

1 Multimodal Physiological Biometrics Authentication

A. RIERA¹, A. SORIA-FRISCH^{1,2}, M. CAPARRINI¹, I. CESTER¹ AND G. RUFFINI¹

¹ Starlab Barcelona S.L., Barcelona

² Universitat Pompeu Fabra, Barcelona

1.1 INTRODUCTION

The term biometry is derived from the Greek words ‘bios’ (life) and ‘metron’ (measure). In the broader sense, biometry can be defined as the measurement of body characteristics. With this non-technological meaning, this term has been used in medicine, biology, agriculture and pharmacy. For example, in biology, biometry is a branch that studies biological phenomena and observations by means of statistical analysis.

However, the rise of new technologies since the second half of the 20th century to measure and evaluate physical or behavioural characteristics of living organisms automatically has given the word a second meaning. In the present study, the term biometrics refers to the following definition [33]:

The term biometry refers to automated methods and techniques that analyze human characteristics in order to recognise a person, or distinguish this person from another, based on a physiological or behavioural characteristic.

Biometry, however, has also acquired another meaning in the last decades, focused on the characteristic to be measured rather than the technique or methodology used [33]:

ii MULTIMODAL PHYSIOLOGICAL BIOMETRICS AUTHENTICATION

A biometric is a unique, measurable characteristic or trait of a human being for automatically recognising or verifying identity.

These definitions contain several important concepts that are critical to biometry:

Unique: In order for something to be unique, it has to be the only existing one of its type, have no like or equal, be different from all others. When trying to identify an individual with certainty, it is absolutely essential to find something that is unique to that person.

Measurable: In order for recognition to be reliable, the characteristic being used must be relatively static and easily quantifiable. Traits that change significantly with time, age, environment conditions or other variables are of course not suitable for biometrics.

Characteristic or trait: Measurable physical or personal behavioural pattern used to recognise a human being. Currently, identity is often confirmed by something a person has, such as a card or token, or something the person knows, such as a password or a personal identification number. Biometrics involves something a person is or does. These types of characteristics or traits are intrinsic to a person, and can be approximately divided into physiological and behavioural. Physiological characteristics refer to what the person is, or, in other words, they measure physical parameters of a certain part of the body. Some examples are fingerprints, that use skin ridges, face recognition, using the shape and relative positions of face elements, retina scanning, etc. Behavioural characteristics are related to what a person does, or how the person uses the body. Voice or gait recognition, and keystroke dynamics, are good examples of this group.

Automatic: In order for something to be automatic it must work by itself, without direct human intervention. For a biometric technology to be considered automatic, it must recognize or verify a human characteristic in a reasonable time and without a high level of human involvement.

Recognition: To recognize someone is to identify them as someone who is known, or to distinguish someone because you have seen, heard or experienced them before (to 'know again'). A person cannot recognise someone who is completely unknown to them. A computer system can be designed and trained to recognise a person based on a biometric characteristic, comparing a biometric presented by a person against biometric samples stored in a database. If the presented biometric matches a sample on the file, the system then recognises the person.

Verification: To verify something is to confirm its truth or establish its correctness. In the field of biometrics, verification is the act of proving the claim made by a person

about their identity. A computer system can be designed and trained to compare a biometrics presented by a person against a stored sample previously provided by that person and identified as such. If the two samples match, the system confirms or authenticates the individual as the owner of the biometrics on file.

Identity: Identity is the answer to the question about who a person is, or the qualities of a person or group which make them different from others, i.e., being a specific person. Identity can be understood either as the distinct personality of an individual regarded as a persistent entity, or as the individual characteristics by which this person is recognised or known. Identification is the process of associating or linking specific data with a particular person.

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in authentication mode or identification mode:

- **Authentication** (Greek: *αυθεντικός*, from ‘authentēs’=‘author’) is the act of proving the claim made by a person about their identity. In other words, the authentication of a person consists in verifying the identity they declare. In the authentication mode, the system validates a person’s identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognised claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., ‘Does this biometric data belong to X?’). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity. Authentication is also commonly referred to as verification.
- **Identification** (Latin: *idem-facere*, ‘to make the same’) is the act of recognizing a person without any previous claim or declaration about their identity. In other words, the identification of a person consists in recognizing them, that person being aware or not of this recognition task being performed. In the identification mode, the system recognises an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual’s identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., ‘Whose biometric data is this?’). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional

methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

In our paper we will describe a system that works on authentication mode, although it is quite straight forward to modify it to work on identification mode [25].

The increasing interest in biometry research is due to the increasing need for highly reliable security systems in sensitive facilities. From defense buildings to amusement parks, a system able to identify subjects in order to decide if they are allowed to pass or not would be very well accepted. This is because identity fraud nowadays is one of the more common criminal activities and is associated with large costs and serious security issues. Several approaches have been applied in order to prevent these problems. Several biometric modalities are already being used in the market: voice recognition, face recognition and fingerprint recognition are among the more common modalities nowadays. But other types of biometrics are being studied nowadays as well: ADN analysis, keystroke, gait, pa print, ear shape, hand geometry, vein patterns, iris, retina and written signature.

New types of Biometrics, such as electroencephalography (EEG) and electrocardiography (ECG), are based on physiological signals, rather than more traditional biological traits. These have their own advantages as we will see in the following paragraphs.

An ideal biometric system should present the following characteristics: 100% reliability, user friendliness, fast operation and low cost. The perfect biometric trait should have the following characteristics: very low intra subject variability, very high inter subject variability, very high stability over time and universal. Typical biometric traits, such as fingerprint, voice and retina, are not universality, and can be subject to physical damage (dry skin, scars, loss of voice, ...). In fact, it is estimated that 2-3% of the population is missing the feature that is required for authentication, or that the provided biometric sample is of poor quality. Furthermore, these systems are subject to attacks such as presenting a registered deceased person, dismembered body part or introduction of fake biometric samples. Since every living and functional person has a recordable EEG/ECG signal, the EEG/ECG feature is universal. Moreover brain or heart damage is something that rarely occurs. Finally it is very hard to fake an EEG/ECG signature or to attack an EEG/ECG biometric system.

EEG is the electrical signal generated by the brain and recorded in the scalp of the subject. These signals are spontaneous because there are always currents in the scalp of living subjects. In other words, the brain is never at rest. Because everybody has different brain configurations (it is estimated that a human brain contains 10^{11} neurons and 10^{15} synapses), spontaneous EEG between subjects should be different; therefore a high inter-subject variability is expected [11].

A similar argument can be applied to ECG. This signal describes the electrical activity of the heart, and it is related to the impulses that travel through it. It provides information about the heart rate, rhythm and morphology. As these characteristics are very subject-dependent, a high inter-subject variability is also expected. This has been shown in previous works [14, 15, 16, 17, 18].

As will be demonstrated using the results of our research, EEG and ECG present a low intra-subject variability in the recording conditions we defined: during one minute the subject should be relaxed and with their eyes closed. Furthermore the system presented herein attains an improvement of classification performance by combining feature fusion, classification fusion and multimodal biometric fusion strategies. This kind of multi-stage fusion architecture has been presented in [22] as an advancement for biometry systems. This paper describes a ready-to-use authentication biometric system based on EEG and ECG. This constitutes the first difference with already presented works [4, 5, 7, 8, 9, 14, 15, 16, 17, 18, 25]. The system presented herein undertakes subject authentication, whereas a biometric identification has been the target of those works. Moreover they present some results on the employment of EEG and ECG as a person identification cue, what herein becomes a stand-alone system.

A reduced number of electrodes have been already used in past works [4, 5, 7, 8, 9, 25] in order to reduce system obtrusiveness. This feature has been implemented in our system. There is however a differential trait. The two forehead electrodes are used in our system, while in other papers other electrodes configurations are used, e.g. [5] uses electrode P4. Our long-term goal is the integration of the biometric system with the ENOBIO wire-less sensory unit [23, 24, 32]. ENOBIO can use dry electrodes, avoiding the usage of conductive gel and therefore improving the user friendliness. In order to achieve this goal employing electrodes on hairless areas becomes mandatory, a condition our system fulfills.

In the following sections, our authentication methodology will be presented. Section 1.2 explains the experimental protocol which is common for EEG and ECG recording. Section 1.3 deals with the EEG extracted features and the authentication algorithms while section 1.4 is dedicated to the ECG features and algorithms. For these two sections, the performances are also individually given. Section 1.5 explains the fusion process carried out to achieve higher performance. Finally, conclusions are drawn in section 1.6 while section 1.7 provides a summary of the chapter.

1.2 EXPERIMENTAL PROTOCOL

A database of 40 healthy subjects (30 males and 10 females, aged from 21 to 62 years) has been collected in order to evaluate the performance of our system. An in-

formed consent along with a health questionnaire was signed and filled by all subjects.

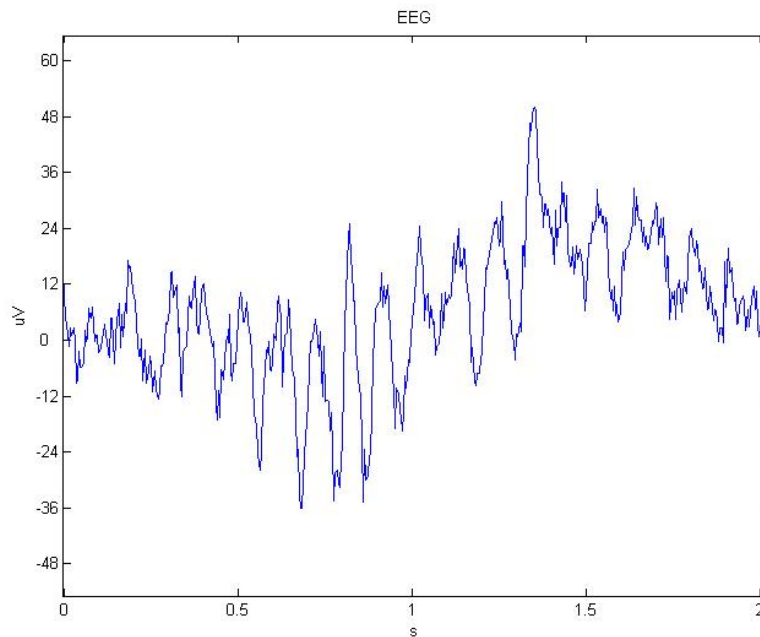
The EEG/ECG recording device is ENOBIO, a product developed at STARLAB BARCELONA SL. It is wireless and implements 4 channel (plus the common mode) device with active electrodes. It is therefore quite unobtrusive, fast and easy to place. Even though ENOBIO can work on dry mode, in this study conductive gel has been used. In Figure 1.1, we can see the ENOBIO sensor integrated in a cap worn by a subject.

Fig. 1.1 ENOBIO 4 lead sensor integrated in a cap. In this picture only 3 channels are connected (grey cables). We can also see the common mode cable connected to the left ear lobe of the subject (black and yellow cable). The ENOBIO sensor is valid for recording EEG and ECG, but it can also measure electrooculogram (EOG) and electromiogram (EMG).



In Figure 1.2, a sample of EEG recorded with ENOBIO is shown. An ECG sample data is also shown in Figure 1.3. Notice that the EEG amplitude is typically about 60 microvolts while ECG amplitude is typically about 1000 microvolts, therefore it is always more complicated to obtain a good EEG recording than an ECG, as the signal to noise ratio is easier to maximize with a stronger signal. No pre-processing has been done on these sample signals.

Fig. 1.2 ENOBIO EEG recording sample of 2 seconds with no pre-processing. The alpha wave (10 Hz characteristic EEG wave) can be seen.

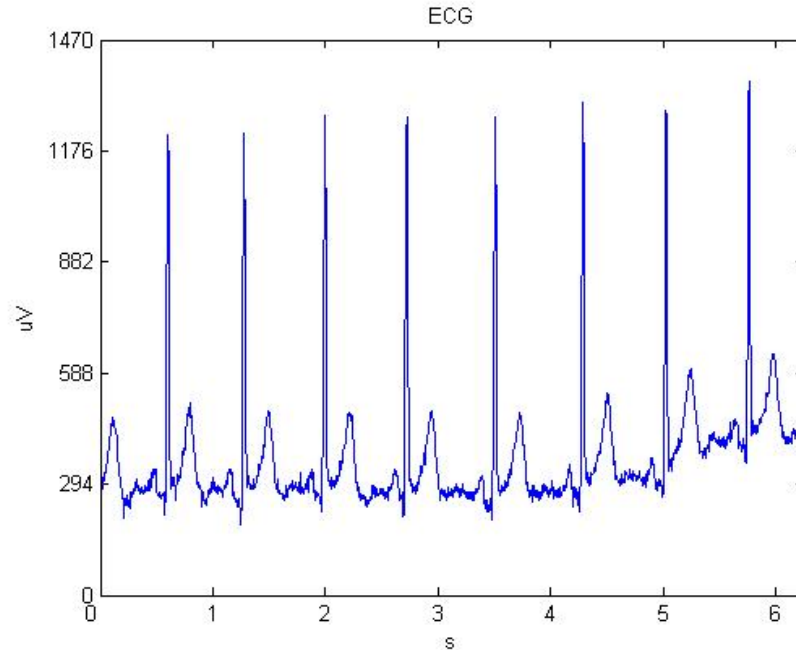


The electrode placement is as follows:

- two on the forehead (FP1 and FP2) for EEG recording
- one on the left wrist for ECG recording
- one on the right earlobe as reference
- one on the left earlobe as the hardware common mode

At this time, conductive gel is used, but in the future ENOBIO will work without gel, using carbon nanotube technology. Some tests have been done using this new electrodes with very positive results [23, 24], but at the moment some biocompatibility studies are being planned in order to approve their commercial use.

The recordings are carried out in a ca environment. The subjects are asked to sit in a comfortable armchair, to relax, be quiet and close their eyes. Then three 3-minute takes are recorded to 32 subjects and four 3-minutes takes are recorded to the 8 subjects, preferably on different days, or at least at different moments of the day. The 32 subject set are used as reference subject in the classification stage and the 8 subjects are the ones that are enrolled into the systems. Then several 1-minute

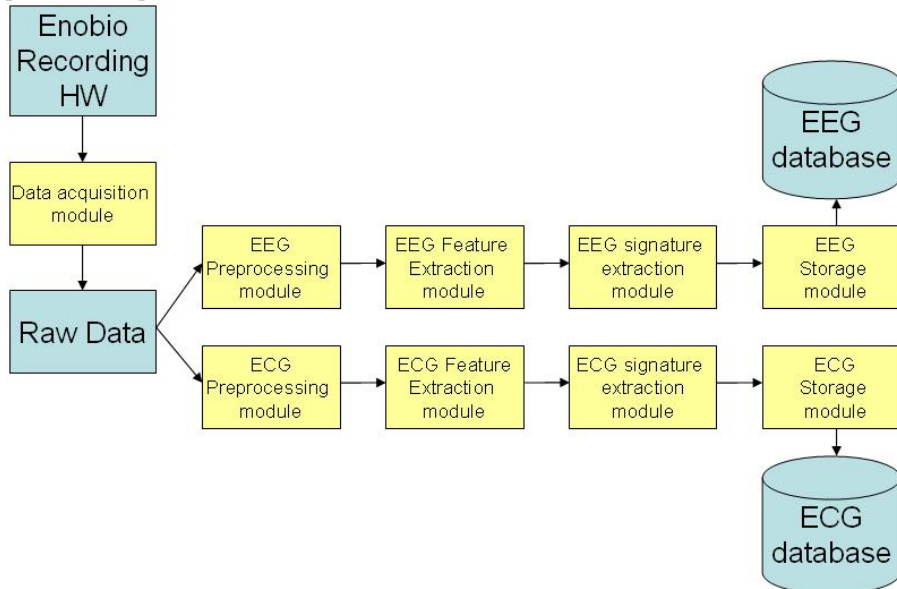
Fig. 1.3 ENOBIO ECG recording sample of approximately 6 seconds with no pre-processing.

takes are recorded afterwards to these enrolled subjects, in order to use them as authentication tests. Both the enrolment takes and the authentication takes are recorded under the same conditions.

1.3 AUTHENTICATION ALGORITHM BASED ON EEG

We begin this section with two flowcharts that describe the whole application, in order to clarify all the concepts involved. As with all the other biometric modalities, our system works in two steps: enrolment and authentication. This means that for our system to authenticate a subject, this subject needs first of all to enroll into the system. In other words, their biometric signature has to be extracted and stored in order to retrieve it during the authentication process. Then the sample extracted during the authentication process is compared with the one that was extracted during the enrolment. If they are similar enough, then they will be authenticated.

Fig. 1.4 The data acquisition module is the software that controls the ENOBIO sensor in order to capture the raw data. Remember that 4 channel are recorded: 2 EEG channels placed in the forehead, 1 ECG channel placed in the left wrist and 1 electrode placed in the right earlobe for referencing the data. At this point the data is separate in EEG data and ECG data and sent to two parallel but different biometric modules for EEG and ECG. Each pre-processing module is explained in detail in the respective pre-processing sections. Then the features are extracted. A detailed explanation of the features used in each module is found in the features sections. For the signature extraction module, four 3-minutes takes are needed. The signature extraction module is explained in detail in the enrolment subsection. Once the signatures are extracted, they are both stored in their respective database for further retrieval when an authentication process takes place.

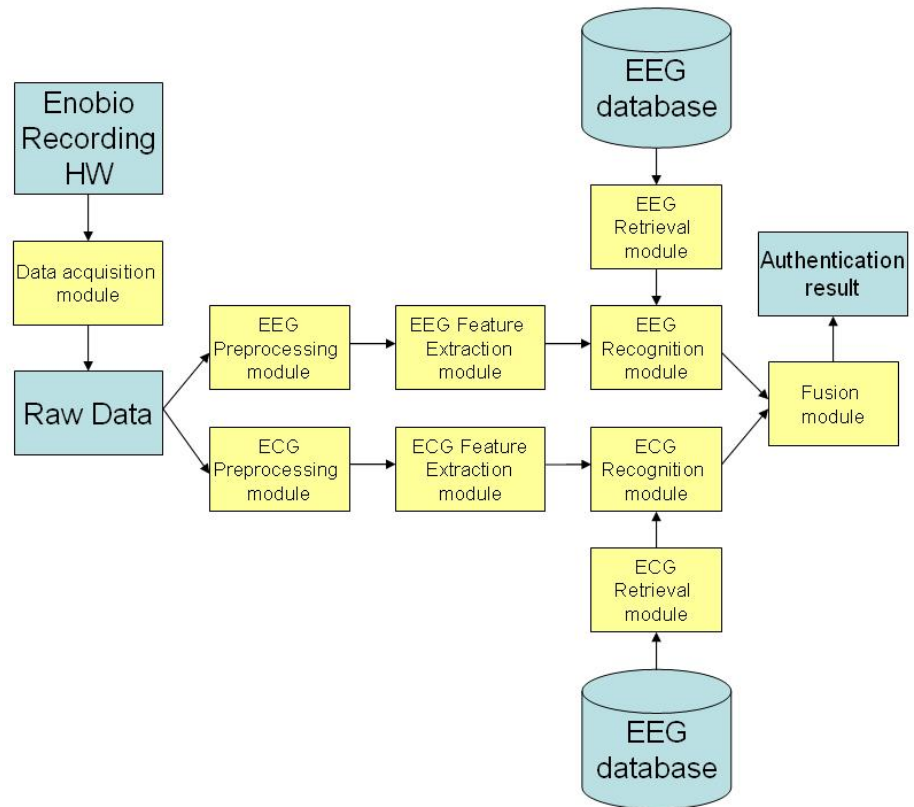


1.3.1 EEG pre-preprocessing

First of all, a pre-processing step is carried on the two EEG channels. They are both referenced to the right earlobe channel in order to cancel the common interference that can appear in all the channels. This is a common practice in EEG recordings. Since the earlobe is a position with no electrical activity, and it is very easy and unobtrusive to place an electrode there with the help of a clip, this site appeared the better one to reference the rest of electrodes. After referencing, a second order pass band filter with cut off frequencies 0.5 and 40 Hz is applied.

Once the filters are applied, the whole signal is segmented in 4 second epochs. Artefacts are kept, in order to ensure that only one minute of EEG data will be used for testing the system. We remind the reader that the subject is asked to close his/her

Fig. 1.5 The flowchart is identical to the enrolment one until the Feature Extraction Module. One difference that is not shown in the scheme is that now we only record 1 minute of data. The recognition module retrieves the claimed subjects EEG and ECG signature from their respective databases. At this point we have the probability that the 1-minute EEG recorded belongs to the claimed subject. We also have the probability that the 1-minute ECG recorded belongs to the claimed subject. The fusion module then takes care to fusion these probabilities to obtain a very confident decision.



eyes in order to minimize eye related artefacts.

1.3.2 Features extracted from EEG

We conducted an intensive preliminary analysis on the discrimination performance of a large initial set of features, e.g. Higuchi fractal dimension, entropy, skewness, kurtosis, mean and standard deviation. We chose the five ones that showed a higher discriminative power. These five different features were extracted from each 4-second epoch and input into our classifier module. All the mentioned features are

simultaneously computed in the biometry system presented herein. This is what we denote as the multi-feature set. The features are detailed in the following.

We can distinguish between two major types of features with respect to the number of EEG channels employed in their computation. Therefore we can group features in single channel features and two channels ones (the synchronicity features).

1.3.2.1 One channel features. Autoregression (AR) and Fourier transform (FT) are the implemented single channel features. They are calculated for each channel without taking into account the other channel. The usage of these features for EEG biometry is not novel [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]. However we describe them for the sake of completeness.

A Autoregression

We use the standard methodology of making an autoregression on the EEG signal and the resulting coefficients as features. The employed autoregression is based on the Yule-Walker method, which fits a p th order AR model to the windowed input signal, $X(t)$, by minimizing the forward prediction error in a least-square sense. The resulting Yule-Walker equations are solved through the Levinson-Durbin recursion. The AR model can be formulated as:

$$X(t) = \sum_{i=1}^n a(i)X(t-i) + e(t) \quad (1.1)$$

We take $n=100$ based on the discrimination power obtained in some preliminary works.

B Fourier transform

The well-known Discrete Fourier Transform (DFT), with expression

$$X(k) = \sum_{j=1}^N x(j)\omega_N^{(j-1)(k-1)} \quad (1.2)$$

$$x(j) = \frac{1}{N} \sum_{k=1}^N X(k)\omega_N^{-(j-1)(k-1)} \quad (1.3)$$

where

$$\omega_N = e^{\frac{-2\pi i}{N}} \quad (1.4)$$

1.3.2.2 Synchronicity features. Mutual information (MI), coherence (CO) and cross correlation (CC) are examples of two-channel features related to synchronicity [19, 20, 21]. They represent some joint characteristic of the two channels involved in the computation. This type of features is used for the first time here.

A Mutual information

The mutual information [12, 21] feature measures the dependency degree between two random variables given in bits, when logarithms of base 2 are used in its computation.

The MI can be defined as:

$$MI_{xy} = E(x) + E(y) - E(xy) \quad (1.5)$$

where E is the entropy operator: E(x) is the entropy of signal x and E(x,y) is the joint entropy of signals x and y.

B Coherence

The coherence measure quantizes the correlation between two time series at different frequencies [19, 20]. The magnitude of the squared coherence estimate is a frequency function with values ranging from 0 to 1.

The coherence $C_{xy}(f)$ is a function of the power spectral density (P_{xx} and P_{yy}) of x and y and the cross power spectral density (P_{xy}) of x and y, as defined in the following expression:

$$C_{xy}(f) = \frac{|P_{xy}(f)|^2}{P_{xx}(f)P_{yy}(f)} \quad (1.6)$$

In this case, the feature is represented by the set of points of the coherence function.

C Correlation measures

The well-known correlation (CC) is a measure of the similarity of two signals, commonly used to find occurrences of a known signal in an unknown one

with applications in pattern recognition and cryptanalysis [13]. We calculate the autocorrelation of both channels, and the cross-correlation between them following:

$$CC_{X,Y} = \frac{cov(X, Y)}{\sigma_X \sigma_Y} = \frac{E((X - \mu_X)(Y - \mu_Y))}{\sigma_X \sigma_Y} \quad (1.7)$$

where $E()$ is the expectation operator, $cov()$ the covariance one, and μ and σ , the corresponding mean and standard deviations values.

1.3.3 EEG Authentication Methodology

The work presented herein is based on the classical Fisher's Discriminant Analysis (DA). DA seeks a number of projection directions that are efficient for discrimination, i.e., separation in classes.

It is an exploratory method of data evaluation performed as a two-stage process. First the total variance/covariance matrix for all variables, and the intra-class variance/covariance matrix are taken into account in the procedure. A projection matrix is computed that minimizes the variance within classes while maximizing the variance between these classes. Formally, we seek to maximize the following expression:

$$J(W) = \frac{W^t S_B W}{W^t S_W W} \quad (1.8)$$

Where:

- W is the projection matrix
- S_B is between-classes scatter matrix
- S_W is within-class scatter matrix

For an n -class problem, the DA involves $n-1$ discriminant functions (DFs). Thus a projection from a d -dimensional space, where d is the length of the feature vector to be classified, into a $(n-1)$ -dimensional space, where $d \geq n$, is achieved. Note that in our particular case, the subject and class are equivalent. In our algorithm we work with 4 different DFs:

- linear: Fits a multivariate normal density to each group, with a pooled estimate of the covariance.
- diagonal linear: Same as 'linear', except that the covariance matrices are assumed to be diagonal.
- quadratic: Fits a multivariate normal density with covariance estimates stratified by group.

- diagonal quadratic: Same as ‘quadratic’, except that the covariance matrices are assumed to be diagonal.

The interested reader can find more information about DA in [13].

Taking into account the 4 DF’s, the 2 channels, the 2 single channel features and 3 synchronicity features, we have a total of 28 different classifiers. Here, we mean by classifier each of the 28 possible combinations of feature, DF and channel. All these combinations are shown in the next table:

We use an approach that we denote as ‘personal classifier’, which is explained herein, for the identity authentication case: the 5 best classifiers, i.e., the ones with more discriminative power, are used for each subject. When a test subject claims to be, for example, subject 1, the 5 best classifiers for subject 1 are used to do the classification. The methodology applied to do so is explained in the next section.

ENROLMENT PROCESS:

In order to select the 5 best classifiers for the N enrolled subjects with 4 EEG takes, we proceed as follows. We use the 3 first takes of the N subjects for training each classifier and the 4th take of a given subject is used for testing it. We repeat this process making all possible combinations (using one take for testing and the others for training). Each time we do this process, we obtain a classification rate (CR): number of feature vectors correctly classified over the total number of feature vectors. The total number of feature vectors is around 45, depending on the duration of the take (we remind the reader that the enrolment takes have a duration of approximately 3 minutes, and these takes are segmented in 4-second epochs). Once this process is repeated for all 28 classifiers, we compute a score measure on them, which can be defined as:

$$score = \frac{average(CR)}{standard\ deviation(CR)} \quad (1.9)$$

The 5 classifiers with higher scores out of the 28 possible classifiers are the selected ones. We repeat this process for the N enrolled subjects.

AUTHENTICATION PROCESS

Once we have the 5 best classifiers for all the N enrolled subjects, we can then implement and test our final application. We now proceed in a similar way, but we only use one minute of recording data, i.e., we input in each one of the 5 best classifiers 15 feature vectors (we remind the reader that the authentication test takes have a duration of 1 minute, and these takes, as we did in the enrolment case, are segmented in

Table 1.1 List of possible classifiers used in our system. Note that the MI, CO and CC features are extracted from both channels so the field channel is omitted in these cases

Classifier ID	Feature*	channel	discriminant Function
1	AR	1	linear
2	AR	1	diagonal linear
3	AR	1	quadratic
4	AR	1	diagonal quadratic
5	AR	2	linear
6	AR	2	diagonal linear
7	AR	2	quadratic
8	AR	2	diagonal quadratic
9	FT	1	linear
10	FT	1	diagonal linear
11	FT	1	quadratic
12	FT	1	diagonal quadratic
13	FT	2	linear
14	FT	2	diagonal linear
15	FT	2	quadratic
16	FT	2	diagonal quadratic
17	MI	-	linear
18	MI	-	diagonal linear
19	MI	-	quadratic
20	MI	-	diagonal quadratic
21	CO	-	linear
22	CO	-	diagonal linear
23	CO	-	quadratic
24	CO	-	diagonal quadratic
25	CC	-	linear
26	CC	-	diagonal linear
27	CC	-	quadratic
28	CC	-	diagonal quadratic

*AR = Autoregression
 FT = Fourier Transform
 MI = Mutual Information
 CO = Coherence
 CC = Cross Correlation

4-second epochs). Each classifier outputs a posterior matrix (Table 1.2). In order to fuse the results of the 5 classifiers, we vertically concatenate the 5 obtained posterior matrices and take the column average. The resulting vector is the one we will use to take the authentication decision. In fact, it is a Probability Density Function (PDF). See Figure 1.6 and 1.7):

- The 1st element is the probability that the single minute test data comes from subject 1.
- The 2nd element is the probability that the single minute test data comes from subject 2
- etc...

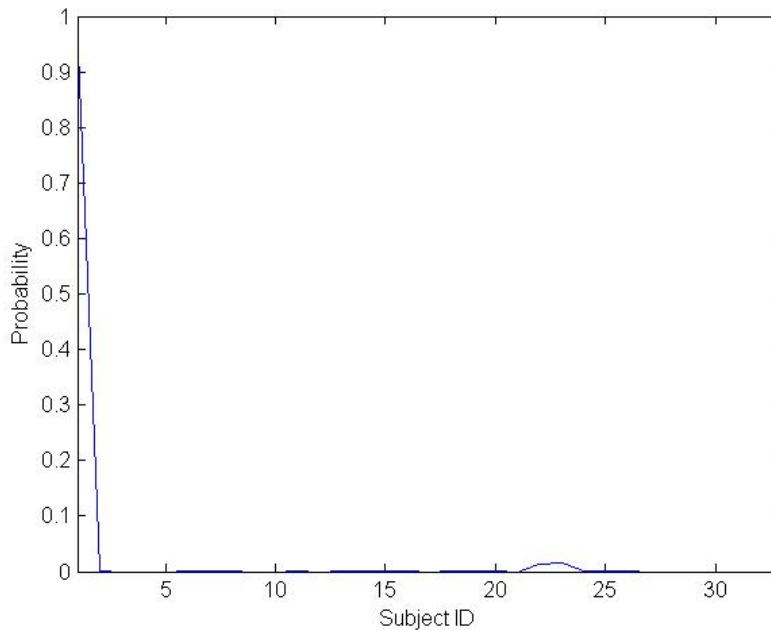
Table 1.2 Posterior matrix of the 15 FT feature vectors extracted from one minute EEG recording of subject 1. Each row represents the probabilities assigned to each class for each feature vector. We see that the subject is well classified as being subject 1 (refer to the last row). Notice that, for simplicity, this posterior matrix represents a 5-class problem (i.e., 4 reference subjects in this case). In our real system, we work with a 33-class problem.

Classified as	Subject 1	Subject 2	Subject 3	Subject 4	Subject 5
Test 1	0.46	0.28	0	0	0.23
Test 2	0.40	0.24	0	0.23	0.11
Test 3	0.99	0	0	0	0.01
Test 4	0.99	0	0	0	0
Test 5	0.99	0	0	0	0
Test 6	0.91	0.01	0.04	0	0.04
Test 7	0.99	0	0	0	0
Test 8	0.99	0.01	0	0	0
Test 9	0.96	0.02	0.02	0	0
Test 10	0.99	0	0	0	0
Test 11	0.16	0.04	0.25	0.53	0
Test 12	0.53	0.35	0	0	0.11
Test 13	0.92	0.07	0	0	0.01
Test 14	0.99	0	0	0	0
Test 15	1	0	0	0	0
average	0.81	0.07	0.02	0.05	0.03

The last step in our algorithm takes into consideration a decision rule over the averaged PDF. We use a threshold applied on the probability of the claimed subject. If the probability of the claimed subject is higher than the applied threshold, then the authentication result is positive. Three values are output by our algorithm:

- binary decision (authentication result)
- score (probability of the claimed subject)
- confidence level (an empiric function that maps the difference between threshold and score to a percentage)

Fig. 1.6 PDF for one of the enrolled subjects. The subject is classified against his training data set (class 1) and the training data sets of the reference subjects (from class 2 to class 33). In this example, he/she will be correctly authenticated with a high confidence level

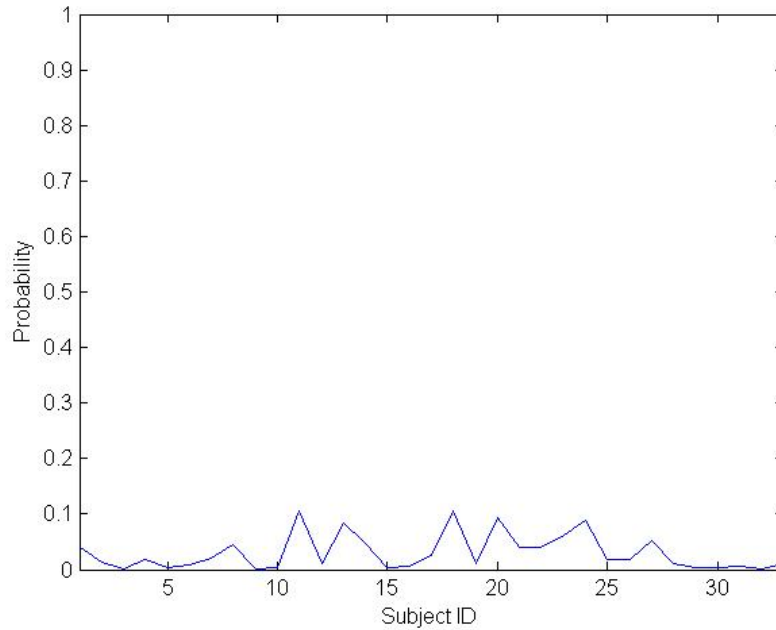


In order to evaluate the performance of the system, we proceed as follows. 32 subjects with three 3-minutes takes are used as reference subjects and the other 8 subjects with four 3-minute takes are enrolled in the system as explained in the ‘enrolment process’ above. For the system testing, we distinguish three cases: when a subject claims to be himself (legal situation) and when a subject claims to be another subject from the database (impostor situation). We have 48 legal situations, 350 impostor situations and 16 intruder situations. What we do, in order to take all the profit from our data, is to make all the possible combinations with the authentication takes. Subject 1 will claim to be subject 1 (legal situation), but he will also claim to be all the other enrolled subjects (impostor situation). An intruder will claim to be all the 8 enrolled subject, one by one. The False Acceptance Rate (FAR) is computed taking into account both the intruder and the impostor cases. The True Acceptance Rate (TAR) only takes into account the legal cases.

The performance of the EEG system using a probability threshold of 0.1 is:

- TAR=79,2%

Fig. 1.7 PDF for an impostor situation. In this case the probabilities are more or less evenly distributed among all classes: the one he claims to be (class 1) and the other reference subject classes (from class 2 to class 33), so in this case he/she will not be authenticated with a high confidence level



- FAR=21,8%

This threshold places our system close to the Equal Error Rate (EER) working point. By definition, at the EER working point the following equation is valid:

$$TAR + FAR = 100\% \quad (1.10)$$

and the compromise between the highest TAR and the lowest FAR is optimal.

1.4 AUTHENTICATION ALGORITHM BASED ON ECG

1.4.1 ECG pre-preprocessing

We reference the ECG channel placed in the left wrist to the right earlobe reference channel. A first difference with the EEG pre-processing is that, in this case, we are

not using 4-seconds epochs. Now, we segment each single heart beat waveform from the ECG signal.

1.4.2 Heart beat waveform as unique feature from ECG

From a large set of different features (Heart Rate Variability related features, geometric features, entropy, fractal dimension and energy), we finally only use the heart beat waveform as input feature in our classifiers, since it is the one that showed the higher discriminative power between subjects.

As previously said, from each minute of data we extract each single heart waveform. For defining the heart beat waveform feature, we decimate to a 144 length vectors. All these vectors in their totality are the heart beat waveform features. Thus, the total number of feature vectors, in this case, depends on the number of heart beat in one minute, i.e., on the heart beat rate.

1.4.3 ECG Authentication Methodology

The authentication methodology is very similar to the one used in EEG. The difference is that now we only have one feature, but we still have 4 DF's, so at the 'best classifier selection' stage, what we do is to select the best DF for each subject. In this modality there is no data fusion. Once the best DF is found, then the classification is made for the 'heart beat shape' feature and for the selected DF.

The outputs for this modality are the same:

- binary decision (authentication result)
- score (probability of the claimed subject)
- confidence level (an empiric function that maps the difference between threshold and score to a percentage)

The performance of the ECG system using a probability threshold of 0.6:

- TPR=97.9%
- FPR=2.1%

This threshold places the performance of our system on the EER working point, as explained in the EEG Authentication Methodology section.

1.5 EEG AND ECG FUSION

At this stage, we have the elements that could lead the system to take a decision based on each of the two modalities. However we have observed that the application of a

decision fusion increases the reliability of the final system in terms of acceptance and rejection rates. In order to achieve the maximum performance of the system, we fuse therefore the results of the EEG and the ECG authentication systems. As both signals are independent and the recording protocols, completely compatible with each other, it is very easy to register both EEG and ECG at the same time with the ENOBIO sensor.

Figure 1.8 shows the bidimensional decision space where the scores probabilities for ECG and EEG are plotted one against the other. As it can be observed the inclusion of both modalities together with their fusion makes the two classes linearly separable. Indeed we can undertake the separation through a surface formally expressed as:

$$\phi_1 = mE + c - C \quad (1.11)$$

where E and C state for the scores probabilities of the claimed subjects respectively for the EEG and ECG modalities, m and c, for the parameters of the lineal decision boundary, and ϕ_1 for this decision boundary. Values over d will be considered as legal subjects, whereas those under d, are classified as impostors as shown in Figure 1.8, where the decision boundary labeled as 1 has been adapted to the test on hand. Such a linear decision surface is easy to optimize, because it lives in a low parametrical space.

One more decision surface ϕ_2 is depicted in Figure 1.8. The relationship between adaptation and generalization capability of a classifier system is very well-known. Therefore ϕ_2 is much more adapted to the test data set used in the simulation presented herein. We expect such a decision boundary to present less generalization capability when new subjects enter into the system. However the performance of ϕ_1 is good enough for a practicable biometric system and furthermore, easier to parameterize.

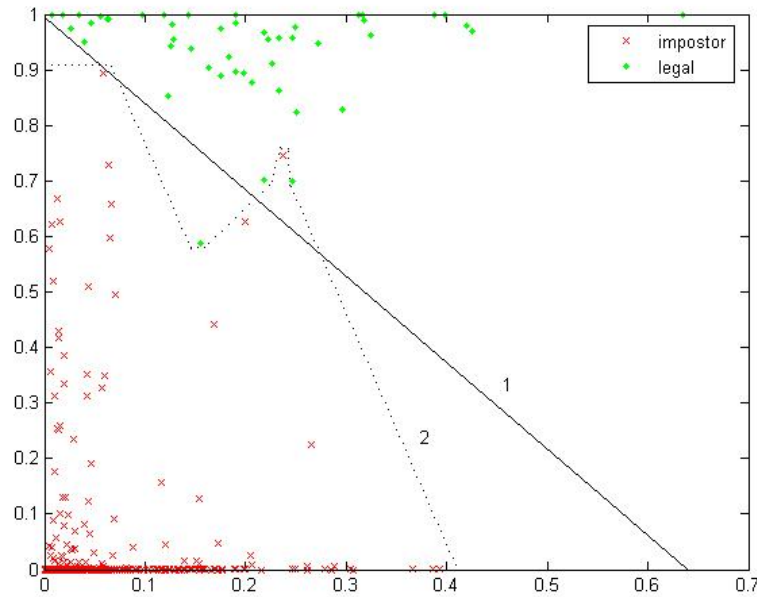
From an application point of view, the decision surface 1 will be useful for a application where security issues are not critical (e.g. access to Disneyland, where we are interested that everybody is authenticated even though some intruders get also access to the facilities), while the surface 2 would be used in an application where the security issues are extremely important (e.g. access to radioactive combustible in a nuclear plant, where we really do not want any intruder to get access, even though some legal subject are not allowed to get access).

The results in terms of TPR and FPR are shown in Table 2.

Table 1.3 Final results after fusion

	TPR	FPR
decision function 1	97.9%	0.82
decision function 2	100	0

Fig. 1.8 Bidimensional decision space. Ordinates represent the ECG probabilities and the abscises the EEG probabilities. Red crosses represent impostor cases and green crosses represents legal cases. Two decision functions are represented



1.6 CONCLUSION

We have presented the performance results obtained by a bi-modal biometric system based on physiological signals, namely EEG and ECG. The results demonstrate the validity of the multi-stage fusion approach taken into account in the system. In this context we undertake fusion at the feature, classification and the decision stages improving this way the overall performance of the system in terms of acceptance and rejection rates.

Moreover, the system presented herein improves the unobtrusiveness of other biometric systems based on physiological signals due to the employment of a wireless acquisition unit (ENOBIO). Moreover two channels were used for the EEG modality and one channel for ECG.

It is worth mentioning the implementation of novel EEG features. The inclusion of synchronicity features, which take into account the data of two different channels, complement quite well the usage of one channel features, which have been traditionally used in biometric systems. On the other hand those two channel features are

used for the first time in such a system. The features undergo a LDA classification with different discriminant functions. Therefore we take into consideration a set of feature-classifiers combinations. This fact improves the robustness of the system and even its performance.

After testing the performance of different ECG features we conclude that the most discriminative one is the heart beat waveform as a whole. For its extraction it is necessary to implement a pre-processing stage. The unique feature undergoes a classification stage similar to the one used with the modality described above. Therefore different discriminant functions of a LDA classifier present different performance for each of the subjects. The inclusion of their combination results in an improvement in the performance of the overall system.

We have demonstrated as well the suitability of including a decision fusion stage, whereby the decision between legal and impostor subjects becomes linear. Moreover the decision fusion allows to decrease the FPR of the system, which constitutes an important feature of a reliable system. Although the corresponding decision boundary was computed on hand of test results, its parameterization is easily attainable. Optimization procedures can be applied to fulfill this aim.

We also wish to mention other possible future applications of our system. Using the ENOBIO sensor, which is unobtrusive and wearable, and through the analysis of EEG and ECG signal, we can not only authenticate the subjects. There are evidences that both EEG and ECG signals can be used to validate the initial state of the subject, that is to detect if the subject is in normal condition and has not taken alcohol, drugs or not suffering from sleep deprivation [26, 27, 28]. Moreover, a continuous authentication system and a continuous monitoring system could also be implemented since the sensor, as already explained, is unobtrusive and wearable.

A further step is to extract emotions from ECG and EEG [29, 30]. This would be very useful for human-computer interactions. As an example, we can think on virtual reality applications where the reactions of the computer generated avatars would take into account the emotions of the subject immersed in the virtual reality environment [32].

1.7 SUMMARY

Features extracted from electroencephalogram (EEG) and electrocardiogram (ECG) recordings have proved to be unique enough between subjects for biometric applications. We show here that biometry based on these recordings offers a novel way to robustly authenticate subjects. In this paper, we presented a rapid and unobtrusive authentication method that only uses 2 frontal electrodes (for EEG recording) and another electrode placed on the left wrist referenced to another one placed at the right earlobe. Moreover the system makes use of a multi-stage fusion architecture,

which demonstrates to improve the system performance. The performance analysis of the system presented in this paper stems from an experiment with 40 subjects, from which 8 are used as enrolled test subjects and 32 are used as reference subjects needed for both, the enrolment and the authentication process.

Acknowledgments

The authors wish to thank STARLAB BARCELONA S.L. for supporting this research and for providing the ENOBIO sensor. STARLAB BARCELONA S.L. is research private company with the goal of transforming science into technologies with a profound and positive impact on society.

The authors also wish to thank the HUMABIO project (Contract number 026990) who funded part of the research explained in this chapter. HUMABIO is a EC co-funded "Specific Targeted Research Project" (STREP) where new types of biometrics are combined with state of the art sensorial technologies in order to enhance security in a wide spectrum of applications like transportation safety and continuous authentication in safety critical environments like laboratories, airports and/or other buildings.

REFERENCES

1. Eischen S., Lucritz J. and Polish J. (1995) Spectral analysis of EEG from Families. *Biological Psychology*, Vol. 41, pp. 61-68.
2. Hazarika N., Tsoi A. and Sergejew A. (1997) Nonlinear considerations in EEG signal Classification. *IEEE Transactions on signal Processing*, Vol. 45, pp. 829-836.
3. Marcel S., Mill J. (2005) Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IDIAP Research Report 05-81*, 11 pp.
4. Mohammadi G. et al. (2006) Person identification by using AR model for EEG signals. *Proc. 9th International Conference on Bioengineering Technology (ICBT 2006)*, Czech Republic, 5 pp.
5. Paranjape R. et al. (2001) The electroencephalogram as a biometric. *Proc. Canadian Conf. on Electrical and Computer Engineering*, pp. 1363-1366.
6. Poulos M. et al. (1998) Person identification via the EEG using computational geometry algorithms. *Proceedings of the Ninth European Signal Processing, EUSIPCO'98*, Rhodes, Greece. September 1998, pp. 2125-2128.
7. Poulos M. et al. (1999) Parametric person identification from EEG using computational geometry. *Proc. 6th International Conference on Electronics, Circuits and Systems (ICECS '99)*, v. 2, pp. 1005-1008.

8. Poulos M. et al. (2001) On the use of EEG features towards person identification via neural networks. *Medical Informatics & the Internet in Medicine*, v. 26, pp. 35-48.
9. Poulos M. et al. (2002) Person identification from the EEG using nonlinear signal classification. *Methods of Information in Medicine*, v. 41, pp. 64-75.
10. Remond A., Ed. (1997) *EEG Informatics. A didactic review of methods and applications of EEG data processing*, Elsevier Scientific Publishing Inc., New York, 1997.
11. Sviserskaya N., Korolkova T. (1995) Genetic Features of the spatial organization of the human cerebral cortex. *Neuroscience and Behavioural Physiology*, Vol. 25, N. 5, pp. 370-376.
12. Deriche M., Al-Ani A. (2001) A new algorithm for EEG feature selection using mutual information. *Acoustics, Speech, and Signal Processing, 2001. Proceedings. '01*, pp. 1057 - 1060 vol.2
13. Duda R. et al., *Pattern Classification*, Wiley, New York, 2001.
14. Biel L. et al. (2001) ECG analysis: a new approach in human identification. *IEEE Transactions on Instrumentation and Measurement*, Vol. 50, N. 3, pp. 808-812.
15. Chang C.K. (2005) Human identification using one lead ECG. Master Thesis. Department of Computer Science and Information Engineering. Chaoyang University of Technology (Taiwan).
16. Israel S. et al. (2005) EGC to identify individuals. *Pattern Recognition*, 38, pp. 133-142.
17. Kyoso M. (2001) Development of an ECG Identification System. Proc. 23rd Annual International IEEE Conference on Engineering in Medicine and Biology Society, Istanbul, Turkey.
18. Palaniappan R. and Krishnan S.M. (2004) Identifying individuals using ECG beats. *Proceedings International Conference on Signal Processing and Communications, 2004. SPCOM '04*, pp. 569-572.
19. Winterer G. et al. (2003) Association of EEG coherence and an exonic GABA(B)R1 gene polymorphism. *Am J Med Genet B Neuropsychiatr Genet*, 117:51-56.
20. Kikuchi M. et al. (2000) Effect of normal aging upon interhemispheric EEG coherence: analysis during rest and photic stimulation. *Clin Electroencephalogr*, 31: 170-174.
21. Moddemeijer R. (1989) On estimation of entropy and mutual information of continuous distributions. *Signal Processing* vol.16 nr.3 pp.233-246

22. Ross A, Jain A. (2003) Information fusion in biometrics. *Pattern Recognition Letters* 24 pp.2115-2125
23. G. Ruffini et al. (2006) A dry electrophysiology electrode using CNT arrays. *Sensors and Actuators A* 132 34-41
24. G. Ruffini et al. (2007) ENOBIO dry electrophysiology electrode; first human trial plus wireless electrode system. 29th IEEE EMBS Annual International Conference.
25. A. Riera et al. (2007) Unobtrusive Biometric System Based on Electroencephalogram Analysis. Accepted at *EURASIP Journal on Advances in Signal Processing*.
26. Hogans et al. (1961) Effects of ethyl alcohol on EEG and avoidance behavior of chronic electrode monkeys. *Am J Physio*, 201: 434-436
27. J. Sorbel et al. (1996) Alcohol Effects on the Heritability of EEG Spectral Power alcoholism: clinical and experimental research
28. S. Jin et al (2004) Effects of total sleep-deprivation on waking human EEG: functional cluster analysis. *Clinical Neurophysiology*, Volume 115, Issue 12, Pages 2825-2833
29. Kazuhiko Takahashi (2004) Remarks on Emotion Recognition from Bio-Potential Signals . 2nd International Conference on Autonomous Robots and Agents.
30. A. Haag et al. (2004) Emotion Recognition Using Bio-sensors: First Steps towards an Automatic System. Springer-Verlag Berlin Heidelberg, ADS, LNAI 3068, pp. 36-48.
31. J. Llobera (2007) Narratives within Immersive Technologies. arXiv:0704.2542.
32. G. Ruffini et al. (2006) First human trials of a dry electrophysiology sensor using a carbon nanotube array interface. arXiv:physics/0701159
33. V. Gracia et al. (2006) State of the Art in Biometrics Research and Market Survey. HUMABIO Project (EU FP6 contract no 026990). Deliverable N.1.4. www.humabio-eu.org