Journal of Computer Security 18 (2010) 161–185
DOI 10.3233/JCS-2010-0369
IOS Press

Biometric template protection in multimodal authentication systems based on error correcting codes *

Savvas Argyropoulos [a,b], Dimitrios Tzovaras [a,**], Dimosthenis Ioannidis [a], Yannis Damousis [a], Michael G. Strintzis [a,b], Martin Braun [c] and Serge Boverie [c]

[a] *Informatics and Telematics Institute, Centre for Research and Technology Hellas, Thermi-Thessaloniki, Greece*
[b] *Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Thessaloniki, Greece*
[c] *Continental Automotive, GmbH, Regensburg, Germany*

The widespread deployment of biometric systems has raised public concern about security and privacy of personal data. In this paper, we present a novel framework for biometric template security in multimodal biometric authentication systems based on error correcting codes. Biometric recognition is formulated as a channel coding problem with noisy side information at the decoder based on distributed source coding principles. It is shown that the proposed method binds the biometric template in a cryptographic key which does not reveal any information about the original biometric data even if it is compromised by an attacker. Furthermore, the advantages of the proposed method in terms of security and impact on matching accuracy are discussed. We assess the performance of the proposed method in the context of HUMABIO, an EU Specific Targeted Research Project, where face and gait biometrics are employed in an unobtrusive application scenario for human authentication. Experimental evaluation on a multimodal biometric database demonstrates the validity of the proposed method.

Keywords: Multimodal biometrics, authentication, biometric template security, distributed source coding

1. Introduction

Human identification has always been a field of primary concern in applications such as access control in secure infrastructures. In contrast to passwords or tokens which can be easily lost, stolen, forgotten, or shared, biometrics offer a reliable solution to the problem of identity management. Especially, the development of systems that integrate two or more biometric traits has received increased interest during the last years as the advantages of multimodal biometric systems become more evident.

*This work was supported by the European Commission under contract FP6-026990 HUMABIO.
**Corresponding author: Dimitrios Tzovaras, Informatics and Telematics Institute, Centre for Research and Technology Hellas, Thermi-Thessaloniki, GR 57001, Greece. Tel.: +302310464160; Fax: +302310464164; E-mail: dimitrios.tzovaras@iti.gr.

Most of the limitations imposed by unimodal biometric systems can be overcome by establishing identity based on multiple sources of information [15].

With the widespread deployment of biometric systems in various applications, there are increasing concerns about the security and privacy principles of biometric technology. Public acceptance of biometrics technology depends on the ability of system designers to demonstrate that these systems are robust, have low error rate, and are tamper proof. Biometric template security is an important issue because, unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. Protecting biometric templates is a challenging task due to intra-user variability in the acquired biometric traits. A template protection scheme with provable security and acceptable recognition performance has thus far remained elusive. Development of such a scheme is crucial as biometric systems are beginning to proliferate into the core physical and information infrastructure of our society.

In this paper, a novel authentication scheme for biometric template security in multimodal systems based on distributed source coding principles is proposed and emphasis is given on the secure storage of the biometric templates. The proposed framework is employed in one of the application scenarios of the Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis (HUMABIO) FP6 EU project [4], namely the airport pilot scenario, based on face and gait modalities, for non-stop and unobtrusive authentication of employees in a controlled area. Experimental results illustrate that the increased security of biometric templates comes at virtually no cost in the performance of the HUMABIO system compared to state-of-the-art machine learning techniques.

1.1. Problem statement

In biometric authentication systems, the user claims an identity and the measured biometric data (*probe*) are compared to the corresponding template(s) of the claimed identity (*gallery*), which have been previously stored in the database, during the enrolment stage. The biometric classifier expert compares the extracted biometric features (biometric *signature*) of the probe with the gallery signature and the system must decide whether the user is a *client* (*genuine* transaction, class ω_0) or an *impostor* (*unauthorized* transaction, class ω_1) based on a decision rule. Thus, the problem of person authentication is a detection problem which can be analyzed by means of a binary hypothesis test. The first hypothesis $H = \omega_0$ accepts a certain candidate claim for a client identity and the second hypothesis $H = \omega_1$ rejects this claim.

Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates. Some of these limitations can be addressed by deploying multimodal biometric systems that integrate the evidence presented by multiple sources of information. A multimodal biometric system uses multiple applications to capture different types of biometrics. This allows the integration of two or more types of biometric recognition and verification systems in order to

meet stringent performance requirements. A multimodal system can combine any number of independent biometrics and overcome some of the limitations arising when using just one biometric as the verification tool. For instance, it is estimated that approximately 3% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject. A multimodal system, which combines the conclusions made by a number of unrelated biometrics indicators, can overcome many of these restrictions. Multimodal biometrics is generally much more resistant to fraudulent technologies, because it is more difficult to forge multiple biometric characteristics than to forge a single biometric characteristic. Thus, HUMABIO aims at designing authentication systems that establish human identity based on multi-biometric evidence.

Another important issue in the design of a biometric system is robustness to fraudulent attacks. As described in [23], attacks in a biometric system can be perpetrated at the sensor, at the communication channel between the sensor or the database and the matcher, at the matcher itself, at the database of the system, and, finally, at the output of the system. In this paper, we focus on the protection of the templates which are stored in the database. A malicious user can steal a template both by intercepting communication through the channel between the database and the authentication system and by breaking into the databases. Although it was believed that it is not possible to reconstruct the original biometric templates from the extracted feature vectors, some counter examples have been developed for faces and fingerprints [29].

In password-based systems the corresponding problem of secure password storage has been investigated in depth and sophisticated encryption methods have been developed [27]. Specifically, prior to storage to the physical medium (e.g., hard disk, USB token), cryptographic codes are applied to the passwords and a hash code is generated with an one-to-one relationship to the original password. The irreversibility of the employed cryptographic codes renders the hash codes useless to the potential attackers of the system since the original data can not be recovered. It must be noted that irreversibility only holds up to the assumptions of the underlying scheme.

However, the representation of biometric traits is not fixed over time (intra-variability) due to changes in the biometric pattern, the environmental conditions, and the sensor. Thus, the existing cryptographic solutions used in password-based applications to enhance security can not be applied. This is due to the fact that the existing cryptographic solutions require the exact match of the prompted and the original signatures to grant access. While it is possible to decrypt the template and perform matching between the query and decrypted template, such an approach is not secure because it leaves the template exposed during every authentication transaction. Moreover, an adversary could compromise the decrypted template if he has access to the encryption algorithm. Thus, novel encryption methods need to be developed to take into account the noise introduced in the representation of the biometric traits and account for their inherent variability [14,30].

A biometric authentication scheme for secure biometric storage was proposed by the authors in [2]. A novel gait authentication scheme from gait sequences based on the extraction of a set of discriminative features was presented. Error correcting codes were employed to transform the stored templates and ensure biometric template privacy. Thus, a compromised biometric template reveals no information about the original biometric data (or the extracted features) of the subjects. However, this scheme can be employed only in unimodal systems. In this paper, we present how this scheme can be extended to the multimodal biometric scenario and highlight how the different modalities can interact and benefit from the other.

1.2. Related work

The biometric template protection schemes proposed in the literature can be broadly classified into two categories: feature transformations and biometric cryptosystems. In the feature transformation approach, a transformation function $\mathcal{F}$ is applied to the biometric template T and only the transformed template $\mathcal{F}(T; K)$ is stored in the database, as depicted in Fig. 1. The parameters of the transformation function are typically derived from a random key K or password. The same transformation function is applied to the probe features P and the transformed query $\mathcal{F}(P; K)$ is directly matched against the transformed template $\mathcal{F}(T; K)$.

Depending on the characteristics of the transformation function $\mathcal{F}$, the feature transform schemes can be further categorized as salting and non-invertible transforms. In salting, $\mathcal{F}$ is invertible, that is, if an adversary gains access to the key and the transformed template, the original biometric template can be recovered. Hence, the security of the salting scheme is based on the secrecy of the key or password. On the other hand, non-invertible transformation schemes typically apply a one-way function on the template and it is computationally hard to invert a transformed template even if the key is known. Again, it should be stressed that irreversibility only holds for the assumptions of the specific scheme. The main drawback of this approach is the tradeoff between discriminability and non-invertibility of the transformation function.

Biometric cryptosystems aim at generating a cryptographic key from biometric features. In a biometric cryptosystem, some public information about the biometric template is stored. This public information is usually referred to as *helper data*.

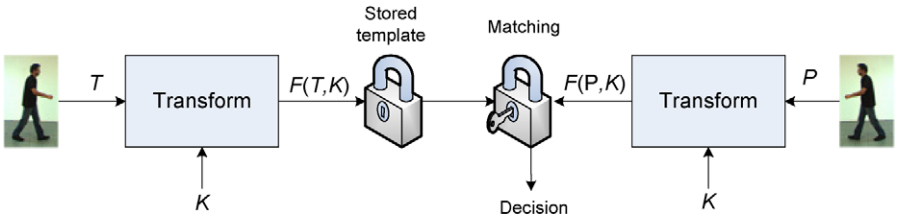


Fig. 1. Biometric template protection using feature transformation.

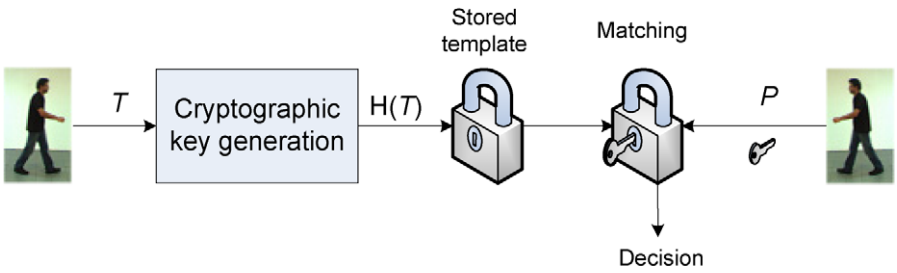


Fig. 2. Biometric template protection using feature transformation.

While the helper data does not reveal any significant information about the original biometric template, it is needed during matching to extract a cryptographic key from the query biometric features. Matching is performed indirectly by verifying the validity of the extracted key, as depicted in Fig. 2. Error correction coding techniques are typically used to handle intra-user variations. These systems perform typically better than feature transformation approaches [14] and the method proposed in this paper lies in this category.

The problem of secure biometric storage using cryptosystems was originally studied in [5]. Error correcting codes were employed to tackle the perturbations in the representation of biometric signals and classification was based on the Hamming distance between two biometric representations. This concept was extended in [16] where a cryptographic framework, called *fuzzy vault*, was developed to protect data in error-prone environments, such as biometric authentication systems, and Reed–Solomon (RS) codes were employed. Also, a biometric cryptosystem scheme was presented in [6] introducing the concept of secure sketch which was later used in [28] to develop a practical scheme for the protection of face images.

Moreover, a methodology based on channel codes and the Slepian–Wolf theorem [26] for secure biometric storage was presented in [19]. Specifically, Low-Density Parity Check (LDPC) codes were utilized for the development of an iris authentication system and security of the biometric templates was rigorously quantified. Additionally, a fingerprint recognition system based on statistical modelling of the enrolled and the measured data was presented in [7].

Furthermore, LDPC codes were also used for biometric authentication in [3]. Similarly to the fuzzy vault concept, the *fuzzy commitment* concept was introduced and the biometric authentication problem was considered as a wire-tap problem. A similar approach, but not in the context of biometric recognition, was presented in [18]. The multimedia authentication problem in the presence of noise was investigated, the theoretical limits of the system were identified, and the tradeoff among fidelity, robustness, and security was discussed. This approach provides intuition for the proposed method in this paper; the biometric recognition problem is considered as the analogous of data transmission over a communication channel, which determines the efficiency of the system. Interestingly, the problem of coding distributed correlated

sources has also attracted much interest in the field of video coding recently. In the seminal work of [22], the Distributed Source Coding Using Syndromes (DISCUS) scheme was proposed. Based on this work, the field of distributed video coding [11] has emerged as a new trend in video coding.

The main scope of this paper is to provide a framework for biometric template protection in multimodal biometric authentication systems. The proposed biometric cryptosystem is based on distributed source coding principles and formulates biometric authentication as a channel coding problem with noisy side information at the decoder. The main idea is that perturbations in the representation of the biometric features at different times can be modelled by a (virtual) noisy channel, which corrupts the original signal. Thus, the enrolment and authentication procedures of a biometric system are considered as the encoding and decoding stages of a communication system, respectively. This formulation enables the exploitation of the Slepian–Wolf theorem to identify the theoretical limits of the system and minimize the size of the templates. Moreover, casting the problem of biometric authentication as a communication problem allows the use of well known techniques in communication systems such as the exploitation of correlation (or noise) channel statistics by integrating them in the soft decoding process of the channel decoder.

2. Biometric authentication using distributed source coding

The Slepian–Wolf theorem addresses the problem of coding distributed (not co-located) sources and decoding them jointly, as depicted in Fig. 3(a). If we consider two random sequences X and Y that are encoded using separate conventional entropy encoders and decoders, the achievable rates are $R_X \geqslant H(X)$ and $R_Y \geqslant H(Y)$, where $H(X)$ and $H(Y)$ are the entropies of X and Y, respectively. However, if the two sequences are jointly decoded the achievable rate region according to the Slepian–Wolf theorem is defined by [26]:

$$R_X \geqslant H(X|Y), \qquad R_Y \geqslant H(Y|X), \qquad R_X + R_Y \geqslant H(X,Y), \tag{1}$$

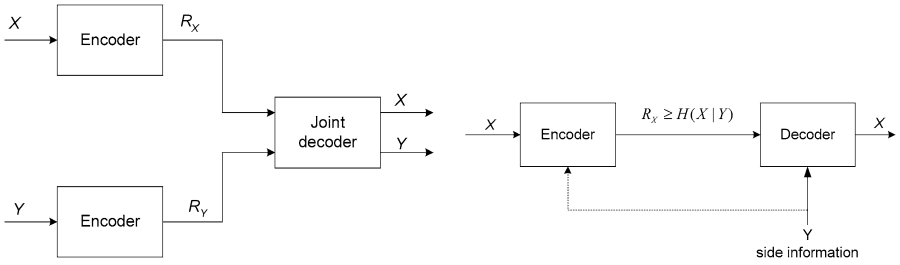


Fig. 3. Conventional source coding of correlated sources.

where $H(X|Y)$ and $H(Y|X)$ are the conditional entropies and $H(X,Y)$ is the joint entropy of X and Y.

The Slepian–Wolf theorem can be also applied in the problem of source coding with decoder side information (Fig. 3(b)). Specifically, if the sequence X is correlated with the sequence Y, which is available only at the decoder, but not at the encoder, the achievable rate for sequence X is $R_X \geqslant H(X|Y)$. Thus, even though the encoder does not have access to the correlated sequence Y, it can compress source X as if Y were available at the encoder. However, the Slepian–Wolf theorem does not provide a practical implementation of the described system.

Biometric authentication can be formulated as a problem of source coding with decoder side information if we consider the gallery and the probe signals as the random variables X and Y respectively. This representation is reasonable since the probe and the gallery signals are correlated and the probe is only available at the decoder (authentication) side. Let x[1] be the original representation of the biometric trait b at the enrolment stage at time t. In general, the probe and gallery data are not identical even in the case of client transactions due to time-related modifications in the biometric pattern, its presentation, and the sensor which captures the raw biometric data. The noise in the biometric signal b' can be modelled by a (virtual) additive noise (or correlation) channel which induces noise w. Thus, at the authentication stage, which takes place at time t', the biometric system needs to detect whether the input signal $y = x + w$ belongs to a genuine or an impostor user.

This model is analogous to data communication over noisy channels and is similar to the notion that Slepian–Wolf coding protects X for "transmission" over the (virtual) noisy channel. At the decoder, Y is regarded as if it were X after transmission over the noisy channel and corrects it using error correcting codes. Intuitively, the noise w_g induced by the channel in case of genuine transactions is small whereas the noise w_i in impostor transactions is relatively large. Thus, the channel decoder can decode the codeword only when the induced noise is small and the error is within the correcting capabilities of the channel code. Otherwise, if the noise of the channel corrupts the signal the resulting codeword can not be decoded and the transaction is rejected as unauthorized. If the selected error correcting code is suitable for error protection on this channel, the decoder will decode X errorlessly and the transaction is authenticated.

In this paper, we extend the Slepian–Wolf theorem to the case of four correlated sources X_1, X_2, X_3 and X_4 to handle multimodal biometric signals. Let R_i denote the rate for X_i, $i \in \{1,2,3,4\}$, then from the extension of the Slepian–Wolf theorem to multiple sources the achievable rate region is:

$$R(\mathbf{S}) > H(X(\mathbf{S})|X(\mathbf{S}^c)), \tag{2}$$

where $\mathbf{S} \subseteq \{1,2,3,4\}$, $R(\mathbf{S}) = \sum_{l \in \mathbf{S}}$ and $X(\mathbf{S}) = \{X_l\colon\ l \in \{1,2,3,4\}\}$.

[1] Throughout this paper, capital symbols will denote stochastic sequences and small symbols will denote their respective realizations.

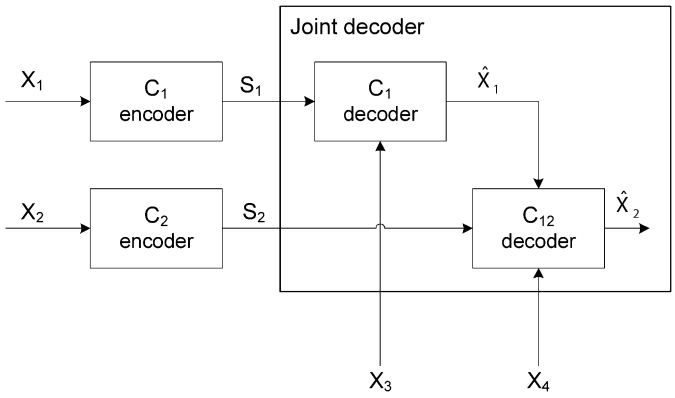


Fig. 4. Architecture of the proposed authentication system based on channel codes.

Figure 4 illustrates the architecture of the proposed biometric authentication method. At the enrolment (encoding stage), the sequences X_1, X_2, which represent the feature vectors of the two biometric signals, are encoded using two separate Slepian–Wolf encoders. The biometric signatures (or templates), which are stored in the database of the system, consist of the generated codewords S_1, S_2. The authentication stage (decoding) consists of two steps: first, X_1 is decoded using the corresponding decoder and X_3, which is the biometric signature corresponding to X_1 provided during the authentication stage. Then, the estimated version $\hat{X}_1$ of X_1 together with X_4 are the input to the second decoder to estimate X_2.

A critical parameter in the design of the system is the rate of the encoders. On one hand, a high rate generates long codewords which increases the security of the templates but also increases the risk of rejecting a legitimate user. On the other hand, a low rate generates small codewords which reduces the strength of the templates and increases the risk of accepting an impostor user. Thus, the design of an effective biometric system based on channel codes involves the careful selection of the channel code rate to achieve the optimal tradeoff between performance and security.

The minimum rate for the representation of the encoded sequences is given by Eq. (2). Since X_3 and X_4 are available at the decoder, X_1 and X_2 can be compressed at rates R_1 and R_2 lower bounded by Eq. (2). Thus, the rate R_1 of the first encoder is lower bounded by $R_1 \geqslant H(X_1|X_2)$ and the rate R_2 of the second encoder is bounded by $R_2 \geqslant H(X_2|X_1, X_3, X_4)$. Thus, we can modify the rate of the encoders to select the tradeoff between performance and security, as it will be analyzed in the following sections.

3. Multimodal biometric authentication framework

This section presents the integration of the proposed multimodal authentication framework in the HUMABIO system. Initially, the application scenario is briefly

described to highlight the unobtrusiveness of the authentication process. Next, we describe the feature extraction process of the gait and face modalities. Finally, we present the multimodal biometric authentication framework based on the distributed source coding principles, as described in Section 2, and quantify the security of the system.

3.1. Application scenario

HUMABIO is a Specific Targeted Research Project (STREP) that focuses its research on emerging and novel biometrics, aiming at enhanced unobtrusiveness of biometrics-based access control systems. Thus, HUMABIO takes into account varying factors and allows flexibility in the system operation. As an example, the face module is designed so that it can operate efficiently even with various facial expressions. However, increased unobtrusiveness has its toll on authentication accuracy. Even the more conventional HUMABIO biometrics (such as face) present lower accuracy than the corresponding algorithms in the literature since the latter results refer to strictly controlled conditions. In order to address this issue, multiple biometrics within HUMABIO are combined with the objective to increase the authentication accuracy of the multimodal system compared to the biometrics it comprises. Based on criteria such as unobtrusiveness level, maturity of the technology, and biometric capacity, face and gait biometrics were selected to be included in the airport application scenario of the HUMABIO system. The aim is to limit the cooperation of the user as much as possible, increase unobtrusiveness and user convenience and maximize user acceptance.

Unobtrusive authentication involves automatic authentication of authorized personnel that can move freely in restricted areas. The operational setup of the system, which is installed in a controlled area in Euroairport in Basel, Switzerland, is depicted in Fig. 5(a). The subject walks along a narrow corridor. When the subject enters the corridor the (claimed) identity is transmitted wirelessly to the system via radio frequency identification (RFID) tag. The aim of HUMABIO is to authenticate the claimed identity by the time the subject reaches the end of the corridor. As the subject walks through the corridor, the gait sequence is captured and the subject's height is estimated. Height information is used to calibrate the position of the camera, as depicted in Fig. 5(b). Face recognition take place at the end of the corridor. By the time the subject reaches the camera its position is already calibrated allowing the unobtrusive face recognition without the need of specific procedures for the collection of the biometric data as it is usually the case with current biometric solutions.

3.2. Face feature extraction

Face feature extraction is carried out in three steps: face detection, face normalization and subspace projection. These steps are described individually in the following sections. A diagram of the whole process carried out for face feature extraction is given in Fig. 6.

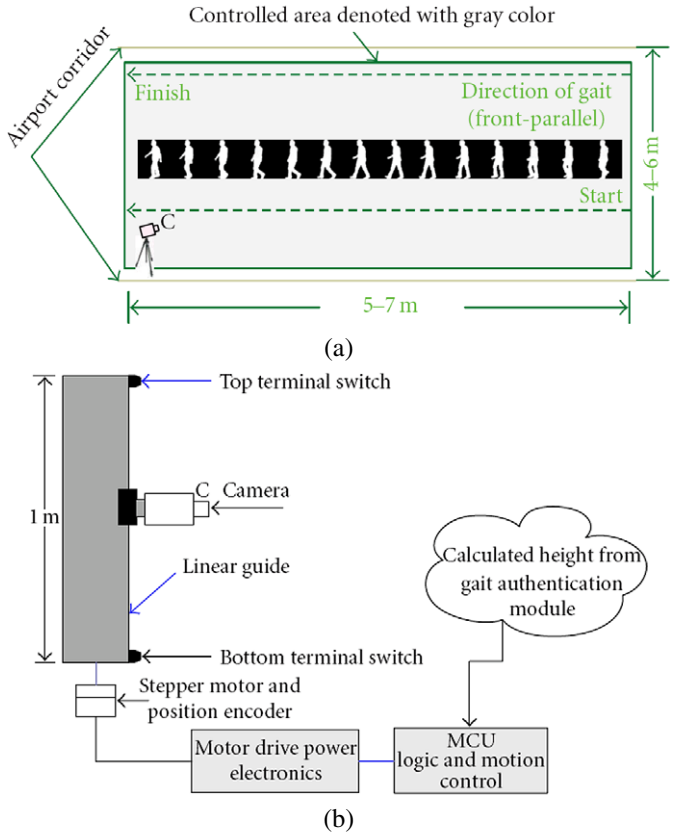


Fig. 5. The HUMABIO airport application scenario: (a) and (b) camera positioning based on height estimation.

(1) *Face detection:* The first step for facial feature extraction is the accurate localization of the area in an input image containing a face. The method applied is a component based approach using detectors similar to these proposed by Viola and Jones [33]. The eye and mouth regions are detected individually and their geometric constellation is verified [35] to eliminate false detections on the component level and geometrically normalize the face. The advantage of the component-based face detection approach over a full-face detection approach is its increased robustness to small in-plane and out-of-plane rotations of the detected face. Furthermore, faces can be localized more accurately and geometric normalization can be performed based on the positions of the components. An accurate localization with small variations in translation and rotation is crucial for further feature extraction.

(2) *Face normalization:* The detected face is normalized geometrically and photometrically before the final feature extraction step. An overview of normalization methods is given in [17]. Geometry normalization assures the detected faces all have

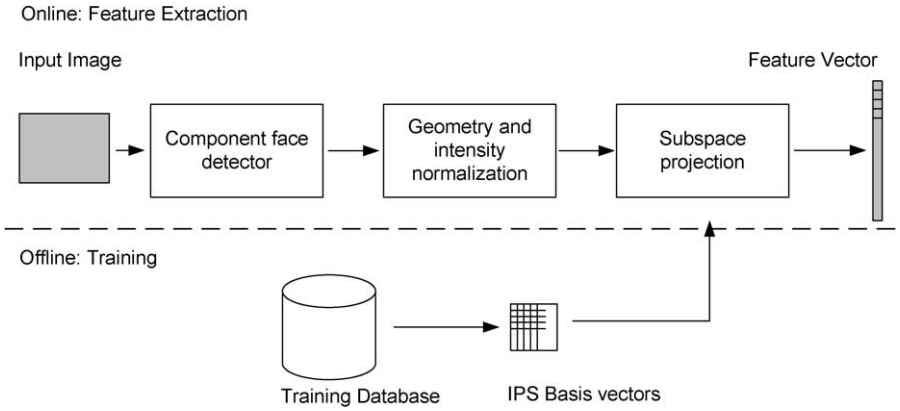


Fig. 6. Diagram of face feature extraction.

the same size and are upright irrespective of the original rotation and size in the image. The normalization is performed by applying a similarity transform (rotation, translation and scaling) to the image region containing the face. Normalization of image intensities corrects variations caused by imperfectly set camera parameters such as exposure time as well as changes in global illumination. Two methods are applied at this point to deal with these variations: first histogram equalization stretches the grey value spectrum and second effects caused by directional light are compensated by fitting and subtracting an illumination plane from the face image.

(3) *Feature extraction:* In the final stage of feature extraction the input is regarded as a N dimensional pixel vector containing the concatenated rows of the normalized face image. In our case the width w and height h of the face images are $w = h = 64$ – thus the dimensionality of a input face is $64 \times 64 = 4096$. The feature space for representing faces is then computed by performing bayesian subspace analysis approach presented in [20]. The subspace dimensionalities are determined using the optimization approach presented in [34]. The dimensionalities for the subspaces were determined beforehand on a large training database containing faces of different individuals exhibiting various facial variations. The linear subspace for representing faces is computed in two steps described below.

In a first step, the dimensionality of the face vector is reduced by applying Principal Component Analysis (PCA) to the Covariance matrix C (see Eq. (3)) of all face vectors $\vec{x_i}$. The first 140 eigenvectors corresponding to the largest eigenvalues of the data covariance matrix C are retained. Thus, the dimension of the face vectors are reduced from $64 \times 64 = 4096$ to $\sim$140.

The subspace dimensionalities are determined using an optimization approach similar to the approach presented in [22]. This optimization approach searches the space of subspace dimensionalities for these values yielding optimal recognition performance. The optimization was carried out on a separate dataset containing approximately 50 different individuals to prevent fitting these parameters to the test dataset

used in the evaluation below. The optimal values for the subspace dimensions were found to be 140 for the PCA subpace and 100 for the IPS subspace.

$$C = \sum_{i=1}^{M} (\vec{x_i} - \vec{m})(\vec{x_i} - \vec{m})^{\mathrm{T}}. \tag{3}$$

In a second step the dimensionality is further reduced by projecting onto the intrapersonal subspace (IPS). The IPS is the linear subspace capturing the intrapersonal variations from all the individuals present in a large training dataset. It is created by computing the eigenvectors of the covariance matrix C_i of face difference vectors of the same individuals (see Eq. (4)) – formally by taking the difference vectors of all faces with same class labels $l(\vec{x_i}) = l(\vec{x_j})$. Given a training set containing rich facial variations the faces captured during the online phase should be represented well in this subspace. The dimensionality reduction in the second step is $\sim$ 40 dimensions. Thus, after this final step the face is represented by an $\sim$100 dimensional feature vector.

For classification in the IPS an individual can be modelled as an anisotropic Gaussian distribution. A maximum likelihood measure [20] can be employed to compute the probability a face vector belongs to a specific class. This maximum likelihood measure can be evaluated computing a Mahalanobis distance for the gaussian case. Practically, as face vectors can be preprocessed by a whitening transform beforehand the distribution transforms to an isotropic Gaussian and distances become simply Euclidean.

$$C_I = \sum_{l(\vec{x_i})=l(\vec{x_j})} (\vec{x_i} - \vec{x_j})(\vec{x_i} - \vec{x_j})^{\mathrm{T}}. \tag{4}$$

Once the basis vectors of the IPS are determined, feature extraction is a linear projection of the original face vector onto the IPS basis.

3.3. Gait feature extraction

The first step in human movement analysis is the extraction of the walking subject's silhouette from the input image sequence. In the proposed framework, 2.5D information is available since the gait sequence is captured by a stereoscopic camera. Using Delaunay triangulation on the 2.5D data, a 3D triangulated hull of the silhouette is generated and is further processed using the 3D Geodesic Transform [12], thus generating the final normalized silhouettes $\tilde{S}_G(x, y)$ and all the transformations are applied to them.

The Generalized Radon transforms are used due to their aptitude to represent meaningful shape characteristics [25]. In particular, the RIT transform of a function $f(\cdot, \cdot)$ is defined as the integral of $f(\cdot, \cdot)$ along a line starting from the center of

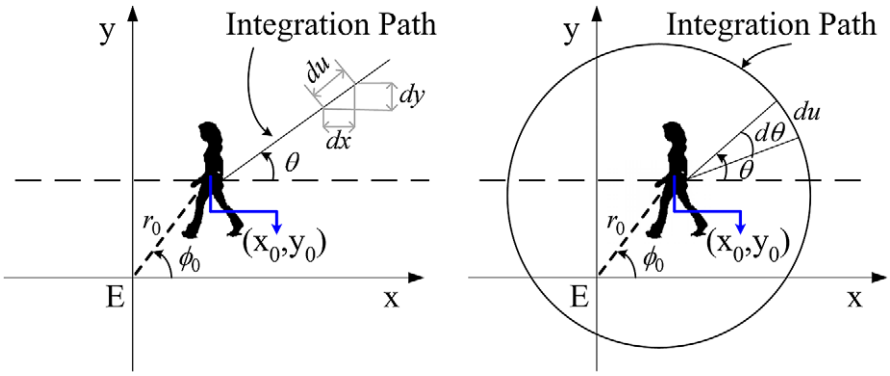


Fig. 7. Application of (a) the Radial Integration Transform and (b) the Circular Integration Transform on a silhouette image.

the silhouette (x_0, y_0) which forms angle θ with the horizontal axis (Fig. 7(a)). In our feature extraction method, the discrete form of the RIT transform is used, which computes the transform in steps of $\Delta\theta$ and is given by:

$$RIT(t\Delta\theta) = \frac{1}{J}\sum_{j=1}^{J} \tilde{S}_G(x_0 + j\Delta u \cdot \cos(t\Delta\theta), y_0 + j\Delta u \cdot \sin(t\Delta\theta)), \tag{5}$$

where $t = 1, \ldots, T$, Δu and $\Delta\theta$ are the constant step sizes of the distance u and angle θ, J is the number of silhouette pixels that coincides with the line that has orientation θ and are positioned between the center of the silhouette and the end of the silhouette in that direction, and $T = 360°/\Delta\theta$.

In a similar manner, the Circular Integration Transform (CIT) is defined as the integral of a function $f(x, y)$ along a circle curve $h(\rho)$ with center (x_0, y_0) and radius ρ. Similar to the RIT transform, the discrete form of the CIT transform is used, as illustrated in Fig. 7(b), which is given by:

$$CIT(k\Delta\rho) = \frac{1}{\mathrm{T}}\sum_{t=1}^{T} \tilde{S}_G(x_0 + k\Delta\rho \cdot \cos(t\Delta\theta), y_0 + k\Delta\rho \cdot \sin(t\Delta\theta)), \tag{6}$$

where $k = 1, \ldots, K$, $\Delta\rho$ and $\Delta\theta$ are the constant step sizes of the radius and angle variables, $k\Delta\rho$ is the radius of the smallest circle that encloses the binary silhouette image $\tilde{S}_G$, and $T = 360°/\Delta\theta$.

Besides the generalized Radon transforms, the use of a novel set of orthogonal moments is also proposed based on the discrete classical weighted Krawtchouk polynomials [36]. These moments assure minimal information redundancy due to their orthogonality and are used to extract local shape characteristics of images.

The weighted Krawtchouk moments Q_{nm} of order $(n + m)$ are estimated using the Krawtchouk polynomials for a silhouette image with intensity function $\tilde{S}_G(x, y)$ as follows:

$$Q_{nm} = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \bar{K}_n(x; p_1, N-1) \times \bar{K}_m(y; p_2, M-1) \cdot \tilde{S}_G(x, y), \tag{7}$$

$$\bar{K}_n(x; p, N) = K_n(x; p, N) \sqrt{\frac{w(x; p, N)}{\rho(n; p, N)}}, \tag{8}$$

where $\bar{K}_n$, $\bar{K}_m$ are the weighted Krawtchouk polynomials, and N, M represent the width and the height of the silhouette image respectively.

Although the study of kinesiological parameters that define human gait can form a basis for identification, there are apparent limitations in gait capturing that make it extremely difficult to identify and record all parameters that affect gait. Instead, gait recognition has to rely on a video sequence taken in controlled or uncontrolled environments. Even if the accuracy with which we are able to measure certain gait parameters improves, we still do not know if the knowledge of these parameters provides adequate discrimination power to enable largescale deployment of gait recognition technologies. Moreover, studies report both that gait changes over time and that it is affected by clothes, footwear, walking surface, walking speed, and emotional condition. As seen, all these parameters can reduce the performance of state-of-the-art gait recognition algorithms up to a level of 15%.

4. Multimodal biometric fusion

The architecture of the multimodal biometric authentication system is depicted in Fig. 8. At the enrolment stage, the face and gait feature vectors X_1 and X_2 are initially extracted as described in the previous section. The extracted feature vectors are encoded using a channel encoder. It must be stressed that the rate of the LDPC encoders in Fig. 8 is different for each modality according to Eq. (2). The resulting codewords S_1 and S_2 comprise the biometric templates of the modalities and are stored to the database of the system. Thus, if the database of the biometric system is attacked, the attacker can not access the original raw biometric data or their corresponding features but only S_1 and S_2, which can not reveal any information as it will be explained in the following.

At the authentication stage, the face and gait feature vectors X_3 and X_4 are extracted. Subsequently, the syndromes S_1 and S_2 which correspond to the claimed identity are retrieved from the database and are fed to the LDPC decoders. These processes are analytically described below.

It must be noted that two unimodal protection systems based on the proposed scheme could be used to protect the biometric templates independently. However, the

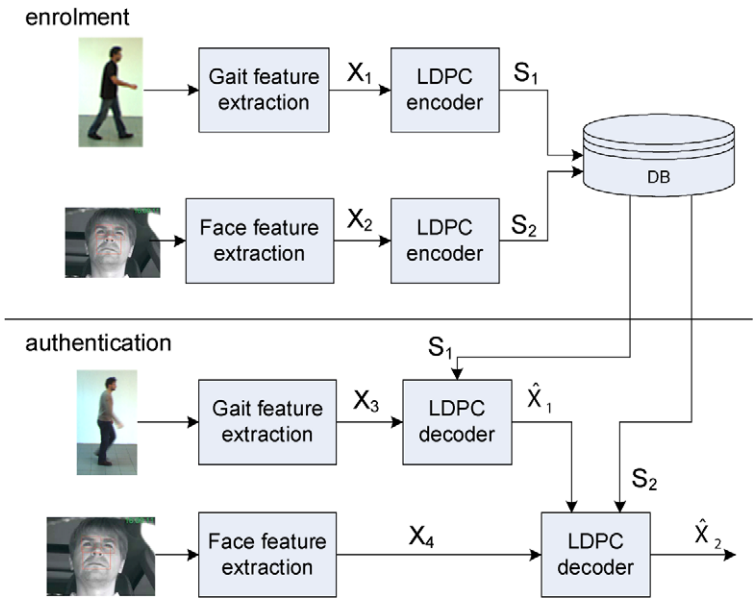


Fig. 8. Block diagram of the proposed multimodal authentication system.

main difference of the proposed scheme with the unimodal case is that the extension of Slepian–Wolf theorem to multiple sources (Eq. (2)) is employed which limits the rate required to represent the templates. Otherwise, if the unimodal protection scheme had been used for every biometric modality independently the rate required to code each feature vector. This in turn would affect the size of the templates and the performance of the system.

Even if liveness detection is out of the scope of the paper, the multimodal framework provides tools to guarantee that even if the user is wearing a mask, in order to fake the system, he/she should also mimic the gait modality. Thus, we are not proposing a solution that will support liveness detection at the sensor level, however, we can support security at the signal level due to the multimodal nature of the proposed framework.

4.1. Enrolment stage

Initially, at the enrolment stage, the biometric signatures of an individual for gait and face modalities are obtained. The extracted features form the vector $\mathbf{x}_i = [x_1^i, \ldots, x_{k_i}^i], i \in \{1, 2\}$, thus $\mathbf{x}_i \in \mathbb{R}^{k_i}$. The feature vector $\mathbf{x}_i$ must be transformed from the continuous to the discrete domain so that it can be further processed by the channel encoder. This mapping can be represented by a uniform quantizer with 2^{L_i} levels. Each component of $\mathbf{x}_i$ is then mapped to an index in the set $\mathcal{Q}$, through the

function $u : \mathbb{R}^{k_i} \rightarrow \mathcal{Q}^{k_i}$, where $\mathcal{Q} = \{0, 1, \ldots, L_i - 1\}$. Each one of the resulting vectors $\mathbf{q}_i = u(\mathbf{x}_i)$ is fed to the Slepian–Wolf encoder, which performs the mapping $e : \mathcal{Q}^{k_i} \rightarrow \mathcal{C}^{n_i}$, where $\mathcal{C} = \{0, 1\}$ and outputs the codeword $\mathbf{c}_i = e(\mathbf{q}_i)$, $\mathbf{c}_i \in \mathcal{C}^{n_i}$.

In this work, the Slepian–Wolf encoder is implemented by a systematic LDPC encoder [10]. LDPC codes were selected due to their excellent error detecting and correcting capabilities. They also provide near-capacity performance over a large range of channels while simultaneously admitting implementable decoders. An LDPC code (n, k) is a linear block code of codeword length n and information block length k which is defined by a sparse $(n - k) \times n$ parity matrix H, where $n - k$ denotes the parity bits produced by the encoder. The code rate is defined as $r = k/n$. A code is a *systematic* code if every codeword consists of the original k-bit information vector followed by $n - k$ parity-bits. In the proposed system, the joint bit-plane encoding scheme of [31] was employed to avoid encoding and storing the L_i bit-planes of the vector $\mathbf{q}_i$ separately. Alternatively, LDPC codes in a high-order Galois-field could be employed, but binary LDPC codes (GF(2)) were selected due to ease of implementation.

Subsequently, the k_i systematic bits of the codeword $\mathbf{c}_i$ are discarded and only the *syndrome* $\mathbf{s}_i$, that is the $n_i - k_i$ parity bits of the codeword $\mathbf{c}_i$, is stored to the biometric database. Thus, the biometric templates of an enrolled user consist of the syndromes $\mathbf{s}_i = [c_{k_i+1} \cdots c_{n_i}]$, $\mathbf{s}_i \in \mathcal{C}^{(n_i - k_i)}$, and their size is $n_i - k_i$. It must be stressed that the rate of the two LDPC encoders is different because the statistical properties of the two modalities are different. Thus, the security of each modality is different, as explained in Section 4.3.

4.2. Authentication stage

At the authentication stage, a user claims an identity $\mathcal{I}$, a new signature is extracted from the biometric features, and the vector $\mathbf{x}_i = [x_1^i, \ldots, x_{k_i}^i]$, $i \in \{3, 4\}$, $\mathbf{x}_i \in \mathbb{R}^{k_i}$, is constructed. The vectors $\mathbf{x}_3$ and $\mathbf{x}_4$, which form the side information corresponding to $\mathbf{x}_1$ and $\mathbf{x}_2$ respectively, are fed to the LDPC decoder. The decoding function $d : \mathcal{C}^{(n_i - k_i)} \times \mathbb{R}^{k_i} \rightarrow \mathcal{Q}^{k_i}$ combines $\mathbf{x}_i$, $i \in \{3, 4\}$, with the corresponding syndromes which are retrieved from the biometric database and correspond to the claimed identity $\mathcal{I}$. The decoder employs belief-propagation [24,37] to decode the received codewords.

If the errors introduced in the side information with regard to the originally encoded signal are within the error correcting capabilities of the channel decoder then the correct codeword is output after a number of iterations and the transaction is considered as a client transaction. More specifically, the gait feature vector $\mathbf{x}_3$ is initially fed to the LDPC decoder. The output of the LDPC decoder is the quantized vector $\hat{\mathbf{q}_1} = d(\mathbf{s}_1, \mathbf{x}_3)$. In general, besides the code rate, the error correcting capabilities of the channel decoder also depend on the information of the noisy channel and the

relationship between the noise induced by the channel and the side information. Accurate modelling of the distribution of the noisy channel can improve the knowledge of the channel decoder by exploiting a priori information, as described in [2] for the gait sequences.

Subsequently, the decoded codeword $\mathbf{q}_1$ is fed to the face LDPC decoder. Then, the decoding function combines $\mathbf{x}_4$, $\hat{\mathbf{x}}_1$, and $\mathbf{s}_2$ to decode the original codeword $\mathbf{x}_2$, thus $\hat{\mathbf{q}}_2 = d(\mathbf{x}_4, \mathbf{s}_2, \hat{\mathbf{x}}_1)$. The correlation between $\mathbf{x}_1$ and $\mathbf{x}_2$ can be modelled by a binary symmetric channel (BSC) with crossover probability p which is unique for each user and stored in the database as part of its template. To detect whether a codeword is correctly decoded we add 16 Cyclic Redundancy Check (CRC) bits at the beginning of the feature vector. By examining these bits the integrity of the original data is detected. If the codeword is correctly decoded, then the transaction is considered as genuine. Otherwise, if the decoder can not decode the codeword (which is indicated if the number of iterations increases over a specific number N_{iter}) a special symbol Ø is output and the transaction is considered as an impostor transaction.

4.3. Biometric template security

Currently, most biometric systems store biometric templates in the form of raw data, e.g., photographs of faces, raw speech signals, etc. If these templates are compromised by attackers they can be used to impersonate legitimate users and gain access to facilities of the protected system. Other systems store features extracted from the raw biometric data. Again, an attacker who access the stored data by fraudulent means can reconstruct the original raw biometric data, especially if the feature extraction algorithm is known.

In general, security refers to how difficult it is for an adversary to gain access to the stored biometric data **x** of the users of the system and there are two quantities associated with it. The first is the "*strength*" of the key **s** which is stored to the database and refers to how difficult it is for an attacker to gain access to it. In [6], the *min-entropy* was suggested as a measure of this quantity. The min-entropy $H_\infty(A)$ of a random variable A is defined as [6]:

$$H_\infty(A) = -\log_2\Big(\max_a \Pr(A = a)\Big). \tag{9}$$

In the proposed scheme, $a \in \{0, 1\}$ since the possible states of the binary random variables are 0 and 1. Also, since min-entropy can be viewed as the worst-case entropy the strength of the key is actually larger in real applications. Otherwise stated, min-entropy provides a worst-case estimate of the predictability of the random variable A. Moreover, the *average min-entropy* of A given B is defined as:

$$\tilde{H}_\infty(A|B) = -\log_2\big(\mathbb{E}\big(2^{-H_\infty(A|B)}\big)\big). \tag{10}$$

The second quantity refers to how difficult it is to guess the original biometric data $\mathbf{x}$ once the stored biometric template $\mathbf{s}$ is compromised[2] and can be measured by the *entropy loss*. The entropy loss $\mathcal{L}$ is defined as:

$$\mathcal{L} = H_{\infty}(A) - \tilde{H}_{\infty}(A|B). \tag{11}$$

In [6], it is proven that the entropy loss can be conveniently bounded by the size of the biometric template, that is $\mathcal{L} \leqslant |\mathbf{s}|$. This result is in accordance with the information theoretic framework for security quantification presented in [8] where the size of the stored biometric template was used to quantify the security of the system.

Following the conclusions of [6] and [8], in the proposed system, security is quantified by the number of bits that comprise the biometric template, which is equal to the number of the parity bits that comprise the syndrome. Since the rate of the encoders for the face and gait modalities are different, the biometric template security of each template is also different. Moreover, if a template is compromised, it can be easily revoked and use another LDPC code to issue a new one. However, it must be noted that the proposed scheme does not provide a means to detect whether a template is compromised. It is worth noting that we are not trying to develop an authentication scheme with the lowest error rates possible. Instead, we study a scheme with reasonable performance in a controlled environment and focus on the tradeoff between the security of the biometric templates and the recognition performance.

The main scope of the proposed system is to protect biometric templates in multimodal biometric authentication systems. Instead of storing the original extracted biometric features a new template is produced which reveals limited information about the original template. In such systems, security is measured by how difficult it is for an attacker to gain access to (or guess) the original biometric data if the biometric template is compromised, which is given by the entropy loss. Bounding the entropy loss by the size of template $|\mathbf{s}|$ means that an attacker needs to try $2^{|\mathbf{s}|}$ different combinations to identify the original biometric data. Thus, the security guarantees of the system is directly related to the entropy loss.

It is also important to note that security of biometric templates comes from the fact that the stored template consists of the parity bits produced by encoding the original biometric features with the LDPC encoder. Thus, even if the stored template is compromised the attacker does not have direct access to the original biometric features. Given that the entropy loss is usually more than 100 bytes, an attacker would need more than 2^{100} attempts to guess the original biometric feature (which is computationally impossible). In other words, the information that is revealed about the original biometric features from the stored template is virtually zero.

[2]Note that we refer to the feature vector $\mathbf{x}$ instead of the raw biometric data b. This is because the biometric template protection scheme is usually applied after the feature extraction algorithm has been determined. Thus, the difficulty in reconstructing raw data from the feature vector is not a design parameter of the security system.

5. Results

Experiments were carried out to demonstrate the validity of the proposed methodology. The multimodal database was created by aggregating two unimodal databases for face and gait, as suggested in [21].

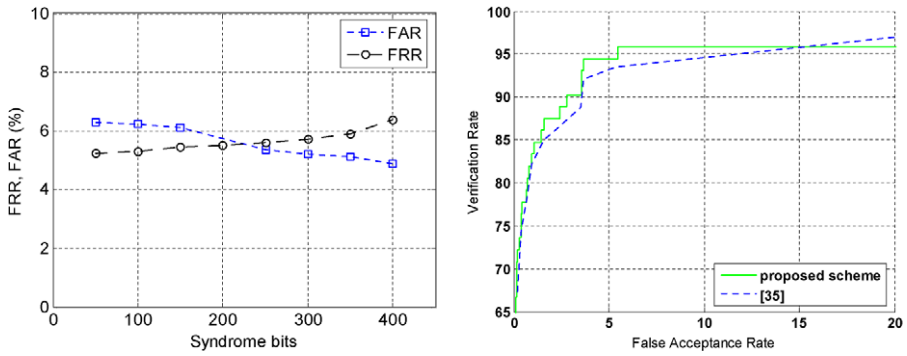
The test database contains 29 different individuals recorded under five different conditions giving 145 sequences in total. While the number of subjects might seem small at first one must consider that these individuals were recorded under varying conditions such as different facial expressions and different illumination conditions. As whole image sequences are available for each individual multiple feature vectors are extracted from one sequence. This number varies between 50 and 300 depending on the number of successful extractions per sequence. From the whole corpus a subset was selected to prove the effectiveness of the fusion approach. While matching feature vectors extracted within the same sequence produces low error rates in general, inter-sequence matches are a more challenging task especially when the variances present in the enrollment sequence differ much from these present in the matching sequence (see [1]). A moderately challenging combination of enrollment and matching conditions was chosen for the evaluation: subjects with neutral facial expression were matched against talking subjects.

The gait database was captured in an indoor environment and consists of 75 people walking in a predefined path in a front-parallel view from the camera. The main course of walking is around six meters and the distance from the camera varies from four meters to six meters. In addition, for each sequence, the 3D depth map was captured using a stereo camera. This is the first database that has depth data for assisted gait recognition. For each subject, two different conditions were captured: (a) the "normal" condition, and (b) the "hat" condition in which the users wear a hat (e.g., there is a slight change in appearance apart from different clothing). The "normal" set was used as the gallery set and the other set was considered as the probe set.

For the creation of the multimodal database, the maximum number of virtual subjects is determined by the size of the smallest unimodal database, thus its population is 29 subjects. The virtual subjects were obtained with natural ordering within each unimodal database. In other words, the Nth virtual user was created using the Nth user trait from each database. Thus, the multimodal database consists of 29 subjects and two recordings. The evaluation was performed using the first half of the subjects (all recordings) for training and the other half of the subjects for testing. Thus, the test set contains subjects that have not been used for training. The sets slide for each run by one subject and in that way the training-testing dataset combinations that are created are equal to the number of subjects. In particular, for each run, 15 subjects were used for training and the remaining 14 were used for testing. Thus, the total number of genuine and impostor transactions in the training set is $15 \times 29 = 435$ and $15 \times 14 \times 29 = 6090$, respectively. The test set contains $14 \times 29 = 406$ genuine and $14 \times 13 \times 29 = 5278$ impostor transactions.

In an authentication scenario (or *verification*), the biometric system is used to grant access to individuals. Initially a subject claims his/her identity and the gait system compares the signature with the stored one in the database. Then, based on the authentication procedure, the system establishes whether the identity of the user is the claimed one. In this respect, authentication results in an one-to-one comparison and is quite different from the identification scenario, in which the system has to determine the identity of users by comparing the measured data with all the enrolled data in the database (one-to-many database). The performance of the biometric system is evaluated in terms of the False Acceptance Rate (FAR), the False Rejection Rate (FRR) and the Equal Error Rate (EER), which corresponds to the point where the FAR is equal to FRR. FAR measures the ratio of impostors who are incorrectly accepted into the system as legitimate users and FRR measures the ratio of genuine users who are rejects as impostors. Also, results are presented using Rate Operating Characteristic (ROC) curves, which present the verification rate (or genuine acceptance rate, GAR) versus the FAR. The FRR can then be computed as 1-GAR.

Figure 9(a) reports the performance results of the gait authentication system as a function of the security bits using the proposed scheme for the protection of the templates. Thus, the horizontal axis represents the numbers of the syndrome bits, while the vertical axis represents the FAR and FRR. The more bits used for the syndrome the more secure is the template since it is more difficult to be broken. On the other hand, increasing the size of the syndrome increases the sensitivity of the system, which results in more authentication failures of legitimate users. Thus, the recognition accuracy of the proposed system can be determined by specifying the code rate r. This is similar to the conventional approach that determines the operating points of the ROC curve by varying the threshold that determines which subjects are granted access. The reported results are also compared with the method presented in [13] using ROC curves, as depicted in Fig. 9(b). It can be seen that



(a) (b)

Fig. 9. (a) ROC curve of the gait authentication system and (b) FAR and FRR as a function of the security in bits.

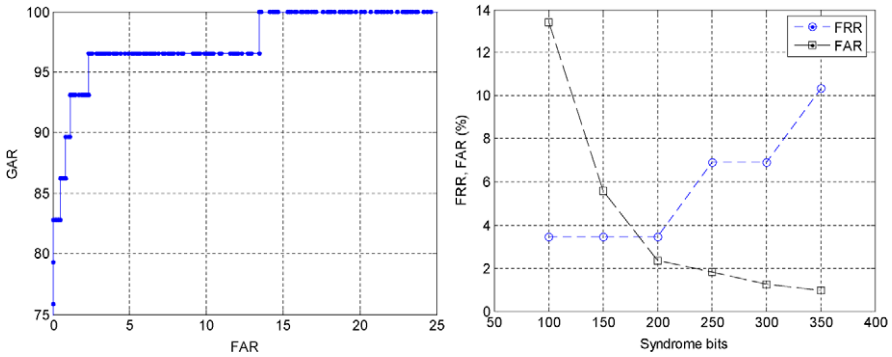


Fig. 10. (a) ROC curve of the face authentication system and (b) FAR and FRR as a function of the security in bits.

the proposed scheme achieves slightly better performance while at the same time it provides security to the stored templates.

Furthermore, the performance of the face authentication system is illustrated in Fig. 10. Specifically, Fig. 10(a) shows the ROC curve of the face module. It must be stressed that if the authentication was based on estimating the Euclidean distances between the gallery and probe feature vectors (rather than using the proposed methodology) the performance of the face classifier would be exactly the same. Thus, it is obvious that the proposed scheme provided template security at no cost in the performance of the face classifier. Moreover, Fig. 10(b) depicts the FAR and FRR rates as a function of the size of the face template. Similar to the gait module, as the size of the templates increases the FRR increases and FAR decreases.

While matching feature vectors extracted within the same sequence produces low error rates in general, inter-sequence matches are a more challenging task especially when the variances present in the enrollment sequence differ much from these present in the matching sequence. Face recognition algorithms are known to be sensitive to data outliers in terms of incorrectly normalized samples and severe intrapersonal variations such as extreme facial expressions and occlusions caused by e.g. glasses and beards. Algorithms are only robust to a certain degree of intrapersonal variations. It is a difficult problem to guarantee proper input to a recognition algorithm, quality measures e.g. ensuring proper localization of the eyes have proven to be an feasible approach to ensure proper input for autonomous recognition systems [17]. A moderately challenging combination of enrollment and matching conditions was chosen for the evaluation: subjects with neutral facial expression were matched against talking subjects.

It must be also noted that throughout all the experiments, the same global thresholds and set of parameters were used. Thus, we may conclude that the performance of the system will not change if more users are enrolled or removed from the system.

Table 1
Equal error rate of the multimodal authentication scheme

Classification method	EER (%)	Security (in bits)
Proposed	3.05	200 (Face)
		260 (Gait)
SVM	2.54	0

Finally, Table 1 presents the results of the multimodal classification scheme using the methodology presented in Section 4. The results are compared (in terms of EER) with a system which performs classification using Support Vector Machines (SVM), a state-of-the-art machine learning algorithm which has been proven to be very satisfactory in multimodal biometric fusion [9,32]. As it can be observed, the increased protection of the stored templates using the proposed scheme comes at virtually no cost in the performance of the authentication system. Specifically, the system achieves more than 200 bits of security by trading approximately 0.5% in performance which is considered negligible.

6. Compliance with privacy legislation

Biometric technology raises privacy concerns primarily because of the personal nature of biometric information. This holds true in particular for covert biometrics and behavioural biometrics. Within the EU, several Directives on data privacy have been adopted, the first and most important of which is Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data. This instrument is binding on EU member states. It is also binding on non-member states (Norway, Iceland and Liechtenstein) that are party to the 1992 Agreement on the European Economic Area (EEA). Also, biometric systems should comply with Directive 58/2002/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy, and The European Charter of Fundamental Human Rights. Privacy provisions are having a great impact on development of biometric technologies EU Directive shaped most privacy laws of EU 27. Nevertheless, it is important to note that each country has still its own unique mix of rules; concomitantly, a good deal of variation exists in the way to which each country deals with biometrics and privacy.

The proposed methodology for biometric template protection in multimodal biometric authentication systems guarantees that HUMABIO fully complies with the aforementioned privacy legislation. Specifically:

- All data associated with the subjects are held private. The inherent encryption of the proposed scheme ensures that even if the biometric templates are compromised they can not be used to circumvent the system.

- The irreversibility of the stored templates prevents and adversary from reconstructing the original biometric data and use them to produce counterfeit biometric surrogates.
- Multimodality makes the system more robust to spoof attacks. Since multibiometric evidence is required for granting access to the system it is more difficult for an impostor to attack and spoof the system.

7. Discussion

In this paper, we presented a novel multimodal biometric authentication scheme to enhance protection of stored biometric data. Biometric recognition was formulated as a channel coding problem with noisy side information at the decoder. A virtual dependency channel was assumed to model the correlation between the biometric data at the enrolment and the authentication stage. Based on the extension of the Slepian–Wolf theorem to many sources, distributed source coding principles were applied to design a multimodal authentication system for the unobtrusive application scenario of the HUMABIO project. The extraction of the face and gait templates was briefly discussed and their integration into the proposed framework was detailed. The experimental results validated the proposed method and demonstrate that the security of the stored templates can be increased only at a negligible penalty in performance compared to unsecure machine learning techniques. Future work should concentrate on more accurate models for the virtual dependency channel to enhance the error correcting performance of the employed decoders.

References

[1] O. Arandjelović and R. Cipolla, A methodology for rapid illumination-invariant gace recognition using image processing filters, 2007 (under review).
[2] S. Argyropoulos, D. Tzovaras, D. Ioanndis and M.G. Strintzis, A distributed source coding framework for biometric authentication, in: *Proc. IEEE Int. Conference on Image Processing*, San Diego, CA, October 2008, pp. 3108–3111.
[3] G. Cohen and G. Zemor, Generalized coset schemes for the wire-tap channel: Application to biometrics, in: *IEEE Int. Symposium on Information Theory*, Chicago, IL, June 2004, p. 46.
[4] I.G. Damousis, D. Tzovaras and E. Bekiaris, Unobtrusive multimodal biometric authentication – the HUMABIO Project concept, *EURASIP Journal on Advances in Signal Processing* **2008** (2008), 1–11.
[5] G.I. Davida, Y. Frankel and B.J. Matt, On enabling secure applications through off-line biometric identification, in: *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, May 1998, pp. 148–157.
[6] Y. Dodis, L. Reyzin and A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, in: *Advances in Cryptology – Eurocrypt*, Lecture Notes in Computer Science, vol. 3027, Springer, Berlin, Germany, 2004, pp. 523–540.
[7] S.C. Draper, A. Khisti, E. Martinian, A. Vetro and J. Yedidia, Using distributed source coding to secure fingerprint biometrics, in: *IEEE Int. Conference on Acoustics, Speech and Signal Processing*, Honolulu, HI, April 2007, pp. 129–132.

[8] S.C. Draper, A. Khistiy, E. Martinian, A. Vetro and J.S. Yedidia, Secure storage of fingerprint biometrics using Slepian-Wolf codes, in: *Information Theory and Applications Workshop*, San Diego, CA, January 2007.

[9] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero and J. Gonzalez-Rodriguez, A comparative evaluation of fusion strategies for multimodal biometric verification, in: *Proc. 4th IAPR Intl. Conf. on Audio-and Video-based Biometric Person Authentication*, Guildford, UK, 2003, pp. 830–837.

[10] R.G. Gallager, *Low-Density Parity-Check Codes*, MIT Press, Cambridge, MA, 1963.

[11] B. Girod, A.M. Aaron, S. Rane and D. Rebollo-Monedero, Distributed video coding, *Proceedings of the IEEE* **93**(1) (2005), 71–83.

[12] D. Ioannidis, D. Tzovaras and K. Moustakas, Gait identification using the 3d protrusion transform, in: *Proc. IEEE Int. Conference on Image Processing*, San Antonio, TX, September 2007, pp. 349–352.

[13] D. Ioannidis, D. Tzovaras, I.G. Damousis, S. Argyropoulos and K. Moustakas, Gait recognition using compact feature extraction transforms and depth information, *IEEE Transactions on Information Forensics and Security* **2** (2007), 623–630.

[14] A. Jain, A. Nagar and K. Nandakumar, Biometric template security, *EURASIP Journal of Advances in Signal Processing* **8**(2) (2008), 1–17.

[15] K. Jain and A. Ross, Multibiometric systems, *Communications of the ACM* **47**(1) (2004), 34–40.

[16] A. Juels and M. Sudan, A fuzzy vault scheme, *Designs, Codes and Cryptography* **38**(2) (2006), 237–257.

[17] S.Z. Li, Face detection, in: *Handbook of Face Recognition*, S.Z. Li and A.K. Jain, eds, Springer, Berlin, Germany, 2004, pp. 13–38.

[18] E. Martinian, Authenticating multimedia in the presence of noise, Master's thesis, Massachusetts Institute of Technology, Cambridge, MA, 2000.

[19] E. Martinian, S. Yekhanin and J. Yedidia, Secure biometrics via syndromes, in: *43rd Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, September 2005.

[20] B. Moghaddam, T. Jebara and A. Pentland, Bayesian face recognition, *Pattern Recognition* **33**(11) (2000), 1771–1782.

[21] N. Poh and S. Bengio, Using chimeric users to construct fusion classifiers in biometric authentication tasks: An investigation, in: *Proc. IEEE Int. Conf. Acoust., Speech and Signal Processing*, Toulouse, France, May 2006, pp. 1077–1080.

[22] S.S. Pradhan and K. Ramchandran, Distributed source coding using syndromes (discus): Design and construction, *IEEE Transactions on Information Theory* **49**(3) (2003), 626–643.

[23] N. Ratha, J. Connell and R. Bolle, An analysis of minutiae matching strength, in: *Proc. 3rd AVBPA*, Halmstad, Sweden, June 2001, pp. 223–228.

[24] W.E. Ryan, An introduction to LDPC codes, in: *CRC Handbook for Coding and Signal Processing for Recording Systems*, B. Vasic and E.M. Kurtas, eds, CRC, Boca Raton, FL, 2005, pp. 1–23.

[25] D. Simitopoulos, D.E. Koutsonanos and M.G. Strintzis, Robust image watermarking based on generalized radon transformations, *IEEE Transactions on Circuits and Systems for Video Technology* **13**(8) (2003), 732–745.

[26] J.D. Slepian and J.K. Wolf, Noiseless coding of correlated information sources, *IEEE Transactions on Information Theory* **19**(4) (1973), 471–480.

[27] W. Stallings, *Cryptography and Network Security: Principles and Practices*, Upper Saddle River, Prentice Hall, NJ, 2006.

[28] Y. Sutcu, Q. Li and N. Memon, Protecting biometric templates with sketch: theory and practice, *IEEE Transactions on Information Forensics and Security* **2**(3) (2007), 503–512.

[29] U. Uludag and A. Jain, Attacks on biometric systems: A case study in fingerprints, *Proceedings of SPIE* **5306** (2004), 622–633.

[30] U. Uludag, S. Pankanti, S. Prabhakar and A. Jain, Biometric cryptosystems: Issues and challenges, *Proceedings of the IEEE* **92**(6) (2004), 948–960.

[31] D.P. Varodayan, A. Mavlankar, M. Flierl and B. Girod, Distributed grayscale stereo image coding with unsupervised learning of disparity, in: *Proc. of Data Compression Conference*, Snowbird, UT, March 2007, pp. 143–152.

[32] P. Verlinde, G. Chollet and M. Acheroy, Multi-modal identity verification using expert fusion, *Information Fusion* **1**(1) (2000), 17–33.

[33] P. Viola and M. Jones, Rapid object detection using a boosted cascade of simple features, in: *Proceedings IEEE Conf. on Computer Vision and Pattern Recognition*, Kauai, HI, 2001, pp. 511–518.

[34] X. Wang and X. Tang, A unified framework for subspace face recognition, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **26**(9) (2004), 1222–1228.

[35] B. Xie, D. Comaniciu, V. Ramesh, M. Simon and T. Boult, Component fusion for face detection in the presence of heteroscedastic noise, in: *DAGM-Symposium*, Magdeburg, Germany, 2003, pp. 434–441.

[36] P.T. Yap, R. Paramesran and S.H. Ong, Image analysis by krawtchouk moments, *IEEE Transactions on Image Processing* **12**(11) (2003), 1367–1377.

[37] J. Yedidia, W. Freeman and Y. Weiss, Generalized belief propagation, in: *Advances in Neural Information Processing Systems*, Denver, CO, December 2000, pp. 689–695.