Combining local, regional and global matchers for a template protected on-line signature verification system

Loris Nanni\textsuperscript{a,}\textsuperscript{*}, Emanuele Maiorana\textsuperscript{b}, Alessandra Lumini\textsuperscript{a}, Patrizio Campisi\textsuperscript{b}

\textsuperscript{a} DEIS, Università di Bologna, Viale Risorgimento 2, 40136 Bologna, Italy
\textsuperscript{b} Università degli Studi “Roma Tre”, Via della Vasca Navale 84, 00146, Roma, Italy

\textbf{A R T I C L E   I N F O}

\textbf{Keywords:}
On-line signature
Ensemble of classifiers
Dynamic Time Warping
Hidden Markov Models
Linear Programming Descriptor
BioHashing
Template protection

\textbf{A B S T R A C T}

In this work an on-line signature authentication system based on an ensemble of local, regional, and global matchers is presented. Specifically, the following matching approaches are taken into account: the fusion of two local methods employing Dynamic Time Warping, a Hidden Markov Model based approach where each signature is described by means of its regional properties, and a Linear Programming Descriptor classifier trained by global features.

Moreover, a template protection scheme employing the BioHashing and the BioConvolving approaches, two well known template protection techniques for biometric recognition, is discussed.

The reported experimental results, evaluated on the public MCYT signature database, show that our best ensemble obtains an impressive Equal Error Rate of 3%, when only five genuine signatures are acquired for each user during enrollment. Moreover, when the proposed protected system is taken into account, the Equal Error Rate achieved in the worst case scenario, that is, when an “impostor” is able to steal the hash keys, is equal to 4.51%, whereas an Equal Error Rate \( \sim 0 \) can be obtained when nobody steals the hash keys.

\textcopyright 2009 Elsevier Ltd. All rights reserved.

\textbf{1. Introduction}

People recognition based on signatures is one of the most commonly employed biometric based authentication methods. In a signature verification system, the individuals can be recognized by measuring and analyzing the activity of signing, which includes information regarding the stroke order, the pressure applied by the pen or its speed, in addition to the visual aspect of the signatures. Being part of everyday life, signature based authentication is perceived as a non-invasive and non-threatening process by the majority of the users. Furthermore, the written signature has a high legal value. On the other hand, the signature can be influenced by physical and emotional conditions, and therefore exhibits a significant variability which must be taken into account in the authentication process.

Several interesting reviews (Dimauro, Impedovo, Lucchese, Modugno, & Pirlo, 2004; Fierrez & Ortega-Garcia, 2003; Ortega-Garcia, Fierrez-Aguilar, Martin-Rello, & Gonzalez-Rodriguez, 2003; Ortega-Garcia, Fierrez-Aguilar, & Simon, 2003; Plamondon & Lorette, 1989; Sakamoto et al., 2005) can be distinguished into three main categories, which differ in the information extracted from the available data:

\begin{itemize}
  \item \textit{(a)} global approaches, where a set of global parametric features (i.e. signature total duration, number of pen-ups, and so on) are extracted from the acquired signatures, and used to train a classifier (Fierrez-Aguilar, Ortega-Garcia, & Gonzalez-Rodriguez, 2005). Some recent works (Nanni & Lumini, 2005; Nanni, 2006) demonstrate that a Random Subspace ensemble of one-class classifiers allows a considerable performance improvement, with respect to a stand-alone one-class classifier.

  \item \textit{(b)} local function based approaches, where the time functions extracted from different signatures are directly matched by using elastic distance measures, such as Dynamic Time Warping (DTW) (Jain et al., 2002), instead to be used as features for a classifier. During the comparative studies performed for the Signature Verification Competition of 2004
\end{itemize}
c) regional function based approaches, where the acquired signatures are analyzed by estimating some regional properties, which are then employed to train a given classifier. The best regional approaches model on-line signatures with Hidden Markov Models (HMMs) (Fierrez-Aguilar, Ortega-Garcia et al., 2005; Fierrez-Aguilar et al., 2005). Moreover, in Nanni and Lumini (2008b) signatures are decomposed employing wavelet transforms, and the Discrete Cosine Transform (DCT) is applied to the resulting approximation coefficients. A Linear Programming Descriptor (LPD) classifier is then trained using the obtained DCT coefficients.

According to some recently published results (Yeung et al., 2004), the most promising approaches belong to the category of local function based methods. However, one of the major research trends in on-line signature verification is to combine different systems, in order to build an ensemble of classifiers (Fierrez-Aguilar, Nanni, Lopez-Penalba, Ortega-Garcia, & Maltoni, 2005; Van, Garcia-Salicetti, & Dorizzi, 2007).

In this work, an ensemble of classifiers belonging to different categories is presented. The ensemble is built by combining:

- a local function based matcher, obtained from the fusion of two variants of the Kholmatov's DTW algorithm (Kholmatov & Yanikoglu, 2005);
- a regional function based matcher, where each signature is represented by a sequence of vectors describing regional properties, and HMMs are employed as classifiers;
- a global approach employing a LPD classifier, trained by global parametric features.

Moreover, the security of a signature based authentication system is also considered. The use of biometric data in an automatic recognition system involves the possibility of identity theft, with the risk of improper use of the stolen information, and, even worse, the impossibility to replace the stolen data. When designing a biometric system, several measures have then to be carefully considered, in order to enhance biometric data resilience against attacks (Ratha, Connell, & Bolle, 2001). The state-of-the-art on biometric template protection is discussed in details in Section 2.

In this paper, a protected signature based authentication system is build as an ensemble of already presented approaches. Specifically, two different solutions for template protection are implemented: the Improved BioHashing (Lumini & Nanni, 2007) and the BioConvolving method proposed in Maiorana, Martinez-Diaz, Campisi, Ortega-Garcia, and Neri (2008).

The experimental results, reported in Section 4, are obtained using the public SUBCORPUS-100 MCYT Bimodal Biometric Database (Ortega-Garcia et al., 2003; Ortega-Garcia, Fierrez-Aguilar, Simon, et al., 2003), which comprises signatures taken from 100 subjects, and confirm the effectiveness of the proposed ensembles of classifiers.

2. Biometric template protection

In the recent past, many solutions have been investigated to secure biometric templates. Among them, the most promising approaches consist in the implementation of cancelable biometrics (Ratha et al., 2001), which can be roughly described as the application of an intentional and repeatable modification to the original biometric templates. Typically, a properly defined cancelable biometrics should satisfy the properties of renewability (it should be possible to revoke a compromised template and issue a new one based on the same biometric data) and security (it should be impossible or computationally unfeasible to obtain the original biometric template from the modified one). Moreover, it should grant that the recognition performance of the protected system does not degrade significantly with respect to an unprotected system.

A classification of the proposed protection methods has been presented in Jain, Nandakumar, and Nagar (2008), where two macro-categories, referred to as Biometric Cryptosystems and Feature Transformation approaches, are considered. Biometric cryptosystems typically employ binary keys to secure the biometric templates, and during the process some public information, usually referred to as helper data, is used. This category can be further divided in key binding systems, where the helper data are obtained by binding a key with the biometric template (Juels & Wattenberg, 1999; Juels & Sudan, 2006), and key generating systems, where both the helper data and the cryptographic key are directly generated from the biometric template (Sutcu, Lia, & Memon, 2007). In a feature transformation approach a transformation function, typically governed by random parameters employed as keys, is applied to the biometric template, thus generating the desired cancelable biometrics. It is possible to distinguish between salting approaches, where the employed transforms are invertible (Teoh, Ngo, & Goh, 2006), and non-invertible transform approaches, where a one-way function is applied to the considered templates (Ratha, Chikkerur, Connell, & Bolle, 2007). The security of salting approaches relies in the secure storage of the transform parameters, whereas when the latter approaches are considered, their security relies in the difficulty to invert the transformation, even if its defining parameters are known. When a feature transformation approach is employed, the transformed templates can remain in the same (feature) space of the original ones, being then possible to employ, in the authentication stage, the matchers designed for the original biometric templates. This allows to guarantee performance which is similar to that of an unprotected approach. Moreover, having the possibility of employing dedicated matchers, a score can be obtained as the output of a recognition process, even if it has been performed in a transformed domain: secure multibiometric systems can therefore be implemented through score-level fusion techniques (Ross, Nandakumar, & Jain, 2006).

Signature template protection have been first considered in Vielhauer, Steinmetza, and Mayerhofer (2002) with a key generation approach, where a set of parametric features was extracted from the acquired dynamic signatures, and a hash function was applied to the feature binary representation, obtained exploiting some statistical properties of the enrollment signatures. In Freire-Santos, Fierrez-Aguilara, and Ortega-Garcia (2006) an adaptation of the fuzzy vault to signature protection has been proposed, employing a quantized set of maxima and minima of the temporal functions mixed with chaff points in order to provide security. Also the fuzzy commitment (Juels & Wattenberg, 1999) (more specifically, its practical implementation known as Helper Data System (Van der Veen, Kevenaar, Schrijen, Akkermans, & Zuo, 2006) has been employed to provide security for the features extracted from an on-line signature, as proposed in Maiorana et al. (2008), Campisi, Maiorana, and Neri (2008), where a user-adaptive error correcting code selection was also introduced. A salting approach has been proposed in Yip, Goh, Ngo, & Teoh (2006), as an adaptation of the BioHashing method (Teoh et al., 2006) to signature templates. Moreover, in Lumini and Nanni (2007) an improved version of the
BioHashing approach, where the procedure is iterated many times to increase the security of the system, has also been employed to protect signature templates. In Maiorana et al. (2008) a signature template protection scheme, where non-invertible transforms are applied to a set of signature sequences, has been presented, and its non-invertibility discussed. The renewability capacity of the approach in Maiorana, Campisi, and Neri (2008) has also been analyzed in Maiorana, Campisi, Ortega-Garcia, and Neri (2008), where additional non-invertible transforms are introduced.

3. Proposed signature based authentication system

As explained above, in this paper we implement a signature based authentication system by combining the following classifiers:

- the local function based matcher presented by Kholmatov in Kholmatov and Yanikoglu (2005), where the distances between reference and test signatures are computed by means of the DTW algorithm, and normalized with respect to the intra-class distances estimated during the enrollment phase;
- the regional function based approach presented in Fierrez-Aguilar, Ortega-Garcia et al. (2005), where HMMs are employed as matcher;
- the global feature based approach presented in Nanni (2006), where a LPD is trained by a set of parametric features.

Moreover, a signature based authentication system where the employed biometric templates are protected is also defined, by building an ensemble based on the following approaches:

- the Improved BioHashing template protection technique (Lumini & Nanni, 2007);
- the BioConvolving template protection technique presented in Maiorana et al. (2008).

A detailed description of the signature features employed in the proposed systems, as well as of the aforementioned matching techniques, is provided in the following.

3.1. Employed on-line signature features

The following discrete-time dynamic sequences are available from a typical acquisition device (the sampling frequency of the acquired signals is set to 100 Hz):

- \( x \): position in horizontal axis;
- \( y \): position in vertical axis;
- \( p \): pressure applied by the pen;
- \( \alpha \): azimuth angle of the pen with respect to the tablet;
- \( \beta \): altitude (elevation) angle of the pen with respect to the tablet.

A signature acquisition begins in correspondence to the first sample with a non-zero pressure value, and its ending is determined by setting a 3 s timer to the pen up. Fig. 1a shows an example of the discrete-time sequences extracted from a given dynamic signature, while Fig. 1b displays the azimuth and altitude pen angles, with respect to the plane of the tablet.

The following other sequences can be calculated by means of the ones above mentioned, and are employed as features in the considered systems:

- \( D_x \): difference between two consecutive \( x \) coordinates;
- \( D_y \): difference between two consecutive \( y \) coordinates;
- \( D_p \): difference between two consecutive pressure values;
- \( \theta \): path-tangent angle;
- \( \nu \): path velocity magnitude;
- \( \rho \): log curvature radius;
- \( a \): total acceleration magnitude.

Fig. 2 illustrates some of the employed functional features, together with their first-order derivatives (employed as signature representation for the HMM based matching approach).

3.2. Dynamic Time Warping (DTW)

This matching approach, proposed by Kholmatov in Kholmatov and Yanikoglu (2005), is based on the computation of DTW.
distances between test and reference signatures, which are then normalized with respect of the intra-class DTW distances, estimated during the enrollment phase. Specifically, for each enrolled signature of a user \(i\), the average values of the following distances are evaluated:

1. distance to their nearest neighbor \((d_{\text{min}})_i\);
2. distance to their farthest neighbor \((d_{\text{max}})_i\);
3. distance to the template signature \((d_{\text{template}})_i\).

The reference template is selected as the signature having the lowest average distance to all the other enrollment signatures. The evaluated distances describe the users' signature variability, and are employed to normalize the DTW distances computed during authentication.

Specifically, each test signature is compared to the signatures in the reference set, thus producing the aforementioned three distance values, which are then normalized with respect of the corresponding average distances computed over the reference set. A three-dimensional feature vector is therefore obtained from each comparison. It is worth pointing out that the same normalization process is done both for signatures acquired during enrollment, and for signatures considered during the authentication process.

Using Principal Component Analysis (PCA) (Duda, Hart, & Stork, 2000), the dimensionality is reduced from three to one (the three features are highly correlated). A Linear Discriminant Classifier (LDC), or, in alternative, a Linear Support Vector Machine (LSVM), is then trained on this feature space.\(^1\)

In the performed experimental results, illustrated in Section 4, the DTW approach is tested employing different sets of functional features. The feature sets which allow to reach the best authentication rates are then combined by means of the sum rule.

### 3.3. Hidden Markov Models (HMM)

Following this approach, a left-to-right HMM is used as in Fierrez-Aguilar, Nanni et al. (2005). Each signature is represented using a set of seven discrete-time sequences \((x, y, p, \theta, v, \rho, a)\), together with their first-order time derivatives, resulting in a signature template consisting of 14 discrete sequences. For more details on the left-to-right Hidden Markov Models, please refer to Fierrez-Aguilar, Nanni et al. (2005).

It is worth pointing out that this approach was ranked in first and second place, for random and skilled forgeries, respectively, during the Signature Verification Competition 2004 (SVC 2004) (Yeung et al., 2004).

### 3.4. Linear Programming Descriptor (LPD)

LPD\(^2\) is a one-class classifier, which is therefore able to determine if a test sample belong to the considered class or not. When applied to signature verification, each individual represents a class, and his signatures are the objects which have to be classified. The description of the target objects is usually obtained by means of parametric feature vectors. For a detailed description of this method see Tax (2001), where a data descriptor is specifically constructed to describe target objects which are classified in terms of distances to other classes.

In the proposed implementation, a LPD is trained employing the set of 100 global features detailed in Fierrez-Aguilar, Nanni et al. (2005).

Moreover, in order to significantly improve the performance of

---

\(^1\) We use the MATLAB function ldc() of the PRTools 3.1.7.

\(^2\) LPD is implemented as in the free DD_Tool 0.95 Matlab Toolbox.
a stand-alone LPD (Nanni, 2006), a random subspace ensemble of features (Ho, 1998) is employed. Specifically, in this work our LPD matcher is based on 100 different training sets\(^3\) created using random subspace. When performing authentication, the maximum similarity score (Kittler, Hatef, Duin, & Matas, 1998) obtained from the pool of 100 classifiers is selected as representative of the matching process.

3.5. BioHashing protection approach (BH)

The BioHashing template protection approach (Teoh et al., 2006) modifies an original biometric template \( t \in \mathbb{R}^n \) in order to generate a biometric vector \( f \in (0.1)^m (m \leq n) \). A pseudo-random number generator is employed to rule the generation of the binary vector, whose expression is therefore dependent on a randomly selected Hash key \( K \). Moreover, a preset threshold \( \tau \) is used to determine the binary vector \( f \). The matching between a test and a reference signature is then computed by means of the Hamming distance between the templates generated by employing the Hash key \( K \).

In Lumini and Nanni (2007) the authors suggested to iterate \( k \) times the BioHashing method, in order to generate \( k \) BioHash codes for each user (\( k = 5 \) in this work). Moreover, they proposed to normalize each biometric vector by its module, and to use several values for \( \tau \) instead of a fixed one (\( \tau \in [-0.1, 0.1] \), with step of 0.05). The verification stage is performed by using the Hamming Distance for each BioHash code, and by combining the \( k \) classifiers with the sum rule. Please refer to Lumini and Nanni (2007) for more details on the Improved BioHashing.

3.6. BioConvolving protection approach (BC)

The generation of cancelable biometrics according to the BioConvolving approach was proposed in Maiorana et al. (2008). Specifically, following this approach it is possible to build transformed templates that can be used for training any function based matcher.

In order to generate a transformed template, each original signature sequence is divided into \( W (W = 2 \text{ in this paper}) \) non-overlapping segments, according to a randomly selected transformation key \( d \). Then, the transformed functions are obtained by performing a linear convolution between the obtained segments. An example of the employed transform is given in Fig. 3, where the \( x \) and \( y \) coordinates of a given signature are modified according to two different keys.

In the present work, each original sequence is normalized to zero mean and unit standard deviation, before performing the convolutions. Moreover, in order to improve the verification performance, we iterate \( k \) times (\( k = 5 \)) the BC method, and combine the obtained similarity scores by means of the sum rule.

The security of the BioConvolving approach depends on the fact that, if an impostor gains access to the stored information, he has to resolve a blind deconvolution problem to retrieve the original template. Moreover, in Maiorana et al. (2008) it was also shown that even if multiple transformed templates are stolen, it is not possible to retrieve the original template.

4. Experimental results

An extensive set of experimental results has been performed using the public SUBCORPUS-100 MCYT (Ortega-Garcia et al., 2003; Ortega-Garcia, Fierrez-Aguilar, Simon, et al., 2003), which comprises signatures taken from 100 subjects. Specifically, 25 genuine signatures are available for each signer, as well as 25 skilled forgeries, which are produced by providing to the forgers the signature images of the clients to be forged.

For each user, the enrollment is performed on the basis of his first five genuine signatures. Moreover, in order to train the employed classifiers, the skilled forgeries of 20 individuals are considered. The authentication tests are therefore performed by considering the remaining 80 subjects of the available database. The similarity score which are then evaluated when testing each approach consist of 80 \( \times \) 20 matching scores from genuine users, and 80 \( \times \) 25 matching scores from impostors. Specifically, the employed database with 100 subjects is divided five times in different ways, in order to generate the training and the testing subsets, and the reported verification results correspond to the average of the performances obtained for each division.

As for the performance evaluation, we adopt the Equal Error Rate (EER) (Jain et al., 2002) and the Area Under the Receiver Operating Characteristic curve (AUC) (Ling, Huang, & Zhang, 2003). The AUC can be interpreted as the probability that the system will assign a higher score to a randomly picked genuine example than to a randomly picked impostor sample: the greater the AUC value, the better the performance of the considered system.

In order to properly evaluate the proposed ensemble and the template protection methods, the following aspects have been investigated:

- Which is the best feature set and the best classifier we can use to design a DTW based authentication system?
- Which is the matching performance of the novel ensemble method, based on the fusion of the considered local, regional and global classifiers (each of which can be considered as the state-of-the-art approach of their categories)?
- Which is the matching performance of the novel signature based authentication system with protected templates, obtained by combining the BH and the BC protection approaches? Moreover, Which is the loss in matching performance between the proposed unprotected and protected systems?

The aforementioned aspects are analyzed in the following Sections.

4.1. Feature and classifier selection for a local based approach

In this Section, we analyze the authentication performance which can be achieved when employing a local function based verification approach. Specifically, the DTW based approach of Kholmatov and Yanikoglu (2005) is considered, and different implementation of this algorithm are tested, by varying the feature set, as well as the used classifier. The original configuration, proposed in Kholmatov and Yanikoglu (2005), employs the \( \Delta x \) and \( \Delta y \) coordinates as feature set, and a LDC as classifier.

In Tables 1 and 2 we compare the performance, in terms of EER and AUC, of some variants of the method in Kholmatov and Yanikoglu (2005), obtained using a different classifier, that is, a Linear SVM (LSVM) instead of LDC, and different sets of features.

Please note that, in all the reported tests, the reference set used for the normalization of the distances in Kholmatov's variants coincides with the training set. Moreover, in the training step, the impostors' patterns (notice that the Kholmatov's methods extract a feature vector comparing a given signature with a reference set) are obtained considering for each individual only the forgeries of that individual: we compare each forgery of an individual \( i \) with each signature that belong to the reference set of the same individual \( i \).

\( ^3 \) Each modified training dataset contains a random subset (60\% in this paper) of all the features.
As can be seen from the results reported in Tables 1 and 2, slightly better results can be obtained when employing a LSVM classifier, with respect to the performances obtained with a LDC classifier, as proposed in Kholmatov and Yanikoglu (2005). The feature set which guarantees the best recognition rates comprises the $D_x$ and $D_y$ signature signals, as noticed in Kholmatov and Yanikoglu (2005). However, similar results can be achieved when employing the signals $D_y$ and $D_p$ as feature set.

On the basis of the observed results, we therefore implement a variation of the DTW based approach proposed in Kholmatov and Yanikoglu (2005), by selecting two distinct feature sets:

- $D_x$ and $D_y$;
- $D_y$ and $D_p$.

and employing a LSVM classifier to train the considered feature spaces. The system generated from the fusion of these two variants by the sum rule, is indicated as Extended Kholmatov (EK), and it is able to achieve an EER equal to 4.96%, with an AUC of 0.988. The proposed local matching based verification system therefore outperforms the one in Kholmatov and Yanikoglu (2005), which can guarantee an EER equal to 5.5% with an AUC of 0.986.

### 4.2. Performances of the proposed ensemble of matchers

In this Section we compare the matching performance of the novel ensemble method with respect to the three different approaches used in the fusion. In Table 3 we report the results

![Fig. 3. Application of two different BC transformations to the $x$ and $y$ coordinates of a given signature. The original and transformed signatures are also shown.](image-url)

| Table 1 | EER (in %) of some variants of the method in Kholmatov and Yanikoglu (2005). |
|---------|-----------------|-----------------|
| EER     | Classifier      | Features        |        |
|         |                 | LDC             | LSVM   |
| $\langle D_x, D_y \rangle$ | 5.5 | 5.3 |
| $\langle D_x, D_p \rangle$ | 6.2 | 6.3 |
| $\langle D_x, D_b \rangle$ | 11.9 | 11.6 |
| $\langle D_y, D_p \rangle$ | 5.6 | 5.6 |
| $\langle D_y, D_b \rangle$ | 11.2 | 11.0 |
| $\langle D_p, D_b \rangle$ | 9.6 | 9.5 |
| **Average** | **8.3** | **8.2** |

| Table 2 | AUC of some variants of the method in Kholmatov and Yanikoglu (2005). |
|---------|-----------------|-----------------|
| AUC     | Classifier      | Features        |        |
|         |                 | LDC             | LSVM   |
| $\langle D_x, D_y \rangle$ | 0.986 | 0.986 |
| $\langle D_x, D_p \rangle$ | 0.980 | 0.980 |
| $\langle D_x, D_b \rangle$ | 0.943 | 0.946 |
| $\langle D_y, D_p \rangle$ | 0.984 | 0.985 |
| $\langle D_y, D_b \rangle$ | 0.953 | 0.954 |
| $\langle D_p, D_b \rangle$ | 0.957 | 0.958 |
| **Average** | **0.967** | **0.968** |

<table>
<thead>
<tr>
<th>Table 3</th>
<th>Results obtained by the weighed sum of EK, HMM and LPD.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Weights</strong></td>
<td><strong>Indicators</strong></td>
</tr>
<tr>
<td>EK</td>
<td>HMM</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>
obtained by our ensemble using different combinations of weights in the sum rule. The considered approaches are denoted by the following abbreviations:

- **EK**, the local based approach employing the fusion of two Kholmatov’s variants, discussed in Sections 3.2 and 4.1;
- **HMM**, the regional based approach employing Hidden Markov Models as matcher, described in Section 3.3;
- **LPD**, the global feature based approach employing Linear Programming Descriptor as matcher, described in Section 3.4.

It is worth noticing that, before performing the fusion, the scores of each classifier are normalized to mean 0 and standard deviation 1.

The results in Table 3 have been obtained by empirically setting the weights used for the fusion, while for improving the performance this choice should be achieved by an optimization process on a training set. Anyway, from the available results the usefulness of the fusion of all three approaches is evident. Specifically, we can see that the proposed EK approach allows to reach the best verification performances for a stand-alone system. The LPD approach, which employs global features, performs better than the HMM one. When combining the two best approaches, that is, the EK and the LPD methods, a significant performance improvement can be obtained, resulting in an EER equal to 4.40%, and an AUC equal to 0.991. Moreover, a further improvement can also be achieved when considering an ensemble of the three classifiers: in this case, the best recognition rate corresponds to an EER equal to 3.81% and an AUC of 0.997. It is worth remarking that the reported results are referred to a system where only five signatures are taken from each user during enrollment, and that the algorithm proposed in Kholmatov and Yanikoglu (2005), which gave the best authentication results in SVC 2004 (Yeung et al., 2004), achieve an EER equal to 5.5% under the same conditions.

4.3. Performances of the proposed protected system

Finally, the verification performance of proposed ensemble of template protection approaches is investigated. As illustrated in Section 3, the proposed protected system is built by combining the BioHashing and the BioConvolving methods, respectively presented in Luminii and Nanni (2007) and Maiorana et al. (2008). It is worth pointing out that the BioHashing is a matching system that requires a fixed length feature vector as input, and uses the Hamming distance for classification purposes. On the other hand, the BioConvolving is a feature transformation approach, which projects an input feature vector in a transformed space having the same dimension of the original one and, therefore, can be coupled to any matching system which represents the considered biometrics with a set of sequences.

In Table 4 the results obtained for a system where only cancelable template are used are reported. Specifically, we performed tests by the BioHashing approach (BH) and by training the proposed EK, HMM and LPD with the cancelable templates provided by the BC approach. It is worth stressing that, in order to improve the achievable verification rates for the EK and the HMM methods, the BC transformations are applied five times to the available signatures, and the similarity scores obtained from the matching of these five cancelable templates are then combined by means of the sum rule. As for the LPD method, a different BC cancelable template is built for each random subspace, and the scores resulting from each LPD classifier are then combined by sum rule. Two different scenarios have been taken into account: a worst case scenario, when an attacker is able to steal the keys of the employed transformations, and a scenario where each impostor does not possess the transformation keys.

When considering the worst case scenario, it can be noticed that the best performance for a protected system employing a stand-alone classifier is met when using the standard Kholmatov’s method in Kholmatov and Yanikoglu (2005), together with the BC baseline approach proposed in Maiorana et al. (2008), and correspond to an EER equal to 12.95, with an AUC of 0.927. On the other hand, the BH protection approach performs better when the impostors do not know the employed transformation keys, reaching an EER ~ 0. The BC protection approach can be employed to implement an ensemble of protected systems, by combining the EK, the HMM, and the LPD matchers. An EER equal to 4.60%, with an AUC of 0.987, can then be achieved for a protected system, even when the impostors can steal the transformation keys. However, overall better recognition rates are obtained when combining the BC based approaches with the BH method: following such approach, an impressive EER equal to 4.51%, with an AUC of 0.988, is obtained for the worst scenario with stolen keys. Moreover, when the impostors do not know the employed transformation keys, we obtain EER = 0.36%, with an AUC of 0.999.

Notice that using the standard Kholmatov’s method and the base approach proposed in Maiorana et al. (2008) we obtain an EER 12.95 of and an AUC of 0.927. The performance of BC + HMM using only one BC cancelable template is (when the key is stolen) an EER of 9.82 and an AUC of 0.956; instead when the key is stolen BC + HMM obtains an EER of 2.30 and an AUC of 0.9948.

The last reported experiment is referred to a system where the BH approach is combined with the standard EK, HMM and LPD matchers (and therefore it is considered as a matcher rather than a template protection technique). In Table 5 we report the performance obtained when an “impostor” is always able to steal the

---

<table>
<thead>
<tr>
<th>Method</th>
<th>Hash key always stolen</th>
<th>Hash key never stolen</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EER (in %)</td>
<td>AUC</td>
</tr>
<tr>
<td>BH</td>
<td>10.74</td>
<td>0.956</td>
</tr>
<tr>
<td>BC + EK</td>
<td>11.78</td>
<td>0.944</td>
</tr>
<tr>
<td>BC + HMM</td>
<td>7.45</td>
<td>0.968</td>
</tr>
<tr>
<td>BC + LPD</td>
<td>12.71</td>
<td>0.942</td>
</tr>
<tr>
<td>0</td>
<td>4.60</td>
<td>0.987</td>
</tr>
<tr>
<td>1</td>
<td>4.89</td>
<td>0.985</td>
</tr>
<tr>
<td>0</td>
<td>5.61</td>
<td>0.980</td>
</tr>
<tr>
<td>1</td>
<td>5.98</td>
<td>0.977</td>
</tr>
<tr>
<td>1</td>
<td>4.94</td>
<td>0.987</td>
</tr>
<tr>
<td>0</td>
<td>5.13</td>
<td>0.985</td>
</tr>
<tr>
<td>1</td>
<td>4.51</td>
<td><strong>0.988</strong></td>
</tr>
</tbody>
</table>

*If we combine these classifiers with the max rule (as when we use the standard biometric template) the performance is very low.*
hash key, as well as those achieved when the key is not stolen.

The obtained experimental results confirm what already stated in other works (Lumini & Nanni, 2007): the fusion among a Bio-Hashing matcher and a pure biometric approach is extremely useful to improve the verification performance, also in cases when the hash key is stolen. In fact, the resulting lowest EER is equal to 3%, with an AUC of 0.994. In our opinion, the results obtained combining the biometric matchers with the BH approach are very interesting. Unfortunately, it is worth pointing out that the employed EK, HMM and LPD biometric matchers are not based on a cancelable template, in this case. So this system can be used only when the cancelable templates are not essential. Otherwise, the best verification rates obtained for a protected system corresponds to an EER equal to 4.51%. However, we have proven that a system where the employed templates are protected against possible attacks can be efficiently implemented, with only a slight loss in performance with respect to the best achievable unprotected system.

5. Conclusions

We introduced a system for on-line signature verification that outperforms several state-of-the-art methods. The main contribution of our work is to propose and validate a new system, which employs a combination of different kind of matchers based on local, global and regional features. It is experimentally shown that the system here proposed outperforms also the method which gave the best verification results in SVC 2004. The best EER which can be achieved employing the proposed combination of matchers is an impressive 3%. Therefore, our results testify that a very low EER can be achieved by employing on-line signature verification, which can then be employed in real world applications, just as fingerprint and iris.

In our opinion, the results obtained when employing the Bio-Hashing template protection scheme, and also the BioConvolving protection approach, are very interesting since we have shown that also using template protection techniques it is possible to obtain a very low EER (4.51% in the worst case scenario, with impostors able to steal the transformation keys).

A possible future work for improving the performance is to use the ensemble of global matcher proposed in Nanni and Lumini (2008a), Nanni and Lumini (2009), where the training data are used to create the different subspaces for training each matcher.

Acknowledgment

The authors would like to thank J. Ferrer-Aguilar and J. Ortega-Garcia for sharing SUBCORPUS-100 MCYT data set. Moreover, the authors want to thank J. Ferrer-Aguilar for the helpful discussions on on-line signature when he was a visiting researcher at the University of Bologna, Italy.

References


