Chapter 18

Multimodal Physiological Biometrics Authentication

Alessandro Riera, Aureli Soria-Frisch, Mario Caparrini, Ivan Cester, and Giulio Ruffini

18.1 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 nontechnological 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 twentieth century to measure and evaluate physical or behavioral characteristics of living organisms automatically has given the word a second meaning. In the present study, the term biometrics refers to the following definition [1]:

Biometry, however, has also acquired another meaning in recent decades, focused on the characteristic to be measured rather than the technique or methodology used [1]:

> *The term biometry refers to automated methods and techniques that analyze human characteristics in order to recognize a person, or distinguish this person from another, based on a physiological or behavioral characteristic.*
>
> *A biometric is a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity.*

Biometrics: Theory, Methods, and Applications. Edited by Boulgouris, Plataniotis, and Micheli-Tzanakou

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 behavioral pattern used to recognize 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 behavioral. Physiological characteristics refer to what the person is; that is, 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, and so on. Behavioral characteristics are related to what a person does, or how the person uses the body. Voice recognition, 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 recognize someone who is completely unknown to them. A computer system can be designed and trained to recognize 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 recognizes 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 about the qualities of a person or group which make them different from others—that

> is, 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 recognized 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 in identification mode:

- **Authentication** (Greek: $\alpha\upsilon\theta\epsilon\nu\tau\iota\kappa\o\varsigma$, from "authentes" = "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 recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, and so on, 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, with that person being aware or not of this recognition task being performed. In the identification mode, the system recognizes 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 chapter we will describe a system that works on authentication mode, although it is quite straightforward to modify it to work on identification mode [2].

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, palm 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 universality. Typical biometric traits, such as fingerprint, voice, and retina, are not universal and can be subject to physical damage (dry skin, scars, loss of voice, etc.). 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, presenting a 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 [3].

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. Because these characteristics are very subject-dependent, a high inter-subject variability is also expected. This has been shown in previous works [4–8].

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: Within 1 min the subject should be relaxed and have 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 multistage fusion architecture has been presented in reference 9 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 [2, 4–8, 10–14]. 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, which herein becomes a stand-alone system.

A reduced number of electrodes have been already used in past works [2, 10–14] 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; for example, reference 11 uses electrode P4. Our long-term goal is the integration of the biometric system with the ENOBIO wireless sensory unit [15–17]. 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 18.2 explains the experimental protocol that is common for EEG and ECG recording. Section 18.3 deals with the EEG-extracted features and the authentication algorithms, while Section 18.4 is dedicated to the ECG features and algorithms. For these two sections, the performances are also individually given. Section 18.5 explains the fusion process carried out to achieve higher performance. Finally, conclusions are drawn in Section 18.6, while Section 18.7 provides a summary of the chapter.

18.2 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 informed 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 a four-channel (plus the common mode) device with active electrodes. It is therefore quite unobtrusive, fast, and easy to place. Even thought ENOBIO can work on dry mode, in this study conductive gel has been used. In Figure 18.1, we can see the ENOBIO sensor integrated in a cap worn by a subject.

In Figure 18.2, a sample of EEG recorded with ENOBIO is shown. An ECG sample data is also shown in Figure 18.3. Notice that the EEG amplitude is typically about 60 μV, while ECG amplitude is typically about 1000 μV; therefore it is always more complicated to obtain a good EEG recording than to obtain a good ECG, because the signal-to-noise ratio is easier to maximize with a stronger signal. No preprocessing has been done on these sample signals.

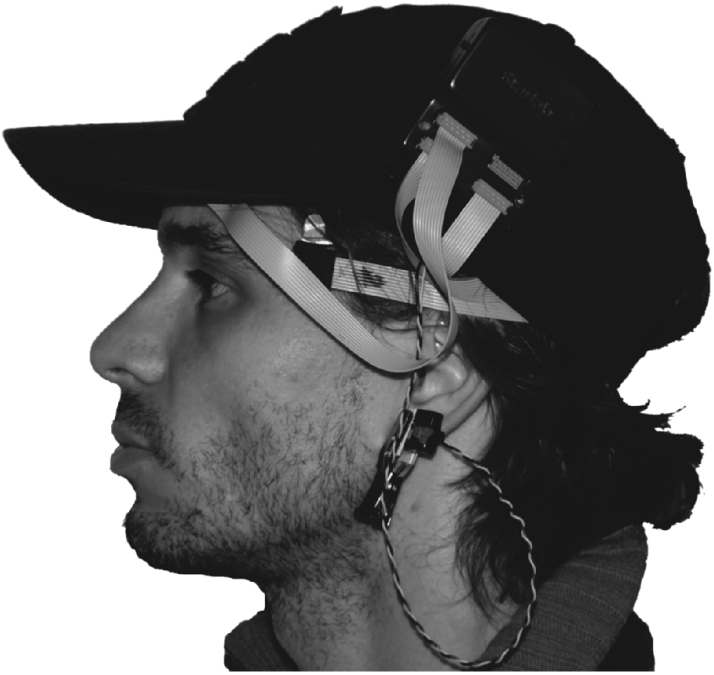

Figure 18.1. ENOBIO four-lead sensor integrated in a cap. In this picture, only three channels are connected (gray cables). We can also see the common mode cable connected to the left earlobe of the subject (black and yellow cable). The ENOBIO sensor is valid for recording EEG and ECG, but it can also measure electrooculogram (EOG) and electromyogram (EMG).

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 [15,16], but at the moment some biocompatibility studies are being planned in order to approve their commercial use.

The recordings are carried out in a calm environment. The subjects are asked to sit in a comfortable armchair, relax, be quiet, and close their eyes. Then three 3-min takes are recorded for 32 subjects and four 3-min takes are recorded for 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-min takes are recorded afterwards for these enrolled subjects, in order to use them as authentication tests. Both the enrollment takes and the authentication takes are recorded under the same conditions.

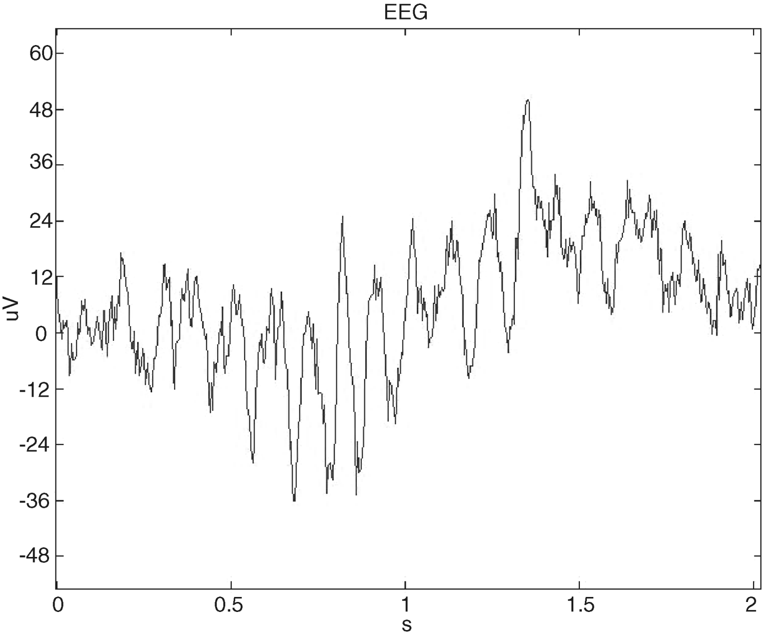

Figure 18.2. ENOBIO EEG recording sample of 2 s with no preprocessing. The alpha wave (10-Hz characteristic EEG wave) can be seen.

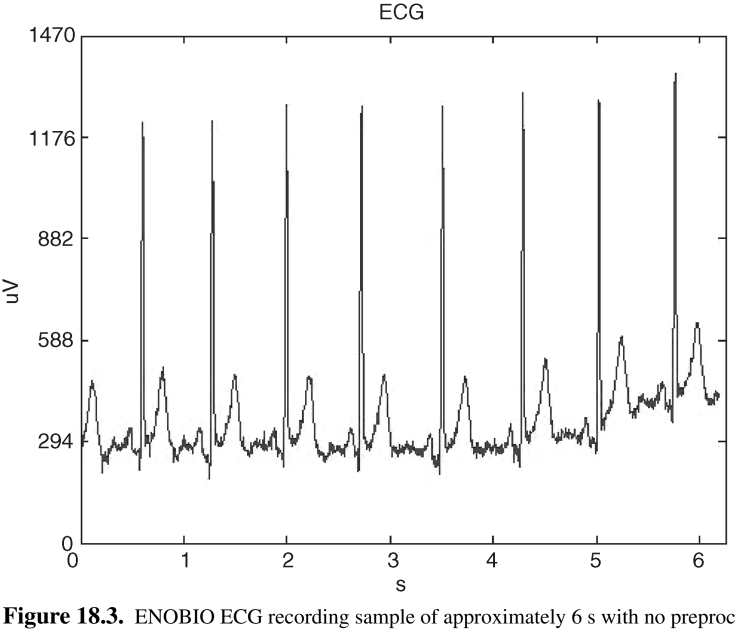

Figure 18.3. ENOBIO ECG recording sample of approximately 6 s with no preprocessing.

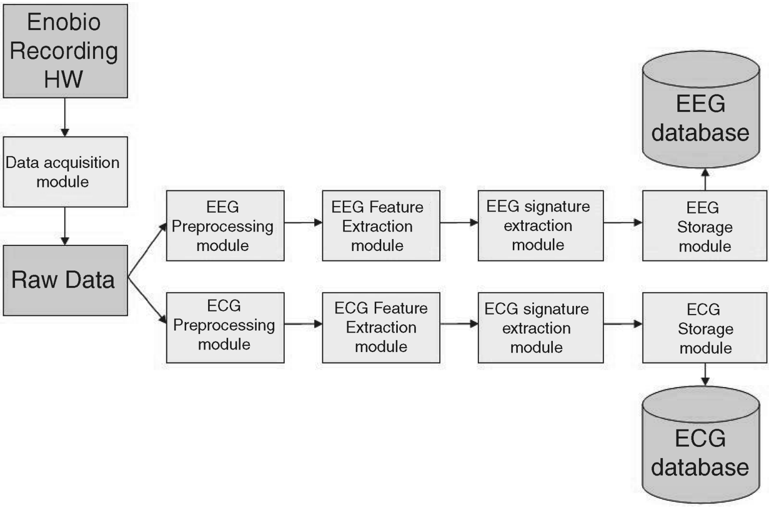

Figure 18.4. The data acquisition module is the software that controls the ENOBIO sensor in order to capture the raw data. Remember that four channels are recorded: two EEG channels placed in the forehead, one ECG channel placed in the left wrist and one electrode placed in the right earlobe for referencing the data. At this point the data are separate in EEG data and ECG data and sent to two parallel but different biometric modules for EEG and ECG. Each preprocessing module is explained in detail in the respective preprocessing 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-min takes are needed. The signature extraction module is explained in detail in the enrollment subsection. Once the signatures are extracted, they are both stored in their respective database for further retrieval when an authentication process takes place.

18.3 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 (Figures 18.4 and 18.5). As with all the other biometric modalities, our system works in two steps: enrollment 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.

18.3.1 EEG Preprocessing

First of all, a preprocessing 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

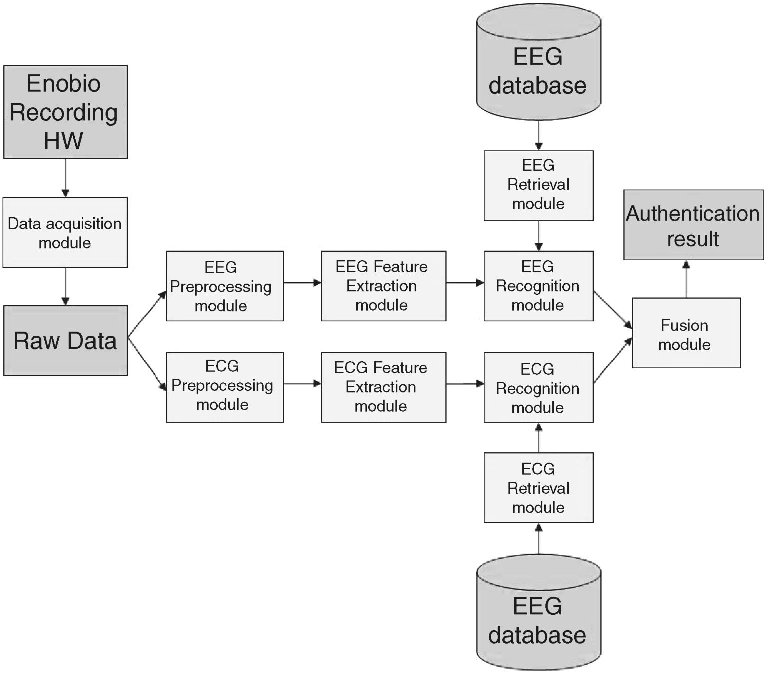

Figure 18.5. The flowchart is identical to the enrollment one until the feature extraction module. One difference that is not shown in the scheme is that now we only record 1 min of data. The recognition module retrieves the claimed subjects EEG and ECG signature from their respective databases. At this point we have the probability that the 1-min EEG recorded belongs to the claimed subject. We also have the probability that the 1-min ECG recorded belongs to the claimed subject. The fusion module then takes care to fusion these probabilities to obtain a very confident decision.

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 cutoff frequencies 0.5 and 40 Hz is applied.

Once the filters are applied, the whole signal is segmented in 4-s epochs. Artifacts are kept, in order to ensure that only 1 min of EEG data will be used for testing the system. We remind the reader that the subject is asked to close his/her eyes in order to minimize eye-related artifacts.

18.3.2 Features Extracted from EEG

We conducted an intensive preliminary analysis on the discrimination performance of a large initial set of features—for example, 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-s 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 multifeature 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).

18.3.2.1 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 [8,10–14,19–22]. However, we describe them for the sake of completeness.

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 pth-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

$$X(t) = \sum_{i=1}^{n} a(i)X(t-i) + e(t). \tag{18.1}$$

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

Fourier Transform. The well-known discrete Fourier transform (DFT) is expressed as

$$X(k) = \sum_{j=1}^{N} x(j)\omega_N^{(j-1)(k-1)}, \tag{18.2}$$

$$x(j) = \frac{1}{N}\sum_{k=1}^{N} X(k)\omega_N^{-(j-1)(k-1)}, \tag{18.3}$$

where

$$\omega_N = e^{\frac{-2\pi i}{N}}. \tag{18.4}$$

18.3.2.2 Synchronicity Features

Mutual information (MI), coherence (CO), and cross-correlation (CC) are examples of two-channel features related to synchronicity [23–25]. They represent some join characteristic of the two channels involved in the computation. This type of features is used for the first time here.

Mutual Information. The mutual information [12,25] 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

$$MI_{xy} = E(x) + E(y) - E(xy), \tag{18.5}$$

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.

Coherence. The coherence measure quantizes the correlation between two time series at different frequencies [23,24]. 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:

$$C_{xy}(f) = \frac{|P_{xy}(f)|^2}{P_{xx}(f)P_{yy}(f)}. \tag{18.6}$$

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

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 [27]. We calculate the autocorrelation of both channels, and the cross-correlation between them following:

$$CC_{X,Y} = \frac{\operatorname{cov}(X, Y)}{\sigma_X \sigma_Y} = \frac{E((X - \mu_X)(Y - \mu_Y))}{\sigma_X \sigma_Y}, \tag{18.7}$$

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

18.3.3 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—that is, separation in classes.

DA is an exploratory method of data evaluation performed as a two-stage process. First the total variance/covariance matrix for all variables and then 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:

$$J(W) = \frac{W^t S_B W}{W^t S_W W}, \tag{18.8}$$

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 four 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 reference 27.

Taking into account the four DFs, the two channels, the two single-channel features, and the three 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 Table 18.1.

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

Enrollment Process. In order to select the five best classifiers for the N enrolled subjects with four EEG takes, we proceed as follows. We use the three first takes of the N subjects for training each classifier and the fourth 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 enrollment takes have a duration of approximately 3 min, and these takes are segmented in 4-s epochs). Once this process is repeated for all 28 classifiers, we compute a score measure on them, which can be defined as

$$\text{score} = \frac{\text{average(CR)}}{\text{standard deviation(CR)}}. \tag{18.9}$$

Table 18.1. List of Possible Classifiers Used in Our System[a]

Classifier ID	Feature[b]	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

[a] Note that the MI, CO, and CC features are extracted from both channels, so the field channel is omitted in these cases.

[b] AR, autoregression; FT, Fourier transform; MI, mutual information; CO, coherence; CC, cross-correlation.

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

It is worth mentioning that using all 28 classifiers would not improve the performance of the system, not to mention that the computational time will also increase considerably in the authentication process. Using five personal classifiers, the authentication process takes around 5 s for EEG and 4 s for ECG. If we use all the 28 classifiers, the personal classifier approach could not be implemented, since all the subjects

Table 18.2. Posterior Matrix of the 15 FT Feature Vectors Extracted from One-Minute EEG Recording of Subject 1[a]

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

[a] 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 five-class problem (i.e., four reference subjects in this case). In our real system, we work with a 33-class problem.

would use the same classifiers. We decided to use five classifiers since this number showed a good compromise between the performance and the computational time.

Authentication Process. Once we have the five 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 1 min of recording data; that is, we input in each one of the five best classifiers 15 feature vectors (we remind the reader that the authentication test takes have a duration of 1 min; and these takes, as we did in the enrollment case, are segmented in 4-s epochs). Each classifier outputs a posterior matrix (Table 18.2). In order to fuse the results of the five classifiers, we vertically concatenate the five 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 18.6 and 18.7):

- The first element is the probability that the single-minute test data come from subject 1.
- The second element is the probability that the single-minute test data come from subject 2.
- etc.

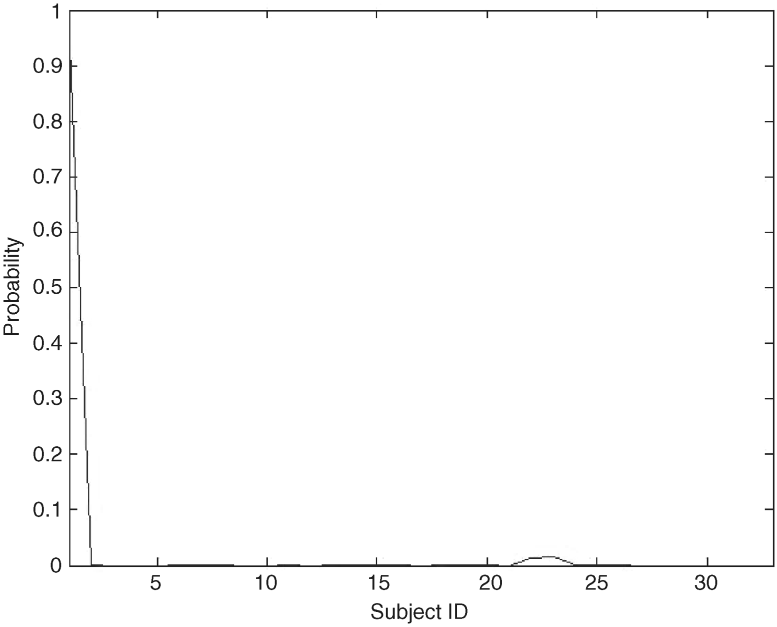

Figure 18.6. PDF for one of the enrolled subjects. The subject is classified against his training data set (class 1) and the training data sets of the reference subjects (from class 2 to class 33). In this example, he/she will be correctly authenticated with a high confidence level.

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)

In order to evaluate the performance of the system, we proceed as follows. 32 subjects with three 3-min takes are used as reference subjects, and the other eight subjects with four 3-min 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

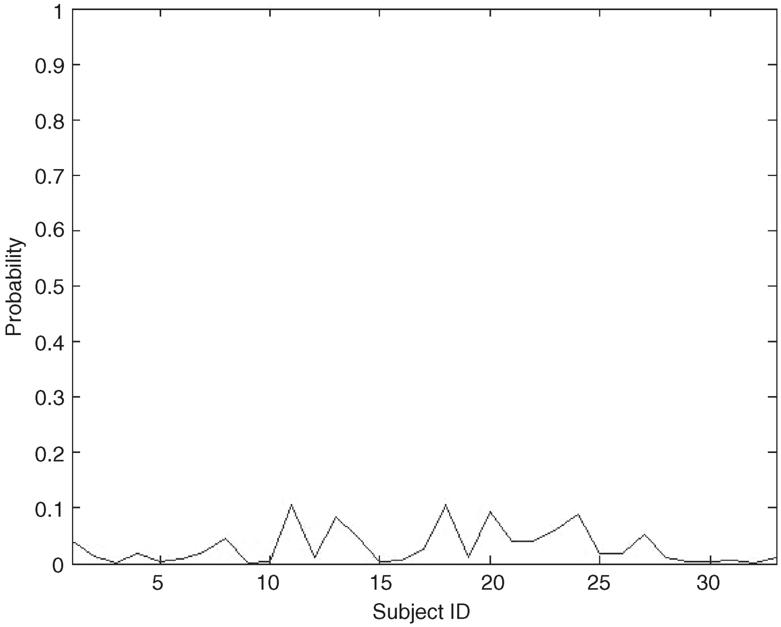

Figure 18.7. PDF for an impostor situation. In this case the probabilities are more or less evenly distributed among all classes: the one he claims to be (class 1) and the other reference subject classes (from class 2 to class 33), so in this case he/she will not be authenticated with a high confidence level.

all eight enrolled subjects, one by one. The false acceptance rate (FAR) is computed taking into account both the intruder and the impostor cases. By definition, the FAR is equal to the number of false instances classified as positive divided by the total number of false instances. The true acceptance rate (TAR) only takes into account the legal cases. Similarly, the TAR is defined as the number of true instances classified as positive divided by the total number true instances.

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

- TAR = 79.2%
- 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:

$$\text{TAR} + \text{FAR} = 100\% \tag{18.10}$$

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

18.4 AUTHENTICATION ALGORITHM BASED ON ECG

18.4.1 ECG Preprocessing

We reference the ECG channel placed in the left wrist to the right earlobe reference channel. A first difference with the EEG preprocessing is that, in this case, we are not using 4-s epochs. Now, we segment each single heartbeat waveform from the ECG signal.

18.4.2 Heartbeat 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 heartbeat 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 heartbeat waveform feature, we decimate to 144 length vectors. All these vectors in their totality are the heartbeat waveform features. Thus, the total number of feature vectors, in this case, depends on the number of heartbeats in one minute—that is, on the heartbeat rate.

18.4.3 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 DFs, 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 “heartbeat 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:

- TAR = 97.9%
- FAR = 2.1%

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

18.5 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 the results of the EEG and the ECG authentication systems. Because 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 18.8 shows the bidimensional decision space where the scores probabilities for ECG and EEG are plotted one against the other. As 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

$$\phi_1 = mE + c - C, \tag{18.11}$$

where E and C are the score probabilities of the claimed subjects respectively for the EEG and ECG modalities, m and c are the parameters of the lineal decision boundary, and ϕ_1 is the decision boundary. Values higher than d will be considered as legal subjects, whereas those lower than d are classified as impostors as shown in Figure 18.8, where the decision boundary labeled as 1 has been adapted to the test

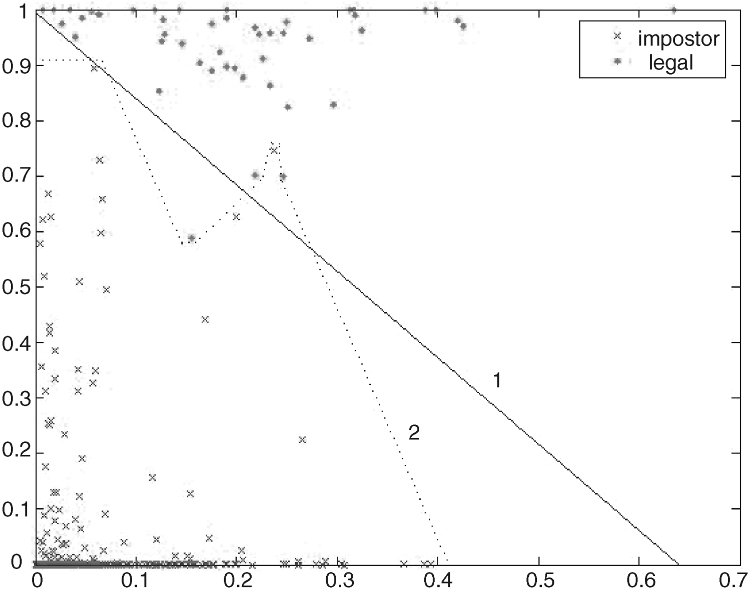

Figure 18.8. Bidimensional decision space. The ordinates represent the ECG probabilities, and the abscissa the EEG probabilities. Red crosses represent impostor cases, and green crosses represent legal cases. Two decision functions are represented.

Table 18.3. Final Results after Fusion

	TAR	FAR
Decision function 1	97.9%	0.82
Decision function 2	100	0

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 18.8. 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 an 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 TAR and FAR are shown in Table 18.3.

18.6 CONCLUSION

We have presented the performance results obtained by a bimodal biometric system based on physiological signals, namely, EEG and ECG. The results demonstrate the validity of the multistage fusion approach taken into account in the system. In this context we undertake fusion at the feature, classification, and decision stages, thereby improving 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 was used 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 heartbeat waveform as a whole. For its extraction, it is necessary to implement a preprocessing 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 from test results, its parameterization is easily attainable. Optimization procedures can be applied to fulfill this aim.

Regarding the security issues, we wish to explain that our system was developed within a European project called HUMABIO (see acknowledgment section and reference 1), in which several biometric modalities are combined to provide a highly reliable decision. All the different modalities are controlled through a central application that interfaces the different sensors with the database. A lot of security aspects have been taken into account and have been implemented in the final system (cryptography, transaction getaway, digital certificates, etc.). The details are beyond the scope of the present chapter. On the other hand, since ENOBIO has a wireless component, some additional security aspects should be taken into account during the data transmission, like data encryption. This is one development that will be implemented in the future.

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 signals, we can authenticate other things in addition to the subjects. There is evidence 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 or drugs or is not suffering from sleep deprivation [28–30]. 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 [31,32]. 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 [33].

18.7 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 chapter, we presented a rapid and unobtrusive authentication method that only uses two 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 multistage fusion architecture, which has been demonstrated to improve the system performance. The performance analysis of the system presented in this chapter 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 enrollment 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 a 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), which funded part of the research explained in this chapter. HUMABIO is an EC cofunded "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 such as transportation safety and continuous authentication in safety critical environments like laboratories, airports, and/or other buildings.

REFERENCES

1. V. Gracia et al., 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, 2006.
2. A. Riera et al., Unobtrusive biometric system based on electroencephalogram analysis, *EURASIP J. Adv. Signal Processing*, accepted.
3. N. Sviserskaya, and T. Korolkova, Genetic features of the spatial organization of the human cerebral cortex, *Neurosci. Behav. Physiolo.* **25**(5):370–376, 1995.
4. L. Biel et al., ECG analysis: A new approach in human identification, *IEEE Trans. Instrume. Meas.* **50**(3):808–812, 2001.
5. C. K. Chang, Human identification using one lead ECG, Master's thesis, Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taiwan, 2005.
6. S. Israel et al., EGC to identify individuals, *Pattern Recognit.* **38**:133–142, 2005.
7. M. Kyoso, Development of an ECG identification system, in *Proceedings of the 23rd Annual International IEEE Conference on Engineering in Medicine and Biology Society*, Istanbul, Turkey, 2001.
8. R. Palaniappan, and S. M. Krishnan, Identifying individuals using ECG beats, in *Proceedings of the International Conference on Signal Processing and Communications, 2004*, SPCOM '04, 2004, pp. 569–572.
9. A. Ross, and A. Jain, Information fusion in biometrics, *Pattern Recognit. Lett.* **24**:2115–2125, 2003.
10. G. Mohammadi et al., Person identification by using AR model for EEG signals, in *Proceedings of the 9th International Conference on Bioengineering Technology* (ICBT 2006), Czech Republic, 2006, 5 pages.
11. R. Paranjape et al., The electroencephalogram as a biometric, in *Proceedings of the Canadian Conference on Electrical and Computer Engineering*, 2001, pp. 1363–1366.

12. M. Poulos et al., Parametric person identification from EEG using computational geometry, in *Proceedings of the 6th International Conference on Electronics*, Circuits and Systems (ICECS '99), Vol. 2, 1999, pp. 1005–1008.
13. M. Poulos et al., On the use of EEG features towards person identification via neural networks, *Medical Informatics & the Internet in Medicine*, Vol. 26, 2001, pp. 35–48.
14. M. Poulos et al., Person identification from the EEG using nonlinear signal classification, *Methods Info. Med.* **41**:64–75, 2002.
15. G. Ruffini et al., A dry electrophysiology electrode using CNT arrays, *Sensors and Actuators A* **132**:34–41, 2006.
16. G. Ruffini et al., ENOBIO dry electrophysiology electrode; first human trial plus wireless electrode system, in *29th IEEE EMBS Annual International Conference*, 2007.
17. G. Ruffini et al., First human trials of a dry electrophysiology sensor using a carbon nanotube array interface, arXiv:physics/0701159.
18. S. Eischen, J. Luctritz, and J. Polish, Spectral analysis of EEG from families, *Biol. Psycholo.* **41**:61–68, 1995.
19. N. Hazarika, A. Tsoi, and A. Sergejew, Nonlinear considerations in EEG signal classification, *IEEE Trans. Signal Processing* **45**:829–836, 1997.
20. S. Marcel, and J. Mill, Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation, IDIAP Research Report 05-81, 2005, 11 pages.
21. M. Poulos et al., Person identification via the EEG using computational geometry algorithms, in *Proceedings of the Ninth European Signal Processing*, EUSIPCO'98, Rhodes, Greece, September 1998, pp. 2125–2128.
22. A. Remond, editor, *EEG Informatics. A Didactic Review of Methods and Applications of EEG Data Processing*, Elsevier Scientific Publishing, New York, 1997.
23. G. Winterer et al., Association of EEG coherence and an exonic GABA(B)R1 gene polymorphism, *Am. J. Med. Genet. B Neuropsychiatr. Genet.* **117**:51–56, 2003.
24. M. Kikuchi et al., Effect of normal aging upon interhemispheric EEG coherence: Analysis during rest and photic stimulation, *Clin Electroencephalogr.* **31**:170–174, 2000.
25. R. Moddemeijer, On estimation of entropy and mutual information of continuous distributions, *Signal Processing* **16**(3):233–246, 1989.
26. M. Deriche, and A. Al-Ani, A new algorithm for EEG feature selection using mutual information, in *Acoustics, Speech, and Signal Processing, 2001*, Vol. 2, Proceedings '01, 2001, pp. 1057–1060.
27. R. Duda et al., *Pattern Classification*, John Wiley & Sons, New York, 2001.
28. X. Hogans et al., Effects of ethyl alcohol on EEG and avoidance behavior of chronic electrode monkeys, *Am. J. Physio.* **201**:434–436, 1961.
29. J. Sorbel et al., Alcohol Effects on the Heritability of EEG Spectral Power alcoholism: clinical and experimental research, 1996.
30. S. Jin et al., Effects of total sleep-deprivation on waking human EEG: Functional cluster analysis, *Clini. Neurophysiolo.* **115**(12):2825–2833, 2004.
31. K. Takahashi, Remarks on emotion recognition from biopotential signals, in *2nd International Conference on Autonomous Robots and Agents*, 2004.
32. A. Haag et al., *Emotion Recognition Using Bio-sensors: First Steps Towards an Automatic System*, ADS, LNAI 3068, Springer-Verlag, Berlin, 2004, pp. 36–48.
33. J. Llobera, Narratives within immersive technologies, arXiv:0704.2542, 2007.