Digital Watermark Detection in Visual Multimedia Content

PhD Thesis Defense

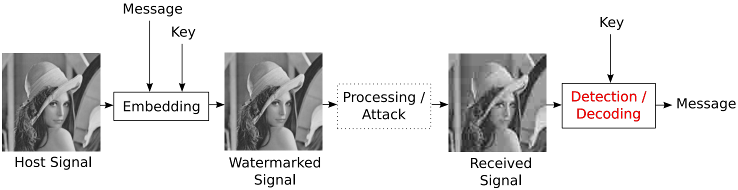
Peter Meerwald

Dept. of Computer Sciences, University of Salzburg

September 2010

Watermarking

- Watermarking is a technology to embed information into multimedia content in an imperceptible, yet detectable way. [Cox et al., 2007]



- Applications: Copyright protection, fingerprinting (traitor tracing), . . .

Motivation and Outline

Thesis supported by Austrian Science Fund (FWF) project P19159 on "Adaptive Streaming of Secure Scalable Wavelet-based Video".

1. Efficient spread-spectrum watermark detection
2. Watermarking of scalable multimedia formats

Other topics

- Watermark detection in raw and demosaicked images
- Attacks on quantization-based watermarking schemes
- Watermark detection in the Dual Tree Complex Wavelet Transform (DT-CWT) domain
- Watermarking of 2D vector graphics

Detection Problem

- Detection problem for additive spread-spectrum watermarking can be formulated as a hypothesis test to decide between absence ($\mathcal{H}_0$) or presence ($\mathcal{H}_1$) of the watermark $\mathbf{w}$ in the received signal $\mathbf{y}$ of length N

$$\begin{aligned} \mathcal{H}_0 : \quad & y[t] = x[t] & t = 1, \ldots, N \\ \mathcal{H}_1 : \quad & y[t] = x[t] + \alpha w[t] & t = 1, \ldots, N \end{aligned}$$

- Likelihood-Ratio Test (LRT) minimizes the probability of miss given a probability of false-alarm [Kay, 1998]

$$L(\mathbf{y}) := \log \left(\frac{p(\mathbf{y}; \mathcal{H}_1)}{p(\mathbf{y}; \mathcal{H}_0)} \right) > \log(\tau) =: T$$

  where $p(\cdot)$ denotes the Probability Density Function (PDF) of the signal and T is the detection threshold

- (Unrealistic) assumption: complete knowledge of the host signal PDF and the embedding strength $\alpha > 0$

Watermark Detector Ingredients

Ingredients

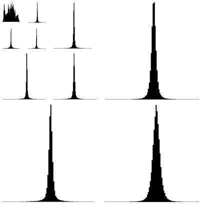
1. Host signal model (which?) with parameter estimates (how?)
2. Detection statistic (based on LRT or Rao Test) depending on host signal model (computationally efficient?)
3. Detection threshold for a given false-alarm rate, e.g. 10^{-6}
   - For the LRT we need parameters of the detection statistic under $\mathcal{H}_0$
   - Rao tests lead to constant false-alarm rate (CFAR) detectors, the threshold does not depend on the signal or embedding strength α
   - Reliable?

Research Questions

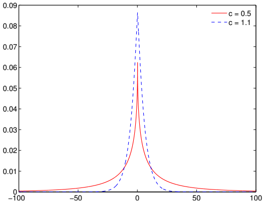
- How do host signal model and parameter estimation approaches change detection performance?
- What is the computational effort for estimation, evaluation of the detection statistic and threshold determination?
- Can we identify a more 'practical' detector than LRT with a Generalized Gaussian (GG) model [Hernández et al., 2000]?

Host Signal Modeling

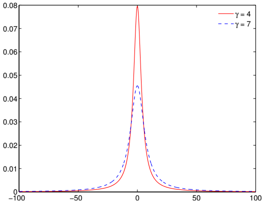
DCT and DWT coefficients of natural images are non-Gaussian
[Birney and Fischer, 1995]



DWT subband histograms



GG



Cauchy

GG distribution

$$p(x|a,c) = \frac{c}{2a\Gamma(1/c)} \exp\left(-\left|\frac{x}{a}\right|^c\right)$$

scale parameter $a > 0$

shape parameter $c > 0$

Cauchy distribution

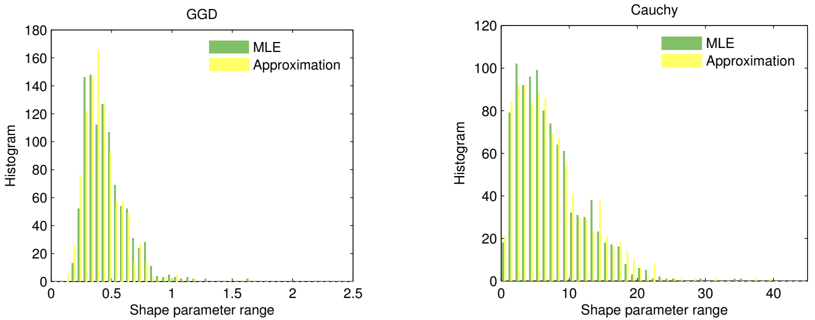
$$p(x|\gamma,\delta) = \frac{1}{\pi}\frac{\gamma}{\gamma^2+(x-\delta)^2}$$

location parameter δ (≈ 0)

shape parameter $\gamma > 0$

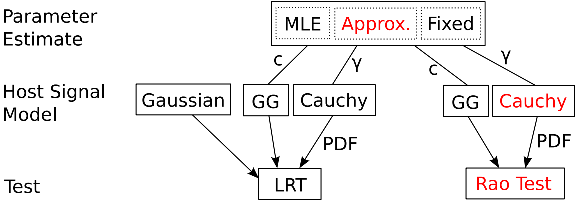
Parameter (GG a, c, Cauchy δ, γ) Estimation Options

- Maximum Likelihood Estimation (MLE) [Varanasi and Aazhang, 1989]
- Approximative methods
  [Krupinski and Purczynski, 2006, Tsihrintzis and Nikias, 1996]
- Fixed settings (e.g. $c = 0.8$, $\gamma = 8$)



GG and Cauchy shape parameter estimates over DWT detail subbands of 1000 natural images

Detection Statistics



Proposed Rao-Cauchy detection statistic

$$\rho_{\text{Rao-C}} = \left[\sum_{t=1}^{N} \frac{y[t]w[t]}{\gamma^2 + y[t]^2} \right]^2 \frac{8\gamma^2}{N}$$

Prior Work

$$\rho_{\text{LC}} = \frac{1}{N} \sum_{t=1}^{N} y[t]w[t] \qquad \rho_{\text{LRT-GG}} = \frac{1}{a^c} \sum_{t=1}^{N} \left(|y[t]|^c - |y[t] - \alpha w[t]|^c \right)$$

$$\rho_{\text{LRT-C}} = \sum_{t=1}^{N} \log \left(\frac{\gamma^2 + y[t]^2}{\gamma^2 + (y[t] - \alpha w[t])^2} \right) \qquad \rho_{\text{Rao-GG}} = \frac{\left(\sum_{t=1}^{N} \operatorname{sgn}(y[t]) w[t] |y[t]|^c \right)^2}{\sum_{t=1}^{N} |y[t]|^{2c}}$$

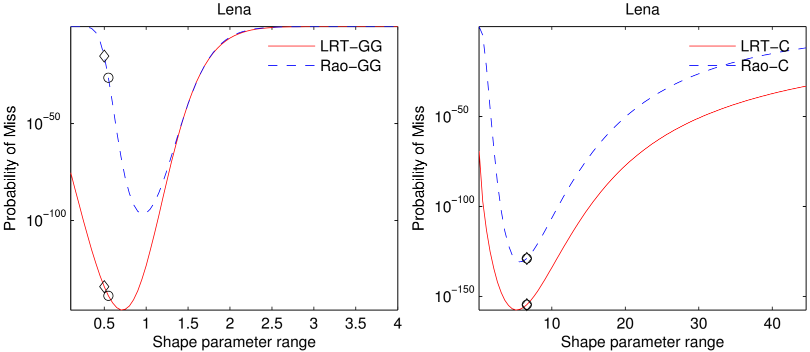
Number of arithmetic operations

Operations	$+, -$	$\times, \div$	pow, log	$\|\cdot\|$, sgn
LC	N	N		
LRT-GG	3N	N	2N	2N
LRT-C	4N	4N	N	
Rao-GG	2N	3N	N	2N
Rao-C	2N	3N		

Arithmetic operations to compute the detection statistic (signal length N)

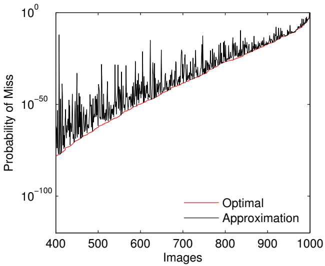
$+, \times$ execute in single cycle; pow, log take hundreds of cycles

Impact of Host Signal Parameter Estimates

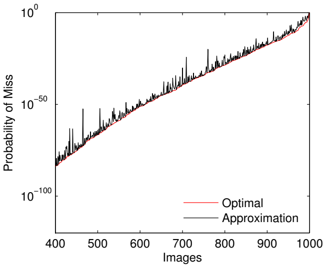


Probability of miss (P_m) as a function of the GG and Cauchy shape parameter (c and γ, resp.) at 16 dB DWR and $P_f = 10^{-6}$. Circle ($\circ$) and diamond ($\diamond$) denote ML and approximate parameter estimates.

LRT-GG versus Rao-C under JPEG Compression



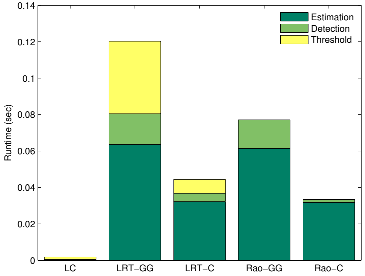
LRT-GG



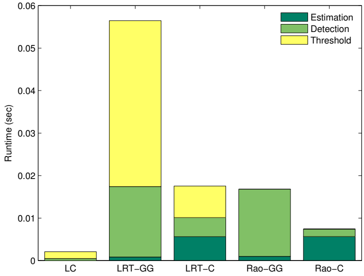
Rao-C

- Performance under attack (JPEG $Q = 70$)
- Better detection performance with Cauchy (better estimates)
- MLE does not improve performance over approximative estimates

Runtime Measurement of Detector Ingredients



MLE



Approximation

Runtime measurements in MATLAB on 2.6 GHz Intel Core2 using MLE and fast approximation for 256×256 detail subband

Summary

- Rao-Cauchy detector provides performance comparable to LRT-GG detector with reduced computational effort
- Cauchy is the favorable model over GG under compression attack, GG ist more sensitive to estimation 'errors'
- MLE does not lead to optimal performance
- Approximative parameter estimates can be used, or even fixed settings
- No threshold determination and embedding strength knowledge necessary for Rao tests

Contribution

Rao detector based on Cauchy host signal model

Kwitt, R., Meerwald, P., and Uhl, A. (2008). A lightweight Rao-Cauchy detector for additive watermarking in the DWT-domain. In *Proceedings of the ACM Multimedia and Security Workshop (MM&Sec '08)*, pages 33–41, Oxford, UK. ACM.

Comparing computational efficiency of spread-spectrum watermark detection approaches

Kwitt, R., Meerwald, P., and Uhl, A. (2009). Efficient detection of additive watermarking in the DWT-domain. In *Proceedings of the 17th European Signal Processing Conference (EUSIPCO '09)*, pages 2072–2076, Glasgow, UK.

Trading host signal model and parameter estimation versus detection performance

Kwitt, R., Meerwald, P., and Uhl, A. (2010). Lightweight detection of additive watermarking in the DWT-domain. *IEEE Transactions on Image Processing*, 2010. (accepted)

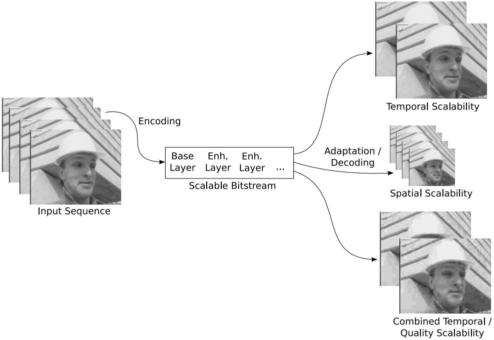
Integer-only LRT based on simplified host signal model

Meerwald, P. and Uhl, A. (2010). Watermark detection on quantized transform coefficients using product Bernoulli distributions. In *Proceedings of the ACM Multimedia and Security Workshop, MM&Sec '10*, pages 175–180, Rome, Italy.

Application: Watermarking Scalable Video

Scalability in Multimedia Coding

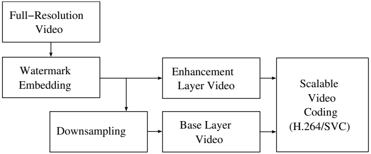
- A *scalable bitstream* efficiently stores multiple representations of the same data with different quality, spatial and/or temporal resolutions.



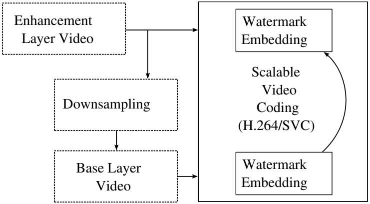
- Standards: JPEG2000 (image), H.264/SVC (video)

Embedding Options

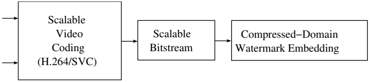
For H.264/SVC Coding



Embedding before encoding

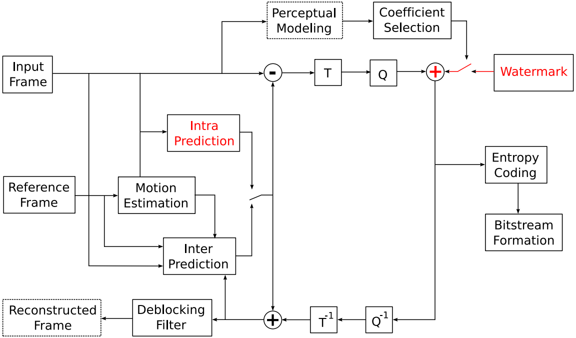


Integrated embedding and coding



Compressed-domain embedding

H.264 Watermarking Framework

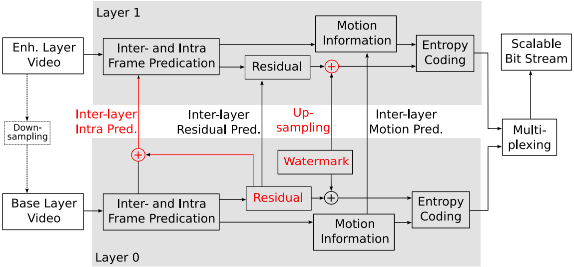


Additive spread-spectrum watermark is embedded in selected *intra* predicted residual 4×4 DCT coefficients
[Noorkami and Mersereau, 2007]

Rao-Cauchy detector significantly improves detection performance over linear correlation detector used in prior work

Watermarking Integrated with H.264/SVC

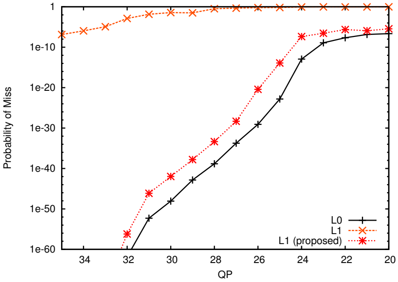
- H.264/SVC introduces inter-layer prediction tools [Schwarz and Wien, 2008], base layer reconstruction is used to predict *intra* coded blocks of enhancement layer



- Considering video with two resolution layers (e.g. L0: QCIF 176×144 and L1: CIF 352×288)

Watermarking Multiple Resolution Layers

- Base-layer (L0) watermarking is insufficient to protect enhancement layer (L1) video
- H.264/SVC codes the difference between L1 data and the prediction derived from the base layer data; L0 watermark 'survives' for coarse quantization (QP > 28) only
- Separate watermarking of layers significantly increases bit rate (+10%)



Experimental Results

- Base layer watermark increases base and enhancement layer bit rate (+3% in L1)
- Proposal: add (upsampled) watermark signal to enhancement layer
  - Reduces L1 bitrate (−1%)
  - Enables watermark detection in enhancement layer
  - Applicable to H.264/SVC resolution and coarse grain quality scalability layers
- Prior work: linear correlation detection
  - Rao-Cauchy detector benefits from quantized transform coefficient statistics
  - Efficient watermark detection important when integrated in video decoding

Contribution

State-of-the-art survey, need for modeling of layer characteristics

Meerwald, P. and Uhl, A. (2008). Toward robust watermarking of scalable video. In *Proceedings of SPIE, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, volume 6819, San Jose, CA, USA.

Incremental watermark detection using multi-channel modeling under JPEG2000 and JPEG compression

Meerwald, P. and Uhl, A. (2008). Scalability evaluation of blind spread-spectrum image watermarking. In *Proceedings of the 7th International Workshop on Digital Watermarking, IWDW '08*, volume 5450 of *Lecture Notes in Computer Science*, pages 61–75, Busan, South Korea. Springer.

Watermarking motion-compensated residual with blind detection and averaging/estimation attacks

Meerwald, P. and Uhl, A. (2008). Blind motion-compensated video watermarking. In *Proceedings of the 2008 IEEE Conference on Multimedia & Expo, ICME '08*, pages 357–360, Hannover, Germany.

Watermarking integrated with H.264/SVC coding

Meerwald, P. and Uhl, A. (2010). Robust watermarking of H.264-encoded video: Extension to SVC. In *Proceedings of the Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP '10*, pages 82–85, Darmstadt, Germany. (accepted)

Summary and Conclusion

Conclusion

- Detection is a crucial component of a watermarking *system;* incorporating the characteristics of the host signal can improve performance
- Assessment of parameter estimation and detection with regard to computational effort
- Proposed and evaluated a lightweight detection approach
- Successful application in watermarking of scalable multimedia formats (and other areas)
- Source code available at `http://www.wavelab.at/sources` to reproduce results

References I

Birney, K. A. and Fischer, T. R. (1995).
On the modeling of DCT and subband image data for compression.
IEEE Transactions on Image Processing, 4(2):186–193.

Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., and Kalker, T. (2007).
Digital Watermarking and Steganography.
Morgan Kaufmann.

Hernández, J. R., Amado, M., and Pérez-González, F. (2000).
DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure.
IEEE Transactions on Image Processing, 9(1):55–68.

Kay, S. M. (1998).
Fundamentals of Statistical Signal Processing: Detection Theory, volume 2.
Prentice-Hall.

Krupinski, R. and Purczynski, J. (2006).
Approximated fast estimator for the shape parameter of Generalized Gaussian distribution.
Signal Processing, 86(2):205–211.

Lin, E. T., Podilchuk, C. I., Kalker, T., and Delp, E. J. (2004).
Streaming video and rate scalable compression: what are the challenges for watermarking?
Journal of Electronic Imaging, 13(1):198–208.

Noorkami, M. and Mersereau, R. M. (2007).
A framework for robust watermarking of H.264 encoded video with controllable detection performance.
IEEE Transactions on Information Forensics and Security, 2(1):14–23.

References II

Piper, A., Safavi-Naini, R., and Mertins, A. (2005).
Resolution and quality scalable spread spectrum image watermarking.
In *Proceeding of the 7th Workshop on Multimedia and Security, MMSEC '05*, pages 79–90, New York, NY, USA. ACM.

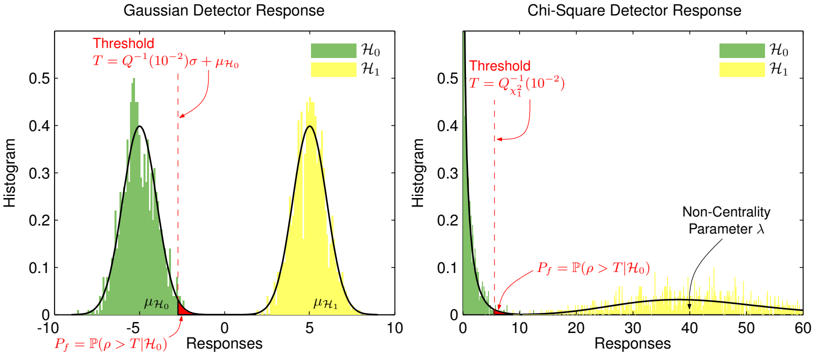
Schwarz, H. and Wien, M. (2008).
The scalable video coding extension of the H.264/AVC standard.
IEEE Signal Processing Magazine, 25(2):135–141.

Tsihrintzis, G. A. and Nikias, C. L. (1996).
Fast estimation of the parameters of alpha-stable impulsive interference.
IEEE Transactions on Signal Processing, 44(6):1492–1503.

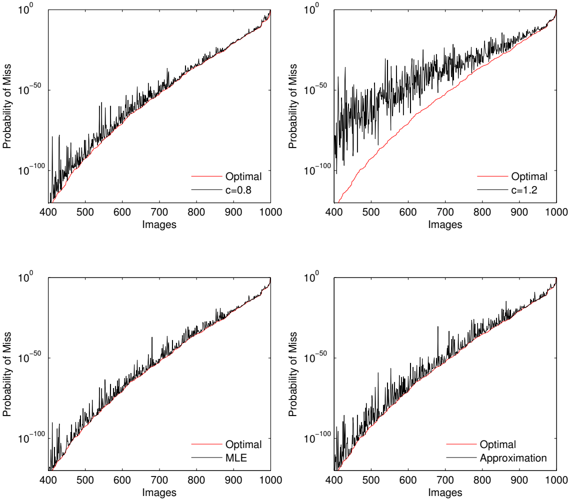
Varanasi, M. and Aazhang, B. (1989).
Parameteric Generalized Gaussian density estimation.
Journal of the Acoustical Society of America, 86(4):1404–1415.

Detector Responses

- The LRT detection statistics follow a Gaussian under both hypothesis with different parameters ($\mu_{\mathcal{H}_0}$, $\mu_{\mathcal{H}_1}$, $\sigma^2_{\mathcal{H}_0} \approx \sigma^2_{\mathcal{H}_1}$).
- The Rao Test detection statistics follow a χ^2 distribution with one degree of freedom under $\mathcal{H}_0$ and a non-central χ^2 distribution with one degree of freedom and non-centrality parameter λ.

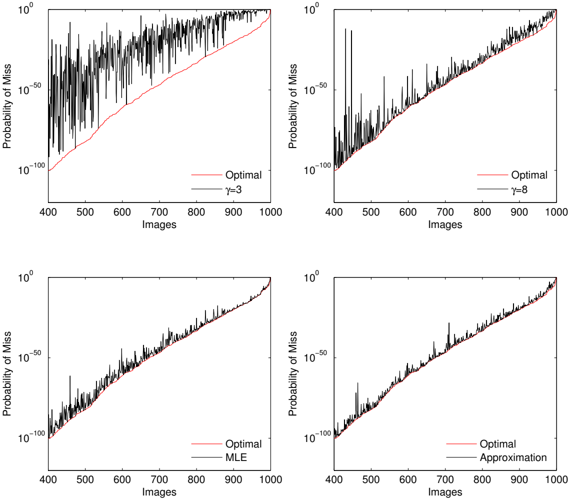


Detection Performance: LRT-GG



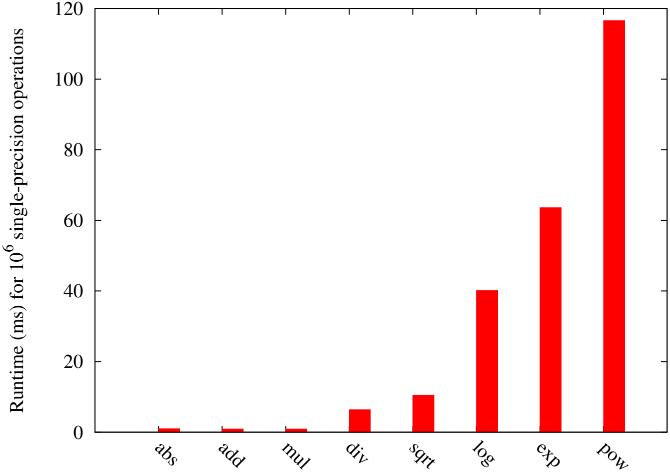
LRT-GG probability of miss (P_m) over 1000 images for different choices of c at 16 dB DWR and $P_f = 10^{-6}$.

Detection Performance: Rao-C

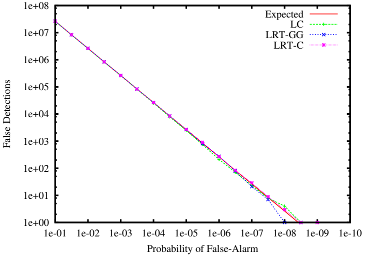


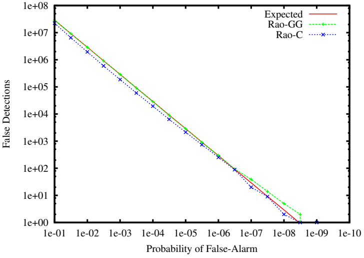
Rao-C probability of miss (P_m) over 1000 images for different choices of γ at 16 dB DWR and $P_f = 10^{-6}$.

Runtime of Single-Percision Operations



False-Alarm Rate versus False Detections





Maximum Likelihood Estimation of Host Signal Model Parameters

To determine the MLEs for the Cauchy or GGD shape parameter, we have to solve

$$\frac{1}{N}\sum_{t=1}^{N}\frac{2}{1+(x[t]/\hat{\gamma})^2}-1=0 \quad \text{(Cauchy)}$$

or

$$1+\frac{\psi(1/\hat{c})+\log\left(\frac{\hat{c}}{N}\sum_{t=1}^{N}|x[t]|^{\hat{c}}\right)}{\hat{c}} - \frac{\sum_{t=1}^{N}|x[t]|^{\hat{c}}\log(|x[t]|)}{\sum_{t=1}^{N}|x[t]|^{\hat{c}}}=0 \quad \text{(GG)}$$

numerically. Approximately the same number of iterations are necessary (Newton-Raphson), however the computation effort is much higher for the GGD.

Fast Parameter Estimation

For the Cauchy parameter, we simply use the iteration starting value

$$\hat{\gamma}_1 = 0.5(x_p - x_{1-p}) \tan(\pi(1-p)),$$

with $0.5 < p < 1$ and x_p, x_{1-p} denoting the sample quantiles with $p = 0.75$.

For the GG shape parameter, [Krupinski and Purczynski, 2006] propose a piecewise approximation of the inversion function

$$\hat{c} = F^{-1}\left(\frac{E_1}{\sqrt{E_2}}\right)$$

based on the absolute mean E_1 and variance E_2 of the data set.

Fast Parameter Estimation Effort

Detector	Operations			
	+,-,==	$\times, \div$	pow, log	abs, sgn
Fast GGD [Krupinski et al., 2006]	3N	N	N	N
Fast Cauchy	Nlog(N)			

Cauchy parameter estimation requires sorting the data.

Rao Hypothesis Test

- Two-sided composite hypothesis testing problem with one nuisance parameter γ
- In contrast to LRT, Rao test does not require to estimate unknown parameter α under $\mathcal{H}_1$
- For symmetric PDFs [Kay, 1998], the Rao test statistic can be written as

$$\rho(\mathbf{y}) = \left[\sum_{t=1}^{N} \frac{\partial \log p(y[t] - \alpha w[t], \hat{\gamma})}{\partial \alpha} \bigg|_{\alpha=0} \right]^2 \mathbf{I}_{\alpha\alpha}^{-1}(0, \hat{\gamma})$$

  $p(\cdot)$ denotes the Cauchy PDF, $\hat{\gamma}$ is the MLE of the Cauchy shape parameter, $\mathbf{I}_{\alpha\alpha}^{-1}$ is an element of the Fisher Information matrix
- Rao test is asymtotically optimal for large data sets

Scalable Watermarking: Properties and Challenges

- Properties of scalable watermarking [Piper et al., 2005]
  - *Detectability*: Watermark should be detectable in any portion of the content which is of acceptable quality.
  - *Graceful improvement*: Increased portions of the content should provide reduced error in watermark detection.
- Other aspects / challenges of watermarking scalable content [Lin et al., 2004]
  - Robustness to scalable coding
  - Integration with scalable coding
  - ...