Analysis of Intra-Person Variability of Features for Off-line Signature Verification

BENCE KOVARI, HASSAN CHARAF
Department of Automation and Applied Informatics
Budapest University of Technology and Economics
1111. Budapest, Magyar Tudosok Korutja 2, Q
HUNGARY
bence.kovari@aut.bme.hu http://www.aut.bme.hu/signature

Abstract: - One of the major challenges in off-line signature verification is the fact that a person's own signature is influenced by a number of external and internal factors. This influence results in a high variability even between signatures written by the same signer. This paper proposes a method which is able to model the intra-person variability of a signature feature and also to identify and eliminate the effects of external factors. To demonstrate the efficiency of the algorithm, a sample signature verifier is constructed and evaluated on the Signature Verification Competition 2004 database. Experiments have shown that by using 3 features (endings, loops and skew vectors) an average error rate of 12% can be achieved by the system. These results may be further improved by increasing the number of features, used during the comparison of signatures.

Key-Words: - signature verification; off-line; classification, normal distribution

1 Introduction

In the past century several studies [1][2][3][4][5] have confirmed that signatures can be used with a high success rates for biometrical identification. There are several methodological guides like [6] which formalize the process of verification. However, as all human experts, even opinions of forensic document examiners (FDE's) are subjective and prone to human errors. Also considering the huge numbers of signed documents created each day, and the limited number of FDE's it is obvious why automated signature verification has been in a focus of researchers for the past few decades.

Computer based signature verification can be divided into two main approaches, the on-line and the off-line approach. In online signature recognition the whole process of signing is captured using some kind of acquisition device (camera, digital tablet etc.), then analyzed and used to make a decision. The aim of off-line signature verification is to decide, whether a signature originates from a given signer merely based on the scanned image of the signature and a few images of the original signatures of the signer. Unlike on-line signature verification, which requires special acquisition hardware and setup, off-line signature verification can be performed independently from the normal signing process, and is thereby less intrusive and more user friendly. On the other hand, important information like velocity, pressure and the difference between up- and down strokes is partially lost.

When evaluating verification approaches we also have to differentiate between them based on the signature database used and the way it was used. A typical signature database is a collection of signatures from several signers, containing some (10-20) original signatures from a given signer and usually also containing several forged signatures (forgeries) for the same signer. We focus on the scenario, where verification systems are trained only using original signatures and tested against both original signatures and skilled forgeries and the verification is performed off-line, as this approach suits the most real world scenarios.

The performance of signature recognition systems is usually measured in terms of equal error rate (EER), which is the point where Type I and Type II errors are equal. One also has to take into consideration, that (although usually created on a lower level) signatures are the results of conscious behavior and can thereby be influenced by a huge amount of factors [1]. In the lack of a common signature corpus and a well defined evaluation methodology, the results of different studies may only be hardly comparable; therefore, the values mentioned later should be only taken as approximations. As of today, when tested against skilled forgeries, even the best off-line verification systems deliver worse or equal error rates than 5-10% [7] [8], in contrast with a human expert, who is able to do the distinction with an error rate of 1% [8].

In the past decade a bunch of solutions (like [9] or [10]) have been introduced, to overcome the limitations of off-line signature verification and to compensate for the loss of accuracy compared to on-line systems. To break the 5% barrier it is essential to identify, understand and compensate for the different sources of error in the algorithms. This paper presents a solution to address the problem of improvement and thereby possibly break the 5% barrier.

This paper concentrates on the final phase of signature verification. In the following section several existing signature verifiers are introduced, with a special emphasis on classification. Then we summarize the classification problems, occurring when dealing with signatures, and propose solutions for them. In the second part of this paper a complete statistical approach is introduced to address the previously identified problems and to give a formal algorithm for signature verification. One of the implications of the introduced model is that we are now able to evaluate and quantify the quality of an original sample signature. Finally experimental results are presented and used to evaluate the effectiveness of our approach.

2 Related work

Typically signature verifiers take advantage of different general properties (global features) of the signature and use them as an input for different simple classifiers [11],[12],[13],[14],[15]. In [16] a more complex approach can be seen, by creating a two-stage neural network classifier. Different groups of features are defined and separate MLP (multilayer perceptron) classifiers are applied to them. These MLPs are relatively simple, containing only one hidden layer. Learning is not done through backpropagation, but through the ALOPEX algorithm, which allows the network not to get "stuck" in local minima or maxima of the response function. The MLPs have a relative wide range of input parameters, in order: 16, 96, and 48 variables. The inputs of the first network are the global features of the signature. The second takes a simplified representation of the signature as an input, by creating a 12*8 grid and measuring the intensity values in each grid cell. The third network processes texture information. The output layer contains a single neutron, delivering a response value between 0 and 1 representing the similarity between the actually measured signature, and the training set. These output values are then processed by an RBF to make the final decision.

A similar approach is taken in [17]. They use global features (height-width proportion, middle point, corner points, etc.), and grid features as inputs. Tests are performed both by using simple MLP classifiers and by using SVMs. SVMs were tested with kernels with linear, polynomial, and radial basis function. The latter seemed to deliver the best results with an average error rate of 7-8% compared to the 16-22% error rates measured when using MLPs.

Another interesting approach can be found in [18]. It utilizes CGS vectors (originally developed for character recognition) to extract global features. The main idea here is, to assign a 1024 bit long binary vector to each image and compare these vectors in the later phases. Images are divided into 4x8=32 segments, and information (like concavity, gradient, structural properties) is encoded into the vector for each segment

These vectors are then compared by several algorithms operating with vector distances. In this scenario, the SVM based solution performs poorly, with an average error rate of 46% while a Naïve Bayes classifier achieved error rates between 20% and 25%

3 Feature extraction

3.1 Preconditions

In the following sections we are going to use a generalized model of signature verifiers (Fig. 1.) as introduced in our previous works [19] [20] [7].

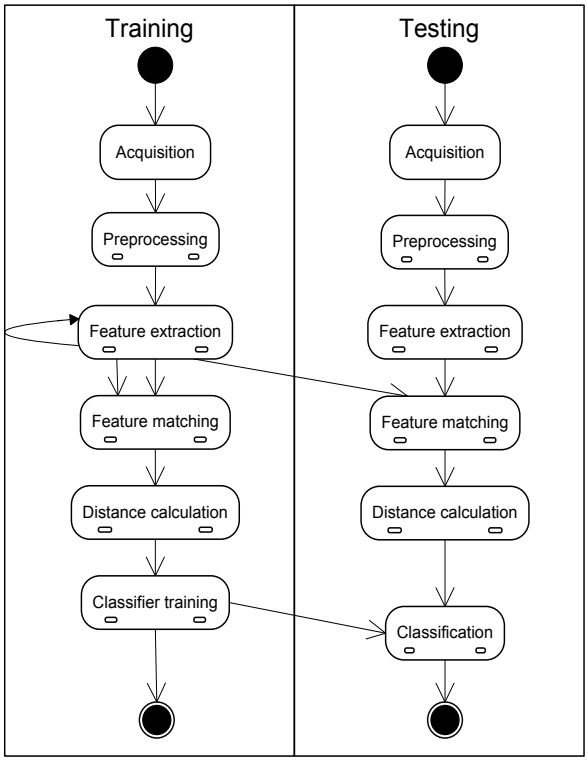

Fig. 1
General architecture of signature verifiers

The aim of off-line signature verification is to decide whether a given signature belongs to a given person. The decision must only be based on *n* samples (original signatures) from the signer. In the followings, we are going to give estimation about the confidence of the above decision.

As it can be seen on Figure 1, signatures undergo several steps till the final decision. Our *n* signatures are usually provided on paper, which must be scanned and noise filtered. After the acquisition and preprocessing phases, several features are extracted. Features are quantitative descriptors of different aspects of the

signature (loop height, pitch, etc.). After that, corresponding features (for example "the height of the first loop") are assigned to each other. It may be possible that some of these features are not existent in all of the samples (for example, several signatures may have a missing first loop). In the followings, only fully matched features are considered. The number of fully matched features is *f*. At this point the two main aspects of a signature verification (number of signatures – *n*, and number of features – *f*) are defined. In the following section we are going to estimate how these two variables influence the confidence level of our final decision.

3.2 Sample features

In the following three subsections we are going to introduce three important features, used in our later experiments.

3.2.1 Skew

The skew information consists of a set of straight lines (skew vectors), where each line represents an imaginary foundation of a component, which can be regarded as an autonomous element of the signature. This definition also allows us to assign skew information to the gaps between signature elements, and according to [1] those spaces are just as peculiar as any other feature of a signature. The following parameters were used to describe a skew vector: start position, end position, length, angle, so the total number of parameters is 6.

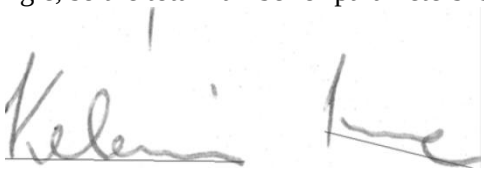

Fig.2. Skew vectors obtained by our algorithm

3.2.2 Loop

Loops in our interpretation are connected regions in the image which are fully enclosed by "signature" pixels.

This definition implies the following 3 important properties:

First: pixels should be unambiguously classified as some belonging to the background ("paper" pixels) or belonging to the signature ("signature" pixels). This is currently done by testing the color components of a pixel against some thresholds.

Second: The region must be connected. Although it sounds logical at the first glance, this is against the traditional definition of a loop, which can be interrupted by other lines. This simplification however allows us a much faster processing of the image.

Third: using fully enclosed regions showed to be an unrealistic target. Because of errors of the pen, and sometimes because of errors of the scanning process, there are often 1-2 pixel wide interrupts in the pen strokes, which would break our definition of loops. To eliminate them, a morphological closing is applied to each image before loop extraction.

Shape descriptors are used to describe the different aspects of loops, thereby allowing an easy comparison. There are several promising formulas described in the literature for calculating shape descriptor values. Instead of choosing one of them, we used as many of them as possible. This will allow us to identify the most significant shape factors in later phases.

The following shape descriptors were used during feature extraction: Perimeter, area, formfactor, maximum diameter, maximum diameter angle, roundness, centroid, bounding box, inscribed diameter, extent, modification ratio, compactness, bounding circle, moment axis angle, convexity, solidity, aspect ratio. A detailed introduction of shape descriptors can be found in [21]. Also note that several definitions for the area of a loop can be obtained, depending on how the bounding pixels of a loop are included in the calculations. Therefore, several shape descriptors which include the area in their calculations are calculated in three different ways, therefore the total number of parameters is 29.

3.2.3 Ending

Endings are the first and the last segments of a stroke. The shape, the length, direction, position and intensity of an ending can be very characteristic for a given signer. In our current setup we used the location of the last pixel as the starting position of an ending, and located consecutively the 10^{th} pixel in the skeleton, the 20^{th} pixel in the skeleton and the first joint in the skeleton. The length and angles of these three vectors provided the main parameters used to characterize the endings providing altogether 12 parameters.

Fig.3. Characteristic vectors for endings

3.3 Statistical interpretation of feature values

A feature (like the height of a given loop) can be seen as a random variable ξ. Although its value may vary from signature to signature, it is safe to assume that the signer is aiming to reproduce his own signature as accurately as possible, while the current result is influenced by a large

number of different factors. Because of these we assume that ξ has a normal distribution with mean m and variance σ_o^2.

$$\xi=N(m_o,\sigma_o) \quad (1)$$

Similarly, the values of forged features can also be represented by a random variable with a normal distribution.

$$\eta=N(m_f,\sigma_f) \quad (2)$$

In addition, because the forger is aiming to forge the original signature, the means of these distributions overlap.

$$M(\eta)=M(\xi) = m_f =m_o=m \quad (3)$$

To distinguish between original and forged signature a threshold must be chosen. Each feature value which falls int the interval $[m-w*\sigma_o;m-w*\sigma_o]$ is seen as original, and each feature value which does not fall into the interval is seen as a forged one. This definition also introduces type I and type II errors (these are usually called false acceptance rate – FAR and false rejection rate – FRR in the field, which can be calculated based on (1), (2), (3) and *w* (see Fig. 4. and Fig 5.).

$$\sigma_f = q\sigma_o \quad (4)$$

$$FAR = P(m - w\sigma_o < \eta < m + w\sigma_o) = 2\Phi\left(\frac{w}{q}\right) - 1 \quad (5)$$

$$FRR = P(m - w\sigma_o > \xi) + P(m + w\sigma_o < \xi) = 2 - 2\Phi(w) \quad (6)$$

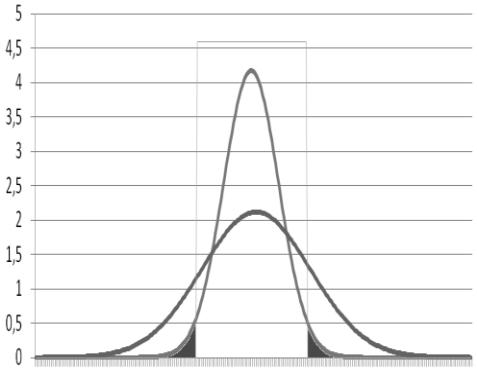

Fig.4
False Rejection Rate

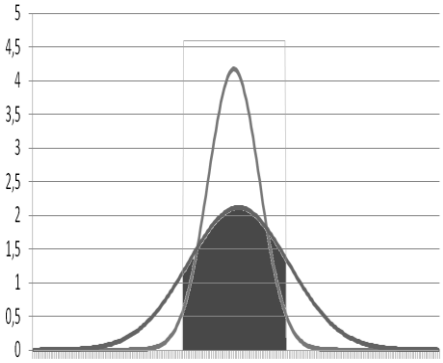

Fig. 5
False Acceptance Rate

The above equations reflect only a theoretical scenario, where both mean and variance are known. In a real world scenario, we only have a (very) limited number of measurements. Therefore the above calculations should be refined for sample mean

$$\hat{m}_n = \hat{m}_n(\xi) = \frac{1}{n}\sum_{i=1}^{n}\xi_i \quad (7)$$

and the sample variance

$$\hat{s}_n^2 = \frac{n}{n-1}\hat{\sigma}_n^2 = \frac{1}{n-1}\sum_{i=1}^{n}(\xi_i - \hat{m}_n) \quad (8)$$

Combining (5), (7) and (9), the probability of a feature value (ξ_{n+1}) falling into a given interval can be calculated as follows.

$$\hat{m}_n - T_a s_n\sqrt{1+\frac{1}{n}} < \xi_{n+1} < \hat{m}_n + T_a s_n\sqrt{1+\frac{1}{n}} \quad (9)$$

The calculation of FAR and FRR should be refined according to (9).

3.4 Multiple features

The above calculations show the accuracy of a signature verification system, which is based on a single feature. However, in real world scenarios we are able to take usage of several different features. Assuming that a signature is represented by *f* independent and normally distributed features, the final decision can be modeled with Bayesian inference.

Let $\Theta = \{\theta_o, \theta_f\}$ denote the originality of a signature, where θ_f denotes the event when the signature is forged and θ_o denotes the event when a signature is original. We have no a priori knowledge about the sample signature, therefore the priori probalbilities of the events are taken as equal $P(\theta_o)= P(\theta_f)=0,5$. In the case of a single feature

and a single observation where x=1 (forgery), the probability that the signature is really a forgery can be calculated as follows:

$P(\theta_o) = P(\theta_f) = 0{,}5$ (10)
$P(x=1|\theta_f) = 1-FAR$
$P(x=1|\theta_o) = FRR$

$$P(\theta_f|x=1) = \frac{P(\theta_f)P(x=1|\theta_f)}{\sum_{j=1}^{2} P(\theta_j)P(x=1|\theta_j)} = \frac{P(\theta_f)P(x=1|\theta_f)}{P(\theta_f)P(x=1|\theta_f) + P(\theta_o)P(x=1|\theta_o)} = \frac{P(x=1|\theta_f)}{P(x=1|\theta_f) + P(x=1|\theta_o)} = \frac{1-FAR}{1-FAR+FRR}$$

$$P(\theta_o|x=1) = \frac{FRR}{1-FAR+FRR} \quad (10)$$

This can be generalized for independent *f* features by using the binomial distribution.

$$P_B(k|\theta_j) = \binom{f}{k} p_j^k (1-p_j)^{f-k} \quad (11)$$

and the Bayesian inference

$$P(\theta_j|k) = \frac{P(\theta_j)P(k|\theta_j)}{\sum_{j=1}^{J} P(\theta_j)P(k|\theta_j)} = \frac{P_B(k|\theta_j)}{\sum_{j=1}^{J} P_B(k|\theta_j)} \quad (12)$$

This means, that given *f* features, and *k* observations where the signature seems to be forged, the probability, that the signature itself is forged is:

$$P(\theta_f|k) = \frac{\binom{f}{k}(1-FAR)^k(FAR)^{f-k}}{\binom{f}{k}(1-FAR)^k(FAR)^{f-k} + \binom{f}{k}(FRR)^k(1-FRR)^{f-k}} = \frac{(1-FAR)^k(FAR)^{f-k}}{(1-FAR)^k(FAR)^{f-k} + (FRR)^k(1-FRR)^{f-k}} \quad (13)$$

Similarly, the probability, that the signature is original is:

$$P(\theta_o|k) = \frac{(FRR)^k(1-FRR)^{f-k}}{(1-FAR)^k(FAR)^{f-k} + (FRR)^k(1-FRR)^{f-k}} \quad (14)$$

To estimate the total probability of error, the above probabilities should be summed for all possible values of *k*:

$$FRR_{total} = \sum_{k=0}^{f}\left(P(\theta_o|k)\right)\left(\binom{f}{k}(1-FAR)^k(FAR)^{f-k}\right) = \sum_{k=0}^{f}\left(\frac{(FRR)^k(1-FRR)^{f-k}}{(1-FAR)^k(FAR)^{f-k} + (FRR)^k(1-FRR)^{f-k}}\right)\left(\binom{f}{k}(1-FAR)^k(FAR)^{f-k}\right) = \sum_{k=0}^{f}\binom{f}{k}\frac{(FRR)^k(1-FRR)^{f-k}(1-FAR)^k(FAR)^{f-}}{(1-FAR)^k(FAR)^{f-k} + (FRR)^k(1-FRR)^{f-}} \quad (15)$$

We could do the same for FAR_{total}, however, because we minimized both errors by using Bayesian inference it would yield the same results.

$$FRR_{total} = FAR_{total} = EER \quad (16)$$

At this point, we are able to predict the accuracy of a system only based on 4 parameters n, f, q and w.

4 Validation

In our experiments the database of the Signature Verification Competition 2004 [8] was used. This is an on-line signature database therefore it contains the stroke information, but no images are provided. The stroke information was used to synthesize signatures similar to the original ones (Figure 7). Stroke points were connected with straight lines, fading out on the line borders. Bicubic interpolation and anti-aliasing were used to make the final image smoother. An example of reproduced signature can be seen on Fig. 1. 1600 signatures from 40 signers (20 originals and 20 forgeries from each) ensure a sample large enough for testing our feature extraction and classification algorithms.

The experimental setup uses 10 original signatures from each signer and a set of generated forgeries for training. Afterwards the classifier is tested with 10 other original and 10 forged signatures. Three different features (endings, skew and loops) are used as features, which resulted in about 5-10 independent features in each signature. Although some of them may seem quiet intuitive, their exact definition and extraction is well defined in our previous works [19].

The resulting average error rates are summarized in table 1. It can be seen, that the values vary largely between different signers. It is however really promising, that this error rate is under 10% at two of the signers.

Although a lot of testing is still in progress, our preliminary measurements and simulations confirm our previous theories.

5 Implications

In the following section we are going to analyze the different implications of the previously introduced statistical model. First, we show how the choice of the acceptance threshold (w) affects the final error rates in a typical verification scenario, then we look for alternatives to improve these results.

5.1 Optimal threshold choice

One of the questions arising is the optimal choice of parameter w. This parameter defines the threshold for the acceptance or rejection of a given feature. To model this, we took a typical verification scenario where the number of original samples (n) is 10 and the number of extracted and matched features (f) is also 10. The results can be seen on Figure 6.

There are several important aspects of this figure. First, when the quality of the forgery is exactly the same as the quality of the original signature (q=1), there is no way to distinguish original signatures from forgeries, therefore the error rates will equal 0.5, which means there is only an 50% chance of a good decision, provided that the chances of a given sample being forged or being original are equal. We should ignore the results where q<1, because these may only be achieved by a forger who can reproduce the signatures better than the original writer. Such a forger cannot be identified with these algorithms. For us, the important part of the graph is where q>1. Obviously, as the value of w raises above a given level, or falls below a given level, the accuracy of the classification decreases. However there is an important range, where 2.4<w<3.0. In this range the equal error rate (EER) is near its minimal achievable level, and this is almost unaffected by the actual value of q (quality of forgeries).

Another conclusion which can be drawn from Figure 6 is that the error rate only drops below 10% (EER<0.1), when the quality of the forgeries becomes worse than 2.0 (q>2.0). Our benchmarks showed, that is near the average forgery quality, therefore, to achieve significantly better error rates than 10%, either the number of original samples or the number of processed features must be increased.

Signer	FAR	FRR
2	16,17%	14,92%
4	19,39%	7,48%
6	12,51%	12,43%
8	3,80%	8,42%
10	20,08%	7,96%
13	16,44%	10,07%
15	10,37%	15,51%
18	3,33%	10,31%
20	11,96%	8,25%
22	17,94%	10,34%
24	8,84%	13,29%
25	30,48%	6,74%
28	12,99%	13,29%
32	16,76%	16,26%
33	18,08%	12,89%
34	14,23%	9,74%
35	6,70%	8,09%
37	1,54%	17,49%
38	13,27%	4,73%
40	6,15%	18,51%
TOTAL	**13,05%**	**11,34%**

Table 1.
Error rates achieved by the statistics based classifier

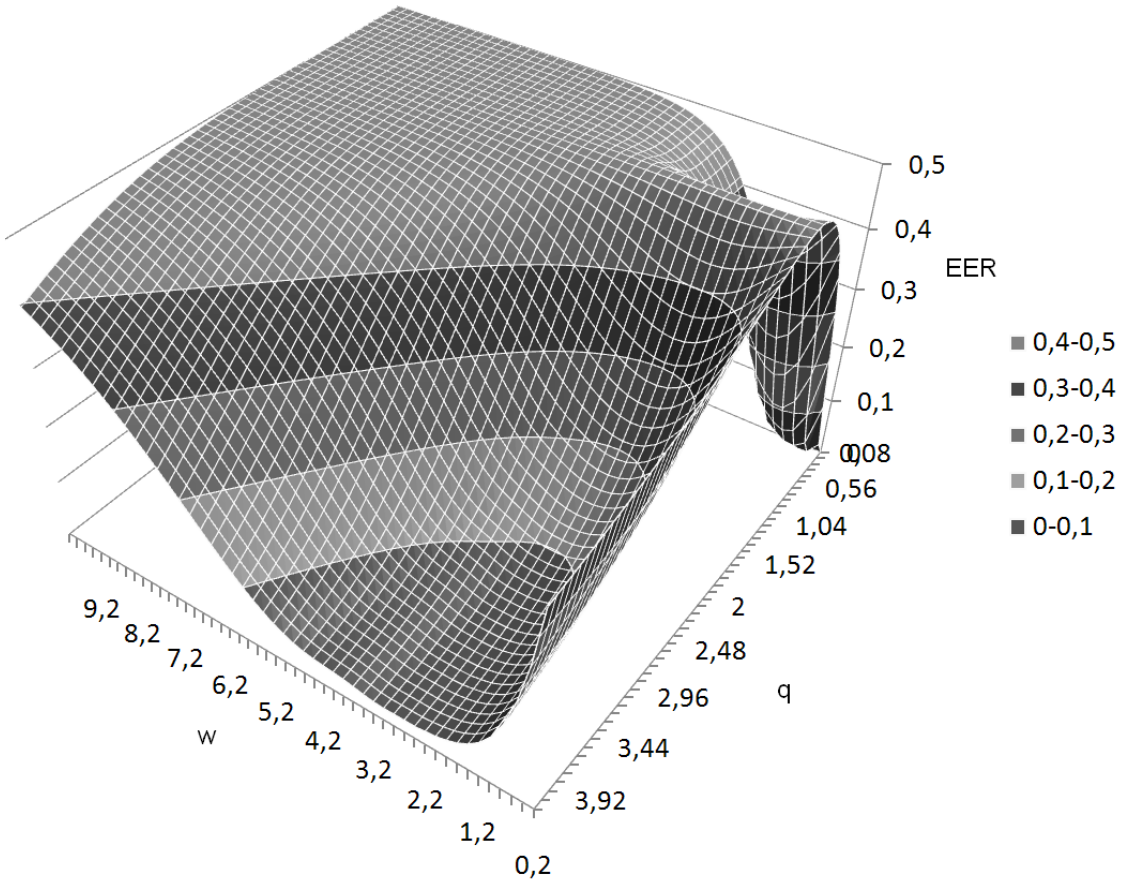

Fig. 6
Relationship of q, w and EER when n=10 and f=10

5.2 Reduction of total error rate

One way to improve the total accuracy of the system is to increase the value of q. We should recall that q was defined as the quotient of the standard deviations of a given feature in the forged and in the original signatures.

$$q = \frac{\sigma_f}{\sigma_o} \tag{17}$$

We (typically) cannot control the quality of the forgeries (σ_f), but we definitely have some control over the quality of original signatures. To increase q, σ_f should be reduced. This could be done by analyzing the individual original samples and identifying outliers. An outlying observation, or outlier, is one that appears to deviate markedly from other members of the sample in which it occurs [22]. In our case this means, that we should examine all measurement values for a given features and if a few of them significantly deviate from the others, apply some additional processing. There are three possible sources for the deviation:

1. *measurement errors*: errors in image processing, feature detection or feature matching can and will often result in false feature values
2. *rare deviation*: the unusual deviation is part of the typical signature of the signer, however, the sample size was too small, to realize this
3. *common deviation*: the unusual deviation was an error in the signature (maybe caused by external conditions) and is not part of the typical signature of the signer.

In many practical cases the acquisition of original samples is performed in a human controlled environment (i.e. in a bank, a bank employee could supervise the acquisition of original signatures). In these scenarios the supervisor can identify and ignore measurement errors and can also ask for additional samples to decide between case 2 and case 3. In fully automated environments we usually cannot distinguish between these three scenarios and also, we cannot ask for additional samples, but we can still choose to drop the outliers from our training set depending on the scale of its deviance. This may have decreasing effect on FAR and an increasing effect on FRR. It is impossible to

predict the effect on EER without further knowledge, but we can simulate the effect on our actual dataset introduced in section 4. Our measurement results (performed with the elimination of outliers at $2.4\sigma_o$) are summarized in Table 2. It can be seen that the average error rate has not significantly changed, however, the relationship of FAR and FRR became more balanced in most of the test cases.

Signer	FAR	FRR
2	15,78%	16,43%
4	17,58%	12,17%
6	17,51%	11,00%
8	4,67%	8,05%
10	16,37%	12,03%
13	18,25%	9,54%
15	14,48%	19,23%
18	3,85%	12,30%
20	11,52%	10,56%
22	18,58%	11,23%
24	3,85%	12,46%
25	23,18%	10,79%
28	13,37%	10,31%
32	22,54%	12,95%
33	20,15%	10,30%
34	11,66%	12,13%
35	6,58%	10,41%
37	6,32%	13,53%
38	10,87%	10,08%
40	7,92%	16,32%
TOTAL	**13,25%**	**12,09%**

Table 2.
Error rates achieved by the statistics based classifier after outlier filtering

5.3 Feedback

One of the main aims of our research is to not only provide a commercial application for signature verification, but to also deliver meaningful details about the reasons behind a single decision.

The whole model of our system was designed to support this scenario (in contrast to many other similar systems), because:

1. The feature set is based on the same features, as used in forensic document examination.
2. Each of the features is matched independently, and each of the matched feature groups is evaluated independently.

As a result of these design principles each signature testing made by our system also tells us, which of the measured features deviated significantly from the usual normal distribution of the signers features.

6 Conclusion

In this paper we discussed problems occurring during feature based off-line signature verification and delivered solutions for the special questions of this problem class. We have shown that the behavior of a feature based off-line signature verification system can be effectively simulated with a statistical approach. The resulting equations allow the prediction of the performance limit of a verification system on a given database and more importantly, can help in the calibration of the system. We have also demonstrated that local features can successfully be used with our system, to distinguish original signatures from forgeries with an acceptable error rate. Our experiments have also shown, that the distribution analysis alone is enough, to filter out outliers, and further outlier filtering will not significantly improve the performance of the whole system.

7 Acknowledgement

This work is connected to the scientific program of the "Development of quality-oriented and harmonized R+D+I strategy and functional model at BME" project. This project is supported by the New Hungary Development Plan (Project ID: TÁMOP-4.2.1/B-09/1/KMR-2010-0002).

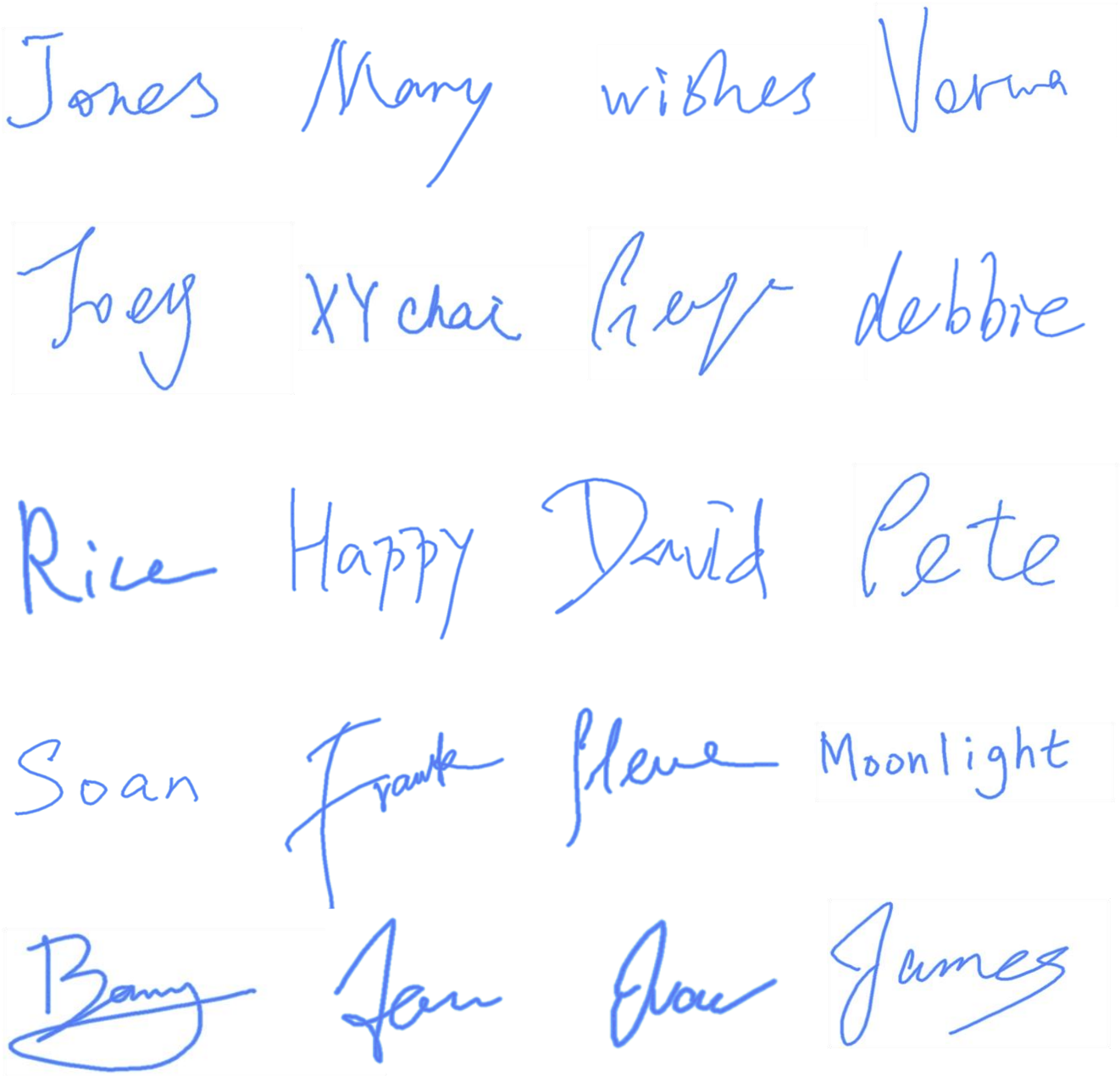

Fig. 7
Samples of the signatures used in the experiments

References

[1] R. A. Huber and A. M. Headrick, "Handwriting Identification: Facts and Fundamentals," CRC Press, LCC, 1999.

[2] K. Franke, "Analysis of Authentic Signatures and Forgeries," Lecture Notes In Computer Science, Proceedings of the 3rd International Workshop on Computational Forensics , vol. 5718, pp. 150-164, 2009.

[3] F. Bryan and R. Doug, "The probative character of Forensic Handwriting Examiners' identification and elemination opinions on questioned signatures," Forensic Science International, vol. 178, no. 1, pp. 54-60, Mar. 2008.

[4] N. S. Sargur, C. Sung-Hyuk, A. Hina, and L. Sangjik, "Individuality of Handwriting: A Validation Study," Sixth International Conference on Document Analysis and Recognition (ICDAR'01), pp. 106-09, 2001.

[5] B. Carolyne, F. Bryan, B. Kaye, and D. Rogers, "Forensic handwriting examiners' opinions on the process of production of disguised and simulated signatures," Forensic Science International, vol. 195, pp. 103-17, Jan. 2010.

[6] F. Bryan and R. Doug, "Documentation of Forensic Handwriting Comparison and Identification Method: A Modular Approach,"

Journal of Forensic Document Examination, vol. 12, pp. 1-68, 1999.
[7] B. Kovari, "The development of off-line signature verification methods, comparative study," in microCAD 2007 International Scientific Conference, 2007.
[8] D.-Y. Yeung, et al., "SVC2004: First International Signature Verification Competition," Lecture Notes in Computer Science, Biometric Authentication, Volume 3072/2004, pp. 16-22, 2004.
[9] S. Akle, M. .-E. Algorri, and A. Salcedo, "Use of wavelet-based basis functions to extract rotation invariant features for automatic image recognition ," WSEAS Transactions on Information Science and Applications, vol. 5, no. 5, pp. 664-673, 2008.
[10]X. D. Zhuang and N. E. Mastorakis, "The curling vector field transform of gray-scale images: A magneto-static inspired approach," WSEAS Transactions on Computers, vol. 7, no. 3, pp. 147-153, 2008.
[11]V. E. Ramesh and M. N. Murty, "Off-line signature verification using genetically optimized weighted features," Pattern Recognition, no. 32, pp. 217-233, 1999.
[12]J. Coetzer, B. M. Herbst, and J. A. d. Preez, "Off-line Signature Verification Using the Discrete Radon Transform and Hidden Markov Model," EURASIP Journal on Applied Signal Processing, vol. 4, pp. 559-571, 2004.
[13]M. A. Ismail and S. Gad, "Off-line Arabic Signature Recognition and Verification," Pattern Recognition, vol. 33, pp. 1727-1740, 2000.
[14]N. L. Othman, J. Shin, and W.-D. Chang, "Chain Code Distance: a Global Feature for On-line Signature Verification," WSEAS Transactions on Computers, vol. 5, no. 9, pp. 2037-2042, 2006.
[15]R. Nerino, "Automatic registration of point-based surfaces ," WSEAS Transactions on Computers, vol. 5, no. 12, pp. 2984-2991, 2006.
[16]H. Baltzakisa and N. Papamarkos, "A new signature verification technique based on a two-stage neural network classifier," Engineering Applications of Artificial Intelligence, vol. 14, pp. 95-103, 2001.
[17]E. Ozgunduz, T. Senturk, and M. Karsligil, "Off-line Signature Verification and Recognition by Support Vector Machine," Thirteenth European Signal Processing Conference, 2005.
[18]M. K. Kalera, S. Srihari, and A. Xu, "Offline Signature Verification and Identification Using Distance Statistics," International Journal of Pattern Recognition and Artifcial Intelligence, vol. 18, no. 7, pp. 1339-1360, 2004.
[19]B. Kovari, B. Toth, and H. Charaf, "Classification Approaches in Off-Line Handwritten Signature Verification," WSEAS Transactions on Mathematics, vol. 8, no. 9, pp. 500-509, 2009.
[20]B. Kovari, I. Albert, and H. Charaf, "A general approach to off-line signature verificatio," WSEAS Transactions on Computers, vol. 7, no. 10, pp. 1648-1657, 2008.
[21]J. C. Rush, The Image Processing Handbook, Fifth edition. North Carolina State University
[22]F. E. Grubbs, "Procedures for detecting outlying observations in samples," Technometrics 11, vol. 11, pp. 1-21, 1969.
[23]A. Kholmatov, "Biometric Identity Verification Using On-Line & Off-Line Signature Verification," 2003.
[24]Kovari, "Time-Efficient Stroke Extraction Method for Handwritten Signatures," in ACS07, The 7th WSEAS International Conference on Applied Computer Science, 2007, pp. 157-161.
[25]Kovari, G. Kiss, and H. Charaf, "Stroke Extraction and Stroke Sequence Estimation for Off-line Signature Verification," The Eighth IASTED International Conference on Visualization, Imaging, and Image Processing.
[26]G. Horváth, et al., Neural Networks. Budapest, 2006.
[27]S. N. Srihari, A. Xu, and M. K. Kalera, "Learning Strategies and Classification Methods for Off-line Signature Verification," Proceedings of the 9th Int'l Workshop on Frontiers in Handwriting Recognition, 2004.
[28]J. Mahmud and C. M. Rahman, "On the power of feature analyser for signature verification," Proceedings of the Digital Image Computing, Techniques and Applications, 2005.
[29]R. Plamondon and G. Lorette, "Automatic Signature Verification and Writer Identification - The State of the Art," Pattern Recognition, vol. 22, no. 2, pp. 107-131, 1989
[30]F. Leerle and R. Palmond, "Automatic Signature Verification - The State of the Art 1989-1993," Int'l Pattern Recognition and Artificial Intelligence, special issue signature verification, vol. 8, no. 3, pp. 643-660, 1994
[31]R. Plamondon and S. N. Sargur, "On-Line and Off-Line Handwriting REcognition: A Comprehensive Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 63-80, 2000
[32]"Pattern Recognition, special issue on automatic signature verification," vol. 8, no. 3, Jun. 1994