# 一种基于H.264/AVC的新型视频隐写算法

报 告 人：周 霈
指导老师：李芝棠教授

# 1.1 课题的背景

- 视频隐写

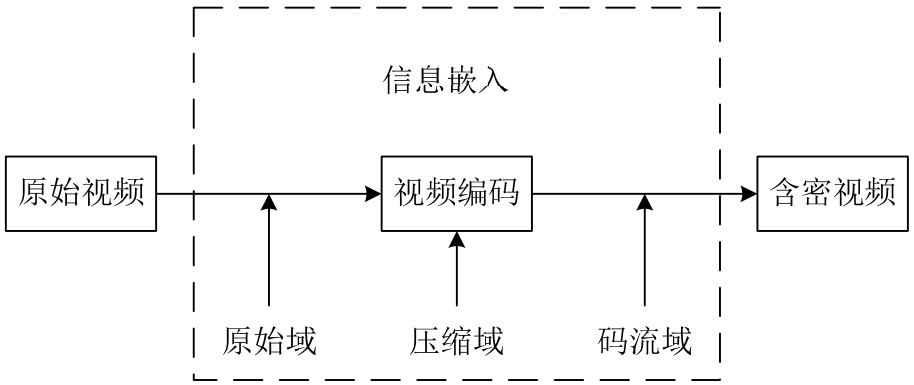
视频隐写作为信息隐藏一个方向，它是除了加密的另外一个比较新方向，开始逐渐为人们所重视。加密是对载体（常见的载体有视频，音频和文本）进行置乱，虽然使用比较复杂的加密方式，截获者很难破译出来有效信息。但是，加密一个很明显的缺点就是对载体加密后很容易引起对方的怀疑，因为它对载体进行了明显的易察觉的改变。然而隐写将秘密信息嵌入到载体中而不损坏载体的质量，也就是截获者就算截获了这个载体，但是其很难引起截获者的怀疑，因为隐写的隐蔽性。

# 1.2课题的意义

在视频隐写的背景下提出了许多相关理论和隐写算法。但多数视频隐写算法都存在一定问题，如隐写容量小、算法鲁棒性不高、对视频质量影响较大或算法安全性不好等缺点。因此，对基于H.264/AVC标准的视频隐写技术进行研究仍具有很大的意义。

# 1.3 国内外现状

随着隐写技术的发展，针对一些常见的视频编码格式学者们提出了不少可行的视频隐写算法，大致分为三类：原始域算法、压缩域算法和码流域算法 。



在量化后的DCT系数中嵌入是当前视频隐写算法的主流。目前提出的算法主要分为以下几类：

1. 直接利用系数的性质，如奇偶性。

2. 人为构建向量或矩阵，与一系列系数载体相乘，得到不同的状态。

3. 统计出特殊的系数的个数来嵌入，如0的个数，正负1的个数。

# 2.1 算法基本思想

用任何一个 DCT 系数yi对3 取模只可能得到三种结果 :

a) yi % 3 = 0 ;
b) yi % 3 = 1 ;
c) yi % 3 = 2 ;

（1）

如果yi % 3 = 0 , 那么 (yi+1) % 3 = 1 ， (yi-1) % 3 = 2 ,因此一个 DCT系数可以通过+1或者-1从其中的一种结果转化为另外两种结果。

在4×4变换块中选n个QDCT系数作为载体，这样得到一个序Y(y1,y2....yn)，然后把Y序列的所有元素对3取模，将得到一个新的序列G(g1,g2…gn)，其中gi = yi % 3 。

统计0,1,2的个数，记为K0，K1，K2。

# 2.1算法基本思想

利用K1和K2的奇偶性来嵌入秘密信息w1和w2。

$$w_i \equiv k_i \bmod 2 \quad (0 \le w_i \le 1) \qquad (2)$$

一般情况下秘密信息wi和ki并不会完全符合公式（2），因此我们需要对其中一些载体系数做出修改，以使得能够正确地提取出秘密信息。修改规则如下：

1) 如果$w1 \neq k1 \bmod 2$ 并且 $w2 \neq k2 \bmod 2$ ,同时修改K1和k2的奇偶性。
2) 如果 $w1 \neq k1 \bmod 2$ 并且$w2 = k2 \bmod 2$ , 修改K1的奇偶性 .
3) 如果 $w1 = k1 \bmod 2$ 并且 $w2 \neq k2 \bmod 2$ , 修改K2的奇偶性 .
4) 如果$w1 = k1 \bmod 2$ 并且 $w2 = k2 \bmod 2$ ,不做任何修改 .

# 2.2信息嵌入

- 下面举个例子，设要嵌入的秘密信息w1 =1且w2 = 0，取n=4，这样选4个QDCT系数做载体，假设系数值分别为1,4,0,3，我们可以得到一个序列Y(1,4,0,3)，把这个序列中的元素都对3取模，就得到一个新的序列G(1,1,0,0)。由此可以计算出 k0 = 2 , k1 = 2 , k2 = 0，此时k1%2=0，k2 %2=0，而二进制秘密信息是10，因此只需要改变k1的奇偶性，把序列Y中一个模3为1的数自减1或者把一个模3为0的数加1就能达到目标。因此有两种修改方法：

- 1）Y中第一个元素1%3=1，把它减1，得到Y′(0,4,0,3),从而得到序列G′(0,1,0,0)，修改后k0=3,k1=1,k2=0，此时k1%2=1，k2%2=0，刚好与二进制秘密信息10相符。

- 2）Y中第三个元素0%3=1，把它加1，得到Y′(1,4,1,3),从而得到序列G′(1,1,1,0)，修改后k0=1,k1=3,k2=0，此时k1%2=1，k2%2=0，刚好与二进制秘密信息10相符。

# 2.3信息提取

在H.264视频解码过程中选择符合嵌入时条件的P4×4块作为提取块，具体提取步骤为：

1.取与嵌入时同样位置的4个QDCT系数yi，组成一个序列Y(y1,y2....yn)；

2.对序列Y中的每一个元素分别进行模3运算，得到序列G(g1,g2…gn)；

3.分别统计G中的元素为0,1和2的个数，记为k0，k1，k2，可以得到秘密信息w0=k1%2, w1=k2%2；

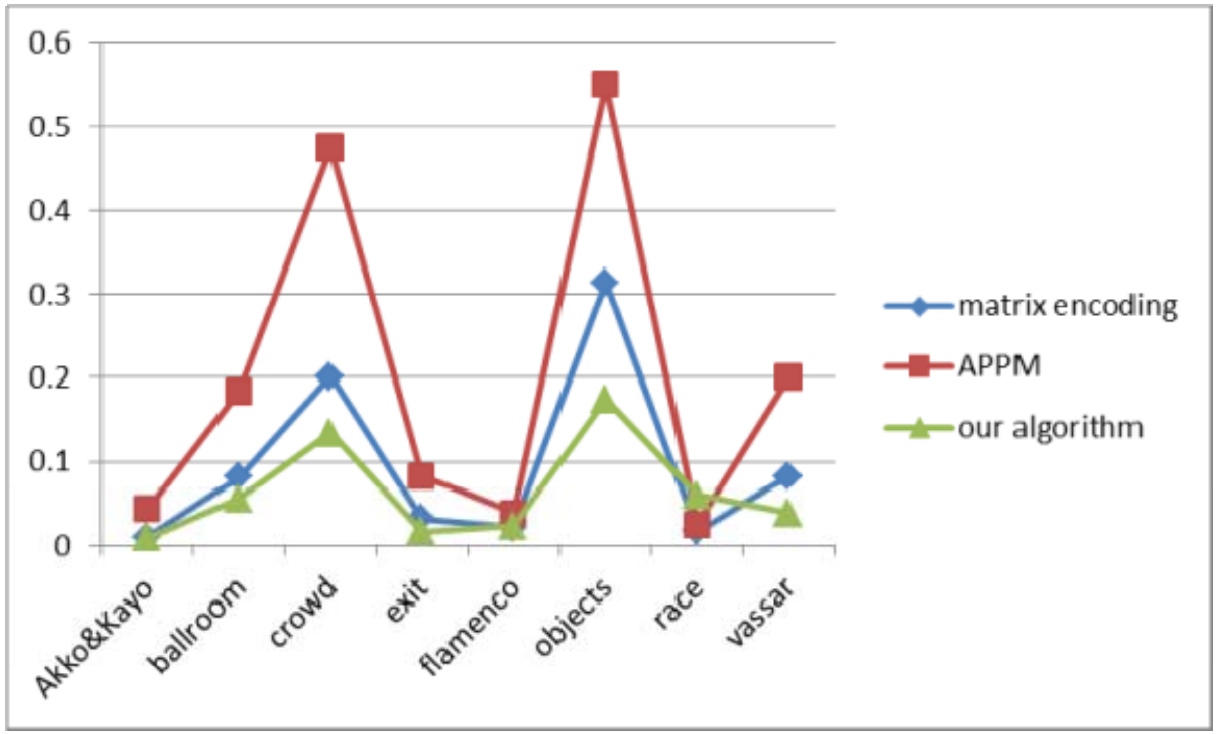
# 3 实验对比

- 矩阵编码一直被认为是一种非常高效的算法，它的三个指数可表示为(1,2k-1,k)。但是由于DCT系数的4×4变化块的载体数量限制，2k-1≤15，从而得出k≤4。在这个实验中为了对比，我们取k=2，即(1,3,2)。

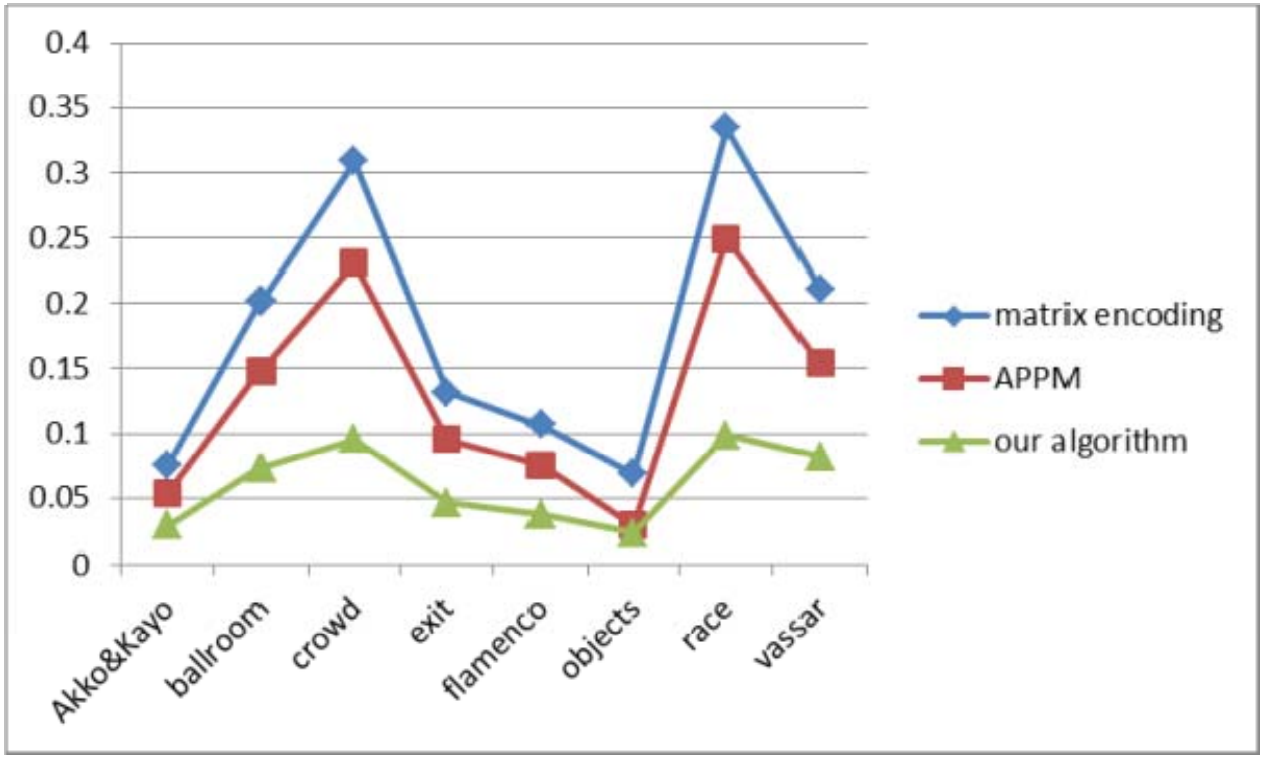
- APPM算法修改1个或者2个DCT系数来嵌入4比特信息，一个块中可以嵌入较多的秘密信息，但是由于修改幅度较大以及修改2个DCT系数的概率较大，实际上的嵌入效率可能并不高。

- 进行实验时，我们在相同的视频中嵌入相同数量的秘密信息来比较PSNR和比特增长率。

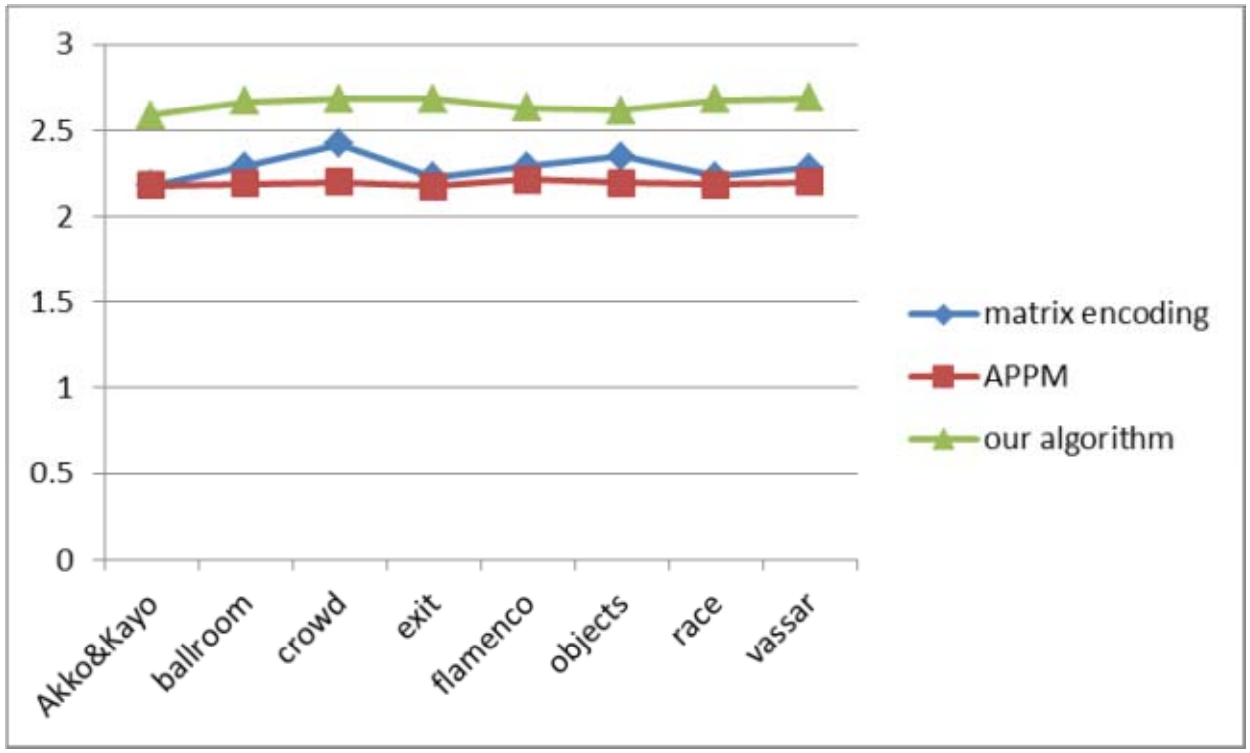
# 3.1 PSNR 下降值


0.6
0.5
0.4
0.3
0.2
0.1
0
Akko&Kayo
ballroom
crowd
exit
flamenco
objects
race
vassar
matrix encoding
APPM
our algorithm

# 3.2 比特增长率


0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
Akko&Kayo
ballroom
crowd
exit
flamenco
objects
race
vassar
matrix encoding
APPM
our algorithm

# 3.3 嵌入效率


3
2.5
2
1.5
1
0.5
0
Akko&Kayo
ballroom
crowd
exit
flamenco
objects
race
vassar
matrix encoding
APPM
our algorithm

# 4 总结

从嵌入效率和安全性方面考虑，本文基于H.264/AVC标准提出来一种全新的信息隐藏算法。跟矩阵编码和APPM算法比较，该算法具有较高的PSNR值和嵌入效率，同时比特增长率较低，在安全性和嵌入效率方面还是比较好的。但是随着N的增加算法的性能提高并不明显，所以该算法适用于载体较少的情况。算法还可以朝模数增加的方向来拓展，这有待下一步研究。

# 谢谢