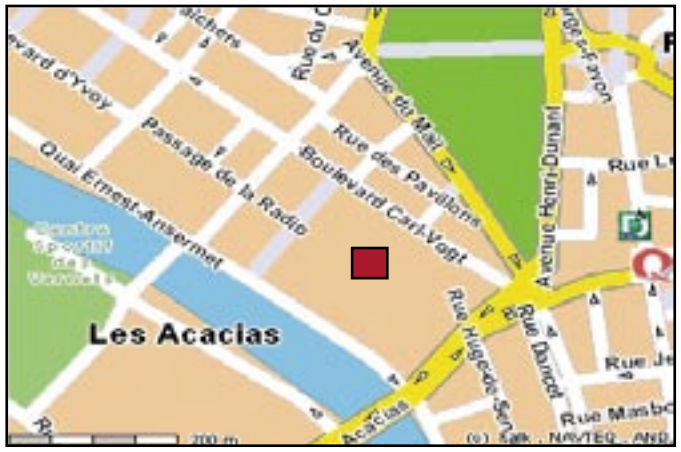
2. How does the output of the optimal watermarking algorithm look like?
For different application scenarios different optimal solutions and algorithms are sought for in digital watermarking.
This challenge proposed here is intended to identify application scenarios with their goals and characteristics. Furthermore the metrics to measure and compare these characteristics for selected algorithms are of interest. For the identified application scenarios the question is raised: how should the benchmarking results for an optimal watermarking algorithm for this application scenario look like? Can they be described within the triangular relationship between robustness, capacity and transparency, or have other characteristics to be considered, too? How can the comparability of benchmarking results be guaranteed? Which optimisation strategies for the parameterisation of watermarking algorithms do exist and how intend to improve the output of the algorithm?

Acknowledgments:
The WaCha 06 workshop is supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Part of the workshop programme and the realisation is supported by the University of Geneva, Department of Computer Sciences.

Workshop venue:

Room MR 070, UniMail, University of Geneva
Boulevard du Pont-d'Arve 40
CH-1211 Geneva, Switzerland



Programme committee:

Mauro Barni
National Inter-University Consortium for Telecommunications, Italy

Patrick Bas
Centre National de la Recherche Scientifique, France

Christian Cachin
IBM Research GmbH, Switzerland

Jana Dittmann
Otto-von-Guericke University Magdeburg, Germany

Andreas Lang
Otto-von-Guericke University Magdeburg, Germany

Fernando Perez-Gonzalez
University of Vigo, Spain

Sviatoslav Voloshynovskiy
University of Geneva, Switzerland

2ND WAVILA CHALLENGE

WaCha 06

GENEVA, SWITZERLAND
SEPTEMBER 28TH, 2006

Agenda:

Session I - Session chair: Patrick Bas

09:00-09:15 Welcome: Sviatoslav Voloshynovskiy
09:15-09:30 ECRYPT and WAVILA Introduction: Jana Dittmann
09:30-10:00 Introduction Challenge I: Mauro Barni, Alessandro Piva
10:00-11:00 Invited Talk: Scott Craver "Noise Calipers: A Technique for Reverse-engineering Correlation Detectors"
11:00-11:30 Paper Presentation: Kazuo Ohzeki, Li Congi, Kouhei Igarashi "Considering Knowledge of Watermarking Algorithm and Finding the Optimal Watermark Algorithm"
11:30-12:00 Discussion on Challenge I

12:00-13:00 Lunch

Session II - Session chair: Oleksiy Koval

13:00-13:15 Introduction Challenge II: Jana Dittmann
13:15-14:00 Invited Talk: Teddy Furon "Is benchmarking just an academic chimera?"
14:00-14:30 Paper Presentation: Andreas Lang, Jana Dittmann, David Megias, Jordi Herrera-Joancomarti "Practical Audio Watermarking Evaluation Tests and its Representation and Visualization in the Triangle of Robustness, Transparency and Capacity"

14:30-14:50 Coffee Break

14:50-15:20 Paper Presentation: Christian Kraetzer "Visualisation of Benchmarking Results in Digital Watermarking and Steganography"
15:20-16:20 Discussion on Challenge II
16:20-16:30 Conclusion: Sviatoslav Voloshynovskiy
16:30 End

Invited Talks:

Scott Craver
(Assistant Professor, Department of Electrical and Computer Engineering at Binghamton University, New York, USA)

Title: *"Noise Calipers: a technique for reverse-engineering correlation detectors"*

Abstract: Oracle attacks can be used to quickly reverse-engineer a secret watermark algorithm instead of attacking the watermark itself. The technique of noise calipers employs an oracle to quickly build a pair of severe false positives from a watermarked image. If a watermark detector uses a common feature-based architecture with a typical detector structure, these noise vectors can be used to plumb the shape of the detection region, and extract information about its use. We show how certain important pieces of information, such as the detector threshold and approximate number of watermarking features, can be leaked by a detector that uses normalized correlation or correlation coefficient.

Teddy Furon
(Researcher at the INRIA Institute, Rennes, France)

Title: *"Is benchmarking just an academic chimera?"*

Abstract: Imagine you are a watermarking designer. You are responsible for implementing a workable watermarking technique (for still images, sound, or movies) in a system, solution of a targeted application. You have read tons of more or less ‚theoretical' papers about watermarking schemes. You are about to select the most appropriate scheme in order to derive it into a true watermarking technique for your real life application. What should you care about? You will certainly face similar questions than the ones raised in Wacha'06 challenge #2: metrics, features, comparability.

If one asks a researcher from the academic world, his advice will be „Benchmark' em all!". This naive statement supposes that benchmarking is possible, relevant, and sufficient. An even worse academic chimera is the third trusted party (a la certimark) which certifies that this watermarking technique is the best for your application. Who knows what the best for you is?

Challenges:

1. Is knowledge of the watermarking algorithm useful for watermark removal? Following an approach similar to that used in cryptography, the problem of watermarking security is often approached by assuming that the attacker has full knowledge of the watermarking algorithm and that he explicitly uses such a knowledge to devise a, possibly optimal, attacking strategy. The assumption underlying the above perspective is that knowing the details of the watermarking algorithm is a great help for the attacker. Whereas in general this is surely true, some recent analyses seem to point out that if the aim of the attacker is limited to watermark removal, or to make it unreadable to the detector/decoder, knowledge of the watermarking algorithm is of limited, if any, help. Some evidence of this fact is given by the effectiveness of some recently proposed blind sensitivity attacks, that are able to remove the watermark while keeping an extremely high PSNR (e.g. more than 50dBs) between the watermarked and the attacked version of the image. Similar results seem to stem from the BOWS contest (http://lci.det.unifi.it/BOWS, run in the period December 2005-June 2006) where very powerful attacks were devised even if the underlying algorithm was not known. A possible interpretation is that whenever the watermarking algorithm results in a very complicated detection region, no particular advantage is got by knowing the watermarking algorithm. On the contrary, such an advantage is a significant one for schemes characterized by simple detection regions.

It is the aim of the second WAVILA Challenge to investigate the above problem trying to answer the following questions: Is knowledge of the watermarking algorithm of any practical help to attackers? Does the answer to the previous question depend on the complexity of the watermark detection/decoding region(s)? If knowledge of the algorithm does not help to reduce the obtrusiveness of the attack, do you think it may still be useful to reduce its complexity? Is watermark robustness more difficult to achieve than watermark security?