8

Biometric Keys for the Encryption of Multimodal Signatures

A. Drosou[1], D.Ioannidis[2], G.Stavropoulos[2], K. Moustakas[2] and D. Tzovaras[2]

[1]*Imperial College London*
[2]*Ce.R.T.H. - Informatics and Telematics Institute*
[1]*UK*
[2]*Greece*

1. Introduction

Biometrics have long been used as means to recognize people, mainly in terms of their physiological characteristics, for various commercial applications ranging from surveillance and access control against potential impostors to smart interfaces (Qazi (2004)) (Xiao (2005)). These systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The biometric methods, that are usually incorporated in such systems, can be categorized to physiological and behavioral (Jain et al. (2004)), depending on the type of used features.

The most popular physiological biometric traits are the fingerprint (Maltoni et al. (2009)) that is widely used in law enforcement for identifying criminals, the face (Chang et al. (2005)) and the iris (Sun & Tan (2009)). However, despite their high recognition performance, static biometrics have been recently overwhelmed by the new generation of biometrics, which tend to cast light on more natural ways for recognizing people by analyzing behavioural traits.

Specifically, behavioural biometrics are related to specific actions and the way that each person executes them. In other words, they aim at recognizing livingness, as it is expressed by dynamic traits. The most indicative cases of behavioural biometric recognition is gait (Goffredo et al. (2009b)), facial expressions (Liu & Chen (2003)) or other activity related, habitual traits (Drosou, Ioannidis, Moustakas & Tzovaras (2010)). As a result behavioural biometrics have become much more attractive to researchers due to their significant recognition potential and their unobtrusive nature. They can potentially allow the continuous (on-the-move) authentication or even identification unobtrusively to the subject and become part of an Ambient Intelligence (AmI) environment.

The inferior performance of behavioural biometrics, when compared to the classic physiological ones, can be compensated when they are combined in a multimodal biometric system. In general, multimodal systems are considered to provide an excellent solution to a series of recognition problems. Unimodal systems are more vulnerable to theft attempts, since an attacker can easily gain access by stealing or bypassing a single biometric feature. In the same concept, they have to contend with a variety of problems, such as noisy data, intraclass variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates, i.e., it is estimated that approximately 3% of the population does not have legible

fingerprints (Fairhurst et al. (2003)). Such biometric system may not always meet performance requirements, may exclude large numbers of people, and may be vulnerable to everyday changes and lesions of the biometric feature.
In this context, the development of systems that integrate more than one biometrics is an emerging trend, since it has been seen that true multimodal biometric systems, that capture a number of unrelated biometrics indicators, have significant advantages over unimodal ones. Specifically, most of the aforementioned 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 systems, in order to meet stringent performance requirements. Moreover, such systems are much more invulnerable to fraudulent technologies, since multiple biometric characteristics are more likely to resist against spoof attacks than a single one.
Last but not least, a major issue of biometric systems is the protection of the sensitive biometric data that are stored in the database, so as to prevent unauthorized and malicious use. Given the widespread deployment of biometric systems and the wide exposition of personal data, public awareness has been raised about security and privacy of the latter. Seemingly, the voting of several laws concerning the ethical and privacy issues of private data provide a universal solution unless it is accompanied by the appropriate technological tools.
Unfortunately, simple password-based systems, that provide regular cryptographic solutions (Uludag et al. (2004)) can not be easily applied, since the representation of behavioural biometric traits is not fixed over time. Thus, the current issue has been confronted with modern, sophisticated encryption methods that do not require the exact match of the prompted and the original signatures in order to grant access.

1.1 Related work

With respect to behavioural biometrics, previous work on human identification can be mainly divided in two main categories. a) sensor-based recognition (Junker et al. (2004)) and b)vision-based recognition. Recently, research trends have been moving towards the second category, due to the obtrusiveness imposed by the sensor-based recognition approaches (Kale et al. (n.d.)). Additionally, recent work and efforts on human recognition have shown that the human behavior (e.g. extraction of facial dynamics features (Hadid et al. (2007)). However, the most known example of behavioural biometrics is the human body shape dynamics (Ioannidis et al. (2007) or joints tracking analysis (Goffredo et al. (2009a)) for gait recognition. In the same respect, the analysis of dynamic activity-related trajectories (Drosou, Moustakas & Tzovaras (2010)) provide the potential of continuous authentication for discriminating people, when considering behavioural signals.
Although there have been already proposed a series of multimodal biometric systems concerning static physiological biometric traits (Kumar et al. (2010)) (Sim et al. (2007)) there are only a few dealing solely with behavioural traits (Drosou, Ioannidis, Moustakas & Tzovaras (2010)). In any case, the main issue in a multimodal biometric system is the optimization of its fusion mechanism. In a multimodal biometric system, integration can be done at (i) feature level, (ii) matching score level, or (iii) decision level. However, matching score level fusion is commonly preferred because matching scores are easily available and contain sufficient information to distinguish between a genuine and an impostor case. In this respect, a thorough analysis of such score-level fusion methods regarding biometric traits has been presented in (Jain et al. (2005)).

Since all biometric systems deal with the issue of storing biometric data, different approaches regarding their security have been suggested. In the current work, an extension of the security template scheme, presented in (Argyropoulos et al. (2009)), is proposed, that bases on Error Correcting Codes (ECC) and the modeling of channel statistics. Channel codes have been previously used for the development of authentication schemes. Earlier, in (Wadayama (2005)), a generic authentication scheme based on channel codes was proposed to improve security and prevent unauthorized access in secure environments. Also, in (Davida et al. (1998)), a channel coding scheme was presented for secure biometric storage. 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. Based on this concept, the fuzzy commitment scheme was introduced to tolerate more variation in the biometric characteristics and provide stronger security (Juels & Sudan (2006)). In this scheme, the user selects at the enrolment a secret message c. Then, the template consists of the difference between the user's biometric data x and c along c with an encrypted version of c. At the authentication, the stored difference d is added to the new biometric representation y and $y + d$ is decoded to the nearest codeword c' using error correcting codes.

In this respect, a series of encryption methods have been developed to account for the inherent variability of biometric signals. Apart from (Davida et al. (1998)), a methodology based on the Slepian-Wolf theorem (Slepian & Wolf (1973)) for secure storage biometric via Low-Density Parity Check ($LDPC$) codes was presented in (Martinian et al. (2005)). 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. The same framework was also employed in (Draper et al. (2007)) in order to secure fingerprint biometrics, image authentication (Yao-Chung et al. (2007)) and biometric authentication as a wire-tap problem (Cohen & Zemor (2004)).

In the seminal work of (Pradhan & Ramchandran (2003)), the distributed source coding using syndromes scheme was proposed. Based on this work, the field of distributed video coding (Girod et al. (2005)) has emerged as a new trend in video coding. Finally, an interesting approach of applying the $LDPC$ methodology in multimodal biometric systems has been proposed in (Argyropoulos et al. (2009)).

Similarly to above, one of the major concerns in applications that grant access based on a password, a pin or a token, is the protection of the original data to prevent malicious use from those who try to access them by fraudulent means. Although this problem in such systems has been investigated in depth and sophisticated encryption methods have been developed (Stallings (2006)), a significant issue remains the possibility of having the password stolen or forgotten. Thus, methods which enable a biometric-related key have been proposed (Álvarez et al. (2009)). Thus, the required pin is always carried by the user, since it is encoded on himself.

1.2 Contribution

In the current chapter, a novel framework for activity related authentication in secure environments based on distributed source coding principles and automatically extracted biometric keys is proposed. The main novelty is the development of an integrated framework

that utilizes biometric key based encryption, in order to assist the channel decoding process and to boost the system's recognition performance. It is shown that the proposed system increases the security of the stored templates and ensures privacy of personal data, while indirectly provides "hybrid" fusion between static and dynamic biometric traits towards improved recognition results. Moreover, unobtrusive, multimodal, on-the-move biometric authentication is presented and evaluated in a bimodal scenario, which utilizes two behavioural traits of the user. Namely, the gait and the activity-related motion trajectories of the head and the hands during specific movements which are seen to provide a powerful auxiliary biometric trait are inspected in terms of biometric means for user authentication.

2. Proposed methodology

The architecture of the proposed biometric recognition framework is illustrated in Figure 1. Initially, from the captured gait image sequence, the moving silhouettes are extracted, the shadows are removed and the gait cycle is estimated using state-of-art (SoA) algorithms (Ioannidis et al. (2007)), (Cucchiara et al. (2001)). Using a stereoscopic camera, we detect those frames in the sequence, whereby the user is standing and we discard them from those where the user is walking. Then the visual hull of the moving silhouette is extracted using disparity estimation. Once a view normalization is applied by rotating the silhouette, the $3D$ reconstructed silhouettes are denoised via spatiotemporal filtering, in order to improve their quality. Finally, two SoA geometric descriptors are extracted based on the sequence Gait Energy Image (GEI).

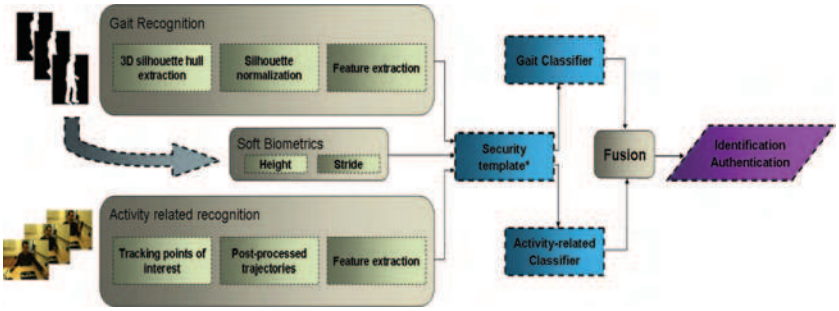


Fig. 1. System Architecture.

The gait recognition follows the principle of a model-free, feature-based analysis of the extracted human silhouettes, whereby geometric methods implement a robust classifier. In the following, the activity-related recognition is performed on the users' movements while they interact with a security panel installed at the end of the corridor. The extracted motion trajectories that are used as the user's biometric traits are classified by a Dynamic Time Warping classifier and its result is finally fused with the corresponding gait results at the score level towards an overall recognition outcome.

3. Behavioural biometrics

As it has already been mentioned, the development a novel biometric recognition method or the improvement of current State of Art (SoA) methodologies in this area, are not within the scope of the current work. In this context, a set of simple but robust activity-related

recognition modules have been utilized in the context of the proposed security framework in order to build a behavioural multimodal recognition system, where the proposed enhanced security template framework (see Section 4) could be tested and evaluated.
In particular, the first biometric modality consists of SoA gait recognition methodology (Ioannidis et al. (2007)) that bases on features extracted from spatiotemporal gait patterns. Similarly, the second modality that has been utilized refers to a novel activity-related concept that has been initially proposed in (Drosou, Moustakas, Ioannidis & Tzovaras (2010)) and deals with the motion related traits left by the user during the performance of some simple activities that are performed on a regular basis. Both aforementioned modalities are not only directly related to the users' physiology, but they are also highly governed by the users' habitual response to external stimuli. Thus, they have been seen to provide significant recognition capacity, both as stand-alones, as well as in multimodal recognition systems (Drosou, Ioannidis, Moustakas & Tzovaras (2010)).
For the convenience of the reader, a short functional description of the aforementioned modalities is included hereafter. Before presenting the security framework, which is the main contribution of the current work, a short description of the utilized biometric modalities is included.

3.1 Gait recognition

Let the term *"gallery"* refer to the set of reference sequences, whereas the term *"probe"* stands for the test sequences to be verified or identified, in both presented modalities.
Initially, the walking human binary silhouette is extracted as described in (Ioannidis et al. (2007)). The feature extraction process of the gait sequences is based on the Radial Integration Transformation (RIT) and the Circular Integration Transform (CIT) (Ioannidis et al. (2007)), but instead of applying those transforms on the binary silhouette sequences themselves, the Gait Energy Images (GEI) are utilized, which have been proven from one hand to achieve remarkable recognition performance and on the other hand to speed up the gait recognition (Han et al. (2006)) (Yu et al. (2010)).
Given the extracted binary gait silhouette images I' and each gait cycles k, the gray level (GEI) (Figure 2) is defined over a gait cycle as:

$$GEI_k = \frac{1}{C_L} \cdot \sum_{k=CycleStart}^{CycleEnd} I'(k) \tag{1}$$

where C_L is the length of the gait cycle and k refer to the gait cycles extracted in the current gait image sequence.

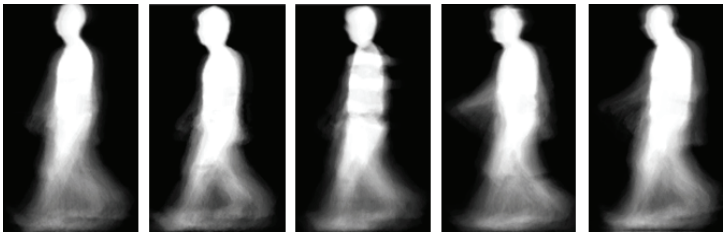


Fig. 2. Gait Energy Images from several users.

The RIT and CIT transforms are applied on the GEI, in order to construct the gait template for each user, as shown in Figure 3 in according to the following equations:

$$RIT_{f(\theta)} = \int f(x_0 + u\cos\theta, y_0 + u\sin\theta)du \tag{2}$$

where u is the distance from the starting point (x_0, y_0).

$$RIT(t\Delta\theta) = \frac{1}{J}\sum_{j=1}^{J} GEI(r_0 + j\Delta u \cdot \cos(t\Delta\theta), y_0 + j\Delta u \cdot \sin(t\Delta\theta)) \quad \text{for } t = 1, ..., T \text{ with } T = 360^o/\Delta\theta \tag{3}$$

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

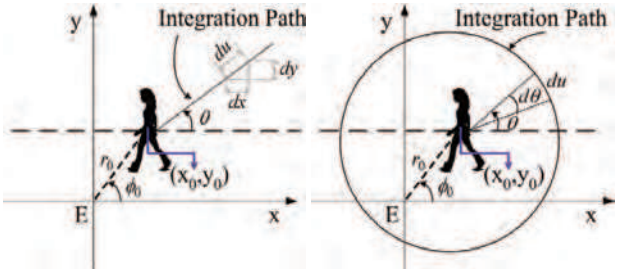


Fig. 3. Applying the RIT (left) and CIT (right) transforms on a Gait Energy Image using the Center of Gravity as its origin.

Similarly, 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. The CIT is computed using the following equation:

$$CIT_{f(\rho)} = \oint_{h(\rho)} f(x_0 + \rho\cos\theta + \rho\sin\theta)du \tag{4}$$

where du is the arc length over the path of integration and θ is the corresponding angle.
The center of the silhouette is again used as the origin for the CIT. The discrete form of the CIT transform is used, as depicted graphically in Figure 3/right.

$$CIT(k\Delta\rho) = \frac{1}{T}\sum_{t=1}^{T} GEI(x_0 + k\Delta\rho \cdot \cos(t\Delta\theta), y_0 + k\Delta\rho \cdot \sin(t\Delta\theta)) \tag{5}$$

for $k = 1, ..., K$ with $T = 360^o/\Delta\theta$, where $\Delta\rho$, and $\Delta\theta$ are the constant step sizes of the radius and angle variables and finally $K\Delta\rho$ is the radius of the smallest circle that encloses the grayscaled GEI (Figure 2).
The extracted RIT and CIT feature vectors are then concatenated, in order to form a single $1D$ biometric trait.

3.1.1 Matching

The comparison between the number of gallery G_{GEI} and probe P_{GEI} gait cycles for a specific feature $E \in \{RIT, KRM\}$ is performed through the dissimilarity score d_E.

$$d_E = \min_{i,j} \left(||\mathbf{s}_i^G - \mathbf{s}_i^P|| \right) \ \forall i, j; i \in [1, G_{GEI}) \text{ and } j \in [1, P_{GEI}) \tag{6}$$

whereby $||\cdot||$ is the L_2-norm between the $\mathbf{s}^G$ and $\mathbf{s}^P$ values of the corresponding extracted feature (i.e. RIT & CIT) for the gallery and the probe collections, respectively.

3.2 Activity-related recognition

The proposed framework extends the applicability of activity-related biometric traits (Drosou, Moustakas, Ioannidis & Tzovaras (2010)), and investigates their feasibility in user authentication applications.

In (Kale et al. (2002)) and (Drosou, Moustakas & Tzovaras (2010)), it is claimed that the traits of a subject's movements during an activity that involves reaching and interacting with an environmental object can be very characteristic for recognition of his/her identity. Indeed, given the major or minor physiological differences between users' bodies in combination with their individual inherent behavioural or habitual way of moving and acting it has been reported that there is increased authentication potential in common everyday activities such as answering a phone call, etc.

In the following, an improved activity-related recognition framework is proposed, that employs a novel method for the normalization of the trajectories of the user's tracked points of interest. The proposed algorithm also introduces a warping method that compensates for small displacements of the environmental objects and has no effect on the behavioural information of the movement at all.

As of today, activity related biometrics, where the activity is associated with reaching and interacting with objects, have always assumed a fixed environment (Drosou, Moustakas & Tzovaras (2010)), which is not always the case in real life scenarios. However, significant performance degradations can be observed due to the small variances in the interaction setting, which are introduced by the arbitrary position of the environmental objects in respect to the user at each trial. Thus, a post-processing algorithm towards the improvement of the overall authentication performance that can be employed into biometric systems which utilize the reaching and interacting concept, is presented in the following.

3.2.1 Motion trajectory extraction

The core of the proposed authentication system used on dynamic motion tracking (4f) is extensively described in (Drosou, Moustakas, Ioannidis & Tzovaras (2010)) and is briefly described in the following so as to make the paper self-contained. The userŠs movements are recorded by a stereo camera and the raw captured images are processed, in order to track the users head and hands via the successive application of filtering masks on the captured image.

Specifically, a skin-colour mask (Gomez & Morales (2002)) (4a) combined with a motion-mask (Bobick & Davis (2001)) (Figure 4d) can provide the location of the palms, while the head can be accurately tracked via a combination of a head detection algorithm (Viola & Jones (2004)) enhanced by a mean-shift object tracking algorithm (Ramesh & Meer (2000)) (4b). Given the pre-calibrated set of CCD sensors mounted on the stereo camera, the real $3D$ information can be easily calculated first by performing disparity estimation (4c) from the

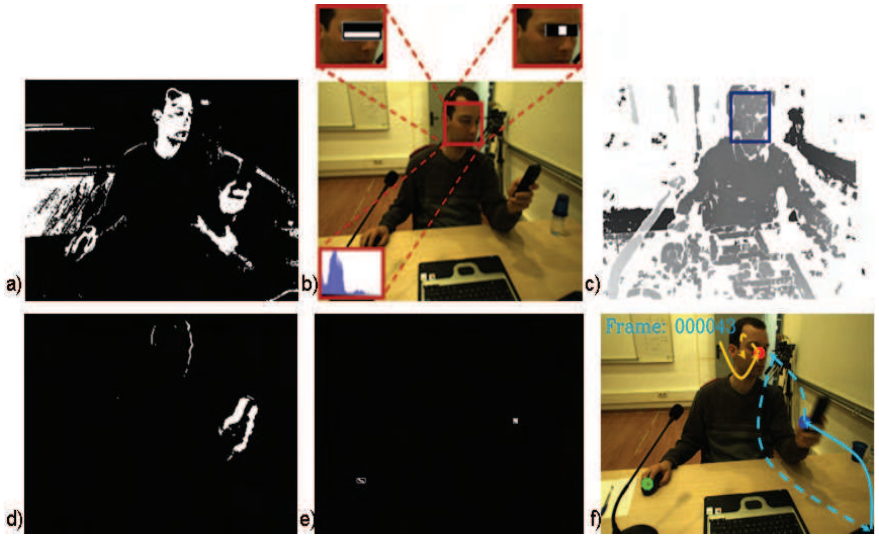


Fig. 4. Tracking methodology: a) Skin filtering - b) Head Tracking - c) Disparity image - d) Motion Detection - e) Possible hands' locations - f) Motion trajectories.

input stereoscopic image sequence and then by mapping the 2.5D information onto the $3D$ space. After post-processing (Drosou, Moustakas, Ioannidis & Tzovaras (2010)) that is applied on the raw tracked points, based on moving average window and Kalman filtering, equally sized and smooth $3D$ motion trajectories are extracted (Figure 5), which are then used as activity related biometric traits for proposed modality.
A motion trajectory for a certain limb l (head or palms) is considered as a $3D$ N-tuple vector $\mathbf{s_l}(\mathbf{t}) = (x_l(t), y_l(t), z_l(t))$ that corresponds to the x,y,z-axes location of limbs center of gravity at each time instance t of an $N - frame$ sequence. The x,y and z data of the trajectories $\mathbf{s_l}$, are concatenated into a single vector and all vectors, produced by the limbs that take part in a specific activity c form the trajectory matrix S_c. Each repetition of the same activity by a user creates a new matrix. Both gallery and probe user-specific set of matrices are subsequently used as input to the Dynamic Time Warping (DTW) algorithm 3.2.2 that has been utilized as classifier for the current biometric modality, in order to provide an authentication score with respect to the claimed ID (gallery).

3.2.2 Matching via DTW

DTW is used for calculating a metric about the dissimilarity between two (feature) vectors. It is based on the difference cost that is associated with the matching path computed via dynamic programming, namely the Dynamic Time Warping (DTW) algorithm. The DTW algorithm can provide either a valuable tool for stretching, compressing or aligning time shifted signals (Sakoe & Chiba (1990)) or a metric for the similarity between two vectors (Miguel-Hurtado et al. (2008)). Specifically, it has been widely used in a series of matching problems, varying from speech processing (Sakoe & Chiba (1990)) to biometric recognition applications (Boulgouris et al. (2004)). The matching between the two vectors is done and a path is found using a rectangular grid (Figure 6).

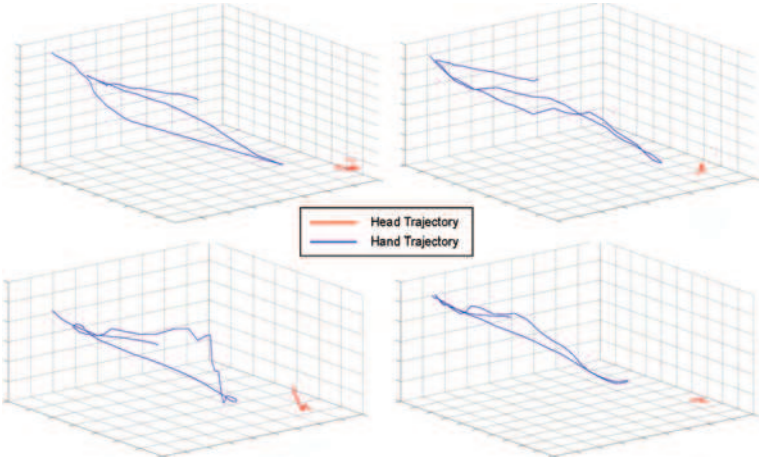


Fig. 5. 3*D* Motion Trajectories extracted during a "Phone Conversation" activity.

A short description of the functionality of *DTW* algorithm for comparing two one-dimensional vectors (probe & gallery signal) is presented below:
The probe vector **p** of length L is aligned along the X-axis while the gallery vector **g** of length L' is aligned along the Y-axis of a rectangular grid respectively. In our case $L \equiv L'$ as a result of the preprocessing steps (Section 3.2.1). Each node (i,j) on the grid represents a match of the i_{th} element of **p** with the j_{th} element of **g**. The matching values of each $\mathbf{p}(i)$,$\mathbf{g}(j)$ pair are stored in a cost matrix C_M associated with the grid. $c(1,1) = 0$ by definition and all warping paths are a concatenation of nodes starting from node $(1,1)$ to node (L,L).
The main task is to find the path for which the least cost is associated. Thus the difference cost between the two feature vectors is provided. In this respect, let $(y_1(k), y_2(k))$ represent a node on a warping path at the instance t of matching. The full cost $D(y_1, y_2)$ associated to a path starting from node $(1,1)$ and ending at node $(y_1(K), y_2(K))$ can be calculated as:

$$D(y_1, y_2) = D(y_1(k-1), y_2(k-1)) + c(y_1, y_2) = \sum_{m=1}^{k} c(y_1(m), y_2(m)) \tag{7}$$

Accordingly, the problem of finding the optimal path can be reduced to finding this sequence of nodes $(y_1(k), y_2(k))$, which minimizes $D(y_1(k), y_2(k))$ along the complete path.

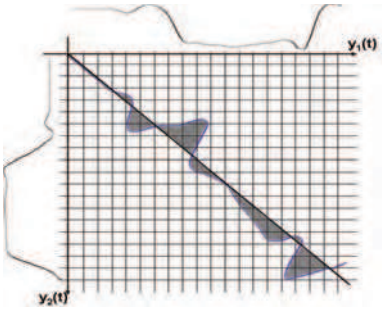


Fig. 6. Dynamic Time Warping Grid.

As stated by Sakoe and Chiba in (Sakoe & Chiba (1990)), a good path is unlikely to wander very far from the diagonal. Thus, the path with minimum difference cost, would be the one that draws the thinnest surface around the diagonal as shown by the dashed lines in Figure 6. In the ideal case of perfect matching between two identical vectors, the area of the drawn surface would be eliminated. The size of the closed area S_A around the diagonal can be calculated by counting the nodes $V(p_i, q_j)$ between the path and the diagonal at every row (Jayadevan et al. (2009)) as indicated by the following equation.

$$V(p_i, q_j) = \begin{cases} 1 \text{ , if } (i > j) \text{ of } N(p_i, q_j) \\ \quad \text{for } j = j, j+1, ..., j+d, \text{ where } d = i - j \\ 1 \text{ , if } (i < j) \text{ of } N(p_i, q_j) \\ \quad \text{for } i = i, i+1, ..., i+d, \text{, where } d = i - j \\ 1 \text{ , if } (i = j) \text{ of } N(p_i, q_j) \\ 0 \text{ , otherwise} \end{cases} \tag{8}$$

Thus, the value $V(p_i, q_j) = 1$ to these nodes. On the contrary, all other nodes lying outside the closed area will be assigned the value $V(p_i, q_j) = 0$. Then, the total area S_A created by the path is mathematically stated as following:

$$S_A = \sum_{i=1}^{L} \sum_{j=1}^{L} V(p_i, q_j) \tag{9}$$

whereby
Finally the total dissimilarity measure D_M between vector $\mathbf{p}$ and $\mathbf{g}$ (Equation 9) can be computed as the product of area size S_c and the minimum full cost $D(L, L)$ (Equation 7):

$$D_M = S_A \cdot D_{min}(L, L) \tag{10}$$

4. Biometric template security architecture

As far as the security of the biometric data is regarded, multiple feature descriptors from the gait modality and the activity-related modality are initially encoded via a Low Density Parity Check ($LDPC$) encoder. In the following, the parity bits of the activity-related modality are encrypted via a biometric-dependent key, so that double secured, non-sensitive biometric data is stored in the database or in smart cards, which are useless to any potential attackers of the system.
The proposed method, which resembles a channel coding problem with noisy side information at the decoder, is shown to improve the authentication rates as they are provided from the modality-specific classifiers. Additionally to the already known key-encryption methodologies, the encryption of the parity bits of the second modality takes place before their storage to the database. The novelty lies in the fact the personal encryption/decryption key used, is inherent in the biometric trait of the first modality and thus, it remains unknown even to each user. Specifically, in the implemented scenario the biometric key is selected according to the height and the stride length of the user.
The architecture (Figure 7) of the proposed security is thoroughly described in the next two Sections, whereby a functional analysis of the utilized distinct components is provided.

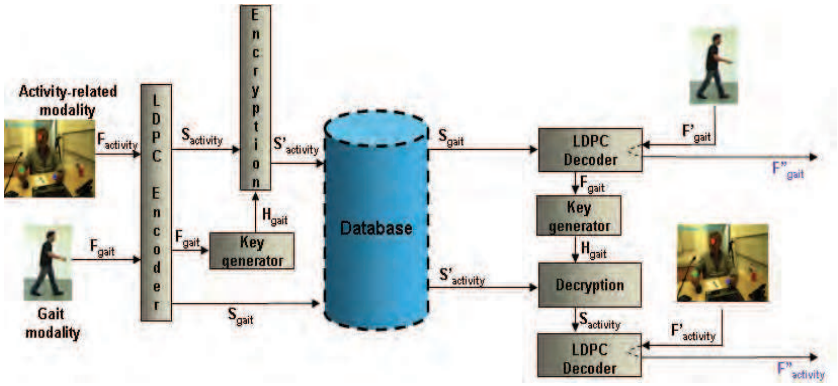


Fig. 7. Security subsystem Architecture.

4.1 Encoding scheme

The first step towards biometric template protection in the current multimodal 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, as presented in (Argyropoulos et al. (2009)). The main idea lies on the fact that perturbations in the representation of the biometric features at different times can be modelled as a 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. The proposed 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.

The architecture of the multimodal biometric authentication system is included in Figure 7. At the enrolment stage, the feature vectors F_{gait} and $F_{activity}$ from the *Gait* and the *Activity - related* modality are initially extracted as described in the previous section. Then, the extracted feature vectors are quantized and encoded using an (n, k) *LDPC* channel encoder. It must be stressed that the rate of the *LDPC* encoders in Figure 7 is different for each modality and is calculated according to the Slepian-Wolf theorem

$$R_X \geq H(X|Y)\ R_Y \geq H(Y|X)\ R_X + R_Y \geq H(X,Y) \tag{11}$$

where R_X and R_Y the achievable rates, $H(X|Y)$ and $H(Y|X)$ are the conditional entropies and $H(X,Y)$ is the joint entropy of X and Y gallery and probe feature vectors, respectively.

The resulting codewords S_{gait} and $S_{activity}$ comprise the biometric templates of the suggested 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_{gait} and $S_{activity}$, which are not capable of revealing sensitive information about the users.

Similarly the gait and activity-related feature vectors F'_{gait} and $F'_{activity}$ are extracted and quantized at the authentication stage. Subsequently, the syndromes S_{gait} and $S_{activity}$ which correspond to the claimed ID are retrieved from the database and are fed to the *LDPC*

decoders. A similar multimodal approach is thoroughly described in (Argyropoulos et al. (2009)). Thereby, two biometric traits, i.e. face characteristics and face, have been combined via concatenation of their feature vectors. Specifically, once the first modality was successfully decoded, the decoded feature vector was concatenated to probe feature vector of the second modality. The full feature vector was fed to a second decoder. Thus, enhanced security was offered, since the second decoder requires that both feature vector resembles the gallery input. In the proposed approach, the system deals with two behavioural biometric traits separately, as far as the *LDPC* algorithm is regarded. However, it must be noted that the two biometric templates in the proposed scheme are not secured independently from each other.
The basic guidelines of the *LDPC* encoding/decoding scheme will be presented below in short, in order to provide a self-consistent paper.
Given 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.
Initially, at the enrolment stage, the biometric signatures of an individual for *gait* and *activityrelated* modalities are obtained. The extracted features form the vector $\mathbf{F_i} = [f_1, \ldots, f_k]$, whereby $i \in gait, activity\ related$ and $f_i \in \mathbb{R}^k$. The feature vector $\mathbf{F_i}$ is then uniformly transformed from the continuous to the discrete domain of 2^L levels through the function $u : \mathbb{R}^k \rightarrow \mathbb{Q}^k$ whereby $\mathbb{Q} = 0, 1 \ldots, l-1$. Each one of the resulting vectors $\mathbf{q} = u(\mathbf{F_i})$ is fed to the Slepian.Wolf encoder, which performs the mapping $e : \mathbb{Q}^k \rightarrow \mathbb{C}^n$ where $C = \{0, 1\}$ outputs the codeword $\mathbf{c} = e(\mathbf{q})$, $\mathbf{c} \in \mathbb{C}^n$.
As already mentioned, herein the Slepian-Wolf algorithm has been implemented by a systematic *LDPC* encoder (Gallager (1963)) (see Figure 8). *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 (Girod et al. (2005)) was employed to avoid encoding and storing the L bit-planes of the vector $\mathbf{q}$ separately.

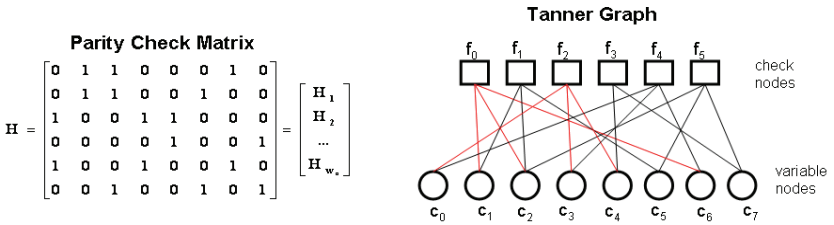


Fig. 8. Encoding via a Parity Check Matrix.

Subsequently, the k systematic bits of the codeword ci are discarded and only the syndrome $\mathbf{s}$, that is the $n-k$ parity bits of the codeword $\mathbf{c}$, is stored to the biometric database. Thus, the biometric templates of an enrolled user consist of the syndromes $\mathbf{s} = [c_{k+1} \dots c_n]$, $\mathbf{s} \in \mathbb{C}^(n-k)$, and their size is $n-k$. It must be stressed that the rate of the two $LDPC$ encoders is different because the statistical properties of the two modalities are different.
Similarly to the enrollment procedure the biometric feature vector $\mathbf{F}'_{\mathbf{i}}$ is obtained quantized at the authentication stage. This, together with encoded syndrome $\mathbf{s}_i^{encoded}$ are fed to the $LDPC$ decoder. The decoding function $d : \mathbb{C}^(n-k) \times \mathbb{R}^k \rightarrow \mathbb{Q}^k$ combines $\mathbf{F_i}$ with the corresponding syndromes which are retrieved from the biometric database and correspond to the claimed identity I. The decoder employs belief-propagation (Ryan (n.d.)) to decode the received codewords.
If the errors introduced in the side information with respect to the originally encoded signal are within the error correcting capabilities of the channel decoder then the correct codeword is output after an experimentally set (N_c=30) number of iterations and the transaction is considered as a client transaction. To detect whether a codeword is correctly decoded we add 16 Cyclic Redundancy Check (CRC) bits at the beginning of the feature vector $\mathbf{F_i}$. 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 ($N_{iter} \geq N_c$) a special symbol $\varnothing$ is output and the transaction is considered as an impostor transaction.
From the above, it is obvious that the level of security and the performance of the system significantly bases on the number of the parity bits in syndrome $\mathbf{s_i}$, apart from the error correcting performance of the channel code.
On the one hand, a channel code with low code rate exhibits high error correcting capabilities, which results in the decoding of very noisy signals. This means, that the channel decoder will be able to decode the codeword even if the noise in the biometric signal has been induced by impostors. Additionally, will consist of many bits and will be more difficult to forge. On the other hand, channel codes of high code rate exhibit limited error-correcting capabilities and reduce the security of the system since the parity bits produced by the channel encoder consist of a few bits. Thus, the design of an effective biometric system based on the channel codes involves the careful selection of the channel code rate to achieve the optimal trade-off between performance and security. In this respect, a method for further securing the syndrome $\mathbf{s_i}$ is proposed in the following section (4.2). Thus, both the security of a long syndrome is preserved, while improved performance is provided.

4.2 Encryption scheme

The second phase of the security template algorithm, that is implemented via an encryption algorithm ("*Keygenerator*" box in Figure 7) has a dual mission. On the one hand, it further ensures the security of the stored biometric syndromes $\mathbf{S_{gait}}$ and $\mathbf{S_{activity}}$ (see Section 4.1) and on the other hand, it provides a novel method for fusing static physiological information with dynamic behavioural traits. An interesting novelty introduced by the specific methodology is that the user is no longer obliged to memorize a pin, in order to secure his data. On the contrary, the personal password is automatically extracted from a series of N_b soft biometric features. Thus, the password can neither be stolen nor copied. The utilized methodology is presented below.
In the current implementation of the proposed framework $N_b = 2$ soft biometric characteristics have been included. However, the framework can be easily extended to

any arbitrary number of soft biometric features, depending on the utilized modalities. In particular, the *Height* and the *StrideLength* (see Figure 9) of the user have been utilized hereby according to the following extendable methodology.

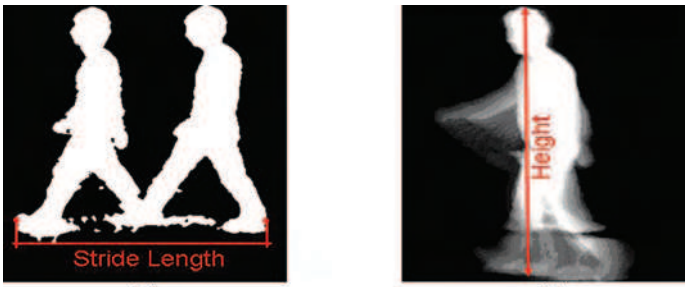


Fig. 9. Stride length (left) and Height (Right) of a user drawn on his/her Gait Energy Image (GEI).

It has been experimentally noticed that the measurement regarding the user's *Stride* are much more noisy than the ones for his/her *Height*. Thus, the ratio of $\frac{Height}{Stride}$ has been preferred over pure *Stride* scores, in order to provide a more uniform score distribution for the second soft-biometric trait.

First, a two dimensional hash table is formed, whereby its dimension is limited by the minimum and maximum expected value of each soft biometric trait, as illustrated in Figure 10/left. The resolution f_s^{height} and f_s^{stride} of the grid in each dimension respectively is scalable, in order to be optimally adjusted to the needs of each implementation of the framework (see Section 6). Thereafter, a unique biometric key is estimated for each cell on the grid (or cube or hypercube in the case of $N_b \geq 2$), according to the corresponding Soft Biometric values. Thus, we can write for the general case of N_b available soft biometric traits

$$Key(n_1, n_2, \ldots, n_{N_b}) = \frac{\sum_{i=1}^{N_b} n_i}{N_b} \tag{12}$$

whereby n_i stands for the index of the hash table (see Figure 10/left) and is calculated as $n_i = int(\frac{v_i}{f_s^i})$. v_i stands for the extracted value of the i^{th} Soft Biometric trait.

In this context, it is expected that the same user will always obtain the same biometric key, since his soft biometric properties will always assign his identity with the same hypercube in the grid.

In the following, the syndromes S_i of the i^th modality are encrypted using the Rijndael implementation (Daemen & Rijmen (1999)) of the Advanced Encryption Standard (AES). Specifically, the $128-bit$ extracted key is used to shuffle the syndrome bits. Simple zero-padding technique is performed on the syndrome bits vector, in the cases where their number is not a whole multiplier of 2^7 bits. Similarly, a $256-bit$ key could have been extracted, however it has been experimentally seen that it offers a bad trade-off between computational resources and security improvement.

In this respect, the biometric key is used to shuffle/deshuffle the syndromes for the claimed ID in the enrollment/authentication phase of the biometric system, respectively. It is easy to understand that most probably an impostor would be assigned to a different cell on the grid, given his different soft biometric characteristics with respect to the claimed ID. Thus, the

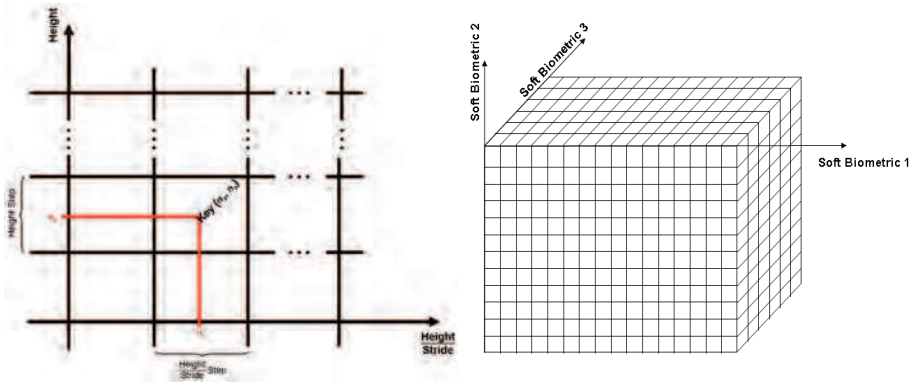


Fig. 10. 2D Soft Biometric Grid (Left) - 3D Soft Biometric Grid (Right)

requested syndrome bits will be wrongly decrypted and the applied dynamic biometric trait will never match the decoded one (see Section 4.1).

5. Score fusion

In order to provide an overall distance score between the user requesting access and the corresponding claimed ID, a fusion of the partial matching distances for each modality has to be performed. The fusion approach that has been utilized for the current biometric system is based on score level fusion. Thus, the optimal fusion score, that would combine unequally amounts of information from each RP is defined as follows

$$S_{tot} = \mathbf{W} \cdot \mathbf{S} = \sum_{j=1}^{N} w_j s_j = w_1 s_1 + w_2 s_2 + \ldots + w_N s_N \tag{13}$$

whereby $\mathbf{W}$ is the weight coefficient matrix with N w_j elements and $\mathbf{S_j}$ the score matrix having as elements the corresponding partial matching distances s_j.
In this respect, the most common problem that has to be solved in a score-level fusion approach is the optimal estimation of matrix $\mathbf{W}$. Given the general structure of a multimodal biometric system, it is expected that the authentication capacity would be higher for some modalities than for some others. Thus, a rational way for defining the partial weight coefficients w_j for each modality is to assign a value proportional to their overall authentication performance, as follows:

$$w_j = 1 - \frac{EER_j}{\sum_{j=1}^{N} EER_j} \tag{14}$$

where EER_j stands for the Equal Error Rate score for the j^{th} modality.
For the current bi-modal ($N = 2$) biometric system, the values for each w_j are defined as:

$$w_1 = 1 - \frac{EER_1}{EER_1 + EER_2}\,;\, w_2 = 1 - \frac{EER_2}{EER_1 + EER_2} \tag{15}$$

In order to provide normalized scores in the range of values for each modality, all scores have been normalized to a common basis according to the following equation:

$$s^{norm} = (\frac{0.5}{T_L})e^{(-\frac{s}{s^{max}})} \tag{16}$$

where s_k^{norm} is the normalized score value, s_k the non-normalized score, s_k^{max} the maximum possible score value and T_k an experimentally set threshold for the k^{th} modality; $k \in \{RIT, CIT, DTW\}$.

6. Results

The current Section starts with a short description of the database on which the experiments have been carried out. In the following, the identification and authentication results of the presented framework implementation are exhibited and qualitatively evaluated. A short discussion about the proposed framework is also included.

6.1 Database

The evaluation of the proposed secure multimodal biometric framework has been performed on the proprietary ACTIBIO-dataset (*ACTIBIO ICT STREP* (2008)). The current annotated database was captured in an ambient intelligence indoor environment and consists of 29 subjects, performing a series of everyday workplace & office activities. The workplace recordings include 29 subjects walking in various paths of $6m$, while being recorded by a stereoscopic camera that was placed $2.5m$ away from the walking path and lateral to the walking direction. In order to test the permanence of the biometric features, the recordings have been repeated in a second session, few months after the first one.

Regarding the office recordings, the same 29 subjects have been recorded in an ambient intelligence (*Am1*) indoor environment, while they have been performing a series of everyday office activities with no special protocol, such as a phone conversation, typing, talking to a microphone panel and drinking water. Each subject repeated the same sequence of activities 8 times in total, split in two sessions while a manual annotation of the database has followed. Among the five cameras that have been recording the users from different view-angles, only the recordings from a frontal stereoscopic camera have been used for the current work.

Within the current work, the traits of the aforementioned modalities have been combined, in order to create 29 user-specific multimodal signatures. In this respect, each subject has been registered to the system (*gallery signatures*) by using his gait biometric signature together with his behavioural response during a phone conversation. Despite the fact that the current dataset does also include complicated gait scenarios, whereby the subject is carrying a bag or a coat, the simplest version has been utilized within the presented work. Similarly, only the "Phone Conversation" activity has been used from the office environment. Similarly, the recordings from each modality for a different repetition have been combined in order to form the *probe signatures* for the system.

6.2 Authentication & verification results

As it has already been stressed out the major contribution of the current framework is that it allows higher level of security of the biometric templates stored in the database, while higher recognition performance is simultaneously provide via the encoding of soft biometrics. The improved level of security can be easily noticed, when considering that the information stored in the database is encrypted. In this respect, not data can be retrieved from the

database without providing the correct key. Further, even if this encryption step is somehow bypassed, the obtained data remain still of no use to the attacker, since they reveal no biometric information as explained in Section 4.1.
Moreover, in order to illustrate the advances performed in the recognition performance via indirect fusion/encoding of the soft biometric traits with the dynamic ones, the initial recognition capabilities of the utilized traits is shown in Figure 11. In the same Figures the reader can notice a slight degradation in the recognition performance of the activity related modality, when the templates that are stored in the database are secured via the $LDPC$ encoding algorithm (Section 4.1). Contrary to the $1D$ feature vector of the gait modality, activity related feature vectors are much more complex. Thus, a degradation in the authentication performance is more likely due to the noisy errors at the decoding. Moreover, a degradation is expected, since this is the trade off for adding enhanced security in the biometric system. Specifically, such a deterioration have been mainly caused by the unintended reconstruction of an impostor's feature vector, so that it resembles a genuine user.

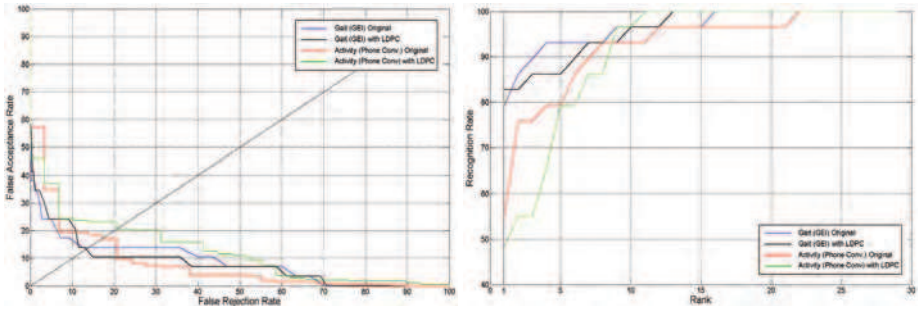


Fig. 11. EER Scores (left) and Identification performance (right) of the proposed modalities prior to encryption.

As it has been mentioned in Section 4.2 the current framework allows a scalable resolution of the hash table that is used for encryption, so that optimal performance of the system is achieved, given different soft biometrics. In this respect, the *Optimal Functional Point* (*OFP*) of the current system has been set according to the results illustrated in Figures 12. Specifically, one can notice that an intense degradation of the system's recognition performance for high resolution values ($\equiv$ large number of available keys in Hash Matrix of Figure 10left). This is caused by the noisy measurements of the soft biometric trait in different repetitions. For instance, let us assume a user that has been registered to the system with a $v_{Height} = 1.79$ and $v_{Stride} = 1.62$. He/she would be assigned the key $K(17, 14)$. A noisy measurement of his soft biometrics at the authentication stage might result that his stored syndrome $\mathbf{s}$ was attempted to be decoded by a different key $Key(n_1^{probe}, n_2^{probe}) \neq K(17, 14)$. Thus, the decrypting would never be successful and the recognition would fail. The reason for which the EER scores of the activity related modality exhibits more fluctuations than the one of the gait bases on the following fact: The soft biometric measurements of some impostors in the authentication stage did not only lie within the same hash bin as the client, but also their activity related traits managed to be decoded via $LDPC$ using the syndrome of the claimed user's ID.
In this concept, it can be concluded that high resolution values, which refer to a big number of bins in the hash table, are intolerant to noisy measurements. On the other hand, small resolution values may result to the fact that all subjects are assigned to the same key K and

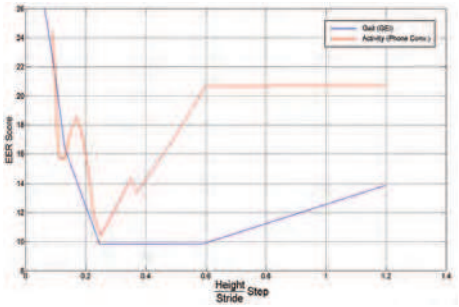


Fig. 12. EER scores of the proposed modalities as a function of the $\frac{Height}{Stride}$ step.

thus, the encryption scheme would have no meaning. On the contrary, there is always an functional point, whereby the recognition performance of the system is optimal.
Moreover, the reader can notice in Figure 12 that for the $\frac{Height}{Stride} step = 0.25$ both modalities achieve their authentication performance. Thus, this value can be considered the system's optimal functional point for a given $Height$ resolution in the hash table, experimentally set at f_s^{Height}.

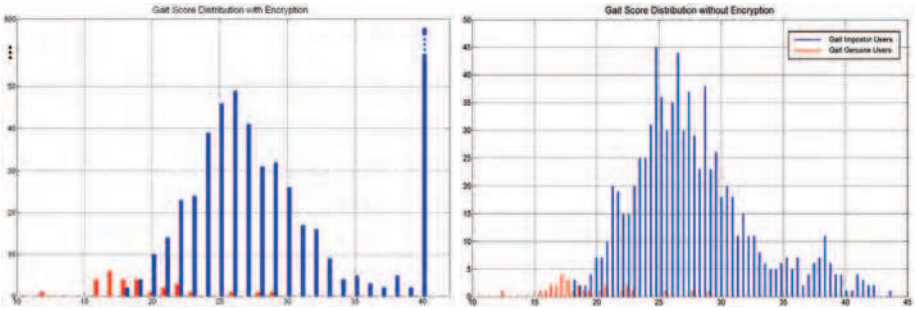


Fig. 13. Client/Impostor Distributions for the gait modality at the optimal functional point(left) and without Encryption(right) via the Biometric key.

Although there seems to be only small changes in the EER scores for small resolution values, the distribution of the genuine/impostor scores significantly changes (see Figure 13).

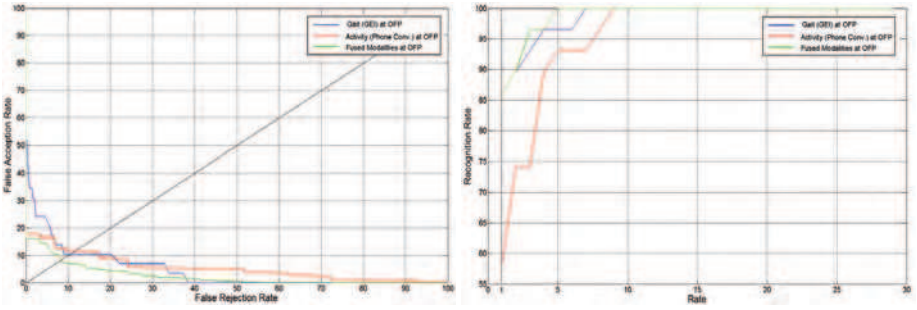


Fig. 14. EER Scores (left) and Identification performance (right) of the proposed system.

Given the optimal functional point of the encryption system, optimal fusion of the soft biometrics with the dynamic traits has been also achieved. In this respect, the current test case of the proposed framework has been evaluated in terms of its overall recognition performance, by performing fusion between the two utilized behavioral biometrics (Sections 3.1 & 3.2) as described in Section 5. The derived optimal recognition performance of the bimodal biometric system system is illustrated in Figures 14, in terms of both authentication and identification capacity.
Concluding, it must be noted that the potential of the proposed framework in terms of recognition performance is significantly high. Given a larger number of soft biometrics, an almost $1-1$ proportion for keys-users can be achieved, which would lead to further decreasing of the recognition error.

7. Conclusions

Summarizing, the advantages of the proposed method in terms of security and impact on matching accuracy for recognition purposes have been thoroughly analyzed and discussed. The performance of the proposed method is assessed in the context of ACTIBIO, an EU Specific Targeted Research Project, where activity-related and gait biometrics are employed in an unobtrusive application scenario for human recognition. The experimental evaluation on a multimodal biometric database demonstrates the validity of the proposed framework. Most important, the dual scope of the current framework has been illustrated. Specifically, the utilization of the encryption algorithm does not only provide enhanced template security; it does also provide indirect fusion with soft biometric characteristics and thus it improves the recognition potential. Finally, the proposed user-specific biometric key, which exclusively depends on the user's biometry, increases the level of unobtrusiveness of the system, since the user is not obliged anymore to memorize pins or to carry ID cards.

8. Acknowledgments

This work was partially supported by the EU funded ACTIBIO IST STREP (FP7-215372) (*ACTIBIO ICT STREP* (2008)).

9. References

ACTIBIO ICT STREP (2008).

Álvarez, F. H., Encinas, L. H. & Ávila, C. S. (2009). Biometric Fuzzy Extractor Scheme for Iris Templates, *World Congress in Computer Science, Computer Engineering and Applied Computing*.

Argyropoulos, S., Tzovaras, D., Ioannidis, D. & Strintzis, M. G. (2009). A Channel Coding Approach for Human Authentication From Gait Sequences, *IEEE Trans.Inf. Forensics Security.* 24(3): 428–440.

Bobick, A. & Davis, J. (2001). The recognition of human movement using temporal templates, *IEEE Trans. Pattern Anal. Mach. Intell.* 23(3): 257–267.

Boulgouris, N., Plataniotis, K. & Hatzinakos, D. (2004). Gait recognition using dynamic time warping, *IEEE 6th Workshop on Multimedia Signal Processing*, Siena, pp. 263–266.

Chang, K. I., Bowyer, K. W. & Flynn, P. J. (2005). An evaluation of multimodal 2D+3D face biometrics., *IEEE transactions on pattern analysis and machine intelligence* 27(4): 619–24.

Cohen, G. & Zemor, G. (2004). Generalized coset schemes for the wire-tap channel: application to biometrics, *IEEE International Carnahan Conference on Security Technology (ICCST)Symposium on Information Theory*, Chicago, IL, p. 46.

Cucchiara, R., Grana, C., Piccardi, M., Prati, A. & Sirotti, S. (2001). Improving shadow suppression in moving object detection with HSV color information, *Intelligent Transportation Systems* pp. 334–339.

Daemen, J. & Rijmen, V. (1999). The Rijndael Block Cipher.

Davida, G. I., Frankel, Y. & Matt, B. J. (1998). On enabling secure applications through off-line biometric identification, *IEEE Symp. Security and Privacy*, Oakland, CA, pp. 148–157.

Draper, S. C., Khisti, A., Martinian, E., Vetro, A. & Yedidia, J. (2007). Using distributed source coding to secure fingerprint biometrics, *Int. Conf. Acoustics, Speech and Signal Processing*, Honolulu, HI, pp. 129–132.

Drosou, A., Ioannidis, D., Moustakas, K. & Tzovaras, D. (2010). Unobtrusive Behavioural and Activity Related Multimodal Biometrics: The ACTIBIO Authentication Concept, *The Scientific World - Special Issue on: Biometrics Applications: Technology, Ethics and Health Hazards* p. accepted for publication.

Drosou, A., Moustakas, K., Ioannidis, D. & Tzovaras, D. (2010). On the potential of activity-related recognition, *The International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISAPP 2010)*.

Drosou, A., Moustakas, K. & Tzovaras, D. (2010). Event-based unobtrusive authentication using multi-view image sequences, *Proc. of ACM Multimedia/Artemis Workshop ARTEMISŠ10*, Florence, pp. 69 – 74.

Fairhurst, M., Deravi, F., Mavity, N., George, J. & Sirlantzis, K. (2003). *Intelligent Management of Multimodal Biometric Transactions*, Springer Berlin-Heidelberg.

Gallager, R. (1963). *Low-Density Parity-Check Codes*, MIT Press, Cambridge, MA.

Girod, B., Aaron, A. M., Rane, S. & Rebollo-Monedero, D. (2005). Distributed video coding, *Proc. IEEE* 93: 71–89.

Goffredo, M., Bouchrika, I., Carter, J. N. & Nixon, M. S. (2009a). Performance analysis for automated gait extraction and recognition in multi-camera surveillance, *Multimedia Tools and Applications* .

Goffredo, M., Bouchrika, I., Carter, J. N. & Nixon, M. S. (2009b). Self-Calibrating View-Invariant Gait Biometrics., *IEEE transactions on systems, man, and cybernetics. Part B, Cybernetics : a publication of the IEEE Systems, Man, and Cybernetics Society* .

Gomez, G. & Morales, E. F. (2002). Automatic feature construction and a simple rule induction algorithm for skin detection, *Proc. of the ICML Workshop on Machine Learning in Computer Vision (MLCV)*, pp. 31–38.

Hadid, A., Pietikäinen, M. & Li2, S. Z. (2007). *Learning Personal Specific Facial Dynamics for Face Recognition from Videos*, Springer Berlin / Heidelberg, pp. 1–15.

Han, X., Liu, J., Li, L. & Wang, Z. (2006). Gait recognition considering directions of walking, *Proceedings of the IEEE Conference on Cybernetics and Intelligent Systems*, pp. 1–5.

Ioannidis, D., Tzovaras, D., Damousis, I. G., Argyropoulos, S. & Moustakas, K. (2007). Gait Recognition Using Compact Feature Extraction Transforms and Depth Information, *IEEE Trans.Inf. Forensics Security.* 2(3): 623–630.

Jain, A. K., Ross, A. & Prabhakar, S. (2004). An Introduction to Biometric Recognition, *IEEE Trans. Circuits Syst. Video Technol.* 14(1): 4–20.

Jain, A., Nandakumar, K. & Ross, A. (2005). Score normalization in multimodal biometric systems, *Pattern recognition* 38(12): 2270–2285.

Jayadevan, R., Kolhe, S. R. & Patil, P. M. (2009). Dynamic Time Warping based Static Hand Printed Signature Verification, *ournal of Pattern Recognition Research* 4(1): 52–65.

Juels, A. & Sudan, M. (2006). A fuzzy vault scheme, *Designs Codes Cryptography* 38(2): 237–257.

Junker, H., Ward, J., Lukowicz, P. & Tröster, G. (2004). User Activity Related Data Sets for Context Recognition, *Proc. Workshop on 'Benchmarks and a Database for Context Recognition'*.

Kale, A., Cuntoor, N. & Chellappa, R. (2002). A framework for activity-specific human identification, *IEEE Proc. International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Vol. 4, pp. 3660–3663.

Kale, A., Sundaresan, A., Rajagopalan, A., Cuntoor, N. P., Roy-Chowdhury, A. K., Kruger, V. & Chellappa, R. (n.d.). Identification of Humans Using Gait, *IEEE Trans. Image Processing* 13: 1163–1173.

Kumar, A., Kanhangad, V. & Zhang, D. (2010). A New Framework for Adaptive Multimodal Biometrics Management, *IEEE Trans.Inf. Forensics Security.* 5(1): 92 – 102.

Liu, X. & Chen, T. (2003). Video-based face recognition using adaptive hidden markov models, *IEEE Proc. Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)* 1: 340–345.

Maltoni, D., Jain, A. & Prabhakar, S. (2009). *Handbook of fingerprint recognition*, 2nd edn, Springer Professional Computing.

Martinian, E., Yekhanin, S. & Yedidia, J. (2005). Secure biometrics via syndromes, *43rd Annual Allerton Conf. on Communications, Control, and Computing*, Monticelo, IL.

Miguel-Hurtado, O., Mengibar-Pozo, L. & Pacut, A. (2008). A new algorithm for signature verification system based on DTW and GMM, *IEEE International Carnahan Conference on Security Technology ICCST* 42: 206–213.

Pradhan, S. S. & Ramchandran, K. (2003). Distributed source coding using syndromes (discus): Design and construction, *IEEE Trans. Inf. Theory* 49(3): 626–643.

Qazi, F. A. (2004). A survey of biometric authentication systems, *Security and Management* pp. 61–67.

Ramesh, D. C. V. & Meer, P. (2000). Real-Time Tracking of Non-Rigid Objects Using Mean Shift, *IEEE Proc. Computer Vision and Pattern Recognition 2007 (CVPR)*, Vol. 2, pp. 142–149.

Ryan, M. G. (n.d.). Visual Target Tracking.

Sakoe, H. & Chiba, S. (1990). Dynamic programming algorithm optimization for spoken word recognition, *Readings in speech recognition* .

Sim, T., Zhang, S., Janakiraman, R. & Kumar, S. (2007). Continuous Verification Using Multimodal Biometrics, *IEEE Trans. Pattern Anal. Mach. Intell.* 29(4): 687 – 700.

Slepian, J. D. & Wolf, J. K. (1973). Noiseless coding of correlated information sources, *IEEE Trans. Inf. Theory* 19: 471–480.

Stallings, W. (2006). *Cryptography and Network Security: Principles and Practices.*, Prentice-Hall: Upper Saddle River, NJ.

Sun, Z. & Tan, T. (2009). Ordinal Measures for Iris Recognition, *IEEE Trans. Pattern Anal. Mach. Intell.* 31(12): 2211.

Uludag, U., Pankanti, S., Prabhakar, S. & Jain, A. K. (2004). Biometric Cryptosystems: Issues and Challenges, *Proceedings of the IEEE* 92(6): 948–960.

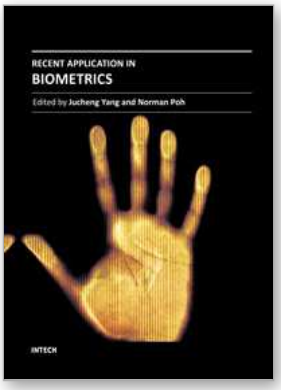
Viola, P. & Jones, M. J. (2004). Robust Real-Time Face Detection, *International Journal of Computer Vision* 57(2): 137–154.

Wadayama, T. (2005). An authentication scheme based on a low-density parity check matrix, *Int. Symp. Information Theory*, pp. 2266–2269.

Xiao, Q. (2005). Security issues in biometric authentication, *Information Assurance Workshop, IAW 2005* pp. 8–13.

Yao-Chung, L., Varodayan, D. & Girod, B. (2007). Image authentication based on distributed source coding, *Int. Conf. on Image Processing*, San Antonio, TX, pp. 5–8.

Yu, C., Cheng, H., Cheng, C. & Fan, K.-C. (2010). Efficient Human Action and Gait Analysis Using Multiresolution Motion Energy Histogram, *Journal on Advances in Signal Processing (EURASIP)* p. 13.



Recent Application in Biometrics

Edited by Dr. Jucheng Yang

ISBN 978-953-307-488-7
Hard cover, 302 pages
Publisher InTech
Published online 27, July, 2011
Published in print edition July, 2011

In the recent years, a number of recognition and authentication systems based on biometric measurements have been proposed. Algorithms and sensors have been developed to acquire and process many different biometric traits. Moreover, the biometric technology is being used in novel ways, with potential commercial and practical implications to our daily activities. The key objective of the book is to provide a collection of comprehensive references on some recent theoretical development as well as novel applications in biometrics. The topics covered in this book reflect well both aspects of development. They include biometric sample quality, privacy preserving and cancellable biometrics, contactless biometrics, novel and unconventional biometrics, and the technical challenges in implementing the technology in portable devices. The book consists of 15 chapters. It is divided into four sections, namely, biometric applications on mobile platforms, cancelable biometrics, biometric encryption, and other applications. The book was reviewed by editors Dr. Jucheng Yang and Dr. Norman Poh. We deeply appreciate the efforts of our guest editors: Dr. Girija Chetty, Dr. Loris Nanni, Dr. Jianjiang Feng, Dr. Dongsun Park and Dr. Sook Yoon, as well as a number of anonymous reviewers.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Anastasios Drosou, Dimosthenis Ioannidis, Georgios Stavropoulos, Konstantinos Moustakas and Tzovaras (2011). Biometric Keys for the Encryption of Multimodal Signatures, Recent Application in Biometrics, Dr. Jucheng Yang (Ed.), ISBN: 978-953-307-488-7, InTech, Available from: http://www.intechopen.com/books/recent-application-in-biometrics/biometric-keys-for-the-encryption-of-multimodal-signatures

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821