

Efficient on-line signature recognition based on multi-section vector quantization

Marcos Faundez-Zanuy · Juan Manuel Pascual-Gaspar

Received: 13 December 2008 / Accepted: 16 December 2009 / Published online: 4 March 2010
© Springer-Verlag London Limited 2010

Abstract This paper proposes a multi-section vector quantization approach for on-line signature recognition. We have used a database of 330 users which includes 25 skilled forgeries performed by 5 different impostors. This database is larger than those typically used in the literature. Nevertheless, we also provide results from the SVC database. Our proposed system obtains similar results as the state-of-the-art online signature recognition algorithm, Dynamic Time Warping, with a reduced computational requirement, around 47 times lower. In addition, our system improves the database storage requirements due to vector compression, and is more privacy-friendly because it is not possible to recover the original signature using the codebooks. Experimental results reveal that our proposed multi-section vector quantization achieves a 98% identification rate, minimum Detection Cost Function value equal to 2.29% for random forgeries and 7.75% for skilled forgeries.

Keywords On-line signature recognition · Vector quantization · DTW

1 Introduction

Handwritten signatures have a long tradition of use in commonly encountered verification tasks, such as financial

transactions and document authentication. They are easily used and well accepted by the general public, and signatures are straightforward to obtain with relatively cheap devices. These are important advantages of signature recognition over other biometrics. Yet, signature recognition also has some drawbacks: it is a difficult pattern recognition problem due to large possible variations between different signatures made by the same person. These variations may originate from instabilities, emotions, environmental changes, etc., and are person dependent. In addition, signatures can be forged more easily than other biometrics.

The signature recognition task can be split into two categories depending on the data acquisition method:

- Off-line (static), the signature is scanned from a document and the system recognizes the signature, analyzing its shape.
- On-line (dynamic), the signature is acquired in real time by a digitizing tablet and the system analyzes shape and the dynamics of writing, using for example: position with respect to the x and y axes, pressure applied by the pen, etc.

Using dynamic data, further information can be extracted, such as acceleration, velocity, curvature radius, etc. [22]. In this paper, we will focus on the online or dynamic signature recognition task.

For a signature verification system, depending on testing conditions and environment, three types of forgeries can be established [22]:

- Simple forgery, where the forger does not attempt to simulate or trace a genuine signature.
- Substitution or random forgery, where the forger uses his/her own signature as a forgery.

M. Faundez-Zanuy (✉)
Escola Universitària Politècnica de Mataró, Barcelona, Spain
e-mail: faundez@eupmt.es

J. M. Pascual-Gaspar
Valladolid, Spain
e-mail: pascualgaspar@gmail.com

- Freehand or skilled forgery, where the forger tries and practices imitating as closely as possible the static and dynamic information of the signature to be forged.

From the point of view of security, the last one is the most damaging and, for this reason, some databases suitable for system development include some trained forgeries [21, 25].

The remaining sections of this paper will be devoted to the task of dynamic signature verification, also known as authentication. This paper is organized as follows: Sect. 2 is focused on template matching dynamic signature recognition, and proposes a signature recognition methodology based on vector quantization (VQ). This approach is compared with the state-of-the-art algorithm for on-line signature recognition, which is Dynamic Time Warping (DTW). Section 3 provides experimental results, and Sect. 4 summarizes the conclusions of this work.

2 Signature recognition based on multi-section VQ

In this section, we present a multi-section vector quantization algorithm for on-line signature recognition. This method is an improved version of the classical vector quantization approach that we proposed in [8], and can also be interpreted as a variant of split-VQ [10].

It has been recently found that the Dynamic Time Warping (DTW) algorithm outperforms HMM for signature verification [14]. For this reason we will use DTW as the baseline algorithm for performance comparison.

Appendix 1 describes the DTW algorithm. In our case, we will use five signatures per person, acquired during enrollment. DTW works out the distance between the test set of vectors and each of the five training sets.

Distance computation implies a warping by means of dynamic programming. We compute five distances, each one being the result of comparing the test sequence with each of the five training repetitions. These five distances are combined using three different approaches, $\min\{\}$, $\text{mean}\{\}$, and $\text{median}\{\}$, in order to obtain the final distance. A more detailed explanation of VQ and DTW algorithms can be found in [8].

Template matching approaches are especially appropriate when a small number of samples are available for training a model. This is the case with on-line signature recognition. However, VQ presents one drawback: it is unable to model the temporal evolution of the signature (it averages all the vectors), which is certainly important for signature recognition. For this reason, we propose a multi-section codebook approach. This proposal is described in detail in Sect. 2.1.

2.1 Proposed algorithm based on multi-section codebook approach

DTW offers one advantage over VQ: it takes into account the temporal evolution of the signature. However, a simple model called the multi-section codebook [1, 2] was proposed in the mid-1980s in speech and speaker recognition. Although this approach was discarded due to the higher accuracies of HMM, we should take into account that signature recognition differs from speech/speaker recognition, because the length of the training set is rather short and it is hard in this situation to estimate an accurate statistical model. This observation is well known in the field of speaker recognition, where higher recognition rates using VQ compared with HMM have been reported for short training/testing sets.

The multi-section codebook approach consists of splitting the training samples into several sections. For example, Fig. 1 represents a three-section approach, where each signature is split into three equal length parts (initial, middle, and final sections). In this case, three codebooks must be generated for each user, each codebook being adapted to one portion of the signature. Each branch works in a similar fashion to the VQ approach, and the final decision is taken by combining individual contributions of each section by simple averaging.

If the database contains P users and the splitter provides S sections, we will have S codebooks for each person. Thus, we will have one codebook per person and section, named $\text{CB}_{p,s}$ for $p = 1, \dots, P$ and $s = 1, \dots, S$.

This proposal is a generalization of the VQ approach, which can be seen as a multi-section approach with just a single section. The multi-section system will be operated as described next.

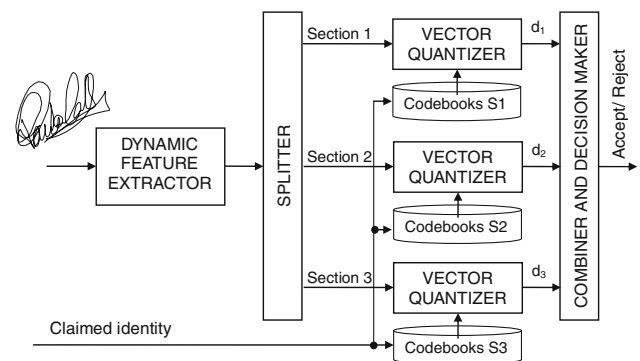


Fig. 1 A multi-section codebook approach for signature verification based on 3 sections

2.1.1 User model computation

For each person, we split the signature into S sections. We concatenate the feature vectors resulting from each of the five training signatures belonging to the same section. Thus, we obtain S training sequences per person. The LBG algorithm is performed in the classical way in order to obtain one codebook per person and section. Each person is thus modeled by a set of S codebooks. Figure 2 schematically represents the process of splitting and generating the training sequences for a given user p . It is assumed that five signatures of the same person are used for training the user model.

Our strategy is similar to a constrained vector quantization approach named split-VQ (also known as partitioned VQ) [10]. The simplest and most direct way to reduce the search and storage complexity in coding a high dimensional vector is simply to partition the vector into two or more sub-vectors. However, rather than splitting vectors, we split the training and testing sequences into sections, which have the same original vector dimension.

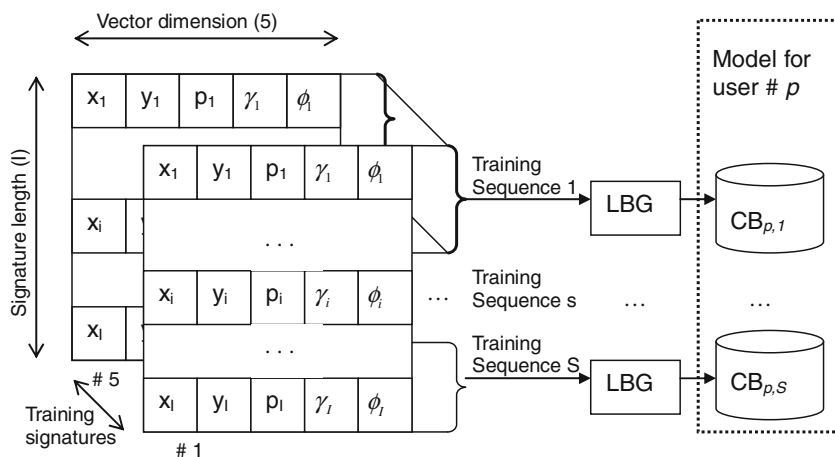
2.1.2 User recognition

The quantization distortion for a given signature and person p must be obtained by computing the combination of the distortions obtained for each part. This can be achieved by a generalization of the procedure described in [8]: $dist_p = combination(d_1, \dots, d_s)$. The most straightforward combination is the $mean\{\}$ function. However, the experimental results revealed that the $min\{\}$ function outperforms simple averaging.

The individual d_s values, for $s = 1, \dots, S$ and person p are obtained by applying the equation

$$d_s = \sum_{i=1}^{I'} \text{NNER}(\vec{x}_i, CB_{p,s}) = \sum_{i=1}^{I'} \min_{\vec{y}_j \in CB_{p,s}} \{d(\vec{x}_i, \vec{y}_j)\}$$

Fig. 2 Schematic representation of the procedure followed to obtain the training sequences and the codebooks for a given user p



where NNER is the Nearest Neighbor Encoding Rule [10]. It is interesting to point out that $I' \cong \frac{l}{5}$ because we split the whole signature into S sections of equal length.

2.2 Computational requirements comparison

In this section, we will compare the computational burden of the state-of-the-art DTW algorithm and the proposed multi-section codebook approach. We will use the following nomenclature:

- J is the average single-signature reference template length.
- I is the candidate's signature length.
- K is the number of reference templates per user.
- L is the number of vectors inside the codebook for the VQ approach.
- S is the number of sections in the multi-section VQ approach.

In our experiments, we have set $K = 5$, and in our database (MCYT) the average length per signature is $J = 454$ vectors.

It is interesting to observe that, due to the vector quantization of the K reference templates per user, the number of reference vectors has been significantly reduced for the VQ algorithm, because all the reference signatures have been clustered together in a single codebook per user. For a codebook of 4–7 bits, we get $L = 16, 32, 64,$ and 128 vectors, respectively, while the original average number of vectors per signature is 454. In addition, for DTW, the procedure must be executed for each reference signature per user (in our experimental data we have used $K = 5$). Thus, even for a 7-bit codebook, the VQ approach requires dealing with approximately 18 times ($5 \times 454/128$) less data.

Dynamic time warping requires the computation of KIJ distance measures. However, the search region can be

restricted to a parallelogram region with slopes 1/2 and 2. Search over this parallelogram requires about $O(KIJ/3)$ distances measures to be computed and the DP equation (1) (see Appendix 1) to be used about $O(KIJ/3)$ times. This latter figure is often referred to as the “number of DP searches” [3].

VQ requires the computation of $O(IL)$ distance measures. It is interesting to observe that the number of computations is the same for VQ and multi-section VQ, because the unique difference between them is the change of codebook depending upon which section a given vector belongs to. Taking into account that each DTW distance computation requires the computation of at least three distances between vectors, we can establish that VQ is approximately 47 times faster than DTW (for a codebook of 4 bits).

In terms of database storage requirements, DTW implies the storage of the whole set of reference signatures, which implies KJ vectors per user. VQ requires L vectors per user, where L is the number of vectors inside the codebook, and this figure must be increased by the number of sections for the multi-section VQ approach.

Table 1 summarizes the computational and database memory requirements. The next section presents the identification and verification rates for several experimental scenarios.

3 Experimental results

3.1 Databases

In this section, we present experimental results obtained with two publically available databases.

3.1.1 MCYT database

We used our previous database MCYT [21] acquired with a WACOM graphics tablet. The sampling frequency for signal acquisition is set to 100 Hz, yielding the following set of information for each sampling instant:

1. position along the x -axis, x_t : [0–12 700], corresponding to 0–127 mm;
2. position along the y -axis, y_t : [0–9700], corresponding to 0–97 mm;
3. pressure p_t applied by the pen: [0–1024];
4. azimuth angle γ_t of the pen with respect to the tablet: [0–3600], corresponding to 0–360°;

5. altitude angle φ_t of the pen with respect to the tablet: [300–900], corresponding to 30–90°;

We have used feature vectors composed of these five measurements. We recruited 330 different users. Each target user produces 25 genuine signatures, and 25 skilled forgeries are also captured for each user. These skilled forgeries are produced by the 5 subsequent target users by observing the static images of the signature to be imitated, trying to copy them (at least 10 times), and then, producing valid forgeries in a relaxed fashion (i.e. each individual acting as a forger is requested to sign naturally, without artefacts, such as breaks or slowdowns). In this way, highly skilled forgeries with shape-based natural dynamics are obtained. Following this procedure, user n (ordinal index) realizes a set of 5 samples of his/her genuine signature, and then 5 skilled forgeries of client $n - 1$. Then, again a new set of 5 samples of his/her genuine signature; and then 5 skilled forgeries of user $n - 2$. This procedure is repeated by user n , making further samples of the genuine signature, and imitating previous users $n - 3$, $n - 4$ and $n - 5$. Summarizing, user n produces 25 samples of his/her own signature (in sets of 5 samples) and 25 skilled forgeries (5 forgeries of each user, $n - 1$ to $n - 5$). In a similar way, for user n , 25 skilled forgeries will be produced by users $n + 1$ to $n + 5$.

We calculate the center of mass of each signature and displace this point to the origin of coordinates.

3.1.2 SVC database

The SVC database [25] is very similar to MCYT. The sub-database released for Task 2 of the First international signature verification competition also includes the same five features as MCYT acquired by a WACOM Intuos graphic tablet with a sampling rate of 100 Hz. The complete SVC database had 100 sets (users) of signature data, but just a subset of 40 users was made available for research after the competition. This database also contains skilled forgeries samples produced by the contributors. There are 20 genuine signatures per user collected through two sessions, 10 signatures per session, with a minimum of 1 week between sessions. Additionally there are 20 skilled forgeries produced by at least four other contributors. The skilled forger was provided with a software animation viewer of the signature to forge. Thus, in this work, we have used a final set of 16,000 signatures (8,000 genuine signatures plus 8,000 skilled forgeries). This is about 10% of the MCYT database size.

Table 1 Database storage and computational requirements for DTW and VQ approaches

Requirements	DTW	VQ	Multi-section VQ
Database memory	KJ	L	SL
Computational (Number of distance computations)	$O(KIJ/3)$	$O(IL)$	$O(IL)$

It must be pointed out that the signatures in the SVC database are mostly in either English or Chinese, and no ‘real’ signatures were used. Instead, the contributors were advised to design a new signature and practice it before the acquisition sessions.

The best results in this competition were EER of 2.84% with skilled forgeries using a DTW-based algorithm and EER of 1.70% with random forgeries using a system based on HMMs.

With both databases, we set the origin of coordinates to the center of mass.

3.2 Conditions of the experiments

Training and testing signatures have been chosen in the following way:

MCYT database

- We performed identification experiments, using the first 5 signatures per person for training and 5 different signatures per person for testing (signatures 6–10). This implies a total number of $330 \times 330 \times 5$ tests.
- We performed verification experiments, using the first 5 signatures per person for training and 5 different genuine signatures per person for testing (signatures 6–10). In addition, we used the 25 available forgeries made by 5 other users. This implies a total number of 330×5 genuine tests plus 330×25 impostor tests (skilled forgeries) and $330 \times 329 \times 5$ impostor tests (random forgeries).

SVC database

- We performed identification experiments, using 5 signatures per person for training and 5 different signatures per person for testing. This implies a total number of $40 \times 40 \times 5$ tests.
- We performed verification experiments, using 5 signatures per person for training and 5 different genuine signatures per person for testing. In addition, we used the 20 skilled forgeries made by other users. This implies a total number of 40×5 genuine tests plus 40×20 impostor tests (skilled forgeries) and $40 \times 39 \times 5$ impostor tests (random forgeries).

However, further study needs to be done on whether these databases can produce statistically significant results. In [11], the minimum size of the test data set N , which guarantees statistical significance in a pattern recognition task, is derived. The goal in this work is to estimate N so that it is guaranteed, with a risk α of being wrong, that the error rate P does not exceed the estimation \hat{P} from the test set by an amount larger than $\varepsilon(N, \alpha)$, that is,

$$\Pr\{P > \hat{P} + \varepsilon(N, \alpha)\} < \alpha$$

Let $\varepsilon(N, \alpha) = \beta P$, and supposing recognition errors to be Bernoulli trials (i.i.d. errors), after some approximations, the following relationship can be derived:

$$N \approx \frac{-\ln \alpha}{\beta^2 P}$$

For typical values of α and β ($\alpha = 0.05$ and $\beta = 0.2$), the following simplified criterion is obtained:

$$N \approx \frac{100}{P}$$

If the samples in the test data set are not independent (due to correlation factors that may include variations in recording conditions, in the type of sensors, etc.), then N must be further increased. The reader is referred to [11] for a detailed analysis of this case, where some guidelines for computing the correlation factors are also given.

Table 2 shows the number of tests done in each condition and, with 95% confidence, the statistical significance in experiments with an empirical error rate, down to \hat{P} . Thus, the experiments of this section are statistically significant, because our errors are higher than those presented in Table 2.

Verification systems can be evaluated using the False Acceptance Rate (FAR, those situations where an impostor is accepted) and the False Rejection Rate (FRR, those situations where a user is incorrectly rejected), also known in detection theory as False Alarm and Miss, respectively. A trade-off between both errors usually has to be established by adjusting a decision threshold. The performance can be plotted in a Receiver Operator Characteristic (ROC) or in a Detection error trade-off (DET) plot [18].

We have used a single point of the DET plot for comparison purposes: the minimum value of the Detection Cost Function (DCF). This parameter is defined as [18]:

$$DCF = C_{\text{miss}} \times P_{\text{miss}} \times P_{\text{true}} + C_{\text{fa}} \times P_{\text{fa}} \times P_{\text{false}}$$

where C_{miss} is the cost of a miss (rejection), C_{fa} is the cost of a false alarm (acceptance), P_{true} is the a priori probability of the target, and $P_{\text{false}} = 1 - P_{\text{true}}$. $C_{\text{miss}} = C_{\text{fa}} = 1$.

Table 2 Statistical significance in experiments, with 95% confidence

	MCYT database (330 users) (\hat{P})	SVC database (40 users) (\hat{P})
Random forgeries	0.02	1.25
Skilled forgeries	1.01	10

3.3 Experimental results

Table 3 shows the experimental results from modeling each user with a codebook, with the experimental conditions as described in the previous section. We have studied codebook sizes ranging from 0 to 9 bits (1–512 clusters). It is interesting to observe that the 0-bit codebook corresponds to modeling each user with a single vector, equal to the average of each dynamical parameter. This is equivalent to the static feature extraction described in the introductory section.

Table 4 shows the results obtained with the state-of-the-art algorithm DTW. For the sake of simplicity, in the multi-section codebook approach, we have used equal size sections. Figure 3 presents the identification rates for different numbers of sections and bits per section. We can observe that the multi-section approach outperforms the baseline VQ algorithm. In addition, the best identification result is obtained for three sections (98%), which compares favorably with the highest identification rate obtained with DTW (see Table 4; 98.9%).

Figures 4 and 5 show the minimum detection cost function value for different numbers of sections, bits per person, random and skilled forgeries, respectively. We can achieve a slight improvement (2.29% for random forgeries and 7.84% for skilled ones) over DTW (see Table 4; 2.33 and 7.84%, respectively).

4 Conclusions

In this paper, we have proposed a multi-section codebook approach for on-line signature recognition. This algorithm

enables us to take into account the temporal evolution of the signature (thanks to the use of several sections), and obtain a significant speed improvement, which has been estimated to be around 47 times. This improvement is due to the lower computational burden of the VQ approach, which has been neglected for signature recognition so far, although it has proven useful in the past for other biometric traits, such as speech, especially for short training and testing sets.

Experimental results on a large database of 330 users (MCYT) reveal:

- Optimal configuration consists of three sections and codebooks of 4 bits per section.
- Identification rates of 98% (3 sections and codebooks of 4 bits per section).
- Minimum detection cost function equals 2.29% for random forgeries and 7.75% for skilled forgeries.

These results are very similar to those provided by DTW (98.91% identification rate and minimum DCF equal to 2.33% for random forgeries and 7.84% for skilled forgeries).

Table 4 Results obtained with DTW and MCYT database. The model size is $5 \times J \times 5$ per user

Combination	Identification rate (%)	Minimum DCF (%)	
		Substitution	Skilled
Min {·}	98.91	2.33	7.84
Mean {·}	96.97	4.34	10.17
Median {·}	98.36	3.17	9.08

Table 3 Experiments with VQ for MCYT and SVC databases. Size ranging from 0 to 9 bit

Model size	Identification rate		Verification errors (%)							
	MCYT (%)	SVC (%)	Substitution (%)				Skilled (%)			
			MCYT		SVC		MCYT		SVC	
			DCF	EER	DCF	EER	DCF	EER	DCF	EER
1 × 5	10.24	60	45.65	46.6	48.14	48.5	45.62	47.03	45.56	49.06
2 × 5	48.67	80	29.21	29.76	33.74	35	36.21	36.43	42.44	46.94
4 × 5	77.21	93	19.49	19.65	24.53	25.1	28.3	28.73	38.56	41.56
8 × 5	91.27	98	10.81	10.91	14.62	15.56	21.2	21.32	31.56	33
16 × 5	95.27	98	6.94	7.09	11.16	11.5	15.98	16.42	23.75	24
32 × 5	95.58	97.5	5.37	5.47	8.29	8.52	13.17	13.51	19	19.5
64 × 5	95.52	96.5	4.8	4.91	6.37	6.62	11.72	12	16.38	17
128 × 5	95.21	96.5	4.31	4.36	5.13	6	11.39	11.70	14.5	15.06
256 × 5	94.24	96	4.39	4.55	5.01	5.42	11.39	11.58	13.5	14
512 × 5	91.82	96	4.8	4.86	5.14	5.5	11.46	11.64	13.25	13.5

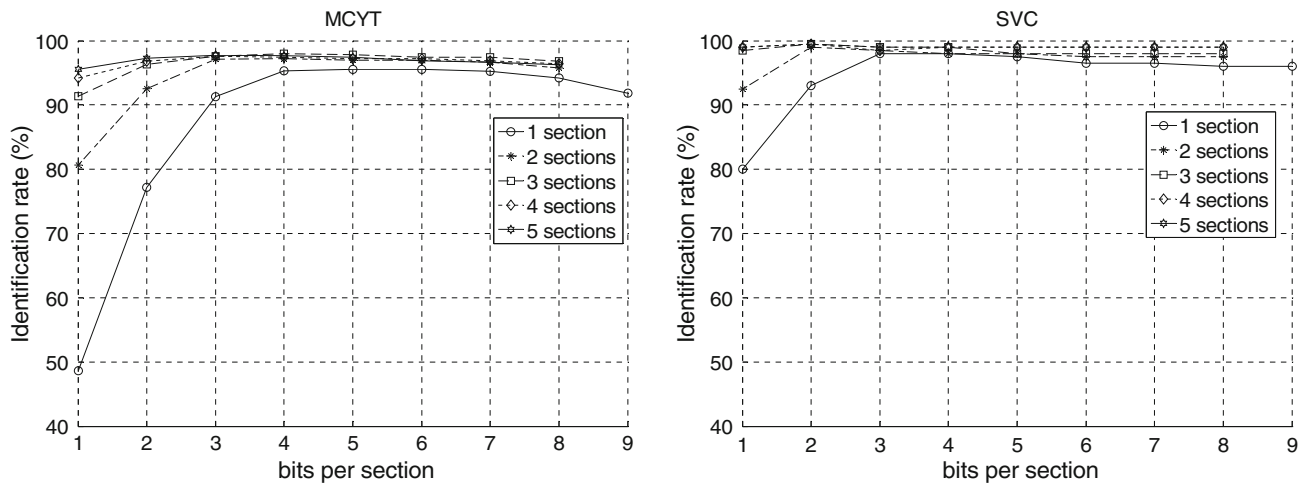


Fig. 3 Identification results for several multi-section codebook approaches, ranging from 1 to 5 sections for MCYT (on the left) and SVC (on the right) databases

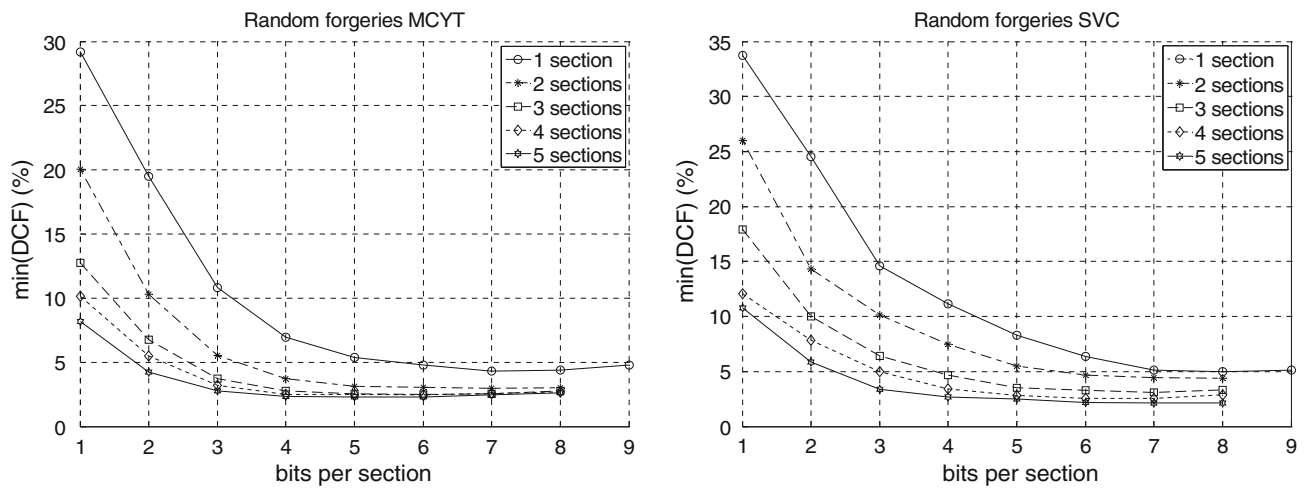


Fig. 4 Minimum DCF for random forgeries and multi-section codebook approach MCYT (on the left) and SVC (on the right) databases

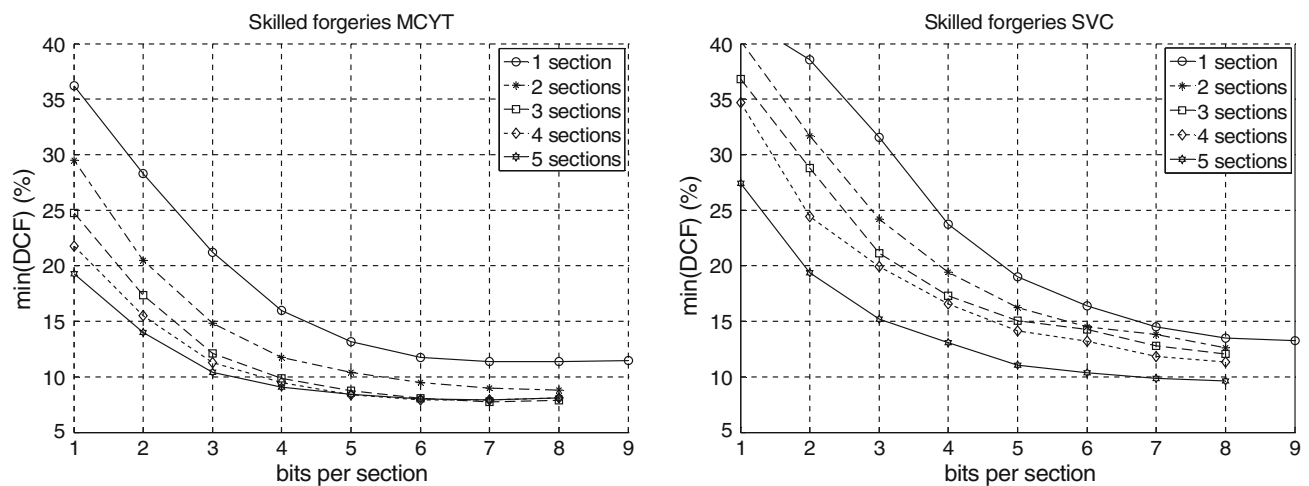


Fig. 5 Minimum DCF for skilled forgeries and multi-section codebook approach MCYT (on the left) and SVC (on the right) databases

In addition, our system improves the database storage requirements due to vector compression, and is more privacy-friendly because it is not possible to recover the original signature using the codebooks.

Acknowledgments This work has been supported by FEDER and MEC, TEC2006-13141-C03-02/TCM, TEC2009-14123-C04-04.

Appendix 1: DTW algorithm

To find the optimal path to (i_k, j_k) we simply take the minimum over all distance predecessors:

$$D_{\min}(i_k, j_k) = \min_{(i_{k-p}, j_{k-p})} \{D_{\min}[(i_k, j_k)|(i_{k-p}, j_{k-p})]\} \quad (1)$$

The simplest case corresponds to three predecessors.

The distance between a reference signature and a candidate’s signature can be computed using the following algorithm:

Initialization:

$$D_{\min}(1, j) = d_N(1, j), \quad j = 1, \dots, \varepsilon$$

$$D_{\min}(i, 1) = d_N(i, 1), \quad i = 2, \dots, \varepsilon$$

$$\delta_1(j) = D_{\min}(1, j), \quad j = 1, \dots, J$$

$$\delta_2(j) = 0, \quad j = 1, \dots, J$$

Recursion:

For $i=2, \dots, I$

For $j=J, \dots, 2$

Compute $D_{\min}(i, j)$ using equation (1)

$$\delta_2(j) = \delta_1(j)$$

$$\delta_1(j) = D_{\min}(i, j)$$

Next j

Next i

Termination

Best path has cost:

$$\tilde{D} = \min \begin{cases} D_{\min}(I, j)/I, & j = J - \varepsilon, \dots, J \\ D_{\min}(i, J)/I, & i = I - \varepsilon, \dots, I \end{cases}$$

This notation is consistent with those provided in (Deller et al. 3). A complete explanation of this dynamic programming technique is beyond the scope of this paper.

Appendix 2: VQ algorithm

Given a distance measure between vectors i and j , such as, for instance, the euclidean distance:

$$D(i, j) = \|i - j\|_2$$

The distance between a codebook and a candidate’s signature can be computed using the following algorithm:

Initialization:

$$\tilde{D} = 0$$

Recursion:

For $i=1, \dots, I$

$$d_{\min} = D(i, 1)$$

For $j=2, \dots, L$

$$d = D(i, j)$$

$$\text{if } d < d_{\min} \Rightarrow d_{\min} = d$$

End

$$\tilde{D} = \tilde{D} + d_{\min}$$

End

Termination

Best match has cost \tilde{D}

References

1. Buck JT, Burton DK, Shore JE (1985) Text-dependent speaker recognition using vector quantization. IEEE ICASSP, pp 391–394
2. Burton DK, Shore JE, Buck JT (1983) A generalization of isolated word recognition using vector quantization. IEEE ICASSP, Boston, pp 1021–1024
3. Deller JR, Proakis JG, Hansen JHL (1987) Discrete-time processing of speech signals. Prentice Hall, Upper Saddle River
4. Faundez-Zanuy M (2004) On the vulnerability of biometric security systems. IEEE Aerosp Electr Syst Magaz 19(6):3–8
5. Faundez-Zanuy M (2005) Data fusion in biometrics. IEEE Aerosp Electr Syst Magaz 20(1):34–38
6. Faundez-Zanuy M (2005) Privacy issues on biometric systems. IEEE Aerosp Electr Syst Magaz 20(2):13–15
7. Faundez-Zanuy M (2005) Biometric recognition: why not massively adopted yet? IEEE Aerosp Electr Syst Magaz 20(8):25–28
8. Faundez-Zanuy M (2007) On-line signature recognition based on VQ-DTW. Pattern Recognition, vol 40. Elsevier, Amsterdam, pp 981–992
9. Faundez-Zanuy M, Monte-Moreno E (2005) State-of-the-art in speaker recognition. IEEE Aerosp Electr Syst Magaz 20(5):7–12
10. Gersho A, Gray RM (1991) Vector quantization and signal compression. Kluwer, Dordrecht
11. Guyon I, Makhoul J, Schwartz R, Vapnik V (1998) What size test set gives good error rate estimates? IEEE Trans Pattern Anal Mach Intell 20(1):52–64
12. Han K, Sethi IK (1996) Handwritten signature retrieval and identification. Pattern Recogn Lett 17:83–90
13. Higgins AL, Bahler LG, Porter JE (1993) Voice identification using nearest-neighbor distance measure. In: IEEE international conference on acoustics, speech and signal processing ICASSP, pp II-375, II-378

14. Houmani N et al (2009) BioSecure signature evaluation campaign 2009 (BSEC'2009). http://biometrics.it-sudparis.eu/BSEC2009/downloads/BSEC2009_results.pdf
15. Ortega-Garcia J, Gonzalez-Rodriguez J, Simon-Zorita D, Cruz-Llanas S (2002) From biometrics technology to applications regarding face, voice, signature and fingerprint recognition systems. Biometrics solutions for authentication in an E-World, Chap 12. Kluwer, Dordrecht
16. Jain A, Bolle R, Pankanti S (1999) Biometrics. Personal identification in a networked society. Kluwer, Dordrecht
17. Jain AK, Duin RPW, Mao J (2000) Statistical pattern recognition: a review. *IEEE Trans Pattern Anal Mach Intell* 22(1):4–37
18. Martin A et al (1997) The DET curve in assessment of detection performance. In: European speech processing conference Eurospeech, vol 4, pp 1895–1898
19. Nanavati S, Thieme M, Nanavati R, Biometrics (2002) Identity verification in a networked world. Wiley, New York
20. Nanni L, Lumini A (2006) Advanced methods for two-class problem formulation for on-line signature verification. *Neurocomputing* 69(7–9):854–857
21. Ortega-Garcia J, Fierrez J, Simon D, Gonzalez J, Faundez-Zanuy M, Espinosa V, Satue A, Hernaez I, Igarza J-J, Vivaracho C, Escudero D, Moro Q-I (2003) MCYT baseline corpus: a multimodal biometric database. *IEE Proc Vision Image Signal Process* 150:395–401
22. Plamondon R, Lorette G (1989) Automatic signature verification and writer identification- the state of the art. *Pattern Recogn* 1(2):107–131
23. Soong F, Rosenberg A, Rabiner L, Juang B (1985) A vector quantization approach to speaker recognition. *IEEE Proc Int Conf Acoust Speech Signal Process* 1:387–390 Tampa
24. Xiao X, Leedham G (2002) Signature verification using a modified Bayesian network. *Pattern Recogn* 35(5):983–995
25. Yeung D, Chang H, Xiong Y, George S, Kashi R, Matsumoto T, Rigoll G, (2004) SVC2004: first international signature verification competition. *Lect Notes Comput Sci LNCS-3072*, Springer, Berlin, pp 16–22
26. Zhang D (2000) Automated biometrics. Technologies and systems. Kluwer, Dordrecht