

1st WAVILA CHALLENGE (WaCha 2005)

Barcelona, Catalonia (Spain), 8-9 June 2005

<http://www.uoc.edu/symposia/wacha05>

Call for Contributions

As part of its activity, the Watermarking Virtual Laboratory (Wavila) of the European Network of Excellence ECRYPT (<http://www.ecrypt.eu.org/index.html>), organizes two working days aiming at discussing some of the hottest themes in watermarking security. These working days 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.
- Four key-note speakers (two for each problem) 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.

All attendees will receive a proceedings volume containing extended abstracts of the talks.

The problems touched by WaCha '05 are:

- **Counterfeiting geometric attacks: is exhaustive search the ultimate solution ?**
- **Efficient and cryptographically secure fingerprinting**

More details are given on the back of this call.

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. For more information about the format of the paper please consult the WaCha web site.

Any questions regarding the program should be directed to the program chairs Fernando Perez-Gonzalez (fperez@tsc.uvigo.es), Mauro Barni (barni@dii.unisi.it) and Stefan Katzenbeisser (katzenbe@in.tum.de).

In order to promote a wider attendance, WaCha will be held right after the 7th Information Hiding Workshop (IH'05, June 6-8, Barcelona <http://www.uoc.edu/symposia/ih05/>). Although registration is required to attend WaCha, no registration fee will be charged.

Important deadlines

Submission of contributions (camera ready paper):

May 6, 2005.

Notification of acceptance:

Within 15 days of submission

Counterfeiting geometric attacks: is exhaustive search the ultimate solution ?

Exhaustive Search (ES) and re-synchronization through Template Matching (TM) are two of the most commonly invoked solutions against geometric attacks, however doubts exist on whether they represent an effective solution to the problem. The former, in fact, dramatically increases the false detection probability, whereas the latter must take into account the probability of synchronization errors. In order to get some insight into the real effectiveness of ES and TM against watermark de-synchronization, the following simple case study can be considered.

Let the host feature sequence \mathbf{f} and the watermarking signal \mathbf{w} be modelled as two i.i.d. Gaussian sequences independent of each other, and let us assume that watermarking is achieved by simply adding a scaled version of \mathbf{w} to \mathbf{f} . In the TM case, a second i.i.d. Gaussian signal (the template) \mathbf{s} is also added to \mathbf{f} , by paying attention to split the available energy between \mathbf{w} and \mathbf{s} . We assume that the attacker cyclically shifts the marked vector by an unknown amount resulting in an attacked sequence \mathbf{r} . According to the ES approach the detector computes the correlation between \mathbf{r} and all the cyclically shifted versions of \mathbf{w} . If at least one of such correlations is above the detection threshold, then the watermark presence is revealed. On its side, a TM detector first exploits the presence of \mathbf{s} within \mathbf{r} in order to re-synchronize \mathbf{w} and \mathbf{r} , then it applies a standard correlation-based detector. It is easy to show that, in this simple scenario, ES outperforms TM. It can also be shown that as the length of \mathbf{f} increases the performance of both methods improve, in that both the false and missed detection probabilities tend to zero.

Despite its simplicity, this simple case study opens up to many interesting investigation directions.

A first question regards the effectiveness of ES detection: apart from complexity issues, is ES the best approach to cope with geometric attacks ? According to the simple case study outlined above the answer seems to be yes, however many important points must be taken into account before giving a final answer: does anything change when a wider class of de-synchronization attacks is allowed? Other approaches to cope with geometric attacks exist, e.g. the use of self-synchronizing – periodic – watermarks, is any of them better than ES ? Does something change when security issues are brought into the picture? In the example above, spread spectrum, 1-bit watermarking is adopted, what about the informed watermarking case?

A second question concerns the possibility of ever defeating geometric attacks. The case study considered above seems to point out that as long as the size of the search space does not increase exponentially, ES (and TM) is an asymptotic-effective solution against de-synchronization. Can this result be demonstrated in a more general set-up? Is it possible to obtain better results by means of informed watermarking? It is not difficult to think about a de-synchronization attack whose dimensionality grows exponentially with the size of the feature sequence, however this may be difficult when perceptual constraints are taken into account. Does such a deadly attack exist ?

Efficient and cryptographically secure fingerprinting

From the early days of watermark research, watermarks were proposed as a tool to track the distribution of digital objects. In this application, each copy of an object receives an individual watermark (fingerprint) that distinguishes it from others. In electronic commerce scenarios this fingerprint may encode information about the buyer of a digital object. It became evident that a robust and secure fingerprinting solution can only be constructed by a combination of watermarking schemes and cryptographic protocols.

Apart of the security properties of watermarking schemes, fingerprinting proposals need to deal at least with two more issues. The first one is related to collusion attacks. Since the marks embedded into the object can be detected by simple comparison of the different copies, such attacks must be prevented. On the other side, buyer security must be prevented in terms of being illegally accused by a dishonest seller. Finally, since identity of the buyer is somehow included in the digital object, buyer anonymity must also be ensured.

During the WaCha we will consider the state-of-the-art in fingerprinting design; both cryptographic and signal-processing aspects will be covered. In particular, WaCha will look into the design of asymmetric (which tries to offer buyer security), and anonymous fingerprinting schemes. In asymmetric fingerprinting scenarios, only the buyer knows the fingerprinted object, whereas anonymous fingerprinting allows the buyer to remain anonymous unless he redistributes the information illegally. Although solutions exist for both problem scenarios, it still remains an open issue to engineer efficient solutions for various media types.