Online Handwritten Verification Algorithms Based on DTW and SVM

Kuo-Kun Tseng[1], Xiao-Xiao An[1], Charles Chen[2]

[1] Department of Computer Science and Technology, Harbin Institute of Technology, Shenzhen Graduate School, China
[2] School of Computer Science and Engineering, Minnan Normal University, China
kktseng@hitsz.edu.cn, 307275246@qq.com, charles.chen@mnnu.edu.cn

Abstract

With the development of computer network and biometric technology, identity verification with biologic characteristic becomes the need in this information era. Hand-written signature verification is a kind of the most acceptable way of identity verification, and as one kind of the most common method of authorization with a long history. Based on DTW (Dynamic Time Warping) and SVM (Support Vector Machine), we present a new algorithm for online hand-written signature verification, which approaches the problem as a two-class pattern recognition problem. We compute the similarities between the test signature and reference signatures using DTW to get the feature vector of test signature, and then classify it into one of the two classes (genuine or forgery) by the SVM classifier. Compared with other classifiers (Bayesian and Artificial Neural Network), SVM has better classification result on hand-written signature verification. The best result of this algorithm yields FAR of 9.50% and FRR of 13.33%, which has better result than single DWT algorithm with FAR of 18.12% and FRR of 10.33%.

Keywords: Hand-written signature verification, Dynamic time warping, Support vector machine

1 Introduction

With the development and popularization of Internet technology, many tasks can be accomplished through the Internet. In the virtual network world, user verification becomes more and more important. As a traditional way of identity authentication, handwritten signature has a long development history. As a way of authorization and authentication, handwritten signature has been widely used in commodity transactions and has been recognized by people. Handwritten signature also plays an important role in financial, commercial and legal affairs. For example, financial institutions require users to provide handwritten signatures to complete the business of opening, closing and paying accounts. At present, handwritten signature is still considered to be the most convenient and reliable means of authorization.

Existing authentication methods include: (1) logo-based authentication, such as identity cards, seals and so on; (2) knowledge-based authentication, such as passwords. However, the existing authentication methods have some defects. Based on the authentication of the logo, the logo is easy to be lost and stolen; based on the authentication of knowledge, the password is easy to be forgotten and stolen. Biometrics-based identity authentication has the innate advantages that the above two kinds of authentication do not have. Biometrics are unique to individuals and accompanied by lifelong information. This feature is invariable or has only minor changes, and it will not change or transfer with the will of human beings. It avoids memorizing complex passwords, carries with logos for authentication, and will not be forgotten, lost, or stolen [1]

Human biological characteristics can be divided into two categories [2-6]: physiological characteristics and behavioral characteristics. Physiological characteristics refer to the intrinsic external characteristics, such as fingerprints, palmprints, faces, retinas, iris, etc., which are not controlled by the brain. Behavioral characteristics refer to the behavior characteristics, such as voice, handwritten signatures, which are solidified after long-term training and displayed under the control of the brain. As a biometric feature of identity authentication, it needs to have the following characteristics [7]: (1) uniqueness, no two people can have the same characteristics; (2) permanence, the characteristics must be unchangeable and changeable; (3) availability, which is easy to collect. In addition, it needs to consider the authentication accuracy, cost, speed, and acceptability.

Handwritten signature is a human behavior characteristic. Compared with other biometric authentication, handwritten signature authentication has a long history, which is more in line with the traditional authentication methods. Handwritten signatures are generally regarded as legal means for administrative and financial institutions to verify

*Corresponding Author: Charles Chen; E-mail: charles.chen@mnnu.edu.cn
DOI: 10.3966/160792642020112106014

personal identity. Handwritten signature is an intrinsic form formed in the brain after long-term training, which controls the external performance of muscle movement. Handwritten signature varies from person to person and is difficult to imitate. However, due to the different internal state (such as tension) and external environment (such as writing tools), the same person's handwritten signature may be different. This is also the challenge of handwritten signature authentication.

2 Literature Review

The research on handwritten signatures can be traced back to the 1960s. A. J. Mancerj first published the report "Feasible Research on Personal Identity Recognition Using Handwritten Signatures", and proposed the possibility of handwritten signatures as personal identification. Many studies have devoted themselves to the research of signature authentication, and have achieved rich results. According to the way of data acquisition, signature authentication technology can be divided into two categories: static signature authentication and dynamic signature authentication [8-9]. In static mode, signature data is digitized through an optical scanner or a camera. This gathering is otherwise called "off-line" [10]. In dynamic mode, clients write their sigantures in a digitizing tablet such as WACOM magnetic tablet. Dynamic acknowledgment is otherwise called "on-line" [11]. At present, biometric recognition technology is a hotspot in the field of identity recognition. Online handwritten signature authentication has also attracted many researchers' attention. Many valuable papers on handwritten signature recognition have appeared in the periodicals in the field of pattern recognition such as IEEE Transaction on Pattern Analysis and Machine Intelligence, Pattern Recognition and some international academic conferences such as ICPR and ICDAR.

Generally speaking, handwritten signature verification methods can be divided into two categories: parameter method and point-to-point method. Dimauro et al. [12] combine three different algorithms for signature verification. Sabourin et al. [13] used the Euclidean distance as the matching algorithm in their paper. It calculates the distance between two signatures. Chen et al. [14] used the correlation coefficient to calculate the relevancy. Perizeau and Plamondon [15] proposed a dynamic time warping and matching skeleton tree verification method. Wu et al. [16] used a split and merge matching algorithm to verify the on-line signature. Nalwa [17] proposed in article that the dynamic information of signature (location, pressure, speed, etc.) should be used to replace the morphological information of signature to authenticate, which achieved good results. Jain et al. [18] proposed an online handwritten signature authentication system by adopting string matching and signer-dependent threshold method. Martens & Claesen [19] and Munich & Peron [20] proposed the method of dynamic time warping (DTW) to verify on-line signature, which is widely used in speech recognition. Fuentes et al. [21] used the hidden Markov model to recognize signatures. Tseng and Huang [22] used neural network method as the classifier. In addition to above signature verification algorithm, some new improved algorithms such as correlation test-based nonlinear adaptive noise cancellation (ANC) [23] and correlation test-based neural network validation [24] can also be used to recognize signature.

After more than 40 years of development, handwritten signature authentication has achieved rich results and related products have come out, but it is not still mature, especially the recognition accuracy is not satisfactory. There is still need for further research.

3 Certification Scheme and Evaluation Criteria

The online signature verification method gets the data during the process of handwriting. In general, the online algorithm obtains the information of handwriting signature such as the position of handwriting, trace, velocity, acceleration and pressure signals. On the other hand, the offline handwriting is to get the signature image/picture by scanner or camera. Online handwriting verification is to process the data in both spatial and time domain. While offline algorithms process the data in only spatial domain [14].

The use of dynamic features greatly improves the reliability of authentication and has a better authentication effect. Therefore, dynamic handwritten signature authentication has a wider application prospect than static handwritten signature authentication. The handwritten signature authentication system consists of data acquisition, preprocessing, feature extraction, signature template library and classification modules, as shown in Figure 1.

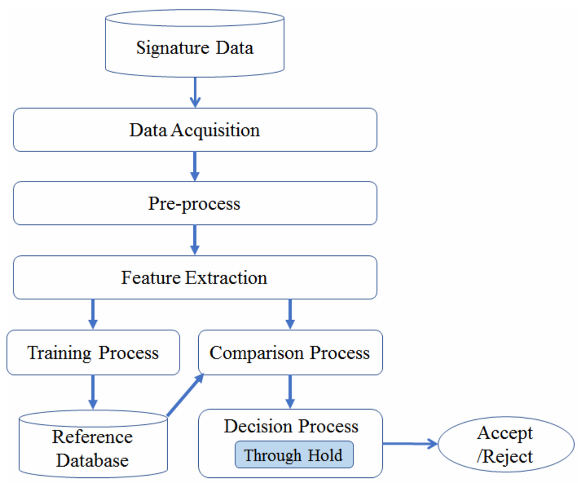


Figure 1. Dynamic handwriting signature verification process

Handwritten signature authentication technology is very similar to speech recognition technology. So some basic technologies in the field of speech recognition can also be applied to the field of online handwritten signature authentication. The recognition ability of the algorithm mainly uses the false rejection rate (FRR) and false acceptance rate (FAR) as the indicators to evaluate the performance of the system. Misrepresentation refers to the rejection of a real signature as a forged signature and the acceptance of a forged signature as a real signature. The corresponding two error rates are defined as follows.

$$FRR = \frac{number\ of\ false\ rejected\ genuine\ signatures}{total\ number\ of\ genuine\ signatures} \quad \textbf{(1)}$$

$$FAR = \frac{number\ of\ false\ accepted\ for\ gery\ signatures}{total\ number\ of\ forgery\ signatures} \quad \textbf{(2)}$$

FAR and FRR will vary with the selected threshold. Ideally, we want to get the optimal threshold, which can completely separate the true signature from the false signature. In practice, the optimal threshold is usually not found. When the threshold increases, FAR increases and FRR decreases; conversely, FAR decreases and FRR increases. Equal Error Rate (EER) is also a common indicator when FAR and FRR are equal.

4 Proposed Methods

4.1 Data Acquisition and Preprocess

At present, dynamic information such as position, pressure, speed and tilt angle of handwritten signature can be easily obtained by handwritten board. Many research institutes will also collect and organize data sharing, providing a unified evaluation standard for the research of handwritten signature authentication. In 2004, the first International Signature Verification Competition (SVC 2004) was held by the University of Science and Technology of Hong Kong. The organizers of the competition provided a unified database of benchmark handwritten signatures and formulated benchmark rules. This activity attracted a large number of researchers to participate in and presented their research results of handwritten signature verification in recent years. Because of the influence of SVC 2004, many researchers use the database provided by SVC 2004 to study handwritten signatures. The algorithm research of this paper also uses this database.

When collecting handwritten data, noise will be introduced due to current instability and other factors. In addition, each time a writer writes a signature, the starting position and size will be different. In order to eliminate the influence of these factors on the authentication effect and eliminate the redundant information in the original data, it is necessary to pre-process the data. The pre-process mainly includes smoothing de-noising and normalization. Smoothing is a common method of de-noising in online handwritten signature authentication. Smoothing can remove interference and distortion, and eliminate the noise introduced in data acquisition. Normalization can transform handwritten data into a unified coordinate space and scale it to the same size, eliminating the influence of different signature positions and sizes on the authentication effect, and avoiding the inconvenience of matching caused by the inconsistency of signature sizes. Suppose the original data is at $(x_i, y_i), i \in [1, N]$, N be the sampling points. The normalization formula is as follows:

$$\bar{x}_i = \frac{x_i - min(x_i)}{max(x_i) - min(x_i)} \times k \quad \textbf{(3)}$$

$$\bar{y}_i = \frac{y_i - min(y_i)}{max(y_i) - min(y_i)} \times k \quad \textbf{(4)}$$

Where $max(x_i)$ 、 $min(x_i)$ 、 $max(y_i)$ 、 $min(y_i)$ are the maximum value and minimum value of original data x 、 y individually, k is the coordinate scale transformation constant. Original data (x_i, y_i) will be normalized as the new coordinate $(\bar{x}_i, \bar{y}_i)$.

4.2 DTW Algorithm

DTW is an algorithm for measuring the similarity of time series with different length based on the idea of dynamic programming [25-26]. DTW algorithm was first widely used in the field of speech recognition. Because of the similarity between online handwritten signature sequence information and speech signal sequence, DTW algorithm began to be applied in the research of handwritten signature authentication. In time series, the length of two time series which need to be comparatively similar may not be equal. In addition, different time series may only have displacements on the time axis, that is to say, in the case of restoring displacements, the two time series are identical. In these complex cases, the distance (or similarity) between two time series can not be effectively calculated by using the traditional Euclidean distance. Based on the principle of optimization, DTW calculates the similarity between two time series by extending and shortening the time series. As shown in Figure 2, the upper and lower solid lines represent two time series, and the lines between time series represent similar points between two time series. DTW uses the sum of the distances between all these similarities, called Warp Path Distance, to measure the similarity between two time series.

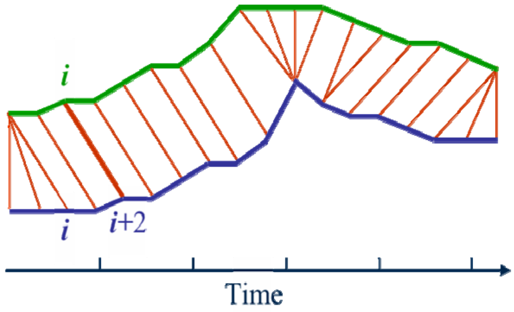


Figure 2. Regulating two time series

The I^{th} signature sequence $S_I = \{P_I(t), t = 1, ..., T_I\}$, each point is a vector $P_I(t) = [x_{I,t}(1), ..., x_{I,t}(N)]$, where $x_{I,t}(n)$ means the information of X 、Y 、pressure, velocity. N is the dimension of each point. T_i is length of i^{th} signature time sequence. For signature *I, J*, the Euclidean distance $d_{I,J}(i, j)$ of i 、j point can be calculated as follows.

$$d_{I,J}(i, j) = \sqrt[2]{\sum_{n=1}^{N}(x_{I,i}(n) - x_{J,j}(n))^2} \quad \textbf{(5)}$$

Using the methodology of dynamic programming, the distance $D_{I,J}(i, j)$ between the lengths i 、j of signatures I and J can be derived from the following recursive relations.

$$D_{I,J}(i, j) = d_{I,J}(i, j) + \begin{cases} D_{I,J}(i-1, j) \\ D_{I,J}(i-1, j-1) \\ D_{I,J}(i, j-1) \end{cases} \quad \textbf{(6)}$$

Where $i = 1, ..., T_I$, $j = 1, ..., T_J$. The similarity $D_{I,J}(T_I, T_J)$ of signature I and J can be calculated from DTW algorithm.

4.3 VM Classification Algorithms

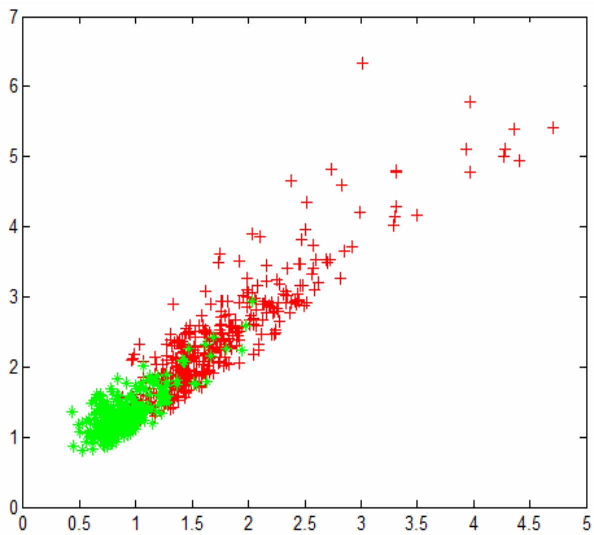
Support Vector Machine (SVM) is a supervised learning method, which can be widely used in statistical classification and regression analysis [27-28]. In 1963, Vapnik proposed a support vector method to solve the problem of pattern recognition. This method selects a set of feature subsets from the training set, so that the partition of feature subsets is equivalent to the partition of the whole data set. This set of feature subsets is called support vector (SV). Support vector machines map vectors to a higher dimensional space in which a maximally spaced hyperplane is established. Two parallel hyperplanes are constructed on both sides of the hyperplane separating data. The distance between two parallel hyperplanes is maximized by separating the hyperplanes. It is assumed that the larger the distance or gap between parallel hyperplanes, the smaller the total error of the classifier.

The similarity of two signature time series with different lengths can be obtained by DTW algorithm. Selecting n real signatures as template signatures, each signature calculates the similarity with n template signatures, and obtains the five-dimensional eigenvectors of the signature. Selecting certain handwritten signatures as training samples, through SVM training, the boundary between real signature and forged signature can be obtained, and the SVM classifier with authentic and false handwritten signature recognition can be obtained.

For n template signatures, the similarities with other n-1 signatures are calculated respectively, and then the mean is calculated. For template signature i, the mean value is T_i. The purpose of computing T_i is to ensure that the normalized eigenvectors can be obtained when the similarities between signatures of different signers and template signatures are calculated. For signature S, the eigenvector is

$$F_S = \begin{bmatrix} D_{S,T}(1)/T_1 \\ D_{S,T}(2)/T_1 \\ \vdots \\ D_{S,T}(n)/T_n \end{bmatrix} \quad \textbf{(7)}$$

Where, $T_{s,T}(n)$ is the similarity between signature S and the n^{th} template, and divided by T_n, to realize the normalization of eigenvector. When n = 2, 1000 signature data are selected and the eigenvectors of each signature are calculated according to formula (7). For each signature, a two-dimensional eigenvector can be obtained, and these two-dimensional vectors can be drawn on the graph. As shown in Figure 3, green asterisks denote real signatures and red plus signs denote forged signatures. Through Figure 3, we can intuitively see that there is a clear demarcation line between real signature and forged signature, which also shows that SVM algorithm can be used for effective classification.



Fugure 3. Spot graph of real and forged signatures based on 2 templates

Because of the great variety of handwritten signatures, handwritten signatures differ greatly from the state and environment of the signers. Our proposed method first uses DTW algorithm to get similarity between the test signature and the template as the feature selection of the signature. At the same time, combined with SVM algorithm, handwritten authentication is transformed into a two-class problem, and good authentication results are obtained.

5 Experiment Result

In this paper, SVC 2004 is used to provide handwritten database. SVC 2004 provides two independent handwritten databases: the first contains only X, Y location and time information, and the second contains additional pressure and pen angle information. It is found that the correct authentication rate is low when only the location information of handwritten signature is used. Pressure information is produced by muscle contraction during the writing process. Muscle contraction is formed by writer's own behavior habits and long-term training. It contains more handwritten signature information for writers. In the process of research, the second database was used as the experimental database. SCV 2004 collected handwritten signature information from 40 people. Each people signs 40 signatures. It contains 20 real signatures and 20 forged signatures. Therefore, SCV 2004 database contains 1600 signatures. Figure 4 shows the original signature data, and Figure 5 shows the pre-processed signature data. After pre-processing, the data is smoothed and normalized to eliminate the influence of noise, signature location and size on authentication.

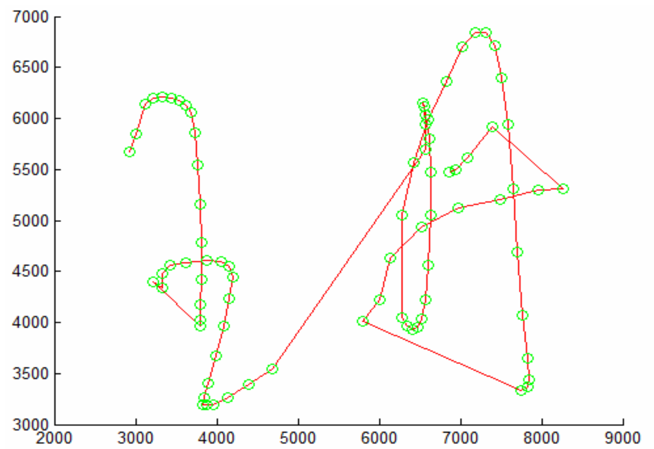


Figure 4. Original signature data

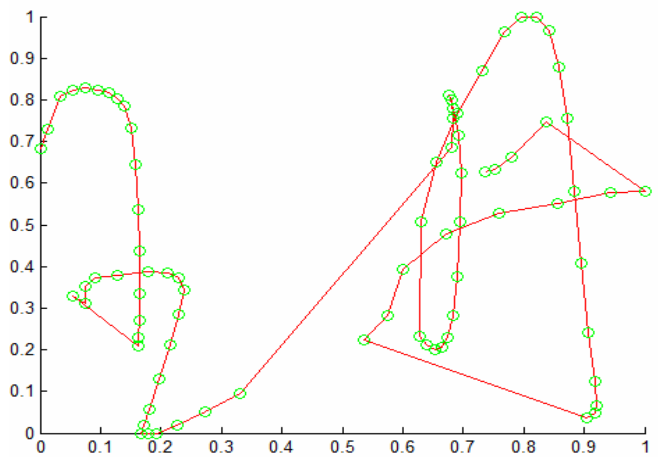


Figure 5. Pre-processed signature data

5.1 DTW Handwritten Signature Verification Algorithms

DTW algorithm can calculate the similarity of two signature sequences with different lengths. Five real signatures are selected as templates. The similarity between test signature and five template signatures is calculated by DTW, and then the mean value is calculated as the similarity S between the real signature and the test signature. Then a suitable threshold F is chosen. When $S < F$, the signature under test is considered to be a real signature, otherwise the signature under test is considered to be a forgery signature. There are two ways to select threshold F: one is to select the unique threshold as the criterion, called common threshold; the other is to select different threshold for different signers, called signer-dependent threshold. Because signatures of different writers are very different, the signer-dependent threshold is usually better than the common threshold. Selecting X, Y position and pressure information as the characteristics of each point, using signer-dependent threshold and DTW for signature verification, the FAR and FRR are 18.12% and 10.33% respectively. As can be seen in Figure 6, for different signers, the verification effect will be very different. Some signers have FARs of 0, while some signers have FARs of 50%. For different signers, the verification effect will be very different, which is also the difficulty of handwritten signature verification research.

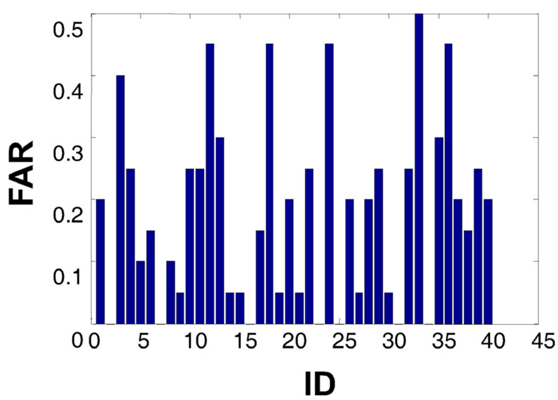


Figure 6. FAR

The handwritten database provided by SCV 2004 contains X, Y position, time, pen tilt and pressure information at each point. The speed and acceleration can be calculated according to the position and time information of X and Y. The experimental results show that better results can be obtained by using X, Y position and pressure information. If unreasonable or excessive combination of handwritten point information is used, the recognition effect will be reduced.

5.2 SVM Handwritten Signature Verification Algorithms

The similarity between each signature and the template is calculated by DTW algorithm as the feature vector of each signature. Then the handwritten signature verification problem is transformed into a two-class problem by training and classification with SVM. The detailed steps are as follows:

(1) For each person's signatures, five real signatures are selected as templates, and the similarities between the five template signatures and other template signatures are calculated respectively, and then the mean value is calculated.

(2) For each test signature, the similarity with five template signatures is calculated, and then divided by the corresponding mean value got from step 1. Those five values are sorted in descending order, which is the eigenvector of the test signature.

(3) Selecting certain signatures as training samples, via SVM classifier training, the SVM classifier with handwritten signature verification ability is got.

(4) Put the test signature into the SVM classifier to verify the results.

We test SVM classifier via using SCV 2004 handwritten signature database. Among the 1600 sample data, 200 real signatures as templates, the other 1400 sample data including 600 real signatures and 800 forged signatures will be used as test data. Table 1 shows the verification effect of SVM classifier. The first one is to use the eigenvectors of the test signature directly; the second one is to arrange the five eigenvectors of the test signature from large to small, and then classify them; the third is to select the minimum and maximum value of the five eigenvectors of the test signature as eigenvectors for training and classification. Via the table, we can see that arranging the five eigenvector values of the test signature in descending order can significantly reduce the error recognition rate. Similar lower error recognition rate can be obtained by choosing only the maximum and minimum values, and the error reception rate is lower than that of the former.

Table 1. SVM classification algorithm

Eigenvectors	FAR (%)	FRR (%)	Average (%)
Not sorted	10.50	16.33	13.42
Descending	9.50	13.33	11.41
maximum and minimum	8.75	14.66	11.71

We also compare SVM classifier with Bayesian classifier and neural network classifier. The comparison result is shown in Table 2. From the table we can see that SVM classifier has better classification effect in handwritten signature verification.

Table 2. Different algorithm comparison

Classifier	FAR (%)	FRR (%)	Average (%)
SVM	9.50	13.33	11.41
Bayesian	13.85	16.56	15.20
neural network	11.78	12.42	12.10

6 Conclusion

In this paper, we improve using single DTW handwritten signature verification algorithm and propose a new handwritten signature verification method by comparing DTW and SVM. Our method converts the handwritten signature verification problem into a binary classification problem. Unlike the selection of feature parameters of handwritten signature in the past, DTW algorithm is used to calculate the similarity between the test signature and the template signature, and get the eigenvector of the test signature. Then the eigenvector of the test signature is processed by SVM classifier, and get the verification. The selection of the characteristic parameters can eliminate the influence of different signatures of the same signer on the verification effect. This paper also compares SVM classifier with Bayesian and Neural Network classifier. The results show that SVM classifier has better classification effect in handwritten signature authentication. Our proposed online handwritten verification algorithm based on DTW and SVM achieves the results of 9.50% FAR and 13.33% FRR. Compared with the single DTW verification algorithm (FAR 18.12%, FRR 10.33%), the verification effect has been improved. This is the contribution of this paper.

References

[1] A. Jain, L. Hong, S. Pankanti, Biometric Identification, *Communications of the ACM*, Vol. 43, No. 2, pp. 90-98, February, 2000.

[2] K. W. Bowyer, V. Govindaraju, N. K. Ratha, Introduction to the Special Issue on Recent Advances in Biometric Systems, *IEEE Transactions on Systems, Man and Cybernetics-Part B: Cybernetics*, Vol. 37, No. 5, pp. 1091-1095, October, 2007.

[3] Y. Chen, J. Yang, C. Wang, N. Liu, Multimodal Biometrics Recognition Based on Local Fusion Visual Features and Variational Bayesian Extreme Learning Machine, *Expert Systems with Applications*, Vol. 64, pp. 93-103, December, 2016.

[4] Y.-L. Huang, C.-H. Lin, F.-Y. Leu, A Batch Verification Scheme by Using the Matrix-Detection Algorithm, *Journal of Internet Technology*, Vol. 13, No. 4, pp. 681-690, July, 2012.

[5] W. Kang, X. Chen, Q. Wu, The Biometric Recognition on Contactless Multi-spectrum Finger Images, *Infrared Physics & Technology*, Vol. 68, pp. 19-27, January, 2015.

[6] K. Reshmi, P. Muhammed, V. Priya, V. Akhila, A Novel Approach to Brain Biometric User Recognition, *Procedia Technology*, Vol. 25, pp. 240-247, August, 2016.

[7] K. Huang, H. Yan, Signature Verification Using Fractal Transformation, *15th International Conference on Pattern Recognition (ICPR-2000)*, Barcelona, Spain, 2000, pp. 851-854.

[8] R. Plamondon, S. N. Srihari, On-line and Off-line Handwriting Recognition: A Comprehensive Survey, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 22, No. 1, pp. 63-84, January, 2000.

[9] R. Ravi Chakravarthi, E. Chandra, Kernel Based Artificial Neural Network Technique to Enhance the Performance and Accuracy of On-Line Signature Recognition, *Journal of Internet Technology*, Vol. 21, No. 2, pp. 447-455, March, 2020.

[10] A. Soleimani, B. Araabi, K. Fouladi, Deep Multitask Metric Learning for Offline Signature Verification, *Pattern Recognition Letters*, Vol. 80, pp. 84-90, September, 2016.

[11] J. Galbally, M. Diaz-Cabrera, M. Ferrer, M. Gomez-Barrero, A. Morales, J. Fierrez, On-line Signature Recognition through the Combination of Real Dynamic Data and Synthetically Generated Static Data, *Pattern Recognition*, Vol. 48, No. 9, pp. 2921-2934, September, 2015.

[12] G. Dimauro, S. Impedovo, G. Pirlo, A. Salzo, A Multi-expert Signature Verification System for Bank Check Processing, *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 11, No. 5, pp. 827-844, August, 1997.

[13] R. Sabourin, G. Genest, F. J. Prêteux, Off-line Signature Verification by Local Granulometric Size Distributions, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 19, No. 9, pp. 976-988, September, 1997.

[14] C. Chen, K. K. Tseng, X. F. Zhang, A Real-World Online Signature Verification System Based on Correlation Algorithm, *International Journal of Computer Applications in Technology*, Vol. 58, No. 4, pp. 321-339, January, 2018.

[15] M. Parizeau, R. Plamondon, A Comparative Analysis of Regional Correlation, Dynamic Time Warping, and Skeletal Tree Matching for Signature Verification, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 12, No. 7, pp. 710-717, July, 1990.

[16] Q. Z. Wu, S. Y. Lee, I. C. Jou, On-line Signature Verification Based on Split-and-merge Matching Mechanism, *Pattern Recognition Letters*, Vol. 18, No. 7, pp. 665-673, July, 1997.

[17] V. S. Nalwa, Automatic On-Line Signature Verification, *Proceedings of the IEEE*, Vol. 85, No. 2, pp. 215-239, February, 1997.

[18] A. K. Jain, F. D. Griess, S. D. Connell, On-line Signature Verification, *Pattern Recognition*, Vol. 35, No. 12, pp. 2963-2972, December, 2002.

[19] R. Martens, L. Claesen, Dynamic Programming Optimization for On-line Signature Verification, *Fourth International Conference on Document Analysis and Recognition*, Ulm, Germany, 1997, pp. 653-656.

[20] M. E. Munich, P. Perona, Continuous Dynamic Time Warping for Translation-invariant Curve Alignment with Applications to Signature Verification, *Seventh IEEE International Conference on Computer Vision*, Kerkyra, Greece, 1999, pp. 1-8.

[21] M. Fuentes, S. Garcia-Salicetti, B. Dorizzi, On Line Signature Verification: Fusion of a Hidden Markov Model and a Neural Network via a Support Vector Machine, *Eighth International Workshop on Frontiers in Handwriting Recognition*, Ontario, Canada, 2002, pp. 253-258.

[22] L. Y. Tseng, T. H. Huang, An Online Chinese Signature Verification Scheme Based on the ART1 Neural Network, *Internal Journal Conference on Neural Networks*, Baltimore, MD, USA, 1992, pp. 624-630.

[23] Q. M. Zhu, L. F. Zhang, A. Longden, A correlation Test-based Validity Monitoring Procedure for Online Detecting the Quality of Nonlinear Adaptive Noise Cancellation, *International Journal of Systems Science*, Vol. 41, No. 9, pp. 1043-1055, March, 2010.

[24] L. F. Zhang, Q. M. Zhu, A. Longden, A correlation-test-based Validation Procedure for Identified Neural Networks, *IEEE Transactions on Neural Networks*, Vol. 20, No. 1, pp. 1-13. January, 2009.

[25] P. Fang, Z. Wu, F. Shen, Y. Ge, B. Fang, Improved DTW Algorithm for Online Signature Verification Based on Writing Forces, *Advances in Intelligent Computing*, Hefei, China, 2005, pp. 631-640.

[26] B. Li, K. Wang, D. Zhang, On-Line Signature Verification Based on PCA and MCA, *International Conference on Biometric Authentication*, Hong Kong, China, 2004, pp. 540-546.

[27] W. S. Lee, N. Mohankrishnan, M. J. Paulik, Improved Segmentation through Dynamic Time Warping for Signature Verification Using a Neural Network Classifier, *1998 International Conference on Image Processing*, Chicago, IL, USA, 1998, pp. 929-933.

[28] A. Kholmatov, B. Yanikoglu, Identity Authentication using Improved Online Signature Verification Method, *Pattern Recognition Letters*, Vol. 26, No. 15, pp. 2400-2408, November, 2005.

Biographies

Kuo-Kun Tseng is an Associate Professor with Shenzhen Peacock B-level talent at Harbin University of Technology (Shenzhen). He received doctoral degree from computer information and engineering, National Chiao Tung University, Taiwan in 2006. His research interests include biometric systems and algorithms. He has published 65 articles in SCI or ACM/IEEE series magazines.

Xiao-xiao An received his M.S. degree from Harbin University of Technology (Shenzhen). He is current a software engineering at Alibaba company. His expertise is in signature verification and watermarking.

Charles Chen is current a Professor in School of Computer Science and Engineering, Minnan Normal University, China. His research interests include pattern recognition, machine learning, information system innovation, intelligent manufacturing, image process, intelligent wastewater treatment process control system and cloud computing.