**Call for contributions:**

## Second WAVILA Challenge (WaCha'06), Geneva, Switzerland

September 28th, 2006
(website: http://omen.cs.uni-magdeburg.de/ecrypt/wacha06/)

As part of its activity, the Watermarking Virtual Laboratory (WAVILA) of the European Network of Excellence ECRYPT organises in conjunction with the two day ACM Multimedia and Security Workshop 2006 (MM&Sec 2006) a working meeting discussing some of the hottest themes in watermarking security and benchmarking. Based on the experiences from the second ECRYPT year this working day will take the form of a challenge: two important problems related to watermarking security will be brought to the attention of the watermarking community and thoroughly discussed.

**Four types of contributions are foreseen:**

- WAVILA researchers will introduce the problems and present WAVILA's preliminary results.
- Researchers from the other ECRYPT VLs will be invited to input to the WaCha`06.
- Key-note speakers not directly involved in WAVILA's activity will give their opinion and present possible solutions to the challenges.
- Researchers who sent a paper 1 month in advance of the challenge will present their approach to the problems.
- All attendees will have the possibility to take active part in the challenge during the second day, when an open discussion will be held.

Final versions of the accepted papers will be published in the ECRYPT proceedings series from the Otto-von-Guericke University, Magdeburg, Germany.

In order to promote a wider attendance, WaCha will be held right after the ACM Multimedia and Security Workshop 2006 (September 26th and 27th, 2006, Geneva, Switzerland; https://msrcmt.research.microsoft.com/ACM2006/CallForPapers.aspx) in the same venue. Although registration is required to attend WaCha, no registration fee will be charged.

**The two problems touched by WaCha'06 are:**

#### 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 (see for instance the blind Newton sensitivity attack described in *P. Comesana, L. Perez-*

*Freire, F. Perez-Gonzalez, "The Blind Newton sensitivity attack", Proceedings of SPIE, Volume 6072, Security, Steganography, and Watermarking of Multimedia Contents VIII, Edward J. Delp III, Ping Wah Wong, Editors, 60720E (Feb. 15, 2006)*), 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 ?

**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 ?

**Instructions for authors:**
Prospective participants are invited to submit a camera ready paper describing their approach to solve the above problems 1 month in advance of the challenge. Submitted papers must follow the LNCS style and should be between 4 and 15 pages long.
Works accepted for contributions to the WAVILA Challenge will be published in the proceedings event.

Any questions regarding the program should be directed to the programme chairs:
**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)