Multimodal Biometric Authentication for VR/AR using EEG and Eye Tracking

Vrishab Krishna
Research Mentorship Program - UCSB
National Public School - Indiranagar
Bangalore, Karnataka, India
krishnavrishab@gmail.com

Yi Ding
University of California - Santa Barbara
Santa Barbara, California, USA
yding@ucsb.edu

Aiwen Xu
University of California - Santa Barbara
Santa Barbara, California, USA
aiwenxu@ucsb.edu

Tobias Höllerer
University of California - Santa Barbara
Santa Barbara, California, USA
holl@cs.ucsb.edu

ABSTRACT

Electroencephalogram (EEG) signals can enable an additional non-intrusive input modality especially when paired with a wearable headset (i.e. AR/VR). A great challenge in using EEG data for Brain-Computer Interface (BCI) algorithms is its poor generalization performance across users. Taking advantage of these inter-user differences, we investigate the potential in using this technology for user authentication – similar to facial recognition in smartphones. Additionally, we evaluate this in combination with eye tracking data which is also readily available in such headsets. We develop a biometric authentication systems for each of these systems and for their fusion. We formulate a

ICMI '19 Adjunct, October 14–18, 2019, Suzhou, China

ACM ISBN 978-1-4503-6937-4/19/10.
https://doi.org/10.1145/3351529.3360655

novel evaluation paradigm using publicly available EEG motor imagery and eye tracking data and demonstrate strong feasibility towards using EEG and eye tracking for authentication.

CCS CONCEPTS

• **Security and privacy** → **Biometrics**; • **Human-centered computing** → **Mixed / augmented reality**; **Virtual reality**.

KEYWORDS

Multimodal biometrics, EEG, Eye Tracking, Machine Learning

ACM Reference Format:

Vrishab Krishna, Yi Ding, Aiwen Xu, and Tobias Höllerer. 2019. Multimodal Biometric Authentication for VR/AR using EEG and Eye Tracking. In *Adjunct of the 2019 International Conference on Multimodal Interaction (ICMI '19 Adjunct), October 14–18, 2019, Suzhou, China.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3351529.3360655

INTRODUCTION

As VR/AR headsets become pervasive, alternative methods for fast, secure, and non-intrusive authentication systems such as face and fingerprint recognition on modern mobile devices must be considered. This is especially important as private information stored in these headsets, such as eye and facial movement as well as financial and geo-tracking information, is an important security risk.

A potential answer to this problem lies in the use of Brain-Computer Interface (BCI) technology. BCIs enable interaction with computing devices via electroencephalogram (EEG) information with applications in education, marketing, security, medicine, and entertainment [1, 15]. Head-mounted devices such as VR/AR headsets offer a natural, non-intrusive way for widespread deployment of this technology. However, the generalizability of BCI algorithms across the EEG data of users is a major challenge. What if we take advantage of these inter-user differences for biometric authentication? Additionally, can we make authentication more accurate using additional modalities/biometrics from head-mounted devices?

Due to its morphological, anatomical, and functional plasticity, EEG based biometrics have been found to have potential discriminating capability [13] enabling it to be a reliable, convenient and universal biometric [7]. As a behavioral biometric, EEG signals are harder to imitate compared to physiological biometrics such as face and iris due to their temporal variations [10]. Another non-intrusive behavioral biometric, eye tracking, which is commonly used in VR/AR headsets, depends on the subtly different reactions of the eyes to stimuli [5] and can thus be easily applied to such systems.

Combinations of biometrics/modalities such as EEG and face [14], EEG and ECG [11], and Eye Tracking and facial recognition [16] have been shown to achieve high levels of accuracy through

EEG	AUC	99%
	Accuracy	98%
	EER	3.4%
	FRR	8.4%
	FAR	1.8%

Figure 1: Results for EEG Authentication: Note that this system is very accurate and the low FAR and FRR values are very valuable in a biometric security system.

Eye Tracking	Accuracy	79%
	Log Loss	0.82
	FRR	36.7%
	FAR	7.4%

Figure 2: Results for Eye Tracking Authentication: Note that the FAR is low but the FRR is high indicating the high rejection of subjects from the system.

multimodal fusion in biometric authentication. The authors did not find previous works combining EEG and eye tracking for the particular use case of biometric authentication.

In this paper, we investigate the feasibility of using EEG and eye tracking with the particular application to biometric security systems. We demonstrate promising results for combining EEG and eye tracking for use in fast and non-intrusive authentication.

METHODS

The proposed method consists of three major steps: EEG authentication, Eye Tracking authentication, and Multimodal Fusion.

EEG Authentication

Task and Dataset: The EEG data used for processing were ERPs generated in a motor imagery task [2, 6, 9]. The left and right fist movements from the EEG Motor Movement/Imagery (EEG MMI) dataset from the Physionet bank [3, 12] were chosen due to the simplicity of such motions in a potential practical application of such a system and the abundant use of such tasks in BCIs.

Preprocessing: The EEG signals are epoched and preprocessed using the MNE package [4]. Each individual epoch was band-pass filtered using a Finite Impulse Response windowed filter between 0.5 Hz to 42 Hz and normalized to zero mean and z-scores from zero.

Classification: The unnormalized cross-correlation is used to measure the similarity between two signals and is applied in a template matching procedure between the 64 electrode signal pairs from the samples being compared. The maximal value of the cross-correlation is used to create a 64×1 feature vector. Support Vector Machines (SVM) with linear and radial basis function (RBF) kernels are applied to this feature vector.

Eye Tracking Authentication

Task and Dataset: The dataset A of the EMVIC 2012 competition, containing positional data of the eye fixations across time, was utilized [8]. The dataset contains eye tracking data from a "jumping dot stimulus" task. Samples were disproportionately grouped towards certain subjects. To reduce dataset bias, we pool subjects with fewer than 40 samples into a separate group called the "unauthorized users group". This procedure has the positive side effect of allowing for more variety and fewer samples per subject for unauthorized users which better reflects real-world conditions.

Classification: A random forest classifier with 100 trees was trained on feature vectors composed of the concatenated eye-tracking signals. The model predicts an array of posterior probabilities that the given sample belongs to each of the possible labels consisting of $n = 5$ authorized users and the unauthorized group (totally $n + 1 = 6$ bins).

Models	FAR	FRR
SVM Fusion	23.6%	29.2%
Weighted Mean	60.5%	23.6%
EEG	42.1%	27.8%

Figure 3: Comparison of fusion methods and EEG baseline in cases of low confidence

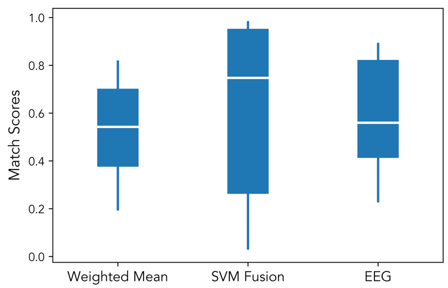

Figure 4: Positive ground truth: The median match-score of the SVM fusion method is far lower compared to the other systems in this case indicating high confidence of a negative prediction.

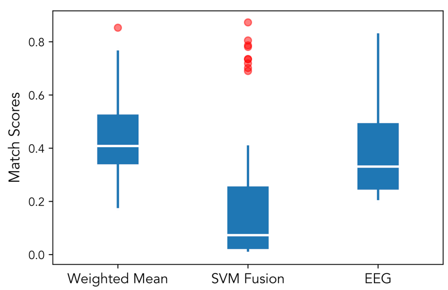

Figure 5: Negative ground truth: The median match-score of the SVM fusion method is far higher compared to the other systems in this case indicating high confidence of a positive prediction.

Multimodal Fusion

Each subject in the EMVIC dataset was matched to a participant in the EEG MMI dataset to create a fused dataset of hypothetical subjects with Motor imagery and Eye Tracking data. We thus have 5 authorized subjects and 32 unauthorized subjects in our newly composed dataset. We conduct match-score level fusion as it preserves adequate discriminating information and is modular in its execution. Here, two fusion methods have been implemented: weighted mean and fusion by SVM with linear kernels, each providing a normalized match-score from the individual predictions.

RESULTS AND DISCUSSION

Individual Modalities:

The results for the individual modalities are provided in Table 1 and Table 2. We tested the EEG system using an 80:20 train-test split. We report only the metrics of the linear kernel SVM due to its significantly better performance compared to the RBF kernel SVM. For the Eye Tracking system, we assume the label with maximum score in the distribution as the match-score. An 80:20 train-test split was applied and the various metrics for the 6 way classification are described.

Multimodal Evaluation

We did not observe appreciable improvement in ROC curves, EER values, and AUC values when using the fusion system versus the EEG system. In fact, the weighted average method performed worse compared to the EEG baseline and the SVM fusion method provided marginal improvements. However, when examining low confidence predictions of the EEG system (0.2 to 0.8). From the median match-score of the SVM fusion method in positive and negative ground truths (Figure 5, Figure 4), the system shows greater decisiveness towards the correct label. This results in the FAR values being significantly lower for the SVM Fusion as compared to other methods without the FRR being affected as can be seen in Table 3. Here, we see eye tracking providing a benefit when EEG confidences are low without affecting the values of high confidence.

CONCLUSIONS AND FUTURE WORK

In this paper, we provide a feasibility study towards the possiblity of using EEG and eye tracking for multimodal biometric authentication. We used an SVM with a linear kernels and random forest classifiers and found greater recognition accuracy than the individual modalities alone when tested on the composition of datasets. Given these positive results, we expect to extend this study effort for a more thorough and robust evaluation. Additionally, as the datasets used in this experiment are smaller than ideal for deep learning methods, we hope to use our newly collected large scale dataset for deep learning evaluations.

REFERENCES

[1] Sarah N. Abdulkader, Ayman Atia, and Mostafa-Sami M. Mostafa. 2015. Brain computer interfacing: Applications and challenges. *Egyptian Informatics Journal* 16, 2 (July 2015), 213–230. https://doi.org/10.1016/j.eij.2015.06.002

[2] R. Das, E. Maiorana, and P. Campisi. 2018. Motor Imagery for Eeg Biometrics Using Convolutional Neural Network. In *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2062–2066. https://doi.org/10.1109/ICASSP.2018.8461909

[3] Goldberger Ary L., Amaral Luis A. N., Glass Leon, Hausdorff Jeffrey M., Ivanov Plamen Ch., Mark Roger G., Mietus Joseph E., Moody George B., Peng Chung-Kang, and Stanley H. Eugene. 2000. PhysioBank, PhysioToolkit, and PhysioNet. *Circulation* 101, 23 (June 2000), e215–e220. https://doi.org/10.1161/01.CIR.101.23.e215

[4] Alexandre Gramfort, Martin Luessi, Eric Larson, Denis A. Engemann, Daniel Strohmeier, Christian Brodbeck, Lauri Parkkonen, and Matti S. Hämäläinen. 2014. MNE software for processing MEG and EEG data. *NeuroImage* 86 (Feb. 2014), 446–460. https://doi.org/10.1016/j.neuroimage.2013.10.027

[5] C. D. Holland and O. V. Komogortsev. 2013. Complex eye movement pattern biometrics: Analyzing fixations and saccades. In *2013 International Conference on Biometrics (ICB)*. 1–8. https://doi.org/10.1109/ICB.2013.6612953

[6] J. Hu. 2009. New biometric approach based on motor imagery EEG signals. In *2009 International Conference on Future BioMedical Information Engineering (FBIE)*. 94–97. https://doi.org/10.1109/FBIE.2009.5405787

[7] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. 2008. Biometric Template Security. *EURASIP J. Adv. Signal Process* 2008 (Jan. 2008), 113:1–113:17. https://doi.org/10.1155/2008/579416

[8] Pawel Kasprowski, Oleg Komogortsev, and Alex Karpov. 2012. First Eye Movement Verification and Identification Competition at BTAS 2012. https://doi.org/10.1109/BTAS.2012.6374577

[9] S. Marcel and J. D. R. Millan. 2007. Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29, 4 (April 2007), 743–752. https://doi.org/10.1109/TPAMI.2007.1012

[10] R. Moskovitch, C. Feher, A. Messerman, N. Kirschnick, T. Mustafic, A. Camtepe, B. Lohlein, U. Heister, S. Moller, L. Rokach, and Y. Elovici. 2009. Identity theft, computers and behavioral biometrics. In *2009 IEEE International Conference on Intelligence and Security Informatics*. 155–160. https://doi.org/10.1109/ISI.2009.5137288

[11] K. Revett, F. Deravi, and K. Sirlantzis. 2010. Biosignals for User Authentication - Towards Cognitive Biometrics?. In *2010 International Conference on Emerging Security Technologies*. 71–76. https://doi.org/10.1109/EST.2010.32

[12] Gerwin Schalk, Dennis J. McFarland, Thilo Hinterberger, Niels Birbaumer, and Jonathan R. Wolpaw. 2004. BCI2000: a general-purpose brain-computer interface (BCI) system. *IEEE Trans Biomed Eng* 51, 6 (June 2004), 1034–1043. https://doi.org/10.1109/TBME.2004.827072

[13] H Van Dis, M Corner, R Dapper, G Hanewald, and H Kok. 1979. Individual differences in the human electroencephalogram during quiet wakefulness. *Electroencephalography and Clinical Neurophysiology* 47, 1 (July 1979), 87–94. https://doi.org/10.1016/0013-4694(79)90035-X

[14] M. Wang, H. A. Abbass, and J. Hu. 2016. Continuous authentication using EEG and face images for trusted autonomous systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. 368–375. https://doi.org/10.1109/PST.2016.7906958

[15] Jonathan R Wolpaw, Niels Birbaumer, Dennis J McFarland, Gert Pfurtscheller, and Theresa M Vaughan. 2002. Brain–computer interfaces for communication and control. *Clinical Neurophysiology* 113, 6 (June 2002), 767–791. https://doi.org/10.1016/S1388-2457(02)00057-3

[16] Wei-Long Zheng, Bo-Nan Dong, and Bao-Liang Lu. 2014. Multimodal emotion recognition using EEG and eye tracking data. In *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 5040–5043.