)$$

同样在解码器端,残差为量化残差,可以通过残 差解码直接获得.将其写成重建块与参考块的差值, 并将对应的 SAD 用式(12)描述如下:

$$SAD(\boldsymbol{B}_{m \times n}^{\prime(H,V)} - \boldsymbol{R}_{m \times n}^{(H,V)}) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} |b_{i,j}^{\prime(H,V)} - r_{i,j}^{(H,V)}|$$
(12)

由于编码器搜索出的运动矢量会尽可能做到最小 SAD, 一般认为编码端的运动矢量均满足局部最优,即编码端最优概率 P<sub>opt</sub> (H,V)是 1, 用式(13)表示如下:

 $P_{opt}(H,V) = P(SAD(\boldsymbol{B}_{m \times n} - \boldsymbol{R}_{m \times n}^{(H,V)}))$ 

$$\leq SAD(\boldsymbol{B}_{m \times n} - \boldsymbol{R}_{m \times n}^{(H \pm \Delta 1, V \pm \Delta 2)})) = 1 (13)$$

当解码时,由于  $B_{m\times n}$ 存在信息丢失无法完全恢 复,隐写分析特征可能使用  $B_{m\times n}$ 的重建块  $B'_{m\times n}^{(H,V)}$ 估 算周围运动矢量  $(H \pm \Delta 1, V \pm \Delta 2)$ 的代价. 假设  $(H+\delta 1, V+\delta 2)$ 是 $(H\pm\Delta 1, V\pm\Delta 2)$ 中最小代价的 一个运动矢量 $(\delta 1, \delta 2$ 分别为 $\pm\Delta 1$ 和 $\pm\Delta 2$ 的一个确 定取值,下同,本文中均用此表示邻域中代价最小的 运动矢量). 局部最优概率由编码端的  $P_{opt}(H,V)$ 变 为了解码端的  $P'_{opt}(H,V)$ . 依据文献[19],在正常情 况下,两者较接近:

$$P'_{opt}(H,V) = P(SAD(\boldsymbol{B}'_{m\times n}^{(H,V)} - \boldsymbol{R}_{m\times n}^{(H,V)})$$

$$\leq SAD(\boldsymbol{B}'_{m\times n}^{(H,V)} - \boldsymbol{R}_{m\times n}^{(H+\delta 1,V+\delta 2)}))$$

$$\approx P_{opt}(H,V)$$
(14)

当运动矢量(H,V)被隐写变为( $\hat{H}$ , $\hat{V}$ )时,会造 成代价增大.此时,若有当代价较小的运动矢量仍在其 邻域中时,则会造成非最优异常,于是有 $P'_{opt}(H,V) >$  $P'_{opt}(\hat{H},\hat{V})$ .如果运动矢量在较大范围内调整,显然 并不能保证调整过后运动矢量依然局部最优,因此 同样会造成 $P'_{opt}(H,V) > P'_{opt}(\hat{H},\hat{V})$ 异常.但是在 这个大的区域内,可能会存在少数特殊的位置,使得 运动矢量依然满足局部最优,此时最优概率不下降, 从而使得 $P'_{opt}(H,V) = P'_{opt}(\hat{H},\hat{V})$ .然而隐写修改并 不能保证一定会使原运动矢量调整到该特殊位置, 所以隐写算法大多都会造成最优概率下降的失真.

为了保持局部最优性,则构造嵌入函数 E(•)需要让最优概率下降最小:

 $E(\bullet) = \arg\min(P'_{obt}(H,V) - P'_{obt}(\hat{H},\hat{V})) (15)$ 

类似式(13),当隐写分析时,含密运动矢量 (Ĥ,Ŵ)在解码端的最优概率,即隐写后残差 SAD 的最小概率为

$$P'_{opt}(\hat{H},\hat{V}) = P(SAD(\boldsymbol{B}^{\prime(\hat{H},\hat{V})}_{m \times n} - \boldsymbol{R}^{(\hat{H},\hat{V})}_{m \times n}))$$

$$\leq SAD(\boldsymbol{B}^{\prime(\hat{H},\hat{V})}_{m \times n} - \boldsymbol{R}^{(\hat{H}\pm\Delta1,\hat{V}\pm\Delta2)}_{m \times n}))(16)$$

若原始最优的运动矢量(H,V)处于隐写后运 动矢量( $\hat{H}$ , $\hat{V}$ )的邻域( $\hat{H} \pm \Delta 1$ , $\hat{V} \pm \Delta 2$ )内,即 (H,V) $\in$ ( $\hat{H} \pm \Delta 1$ , $\hat{V} \pm \Delta 2$ )时,( $\hat{H}$ , $\hat{V}$ )的 SAD 显然 非最小,即( $\hat{H}$ , $\hat{V}$ )非最优.

$$SAD(\boldsymbol{B}_{m \times n} - \boldsymbol{R}_{m \times n}^{(\hat{H}, \hat{V})}) \geq \\ \min(SAD(\boldsymbol{B}'_{m \times n}^{(\hat{H}, \hat{V})} - \boldsymbol{R}_{m \times n}^{(\hat{H} \pm \Delta 1, \hat{V} \pm \Delta 2)})) \quad (17)$$

此时,在( $\hat{H}\pm\Delta1$ , $\hat{V}\pm\Delta2$ )中,由于可能存在比 (H,V)代价更小的运动矢量,于是( $\hat{H}$ , $\hat{V}$ )非最优的 可能性更大.对于常见的运动矢量 LSB 隐写,隐写 后的运动矢量( $\hat{H}$ , $\hat{V}$ )最优概率存在一个由(H,V) 代价确定的上限:

$$P'_{opt}(\hat{H}, \hat{V}) \leq P(SAD(\boldsymbol{B}'_{m \times n}^{(\hat{H}, \hat{V})} - \boldsymbol{R}_{m \times n}^{(\hat{H}, \hat{V})})$$
$$\leq SAD(\boldsymbol{B}'_{m \times n}^{(\hat{H}, \hat{V})} - \boldsymbol{R}_{m \times n}^{(H, V)})) \quad (18)$$

基于本文以上分析,最优概率  $P'_{opt}(\hat{H},\hat{V})$ 在压缩过程中可以得到如下两个情况及其结论:

**情况1.** 若残差在压缩过程中被无损保存,其 在解码端都能被无损重建.

$$\boldsymbol{B}_{m \times n} = \boldsymbol{B}'_{m \times n}^{(\hat{H}, \hat{V})} = \boldsymbol{B}'_{m \times n}^{(H, V)}$$
(19)

这种无损重建的情况可以看成是对残差的无损 压缩过程.此时所关注的解码端的局部最优性事实 上与编码端完全相同.即运动矢量(*H*,*V*)的代价必 然达到邻域最小.而若要(*Ĥ*,*V*)也最优,则(*Ĥ*,*V*) 代价必须与(*H*,*V*)代价相等.

$$P_{opt}'(\hat{H},\hat{V}) = P(SAD(\boldsymbol{B}_{m \times n} - \boldsymbol{R}_{m \times n}^{(\hat{H},\hat{V})})$$
$$= SAD(\boldsymbol{B}_{m \times n} - \boldsymbol{R}_{m \times n}^{(H,V)})) \qquad (20)$$

情况 2. 若进行压缩量化,则量化残差  $D'_{m\times n}^{(H,V)}$ 能量变小,这个过程可以看作重建块  $B'_{m\times n}^{(\hat{H},\hat{V})}$  在接近 参考块  $R_{m\times n}^{(\hat{H},\hat{V})}$ :

$$\boldsymbol{B}_{m\times n}^{\prime(\hat{H},\hat{V})} = \boldsymbol{R}_{m\times n}^{(\hat{H},\hat{V})} + \boldsymbol{D}_{m\times n}^{\prime(\hat{H},\hat{V})}$$
(21)

特别地,若量化后残差为 0,即  $D'_{m\times n}^{(H,V)} = 0,则重$ 建块等于参考块,即  $B'_{m\times n}^{(\dot{H},\dot{V})} = R_{m\times n}^{(\dot{H},\dot{V})}$ .此时运动矢量 代价一定达到局部最低代价,即局部最优.

$$P_{opt}'(\hat{H},\hat{V}) =$$

$$P\left(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \left| r_{i,j}^{(\hat{H},\hat{V})} - r_{i,j}^{(\hat{H}+\delta_{1},\hat{V}+\delta_{2})} \right| \ge 0 \right) = 1$$
(22)

基于以上两点,可见运动矢量进行改动后,代价 增加越小或者压缩量化越剧烈,新运动矢量的局部 最优性越好.

对于纹理复杂的宏块,当调整运动矢量后,残差 很可能极大增加,不利于局部最优性的保持.同时, 该类型宏块残差可能会包含更多的低频信号,不利 于 DCT 量化抹除.因此纹理越复杂,越不利于保持 隐写运动矢量的局部最优性.

对于纹理平坦的宏块,宏块像素数值基本相同, 而当运动矢量进行加减1调整以后,嵌入前后的两 个参考块之间也存在较大的重叠区域.这导致总体 代价不会有显著增加.

基于以上分析,使用相邻像素变化较为平缓的 宏块进行隐写可以较好保持运动矢量的局部最优概 率.并且由于残差代价增加较小,视频码率也可以得 到很好控制.

#### 3.2 本文对运动矢量相关性的分析

运动矢量相关性一般是指运动矢量与其他运动 矢量的相似性.相似性可表现为一定概率的相同或 者接近.一般单帧视频运动矢量较为一致,其各分量 可近似看成以均值附近密集,而距离均值越远越稀 疏的分布.假设当一个运动矢量的分量使用加1进 行隐写改动时,其与剩余的每个运动矢量的对应分 量相似性都会变化(可能更接近也可能相差更大). 若其与更多的运动矢量靠近,而与较少的运动矢量 远离时,可认为利用加1嵌入对此运动矢量相关性 的保持要好于减1进行的改动,反之亦然.

一般地,假设有 t 个相邻运动矢量的序列,这里 记为 $(H_1, V_1), (H_2, V_2), \dots, (H_i, V_i), \dots, (H_t,$  $V_i)$ .现在若仅仅对运动矢量 $(H_i, V_i)$ 的 H 分量进 行隐写改动,其余分量均不变,那么隐写后该运动矢 量序列变为 $(H_1, V_1), (H_2, V_2), \dots, (\hat{H}_i, V_i), \dots,$   $(H_t, V_t)$ . 这里一般  $\hat{H}_i = H_i \pm 1$ , V 分量隐写前后不 变化. 隐写后应当使得  $\hat{H}_i$  与剩余 H 分量平均距离  $\mu_t$ 最近

$$\hat{H}_i = H_i \pm 1 = \arg\min|H_i \pm 1 - \mu_h|$$
 (23)

基于以上分析,一种相比于随机加减1更好的 保持运动矢量 H 分量相关性的嵌入规则如下:

$$\hat{H}_i = \begin{cases} H_i + 1, \ H_i \leq \mu_h \\ H_i - 1, \ H_i > \mu_h \end{cases}$$
(24)

事实上,以V分量隐写与H分量同理,运动矢量V分量嵌入规则如下:

$$\hat{V}_{i} = \begin{cases} V_{i} + 1, \ V_{i} \leq \mu_{v} \\ V_{i} - 1, \ V_{i} > \mu_{v} \end{cases}$$
(25)

这里 µ<sub>h</sub>和µ<sub>v</sub>分别是该视频帧内水平和垂直分 量均值.理论上,使用加减1匹配嵌入可以让更多运 动矢量分量聚拢,提高运动矢量一致性,降低隐写带 来的相关性异常.

# 4 AMC 隐写与提取算法

#### 4.1 宏块复杂度

基于 3.1 节的分析,纹理平坦的宏块更有利于 保持局部最优.为了描述宏块  $B'_{m\times n}^{(H,V)}$ 纹理,本文定 义重建块  $B'_{m\times n}^{(H,V)}$ (参照式(7)定义)的复杂度如下:  $C(B'_{m\times n}^{(H,V)}) =$ 

$$\left\lfloor \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-2} (b'_{i,j}^{(H,V)} - b'_{i,j+1}^{(H,V)})^2 + \sum_{i=0}^{m-2} \sum_{j=0}^{n-1} (b'_{i,j}^{(H,V)} - b'_{i+1,j}^{(H,V)})^2}{(m-1)n + m(n-1)} \right\rfloor$$
(26)

其中, [•」为下取整操作.式(26)用于计算重建块在 水平和垂直两个方向上像素差值平方的均值, 描述 了宏块中相邻像素的跳变剧烈程度.若 C(**B**'<sup>(H,V)</sup><sub>m×n</sub>) 数值越大, 表明重建块 **B**'<sup>(H,V)</sup><sub>m×n</sub> 纹理越复杂, 反之宏 块越平坦.

图 5 中,图 5(a)、图 5(b)、图 5(c)和图 5(d)分

别为 bridge、foreman、flower、stefan 视频序列在以 比特率为 1000 Kbps 压缩后宏块复杂度的概率分 布.图 5(a)表明 bridge 视频有超过 80%的宏块复杂 度低于 100,几乎全部的宏块复杂度不超过 400. 图 5(b)表明 foreman 视频有超过 70%的视频复杂 度不高于 100,几乎全部的宏块复杂度不超过 500. 图 5(c)表明 flower 视频有超过 50%的宏块复杂度低 于 100,其余宏块复杂度几乎均匀分布于 100~3000 之间.图 5(d)表明 stefan 视频有接近 40%复杂度的 宏块小于 100,其余复杂度分布于 100~1500 之间.

基于以上对比,可以看出虽然不同视频宏块复杂度分布差异较大,但多数宏块仍集中于复杂度数 值较小一端.利用低复杂度宏块进行隐写,可以提供 足够隐写空间.另一方面说明,某些视频由于宏块复 杂度普遍较大,如果不进行复杂度挑选而进行隐写, 有极大可能造成局部最优概率异常.

图 6 中,图 6(a)、图 6(b)、图 6(c)分别为 foreman 视频在 100 Kbps、1000 Kbps 和 3000 Kbps 比特率 下,宏块复杂度的概率分布.在低数值端,压缩率对 复杂度分布影响较大,压缩越剧烈,低复杂度宏块数 目越多.在高数值端(大于 500),压缩率对复杂度分



图 6 foreman 在不同压缩率下的复杂度分布



布影响较小.该规律表明,视频运动矢量隐写时,比特率越低,宏块复杂度相对越低,同时由于残差 SAD 也会因为低比特率变得更小甚至为 0,更有利于运动矢量局部最优保持.

图 7 为 foreman 视频多个比特率下,取所有的 宏块复杂度均值.对于同一视频,比特率与复杂度均 值基本呈正相关.



图 7 比特率与宏块复杂度的关系

#### 4.2 运动矢量 LSB 匹配修改

基于 3.2 节的分析,本文隐写算法使用 LSB 匹 配将每个宏块中运动矢量 H 分量和 V 分量各嵌入 1 比特秘密信息,其中每个宏块可以嵌入 s<sub>1</sub>与 s<sub>2</sub>共 2 比特秘密信息.

H分量嵌入函数如式(27):

$$\hat{H} = \operatorname{Emb}(H, \mu_h, s_2) = \begin{cases} H, & \operatorname{LSB}(H) = s_2 \\ H+1, & H \le \mu_h \\ H-1, & H > \mu_h \end{cases}$$

$$(27)$$

V分量的嵌入函数如式(28):

$$\hat{V} = \text{Emb}(V, \mu_{v}, s_{1}) = \begin{cases} V, & \text{LSB}(V) = s_{1} \\ V+1, & V \le \mu_{v} \\ V-1, & V > \mu_{v} \end{cases}$$
(28)

本文实验的视频大多以静止镜头为主,运动矢 量水平和垂直分量的均值接近 0.为了方便,嵌入算 法 μ, 与 μ, 均取 0.

#### 4.3 AMC 隐写算法

隐写过程分为两次压缩:第1次压缩用于统计载体复杂度分布,确定隐写阈值;第2次压缩则进行隐写.隐写时,对于当前帧 $F_B$ 中每一个包含运动矢量的当前块 $B_{m\times n}$ ,进行正常编码,得到最优运动矢量(H,V)及对应的重建块 $B'_{m\times n}^{(H,V)}$ .若 $C(B'_{m\times n}^{(H,V)}) \leq \lambda$ ,则进行运动矢量的改写嵌入,否则保持不变.嵌入完毕,得到隐写后运动矢量 $(\hat{H},\hat{V})$ 及新的重建块

 $B'_{m\times n}^{(\hat{H},\hat{V})}$ ,将这个重建块放入编码帧 $F'_{B}$ .若 $C(B'_{m\times n}^{(H,V)}) \leq \lambda$ ,则此嵌入比特有效,k+2,否则,k-2,但放入编码 帧 $F'_{B}$ 中的 $B'_{m\times n}^{(\hat{H},\hat{V})}$ 保留,即(H,V)被改写为( $\hat{H},\hat{V}$ ), 但未嵌入秘密信息.

λ 为复杂度的自适应阈值,其在视频第一次压缩时计算:统计所有宏块复杂度数值  $c = C(\mathbf{B}'_{m \times n}^{(H,V)})$ 及其出现次数  $n_i$ . 然后从  $\lambda = 0$  开始,依次计算满足阈值的宏块数目 N.

$$N = \sum_{c=0}^{\lambda} n_i \tag{29}$$

若隐写嵌入需要使用宏块个数为 N<sub>0</sub>,则复杂度 自适应阈值取

 $\lambda = \arg\min(N - N_0) \ge 0 \tag{30}$ 

载体视频重新进行第2次编码压缩实现嵌入, 单帧的 AMC 嵌入算法如下.

算法1. AMC嵌入算法.

输入:参考帧  $F_R$ ,当前帧  $F_B$ , $\lambda$ ,信息  $S_i$ , $i=1,2,\cdots$ 输出:隐写帧  $F'_B$ 

1. 
$$k = 0$$

6.

2. FOR EACH  $B_{m \times n}$  IN  $F_B$  DO:

- 3. 获得当前块的运动矢量(H,V)
- 4. 以(H,V)编码宏块  $B_{m \times n}$ 得到  $B'_{m \times n}^{(H,V)}$ :  $B'_{m \times n}^{(H,V)} = R_{m \times n}^{(H,V)} + iDCT(iQ(Q(DCT(B_{m \times n} - R_{m \times n}^{(H,V)}))))$

5. IF 
$$C(\mathbf{B}'^{(H,V)}) \leq \lambda$$
 THEN(控制局部最优)

$$\hat{H} = \operatorname{Emb}(H, 0, S_k)$$
(控制  $H$  相关性)  
 $\hat{V} = \operatorname{Emb}(V, 0, S_{k+1})$ (控制  $V$  相关性)

7. 以(Ĥ, Ѷ) 编码 
$$\boldsymbol{B}_{m \times n}$$
得到  $\boldsymbol{B}'^{(H,V)}_{m \times n}$ :  
 $\boldsymbol{B}'^{(\hat{H},\hat{V})}_{m \times n} = \boldsymbol{R}^{(\hat{H},\hat{V})}_{m \times n} + iDCT(iQ(Q(DCT(\boldsymbol{B}_{m \times n} - \boldsymbol{R}^{(\hat{H},\hat{V})}_{m \times n}))))$ 

- 8. k = k + 2
- 9. 将隐写后重建块  $\boldsymbol{B}'_{m\times n}^{(\hat{H},\hat{V})}$  放入隐写帧  $F'_{B}$
- 10. IF  $C(\boldsymbol{B}'_{m \times n}^{(\hat{H},\hat{V})}) > \lambda$  THEN

- 12. END IF
- 13. ELSE 将原重建块  $B'_{m\times n}^{(H,V)}$  放入编码帧  $F'_B$
- 14. END IF
- 15. END FOR
- 16. RETURN  $F'_B$

嵌入流程通过选择复杂度低于阈值的宏块进行 运动矢量隐写操作.每个运动矢量可以嵌入 2 比特 信息.由于嵌入过程可能会造成重建块复杂度高于 阈值,使得在提取端无法正确提取该 2 比特信息,导 致提取失败.因此,嵌入时使用 k 表示已嵌入秘密信 息比特的长度,即嵌入进度.嵌入算法需要对嵌入后 的宏块复杂度进行再计算,若高于阈值 λ,运动矢量 的修改操作不变动,仅将嵌入进度回退2比特,这样 隐写算法会选择下一位置重新嵌入.

#### 4.4 AMC 提取算法

单帧的 AMC 提取算法如算法 2. **算法 2.** AMC 提取算法. 输入:隐写帧  $F'_{B}$ ,复杂度阈值  $\lambda$ 输出:k 比特秘密信息  $S_{i}$ , $0 \leq i < k$ 

- 1. FOR EACH  $B'_{m \times n}^{(H,V)}$  IN  $F'_B$  DO:
- 2. k = 0
- 3. IF  $C(\boldsymbol{B}'_{m \times n}^{(H,V)}) \leq \lambda$  THEN
- 4. 提取  $S_k = \text{LSB}(H)$ ,  $S_{k+1} = \text{LSB}(V)$
- 5. k = k + 2
- 6. ELSE 继续下一宏块
- 7. END IF
- 8. END FOR
- 9. RETURN  $S_i$ ,  $0 \leq i < k$

遍历所有满足条件  $C(\mathbf{B}'_{m\times n}^{(H,V)}) \leq \lambda$  的宏块,依次 提取运动矢量 H 和 V 分量 LSB 位,并将 2 比特秘密信息放入提取比特序列. 当秘密信息提取长度达到参数约定长度后,停止提取,并返回提取的秘密信息比特序列.

### 5 对比实验

#### 5.1 实验样本库

实验共使用到 YUV 标准视频库 34 段,以 1000 Kbps(该比特率在 352×288 视频中较普遍使 用)恒定比特率、采用编码器默认的半像素精度运动 矢量制作全 P 帧视频. 本文使用 Xvid-1.3.2<sup>①</sup> 编解 码 MPEG-4 视频进行实验,均使用 16×16 宏块进 行运动矢量嵌入. 样本隐写算法包括 Xu<sup>[6]</sup>、Alv<sup>[7]</sup>和 Cao<sup>[8]</sup>、Zhang<sup>[12]</sup>以及本文 AMC 算法. 为了进行更 好的对比,排除 STC 编码对 Zhang 隐写效果的提升 作用,本文将式(26)中取整前宏块复杂度作为代价 函数结合 STC 对水平分量 H 和垂直分量 V 分别嵌 入,制作 AMC-STC 隐写样本.以上这些隐写算法包 括 0.2 bpmv、0.4 bpmv、0.6 bpmv、0.8 bpmv 共 4 种 相对嵌入率.其中AMC 隐写算法另外制作 1.0 bpmv 嵌入率样本用于视觉画面对比. 这里 bpmv(bit per motion vector)表示平均每个运动矢量(包括 H 和 V两个分量)嵌入的比特数.

为了达到嵌入率要求,以及各类算法的最优,本 文中 Xu 算法选择运动矢量分量绝对值大于 0 的宏 块嵌入,Aly 算法使用残差不为 0 的宏块进行嵌入. 以上两种算法阈值选定主要考虑其满足足够的嵌入 容量,事实上,这两种算法阈值的选择对于本文实验 对比效果影响较小. Cao 算法次优运动矢量参数选 取阈值 1.1,即次优运动矢量代价不高于原始运动 矢量代价 1.1 倍. 该阈值越低对于 Cao 算法的安全 性相对越高. 阈值 1.1 可以使得 Cao 算法具备较高 的安全性,且具备足够的嵌入空间.

### 5.2 不可见性测试

为了使得选取的视频具有普遍性,依据宏块复杂 度自适应阈值由低到高,依次选取 bridge、foreman、 flower 和 stefan 共 4 段视频的 cover 样本,以及对 应的相对嵌入率为 1.0 bpmv,比特率为 1000 Kbps 的 stego 样本,进行对应帧画面比较.

利用算法 1 嵌入,图 8 中 stego 样本自适应阈值 λ 依次为 2,22,106 和 275. 画面对比表明,在1.0 bpmv





cover

stego

图 8 视频隐写前后画面对比

① Xvid Codec 1.3.2 [EB/OL]. https://www.xvid.com/ download/

(单位:Kbps)

较高嵌入率下,隐写失真不可察觉.为了进行更精确的失真度对比,本文对4段视频各个嵌入率样本计算对应的峰值信噪比 *PSNR*(Peak Signal to Noise Ratio),公式如下:

$$MSE = \frac{1}{width \times height} \sum_{i=1}^{height} \sum_{j=1}^{width} (x_{i,j} - y_{i,j})^{2} (31)$$

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{32}$$

这里 MSE(Mean Square Error)为均方误差, width 和 height 分别为视频帧的宽度和高度,x<sub>i,j</sub>为 原始未压缩视频帧中第 i 行第 j 列的亮度像素,y<sub>i,j</sub> 为压缩后视频帧中第 i 行第 j 列的亮度像素.分别 计算 cover 样本和各 stego 样本相对原始未压缩视 频的 PSNR,求得多帧均值对比如表 1 所示.

		表 1	PSNR 对比		(单位:dB)
样本	嵌入率	bridge	foreman	flower	Stefan
cover	\	39.60	38.79	30.36	33.18
Xu	0.2	39.57	38.66	30.21	33.01
Aly	0.2	39.56	38.64	30.05	33.03
Cao	0.2	39.60	38.75	30.35	33.18
Zhang	0.2	39.58	38.78	30.32	33.18
AMC	0.2	39.59	38.78	30.35	33.18
Xu	0.4	39.53	38.54	30.11	32.97
Aly	0.4	39.50	38.50	29.83	32.85
Cao	0.4	39.58	38.72	30.32	33.16
Zhang	0.4	39.58	38.77	30.32	33.17
AMC	0.4	39. 58	38.75	30.35	33.18
Xu	0.6	39.48	38.41	29.95	32.83
Aly	0.6	39.46	38.42	29.66	32.79
Cao	0.6	39.55	38.72	30.31	33.11
Zhang	0.6	39.57	38.70	30.29	33.14
AMC	0.6	39.57	38.72	30.33	33.18
Xu	0.8	39.41	38.27	29.78	32.67
Aly	0.8	39.39	38.31	29.39	32.63
Cao	0.8	39.51	38.68	30.29	33.10
Zhang	0.8	39.56	38.68	30.27	33.14
AMC	0.8	39.55	38.71	30.32	33.15

相对人的视觉,各类算法都能做到不可察觉.但 PSNR的数值表明算法画面失真程度存在差异,有可能会被潜在的隐写分析方法捕捉,从而导致算法 安全性下降.

表1可以看出 cover 样本 PSNR 数值基本高于 所有 stego,表明隐写嵌入一般都会不同程度造成画 面质量下降.

Xu和 Aly 算法会较大影响画面质量,峰值信 噪比相比 cover 低大约 0.1 dB~0.6 dB 左右,最高 下降 0.97 dB.

Cao 样本相比 cover 峰值信噪比下降 0.1 dB 左 右,下降幅度较小.

Zhang 样本与 Cao 样本相比,其画面质量相差 不大,均能保持和 cover 接近的峰值信噪比.

本文 AMC 算法在隐写样本中画面质量最高, PSNR 数值和 cover 相差约 0~0.05 dB. 其在未使 用编码情况下,修改率要高于 Zhang 算法,但画面 质量依然较好. 在某些情况下,AMC 相比 cover 的 PSNR 数值差距小于 0.01 dB 或者和 cover 相同,隐 写对画面几乎未造成失真.

#### 5.3 比特率测试

比特率的增加是另一种隐写失真,其反应了隐 写运动矢量带来的残差代价增加情况.本文选择编 码器默认固定量化步长(编码器中 quant = 4,这样 可以保证各样本处于同样的压缩强度)制作 cover 和 stego 样本,比特率越高,代表其残差代价越大. 各视频比特率(单位:Kbps)对应如表 2 所示.

表 2 比特率对比

样本	嵌入率	bridge	foreman	flower	Stefan
cover	\	670.72	1019.31	3362.13	2579.34
Xu	0.2	694.19	1048.32	3444.05	2632.82
Aly	0.2	708.27	1050.88	3489.71	2646.47
Cao	0.2	684.80	1024.00	3367.68	2586.17
Zhang	0.2	680.53	1021.87	3368.53	2582.76
AMC	0.2	672.00	1020.59	3362.56	2581.62
Xu	0.4	712.11	1073.92	3505.49	2676.05
Aly	0.4	742.83	1085.44	3620.27	2719.29
Cao	0.4	697.17	1028.27	3372.80	2589.58
Zhang	0.4	680.53	1023.57	3373.23	2589.58
AMC	0.4	673.28	1021.87	3364.69	2581.62
Xu	0.6	733.01	1102.93	3588.69	2732.94
Aly	0.6	772.27	1109.33	3712.43	2770.49
Cao	0.6	710.40	1033.81	3379.20	2598.68
Zhang	0.6	681.81	1037.65	3382.19	2597.55
AMC	0.6	674.13	1025.28	3364.69	2581.62
Xu	0.8	761.17	1142.61	3700.48	2806.90
Aly	0.8	822.19	1143.04	3841.28	2816.00
Cao	0.8	724.48	1038.51	3385.17	2605.51
Zhang	0.8	684.37	1041.49	3396.27	2608.92
AMC	0.8	676.27	1029.55	3366.83	2593.00

从表 2 可以看出,cover 样本的比特率低于所有 stego 样本,表明这些视频运动矢量隐写算法不可避 免会不同程度引入比特率增加异常:

Xu 样本随着嵌入率增加,比特率的增量从 2% 逐渐升高到 10% 左右.

Aly 样本比特率增长最显著,比特率的增量由 2%逐渐升高到10%以上,其中 Aly 的0.8 bpmv 的 bridge 视频,相比 cover 比特率增量达到18%,在所 有样本中增长最高.

Cao 样本比特率增量大部分在 0.2%~2.0% 之间,相比前两种算法,比特率得到了更好的控制. 0.8 bpmv的 bridge 视频比特率增量达到 7.0%.

Zhang 样本比特率增量几乎全部处于 0.1%~2.0%之间,优于 Cao 样本.

本文的 AMC 样本,没有使用 STC 编码,想比 Zhang 算法与 cover 比特率更为接近,比特率增量 全部在 0.1%~1.0%之间,增加最少.其比特率增 量只有其他 4 种算法的 1%~50%左右.

Xu和 Aly的算法在隐写时没有考虑码率增长问题,不能很好控制残差代价,比特率增加最为显著.Cao方法使用次优运动矢量隐写降低比特率失真,但是宏块次优运动矢量代价依然可能有较大增加,并且一个宏块只能嵌入1比特秘密信息造成其需要修改更多运动矢量.Zhang方法更多关注局部最优性,比特率失真较大,借助STC编码大大降低了运动矢量的修改次数,但是被修改的运动矢量依然可能造成较大的比特率增长.AMC 隐写在纹理平坦的宏块中,本文在第3节的理论分析部分讨论了纹理平坦的宏块运动矢量的隐写残差代价增加较小,因此其对比特率控制相对较好.

#### 5.4 抗隐写分析测试

反检测能力主要利用同样嵌入率下隐写样本被 隐写分析算法检测准确率高低进行评估.隐写算法 检测错误率越高,则隐写算法越难被检测,算法安全 性相对越高.

训练样本.分别针对每一种隐写算法,在视频 库中,随机选取 17 段 stego 视频及其对应的 17 段 cover 视频用于训练,其中 stego 视频包含 0.2 bpmv、 0.4 bpmv、0.6 bpmv 和 0.8 bpmv 共 4 种嵌入率.为 了保证训练正负样本数目对等,对于每一种嵌入率, 分别选取视频前 100 个 P 帧,即共 1700 个 cover 帧 和 1700 个 stego 帧用于训练.

测试样本.使用训练样本随机挑选后剩下的17 段 stego 视频和剩余的 cover 视频用于测试.其中 stego 视频同样包含 0.2 bpmv、0.4 bpmv、0.6 bpmv、 0.8 bpmv 共4种嵌入率.对于每一种嵌入率,分别 选取所有视频前100个 P帧,共1688个 cover 帧和 1688个 stego 帧用于测试(该测试样本中 stefan 视 频仅88个 P帧).

特征.本文使用 AoSO<sup>[19]</sup>特征和 Wang<sup>[15]</sup>特征 进行隐写分析, AoSO 特征属于最优性特征, 而 Wang 特征属于相关性特征.

分类器. libsvm-3.18 C 程序版<sup>①</sup>,多项式核.

为了保证对比的真实可靠,以上样本和训练参数的选择均未进行挑选,检测错误率对应如表 3.

表 3	隐写算法被检测的错误率
-----	-------------

特征	样本	0.2	0.4	0.6	0.8
	Xu	9.96	5.63	3.47	2.38
	Aly	7.87	6.22	4.59	3.32
1.50	Cao	39.07	31.91	24.91	20.29
A050	Zhang	48.05	49.29	48.20	42.96
	AMC	43.63	39.01	33.65	29.91
	AMC-STC	50.45	45.08	37.56	29.92
	Xu	29.06	21.77	17.09	11.82
	Aly	33.50	26.69	22.60	20.65
117	Cao	42.51	36.05	30.10	25.27
w ang	Zhang	40.35	36.76	36.17	30.51
	AMC	43.07	34.81	26.22	23.41
	AMC-STC	50.00	40.44	35.55	29.24

表 3 中,综合两种算法,Xu 和 Aly 安全性相对 较低.Cao 安全性强于 Xu 和 Aly.而 Zhang、AMC、 AMC-STC 安全性相对较高.

基于局部最优性的 AoSO 特征的检测结果表明,AMC 的局部最优性好于 Xu、Aly 和 Cao.由于 未使用 STC 编码,其修改率较高,因此和 Zhang 算 法相比相差较大.而 AMC 在使用 STC 编码后,安 全性有较大提高,嵌入率不大的情况下,AMC 算法 相比 Zhang 均难以被 AoSO 检测,在较高嵌入率 下,借助 STC 编码,其与 Zhang 差距缩小.

基于相关性的 Wang 特征的检测结果表明,本 文 AMC 算法使用加减 1 匹配嵌入对相关性的控制 好于 Xu 和 Aly 的 LSB 修改,而和 Cao 的次优运动 矢量以及 Zhang 的局部最优运动矢量相比相关性 保持相当.而 AMC-STC 的反检测能力在低嵌入率 下优于其他算法,在高嵌入率下与 Zhang 也基本 相当.

总体看来,在嵌入率较低情况下,AMC 隐写对 于两类特征都有较好的反检测效果.

#### 5.5 速度与容量

分别以 0.5 bpmv 嵌入率进行嵌入速度实验,嵌入 34 段视频,全 P 帧编码,总共编码 8010 帧.硬件 条件:I5-3470 3.20 Hz 四核处理器,8 GB DDR3 内 存,500 GB 机械硬盘,64 位 Win8.1 系统.嵌入时间 如表 4 所示.

表 4 隐写算法嵌入速度比较

样本	总时间/s	帧数量	平均时间/s
cover	121	8010	0.015
Xu	252	8010	0.031
Aly	287	8010	0.036
Cao	346	8010	0.043
Zhang	575	8010	0.072
AMC	357	8010	0.045

① LIBSVM [EB/OL]. http://www.csie.ntu.edu.tw/~cjlin/libsvm/index.html.

由表 4 看出, cover 样本仅使用一次压缩,效率 最高, Xu和 Aly 等算法由于嵌入规则简单,比 AMC 快速,但为了追求最小化失真, Zhang 算法 STC 编 码需要耗费较多时间.

AMC 隐写算法每个运动矢量都可以隐写 2 比特 秘密信息,因此其最大嵌入率可以达到 2.0 bpmv, 各隐写算法隐写嵌入率比较如表 5 所示.

表 5 隐写算法嵌入率比较

隐写算法	最大嵌入率/bpmv	隐写算法	最大嵌入率/bpmv
Xu	1.0	Zhang	1.0
Aly	2.0	AMC	2.0
Cao	1.0		

由于 AMC 单个宏块可以嵌入 2 比特秘密信息,故隐藏容量可以达到大多数隐写算法的 2 倍.

## 6 结 语

本文在理论上分析了运动矢量隐写对运动矢量 局部最优性和相邻相关性的影响,将二者进行分离, 分别予以控制.基于这一隐写思路,提出一种可不依 赖编码的最小化失真的自适应隐写算法,实验结果 支持了理论分析的相关结论,隐写失真控制要好于 目前隐写算法,同时在反检测方面对于两类特征都 有不错的安全性.虽然目前视频编码标准很多,但从 宏块角度来看,各类编码均采用残差预测实现压缩, 而运动矢量相关性和局部最优性在本质上完全相 同.因此,文中关于运动矢量的理论分析和隐写算法 具有普遍有效性.对于宏块复杂度的定义既可以不 使用编码进行 AMC 隐写,也可以将复杂度作为代 价结合 STC 降低隐写修改率,进一步提升隐写算法 性能.相比于目前已有的 STC 隐写,由于其代价函 数在嵌入端确定的隐写路径在提取端无法获得,故 已有的运动矢量隐写算法必须依赖编码,无法使用 阈值.事实上,在现实中,常见视频尺寸大多高于标 准视频库的视频尺寸,视频帧中低复杂度的宏块比 例相对更高,对于 AMC 隐写将更加有利.

**致 谢** 感谢匿名审稿人对本文提出的宝贵修改意 见和建议!

#### 参考文献

 Wang Shuo-Zhong, Zhang Xin-Peng, Zhang Wei-Ming. Recent advances in image-based steganalysis research. Chinese Journal of Computers, 2009, 32(7): 1247-1263(in Chinese)

(王朔中,张新鹏,张卫明.以数字图像为载体的隐写分析研 究进展.计算机学报,2009,32(7):1247-1263)

- [2] Li Bin, He Jun-Hui, Huang Ji-Wu, et al. A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 2011, 2(2): 142-172
- [3] Sadek M M, Khalifa A S, Mostafa M G M. Video steganography: A comprehensive review. Multimedia Tools and Applications, 2015, 74(17): 7063-7094
- [4] Hu Yang, Zhang Chun-Tian, Su Yu-Ting. Information hiding for H. 264/AVC. Acta Electronica Sinica, 2008, 36(4): 690-694(in Chinese)
  (胡洋,张春田,苏育挺. 基于 H. 264/AVC 的视频信息隐藏 算法. 电子学报, 2008, 36(4): 690-694)
- [5] Huang Hui-Yu, Yang Cheng-Han, Hsu W H. A video watermarking technique based on pseudo-3-D DCT and quantization index modulation. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 625-637
- [6] Xu Chang-Yong, Ping Xi-Jian, Zhang Tao. Steganography in compressed video stream//Proceedings of the 1st International Conference on Innovative Computing, Information and Control (ICICIC'06). Beijing, China, 2006, 1: 269-272
- [7] Aly H A. Data hiding in motion vectors of compressed video based on their associated prediction error. IEEE Transactions on Information Forensics and Security, 2011, 6(1): 14-18
- [8] Cao Yun, Zhao Xian-Feng, Feng Deng-Guo, et al. Video steganography with perturbed motion estimation//Proceedings of the 13th International Conference on Information Hiding(IH 2011). Prague, Czech Republic, 2011: 193-207
- [9] Cao Yun, Zhang Hong, Zhao Xian-Feng, et al. Video steganography based on optimized motion estimation perturbation//Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. Portland, USA, 2015; 25-31
- [10] Filler T, Judas J, Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 920-935
- [11] Yao Yuan-Zhi, Zhang Wei-Ming, Yu Neng-Hai, et al. Defining embedding distortion for motion vector-based video steganography. Multimedia Tools and Applications, 2015, 74(24): 11163-11186
- Zhang Hong, Cao Yun, Zhao Xian-Feng. Motion vectorbased video steganography with preserved local optimality. Multimedia Tools and Applications, 2016, 75(21): 13503-13519
- [13] Zhang Cheng-Qian, Su Yu-Ting, Zhang Chun-Tian. A new video steganalysis algorithm against motion vector steganography// Proceedings of the Wireless Communications, Networking and Mobile Computing 2008 (WiCOM'08). Dalian, China, 2008: 1-4

- [14] Su Yu-Ting, Zhang Cheng-Qian, Zhang Chun-Tian. A video steganalytic algorithm against motion-vector-based steganography. Signal Processing, 2011, 91(8): 1901-1909
- [15] Wang Li-Na, Wang Min-Jie, Zhai Li-Ming, et al. H. 264/ AVC video steganalysis algorithm based on motion vector abnormal correlation. Acta Electronica Sinica, 2014, 42(8): 1457-1464(in Chinese)

(王丽娜,王旻杰,翟黎明等.基于相关性异常的 H.264/ AVC 视频运动矢量隐写分析算法.电子学报,2014,42(8): 1457-1464)

[16] Ye Hui, Zhang Wei-Ming, Yao Yuan-Zhi, et al. Motion vectorbased video steganalysis using spatial-temporal correlation// Proceedings of the Image and Signal Processing(CISP 2013).



WANG Li-Na, born in 1964, Ph.D., professor, Ph. D. supervisor. Her research interests focus on information hiding and cloud computing security. Cherbourg, France, 2013, 1: 148-153

- [17] Cao Yun, Zhao Xian-Feng, Feng Deng-Guo. Video steganalysis exploiting motion vector reversion-based features. Signal Processing Letters, 2012, 19(1): 35-38
- [18] Ren Yan-Zhen, Zhai Li-Ming, Wang Li-Na, et al. Video steganalysis based on subtractive probability of optimal matching feature//Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security. Salzburg, Austria, 2014: 83-90
- [19] Wang Ke-Ren, Zhao Hong, Wang Hong-Xia. Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value. IEEE Transactions on Information Forensics and Security, 2014, 9(5): 741-751

XU Yi-Bo, born in 1986, Ph. D. candidate. His research interests focus on information hiding.

**ZHAI Li-Ming**, born in 1989, Ph. D. candidate. His research interests focus on information hiding.

**REN Yan-Zhen**, born in 1973, Ph.D., associate professor. Her research interests focus on information hiding.

#### Background

Modern steganography is the art and science of covert communication which sends secret messages under the camouflage of regular-looking cover media without arousing any suspicion. There are many types of digital media, which can be used as the cover for embedding, such as digital images, videos and audios. The research on steganography method based on motion vector, with its vast capacity for hiding information, simple embedding procedure and high quality of video images, have become more and more prevailing nowadays. On the other hand, steganalysis aims to detect the presence of the hidden secret data in those stego media though the statistical evidence. In order to resist detection, a secure steganoraphic scheme lies in minimizing different kind of distortions caused by the embedding modification. With the invention of STCs, the study of information hiding has turned into designing a good distortion model. The anti-detection to a given steganalysis feature has been solved successfully by the existing methods. However, it does not mean that any distortion of this method has been controlled well. We believe that any type of distortion can become a potential risk for steganography. In addition, it is still lack of reasonable theoretical analysis on distortion control.

As we know, with the development of video motion vector steganography, many people have taken the protection of local optimality into account, but the adjacent correlation of motion vectors seems to be ignored. In this paper, with the theory analysis in detail, a novel steganography algorithm based on video motion vector is proposed. The low complexity macroblocks are chosen for embedding by the adaptive threshold of complexity to keep the local optimality and the correlation of adjacent motion vectors. Experimental result shows that it has a good anti-steganalysis performance against the classic steganalysis algorithm. Especially, the distortion of bitrate increase and the quality of the video image maintains well, and it has a strong anti-steganalysis capability against steganalysis algorithm based on local optimization or neighbor correlation.

This work is supported by the State Key Program of National Natural Science of China (No. U1536204), the National Key Technology R&D Program (No. 2014BAH41B00), the National Natural Science Foundation of China (No. 61373169) and the National High Technology Research and Development Program (863 Program) of China (No. 2015AA016004).