Side informed algorithms for image authentication and forensics

Gabriel Domínguez Conde
Advisors: Fernando Pérez González and Pedro Comesaña Alfaro

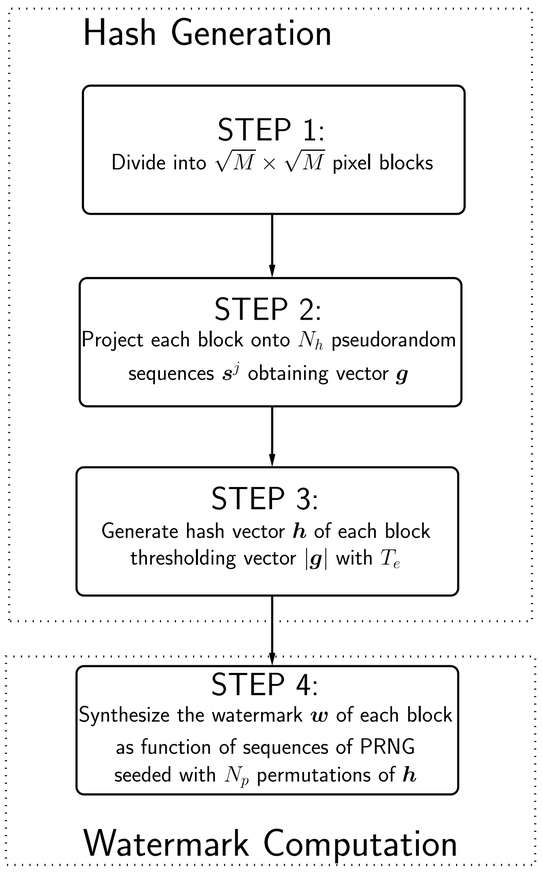
Signal Processing and Communications Group

Universidade Vigo

2013 Workshop on Monitoring PhD Student Progress, Vigo (Galicia)

Performance Analysis of the Fridrich-Goljan Self-Embedding Authentication Method

Hash and Watermark Computation

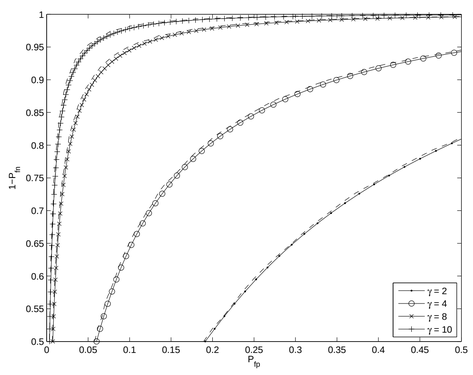


Detection & Performance Analysis

- The hash and the watermark are recomputed using the received image
- The decision of presence or absence of the estimate of the watermark is formulated as the following hypothesis test:

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{z} = \eta\left(\mathbf{x} + \gamma\hat{\boldsymbol{w}}\right) + \mathbf{n} \\ \mathcal{H}_1 &: \mathbf{z} = \mathbf{x} + \gamma\hat{\boldsymbol{w}} \end{aligned}$$

- We model the effect of the embedding and the attack on the estimate of the hash on the detector side and how a non-perfect estimate of the watermark deteriorates the overall performance
- The performance of the algorithm is measured by means of the receiver operating characteristic (ROC) curve



Analytical (dashed lines) and empirical (solid lines) ROCs for a set of 14 images.

Conclusions

- The performance analysis of the self-embedding authentication method proposed by Fridrich and Goljan was carried out, verifying its accurateness empirically
- The embedding process of a self-embedding authentication method can modify the robust hash of the image corrupting the reconstructed watermark

Publications

- Domínguez-Conde. G; Comesaña, P.; and Pérez-González, F., "Performance Analysis of Fridrich-Goljan Self-Embedding Authentication Method," in IEEE International Conference on Image Processing (ICIP), Cairo, Egypt, 2009.
- Domínguez-Conde, G.; Comesaña, P.; and Pérez-González, F., "Performance Analysis of Fridrich-Goljan Self-Embedding Authentication Method," Information Forensics and Security, IEEE Transactions on , vol.4, no.3, pp.570-577, Sept. 2009.

Flat Fading Channel Estimation Based on Dirty Paper Coding

Background

Channel estimation transversal problem:

- Multimedia forensics
- Acoustic applications
- Communications

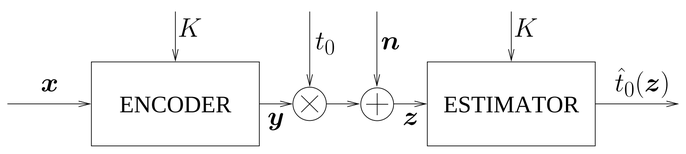
Some drawbacks of traditional training-based estimation techniques:

- The training signals must be frequently sent in order to update the channel state information in fast-varying channels
- The information bearing signal has to be shut down, requiring the implementation of additional logic to synchronize the pilot sequence slot

More recently, Superimposed Training is proposed sharing key elements with watermarking:

- Adding a known sequence to the information sequence
- Power restricted signals
- Host-interference

Problem Formulation



Block diagram of the flat fading channel estimation problem.

- $\boldsymbol{x}$ Information sequence
- K Secret key
- $\boldsymbol{y} = \boldsymbol{x} + \alpha\left(\mathcal{Q}_\Delta(\boldsymbol{x} - \boldsymbol{d}) - (\boldsymbol{x} - \boldsymbol{d})\right)$
- t_0 Scaling factor
- $\boldsymbol{n}$ Channel noise
- $\boldsymbol{z} = t_0\boldsymbol{x} + \boldsymbol{n}$
- $\hat{t}_0(\boldsymbol{z})$ Estimate of the scaling factor

Proposed DPC-based Estimation Technique

- Requirements:
  - No interruptions in the transmission
  - Power restrictions in the embedding distortion
  - Accurate estimation with few samples
  - Affordable computational resources
- Work hypotheses:
  - Host to Quantizer Ratio (HQR) $\triangleq \frac{12\sigma_X^2}{\Delta^2}$
  - Self-Noise to Channel-Noise ratio (SCR) $\triangleq \frac{(1-\alpha)^2 t_0^2 \Delta^2}{12\sigma_N^2}$
  - Total-Noise to Quantizer Ratio (TNQR) $\triangleq \frac{(1-\alpha)^2 t_0^2 \Delta^2/12 + \sigma_N^2}{t_0^2\Delta^2/12}$
  - Total-Noise to Host Ratio (TNHR) $\triangleq \frac{(1-\alpha)^2 t_0^2 \Delta^2/12 + \sigma_N^2}{t_0^2\sigma_X^2}$
- Two Considered Scenarios:
  - High-SNR: HQR$\gg 1$, SCR$\ll 1$, and TNQR $\ll 1$
  - Low-SNR: HQR$\gg 1$, SCR$\ll 1$, TNQR > 1, and TNHR $\ll 1$

Maximum Likelihood Estimation

Without *a priori* knowledge on t_0, the Maximum Likelihood estimation is followed:

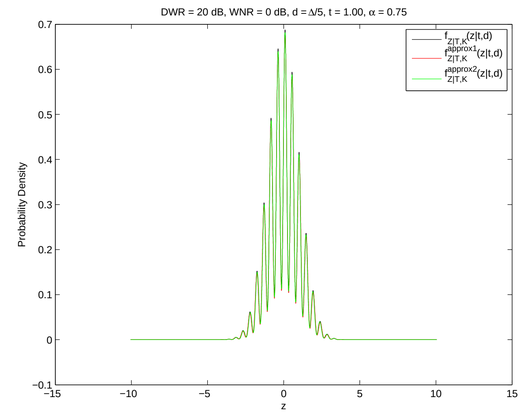
$$\begin{aligned} \hat{t}_0(\boldsymbol{z}) &= \underset{t}{\operatorname{argmax}}\, f_{\boldsymbol{Z}|T,K}(\boldsymbol{z}|t,d) \\ &= \underset{t}{\operatorname{argmin}} -\sum_{i=1}^{L} \log\left(f_{Z|T,K}(z_i|t,d_i)\right), \end{aligned}$$

Assuming that:

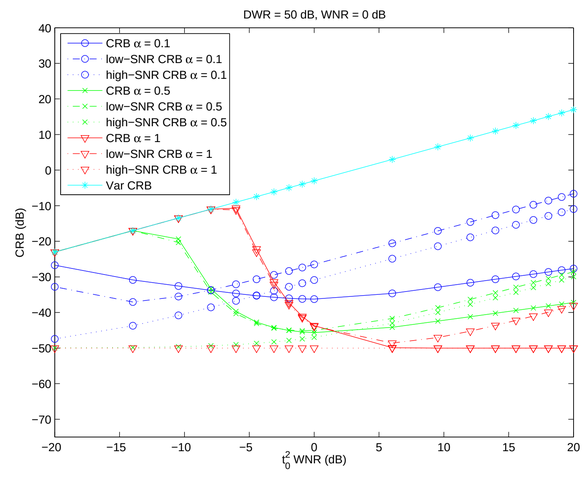
- $\boldsymbol{X}$ i.i.d
- $\boldsymbol{D} \sim \mathcal{U}([-\Delta/2, \Delta/2]^L)$
- $\boldsymbol{N}$ i.i.d and independent of $\boldsymbol{X}$ and $\boldsymbol{D}$

For the sake of mathematical tractability Gaussian distributed host and Gaussian distributed noise are assumed for the low-SNR and the high-SNR cases.

Example: Probability Density Function Approximations for Low-SNR

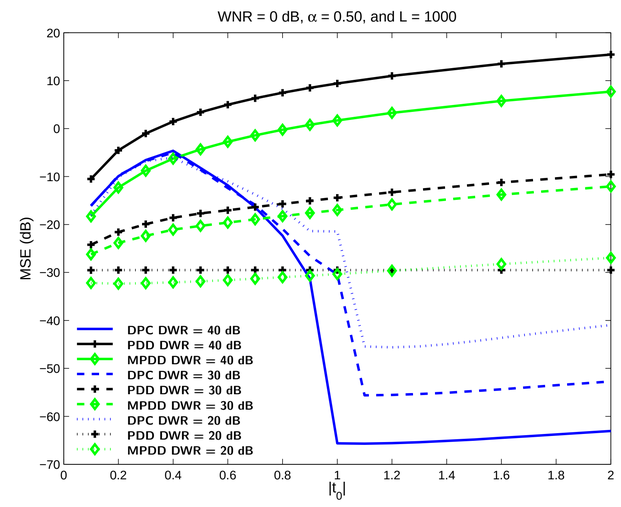


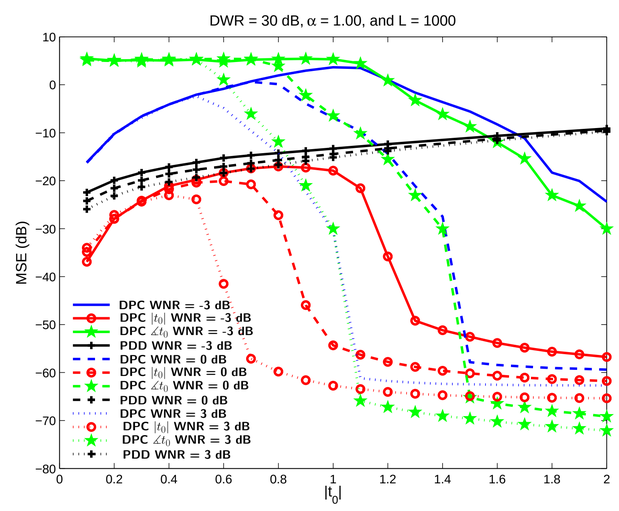
Example: Cramér-Rao Bound Approximations



Complex Scaling Factor Estimation for High-SNR

- Codebook defined in polar coordinates
- Problem decoupled: a) an estimator $|\hat{t}_0(\boldsymbol{z})|$ of the magnitude and b) an estimator $\measuredangle\hat{t}_0(\boldsymbol{z})$ of the argument





Publications

- Domínguez-Conde. G; Comesaña-Alfaro, P.; and Pérez-González, F., "Flat Fading Channel Estimation Based on Dirty Paper Coding", IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2014. Submitted.