Forensic Signature Verification Competition : 4NSigComp2010

12th International Conference on Frontiers in Handwriting Recognition (ICFHR2010),

November 16-18, 2010, Kolkata, India

Background

Forensic signature verification is done by visual comparison by trained Forensic Handwriting Experts (FHEs). The authenticity of the questioned signature is estimated by weighing the particular similarities/differences observed between the features of the questioned signature and the features of several known signatures of a reference writer. Automated signature verification tools can help FHEs in evaluating the probability of the evidence in light of the two research hypotheses under investigation:

Hypothesis 1: The questioned signature is an authentic signature normally used by the reference writer;

Hypothesis 2: The questioned signature is the product of a forgery process.

H2a: ..and is simulated by another writer than the reference writer;

H2b: ..and is disguised by the reference writer;

The FHE weighs the observations in light of two hypotheses H1 vs. H2. The interpretation of the observed similarities/differences in signature analysis is not as straightforward as in other forensic disciplines such as DNA or fingerprint evidence, because signatures are a product of a behavioral process that can be manipulated by the reference writer himself, or by a person other than the reference writer. In signature verification research, a 100% perfect match does not necessarily support Hypothesis 1, because a perfect match can occur if a signature is traced. Also, differences between signatures do not necessarily support Hypothesis 2, because slight changes can be put into a signature image by the reference writer when disguising his signature for the purpose of denial, or can occur due to a within-writer variation.

Because forensic signature verification is performed in a highly subjective manner, the discipline is in need for a scientific, objective base. The use of automatic signature verification tools can objectify the FHEs opinion about the authenticity of a questioned signature. However, to our knowledge, signature verification algorithms are not widely accepted by the FHEs. The objective of this competition is to compare automatic signature verification performances on new unpublished forensic-like datasets to bridge the gap between recent technology developments and the daily casework of the forensic examiner. We consider the opportunity to conduct a performance evaluation of algorithms a basic contribution in establishing the scientific basis for the discipline of forensic signature comparison. The 4NSigComp2010 comprises two scenario’s described below.

The first scenario aims at a comparison between FHEs opinions on authorship of signatures and the systems performances to detect skilled forgeries (simulated and disguised signatures) from genuine signatures of a reference writer. The second scenario aims at performance evaluation of automated systems in a new large dataset that comprises genuine, simulated signatures produced by unskilled imitators or random signatures (genuine signatures from other writers).

Scenario 1: Detection of simulated and disguised signatures

This scenario will be the first to relate system performances to the performance of FHEs who gave their opinion on the authenticity of the signatures. We assume that participants in the competition never had access to the signatures that have been collected by La Trobe University for the purpose of testing the expertise of FHE's. We might ask participants to sign an informed consent that these data and results were indeed unknown before entering the competition and during participation in the competition. Found and Rogers (2005) published FHEs' correct versus incorrect answers regarding the authorship of 799 questioned signatures over 5 years of research (one signature test per year). In total, 29.811 opinions have been collected. Results show that FHEs are significantly more confident in identifying genuine signatures than in identifying disguised signatures or simulated signatures. In this scenario, we have prepared data of several of these signature tests. A questioned signature can either be genuine, written by the writer of the reference signatures, or the signatures can be created by a disguise or simulation process. A disguise process is defined as: an attempt by a writer to purposefully alter his signature in order to avoid being identified or for him to deny writing the signature. A simulation process is defined as: an attempt by the writer to imitate the signature characteristics of a visual or mental model.

Scenario 1: Signatures

The images are scanned at 600dpi color format. The training dataset will consist of 209 images, of which 9 reference and 200 questioned signatures. Filenames will reveal the true score. For example: 001_001_002.bmp refers to writer (001) writing the signature of himself/herself(001), second time (002). In case of a disguise process an example filename will be 001_999_003.bmp: the reference writer (001) disguising his signature to an arbitrary person (999) for the third time (003). In case of a simulation an example filename can be 002_001_005.bmp: writer (002) imitating the signature of writer (001) for the fifth time (005). The evaluation dataset will consist of 125 images, containing 25 reference signatures and 100 questioned signatures.

Scenario 2: Detection of skilled versus non-skilled simulated signatures

The second scenario aims at evaluating the performance of signature verification systems in a security less critical environment. The questioned signatures can either be genuine (written by the reference writer), or forged (simulated by other writers than the reference writer), or a random forgery (genuine signature of other writers).

The signature corpus employed in this competition scenario will be a subset of the GPDS960signature corpus. This database was collected by Grupo de Procesado Digital de Señales, Universidad De Las Palmas De Gran Canaria, Spain. The genuine signatures were taken from 960 individuals. The simulated signatures were produced by unskilled imitators with unrestricted practicing.

Scenario 2: Signatures

The reference set contains signatures of 400 individuals: 4 genuine signatures for each individual. The signature images were scanned at the resolution of 300 dpi and stored in black and white "bmp" format. The genuine signature image files are named xxx\c-xxx-yy.bmp where xxx is the signer number and ranged from 301 to 700 whilst the repetition yy ranged from 01 to 04.

Testing data contains 30000 questioned signature images in "bmp" format named c-xxxxx-yyy.bmp being xxxxx the number of file from 00001 to 30000 and yyy the identity claimed. The test data includes original signatures, random signatures and simulated forgeries of each user. Hereby, random signatures are genuine signatures belonging to a different writer. The simulated forgeries were produced using different static images of the genuine signature. The simulators were allowed to practice imitating signatures for as long as they wish. A similar database named GPDS300signature could be used to test the developed algorithm. Details for the acquisition can be found at http://www.gpds.ulpgc.es/download/index.htm.

After the competition, the database GPDS960signature will be made available to the public under the similar terms and conditions for GPDS300signature database. This database includes the GPDS300signature database, the database employed in this competition plus 260 new set of signatures.

Test and evaluation process

Each signature verification tool is to be run on the reference and question signature sets. The program is asked to return similarity scores that are ranked numerically, where a high score indicates a higher similarity between the questioned and the reference signature.

Evaluation of performance

In scenario 1, performance will be evaluated in Detection Error Tradeoff (DET) curves containing Equal Error Rates based on the similarity scores. In scenario 2, the false rejection rate (FRR), and false acceptance rate (FAR) for random forgeries, and false rejection rate for simulated forgeries will be computed.

System testing and other details

Detailed requirements will be provided to the participants in a README file after signing up for the competition.

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 email Elisa van den Heuvel (e.van.den.heuvel@nfi.minjus.nl) to join the competition. We would like to encourage you to participate in both scenario's if possible.

Schedule for both scenario's

Training set available: April 15, 2010.

Deadline for submitting verification tool: May 14th, 2010.

Presentation of performance at ICFHR 2010.

Contact Address :

Please contact Elisa van den Heuvel (e.van.den.heuvel@nfi.minjus.nl) if you have any questions or problems concerning the procedure.

Competition Organizing committee

Marcus Liwicki, Ph.D., German Research Center for Artificial Intelligence, Kaiserslautern, Germany;

Michael Blumenstein, Ph.D., Griffith University, Queensland, Australia;

Bryan Found, Ph.D., La Trobe University, Melbourne, Australia;

Miguel A. Ferrer, Ph.D., Universidad de Las Palmas de Gran Canaria, Spain;

C. Elisa van den Heuvel, Ph.D., Netherlands Forensic Institute, The Hague, The Netherlands.