A Smart phone Identification Method Based on Gesture

Di XU[1], Quan ZHANG[2]

[1]*School of Electronic Science and Engineering, National University of Defense Technology, China*
[2]*School of Electronic Science and Engineering, National University of Defense Technology, China*

Abstract. In order to promote the practicality of smart phone identification based on gesture, we introduce weighted morphological characteristics and early termination of authentication into dynamic time warping (DTW) algorithm, which based on characteristic moving data captured by in-built accelerometer and gyroscopes, and put forward an effective identification algorithm (ME-DTW) for smartphone. The algorithm controls the contribution made by the difference between the latitudes to the total Euclidean distance by smartphone morphological characteristics. It also introduces restricted areas touch trigger gesture acquisition scheme and authentication gesture length selection scheme based on normal distribution, which effectively improve the identification accuracy and efficiency. Experimental results show that: when others imitate gestures attack false acceptance rate tends to 0%, the personal identification false rejection rate remained at 3.29%, which can meet most practical security needs

1. Introduction

With the development of mobile information technology, smart phones are widely used to manage personal information, mobile payments, etc. as data processing terminals. These applications require high smart phone security, because the loss and disclosure of user privacy information will bring great security risk. Thus a more flexible, safer identification mechanism on the smart phone has become a hot issue of common concern.

Subscriber identity is verifying the legal status of the users before they enter the system or an application. It prevents the system from abusing by illegal users and privacy information from leaking. The traditional identification methods are insecure, including password, PIN-code, etc., which may be stolen or cracked easily. Biometrics complement or substitute the traditional methods which benefits from its features of safety, reliability and convenience. However, current biometric identification methods, such as face recognition [1], fingerprint identification [2], iris recognition [3] and handwritten signatures [4], have the drawbacks of requiring high cost of technology or specific hardware, or being affected by the surrounding environment easily. Meanwhile, the face, fingerprint, iris and signature are significant features that determine someone uniquely and cannot be changed or replaced anymore. The leak of these features would cause irreversible identity fake threat. This article puts forward a gesture-based identification method using characteristic moving data captured by in-built accelerometer and gyroscope. This method uses biometrics to ensure the safety and avoid the leak of privacy features.

Currently, smart phones are generally equipped with 3-axis accelerometers and 3-axis gyroscopes, with the advantages of low price, high sensitivity, small size and low power consumption. Gesture-based identification means that the users hold the smart phones in hand and make signatures in air, meanwhile the in-built accelerometer and gyroscope collect the 3-axis acceleration and rotation data of each time frame, as the biometric characteristic to identify users. Motion gesture trail can be seen as a special form of handwriting in space. Because of individual organisms mechanism structures (muscle length, arm length, etc.) and behavior traits difference, when different people wave the same gesture, the final size, shape and intensity of the tracks will be different. However for the same person it will be relatively stable over a period of time.

At present, international and domestic academics have achieved some results on gesture-based identification. The most representative method are Dynamic Time Warping (DTW) technology and Hidden Markov Models (HMMs) model. In [5] accelerometer data are quantized to reduce the computational burden, noise and extrinsic changes, then similarity between sequences is measured by DTW. In [6] the Sliding Window and Bottom-up (SWAB) method is applied to segment gesture data, and then HMMs is used to identify the user. The identification in smartphones has special request of small samples, timeliness and accuracy. The learning-based methods (such as HMM, etc.) are not suitable resource-constrained smartphones since they need a lot of training samples while the DTW-based method is more suitable for it demands less samples and has good identification effect. However the practical use is restricted by its efficiency and accuracy. In [7] an improved Half

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

Dynamic Time Warping (HDTW) algorithm is put forward to reduce the time complexity effectively. In [8] the bending slope of matching path is constrained to reduce the amount of calculation and improve the efficiency. In [9] the endpoint alignment restriction is canceled to improve the identification accuracy. In order to further increase the efficiency and accuracy of the DTW, we introduce restricted areas touch trigger gesture acquisition scheme to collect accelerometer and gyroscope data. After pre-processing and authentication gesture length selection based on normal distribution, we put forward an effective identification algorithm ME-DTW which combines weighted morphological characteristics and early termination of authentication to measure the similarity. Finally, we compare the matching result with threshold.

The rest of the paper is organized as follows: Section 2 describes the identification procedure. Then, section 3 explains the details of gestures acquisition and pre-processing including smoothing and normalization. The proposed algorithm ME-DTW is detailed in Section 4, in which firstly an overview of traditional DTW algorithm is introduced, followed by detailed descriptions of weighted morphological characteristics, early termination of authentication and pseudo-code of ME-DTW. Section 5 presents experimental results including the pre-processing effect, threshold setting and simulation results by MATLAB. Finally, the conclusions and future work are presented in Section 6.

2. Identification Procedure

The overall identification process takes place in two phases: registration phase and authentication phase, as shown in Fig.1.

In registration phase, a certain number of registration gestures are collected. After pre-processing, an optimal gesture is selected as a template. The selection method is calculating the distance between any two registration gestures, and the template is the one which has the minimum distance with all the other gestures. The threshold is determined by the maximum distance between the template and other registration gestures.

In authentication phase, after pre-processing and length screening, the authentication gesture matches the template using ME-DTW algorithm which is proposed in this paper. Finally, we give the identification result.

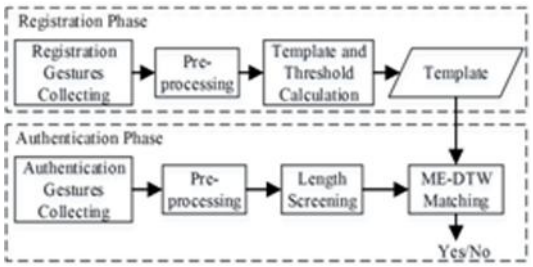


Figure 1. Flowchart of Identification Using Gestures

3. Gesture Acquisition and Pre-Processing

3.1. Gesture Acquisition

In order to improve the security and accuracy of the software, we present a restricted area touch trigger gesture acquisition scheme. The touch trigger refers to that when a user holds the smartphone with his thumb touching the designated area of screen, the sensors begin to collect gesture data. Once the thumb left designated area, the gesture data collection finishes. This way can not only intercept effective period of gesture, save the time and space of endpoint detection, but also make user collect the gesture with almost similar holding manner, so the gestures have a better consistency and it increases the difficulty for attacker to trigger program.

While we touch the screen, the in-built accelerometers and gyroscopes begin to collect the 3-axis acceleration and 3-axis rotation data in every time frame as the original gesture data. The data are stored in a matrix of *n* rows 6 columns, where the stand for the time point, the first three columns represent the changes of accelerometer in 3-axis, and the rest represent the changes of gyroscope in 3-axis. Therefore, a gesture can be represented as

$$A=\begin{bmatrix} a_{x1} & a_{y1} & a_{z1} & g_{x1} & g_{y1} & g_{z1} \\ a_{x2} & a_{y2} & a_{z2} & g_{x2} & g_{y2} & g_{z2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{xn} & a_{yn} & a_{zn} & g_{xn} & g_{yn} & g_{zn} \end{bmatrix} \quad (1)$$

where *a* stands for accelerometer data and g stands for gyroscope data.

3.2 Smoothing

When collecting the data, sensors always suffer from two kinds of noises, one of which is the accuracy of the sensors themselves, the other is tiny shake of the hand. Taking into account of the resource-constrained of the smartphones, we introduce Simple Moving Average (SMA) to smooth the noise. Just from the start point of a gesture, we calculate the average of *m* consecutive sensor data for each incoming data as

$$\begin{aligned} \overline{a}_i &= \left(a_{i-m+1}+a_{i-m+2}+\cdots+a_i\right)/m \\ &= \overline{a}_{i-1}+\left(a_i-a_{i-m}\right)/m \end{aligned} \quad (2)$$

where *m* denotes the window size of the data segment and this paper *m* is set to 5. The processing of the rotation data is similar to this.

3.3 Normalization

In this paper we introduce z-score standardization method to normalize acceleration and rotation data in order to

make them have the same influence in subsequent similarity measure. It is obtained as

$$a'_{di} = \frac{a_{di} - \overline{a}_d}{\sigma a_d}, d = x, y, z \tag{3}$$

$$g'_{di} = \frac{g_{di} - \overline{g}_d}{\sigma g_d}, d = x, y, z \tag{4}$$

where $a'_{xi}, a'_{yi}, a'_{zi}, g'_{xi}, g'_{yi}, g'_{zi}$ stand for the normalized 3-axis acceleration and rotation data at time of, $\overline{a}_x, \overline{a}_y, \overline{a}_z, \overline{g}_x, \overline{g}_y, \overline{g}_z$ stand for the average of the 3-axis acceleration and rotation data and $\sigma a_x, \sigma a_y, \sigma a_z, \sigma g_x, \sigma g_y, \sigma g_z$ stand for the standard deviation respectively.

4 Identification Algorithm ME-DTW

In this paper we propose ME-DTW algorithm which combines weighted morphological characteristics and early termination of authentication to calculate the similarity between the authentication gestures and template. Before that, authentication gesture length should be filtered to reduce calculation.

We introduce an authentication gesture length selection scheme based on normal distribution. For one gesture track, gesture length of the same person will be in a certain range, meanwhile different people will be different.

For *m* registration data, of which lengths are respectively, with length mean value and standard deviation which is defined as

$$\sigma_L = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(L_i - \mu_L)^2} \tag{5}$$

the probability distribution function is defined as

$$\begin{aligned} &P\left(\mu_L - k\sigma_L < L < \mu_L + k\sigma_L\right) \\ &= \Phi\left(k\right) - \Phi\left(-k\right) = 2\Phi\left(k\right) - 1 \end{aligned} \tag{6}$$

Since the normal distribution 3σ criteria that the probability of distribution of values in the interval is 0.9974, the authentic user gestures length are almost entirely contained in the interval. So we can rule out most invalid authentication data to make a preliminary screening.

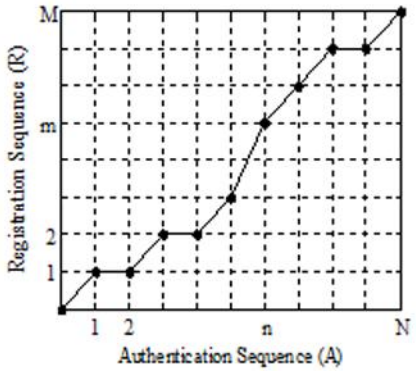


Figure 2.DTW Optimal Path

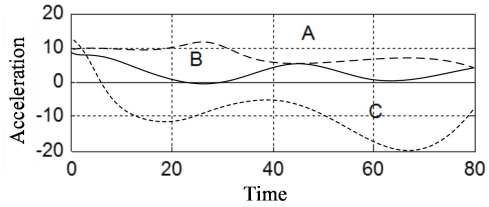


Figure 3.Schematic Diagram of Morphological Weighted Euclidean Distance.

4.1 DTW Algorithm

Dynamic Time Warping is an algorithm that combines time alignment and distance measurement together, with excellent effect on non-linear time normalization. It has been widely utilized in the field of speech recognition [8].

DTW can adjust the correspondence between the different elements of two time series to obtain an optimal matching curved path. Hence it can measure the distance between two time series with different length and obtain a minimum cumulative distance. DTW optimal path seeking is shown in Fig. 2.

When measuring the similarity between registration sequence with the length of *M* and authentication sequence with the length of *N*, we firstly construct a cumulative distance matrix D of. The value stands for accumulated value of the minimum distance distortion of each matching points from to if the and match. In order to control the slope of the match path, we set it in the range of 0 to 2. Theis finally calculated as

$$\begin{aligned} &D\left(i,j\right) = d\left(R_i, A_j\right) + \\ &\min\left(D\left(i,j-1\right), D\left(i-1,j-1\right), D\left(i-2,j-1\right)\right) \end{aligned} \tag{7}$$

where denotes the Euclidean distance between at moment and at moment, which is computed as

$$d\left(R_i, A_j\right) = \sqrt{\Sigma_{k=1}^{6}\left(R_{ik} - A_{jk}\right)^2} \tag{8}$$

Ultimately, the matching path begins at and finishes at, and theis the final shortest cumulative distance between and.

4.2ME-DTW Algorithm

4.2.1Weighted Euclidean distance base on Morphology

In DTW, the Euclidean distance-based similarity measure cannot reflect the trend of the time series. As shown in Fig. 3, the gestures A and B have substantially opposite shape, while gestures B and C have substantially similar shape. However, the distance between the gestures A and B will be less than the distance between the gestures B and C, which does not meet the people's visual and intuitive judgment.

Therefore, we introduce weighted morphological characteristics into DTW. It controls the difference between the latitudes contributing to the total Euclidean distance by morphological characteristics. Hence the morphological differences play a certain role in the similarity metric. For registration and authentication sequence R and, firstly we calculate corresponding slope sequences in each axis. For, the slope of the point in -axis is given as

$$SR_{ik} = R_{ik} - R_{(i-1)k} . \tag{9}$$

The slope can be discretized to as

$$SR'_{ik} = \begin{cases} 1, & SR_{ik} > 0 \\ 0, & SR_{ik} = 0 \\ -1, & SR_{ik} < 0 \end{cases} . \tag{10}$$

It is same to authentication sequence. When and match, and are the discretized slope values in the -axis, so the divergence can be defined as

$$S_{ijk} = \left| SR'_{ik} - SA'_{jk} \right| + 1 . \tag{11}$$

It means if two points of two sequences in current axis have the same morphology, divergence gets the minimum value of 1, and if opposite it gets the maximum value of 3.

The divergence is used as the weighted factor of Euclidean distance as

$$d\left(R_i, A_j\right)' = \sqrt{\Sigma_{k=1}^{6} S_{ijk} \left(R_{ik} - A_{jk}\right)^2} . \tag{12}$$

The greater the morphological difference between two points of two gestures is, the greater the weighting factor will be, so the distance between the matching points will also be greater, which stresses the importance of morphological characteristics to some extent.

In our algorithm, in order to reduce the computational complexity of the algorithm and prevent pathological match that a short segment of one sequence match with a large segment of another sequence, we restrict the distance between two matching points in different sequence. The matching point in the curved path must satisfies $\mathrm{M} / \mathrm{N} \times j - r \le i \le M / N \times j + r$, where is the maximum length difference between the template and the other registration gestures.

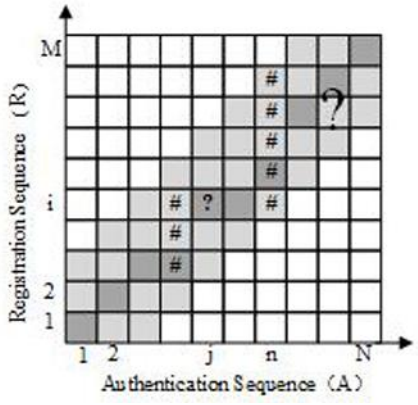


Figure 4. Early Termination of Authentication (If "#"overflow, "?"must overflow)

4.2.2Early termination algorithm

DTW needs to calculate the accumulative distortion values of all the point in limited matching region. In fact, there is no sense to do subsequent calculation when the distortion exceeds a certain threshold. Therefore, we further introduce early termination algorithm. If a column points of authentication gesture in the cumulative distance matrix are greater than the threshold as the column *n* of in Fig. 4, the final shortest cumulative distance must be greater than the threshold, so there is no need to calculate the cumulative distances in following "?" area. The authentication is failure. By this way we can exit calculation process rapidly once the data distortion is large, thereby the calculation is reduced in authentication phase.

Meanwhile, in the column) of in Fig. 4, if ,, are all overflowing when we calculate , the calculation of and can be omitted for must overflow. We assign the maximum value to directly.

4.2.3*ME-DTW algorithm description*

We design ME-DTW based on the above ideas as shown in Algorithm 1. The algorithm uses two arrays of length M to store the current needed cumulative distance matrix column vector whose space complexity limits in.

Row 1 is the screening of the authentication sequence length. If the length meets the requirement, we initialize the cumulative distance vector of based on row 2 to row 12. Then we calculate the cumulative distance per column in the limit match region based on rows 13 to 41. If ,, can be omitted as rows 19 to 22. We use the divergence weighted Euclidean distance to calculate the distance between two points, as shown in rows 24 and 28. If any column of cumulative distance sequence overflow, early termination can be shown in rows 35 to 36. After a column of cumulative distance calculation, we replace the old array by new array and repeated rows13 to 41 to calculate the next column cumulative distance. If there is no intermediate exit, it returns authentication success.

Algorithm 1. ME-DTW algorithm

Input: registration data $R = \{R_i | 1 \le i \le M\}$, authentication data $A = \{A_j | 1 \le j \le N\}$, the maximum difference between registration gestures and template r, authentication sequence length interval $[L_{min}, L_{max}]$, threshold τ;
Output: when optimal matching path cumulative distance is less than the threshold value, return *true*, else return *false*;
1. if$(N < L_{min}) || (N > L_{max})$ return *false*.
2. else new $oldD[\,]$ and $newD[\,]$, initialize oldD[1,…, M] ← ∞, newD[1,… M] ← ∞;
3. $oldD[1] \leftarrow d(R_1, I_1)$;
4. //initialize the cumulative distance sequence of j=1.
5. $j \leftarrow 1$;
6. for $i \leftarrow 2$ to r.
7. if $oldD[i-1] > \tau$, then.
8. $oldD[i] \leftarrow \infty$;
9. else.
10. $oldD[i] \leftarrow oldD[i-1] + d(R_i, A_1)$;
11. endif.
12. endfor.
13. for $j \leftarrow 2$ to N do.
14. $overflow \leftarrow true$;
15. $i_{max} \leftarrow min(M/N * j + r), M)$;
16. $i_{min} \leftarrow max(1, (M/N * j - r))$;
17. for $i \leftarrow i_{min}$ to i_{max}.
18. if i > 2.
19. $v \leftarrow min(oldD[i], oldD[i-1], oldD[i-2])$;
20. //if voverflow, omit the calculation of $D(i,j)$.
21. if $v > \tau$ then.
22. $newD[i] \leftarrow \infty$;
23. //$d(R_i, A_j)'$ is weighted Euclidean distance based on divergence.
24. else $newD[i] \leftarrow v + d(R_i, A_j)'$;
25. elseif i = 1.
26. $newD[i] \leftarrow oldD[i] + d(R_i, A_j)$;
27. elseif i = 2.
28. $newD[i] \leftarrow min(oldD[i], oldD[i-1]) + d(R_i, A_j)'$;
29. endif.
30. if $newD[i] < \tau$ then.
31. $overflow \leftarrow false$;
32. endif.
33. endfor.
34. //early termination if one column overflow.
35. if *overflow* then.
36. return *flase*.
37. else.
38. $oldD[\,] \leftarrow newD[\,]$;
39. $newD[\,] \leftarrow \infty$;
40. endif.
41. endfor.
42. endif.
43. return $oldD[M] \le \tau$.

5 Experiment and Evaluation

5.1Data acquisition and Pre-processing

The gesture-based identification method is designed for usage on smartphones. We choose Samsung N9100 to collect sensor data, because it fulfils the requirements and is available on the market. It came to market in September 2014 with the CPU of Qualcomm snapdragon 805, RAM of 3GB, operating system version of Android 5.0.1 and has built-in accelerometer, gyroscope and linear accelerometer. The linear accelerometer is more suitable for this experience for it can measure the acceleration without gravity.

There are four grades of sensor sampling rates: FASTEST, GAME, NORMAL and UI, of which the sampling rate and power consumption are reduced accordingly. We choose GAME level which can reduce the power dissipation as much as possible without the loss of the gesture information.

False Rejection Rate (FRR) and False Acceptance Rate (FAR) are used to verify the security of the algorithm. FRR represents the possibility of authentic rejection. FAR represents the probability of attacker acceptance. The smaller the FRR and FAR are, the higher the security of the algorithm has. Eight gesture tracks were designed as shown in Fig. 5. The database I is the gestures that collected by author for 10 consecutive days of each track 15 times. At last we obtain a database of 1200 samples to calculate the FRR. The database II is the gestures collected from 5 volunteers for each track 50 times that imitating the author. At last we obtain a database of 2000 samples to calculate the FAR.

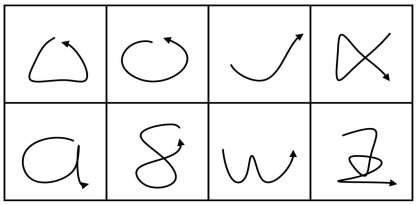


Figure 5.Gestures Track Samples

The original 3-axis acceleration waveform of one of the author gestures is shown in Fig. 6. After smoothing by SMA is shown in Fig. 7 and after normalization is showed in Fig. 8. It can be concluded that SMA smooth the data well and the normalization constraint the size of accelerometer well, thus reduce the calculation and ultimately improve the efficiency.

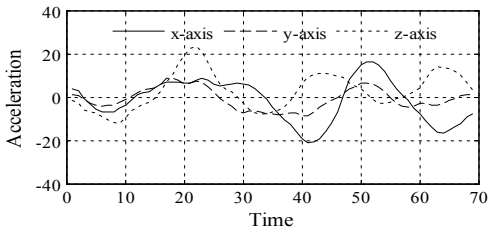


Figure 6. Original Gesture Data

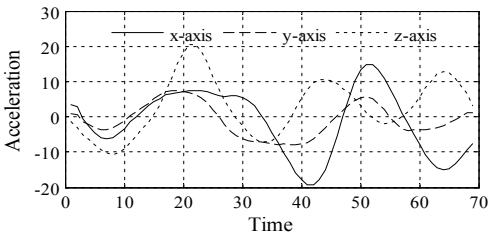


Figure 7. Gesture Data afterDenoising

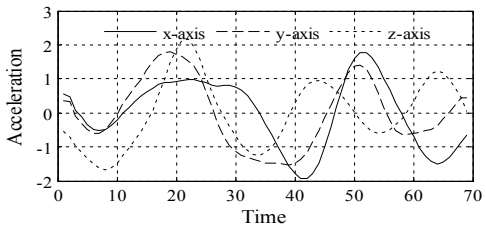
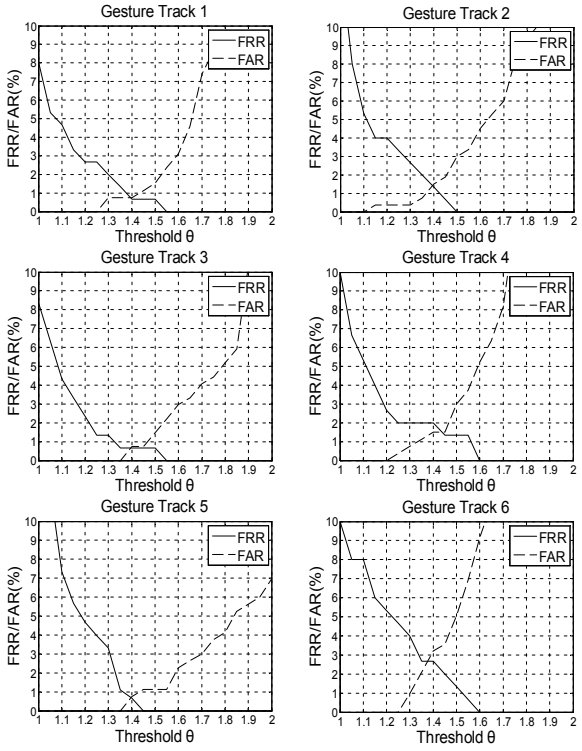


Figure 8. Gesture Data after Normalization

5.2Parameter Setting

We collect 10 registration gestures on account of the actual operation and user experience. The gestures taken by the author on the first day are used as registration gesture samples, wherein the maximum distance between the template and other registration gestures is. The threshold is multiplying a parameter since the one-time collected registration gestures have large similarity. Threshold has great influence on recognition accuracy, so optimizing the is needed. For the eight gesture tracks shown in Fig. 5, FRR and FAR have sensitive changes with different as shown in Fig. 9. When we attach more importance in identification security, the FAR must tends to 0%. The of eight gesture tracks are 1.25, 1.1, 1.35, 1.2, 1.35, 1.25, 1.2, 1.15, concentrating in the vicinity of 1.2. Sois set to 1.2 approximately in the condition of high security requirement. Therefore, when it is used just for general occasions, Equal Error Rate (EER) is used to evaluate the security. When FRR equals to FAR, the θ of corresponding eight gesture tracks are 1.4, 1.4, 1.4, 1.45, 1.4, 1.35, 1.4, 1.45, concentrating in the vicinity of 1.4. So is set to 1.4 approximately in condition of general applications.



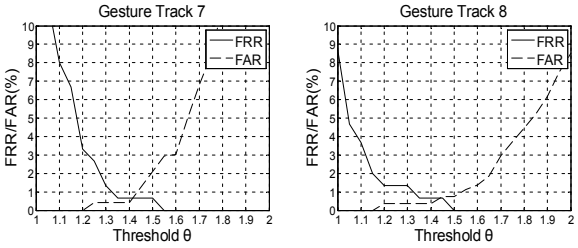


Figure 9. The Relationship between Misjudgment Rate and Threshold of Eight Gesture Tracks

5.3Simulation Analysis

5.3.1Compare ME-DTW with DTW

In the following, the performance of ME-DTW proposed in this paper and traditional DTW are compared. We primarily measure the impact of weighted Euclidean distance to the matching precision. We verify the validity of the two algorithms respectively based on the database I and II. The experimental results are shown in Tab. 1.

Table 1.Compare with ME-DTW and DTW

Gesture track	FRR/%		FAR/%	
	ME-DTW	DTW	ME-DTW	DTW
1	2.67	4.00	0	6.75
2	4.00	3.33	0.38	3.76
3	2.33	1.33	0	3.70
4	2.67	3.33	0	6.72
5	4.67	6.00	0	2.23
6	5.33	5.33	0	5.46
7	3.33	2.00	0	0.37
8	1.33	1.67	0.37	1.35
mean	3.29	3.37	0.09	3.79

As shown in Tab. 1, the mean FRR of ME-DTW is 3.29% and FAR is 0.09%, showing that the ME-DTW has high security.

ME-DTW has little impact on FRR compared with DTW, because for the registration and authentication gestures from one user, the ME-DTW will increase their distance a bit, but the threshold will also have a corresponding increase. However, ME-DTW presents significantly better FAR values of eight gesture tracks in varying degrees, with the mean of 3.70% less. ME-DTW greatly increase the distance between gestures from authentic user and attacker based on the morphological Euclidean distance. In summary, ME-DTW reduce the FAR under the premise of protecting FRR, which improves the security of the identification system.

5.3.2Compare Collecting Gyroscope Data or Not

Most domestic and international surveys about motion gesture-based identification collect acceleration as raw data. In the following, the performance of collecting both accelerometer and gyroscope data and only acceleration data are compared. We use ME-DTW and both database I and II. The results shown in Tab. 2.

As shown in the Tab. 2, when using both accelerometer and gyroscope have nearly equal FRR with only accelerometer, the FAR of the former is greater than the latter in different degrees of eight gesture tracks, with the average increase of 14.86%. The conclusion is that the rotation information as a biological characteristic enlarges the distance between template and authentication gesture especially for the attacker. It makes it possible to distinguish the intruders better, so the rotation information can be an effectively biological characteristic to improve the security of identification system.

Table 2. Compare with Collect Accelerometer and Gyroscopes And Only Accelerometer Data

Gesture track	FRR/%		FAR/%	
	A+G	A	A+G	A
1	2.67	8.67	0	16.4
2	4.00	5.33	0.38	7.89
3	2.33	1.33	0	22.2
4	2.67	2.00	0	13.4
5	4.67	8.67	0	13.3
6	5.33	1.33	0	23.8
7	3.33	0	0	20.4
8	1.33	0	0.37	1.50
mean	3.29	3.41	0.09	14.86

5.3.3ME-DTW Identification Efficiency

In the following, we test the influence of identification efficiency by introducing weighted morphological characteristics and early termination of authentication into DTW. ME-DTW is the algorithm proposed in this article, and M-DTW only introduces weighted morphological characteristics into DTW. MATLAB R2014a is used to simulate the actual running time of the identification. The results are shown in Tab. 3.

Table 3. The Total Time For 270 Times Gesture Identification Of Three Algorithms

Gesture track	ME-DTW/s	M-DTW/s	DTW/s
1	1.123	1.052	0.972
2	0.920	1.072	0.996
3	0.723	0.748	0.670
4	1.120	1.144	1.024
5	1.094	1.151	1.088
6	1.163	1.107	1.027
7	1.035	1.144	1.032
8	1.220	1.601	1.498
mean	1.050	1.127	1.038

As shown in Tab. 3, for ME-DTW, the average time of 270 times gesture identification for eight gesture tracks is 1.050s shown in Fig. 5, while for S-DTW is1.127s and for DTW is 1.038s. S-DTW consume slightly more than DTW due to the introduction of weighted morphological characteristics, while the early termination makes amends on the efficiency that the time cost of ME-DTW is substantially flat with DTW. In order to obtain better system security, ME-DTW sacrifice a small amount of computing time, but is redeemed by the early termination. Finally, the average cost of a single identification is about 3.89ms simulated by MATLAB, so the ME-DTW features good real-time performance.

6. Conclusion and Future Work

In this paper, we presented MD-DTW that controls the difference between the latitudes contributing to the total Euclidean distance by smartphone morphological characteristics to enhance identification accuracy and introduces early termination to guarantee the efficiency. Meanwhile, we proposed restricted areas touch trigger gesture acquisition scheme and authentication gesture length selection scheme to improve the accuracy and efficiency. Experimental results show that: when FAR tends to 0%, the FRR remained at 3.29%, which can meet most practical security needs.

In part of our future work, we plan to expand our dataset by acquiring more samples of gestures per user and also, by increasing the number of users in our databases. Besides, we plan to test the identification in the real smartphone of the time-consuming.

References

1. Ijiri Y, Sakuragi M, Lao S. Security Management for Mobile Devices by Face Recognition[C]// Proceedings of the 7th International Conference on Mobile Data Management. IEEE Computer Society, 2006:49-49.
2. Yong J C, Ong T S, Goh M K O, et al. Integrating Palmprint and Fingerprint for Identity Verification[C]// Proceedings of the 2009 Third International Conference on Network and System Security. IEEE Computer Society, 2009:437-442.
3. Jeong D S, Park H A, Kang R P, et al. Iris recognition in mobile phone based on adaptive gabor filter[J]. Lecture Notes in Computer Science, 2005, 3832:457-463.
4. Argones R E, Alba Castro J L. Online Signature Verification Based on Generative Models[J]. IEEE Transactions on Systems Man & Cybernetics Part B Cybernetics A Publication of the IEEE Systems Man & Cybernetics Society, 2012, 42(4):1231-1242.
5. Liu J, Zhong L, Wickramasuriya J, et al. uWave: Accelerometer-based personalized gesture recognition and its applications[J]. Pervasive & Mobile Computing, 2009, 5(6):657-675.
6. Junker H, Amft O, Lukowicz P, et al. Gesture spotting with body-worn inertial sensors to detect user activities[J]. Pattern Recognition, 2008, 41(6):2010-2024.
7. Zhou Z, Miao M. Gesture Authentication Research Based on Improved Dynamic Time Warping and Mutual Information De-Noising (In Chinese) [J], Chinese Journal of Sensors and Actuators, 2014(8):1070-1076.
8. Hu J, Chen R, Li Z. Discussion of DTW algorithm in speech recognition (In Chinese) [J]. Image

Processing and Multimedia Technology, 2011, 30(3):30-32.
9. Gao H, Cao X, Wang L,et al. An Identity Authentication Method Based on Dynamic Gesture and Its Application in Mobile Phone (In Chinese) [J]. Acta Electronica Sinica, 2014(9):1857-1862.