Putting “Reproducible Signal Processing” into practice:

A case study in Watermarking

M. BARNI, G. BARTOLI - (UNIVERSITY OF SIENA, ITALY)
F. PÉREZ-GONZALEZ, P. COMESAÑA - (UNIVERSITY OF VIGO, SPAIN)
Signal processing and scientific methodology

- Many signal processing papers lack rigorous experimental validation
  - Theoretical papers are often verified by a single experiment carried out on a single signal/image
  - Performance are only rarely compared with those of competing schemes
  - Improvements are often justified by comparing with only one similar algorithm performing worse

- Even worse: vaguely described experimental conditions → no reproducibility of results
- Often, readers must simply trust the authors!
Why is this so?

- We all recognize the importance of good experiments but ...
  - Lack of time
  - Lack of research groups devoted to experimental signal processing or implementing someone else’s algorithms
  - Non-rewarding work
  - Intellectual property issues
- Encourage good experimental research
- Define a rigorous format for experiment description
Our approach to RSP

- A straightforward approach... **share** the software and the data set

- **Problems:**
  - **Portability:** which format should be used?
  - **Readability:** are the authors correctly implementing the described algorithm?
  - **Licensing problems:** open source or binary format?

- Algorithms and experiments have always to be carefully described:
  - Description (a block diagram or a pseudo-code)
  - Parameters
  - Dataset
A case study (in watermarking)

- UNIVigo provided an RSP description of a paper
- UNISI tries to reproduce UNIVigo’s results

- Goals of an *oracle attacker*:
  - Try to remove the watermark from a host signal/image

- Features:
  - *No knowledge* about the watermarking algorithm
  - Suitable for attacking *general detection functions*
  - Based only on the *binary output* of the detector
Algorithm steps

1. Step 1: Get perturbation and find \( \alpha \) such that \( y + \alpha s \) is on the boundary.
2. Step 2: Numerically evaluate gradient of \( dy(h_y(s)) \) and possibly Hessian on the boundary.
3. Step 3: Update
   \[ s_{k+1} = s_k - \xi_k \cdot \left[ \nabla^2 (d_y \circ h_y)(s_k) \right]^{-1} \cdot \nabla (d_y \circ h_y)(s_k) \]
4. Step 4: Go back to 1.
Our RSP objective

- To reproduce the results obtained by the authors of the paper (University of Vigo)

The Blind Newton Sensitivity Attack – (University of Vigo)

Parameters:
- DWR = 16 dB
- Pfα = 10^4(-4)
- N = 2048
- N = 4 [JANIS order]
- ck = 0.5 [GGauss shape]

- SS [-6.044 dB]
- SS-Angle [-6.044 dB]
- JANIS [-2.875 dB]
- G Gauss [-1.775 dB]
The experience we made

- **Originale paper (common problems)**
  - Focus on the algorithm core
  - Missing informations on initialization and/or stop condition details

- **Vigo** supplied material:
  - pseudo-code description
  - initialization procedure
  - Data set: synthetic random sequences (algorithm provided)

- **Siena** implemented the BNSA algorithm
  - The implementation of BNSA did not raise any particular problem
  - Nevertheless, several ambiguities were still present…
Insights we’ve got

- How to interpret graphs with no tables? How were the results on the 100-trials sequences averaged?
  - UniVIGO itself had difficulties in reproducing results.
- A few ambiguities about the initialization like 0/0 singularities or infinite loops
  - This was explained with direct communication between the two universities.
- UNIVigo used an approximation of the gradient instead of the true Hessian (different plots in the paper used different set-ups)
  - Siena obtained comparable results also with the approximated version (scientific insight)
Insights we’ve got

**MAIN PROBLEM**

- The re-implementation of *watermarking methods* (SS, SS-Angle, JANIS, GG) raised several interpretation problems
  - Communication between UNIVigo and UNISI was necessary
- **Estimation of false detection** probability was crucial for reproducibility, however, the way it was estimated was not clear
  - Different assumptions (no widely accepted solution) for the estimation
  - How often were the statistical parameters refreshed?
Reproduced results (1)

BNSA – SpreadSpectrum

- University of Vigo [-6.0403 dB]
- University of Siena [-5.9558 dB]

Power [dB]

Iterations

14/04/2007
Reproduced results (2)

BNSA :: Spread–Spectrum Angle

- University of Vigo \([-6.0426 \text{ dB}]\)
- University of Siena \([-5.8172 \text{ dB}]\)

Power [dB] vs. Iterations

14/04/2007 12
Reproduced results (3)

- University of Vigo: $-2.5939$ dB
- University of Siena: $-1.046$ dB
Reproduced results (4)

BNSA :: Generalized–Gaussian

Power [dB]

Iterations

University of Vigo \([-1.7454 \, \text{dB}\)]

University of Siena \([-2.0363 \, \text{dB}\)]
Conclusions

- **RSP is extremely insightful:**
  - We both gained a greater deal of knowledge about BNSA than an occasional reader

- **RSP relies on previous RSP:**
  - Ambiguities of involved papers are carried over future uses → more general consistence is needed

- **RSP is tough:**
  - The whole experience was harder than expected → experimental-research groups should be encouraged