Journal of Universal Computer Science, vol. 14, no. 2 (2008), 237-251
submitted: 15/6/07, accepted: 17/11/07, appeared: 28/1/08 © J.UCS

Combining Classifiers in the ROC-space for Off-line Signature Verification

Luiz S. Oliveira, Edson Justino
(Pontifícia Universidade Catolica do Paraná, Brazil
{soares,justino}@ppgia.pucpr.br)

Robert Sabourin
(École de Technologie Superieure, Canada
robert.sabourin@etsmtl.ca)

Flávio Bortolozzi
(Faculdades OPET, Brazil
flavio.bortolozzi@opet.com.br)

Abstract: In this work we present a strategy for off-line signature verification. It takes into account a writer-independent model which reduces the pattern recognition problem to a 2-class problem, hence, makes it possible to build robust signature verification systems even when few signatures per writer are available. Receiver Operating Characteristic (ROC) curves are used to improve the performance of the proposed system.

The contribution of this paper is two-fold. First of all, we analyze the impacts of choosing different fusion strategies to combine the partial decisions yielded by the SVM classifiers. Then ROC produced by different classifiers are combined using maximum likelihood analysis, producing an ROC combined classifier. Through comprehensive experiments on a database composed of 100 writers, we demonstrate that the ROC combined classifier based on the writer-independent approach can reduce considerably false rejection rate while keeping false acceptance rates at acceptable levels.

Key Words: Signature Verification, Pattern Recognition
Category: H.3.7, H.5.4

1 Introduction

In the last few decades many methods have been developed in pattern recognition area, regarding the signature verification problem, which can be categorized into on-line and off-line [Plamondon and Srihari, 2000]. In general, on-line systems achieve better performance since they can count on dynamic features such as, time, pressure, and speed, which can be easily obtained from the on-line mediums [Nalwa, 1997]. On the other hand, off-line systems are difficult to design as many desirable characteristics such as the order of strokes, velocity, and other dynamic information are not available in the off-line case. The verification process has to rely only on the features that can be extracted from the trace of the static signature image [Hanmandlua et al, 2005].

To deal with the problem of off-line signature verification, researchers have investigated two different approaches. The first one, and commonly used, is the writer-specific model (also known as personal model) which is based on two different pattern classes, ω_1 and ω_2, where ω_1 represents the genuine signature set, for a specific writer and ω_2 represents the forgery signatures set. The forgeries usually are divided into three different subsets (random, simple, and simulated forgeries). The random forgery is usually a genuine signature sample belonging to a different writer, who is not necessarily enroled in the signature verification system. The simple forgery is a signature sample with the same shape as the genuine writer's signature. The simulated forgery is a reasonable imitation of the genuine signature model [Justino et al, 2001].

The main drawbacks of the writer-specific approach are the need of learning the model each time a new writer should be included in the system and the great number of genuine samples of signatures necessary to build a reliable model. In real applications, usually a limited number of signatures per writer is available (4 to 6 samples in general) to train a classifier for signature verification, which leads the class statistics estimation errors may be significant, hence, resulting in unsatisfactory verification performance. To surpass this problem, some alternative approaches have been proposed in the literature. Huang and Yan [Huang and Yan, 1997] generate more data through transformations of the genuine signatures. Santos et al [Santos et al, 2004] use the concept of dissimilarity representation [Pekalska and Duin, 2002]. Instead of having one model per writer, only two classes are considered: genuine and forgery.

In this paper we take into account the framework initially proposed by Santos et al [Santos et al, 2004]. It is based on a forensic document examination approach and can be defined as writer-independent approach as the number of models does not depend on the number of writers. In this light, it is a global model by nature, which reduces the pattern recognition problem to a 2-class problem, hence, makes it possible to build robust signature verification systems even when few signatures per writer are available. Support Vector Machines (SVM) are used as classifiers because they have been proved to be quite efficient with 2-class problems.

An important aspect in signature verification that is very often neglected is the class distribution. A tacit assumption in the use of recognition rate as an evaluation metric is that the class distribution among examples is constant and relatively balanced. In signature verification this is rarely the case. Usually one has few genuine signatures and a bunch of forgeries to train a model. In this context, ROC (Receiver Operating Characteristic) curves are attractive due to its property of being insensitive to changes in class distribution. If the proportion of positive to negative instances changes in a test set, the ROC curves will not change [Fawcett, 2006].

The contribution of this paper is two-fold. First we analyze different fusion strategies using ROC and demonstrate that the results of the writer-independent approach can be considerably improved (about 7%) when a suitable fusion strategy is applied. Second, we show that such results can be further improved by combining classifiers without the need for joint training. This combination is based on the maximum likelihood analysis of the ROC classifiers. Comprehensive results on a database composed of 100 writers shows that the combined ROC classifier based on the writer-independent approach can reduce considerably the false rejection rate while keeping the false acceptance at acceptable levels.

The remaining of the paper is organized as follows: Section 2 presents a background on ROC. Section 2.1 introduces the ROC combination method which is based on maximum likelihood analysis. Section 3 describes how the writer-independent approach works. Section 4 presents the database used in this work. Section 5 shows how the off-line signature verification system based on the writer-independent approach has been implemented and Section 6 discusses how this system can be further improved using ROC combined classifier. Finally, Section 7 discusses the results and Section 8 concludes this work.

2 Background on ROC

Receiver Operating Characteristic (ROC) curves are two-dimensional graphs in which true positive rate (TPR) is plotted on the Y axis and false positive rate (FPR) is plotted on the X axis. In this way, For a given classifier C, the ROC is a set of points $(fp_C(k_C), tp_C(k_C))$ where k_C is the parameter that governs the decision process. An ROC graph depicts relative trade-offs between benefits (true positives) and costs (false positives). Each classifier produces an (fp, tp) pair corresponding to a single point in the ROC space.

Several operational points in ROC space are important to note. The lower left point (0, 0) represents the strategy of never issuing a positive classification. In this case, such a classifier commits no false positive errors but also gains no true positives. The opposite strategy, of unconditionally issuing positive classifications, is represented by the upper right point (1, 1). The point (0, 1) represents perfect classification. Usually, one point in the ROC space is better than another if it is to the northwest (TPR is higher, FPR, or both) of the first. In the context of signature verification genuine signatures and forgeries are considered to be positive and negative instances, respectively. For an extensive review of ROC, please refer to [Fawcett, 2006].

2.1 Combining Classifiers in the ROC space

The strategy used in this work was introduced by Haker et al in [Haker et al, 2005]. It is based on the calculation of a combined ROC using maximum likelihood analysis to determine a combination rule for each ROC operating point. Let us consider the ROC for two different classifiers A and B and their respective parameters k_A and k_B. The performance of classifiers C_A and C_B are represented in the ROC space by the points, (fp_A, tp_A) and (fp_B, tp_B), respectively. Given an input pattern, both classifiers will produce an output either positive (+) or negative (-), giving us a total of 4 possible cases. For each case we have an expression of the maximum likelihood estimation (MLE) of the unknown truth T (Table 1).

Table 1: Binary Output for Classifiers A and B and the Maximum Likelihood Combination

C_A	C_B	Combination MLE for truth T
+	+	$P(A=1,B=1\|T=1) \geq P(A=1,B=1\|T=0)$
+	-	$P(A=1,B=0\|T=1) \geq P(A=1,B=0\|T=0)$
-	+	$P(A=0,B=1\|T=1) \geq P(A=0,B=1\|T=0)$
-	-	$P(A=0,B=0\|T=1) \geq P(A=0,B=0\|T=0)$

Each inequality (logical expression) in the rightmost column evaluates either to + or -, and the resulting value is the maximum likelihood estimate of the truth T. If conditional independence is assumed, then $P(A = 1, B = 1|T = 1) = P(A = 1|T = 1)P(B = 1|T = 1) = tp_A tp_B$. Proceeding similarly for the other terms in the rightmost column of Table 1, we get Table 2.

Table 2: Binary Output for Classifiers A and B and the Maximum Likelihood Combination

C_A	C_B	Combination MLE for truth T
+	+	$tp_A tp_B \geq fp_A fp_B$
+	-	$tp_A(1-tp_B) \geq fp_A(1-fp_B)$
-	+	$(1-tp_A)tp_B \geq (1-fp_A)fp_B$
-	-	$(1-tp_A)(1-tp_B) \geq (1-fp_A)(1-fp_B)$

From the assumptions detailed above, $tp_A tp_B = fp_A fp_B$ and $(1-tp_A)(1-tp_B) = (1-fp_A)(1-fp_B)$, so whenever A and B are in agreement their common output is the maximum likelihood estimate of T. Thus, the middle two rows of the Table 2 need to be determined, resulting in one of 4 possible MLE combination schemes, which are described in Table 3.

Using again the assumption of conditional independence, Table 4 shows how to to calculate the false positive and true positive rate for these schemes. In practice, this means that decision processes can be combined without retraining, since there is no need to estimate joint distributions for the output of A and B, nor the need to know the distribution of the underlying truth T.

As stated before, the classifiers (ROC) A and B are governed by the parameters k_A and k_B, respectively. In other words, k_A and k_B are thresholds applied to the outputs s_A and s_B Thus A returns the estimate $T = 1$ if and only if $s_A > k_A$. The same holds for B. Therefore, a new decision rule is necessary for each scheme described so far. Let

Table 3: Schemes for combining classifiers A and B

C_A	C_B	$S_{A\&B}$	S_A	S_B	$S_{A\|B}$
+	+	+	+	+	+
+	-	-	+	-	+
-	+	-	-	+	+
-	-	-	-	-	-

Table 4: FPR and TPR for the combination schemes

Scheme	FPR	TPR
$S_{A\&B}$	$fp_A fp_B$	$tp_A tp_B$
S_A	fp_A	tp_A
S_B	fp_B	tp_B
$S_{A\|B}$	$fp_A + fp_B - fp_A fp_B$	$tp_A + tp_B - tp_A tp_B$

Υ be the combined classifier, created as described above. For a chosen operating point (fp, tp) on the ROC for Υ, we have associated thresholds k_A and k_B and an associated MLE combination rule. The new decision rules s for Υ are defined as function of s_A and s_B as follows: $\min(s_A - k_A, s_B - k_B)$, $s_A - k_A$, $s_B - k_B$, and $\max(s_A - k_A, s_B - k_B)$ for the schemes $S_{A\&B}$, S_A, S_B, and $S_{A|B}$, respectively. The combined classifier Υ will assign "+" when $s > 0$, otherwise, it will assign "-". Algorithm 2.1 shows the pseudo-code for the combined ROC.

3 The Writer-Independent Approach

The global approach is based on the forensic questioned document examination approach. It classifies a handwriting sample, in terms of authenticity, into genuine and forgery, which means that any pattern recognition problem can be reduced to a 2-class problem. In the case of signature verification, the experts use a set of n genuine signature samples $Sk_i, (i = 1, 2, 3, \ldots, n)$ as references and then compare each Sk with a questioned sample Sq. The idea is to verify the discrepancies among Sk and Sq. Let V_i be the graphometric features extracted from the reference signatures and Q the graphometric features extracted from the questioned signatures. Then, the dissimilarity feature vectors $Z_i = (V_i - Q)$ are computed to feed the classifiers C_i, which provide a partial decision. The final decision D depends on the fusion of these partial decisions, which are usually obtained through the majority vote rule. Figure 1 depicts the global approach.

Algorithm 1 ROC Combination

FPComb {buffer for combined false positives}
TPComb {buffer for combined true positives}
for $j = 1$ to $length(fp_A)$ **do**
  for $k = 1$ to $length(fp_B)$ **do**
    fpA = $fp_A(j)$
    tpA = $tp_A(j)$
    fpB = $fp_B(k)$
    tpB = $tp_B(k)$
    if $(tpA * tpB >= fpA * fpB)$ AND $(\sim (tpA * (1 - tpB) >= fpA * (1 - fpB)))$ AND $(\sim ((1 - tpA) * tpB >= (1 - fpA) * fpB))$ AND $(\sim ((1 - tpA) * (1 - tpB) >= (1 - fpA) * (1 - fpB)))$ **then**
      FPComb(j,k) = fpA*fpB;
      TPComb(j,k) = tpA*tpB;
    else if $tpA*tpB >= fpA*fpB)$ AND $(tpA*(1-tpB) >= fpA*(1-fpB))$ AND $(\sim ((1 - tpA) * tpB >= (1 - fpA) * fpB))$ AND $(\sim ((1 - tpA) * (1 - tpB) >= (1 - fpA) * (1 - fpB)))$ **then**
      FPComb(j,k) = fpA;
      TPComb(j,k) = tpA;
    else if $(tpA * tpB >= fpA * fpB)$ AND $(\sim (tpA * (1 - tpB) >= fpA * (1 - fpB)))$ AND $((1 - tpA) * tpB >= (1 - fpA) * fpB)$ AND $(\sim ((1 - tpA) * (1 - tpB) >= (1 - fpA) * (1 - fpB)))$ **then**
      FPComb(j,k) = fpB;
      TPComb(j,k) = tpB;
    else if $(tpA * tpB >= fpA * fpB)$ AND $(tpA * (1 - tpB) >= fpA * (1 - fpB))$ AND $((1 - tpA) * tpB >= (1 - fpA) * fpB)$ AND $(\sim ((1 - tpA) * (1 - tpB) >= (1 - fpA) * (1 - fpB)))$ **then**
      FPComb(j,k) = fpA + fpB - fpA*fpB;
      TPComb(j,k) = tpA + tpB - tpA*tpB;
    end if
  end for
end for

4 Database

The signature database used in this work is composed of 100 writers and it has been divided into training and testing databases. The training set contains 40 writers with 4 genuine and one random forgery per writer. Computing the distance feature vector among the 4 genuine samples of each author gives us 240 positive samples. The negative samples are found by computing the distance feature vector among the random forgery of each author with the 4 genuine samples of the 40 writers, which gives us 288 negative

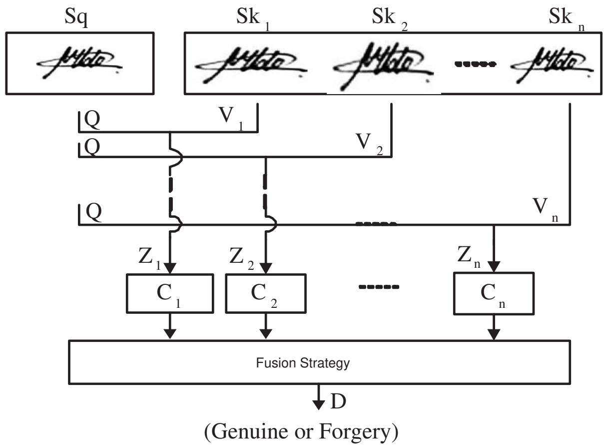

Figure 1: Architecture of the global approach.

samples. These 528 samples make then our training set, which is used to feed an SVM classifier. The validation is done using k-fold cross validation ($k = 10$).

The testing set is composed of the remaining 60 writers with 20 samples per writers. These 20 samples contain 5 genuine signatures, 5 random forgeries, 5 simple forgeries, and 5 simulated forgeries. This approach must consider a reference set, which we have defined as Sk. In our experiments, Sk is composed of 5 genuine samples per writer.

5 Signature Verification Method

The signature verification method works as follows. First the image is segmented using a grid. After some experiments, we have noticed that the size of the grid depends on the graphometric feature being used. In this work we consider two different feature sets, Slant and Distribution. To compute the Slant we have applied the concept presented by Hunt and Qi [Hunt and Qi, 1995], which determines the slant in two steps. First, a global slant is computed over the entire image and then the slant for each cell is computed as well. In this way, each cell has a slant value and the final local value is the most frequent value in the matrix. In this work, the image was segmented into 8 vertical $\times$ 10 horizontal cells. The Distribution of pixels is based on four measures as depicted in Figure 2. In this case we have used 5 vertical $\times$ 5 horizontal cells where each of them is divided into four zones. Then, the width of the stroke is computed in four direction (limited to the zones). These values are represented by the letters A, B, C, and D in Figure 2. A more complex approach, but based on the same idea was proposed by Sabourin et al [Sabourin et al, 1997].

Following the protocol introduced previously, these features are extracted from the questioned (Sq) and reference (Sk) images as well. This produces the aforementioned

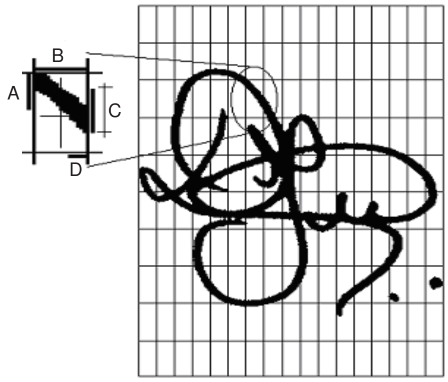

Figure 2: An example of Distribution of pixels. It uses a different number of cells to better illustrate the process.

graphometric feature vectors V_i e Q. Once those vectors are generated, the next step consists in computing the dissimilarity feature vector $Z_i = (V_i - Q)$, which will feeds SVM classifiers. Finally, the final decision is taken based on the majority vote rule. Since we have 5 ($n = 5$) reference images, the questioned image Sq will be compared 5 times, yielding 5 votes.

The recognition rate of the system trained with Slant and Distribution are 83.0% and 84.6%, respectively. Figure 3 shows the ROC for the two classifiers considered in this work. Since the combination rule used in this case is voting, the curve is actually a step function. Due to the different class distribution we are dealing with, the impacts of higher false negatives are more important than the impacts of true positives. This can be observed in Figure 3.

It is important to notice that the SVM has been trained with samples coming from the 40 writers of the training set. The recognition rates is then computed based on the 60 writers who did not contribute to the training of the writer independent classifier. Two hypotheses have been done here: (1) the approach will generalize well for genuine signatures from unknown writer if the intra-class variability of "genuine signatures" is reasonably low and (2) the elimination of random forgeries (e.g., low false positive rate) results in a good detection of simple forgeries according to the nature of this class of forgeries. Table 5 reports the error rates separately for genuine and the three different classes of forgeries.

Statically speaking, the genuine error is known as Type I error, or false rejection as the system classifies genuine signatures as forgeries. The other three columns are known as Type II error, or false acceptance. In this work we have chosen the operational point in the ROC that maximizes the overall recognition rate. In some cases, though, this

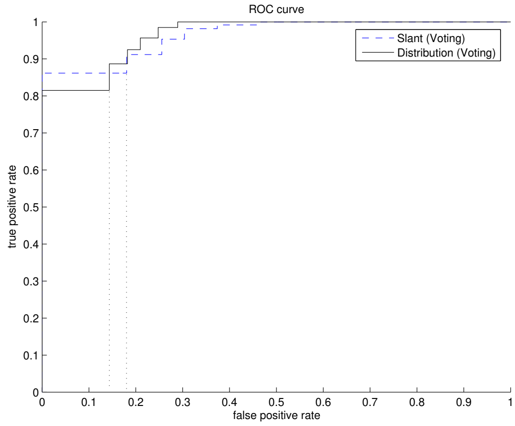

Figure 3: ROC for Slant and Distribution classifiers.

Table 5: Error rates for the baseline system

Features	Genuine	Random	Simple	Simulated
Slant	3.40	4.20	3.95	5.37
Distribution	4.60	4.54	2.37	3.83

choice can be made based on the maximum Type II error than can be accepted. In the context of signature verification, the challenge is to minimize as much as possible the Type II error while keeping the Type I error at acceptable levels.

6 Improving performance using ROC

The first question one could raise at this point would be: Is voting the best combination scheme for this kind of approach? To answer that, we have assessed different combination schemes using ROC, which is quite appropriate in this case as the class distribution among examples is not balanced. It also makes it easy to compare different classifiers for a fixed FPR. Figure 4 depicts the ROC for the Distribution classifier using five different combination schemes, namely, Voting, Mean, Median, Min, and Max. To be able to do that, the SVM classifier had to be modified to yield a probabilistic output [Platt, 1999].

Figure 4 shows clearly that for the same FPR (0.14), the Max strategy improves the TPR from 0.81 to 0.90. In this case, instead of combining the five reference images by Voting, we get the Max probability produced the the classifier. In terms of recognition rate, the operational point (fp, tp) that maximizes performance in this case is (0.06,

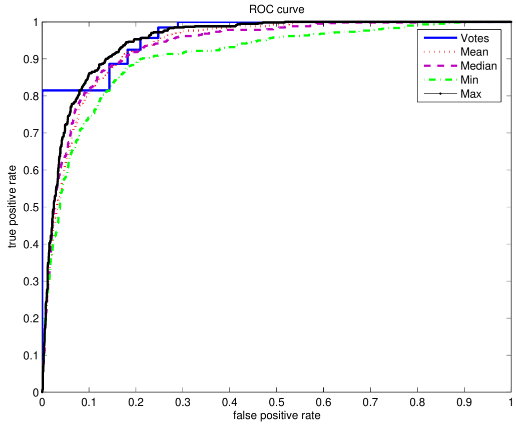

Figure 4: Different combination schemes for the Distribution classifier.

0.77), raising the recognition rate from 84.6% to 89.7%. For the other classifier trained with the feature set Slant, we have observed the same behavior. Max was the best fusion strategy and the recognition rate was increased to 89.5%. Table 6 reports the error rates for the classifiers using Max rules as fusion strategy.

Table 6: Error rates for the baseline system using Max rule as fusion strategy

Features	Genuine	Random	Simple	Simulated
Slant	4.37	2.50	1.70	1.91
Distribution	5.75	2.29	1.12	1.12

As we can observe, the false acceptance has been considerably reduced, but on the other hand the false rejection has been increased for both feature sets. In order to improve the trade-off between false rejection and false acceptance we combined both classifiers using the methodology described in Section 2.1. We have performed different experiments, but the set-up that brought an improvement in terms of the recognition rate was the the combination of classifiers trained with Slant and Distribution, both using Max as fusion strategy. Figure 5 shows all the (fp, tp) pairs generated by Haker's algorithm and the combined ROC classifier as well.

It is clear from this Figure that this combination can improve TPR for a given FPR. For example, if we fixed the FPR at 0.05% and 1%, we can raise the TPR from 0.725% to 0.905% and from 0.83% to 0.96%, respectively. In both cases, the im-

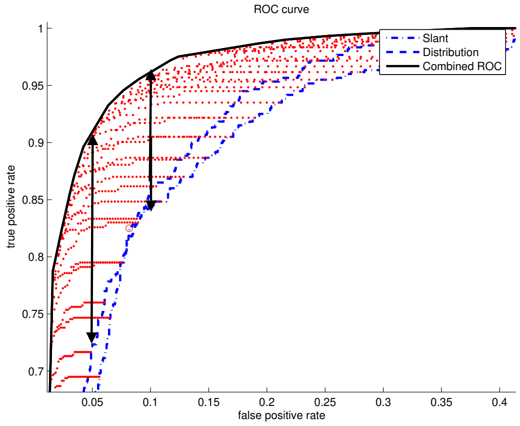

Figure 5: Different combination schemes for the Distribution classifier.

provements are quite impressive. It is important to remember, though, that this algorithm relies on the assumption of conditional independence. In other words, the combined ROC is the upper-bound that could be achieved if both Slant and Distribution classifiers were conditionally independents. In terms of recognition rate, the upper-bound would be 93.16%, since the pair (fp, tp) that maximizes performance is (0.017, 0.778). Considering that the testing set contains 600 positive and 1800 negative samples, $93.16 = ((600 \times 0.7798) + (1800 - (1800 \times 0.0177))/2400)$

However, in practice, the performance observed during the experiments was 91.8%. This corroborates to the fact that the classifiers we have used in this work do not hold the assumption of conditional independence. Nevertheless, the algorithm still brought more than 1% of improvement. This proves that it can be applied even when there is no guarantee of conditional independence. Table 7 reports the error rates of the classifiers using Max as fusion strategy and the error rates for the ROC combined classifier.

Table 7: Error rates after combination

Features	Genuine	Random	Simple	Simulated
Slant	4.37	2.50	1.70	1.91
Distribution	5.75	2.29	1.12	1.12
Combination	4.70	2.04	1.33	1.12

7 Discussion

In order to give a better insight about the results presented so far, let us report the results achieved by a writer-specific approach (one model per user) on the same database using mostly the same graphometric features we have used here. The results reported in Table 8 show the error rates for the different number of signatures used to build the author's model. These results were first published in [Justino et al,, 2005].

Table 8: Error rates for the writer-specific approach [Justino et al,, 2005]

Writers	Genuine	Random	Simple	Simulated
5	18.2	0.10	0.0	1.5
10	12.1	0.10	0.0	3.2
15	10.2	0.10	0.0	3.5

As we can notice, this kind of approach decimates the false acceptance for random forgeries and eliminates simple forgeries. On the other hand, the false rejection is above the acceptable levels for real applications even when more than 15 signatures are used to train the author's model. Another interesting thing to observe is that the false acceptance for simulated forgeries increases as we build more specialized models (more signatures). This kind of over-fitting is clearly depicted in Figure 6.

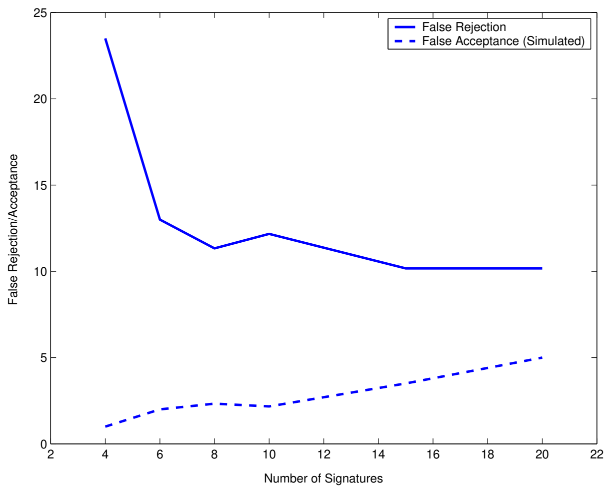

Figure 6: Different combination schemes for the Distribution classifier.

As discussed before, when building a signature verification system, the main challenge is to achieve low false acceptance (Type II error) while maintaining the false rejection(Type I error) at acceptable levels. Analyzing the rates reported in Tables 7 and 8 we can affirm that the writer-independent model offers a much better trade-off than the writer-specific model. In addition, we could observe that the ROC combined classifier brought an improvement to this trade-off by reducing the false rejection. It is worth of remark that the number of training samples used per author in the writer-independent model is equal to S_k. As stated somewhere else, in our experiments $S_k = 5$.

Comparing results with the literature it is not an easy task in off-line signature verification. Most of the researchers do not share the same databases and very often restrict their databases to one type of forgery. However, analyzing some works in the literature we can state that the ROC combined classifier compares favorably [Armand et al., 2006] [Chen and Srihari, 2005] [Hanmandlua et al, 2005].

Figure 7 shows some examples of false acceptance, i.e., forgeries that have been accepted by the system.

Figure 7: Examples of signatures misclassified by the combined ROC classifier.

8 Conclusions

In this paper we have addressed two important issues of the writer-independent approach for off-line signature verification. First we have analyzed the impacts of choosing different fusion strategies to combine the partial decision yielded by the classifiers.

Our experiments have shown that the Max rule is more effective than the original Voting proposed in [Santos et al, 2004].

Thereafter, we have demonstrated that the results of the classifiers using Max rule could be further improved. The strategy used to combine the classifiers was based on the calculation of a combined ROC, using maximum likelihood analysis to determine a combination rule for each ROC operating point. The advantage of such a strategy is that it is not based on learning classifier combination functions from data.

The efficiency of the ROC combined classifier was proved on a database composed of 100 writers. Compared to the writer-specific approach, the writer-independent system yielded a more interesting trade-off between false rejection and false acceptance.Future works include testing other feature sets and the impacts of the number of the references (S_k) on the system.

Acknowledgements

This research has been supported by The National Council for Scientific and Technological Development (CNPq) grant 475645/2004-9.

References

[Armand et al., 2006] Armand S., Blumenstein M., and Muthukkumarasamy V. (2006). Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural-based Classification In Proc. 2006 International Joint Conference on Neural Networks, pages 684–691.

[Chen and Srihari, 2005] Chen S. and Srihari S. (2005). Use of Exterior Contours and Shape Features in Off-line Signature Verification In Proc. 8th International Conference on Document Analysis and Recognition, pages 1280–1284.

[Fawcett, 2006] Fawcett T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters*, 27(8):861–874.

[Huang and Yan, 1997] Huang K. and Yan H. (1997). Off-line signature verification based on geometric feature extraction and neural network classification. *Pattern Recognition*, 30(1):9–17.

[Hunt and Qi, 1995] Hunt R. and Qi Y. (1995). A multi-resolution approach to computer verification of handwritten system. *IEEE Trans. on Image Processing*, 4:870–874.

[Haker et al, 2005] Haker S., Wells W. M., Warfield S. K., Talos I., Bhagwat J. G., Goldberg-Zimring D., Mian A., Ohno-Machado L., and Zou K. H. (2005). Operating Characteristics and Maximum Likelihood Estimation In Proc. 8th International Conference on Medical Image Computing and Computer Assisted Intervention, pages 506–514.

[Hanmandlua et al, 2005] Hanmandlua M., Yusofb M., and Madasuc V. K. (2005). Off-line signature verification and forgery detection using fuzzy modeling. *Pattern Recognition*, 38(3):341–356.

[Justino et al, 2001] Justino E., Bortolozzi F. and Sabourin R. (2001). Off-line signature verification using HMM for random, simple and skilled forgeries In Proc. 6th International Conference on Document Analysis and Recognition, pages 1031–1034.

[Justino et al,, 2005] Justino E., Bortolozzi F. and Sabourin R. (2005). A comparison of SVM and HMM classifiers in the off-line signature verification. *Pattern Recognition Letters*, 26:1377–1385.

[Nalwa, 1997] Nalwa V. S. (1997). Automatic On-line signature verification. *Proceeding of the IEEE*, 85(2):215–239.

[Pekalska and Duin, 2002] Pekalska E. and Duin R. P. W. (2002). Dissimilarity representations allow for building good classifiers. *Pattern Recognition*, 23:943–956.

[Platt, 1999] Platt J. (1999). Probabilistic Outputs for Support Vector Machines and Comparison to Regularized Likelihood Methods. *Advances in Large Margin Classifiers*, 61–74.

[Plamondon and Srihari, 2000] Plamondon R. and Srihari S. N. (2000). On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 22(1):63–84.

[Sabourin et al, 1997] Sabourin R., Genest G., and Preteux F. (1997). Off-line Signature Verification by Local Granulometric Size Distributions. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 19(9):976–988.

[Santos et al, 2004] Santos C., Justino E., Bortolozzi F. and Sabourin R. (2004). An Off-Line Signature Verification Method Based on Document Questioned Experts Approach and a Neural Network Classifier In Proc. 9th International Workshop on Frontiers in Handwriting Recognition, pages 498–502.