Call for Participation
Signature Verification Competition

On- and Offline Skilled Forgeries
http://sigcomp09.arsforensica.org

10th International Conference on Document Analysis and Recognition (ICDAR2009), July 26-29, 2009, Barcelona, Spain

Background

The Netherlands Forensic Institute, located in The Hague, www.forensicinstitute.nl, is in search for a signature verification system that can be implemented in forensic casework and research. The use of automatic signature verification tools can aid the forensic handwriting experts in drawing their conclusion about the authenticity of a questioned signature, but is not widely accepted nor implemented in most forensic laboratories. In our opinion, we need to bridge the gap between recent technology developments and the implementation of new automated tools in forensic casework. As a first step, the Netherlands Forensic Institute wants to take the lead in comparing different signature verification algorithms systematically for the forensic community, with the objective to establish a benchmark on the performance of such methods.

The objective of this competition is to allow researchers and practitioners from academia and industries to compare their performance in signature verification on a new unpublished forensic-like datasets. Authentic signatures and skilled forgeries were collected while writing on a paper attached to a digitizing tablet. The collected signature data are available in an *on-* and *offline* format. Participants can choose to compete on the *online* data or *offline* data only, or one can choose to *combine* both data.

In forensics, online signature verification is not yet a common type of criminal casework for a forensic expert because questioned signatures and the collected reference (known) signatures are commonly supplied offline. However, it cannot be excluded that forensic experts will receive questioned online signatures in the near future. Systems that combine both on- and offline information could become of interest to the forensic experts, if such systems appear to be helpful in verifying an offline questioned signature to reference signatures collected on a paper attached to a digitizing tablet by a the criminal investigation department. In the competition, it is allowed to use the combined data formats for both the reference and the questioned signature. However, a more forensic-like situation would be to compare a questioned offline signature vs. a combined on-offline reference sample. Therefore, we encourage participants to test their systems on this scenario also.

This competition is not an official certification test because we cannot use real forensic data, but we did attempt to collect our data in a way that is close to real forensic casework. Of course we realize that the performance of systems can vary significantly with how forgeries are provided. Therefore, we offer a larger number of skilled forgeries in the training data compared to the data in the evaluation phase. The training and evaluation phase consist of highly comparable data, collected under similar conditions and digitized with similar image scanners and WACOM Intuos2 tablets, yet the data were collected in different laboratories in different years.

We hope that, with this competition, researchers can identify areas where possible improvements to their algorithms could be made. Next to that, we have the intent to present the results of the competition at international forensic conferences and at other forensic laboratories. For the ICDAR proceedings, we will describe the evaluation data in general terms. For competitors, this publication can be referred to in future publications. We also have the intent to publish results in

an extended article. This publication will include anonymous results from participants. If competitors wish to publish about their results, describing the data distributed in this competition, the draft should be sent in for a four week review by the NFI. For correct wording of the description of the data, we will publish a sample text on the website. The evaluation dataset will be made available to the competitors after the competition.

We invite all researchers and developers in the field of signature verification to register and participate in the ICDAR 2009 signature verification competition for off- and online skilled forgery data.

Participants
Participants of both academia and industry are invited to enter the competition. Organizers of this event will not participate in the competition. Participants can participate anonymous and/or they can choose to be anonymous in publications. Participants can register via the website (http://sigcomp09.arsforensica.org) or email to the organizers and chair, Elisa van den Heuvel (sigcomp09@arsforensica.org) to join the competition.

Training and evaluation process
The objective is to run each signature verification tool on the evaluation signature dataset. The training and evaluation data are collected offline and online. Participants are asked to return similarity scores that are ranked numerically, where a higher score indicates a higher similarity between the questioned signature and the reference signature. Similarity scores should be ranked numerically, where higher indicates a higher similarity between the questioned signature and the reference signature. A second binary score is requested for the decision if the questioned signature is written by the same writer as the reference signature (score 1) or not (score 0).

Submission of executables
Participants are required to submit a software tool that is able to compare one (1) questioned signature against one (1) reference signature and that outputs a similarity score and a decision score. The tool must be made available as a Linux or Windows-win32 command line application (.o /.exe file) or a standalone java J2SE application (.jar file).

The interface of the verification tool (called sigVerify) consists of 4 parameters, separated by spaces.
- The type of data being used (online, offline, or combined)
- The path and filename without extension of the questioned signature
- The path and filename without extension of the reference signature
- The path and filename of the output file

For offline verification:
E.g. *sigVerify offline filename_questioned filename_reference filename_output.txt*
For online verification:
E.g. *sigVerify online filename_questioned filename_reference filename_output.txt*
For combined verification:
E.g. *sigVerify combined filename_questioned filename_reference filename_output.txt*
For offline-combined verification:
E.g. *sigVerify offcombined filename_questioned filename_reference filename_output.txt*

The tool writes a result line in the output file that should have the following format:

questioned signature reference signature similarity score decision score

When the output file already exists, the tool should append the result line to the bottom of the already existing result lines.

The filename of the output file should have the following format:
6 or less characters for the name of the institute and system identifier in cases of more than one system per institute (e.g. myLab1 and myLab2)
2 characters for classifier (on=online, of=offline, co=combined, fo=offline for questioned signature vs. combined for reference signature)
1 character for image resolution (3=300dpi, 6=600dpi)
1 character for tones used in the images (c=24bit rgb-color, g=8bit grayscale, b=binary)

Participants must deliver the verification tool and all software needed to run it in a single ZIP file. This ZIP file must also contain a readme.txt file with all relevant information of installing and running the tool. In addition we ask for a short description of the fundamental approach (2000 words extended attracts) and references to further publications if available.

The executable will not be used for purposes other than the ICDAR2009 competition. Performances will be published in the ICDAR proceedings and in an extended journal publication. After the competition, all executables will be destroyed. If a team chooses to use some expiration mechanism, the expiration should be set to 31 December 2009.

Evaluation of performance
Performance will be evaluated in Detection Error Trade-off (DET) curves containing Equal Error Rates based on the similarity scores. Additional experiments will be conducted for an extended journal publication.

Training and evaluation datasets
The original signature images are scanned at 600dpi and have 24bit RGB-color. We will also provide 600dpi grayscale (8bit) and binary formats, and 300 dpi color, grayscale and binary formats.

The offline training dataset will be constituted of 1905 images, green ink on white paper (true color 24bit data, grayscale and binary data all in 300 dpi and 600 dpi, TIF format). The online training dataset will consist of 1905 ASCII-files with the format: pen tip positions X and Y, pressure Z, pen tilt (0-90 degrees) and azimuth (0-360 degrees)). Sampling rate was 200 Hz. Filenames will reveal the true score.

The offline evaluation dataset will consist of 1953 images, black ink on white paper. The online evaluation dataset will consist of 1953 ASCII-files in the same format as described for the training data with similar sampling rate. A detailed description of the datasets will be provided in README files to the competitors.

In the training and the evaluation phase, signatures can either be authentic: written by a authentic writer, or forged: forgery of a signature of the authentic writer. The training set consists of a small group of authentic writers and a large number of skilled forgeries whereas the evaluation set consists of a large group of authentic writers and a smaller number of skilled forgeries.

Schedule
Training set available: January 16th, 2009
Deadline for submitting verification tool: March 9th, 2009
Presentation of performance at ICDAR 2009 in a special session.

Organizing committee
Linda C. Alewijnse, MSc
Vivian L. Blankers, BSc
Niels H. van Eijck, BSc
C. Elisa van den Heuvel, Ph.D. (Chair)[1]

Netherlands Forensic Institute
P.O. Box 24044
2490 AA The Hague
The Netherlands
T +31 70 888 6308
M +31 6 4142 9310
E e.van.den.heuvel@nfi.minjus.nl

Katrin Franke, Ph.D.
Norwegian Information Security Laboratory
Gjøvik University College,
P.O. Box 191
N-2802 Gjøvik
Norway
T +47 61 135 254
E kyfranke@ieee.org

Louis G. Vuurpijl, Ph.D.
Donders Institute for Brain, Cognition and Behavior
Radboud University Nijmegen
P.O. Box 9104
6500 HE Nijmegen
The Netherlands
T +31 24 361 5981
E l.vuurpijl@donders.ru.nl

Short CV C. Elisa van den Heuvel
Elisa van den Heuvel started in 2005 as scientific forensic handwriting expert in training at Netherlands Forensic Institute. Her scientific background lies primarily in human motor control with special emphasis on handwriting/signature movement execution. In chronology, she received her M.Sc. from Radboud University of Nijmegen in 1996, and her Ph.D. at Vrije Universiteit Amsterdam (VUA) in 2000. During her PhD research she also worked at Motor Control Lab, Arizona State University, Tempe, USA as a visiting research scholar. In 2000, she started as postdoc at Biomechanics at VUA where she studied preclinical symptoms of Parkinson's disease. Since 1997, Elisa van den Heuvel has published several scientific journal articles and peer-reviewed conference articles. She co-presented a Tutorial at ICDAR in 2007 on Computational Forensics. http://www.forensicinstitute.nl

Short CV Katrin Franke
Katrin Franke is associate professor at the Norwegian Information Security laboratory in Gjøvik, Norway. She obtained her Ph.D. degree at the Artificial Intelligence Institute, University of Groningen, The Netherlands in 2005, and her M.Sc. in Electrical Engineering from the Technical University of Dresden in Germany. After graduation in 1994, Mrs. Franke began to conduct research at the Fraunhofer Society in Germany. She focused on digital image processing and pattern recognition. Until December 2006, she has worked as a scientific project manager in charge of founded research and industrial projects on document processing, signature analysis and custom-stamp analysis, applied in banking and in forensics. These projects have brought forth software modules and software systems, now operating in banks in Germany, the United Kingdom, South Africa and Jamaica as well as in forensic laboratories in Germany. In total, Mrs. Franke has published more that 60 scientific journal articles, peer-reviewed conference articles and edited books. She is a member of several international editorial boards, program committees, and initiated the International Workshop on Computational Forensics (IWCF) in 2007. http://kyfranke.com

Short CV Louis G. Vuurpijl
Louis Vuurpijl received his Ph.D. in computer science in 1998 for research on neural networks and parallel processing. He has been involved in various forms of image processing and neural network-based image recognition such as the detection of ground-cover classes in satellite imagery. Louis Vuurpijl has been affiliated with the Donders Institute (former NICI) since 1995, conducting research on pen computing, image retrieval, online handwriting recognition, forensic document analysis, and multimodal interaction. He is an assistant professor and lectures on artificial intelligence, robotics, and cognitive science. Louis Vuurpijl is member of the board of the international Unipen Foundation and is involved in several national and European research projects. http://hwr.nici.kun.nl/~vuurpijl

[1] Please contact the chair Elisa van den Heuvel (sigcomp09@arsforensica.org) if you have any questions or problems concerning the procedure.