Survey of EEG-based biometric authentication

Conference Paper · January 2018

DOI: 10.1109/ICAwST.2017.8256471

3 authors:

Isuru Jayarathne
The University of Aizu
3 PUBLICATIONS **9** CITATIONS
SEE PROFILE

Michael Cohen
The University of Aizu
169 PUBLICATIONS **820** CITATIONS
SEE PROFILE

Senaka Amarakeerthi
University of Sri Jayewardenepura
20 PUBLICATIONS **24** CITATIONS
SEE PROFILE

2017 IEEE 8th International Conference on Awareness Science and Technology (iCAST 2017)

Survey of EEG-Based Biometric Authentication

Isuru Jayarathne & Michael Cohen
Spatial Media Group
University of Aizu
Aizu-Wakamatsu, Fukushima 965-8580; Japan
E·mail: {d8191101, mcohen}@u-aizu.ac.jp

Senaka Amarakeerthi
Faculty of Technology
University of Sri Jayewardenepura
Gangodawila, Nugegoda; Sri Lanka
E·mail: senaka@sjp.ac.lk

***Abstract*—User authentication systems based on EEG (electroencephalography) is currently popular, marking an inflection point in the field. Recently, the scientific community has been making tremendous attempts towards perceiving uniqueness of brain signal patterns. Several types of methodical approaches have been proposed and prototyped to analyze EEG data with various signal-processing methods and pattern-recognition algorithms. Even though there are many stimulation methods to produce reasonable distinctiveness between subjects, optimization and lowering task complexity are still desirable from techno-economic points of view. With recent technological advancement of EEG signal capturing devices, the process is getting comparatively simpler as devices are capable of providing better portability with reduced calibration time. However, most detailed analysis suggests that a minimal number of most appropriate channels should be selected for better results, even if a system is equipped with the most advanced hardware. Researchers are now focusing on implementing computationally low cost systems with better accuracy, regardless of complexity of the tasks. This paper is a review of several approaches, providing an overview of crucial design considerations in handling EEG data for extended accuracy and practical applicability to authentication.**

***Index Terms*—EEG, biometrics, pattern-recognition.**

I. Introduction

A security system is a prominent method of providing a form of protection for any kind of asset. Most security systems have a sequential process to achieve better protection. Authentication is a part of such sequential processes, verifying that a user has privilege to access a system. There are several types of methods used, including knowledge, possessions, and biometric attributes. The knowledge can be described as "something you know," such as a user name and password pair. Possessions refers to "something you have," such as smart cards, RFID tags, certificates, etc. Biometrics can be described as encoding "something you are," such as fingerprints, palm-prints, retina scans, voice profiles, etc. representations [1]. Compared with other methods, biometric authentication provides better reliability, mobility, and more effortless use.

Authentication systems currently in use have several vulnerabilities. As an example, physical devices such as smart cards, RFID tags, dongles, etc. can be stolen, misplaced, misused, or damaged. On the other hand, conventional authentication methods, which involve knowledge such as username and password, can also be penetrated by coercion, besides credentials being vulnerable to being stolen, disfigured, or forgotten. Even though biometrics cannot be stolen, some systems can be easily misled with forgery or fake replicas. Also, some protection procedures can be overridden by spoofing and forcing. Fingerprints and palm-prints can be duplicated, and iris scans can be tricked by high resolution images. Such weaknesses suggest how conventional security systems become vulnerable, even with simple attack tactics, and such considerations highlight the importance of considering new strategies which can prevent unauthorized parties from entering a system.

With state of art of signal processing and machine learning techniques, researchers are exploring novel styles of authentication using electroencephalography (EEG). EEG is a robust biometric trait, and EEG-based authentication is safer than older techniques. This paper mainly reviews four EEG authentication studies. Additionally, several other studies are briefly discussed, comparing results and indicating out the most sensitive and important design considerations, which have heavy interdependence with accuracy and user-friendliness.

II. User Identification vs. Authentication

Ever since information started to be recorded and processed in digital form, in fields such as health care, finance, education, and government, Securing information systems has been vital. A so-called CIA triad (confidentiality, integrity, availability) model guides polices for information security [2]. Contemporary information systems use various kinds of security methods. Every security method includes an authentication process. Identification is the process of presenting an identity to a system, and authentication can be described as the validation of such identity. For such validation process, as mentioned above, some evidence should be provided [3], such as knowledge, possession, or biometric attributes.

III. Electroencephalography

There are various techniques designed for capturing brain activity, including Magnetencephalography (MEG), Functional Magnetic Resonance Imaging (fMRI), Near-Infrared Spectroscopy (NIRS) [4], Positron Emission Tomography (PET), and Electroencephalography (EEG) [5]. EEG is an electrophysiological monitoring method to record dynamics of electrical activity of a human brain. Unlike other techniques, EEG is not terribly expensive, and is non-invasive and allows completely passive recording.

Lately, EEG has become popular among researchers because of recent technological advances of EEG signal capturing de-

TABLE I
CONSUMER-GRADE WIRELESS HEADSETS FOR EEG DATA CAPTURE

Device name	Channels	Electrode
NeuroSky Mindwave	1	Dry
Muse	2	Dry
EMOTIV Insight	5	Dry
EMOTIV Epoc+	14	Wet
OpenBCI	16	Dry
mBrainTrain	24	Wet
ENOBIO 32	32	Dry
Cognionics Mobile-72	64	Dry

vices. Compared to other brain experimentation devices, EEG devices are reasonably priced and feature ease of calibration and use. Unlike most of the brain signal capture techniques mentioned above, specialized medical knowledge is not required to use EEG devices. Table I lists some consumer-grade wireless EEG acquisition devices [6]. The most important specifications of such a device are the number of electrode channels, electrode type, brain lobes covered, calibration time, portability, and customizability. For best results and for the sake of convenience, a device should be selected based on the particular application as well as affordability.

International standards have been established for electrode placement on the skull of the human brain. Jasper et al. proposed [7] the 10-20 system for the capture of EEG signals. An extension of the 10-20 system, the so-called 10% system or 10-10 system, was proposed by Chatrian et al. [8]. Oostenveld et al. proposed [9] the 10-5 system for high resolution EEG signal acquisition. The devices in Table I are designed according to these international electrode placement standards and conventions.

EEG signals are normally described in terms of rhythmic activity of brain waves. The amplitudes and frequencies of signals change from one state to another. Five major frequency bands have been identified. In increasing order of frequency, they are called delta (δ), theta (θ), alpha (α), beta (β), and gamma (γ). Table II describes the frequency bands and related brain states [10]. Frequency band or bands are experimentally chosen according to which brain state is being explored.

EEG signals can be contaminated by other electrobiological signals, such as those captured by an electrocardiogram (ECG/EKG) generated in the heart, electromyogram (EMG) signals generated in muscles, or electro-oculogram (EOG) signals generated by eye movements [5]. Since EEG recording devices are highly sensitive, captured EEG signals may be corrupted with 50 or 60 Hz AC power line “hum” interference. However, line noise is normally not a problem because considered frequencies usually lie below 50 Hz.

TABLE II
FREQUENCY BANDS AND CORRESPONDING BRAIN STATES

Identifier	Frequency band (Hz)	Brain state
Delta, δ	$1-4$	Primarily associated with deep sleep.
Theta, θ	$4-8$	Appear as consciousness slips towards drowsiness.
Alpha, α	$8-13$	Usually found over the occipital region. Indicates relaxed awareness without attention.
Beta, β	$13-30$	Associated with active thinking and concentration.
Gamma, γ	$30-100$	Represent binding of different populations of neurons.

IV. EEG FOR USER AUTHENTICATION

As noted above, biometric traits are more reliable and easier to use in authentication systems compared to other methods. Passwords, smart cards, and RFID tags can be forgotten or stolen. Even though biometrics can overcome such problems, conventional biometrics can be misused by coercion. However, using EEG as a biometric trait has many potential advantages over traditional biometrics:

- A predefined brain state which authenticates a system is impossible to evoke by insistence or coercion.
- No non-living brain can produce an EEG, which prevents breaching an authentication system by assassinating a user.
- Even though most other biometric traits are visible, EEG biometrics are invisible, making them uncapturable by other parties [11].
- If a brain state is selected for authentication, it can be suppressed by a user in coercion situations [12].

Therefore, this kind of authentication system provides protection not only for the asset, but also for users. An EEG-based biometric satisfies the requirements of universality, uniqueness, permanency, collectability, performance, acceptability, and robustness to be accepted as a authentication method [13].

Generally, EEG-based authentication studies include several common steps, such as data capture, pre-processing, feature extraction, and classification or pattern recognition. Also, accuracy of any system depends on several parameters, such as complexity of task, number of electrodes, electrode type, features, and classification algorithms. In practice, task complexity, preparation time, and processing time should be reduced to ensure user-friendliness of a system.

978-1-5386-2965-9/17/$31.00 © 2017 IEEE

V. Selected EEG-Based Biometric Authentication Studies

In this section, we highlight four studies representation of this research area, selected partly because of their successfullness as measured by reported accuracy.

A. ERP → CC

Ruiz-Blondet et al. [11] introduced a protocol called CEREBRE, which uses EEG signals to authenticate a user. 400 images— 100 sine gratings, 100 low frequency words, 100 images of foods, and 100 celebrity faces— were used as stimuli. Among those categories, an oddball stimuli category also was included to further evolve the sought EEG pattern. The experiment was performed with 50 participants. Brainvision Brainamp DC with 26 EEG electrodes and 3 EOG electrodes was used to acquire data at 500 Hz sampling rate. Event-Related Potentials (ERP) were filtered with a band-pass filter (1–55 Hz), and a simple discriminant function based on normalized cross-correlation was used for classification.

Results confirm that, visual tasks activate middle occipital electrodes. Both maximal (all channels, all classifiers) and minimal (3 channels, 4 categories) classifiers showed 100% accuracy, but the minimal classifier showed maximum accuracy when all the trials were used. The results indicate that the single-stimulus classifiers based on food and oddball stimuli are the most accurate. Identity classification based on resting state EEG has shown extremely poor performance. Authentication based on memory recall task (which some studies call "pass-thoughts") also showed poor performance, due to the variable time taken to think. This study indicates that up to at least 6 months, ERP biometric identification does not significantly degrade.

B. PSD & COH → Mahalanobis distance & match-score fusion

La Rocca et al. [14] suggested a method for finding distinctiveness based on EEG spectral coherence connectivity. The basic idea is to use the information exchanged between different areas of the brain to establish distinctiveness. The proposed method was tested with a data set collected from 108 subjects during eyes-closed and -open resting state conditions. EEG data was recorded using a 64-channel system with sampling rate of 160 Hz. Data was down-sampled to 100 Hz and extracted up to 50 Hz using an anti-aliasing low-pass filter. Power spectral density (PSD) and spectral coherence (COH) analysis methods were used to extract spectral features. PSD is the frequency response of a random or periodic signal, indicating average power distributed as a function of frequency. COH quantifies the level of synchrony between two stationary signals at specific frequencies. Mahalanobis distance-based classifiers and match-score fusion algorithms were used separately to calculate distinctiveness. This analysis was done over three different brain macro-areas (F: frontal, C: central, P: parieto-occipital).

The single element classifier with PSD eyes closed data showed 90.49% accuracy for the P zone. The match-score fusion algorithm showed 100% accuracy for COH features of eyes-closed data in all zones and eyes-open in only the frontal zone. This method is robust and highly accurate for identifying people. Even though match-score fusion with COH features shows better accuracy, COH requires EEG signals to be (quasi)stationary, and analysis takes around 20 min. to process. On conventional hardware, classification performance may not perform well with a large number of subjects (> 100).

C. CC → LDA

Chen et al. [12] proposed an authentication system based on rapid serial visual presentation (RSVP) stimuli. 29 participants were recruited, and the BrainAmp amplifier was used to acquire EEG signals. Data collection was performed with both wet and dry electrodes separately. A set of three symbols was used as targets, and users were instructed to count the instances among a stream of randomly generated trials. 600 trials, consisting of 72 targets and 528 non-targets, were conducted to collect EEG data. The significant features were calculated by point-biserial correlation coefficients. Correlations were transformed into z-scores for each subject using Fisher's transformation. Regularized linear discriminant analysis was used to perform classification of ERP components.

In single trial classification scenarios, average accuracy for 28- and 16-channel wet configurations were 87.8% and 85.9%, and for the 16-channel dry configuration, it was 78.2%. Both wet and dry electrode setups showed 100% accuracy with 10.7 s and 27.0 s average login times respectively with more trials. According to this study, knowledge-based methods (introduced in the study) can successfully be adjusted to any true acceptance rate (TAR) level according to required security level. Low level of TAR reduces the time taken for a login process. After the system has been trained for a new password, no positive response is shown for the older one. The authors note that a password can be successfully hidden in coercion situations. However, the need for data calibration for each subject limits the scope of applicability.

D. Cosine similarity → LDA

Chuang et al. [15] performed a task-wise method comparison to determine the best performing approach in terms of usability and security. 15 subjects were recruited and the NeuroSky MindSet (later replaced by MindWave) was used to acquire data. The EEG headset has a single channel placed on the frontal polar (Fp1) area on the head. Seven tasks were performed, including breathing, simulated finger movement, sport activity, singing/passage recitation, audio listing, color identification, and pass-thought. A questionnaire was administered to check user friendliness of the tasks. Only alpha and beta frequency bands were extracted, and signals were flattened in the time domain to simplify the data into a single dimension. Cosine similarity of the vector representation was used to quantify similarity between pairs of signals. Similarities of signals within each subject and between different subjects were checked. The k-nearest Neighbour (k-NN) algorithm was used for classification.

978-1-5386-2965-9/17/$31.00 © 2017 IEEE

Audio, sport, and color tasks showed the best classification accuracies. However, the proposed method showed 99% accuracy using custom task and custom acceptance thresholds for each subject. According to results of the questionnaire, the pass-thought task was the most difficult to perform, and breathing, audio, and color tasks were the easiest. This study concluded that it is possible to achieve high accuracy even with appealing user friendliness.

E. Other

Besides the studies discussed above, Table III summarizes some other studies with achieved accuracy and other characteristics. Generally, accuracy of each system depends highly on these aspects. Even if it is very hard to quantify simplicity of tasks, relaxation is perhaps the simplest. Even though complex tasks give better accuracy, relaxation is easiest for users. Selected studies have different kinds of attributes, such as different task(s), different numbers of channels, and different algorithms to achieve better accuracy. Change of accuracy according to these parameters is noted by this table. Palaniappan [16] and Ashby et al. [17] determined that combination of several tasks increases accuracy by analyzing across different numbers of task combinations. Riera et al. [18] proposed an authentication system using combination of EEG and ECG signals. Changes of the ECG signals when one is in a coercion situation can be advantageous for discriminating the situation. Even if the task is relaxation, this study achieves higher accuracy than other studies which used same the task because of the additional ECG channel. According to the method proposed by Jayarathne et al. [19], it is possible to authenticate a person by having them think of a particular number. Compared to tasks used in other studies, such an imagining task makes it easy to perform anywhere. Unlike other studies, Yeom et al. [20] proposed a approach to evoke unique EEG pattern using self- and non-self face images. EEG patterns must be unique because each subject has their own idiosyncratic response to self-face.

VI. Discussion

The experimental conclusions reviewed above further emphasize the notion that EEG signals can be used to implement robust authentication systems. However, the best method is still not obvious, since it depends on the required security level and user friendliness. The parameters should be carefully engineered to implement a fairly good EEG-based authentication system, as detailed below.

A. Task simplicity or complexity

Most of the studies surveyed reported that more robustness and high accuracy can be achieved with higher task complexities [11][12][17], but higher task complexities make a system less usable, because both authentication and system training are highly time-consuming, which compromises an important property of good authentication systems.

B. Number of channels and electrode type

As mentioned earlier, both consumer- and clinical-grade headsets are used in this kind of research. Some studies especially focus on accuracy changing against the number of channels used [11]. Even though the number of channels has less impact on accuracy, in case security is significantly prioritized, a large number of channels ensures extra protection. Fewer channels can be processed at reduced computational power and provides extra user-friendliness [15]. Chen et al. [12] reported that wet electrodes generally have better signal quality compared to dry ones, but calibration time is higher.

C. Number of subjects and trials

Using more data points increases accuracy of classification algorithms. Chen et al. [12] confirmed that by performing single- and multi-trial classification. According to the La Rocca et al. [14] classifications, using fewer subjects provides better accuracy than considering more subjects, as similar subjects can be found in a large set. Therefore, systems which show fairly good accuracies with fewer numbers of subjects may not represent a robust solution for larger populations, as there is increased risk of hacking the system. Yeom et al. [20] proposed performing subject-specific stimulation to overcome such problems.

D. Computational cost

Generally, computational cost depends on several factors, including feature-extraction algorithms, machine learning or pattern recognition algorithms, task complexity, and number of channels. Combination of several extracted features can increase accuracy even if the classification takes a long time to process. Methods can be selected according to requirements of the system.

E. Stability of EEG patterns over time

Some EEG signal patterns for specific stimuli can change over time. In particular, accuracy of systems trained by preference-based tasks [11] can degrade as user tastes change. Some studies [22] collected data over a long period of time to confirm persistence. In practical situations, training such a system is laborious, since training data must be collected for a considerable time period to ensure the permanency.

F. Changeability of EEG-based biometrics

Conventional biometrics cannot be changed because they are fixed attributes of humans, but username-password system credentials can be changed. However, EEG-based biometrics can be used either way. Suggested tasks of most studies assume changeable brain activities. Even though an EEG signal pattern differs from person to person, the task can be changed to ensure protection of an asset [11]. The proposed system of Yeom et al. [20] mentioned above cannot be changed because it uses subject-specific stimulation.

978-1-5386-2965-9/17/$31.00 © 2017 IEEE

TABLE III
SUMMARY OF VARIOUS STUDIES (IN DECREASING ORDER OF ACCURACY)

Author(s)	Channels	No. of Subjects	Task	Derived or Extracted Features	Classifier	Avg. accuracy
Ruiz-Blondet et al. [11]	3	50	visual stimulation of 400 images	Event-Related Potentials (ERP)	normalized cross-correlation	100%
La Rocca et al. [14]	64	108	relaxation with opened eyes and closed eyes	Power Spectral Density (PSD), Spectral Coherence (COH)	Mahalanobis distance-based classifier and match-score fusion	100%
Chen et al. [12]	16	29	Rapid Serial Visual Representation (RSVP)	point-biserial correlation coefficients, Fisher's transformation	Linear Discriminant Analysis (LDA)	100%
Palaniappan [16]	6	6	5 tasks: relaxation, math activity, geometric figure rotation, mental letter composition, visual countings	Auto-regressive coefficients (AR), Spectral Power (SP), Inter-Hemispheric Power Difference (IHPD), Inter-Hemispheric Linear Complexity (IHLC)	LDA	100%
Ashby et al. [17]	14	5	4 tasks: relaxation, limb movement, visual counting, geometric figure rotation	AR, SP, IHPD, IHLC, PSD	Support Vector Machine (SVM)	100%
Chuang et al. [15]	1	15	7 tasks: breathing, simulated finger movement, sport activity, singing/passage recitation, audio listing, color identification, and pass-thought	Cosine similarity of the vector representation	k-Nearest Neighbour (k-NN)	99%
Palaniappan et al. [21]	61	20	drawings of common objects as visual stimulation	multiple signal classification (MUSIC)	k-NN, Elman Neural Network (ENN)	98%
Riera et al. [18]	4	-	relaxation	AR, Fast Fourier Transform (FFT), mutual information, coherence, cross correlation (EEG and ECG data)	Fisher Discriminant Analysis (FDA)	98%
Jayarathne et al. [19]	14	12	imagining four digit number as cognitive task	Common Spatial Patterns (CSP)	LDA	97%
Riera et al. [22]	2	51	relaxation with closed eyes	Higuchi fractal dimension, entropy, skewness, standard deviation, AR	LDA	97%
Liew et al. [23]	8	10	apprehension of images as visual stimulation	coherence, cross-correlation, mean amplitude	Fuzzy-Rough Nearest Neighbour (FRNN)	92%
Yeom et al. [20]	18	10	apprehension of images of faces including self-face as visual stimulation	difference of average signals, positive/negative peaks at specific latencies	non-linear SVM classifier	86.1%
Poulos et al. [24]	2	4	relaxation with closed eyes	spectral features	Learning Vector Quantization (LVQ)	80%–100%

VII. CONCLUSION

EEG signals contain discriminative information which is stable across time, and research surveyed here shows high accuracy for various approaches. Better discriminative features, including characteristics considered by all the systems detailed in §V and most of those in Table III, are mostly found in the time-domain as opposed to frequency-domain analysis. Even simple pattern recognition algorithms can be used to distinguish among users. Deep learning techniques need too much data to be deployed for such applications of EEG characterization and discrimination. EEG-based authentication systems should be designed by tuning above-discussed parameters according to desired security and usability levels. Even though some studies confirmed that significant changes don't happen for some period of time even as personal taste evolves, long-term behaviors of EEG signal patterns have yet to be characterized.

Especially considering increased population of twins or triplets with IVF (in vitro fertilization), it would be interesting to do such experiments on identical (monozygotic) twins. Since such siblings might be expected to have similar thought processes, confusable responses to non-specific tasks such as relaxation coved disrupt authentication.

978-1-5386-2965-9/17/$31.00 © 2017 IEEE

References

[1] J. Harper, *Identity Crisis: How identification is overused and misunderstood*. Cato Institute, 2006.

[2] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Cengage Learning, 2011.

[3] G. Doe, "Difference Between Identification & Authentication," http://itstillworks.com/difference-between-identification-authentication-3471.html, [Online; accessed 26-June-2017].

[4] F. F. Jobsis, "Noninvasive, infrared monitoring of cerebral and myocardial oxygen sufficiency and circulatory parameters," *Science*, vol. 198, no. 4323, pp. 1264–1267, 1977.

[5] IMOTIONS, *EEG Pocket Guide*. IMOTIONS, 2016.

[6] B. Farnsworth, "Top 14 EEG Hardware Companies [Ranked]," https://imotions.com/blog/top-14-eeg-hardware-companies-ranked/, [Online; accessed 28-June-2017].

[7] H. H. Jasper, "The ten twenty electrode system of the international federation," *Electroencephalography and Clinical Neurophysiology*, vol. 10, pp. 371–375, 1958.

[8] G.-E. Chatrian, E. Lettich, and P. L. Nelson, "Modified Nomenclature for the" 10%" Electrode System1." *J. of Clinical Neurophysiology*, vol. 5, no. 2, pp. 183–186, 1988.

[9] R. Oostenveld and P. Praamstra, "The five percent electrode system for high-resolution EEG and ERP measurements," *Clinical Neurophysiology*, vol. 112, no. 4, pp. 713–719, 2001.

[10] S. Sanei and J. A. Chambers, *EEG Signal Processing*. John Wiley & Sons, 2013.

[11] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "CEREBRE: A novel method for very high accuracy event-related potential biometric identification," *IEEE Trans. on Information Forensics and Security*, vol. 11, no. 7, pp. 1618–1629, 2016.

[12] Y. Chen, A. D. Atnafu, I. Schlattner, W. T. Weldtsadik, M.-C. Roh, H. J. Kim, S.-W. Lee, B. Blankertz, and S. Fazli, "A high-security EEG-based login system with RSVP stimuli and dry electrodes," *IEEE Trans. on Information Forensics and Security*, vol. 11, no. 12, pp. 2635–2647, 2016.

[13] A. Almehmadi and K. El-Khatib, "The state of the art in electroencephalogram and access control," *ICCIT: Proc. 3rd Int. Conf. on Communications and Information Technology, 2013*, pp. 49–54.

[14] D. La Rocca, P. Campisi, B. Vegso, P. Cserti, G. Kozmann, F. Babiloni, and F. D. V. Fallani, "Human brain distinctiveness based on EEG spectral coherence connectivity," *IEEE Trans. on Biomedical Engineering*, vol. 61, no. 9, pp. 2406–2412, 2014.

[15] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I think, therefore I am: Usability and security of authentication using brainwaves," in *Proc. Int. Conf. on Financial Cryptography and Data Security*. Springer, 2013, pp. 1–16.

[16] R. Palaniappan, "Electroencephalogram signals from imagined activities: A novel biometric identifier for a small population," in *Proc. Int. Conf. on Intelligent Data Engineering and Automated Learning*. Springer, 2006, pp. 604–611.

[17] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, "Low-Cost Electroencephalogram (EEG)-Based Authentication," in *NER: Proc. 5th Int. IEEE/EMBS Conf. on Neural Engineering*, 2011, pp. 442–445.

[18] A. Riera, S. Dunne, I. Cester, and G. Ruffini, "STARFAST: A wireless wearable EEG/ECG biometric system based on the ENOBIO sensor," in *Proc. Int. Workshop on Wearable Micro and Nanosystems for Personalised Health*, 2008.

[19] I. Jayarathne, M. Cohen, and S. Amarakeerthi, "BrainID: Development of an EEG-based biometric authentication system," in *IEMCON: Proc. Information Technology, Electronics and Mobile Communication Conf.* IEEE, 2016, pp. 1–6.

[20] S.-K. Yeom, H.-I. Suk, and S.-W. Lee, "Person authentication from neural activity of face-specific visual self-representation," *Pattern Recognition*, vol. 46, no. 4, pp. 1159–1169, 2013.

[21] R. Palaniappan and D. P. Mandic, "Biometrics from brain electrical activity: A machine learning approach," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 738–742, 2007.

[22] A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini, "Unobtrusive biometric system based on electroencephalogram analysis," *EURASIP J. on Advances in Signal Processing*, vol. 2008, p. 18, 2008.

[23] S.-H. Liew, Y.-H. Choo, Y. F. Low, and Z. I. M. Yusoh, "Identifying Visual Evoked Potential (VEP) Electrodes Setting for Person Authentication," *Int. J. Adv. Soft Comput. Appl.*, vol. 7, no. 3, pp. 85–99, 2015.

[24] M. Poulos, M. Rangoussi, and N. Alexandris, "Neural network based person identification using EEG features," in *Proc. Int. Conf. on Acoustics, Speech, and Signal Processing*, vol. 2. IEEE, 1999, pp. 1117–1120.

978-1-5386-2965-9/17/$31.00 © 2017 IEEE