

一种基于 α 稳定分布模型的 DCT 域 隐藏信息检测新方法

孙中伟, 许 刚

(华北电力大学电气与电子工程学院, 北京 102206)

摘 要: 本文提出一种离散余弦变换 (DCT) 域加嵌入隐藏信息的鲁棒检测方法. 该方法使用具有代数拖尾的 α 稳定分布模型来描述交流 DCT 系数统计分布的尖峰脉冲和强拖尾特性, 并利用隐藏信息的不可感知特性, 在弱信号条件下依概率模型进行统计推断, 从而实现广义 Neyman Pearson 准则下隐藏信息的鲁棒检测. 实验结果表明: (1) 新检测器的性能比目前广泛采用的匹配滤波器的性能优越; (2) 新方法基于广义高斯分布模型的检测方法相比性能相当, 却不需要“点消除”过程, 从而简化了检测器的实现.

关键词: 信息隐藏; 离散余弦变换 (DCT); α 稳定分布; 检测器

中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2008) 04-0720-05

Robust Detection of DCT-Domain Hidden Information Based on the α -Stable Models

SUN Zhongwei, XU Gang

(School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China)

Abstract: This paper presents a robust detection approach for the hidden information in the discrete cosine transform (DCT) domain. The proposed approach uses the α stable distributions, which are more accurate probability models than the gaussian and generalized gaussian distributions for those heavy tailed non gaussian data with the algebraic tails, to model AC DCT coefficients with distinct impulse distributional behavior. By applying the statistical inference on the probability models under the generalized Neyman Pearson criterion, the robust detection structure is then developed. The resulting detector is based on the statistical signal detection theory and it exploits the imperceptibility constraints of the hidden information. Experiments show that: a) the novel detector is superior over the matched filter and b) though the performance of the novel detector is close to that of the detector based on the generalized gaussian models, the proposed detector does not need the “point elimination process”, which simplifies the realization of the new detector.

Key words: information hiding; discrete cosine transform (DCT); α stable distribution; detector

1 引言

作为信息安全领域的一个新方向, 信息隐藏技术的理论、方法及应用研究正受到越来越广泛的关注. 简单地讲, 信息隐藏就是将保密信息隐藏于另一非保密的载体中, 然后通过非保密的载体来传递秘密信息. 这里的载体可以是图像、音频和视频, 也可以是信道, 或者某套编码体制甚至整个系统. 目前, 受知识产权保护这一应用需求所推动, 数字多媒体作品的版权保护已经成为信息隐藏技术的一个研究重点, 而版权标记是数字作品版权保护的一种有效技术. 例如, 数字水印技术将某些能证明版权归属的信息以不可感知的形式嵌入到原始媒体数据中, 用以证明创作者对作品的所有权, 同时通过对水印的探测和分析保证数字多媒体作品的完整可靠性. 数字指纹技术则是为了防止未经授权的作品的拷贝

与发行, 因为出品人可以将表明用户身份的信息作为指纹嵌入到数字作品中, 一旦发现未经授权的拷贝, 就可以从拷贝中提取指纹, 从而为追查盗版者提供线索.

一个信息隐藏系统包括信息嵌入和信息检测或提取两个主要的过程, 视其应用场合的不同, 它在不可感知性、安全性、信息嵌入量、计算复杂性、鲁棒性或易碎性等方面的要求会各不相同. 本文以多媒体作品的版权保护为应用背景, 研究数字图像离散余弦变换 (DCT) 域加嵌入隐藏信息的鲁棒检测问题. 从已有的文献来看, 确实已经存在许多隐藏信息的检测算法, 但是其中绝大多数都采用了匹配滤波器 (Matched filter) 的方法. 虽然它们能够提供可接受的性能, 但是这些方法既不是优化的, 又缺乏赖以支撑的理论基础. 由信号检测的基本理论可知, 使用匹配滤波器检测隐藏的信息只有在载体服从高斯分布时才是最优的^[1]. 研究结果表明, 在数字图

像的时/空域或者变换域,以高斯分布来对载体图像进行统计建模是不合适的^[2~4]。因此,从隐藏信息检测的角度来看,使用匹配滤波器没有考虑到载体图像的实际统计分布特性,其优化条件不复存在,检测性能也随之严重退化。针对这些问题,不少学者提出了基于广义高斯分布 (Generalized Gaussian Distribution, GGD) 模型的 DCT 域隐藏信息的检测方法^[5~7],其检测性能也得到了相应的提高。由概率统计的基本知识可知,针对具有强拖尾 (heavy-tail) 统计分布特性的数据,广义高斯分布是其统计建模的一种可行的选择。但是,它和高斯分布一样,其概率密度函数的拖尾同样具有指数衰减的特性,而图像 DCT 变换之后其交流系数的概率分布更多地表现出代数拖尾的特性。因此,采用广义高斯分布来建立图像交流 DCT 系数的统计分布模型时,需要采取称为“点消除 (point elimination)”的技术才能获得隐藏信息检测的稳定性^[5]。在文献[2]和[4]中,作者虽然认识到使用 α 稳定分布能更好地描述 DCT 交流系数的统计分布特性,但是他们都采用了 Cauchy 分布的形式。与高斯分布是广义高斯分布的特例一样, Cauchy 分布也只是 α 稳定分布的一个特例。

非高斯 α 稳定分布最重要的特征体现在概率分布上的稳定性及其概率密度函数的代数拖尾。它可以为不同领域的许多现象提供非常有用的模型,已经成功地应用于物理学、经济学、信息工程等领域中^[8]。例如,在信号处理和通信领域,针对信号噪声的尖峰脉冲特点,基于信号噪声的 α 稳定分布假设而导出的算法就具有很好的鲁棒性^[9]。本文针对 DCT 域数字图像中隐藏信息的鲁棒检测技术开展研究,采用 α 稳定分布来建立交流 DCT 系数的统计分布模型,利用隐藏信息的不可感知特性,提出一种 DCT 域隐藏信息检测新方法,并对新的检测方法进行实验。

2 稳定分布模型

统计信号处理通常涉及如何利用概率模型来描述观测信号和噪声的问题。在传统的信号处理中,高斯噪声模型占据主导地位,这是因为高斯模型比较简单,同时,在这种模型基础上设计的信号处理算法易于进行理论上的解析分析。例如,在通信问题中,如果采用加性高斯噪声模型来描述信道噪声,则接收机的设计可以大大简化。

尽管高斯噪声模型能够很好地描述许多信号噪声,但是在实际应用中还会遇到大量具有显著尖峰脉冲特性的噪声。它们的衰减过程比高斯噪声的衰减过程要慢,从而造成了强拖尾现象。在这种情况下,如果仍然采用高斯噪声模型来设计信号处理系统,由于模型与信号噪声不能很好地匹配,将会出现设计的信号处理器性能

显著退化的问题。非高斯信号处理是近年来迅速发展起来的一个信号处理的新领域,其中 α 稳定分布为描述这类具有显著尖峰脉冲状波形和强拖尾的概率密度函数提供了非常有用的理论工具。

如果随机变量 X 存在参数 $0 < \alpha \leq 2, \gamma \geq 0, -1 < \beta \leq 1$ 和实数 a , 使其特征函数具有如下的形式:

$$\phi(u) = \exp\{j\alpha u - \gamma |u|^\alpha [1 + j\beta \operatorname{sgn}(u) \omega(u, \alpha)]\} \quad (1a)$$

$$\omega(u, \alpha) = \begin{cases} \tan(\pi\alpha/2), & \alpha \neq 1 \\ (2/\pi) \log|u|, & \alpha = 1 \end{cases} \quad (1b)$$

$$\operatorname{sgn}(u) = \begin{cases} 1, & u > 0 \\ 0, & u = 0 \\ -1, & u < 0 \end{cases} \quad (1c)$$

则称随机变量 X 服从 α 稳定分布。式中 α 称为特征指数,它决定该分布脉冲特性的程度。 α 值越小,所对应分布的拖尾越厚,脉冲特性也就越显著。反之,其脉冲特性就减弱。 β 称为对称参数,用于确定分布的斜度。当 $\beta=0$ 时,称为对称 α 稳定分布,记为分布 SaS。高斯分布和柯西分布都属于 SaS, 分别对应 $\alpha=1$ 和 $\alpha=2$ 的情形。参数 γ 为分散系数,它是样本相对于均值分散程度的度量。参数 a 称为位置参数。

α 稳定分布作为建模工具非常灵活,主要原因在于它的特征指数 α 可用于控制概率密度函数拖尾的厚度,且 α 稳定分布随机变量的概率密度存在且连续。但是,除了象高斯分布、柯西分布和 Levy 分布等很少的例外之外, α 稳定分布没有封闭形式 (closed-form) 的显式表达式。不过其概率密度函数的计算可以通过展开为幂级数并进行数值计算来实现,很多使用概率密度函数的工作也可以通过特征函数的变换来实现。

图像压缩与编码的研究结果表明,数字图像在 DCT 变换之后,其交流系数的概率分布一般都具有尖峰脉冲和代数拖尾特性。利用极大似然估计法^[10~12],一些典型图像的 α 参数估计值如表 1 所示。如果使用 Cauchy 分布来建立变换系数的统计分布模型,其特征指数 α 等于 1。显然,这与 DCT 交流变换系数的实际统计特性存在很大的差异。

表 1 典型图像的 α 参数估计值

图 像	α	图 像	α
Baboon	1.2696	Bridge	1.6212
Peppers	1.2760	Goldhill	1.2606
Boat	0.9185	Lenna	1.1656
Cameraman	0.7990	Moon	1.2229
F16	0.9548	Harbor	0.7866

图 1 所示为部分测试图像 DCT 交流系数的概率分布直方图及其估计出的 α 稳定分布概率密度函数。可以看出,使用 α 稳定分布模型能与数据的实际分布非

常好地吻合. 而使用广义高斯分布模型, 如果不应用点消除技术, 很难获得这样的拟合结果^[13].

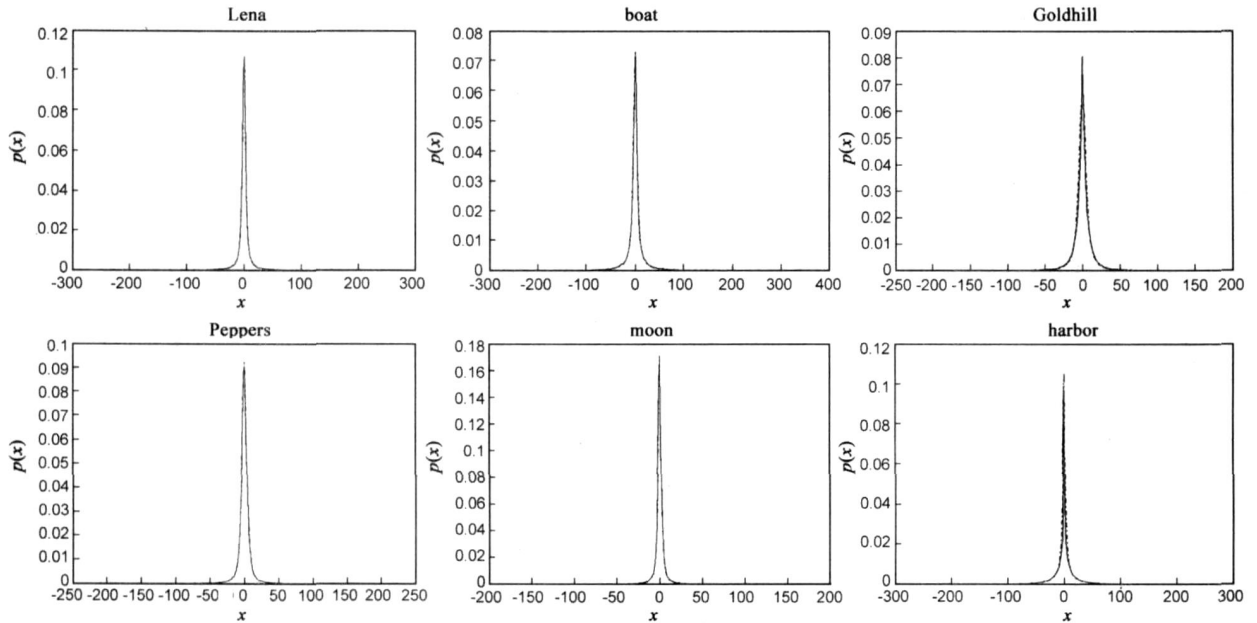


图 1 交流 DCT 系数的 α 稳定分布拟合结果

3 检测方法描述

图像 DCT 变换之后, 选取待修改的交流 DCT 变换系数序列 $X = \{x_1, x_2, \dots, x_N\}$ 作为载体, 那么, 按如下的规则可完成隐藏信息 $W = \{w_1, w_2, \dots, w_N\}$ 的嵌入:

$$y_i = x_i + \theta w_i \quad (2)$$

其中 $1 \leq i \leq N$, θ 为信息嵌入的强度因子, 它满足 $\theta > 0$. DCT 反变换, 即获得包含隐藏信息的图像.

从统计学的观点看, 隐藏信息的检测本质上属于二元假设检验的问题, 有两种可能的判决结果, 相应地有两个假设: 原假设 H_0 对应待检测图像未嵌入信息 W , 备择假设 H_1 对应待检测图像嵌入了 W . 由信息的嵌入过程可知, 该二元假设检验问题可表示为:

$$\begin{aligned} H_0: Y &= X \\ H_1: Y &= X + \theta W \end{aligned} \quad (3)$$

其中 $Y = \{y_1, y_2, \dots, y_N\}$ 是接收到的观测信号序列.

不可感知性是信息隐藏的一个基本特征, 这就决定了隐藏信息的检测是一个弱信号检测问题. 另外, 对于检测器来说, 因为信息的嵌入强度 θ 也是未知的, 因此, 上述二元假设检验属于复合假设检验.

如果分别用 $p_Y(Y; H_0)$ 和 $p_Y(Y; \theta, H_1)$ 表示 Y 在 H_0 为真和 H_1 为真时的概率密度函数, 那么, 它们的对数似然比为

$$l(Y) = \ln \frac{p_Y(Y; \theta, H_1)}{p_Y(Y; H_0)} = \ln p_Y(Y; \theta, H_1) - \ln p_Y(Y; H_0) \quad (4)$$

对上式中的 $\ln p_Y(Y; \theta, H_1)$ 用泰勒公式展开, 在弱信号

的条件下忽略二阶和以上的导数, 可导出:

$$l(Y) = - \sum_{i=1}^N w_i \frac{f'(x_i)}{f(x_i)} \underset{H_0}{>} \underset{H_1}{<} \eta \quad (5)$$

式中 η 为判决阈值, 其值由选取的判决准则来决定.

定义 $g_{LO}(x) = \frac{f'(x)}{f(x)}$, 那么检验统计量 $l(Y)$ 又可写成:

$$l(Y) = \sum_{i=1}^N \left[- \frac{f'(x_i)}{f(x_i)} w_i \right] = \sum_{i=1}^N g_{LO} w_i \quad (6)$$

与计算 SaaS 的概率密度函数一样, 函数 $g_{LO}(x)$ 也可以通过数值计算的方法获得, 如图 2 所示.

为了简化 $g_{LO}(x)$ 的计算, 可以用打孔器 (hole puncher)、剪刀 (clipper)、硬限幅器 (hard limiter) 以及组合曲线等基本形状来近似地替代 $g_{LO}(x)$ 的非线性形状^[14, 15]. 利用这些非线性曲线来替换 $g_{LO}(x)$ 各具特点, 例如, 在输入值很小的情况下, 打孔器提供了 $g_{LO}(x)$ 的一个很好的近似. 从 $g_{LO}(x)$ 的渐近特性可以看出, 在原点附近, 它可近似地看成是一个线性函数, 但是当输入值增大时, $f_{\alpha, \gamma}(x) \approx C |x|^{-\alpha-1}$, 也就是说, 当 x 趋向 $\pm \infty$ 时, $g_{LO}(x)$ 趋向 $(\alpha + 1)/x$. 因此, 这里采用如下的非线性函数来近似表示 $g_{LO}(x)$:

$$g_{LSO}(x) = \begin{cases} cx, & |x| \leq \lambda \\ (\alpha + 1)/x, & |x| > \lambda \end{cases} \quad (7)$$

其中 $\lambda = \arg \max g_{LO}(x)$, $c = (\alpha + 1)/\lambda^2$, λ 的取值取决于参数 α .

由文献[9]可知, 尽管 SaaS 具有无限方差, 检验统计量 $l(Y)$ 是一个具有有限均值和方差的渐近高斯随机

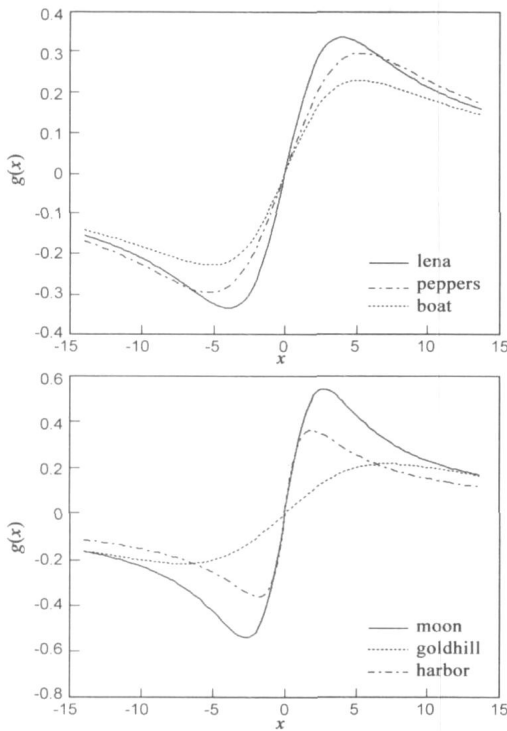


图 2 测试图像的 $g_{LO}(x)$ 曲线

变量, 在假设 H_0 成立的条件下, 其均值和方差分别为:

$$\mu = E(l(Y)|H_0) = \sum_{i=1}^N w_i \int_{-\infty}^{\infty} \frac{df(x_i)}{dx_i} dx_i \quad (8a)$$

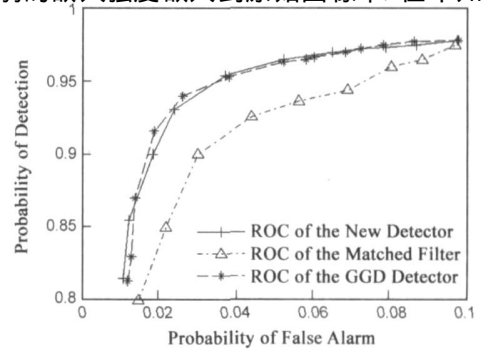
$$\sigma^2 = \sum_{i=1}^N w_i^2 \text{var} \left(\frac{df(x_i)}{dx_i} \right) \quad (8b)$$

可以看出: 在 H_0 下, 检验统计量 $l(Y)$ 的渐近概率密度函数的均值为零, 方差的大小则由参数 α 所决定, 与未知参数 θ 无关. 对于给定的判决阈值, 理论上有一个恒定的虚警概率与之对应. 因此, 推导出的隐藏信息检测方法实质上是根据广义 Neyman-Pearson 准则, 使得在固定虚警概率的情况下, 检测器的势函数在 $\theta = 0$ 附近的斜率达到最大.

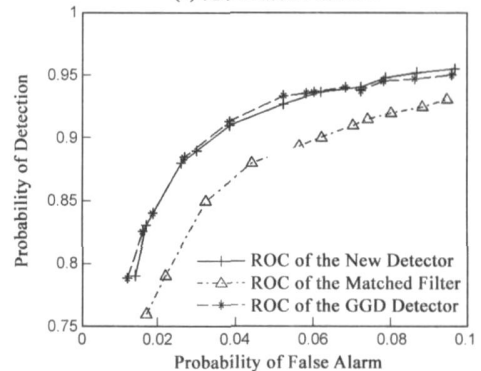
4 仿真实验

在仿真实验中, 我们采用 512×512 的 Lena 图像作为测试图像. 隐藏信息为“信息安全”的图标, 对它进行扩频调制嵌入到原始载体图像中, 实验参数和文献[13]一样. 使用接收机工作特性(Receiver Operation Characteristic, ROC)作为检测器性能的衡量标准. ROC 是以判决阈值 η 作为参变量, 检测概率 P_D 随虚警概率 P_{FA} 变化的函数关系. 具体步骤如下: (1) 首先对 Lena 图像进行 DCT 变换, 获得 DCT 变换系数. (2) 利用极大似然估计法求出交流 DCT 系数的 SaS 统计模型特征指数 α 的估计值. 由于隐藏的信息是一种弱信号, 可假定它不会改变原始图像的统计分布特性, 因此, 可用检测图像的估

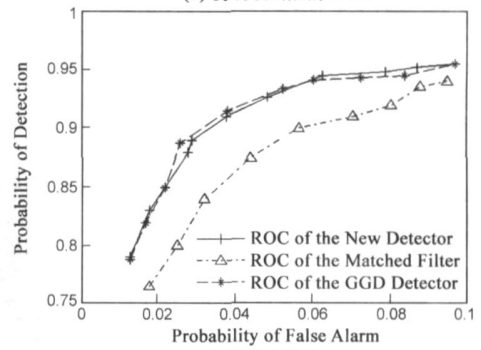
计值替代原始图像的估计值^[5-7]. (3) 由 α 的估计值确定 $g_{LO}(x)$ 的非线性近似曲线. (4) 根据设定的判决阈值 η 由式(5)作隐藏信息是否存在的蒙特卡罗仿真实验. 每次实验, 根据不可见约束条件, 将隐藏信息扩频调制后以弱的嵌入强度嵌入到原始图像中. 在不知道嵌入



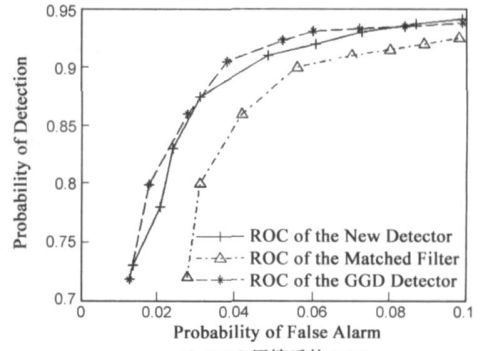
(a) 无攻击情况下的 ROC



(b) 剪切攻击后的 ROC



(c) 加噪攻击后的 ROC



(d) JPEG 压缩后的 ROC

图 3 检测器的检测性能比较

强度的情况下,作隐藏信息是否存在的检测时.如果检验统计量 $l(Y)$ 大于判决阈值 η ,则检测到信息的存在.同样,原始图像并不嵌入信息,利用式(5)分别进行隐藏信息存在与否的检测,如果统计量 $l(Y)$ 的绝对值大于 η ,则发生一次虚警.

为了考察算法的鲁棒性,我们对图像进行了常见的剪切、加噪、JPEG 压缩等图像处理 and 干扰之后的隐藏信息检测实验.其中剪切实验采取随意切除方式;JPEG 压缩的质量系数为 0.88;抗噪声攻击实验添加的是高斯白噪声,信噪比为 33.65dB.作为检测性能的比较,我们分别使用匹配滤波器以及基于 GGD 模型并使用了点消除技术的检测器进行蒙特卡罗仿真实验,部分实验结果如图 3 所示.

可以看出,本文提出的基于 α 稳定分布模型的检测器与基于 GGD 模型的检测器都比线性相关检测器获得的更好的检测结果.尽管新提出的检测器与 GGD 检测器的性能相近,但是 GGD 检测器需要点清除过程,至于具体需要消除哪些点取决于相应的数字媒体,并且还需要一定的技巧,目前还不存在一个通用的解决办法.因此,基于 α 稳定分布模型的检测器比采用 GGD 模型的检测方法实现起来更加简单,检测性能也更加稳定.

5 结论

信息隐藏技术的研究还面临许多问题,如其理论基础还不完善,实用化技术还欠成熟.本文以统计信号处理理论作为隐藏信息鲁棒检测的理论基础,使用 α 稳定分布模型来描述交流 DCT 系数的统计分布特性,并利用隐藏信息的不可感知特性,提出了一种 DCT 域加嵌入隐藏信息的鲁棒检测方法.由于 α 稳定分布模型在绝大多数情况下能更好地描述交流 DCT 系数的强拖尾特性,因此,本文在弱信号条件下根据 α 稳定分布概率模型进行统计推断,推导出的隐藏信息检测方法比采用匹配滤波器的方法性能优越,比基于广义高斯模型的方法实现起来简单.尽管本文研究的对象是数字图像,但提出的检测算法很容易扩展到音频和视频内容,而且很容易与相应的视觉或听觉感知掩蔽模型结合起来,从而获得更好的检测性能.

参考文献:

- [1] H V Poor. An Introduction to Signal and Estimation[M]. New York: Springer Verlag, 1994.
- [2] E Sayrol, J Vidal, S Cabanillas, et al. Optimum watermark detection in color images[A]. ICIP'99[C], vol. 2, 1999. 231-235.
- [3] R W Buccigrossi, P Simoncelli. Image compression via joint statistical characterization in the wavelet domain[J]. IEEE Trans Image Processing, 1999, 8(12): 1688-1701.
- [4] A Briassouli, P Tsakalides, A Stouraitis. Hidden messages in

heavy tails: DCT domain watermark detection using alpha stable models[J]. IEEE Trans Multimedia, 2005, 7(4): 700-715.

- [5] J R Hernández, M Amado, Fernando Pérez González. DCT domain watermarking techniques for still images: Detector performance analysis and a new structure[J]. IEEE Trans on Image Processing, 2000, 9(1): 55-68.
- [6] Q Cheng, T S Huang. An additive approach to transformed domain information hiding and optimum detection structure[J]. IEEE Trans Multimedia, 2001, 3(3): 273-283.
- [7] Q Cheng, T S Huang. Robust optimum detection of transform domain multiplicative watermarks[J]. IEEE Trans Signal processing, 2003, 51(4): 906-924.
- [8] Robert J Adler, Raisa E Feldman, Murad S Taqqu. A Practical Guide to Heavy Tails: Statistical Techniques and Applications[M]. Boston: Birkhuser, 1998.
- [9] C L Nikias, M Shao. Signal Processing with Alpha Stable Distributions and Applications[M]. John Wiley, 1995.
- [10] J P Nolan. Maximum likelihood estimation and diagnostics for stable distributions[OL]. <http://academic2.american.edu/~jpnolan/stable/mle.ps>.
- [11] J P Nolan. Numerical calculation of stable densities and distribution functions[J]. Commun Statist - Stochastic Models, 1997, 13(2): 759-774.
- [12] J S Bodenschatz, C L Nikias. Maximum likelihood symmetric α stable parameter estimation[J]. IEEE Transactions on Signal Processing, 1999, 47(5): 1382-1384.
- [13] 孙中伟, 朱岩, 冯登国. DCT 域图像水印的局部优化检测性能研究[J]. 电子学报, 2005, 33(5): 864-867.
Sun Zhongwei, Zhu Yan, Feng Dengguo. The performance analysis of DCT-domain watermark detection based on local optimum detection[J]. Acta Electronica Sinica, 2005, 33(5): 864-867. (in Chinese)
- [14] E E Kuruoglu, P W J Fitzgerald, W J Rayner. Near optimal detection of signals in impulsive noise modeled with a symmetric α stable distribution[J]. IEEE Communications letters, 1998, 2(10): 282-285.
- [15] E E Kuruoglu, P J W Rayner, W J Fitzgerald. A near optimal receiver for detection in α stable distributed noise[A]. Proc. of the Ninth IEEE SP Workshop on Statistical Signal and Array Processing[C]. 1998. 419-422.

作者简介:



孙中伟 男, 1969 年出生, 博士, 副教授. 主要研究方向为多媒体信号处理及信息安全.

E-mail: sunzwen@yahoo.com.cn