한국지능정보시스템학회논문지 제7권 제2호 2001년 12월(pp. 143~151)

An On-Line Signature Verification Alogrithm Based On Neural Network

Wan-Suck Lee
PassSign Corp. LTD.
(wslee@passsign.com)
Seong-Hoon Kim
Dept. of Computer Engineering,
Youngdong University
(escher@youngdong.ac.kr)

This paper investigates the development of a neural network based system for automated signature authentication that relies on an autoregressive characterization for the segments of a signature. The primary contributions of this work are tow-fold: a) the development of the neural network architecture and the modalities of training it, b) adaptation of the dynamic time warping algorithm to formulate a new method for enabling cosistent segmentation of multiple signatures from the same writer. The performance of the signature verification system has been tested using a sizable database that includes a comprehensive set of simulated and realistic forgeries. False Acceptance and False Rejection error rates of 0.78% and 1.6% respectively were obtained in tests conducted using 1920 skilled forgeries.

Key words: Signature Verification, Neural Network, Skilled Forgery

1. Introduction

There has been widespread interest in the field of biometric personal identification in recent years[1]. In particular, signature verification is of special interest. A signature verification system can be used in applications such as controlling access to a room, authorizing a financial transaction, etc. In the latter category large amounts of money are sanctioned everyday through credit card and check-based transactions on the basis of a signature. According to the National Fraud Information Center, credit card fraud in the United States alone amounts to more than $ 1 billion per year. Even today, when formal signature verification is carried out, it is generally done manually; a test signature is made on the basis of this comparison. While experts do well in verifying signatures, it would be extremely useful to automate this process. It is fair to assume that an automated signature verification system would be of considerable value in reducing incidences of fraud.

Many researchers have worked on both dynamic and static signature vefication problems. On reviewing the literature it was realized that a direct comparison of results from different researchers is often not possible. This is due to

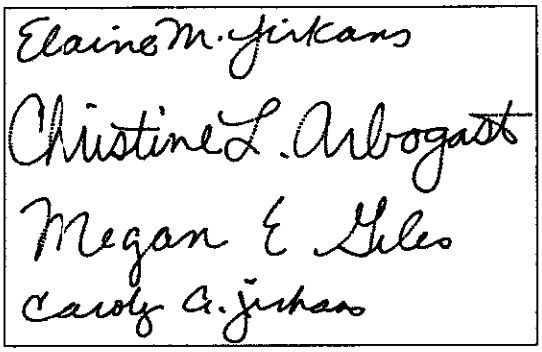
factors such as different data used, field conditions, training and test data size, and the way in which the issue of forgery was handled[2]. Three major survey papers [2], [3], and [4] have been published in this area covering both the static and dynamic signature verification areas.

The principle creative contribution of this paper is a new technique for carrying out on-line signature verification. The techinque is based on an autoregressive(AR) characterization of a signature developed earlier[5]. However, it builds on this by: a) developing a neural network architecture for carrying out signature authentication, and b) employing the dynamic time warping (DTW) algorithm to develop a method for ensuring consistent segmentation of signatures. The segmentation enables the nonstationary evolution of the signature to be captured.

Section 2 describe the realistic forgery database and Section 3 discusses the details about preprocessing and modeling of signature data. In Section 4, the design of the signature verification system based on neural network architecture is presented. Section 5 shows the experiments and results.

2. The Database

The signatures were recorded dynamically using a Wacom digitizing tablet that provided a uniformly time-spaced (x,y) coordinate sequence of points along the signature at a sampling rate of 205 samples/second. The tablet had a maximum spatial resolution of 1200 points/inch. The genuine writer population consisted of 16 writers each of whom provided a total of 150 signatures (for a total of 2400 signatures) collected in a distributed manner over a period of time. The random forgeries were also drawn from the above data set. The signatures of a particular writer, while characterizing that writer, also doubled as random forgeries of the other 15 writers in the population. Some samples of the genuine signatures are shown in <Figure 1>.

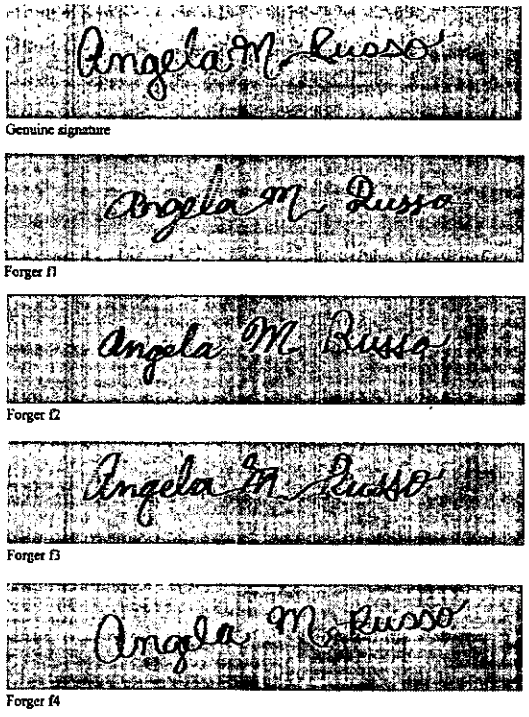


<Figure 1> Genuine signature samples

Additionally, a data set of casual and skilled forgeries was collected for this study. Casual forgeries are those signatures that result when the forger knows the spelling of the genuine signature but has not seen the exact form. Each one of 16 writers was asked to "sign" the fictitious name of John Q. Public 100 times, thus providing a total of 1600 signatures. Once again both genuine signatures and casual forgeries were drawn from this data set in a non-overlapping fashion. We should point out that the use of a single fictitious name, rather than the actual names of the 16 writers, actually makes this study a worst case variant of the corresponding real-life casual forgery situation; this point is elaborated on in Section 6.

Unlike the casual forgery, the skilled for-

gery is executed after some practice in forging the genuine signatures of writers in the population. Understandably then, collection of such a database is a much more arduous task, even with a cooperative group of gorger subjects. On the basis of trials 8 additional writers were recruited exclusively as forgers; these subjects were very skillful and highly motivated in providing forgeries. Then 8 genuine writers from the original population of 16 were selected as the forgery targets. This last choice was made on the basis of the perceived case with which their signatures were copied; typically it amounted to picking writers whose signatures were clearly contoured. Each forger was provided with a hard copy of 10 genuine signatures of a writer to be forged, and given the opportunity to practice as long as he/she wished. The forgers were also allowed to look at the genuine signatures while they were executing the forgeries. The forgers were also informed in advance that the dynamic characteristics of the signature would be used in our verification system. Specifically, they were told that if they slowed down inordinately in executing a forgery - due to the meticulousness of their efforts at doing a good job - it would be almost impossible for their signatures to pass scrutiny. This instruction produced the effect of reflecting the following real-life situation. A forger being watched while executing a signature slows down to the extent needed to produce what he/she considers to be a reasonable spatial reproduction of the original signature, while not arousing any suspicion on the part of the observer. Each of the 8 forgers provided 30 samples of each of the 8 genuine writers, resulting in a total of 1920 skilled forgeries. Some samples of skilled forgeries are provided in <Figure 2> along with the forged signature. The sequence of steps involved in the preprocessing and modeling of the signature are discussed in the next section.



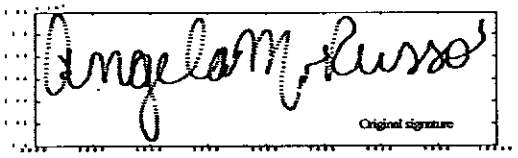
<Figure 2> Skilled forgery samples

3. Signature Preprocessing and Modeling

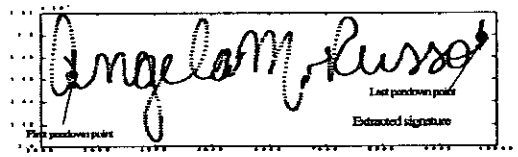
The sampled (x,y) coordinate sequence corresponding to each signature was subjected to the following preprocessing steps. First, the signature contour was redefined using just 256 points that were re-positioned along it at equal-arc-length intervals, so that were re-positioned

along it at equal-arc-length intervals, so that we had uniform spatial sampling for each signature. Second, a straight line was numerically fitted to the signature. Finally, each signature was converted to a 1-D sequence by computing the perpendicular distance to the fitted line, as shown in <Figure 3>.

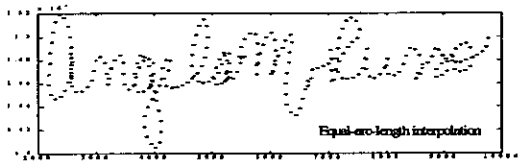
In order to capture the non-stationarity of the signatures, a segmentation scheme was implemented; each segment was modeled separately by a stationary model as discussed below. The spatial evolution of the signature was thus represented by the sequence of feature vectors corresponding to all the segments. The segmentation was carried out as follows. A master signature for each one of the writers was divided into 8 uniform segments and, through the use of the dynamic time warping algorithm[6], segment boundaries were located for all other signatures that best corresponded to the segment boundaries of the master signature. A by-product of the warping process is the generation of a distortion measure whose value is lower the more similar the two sequences are. This distortion measure was included as an additional feature characterizing the signature. Each segment delineated through the application of the DTW algorithm was modeled by a 2'nd order Autoregressive (AR) Model. A much more detailed discussion of the above processes, including parametric choices, can be found in [6]. The neural network architecture formulated to carry out the verification task is discussed in Section 4.



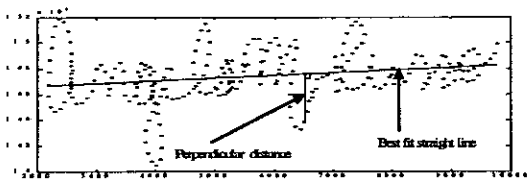
(a) Original signature



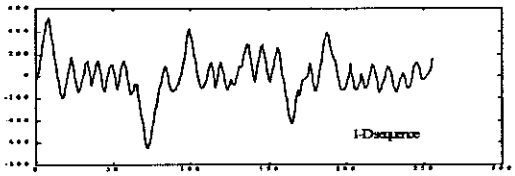
(b) Extracted signature



(c) after Equal-arc-length interpolation



(d) Best-fit straight line and perpendicular distance

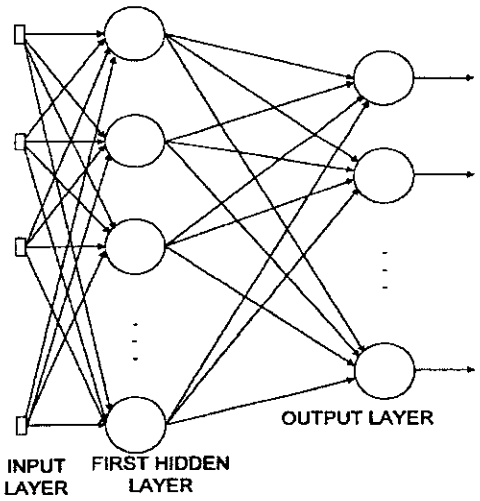


(e) 1-D sequence of perpendicular distances

<Figure 3> Instances of preprocessing steps

4. Neural Network Architecture

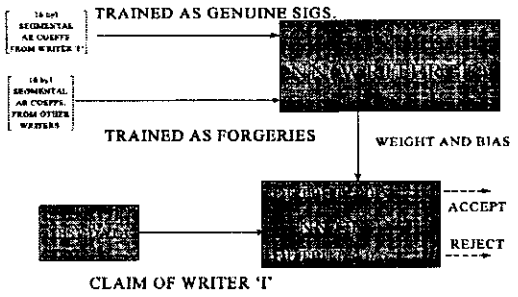
A separate multilayer perceptron, as shown in <Figure 4>, was used for each one of the 16 genuine writers to implement verification. It was trained using the backpropagation algorithm. The network had one hidden layer with 16 neurons; this was established on the basis of trial and error. The output layer had 1 neuron with target values of 1 and 0 corresponding to the genuine writer class and forgery class respectively.



<Figure 4> Neural network architecture

The input layer accommodated either a 17 of 18-feature input constructed as follows. A total of 16 AR coefficients resulted from the 2'nd order model for each of the 8 signature segments. The distortion value resulting from the use of the DTW algorithm to warp the test signature to the claimed reference writer's master signature was the 17th element. The time of execution of each signature was used in selected experiments with skilled forgeries and formed the 18th element of the input (more on this later in Section 6).

A total of 16 neural networks(one per writer) made up of weights and biases were generated. The verification process is shown in <Figure 5>; when an identity claim is made, the feature vector of the claimant is input to the neural network of the claimed identity. If the corresponding output of the network is above 0.5, the identity claim is accepted, otherwise declared as a forgery. The choice of the threshold determines the relative magnitudes of FA and FR types of errors - it can be altered to tradeoff one for the other depending on the application. The various types of verification experiments involving forgeries that were carried out are discussed in the next section.



<Figure 5> The neural network training and testing process

5. Experiments and Results

Several experimental verification paradigms were investigated to assess the impact of forgeries on performance. For the sake of compactness of description in the table of results that follows, these experiments have been tagged with

a character string identifier in parenthesis. Initially random forgeries (RF) were used to establish a baseline of performance. These results are similar to the ones reported in [6] except that DTW distortion was included as an additional feature, The input to the neural network was a 17-element vector (16 AR coefficients form the 8 segments + DTW distortion). Each writer's neural network was trained with 100 genuine signatures and 150 random forgeries, and subsequently tested with 50 genuine signatures and 150 random forgeries. Then the casual forgery database (CF) was used and the above experiment was repeated using the same feature set. The only difference was that 50 instead of 100 genuine signatures were used to train each writer's neural network.

Finally, the skilled forgeries were considered and four experimental variations were formulated using this database. First, 4 out of the 8 forgers (chosen on a random basis) were exclusively used for training purposes, with the remaining 4 used for testing (SF1). This experiment was repeated by swapping the set of forgers between the training and testing phases. Secondly, one half of the skilled forgeries from all 8 forgers were used for training with the remaining half used for testing (SF2). This experiment was also repeated with a swapping of forgeries between the training and testing phases. Both SF1 and SF2 used 17-element input feature vectors. Lastly, SF1 and SF2 were repeated (labeled SF3 and SF4), this time including the time of execution of the signature as an additional feature, resulting in an 18-element vector (16 AR coefficients + DTW distortion + time of execution). In all these four experiments (SF1-SF4), each writer's network was trained using 100 genuine signatures and 120 skilled forgeries and tested with 50 genuine signatures and 120 skilled forgeries. However, it should be noted that swapping of data between the training and test data sets effectively doubled the number of verification tests.

The results of the above experiments are summarized in <Table 1>. Readers should note that additional experimental variations and more details could be found in [7].

<Table 1> Verification results

Experimental variations	False Acceptance(%)	False Rejection(%)
RF	0.08	0.25
CF	1.00	3.62
SF1	13.9	7.10
SF2	2.29	9.00
SF3	8.20	1.00
SF4	0.78	1.60

From <Table 1> it is seen that the use of casual forgeries (CF) results in a deterioration in performance compared to random forgeries (RF) - 1% vs. 0.08% for FA and 3.62% vs. 0.25% for FR. A couple for reasons for the drop in accuracies, which of beyond the nature of the forgeries considered, and as follows. First, a reduced number of signatures (50 vs. 100) were used in the training process. Secondly, when writers sign their own names they exhibit much more consistency than when they "sign" the fictitious name of John Q. Public, due to the amount of practice that they have had with executing their own signature. In this context, it is conceded that the random forgery database is an artificial one.

However, its use produces results that are worse than would be obtained with true casual forgeries.

The results of the first skilled forgery experiment (SF1) represent a significant drop-off in performance in comparison with the random forgery (RF) case - 13.9% vs. 0.08% and 7.1% vs. 0.25% for FA and FR respectively. This was the experiment where the 8 forgers were divided evenly between the training and testing phases of the experiment. It is evident that the classifier performance if very sensitive to the nature of the forgeries included in the experiment. Additionally, the selection of the subset of the forger population to be used in the training vs. testing phases also affects the accuracy obtained. This fact is confirmed by the results of the next experiment (SF2). Here the signatures of the 8 forgers were divided evenly between the training and testing phases, thus providing the neural network with a more broad-based forgery training set. Improved FA error rates of 2.29% vs. 13.9% are obtained. However, the FR error rates increase from 7.1% to 9% as a result of the improved forgery definition; it should be noted that the tradeoff between the two types of errors is adjustable through the bias of the output neuron. While having samples of a forger's work to train the neural network is not a viable option, the SF2 results are nevertheless revealing in as much as they highlight the importance of the modalities of the training process, in particular the inclusion of good skilled forgeries. An examination of the confusion matrix corresponding to this verification experiment also revealed that some writers were easier to forge than others, and that some forgers were more skilled than others.

While the improvement in results obtained between SF1 and SF2 was encouraging, the need to find ways of improving them even further was realized. It was decided to investigate the effect of including an additional feature to characterize signatures that was related to signature dynamics, viz., the time of execution. It was found that writers were quite consistent in their signature execution time. Unlike the spatial contour of a signature, this aspect of a signature is hidden, and one that is not easily reproduced by a forger. Experiments SF1 and SF2 were repeated with the inclusion of the time of execution of the signature as the 18th imput element. This produced dramatic improvements in accuracies. For instance, comparing SF3 and SF1, FA error rates improve from 13.9% to 8.2% and FR error rates improve from 7.1% to 1% respectively. Similarly, comparing SF4 and SF2, FA error rates improve from 2.29% to 0.7% and FR error rates improve from 9% to 1.6% respectively. Finally, comparing SF3 and SF4, while the FA error rate decreases significantly from 8.2% to 0.78%, the FR error rate is once again affected by the superior definition of forgeries (as discussed earlier) and increases slightly from 1% to 1.6%. The SF4 error rates represent the best results obtained with the skilled forgery database.

From the above discussion it is clear that the methodology of training is a key factor affecting performance. the best results obtained with skilled forgeries corresponded to using one half of the skilled forgery database uniformly picked from all 8 forgers to train the network, with the other half used for testing. While getting potential forgers to provide samples is obviously not feasible, the result highlights the importance of

assembling a database of signatures that is comprehensive and representative. Additionally, the potential of the duration of execution of the signature as an additional feature not easily imitated by forgers has been established; its inclusion is critical to performance. An extension of this approach, which uses individual times of execution of each segment of the signature, is worth investigating.

6. Conclusions

A neural network architecture consisting of a multilayer perceptron with a single hidden layer has been developed for signature verification. We are confident that the results obtained with random and casual forgeries will hold up with larger signature databases. The skilled forgery investigation, however, is of a preliminary nature. But despite the fact that the results are somewhat poorer with the inclusion of skilled forgeries, it is important to put them in context. Let us look at the conditions under which the skilled forgery database was created. The forgers were given an unlimited amount of time to practice forgeries and were allowed to look at the original signatures while providing the forgeries. It can be argued that the former situation is conceivable (though perhaps not universally likely) in a real-life situation. However, the latter situation is probably unlikely and unworkable (for the forger) in the majority of circumstances, where the person signing would be under observation. But it is evident that, despite the fact that a truly skilled forgery database is hard to acquire, it is necessary to conduct a more comprehensive investigation of the skilled forgery case, in order to validate the methods developed here for commercial use.

References

[1] Benjamin Miller, "Vital Signs of Identity," IEEE Spectrum(Feb. 1994), 22-30.

[2] R. Plamondon and G. Lorette, "Automatic Signature Verification and Writer Identification: the State of the Art," Pattern Recognition, Vol 22(1989), 107-131.

[3] F. Leclerc and R. Plamondon, "Automatic Signature Verification: The State of the Art-1989-1993," Int. J. Pattern Recognition and Artificial Intelligence, Vol. 8, No. 3 (June 1994), 643-660.

[4] Vishvjit S. Nalwa, "Automatic On-Line Signature Verification," Proceedings of the IEEE, Vol. 85, No. 2(1997), 213-239,.

[5] N. Mohankrishnan, Mark J. Paulik, and Mohamad Khalil, "On-line Signature Verification Using a Nonstationary Autoregressive Model Representation," Proceedings of the IEEE International Symposium on Circuits and Systems(May 1993), Chicago, Illinois, 2303-2306.

[6] Wan-Suck Lee, N. Mohankrishnan, and Mark J. Paulik, "Improved Segmentation through Dynamic Time Warping for Signature Verification using a Neural Network Classifier," Proceedings of 1998 IEEE International Conference on Image Processing(October 1998), Chicago, Illinois.

[7] Wan-Suck Lee, "A Neural Network Based On-Line Signature Verification System," Doctor of Engineering Dissertation, University of Detroit Mercy, Detroit, Michigan, 1998.

국문요약

신경망 기반의 온라인 서명 검증 알고리듬

이완석*
김성훈**

이 논문은 서명의 분할 영역에 대한 자기회귀적(autoregressive) 특징을 사용하는 신경망 기반의 서명 검증 시스템에 대해 다루고 있다. 이 논문에서 특기할 사항으로, 첫 번째, 서명 검증을 위한 신경망 구조의 설계와 학습 방법을 제시하고 있으며, 두 번째는 동일 서명자로부터 얻은 여러개의 서명에 대한 분할의 일관성을 위해서 DTW 알고리듬을 적용한 것이다. 서명 검증 시스템의 성능분석을 위하여 정교하게 만들어진 방대한 양의 모조 서명 데이터베이스를 사용하였다. 1920개의 정교한 모조 서명에 대해 모조서명 인정율 0.78%, 진서명 거부율 1.6%의 결과를 보였다.

* 주식회사 패스사인 대표이사
** 영동대학교 컴퓨터공학과 조교수