Exploiting Data Redundancy for Error Detection in Degraded Biometric Signatures Resulting From in the Wild Environments

João Neves and Hugo Proença

1 IT - Instituto de Telecomunicações, Department of Computer Science, University of Beira Interior, Covilhã, Portugal

Abstract—An error-correcting code (ECC) is a process of adding redundant data to a message, such that it can be recovered by a receiver even if a number of errors are introduced in transmission. Inspired by the principles of ECC, we introduce a method capable of detecting degraded features in biometric signatures by exploiting feature correlation. The main novelty is that, unlike existing biometric cryptosystems, the proposed method works directly on the biometric signature. Our approach performs a redundancy analysis of non-degraded data to build an undirected graphical model (Markov Random Field), whose energy minimization determines the sequence of degraded components of the biometric sample. Experiments carried out in different biometric traits ascertain the improvements attained when disregarding degraded features during the matching phase. Also, we stress that the proposed method is general enough to work in different classification methods, such as CNNs.

I. INTRODUCTION

Biometric systems work by extracting distinctive sets of features from body traits, which subsequently fed a classifier to determine the subject identity. Usually, the feature encoding process is performed using handcrafted descriptors yielding a compact representation, but still highly redundant [3],[17].

The use of data redundancy is a key assumption in error-correcting codes (ECC). In these approaches, redundant data are generated and added to the encoded representation in a deterministic manner using pre-built models. As an illustration, Fig. 1 depicts the operation mode of convolutional codes, where it can be observed the main insight of ECC: an observed variable $o_i$ can be determined to be noisy by analyzing the previous observations $o_1, o_2, ..., o_{i-1}$ to which the $o_i$ is dependent. In this context, an error is defined as an impossible observed value given a set of past observed values.

Motivated by the fact that most biometric methods rely on redundant descriptors to perform classification, we follow the principles of ECC to develop a method capable of detecting corrupted features in biometric signatures by relying on the correlation between subsets of features.

Unlike the existing biometric cryptosystems, the proposed method works directly on the biometric signatures. This is advantageous for highly-degraded signatures but introduces different challenges. First, feature vectors obtained from different biometric traits do not follow deterministic relations between their components as in the case of ECC methods. Second, features dependencies greatly vary with respect to the type of data. To address these problems, our approach infers feature correlations from training data and a relaxed error definition is introduced: the soft assignment of the $i^{th}$ to a corrupted state is modeled by the likelihood of observing $o_i$ given $\{o_j, j \in D\}$, being $D$ the indices of the features to which $i$ is dependent. The proposed model operates in two phases: 1) redundancy analysis; and 2) state inference. While the former determines the dependent pairs of features, the latter analyzes these relations to decide - at test time - the most likely set of corrupted components given an observed probe descriptor. In this phase, inference is performed with a Markov Random Field (MRF) because it is a straightforward encode both unary costs and pairwise constraints between features.

To illustrate the usefulness of the proposed method, we assess the performance improvement of different biometric recognition methods when coupled with the proposed error detection method. Also, we report the performance in an image classification dataset using Convolutional Neural Networks (CNN) descriptors, in order to show the flexibility of the proposed approach.

The remainder of this paper is organized as follows: Section 2 summarizes the most prominent applications of ECC in the biometrics field. Section 3 provides a description of the proposed model. Section 4 regards the empirical evaluation and the corresponding results. Finally, the conclusions are given in Section 5.

II. RELATED WORK

Error control techniques operate either by adding check bits to the original message (systematic scheme) or encoding the message in a specific representation (non-systematic). The rationale behind both approaches is the augmentation of the transmitted message size by adding redundant data. The deterministic relations between the new representation and the original data allow the decoder to check if an encoded message is valid, locate the corrupted components, and in some techniques recover the original data.

Linear ECC are one kind of systematic scheme widely used in biometric cryptosystems [18],[6],[15]. Let $H$ be an $N$-dimensional Hamming space, linear ECC methods work by mapping input data to elements of $H$, denoted as codewords. The set of valid codewords, usually denoted as $C$,
are chosen such that they are separated at least by a Hamming
distance of \( d \). Correction is performed by transforming an
encoded sequence to the its nearest codeword in \( C \). This
strategy ensures a correct assignment if no more than \( \left\lfloor \frac{d+1}{2} \right\rfloor \)
bit errors occur [10].

In [2], [6], [7], [8], [11], [14], different linear ECC
methods, such as the Hadamard codes, Reed-Solomon codes
and the low-density parity-check codes, are used to correct
errors in iris codes. However, these methods are highly
limited by the number of errors than can be corrected in
the original feature vector, restraining their applicability to
data with large intra-class variations.

As an example, the work of Kanade et al. [8] introduces a
novel way to use ECC to reduce the variabilities in biometric
data by using Hadamard codes in a block-wise manner. Even
though these codes ensure successful regeneration up to 25%
of bit corruptions in the encoded message, this percentage is
reduced exponentially in the original feature vector.

Aiming at extending the applicability of ECC methods,
the Error-Correcting Output Codes (ECOC) were introduced
as a machine learning ensemble method. This approach is
believed to improve performance both by decomposing the
multi-class problem into a number of two-class problems, as
well as by correcting errors in the decision-making stage [4].
Different biometric recognition methods exploit variations of
this technique [21], [9]. A prominent example is the face
verification method of Kittler et al. [9], where the authors
assume that multiple images of the same client identity
are available, and the verification score is determined by a
statistical test using first order Minkowski distance.

III. PROPOSED METHOD

We first define the notation used to describe the proposed
approach.

- \( F_c \): the set of feature vectors obtained from non-
degraded data;
- \( F_d \): the set of feature vectors obtained from degraded
data;
- \( F = F_c \cup F_d \);
- \( f_i \): the \( i^{th} \) component of a feature vector;
- \( c_i = \{0,1\} \): the state of \( f_i \) determining if the compo-
nent is corrupted (1) or not (0).

As illustrated in Fig. 2, the proposed model is composed
of two phases: 1) redundancy analysis and 2) state inference.
The first aims at determining the pairs of features that are
related, allowing the latter phase to exploit this informa-
tion to infer the sequence of states that best explains the
observed data.

A. Redundancy Analysis

Contrary to ECC methods, where bit dependence is pre-
determined using handcrafted state transition models, the
proposed method requires the inference of data redundancies
from training data. For this purpose, we rely on the Pearson
correlation to determine the pairwise dependence between all
feature pairs. This produces the correlation matrix \( M \) that is
used to determine the indices to which the \( i^{th} \) is connected:

\[
L(i) = \{ j | M(i,j) \geq \nu \},
\]

where \( \nu \in [0,1] \) denotes the minimum confidence degree
for considering two components as dependent.
is used to determine the pairs that in-
vertices, representing the components of
i
\in
\{0,1\}
and subsequently derive
\text{corrupted given an observed }
\hat{\theta}_{1,j}(v_i,v_j) \propto P(f_i,f_j)
\text{and }
\hat{\theta}_{0,j}(v_i,v_j) \propto P(f_i,f_j)
\text{are the labels of the }
\text{corrupted }
\{0,1,0,0,1\}
\text{determines } f_2
\text{and } f_5
\text{as being corrupted.}
\text{In this paper, the MRF was optimized according to the }
\text{Loopy Belief Propagation [5] algorithm. Even though it is }
\text{not guaranteed to converge to a global minimum on loopy }
\text{non-submodular graphs (such as our MRF), we concluded that }
\text{the algorithm provides good approximations (refer to Section IV).}
\text{B. State Inference}
\text{The proposed model is depicted in the Fig. 2 and is }
\text{composed by } n_v \text{ vertices, representing the components of }
\text{the feature vector. Also, to each vertex can be assigned one }
\text{label } \{0,1\}, \text{denoting whether a component of the feature }
\text{vector is corrupted or not. The rationale behind this structure }
\text{is threefold: 1) the dependence between features can be }
\text{modeled with the existence of edges between vertices; 2) }
\text{the probability of a feature being corrupted given a subset }
\text{of observed features can be modeled by pairwise costs; 3) the }
\text{probability of a feature being corrupted given its observed }
\text{value can be represented by the unary potentials. }
\text{Let } G = (V, E) \text{ be a graph representing a MRF, composed }
\text{of a set of } n_v \text{ vertices } V, \text{linked by } n_e \text{ edges } E. \text{The MRF }
\text{is a representation of a discrete latent random variable } L =
\{L_i\}, \forall i \in V, \text{where each element } L_i \text{ takes one value } l_u
\text{from a set of labels.}
\text{In this problem, a MRF configuration } l = \{l_1, \ldots, l_{n_v}\}
\text{determines the set of corrupted components of the feature }
\text{vector. The number of edges in } G \text{ is determined by the }
\text{pairwise dependence between features, i.e., the vertices are }
\text{connected if and only if the feature pair } (i,j) \text{ is redundant }
\text{(discussed in Section III-A). Each edge encodes the cost of }
\text{assigning the class } l_u \text{ to the } i^{th} \text{ feature vector component }
\text{and the class } l_v \text{ to the } j^{th} \text{ feature vector component.}
\text{The energy of a configuration } l \text{ of the MRF is the sum of the }
\text{unary } \theta_i(l_u) \text{ and pairwise } \theta_{i,j}(l_u,l_v) \text{ potentials: }
\text{E}(l) = \sum_{i \in V} \theta_i(l_u) + \sum_{(i,j) \in E} \theta_{i,j}(l_u,l_v). \quad (2)
\text{According to this formulation, determining the corrupted }
\text{components of the feature vector is equivalent to infer the }
\text{random variables in the MRF by minimizing its energy: }
\hat{l} = \arg \min_l E(l), \quad (3)
\text{where } \hat{l}_1, \ldots, \hat{l}_{n_v} \text{ are the labels of the } n_v \text{ feature vector }
\text{components. As an example, if a five length feature vector }
\text{is considered, the configuration } \{0,1,0,0,1\} \text{ determines } f_2
\text{and } f_5 \text{ as being corrupted.}
\text{C. Unary and Pairwise Potentials}
\text{Let } X_u \in F_u \text{ and } X \in F \text{ be samples acquired during the }
\text{training phase. These data can be used to determine the }
\text{posterior probability of } f_i \text{ being corrupt given an observed }
\text{value of this component, which according to the Bayes theorem is }
\text{defined as:}
\text{P}(c_i | f_i) = \frac{P(f_i | c_i) P(c_i)}{P(f_i)}. \quad (4)
\text{Considering that during the training phase it may be }
\text{cumbersome to obtain a sample from } F_{d_i}, \text{it is not possible to }
\text{obtain } P(f_i | c_i = 1) \text{ in a straightforward way. Consequently, }
\text{we use } X \text{ to estimate } P(f_i) \text{ and subsequently derive } P(c_i =
Fig. 3. Comparison between the iris noise mask obtained from [13] and the degraded regions inferred from our approach. a) Original iris code. b) Iris noise mask of [13]. c) Degraded components identified by our method reshaped to the original iris code size. Note that our approach was able to identify non-iris regions, whereas the geometric-based approach used in [13] overestimated the boundaries of non-iris regions.

1 | $f_i$) from its complement. The unary costs are thus defined as $\theta_i(l_u) = 1 - P(c_i = l_u | f_i)$.

While the unary potentials disregard any information from neighbors and are meant to emphasize the necessity of each observation being coherent with the typical distribution of the $i^{th}$ feature vector component, the pairwise potentials model the observation of $f_i$ being coherent with the observed value of $f_j$, to which $f_i$ depends. Again, this can be measured using the posterior probability of $f_i$ being corrupt given an observed value of $f_i$ and $f_j$, which according to the Bayes theorem is defined as:

$$P(c_i | [f_i, f_j]) = \frac{P([f_i, f_j] | c_i) P(c_i)}{P(f_i, f_j)}.$$  \hspace{1cm} (5)

The pairwise costs between two adjacent vertices $\theta_{i,j}(l_u, l_v)$ are then defined as:

$$\theta_{i,j}(l_u, l_v) = \begin{cases} P(l_u, l_v | [f_i, f_j]), & \text{if } l_u = 0 \text{ and } l_v = 0, \\ 0.5, & \text{if } l_u \neq l_v, \\ 1 - P(l_u, l_v | [f_i, f_j]), & \text{otherwise.} \end{cases} \hspace{1cm} (6)$$

Similarly to the unary costs, $P([f_i, f_j])$ is directly estimated from $X$.

D. Feature Matching

After obtaining the corrupted component mask $m^y$ of the probe descriptor $y$, feature matching should be modified to allow disregarding degraded components when determining the scores between $y$ and training samples $x$ using a classifier $\Phi$. Accordingly, the score is determined by:

$$s(x_i, y) = \Phi(m^y x_i, m^y y).$$  \hspace{1cm} (7)

IV. RESULTS AND DISCUSSION

The proposed method was validated in three distinct datasets, namely, the CASIA-Thousand [1], the AR-Database [12] and the ILSVRC [19]. While the first and the second regard biometric traits (iris and face, respectively), the latter was designed for use in visual object recognition. The rationale to include this set was to evidence the flexibility of the proposed approach. It should be stressed that no particular concerns were taken in optimizing the recognition methods for the used datasets, meaning that the focus was put in the performance gap between both recognition schemes than in the recognition errors in absolute values, which are out of the scope of this paper.

A. Iris Recognition Performance

To exemplify the usefulness of the proposed method for iris recognition, we compared the performance of Masek’s algorithm [13] using four strategies: 1) the original iris code (baseline); the masked iris code obtained from our error
Fig. 5. Comparison between the original performance of the recognition methods and the performance obtained by disregarding degraded components of the image descriptor during the matching phase. The image classification performance obtained with a CNN descriptor was assessed using CMC curves and the corresponding AUC (in parentheses).

detection approach; 3) the noise free iris code obtained from the original recognition method; and 4) the masked noise free iris code obtained from combining the second and third strategies.

The experiments were carried out in a subset of the CASIA-Thousand database that was obtained by manually discarding images segmented incorrectly. These data were subsequently separated into training and test sets, comprising 600 and 400 different eyes, with about 6000 and 4000 images, respectively. Additionally, we screened, through visual inspection, the training images to obtain a sample of $F_c$, i.e., a set of images where iris is not heavily occluded by eyelids, eyelashes, shadows, or specular reflections. At the end, 244 images were kept as a sample of $F_c$, while the 6000 training images were considered as a sample of $F$ (Fig. 6 show exemplars of these two sets).

The Receiver Operating Characteristic (ROC) curves and the corresponding Area Under Curve (AUC) for the described variants are compared in Fig. 4 and evidence the benefits of withdrawing corrupted features from the matching phase (0.97 vs 0.96 regarding AUC). However, the proposed method was not able to overcome the original method when coupled with its noise iris mask.

The comparison between the corrupted bit locations obtained from our method and the noise iris mask inferred from the Masek’s method is depicted in Fig. 3. It can be seen that our approach failed to identify some corrupt components. This can be explained by the fact that the iris noise mask was derived using mainly geometric-based information, which is not available to our method. Nevertheless, it should be noted that combining both masks - using bit intersection - outperforms the remaining variants, suggesting that noise regions identified by method of Masek were overestimated.

Fig. 6. Representative examples of the data used in the experiments. The first column illustrates images assigned to $F_c$ for being considered as non-degraded, while the remaining columns comprises both degraded and non-degraded images available in $F$.

B. Face Recognition Performance

Regarding face recognition, we used the AR database to determine the usefulness of the proposed method, since the design of this set ensured a clear distinction between the degradation factors of each image. In the experiments, non-degraded frontal images were used as training data, while images corrupted by varying illumination, occlusion and facial expression served as test data. For feature extraction, we relied on the VGG Face Descriptor [16], a CNN implementation based on the VGG-Very-Deep-16 architecture adapted for the task of face verification. In accordance to [16], data was fed to a pre-trained CNN and the 4,096-dimensional descriptor of the final Fully Connected (FC) layer was used as image descriptor. Fig. 4 depicts the Cumulative Match Characteristic (CMC) curves for baseline and the proposed method.

The explanation for this improvement lies in the fact that the state of a component is inferred in a consensual manner. For example, degradation factors affecting a particular region of the image (e.g., occlusions) may induce large deviations in some components of the image descriptor. In an unary-based approach, each component would only be classified as degraded in case of an extreme variation. On contrast, in our
method the value of a degraded component is considered incongruent with a subset of non-degraded observations, whose pairwise potentials force the component state to be corrupt in the final MRF configuration.

C. Image Classification Performance

In order to demonstrate the flexibility of our approach, we also assessed its performance in the field of image classification. For this purpose, we used the data available from the ILSVRC [19] - a state-of-the-art image classification challenge - containing 150,000 validation and test images of 1000 object categories. For each category, 75 images were corrupted to serve as test set, while the remaining images were used for training. Corruption was performed using synthetic occlusions (80 random patches of variable size), as illustrated in Fig. 6.

The image descriptors were extracted using one of the best performing methods on the ILSVRC 2014 challenge [20]. Again, we used the last FC layer of the pre-trained CNN, and the descriptors were compared with the L2 distance. The comparison between the CMC curves of Fig. 5 shows a performance improvement when correcting descriptors of images degraded by synthetic occlusions. Even though these occlusions are not realistic, it should be noted that the experiments on the ILSVRC set aimed only at evidencing the flexibility of the proposed approach.

V. CONCLUSIONS

In this paper, a method for determining degraded components of biometric signatures was introduced. Unlike ECC-based biometric cryptosystems, our approach works directly on the visual descriptor, providing additional robustness to high-magnitude errors and highly degraded feature vectors. The proposed method assumes that data redundancy in biometric signatures resulting from unconstrained scenarios can be used for the detection of degraded components. Though it seems a limiting assumption, the experiments show an improvement in the recognition performance when disregarding the degraded components during the matching phase. These results not only evidence the feasibility of the proposed method, but also suggest that visual descriptors actually contain redundant and low-entropy features.

As further directions for this work, we are currently investigating ways to simultaneously perform detection and correction of the degraded components.

A. Acknowledgements

This work is supported by ‘FCT - Fundação para a Ciência e Tecnologia’ (Portugal) through the project ‘UID/EEA/50008/2013’, the research grant ‘SFRH/BD/92520/2013’, and the funding from ‘FEDER - QREN - Tipo 4.1 - Formação Avançada’, co-founded by the European Social Fund and by national funds through Portuguese ‘MEC - Ministério da Educaçao e Ciência’.

REFERENCES