Bioelectrical Signals: A Novel Approach Towards Human Authentication

Hamed Aghili

Abstract Human authentication based on electrical bio-signals, or bioelectrical signals, is a rapidly growing research area due to increasing demand for establishing the identity of a person, with high confidence, in a number of applications in our vastly interconnected society. Studies show that bioelectrical signals can be not only employed for diagnostic purposes in medicine, but also used in human authentication since they have unique features among individuals. This article reviews examples of up-to-date researches that have applied bioelectrical signals like Electrocardiogram (ECG), Electroencephalogram (EEG) and Electrooculogram (EOG) in human authentication. Utilizing bioelectrical signals provides a novel approach to user authentication that contains all the crucial attributes of previous traditional authentication. The most significant reasons for deployment of electrical bio-signals in user authentication include their measurability, uniqueness, universality and resistance to spoofing, while other conventional biometrics like face shape, hand shape, fingerprint and voice can be artificially generated.

Keywords Human authentication · Biometrics · Bioelectrical signals
Electroencephalogram signal · Electrocardiogram signal · Electrooculogram signal

1 Introduction

Authentication is carried out in a wide range of areas of different levels of security and importance. Not having a comprehensive understanding of the requirements for authentication according to different circumstances, we use the same traditional authentication, either through an object for example an ID card or via knowledge like passwords, for every situation. This is while new authentication methods have advanced even beyond using conventional biometrics, and are applying

H. Aghili (✉)
Department of Electrical Engineering (Robotic Engineering),
Payame Noor University (PNU), Tehran, Iran
e-mail: engineer.aghili@gmail.com

S. Montaser Kouhsari (ed.), *Fundamental Research in Electrical Engineering*, Lecture Notes in Electrical Engineering 480,
https://doi.org/10.1007/978-981-10-8672-4_1

bio-electrical signals for authentication purposes. The recent studies have shown that bio-signals can provide human authentication with the resistance to fraudulent attacks since they have specific features that are unique among individuals. In this article we introduce bioelectrical signals and mention their advantage over other conventional biometrics. After that we review some researches that have been carried out in the field of applying Electrocardiogram, Electroencephalogram and Electrooculogram signals for human authentication.

2 What Are Bioelectrical Signals?

Bio-signals are records of a biological event such as a beating heart or a contracting muscle. The electrical, chemical, and mechanical activity that occurs during these biological events often produces signals that can be measured and analyzed [1]. Bio-signals are divided into six groups according to their physiological origin: bioelectrical signals, bio-magnetic signals, bio-chemical signals, bio-mechanical signals, bio-aquatic signals and bio-optical signals. The bio-signal of our interest in this article is bioelectrical signals. Bioelectrical signals are those that are generated by the summation of electrical potential differences across an organ [2]. Via surface electrodes attached or close to the body surface, signals from a broad range of sources can be recorded [3] precisely, if a nerve or muscle cell is stimulated, it will generate an action potential that can be transmitted from one cell to adjacent cells via its axon. When many cells become activated, an electric field is generated. These changes in potential can be measured on the surface of the tissue or organism by using surface electrodes [1]. Bioelectrical signals are very low amplitude and low frequency electrical signals [4]. These signals are generally used for medical diagnosis, but research findings confirm that since they have unique features among individuals, they can also be used for human authentication. The examples of bioelectrical signals are Electrocardiogram, Electroencephalogram, Galvanic skin response and Electrooculogram “Fig. 1”.

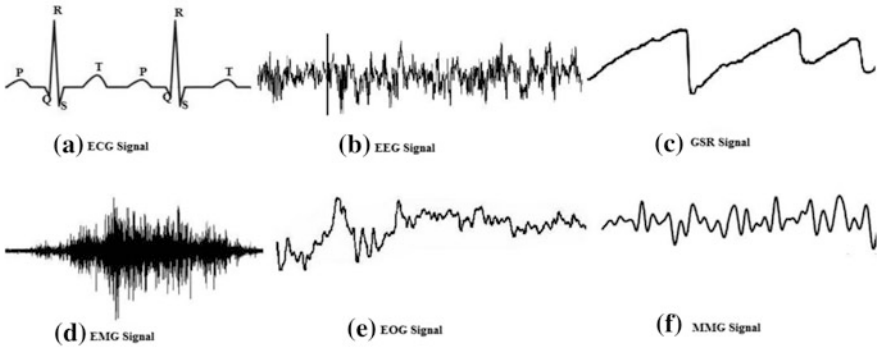

Fig. 1 Bioelectrical signals [2]

3 The Advantage of Bioelectrical Signals Over Conventional Biometrics

Biometric authentication systems use a variety of physical or behavioural characteristics including fingerprint, face, hand geometry, iris and voice pattern of an individual to establish identity. By using biometrics it is possible to establish an identity based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password [5]. Although this conventional biometrics is unique identifiers, they are not confidential and neither secret to an individual since people put biometric traces anywhere. So, the original biometric can be easily obtained without the permission of the owner of that biometric. For example, in case of fingerprints, an artificial finger, known as a gummy finger, can be made by pressing a live finger to plastic material, and then mould an artificial finger with it or by capturing a fingerprint image from a residual fingerprint with a digital microscope, and then make a mould to produce an artificial finger [6]. In addition, thanks to the recent advancement in digital cameras and digital recording technologies, the acquisition and processing of high quality images and voice recordings has become a trivial task. Therefore, Iris scanners can be spoofed with a high resolution photograph of an iris held over a person's face [7]. The vulnerability of conventional biometrics to spoof has caused considerable concern especially in those fields that require high reliable user authentication. This heightened concern leads to great interest in assessing the probability and efficiency of using bioelectrical signals in authentication systems. Using bioelectrical signals as biometrics offers several advantages. In addition to their uniqueness, bioelectrical signals are confidential and secure to an individual. They are difficult to mimic and hard to be copied. To be more precise, the biological information of a person is genetically governed from deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) proteins. Eventually, the proteins are responsible for the uniqueness in the certain body parts. Similarly, the organs like heart and brain are composed of protein tissues called myocardium and glial cells, respectively. Therefore, the electrical signals evoked from these organs show uniqueness among individuals [4]. So, by using bioelectrical signals as biometrics we can benefit from sufficiently invulnerable authentication systems.

4 The Electroencephalogram Signal as a Biometric

As mentioned above the electroencephalogram (EEG) signal is one of the bioelectrical signals generated by brain activity, and can be recorded by positioning voltage sensitive electrodes on the surface of the scalp "Fig. 2". Typically, from 11 to 256 electrodes are placed on the scalp, each provides a time series sampled at 5.5–1.5 kHz, and generated hundreds of megabytes of data that must be analyzed in order to extract useful information. The feature space of EEG data is very large

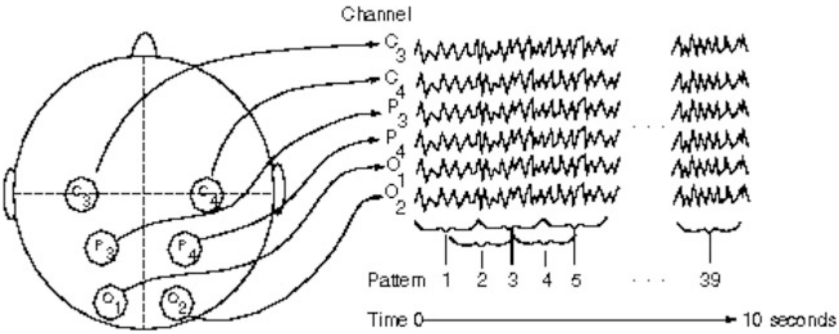

Fig. 2 Signal acquisition (www.cs.colostate.edu)

coming from the fact that information is usually accumulated throughout parallel (across every single electrode) as well as considering the human brain is really an extremely complex dynamical system [1]. The EEG can reflect both the spontaneous activity of the brain with no specific task assigned to it, and the evoked potentials, which are the potentials evoked by the brain as a result of sensory stimulus [8]. EEG-based authentication has been studied nowadays and researches have demonstrated that the EEG brainwave signals could be used for individual authentication. These researches can be categorized into three groups based on the type of signal acquisition protocol used in authentication task and the mental state of the subject during signal acquisition [9]; EEG recordings while relaxation with closed or open eye; EEG recordings while being exposed to visual simulation; EEG recordings while performing mental tasks. The example of each category is explained in the following:

Gui et al. [10] have presented an EEG-based biometric security framework. The data flow of authentication framework contained four steps. The first step was to collect raw EEG signals. 1.1 s of raw EEG signals was recorded from 6 midline electrode sites from 32 adult participants. Since it is argued that the brain activities are very focused during the visual stimulus process, the participants were asked to silently read an unconnected list of texts which included 75 words. In the next part, the noise level of raw EEG signals was reduced through ensemble averaging and low-pass filter. Ensemble averaging is a very effective and efficient technique in reducing noise because the standard deviation of noise after average is reduced by the square root of the number of measurements. After ensemble averaging, a 65 Hz low-pass filter was followed to remove the noise out of the major range of the EEG signals. In the third part, frequency features were extracted using wavelet packet decomposition. A wavelet is a mathematical function which can be used to divide a continuous-time signal into different scale component. A 4 level wavelet decomposition of the EEG signal after low pass filtering with 65 Hz was used to get the 5 EEG sub-bands, namely delta band (5–4 Hz), theta band (4–1 Hz), alpha band (1–15 Hz), beta band (15–35 Hz), and gamma band. Since the energy distributions of the frequency components are quite different for each individual, it was possible to adopt those frequency components as the features to represent the EEG signals. The mean, standard deviation and entropy were also calculated to form the feature vectors. So, there were 3 × 5 = 15 features for each subject. Finally, in classification part, the input feature vector was compared to the feature vectors that have been stored in dataset to authenticate the identity of the subject.

Nakanishi et al. [11] are also other researchers who have proposed new feature of EEG signals for authentication. They have used the concavity and convexity of spectral distribution in the alpha band of EEG signal in authentication to reduce the computational load for feature extraction, and authentication was done based on a linear combination of these features. They applied a consumer-use electroencephalograph that had only one electrode (single-channel) and was more convenient and practical compared to multi conventional channel measurements which increase the number of processing data, and require subjects to set a number of electrodes on the scalp. The single electrode was set on the frontal region of a head by using a head-band and subjects were asked to sit on a chair at rest with eye closed in quiet room that was the most suitable circumstances under which alpha wave can be detected. They adopted the spectrum analysis based on fast Fourier transform because it makes it easy to filter the spectrum in the alpha band and the concavity as well as the convexity of spectral distribution was used for distinguishing individuals. The concavity of spectral distribution was defined by detecting the maximum of the power spectrum and then calculating its tenth part and adopting it as a criterion. Then, frequencies of which power spectral values that were under the criterion were squared and summed. In addition to the concavity, the convexity of spectral distribution was another important feature. To define the convexity of spectral distribution the power spectral values in the alpha band were ranked and then the values and the frequencies of the top three were averaged. Next, the spectral values, which were greater than the averaged power spectrum, were summed. These three obtained features were as features which represent the convexity in spectral distribution. Finally, the subject authentication was done according to some calculation on combination of these obtained features.

Another research has been carried out by Liu et al. [12]. They recruited twenty right-handed subjects with normal or corrected-to-normal visual acuity and 64-channels EEG signals were recorded continuously by electrodes that were placed on the scalp. Two hundred and sixty color pictures were presented to the subject on a computer monitor located 1 m away from him. Stimulus duration of each picture was 3 s and all pictures were common and meaningful, identified and named easily. To find out suitable EEG features, several methods were employed to extract the EEG biometric features, including AR model, one of the most popular algorithms of feature extraction in which the series are estimated by a linear difference equation in time domain, power spectrum of the time-domain analysis that provides basic information of how the power distributes as a function of time, power spectrum of the frequency-domain analysis that provides basic information of how the power distributes as a function of frequency and phase-locking value which is a method to describe the synchronism between two signals. Then, all of the above-mentioned features were given to a support vector machine for classification respectively.

5 The Electrocardiogram as a Biometric

The heart makes use of electrical activity to activate the muscles required to pump blood through the circulatory system. By laying sensitive recording electrodes at certain regions around the heart, the signals can be recognized. The signals generated by the heart beat forms a regular pattern that records the electrical activity of the heart [1]. This signal is known as Electrocardiogram and can be used in human authentication. Recent works in the ECG biometric recognition field can be categorized as either fiducial point dependent or independent. Fiducials are specific points of interest on the ECG heart beat, namely, P, QRS and T waves that are shown in "Fig. 3". By using these features a reference vector is produced to use for authentication. Israel et al. [13] have shown that ECG attributes are unique to each individual and can be used in human authentication. In their experimentation, data were collected at high temporal resolution from twenty nine individuals. At first step, a filter was designed and used to extract ideal data from raw ECG data and to locate fiducial positions by removing non-signal artifacts. The raw data contained both low and high frequency noise components associated with changes in baseline electrical potential of the device and the digitization of the analog potential signal respectively. After applying filtering, the ECG trace fiducial positions were located. For human identification, attributes were extracted from the P, R, and T complexes and four additional fiducial points which were named L′, P′, S′ and T′. Physically, the L′ and P′ fiducials indicate the start and end of the atrial depolarization and S′ and T′ positions indicate the start and end of ventricular depolarization "Fig. 4".

Attributes that show the unique physiology of an individual were extracted by calculating the distance among the ECG fiducials. Classification was performed on heartbeats using standard linear discriminate analysis. A conversion was required to link the performance of the heartbeat classification to human identification. Standard, majority and voting were used to assign individuals to heartbeat data. The conversion was performed using contingency matrix analysis. Steven A. Israel et al. also demonstrated that the extracted features are independent of sensor location by

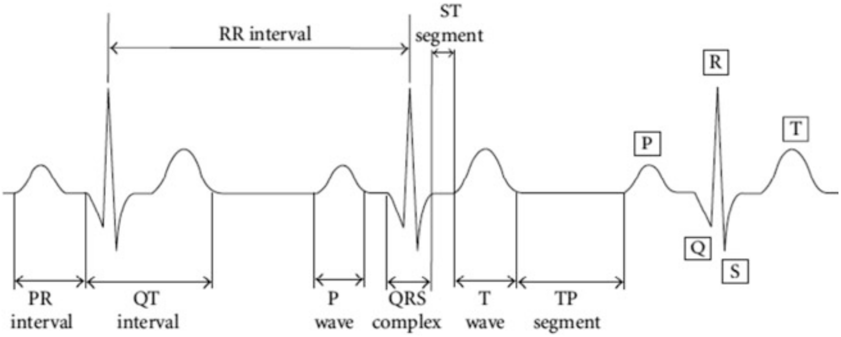

Fig. 3 A typical ECG signal that includes three heartbeats [4]

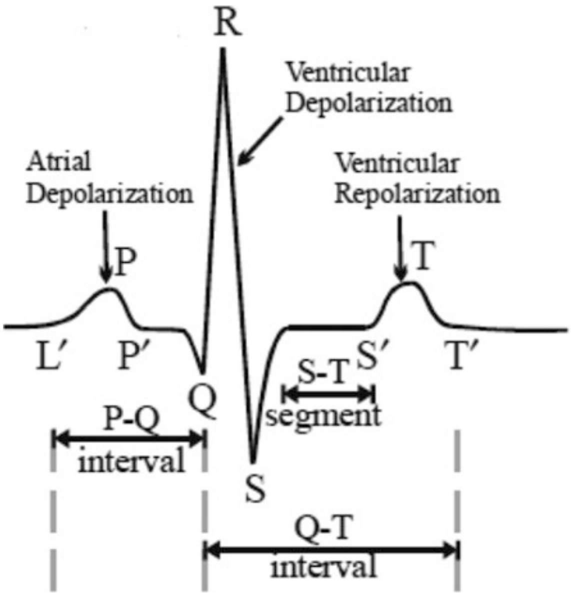

Fig. 4 Fiducial points' physical positions [13]

collecting ECG data at two electrode placements, one at the base of the neck and another one at fifth intercostals spacing. After testing they found a strong agreement between neck and chest ECG data which proved that the extracted ECG attributes are independent of sensor location. In addition, they proved that ECG attributes invariant to the individual's state of anxiety. Dey et al. [9] also used ECG as a biometric feature to authenticate a person. They generated an ECG feature matrix by using the features extracted from ECG, namely the time durations for the R-R, S-S, Q-Q, T-T, P-R, Q-T, and QRS intervals. Then, an inner product was performed between this feature matrix and a constant matrix. The product is then compared with a previously set threshold. If the result lied above the threshold, a binary value of 1 was assigned to it; otherwise 5. The combination of 1 and 5 produced the ECG-Hash code. After that, another ECG-Hash code was generated by using the original feature matrices and constant matrices in the same way as mentioned above. A matching was performed between these two ECG-Hash codes. On the event of a match, the individual was authenticated. Else, the authentication procedure failed.

Matos et al. [14] are other researchers that applied ECG as a biometric for human authentication by using the "the off-the-person approach". In this approach, as opposed to common ECG-based biometric systems that collects date by placing sensors on chest area, the ECG were acquired at the fingers with dry Ag/AgCl electrodes, and using a custom ECG sensor which consists of a differential sensor design with virtual ground when subjects were at resting situation. Then features were extracted based on a frequency approach and was based on Odinaka algorithm in which a single heart beat was divided into 64 ms windows, the analysis was performed in the frequency domain, computing the short time Fourier transform for each window. Finally a matching was performed on extracted features to do authentication.

6 The Electrooculogram as a Biometric

There are different types of eye movements like saccade and smooth pursuit which comprise enough information to human authentication, and among them saccade is the most popular and simplest for biometric authentication. According to measurement methods, eye movement signals can be divided into two groups: electrooculographical and videooculographical [2]. In Electrooculography the cornea-retinal potential that exists between the front and the back of the human eye is measured by placing electrodes left and right or top and above eye, and in video oculography the horizontal, vertical and torsional position components of the movements of both eyes are recorded by small cameras. Compared to other bioelectrical signals, fewer researches have been carried out in the field of applying eye oriented bioelectrical signals in human authentication. One of these few researches has been carried out by Abo-Zahhed et al. [15]. They have proposed a new biometric authentication based on the eye blinking waveform and used the Neurosky Mindwave wireless headset to collect the raw eye blinking signal of 25 healthy subjects. The headset is actually for recording EEG signals, but by placing the armed sensor which is made of dry electrode on forehead above the eye; it can be used to measuring EOG signals. Each subject was asked not to do any eye movement, and to make 1–12 eye blinks when signal recording was performing in quiet and normal temperature environment at daylight. The first step was isolating EOG signal from EEG signal through the technique of Empirical Mode Decomposition. Precisely, the raw EEG signal was decomposed into Intrinsic Mode Functions and after analyzing them, it was found that the first two IMFs belonged to EEG and others were related to EOG signals. After this step, eye blinking signal was extracted from EOG signal with the help of its largest amplitude in EOG signal. Then, a certain threshold was adopted to detect the positive and negative peaks of the eye blink. The next step was feature extraction and four groups of features were extracted based on time delineation of the eye blinking waveform and its derivatives "Fig. 5".

Amplitude of positive peak of eye blink, area under positive pulse of eye blink, slope at the onset of positive pulse and position of positive peak of first derivative of eye blinking signal are one sample of each group. To evaluate the performance of system, the proposed system was tested under each four group of features, and based on achieving results, Abo-Zahhed et al. came to conclusion that the group of feature which was including area under positive pulse of eye blink, area under negative pulse of eye blink, energy of the positive pulse of eye blink, energy of the

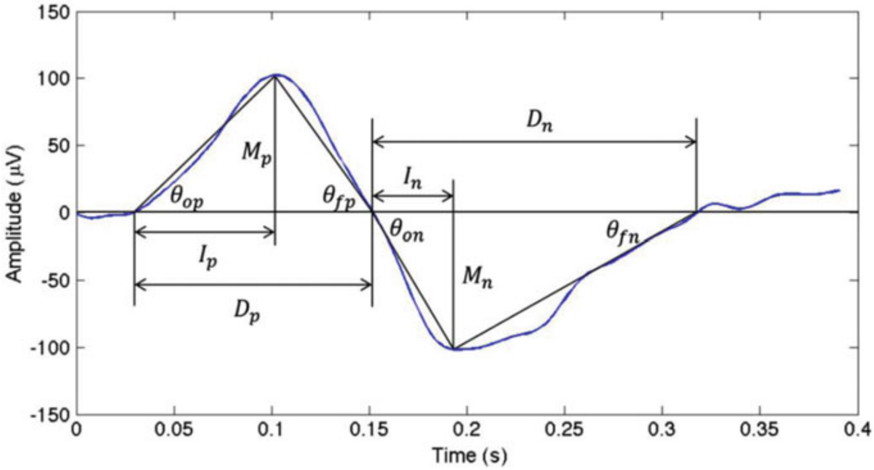

Fig. 5 Features extracted from eye blinking [11]

negative pulse of eye blink, average value of positive pulse of eye blink and average value of negative pulse of eye blink was the best for authentication of the subjects.

Juhola et al. [10] also have introduced a method in which a subject's saccade was applied to authentication. From their point of view, saccades are easy to stimulate and natural while reading or looking at the surroundings all the time. They decreased data for authentication process by using only the saccades parts of eye movements' signals. They asked each subject to sit down at a computer and the computer system had to verify him or her to be or not to be the authenticated subject. The system consisted of a device able to detect a subject's saccades and a program that computed features from saccades. They employed two small video cameras, one for each eye, to follow the pupils of a subject's eyes. Every subject was seated in chair at a fixed location and with the same distance from the stimulation device and was due to look at a small, horizontally jumping target and his or her eye movements were recorded for the authentication purpose. Signals given by this video-oculography system could be typically measured with a low sampling frequency, in this case with 35 Hz. After the recognition of every valid saccade, its amplitude, accuracy, latency and maximum velocity were computed to be used in authentication process "Fig. 6".

Latency is the time difference between the beginnings of the stimulus movement and response, accuracy is equal to the difference of the amplitudes of the stimulation and saccade and to compute the maximum angular velocity, the first derivative was approximated by differentiating an eye movement signal numerically and searching for the maximum velocity during the eye movement. They took these four particularly after having observed how clearly they varied between individuals. In addition, they applied EOG signal to user authentication and although the VOG signals contained less noise than the EOG signals, in most situations the EOG

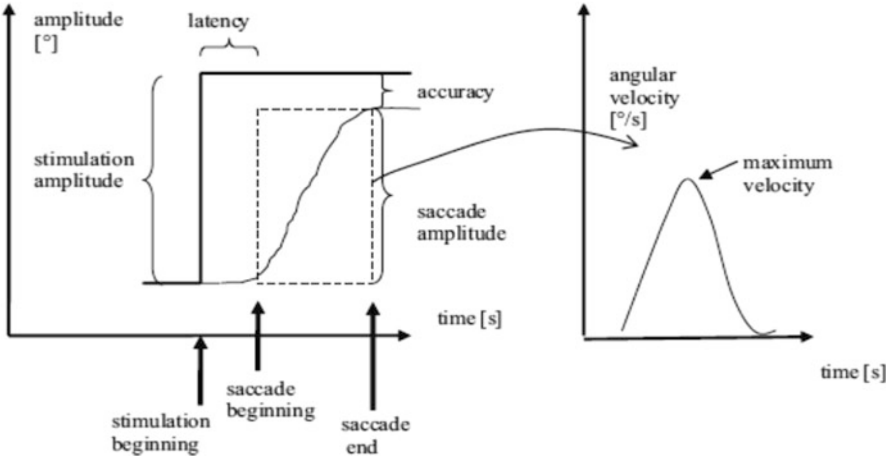

Fig. 6 An ideal saccade as a response to stimulation [11]

measurements achieved better results on the average than the VOG measurements. They supposed that the higher original sampling frequency of the EOG signals leads to better authentication results.

7 Conclusion and Discussion

This article has presented some of researches that have been carried out in the field of applying bioelectrical signals in human authentication. All of these researches agree that each bioelectrical signal has its own confidential physiological features which cannot be stolen and mimic. So, through these highly secured features, bioelectrical signals offer more advantage compared with conventional biometrics like fingerprint or iris for human authentication. But there are some issues and challenges involved in applying bioelectrical signals as biometrics. Firstly, all of mentioned researches have been done under laboratory condition with limited subjects. Therefore, the performance of bioelectrical -signal based authentication system might decline in practical real condition with more subjects secondly, the data acquisition of bioelectrical chest or EEG signals can be recorded by placing some electrodes over the scalp and the placement of electrodes to right position may cause distortion in the recorded signal. So, the data acquisition of bioelectrical signals could be an obstacle in applying these signals to human authentication in non-laboratory condition. Lastly, it should be considered that bioelectrical signals might be dependent to the mental and emotional state of subject. For example, fatigue, alcohol and aging could affect EOG signals, or EEG and ECG signals might vary with stress and anxiety.

References

1. Enderle JD, Bronzino JD (2012) Introduction to biomedical engineering. Academic press
2. Pal A, Gautam AK, Singh YN (2015) Evaluation of bioelectric signals for human recognition. Procedia Comput Sci 41:747–753
3. Van Den Broek EL, Spitters M (2013) Physiological signals: the next generation authentication and identification methods?. In: 2013 European intelligence and security informatics conference (EISIC). IEEE, pp 159–162
4. Singh YN, Singh SK, Ray AK (2012) Bioelectrical signals as emerging biometrics: issues and challenges. ISRN Sig Process 2012
5. Jain AK, Ross AA, Nandakumar K (2011) Introduction to biometrics. Springer Science & Business Media
6. Matsumoto T, Matsumoto H, Yamada K, Hoshino S (2002) Impact of artificial gummy fingers on fingerprint systems. In: electronic imaging 2002. International Society for Optics and Photonics, pp 275–219
7. Roberts C (2007) Biometric attack vectors and defences. Comput Secur 26(1):14–25
8. Hadjileontiadis LJ (2006) Biosignals and compression standards. In: M-Health. Springer US, pp 277–292
9. Dey M, Dey N, Mahata SK, Chakraborty S, Acharjee S, Das A (2014) Electrocardiogram feature based inter-human biometric authentication system. In: 2014 international conference on electronic systems, signal processing and computing technologies (ICESC). IEEE, pp 355–354
10. Gui Q, Jin Z, Xu W (2014) Exploring EEG-based biometrics for user identification and authentication. In: 2014 IEEE signal processing in medicine and biology symposium (SPMB). IEEE, pp 1–6
11. Nakanishi I, Baba S, Miyamoto C (2009) EEG based biometric authentication using new spectral features. In: International symposium on intelligent signal processing and communication systems, 2009. ISPACS 2009. IEEE, pp 651–654
12. Liu S, Bai Y, Liu J, Qi H, Li P, Zhao X, … Li Q (2014) Individual feature extraction and identification on EEG signals in relax and visual evoked tasks. In: Biomedical informatics and technology. Springer, Berlin, Heidelberg, pp 355–311
13. Israel SA, Irvine JM, Cheng A, Wiederhold MD, Wiederhold BK (2000) ECG to identify individuals. Pattern Recogn 31(1):133–142
14. Matos A C, Lourenço A, Nascimento J (2014) Embedded system for individual recognition based on ECG biometrics. Procedia Technol 17:265–272
15. Abo-Zahhad M, Ahmed SM, Abbas SN (2015) A novel biometric approach for human identification and verification using eye blinking signal. Signal Process Lett IEEE 22(7): 176–115