EEG-based Person Authentication Method Using Deep Learning with Visual Stimulation

Supawich Puengdang
Mahidol Wittayanusorn School
Nakhon Pathom, Thailand
supawich@gmail.com

Teerapath Sattabongkot
Mahidol Wittayanusorn School
Nakhon Pathom, Thailand
teerapaths@gmail.com

Suppawong Tuarob
Information and Communication Technology (ICT)
Mahidol University, Thailand
suppawong.tua@mahidol.edu

Boonnatee Sakboonyarat
Mahidol Wittayanusorn School
Nakhon Pathom, Thailand
boonnatee@mwit.ac.th

Abstract*— Biometric authentication methods, such as fingerprint, used nowadays still have numerous potential security concerns and can be forged physically. To mitigate this issue, recent research has established non-physical signals such as brainwaves as viable sources for secured person authentication. As the brain signal has been found to be unique for individuals, electroencephalogram (EEG) signals can be potentially utilized as an identity discrimination tool, especially since EEG reflects the delicate difference in individuals' mental characteristics. However, the existing EEG-based authentication methods not only apply one or few techniques to stimulate the signals but also there are some vulnerabilities in the limited scope of the study. Therefore, we propose to combine steady-state visual evoked potential (SSVEP) and event-related potential (ERP) features to discriminate the distinction between individuals and apply the Long Short-Term Memory (LSTM) network for the analysis. The proposed methodology is divided into three stages. Firstly, we collect raw EEG data from the 20 human subjects, whose brains were stimulated by 7.5 Hz square SSVEP with targeted and non-targeted Snodgrass-Vanderwart's set of images as ERP stimulus. Then, the raw data is pre-processed by a notch filter, band-pass filter, and eye blink artifacts removal. The LSTM architecture is used to process data of individuals for predicting the results. After prediction, the performance is evaluated based on False Acceptance Rates and False Rejection Rates. The EEG-based authentication method with visual stimulus demonstrates high verification accuracy and can be applied with some improvement in the future through the use of brain connectivity techniques.

***Keywords*— EEG, personalized authentication, LSTM, deep learning**

I. INTRODUCTION

The ability to automatically authenticate or identify individuals has been a focal point of computer science research in the past few decades, that has involved multi-disciplinary sciences working together to constantly develop more accurate, faster, and more convenient automated methods that are less prone to impersonation.

The person authentication technology enables recognition of individuals through their unique personification and identification. Authentication is the act of proving the claim made by a person about their identity. In other words, the authentication of a person consists of a set of actions aiming to verify the identity they declare. In the authentication mode, the system validates a person's identity by comparing the captured biometric data with her own biometric templates stored in the system database [1]. Many methods of biometric authentication have been extensively used to identify people by exploiting human innate physical appearances including fingerprint, iris, and facial structure [2]. However, identities generated from these methods can also be physically forged and they still have numerous potential security issues that potentially cause many problems in privacy risks [3]. To mitigate this problem, various researchers (e.g. Palaniappan et al., Mu et al. and Min et al.) have investigated person authentication through brainwave, since such non-physical signals can be used to characterize individuals [4], and are difficult to impersonate with the current technology [5].

Brainwave signals have been explored particularly through electroencephalogram (EEG), the brain signal that has been observed in large-scale oscillations, in health science contexts for years. Much attention has been paid to EEG signals in medical applications rather than other areas of application such as individual authentication, in which the existing EEG-based authentication methods still face certain limitations. First, such existing methods apply only one or a few techniques to stimulate the brain [6]. Second, they have some vulnerabilities stemming from focusing only on some limited area of EEG for specific scope of studies [7]. Despite these limitations, overall EEG data analysis is one of the most complex biometric identification methods, which has recently been made promising with the rise of deep learning technological advances. Therefore, the purpose of this study is to investigate the possibility to utilize deep learning techniques in EEG-based authentication frameworks. The success of this research would not only enable resilient and impersonation-tolerant methodology for automated authentication, but also provide a building block for related research on non-physical based biometric authentication methods to build upon. In the research, we will combine SSVEP and ERP features for a more effective distinction between individuals and apply Long Short-Term Memory networks to analyse the data derived from the EEG signal.

II. BACKGROUND AND RELATED WORKS

A recurrent neural network (RNN) is a class of artificial neural networks where connections between units form a directed graph along a sequence. Such a network is used in sequence processing. As a simple example, if a training dataset contains an arithmetic sequence, e.g. 1,3,5, it is possible to train the RNN to predict that the next number would be 7. However, we must engineer the features that can

Mahidol Wittayanusorn School, Nakhon Pathom, Thailand.

978-1-5386-7512-0/19/$31.00 @2019 IEEE

infer that the different between numbers is 2 so the model can make correct prediction. Nonetheless, most of challenging real world prediction problems are not as simple as the sequence prediction, due to the high dimension of the data that requires advanced feature engineering techniques capable of discriminating the target attributes. Therefore, in order to build a successful prediction models for real-world data, it would require not only the right learning algorithms, but also the efficient feature extraction that can precisely draw useful characteristics from the data.

Although RNN can find features of numerical data, they do not fit for large scale sequence. Long sequences can be difficult to learn by RNN since it is trained by back-propagation through time (BPTT) and that causes the problem of vanishing gradient To overcome such issues, Long-short term memory (LSTM) has been invented, that allows the model to put more weight on more recent data, while maintaining important information from the past. Then, RNN cell is replaced by a gated cell for solving this problem. The gate control which information should be remembered in memory and which are not. The memory that was added to LSTM cell makes it able to remembers its previous steps. In this research, we choose to explore the LSTM since the brain signals of an individual are collected at fine time scales, resulting in a long time series that is ineffectively modelled by the traditional RNN models.

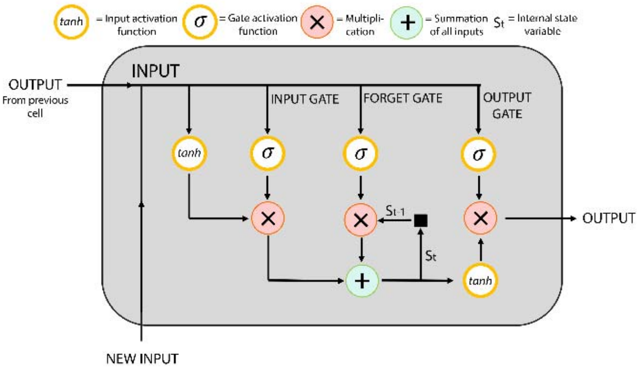

Fig. 1. The architecture of LSTM cell

LSTM uses sequential path from older past cells to the current one. A simple explanation is to fill the word in sentence, for example, “I lived in Thailand for 20 years. I then moved to Singapore…. I can speak fluent___.” Firstly, the model is able to recognize that the person lived in Thailand for several years; however, an RNN would forget this feature after several processing steps. However, when processing such a sequence, LSTM would remember important information and can answer correctly while passing through long sentences.

Recent studies have demonstrated that the EEG brainwave signals could be used for individual authentication. Shashank N et al. [8] implemented Snodgrass & Vanderwart’s picture set in stimulation. They used k-Nearest Neighbor algorithm (kNN) to classify EEG samples. They designed three scenarios including Side-by-side identification of all the subjects, identification of one subject from all the other subjects, and identifying a small group of subjects from the others. Their method yielded the accuracy of 88.88%, 90%, and 85.71% respectively.

The feature of this paper is the experiment scenarios. Their experiment method is reliable and accurate. Nevertheless, the selected McClellan FIR filter, Multi-wavelet transformation method and K-Nearest Neighbor algorithm (kNN) together with the small number of participants do not give the satisfy result.

Yanru Bai et al. [9] worked with biometric systems based on VEPs with multiple features. Their method yielded classification accuracy of 96.25% across 20 subjects was obtained on SVM using AR model parameters as features. They also focused on exploring effective optimization strategies for feature selection and channel simplification. The highest classification accuracy achieved was 97.25% with 32 optimal channels selected by RFE-SVM.

This paper prominent point is about the selection of feature extraction. It additionally provides an information about channels optimization to increase an accuracy. However, the paper spend practice only with SVM and it may create an error with the enormous data.

Palaniappan et al. [10] improved VEP features classification with Principal Component Analysis (PCA) and normalization. They extract the gamma band range with A 10th order forward and 10th order reverse Butterworth digital filters. In addition, they achieved satisfying results with the Simplified Fuzzy ARTMAP classifier (SFA), Linear Discriminant classifier (LD), and k-Nearest Neighbour classifier (kNN). PCA and normalization improved SFA classification performance from 71.14% to 92.84%. For LD, the improvement in classification performance was from 84.00% to 96.50%, while 66.12% to 92.04% for kNN.

The paper focus on the use of PCA and normalization, with 61 channels, in improving the classification accuracy. Although they analyse only with LD and kNN model, they show the contrast in accuracy compare to the data without them. However, they do not show the effect when they reduce the channels. The channels are somewhat too many to be practical used. Consequently, the lessen channels will show the possibility to be used in the actual system.

Nonetheless, the following papers worked with only single style of brain stimulation. Comparing to other researches, we particularly used two visual stimulation rather than one. Combination of SSVEP and ERP, as our hypothesis, will improve the result. We expected the SSVEP to distinct the ERP feature and compile with higher accuracy. Moreover, two features create a more complex data which enhance the system security. If the person does not know exactly the time and how the brainwave is stimulated, it is impossible to penetrate the system.

III. Methodology

The proposed methodology is divided into three stages. The first stage is to record EEG signals obtained from human volunteers. In the next stage, these signals will be pre-processed with notch filter, bandpass filter in the range of 0.5 to 7 Hz, eye-blink noise removal, and normalization. In the final stage, we will classify individual data using deep learning approach and then measure the accuracy of the method.

A. Data Collection

We acquired the EEG data from twenty healthy Thai subjects (10 males and 10 females, whose ages range between 15-50 years). Each subject sat in front of a 12.2”

LED display for 30 to 45 minutes. Measurements were taken from F3, F4, P3, P4, O1, and O2 channels that were placed on the subject's scalp, which are sampled at 250 Hz according to [11]. The maximum impedance of each electrode was limited to 50 kΩ. The electrode positions are located at standard sites on the scalp, according to an extension of Standard Electrode Position Nomenclature (American Encephalographic Association). All the subjects participated in the experiment for two times on different days. At the beginning of the experiment session, the purpose and description of the experiment were declared to the subjects. They could reject or have the right to stop the monitoring at any time. The data was collected into the private database and will be deleted after this research is completed.

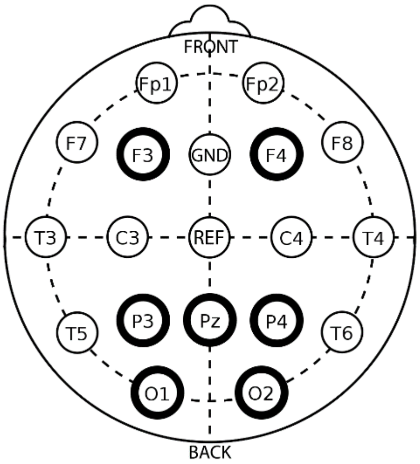

Fig. 2. Electrode positions used in the experiment

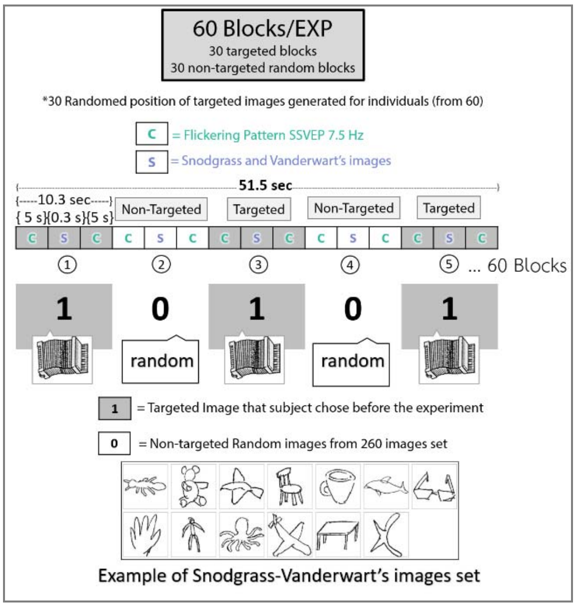
60 Blocks/EXP
30 targeted blocks
30 non-targeted random blocks
*30 Randomed position of targeted images generated for individuals (from 60)
C = Flickering Pattern SSVEP 7.5 Hz
S = Snodgrass and Vanderwart's images
51.5 sec
-----10.3 sec-----
5 s 0.3 s 5 s
Non-Targeted
Targeted
Non-Targeted
Targeted
C S C C S C C S C C S C C S C
① ② ③ ④ ⑤ ... 60 Blocks
1
0
1
0
1
random
random
1 = Targeted Image that subject chose before the experiment
0 = Non-targeted Random images from 260 images set
Example of Snodgrass-Vanderwart's images set

Fig. 3. Overall experimental procedure

To obtain EEG signals, we use steady-state visual evoked potentials (SSVEP) and event-related potential (ERP) to stimulate certain lobe controlling visibility and recognition. SSVEP is an evoked potential caused by a visual stimulus at specific frequencies and it influences the brain to generate EEG at the same frequency [11]. In this study, ERP will be generated from Snodgrass and Vandewart's 260 images [12], similarly to the process conducted by Palaniappan et al. (2003) [2]. The process as shown in Fig. 3 involves a recognition of a repeatedly shown image that appears for 300 milliseconds, among other random images in the sequence, to generate P300 components according to Yu et al., 2016 [13]. The SSVEP features will be generated when the subject is faced with 7.5 Hz flashing lights for five seconds and inserted between the showing of the Snodgrass and Vandewart's images.

B. Data Pre-processing

The raw data is processed to obtain proper features before being used to train the model. First, the raw data at 50 Hz frequency is attenuated in the specific ranges to very low levels by a narrow band-stop filter called the notch filter. Then, the usable range of frequencies that passes within 0.5 Hz to 7 Hz, and frequencies outside that range will be rejected. After that, eye blink artifact which can interrupt the available feature is removed by applying cross-correlation. The data pre-processing steps are summarized in Figure 4.

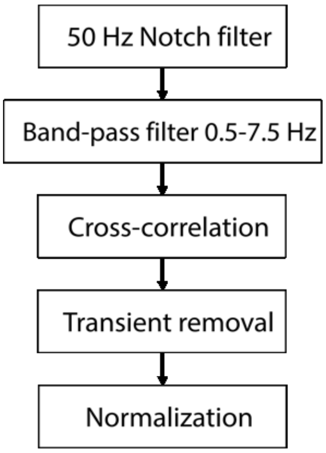

Fig. 4. Pre-processing procedure

C. Deep Learning Approach

To use the obtained EEG data for the individual authentication process, we firstly invent the software based on the Recurrent Neural Network (RNN) architecture called Long Short-Term Memory (LSTM) that is capable of effective learning and remembering over a long sequence of inputs.

The model uses Adam (adaptive moment estimation) optimizer with standard parameter setting. The learning rate is 0.001 and the batch size is 8. The model classifies through the binary classification between a pair of individuals' input data and uses sigmoid activation function at an dense layer.

TABLE I. TRAINING-VALIDATION-TEST SPLIT FOR EACH MODEL

	Training	*Validation*	*Test*
10-fold Dataset	80%	10%	10%
Positive Dataset	48	6	6
Negative Dataset	48	6	6
Total	96	12	12

A personalized model is trained for each of the 20 test subjects. An available pre-processed data from each experiment is shaped to samples, timesteps, and features. A model was trained with 60 positive samples from the targeted blocks of an authorized subject and 60 negative samples from random subjects' data to specify the threshold. Each sample has 2,630 timesteps and seven features from electrode channels. Then, we split the data into train set, validation set, and test set with the ratio of 8-1-1 for 10-fold cross validation, where the test subjects are randomly split into 10 sub-groups as shown in Table I. For each group i (10%), all the subjects in this group become test subjects, the next sub group becomes the validation set, and the remaining 80% of the population is fed into the training set. The classification performance from the 10 folds are then averaged, reported, and analysed. We use two main evaluation metrics in our experiments: False Rejection Rate (FRR) and False Acceptation Rate (FAR). FRR quantifies the rate at which the system falsely rejects a true authentication attempt (i.e. overkill rate), defined as the ratio of the number of incorrect rejections over all the authentication attempts. Similarly, FAR measures the rate at which the system incorrectly accepts authentication attempts (i.e. escapee rate), defined by the proportion of the number of incorrectly accepted authentication over the number of all the authentication attempts.

We implemented the model with Python via Keras, an open source neural network library written in Python, as a tool for running Tensorflow. The parameters of LSTM are shown in Table II.

TABLE II. LSTM PARAMETERS

Parameters	**Value**
Type	Bidirectional
Number of layers	1
Learning rate	0.01
Number of units	100
Number of epochs	30-50
Number of batch sizes	8
Activation function	Sigmoid

IV. RESULTS

After predicting with dataset splitting technique, called 10-fold cross validation, the results are evaluated with the performance effectiveness measured via False Acceptance Rate and False Rejection Rate according to Biometric Evaluation Standards. We achieve an average accuracy of 91.44% with this method of stimulation using deep learning approach from each model's 10-fold cross validation. The average training time for each model is 28.5 minutes (2.85 minutes for a fold).

TABLE III. ERROR RATE OF THE MODEL

Subject	***FAR (%)***	***FRR (%)***
1	11.11	15.56
2	7.78	11.11
3	4.44	10.00
4	7.78	10.00
5	6.67	7.78
6	10.00	23.33
7	8.89	11.11
8	11.11	23.33
9	0.00	0.00
10	10.00	23.33
11	1.11	1.11
12	5.00	8.33
13	6.67	11.67
14	4.44	5.56
15	10.00	1.67
16	10.00	16.67
17	0.00	6.67
18	1.67	5.00
19	5.00	8.33
20	10.00	10.00
Average	**6.58**	**10.53**

Table III shows the results of the experimental study from 20 subjects in term of percentage of False Rejection Rate (FRR) and False Acceptation Rate (FAR). The false acceptation rate, or FAR, is the measure of the likelihood that the data will incorrectly accept an access attempt by an unauthorized user. While the false recognition rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. The average result of FAR is 6.58%. The average result of FRR is 10.53%.

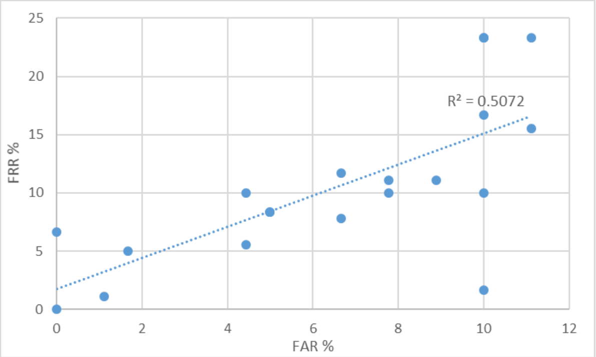

Fig. 5. Pre-processing procedure

Figure 5 displays the FAR-vs-FRR plot from the 20 participants. It is interesting to note that an R^2 of 0.5 is observed between the two variables, indicating positive correlation between the magnitudes of FAR and FRR. That is, our proposed personalized EEG-based authentication has shown very effective among certain group of participants, while less accurate on the others. Such an insight could shed light on the path-forward of further investigating into those individuals whose performance is poor and identify common features that could be used to further minimizing the performance gap.

The 91.44% average accuracy of the method from 20 models of subjects demonstrates higher performance than 90.25% Palaniappan et al. [10] method using VEP features. The direct time domain EEG data for an input section we used is compatible with the LSTM model we implemented. The analyzing of EEG depended on time series dataset help improve the recognition of details in a small dataset. The average compilation time and also the number of channels used in the experiment is significantly less than the reference methods. It proves that a small EEG datasets we used for training each model are enough for improving the model accuracy to higher than 90%.

V. Discussion and Conclusion

In this manuscript, we make a new method of EEG-based person authentication using deep learning. This method using LSTM of SSVEP and ERP features demonstrates fairly high verification accuracy of 91.44%. The method can be accessed by a wider range of user who has ordinary eyes and brain. The combining of two stimulation techniques with only seven channels shows that it is worth taking a further investigation. The method can be used with another biometric method to increase efficiency. However, the accuracy can be ameliorated with some improvement in the future.

References

[1] Mu, Z., Hu, J., Min, J., & Yin, J. (2017). Comparison of different entropies as features for person authentication based on EEG signals. IET Biometrics, 6(6), 409-417.

[2] Palaniappan, R., & Ravi, K. V. R. (2003). A new method to identify individuals using signals from the brain. In Information, Communications and Signal Processing, 2003 and Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint Conference of the Fourth International Conference on IEEE, 3, 1442-1445.

[3] Linnartz, J. P., & Tuyls, P. (2003). New shielding functions to enhance privacy and prevent misuse of biometric templates. In International Conference on Audio-and Video-Based Biometric Person Authentication, 393-402.

[4] Boribalburephan, P., & Sakboonyarat, B. (2012). An algorithm development for handwritten character recognition by personal handwriting identity analysis [PHIA]. 4th International Conference on Knowledge and Smart Technology (KST), 6-10.

[5] Palaniappan, R., & Mandic, D. P. (2007). EEG based biometric framework for automatic identity verification, J. VLSI Signal Process. Syst. Signal Image Video Technol, 49, 243–250.

[6] Zúquete, A., Quintela, B., & Cunha, J. P. S. (2010). Biometric authentication using electroencephalograms: a practical study using visual evoked potentials. Electrónica e Telecomunicações, 5(2), 185-194.

[7] Basar, E., Basar-Eroglu, C., Demiralp, T., & Schurmann, M. (1995). Time and frequency analysis of the brain's distributed gamma-band system. IEEE Engineering in Medicine and Biology Magazine, 14(4), 400-410

[8] Shashank, N., & CR, M. R. (2016). Eeg Based Person Identification And Authentication Using Bci. International Journal Of Engineering And Computer Science, 5(12).

[9] Bai, Y., Zhang, Z., & Ming, D. (2014, August). Feature selection and channel optimization for biometric identification based on visual evoked potentials. In Digital Signal Processing (DSP), 2014 19th International Conference on (pp. 772-776). IEEE.

[10] Palaniappan, R., & Ravi, K. V. R. (2006). Improving visual evoked potential feature classification for person recognition using PCA and normalization. Pattern Recognition Letters, 27(7), 726-733.

[11] Phothisonothai, M. (2015). An investigation of using SSVEP for EEG-based user authentication system. 2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), 923-926.

[12] Snodgrass, J.G. & Vanderwart, M. (1980). A standardized set of 260 pictures: Norms for name agreement, image agreement, familiarity, and visual complexity. J. Exp. Psychol. Hum. Learn. Mem., 6, 174–215.

[13] Yu, M., Kaongoen, N., & Jo, S. (2016). P300-BCI-based authentication system. In Brain-Computer Interface (BCI), 4th International Winter Conference on IEEE, 1-4.