An Approach to Improve Accuracy Rate of On-line Signature Verification Systems of Different Sizes

Rodrigo S. A. Araujo[1], George D. C. Cavalcanti[1,2], Edson C. B. C. Filho[2]
[1]*AiLeader Technologies – Recife – PE - Brazil*
[2]*Federal University of Pernambuco, Centro de Informática, Recife – PE, Brazil, 50.740-540*
{rsaa, gdcc}@aileader.com.br, {gdcc, ecdbcf}@ cin.ufpe.br

Abstract

This paper discusses the problem of size variation in on-line signature verification systems. The main idea of the article is to investigate the influence of the size variation in the feature extraction techniques and how this distortion can affect the final classification performance of the systems. In this study a new classification approach was suggested based on Kholmatov and Yanikoglu work in order to measure this performance. Besides that, a feature selection technique was applied in the description of the patterns with the purpose of over come the size variation problem. All the experiments were performed in a database constructed with signatures of three different sizes and skilled forgeries. This kind of study plays an important role in the implementation of systems that uses different signature sources.

1. Introduction

Concerns about security and privacy have been increasing in many countries due to problems of identity theft [1]. The use of biometric authentication systems is one of the best alternatives to combat this problem since it eliminates the need to remember a password, PIN, or carry a token, thus reducing identity information exposure [2]. In particular, signature is still one of the most acceptable and less intrusive biometric indicator [3].

There are two types of signature verification systems according to data acquisition: on-line systems, whose data are captured dynamically through a pressure-sensitive device and off-line systems where you only have access to scanned images.

The utilization in real applications which integrate different signature databases is the main motivation of this work. The development of this sort of verification systems requires a special attention due to aspects that can influence the design of the signatures. One of these aspects is the signature size [4]. The analysis of this property done in this paper can contribute in the resolution of this kind of problems.

Mahmud and Rahman [5] verify the signatures using features analysis and a non linear classifier for off-line systems. The input image is made size invariant through a preprocessing technique, which scales the signatures in a fixed size. Doria et al. [6] also have studied the influence of size in off-line signature systems; however, in his work he rejects the idea of using scaling algorithms due to the loss of information caused, since the size variation is non linear. Thus, he proposes the isolation of the body of the signature, which is less invariant, in order to verify the patterns.

Works related to on-line verification systems have also been done, as in Silva and Freitas [7] which applies wavelet transforms as a mean of generating features from signatures.

In this work, it has been specifically studied the influence of the size variation in the signature formation concerning on-line verification systems and how the available signing space can alter the way somebody sign. In order to accomplish this aim a database constructed with signatures of three different sizes was constructed. A feature selection approach was applied in order to minimize the distortions of size variation. [1]

The section 2 of the paper will show the data acquisition process; in section 3 will be explained the features used in the system; in section 4, the enrollment and verification processes will be discussed; in section 5, a description of all the experiments will be done; and finally in section 6, the conclusion and the future works will be placed.

[1] This proposed approach is registered under the iSign® software intellectual property submitted to INPI-DEPE (Brazil) in 03/14/2004 under the protocol number 00058270.

Ninth International Conference on Document Analysis and Recognition (ICDAR 2007)
0-7695-2822-8/07 $25.00 © 2007 IEEE

2. Data acquisition

The data were acquired from a WACOM tablet model CTE-430. A total of 1828 signatures, including forgeries, were collected from a group of 20 people containing 6 women and 14 men of different ages. Besides, 10% of the signatures were written by left-handed people. All volunteers contributed with 20 authentic signatures of 3 different sizes: 4 small sizes (7,0cm x 1,0cm), 12 medium sizes (8,0cm x 2,0cm) and 4 large sizes (9,5cm x 4,0cm). These 3 sizes represent respectively the spaces of a Brazilian bank check, an identification document and a credit card. As can be seen in Figure 1, there is a visible difference between the signatures, mostly when we look at the large signatures. Although public databases can be found on the internet, such as, the Unipen Project, they are not suitable to our problem; since the paper investigation relies on size variation which is not the focal point of these databases.

The forgery database was divided into two kinds of forgeries: random forgeries and skilled forgeries. In the random forgery the forger has either no knowledge about the original signature and does not try to imitate the shape of the signature. In the skilled forgery the forger can see the genuine signature and he also has time to practice the imitations, although they are not professional. This database contains from 10 to 12 medium simple forgeries and 10 to 12 medium skilled forgeries per class.

The raw data available from the tablet consists of X-, Y-coordinates, pressure and time.

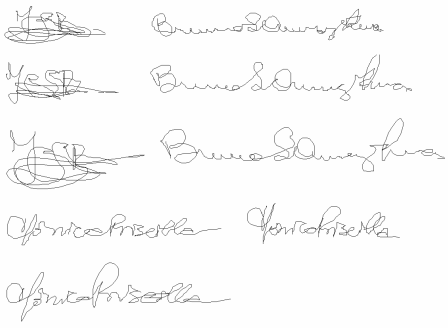

Figure 1. Samples of small, medium and large signatures.

3. Feature extraction

A total of 35 features were implemented in this paper and they were based on a subset of features used in [8]. This set of features is based on coordinates, average speeds and duration which are confirmed to be among the most consistent features as shown in [9], it also makes a comparative study of features used in on-line signature verification systems. The complete feature list can be seen in Table 1.

Table 1. List of features used.

Feature #	Feature description
T1	Average writing speed
T2	Maximum writing speed
T3	Time of maximum speed
T4	Total signing duration
T5	Total pen down duration
T6	Minimum horizontal writing speed
T7	Time of min. horizontal writing speed
T8	Total dots recorded
T9	Average dot execution time
T10	Number of pen ups
T11	Time of 2nd pen down
T12	Duration of Vx > 0
T13	Duration of Vx < 0
T14	Duration of Vy > 0
T15	Duration of Vy < 0
T16	Average positive Vx
T17	Average negative Vx
T18	Average positive Vy
T19	Average negative Vy
T20	Total Vx = 0 events recorded
T21	Total Vy = 0 events recorded
T22	Maximum Vx – Average Vx
T23	Maximum Vy – Average Vy
T24	Maximum Vx – Minimum Vx
T25	Maximum Vx – Minimum Vy
T26	Maximum Vy – Minimum Vy
T27	Max. X time / total time of pen down
T28	Min. X time / total time of pen down
T29	(Max X - Min X) x (Max Y – Min Y)
T30	Initial X - Minimum X
T31	Final X - Maximum X
T32	Final X - Minimum X
T33	(Max X - Min X)/(Max Y - Min Y)
T34	Standard deviation of X
T35	Standard deviation of Y

All the features are invariant with respect to translation. This aspect is fundamental for our experiment since the signature samples were collected in different areas of the tablet.

4. Enrollment and signature verification using template, nearest and farthest distances

The enrollment and verification process are based on Kholmatov and Yanikoglu [10]. In fact, it is an adaptation of the original approach, which consists of calculating the aligning distances between test signatures and three different reference signatures, using Data Time Warping (DTW). The idea in this paper is to improve their approach creating distances between feature vectors, which have much more information then the signature plot, since the feature vectors contain time related information, such as, speed and duration.

For each class, the process starts with the distance calculation of all the reference data among themselves. Later on, the signature which has the minimum average distance to all patterns is designated as being the template signature. Afterwards, it is calculated the average of the minimum distances ($\overline{d\min}$), the average of the maximum distances ($\overline{d\max}$) and the average distances to the template ($\overline{dtemplate}$). Those distances will be called respectively of

- Average of distances of reference signatures to their nearest neighbor ($\overline{d\min}$);
- Average of distances of reference signatures to their farthest neighbor ($\overline{d\max}$);
- Average of distances of reference signatures to the template signature ($\overline{dtemplate}$).

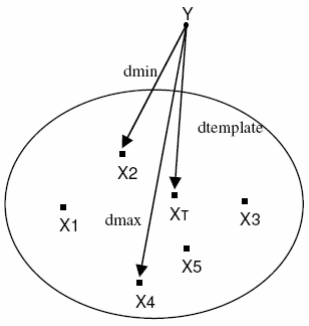

Figure 2. Y represents the test pattern. X_T represents the template signature, dmin, dmax e dtemplate represents the distances.

These distances describe, in a way, the signatures variations of the class and consequently, they are used to normalize d*min*, d*max* and d*template*, which are respectively the distance between the test signature and the nearest neighbor, the distance between the test signature and the farthest neighbor and the distance between the test signature and the template signature of the class. Figure 2, shows these three distances.

During the verification process, as was explained before, d*min*, d*max* and d*template* are normalized, and consequently, all the signatures will be at the same distance scale.

In order to verify if a signature belongs to a specific class, a threshold is calculated for each distance. This threshold is set based on the false patterns to guarantee a zero false acceptance rate. Thus, all test patterns that have distances smaller than the threshold belongs to the verified class.

4.1. Method of evaluation

Based on the distance of a test pattern and the threshold, two types of error rates are calculated: False Reject Rate (FRR) and False Accept Rate (FAR), where the false rejection represents the situation that an authentic user is not considered as being from the class and a false acceptance represents a situation where an impostor is considered as being from the class. These two rates are inversely correlated. In order to compare the performance of the system, it will be kept a zero FAR as was explained before and the FRR will be used as an evaluation measure of error performance of the system.

5. Experiments

For these experiments a total of twenty classes were used and each class has three different sets of signature, which are the small set (S), the medium set (M) and the large set (L). All the verification experiments have used medium signatures as training set, which represents a bank check size area. The decision for the medium training set was taken due to the vast number of articles related to bank check signatures.

5.1. Signature verification using three distances

The system was trained with 8 medium signatures and afterwards it was tested with 4 medium, 4 small and 4 large signatures. This experiment was performed 30 times and the result shown below is the mean of all executions. To perform this experiment, feature vectors containing 35 features were used. The results for each distance can be seen in Table 2.

Table 2. Error rates using the 35 features. Considering zero FAR for skilled forgeries.

Distance	FRR (%) with 35 features		
	S	M	L
d*template*			
Mean	12,63	2,88	21,54
Std. Deviation	3,57	1,97	4,81
D*min*			
Mean	10,75	2,58	21,79
Std. Deviation	3,84	1,83	5,17
D*max*			
Mean	12,13	4,13	22,54
Std. Deviation	3,52	1,83	5,01

The presented results show a great difference among the three sets of signature. The medium (M) set had a low error rate; in contrast, the small (S) set and the large (L) set had higher error rates. These results can be explained by the fact that the system was trained with medium signatures and tested with small and large signatures, which are visually different and also different when it takes in account their features [4]. This experiment is showing that the difference in the size affects the verification error rates.

In order to demonstrate the dispersion that was verified by the error rates, a 3D graphic was plotted (Figure 3). The darker stars represent the M signatures, while the triangle and the circle represent the S and L signatures. From Figure 3 it is possible to see that the M signatures are in a cluster next to the origin of the graphic, however, the S and L signatures are mixed and separated from the M signatures.

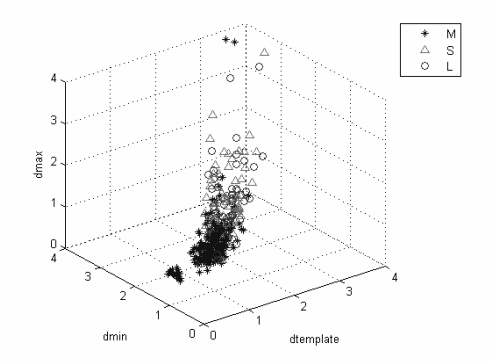

Figure 3. 3D graphic of S, M and L signatures using dtemplate, dmin and dmax.

5.2. Statistical analysis

In order to verify the statistical relevance of this result three distances were calculated. The first was the distance between the test signatures of the small group to the center of the medium group. The second was the distance between the test signatures of the large group and the center of the medium group and the last one was the distance between the test signatures of the medium group and the center of the medium group. The arithmetic mean of all these distances was submitted to a hypotheses test with the significance level of 1% [4]. The limits for the acceptance region of the test for a 99% confidence interval must be greater than 2.58 or less than -2.58 for a normal distribution; since the results for the mean distance of large signatures to medium signatures was z = -2,8517 and the mean distance of short signatures to medium signatures was z = -3, 5698, it was verified that these means are very different .

The results show that even if you use genuine signatures, significant differences will be verified when signatures of different sizes are used in the system. This difference is exactly what it is shown by this statistical test. It says these signatures are different with 99% of relevance.

5.3. Feature selection

Based on the standard deviation of all the features, a second experiment was performed in order to verify the existence of a specific group of features that can give similar results for signatures of different sizes.

A new set of features was created for each class with the objective of minimize the error rates per class. For each class it was separated the first 20 features of less standard deviation, which means the features with less interclass variation. This experiment was also performed 30 times with different training sets.

Table 3. Error rates using local feature selection for dtemplate, dmin, dmax.

Distance	FRR (%) local feature selection		
	S	M	L
D*template*			
Mean	4,04	2,83	4,25
Std. Deviation	3,21	1,88	2,09
D*min*			
Mean	3,20	1,96	5,63
Std. Deviation	2,70	1,30	2,29
D*max*			
Mean	9,50	5,79	9,38
Std. Deviation	4,28	2,04	3,14

Observing Table 3, it is easy to see the evident improvement in the results when compared to Table 2. The M error rate was kept almost at the same level. The S and L error rates, on the other hand, have dropped to from 12,63 and 21,54 respectively to 4,04 and 4,25, if the d*min* is observed for instance. Thus, the results have reached similar error rates independently of signature sizes, which give us a direction of a consistent feature set to deal with this size variation.

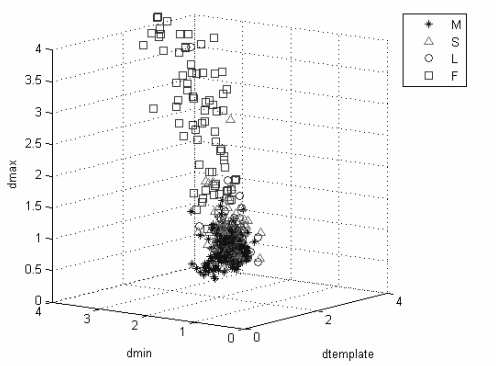

Figure 4. 3D graphic of S, M and L signatures using local feature selection.

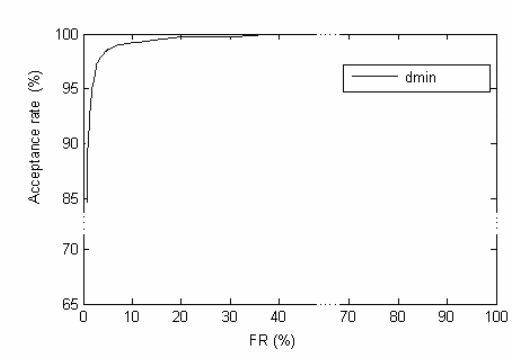

Figure 5. ROC curve of the three distances.

These results can also be seen in Figure 4, which shows all the three sizes grouped in the origin of the graph as an expected unique cluster and the false signatures, represented by F label, separated from that cluster. In Figure 5 is possible to verify the ROC curve of d*min*, which was the distance that has best error rates and in one of the points had 5,3% of false rejection and 98,9% of acceptance. A linear combination of the three distances was also done; however, it did not improve the results.

6. Conclusion

Based on our experiments and on statistical tests, it was verified that there is a substantial difference between medium, small and large signatures. The small and large signatures have influenced the results of the verification process when compared to medium signatures. We can imply from this that signing in areas of different sizes can alter the way a person writes his name, as a consequence, the feature extraction is also influenced. This conclusion can strongly affect the way the on-line verification systems are built.

Finally, as a future work, more signatures must be collected in order to have a more representative database with more testing signatures of small and large sizes. Also, include small and large signatures in the reference set to try other training approaches.

Acknowledgments

This work was supported in part by the Brazilian National Research Council CNPq (478534/2006-0).

7. References

[1] S. Prabhakar, S. Pankanti and A.K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, vol. 1, no. 2, 2003, pp. 33-42.

[2] W. Wang, Y. Yuan and N. Archer, "A Contextual Framework for Combating Identity Theft", IEEE Security and Privacy, vol. 4, no. 2, 2006, pp. 30-38.

[3] A.K. Jain, F.D. Griess, and S.D. Connell, "On-line signature verification", Pattern Recognition vol.35, no. 12, 2002, pp. 2963-2972.

[4] R. S. A. Araujo, G. D. C. Cavalcanti, and E.C.B.C. Filho, "On-line verification for signatures of different sizes", Proc. of the Tenth IWFHR, 2006, pp. 539-544.

[5] J. Mahmud and C. M. Rahman, "On the Power of Feature Analyzer for Signature Verification", Proceedings of the Digital Imaging Computing: Techniques and Applications, 2005, pp. 217-222.

[6] R. C. Doria, E. C. B. C. Filho and E. F. A. Soares, "How Distortions Influence Moment Based Techniques", The Sixth PRIP, 2001, pp. 219-226.

[7] A. V. Silva and D. S. Freitas, "Wavelet-based Compared to Function-based On-line Signature Verification", Proceedings of the XV SIBGRAPI, 2002, pp. 218- 225.

[8] L. L. Lee, T. Berger and E. Aviczer, "Reliable On-Line Human Signature Verification Systems", IEEE Transaction on PAMI, 1996, vol. 18, no. 6, pp. 643-647.

[9] H. Lei and V. Govindaraju, "A Comparative Study on the Consistency of Features in On-line Signature Verification", Pattern Recognition Letters 26(15), 2005, pp. 2483-2489.

[10] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method", Pattern Recognition Letters 26 2005, pp. 2400-2408.