Exploring EEG-based Biometrics for User Identification and Authentication

Qiong Gui, Zhanpeng Jin
Department of Electrical and Computer Engineering
Binghamton University, State University of New York (SUNY)
Binghamton, NY 13902-6000
Email: {qgui1, zjin}@binghamton.edu

Wenyao Xu
Department of Computer Science and Engineering
University at Buffalo, State University of New York (SUNY)
Buffalo, NY 14260-2500
Email: wenyaoxu@buffalo.edu

Abstract—As human brain activities, represented by EEG brainwave signals, are more confidential, sensitive, and hard to steal and replicate, they hold great promise to provide a far more secure biometric approach for user identification and authentication. In this study, we present an EEG-based biometric security framework. Specifically, we propose to reduce the noise level through ensemble averaging and low-pass filter, extract frequency features using wavelet packet decomposition, and perform classification based on an artificial neural network. We explicitly discuss four different scenarios to emulate different application cases in authentication. Experimental results show that: the classification rates of distinguishing one subject or a small group of individuals (e.g., authorized personnel) from others (e.g., unauthorized personnel) can reach around 90%. However, it is also shown that recognizing each individual subject from a large pool has the worst performance with a classification rate of less than 11%. The side-by-side method shows an improvement on identifying all the subjects with classification rates of around 40%. Our study lays a solid foundation for future investigation of innovative, brainwave-based biometric approaches.

I. INTRODUCTION

Identification and authentication are forms of recognizing persons. Although identification and authentication share large similarities, differences still exist between them since authentication is confirming or denying an identity claim by a particular individual, while identification is to recognize an individual from a group of people based on the identity claimed by the person [1]. Unlike widely used methods of individual identification and authentication, like passwords, PINs, and RF cards, which are easily forgotten, stolen or lost, "biometrics" which refers to the technique used to identify individuals using unique human biological features, such as fingerprints, face, iris and voice [2], are more attractive.

Electroencephalogram (EEG) records the brain's electrical activity by measuring the voltage fluctuations on the scalp surface with simple placement of the electrodes on the skin [3]. The brain signals are brain activities determined by the person's unique pattern of neural pathways and thus is impossible to imitate [4], [5]. Those signals can be influenced by mood, stress and mental state of the individual [6] which makes them very difficult to be obtained under force and threat. Furthermore, brain signals are related to the subject's genetic

information, making them unique for each individual [7]–[9] and stable over time [10]. Therefore, brain signals are more reliable and secure and have been proposed as an identification and authentication biometric [11], [12].

This paper presents a general framework of EEG-based user identification and authentication. A single channel was used for noise reduction by ensemble averaging and low pass filter. Wavelet packet decomposition was used for feature extraction and then a neural network was adopted for classification. Four different scenarios were discussed to emulate different cases in authentication. The rest of the paper is organized as follows: Section II gives a brief introduction of previous work. Section III presents the system architecture and algorithmic details of the proposed EEG-based authentication framework. Finally, we discuss the application scenarios and corresponding experimental results.

II. RELATED WORK

EEG-based identification and authentication has been studied nowadays and these preliminary works have demonstrated that the EEG brainwave signals could be used for individual identification and authentication.

Palaniappan [13] proposed a two-stage threshold method to verify 5 subjects based on the features of autoregressive coefficients (AR), channel spectral powers and inter-hemispheric channel spectral power differences (IHPD), inter-hemispheric channel linear complexity (IHLC), and non-linear complexity on 6 channels. This method reached a false reject error (FRE) ranging from 0 to 1.5%. He et al. [1] used the naive Bayes model for authentication on 4 subjects based on mAR features and got a half total error rate (HTER) of 6.7%. He and Wang [14] also used the naive Bayes model for authentication on 7 subjects and got a HTER ranging from 2.2% to 7.3%. Kathikeyan and Sabarigiri [15] also used this model based on AR and power spectral density (PSD) and had an equal error rate (EER) of 4.16%. Based on the Gaussian Mixture Model (GMM), Marcel and Millan [6] got a HTER of 6.6% to 42.6%, while Nguyen et al. [16] had a error rate of 4.41% to 7.53%.

Ashby et al. [17] extracted the AR, PSD, spectral power (SP), IHPD and IHLC from the 14 EEG channels and used the linear support vector machine (SVM) classifier for authentication on 5 individuals and got the false rejection rate (FRR) of 2.4% to 5.1%, and the false acceptance rate (FAR) of 0.7% to 1.1%. Brigham and Kumar [18] also used the linear SVM for classification only on AR and had the accuracy of

Fig. 1. General Structure of the Authentication System

99.76% with the 6 subjects test and 98.96% with the 122 subjects test. Nguyen et al. [19] used the linear SVM to test several databases which had subjects of 3, 9, 40, 20, and 122. Based on the features from speech recognition applied in EEG signal authentication, the accuracies varied from 18.36% to 100%. Yeom et al. [20], [21] used the signal difference and least square error of time derivative features on 18 channels with the Gaussian kernel SVM on 10 subjects and got the accuracy around 86%. Dan et al. [22] used the polynomial kernel SVM based on wavelet transform (WT) and AR from single channel. The average accuracy was 85% on 13 subjects. Since the theory of SVM limits the classification categories to 2 classes, if the classification categories are 3 or more, one against one (any two classes) and one against all (considering a random class as the first group and all the other classes as the second group) are the two strategies. Ferreira et al. [23] used the linear and radial basis function (RBF) SVM to classify 13 subjects on the gamma band SP. One against one method got an error rate of 15.67% to 38.21% and one against all method got an error rate ranging from 17.43% to 30.57%. Liang et al. [24] extracted AR from 8 channels on 7 subjects. The one against one SVM got an accuracy of 45.52% to 54.96% and one against all got an accuracy of 48.41% to 56.07%.

Neural network (NN) is another popular classifier used in human identification and authentication. At the early stage of EEG-based biometric, learning vector quantizer (LVQ) was adopted by researchers. Poulos et al. [25] proposed a linear rational model of ARMA type to fit the alpha band EEG signals on single channel. For the 75 people being tested, to distinguish a specific person from others, correct classification scores of LVQ classifier in the range of 72% to 84% were obtained. Poulos et al. [26], [27] also used the LVQ NN to identify each subject out of 4 subjects from the other 75 subjects, but used the FFT feature and got an accuracy ranging from 80% to 100%. Poulos et al. [28] extended their studies by AR and bilinear model features. This paper had an accuracy of 56% to 88%.

Later the classic feed-forward and back-propagation NN was adopted. Palaniappan [29] used visual evoked potential (VEP) signals to identify 20 individuals by the NN classifier. Using the SP from gamma band of 61 electrodes, it gave an average accuracy of 99.06%. Shedeed [30] used the NN to identify 3 subjects based on fast Fourier transform (FFT) and wavelet packet decomposition (WPD) from 4 channels and got an correct classification rate from 66% to 93%. Hu [31] also used the NN to make decisions. The experiment got a true acceptance rate (TAR) from 80% to 100% and a false acceptance rate (FAR) from 0 to 30% on seven features when 3 subjects being tested. This NN also adopted by Hema [32] for EEG authentication on PSD features from Beta waves. To identify 6 individuals, it reached an average accuracy of 94.4 to 97.5%. Liang et al. [24] used the back-propagation NN to classify 7 subjects on AR from 6 channels and got a

accuracy of 42.87% to 50.14%. Mu and Hu [33] also used back-propagation NN to identify AR and fisher distance from 6 channels on 3 subjects and got an accuracy of 80.7% to 86.7%. Based on WT and AR from a single channel, Dan et al. [22] got a accuracy of 65% to 75% on 13 subjects. Hema and Osman [34] used PSD and feed forward NN and got an accuracy of 79.9% to 89.95%.

III. SYSTEM ARCHITECTURE

The data flow of the identification/authentication framework contains four parts as shown in Figure 1. The first step is to collect raw EEG signals. After that, ensemble averaging and low-pass filter are adopted to reduce the noise. Then based on the five major frequency sub-bands of the EEG signals, WPD is used to extract the features of the EEG signals. One part of these features is the training dataset to the neural network and the other feature vectors are used to evaluate the performance of the system.

A. Signal Acquisition

The raw EEG signals were collected from 32 adult participants (11 females, age range 18-25, mean age 19.12) using "EASY CAP" device (Ammersee, Germany) from 6 midline electrode sites (Fpz, Cz, Pz, O1, O2, Oz) [35]. The data was sampled at 500 Hz. 1.1 seconds of raw EEG signals were recorded, which made 550 samples for each channel. It is argued that the brain activities are very focused during the visual stimulus process known as VEPs [9]. Thus in this experiment, we collected the EEG signals using visual stimuli and the participants were asked to silently read an unconnected list of texts which included 75 words (e.g., BAG, FISH), 75 pseudowords (e.g., MOG, TRAT), 75 acronyms (e.g., MTV, TNT), 75 illegal strings (e.g., BPW, PPS), and 150 instances of their own names. Each human subject was tested twice: one test was used for training and the other was used for testing [36]. In this paper, we analyzed the brain response to the acronyms stimuli from the single channel of Oz, which was suggested to be the best channel to present the subject's brain activity. Figure 2 gives a general impression of the raw data collected from Channel Oz. From the waveform we can see that the raw EEG signals had a lot of noises since the signals changed rapidly.

B. Pre-Processing

Since the raw EEG signals are noisy, we first need to reduce the noise. Ensemble averaging [37] is a technique by averaging multiple measurements. Although it is a simple signal processing, it is very effective and efficient in reducing noise because the standard deviation of noise after average is reduced by the square root of the number of measurements. Thus the EEG signals were first ensemble averaged for 50
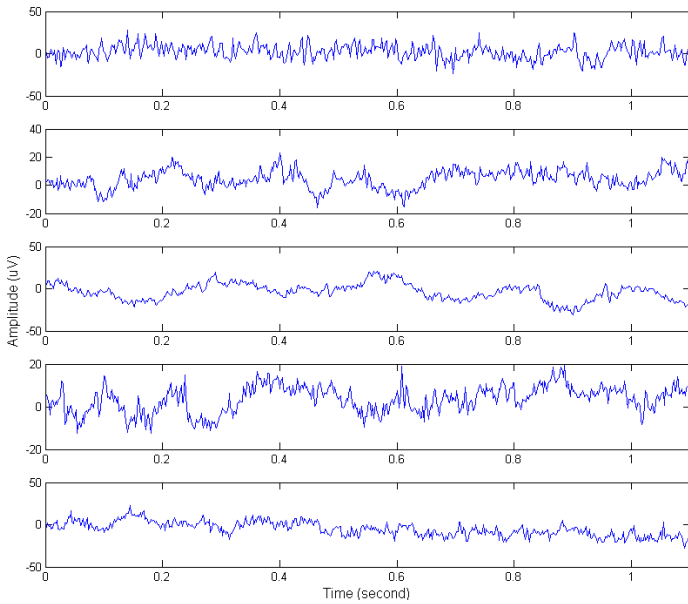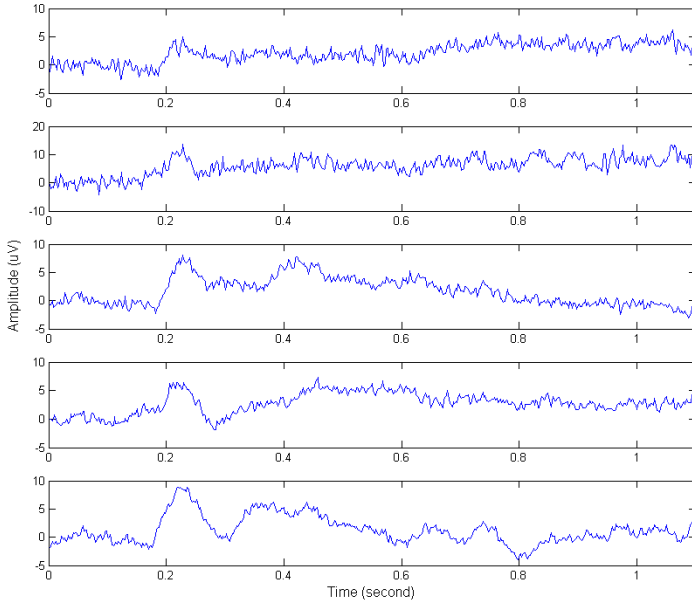
Fig. 2. Raw EEG Signals

Fig. 3. EEG Signals after Ensemble Averaging

individual measurements. Figure 3 shows the data after ensemble averaging. From the plots, we can see the averaged signals were much smoother than the raw data. After ensemble averaging, a 60 Hz low-pass filter was followed to remove the noise out of the major range of the EEG signals.

C. Feature Extraction

There are many different techniques to extract the features of the EEG signals after pre-processing, which can be roughly classified into three types: time-domain feature extraction, frequency-domain feature extraction, and time-frequency domain feature extraction. The statistical features, such as mean, median, and variance, belong to the time domain. The frequency domain features use Fourier Transform to analyze the frequency distribution of the EEG signals. The time and

frequency domain is WT based. WT seems to be the most appropriate method for EEG signal feature extraction [38].

EEG signals have five major frequency bands: delta (0-4 Hz), theta (4-8 Hz), alpha (8-15 Hz), beta (15-30 Hz), and gamma (30-60 Hz) bands [39]. For different individuals, the energy distributions of the frequency components are quite different and make it possible to adopt those frequency components as the features to represent the EEG signals [40]. WPD is a downsampling process in which the signal is passed through multi-level filters to analyze the time-frequency information. 4-levels WPD was applied on the pre-processed EEG signals. Coefficients from node (1, 1), (2, 1), (3, 1), (4, 0) and (4, 1) from Figure 4 representing the Gamma, Beta, Alpha, Delta and Theta frequency bands were extracted. Then the mean (μ_x), standard deviation (σ_x) and entropy ($\varepsilon(x)$) [30] were calculated to form the feature vectors.

$$
\begin{aligned}
\mu_x &= \frac{1}{N}\sum_{i=1}^{N} x_i \\
\sigma_x &= \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu_x)^2} \\
\varepsilon(x) &= -\sum_t x^2(t)\log\left(x^2(t)\right)
\end{aligned}
\tag{1}
$$

Since there were three parameters (mean, standard deviation and entropy of each coefficient node) and 5 nodes for each subject, then we had $3 \times 5 = 15$ features for each subject.

D. Classification

Classification is the process to check the identity of input vectors to the feature vectors that has been stored in the database. Artificial Neural Networks (ANNs) have been widely used by researchers to classify the EEG signals. In this study, we use the feed-forward, back-propagation, multi-layer perception NN as the classifier for EEG pattern classification. Extracted features were defined as inputs to the neural network. For each training dataset, 70% of data was used for training and the remaining 30% of data was used for validation. We varied the number of neurons in the hidden layer from 5 to 50 with the incremental of 5. Therefore, 10 cases of different numbers of neurons were tested to see their performance and which one had the best result.

IV. EXPERIMENT RESULTS

A. Scenarios

In the experiment, we considered four different application scenarios that may be involved for user authentication.

a) SCENARIO I: Identify all the 32 subjects: The goal of this scenario was to accurately identify each one of the 32 subjects. Therefore, the training dataset included all the features of the 32 subjects and correspondingly the outputs had 32 different classes. Based on the training dataset, a NN model was built to test the inputs.

b) SCENARIO II: Side-by-side identification of all the 32 subjects: The purpose of the side-by-side method was to improve the accuracy of identifying the 32 subjects. The difference between side-by-side and SCENARIO I was that side-by-side method made several smaller size training datasets based on different combinations of different subjects. Then sub-models were built after training these small size datasets.

(0,0) 0-60Hz															
(1,0) 0-30Hz								(1,1) 30-60Hz Gamma							
(2,0) 0-15Hz				(2,1) 15-30Hz Beta				(2,2)				(2,3)			
(3,0) 0-8Hz		(3,1) 8-15Hz Alpha		(3,2)		(3,3)		(3,4)		(3,5)		(3,6)		(3,7)	
(4,0) 0-4Hz Delta	(4,1) 4-8Hz Theta	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)	(4,7)	(4,8)	(4,9)	(4,10)	(4,11)	(4,12)	(4,13)	(4,14)	(4,15)

Fig. 4.   4-Level Wavelet Packet Decomposition Tree

After that, we made a decision based on all the outputs of the sub-models. There were two different cases to build the sub-models in this scenario which were similar to the situation when SVM algorithm dealing with 3 or more categories of classification. One was choosing all the data from training dataset of one specific subject and also randomly chose the same size data from the same dataset of all the other subjects. Then these data were used as training dataset to obtain one sub-model. Since there were 32 subjects, there were 32 different sub-models that needed to be calculated. When testing the performance, winner-takes-all classification principle was adopted and the class label which had the highest output value would be the predicted subject. Another way, shown in Figure 5, was first to get all the possible sub-models between any two different subjects. Because the 2-combinations from 32 was 496, there were 496 different cases for 32 subjects. The final result was determined by the majority voting strategy and the class which appeared most frequently in the predictions of all the 496 sub-models would be the final decision.
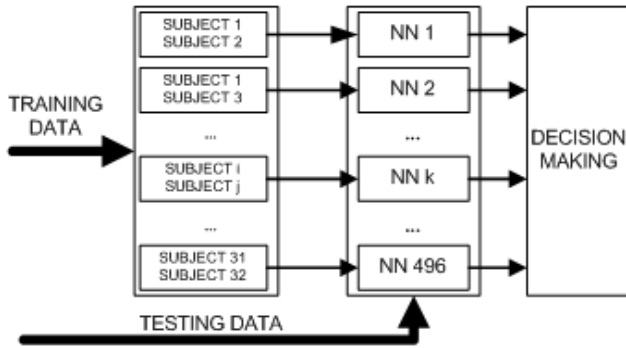

Fig. 5.   General Structure of Side-by-Side Method

c) SCENARIO III: Identify one subject from all the other 31 subjects: This scenario was to evaluate the performance of how accurately it can identify one subject from others. The training dataset was combined by all the data from the training dataset of one specified subject and randomly selected the same size data from the same dataset of all the other subjects.

d) SCENARIO IV: Identify a small group of subjects from the others: This scenario was to simulate the case that the authentication system may allow a small group of individuals (e.g., authorized personnel) to access the system. We tested two cases: allowing 2 persons to have access or 3 persons to have the access. The training set of this type was to select all the training data for the allowed individuals and also the same size training data of other people which were chosen randomly.

B. Evaluation Method

To evaluate the performance of each scenario, we used the *Correct Classification Rate* ($CCrate$) in the following equation:

$$CCrate = \frac{C_t}{T_n} * 100\% \tag{2}$$

where C_t is the total number of correct classifications and T_n is the total number of testing trials [41].

C. Results and Discussion

Table I listed the classification rates of each scenario.

SCENARIO I of identifying all the 32 subjects had the worst accuracy ranging from 5.75% to 10.68%. The hidden layer of 25 neurons had the best accuracy and increasing the neurons did not help improve the performance.

SCENARIO II using the side-by-side method showed better performance at identifying all the 32 subjects. The accuracy for 32 sub-models varied from 28.71% to 36.27% and 40 neurons got the highest accuracy of 36.27%. When the neuron number increased, the accuracy only decreased by around 2% to 3%. When using less neurons, the accuracy decreased to about 31% to 33%. The 496 sub-models had higher accuracy than the 32 sub-models with the accuracy ranging from 46.34% to 47.50% and was about 10% higher than 32 sub-models.

SCENARIO III was the case of identifying one specific person from others. The hidden layer of 45 neurons had the best average accuracy of 94.04%. Increasing or decreasing the neuron number did not change the accuracy too much since the minimum average accuracy is 92.70%. Although the brainwaves of different people are different, it can happen that the brainwaves for some people are very close and for some others they are quite different. Therefore, it may be hard to distinguish some individuals, but very easy to differentiate others. This can be shown by the minimum and maximum accuracies in the table. To identify one from others, the worst case was 79.06% accuracy while the best case was 99.87%.

SCENARIO IV was testing the case of identifying a small group of individuals from others. The 496 cases were to identify the specific 2 persons from the other remaining 30 subjects. With 20 neurons in hidden layer, the accuracy was the highest of 90.03%. The range of average accuracy was from 88.7% to 90.03% with no big differences. The minimum accuracy was 70.06% and the maximum is 99.2%. The 4960

TABLE I.   CLASSIFICATION RATES FOR DIFFERENT SCENARIOS

SCENARIOS	Description	# of Neurons	Correct Classification Rate		
			Minimum	Maximum	Average
I	1 case	5			8.46%
		10			5.75%
		15			7.69%
		20			7.39%
		25			**10.68%**
		30			7.28%
		35			7.29%
		40			6.34%
		45			6.79%
		50			8.05%
II	32 sub-models	5			28.71%
		10			33.11%
		15			33.02%
		20			31.73%
		25			33.85%
		30			33.30%
		35			30.90%
		40			**36.27%**
		45			34.43%
		50			34.36%
	496 sub-models	5			46.34%
		10			47.09%
		15			**47.50%**
		20			47.20%
		25			47.10%
		30			46.84%
		35			46.98%
		40			46.71%
		45			46.80%
		50			46.66%
III	32 cases	5	83.40%	99.87%	93.48%
		10	86.24%	97.99%	93.60%
		15	79.23%	99.52%	92.72%
		20	82.73%	99.68%	93.71%
		25	85.13%	99.04%	93.18%
		30	79.06%	97.87%	93.47%
		35	83.36%	99.36%	93.09%
		40	79.18%	99.28%	93.37%
		45	81.68%	99.52%	**94.04%**
		50	83.91%	99.61%	92.70%
IV	496 cases	5	70.06%	99.20%	88.7%
		10	76.00%	98.88%	89.67%
		15	74.83%	99.12%	89.94%
		20	75.13%	98.37%	**90.03%**
		25	73.79%	98.53%	89.93%
		30	74.88%	98.50%	89.87%
		35	72.48%	99.04%	89.93%
		40	72.94%	99.01%	89.51%
		45	70.86%	99.15%	89.71%
		50	74.04%	98.41%	89.60%
	4960 cases	5	63.73%	97.84%	84.82%
		10	69.67%	98.99%	86.53%
		15	68.37%	98.75%	86.89%
		20	68.31%	98.75%	**87.06%**
		25	66.66%	98.69%	87.03%
		30	68.81%	98.81%	86.97%
		35	68.16%	98.90%	86.81%
		40	65.61%	98.64%	86.71%
		45	68.79%	98.63%	86.64%
		50	65.41%	98.64%	86.54%

the recorded EEG signals for some subjects had very similar patterns. Thus, when we tried to distinguish one out of these subjects, the NN classifier cannot separate all the feature vectors correctly. It was more likely to have some misclassifications which would lower the accuracy. When we increased the number of subjects to be identified, the accuracies, including average, minimum and maximum, were decreased. The reason was that to identify two or three subjects, the classifier should separate three or four different groups. When some groups had close patterns, the classifier may not be so robust to show the tiny differences between these groups. This could increase the misclassified subjects and lead to lower accuracy as shown by the lower accuracies in SCENARIO IV. When we tried to identify all the 32 subjects in SCENARIO I, the accuracy was very low since the training dataset included all the feature data of all the 32 subjects. Therefore it is hard to distinguish the slight differences among them by the neural network weights which trained all the data of the 32 subjects at the same time. The side-by-side method in SCENARIO II improved the performance of identifying all the 32 subjects. For the 32 sub-models case, each sub-model hold the information of one out of the 32 subjects being test from the other subjects. For example, the first sub-model trained the dataset which included the first subject labeled as 1 and randomly selected vectors from other subjects labeled as 0. When there was a new input vector for testing, each subject would give out a result value in the range of 0 to 1 to show its prediction. The distances from the output value to 0 and 1 would show the probability of the output. The total output had 32 values and the maximum one showed that the final decision is most likely to be the label which had the maximum output. Since it was easier to identify one subject from other subjects, the accuracy of the preliminary decision made by the sub-models was improved and lead to an improved final decision. For the 496 sub-models case, each sub-model would distinguish any two subjects of 32 subjects. Since the training dataset only included the information of 2 subjects, it was more likely to identify the tiny differences between them although some may have had very close patterns. Thus at this stage, the output results were improved compared to 32 sub-models. The final results were about 10% higher than the 32 sub-models case. Also we can see from the table that the accuracies for different numbers of neurons did not vary too much. Thus, we can use less neurons to save resources with sacrificing only a little accuracy. Also we can see although SCENARIO II performs better than SCENARIO I, it still had worse performance than SCENARIO III and SCENARIO IV. This was because some outputs of the sub-models could give wrong decisions when the input subjects had very close feature vectors and this further influenced the final decision.

V.   CONCLUSION

In this paper we focused on a pilot study of how to use EEG signals for identification/authentication. Ensemble averaging and low pass filter were used for noise reduction and wavelet packet decomposition was used for feature extraction. The neural network was used for classification. We tested four scenarios to emulate the authentication cases. The classification rates of identifying one subject from others or a small group of individuals from others had high accuracies that were around 90%. Identifying all the subjects had the worst performance. It was difficult to correctly identify all the 32 subjects. The side-

cases were to identify 3 specific individuals from the other 29 subjects. The optimal number of neurons was 20 with the accuracy of 87.06%. The minimum accuracy is 63.73% and the maximum is 98.99%. The performance of identifying 3 individuals was a little lower than identifying 2 persons. It seemed that recognizing more individuals from others would lower the performance. From the table, we can see that 20 neurons in the hidden layer could be a good choice to identify 2 or 3 individuals when 32 subjects were being tested.

From the results, we can see that identifying one person from others in SCENARIO III had the highest average accuracy; but for some individuals, the accuracy of identifying them was low which can be 79.06%. This was mainly because

by-side method improved the performance of identifying all the subjects. Due to the improvement on the training datasets, the classification rates reached about 33% and 47% and was about 5 times the accuracies of identifying all the 32 subjects.

REFERENCES

[1] C. He, X. Lv, and J. Wang. Hashing the mar coefficients from EEG data for person authentication. In *IEEE Int'l Conf. Acoustics, Speech and Signal Processing (ICASSP)*, pages 1445–1448, April 2009.

[2] A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini. Unobtrusive biometric system based on electroencephalogram analysis. *EURASIP J. Adv. Sig. Proc.*, 2008, 2008.

[3] E. Maiorana, G. E. Hine, D. La Rocca, and P. Campisi. On the vulnerability of an EEG-based biometric system to hill-climbing attacks algorithms' comparison and possible countermeasures. In *IEEE 6th Int'l Conf. Biometrics: Theory, Appl. and Syst. (BTAS)*, pages 1–6, Sept 2013.

[4] R. Palaniappan and D. P. Mandic. Biometrics from brain electrical activity: A machine learning approach. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4):738–742, 2007.

[5] D. S. Bassett and M. S. Gazzaniga. Understanding complexity in the human brain. *Trends in Cognitive Sciences*, 15(5):200 – 209, 2011.

[6] S. Marcel and J. D. R. Millan. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4):743–752, April 2007.

[7] D. J. A. Smit, D. Posthuma, D. I. Boomsma, and E. J. C. Geus. Heritability of background eeg across the power spectrum. *Psychophysiology*, 42(6):691 – 697, 2005.

[8] R. B. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles. The electroencephalogram as a biometric. In *Canadian Conf. Electrical and Computer Engineering*, volume 2, pages 1363–1366 vol.2, 2001.

[9] A. Zquete, Bru. Quintela, and J. P. da Silva Cunha. Biometric authentication using brain responses to visual stimuli. In A. L. N. Fred, J. Filipe, and H. Gamboa, editors, *BIOSIGNALS*, pages 103–112. INSTICC Press, 2010.

[10] M. Näpflin, M. Wildi, and J. Sarnthein. Testretest reliability of resting EEG spectra validates a statistical signature of persons. *Clinical Neurophysiology*, 118(11):2519 – 2524, 2007.

[11] J. Thorpe, P. C. van Oorschot, and A. Somayaji. Pass-thoughts: Authenticating with our minds. In *Proc. 2005 Workshop on New Security Paradigms (NSPW)*, pages 45–56, 2005.

[12] D. La Rocca, P. Campisi, and G. Scarano. Eeg biometrics for individual recognition in resting state with closed eyes. In *Proc. Int'l Conf. Biometrics Special Interest Group (BIOSIG)*, pages 1–12, Sept 2012.

[13] R. Palaniappan. Two-stage biometric authentication method using thought activity brain waves. *Int'l J. Neural Systems*, 18(01):59–66, 2008.

[14] C. He and J. Wang. An independent component analysis (ica) based approach for EEG person authentication. In *3rd Int'l Conf. Bioinformatics and Biomedical Engineering (ICBBE)*, pages 1–4, June 2009.

[15] T. Kathikeyan and B. Sabarigiri. Countermeasures against iris spoofing and liveness detection using electroencephalogram (eeg). In *IEEE Int'l Conf. Computing, Commun. and Appl. (ICCCA)*, pages 1–5, 2012.

[16] P. Nguyen, D. Tran, X. Huang, and W. Ma. Motor imagery EEG-based person verification. In *Advances in Computational Intelligence*, pages 430–438. Springer, 2013.

[17] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein. Low-cost electroencephalogram (EEG) based authentication. In *IEEE/EMBS 5th Conf. Neural Engineering (NER)*, pages 442–445, April 2011.

[18] K. Brigham and B. V. K. V. Kumar. Subject identification from EEG signals during imagined speech. In *4th Int'l Conf. Biometrics: Theory Appl. and Syst. (BTAS)*, pages 1–8, Sept 2010.

[19] P. Nguyen, D. Tran, X. Huang, and D. Sharma. A proposed feature extraction method for eeg-based person identification. In *Int'l Conf. Artificial Intelligence (ICAI)*, 2012.

[20] S.-K. Yeom, H.-I. Suk, and S.-W. Lee. EEG-based person authentication using face stimuli. In *Int'l Winter Workshop on Brain-Computer Interface (BCI)*, pages 58–61, Feb 2013.

[21] S.-K. Yeom, H.-I. Suk, and S.-W. Lee. Person authentication from neural activity of face-specific visual self-representation. *Pattern Recognition*, 46(4):1159 – 1169, 2013.

[22] D. Zhu, X. Zhou, and Q. Guo. An identification system based on portable EEG acquisition equipment. In *Proc. 3rd Int'l Conf. Intelligent System Design and Engineering Appl.*, pages 281–284, 2013.

[23] A. Ferreira, C. Almeida, P. Georgieva, A. Tome, and F. Silva. Advances in EEG-based biometry. In A. Campilho and M. Kamel, editors, *Image Analysis and Recognition*, volume 6112 of *Lecture Notes in Computer Science*, pages 287–295. Springer Berlin Heidelberg, 2010.

[24] N.-Y. Liang, P. Saratchandran, G.-B. Huang, and N. Sundararajan. Classification of mental tasks from eeg signals using extreme learning machine. *Int'l J. Neural Systems*, 16(01):29–38, 2006.

[25] M. Poulos, M. Rangoussi, V. Chrissikopoulos, and A. Evangelou. Person identification based on parametric processing of the eeg. In *6th IEEE Int'l Conf. Electronics, Circuits and Systems (ICECS)*, volume 1, pages 283–286. IEEE, 1999.

[26] M. Poulos, N. Rangoussi, A. Alexandris, and M Evangelou. On the use of EEG features towards person identification via neural networks. *Informatics for Health and Social Care*, 26(1):35–48, 2001.

[27] M. Poulos, M. Rangoussi, and N. Alexandris. Neural network based person identification using EEG features. In *IEEE Int'l Conf. Acoustics, Speech, and Signal Processing*, volume 2, pages 1117–1120, Mar 1999.

[28] M. Poulos, M. Rangoussi, N. Alexandris, and A. Evangelou. Person identification from the EEG using nonlinear signal classification. *Methods of information in Medicine*, 41(1):64–75, 2002.

[29] R. Palaniappan. Method of identifying individuals using vep signals and neural network. *Science, Measurement and Technology, IEE Proceedings -*, 151(1):16–20, Jan 2004.

[30] H.A. Shedeed. A new method for person identification in a biometric security system based on brain EEG signal processing. In *World Congress on Information and Communication Technologies (WICT)*, pages 1205–1210, Dec 2011.

[31] J.-F. Hu. Biometric system based on EEG signals by feature combination. In *Int'l Conf. Measuring Technology and Mechatronics Automation (ICMTMA)*, volume 1, pages 752–755, March 2010.

[32] C. R. Hema, M. P. Paulraj, and H. Kaur. Brain signatures: A modality for biometric authentication. In *Int'l Conf. Electronic Design (ICED)*, pages 1–4, Dec 2008.

[33] Z. Mu and J. Hu. Research of EEG identification computing based on ar model. In *Int'l Conf. Future BioMedical Information Engineering (FBIE)*, pages 366–368. IEEE, 2009.

[34] C. R. Hema and A. Osman. Single trial analysis on EEG signatures to identify individuals. In *6th Int'l Colloquium on Signal Processing and Its Applications (CSPA)*, pages 1–3. IEEE, 2010.

[35] S. Laszlo, M. Ruiz-Blondet, N. Khalifian, F. Chu, and Z. Jin. A direct comparison of active and passive amplification electrodes in the same amplifier system. *J. Neuroscience Methods*, 235(30):298–307, 2014.

[36] M. Ruiz-Blondet, N. Khalifian, B. C. Armstrong, Z. Jin, K. J. Kurtz, and S. Laszlo. Brainprint: Identifying unique features of neural activity with machine learning. In *Proc. 36th Annual Conf. of the Cognitive Science Society*, July 2014.

[37] J. L. Semmlow. *Signals and Systems for Bioengineers: A MATLAB-based Introduction*. Academic Press series in biomedical engineering. Elsevier/Academic Press, 2012.

[38] M. Huang, P. Wu, Y. Liu, L. Bi, and H. Chen. Application and contrast in brain-computer interface between hilbert-huang transform and wavelet transform. In *9th Int'l Conf. Young Computer Scientists (ICYCS)*, pages 1706–1710, Nov 2008.

[39] S. A. Asha, C. Sudalaimani, P. Devanand, T.E. Thomas, and S. Sudhamony. Automated seizure detection from multichannel EEG signals using support vector machine and artificial neural networks. In *Int'l Multi-Conf. Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*, pages 558–563, March 2013.

[40] I. Omerhodzic, S. Avdakovic, A. Nuhanovic, and K. Dizdarevic. Energy distribution of EEG signals: EEG signal wavelet-neural network classifier. *CoRR*, abs/1307.7897, 2013.

[41] H. A. Shedeed, M. F. Issa, and S. M. El-Sayed. Brain EEG signal processing for controlling a robotic arm. In *8th Int'l Conf. Computer Engineering Systems (ICCES)*, pages 152–157, Nov 2013.