ICFHR2012 Competition on Automatic Forensic Signature Verification (4NsigComp 2012)

Marcus Liwicki*, Muhammad Imran Malik*, Linda Alewijnse†, Elisa van den Heuvel†, Bryan Found‡

*German Research Center for AI (DFKI GmbH)
Knowledge Management Department, Kaiserslautern, Germany
{firstname.lastname}@dfki.de
†Netherlands Forensic Institute, The Hague, The Netherlands
lalewijnse@nfi.minvenj.nl, e.van.den.heuvel@nfi.minjus.nl
‡La Trobe University Bundoora Campus, Victoria 3086, Australia
b.found@latrobe.edu.au

Abstract—This paper presents the results of the ICFHR2012 Competition on Automatic Forensic Signature Verification jointly organized by PR-researchers and Forensic Handwriting Examiners (FHEs). The aim is to bridge the gap between recent technological developments and forensic casework. A forensic like training set containing disguised signatures along with skilled forgeries and genuine signatures was provided to the participants. They were motivated to report the results in Likelihood Ratios (LR). This has made the systems even more interesting for application in forensic casework. For evaluation we used both the traditional Equal Error Rate (EER) and forensically substantial Cost of Log Likelihood Ratios ($\hat{C}_{llr}$). The system having the best Minimum Cost of Log Likelihood Ratio ($\hat{C}_{llr}^{min}$) is declared winner. Various experiments both including and excluding disguised signatures from the test set are reported.

Keywords—Disguised signatures, verification, handwriting examiners, evaluation, standard, forensic casework, likelihood ratios

I. INTRODUCTION

The topic of writer identification and verification has been addressed in the literature for several decades [1], [2]. Usually, the task is to identify the writer of a handwritten text or signature or to verify his or her identity. Work in writer verification can be differentiated according to the available data. If only a scanned or a camera captured image of the handwriting is available then writer classification is performed with offline data. Otherwise, if temporal and spatial information about the writing is available, writer classification is performed with online data. Usually, the former task is considered to be less difficult than the offline classification [2]. Surveys covering work in automatic writer identification and signature verification until 1993 are given in [2]. Subsequent works up to 2000 and 2008 are summarized in [3] and [4] respectively. Most approaches are tested on specially collected data sets which were acquired in controlled environments.

In the past, several competitions were organized to measure the detection rate of several classifiers, some are:

- First International Signature Verification Competition (SVC 2004), online data, 100 signature sets: 20 (genuine, forged)/author [5]
- BioSecure Signature Evaluation Campaign 2009, online data from DS2-382, DS3-382 [6]
- SigComp 2009 [7], online and offline data, 1 reference signature (several authors)
- 4NSigComp 2010 [8], offline data, 25 reference signatures (1 author)
- SigComp 2011 [9], online and offline data Chinese and Dutch signatures, 12 reference signatures (several authors)

Most of the current research in the field of signature verification does not take the real needs of Forensic Handwriting Experts (FHEs) into account. In their routine casework they often work with offline signatures produced in uncontrolled real world environments. The most crucial fact is that they also have to deal with the possibility of disguised signatures where an authentic author tries to disguise his or her signature in order to make it seem like a forgery. The disguised signatures differ from genuine signatures in the author's intent when they are written. A genuine signature is written by an author with the intention of being positively identified by some automated system or by an FHE. A disguised signature, on the other hand, is written by the genuine author with the intention of denial, that (s)he has written that particular signature, later. These signatures are more difficult to analyze compared to the signatures produced in controlled environments. In order to investigate these signatures and evaluate the performance of some of the state-of-the-art systems on data containing disguised signatures, we previously organized the 4NsigComp2010 [8]. It was the first signature verification competition focusing explicitly the classification of disguised, simulated/forged and genuine
signatures.

Another very important issue that has arisen quite repeatedly in the recent past is "what should an automatic signature verification system output in order to be useful for FHEs"?

Automatic systems traditionally report a boolean (yes/no) decision or a probability/similarity score. These decisions or similarity scores are inappropriate for presenting in the courts and therefore are not required by FHEs (for more details see [10]).

We have now organized the ICFHR2012 Competition on Automatic Forensic Signature Verification (4NsigComp2012) for detecting skilled forgeries and disguised signatures. The major emphasis of this competition is, therefore, twofold. First, it evaluates the performance of the state-of-the-art systems in classifying disguised, forged, and genuine signatures. Second, it motivates the signature verification community to enable their systems to report the likelihood ratios instead of only reporting the evidence/similarity score/probability. This is important as it allows one to combine the FHE’s evidence (from the results of an automated system) with other evidence presented in a court of law.

In the 4NsigComp2012, we ask to produce a comparison score (e.g. a degree of similarity or difference), and the evidential value of that score, expressed as the ratio of the probabilities of finding that score when the questioned signature is a genuine signature and when it is a forgery (i.e. the likelihood ratio). Note that this competition follows the strategy of the SigComp 2011 [9], i.e., introducing a paradigm shift from the “decision paradigm” to an evidential value that impacts the task in the competition. The issue is not the pure classification, since

- an FHE cannot and was never asked to decide on authorship,
- an FHE cannot know the probability of authorship based on handwriting comparison alone, and
- classification brings with it the probability of an error of which the cost is undefined.

The true issue is to find the likelihood ratio (LR) for a comparison: the probability of finding a particular score given that Hypothesis $H1$ (i.e., the reference author has written this signature) is true, divided by the probability of finding the score when the alternative Hypothesis $H2$ (i.e., the reference author has not written this signature) is true. $H1$ corresponds to intra-source scores (same author) and $H2$ to inter-source scores (different authors).

The relevant graphs therefore show histograms of some measure of similarity (or difference; or any continuous measure that used to be compared to some threshold in a classification task) for intra-source and inter-source comparisons. Such graphs make it possible to assess the value of the evidence given both hypotheses, which is of major importance to forensic experts and the courts. Therefore, in this competition we have had a closer look at the likelihood ratios.

### II. Background

Forensic signature verification is done by visual comparison by trained 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/specimen writer.

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 writer. In signature verification research, a 100% perfect match does not necessarily support $H1$, because a perfect match can occur if a signature is traced. Also, differences between signatures do not necessarily support $H2$, because slight changes can occur due to a within-writer variation.

Since forensic signature verification is performed in a highly subjective manner, the discipline is in need for scientific, objective methods. The use of automatic signature verification tools can objectify the FHE’s opinion about the authenticity of a questioned signature. However, to our knowledge, signature verification algorithms are not widely used by the FHEs. The objective of this competition is to compare automatic signature verification performances on new, unpublished, forensically relevant datasets to bridge the gap between recent technological developments and the daily casework of FHEs.

### III. Data Description

The data contain only offline signature samples. The signatures were collected under supervision of Bryan Found and Doug Rogers in the years 2001, 2002, 2004, 2005 and 2006, respectively. The images were scanned at 300dpi resolution and cropped at the Netherlands Forensic Institute for the purpose of this competition.
A. Training Set

The training set comprised training and test set of the 4NsigComp2010, i.e., a previous competition of this series. In all it has data from two specimen writers/authors A and B, respectively. There are 9 reference signatures from writer A and 200 questioned signatures. From these 200 questioned signatures, 76 are genuine, 104 simulated/forged, and 20 disguised signatures. There are 25 reference signatures from writer B and 100 questioned signatures. From these 100 questioned signatures, 3 are genuine, 90 simulated/forged, and 7 disguised signatures. For further details refer to [8].

B. Test Set

For the test set signature samples were provided by the Forensic Expertise Profiling Laboratory (FEPL) of La Trobe University. It contained signature samples from three specimen writers/authors, 'A1', 'A2', and 'A3' respectively. The questioned samples were a mixture of genuine signatures, disguised signatures and skilled forgeries as given in tables I and II. All signatures were written using the same make of ball-point pen and the same make of paper. The questioned samples were numbered randomly, scanned and inkjet or laser printed into a booklet.

Test Set Acquisition Details: For specimen author 'A1', 3 normal signatures per day (written with a ball point pen) over a fifteen day period, 6 disguised signatures per day (written with a ball point pen) over a fifteen day period, and 6 normal signatures per day (written with a pencil) over a three day period were collected. From normal signatures pool the genuine and reference signatures for specimen author 'A1' were drawn.

For forging the signatures of specimen author 'A1', two 'forgers' were selected from the academic staff at La Trobe University. Each of the forgers was provided with 6 normal samples of the questioned signature written by 'A1'. Forgers were instructed that they could use any or all of the supplied specimen signatures as models for their forgeries. Forgers were also instructed that their forgeries must be unassisted (not tracings). Each forger was asked to complete the following task each day over a 10 day period.

- 25 practice signatures (ball point pen)
- 5 forgeries (ball point pen)
- 5 forgeries (pencil)

The forgeries, other than the practice attempts, were used as a pool from which the questioned forged signatures were selected.

For specimen author 'A2' and 'A3', the normal and disguised signatures were written over a 10 and 15 days period respectively. From normal signatures pool the genuine and reference signatures were drawn for these specimen authors.

For forging the signatures of specimen author 'A2', 31 adult 'forgers' contributed. These individuals were volunteers drawn from a single private company. Each of the forgers was provided with 3 original normal samples of the signature written by the specimen writer. These forgers were instructed similar to the forgers of 'A1', mentioned above.

For forging the signatures of 'A3', 6 adult 'forgers' contributed. These individuals were volunteers. Each of the forgers was provided with 3 original normal samples of the signature written by the specimen writer. These forgers were also instructed as above.

IV. Submitted Systems

In total, we received five systems from five different institutions for this competition. In the following we will list these systems and their brief descriptions, if we are provided with. Participants were allowed to be anonymous upon request.

A. Griffith University

This signature verification system employs the Gaussian Grid feature extraction technique [11] developed by the Blumenstein Lab at the School of (ICT) and the Institute for Integrated and Intelligent Systems (IIS), Griffith University in Australia. For completeness some details are included here, for further details refer to [11]. The Gaussian Grid feature extraction technique employs signature contours as its input. The following steps are performed. First, the input signature contour image is divided into \( m \times n \) zones. Then by tracing the contours in each block the 4-direction chain code histogram of each block is created. Every step from a pixel to its adjacent one of the four directions (horizontal, vertical, left-diagonal, and right-diagonal) are counted. There are four matrices of size \( m \times n \) for each direction, namely \( H \), \( V \), \( L \), and \( R \). After that Gaussian smoothing filter is applied and the value of each element of each matrix obtained is adjusted by dividing its value by the maximum value of the four matrices. Further from the two-matrix pairs horizontal (H) and vertical (V) matrices,
left-diagonal (L) and right-diagonal (R) matrices, two new matrices are established. Eventually the feature vector is formed by merging the six matrices. The common set of parameters for the Support Vector Machines (SVMs) were determined during the authors’ research using the GPDS-160 [12] signature corpus and had been reported in an ICDAR 2011 publication [11]. The SVM software employed was Libsvm [13]. This system is given the ID 1 in our experiments.

B. Qatar University

The proposed method combines through a logistic regression classifier hundreds of geometrical features that were made available in Arabic writer identification contest ICDAR2011 [14]. These features are based on number of holes, moments, projections, distributions, position of barycenter, number of branches in the skeleton, Fourier descriptors, tortuosities, directions, curvatures and chain codes. For more details about these features refer to [14]. Calibration is done using the s_cal method which gave the best results for the training set. This system is given the ID 2 in our experiments.

C. Sabanci University

In this system the input signature is first processed to remove outlier pixels to deal with flourishes that significantly degrade registration and to thin the signature to deal with pen thickness variations. We then extract two complementary features from each signature: Histogram of oriented gradients (HOG) and local binary patterns (LBP). For classification, we use Support Vector Machines (SVMs) in two different ways: User based SVMs (USVM) and a global SVM (GSVM). The USVMs are trained online with the given references of a user as positive examples and additional random forgeries as negative examples. The GSVM is trained offline using a private database, to discriminate between acceptable variations occurring in genuine signatures and those occurring in forgeries. For this, difference vectors that occur between a genuine signature and its corresponding references are given as positive examples, while the difference vectors that occur between a forgery and its claimed references are given as negative examples.

For the GSVM, we align the query signature to each of the references first, before computing the difference vectors. Furthermore, we only use the HOG features that are found to be more successful, for simplicity. The system finally computes a weighted average of the scores returned from the 3 classifiers (2 user-dependent USVMs using HOG or LBP features and one user-independent GSVM using HOG features), using weights that are learnt from a validation set. We have found that while USVMs are more successful in general, the GSVM contributes positively in the classifier combination (see [15]). This system is given the ID 3 in our experiments.

D. Anonymous System I

This participant decided to remain anonymous however provided us the following details. Given a scanned image as an input, first binarization, and then normalization with respect to skew, writing width and baseline location are performed. To extract the feature vectors from the normalized images, a sliding window approach is used. The width of the window is varied from one to three pixel and following geometrical features are computed at each window position, the mean pixel gray value, the centroid, vertical and horizontal second order moments, the locations of the uppermost, and lowermost black pixel and their positions and gradients with respect to the neighboring windows, the black to white transitions present within the entire window, the number of black-white transitions between the uppermost and lowermost pixel in an image column, and the proportion of black pixels to the number of pixels between uppermost and lowermost pixels are used. These features are already proposed in [16]. For classification various classifiers were employed and the best result were obtained by Gaussian Mixture Models. This system is given the ID 4 in our experiments.

E. Anonymous System II

This participant also decided to remain anonymous however provided us the following details. This system is based on the methods introduced in [17]. First, the signature image is spatially smoothed followed by binarization via combinations of local and global binarization techniques. After that the signature image is located and centralized via center of gravity and then divided into 64 cells. Then various features are extracted from each cell including, size of cell, it’s center point, centroid, angle of inclinations each black pixel makes with the corners of the corresponding cell, Note
that the approach divides the signature into 64 small parts, which can be seen as a local feature extraction technique. However, since this division is based on a global analysis and the number of extracted features is fixed, disregarding the length of the signature, this approach is considered as a global approach. After computing these feature vectors, thresholds are computed using means and variances. Following that, nearest neighbor approach is applied to decide on the result of each feature vector and finally a voting based classification based on different voting strategies is made. This system is given the ID 5 in our experiments.

V. EXPERIMENTS AND EVALUATION

As stated earlier, the basic aim of the 4NsigComp2012 is to gauge the performance and applicability of some of the state-of-the-art signature verification systems in real forensic casework. For this purpose, we included disguised signatures in the dataset and motivated the participants to report the score of similarity/difference along with the evidential value of that score, i.e., the likelihood ratio. Note that since the disguised signatures are from genuine author, where (s)he has tried to imitate a forgery, therefore if we are to establish authorship the disguised signatures must lay in the positive authorship category.

We evaluated the systems according to several measurements. First, we generated ROC-curves to see at which point the equal error rate is reached, i.e., the point were the false acceptance rate (FAR) equals the false rejection rate (FRR). At this specific point we also measured the accuracy, i.e., the percentage of correct decisions with respect to all questioned signatures. Next, we measured the cost of the log-likelihood ratios $\hat{C}_{llr}$ (see [18]) using the FoCal toolkit, and finally, the minimal possible value of $\hat{C}_{llr}$, i.e., $\hat{C}_{llr}^{\text{min}}$ as a final assessment value. Note that the $\hat{C}_{llr}^{\text{min}}$ always between 0 and 1, and a smaller value of $\hat{C}_{llr}^{\text{min}}$ denotes a better performance of the method.

We performed various experiments on the complete test set as well as on each authentic author individually. We report all these results in this paper, however, the winner is the system that performed best on the complete test set, i.e., Griffith University: system ID 1.

The experiments were divided into two evaluation categories. The Evaluation 1 for all the experiments considered genuine, forged and disguised signatures. The Evaluation 2 for all the experiments considered only genuine and forged signatures. The disguised signatures were removed from the test set for Evaluation 2 in all the experiments. We also performed the same two evaluations on each reference author individually. Table III shows the results where we tested all the system on the complete test set including disguised signatures. This was the actual metric for comparing system performance as described to the participants already. Here system 1 outperforms all the other systems both on accuracy and FRR/FAR as well as on $\hat{C}_{llr}^{\text{min}}$ scale.

When we removed the disguised signatures from the test set and performed Evaluation 2, given in Table IV, system 3 performed better on the accuracy and FRR/FAR, still system 1 performed best on the $\hat{C}_{llr}^{\text{min}}$ scale. Note that this is an example where a system performing better on FRR/FAR may not perform better on $\hat{C}_{llr}^{\text{min}}$. Later we performed the same experiments for each authentic author individually. Tables V, VI, VII, VIII, IX, and X detail these results. Note that different systems performed better for different authors individually. System 1 performed better for author 1, system 3 performed better for author 2, and system 2 performed better for author 3. Still on the complete dataset system 1 was the winner, this can be explained by difference in the sizes of the data from three authors. Author 1 has the largest data, which impact the overall results.

The results also show that the grid-based features which actually focus on many small regions of the signature seem to be the most efficient features for this dataset. However, we can also observe that the effectiveness of the features vary from one writer to another, i.e., the global geometric descriptors by System ID 2 work better for author A3. Thus it is hard to draw some general conclusions of these results. Note that System 5 also uses features from many small regions, however, instead of using a static grid it applies a more sophisticated method, which finally works worse on this data set.

VI. SUMMARY

In this paper we presented the results of the 4NsigComp2012. Note that it is a continuation of a previous signature verification competition, i.e., 4NsigComp2010. In the current competition we used a significantly larger dataset\(^1\) as in 4NsigComp2010. The focus of current com-

\(^1\)The dataset of the 4NsigComp2012 is also made publicly available at http://www.iapr-tc11.org/mediawiki/index.php/Datasets_List.
petition was not only to evaluate some of the state-of-the-art signature verification systems on forensically relevant data containing disguised signatures but also to motivate PR-researchers to produce evidential values of their systems’ scores. It is a high time for this movement since by considering real forensic data and reporting results the way forensic handwriting examiners demand will enable vast application possibilities for automatic verification systems in forensic casework.

In future we plan to make the dataset even more larger and diverse. We also plan to include signature samples written in different languages and yet analyze the systems capability to classify disguised, genuine, and forged signatures at the same time. Another important aspect is the applicability of the overall systems to real forensic cases, which motivate us to evaluate the usability as well.

REFERENCES


