CrossMark

Quantifying dynamic time warping distance using probabilistic model in verification of dynamic signatures

Rami Al-Hmouz[1] · Witold Pedrycz[1,2] · Khaled Daqrouq[1] · Ali Morfeq[1] ·
Ahmed Al-Hmouz[3]

Abstract One of the multimodal biometric scenarios is realized by considering several features coming from a single biometric entity. Dynamic signature verification has been utilized considering such scenarios. We present a new approach, namely probabilistic dynamic time warping, to verify dynamic signatures where we use dynamic time warping in realizing distance determination in the verification process. Signatures are segmented into several segments, where probability of each segment is quantified with the aid of a relative distance associated with two selected threshold levels. The final decision is achieved by combining all segment probabilities using a Bayes rule. Experiments demonstrate improvement of equal error rate for the proposed approach for the random forgery. The method has been tested on synthetic dataset and two publicly available databases of dynamic signatures, namely SCV2004 and MCYT100.

✉ Rami Al-Hmouz
ralhmouz@kau.edu.sa

Witold Pedrycz
wpedrycz@ualberta.ca

Khaled Daqrouq
kdaqrouq@kau.edu.sa

Ali Morfeq
morfeq@kau.edu.sa

Ahmed Al-Hmouz
aa998@uowmail.edu.au

1 Department of Electrical and Computer Engineering Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia

2 Department of Electrical & Computer Engineering, University of Alberta, Edmonton, AB T6R 2V4, Canada

3 Department of Information Technology, Middle East University, Amman, Jordan

1 Introduction

Biometric recognition is about using anatomical and/or behavioral traits of individuals (Jain et al. 2006). Many applications (i.e., airport security, laptops, automatic teller machine) have adopted human biometrics for access control and security. These biometrics include speech, iris, face (both still and talking one), signature, handwriting, fingerprint, hand, and keystroking. The domain of application is the major factor, which implies a certain selection of the most suitable biometrics. Multimodal biometrics use multiple biometrics of the same or different natures (Ross et al. 2006). Data can be generated by different biometrics. For example, they may include signature and voice. Some data can be generated from the same biometric trait (e.g., those might be multiple images of an iris, scans of the same finger, or multiple speech utterances) (Saylor 2012). The usage of multiple feature techniques where the features are extracted from a single source of biometric falls under the umbrella of multimodal biometrics.

The combination of multiple biometrics leads to the better identification compared to the case when a single biometric is being used. The rationale behind this improvement is that it is unlikely for multiple biometrics to produce the same error in the overall recognition process. Multimodal biometrics help in situations where accuracy becomes essential for applications that require to produce the minimum identification error.

Springer

The multimodality of biometrics calls for an efficient fusion process of the partial results produced by individual components of the system, either with regard to different modalities exploited in the biometric channels or/and different ways of processing data coming from the same biometric modality. From the perspective of fusion process, recalling a large number of alternatives considered in the literature, an interesting and promising direction emerges under the name of meta-recognition (Scheirer et al. 2011). It focuses on an analysis of post-recognition scores to assess the quality of prediction results. The underlying view at the recognition process invokes the extreme value theorem (Scheirer et al. 2010). Hidden Markov models (HMMs) were used in multifeatures-based human activity recognition and in feature reduction encountered in face recognition (Jalal et al. 2017; Elgarrai et al. 2016). In (Srivastava et al. 2016), the biometric system performance of gait and hand vein was improved when combined in a multimodal system.

Signature is a behavioral biometric (not like iris or fingerprint). It is not unique, and in comparison with iris-based biometrics, it is easy to forge. However, signature is commonly acceptable in applications that require low authentication. Signature verification is divided into two categories of approaches, namely static (offline) and dynamic (online). Static signature verification treats signature images as an input to the system and exploits pattern recognition techniques to realize verification. Online signature verification uses signatures captured by tablet devices, while the verification relies on a collection of features of the acquired signature. Such features (properties) used in the online verification include features such as pen position, pressure, elevation angles, azimuth, and others that can be extracted from the captured features such as speed, acceleration, and angle. These features used in the verification process make online signature more difficult to forge compared to the one of the static signatures.

A comparison process involving dynamic time warping (DTW) is realized in the verification process, see (Bellman 1957; Aparna Lakshmi Ratan 2000). DTW leads to the quantification of distance between two vectors of different lengths where these vectors concern the data describing the training templates and the test signature. The distance between training templates and the test signature is determined in order to arrive at the acceptance or rejection decision of the signature. In the detection process, a certain threshold is involved. In (Xiao and Siqi 2017), motion retrieval was obtained using query-based motion feature; the motion was verified using canonical time warping matching. Two thresholds have been investigated in (Jain et al. 2002); local and global thresholds are set for each signer-dependent and signer-independent approaches.

Signature verification-based DTW is considered as a deterministic method. Once a threshold has been set, all the signatures compared with the template and producing the distance falling below this threshold are considered to be genuine signatures; otherwise, they are recognized as forgeries. The threshold level can be varied in order to produce the best performance expressed in terms of the resulting equal error rate (EER).

Online signature verification approaches can be categorized as follows:

1. *Parametric-based approach* global features derived from the signature features are encountered in many signature verification studies, see (Ketabdar et al. 2005; Fierrez-Aguilar et al. 2005). Features such as total signature time duration, number of pen ups, pen down time ratio, average, maximum speed are considered.
2. *Functional-based approach* Here we compare the similarities of signatures that are represented as time functions (Maiorana 2010; Jeong and Jeong 2011). Time-based functions include position trajectory, velocity, acceleration, force, or pressure. This approach showed better performance than when using global features (Fierrez-Aguilar 2005); however, it is subject to some time constraints.
3. *Regional-based method* here signatures are segmented into several regions. Segments related to high, low, medium, and small values of velocity and pressure are identified and investigated in (Cpalka and Zalasiński 2014; Cpalka et al. 2014).

In (Nanni 2006), a method involving global information based on single-class classifiers was presented. The author reported that a fusion of linear programming description (LPD) and principal component analysis description (PCAD) outperforms the work of Parzen window classifier (PWC). In general, DTW approaches were used in functional methods (Jeong et al. 2011; Banko and Janos 2012) and hidden Markov models [HMMs (Fierrez et al. 2007; Humm et al. 2009)] for regional methods.

The motivation behind this study is to improve the online signature EER that involves the DTW approach in the verification process. We propose a probabilistic dynamic time warping (PDTW) that exhibits an ability of verifying online signatures falling in the false rejection and false acceptance domains of verification techniques that consider normal DTW. The strength of PDTW comes from the use of several signature segments (partitions or features) that are present in multimodal scenarios. The distances of multiple segments that are obtained from multiple DTWs are modeled to produce probability scores of accepting or rejecting the signers. The probability of segments is computed according to the distance score relative to the two selected thresholds.

In signature verification that involves DTW distance, we select the best threshold value to maximize EER. In addi-

tion, most of the reported works in the literature that involve signature segments (Cpalka and Zalasiński 2014; Cpalka et al. 2014) select the signature areas that are associated with low, medium, and high pen speed and pressure. In PDTW, each segment distance is modeled in a probabilistic approach based on two selected thresholds. It is essential to stress that, while being promising, so far this approach has not been studied in the literature.

The paper is structured as follows. In Sect. 2, we briefly recall the notion of the dynamic time warping distance. In Sect. 3, we present a new probabilistic dynamic time warping and discuss their properties. Experimental results are reported in Sect. 4. Conclusions are offered in Sect. 4.

2 Dynamic time warping

Each person has a signature that exhibits a certain geometric shape. The features of signature are inherently embedded in the shape and can be extracted using different extraction techniques. The shapes of one's signature could vary significantly being strongly affected by the conditions in which the signature has been collected. Having this in mind, before any further processing, the raw signature data need to be standardized in order to eliminate or reduce such variability. Features of dynamic signature can include the coordinates (x position, y position), which also can vary depending upon different conditions. An illustrative example is displayed in Fig. 1a. To reduce the variability, z-score is one of the most common approaches to alleviate this deficiency.

Let $S = [xy]$ be the features of a given signature of length n recorded in both x and y coordinates. Then the original vectors x, y are standardized in a well-known manner where the successive coordinates of the normalized vector read as follows (see also Fig. 2b):

$$X_i = \frac{x_i - \bar{x}}{\sigma_x}$$
$$Y_i = \frac{y_i - \bar{y}}{\sigma_y}. \tag{1}$$

$i = 1, 2, \ldots, n$. Here $\bar{x}, \sigma_x, \bar{y}, \sigma_y$ are the mean and standard deviation of the coordinates of the original vectors x and y.

DTW generates the distance between two unaligned vectors through the minimization of the accumulated distances of the sequence. Let $S_1 = \{ s_{11}, s_{12}, \ldots s_{1M} \}$ be the template signature of length m and $S_2 = \{s_{21}, s_{22}, \ldots s_{2N} \}$ is the test signature of length n, and both signatures have been formed by vector of features (s) of length n. The distance between S_1 and S_2 is calculated by forming the matrix D of dimensionality ($M + 1 \times N + 1$). The element of $D(M + 1, N + 1)$ is considered as the distance between S_1 and S_2 computed in the form

$$\mathbf{D}(i, j) = \|\mathbf{s}_{1i} - \mathbf{s}_{2j}\| + \min \begin{cases} \mathbf{D}(i, j-1) \\ \mathbf{D}(i-1, j) \\ \mathbf{D}(i-1, j-1) \end{cases} \tag{2}$$

The initialization of D is carried out in the form: $D(1, 1) = 0$, $D(1, j) = \inf$, $D(i, 1) = \inf$. (where practically inf is treated as a large positive number). The distance is the Euclidean one,

$$\|\mathbf{s}_{1i} - \mathbf{s}_{2j}\| = \sqrt{\sum_{k=1}^{n} \left(s_{1i}^k - s_{2j}^k\right)^2} \tag{3}$$

Figure 2 shows the optimal path of D that is computed between a template signature ($n = 128$) and a genuine signature ($m = 139$) Fig. 2a, with $D(129, 140) = 24.06$ and a forgery signature ($m = 195$) Fig. 2b with $D(129, 196) = 43.18$. The optimal path for the genuine signatures is formed of elements of the matrix shown in darker color (black refers to elements having 0 values in D) compared to brighter levels for the forgery signatures.

In an ideal case, the threshold between DTW distances produced for the genuine signatures and forgery signatures can be used as a simple mechanism to discriminate between further genuine and forgery signatures.

It should be noted that the test signatures are tested against a group of template signatures (training). The average distances are computed and compared with some predefined threshold. The values of false rejection rate (*FRR*) and false acceptance rate (*FAR*) depend on the selected threshold value. The *FRR* and *FAR* criteria are in conflict: Moving the threshold in either direction might improve one of the rates but simultaneously may degrade another one.

The best performance expressed in terms of both rates is recorded to calculate the *EER*. Hence, another source of information using the concept of multimodal is essential to improve the performance of the verification system as we explain in the next section.

3 Probabilistic dynamic time warping

It is clearly visible in Fig. 1a that for the same signer there are segments of signatures that are almost identical, while other segments exhibit some variation. The same argument is valid for x and y coordinates in which the variation of signatures over the x coordinates is lower than the variation over the y coordinate, refer to Fig. 1b. We can take advantage of this in forming a classification mechanism. Signatures can be partitioned into segments, each segment is verified individually, and a final decision is taken based on all segment decisions. The essence of this process is shown in Fig. 3.

In order to combine all segment decisions to form the final decision, each distance of DTW for each segment is modeled
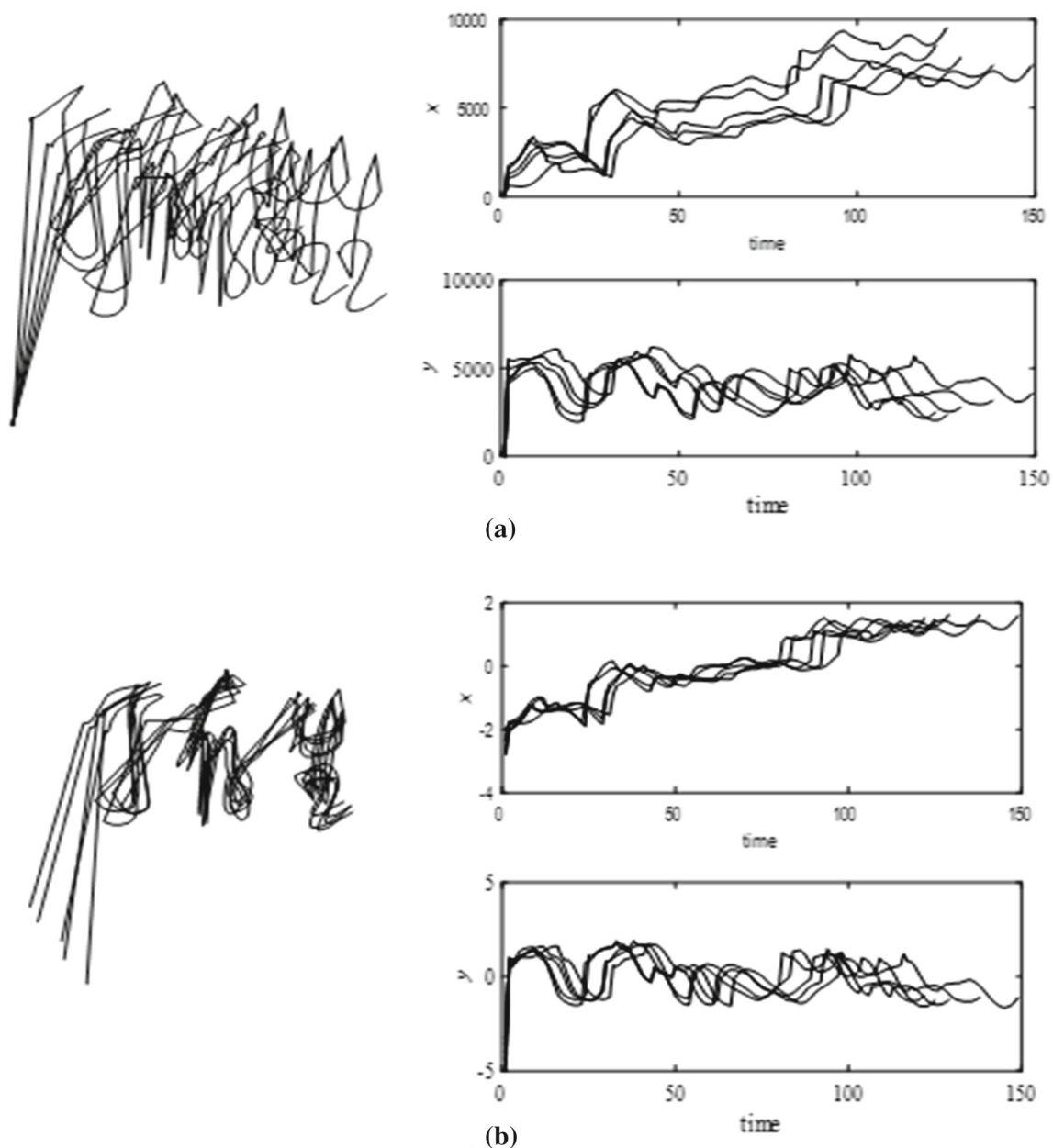
Fig. 1 Five illustrative signatures along with their features in the $x - y$ coordinates: raw data **a** and their **b** normalized version

as a probability score of being a genuine/forgery signature. Instead of a single threshold, we propose two thresholds (a_i and b_i) to compute the score for each segment. The crux of using two thresholds is to express the results of verified segments in terms of probabilistic scores that will be combined in the later stages of processing. Each segment yields a certain value of probability expressing how likely this segment supports genuine and forgery signatures (see Fig. 4) according to the values of a_i and b_i. The probability of the segment distance is computed in the following form:

$$p\left(segment_i\right) = \begin{cases} 1 - \frac{dist_i}{dist_i + a_i}, & dist_i \leq a_i \\ \frac{b_i - dist_i}{(b_i - dist_i) + (b_i - a_i)}, & a_i < dist_i \leq b_i \\ 0, & dist_i > b_i \end{cases}$$

$i = 1, 2, \ldots m$ and $0 < a_i < bi$ (4)

Another look at the way how the value of DTW $dist$ is expressed in terms of a probabilistic score considering the value of $a = 0.6$ and $b = 1.1$ is shown in Fig. 5.

In general, it is unlikely that a genuine signature could have all segment probabilities close to 0. In contrast, a
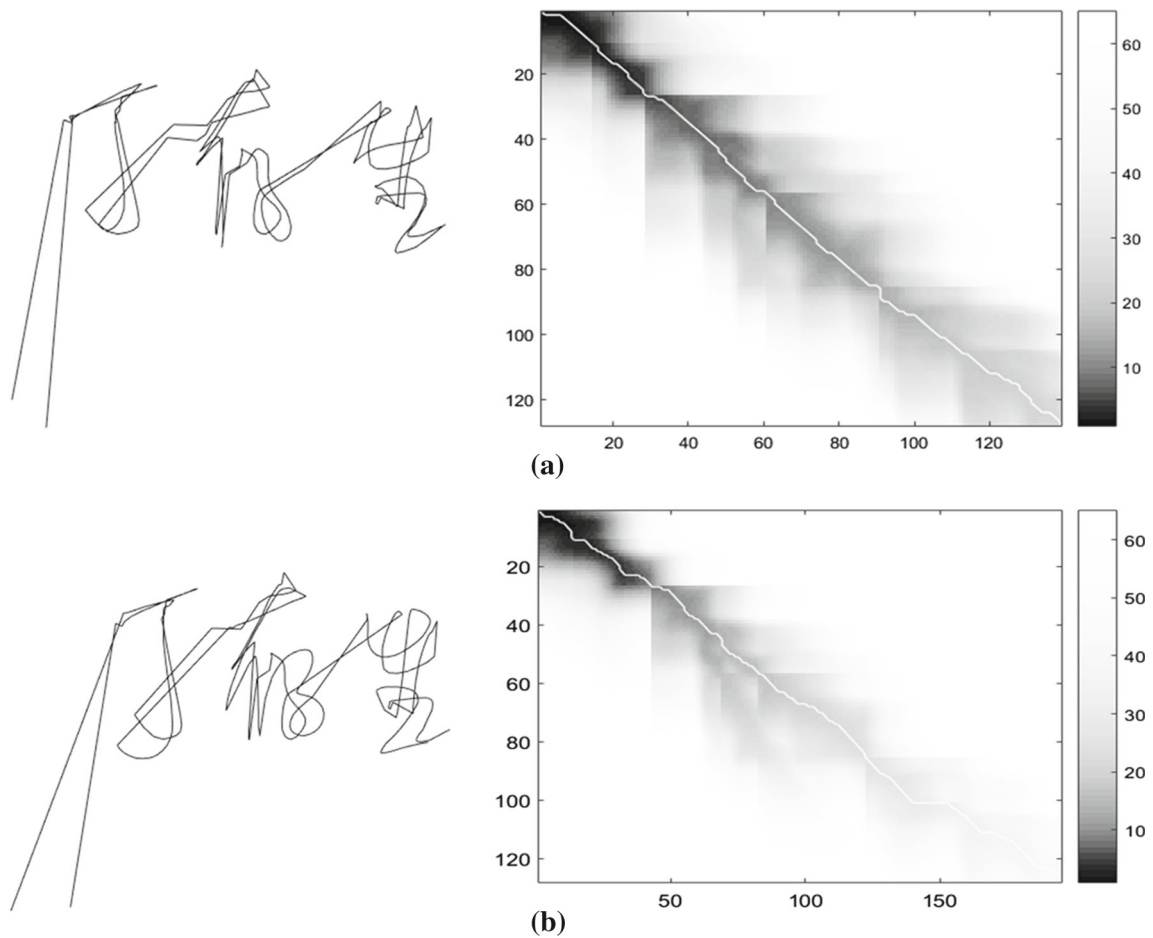
(a)

(b)

Fig. 2 Accumulated distance matrix and optimal path between a template and **a** genuine signature, **b** forgery signature

forgery signature might have one of its segments coming with the high probability (close to 1); this probability will be eliminated by other segment low probabilities in the fusion process. In the PDTW verification process, the aim is to maximize the probabilities of segments that are positioned below or above a_i for genuine signatures and minimize the segment probabilities for forgery signatures. The fusion mechanism is aimed at reaching a final decision following the Bayes rule (assuming that the segments are independent).

$$
\begin{aligned}
&P\left(signature/segment_{1,2,\ldots,m}\right) \\
&=\frac{p_1 \cdot p_2 \cdots p_m}{p_1 \cdot p_2 \cdots p_m + (1-p_1) \cdot (1-p_2) \ldots (1-p_m)}
\end{aligned} \tag{5}
$$

The denominator is a normalization term. The final decision of verification process reads as follows

$$
decision = \begin{cases} \text{genuine}, & P \geq 0.5 \\ \text{forgery}, & P < 0.5 \end{cases} \tag{6}
$$

Like the DTW approach, we used predefined values of the thresholds to compute EER at which *FAR* and *FRR* are equal.

We adopted particle swarm optimization (PSO) to optimize the threshold values of EER. The values of thresholds have been determined on a basis of the test signatures.

3.1 Particle swarm optimization

In case of a single threshold, EER is determined using different values of thresholds. In our case, instead of a single threshold we used two thresholds. We computed FAR and FRR for different combinations of threshold values. This process can be realized by invoking a certain iterative procedure; however, it is time-consuming. To make it computationally viable we used PSO to determine the optimal threshold values which produce minimum *FAR* and *FRR* in a faster way.

In order to determine the minimum EER, the thresholds a_i and b_i are optimized to maximize the difference between the average probabilities of genuine and the forgery signatures. A generic PSO is used to optimize $2*m$ variables associated with all m segments. Initially, PSO generates particles (population) at random. Each particle is represented by a vector of dimensionality $2m$ that moves in the swarm over the search
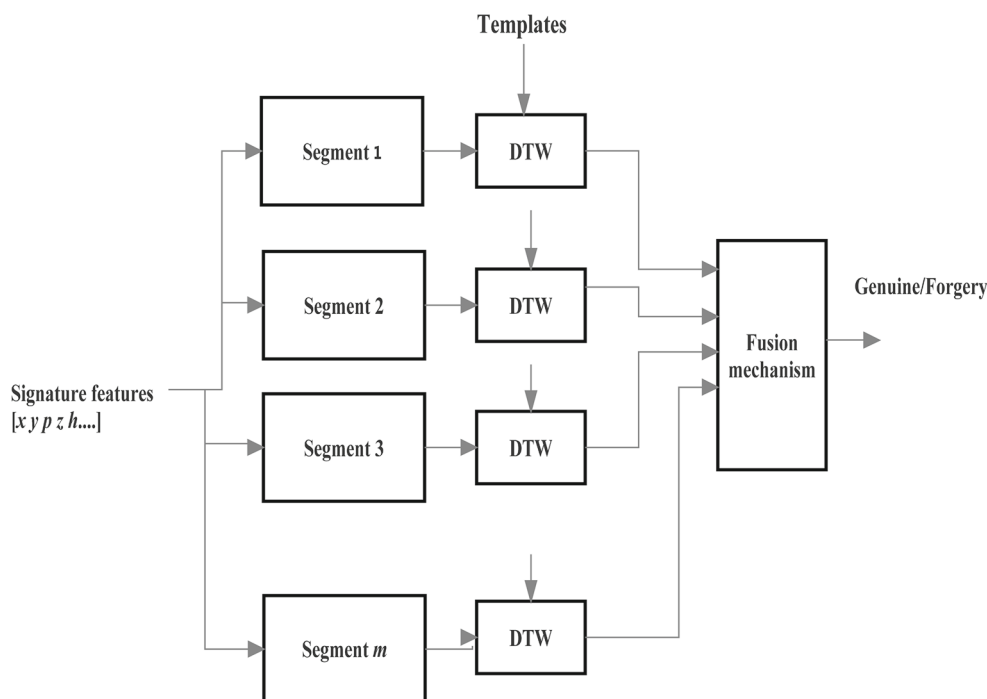
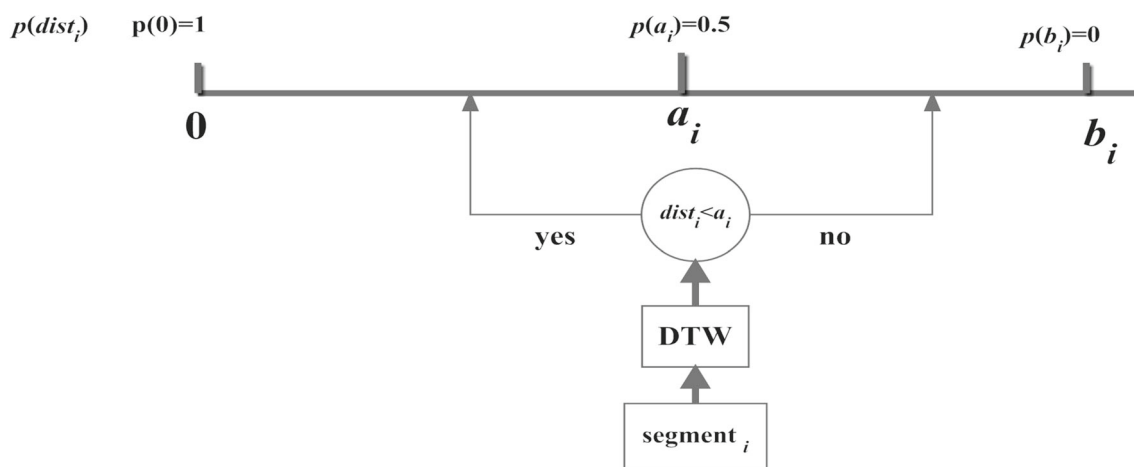**Fig. 3** Probabilistic DTW verification fusion mechanism

Fig. 4 Computing PDTW distance using two thresholds (a_i, b_i)

space with a certain velocity (Kennedy et al. 1995). PSO is relatively simple and comes with a low computing overhead. The objective function optimized by the PSO for each signer samples comes in the form:

$$\arg \max_{a1,a2,...,am,b1,b2,...,bm} \frac{1}{N} \sum_{g=1}^{N} P_g - \frac{1}{M} \sum_{f}^{M} P_f \qquad (7)$$

where P_g and P_f are the probabilities of genuine and forgery signatures, respectively. N and M are the number of samples of genuine and forgery signatures, respectively.

As an illustration, Fig. 6 shows the features of the three signatures (template, genuine, forgery). The DTW distance between the template and the genuine signature is 30.96, whereas the distance between the template and the forgery is 27.74. A threshold value located in the range [27.74, 30.96] places the genuine signature in the false rejection and the forgery signature in the false acceptance. However, considering each feature individually using the PDTW approach, the DTW distance between the template and genuine signatures in the x and y coordinates is 7.94 and 22.04, respectively. The distances for the same features between template and forgery signatures are 10.51 and 18.55 along the x and y coordinates.
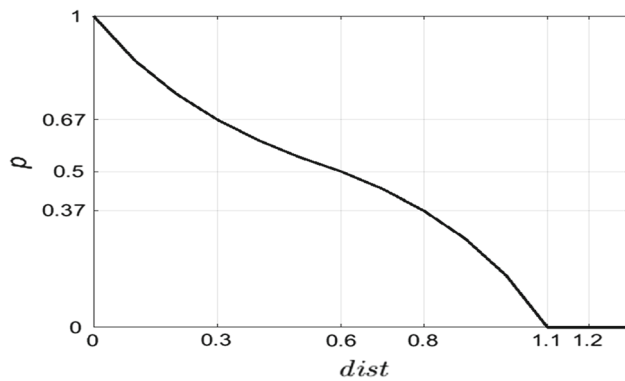
Fig. 5 p versus *dist* for $a = 0.6$ and $b = 1.1$

In the optimization process, the threshold values could converge to values $a_x = 8.52$, $b_x = 13.75$, $a_y = 24.33$, and $b_y = 34.63$, according to the following probabilities:

	genuine	forgery
x	0.52	0.30
y	0.52	0.57

The genuine segments (x and y) are verified as genuine, and the verification of forgery x segment is forgery, and y segment is genuine. Although the y segment of the forgery signature is verified as a genuine signature (0.57), this score is suppressed by the x segment verification score (0.3). According to (4), the final decision becomes

genuine	forgery
0.54	0.36

Now, the verification scores, which are greater than 0.5, are considered as genuine signatures.

The formation of the segments of the signature ($n \times p$) can be realized in different ways:

(1) *Case* 1 dividing the signature data into m segments of equal size: Each segment has p feature numbers of the original signature, and each segment has the size of ($n/m \times p$) as shown in Fig. 7.

(2) *Case* 2 consider each feature (i.e., coordinate and pressure) as a single segment. Each segment is described by a single feature, and the total number of segments (m) is equal to the number of features present in the original signature, and each segment has the size of ($n \times 1$); see Fig. 8.

The most important issue (implying the quality of the discrimination process) in the segmentation process is to find segments of genuine signatures that have low data variations, while the variation of the same segments of forgery signatures is high. Signatures can be also segmented in many ways. For instance, one can realize segmenting on a basis of landmarks present in the signatures (say, pen up/down). The PDTW approach can be applied to improve the EER.
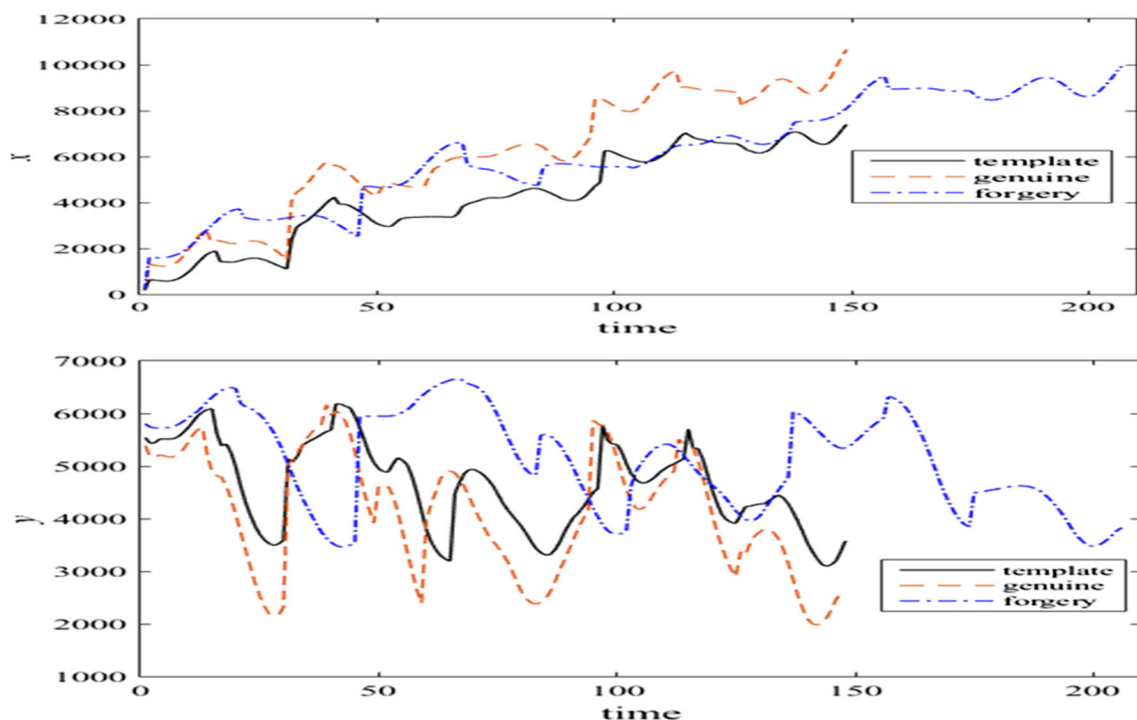

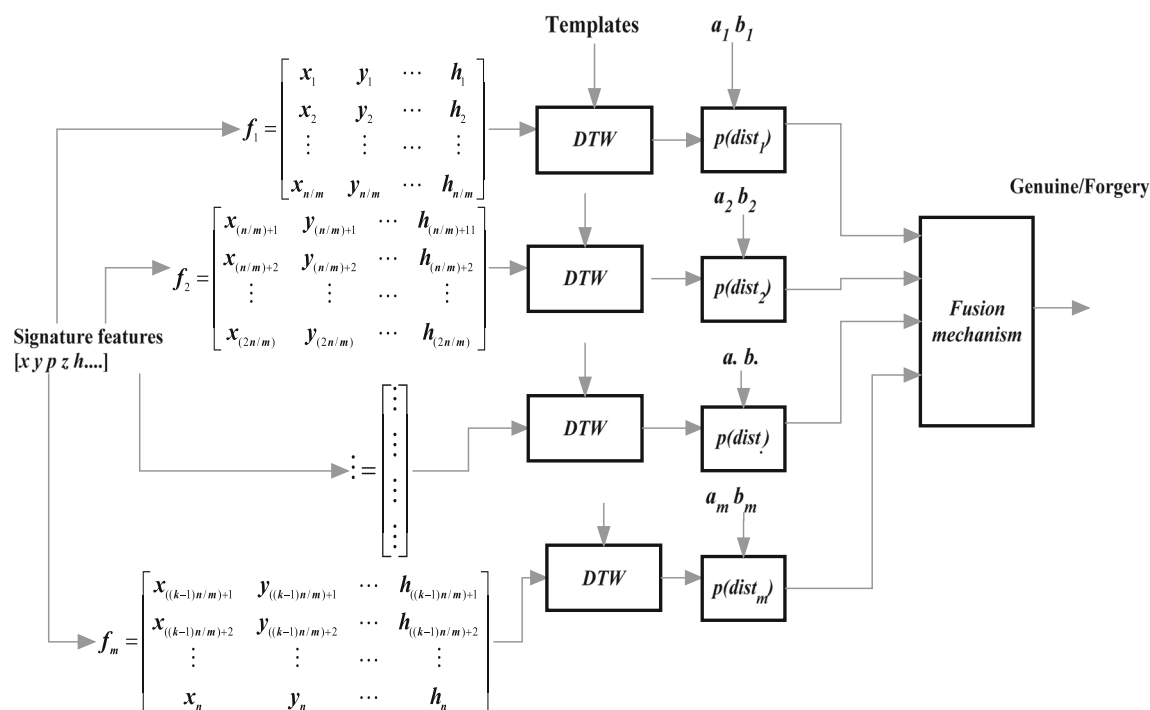**Fig. 6** x, y coordinates of template, genuine, and forgery signatures

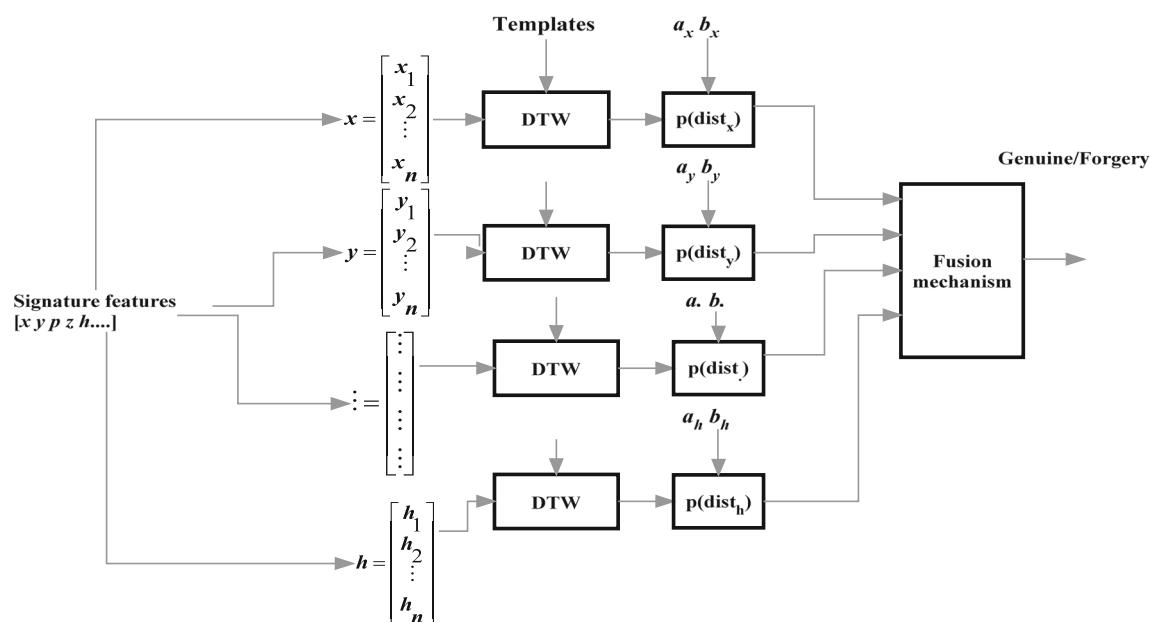**Fig. 7** Case 1 signature segmentation (*m* segments)

Fig. 8 Case 2 signature segmentation (feature per segment)

4 Experimental results

The PDTW has been tested on synthetic data and two publicly available datasets. In this section, we report results obtained with the use of the proposed approach and offer pertinent analysis.

4.1 Synthetic dataset

Two polynomial functions have been used to simulate (x, y) coordinates of synthetic signatures. We generated 500 points for each signature, see Fig. 9.
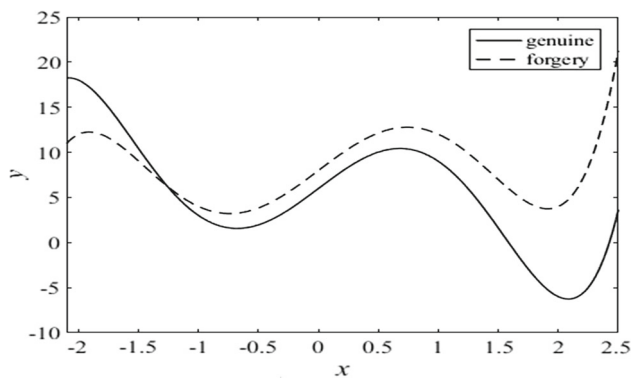
Fig. 9 Synthetic signatures

Table 1 EER (%) of synthetic signatures case 1 and case 2 (bold: minimum EER)

		m	
PDTW	Case 1	2	0.11
		5	0.23
		7	0.32
		10	0.38
	Case 2	2	**0.10**
DTW	1		0.16
Improvement (%)			37.50

$$y = x^5 - 8x^3 + 10x + 6 \longrightarrow \text{genuine}$$
$$y = x^5 - 7x^3 + 10x + 8 \longrightarrow \text{forgery}$$

The samples were simulated by a uniform selection of 100 data points and shifting both the x and y coordinates by a random normally distributed number ($\mu = 2$, $\sigma = 1$). We generated 100 samples of genuine and 100 samples of forgery signatures. Twenty samples of genuine and twenty samples of forgery were used to tune the algorithm to find the values of a and $\underline{b}$ for cases 1 and 2, and the rest of the data were used to obtain the EER. The EER results are tabulated in Table 1. An improvement of EER is achieved for case 1 and case 2. Both cases of PDTW ($m = 2$) show improvement over the DTW method; however, increasing the value of m degrades the performance.

4.2 Public datasets

Two publicly available databases are also used to evaluate the proposed algorithm (see Table 2). The feature vectors of datasets have different lengths. These features may include x position, y position, pressure p, azimuth z, and altitude l of the pen. The size (length) of the feature vectors varies for each signature sample. The number of templates (reference signatures) is chosen in the same way as reported in the literature (Yeung et al. 2004; Ortega-Garcia et al. 2003) (i.e.,

the template signatures were selected from the genuine signatures). It should be noted that we ignore sample features when the pen is up/down the air (b) and the time stamp (t).

The first five genuine signatures for each signer were used as templates, and the remaining genuine signatures are used in the testing phase. The values of EER are reported for random forgery (RF) that were randomly selected from other signers in the same dataset. It should be noted that the database provided simulated signatures of each signer. The commonly exercised protocol of the database is to use only genuine signatures in the training phase (Yeung et al. 2004; Ortega-Garcia et al. 2003). However, testing simulated forgery is not applicable in our case because the thresholds a and b should be tuned using the data coming from two classes. Therefore, the training phase used only samples of signers' genuine signatures.

PSO is used as an optimization tool to optimize the values of the thresholds. The parameters of PSO are set as follows: Swarm size -100 individuals, number of generations 200, cognitive acceleration coefficient, and the social acceleration coefficient were set to 2 as suggested in Kennedy et al. 2001. The selected values of PSO parameters showed convergence to the optimized thresholds before reaching 200 generations in most signer samples. The values of the optimized fitness function (EER) reported for one of the experiments are visualized in Fig. 10. The convergence is visible after 40 generations.

We used two types of segments to demonstrate the effectiveness of the PDTW approach in comparison with the DTW method:

(1) Feature data are segmented into m segments of equal size. Table 3 shows the EER results for RF when varying the values of m.

The best performance is reported for $m = 1$ and $m = 2$ for all database. Increasing the values of m degrades the EER because of the increasing variations in between signature and template. The segments for templates and the test signatures are extracted based on the signature size (time). Also, signatures for the same signer have different time stamps. Therefore, we might calculate DTW of segments that do not completely overlap; the number of miss-overlapped segments increased as the number segments increased.

(2) Each feature is used as a separated segment; the number of segments (m) for SCV2004 (task 2) and MCYT100 is 2 and 5 respectively (see Table 4).

The essence of the study stems from the usage of the results coming from various segments in a probabilistic form that creates a way to improve EER. If $m = 1$ in case 1, this means that only one segment is available in which PDTW also shows improvement over DTW approach.

Table 2 Details of public signature databases

|	No. of signers	No. of genuine	No. of forgery	Features	Total
SCV2004 task 2 Yeung et al. (2004)	40	20	20	$x\,y\,b\,z\,l\,p$	1600
SUBCORPUS-MCYT100 Ortega-Garcia et al. (2003)	100	25	25	$x\,y\,p\,z\,l$	5000
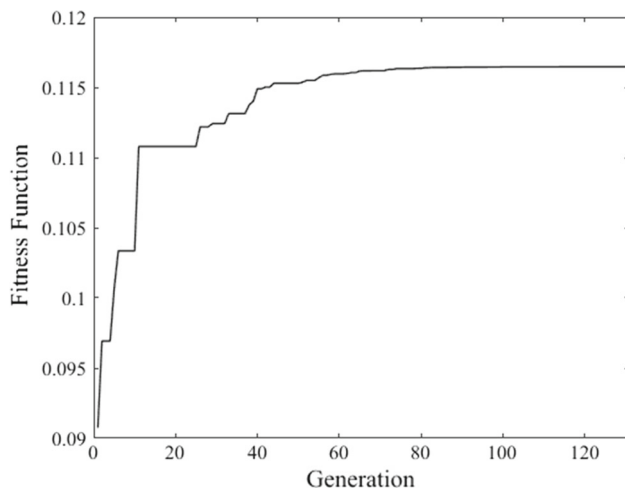
Fig. 10 The fitness function (6) values reported in successive generations of the PSO

Table 3 EER (%) (random forgery) of PDTW case 1 (bold: minimum EER)

	m	SCV2004 task 2	MCYT100
PDTW	2	**0.0025**	**0.0118**
	5	0.0092	0.0290
	7	0.0192	0.0425
	10	0.0392	0.0625
DTW	1	0.050	0.0712
Improvement (%)		95.00	83.43

Table 4 EER (%) (random forgery) of PDTW case 2

	SCV2004 task 2	MCYT100
PDTW	0.0175	0.0187
DTW	0.0500	0.0712
Improvement (%)	65.00	73.74

More segments can lead to the better performance under the assumption that the signatures are long enough and the alignment of the segments has been completed. This offers a potential of fine-tuning of signatures. In case 1, the segments are obtained by dividing the signatures into segments of equal length. This split cannot guarantee that the DTW distance is determined between the same parts of signatures because signatures might have different lengths (refer to Fig. 11).
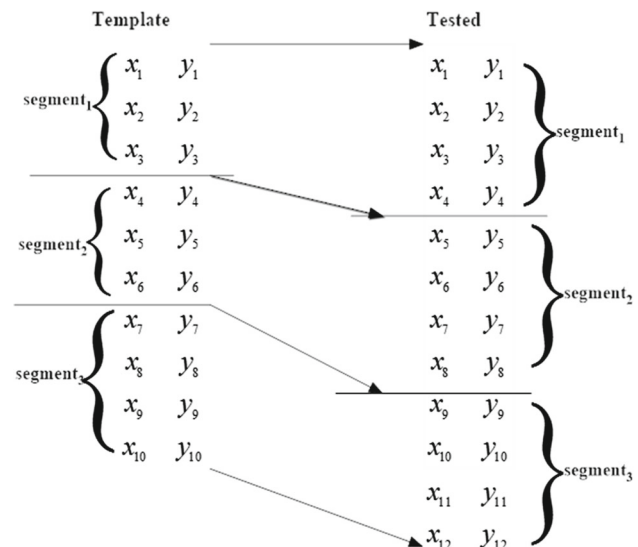
Fig. 11 Signature segments for $m = 3$

Having said that, the best performance is achieved when the alignment is available (case 2 and case 1 for $m = 2$), because this exhibits the maximum overlap between the segments that refer to the same parts.

We conclude that PDTW shows improvement for all datasets compared to the results produced by the DTW method. The minimum improvement is 65%.

A comparative view of the PDTW results with the results reported in the literature is included in Table 5. It is apparent that the PDTW produced a significant improvement of EER compared to the reported studies in terms of the values. It should be noted that in different ways, feature extraction and classification approaches are involved in the comparative studies that include locally based feature, region-based features, DCT features, PCA features, and fusion-based features. Furthermore, some previous studies used the full dataset of MCYT (Fierrez et al. 2007; Fierrez-Aguilar et al. 2005; Garcia-Salicetti et al. 2007; Pascual-Gaspar et al. 2009).

5 Conclusions

Probabilistic dynamic time warping is a new approach of signature verification that can reduce the equal error rate for any signature identification system that adopts dynamic time

Table 5 EER results reported in selected studies

Reference	Dataset	EER (RF)
Fierrez-Aguilar et al. (2005)	MCYT	0.24
Yeung et al. (2004)	MCYT	0.05
Garcia-Salicetti et al. (2007)	MCYT	1.22
Nanni (2006)	MCYT100	2.10
Pascual-Gaspar et al. (2009)	MCYT	0.29
	SCV2004 (task 2)	0.00
Yeung et al. (2004)	SCV2004 (task 2)	3.02
Fierrez-Aguilar et al. (2005)	SCV2004 (task 2)	0.15
Rashidi et al. (2012)	SCV2004 (task 2)	0.14
Case 1	SCV2004 (task 2)	0.002
	MCYT100	0.012
Case 2	SCV2004 (task 2)	0.018
	MCYT100	0.019

warping to quantify the distance between signatures. The use of multithresholds and multisegments makes the method robust in the presence of variations of certain parts in signatures.

There are several promising directions of research worth pursuing in the future. The best performance was recorded when considering each feature vector as a single segment. Estimating the absence of certain marks in signatures in order to segment the signature would constitute future and promising directions of research worth investigating. As noted earlier, another interesting alternative to be studied in the context of the multimodal biometrics would be to engage the ideas of meta-recognition.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Banko Z, Janos A (2012) Correlation based dynamic time warping of multivariate time series. Exp Syst Appl 39:12814–12823

Bellman R (1957) Dynamic programming. Princeton University Press, Princeton

Cpalka K, Zalasiński M (2014) On-line signature verification using vertical signature partitioning. Exp Syst Appl 41:4170–4180

Cpalka K, Zalasiński M, Rutkowski L (2014) New method for the on-line signature verification based on horizontal partitioning. Patt Recognit 47:2652–2661

Elgarrai Z, Elmeslouhi O, Kardouchi M, Allali H, Selouani S-A (2016) Offline face recognition system based on gabor fisher descriptors and Hidden Markov Models. Int J Interact Multimed Artif Intell 4(1):11–14

Fierrez J, Ortega-Garcia J, Ramos D, Gonzalez-Rodriguez J (2007) HMM-based on-line signature verification: feature extraction and signature modeling. Patt Recognit Lett 28(16):2325–2334

Fierrez-Aguilar J, Nanni L, Lopez-Penalba J, Ortega-Garcia J, Maltoni D (2005) An on-line signature verification system based on fusion of local and global information. In: Kanade T, Jain A, Ratha NK (eds) AVBPA 2005, vol 3546. LNCS. Springer, Heidelberg, pp 523–532

Fierrez-Aguilar J, Krawczyk S, Ortega-Garcia J, Jain A.K (2005) Fusion of local and regional approaches for on-line signature verification. In: S.Z Li , Sun Z, Tan T, Pankanti S, Chollet G, Zhang D (eds.) IWBRS 2005. LNCS Springer, Heidelberg, vol. 3781, pp. 188–196

Garcia-Salicetti S, Fierrez-Aguilar J, Alonso-Fernandez F, Vielhauer C, Guest R, Allano L, Trung TD, Scheidat T, Van BL, Dittmann J, Dorizzi B, Ortega-Garcia J, Gonzalez-Rodriguez J, di MB, Castiglione M, Fairhurst M (2007) Biosecure reference systems for on-line signature verification: a study of complementarity. Ann Telecommun Spec Issue on Multim Biom 62(1–2):36–61

Humm A, Hennebert J, Ingold R (2009) Combined handwriting and speech modalities for user authentication in systems. IEEE Trans Man and Cybern Part A: Syst Hum 39(1):25–35

Jain A, Griess F, Connell S (2002) On-line signature verification. Patt Recognit 35(12):2963–2972

Jain A, Ross A, Pankanti S (2006) Biometrics: a tool for information security. IEEE Trans Inform Forensics and Sec 1(2):125–143

Jalal A, Kamal S, Kim D (2017) A depth video-based human detection and activity recognition using multi-features and embedded Hidden Markov Models for health care monitoring systems. Int J Interact Multimed Artif Intell 4(4):54–62

Jeong YS, Jeong MK, Omitaomu OA (2011) Weighted dynamic time warping for time series classification. Patt Recognit 44:2231–2240

Jeong YS, Jeong MK, Omitaomu OA (2011) Weighted dynamic time warping for time series classification. Patt Recognit 44:2231–2240

Kennedy J, Eberhart RC, Shi Y (2001) Swarm Intelligence. Morgan Kaufmann, San Francisco

Kennedy J, Eberhart R (1995) Particle swarm optimization in neural networks. Proceedings IEEE International Conference on 1995, vol. 4, pp. 1942–1948

Ketabdar H, Richiardi J, Drygajlo A (2005) Global feature selection for on-line signature verification. In: Proceedings of 12th international graphonomics society conference, Italy, pp. 59–63

Maiorana E (2010) Biometric cryptosystem using function based on-line signature recognition. Exp Syst Appl 37:3454–3461

Nanni L (2006) Experimental comparison of one-class classifiers for on-line signature verification. Neurocomputing 69(7):869–873

Ortega-Garcia J, Fierrez-Aguilar J, Simon D, Gonzalez J, Faundez-Zanuy M, Espinosa V, Satue A, Hernaez I, Igarza JJ, Vivaracho C, Escudero D, Moro Q.I, (2003) MCYT baseline corpus: a bimodal biometric database. In: Proceedings vision, image and signal processing, IEE, vol. 150, no. 6, pp. 395–401

Pascual-Gaspar J, Cardenoso-Payo V, Vivaracho-Pascual CE (2009) Practical on-line signature verification, lecture notes in computer science. Adv Biom 5558:1180–1189

Rashidi S, Fallah A, Towhidkhah F (2012) Feature extraction based DCT on dynamic signature verification. Sci Iranica 19(6):1810–1819

Ratan AL, Grimson WE, Wells WM (2000) Object detection and localization by dynamic template warping. Int J Comput Vision 36(2):131–147

Ross A, Nandakumar K, Jain AK (2006) Handbook of multibiometrics, 1st edn. Springer, New York

Saylor M (2012) The mobile wave: how mobile intelligence will change everything. Perseus Books/Vanguard Press, New york

Scheirer WJ, Rocha A, Micheals R, Boult TE (2010) Robust fusion: extreme value theory for recognition score normalization. ECCV 2010:481–495

Scheirer WJ, Rocha A, Micheals R, Boult TE (2011) Meta-recognition: the theory and practice of recognition score analysis. Patt Anal Mach Intell IEEE Trans 33(8):1689–1695

Srivastava S, Bhardwaj S, Bhargava S (2016) Fusion of palm-phalanges print with palmprint and dorsal hand vein. Appl Soft Comput 47:12–20

Xiao Q, Siqi L (2017) Motion retrieval based on dynamic Bayesian network and canonical time warping. Soft Comput 21(1):267–280

Yeung DY, Chang H, Xiong Y, George S, Kashi R, Matsumoto T, Rigoll G (2004) SVC 2004: first international signature verification competition. In: Proceedings of the international conference on biometric authentication, LNCS, 3072, pp. 16–22