

# 扩展变换抖动调制水印算法中投影向量的研究

肖俊 王颖

(中国科学院研究生院,信息安全国家重点实验室,北京 100049)

**摘要** 扩展变换抖动调制(spread transform dither modulation, STDM)是一种性能很好的水印算法,该算法中用于扩展变换的投影向量是影响其性能的一个重要因素。本文研究STDM中的投影向量,对随机投影向量、均匀投影向量、平行投影向量、从频率角度选择的投影向量和从HVS角度选择的投影向量进行了介绍,并对选择各种投影向量时STDM的鲁棒性进行了比较与分析,得到了不同噪声攻击下,使得STDM水印算法的鲁棒性达到最优的投影向量选择方法。此外,为了充分利用HVS的特性,介绍了结合HVS综合选择投影向量的方法,实验结果说明该方法可以进一步改善STDM算法的视觉效果和鲁棒性。

**关键词** 数字图像 水印算法 量化 抖动调制 投影向量 HVS

中图分类号: TP309 文献标识码: A 文章编号: 1006-8961(2006)12-1799-07

## Project-vector of Spread Transform Dither Modulation Watermarking Algorithm

XIAO Jun, WANG Ying

(The Graduated School of the Chinese Academy of Sciences, Information Security State Key Laboratory, Beijing 100049)

**Abstract** Spread Transform Dither Modulation(STDM) is a watermarking algorithm having good performance. In this algorithm, the Project-vector used for spread transform is an important factor that affects its performance. This paper studies on the project-vector of STDM. Random project vector, uniform project vector, parallel project vector, project vector chosen according frequency and project vector chosen according HVS are introduced, the robustness under different project vectors is compared and analyzed, the way of choosing project-vectors that makes the robustness of STDM best under different attacks is obtained. Further, in order to make full use of the HVS's characteristics, choosing project-vector combined with HVS is introduced, and the experiment results show that by using this method, the visual quality and robustness of the STDM algorithm can be improved further.

**Keywords** digital image, watermarking algorithm, quantization, dither modulation, project-vector, HVS

## 1 引言

数字水印因其在知识产权保护、认证等方面的重要应用价值,已成为信号处理领域最热门的研究课题之一<sup>[1]</sup>。从水印的嵌入过程来看,目前最受青睐的水印方法是基于扩频<sup>[2~4]</sup>和基于量化<sup>[5~7]</sup>的方法。这两类方法各有优缺点<sup>[8]</sup>。基于扩频的方法对噪声不

敏感,但不易实现盲检测;基于量化的方法容量大<sup>[6,9]</sup>,在失真较小时解码的误码率很低,并且容易实现盲检测。在实际应用中,盲检测与大容量是倍受关注的问题,而基于量化的方法在这两方面都表现良好,尤其是扩展变换抖动调制(STDM)<sup>[5]</sup>算法。该算法可以实现盲检测,并且在鲁棒性、有效载荷及误码率等性能方面表现出良好的性能。正因为STDM具有良好的性能,Fernando等人<sup>[8]</sup>在研究扩频水印与量

化水印的基础上,对 STDM 的思想进行了扩展。

STDM 算法在嵌入水印前,要进行扩展变换,而投影向量是 STDM 中进行扩展变换的基础,原则上,投影向量可以随机选择,但是选择不同的投影向量会对水印系统产生怎样的影响,以及如何选择投影向量才能使得 STDM 水印算法的鲁棒性等性能更好,是一个值得研究的问题。本文主要研究 STDM 中投影向量的选择问题,得到了不同噪声攻击下,选择投影向量的方法,为鲁棒性 STDM 算法的设计提供指导。

### 2 STDM 水印方案

STDM 不是针对原始图像的某一系数进行量化,而是先对从原始数据中获得的提取向量进行投影变换,然后对投影所得数据进行抖动调制,这样使得只集中于一个变换系数上的嵌入失真随之扩展,这样可以满足峰值失真限制。

STDM 方法中水印的嵌入过程如图 1 所示。其中  $X$  是从原始信号中得到的向量,  $V$  是选择的投影向量,  $d(m)$  是抖动量,  $m$  称为索引,它与水印信息相对应。  $X$  首先与投影向量  $V$  内积,得到待量化系数  $\tilde{x}$ , 然后对  $\tilde{x}$  进行抖动调制得到  $\tilde{s}$ , 最后得到嵌入水印后的向量  $S = \tilde{s}X + V - \tilde{x}V$ 。抖动调制首先用水印信息对载体数据进行抖动, 然后进行量化, 从而实现水印的嵌入, 其实现框图如图 2 所示。

对于 STDM 方法,水印的提取过程是嵌入过程

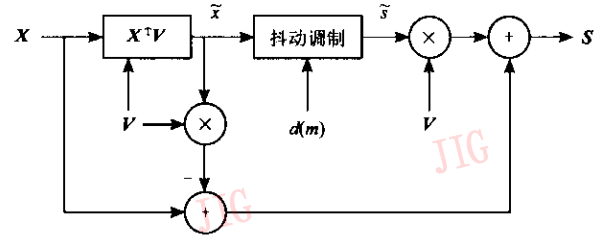


图 1 STDM 方法的嵌入过程

Fig. 1 Embedding process of STDM

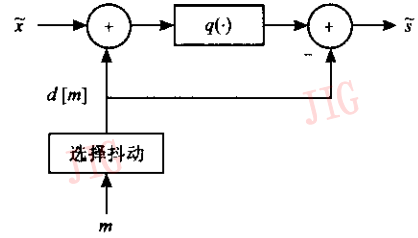


图 2 抖动调制的实现(其中  $q(\cdot)$  为量化器函数)

Fig. 2 Realization of dither modulation

( $q(\cdot)$  is the quantization function)

的逆过程,具体实现过程如图 3 所示。其中  $Y$  是从检测器所接收到的图像中得到的向量(用与嵌入时获得向量  $X$  相同的方法获得)。解码时,一般采用最小距离检测,即  $\hat{m} = \arg \min_{l \in \{0,1\}} (y - s_l)^2$ , 其中  $y$  是对  $Y$  进行投影所得到的数据,  $s_l[0]$  和  $s_l[1]$  分别表示假设  $y$  中隐藏着水印信息 0 和 1 的情况下,对  $y$  进行抖动调制所得到的数据。

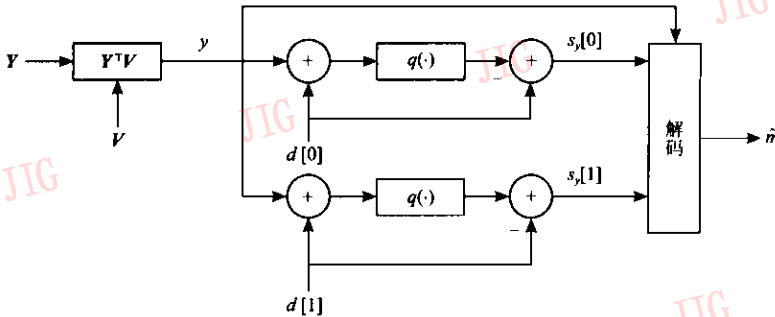


图 3 水印提取过程

Fig. 3 Water extracting process

### 3 STDM 算法中的投影向量

从 STDM 算法的原理中可以看出,投影向量是影响 STDM 性能的一个重要因素。投影向量原则上可以随机选择,只要保证投影向量本身是单位向量

就可以,但采用不同的投影向量水印算法的性能差别却很大。选择投影向量的方法很多,这里对随机投影向量、均匀投影向量、平行投影向量、从频率的角度选择的投影向量和从 HVS 的角度选择的投影向量进行介绍。

为了便于说明,先对有关符号进行说明:

$X_0$  表示原始图像(假设其大小为  $N \times N$ )  $X_0[i, j]$  ( $1 \leq i, j \leq N$ ) 是图像数据的空域表示,  $C_0[k, i, j]$  ( $1 \leq i \leq M, 1 \leq j \leq M, 1 \leq k \leq (N \times N) / (M \times M)$ ) 表示对  $X_0$  做  $M \times M$  块 DCT 变换之后第  $k$  块中的第  $i$  行第  $j$  列的元素。 $X_1[k]$  表示将第  $k$  块进行按行扫描所得到的列向量, 相应地  $X_1[k, i]$  ( $1 \leq i \leq M \times M$ ) 表示第  $k$  个列向量中的第  $i$  个元素;  $V[k]$  表示第  $k$  块的投影向量, 相应地  $V[k, i]$  ( $1 \leq i \leq M \times M$ ) 表示第  $k$  块的投影向量中的第  $i$  个元素。另外在每个  $M \times M$  的 DCT 系数块中只提取一个向量进行 STDM 嵌入, 并将  $X_1[k]$  作为从第  $k$  块提取的向量。

随机投影向量、均匀投影向量及平行投影向量等 3 种投影向量的构造较简单。随机投影向量的各个元素是一个随机序列构成的单位向量; 均匀投影向量是各个分量值相等的单位向量; 平行投影向量是将  $X_1[k]$  归一化得到的向量, 即  $V[k] = X_1[k] / |X_1[k]|$ 。这样, 将  $X_1[k]$  向  $V[k]$  投影相当于求其模值。下面分别介绍从频率的角度选择投影向量和从 HVS 的角度选择投影向量的方法。

### 3.1 从频率的角度选择投影向量

从频率的角度进行选择, 主要是考虑到 DCT 变换域下, 不同频率的系数具有不同的特点, 例如低频系数受低通滤波的影响很小。利用这些特点构造投影向量, 使得抖动调制只影响那些我们希望影响的系数, 从而获得预期的性能。一般, 从鲁棒性的角度考虑, 在低频和中频系数上嵌入水印比较好, 因此可以构造投影向量, 使得抖动调制只影响低频或者中频系数。

根据文献 [6] 中确定 DCT 域变换系数频率的方法, 可以得到  $C_0[k, i, j]$  的频率, 进而确定  $X_1[k, i]$  的频率。最后按照下面的方法构造低频投影向量

$$V[k, i] = \begin{cases} 1 & X_1[k, i] \text{ 是低频系数} \\ 0 & \text{其他} \end{cases}$$

$$1 \leq k \leq (N \times N) / (M \times M), 1 \leq i \leq M \times M$$

对  $V[k]$  进行归一化, 得到低频投影向量。如果低频系数包含直流分量在内, 则称之为含 DC 的低频向量, 否则称之为不含 DC 的低频向量。

类似地, 可以构造中频投影向量。

### 3.2 从 HVS 的角度选择投影向量

利用视觉模型可以改善水印系统的保真度, 因此考虑利用 Watson 基于 DCT 域的视觉模型<sup>[10]</sup>来构造投影向量。

Watson 模型由一个敏感度函数、两个基于亮度和对比掩蔽的掩蔽部分以及一个合并部分组成。

Watson 模型中首先定义了一个频率敏感度表, 表中的每个元素用  $W[i, j]$  表示; 对  $W[i, j]$  进行亮度掩蔽, 得到亮度掩蔽值  $t_L$ ; 对  $t_L$  进行对比度掩蔽, 得到掩蔽阈值  $s[i, j, k]$ , 它表示块 DCT 的各系数在一个 JND (just noticeable difference) 范围内可以进行的变化。因此, 构造投影向量使得抖动调制只影响掩蔽阈值大于特定阈值的系数, 从而减少视觉失真。可以根据下式构造投影向量:

$$V[k, n] = \begin{cases} 1 & s[i, j, k] > T \\ 0 & \text{其他} \end{cases}$$

$$1 \leq n \leq M \times M, 1 \leq i, j \leq M$$

其中,  $T$  是一个预先定义的阈值。最后进行归一化处理得到最终的投影向量。

## 4 实验结果与分析

下面主要分析比较选择不同投影向量时 STDM 水印系统的鲁棒性, 重点针对 JPEG 压缩和高斯噪声的抵抗能力进行分析, 其目的是确定最佳的投影矢量, 使 STDM 算法的鲁棒性最佳。

对大量图像进行实验, 并且都得到了相同的结论, 但是出于篇幅的原因, 下面仅给出选择  $256 \times 256$  的 Lena 灰度图像作为原始载体图像, 将  $20 \times 16$  的二值图像作为水印图像的实验结果。实验中, 每 3 个 DCT 域的  $8 \times 8$  系数块嵌入 1 个相同的水印数据, 也就是说嵌入率为  $1 / (3 \times 64)$  bpp; 采用峰值信噪比 PSNR 来衡量失真, 这里的峰值信噪比定义为可能的最大像素灰度值的平方与对每个像素引入的嵌入失真的均值之比。在嵌入失真与嵌入速率相同的情况下, 当误码率一定时, 含水印图像抵抗 JPEG 压缩的能力可用 JPEG 压缩因子  $Q$  来度量。图 4 所示的是在不出现误码的情况下, 嵌入水印后图像的峰值信噪比与能够对抗的 JPEG 压缩强度之间的关系。在峰值信噪比均为 39.2 dB 时, JPEG 压缩与误码率之间的关系如图 5 所示。由图 4 和图 5 可见, 就抗 JPEG 压缩的能力而言, 选择平行向量作为投影向量最佳, 因其在相同的压缩因子下误码率最低。选择低频向量时次之, 利用 HVS 得到的投影向量和均匀向量的情况最差。

平行向量之所以最好, 是因为平行向量本身有一个自适应的作用——当某一分量大时, 最后扩展到此分量上的数值也大, 反之亦然。低频向量的性能也比较好, 是因为 JPEG 压缩对低频的破坏

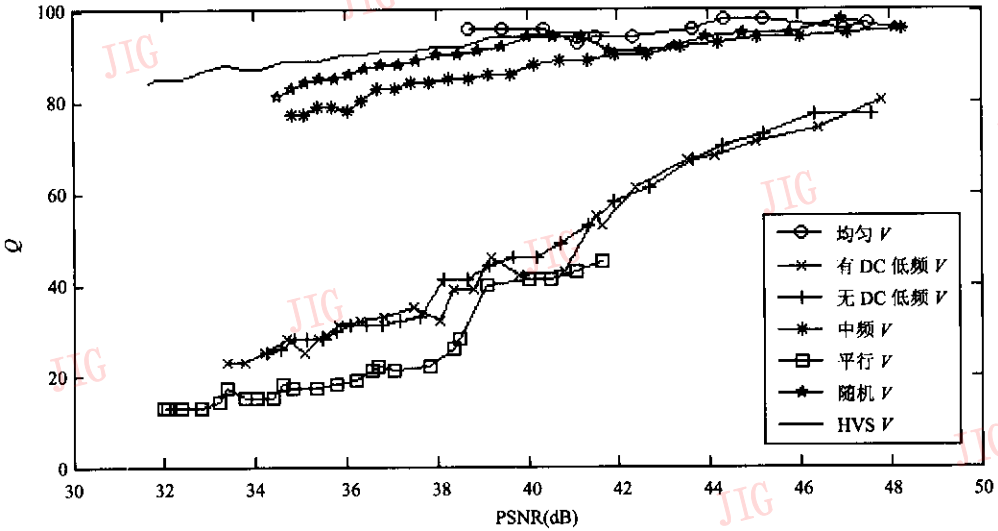


图 4 无误码的情况下 峰值信噪比与能够对抗的 JPEG 压缩强度之间的关系

Fig. 4 Relation between PSNR and JPEG compression strength , when no bit err occurs

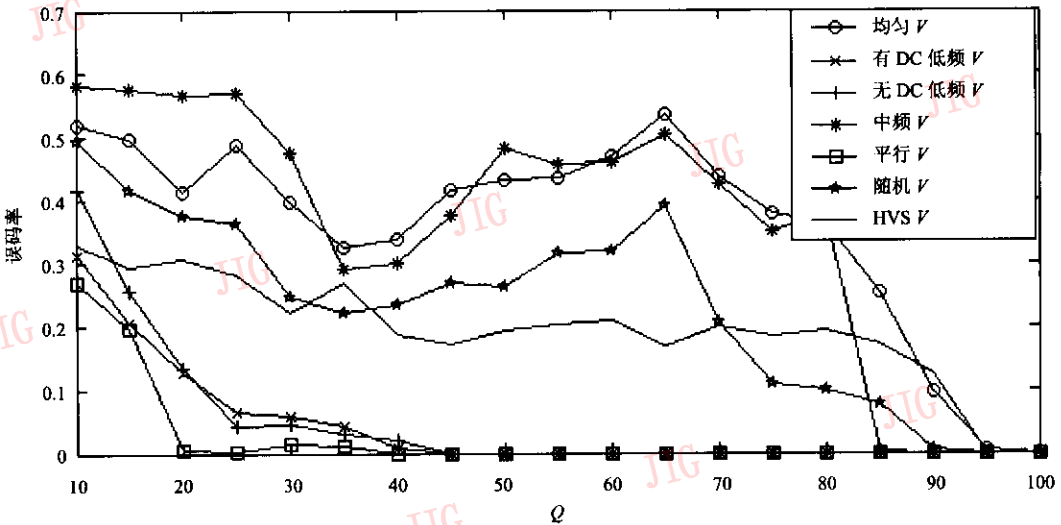


图 5 在峰值信噪比为 39.2dB 时 ,JPEG 压缩因子与误码率之间的关系

Fig. 5 Relation between JPEG compression strength and bit err ratio , when PSNR = 39.2dB

比较小 ;其他向量没有上述两个优点 ,均匀向量的特点甚至与平行向量的特点相冲突 ,其性能较差。另外 ,HVS 的性能并不好 ,这是因为 HVS 一般是在满足鲁棒性的条件下提高视觉效果 ,而仅仅从 HVS 的角度考虑不能得到理想的结果。

在嵌入失真与嵌入速率相同的情况下 ,当误码率一定时 ,含水印图像对高斯噪声的鲁棒性用高斯噪声的强度来度量。当峰值信噪比为 39.2dB 时 ,高斯噪声的方差 var 与误码率之间的关系如图 6 所示。从图 6 可见 ,当噪声方差一定时 ,中频向量的误

码率最低 ,所以就抗高斯噪声的能力而言 ,中频向量最优。其次是不含 DC 分量的低频向量、含 DC 的低频向量和利用 HVS 得到的向量以及平行向量 ,最差的仍然是均匀向量。

采用各种投影向量时的量化步长如表 1 所示。结合表 1 ,从投影向量和量化步长的角度可对上述结果进行解释。中频向量由于量化步长最大而性能最佳 ,含 DC 分量的低频向量、不含 DC 的低频向量、利用 HVS 得到的向量以及平行向量性能接近 ,这是量化步长与系数选择的优缺点相互中和的结果 ,随

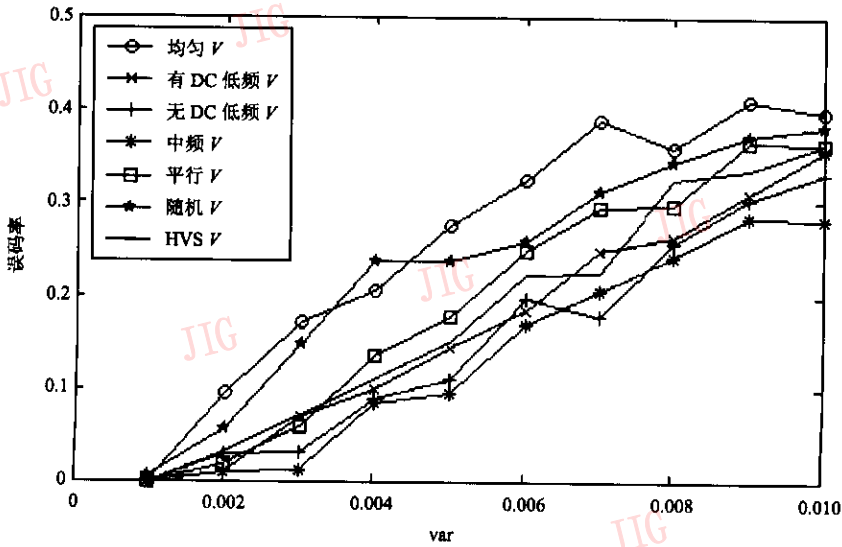


图 6 在峰值信噪比为 39.2dB 时,高斯噪声方差与误码率之间的关系

Fig. 6 Relation between Gas noise 's variance and bit err ratio , when PSNR = 39.2dB

表 1 采用各种投影向量时的量化步长

Tab.1 Quantization setp under different project-vector

| 类别   | 均匀向量 | 含 DC 低频向量 | 不含 DC 低频向量 | 中频向量 | 平行向量 | 随机向量 | HVS 向量 |
|------|------|-----------|------------|------|------|------|--------|
| 量化步长 | 77   | 81        | 85         | 90   | 80   | 85   | 80.5   |

机向量和均匀向量不仅不具有突出优点,相反还具有某一方面的缺点,例如,选择随机向量时,虽然其量化步长也比较大,但是随机向量对扩展系数没有较好的选择性,所以性能不好。

综合以上两个实验结果可以发现,选择不同的投影向量,系统的性能差别很大。对抗 JPEG 压缩时,选择平行向量可以得到最佳性能;对抗高斯噪声时,中频向量可以获得最佳性能,而低频向量在两种情况下都是次优的。

### 5 结合 HVS 综合选择投影向量

理论上 HVS 是可以改善系统的性能的,但是从上面的实验可以发现仅仅利用 HVS 不能得到满意的结果。将 HVS 与其他选择投影向量的方法相结合来共同确定投影向量,从而进一步改善系统的性能。

一般,要减小嵌入失真,鲁棒性就要做出一定的让步,并且在满足鲁棒性要求的情况下这个让步是值得的。利用 HVS 和其他选择方法来构造综合投影向量,就是想让这个“让步”尽量小。下面以选择低频向量的情况为例来说明如何结合 HVS 选择投

影向量。

在得到掩蔽阈值  $s[i, j, k]$  之后,可以结合掩蔽阈值构造投影向量,例如:

$$d[k, n] = \begin{cases} 1 & F[i, k, j] \leq 1/4 \text{ 且 } s[i, j, k] > T \\ 0 & \text{其他} \end{cases}$$

$$1 \leq n \leq 64, 1 \leq i, j \leq 8$$

但是由于 STDM 是基于量化的,如果直接这样构造,则没有与量化引入的失真相联系,而且在研究过程中发现,这样的结果不理想。为了与量化引起的嵌入失真联系在一起,需要进行合并得到可感知距离  $d[i, j, k]$ 。然后按照类似的方法构造投影向量:

$$d[k, n] = \begin{cases} 1 & F[i, k, j] \leq 1/4 \text{ 且 } d[i, j, k] > T_0 \\ 0 & \text{其他} \end{cases}$$

$$1 \leq n \leq 64, 1 \leq i, j \leq 8$$

其中,  $T_0$  是一个阈值,以  $d[i, j, k]$  的均值作为此阈值,最后进行归一化处理。

为了说明结合 HVS 能够改善性能,对仅利用低频条件选择的低频投影向量和结合 HVS 的低频投影向量做了比较实验。首先,从视觉效果的角度进行比较,图 7 给出的是量化步长均为 81 的情况下,



(a) 采用低频向量作为投影向量的情况  
(PSNR = 39.2dB)



(b) 低频条件与 HVS 相结合得到的投影向量时的情况  
(PSNR = 39.7dB)

图 7 量化步长均为 81 时,嵌入水印后的图像质量比较

Fig. 7 Compare of watermarked image's quality, when quantization steps are 81

嵌入水印后的图像质量比较,可以发现结合 HVS 时视觉效果得到了改善,然后,在嵌入水印后的图像峰值信噪比相同(均为 39.2dB)的情况下,对抵抗 JPEG 压缩与高斯噪声攻击的性能进行了比较,如图 8、9 所示。从图 8 和图 9 可以发现,结合 HVS 选择的低频向量不仅不影响其抵抗 JPEG 压缩攻击的能力,尤其是在压缩因子小于 35 的情况下,还可以提高抵抗 JPEG 压缩的能力,而且抵抗高斯噪声的性能有所增强。这说明结合 HVS 选择投影向量可以使得系统鲁棒性有所改善。

综合以上两个实验可见,综合 HVS 选择的投影向量,不仅能够改善视觉效果,而且不影响其鲁棒性,甚至可以进一步提高其鲁棒性。至于 HVS 与其他选择方法相结合的情况都可类似上面的过程进行。

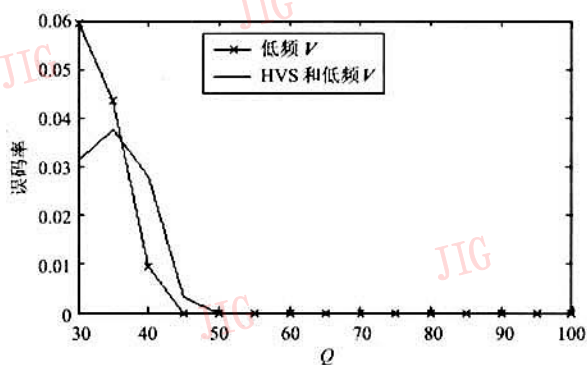


图 8 峰值信噪比相同的情况下, JPEG 压缩与误码率的关系

Fig. 8 Relation between JPEG compression and bit err ratio, under the same PSNR

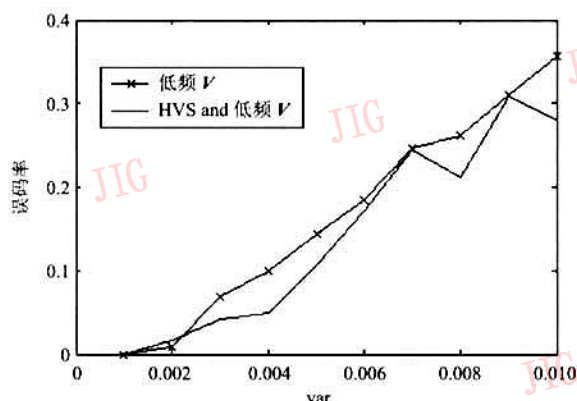


图 9 峰值信噪比相同的情况下,高斯噪声与误码率的关系

Fig. 9 Relation between Gas noise and bit err ratio, under the same PSNR

## 6 结 论

对 STDM 中的投影向量进行了讨论。研究结果表明,选择不同的投影向量对 STDM 算法的鲁棒性有很大的影响,就对抗 JPEG 压缩的性能而言,选择平行向量最佳,就对抗高斯噪声的性能而言,选择中频向量时最佳。另外仅从 HVS 的角度来选择投影向量,不能得到理想的性能,但是为了充分利用 HVS 可以改善视觉效果的特点,将 HVS 与其他选择方法相结合来共同确定投影向量。实验结果表明,结合 HVS 来选择投影向量不仅可以减少嵌入失真,改善嵌入水印后图像的视觉效果,而且不影响其鲁

棒性,甚至可以进一步提高其鲁棒性。

### 参考文献(References)

- 1 Cox I J, Miller M L, Bloom J A. Digital Watermarking[ M ]. San Francisco : Mordan Kaufmann Publishers ,2002 :5 ~6.
- 2 Cox I J, Kilian J, Leighton T. Secure spread spectrum watermarking for multimedia[ J ]. Proceedings of IEEE International Conference on Image Processing ,1997 ,**6**( 12 ) :1673 ~1687.
- 3 Hartung F, Su J K, Girod B. Spread spectrnm watermarking : malicious attacks and counter-attacks[ A ]. In :Proceedings of SPIE , Security and Watermarking of Multimedia Contents[ C ], San Jose , CA , USA ,1999 :147 ~158.
- 4 Zou Xiao-xiang , Li Jin-tao. Asymmetric watermark based on spread spectrum[ J ]. Computer Science ,2002 ,**29**( 9 ) :63 ~65. [ 邹潇湘 ,李锦涛. 基于扩频的非对称数字水印[ J ]. 计算机科学 ,2002 ,**29**( 9 ) :63 ~65. ]
- 5 Chen B , Wornell G W. Quantization index modulation : a class of provably good methods for digital watermarking and information embedding[ J ]. IEEE Transactions on Information Theory ,2001 ,**47**( 4 ) :1423 ~1443.
- 6 Chen B , Wornell G W. Quantization index modulation methods for digital watermarking and information embedding of multimedia[ J ]. Journal of VLSI Signal Processing Systems ,2001 ,**27**( 1 ) :7 ~33.
- 7 Sullivan K , Bi Z , Madhow U. Steganalysis of quantization index modulation data hiding[ A ]. In : IEEE International Conference on Image Processing[ C ], Singapore ,2004 :1165 ~1168.
- 8 Fernando P G , Balado F , Juan R H. Performance analysis of existing and new methods for data hiding with known-host information in additive channels[ J ]. IEEE Transactions on Signal Processing ,2003 ,**51**( 4 ) :960 ~980.
- 9 Eggers J J , Bauml R , Tzschoppe R. Scala costa scheme for information embedding[ J ]. IEEE Transactions on Signal Processing ,2003 ,**51**( 4 ) :1003 ~1019.
- 10 Watson A B. DCT quantization matrices visually optimized for individual images[ J ]. SPIE : Human Vision ,Visual Processing and Digital Display IV ,1993 ,**1913**( 14 ) :202 ~216.