Curve aligning approach for gait authentication based on a wearable accelerometer

2012 Physiol. Meas. 33 1111

(http://iopscience.iop.org/0967-3334/33/6/1111)

IOP PUBLISHING PHYSIOLOGICAL MEASUREMENT

Physiol. Meas. **33** (2012) 1111–1120 doi:10.1088/0967-3334/33/6/1111

Curve aligning approach for gait authentication based on a wearable accelerometer

Hu Sun and Tao Yuao[1]

Department of Automation, TNList, Tsinghua University, Beijing, People's Republic of China

E-mail: yt@tsinghua.edu.cn

Received 30 December 2011, accepted for publication 25 April 2012
Published 24 May 2012
Online at stacks.iop.org/PM/33/1111

Abstract

Gait authentication based on a wearable accelerometer is a novel biometric which can be used for identity identification, medical rehabilitation and early detection of neurological disorders. The method for matching gait patterns tells heavily on authentication performances. In this paper, curve aligning is introduced as a new method for matching gait patterns and it is compared with correlation and dynamic time warping (DTW). A support vector machine (SVM) is proposed to fuse pattern-matching methods in a decision level. Accelerations collected from ankles of 22 walking subjects are processed for authentications in our experiments. The fusion of curve aligning with backward–forward accelerations and DTW with vertical accelerations promotes authentication performances substantially and consistently. This fusion algorithm is tested repeatedly. Its mean and standard deviation of equal error rates are 0.794% and 0.696%, respectively, whereas among all presented non-fusion algorithms, the best one shows an EER of 3.03%.

Keywords: gait authentication, accelerometer, curve aligning, support vector machine, fusion

(Some figures may appear in colour only in the online journal)

1. Introduction

Gait authentication based on a wearable accelerometer is a newly emerged biometric which uses accelerations to identify people. Compared with password, ID card and other biometric techniques such as voice- and video-based gait, accelerometer-based gait has its advantages. It cannot be lost or stolen; it is sound-invariant, lighting-invariant and viewpoint-invariant.

[1] Author to whom any correspondence should be addressed.

Table 1. A summary of gait authentications based on wearable accelerometer.

Study	Method(s)	Location(s) of accelerometers	Number of subjects	EER(s) (%)
Ailisto *et al* (2005)	Correlation	Waist	36	6.4
Mantyjarvi *et al* (2005)	Correlation, FFT, histogram, higher order moments	Waist	36	7–19
Vildjiounaite *et al* (2006)	Correlation, FFT	Hand, breast pocket, hip pocket	31	13.7–17.2
Gafurov *et al* (2006)	Histogram, cycle length	Ankle	21	5– 9
Gafurov *et al* (2007)	Absolute distance, correlation, histogram, higher order moments	Trousers pocket	50	7.3–20
Liu *et al* (2007)	DTW	Waist	35	6.7
Gafurov *et al* (2010)	Euclidean distance	Ankle	30	1.6–21.4
Li *et al* (2011)	DTW	Ankle	22	3.3

Thanks to developments of micro-electro-mechanical systems and micro-processors, a system of accelerometer-based gait authentication can be easily integrated into smart phones, multi-media players, digital cameras and all kinds of other personal digital assistances (PDAs). It can cooperate with other systems such as password, ID card, fingerprint, etc or replace them to ensure the safe use of these digital devices. What's more, technologies of accelerometer-based gait authentication can be applied to evaluate people's gait for medical purposes, such as gait correction and early detection of neurological disorders, where voice and fingerprint can hardly help.

Early medical studies (Murray *et al* 1964) have proved that human gait contains the information of identity. And psychophysical studies (Johannson 1973) reveal the feasibility to identify such information. The first research paper on accelerometer-based gait authentication is proposed by Ailisto *et al* (2005). Correlation is used as a method for matching gait patterns. An EER (a detailed introduction for calculating EER is presented by Vildjiounaite *et al* 2006) of 6.4% is achieved in tentative experiments with 36 subjects. Table 1 summarizes the recent studies on accelerometer-based gait authentication. Allocations of wearable accelerometers, methods for matching gait patterns, size of experimental data and authentication performances are listed in the table. But some special procedures of processing accelerations are not. For example in the work of Gafurov *et al* (2006), accelerations in backward–forward, vertical and lateral directions are combined before authentication, whereas in a majority of other studies, accelerations in different directions are used for authentication separately. Li *et al* (2011) extract feature points from accelerations to obtain to-be-matched patterns (also mentioned as feature vectors), whereas most others treat accelerations as to-be-matched patterns directly. Numerically, Gafurov *et al* (2010) have reached a lowest EER of 1.6%, which is an encouraging result.

All the studies mentioned above use only one pattern-matching method during an authentication; thus, a good performance can hardly be guaranteed. The EER of 1.6% (Gafurov *et al* 2010) is restricted to some specific conditions, even including what types of shoes subjects wear. Generally speaking, each pattern-matching method may have some disadvantages or limitations. For example, correlation is insensitive to difference in absolute values which means that correlation can hardly distinguish two signals with similar outlines but quite different absolute values. And Euclidean distance is insensitive to difference in relative values

which may lead to the following situation: let $\mathbf{a}$,β,γ denote three normalized vectors whose components consist of a constant value, ascending values and descending values, respectively. The Euclidean distances between $\mathbf{a}$ and β, $\mathbf{a}$ and γ, and β and γ may be the same but β and γ are just opposite in relative values. So we come to the idea of putting different methods for matching gait patterns together so that they can complement each other to ensure a steadily good performance.

In this paper, curve aligning is introduced for matching gait patterns and a support vector machine (SVM) is proposed to promote authentication performances by fusing pattern-matching methods. We collected gait accelerations from subjects' ankles with a triaxial accelerometer. It turns out that the fusion of curve aligning with backward–forward accelerations and DTW with vertical accelerations promotes authentication performances substantially and consistently. The proposed fusion algorithm is not only a good algorithm for gait authentication based on wearable accelerometers, but it also provides a way of fusion which may be useful in other areas. The rest of this paper is organized as follows. Section 2 proposes the curve aligning method and how our authentications are carried out. Section 3 shows the results. Section 4 discusses some authentication details, main features and potential applications on our proposed algorithms. Section 5 concludes this paper.

2. Materials and methods

2.1. Curve aligning: a new method for matching gait patterns

Curve aligning is a smart approach to find the optimal correspondence or alignment between 2D curves. It has been successfully applied in object recognition based on silhouettes (Ayache and Faugeras 1986, Gdalyahu and Weinshall 1999), handwritten character recognition (Connell and Jain 1998, Wirtz 1997), tracking (Cohen *et al* 1992), etc. In this paper, the theoretical background and programming of curve aligning are based on Sebastian *et al* (2003).

2.1.1. Theoretical background of curve aligning. Let $C|_{[d_1,d_2]}$ denote the portion of the curve C from d_1 to d_2, and $\bar{C}|_{[\bar{d}_1,\bar{d}_2]}$ denote the portion of the curve $\bar{C}$ from $\bar{d}_1$ to $\bar{d}_2$. And let $g|_{([d_1,d_2],[\bar{d}_1,\bar{d}_2])}$ denote an alignment between $C|_{[d_1,d_2]}$ and $\bar{C}|_{[\bar{d}_1,\bar{d}_2]}$ with restrictions $g(d_1) = \bar{d}_1$ and $g(d_2) = \bar{d}_2$, which indicate that the start points and the endpoints of the two curves are aligned together, respectively. Define a measure $\mu[g]|_{([d_1,d_2],[\bar{d}_1,\bar{d}_2])}$ to denote the cost of the alignment of $g|_{([d_1,d_2],[\bar{d}_1,\bar{d}_2])}$.

Consider two infinitesimal curve segments $C|_{[A,B]}$ and $\bar{C}|_{[\bar{A},\bar{B}]}$ with lengths $\mathrm{d}s$ and $\mathrm{d}\bar{s}$ and tangent angles $\mathrm{d}\theta$ and $\mathrm{d}\bar{\theta}$ at the endpoints. Their start points A and $\bar{A}$, and their tangents at start points are aligned. As a result, the cost of matching the infinitesimal curve segments is the degree by which the endpoints differ. See figure 1. In this paper, the cost is formulated as

$$\mu[g]|_{([A,B],[\bar{A},\bar{B}])} = |\mathrm{d}\bar{s} - \mathrm{d}s| + |\mathrm{d}\bar{\theta} - \mathrm{d}\theta| \tag{1}$$

where $|\mathrm{d}\bar{s} - \mathrm{d}s|$ penalizes 'stretching' and $|\mathrm{d}\bar{\theta} - \mathrm{d}\theta|$ penalizes 'bending'. Therefore,

$$\mu[g]|_{([d_1,d_2],[\bar{d}_1,\bar{d}_2])} = \int_{C|_{[d_1,d_2]}} (|\mathrm{d}\bar{s} - \mathrm{d}s| + |\mathrm{d}\bar{\theta} - \mathrm{d}\theta|)\mathrm{d}s. \tag{2}$$

The optimal alignment is defined as

$$\tilde{g} = \arg\min_{g} \mu[g]|_{([d_1,d_2],[\bar{d}_1,\bar{d}_2])}. \tag{3}$$

And the minimum cost $\mu[\tilde{g}]|_{([d_1,d_2],[\bar{d}_1,\bar{d}_2])}$ is defined as an editor distance between $C|_{[d_1,d_2]}$ and $\bar{C}|_{[\bar{d}_1,\bar{d}_2]}$. So the editor distance can be a measure of similarity between curves. A smaller editor distance indicates that the corresponding curves are more similar.

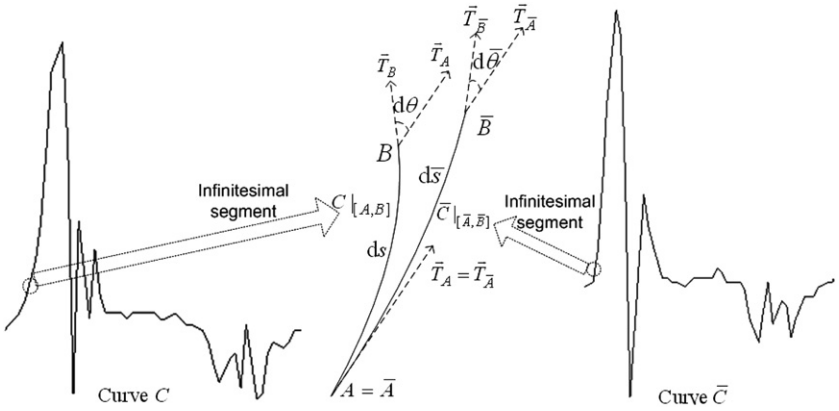

Figure 1. Illustration of curve aligning. $C|_{[A,B]}$, $\bar{C}|_{[\bar{A},\bar{B}]}$ are two infinitesimal curve segments with lengths ds and d$\bar{s}$ respectively; their start points and tangents at start are overlapped ($\bar{A} = A$, $\vec{T}_{\bar{A}} = \vec{T}_A$); the cost of aligning the two infinitesimal segments is defined by $|d\bar{s} - ds| + |d\bar{\theta} - d\theta|$.

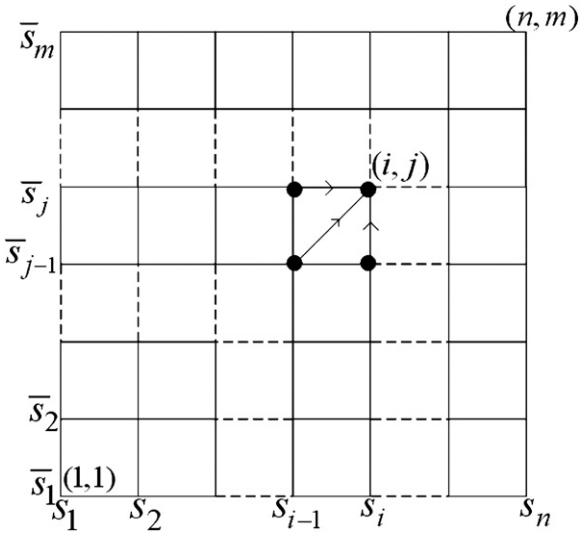

Figure 2. Illustration of a dynamic algorithm for estimating the editor distance between C and $\bar{C}$. The coordinates $s_1, s_2, \ldots, s_n$ and $\bar{s}_1, \bar{s}_2, \ldots, \bar{s}_m$ are discrete samples of C and $\bar{C}$, respectively; the entry at (i, j) represents $\delta(i, j)$; the cost at (i, j)−$\varepsilon(i, j)$ is the sum of $\delta(i, j)$ and the minimum value of $\varepsilon(i-1, j)$, $\varepsilon(i, j-1)$ and $\varepsilon(i-1, j-1)$; the alignment starts at (1, 1) and ends at (n, m).

2.1.2. Programming of curve aligning. In the above descriptions C and $\bar{C}$ are continuous curves. They are sampled for programming. Let $(s_1, s_2, \ldots, s_n)$ and $(\bar{s}_1, \bar{s}_2, \ldots, \bar{s}_m)$ denote the sample points of C and $\bar{C}$. In our experiments, $(s_1, s_2, \ldots, s_n)$ and $(\bar{s}_1, \bar{s}_2, \ldots, \bar{s}_m)$ are two to-be-matched gait patterns from gait accelerations.

Let $\varepsilon(i, j)$ denote the cost of aligning the curve segments $C|_{[s_1, s_i]}$ and $\bar{C}|_{[\bar{s}_1, \bar{s}_j]}$, and $\delta(i, j)$ denote the cost of aligning sub-segments $C|_{[s_{i-1}, s_i]}$ and $\bar{C}|_{[\bar{s}_{j-1}, \bar{s}_j]}$, which are treated as two infinitesimal curve segments as depicted in figure 1. A dynamic algorithm for calculating $\varepsilon(i, j)$ (see figure 2) can be expressed as

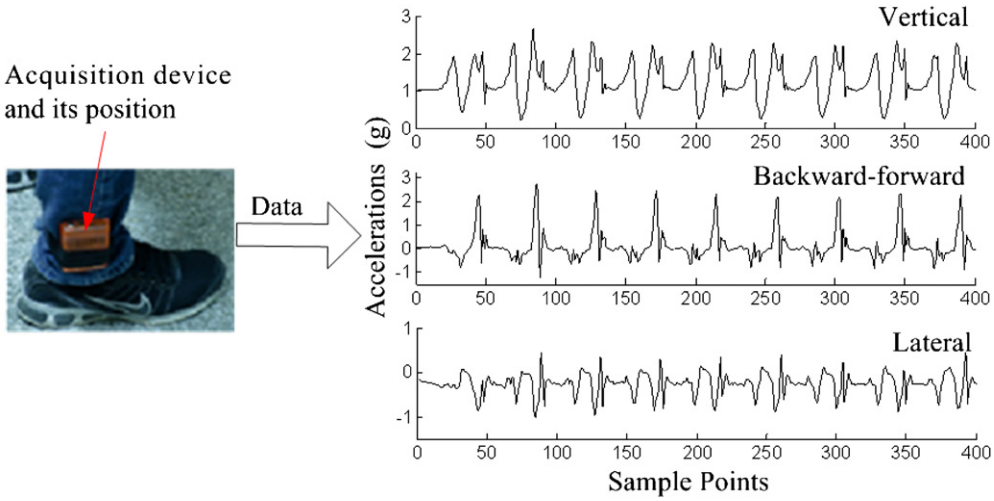

Figure 3. Acquisition and display of gait accelerations in three directions.

$$\varepsilon(i, j) = \delta(i, j) + \min[\varepsilon(i-1, j), \varepsilon(i, j-1), \varepsilon(i-1, j-1)] \tag{4}$$

where $\delta(i, j)$ is estimated according to equation (1). In order to make it feasible to calculate curve lengths and tangent angles, two third-order polynomials are used to fit (s_{i-1}, s_i, s_{i+1}) and $(\bar{s}_{j-1}, \bar{s}_j, \ldots, \bar{s}_{j+1})$, respectively.

The final result $\varepsilon_A(n, m)$ is an estimation of the editor distance between C and $\bar{C}$.

2.2. Authentication details in our experiments

2.2.1. Data acquisition. The device for data acquisition is designed by us ourselves. It includes a microcontroller (uPD78F0485), a triaxial accelerometer (ADXL345), a flash chip (K9K8G08U0A) and some other units. The device has a size of 85 mm × 55 mm × 25 mm and weighs 46 g. It is attached to subjects' right ankles and works at a sampling frequency of 50 Hz. See figure 3. Accelerations in backward–forward, vertical and lateral directions are collected by the accelerometer and stored in the flash chip first. Then the data are transferred to a personal computer through a USB cable.

The total number of subjects is 22, out of which 16 are males and 6 are females: 23–52 years old, 1.62–1.83 cm tall, 46–71 kg heavy. Each subject was told to walk four times their normal speed on a flat surface about 20 m long; therefore, four gait sequences were acquired from every one.

2.2.2. Non-fusion authentications. When we address two pieces of accelerations in the same direction, the purpose of authentication is to decide whether or not they come from the same subject. Procedures of preprocessing each piece of accelerations include mean removal, filtering, cycle division, etc. Note that a low-pass Butterworth filter with a cut-off frequency of 20 Hz is employed during filtering. In our experiments, each step is treated as a gait cycle. Four serial gait cycles in the middle of each piece are extracted at the end of cycle division. All accelerations in one gait cycle compose a gait pattern; therefore, we obtain four gait patterns from each piece of accelerations. Then every two-gait patterns from different pieces are matched by curve aligning, correlation (Ailisto *et al* 2005) and DTW (Li *et al*

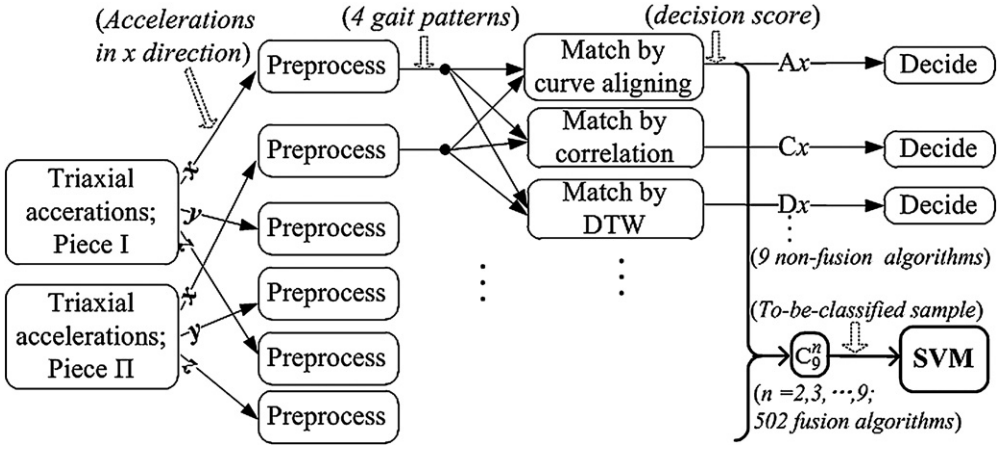

Figure 4. Diagram of gait authentications. Accelerations in different directions are processed separately and the four gait patterns are four processed gait cycles; a decision score is produced by matching one set of four gait patterns with another; the three methods for matching gait patterns together with the three directions (x, y and z) of accelerations lead to nine different non-fusion algorithms, which are represented by Ax, Cx, Dx and so on; a to-be-classified sample is a combination of decision scores corresponding to the nine non-fusion algorithms.

2010). Thus 16 matching scores are produced. In the case of curve aligning and DTW, a low score indicates a high level of similarity; thus, the minimum score is chosen as a final decision score. Inversely in the case of correlation, a high score indicates a high level of similarity; thus, the maximum score is chosen as a final decision score. Figure 4 depicts our methods.

In authentications with non-fusion algorithms, the decision score is compared with a threshold directly. For the sake of convenience, the non-fusion algorithms are denoted by letter combinations Ax, Cx, Dx, Ay, Cy, Dy, Az, Cz and Dz, where the uppercase letters A, C and D correspond to curve aligning, correlation and DTW, respectively, and the lowercase letters x, y and z stand for vertical, backward–forward and lateral accelerations, respectively. For example, Ax denotes the non-fusion algorithm with curve aligning using vertical accelerations.

2.2.3. Fusion authentications with the SVM. The SVM is a powerful solution to nonlinear classification problems (Shigeo 2005). And it has been successfully applied in activity identification with wearable sensors (Preece *et al* 2009, Sprager and Zazula 2009), which is closely related to gait authentication based on a wearable accelerometer.

A classical nonlinear SVM classifier, with a cubic polynomial as its kernel function, is used in our authentications. Detailed knowledge on the SVM is presented in Cortes and Vapnik (1995) and Shigeo (2005). In our fusion algorithms, the classifier's inputs are to-be-classified samples whose components are decision scores from the non-fusion algorithms (see figure 4). Its outputs are binary values$\{-1, +1\}$, which indicate the authentication results. By changing the threshold in the classifier's output function, we are able to evaluate the fusion performance in terms of EER.

Note. Denotations of the included non-fusion algorithms are integrated to represent the fusion algorithm. For example, AxCx represents the fusion of Ax and Cx with the SVM.

Table 2. Performances of non-fusion algorithms (EERs,%). A, C, D and *x*, *y*, *z* in the parentheses represent the three methods and the three directions, respectively. Every intersection indicates a non-fusion algorithm; for example, the upper-left corner (9.09) corresponds to the algorithm A*x* and the lower-right corner (5.30) corresponds to the algorithm D*z*.

	Directions of accelerations that are used for authentication		
Methods for matching gait patterns	Vertical (*x*)	Backward–forward (*y*)	Lateral (*z*)
Curve aligning (A)	9.09	5.36	9.09
Correlation (C)	7.63	8.52	6.06
DTW (D)	3.03	6.82	5.30

3. Results

3.1. Non-fusion algorithms

As mentioned above, the total number of subjects is 22 and 4 gait sequences are acquired from each subject. Thus in each experiment designed to test a non-fusion algorithm, there are $132(C_4^2 \times 22 = 132)$ genuine trials and $3696(C_{22}^2 \times C_4^1 \times C_4^1 = 3696)$ imposter trials. EER is used as the evaluation criterion. The results are shown in table 2.

Curve aligning has the lowest EER (5.36%) when backward–forward accelerations are processed for authentication, which says that curve aligning is a better choice than correlation and DTW when backward–forward accelerations from one's ankle are used for authentication. However its EER is the highest when vertical or lateral accelerations are processed for authentication (both 9.09%). This indicates that curve aligning is sensitive to directions of accelerations.

3.2. Fusion algorithms with the SVM

We have tried all possible combinations of the 9 non-fusion algorithms; thus, a total number of $502(C_9^2 + C_9^3 + C_9^4 + C_9^5 + C_9^6 + C_9^7 + C_9^8 + C_9^9 = 502)$ fusion algorithms are compared with each other. Twofold cross validation is applied to evaluate each of the fusion algorithms. Experiments are carried out as follows: the 22 subjects are randomly split into two 11-subject groups, namely G_1 and G_2; the designed SVM is trained and tested twice—each time one of the two groups is used for training and the other is used for testing; thus, two EER values are yielded; the above steps are repeated 100 times; finally a mean EER and a standard deviation are worked out for each fusion algorithm. Figure 5 shows the process. Note that there are $66(C_4^2 \times 11 = 66)$ genuine trials and 880 $(C_{11}^2 \times C_4^1 \times C_4^1 = 880)$ imposter trials in every training and testing data set.

Table 3 lists the top 20 fusion algorithms, where mean EERs are in ascending order. In fact the 20 mean EERs do not differ much with one other and the deviations are relatively large, so the ranks are not exactly the same in different tests. But according to our repeated experiments the following results do not change: A*y* and D*x* are involved in all the top 20 fusion algorithms, which indicates that the 'cooperation' of curve aligning and DTW is a key factor to ensure a good fusion performance; the fusion algorithm—A*y*D*x* (the fusion of curve aligning with backward–forward accelerations and DTW with vertical accelerations)—has the lowest EER; its standard deviation is always in the top 3 of the smallest ones; A*y*D*x* is the only fusion of two non-fusion algorithms in the table, which says it is simpler than any other fusion algorithm in the top 20.

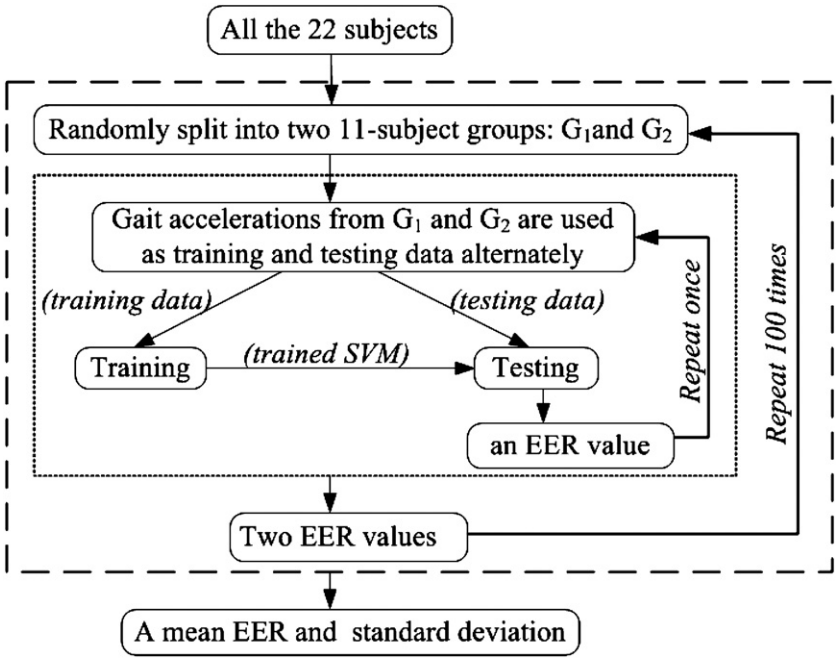

Figure 5. Illustration of how a fusion algorithm is evaluated with twofold cross validation. The experimental data come from 22 subjects.

Table 3. Top 20 fusion algorithms with EER results which are expressed in the form of *mean* ± *standard deviation*, in percentages.

Ranks	Fusion algorithms	EER results	Ranks	Fusion algorithms	EER results
1	A*y*D*x*	0.794 ± 0.696	11	A*x*A*y*D*x*D*z*	1.07 ± 0.776
2	A*x*A*y*A*z*C*z*D*x*	0.956 ± 0.814	12	A*x*A*y*A*z*C*y*D*x*	1.09 ± 0.874
3	A*y*A*z*D*x*	0.963 ± 0.847	13	A*x*A*y*C*y*D*x*D*z*	1.09 ± 0.959
4	A*x*A*y*A*z*D*x*	0.980 ± 0.732	14	A*y*C*z*D*x*	1.10 ± 1.05
5	A*x*A*y*C*z*D*x*D*z*	1.00 ± 0.950	15	A*y*A*z*D*x*D*z*	1.12 ± 0.843
6	A*x*A*y*A*z*C*y*D*x*D*z*	1.00 ± 0.999	16	A*x*A*y*A*z*C*z*D*x*D*z*	1.12 ± 1.24
7	A*x*A*y*D*x*	1.01 ± 0.736	17	A*x*A*y*A*z*C*y*D*x*D*y*D*z*	1.13 ± 0.897
8	A*y*D*x*D*z*	1.04 ± 0.815	18	A*x*A*y*C*x*D*x*	1.16 ± 0.906
9	A*x*A*y*A*z*D*x*D*z*	1.05 ± 0.955	19	A*x*A*y*A*z*D*x*D*y*D*z*	1.16 ± 1.03
10	A*y*C*x*D*x*D*z*	1.07 ± 0.951	20	A*x*A*y*A*z*C*x*C*y*D*x*D*z*	1.16 ± 0.850

On the other hand, among all presented non-fusion algorithms in table 2, the best one (D*x*) has an EER of 3.03%, which is much higher than 0.794%. It is obvious that A*y*D*x* promotes authentication performances on a large scale.

4. Discussion

4.1. Scales about curve aligning

To obtain a good performance, accelerations are in gravity acceleration and time is in seconds during the computation of editor distance. Usually different scales will make 'stretching' and

'bending' costs differ in both absolute values and relative values. Thus the authentication is not invariant to scales. We tried to set the acceleration scale to (gravity acceleration)$\times 10^{-3}$, but performances of curve aligning dropped dramatically in our experiments. So the choice of scales does matter. A general ideal is that 'stretching' and 'bending' costs would not differ too much at a suitable choice. If they differ too much, it can be approximated that the corresponding editor distance contains only the greater item, 'stretching' or 'bending' costs.

4.2. Installation errors of wearable accelerometers

Being sensitive to acceleration directions is the main shortcoming of curve aligning. Therefore, installation errors of wearable accelerometers must be taken into account in practical applications. How to compensate orientation and location errors is beyond the scope of this paper. Hopefully there have been effective methods to deal with this issue (Thiemjarus 2010, Jiang *et al* 2011).

4.3. Imbalance between genuine trials and imposter trials during the training for the SVM

There are 66 genuine trials in our training set whereas the number of imposter trials is 880. The two trials are largely unbalanced. When we use all the data directly, the optimization problem in the training process for the SVM becomes rather challenging. More seriously, the trained SVM performs poorly in the test set. To solve this unbalance problem, we choose only 66 of 880 imposter trials, randomly. Thus 814 imposter trials are discarded. How to make full use of the training data is a topic that requires further exploring.

4.4. From matching scores to a decision score

There is no doubt that the methods for matching gait patterns (curve aligning, correlation and DTW) play an important role in authentications. Meanwhile some other processes matter a lot. For example every time we match two pieces of accelerations, four gait patterns are extracted from each piece and then 16 matching scores are produced out of a complete combination. In the case of correlation, the maximum of the 16 matching scores is chosen as a decision score, whereas in the case of curve aligning and DTW, the minimum is chosen. In fact we have explored a number of other choices such as the mean of the 16 matching score, the mean of the maximum (or minimum) 8 (or 4, or 2), etc. None of them outperforms our final choice.

4.5. Main features and potential applications

Compared with other studies of accelerometer-based gait authentications, the most significant superiority of A*y*D*x* is its low EER. But A*y*D*x* has a high computational complexity due to its middle steps of curve aligning and SVM training. However thanks to the development of micro-processors, computations would not be a problem in most cases. Therefore the mentioned potential applications—identity identification, medical rehabilitation and early detection of neurological disorders—are all feasible according to the achieved performance.

5. Conclusion

This paper proposes a novel method for pattern matching in accelerometer-based gait authentication—curve aligning. It outperforms correlation and DTW when backward–forward accelerations from one's ankle are used for authentication. Furthermore, the SVM is presented to fuse different methods for matching gait patterns. The mean EER and standard deviation

of A*y*D*x* (the fusion of curve aligning with backward–forward accelerations and DTW with vertical accelerations) in our experiments are 0.794% and 0.696%, respectively, which indicate an encouraging progress. Meanwhile, the results suggest that when applied to proper gait accelerations, curve aligning and DTW would complement each other effectively with the help of the SVM.

References

Ailisto H, Lindholm M, Mantyjarvi J, Vildjiounaite E and Makela S M 2005 Identifying people from gait patterns with accelerometers *Proc. SPIE* **5779** pp 7–14

Ayache N and Faugeras O D 1986 A new approach for the recognition and positioning of two-dimensional objects *IEEE Trans. Pattern Anal. Mach. Intell.* **8** 44–54

Cohen I, Ayache N and Sulger P 1992 Tracking points on deformable objects using curvature information *Computer Vision—ECCV'92 Lecture Notes in Computer Science (588)* (Berlin: Springer) pp 458–66

Connell S D and Jain A K 1998 Learning prototypes for on-line handwritten digits *Int. Conf. on Pattern Recognition* ed A K Jain *et al* (Los Alamitos, CA: IEEE Computer Society Press) pp 182–4

Cortes C and Vapnik V 1995 Support-vector networks *Mach. Learn.* **20** 273–97

Gafurov D, Helkala K and Sondrol T 2006 Gait recognition using acceleration from MEMS *Proc. 1st Int. Conf. on Availability, Reliability and Security* pp 432–7

Gafurov D, Snekkenes E and Bours P 2007 Gait authentication and identification using wearable accelerometer sensor *Proc. 2007 IEEE Workshop on Automatic Identification Advanced Technologies* pp 220–5

Gafurov D, Snekkenes E and Bours P 2010 Improved gait recognition performance using cycle matching *Proc. 24th IEEE Int. Conf. on Advanced Information Networking and Applications Workshops* pp 836–41

Gdalyahu Y and Weinshall D 1999 Flexible syntactic matching of curves and its application to automatic hierarchical classification of silhouettes *IEEE Trans. Pattern Anal. Mach. Intell.* **21** 1312–28

Jiang M, Shang H, Wang Z L, Li H Y and Wang Y C 2011 A method to deal with installation errors of wearable accelerometers for human activity recognition *Physiol. Meas.* **32** 347–58

Johannson G 1973 Visual perception of biological motion and a model for its analysis *Percept. Psychopsys.* **14** 201–11

Li Y X, Wang X and Qiao F 2011 Gait authentication based on acceleration signals of ankle *Chin. J. Electron.* **20** 447–51

Liu R, Duan Z, Zhou J and Liu M 2007 Identification of individual walking patterns using gait acceleration *Proc. 1st Int. Conf. on Bioinformatics and Biomedical Engineering* pp 543–46

Mantyjarvi J, Lindholm M, Vildjiounaite E, Makela S M and Ailisto H 2005 Identifying users of portable devices from gait pattern with accelerometers *Proc. Int. Conf. on Acoustics, Speech and Signal Processing* pp 973–6

Murray M P, Drought A B and Kory R C 1964 Walking patterns of normal men *J. Bone Joint Surg.* **46** 335–60

Preece S J, Goulermas J Y, Kenney L P J, Howard D, Meijer K and Crompton R 2009 Activity identification using body-mounted sensors—a review of classification techniques *Physiol. Meas.* **30** R1–33

Sebastian T B, Klein P N and Kimia B B 2003 On aligning curves *IEEE Trans. Pattern Anal. Mach. Intell.* **25** 116–22

Shigeo A 2005 *Support Vector Machines for Pattern Classification* (London: Springer)

Sprager S and Zazula D 2009 A cumulant-based method for gait identification using accelerometer data with principal component analysis and support vector machine *WSEAS Trans. Signal Process.* **5** 369–78

Thiemjarus S 2010 A device-orientation independent method for activity recognition *Proc. 2010 Int. Conf. on Body Sensor Networks* pp 19–23

Vildjiounaite E, Makela S M, Lindholm M, Riihimaki R, Kyllonen V, Mantyjarvi J and Ailisto H 2006 Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices *Proc.4th Int. Conf. on Pervasive Computing* pp 187–20

Wirtz B 1997 Average prototypes for stroke-based signature verification *Proc. 4th Int. Conf. on Document Analysis and Recognition* pp 268–72