Chapter 5
Eye Blinking EOG Signals as Biometrics

Sherif N. Abbas and M. Abo-Zahhad

5.1 Introduction

In the last decade, biometric authentication has gained an increased attention in privacy and security related issues. This is due to the uniqueness of these traits and also due to the development of applications that needs high security like e-banking, remote access control, tele-medicine, etc. However, due to the advanced hacking and spoofing techniques, conventional biometric traits like finger-print and facial characteristics have been shown that they can be easily forged. In [1], Matsumoto et al. showed that a commercial finger-print system can be easily breached using fake finger-prints, where a true acceptance rate ranging from 65 % up to 100 % was achieved using gummy fingers tested over 11 different commercial finger-print systems. Moreover, in [2], it was shown that face recognition technique can be easily spoofed using printed face models. This leads the scientific community to investigate the feasibility of other physiological or behavioral traits for the purpose of biometric authentication like Electro-Encephalo-Gram (EEG) (brainwaves) signals [3], Electro-Cardio-Gram (ECG), and Phono-Cardio-Gram (PCG) signals [4]. One of the bio-electrical signals that has not been much investigated in previous works is the Electro-Oculo-Gram (EOG) signals.

EOG signal is the electrical recording of the eyeball and eyelid movements by means of electrode placed near the eye. EOG signals have some advantages over conventional biometric traits such as using finger-print and facial characteristics. These signals cannot be easily forged nor be captured at a distance like finger-print and face. Moreover, they are one dimensional, low frequency signals that can be easily processed. Regarding uniqueness, Jesper Rønager (an expert neurologist)

S.N. Abbas (✉) • M. Abo-Zahhad
Department of Electrical and Electronics Engineering, Faculty of Engineering, Assiut University, Assiut, Egypt
e-mail: sherif.siha13@eng.au.edu.eg; zahhad@yahoo.com

R. Jiang et al. (eds.), *Biometric Security and Privacy*, Signal Processing for Security Technologies, DOI 10.1007/978-3-319-47301-7_5

stated that eye blinking patterns are distinct because when the eye blinks, many electrical signals flows through the neurons of the brain that can be collected easily by electrodes placed near the eyes [5]. Since every person has a unique complicated neural network that consists of billions of neurons, eye blinking signals are unique. All these reasons motivate the authors to investigate the distinctiveness of the eye blinking signals and the feasibility of using these signals as biometric traits. The next paragraph presents a brief review of using EOG signals as biometric traits.

EOG signals have been employed previously in biometric authentication systems, however, only eye movement EOG signals have been investigated for human identification task. EOG signals were recorded from users while following a moving target with their eyes that is displayed on a screen in front of the user. This produces rapid vertical or horizontal eye movements known as saccades [6]. In [7], saccades from 30 subjects were collected and features based on amplitude, accuracy, latency, and maximum velocity were computed. Using different classifiers and different verification protocols, correct verification results in the range 96–100 % were achieved. In [8], a similar approach was adopted for biometric verification based on eye movements. The system was build using a database of 40 subjects (19 healthy subjects and 21 otoneurological patients) recorded with electro-oculography. Achieved verification results were in range 86–97 %. Although eye movement EOG signals showed high performance as biometrics, however, recording eye movement EOG signals requires a lot of effort to be done by users following the moving target which makes this technique impractical for biometric authentication. In this chapter, a new biometric authentication technique is investigated using EOG signals that are recorded while performing eye blinking tasks.

The remainder of this chapter is organized as follows. Section 5.2 provides a detailed description about the dipole model of the eye and the origin of the eye blinking waveform. Section 5.3 describes the adopted algorithms for the main components of the proposed system; pre-processing, feature extraction, feature selection, and classification. The achieved results are presented in Sect. 5.4 for identification and verification tasks. Finally, Sect. 5.5 summarizes the main conclusions and future directions.

5.2 Origin of Eye Blinking EOG Signals

As mentioned earlier, electro-oculography is the electrical recording of the potential generated due to eyeball or eyelid movements. EOG can be recorded by skin electrodes placed around the eye. The amplitude of the EOG signals ranges between 10 and 200 μV with a frequency falling in the range 0.5–15 Hz. The eyes are electrically charged; positive at the cornea and negative at the retina [9]. When the eyes or eyelids move, the potential field arising from the charge changes generates a large amplitude electric signal, which is detectable by any electrodes near the eye [10].

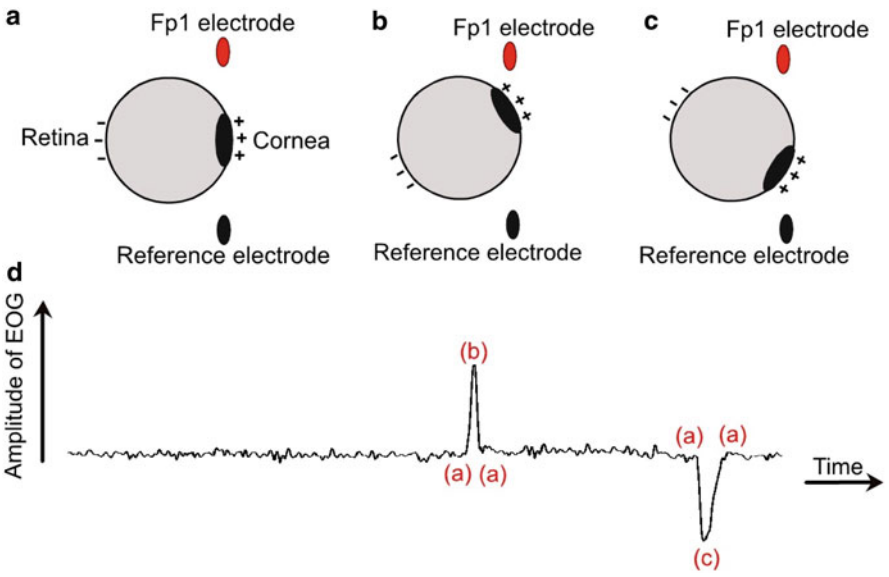

Fig. 5.1 The dipole model of eyeball with waveform of EOG signal when the cornea is in the center (**a**), rotating upwards (**b**), and downwards (**c**), EOG signal (**d**)

As shown in Fig. 5.1, when the eyeball rotates upwards, the positive pole (cornea) becomes closer to Fp1 electrode and produces a positive deflection. Similarly, when the eyeball rotates downwards, the positive pole (cornea) becomes far away from Fp1 (closer to the reference electrode) producing a negative deflection. This is similar to what happens when the eye blinks. When the eyelid closes, the cornea becomes closer to Fp1 and a positive pulse is produced. But, when the eyelid opens, the cornea rotates away from Fp1 and a negative pulse is produced. The eye blinking duration usually ranges from 300 to 400 ms. In the next section, the proposed system for human authentication using eye blinking EOG signals is described in details.

5.3 Proposed Approach for Eye Blinking EOG Biometric System

Any biometric authentication system consists of four basic modules [11]: (1) data acquisition device: which is the sensor used to acquire the biometric data, (2) pre-processing module: where the acquired data is processed and made ready for feature extraction, (3) feature extraction module: where the features discriminating between the individuals are extracted from the pre-processed data, and classification module: where features extracted are compared against the stored template, then the user's identity is established (identification mode) or the claimed identity is accepted or

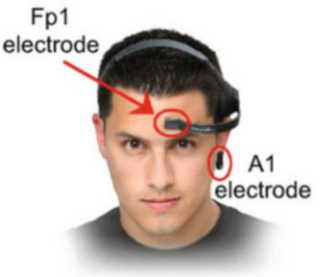

Fig. 5.2 The Neurosky headset

rejected (verification mode). Moreover, a feature selection module is added for the proposed system in order to improve its performance. The proposed techniques for these modules are described in this section.

5.3.1 Data Acquisition

All EOG signals used for the proposed system were recorded using Neurosky Mindwave headset as shown in Fig. 5.2. The headset consists of an ear clip and a sensor arm. This headset is actually used for recording EEG signals; however, it can be used to measure EOG signals as the arm sensor is resting on the forehead above the left eye (Fp1 position). The reference electrode is on the ear clip (A1 position). The sensor of Neurosky headset is made of dry electrode which does not require any skin preparation or conductive pastes. Also, the headset is wireless which makes it suitable for practical implementation of biometric authentication systems. The sampling rate of the device is 512 Hz.

The raw signal was collected from 40 users. Only 11 users out of 40 performed two session recordings with different time separation between the two sessions, however, the 29 remaining users performed only one session (1 day) recordings. More information about the recorded database is provided in Table 5.1. In one session, 6–10 trials were recorded with duration of 20 s each. Each user was asked to make 8–12 natural eye blinks in each trial. The users were asked not to do any eye movements as possible. Figure 5.3 shows the recorded eye blinking signal using Neurosky headset. MATLAB software was used for recording the raw signal from Neurosky headset and further processing. The ThinkGear Communication Driver (TGCD) [12] was used to connect Neurosky headset with Matlab through Bluetooth connection. The relation between the recorded raw values, V_{raw}, and the actual voltage, V_{actual}, is given by the following equation:

$$V_{\text{actual}} = \frac{1.8 V_{\text{raw}}}{4096 \times 2000} \tag{5.1}$$

where 1.8 is the reference voltage, 4096 is the maximum digital range, and 2000 is the amplifier gain of the Neurosky headset.

Table 5.1 Description of the recorded database (S1: first session and S2: second session)

User ID	Age	Number of sessions	Number of trials per sessions	Duration between sessions
1	24	1	7	–
2	34	1	9	–
3	74	1	9	–
4	40	1	8	–
5	23	1	9	–
6	26	2	S1: 7	16 months
			S2: 6	
7	30	1	7	–
8	23	1	10	–
9	23	1	8	–
10	27	1	8	–
11	26	1	7	–
12	28	1	10	–
13	28	1	9	–
14	31	1	7	–
15	27	1	8	–
16	29	1	10	–
17	24	1	10	–
18	27	2	S1: 7	45 days
			S2: 7	
19	28	2	S1: 8	–
			S2: 7	–
20	27	1	7	–
21	26	2	S1: 8	16 months
			S2: 10	
22	26	1	9	–
23	30	2	S1: 7	12 days
			S2: 7	
24	30	1	8	–
25	28	2	S1: 9	9 months
			S2:7	
26	24	1	10	–
27	32	2	S1: 10	13 months
			S2: 8	
28	22	2	S1: 6	18 days
			S2: 7	
29	23	1	8	–
30	24	2	S1: 7	2 months
			S2: 7	

(continued)

Table 5.1 (continued)

User ID	Age	Number of sessions	Number of trials per sessions	Duration between sessions
31	23	1	7	–
32	22	1	8	–
33	22	1	6	–
34	23	1	7	–
35	22	1	9	–
36	23	2	S1: 6	18 days
			S2: 7	
37	22	1	7	–
38	22	1	6	–
39	25	1	7	–
40	26	2	S1: 6	16 days
			S2: 7	

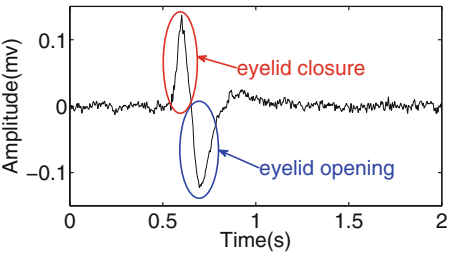

Fig. 5.3 The recorded eye blinking signal

5.3.2 Pre-processing

As mentioned in Sect. 5.3.1, the Neurosky headset is used to measure EEG signals. Therefore, the main purpose of the pre-processing stage is to isolate EOG signals from brainwaves. Also, pre-processing stage involves eye blinking waveforms extraction.

For EOG isolation, the recorded data is decomposed up to the third level using discrete wavelet decomposition. The mother wavelet used for decomposition is the Daubechies wavelet of the second order (db2) because it resembles the eye blinking waveform as shown in Fig. 5.4. Figure 5.5 shows the decomposed signals up to the third level where the approximation coefficients at the third (a_3) represent the isolated EOG signal.

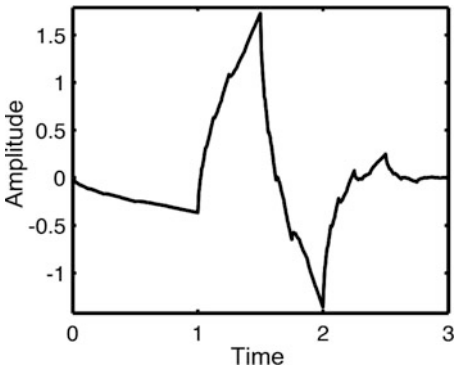

Fig. 5.4 The second order Daubechies (db2) wavelet function

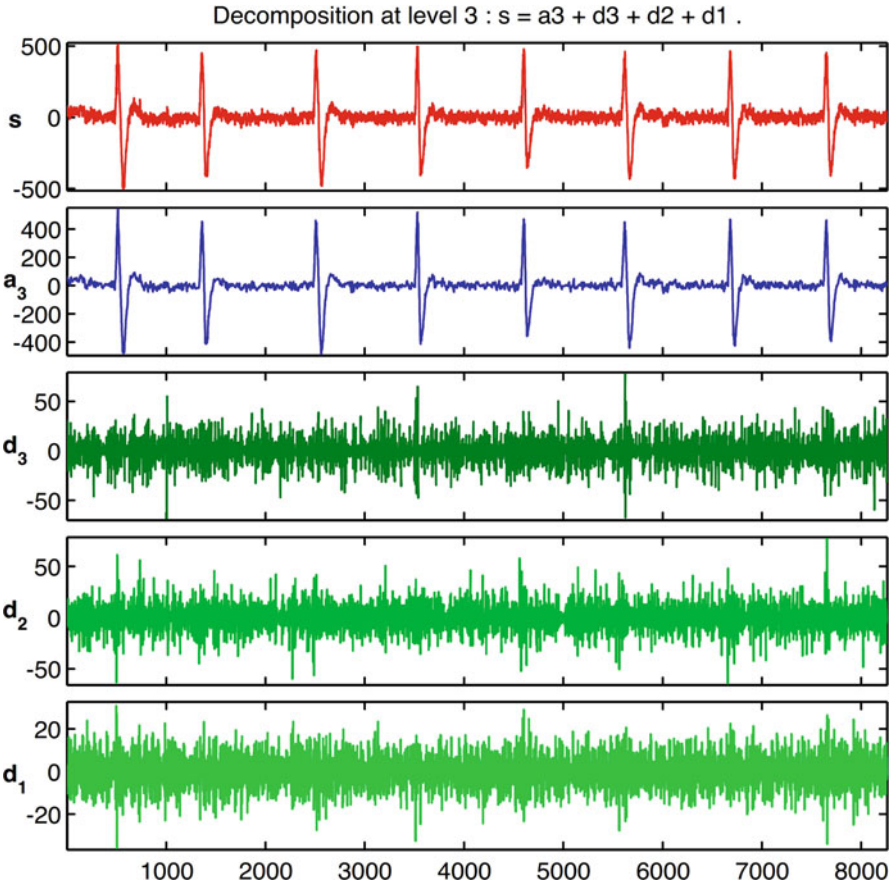

Fig. 5.5 Decomposition of the recorded signal using db2 wavelet up to the third level (s: the recorded signal, d_1, d_2, d_3: detailed coefficients at the first, second, third levels, and a_3: approximation coefficients at the third level)

For eye blinking extraction, the following procedure is followed:

1. The first step is detecting the maximum positive value in the EOG signal. It is expected to be the positive peak of the eye blinking waveform.
2. In the next step, the onset of the positive peak is detected by decreasing the sample index until the sample value is less than 5 % of the detected positive peak in step 1.
3. Next, the maximum negative value is detected within a duration of 400 ms (about 200 samples) from the position of the positive peak detected in step 1. It is expected to be the negative peak of the eye blinking waveform.
4. Then, the offset of the negative peak is detected by increasing the sample index until the sample value is less than 5 % of the detected negative peak in step 3.
5. If the value of the detected negative peak (in step 3) is less than 35 % of the detected positive peak (in step 1), then this waveform is discarded because the detected waveform is not considered a typical eye blinking waveform. Otherwise, the onset and the offset of the eye blinking waveforms are stored. After that, the samples between onset and offset are replaced by zeros.
6. The steps 1–5 are repeated until the value of the detected positive peak is less than 50 % from the first positive peak detected.

The steps for detecting eye blinking waveform are described in Fig. 5.6. The algorithm used for detecting the eye blinking waveform has some advantages like neglecting any spikes present in the signal due to electrodes movement and also neglecting the deformed eye blinking signals. Now, features are ready to be extracted from the detected eye blinking waveforms as discussed in the following section.

5.3.3 *Feature Extraction*

After extracting eye blinking waveforms from each trial, features are extracted based on the time delineation of the eye blinking waveform [13, 14]. In other words, the features extracted determine the shape (pattern) of the eye blinking waveform in the time domain. Examples of features extracted from the eye blinking waveform are positive and negative peaks values and their position, duration, and energy of the positive and negative pulses. The extracted features are described in details in Table 5.2 and some of them are illustrated in Fig. 5.7. This type of features was shown to achieve high CRRs in previous works [13, 14].

5.3.4 *Feature Selection*

The extracted features, described in Sect. 5.3.3, are concatenated together to form the feature vector that is used to train the classifier. However, some of these

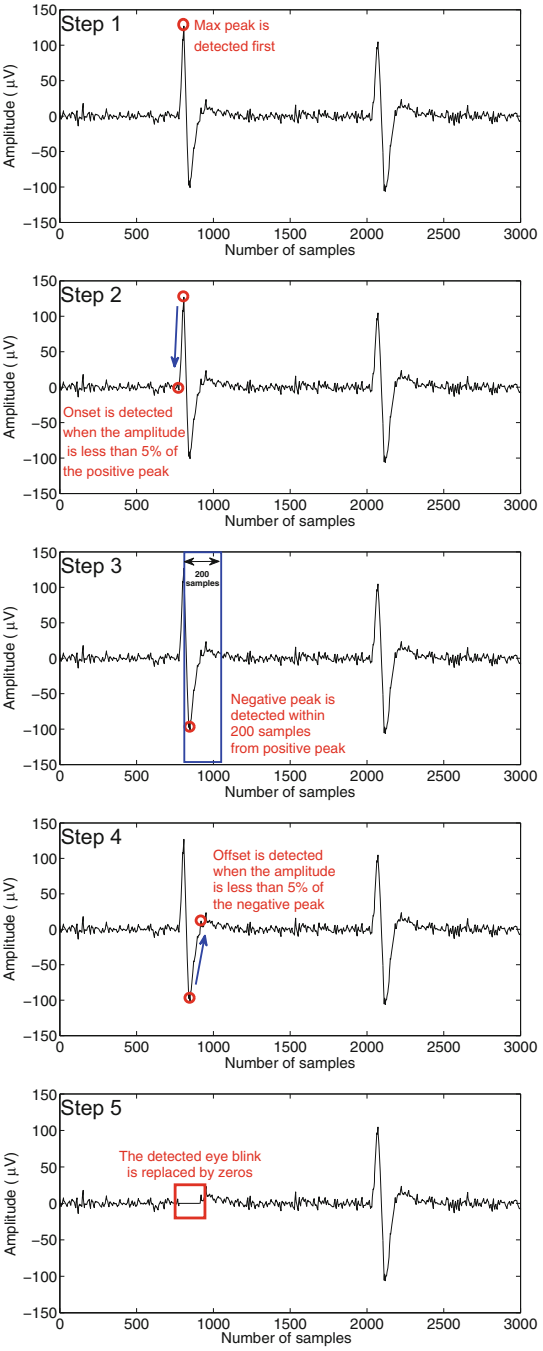

Fig. 5.6 Illustration of the steps for eye blinking waveform detection

Table 5.2 Description of the features extracted from the eye blinking waveform

Symbol	Description
M_p	Amplitude of positive peak of the eye blink
I_p	Position of positive peak from the onset of positive pulse
M_n	Amplitude of negative peak of the eye blink
I_n	Position of negative peak from the onset of negative pulse
A_p	Area under positive pulse of the eye blink
A_n	Area under negative pulse of the eye blink
E_p	Energy of the positive pulse of the eye blink
E_n	Energy of negative pulse of the eye blink
Av_p	Average value of the positive pulse of the eye blink
Av_n	Average value of negative pulse of the eye blink
D_p	Duration of positive pulse of the eye blink
D_n	Duration of negative pulse of the eye blink
S_{op}	Slope at the onset of the positive pulse ($\tan(\theta_{\text{op}})$)
S_{on}	Slope at the onset of the negative pulse ($\tan(\theta_{\text{on}})$)
S_{fp}	Slope at the offset of the positive pulse ($\tan(\theta_{\text{fp}})$)
S_{fn}	Slope at the offset of the negative pulse ($\tan(\theta_{\text{fn}})$)
M_{p1}	Amplitude of positive peak of first derivative of the eye blink signal
M_{n1}	Amplitude of negative peak of first derivative of the eye blink signal
I_{p1}	Position of the positive peak of first derivative of the eye blink signal
I_{n1}	Position of the negative peak of first derivative of the eye blink signal
N_{z1}	Number of zero crossings of the first derivative of the eye blink signal
N_{z2}	Number of zero crossings of the second derivative of the eye blink signal

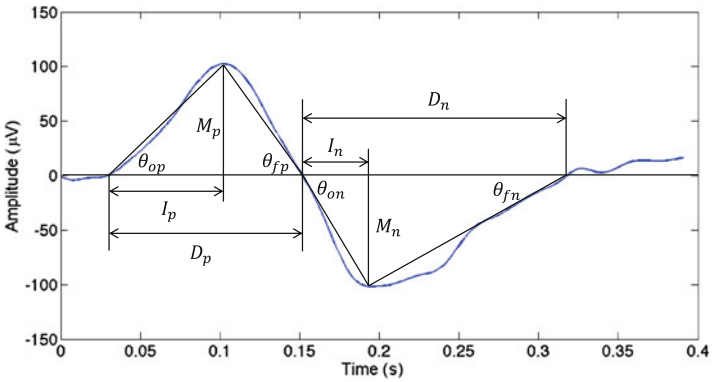

Fig. 5.7 Examples of extracted features from eye blinking waveform

features may be not unique for each subject and so it will degrade the classifier performance. Therefore, a Feature Selection (FS) technique is added to select a subset of the available features to minimize the classifier error (or maximize the classifier accuracy) and remove redundant or irrelevant features. Assuming an

original feature vector of length, N_f, which is equal to 22 in our case, the objective of feature selection is to identify the most informative subset of M_f features ($M_f < N_f$).

The most important factors that should be considered for a feature selection technique are the accuracy and the search strategy. In [15], a new feature selection technique is proposed that was based on Differential Evolution (DE) with a new statistical measure to aid in the selection of the most relevant features. DE is a population-based method for minimizing a cost function. The first step in DE is generating a population of members (random feature vectors) of dimension to be optimized. The next step is to generate mutant population based on a weighted difference of the original population. In order to overcome real number problem and to apply DE for feature selection problem, a roulette wheel weighting scheme is utilized where a cost weighting is implemented in which the probabilities of each feature are calculated from the distribution factors associated with it. More details about Differential Evolution Feature Selection (DEFS) can be found in [15–17]. DEFS technique showed better performance in accuracy than other familiar FS techniques as stated in [16]. Therefore, the DEFS MATLAB program, available in [18], is employed for the proposed biometric authentication system.

5.3.5 *Classification*

The classifier adopted for the proposed system is the Discriminant Analysis (DA) classifier. DA assumes that the features extracted from every user, s, in the database have a multivariate Gaussian distribution as follows [19]:

$$P_s(x_f) = \frac{1}{(2\pi)^{\frac{N_f}{2}} |\Sigma_s|} e^{-\frac{1}{2}(x_f-\mu_s)^T \Sigma_s^{-1}(x_f-\mu_s)} \tag{5.2}$$

where N_f is the dimension of the testing feature vector, x_f. μ_s and Σ_s are the mean and the covariance of the feature vectors of the user s. The mean and covariance for each user are calculated using the following criteria.

The training feature vectors, $t_s^i, i = 1, 2, \ldots, n_{ts}$ (n_{ts} is the total number of feature vectors extracted for user s), extracted from every eye blinking pattern are concatenated together to form the training feature matrix, T_s, where T_s is the training feature matrix for the user s and $T_s \in R^{N_f \times n_{ts}}$. The mean is then calculated using the following equation:

$$\mu_s = \frac{1}{n_{ts}} \sum_{i=1}^{n_{ts}} t_s^i, \quad \mu_s \in R^{N_f \times 1} \tag{5.3}$$

Then, the covariance matrix is estimated according to the following equation:

$$\Sigma_s = \frac{1}{n_{ts}} (T_s - \mu_s)(T_s - \mu_s)^T, \quad \Sigma_s \in R^{N_f \times N_f} \tag{5.4}$$

The classifier decision can be carried using two decision rules as discussed in the following sections.

5.3.5.1 Linear Decision Rule

Linear Discriminant Analysis (LDA) assumes that all the users (classes) have the same covariance Σ. The classifier decision is performed using the optimum Bayes rule which maximizes the posterior probability equation or its logarithm which is given by

$$D_{s(\mathrm{LDA})}(x_f) = -\frac{1}{2}(x_f - \mu_s)^T \Sigma^{-1}(x_f - \mu_s) + \log(f_s), \quad s = 1, 2, 3, \ldots, S \tag{5.5}$$

where the covariance matrix, Σ, is calculated using Eq. (5.4) after concatenating all the training feature matrices from all users. f_s is the prior probability for the user s which is assumed to be uniform and S is the total number of users registered in the system. The unknown feature vector is assigned to the user s if it has the highest posterior probability (i.e., max $D_{s(\mathrm{LDA})}, s = 1, 2, 3, \ldots, S$).

5.3.5.2 Mahalanobis Decision Rule

The decision of the classifier in this case is estimated by calculating the Mahalanobis distance between the unknown feature vector x_f and the mean and the variance for each user, s, as follows:

$$D_{s(\mathrm{Mahal})}(x_f) = \sqrt{(x_f - \mu_s)^T \Sigma_s^{-1}(x_f - \mu_s)}, \quad s = 1, 2, 3, \ldots, S \tag{5.6}$$

The unknown feature vector is assigned to the user s if it has the minimum Mahalanobis distance (i.e., min $D_{s(\mathrm{Mahal})}, s = 1, 2, 3, \ldots, S$). As a summary, Fig. 5.8 shows a brief description of the proposed system.

5.4 Experimental Setup and Results

In general, the performance of the proposed system is evaluated in identification and verification modes using K-fold cross validation. For the proposed system, only six trials, with the largest number of eye blinking waveforms, were selected for each user from the whole set of trials. Then, the proposed system is tested under two protocols: one session test (S1 protocol) and two session test (S1–S2 protocol).

In S1 protocol, five trials are selected for the training from S1 session and the remaining trial from the same session is used for testing. This is repeated six times, where every time a different trial is chosen for testing and the remaining five trials are used for training. In S1–S2 protocol, the six trials in S1 session are used for training and one trial is selected from S2 session for testing. Again, this is repeated six times, where every time a different trial is chosen from S2 session

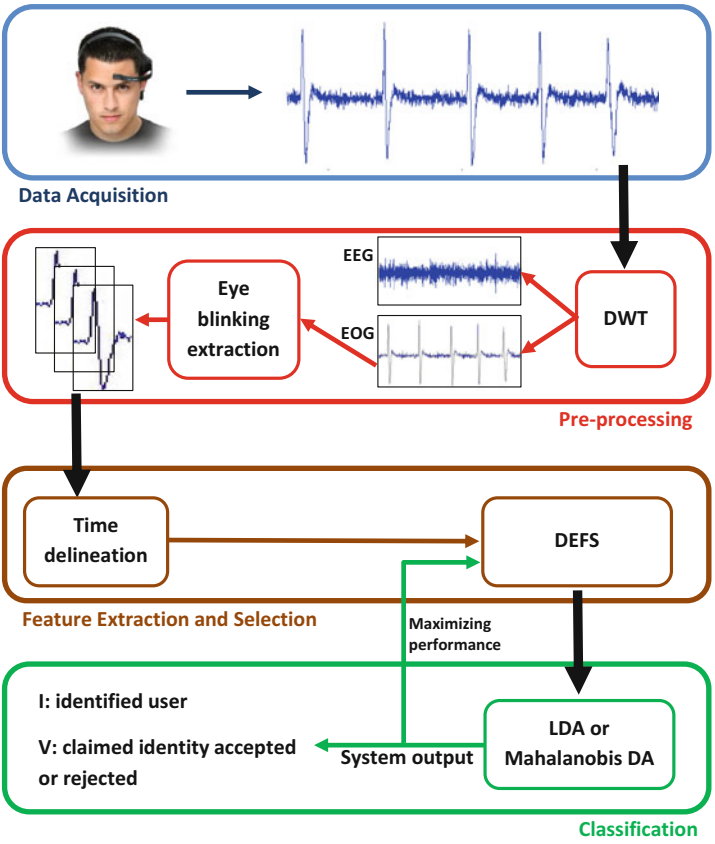

Fig. 5.8 Block diagram of the proposed eye blinking EOG-based biometric authentication system

for testing. Finally, the average CRR (in identification mode) or the average error rates (in verification mode) are calculated. This will be discussed in details in the following two sections.

5.4.1 Identification Mode

For evaluating the proposed system in identification mode, one trial is selected from each user to generate the test samples. Then, the proposed system generates the identity of each testing sample for each user according to Eq. (5.5) or Eq. (5.6). The CRR for this experiment is defined as follows:

$$\mathrm{CRR}(j) = \frac{\text{Number of correctly identified users in step } j}{\text{Total number of users}} \tag{5.7}$$

The previous step is repeated for six times. In each time, one trial (which has not been selected before) is selected from each user to generate the test samples. Finally, the average CRR, CRR_{av}, is calculated using the following equation:

$$CRR_{av} = \frac{1}{6}\sum_{j=1}^{6} CRR(j) \tag{5.8}$$

In identification mode, CRR_{av} is evaluated under different number of features that were selected using DEFS technique as discussed in Sect. 5.3.4. Figure 5.9 shows the achieved CRR_{av} using S1 protocol (one session test) over 40 users. In this test, Mahalanobis distance classifier showed better recognition rates than LDA. Based on the achieved results, using DEFS, a better CRR_{av} up to 93.75 % can be obtained using less number of features (12, 13, 14, and 15 features only) in comparison to a CRR_{av} of 89.58 % using the whole set of features (22 features). The feature subsets achieved highest CRR_{av} for LDA and Mahalanobis DA are provided in Tables 5.3 and 5.4, respectively.

Figure 5.10 shows the achieved results using S1–S2 protocol in comparison with S1 protocol only for the users who performed the two session recordings (11 users only). Due to the problem that biometric traits change over time, a decrease in the CRR is shown for the S1–S2 protocol. Using Mahalanobis distance classifier, a decrease of about 36 % is achieved (from 100 % using S1 protocol to 63.64 % using S1–S2 protocol). Also, using LDA, the CRR_{av} decreased from 96.97 % (using S1 protocol) to 62.12 % (using S1–S2 protocol).

5.4.2 *Verification Mode*

For evaluating the proposed system in verification mode, each user in the database tries to access the system with his true identity (genuine) and with a false identity (the remaining identities in the database). For the claimed identity, I, provided by each user, s, the database is divided into two classes; the I-related database and the I-non-related database. Then, the claimed identity is accepted or rejected according to the following relation:

$$V_s = \begin{cases} 1, & \text{if } \frac{D_I(x_f)}{D_{\text{non}-1}(x_f)} \geq T_s \\ 0, & \text{if } \frac{D_I(x_f)}{D_{\text{non}-1}(x_f)} < T_s \end{cases} \tag{5.9}$$

where V_s is the output of the system in verification mode, "1" means that the system accepts the claimed identity, and "0" means that the system rejects the claimed identity. Also, $D_I(x_f)$ represents the probability that the claimed identity belongs to I-related class [estimated using Eq. (5.5)] or the Mahalanobis distance between the testing sample and the I-related class [estimated using Eq. (5.6)]. Similarly,

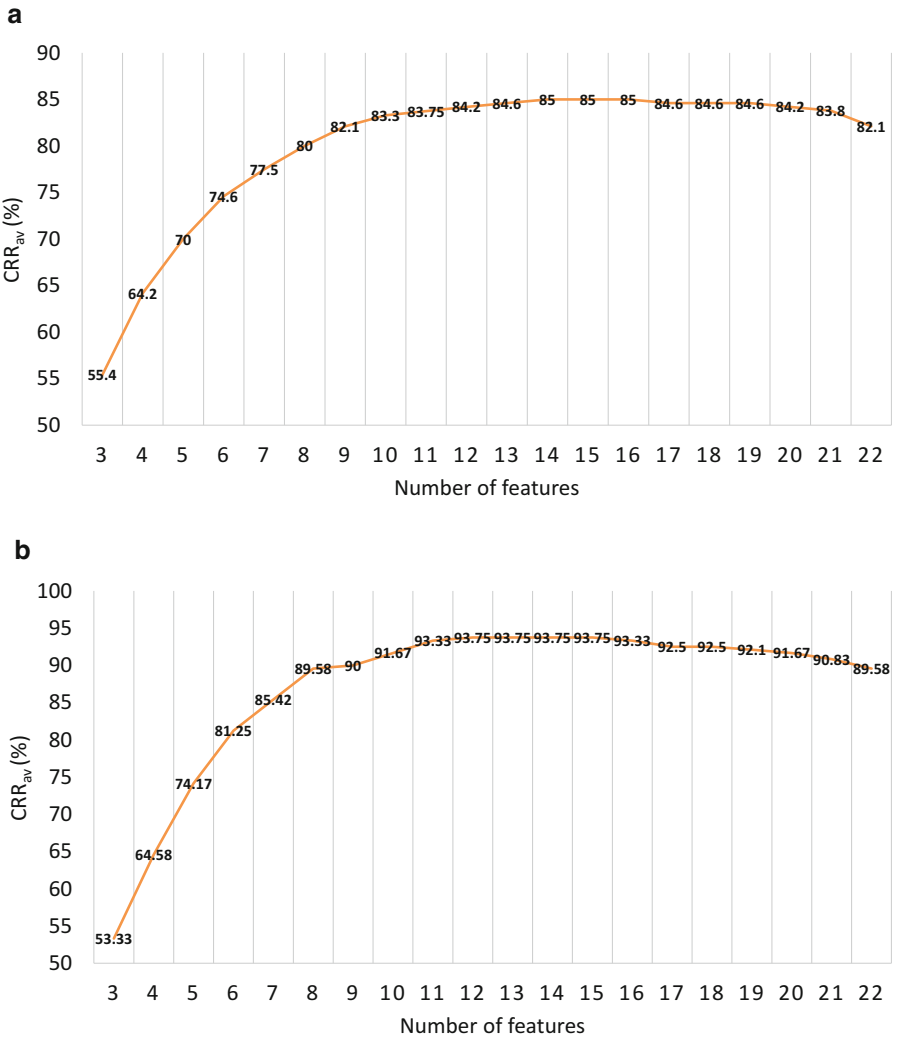

Fig. 5.9 The CRR_{av} achieved for the proposed system under S1 protocol. (**a**) LDA classifier. (**b**) Mahalanobis DA classifier

$D_{non-I}(x_f)$ represents the probability that the claimed identity belongs to I-non-related class [estimated using Eq. (5.5)] or the Mahalanobis distance between the testing sample and the I-non-related class [estimated using Eq. (5.6)].

The similarity threshold, T_s, defines the degree of security of the system. In this mode, two error rates are defined; False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR defines the number of times the system incorrectly matches a sample from one person to a template from another (accepts an imposter). FRR defines the number of times the system does not recognize a sample as coming from

Table 5.3 Features selected using DEFS [15] that achieved highest CRR_{av} using LDA classifier

Number of features	CRR_{av} (%)	Selected features using DEFS
14	85	$M_p, I_p, M_n, A_n, Av_p, Av_n, D_p, S_{op}, S_{on}, S_{fn}, M_{p1}, M_{n1}, I_{n1}, N_{z1}$
15	85	$M_p, I_p, M_n, A_p, A_n, Av_p, Av_n, D_p, S_{op}, S_{on}, S_{fn}, M_{p1}, M_{n1}, I_{n1}, N_{z1}$
16	85	$M_p, I_p, M_n, A_p, A_n, Av_n, D_p, S_{op}, S_{on}, S_{fp}, S_{fn}, M_{p1}, M_{n1}, I_{p1}, I_{n1}, N_{z1}$

Table 5.4 Features selected using DEFS [15] that achieved highest CRR_{av} using Mahalanobis DA classifier

Number of features	CRR_{av} (%)	Selected features using DEFS
12	93.75	$M_p, M_n, A_p, A_n, E_p, Av_p, Av_n, S_{on}, S_{fp}, M_{p1}, I_{p1}, N_{z1}$
13	93.75	$M_p, M_n, A_p, E_p, Av_p, Av_n, D_p, D_n, S_{on}, M_{p1}, I_{n1}, N_{z1}, N_{z2}$
14	93.75	$M_p, M_n, A_p, A_n, E_p, Av_p, Av_n, D_p, S_{on}, S_{fp}, M_{p1}, I_{p1}, I_{n1}, N_{z1}$
15	93.75	$M_p, I_p, M_n, A_p, A_n, E_p, Av_p, Av_n, D_p, D_n, S_{on}, S_{fn}, M_{p1}, N_{z1}, N_{z2}$

the same individual who produced the template (rejects a genuine). These error rates depend on the similarity threshold, T_s; as T_s increases, FAR decreases and FRR increases making the system more secure. However, as T_s decreases, FAR increases and FRR decreases making the system less secure. At a given value of T_s, FAR and FRR will have the same values, i.e., EER.

Every time the experiment is run, a new testing trial is chosen. This is repeated for six times, then, the average FAR and FRR values for different values of T_s are computed. Figure 5.11 shows the error rates using the two decision rules under S1 protocol (40 users). As shown, the two decision rules achieved approximately the same EER (7.5 % for LDA and 7.45 % for Mahalanobis DA). This test is performed using the whole set of features (22 features).

Figures 5.12 and 5.13 show the EER for the proposed system under S1–S2 protocol in comparison with S1 protocol using LDA and Mahalanobis DA classifiers. Again, an increase in the error rates is achieved because of the large time separation between the training and testing samples where an EER of 22.5 % and 32 % were obtained using LDA and Mahalanobis DA classifiers, respectively. This test is performed using the whole set of features (22 features).

5.5 Discussion and Future Work

In this chapter, the authors presented a new technique for human authentication using eye blinking waveforms extracted from EOG signals. The proposed system used time delineation to extract important features from the eye blinking waveform. Over a population of 40 users, the proposed system successfully detected the identity

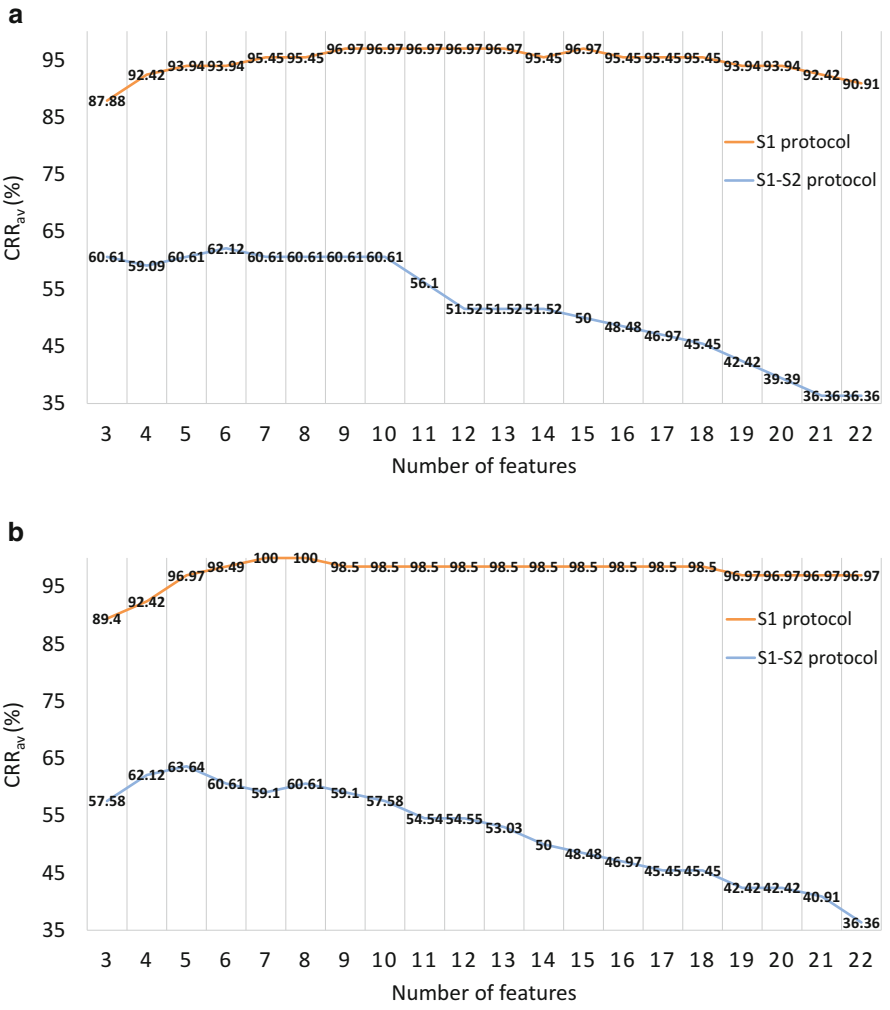

Fig. 5.10 A comparison between CRR_{av} achieved for the proposed system under S1 and S1–S2 protocols. (**a**) LDA classifier. (**b**) Mahalanobis DA classifier

of the users with accuracy up to 93.72 % in identification mode (S1 protocol). In verification mode, the proposed system rejects the true identity and accepts false identity with an EER of 7.45 % (S1 protocol). Also, the issue of permanence was tested for the proposed system using S1–S2 protocol. Although the achieved results for the proposed system look promising, there are some issues that need to be addressed in the future as stated in the following points:

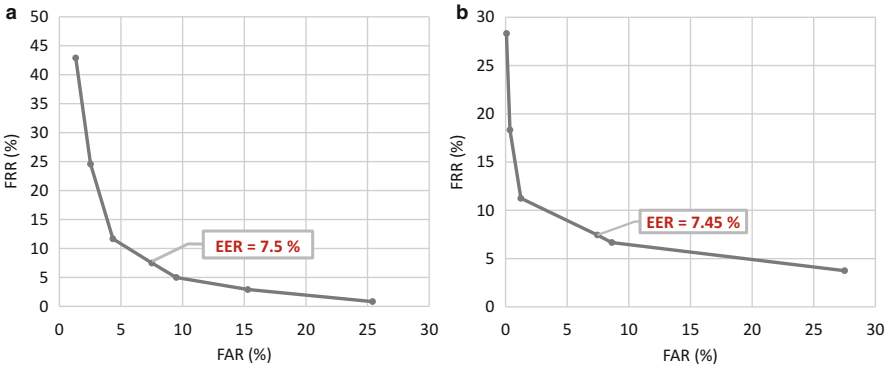

Fig. 5.11 False acceptance and rejection rates at different values of similarity threshold. (**a**) LDA classifier. (**b**) Mahalanobis DA classifier

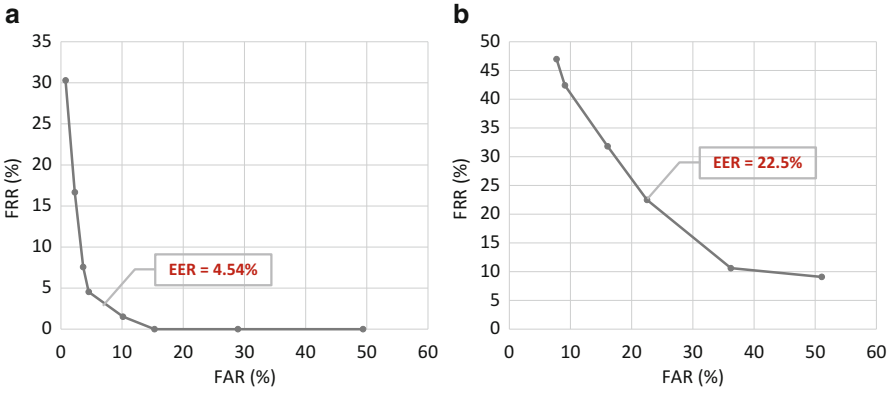

Fig. 5.12 A comparison between EERs of S1 and S1–S2 protocols using LDA classifier. (**a**) S1 protocol. (**b**) S1–S2 protocol

- Population (number of users): For building practical biometric system, the discrimination ability of the eye blinking waveform should be tested over large population, may be thousands of users.
- Permanence (stability of the biometric trait over time): As discussed in Sect. 5.4, using testing samples that were recorded after a large time separation from the training samples degrades the system's performance. This issue needs to addressed in the future. A possible solution for this issue is to use training samples recorded at different time intervals for the same user. This may enhance the system's performance.
- Factors affecting eye blinking: The degree of concentration or fatigue may affect the strength of the eye blinking waveform, hence, affecting the performance of the system. Therefore, these factors should be addressed in future work.

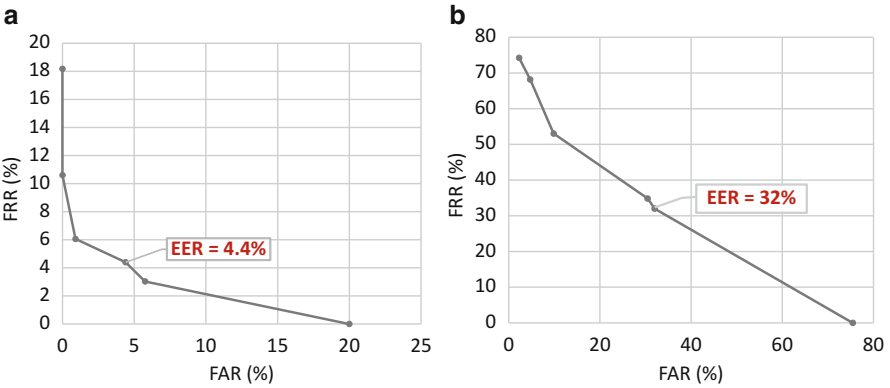

Fig. 5.13 A comparison between EERs of S1 and S1–S2 protocols using Mahalanobis DA classifier. (**a**) S1 protocol. (**b**) S1–S2 protocol

- Feature extraction technique: Different techniques for feature extraction may be tested and compared with the proposed one.
- Fusion with other traits: Eye blinking EOG biometric trait can be fused with other traits like EEG signals to build a multi-modal system to improve the performance of the EEG-based biometric authentication systems [20].

Although the achieved simulation results are promising, eye blinking EOG signals still need a lot of investigation to discuss the previous issues before considering these signals as biometric traits for identifying humans.

References

1. T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, Impact of artificial gummy fingers on fingerprint systems, in *SPIE Proceedings*, vol. 4677. Optical Security and Counterfeit Deterrence Techniques IV (2002), pp. 275–289
2. N. Erdogmus, S. Marcel, Spoofing face recognition with 3D masks. IEEE Trans. Inf. Forensics Secur. **9**(7), 1084–1097 (2014)
3. M. Abo-Zahhad, S.M. Ahmed, S.N. Abbas, State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals. IET Biometrics **4**(3), 179–190 (2015)
4. M. Abo-Zahhad, S.M. Ahmed, S.N. Abbas, Biometric authentication based on PCG and ECG signals: present status and future directions. Signal Image Video Process. **8**(4), 739–751 (2014)
5. J. Klonovs, C.K. Petersen, Development of a mobile EEG-based feature extraction and classification system for biometric authentication. M.Sc. thesis, Aalborg University Copenhagen, 2012
6. U. Saeed, A survey of automatic person recognition using eye movements. Int. J. Pattern Recognit. Artif. Intell. **28**(8), 1456015 (2015)
7. Y. Zhang, J. Rasku, M. Juhola, Biometric verification of subjects using saccade eye movements. Int. J. Biometrics **4**(4), 317–337 (2012)

8. M. Juhola, Y. Zhang, J. Rasku, Biometric verification of a subject through eye movements. Comput. Biol. Med. **43**(1), 42–50 (2013)
9. P. Berg, M. Scherg, Dipole models of eye movements and blinks. Electroencephalogr. Clin. Neurophysiol. **79**(1), 36–44 (1991)
10. D. Denney, C. Denney, The eye blink electro-oculogram. Br. J. Ophthamol. **68**(4), 225–228 (1984)
11. J. Wayman, A. Jain, D. Maltoni, D. Maio, *An Introduction to Biometric Authentication Systems* (Springer, London, 2005)
12. ThinkGear Connection Driver (2014). Available at: http://developer.neurosky.com/docs/doku.php?id=app_notes_and_tutorials. Accessed 13 May 2015
13. M. Abo-Zahhad, S.M. Ahmed, S.N. Abbas, A novel biometric approach for human identification and verification using eye blinking signal. IEEE Signal Process. Lett. **22**(7), 876–880 (2015)
14. M. Abo-Zahhad, S.M. Ahmed, S.N. Abbas, A new biometric modality for human authentication using eye blinking, in *IEEE Proceedings. Cairo International Biomedical Engineering Conference (CIBEC)* (2014), pp. 174–177
15. R.N. Khushaba, A. Al-Ani, A. Al-Jumaily, Differential evolution based feature subset selection, in *IEEE Proceedings. International Conference Pattern Recognition (ICPR)* (2008), pp. 1–4
16. R.N. Khushaba, A. Al-Ani, A. Al-Jumaily, Feature subset selection using differential evolution and a statistical repair mechanism. Expert Syst. Appl. **38**(9), 11515–11526 (2011)
17. A. Al-Ani, A. Alsukker, R.N. Khushaba, Feature subset selection using differential evolution and a wheel based search strategy. Swarm Evol. Comput. **9**, 15–26 (2013)
18. MATLAB Program for Differential Evolution Based Feature Selection (DEFS) (2015). Available at http://www.mathworks.com/matlabcentral/fileexchange/30877. Accessed 13 May 2015
19. S. Theodoridis, K. Koutroumbas, *Pattern Recognition*, 4th edn. (Academic, New York, 2008)
20. M. Abo-Zahhad, S.M. Ahmed, S.N. Abbas, A new multi-level approach to EEG based human authentication using eye blinking. Pattern Recogn. Lett. (2015). doi:10.1016/j.patrec.2015.07.034