Call for papers

Third Wavila Challenge, WaCha'07

supported by the European Network of Excellence ECRYPT
June 14th, 2007, Saint Malo (France)
http://wacha07.irisa.fr/

As part of its activity, the Watermarking Virtual Laboratory (WAVILA) of the European Network of Excellence ECRYPT organizes in conjunction with the three day International Workshop on Information Hiding (IH07, June 11st-13th, 2007, St Malo, France; http://ih07.irisa.fr/) a working meeting discussing some of the most important themes in watermarking. Although registration is required to attend WaCha'07, no registration fee will be charged.

Based on the experiences from the third 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*. Beside the participation of guest speakers, participants are invited to submit a contribution to any of the two challenges.

Contributions:

Four types of contributions are foreseen:

1. **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'07.
2. **Key-note speakers** not directly involved in WAVILA's activity will give their opinion and present possible solutions to the challenges.
3. **Researchers who send a paper** 1 month in advance of the challenge may present their approach to the problems.
4. **All attendees** will have the possibility to take active part in the challenge during the day, when an **open discussion** will be held.

Accepted contributions can be published in the workshop proceedings (ECRYPT proceedings series from the Otto-von-Guericke University, Magdeburg, Germany), if the author agrees to the publication.

Challenge 1: "What kind of security does perceptual hashing offer?"

Guest speaker: Kivanc Mihcak (Bogazici University), tutorial talk on perceptual hashing

While the robustness/invariance aspects of perceptual hashing schemes have received significant

attention over the last years, the issue of security has received little attention so far apart from attacks against some popular schemes and a few recent suggestions how to assess security in such schemes (e.g. conditional entropy, unicity distance).

The main goal of this challenge is to provide original contributions in the area of security of perceptual hashing schemes, especially focussing on the following aspects:

- Perceptual hash functions have been proposed mainly for authentication (e.g. integrity checks) and content identification (visual database search, music recognition, content blocking/filtering). Do these (and other) different application scenarios have implications for the security of hash functions, e.g. are attack scenarios different ? Are the requirements with respect to security different ? Is there a universally secure robust hash function for all types of scenarios?

- What is the relation between classical cryptographically strong hash functions and the security of robust hashing? contrasting to classical hash functions there is in most cases a notion of degree of similarity in robust hashing (mostly hamming distance between hash strings) --- do we really need this? which attacks are explicitly enabled by this property? Are there better solutions? Are perceptual hashes cryptographically secure?

- How can we assess/measure/compare the security of existing robust hashing schemes? Is there a tradeoff between robustness, execution speed, and security? Which current schemes are best with respect to security?

Challenge 2: " How to learn secrets in watermarking and steganography?"

Guest speaker 1: Pierre Comon (CNRS), tutorial talk on Blind Source Separation and independent component analysis

Guest speaker 2: Thomas Villmann (University Leipzig), tutorial talk on Machine learning and classification techniques

Beside classical performance measures such as capacity or imperceptibility, the constraint of security is also a fundamental requirement for many watermarking or steganographic techniques. Security based attacks are aimed at gaining knowledge about the secrets of the embedding algorithm. In steganalysis, it consists in finding the embedding algorithm for example or just proving that the content contains an hidden message.

Security analysis of watermarking and steganographic schemes can be achieved either from a theoretical or from a practical way. Theoretical security analysis often uses information theoretic measures such as equivocation or Kullbach-Leibler divergence but they do not give any practical clues on methods to assess the security of real-life schemes.

The objective of this challenge is to present a wide panorama of practical methods that can be used in order to reveal the secrets of watermarking and steganographic techniques.

The challenge will first begin with one tutorial on learning machines such as Support Vector Machines, Blind Source Separation methods, clustering techniques or neural networks.

The participants of this challenge are asked to present a methodology involving secret estimation/detection and a learning process. A special interest will be devoted on presenting the learning method and its possible usage according to different parameters such as the number of observations, the dimension of the observations, the embedding capacity and the embedding distortions.

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 (hence before ~~May, 14th, 2007~~ extended to May, 24th, 2007 !). Submitted papers must follow the LNCS style and should be between 4 and 15 pages long.

Contact:

Submissions and questions should be sent to the following email contact:
wacha07(at)listes(dot)irisa(dot)fr