Journal of Physics: Conference
Series

PAPER • OPEN ACCESS

The Wavelet packet decomposition features applied in EEG based authentication system

The Wavelet packet decomposition features applied in EEG based authentication system

Fatin Atiqah Rosli[1], A. Saidatul[2], Azian Azamimi Abdullah[3], Roy Francis Navea[4]

[1,2,3] Biomechanics, Signals and Modeling Cluster, Sport Engineering Research Centre (SERC), Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP) Arau, Perlis, Malaysia.
[4]Department of Electronics and Communications Engineering, John Gokingweig Jr. College of Engineering De La Salle University, Manila, Philippines

[1]fatinatiqah@studentmail.unimap.edu.my, [2]saidatul@unimap.edu.my

Abstract. Biometric authentication is recently used for verification someone's identity according to their physiological and behavioural characteristics. The most popular biometric techniques are fingerprints, facial and voices recognition. However, these techniques have disadvantage in which it can be easily to be imitated and mimicked by hackers to access a device or a system. Therefore, this study proposed electroencephalogram (EEG) as a biometric technique to encounter this problem. The wavelet packet decomposition is explored in this study for feature extraction method. The wavelet packet decomposition feature is represented in the average wavelet, root mean squared (RMS) wavelet and power wavelet were selected as features to extract a meaningful information from the original EEG signal based on the visual representation. These features were applied to classify between familiar and unfamiliar image responses (visual representation) and to recognize 13 subjects by using Support Vector Machine (SVM), k-Nearest Neighbor (KNN) and Random Forest (RF). The analysis of the classification between familiar and unfamiliar images responses obtained that gamma frequency (30 – 45 Hz) achieved the highest correct recognition rate (CRR) and KNN obtained the accuracy of 92.8% was obtained with KNN in the classification between familiar and unfamiliar image responses. Using the gamma frequency band, the classification between the EEG responses of the 13 subjects was evaluated using the percentage of false acceptance rate (FAR) and false rejection rate (FRR). From the overall view, the value of FAR is lower than FRR. These values were used in authentication system as threshold for security level. As the result of classification between the subjects, SVM performed better compared as KNN and RF in which the error rate for acceptance of unauthorized person and rejection of authorized person were the lowest.

1. Introduction

Biometric authentication system is a tool usually used in cybersecurity to recognize between a person according to physiological and behavioral characteristics using human features [1]. Human feature also known as biometric trait can be either fingerprints, iris, voices, palms, electrocardiography (ECG), electromyography (EMG) and electroencephalograph (EEG) [2] which have unique ability to differentiate between persons. The biometric authentication recently has becoming popular due to the traditional authentication system such as Personal Identification Number (PIN) and text-based password have disadvantages as it tends to be forgotten and stolen [3] [4]. Therefore, the biometric have been used to improve the authentication system as the biometric trait implemented in the system as an individual recognition to access a server or a device.

This research implemented EEG in biometric authentication because each human holds specific and unique natural characteristics which different person produces different signal, and it is impossible to be imitated and mimicked. Recent studies revealed that EEG is universal and more robust compared to other traits. Development in biometric authentication system involve an advanced technique by capturing EEG signal using EEG devices such as EMOTIV EPOC+, processing the signals and implementing artificial intelligent (AI) to predict a person. Christopher et. al. [5] used Mindwave mobile to capture EEG signal whereas Kaur et. al. [6] used EMOTIVE EPOC+ and performed eyes close activity. In addition, Ong et. al. [7] used EEGO to record EEG by performing visualize image.

Moreover, this research focused on the improvement of feature extraction. The feature extraction is a process dimensionality reduction which minimize a data to be a manageable group of datasets while accurately describing the original data. Therefore, the wavelet packet decomposition (WPD) was applied in this research by improving the feature representation so that WPD can be defined in various way.

This paper is structured as follow: Section 2 reviewed the feature extraction from recent research, Section 3 describes the methodology which include experimental protocol and signal processing, Section 4 shows the experimental result and Section 5 concludes the finding of this research.

2. Literature Review

EEG is a brain signal which captured an electrical activity produced by trillion of neurons in non-invasive way. Early on, the purpose of EEG signal was focused on the diagnostic purposed to detect an abnormality such as epilepsy and schizophrenia and EEG was introduced in 1980 as a biometric trait as user recognition [5][8]. The brain signal produces five main frequency which describe the brain activity: delta, theta, alpha, beta and gamma. Delta (1 – 4 Hz) and theta (4 – 8 Hz) frequency usually present in human sleep condition whereas alpha (8 – 13 Hz), beta (13 – 30 Hz) and gamma (30 – 100 Hz) dominant in human wakeful state.

EEG signals exist in non-linear characteristics because the brain generated the signal in non-linear mechanism. The signal can be represented in time domain and frequency domain to describe the characteristic of signal which can be used as feature extraction. The most popular feature extraction method used by mostly researchers in EEG based authentication is power spectral density (PSD). Ong et. al. [7] applied PSD for alpha, beta, gamma, alpha-beta and alpha-beta-gamma frequency and achieved 89.21% of accuracy by evaluating the classification using K-nearest neighbors (KNN) classifier. Thomas et. al. [9] extracted the average of band power for alpha, beta and gamma and obtained 88.33% of accuracy. Kumar et. al. [10] converted the raw signal into discrete Fourier transform (DFT) for theta, alpha, low beta, high beta and gamma and represented the DFT using mean and standard deviation. Zhang et. al. [11] combined features based on autoregression (AR) model and sample entropy and achieved 99.53% by support vector machine (SVM).

3. Methodology

This research consists of two part of methodology which is the experimental protocol and EEG signal processing. The experimental protocol explained in Section 3.1 and the EEG signal processing discussed in Section 3.2. The flow of methodology constructed in Figure 1.

3.1. The experimental protocol

The experimental protocol was designed to achieve a goal of finding evidence to reveal EEG signal used for authentication system between subjects. This research designed the experimental protocol based on visual representation which familiar and unfamiliar images were exposed to the subjects while the EEG signal was recorded. It is applicable in the authentication procedures of cybersecurity system that could improve the identification accuracy and assist for generalization of the recognition process under a variety of recognition condition in the individual [12].

This research collected EEG signal from 13 healthy subjects (seven females and six males aged between 20 to 30 years old). All subjects were Malaysian, in good health and had not influenced by drugs and alcohol. Before started the experiments, all subjects were requested to fill in the Informed Consent form and a form to gather the familiarity information from the subjects.

The EEG-based authentication in this study is based on the visual stimuli by asked the subjects to watch images. The visual stimuli are composed of familiar and unfamiliar as represented as Set A and Set B in ach of the set performed seven categories includes nickname image (BLOCK A), group of people image (BLOCK B), logo image (BLOCK C), moving image (BLOCK D), object image (BLOCK E), personal image (BLOCK F) and famous image (BLOCK G). The block is separated with rest task in 30 seconds whereas during the pre-experiment and post experiment performed close eye in 60 seconds. The images were exposed 12 images in autonomous manner to the subjects for 60 seconds for each block to reduce interaction between the investigator and the subjects. Therefore, the experiment for one subject took approximately 1440 seconds or 24 minutes and the flow of the experimental protocol as shown in Figure 2.

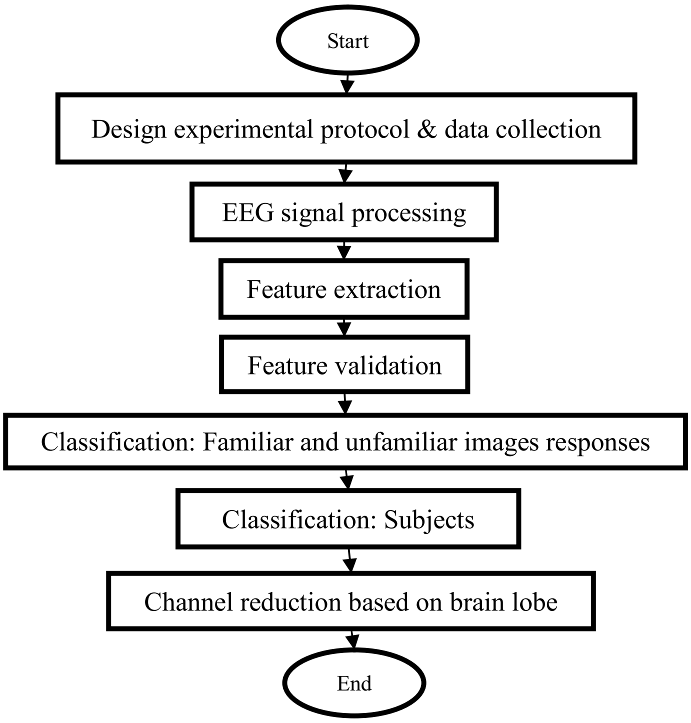
Start
Design experimental protocol & data collection
EEG signal processing
Feature extraction
Feature validation
Classification: Familiar and unfamiliar images responses
Classification: Subjects
Channel reduction based on brain lobe
End

Figure 1. The flow of methodology

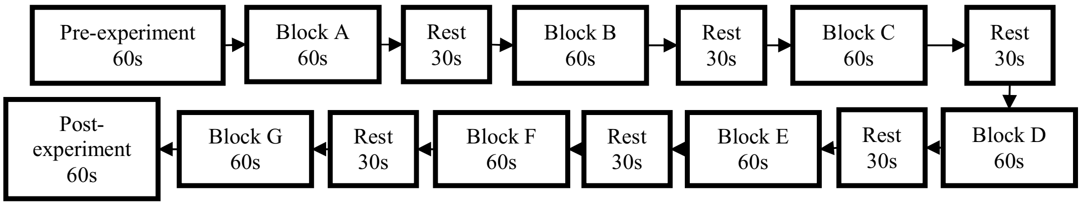

Figure 2. The flow of experimental protocol

The EEG device used in this experiment was EMOTIV EPOC+ with 14 channels (AF3, AF4, F7, F8, F3, F4, FC5, FC6, T7, T8, P7, P8, O1 & O2) as a media to record the EEG signals as follows the international 10/20 electrode location system as shown in Figure 3 (a) and Figure 3 (b).

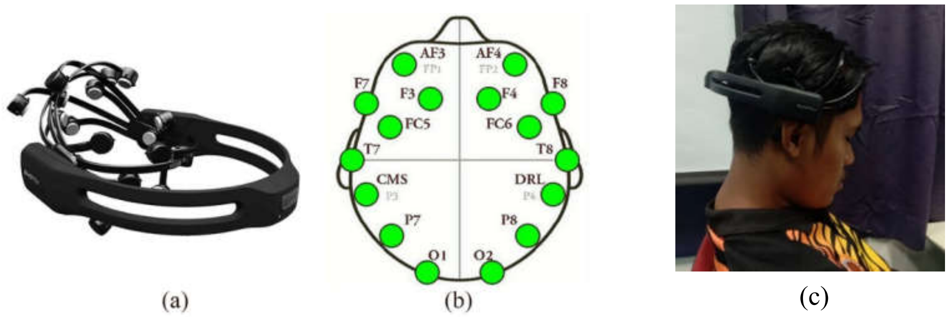

Figure 3. (a) EMOTIV EPOC+ device (b) The electrode placement according to the international 10/20 electrode location system (c) The attachment of EEG device

Table 1. The experimental parameters

Parameters	**Values**
Device	EMOTIV EPOC+
Channels	14 channels (AF3, AF4, F7, F8, F3, F4, FC5, FC6, T7, T8, P7, P8, O1 & O2)
Participants	13 subjects (7 females and 6 males between 20 to 25 years old)
Sampling rate	128 Hz
EEG length data	7 680 x 2 set x 7 category x 13 subjects = 1 397 760
Time Duration	1 440 seconds per subjects

3.2. EGG signal processing

3.2.1. Signal Pre-processing. After collecting the EEG signals, the next step is the EEG signal pre-processing which performed the common average reference (CAR), baseline removal and independent component analysis (ICA) to remove the unwanted artifacts and noise which captured during the experiment session. The pre-processing was applied to extract the meaningful EEG signals because the recorded EEG during the experiment was contaminated by biological noise such as eye movement, eyeblink, tongue movement, and surrounding artifacts.

After the artifacts were removed, was performed to extract four types of brain waves which included all frequency (8 – 45 Hz), alpha (8 – 13 Hz), low beta (13 – 20 Hz), high beta (20 – 30 Hz) and gamma (30 – 45 Hz). Moreover, the EEG signals segmented from 60 seconds into 1 seconds per epoch because the recorded EEG signals were lengthy. As a result, there were 840 epochs for each subject and 10 920 datasets and 14 channels dimensional from 13 subjects (10 920 x 14).

3.2.2. Feature Extraction. The wavelet-based feature possesses well in time and frequency feature localised [13]. The signal is decomposed into 2 sub-space (high and low frequency information) for each level which at the end it will decompose into coefficients as shown in equation (1). The WPD cannot extract single frequency component rather it decomposes into a new resolution of the sub-space. Hence, this research converted the signal into wavelet packet decomposition (WPD) signals with 3 level of decomposition using db4 wavelet function and calculated the average, root means squared (RMS) and power of the signals as the feature representation. Ting et al. [14] were proposed the WPD as feature extraction for brain computer interface (BCI) and revealed that it provides more information and improves the classification performance.

There were three feature representation for the WPD; the average wavelet, RMS wavelet and the power wavelet calculated according to equation (2), (3) and (4) respectively. 14 channels (C=1,2,3, …,14) and the sampling rate for each channel is N (N=128).

$$\text{The decomposition coefficients,} \ \mathrm{d}_{\mathrm{j}}^{\mathrm{n}}(\mathrm{k}) = 2^{\frac{\mathrm{j}}{2}} \ \mathrm{d}^{\mathrm{n}}(2^{\mathrm{j}} - \mathrm{k}) \tag{1}$$

Where j is the level of decomposition, n is the frequency factor and k is the shift factors.

$$The\ average\ wavelet\ = \frac{\sum_k d_j^n(k)}{N} \tag{2}$$

$$The\ RMS\ wavelet\ = \sqrt{\frac{\sum_k d_j^n(k)^{\,2}}{N}} \tag{3}$$

$$The\ Power\ wavelet\ = \frac{\left|d_j^n(k)\right|^2}{N} \tag{4}$$

3.2.3. Classification. The classification is a pattern recognition algorithm which can classify and predict the targets by referring modelling problems using machine learning and deep learning algorithm. The dataset consists of two parameters which the first set is the input, X as indicates the feature set and the second set is the output, T as indicates the targets. Classification can either be a supervised learning or an unsupervised learning method, the supervised learning was used because it requires the output to train the model and provides answers to evaluate the performance of the model. Therefore, this research implemented the supervised learning in conjunction with SVM, Random Forest (tree=250) and k-Nearest Neigbhor (K=7) for the classification between familiar and unfamiliar images responses and predict between the 13 subjects.

3.2.4. Performance Metric. The performance of the classification model was assessed by the performance metrics because it is crucial to compare the quality of each model. The performance of classification between the familiar and unfamiliar image responses of EEG and the classification between the subjects evaluated using accuracy and error rate in percentages. A 10-fold cross validation was used to check the validity response of each model.

The operation in a basic authentication system is involves three operational modes which is registration/enrollment mode, verification mode and identification mode respectively. The flow of the operational mode shows in Table 2. Thus, this research developed a verification mode in authentication system through familiar and unfamiliar images responses while the identification mode utilized in order to recognize between the subjects. These modes are assisted by machine learning algorithm and the performance of the classification between familiar and unfamiliar image response was evaluated by correct recognition rate (CRR) in verification mode whereas the classification between the subjects in identification mode evaluated by false acceptance rate (FAR) and false rejection rate (FRR). The definition of FAR and FRR is the result of error rate in biometric measurements in which unauthorized person are incorrectly accepted and authorized person are incorrectly rejected respectively [15].

Table 2. The operational mode in basic authentication system

MODE	EXPLANATION
Registration/ enrollment	Build a biometric template by capturing the sample data during data collection and stored in a database
Verification	Capture a new data and compare to the biometric template
Identification	The compared data find the individual which produces the biometric template in the database

$$Correct\ Recognition\ Rate\ (CRR)\ = \frac{No.of\ correct\ prediction}{Total\ of\ the\ overall\ samples} \times 100 \tag{5}$$

$$False\ Acceptance\ Rate\ (FAR)\ = \frac{False\ Positive}{False\ Positive + True\ Negative} \times 100 \tag{6}$$

$$False\ Rejection\ Rate\ (FRR)\ = \frac{False\ Negative}{False\ Negative + True\ Positive} \times 100 \qquad (7)$$

4. Experimental Result

This research explored the wavelet-based feature used for feature extraction and the performance of the features evaluated by using SVM, RF and KNN classifiers.

4.1. Performance evaluation according to the classification between familiar and unfamiliar images response (Verification mode)

The classification between familiar and unfamiliar images response developed in verification mode was determined by classification method using SVM, RF and KNN and determined the most informative frequency between alpha, low beta, high beta and gamma obtained using WPD features.

Table 3 shows all the WPD features obtained above 80% of CRR for three WPD features and found that gamma is the most informative frequency. Therefore, the next analysis has been done by using gamma frequency. In addition, KNN (92.8%, 92.1%, 91.8%) performed better than SVM (90.9%, 91.4%, 90.9%) and RF (88.9%, 86.3%, 86.6%) in verification mode. At the same time, the average wavelet also achieved slightly higher CRR compared to the power wavelet and RMS wavelet.

Table 3. The average CRR for three classification between familiar and unfamiliar image response.

	Accuracy (%)											
	Average Wavelet				**RMS Wavelet**				**Power Wavelet**			
	α	Lβ	Hβ	γ	α	Lβ	Hβ	γ	α	Lβ	Hβ	γ
SVM	86.4	87.1	90.2	**90.9**	86.3	87.4	90.0	**91.4**	86.2	86.9	88.3	**90.9**
RF	81.9	82.9	86.9	**88.9**	80.90	82.1	86.0	**86.3**	80.7	82.0	85.3	**86.4**
KNN	85.3	88.6	91.0	**92.8**	85.9	88.3	90.9	**92.1**	85.4	87.6	89.1	**91.8**

4.2. Performance evaluation according to the classification between subjects (Identification mode)

The classification between the subjects developed in identification mode was determined by classification method using SVM, RF and KNN and using gamma.

Table 4 to Table 6 shows that all classifiers succeeded to recognize the responses of the 13 subjects. From overall view, the FAR is lower than FRR as refers to the theory of basic authentication as if the higher security the more the FRR and the less the FAR [15]. In order to develop convenience and more user friendly, the threshold of FAR and FRR must be set to optimum in which if the threshold FAR is reduced to the lowest possible level, the FRR is likely rise sharply (more secure but less convenience) and vice versa. In the practical system, it is impossible for FAR and FRR reach an ideal level. From the results, the optimum level of threshold will be set in the future to develop more robust EEG based authentication system.

Table 4. FAR and FRR for the classification between subjects using SVM

Support Vector Machines
FAR (%) & FRR (%)

	001	**002**	**003**	**004**	**005**	**006**	**007**	**008**	**009**	**010**	**011**	**012**	**013**
Average	0.09	0.07	0.09	0.12	0.13	0.10	0.26	0.89	0.70	0.20	0.44	0.43	0.09
Wavelet	0.84	2.80	2.81	0.84	2.71	1.43	0.73	9.64	4.35	3.30	5.56	4.78	9.46
RMS	0.09	0.04	0.10	0.21	0.13	0.12	0.25	0.98	0.76	0.21	0.55	0.48	0.66
Wavelet	0.60	2.90	2.92	1.68	3.05	1.66	0.97	11.7	5.22	3.65	5.08	5.26	11.0
Power	0.12	0.04	0.16	0.24	0.12	0.12	0.30	1.23	0.89	0.27	0.56	0.52	0.78
Wavelet	1.31	3.01	3.06	6.10	3.16	2.13	0.86	11.7	5.78	4.13	6.22	4.37	13.1

Table 5. FAR and FRR for the classification between subjects using RF

Random Forrest
FAR (%) & FRR (%)

	001	**002**	**003**	**004**	**005**	**006**	**007**	**008**	**009**	**010**	**011**	**012**	**013**
Average	0.53	0.40	0.36	0.65	0.38	0.36	0.50	1.52	1.74	0.55	0.10	0.90	1.21
Wavelet	4.72	3.61	3.60	2.15	12.5	7.80	3.89	22.5	8.17	7.43	11.3	8.55	22.5
RMS	0.53	0.33	0.43	0.58	0.51	0.48	0.59	1.71	1.91	0.57	0.96	1.03	1.33
Wavelet	3.32	7.03	7.11	1.51	11.8	10.7	4.89	21.2	9.03	9.38	12.9	10.5	23.9
Power	0.55	0.34	0.44	0.64	0.46	0.46	0.57	1.83	1.92	0.62	0.92	1.03	1.31
Wavelet	3.33	5.96	6.02	1.27	13.4	10.6	5.67	20.4	9.93	10.2	11.7	10.4	24.8

Table 6. FAR and FRR for the classification between subjects using KNN

K-Nearest Neighbhors
FAR (%) & FRR (%)

	001	**002**	**003**	**004**	**005**	**006**	**007**	**008**	**009**	**010**	**011**	**012**	**013**
Average	0.03	0.02	0.08	0.12	0.13	0.03	0.19	1.40	0.76	0.20	0.57	0.53	0.55
Wavelet	0.71	1.87	1.87	0.36	2.13	2.22	0.24	12.5	7.06	3.30	5.33	4.50	13.8
RMS	0.06	0.02	0.10	0.18	0.14	0.05	0.21	1.51	1.02	0.19	0.69	0.59	0.74
Wavelet	0.82	2.67	2.70	0.84	2.82	3.02	0.49	12.9	8.67	4.42	6.55	4.64	16.6
Power	0.05	0.07	0.15	0.19	0.18	0.08	0.28	1.66	1.00	0.23	0.61	0.62	0.78
Wavelet	1.18	3.36	0.60	1.79	2.72	2.80	0.37	13.0	6.93	5.88	7.48	5.01	16.2

The average values of FAR and FRR were used to compare the results of the classifiers as shown in Table 7. In the identification mode, the SVM performed better in classification between the subjects which the percentage of FAR and FRR is the lowest compared to the other classifiers by using three WPD features. This means that the error rate for acceptance of unauthorized person and rejection of authorized person were the lowest.

Table 7. The average of FAR and FRR for the classification between subjects

	SVM		**RF**		**KNN**	
	FAR (%)	**FRR (%)**	**FAR (%)**	**FRR (%)**	**FAR (%)**	**FRR (%)**
Average Wavelet	0.28	3.79	0.77	9.08	0.35	4.30
RMS Wavelet	0.35	4.28	0.84	10.2	0.42	5.16
Power Wavelet	0.41	4.99	0.85	10.3	0.45	5.17

5. Conclusion

This research extracted WPD as a feature and adopted the average wavelet, RMS wavelet and power wavelet for EEG based authentication system in verification and identification mode. The WPD achieves better performance for both modes. Comparing with other approaches of feature extraction in Table 8, it gives more information from the original signal and the effectiveness of the features is proved by the classification using SVM, RF and KNN.

In the future work, this research plan to increase the number of subjects for develop larger database of EEG for authentication system. Moreover, the feature fusion will be explored and implemented in this research towards the development of robust EEG based authentication system incorporates with larger database to improve the performance of the system.

Table 8. Comparison between recent studies

Study	**Feature Extraction**	**Results**
Ong et. al. [7]	PSD feature	89.2%
Thomas et al. [9]	Band power feature	88.3%
This research	WPD feature	92.8%

ACKNOWLEDGEMENT
The authors would like to thank the Faculty of Electronic Engineering, Universiti Malaysia Perlis for the lab facilities and those who contributed directly and indirectly. This project was supported by FRGS grant (9003-00688)

References

[1] Thomas K and Vinod A P 2017 Toward EEG-based biometric systems: The great potential of brain-wave-based biometrics *IEEE Systems, Man and Cybernetics Magazine* **3** pp 6-15.

[2] Abo-Zahab M Ahmed S and Abbas S 2015 State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals ", *IET Biometrics* **4** pp 179-190.

[3] Shen C Yu Y Xu H Yang G and Guan X 2016 User practice in password security: An empirical study of real-life passwords in the wild *Computers & Security* **61** pp 130-141.

[4] Nicholson J Coventry L and Briggs P 2013 Faces and Pictures: Understanding age differences in two types of graphical authentications *International journal of human-computer studies* **71** pp 958-966.

[5] Poulus M Rangoussi M and Alexandris N 1999 *IEEE Int. Conf. on Acoustics, Speech and Signal Processing – Proceedings* (USA: Phoenix) pp 1117-1120.

[6] Kaur B Kumar P Roy P P and Singh D 2017 *4th IAPR Asian Conf. on Pattern Recognition* (China: Nanjing) pp 459-464.

[7] Ong Z Y Saidatul A and Ibrahim Z 2018 Power Spectral Density Analysis for Human EEG based Biometric Identification *Int. Conf. Computer Approach Smart System Design Application* (Malaysia: Kuching) pp 1-6.

[8] Campisi P and La Rocca D 2014 *IEEE transactions on information forensics and security* **5** pp 782-800.

[9] Thomas K P and Vinod A P 2018 EEG-based biometric authentication using gamma band power during rest state *Circuit, Systems, and Signal Processing* **37** pp 277-289.

[10] Kumar P Saini R Roy P P and Dogra D P 2017 A bio-signal based framework to secure mobile devices *J. of Network and Computer Appl.* **89** pp 62-71.

[11] Zhang X Yao L Huang C Gu Yang T and Lin Y 2017 Deepkey: An EEG and gait based dual-authentication system *Preprint arXiv/1706.01606*

[12] Britton J W Frey L C Hopp J L Korb P Koubeissi M Z Lievens W E Pestana-Knight E M and St Louis E K 2016 *Electroencephalography (EEG): an introductory text and atlas of normal and abnormal findings in adults, children, and infants* (Chicago: American Epilepsy Society)

[13] Wickerhauser M V 1996 *Adapted wavelet analysis: from theory to software* (CRC Press) pp 237.

[14] Ting W Guo-Zheng Y Bang-Hua Y and Hong S EEG feature extraction based on wavelet packet decomposition for brain computer interface *Measurement* **41** pp 618-625.

[15] Obaidat M S Traore I and Woungangang I 2019 *Biometric-based physical and cybersecurity systems* (Cham: Springer International Publishing) pp 1-10.