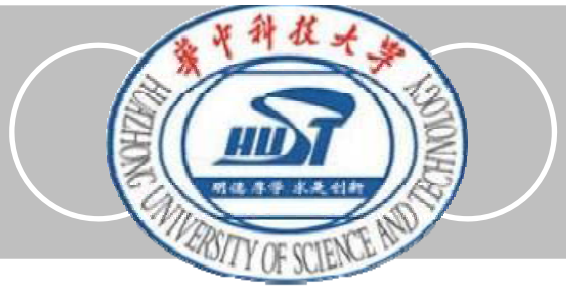


一种基于EMD算法的新型矩阵编码视频隐写算法

报告人 钱立云

指导老师 李芝棠教授

目录

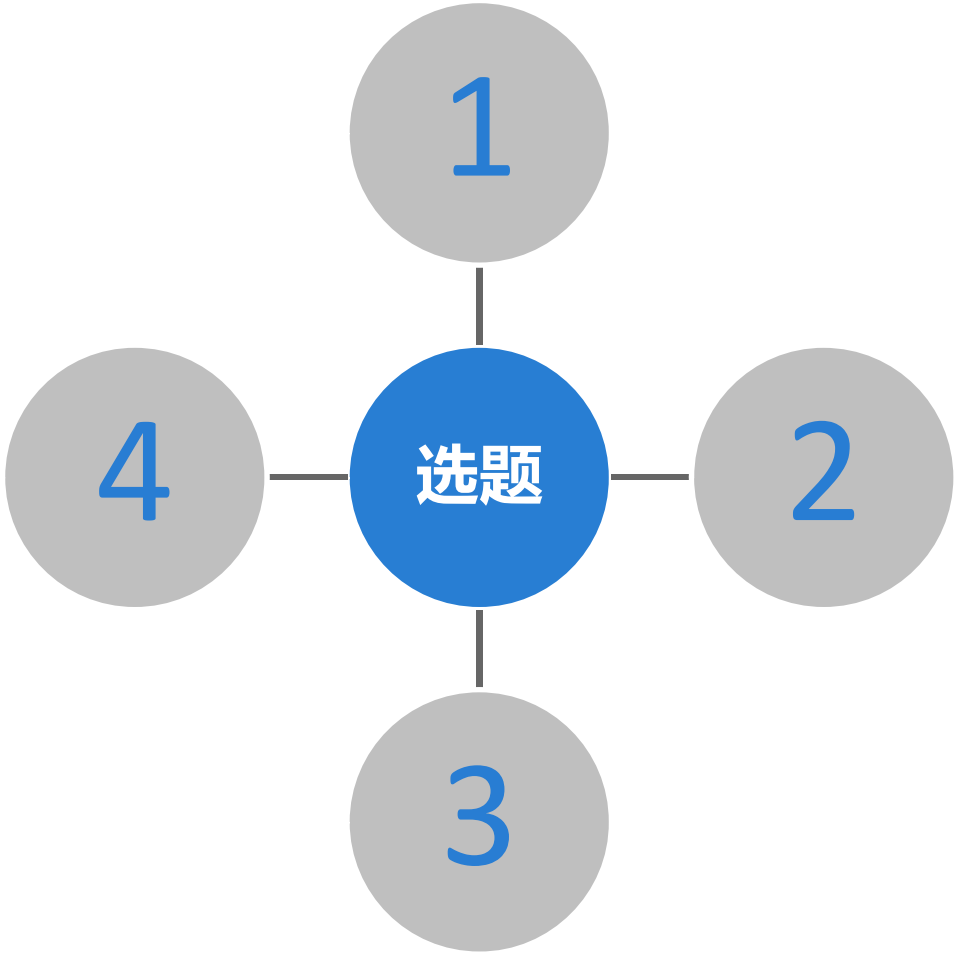
选题背景与国内外概况

1 课题背景

2 国内外研究概况

3 研究条件与意义

4 课题选择



一 选题背景及意义

1 课题背景

一、网络通信技术迅速发展，网络通信安全问题日益严重

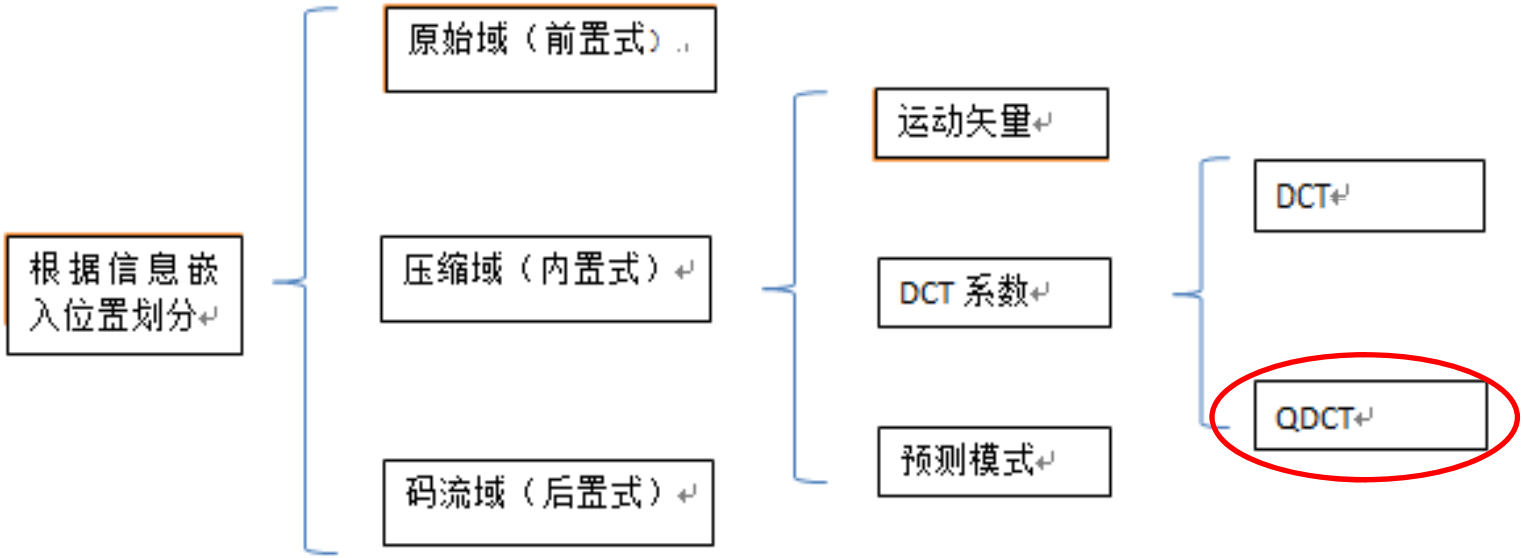
二、传统加密技术局限性

三、信息隐藏技术优势

选题背景及意义

2 国内外研究概况

目前视频信息隐藏的研究已取得了丰硕的研究成果。



一 选题背景及意义

3 研究条件与意义

一、多媒体技术的快速发展为信息隐藏提供了很好的条件和环境。

二、传统的基于H.263等标准的视频隐写算法的不可移植性

一 选题背景及意义

4 课题选择及技术背景

课题选择： 一种基于EMD算法的新型矩阵编码视频隐写算法

技术背景： H.264/AVC是JVT于2003年5月正式公布的新一代视频编码协议,是目前最新的、压缩效率最高、适用范围最广的视频编解码标准。

二 研究内容及研究思路

1 研究内容

一种基于EMD算法的新型矩阵编码视频隐写算法

2 研究思路

通过结合EMD算法提出一种新的矩阵编码隐写算法（NME）

二 研究内容及研究思路

1 研究内容

一种基于EMD算法的新型矩阵编码视频隐写算法(NME)

二 研究内容及研究思路

2 研究思路

1、EMD算法

EMD的核心为公式$f(a_1, a_2 \dots a_n) = (\sum_{i=1}^{n} a_i * i) \bmod (2n+1)$，其中（$a_1 \dots a_n$）为n个系数构成的载体向量。

为了简便，我们举例说明通过两个系数构成的载体向量嵌入一个4进制的数的情况。选择系数a_1，a_2构成载体向量A。假设4进制的秘密信息为$s_{(4)}$，先计算函数值$f(a_1, a_2) = (a_1 + 2a_2) \bmod 4$，再计算距离$d = s_{(4)} - f$，然后根据d的值查找表1，得到$\Delta a_1, \Delta a_2$,调整向量A生成新的向量$\tilde{A} = (a_1 + \Delta a_1, a_2 + \Delta a_2)$，则$\tilde{A}$满足$f(\tilde{A}) = s_{(4)}$，提取信息时只要计算出$f(\tilde{A})$的值即可。这是因为$f(\tilde{A}) = f(a_1 + \Delta a_1, a_2 + \Delta a_2) = f(a_1, a_2) + f(\Delta a_1, \Delta a_2) = (f(A) + \Delta d) \bmod 4$，又因为根据表1可知$\Delta d \bmod 4 = d \bmod 4$，所以$f(\tilde{A}) = (f(A) + d) \bmod 4 = s_{(4)}$。

二 研究内容及研究思路

2 研究思路

1、EMD算法

模版：

d	△a1	△a2	△d
0	0	0	0
1	+1	0	+1
2	0	+1	+2
3	-1	0	-1
-1	-1	0	-1
-2	0	-1	-2
-3	+1	0	+1

表1.EMD算法2系数嵌4进制数的模版

二 研究内容及研究思路

2 研究思路

2、NME算法

NME基本思想就是通过构建最优矩阵以及模版，微调由4个系数值构成的载体向量来嵌入两个4进制的秘密信息。

假设s_1，s_2代表两个4进制的秘密信息，即s_1，$s_2 \in \{0,1,2,3\}$,$B = (b_1 b_2 \dots b_4)^T$表示由4个系数值构成的载体向量。我们根据最优变化矩阵$C = \begin{pmatrix} -1 & 0 & 0 & 2 \\ 0 & -1 & 2 & 0 \end{pmatrix}$，计算向量$A = (a_1, a_2)^T = C * B (\mathrm{mod}\ 4)$,即
$a_1 = (b_1 * (-1) + b_2 * 0 + b_3 * 0 + b_4 * 2)\%4$;$a_2 = (b_1 * 0 + b_2 * (-1) + b_3 * 2 + b_4 * 0)\%4$;然后计算距离$d_1$，$d_2$，即$d_1 = s_1 - a_1$，$d_2 = s_2 - a_2$。接下来如table1所示，根据$d_1$，$d_2$的值得到$\Delta d_1$，$\Delta d_2$的值，最后根据$\Delta d_1$，$\Delta d_2$的值查找模版table2，得到变化向量$\Delta B$,微调载体向量生成新的向量$\tilde{B} = B + \Delta B$,用$\tilde{B}$代替 B，新的$\tilde{B}$满足条件：$C * \tilde{B} (\mathrm{mod} 4) = \tilde{A} = (\tilde{a_1}, \tilde{a_2})^T =$ （s_1，s_2）^{T},即$s_1 = \tilde{a_1}$，$s_2 = \tilde{a_2}$。当提取秘密信息时，只需要根据$\tilde{B}$计算出$\tilde{A}$即可。

二 研究内容及研究思路

2 研究思路

2、NME算法

模版：

d1/ d2	0	1	2	3	-1	-2	-3
△d1/△d2	0	1	2	-1	-1	-2	1

TABLE 1

Δd_1 \ $\Delta d2$	0	1	2	-1	-2
0	不改变	0,-1,0,0	0,0,1,0	0,1,0,0	0,0,-1,0
1	-1,0,0,0	-1,-1,0,0	-1,0,1,0	-1,1,0,0	-1,0,-1,0
2	0,0,0,1	0,-1,0,1	0,0,1,1	0,1,0,1	0,0,-1,1
-1	1,0,0,0	1,-1,0,0	1,0,1,0	1,1,0,0	1,0,-1,0
-2	0,0,0,-1	0,-1,0,-1	0,0,1,-1	0,1,0,-1	0,0,-1,-1

TABLE 2

三 实验结果

1

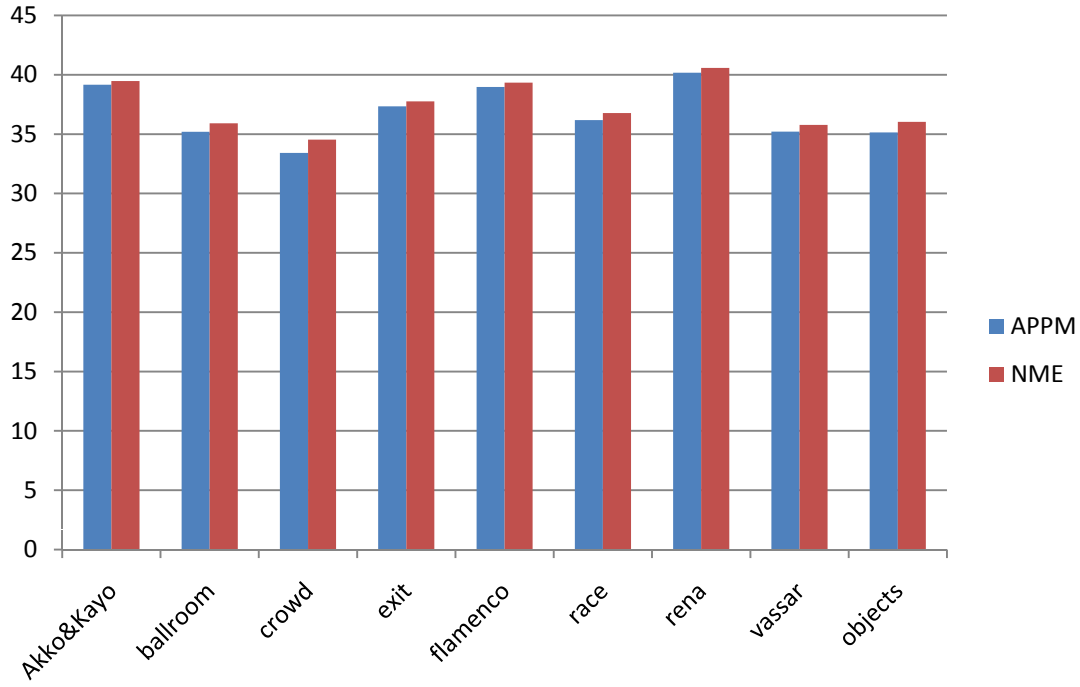


Fig.1 PSNR

三 实验结果

2

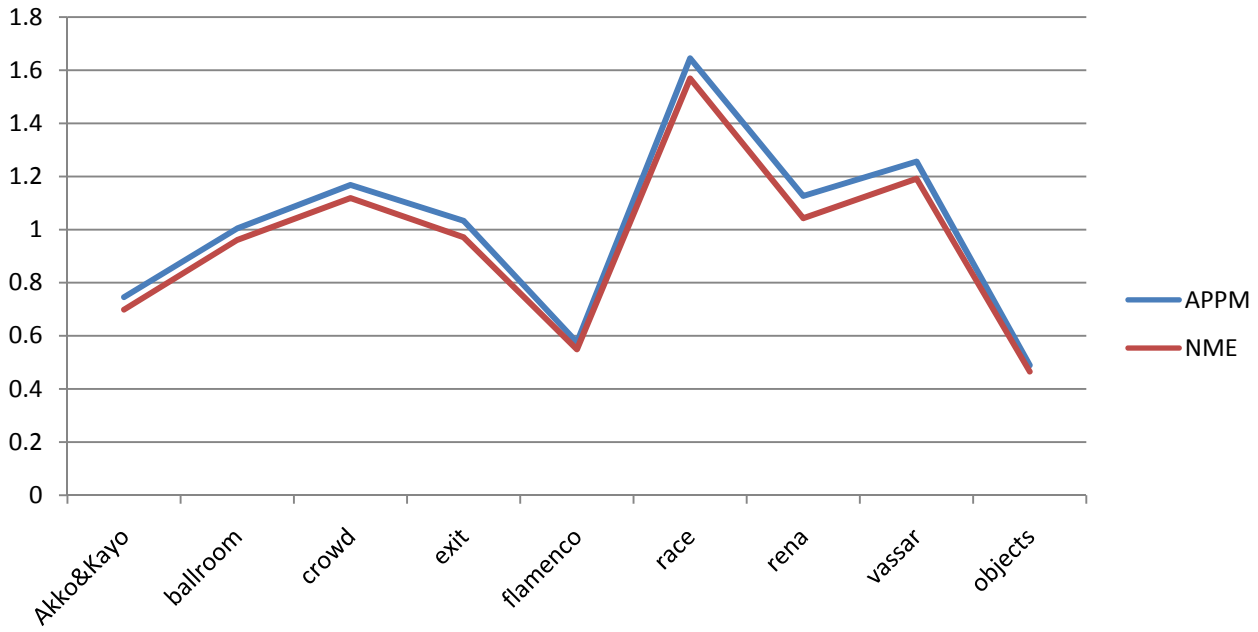


Fig.2 特增长率

三 实验结果

2

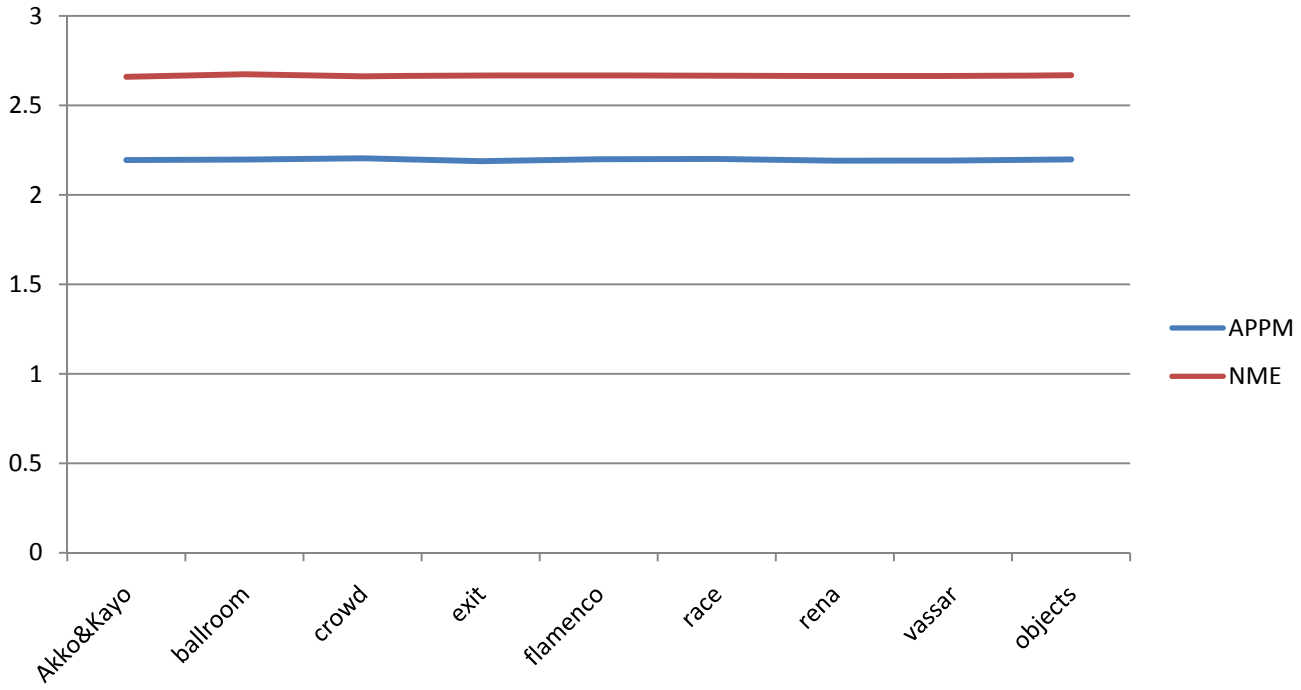
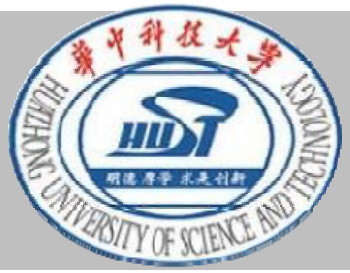


Fig.3嵌入效率

四 总结

本文为信息隐藏提出了一种新的思路和方法，NME算法本质是通过构建新的矩阵，并通过调制系数向量来实现信息隐藏，它的可扩展空间比较大，改变载体向量系数的个数，或者改变一次性嵌入的秘密信息的进制数或者个数，都会对最优矩阵以及实验结果产生影响，这些后期都还值得进一步的研究。



谢谢~

2015年11月22日