Chinese Journal of Electronics
Vol.21, No.3, July 2012

Accelerometer-based Gait Authentication via Neural Network*

SUN Hu, YUAN Tao, LI Xiaopeng and HU Yu

(*Department of Automation, TNList, Tsinghua University, Beijing 100084, China*)

Abstract — Gait authentication based on accelerometers is a nonintrusive biometric measurement. It is a novel and feasible way to enhance the security of portable electronic devices. To boost authentication performances, a decision-level data fusion algorithm via neural network is proposed in this paper. The proposed algorithm fuses acceleration signals in different directions and classical approaches for matching gait patterns such as correlation, Euclidean distance *etc*. In our experiments, data sets for training and test consist of 17, 20 subjects separately. The Equal error rate (EER) is cut to 0.82%, which is much lower than other proposed approaches so far.

Key words — Gait authentication, Fusion, Neural network, Accelerometer.

I. Introduction

Personal digital assistants (PDAs) like smart phones, multimedia players, digital cameras *etc*., have been greatly integrated into people's daily life. As some of the PDAs are expensive and some hold precious data, increasingly growing attentions are paid to security issues, especially user authentication. Miniaturized accelerometers in size of millimeters can be easily integrated into PDAs[1], thus accelerometer-based gait authentication is feasible. Compared with other authentication techniques, accelerometer-based gait has its own advantages. For example, the gait data cannot be stolen or lost like password or ID card; it overcomes limitations due to sound, lighting and viewpoint variations, which voice and video-based gait suffer inevitably.

As a result, accelerometer-based gait authentication is appealing. A number of related studies have been proposed since 2005[2−7]. They differ with each other in allocations of accelerometers (waist, ankle, trousers' pocket, *etc*.), in approaches for calculating match values (correlation, histogram, high order moment, Manhattan distance, Dynamic time warping (DTW), *etc*.) and so on. Numerically, a lowest EER of 1.6% is achieved in Ref.[7]. In the above studies, match values are always compared with thresholds directly for authentication, while in Ref.[8], five match values originating from accelerations of five differently allocated accelerometers, are fused by a voting scheme for identification, which is quite similar to authentication.

This paper presents a decision-level data fusion algorithm via neural network. Match values from different approaches of calculation, and from accelerations in different directions are fused. Only one triaxial accelerometer is utilized to collect vertical, backward-forward and lateral acceleration signals. Lateral signals are omitted because they are not so distinctive compared with the others[6]. We select time domain correlation, frequency domain correlation, and Euclidean distance to calculate match values for the consideration that characteristics of time domain and frequency domain, relative changes and absolute values can compensate each other respectively. The three approaches for calculating match values are applied to vertical and backward-forward signals separately, thus six types of match values are produced. The neural network's inputs are the six types of match values and its output is a fusion score which is compared with a threshold. Comparing the six types of match values with thresholds separately, we get six non-fusion authentication algorithms, whose EERs range from 3.3% to 8.4% in our experiments. Still, the fusion algorithm outperforms them substantially, with an EER of 0.82%.

The rest of this paper is organized as follows: Section II introduces the three selected approaches for calculating match values and the way of using them; Section III describes the employed neural network; Section IV shows our experiments and the results; Finally, Section V concludes this paper and lists some future work.

II. Approaches for Match Values

The triaxial accelerometer is attached to subjects' waists. Sampling frequency is set to 640Hz. Before the calculation of match values, main procedures for processing acceleration signals include filtering, cycle division, normalization and mean cycle determination, which are often introduced in related studies[2−7]. In our studies, every step is regarded as a gait cycle; right and left cycles are treated separately; and each determined mean cycle composes a gait vector. Thus we get a pair of gait vectors from every signal sequence at the end of these procedures. Both of the gait vectors have a length of 128 and their values are restricted into $[-1, 1]$.

For two to-be-matched signal sequences in the same direction (vertical or backward-forward), two pairs of gait vectors

*Manuscript Received July 2011; Accepted Nov. 2011.

are produced. We use $(\boldsymbol{t}_{a1}, \boldsymbol{t}_{b1})$ and $(\boldsymbol{t}_{a2}, \boldsymbol{t}_{b2})$ to denote the vector pairs. Details of the three selected approaches for calculating match values (s_1, s_2, s_3) are as follows:

(1) Time domain correlation

$$\begin{aligned} s_1 = \max\{&\mathrm{cor}(\boldsymbol{t}_{a1}, \boldsymbol{t}_{a2}), \mathrm{cor}(\boldsymbol{t}_{a1}, \boldsymbol{t}_{b2}), \\ &\mathrm{cor}(\boldsymbol{t}_{b1}, \boldsymbol{t}_{a2}), \mathrm{cor}(\boldsymbol{t}_{b1}, \boldsymbol{t}_{b2})\} \end{aligned} \tag{1}$$

(2) Frequency domain correlation

$$\begin{aligned} s_2 = \max\{&\mathrm{cor}(\boldsymbol{f}_{a1}, \boldsymbol{f}_{a2}), \mathrm{cor}(\boldsymbol{f}_{a1}, \boldsymbol{f}_{b2}), \\ &\mathrm{cor}(\boldsymbol{f}_{b1}, \boldsymbol{f}_{a2}), \mathrm{cor}(\boldsymbol{f}_{b1}, \boldsymbol{f}_{b2})\} \end{aligned} \tag{2}$$

Here $\boldsymbol{f}_{a1}, \boldsymbol{f}_{a2}, \boldsymbol{f}_{b1}$ and $\boldsymbol{f}_{b2}$ are FFT coefficients of $\boldsymbol{t}_{a1}, \boldsymbol{t}_{b1}, \boldsymbol{t}_{a2}$ and $\boldsymbol{t}_{b2}$ respectively.

(3) Euclidean distance

$$\begin{cases} s_3' = \min\{\mathrm{dis}(\boldsymbol{t}_{a1}, \boldsymbol{t}_{a2}), \mathrm{dis}(\boldsymbol{t}_{a1}, \boldsymbol{t}_{b2}), \\ \qquad\quad \mathrm{dis}(\boldsymbol{t}_{b1}, \boldsymbol{t}_{a2}), \mathrm{dis}(\boldsymbol{t}_{b1}, \boldsymbol{t}_{b2})\} \\ s_3 = 1 - \dfrac{s_3'}{\sqrt{128 \times 4}} \end{cases} \tag{3}$$

In the above equations, cor(.) means the calculation of correlation and dis (.) means the calculation of Euclidean distance. "Right" and "left" steps are not distinguished from each other. Instead, four different combinations of the two to-be-matched vector pairs are taken into account. All the match values are restrained into $[-1, 1]$ and a higher value indicates the two vector pairs are more similar.

Applying the three approaches to vertical and backward-forward accelerations separately, we get six types of match values, which are denoted by $c_1, c_2, \cdots, c_6$ in this paper, corresponding to six non-fusion authentication algorithms, which are denoted by V1, V2, V3, B1, B2 and B3. Here the letters "V" and "B" represent signal directions (vertical and backward-forward); and their following integers "1" "2" and "3" indicate the approaches for the calculation of match values.

III. Fusion via Neural Network (FNN)

To fuse the six types of match values-$c_1, c_2, \cdots, c_6$, a good pattern classifier is crucial to guarantee the performance of the fusion algorithm. In the area of pattern recognition, there are many approaches that we can choose from: k-nearest neighbors, Principal component analysis (PCA), fuzzy clustering, canonical analysis, and fractal dynamics, neural network, wavelet methods and so on[9−11]. Chau[11] points out that neural network facilitate gait analysis because of its highly flexible, inductive, non-linear modeling ability and that the non-linear property of multi-layered neural networks is powerful for analysis of complicated gait variable relationships which have traditionally been difficult to model analytically.

1. Description of the employed neural network

Considering Chau's conclusion in Ref.[11], we employed a multi-layered feed-forward neural network. It is shown in Fig.1. Each type of match value corresponds to an input node. To promote the network's non-linear classifying ability, a hidden layer is employed. Every authentication result is binary, so one output neuron is sufficient. The p to-be-fused match values $(c_1, c_2, \cdots, c_p)$ compose an input vector and w_{ij}, v_j $(i = 1, 2, \cdots, p;\ j = 1, 2, \cdots, q)$ are referred to as connection weights.

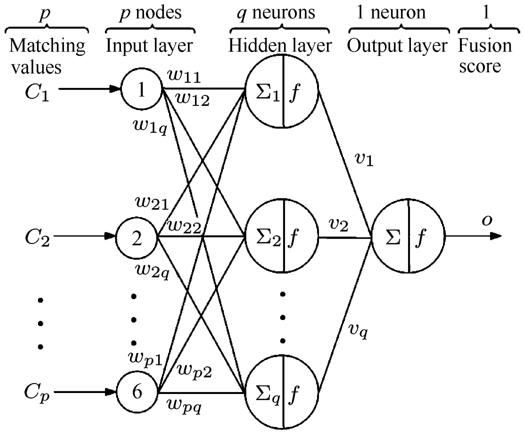


Fig. 1. Architecture of the employed neural network

Let y_j represent the output of the jth neuron in the hidden layer and b_j represent its bias. Particularly, b_0 represents the bias of the output neuron. The employed neural network can be expressed by the following equations[12]

$$\begin{cases} y_j = f\left(\sum_{i=1}^{p} c_i w_{ij} - b_j \right), \quad j = 1, 2, \cdots, q \\ o = f\left(\sum_{j=1}^{q} y_j v_j - b_0 \right) \\ f(x) = \dfrac{e^x - e^{-x}}{e^x + e^{-x}} \end{cases} \tag{4}$$

where $f(x)$ is called transfer function. Crucially speaking, every multi-layered feed-forward neural network using a linear transfer function has an equivalent single-layer network; a non-linear function is therefore necessary for a network to gain the ability of non-linear classifying[12]; hyperbolic tangent is chosen because it has an easily calculated derivative which eases the process of optimizing the connection weights and biases-the training process.

In our case, 6 types of match values are intended to be fused, thus p is set to 6. To some extent, the number of neurons in the hidden layer is flexible. It is usually balanced among training time, and classifying ability, classifier's generalizing ability and stability. Considering all these facts, we have chosen 8 neurons in the hidden layer $(q = 8)$. The employed neural network algorithm actually fuses and compares all the combinations of the six types of match values by tuning the connection weights w_{ij}. For example, only c_1 and c_2 are fused when the connection weights w_{ij} $(i = 3, 4, 5, 6;\ j = 1, 2, \cdots, 8)$ are all set to zero. Consequently once the connection weights are sufficiently optimized, the employed neural network is due to outperform, or at least equal to any other similar neural network with less input nodes.

2. The training process

Apparently once its architecture and transfer function $f(x)$ are chosen, the neural network's output is determined by the connection weights and biases. As is mentioned above, the process of optimizing these parameters is called the training process. During the training process, our input vectors are randomly divided into two groups: 80% for training the parameters and 20% for validation. Every input vector is associated with an authentication target, '1' or '0', which is the perfect output of the neural network at the input vector and indicates whether or not the input vector originates from the same subject. Generally, the weights and biases are adjusted according to the difference between the targets and actual outputs. Scaled conjugate gradient back propagation (as presented by Moller in Ref.[13]) is adopted for the training because of its fast speed. When the average squared difference between all targets and actual outputs on the validation data set stops decreasing, the training process stops.

IV. Experiments and Results

1. Experimental data

To evaluate the performance of the employed neural network, we collected gait acceleration from 37 subjects. The training data set and the test data set respectively consist of 17 subjects and 20 subjects. The collection device (micro control unit: uPD78F0485) was attached to subjects' waists and the sampling frequency was set to 640Hz. Each subject was told to walk 4 times with their normal pace on a flat surface; therefore 4 gait sequences were acquired from everyone. Hence in the training data set, there are 102 ($C_4^2 \times 17 = 102$) input vectors witha target '1', and 2448 ($C_{17}^2 \times C_4^1 \times C_4^1 = 2448$) input vectors with a target '0'. In the test data set, the amounts of the two types of input vectors are 120 ($C_4^2 \times 20 = 120$) and 3040 ($C_{20}^2 \times C_4^1 \times C_4^1 = 3040$) respectively.

2. Authentication rules and evaluation criteria

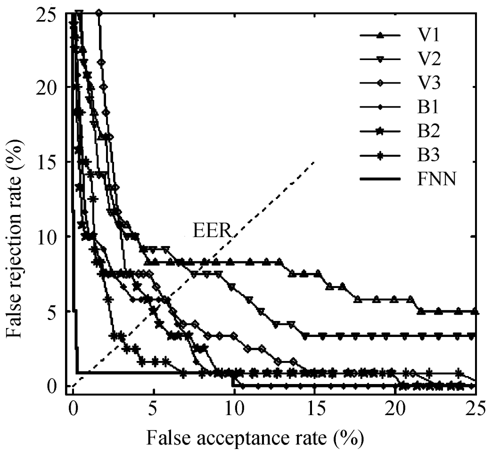
Here authentication rules are ways of working out authentication results using match values or the neural network's outputs. Let t denote a predefined threshold. For the six non-fusion algorithm, the authentication is done due to $\mathrm{sgn}(c_i - t)$, $i = 1, 2, \cdots, 6$; for FNN, the authentication is done due to $\mathrm{agn}(o - t)$. If the result is '1', the corresponding match value or fusion score is considered to originate from the same subject. Otherwise it is considered to originate from different subjects.

False acceptance rate (FAR), False rejection rate (FRR) and Equal error rate (EER) are used as evaluation criteria. FAR is the rate of mis-authentications in the 3040 imposter trials; FRR is the rate of mis-authentication in the 120 genuine trials. As the thresholds change consecutively from 0 to 1, FAR decreases from 1 to 0 while FRR increases from 0 to 1. EER is the point where FAR and FRR are equal.

3. Results and their indications

On the test data set, performances of the six non-fusion authentication algorithms (V1, V2, V3, B1, B2 and B3) and the Fusion algorithm (FNN) are compared with each other.

Detection error tradeoff curves (FARs vs. FRRs, sometimes also called Receiver operating characteristic curves) are depicted in Fig.2 and details about EERs are shown in Table 1. Apparently FNN promotes authentication performances substantially compared with the six non-fusion algorithms-V1, V2, V3, B1, B2, B3. Its EER (0.82%) is much lower than those of the non-fusion algorithms (3.3%∼8.4%). Taking into account that EERs in previous studies[2−7] range between 1.6%and6.4%, it is reasonable to treat 0.82% in this paper as a significant progress. The results have also proved that FNN is an efficient way of fusing accelerations from waists in backward-forward, vertical directions, as well as the three selected approaches for calculating match values.



Notes: V1, V2, V3, B1, B2 and B3 represent the six non-fusion authentication algorithms. FNN represent the fusion algorithm via neural network. V1: vertical acceleration, time domain correlation; V2: vertical acceleration, frequency domain correlation; V3: vertical acceleration, time domain Euclidean distance; B1: backward-forward acceleration, time domain correlation; B2: backward-forward acceleration, frequency domain correlation; B3: backward-forward acceleration, time domain Euclidean distance; FNN: fusion via neural network

Fig. 2. Detection erroe tradeoff (DET) curves of different algorithms

Table 1. EERs of different algorithms

Algorithm	V1	V2	V3	B1	B2	B3	FNN
EER(%)	8.4	7.5	5.9	5.9	5.0	3.3	0.82

V. Conclusion and Future Work

FNN-the proposed fusion algorithm via neural network, requires one triaxial accelerometer attached to subjects' waists, in order to imitate one carrying a PDA. Compared with the presented six non-fusion algorithms, FNN promotes authentication performances substantially. It has an EER of 0.82%, which is much lower than those of the non-fusion algorithms. FNN is not only an outstanding algorithm itself, but also it provides a way of fusing match values that may be useful in other areas of pattern recognition.

Usually gait accelerations are not invariant to body injury, burden and fatigue, *etc.* How to improve the robustness of the authentication algorithm with these factors is a challenging topic in future studies. Meanwhile the proposed authentications were running in an off-line mode, how to tackle an on-line mode with acceptable computational complexity is another challenging topic.

References

[1] T. Yuan and B. Wang, "Accelerometer-based Chinese traffic

police gesture recognition system", *Chinese Journal of Electronics*, Vol.19, No.2, pp.270-274, 2010.

[2] H.J. Ailisto, M. Lindholm, J. Mäntyjärvi *et al.*, "Identifying people from gait pattern with accelerometers", in *Proceedings of the Society of Photo-optical Instrumentation Engineers, Biometric Technology for human Identification II Conference*, Orlando, FL, USA, Vol.5779, pp.7–14, 2005.

[3] J. Mäntyjärvi, M. Lindholm, E. Vildjiounäite, S.M. Mäkelä and H.J. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers", in *Proceedings of 30th IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Philadelphia, Pa, USA, Vol.2, pp.973–976, 2005.

[4] D. Gafurov, E. Snekkenes and P. Bours, "Gait authentication and identification using wearable accelerometer sensor", in *Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies*, pp.220–225, Algernon, Italy, 2007.

[5] R. Liu, J. Zhou, M. Liu and X. Hou, "A wearable acceleration sensor system for gait recognition", in *Proceedings of Second IEEE Conf. Indust. Electron. Applic.*, pp.2654–2659, Harbin, China, 2007.

[6] Y. Li, X. Wang and F. Qiao, "Gait authentication based on acceleration signals of ankle", *Chinese Journal of Electronics*, Vol.20, No.3, pp.447–451, 2011.

[7] D. Gafurov, E. Snekkenes and P. Bours, "Improved gait recognition performance using cycle matching", in *Proceedings of 24th IEEE Int. Conf. on Advanced*, Perth, Australia, pp.836–841, 2010.

[8] G. Pan, Y. Zhang and Z. Wu, "Accelerometer-based gait recognition via voting by signature points", *Electronics Letters*, Vol.45, No.22, pp.1117–U26, 2009.

[9] T. Chau, "A review of analytical techniques for Gait data. Part 1: Fuzzy, statistical and fractal methods", *Gait and Posture*, Vol.13, No.1, pp.49–66, 2001.

[10] M.S. Nixon, T. Tan and R. Chellappa, *Human Identification Based on Gait*, Springer-Verlag, Boston, USA, 2006.

[11] T. Chau, "A review of analytical techniques for Gait data, Part 2: Neural network and wavelet methods", *Gait and Posture*, Vol.13, No.2, pp.102–120, 2001.

[12] C.M. Bishop, *Neural Networks for Pattern Recognition*, Oxford University Press, New York, USA, 1996.

[13] M.F. Moller, "A scaled conjugate-gradient algorithm for fast supervised learning", *Neural Networks*, Vol.6, No.4, pp.525–533, 1993.

SUN Hu was born in Hunan Province in 1986. He is currently a M.S. candidate in Department of Automation, Tsinghua University. His main research interests include biometric identification, pattern recognition, signal processing and data fusion.

YUAN Tao Senior researcher and Director of Tsinghua-Renesas Embedded System Center. His main research interests include biometric identification, embedded system,MEMS measurement system and its application.

LI Xiaopeng was born in 1988. He is currently a M.S. candidate in Department of Automation, Tsinghua University. His main research interests include embedded system,MEMS measurement system and its application.

Hu Yu was born in 1985. He is a Ph.D. candidate in Delft University of Technology, the Netherlands. His main research topic is the control and optimization of intelligent transportation systems.