BRAIN-BASED AUTHENTICATION: TOWARDS A SCALABLE, COMMERCIAL GRADE SOLUTION USING NONINVASIVE BRAIN SIGNALS.

Ronen Kopito,[1] Aia Haruvi,[1] Noa Brande-Eilat,[1] Shai Kalev,[1] Eitan Kay,[1] Dan Furman.[1]

[1] *Arctop Inc., R&D, Kaufmann St. 4, Tel Aviv-Yafo, 6801296, Israel.*

ABSTRACT

In this study we report on a field test where we asked if it is feasible to deliver a scalable, commercial-grade solution for brain-based authentication currently given available head wearables. Sixty-two (62) participants living across the United States in autumn 2020 completed four (4) at-home sessions over a single (1) week. In each session there were six (6) authentication events consisting of rapid presentation of images (10Hz) that participants watched for 10 seconds while recording their brain signal with an off-the-shelf brain signal measuring headband. The non-stationary nature of the brain signal, and the fact that the signal results from a superposition of hundreds of simultaneous processes in the brain that respond to context makes the data unique in time, unrepeatable, and unpredictable. Even when a participant watched identical stimuli, we find no two periods of time to be alike (Fig. 4B) and furthermore, no two combinations of time periods are alike. Differences within people (intra-) and across people (inter- participant) from session to session were found to be significant, however stable processes do appear to be underlying the signal complexity and non-stationarity. We show a simplified brain-based authentication system that captures distinguishable information with reliable, commercial-grade performance from participants at their own homes. We conclude that noninvasively measured brain signals are an ideal candidate for biometric authentication, especially for head wearables such as headphones and AR/VR devices.

1. Introduction

Authentication confirms that users are who they say they are. A simple example of an authentication method is an alphanumeric password, 'abc123,' while a complex example is a digital fingerprint, as is captured by scanners found in most smartphones today. Effective authentication is critical to security for both consumers and enterprises. Because of the high frequency of use of authentication systems, methods need to be convenient in addition to secure. That balance - between convenience and security - is a defining characteristic of authentication systems. Strong authentication systems that are very secure are often very cumbersome to implement and maintain, while weak authentication methods are convenient but have been responsible for countless data breaches because of their equivalent ease of being hacked (in any number of ways). The "password chaos" of modern life seems to have reached a boiling point and it is clear that future personal and professional computing systems will need improved methods that both deliver increased security along with an increased convenience that insures adherence to the security protocols.

Biometric authentication is any method that uses natural occurring information, such as fingerprints, faces, palm veins, irises, and brain signals, to verify one's identity. Biometrics are always innate, intrinsic measures to the individual, although there are many variations. For example fingerprints are static, and most people only have 10: so if fingerprints are stolen, the victim has a biometric issue for life. Unlike fingerprints or other visible biometrics that can be surveilled by cameras or microphones,

like eye irises, faces, gait, and speech, brain signals are invisible and are thus one of the more unique biometric signatures.

Brain-based authentication is the process of verifying an individual's identity by using their brain signal. Since at least the late 1980's[1] neuroscientists have observed that noninvasively measured human brain signals carry personally identifying information[2,3] that differentiates between family members and across a broad population.[4,5] Brain signals are always changing and extremely complex, and therefore make an ideal candidate for use as a biometric.[6,7,8] Indeed, many groups have attempted to build biometric authentication systems based on these signals.[9,10,11,12,13,14,15,16,17,18,19] The overall usability of systems in the literature has been reported to be increasing since 2010,[20] however most are still far from proving field-viability and having utility for existing authentication providers.[21,22] Brain data is commonly collected in a laboratory under controlled conditions where a trained technician was an essential part of the brain measurement procedure, and often tests of performance are only done with a small number of people, with all measurements taking place in a single session which maps poorly to normal daily consumer electronics use-cases where individuals take off and put back on the brain measurement device between authentication events.[23,24,25,26]

While brain biometric identity appears to be one of the most natural, powerful methods for head wearables, its robustness has not been sufficiently vetted in real world conditions that parallel the end use cases such as:

- Professionals who work remotely and wear headsets as part of their daily work and need to be authenticated across applications throughout the day.
- Gamers in VR who want a seamless, hands-free and voice-free way of authorizing in-game purchases and having their profile load on different devices.
- e-Commerce consumers whose check-out experience can be smoother and more secure without all the chaos of current passwords and 2-factor authentication systems.
- Medical and other high-strain environments where the ability to authenticate using a minimal sensor that only needs minimal contact provides extra utility.
- Air gapped security systems where there are strict demands on performance and all biometric processing needs to be performed on-edge.

We set out to perform here a generalizable field test of brain-based authentication using brain signals measured noninvasively from people in their regular, real world contexts, that would speak to the use-cases. This feasibility test "in the wild" advances the applied science of brain biometric analysis towards practicality and scalable implementations since here all participants were completely new (naïve users) to the system, enrolled themselves from home using a self-guided calibration, used a comfortable head wearable for hours at a time with minimal data and battery requirements, and performed repeated authentication measures across several different days, simulating the need for authentication to work regardless of time of day and to be robust to changes in brain state and ambient noise inherent to the measurements.

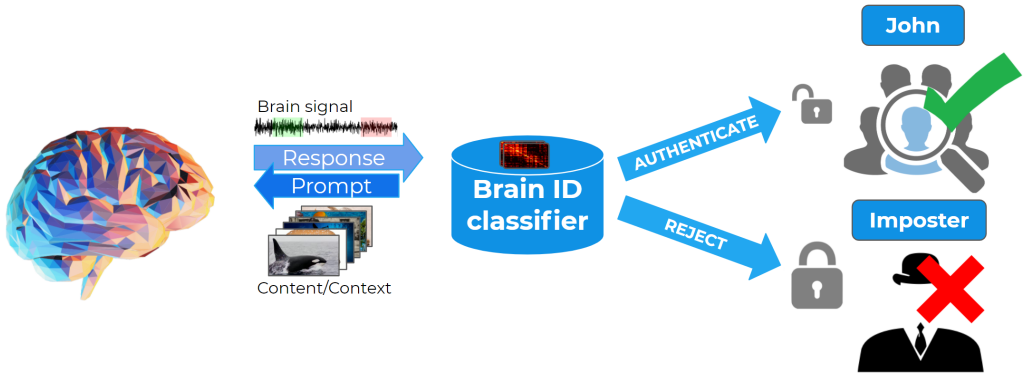


Fig. 1. Schematic illustration of the brain-based authentication process. Brain signal is recorded while participants watch images ("Prompt"). The brain response (e.g. "John's brain signal") is fed into a trained classifier of that participant. The classifier decides if the brain pattern matches the participant (authenticates "John") or not (rejects).

2. Methods

a. *Participants.* Sixty-two (62) participants completed four (4) sessions over a single (1) week at their own home. Adult participants were recruited from an opt-in screening panel and came from all five (5) major regions of the continental United States (Northeast, Southwest, West, Southeast, and Midwest). Only participants who reported, normal vision, or vision that was corrected to normal with contact lenses were included. We excluded volunteers who reported using medication that might influence the experiment or other neurological or psychiatric conditions that could influence the results. Written informed consent was obtained from all participants before screening and the main experimental sessions. Thirteen (13) participants were ultimately excluded for problematic survey response patterns within the study and/or invalid brain data, leaving 49 participants (mean age= 36, SD=8.25, 16 females) enrolled and eligible to be included in the analysis.

b. Sessions. Individuals participated in the study from their own homes where they recorded sessions at their own pace, over one week as detailed in Haruvi et al 2021.[27] Each participant received a kit that included headphones (Sony), a brain signal measuring headband (InteraXon) and a tablet computer (Samsung) with a designated app (Arctop) to perform the experiment. Each participant recorded four sessions, one hour long each. Towards the end of each session, six (6) authentication events were presented. Each authentication event started with a message declaring the upcoming event and instructing the participant to stay steady, a fixation period which enables the participant time to get prepared (2 seconds) and then presentation of rapid images at 10Hz for 10 seconds (Fig. 2).

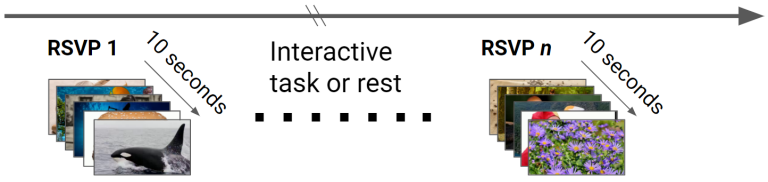


Fig. 2. Time course of authentication using rapid serial visual presentation (RSVP) prompts. At each authentication event a sequence of images rapidly (10Hz) changes for 10 seconds while the brain response is recorded. In each session, six RSVP events were presented to each participant.

c. Data Acquisition. While participants were engaging in a variety of tasks, their electrical brain activity was recorded using InteraXon's Muse-S device, a portable, noninvasive electroencephalography (EEG) device weighing 41 grams. The device includes four dry fabric EEG sensors (sampling rate: 256 Hz), photoplethysmography (PPG) sensors (for heart rate) and motion sensors (gyroscope and accelerometer). The EEG sensors are located on the scalp, two frontal channels (AF7 and AF8) and two temporals which rest behind the ears (TP9 and TP10), with the reference channel at Fpz. The headbands were put on by participants themselves with the assistance of a Quality Assurance screen that started each session by showing participants in real-time their signal quality, making it easy to adjust the headband properly for optimal signal quality (Fig. 3).

d. Preprocessing and feature extraction. Data analysis was performed only within the RSVP event, where the filtered signal was segmented into epochs of 2 seconds in length, using a sliding window with a stride of 250ms (4Hz) such that an event included 31 epochs. A band-pass filter (0.5-46Hz) was applied on each channel. Comprehensive feature extraction and engineering was not the goal of this current study. Here we aimed for effective information capture without deeper optimization to first test the core principles. Accordingly, for each EEG epoch, the following features were calculated: power spectrum features - each segment was transformed to the frequency domain using Welch method, and for each channel, the average power for each of the traditional frequency bands (Alpha, Beta, Gamma, Delta, Theta) was calculated. Power spectrum interactions, time domain features such as averages, standard-deviations, kurtosis, entropy and number of zero-crossing points. Pairwise correlations between channels in the different frequency bands were calculated as well. For each epoch, a total of 140 features were extracted.

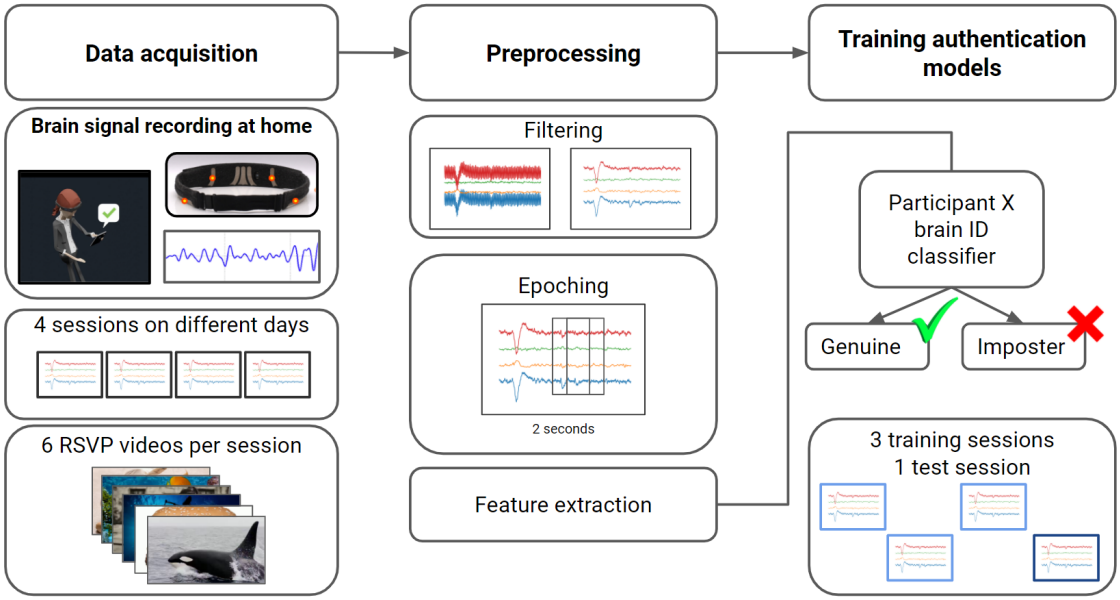


Fig. 3. Schematic illustration of the processing pipeline. Data acquisition included at home EEG recordings of 4 sessions, each on a different day. Each session included 6 RSVP videos (Fig 2). EEG processing included filtering the signal, feature extraction and training a machine learning authentication classifier per participant. The classifier decided if the input belongs to the participant (Genuine) or not (Imposter).

e. Models training. For each participant we had a total of 24 RSVP events (Supp. Video 1), which we collected over the 4 sessions. For each participant, three sessions (18 events), were chosen randomly to be used for training. The fourth session was used for testing (6 events). The authentication

prediction works on two levels for each event, once at the epoch level, and second is the final conviction regarding the whole event identity (genuine or imposter).

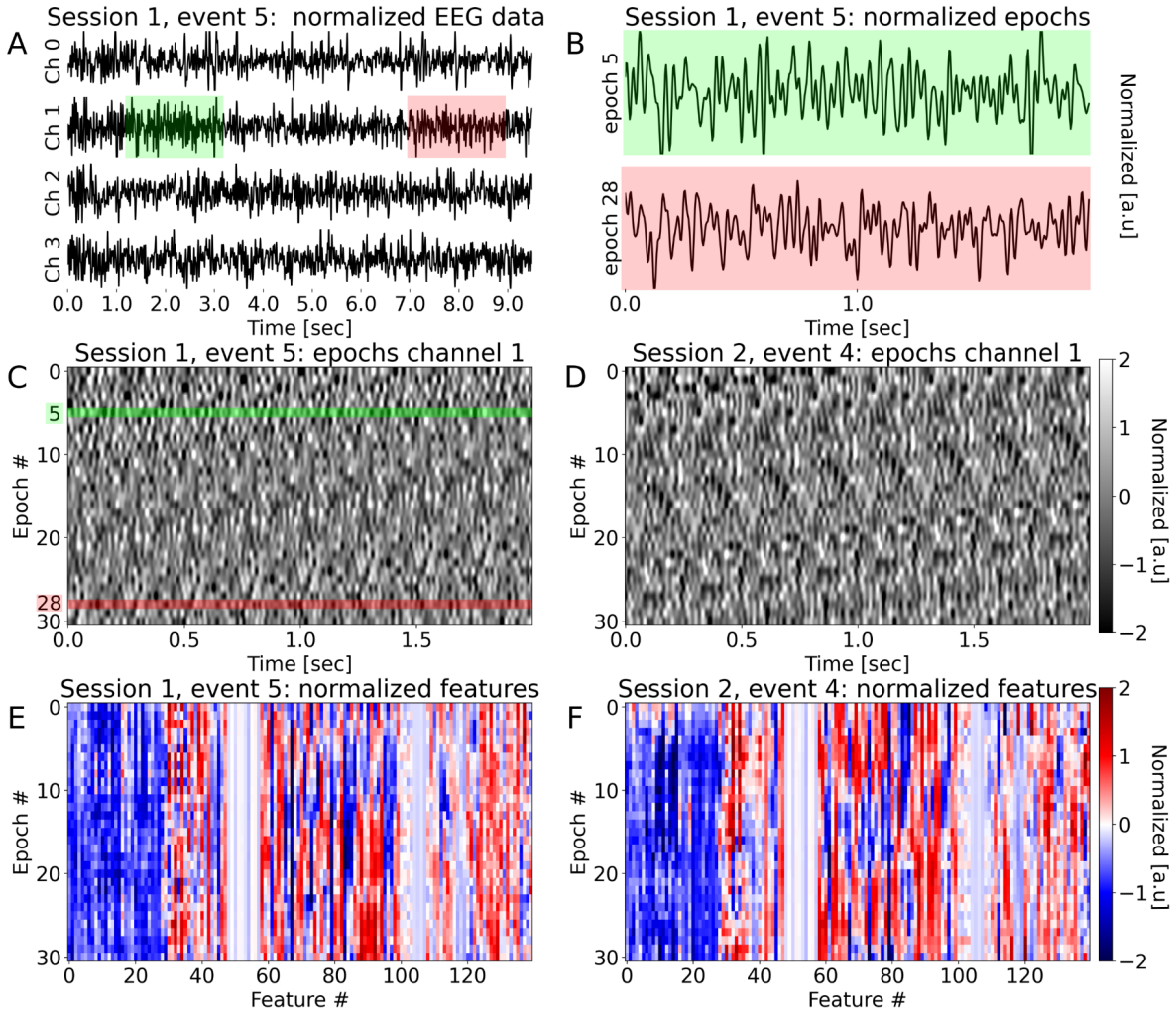


Figure 4. Event epoching. **A**. The RSVP authentication event is a normalized filtered EEG signal composed of four channels, 9.5 seconds long. Each event signal is segmented into 31 epochs (where each epoch carries 4 channels), 2 seconds in length, and with a sliding window of 0.25 sec stride. **B**. Channel-1 of epochs #5, and #28 (top, bottom) are shown for demonstration. Note, that the shaded areas colored in green and red in panel A correspond for these epochs respectively. **C.** The epochs of the event signal in A, can be rearranged into an image (here again just channel-1 is shown). Where each row is an epoch, and the epochs are time ordered vertically. In **C** and **D**, events which were taken from the same participant (#39), but from different sessions are shown. **E**, **F** the corresponding features of the epochs presented in C, D are presented. Note that the calculation of epoch features involves all epoch channels. While the non-stationary nature of the EEG data dictates that the events (as shown in C, D) are totally not resembled to each other. The features images (E, F) demonstrates high similarity.

For each participant an authentication model was trained first at the epoch level. Model classification was done with XGBoost classifier (binary classification). Epochs (feature space, 140 features per epoch) of genuine identity were labeled as one (186 epochs), while epochs from the rest of the participants were of imposter identity, and labeled as zero (26784 epochs). Thirty percent of training

data (random and equal split) was dedicated for validation and to determine epoch thresholding. Standardization procedure over the training epochs was applied. Later, the training features means and standard deviation values were used to normalize the validation and testing data. Epoch's threshold for classification was optimized to minimize false acceptance rate (FAR), while maximizing true rejection rate (see Supp. Fig. 3). Epochs prediction for the validation data after thresholding exhibited high accuracy for all participants (average accuracy=0.9865, STD=0.00929). A final decision about participant identity was given at the event level. Event threshold, as before, was determined by an optimization algorithm, but here it was done over the validation data.

After thresholding, mean event accuracy for the validation data was 0.9965, with STD=0.00041. The number of events in the validation data is 294, suggesting that after thresholding all events were identified correctly except one. For the epoch level at the test data we have used the same epoch thresholding as calculated in the training process, while for the event threshold we applied a constraint which demands a minimum of 40% of epochs to pass in order to declare the event as genuine.

3. Results

Using brain signals captured during discrete RSVP events (10 seconds of brain data sampled at 256Hz, containing 2 forehead region and 2 ear region brain data channels), we computed brain-based identities. We found that the non-stationary nature of the signal reflecting the superposition of hundreds of simultaneous processes in the brain makes the signal unique in time, unrepeatable, and unpredictable: even when the brain is stimulated by identical stimuli, no two epochs are alike (Fig. 4B). Furthermore, no two events are alike: in Fig. 4C & 4D, the epochs of an event (EEG signal space) are aligned vertically, ordered in time, creating an identity image. This representation showcases how none of the epochs are identical, nor are the full identities at the event level. In contrast, epochs of the same events as previous at the feature space level are on the average highly correlated (Fig. 4E & 4F).

The performance of our authentication system is summarized in Fig. 5. The averaged false acceptance rate (FAR) is 9% and the false rejection rate (FRR) is 13%, making the solution sufficient for certain commercial authentication use-cases, but not all. The averages shown here are the means over the individuals' FAR, FRR. Out of the total number of participants in this experiment (49), 37 participants have FRR=0, where 24 participants have FRR=0 and FAR<=9% (Supp. Table 1).

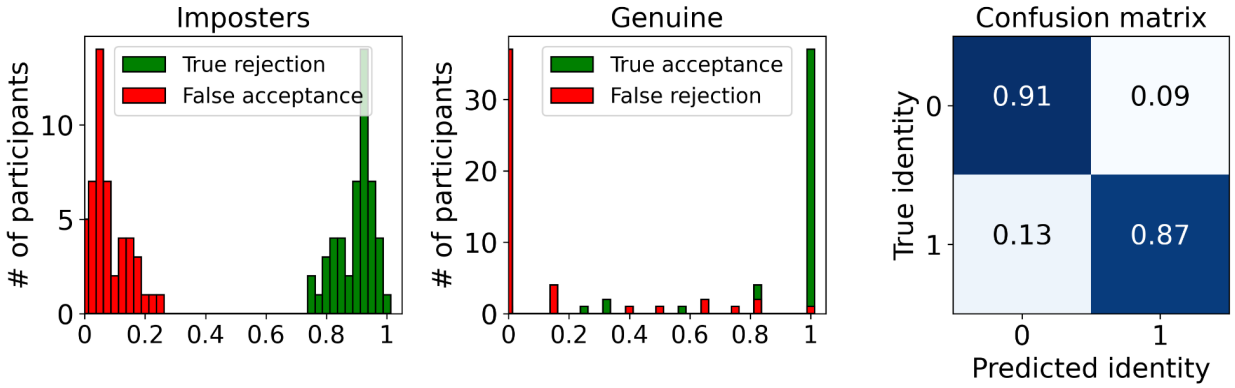


Figure 5. Summary of model performance. Forty nine participants were included in the final test. Each participant had six genuine events, and 287 imposter events. All together in this experiment we used 294 genuine events, and 14063 imposter events. In **A**, and **B** histograms of authentication system performance at the participant level is present. In A, the performance regarding imposters (true rejection rate, and false acceptance rate). In B, the performance regarding genuines identities (true acceptance rate, and false rejection rate). These values were first calculated per each participant, and then distribution was calculated. **C**, A confusion matrix summary, showing the averaged performance over all participants. A detailed performance summary per each participant can be found in supp. Table 1.

In Fig. 6(A-D), four examples of participants' brain identities are presented. Indeed, it is apparent that each brain identity carries a unique pattern that is distinguishable from the others. We would like to generalize the idea of brain identity over all the participants in our experiment, and of course for this reason the human eye is inadequate to define the important characteristics and their weightings. So we proceed in a more mathematically forward manner, with a rigorously and quantified method where we posit that if the RSVP events are going to be used in our authentication system as the brain identity, two criteria must be fulfilled:

1. Similarity between different events of the same person is kept high: even and especially, for events which were recorded at different occasions.
2. Events of different people are distinguishable.

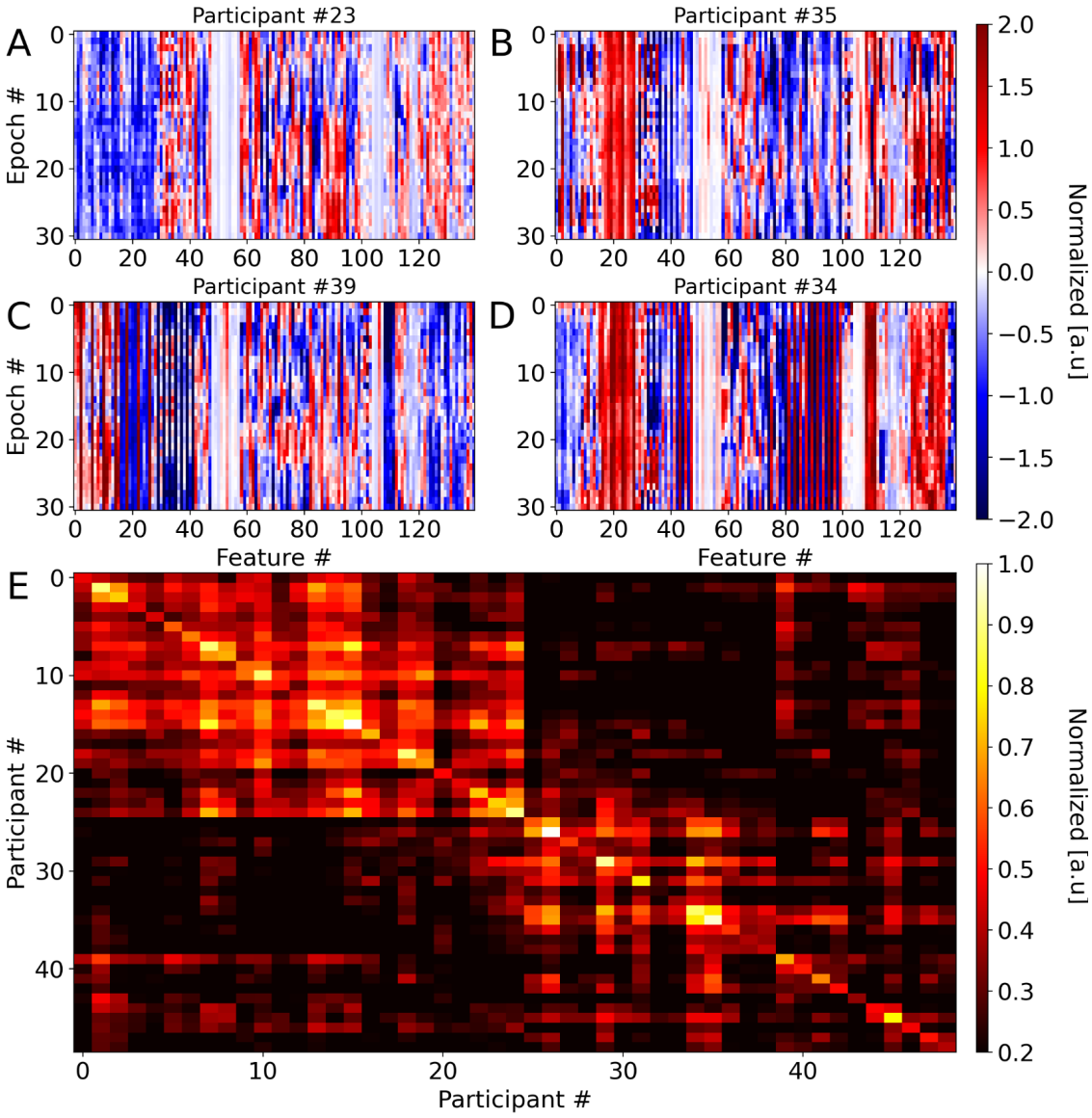


Figure 6. Similarity among intra and across inter participants events. Panels **A**, **B**, **C**, and **D** show the features of single event for different participants (#23, #35, #,39, and #34 respectively). The pattern of an event appears more robust, as the features values are repeatedly conserved across many epochs . On the other hand, it looks like for each participant the pattern is specific. The similarity (or dis-similarity) between events can be measured by a correlation coefficient. In **E** we present the event correlation matrix, where element E*ij*, is the average pairwise correlation across all training events of participant *i* and participant *j*. Note that the intra-correlation coefficients (diagonal) are usually higher than inter-correlation (off-diagonal), suggesting that for the same participant the pattern of different events is conserved, and patterns of different participants are different. This understanding leads us to the idea of an authentication system by events. Also note that the order of the participants in E, is in accordance with the hierarchy cluster tree shown in **Supp. Fig. 1**. The matrix here is normalized.

The similarity between two events (at the feature space) can be measured by the Pearson correlation coefficient between the means of the events giving the similarity between two participants as the mean of all pairwise events correlations of these participants. In Fig. 6E, the normalized correlation matrix across all participants is presented. Values are represented by colors (colorbar 0.2-1), higher values suggest higher similarity. The participants' order along the axes was determined using a hierarchical clustering algorithm (see Supp. Fig. 1). The averaged similarity between events belonging to one participant (intra correlation) is the diagonal element of the correlation matrix, while the averaged similarity between events of two different participants (inter correlation), is the off diagonal matrix. In general, we have found that for all participants, the similarity of intra correlation is higher than the inter correlation (Fig. 6E, Supp. Fig 2).

The histograms in Supp. Fig. 2, shows that most of the inter- and intra-participant correlation are indeed separated: the intra-correlation of more than half of the participants is higher than 0.7, where most of the inter-correlations are lower than 0.35. The inset in Supp. Fig. 2 suggests a linear relation between the mean inter-correlation of a participant and its intra correlation. Namely, participants having relatively low intra-correlation (~0.5), their inter-correlations will be low as well (~0.25).

For the trained model, a brain identity probability above the threshold was determined to be a genuine identity, while those below the threshold were judged imposters. In Fig. 7A,B,&C, one can find an explicit example for this thresholding step. In our system the final identity is regarding the full RSVP event. Here, only events where more than 40% of epochs were passing the epoch threshold will be regarded as belonging to genuine identity, otherwise it is an imposter Fig. 7A1,B1&C1.

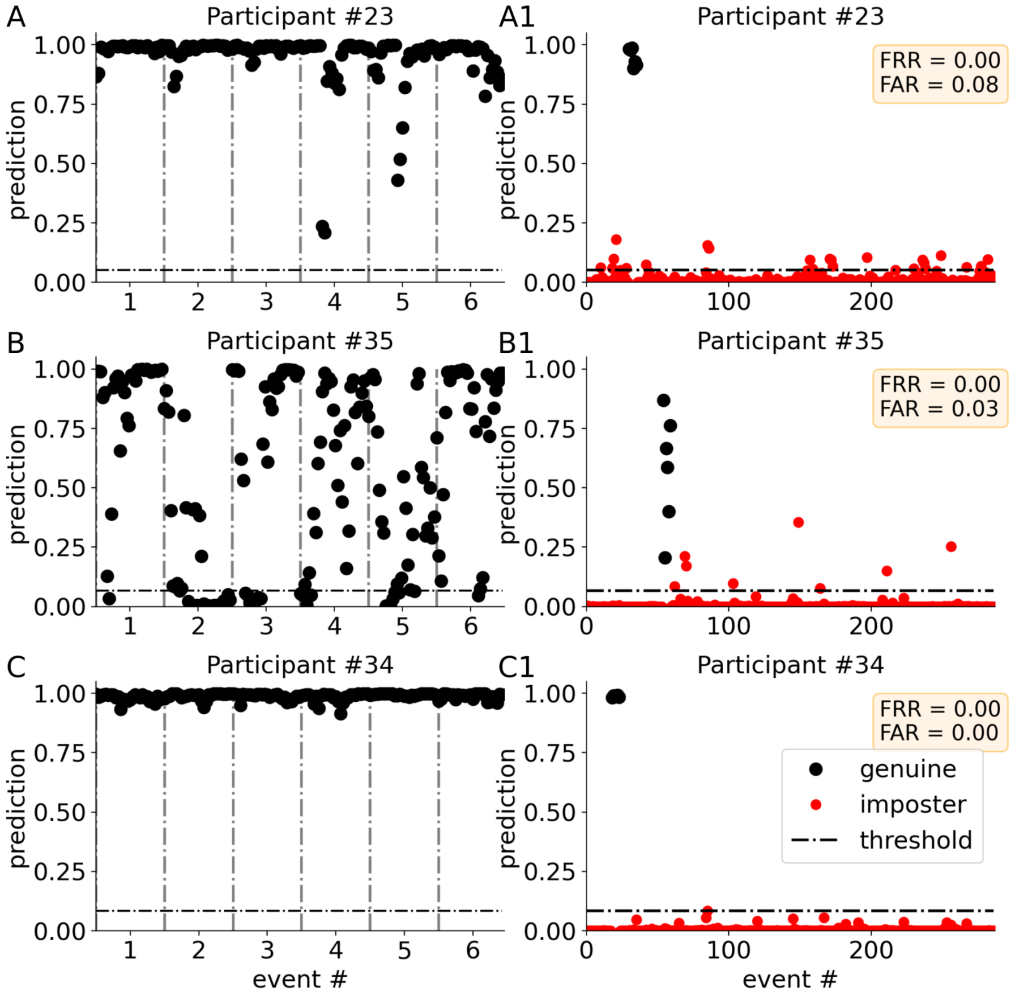


Figure 7. Event prediction. The events are segmented into 31 epochs. The probability of each epoch to be of a genuine identity or of an imposter one is determined by a model. Probabilities above the threshold (black dash line) belong to genuine identity, and if below the threshold, to an imposter. Threshold was determined previously in the training process (see Supp. Fig. 3). **A**, **B**, **C** the predictions of three models trained for three participants (sub #23, # 35, #34 respectively) are presented. Here the epochs under test are only of genuine identity (black dots). While in **A**, and **C** all predictions are above threshold, in **B** some of the predictions are below the threshold. The final decision whether the event is of genuine identity is determined only if more than 40% of epochs are above the threshold. In **A1**, **B1**, **C1** full test prediction is shown for the same three participants. The test included 294 events, where each participant has 6 genuine events. Events of genuine identity are marked in black dots and imposter events are in red dots. In all three cases all genuine events were identified correctly, having zero false rejection rate (FRR=0). As for the imposters, only in **C1**, all imposter events are below the threshold, with zero false acceptance rate (FAR=0). The final FRR and FAR of each participant is shown in the yellow windows.

We asked what will be the performances of the authentication system when only certain brain signal information is considered. Explicitly, we repeated the training procedure (Methods) but this time with only the power spectrum features of the following brainwave modes: Delta(0.5-4Hz), Theta(4-8Hz), Alpha(8-12.5), Beta(12.5-30Hz) and Gamma(30-48), and with some combinations (Alpha-Beta, and Theta-Alpha-Beta). We found, Fig. 8, that usually for these features FRR can reach low values while the FAR is high. The system can never reach low values for both quantities. As the number of features is increasing the better the performances of the authentication system.

Features type	False acceptance rate	False rejection rate
Delta	0.83	0.02
Theta	0.82	0.02
Alpha	0.75	0.03
Beta	0.36	0.17
Gamma	0.28	0.22
Alpha Beta	0.30	0.14
Theta Alpha Beta	0.27	0.13
All PSD brain waves	0.17	0.16
All features	0.09	0.13

Figure 8. Model performance as function of feature types. The same training and testing datasets were used for all models. The power spectrum density (PSD) of the following frequency bands were used as features. Delta(0.5-4Hz), Theta(4-8Hz), Alpha(8-12.5), Beta(12.5-30Hz) and Gamma(30-48). Each bandpass has four features, corresponding to the number of eeg channels. When using only one type of brainwave, the averaged FRR may reach low levels, but the FAR always remains high. Even when all brain signal PSD features are used, both FAR and FRR do not cross 0.85.

Given that the goal of this current field test was to evaluate feasibility of a scalable, commercial-grade brain-based authentication system, advanced data engineering methods were not applied to boost performance further. Future field tests will report on our use of other feature sets in concert with different machine-learning architectures to deliver superior, product level authentication performance.

4. Discussion

We set out to perform a generalizable field test of a brain-based authentication method using noninvasively measured brain signals, where all participants were completely new (naive users) to the system, enrolled themselves from home, used a comfortable head wearable for hours at a time with minimal data and battery requirements, and performed repeated authentication measures across several different days. In whole, this amounted to a reasonable simulation of the real contexts authentication methods need to operate in to be commercially viable. Specifically, these methods must work regardless of time of day and to be robust to changes in brain state (before coffee, after coffee, etc.) and ambient noise inherent to measurements made outside of controlled laboratory conditions.

In the current test we used a simplified feature set and simplified machine learning methods to evaluate the basic premise that brain-based authentication was approaching commercial-grade levels. Many variations on the approach taken here are possible and based on the results several questions may arise. For example, because high correlation was visible not just among epochs of the same event, but also between the events themselves, one could argue that the epoch level is all that is needed - why not use it as the brain identity? It's possible, but the correlation among epochs is high on the average, and therefore the use of a few epochs instead of only one increases both the sensitivity (true acceptance rate) and specificity (true rejection rate) of the authentication system in our findings here. These are all tunable parameters depending on the demands of the authentication

task, and future research will clarify the timescales at which the optimal information for identification verification occurs.

Wearables that touch the head, such as headphones or AR/VR devices, are a natural form factor for brain-based authentication. The demand for both strong and convenient authentication solutions drove our design of the paradigm for prompt-response analysis, and it is notable that the rapid image prompt-response paradigm evaluated here (with users watching images on a tablet while wearing a headband) has been validated in AR (Supp. Video 2) using a Microsoft Hololens.

Given the performance observed here and ease-of-use of this method for head wearables, brain-based authentication appears to be one of the most intuitive and powerful authentication solutions for next generation headworn computers. Brain identities, like any other biometric identity, will need to conform to privacy standards and be offered within protected software and chip architectures such as those pioneered for fingerprint scanners and face recognition.

Biometrics are uniquely comfortable and convenient to use because they do not require the user to remember anything (like a password), and carry anything (like a physical key). Biometrics offset the cognitive load of password management plus the risks associated with alphanumeric passwords, and offer the promise of obviating passwords altogether in future computing ecosystems. For now, brain identity is at a nascent stage of adoption and the solution presented here represents one of the more scalable designs, since we can easily increase the dataset to more participants and more events within the principled framework of forcing divergences in inter-participant data and convergences intra-participant data.

Furthermore, the wearable headband that people put on themselves in this test to measure their brain signal is a consumer device that is currently available and shipping worldwide, highlighting the lack of need for exotic or rare materials to acquire sufficient brain signal, nor specialized laboratories or facilities. More information in the brain signal remains unexplored here being outside the scope of the current field test and report. Future research will develop out concepts related to the information boundary in the signal further, the takeaway here is primarily related to the applied goal of passwordless authentication: for which brain-based authentication was found to be a comfortable, natural method. For head wearables in particular, brain biometric identity warrants continued testing across expanded participant populations and implementation in commercial devices that can benefit.

5. Conclusion

Here we showed that a relatively simple brain-based authentication system could use noninvasively measured brain signals from consumer quality head wearable devices to differentiate between users with high degree of certainty. Authentication using noninvasively-measured brain signals in this way was found to not only be feasible, but robust: the correlation matrices derived from the current test find our computed brain identities to be readily distinguishable between different participants and consistently similar among participants, satisfying the core requirements of a commercial-grade biometric authentication system. The complexity inherent to human brain signals was, therefore, found to not be too volatile to be leveraged for steady, reliable use as a passwordless authentication method.

We built and validated a scalable software infrastructure for brain-based authentication at a commercial-grade, where the framework here provides easily for continual performance improvement with additions of new participants. As the methods were designed around generalizable patterns observable during limited windows of time, at any time, it is clear that there is value to continued data collection at larger scales and across additional contexts. For both inter-subject variability and to further clarify the invariant patterns underlying intra-participant variability, expanded data collection can be beneficial, however the present sample is sufficient to conclude that brain-based authentication is already a viable method for commercial use.

References

1. Stassen, H. H., G. Bomben, and P. Propping. "Genetic aspects of the EEG: an investigation into the within-pair similarity of monozygotic and dizygotic twins with a new method of analysis." Electroencephalography and clinical neurophysiology 66, no. 6 (1987): 489-501.
2. Poulos, Marios, Maria Rangoussi, and Nikolaos Alexandris. "Neural network based person identification using EEG features." In 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings. ICASSP99 (Cat. No. 99CH36258), vol. 2, pp. 1117-1120. IEEE, 1999.
3. Poulos, M., M. Rangoussi, N. Alexandris, and A. Evangelou. "Person identification from the EEG using nonlinear signal classification." Methods of information in Medicine 41, no. 1 (2002): 64-75.
4. Marcel, Sebastien, and José del R. Millán. "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation." IEEE transactions on pattern analysis and machine intelligence 29, no. 4 (2007): 743-752.
5. Van Beijsterveldt, C. E. M., and G. C. M. Van Baal. "Twin and family studies of the human electroencephalogram: a review and a meta-analysis." Biological psychology 61, no. 1-2 (2002): 111-138.
6. Thorpe, Julie, Paul C. Van Oorschot, and Anil Somayaji. "Pass-thoughts: authenticating with our minds." In Proceedings of the 2005 workshop on New security paradigms, pp. 45-56. 2005.
7. Wang, Min, Jiankun Hu, and Hussein A. Abbass. "BrainPrint: EEG biometric identification based on analyzing brain connectivity graphs." Pattern Recognition 105 (2020): 107381.
8. Piplani, Tanya, Nick Merill, and John Chuang. "Faking it, Making it: Fooling and Improving Brain-Based Authentication with Generative Adversarial Networks." In 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1-7. IEEE, 2018.
9. Abo-Zahhad, Mohammed, Sabah Mohammed Ahmed, and Sherif Nagib Abbas. "State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals." IET Biometrics 4, no. 3 (2015): 179-190.
10. Armstrong, Blair C., Maria V. Ruiz-Blondet, Negin Khalifian, Kenneth J. Kurtz, Zhanpeng Jin, and Sarah Laszlo. "Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics." Neurocomputing 166 (2015): 59-67.
11. Ashby, Corey, Amit Bhatia, Francesco Tenore, and Jacob Vogelstein. "Low-cost electroencephalogram (EEG) based authentication." In 2011 5th International IEEE/EMBS Conference on Neural Engineering, pp. 442-445. IEEE, 2011.
12. Campisi, Patrizio, and Daria La Rocca. "Brain waves for automatic biometric-based user recognition." IEEE transactions on information forensics and security 9, no. 5 (2014): 782-800.
13. Maiorana, Emanuele, Daria La Rocca, and Patrizio Campisi. "On the permanence of EEG signals for biometric recognition." IEEE Transactions on Information Forensics and Security 11, no. 1 (2015): 163-175.
14. Mohanchandra, Kusuma, G. M. Lingaraju, Prashanth Kambli, and Vinay Krishnamurthy. "Using brain waves as new biometric feature for authenticating a computer user in real-time." International Journal of Biometrics and Bioinformatics (IJBB) 7, no. 1 (2013): 49.
15. Mu, Zhendong, Jianfeng Hu, and Jianliang Min. "EEG-based person authentication using a fuzzy entropy-related approach with two electrodes." Entropy 18, no. 12 (2016): 432.
16. Palaniappan, Ramaswamy. "Two-stage biometric authentication method using thought activity brain waves." International journal of neural systems 18, no. 01 (2008): 59-66.

17. Paranjape, R. B., J. Mahovsky, L. Benedicenti, and Z. Koles. "The electroencephalogram as a biometric." In Canadian Conference on Electrical and Computer Engineering 2001. Conference Proceedings (Cat. No. 01TH8555), vol. 2, pp. 1363-1366. IEEE, 2001.
18. Ruiz-Blondet, Maria V., Zhanpeng Jin, and Sarah Laszlo. "CEREBRE: A novel method for very high accuracy event-related potential biometric identification." IEEE Transactions on Information Forensics and Security 11, no. 7 (2016): 1618-1629.
19. Thomas, Kavitha P., and A. Prasad Vinod. "EEG-based biometric authentication using gamma band power during rest state." Circuits, Systems, and Signal Processing 37, no. 1 (2018): 277-289.
20. Yang, Su, and Farzin Deravi. "On the usability of electroencephalographic signals for biometric recognition: A survey." IEEE Transactions on Human-Machine Systems 47, no. 6 (2017): 958-969.
21. Revett, Kenneth, and Sergio Tenreiro de Magalhães. "Cognitive biometrics: Challenges for the future." In International Conference on Global Security, Safety, and Sustainability, pp. 79-86. Springer, Berlin, Heidelberg, 2010.
22. Curran, Max T., Jong-kai Yang, Nick Merrill, and John Chuang. "Passthoughts authentication with low cost EarEEG." In 2016 38th Annual international conference of the IEEE engineering in medicine and biology society (EMBC), pp. 1979-1982. IEEE, 2016.
23. Del Pozo-Banos, Marcos, Jesús B. Alonso, Jaime R. Ticay-Rivas, and Carlos M. Travieso. "Electroencephalogram subject identification: A review." Expert Systems with Applications 41, no. 15 (2014): 6537-6554.
24. Marcel, Sebastien, and José del R. Millán. "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation." IEEE transactions on pattern analysis and machine intelligence 29, no. 4 (2007): 743-752.
25. Näpflin, Markus, Marc Wildi, and Johannes Sarnthein. "Test–retest reliability of resting EEG spectra validates a statistical signature of persons." Clinical Neurophysiology 118, no. 11 (2007): 2519-2524.
26. Näpflin, Markus, Marc Wildi, and Johannes Sarnthein. "Test–retest reliability of EEG spectra during a working memory task." Neuroimage 43, no. 4 (2008): 687-693.
27. Haruvi Aia, Ronen Kopito, Noa Brande-Eilat, Shai Kalev, Eitan Kay, and Dan Furman. "Differences in the effects on human focus of music playlists and personalized soundscapes, as measured by brain signals." Biorxiv (2021).

Author information

Affiliations
Arctop Inc., R&D, Kaufmann St. 4, Tel Aviv-Yafo, 6801296, Israel.

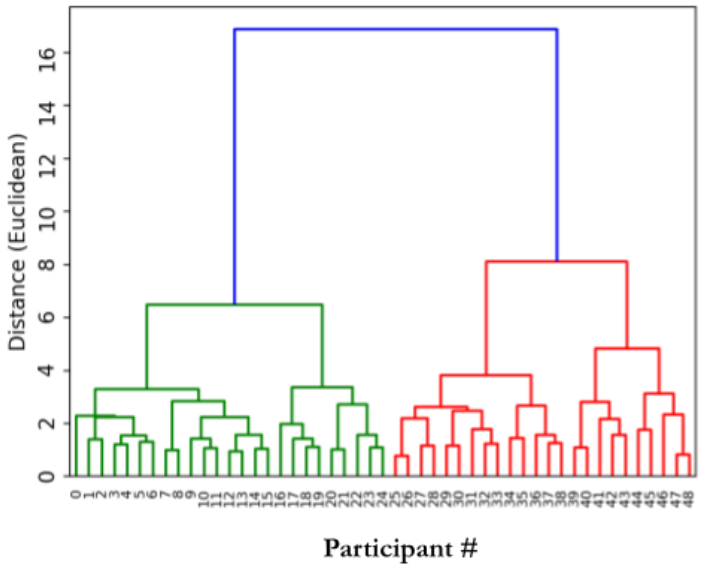
Corresponding author

Correspondence to Dan Furman, Ph.D., (dan@arctop.com)

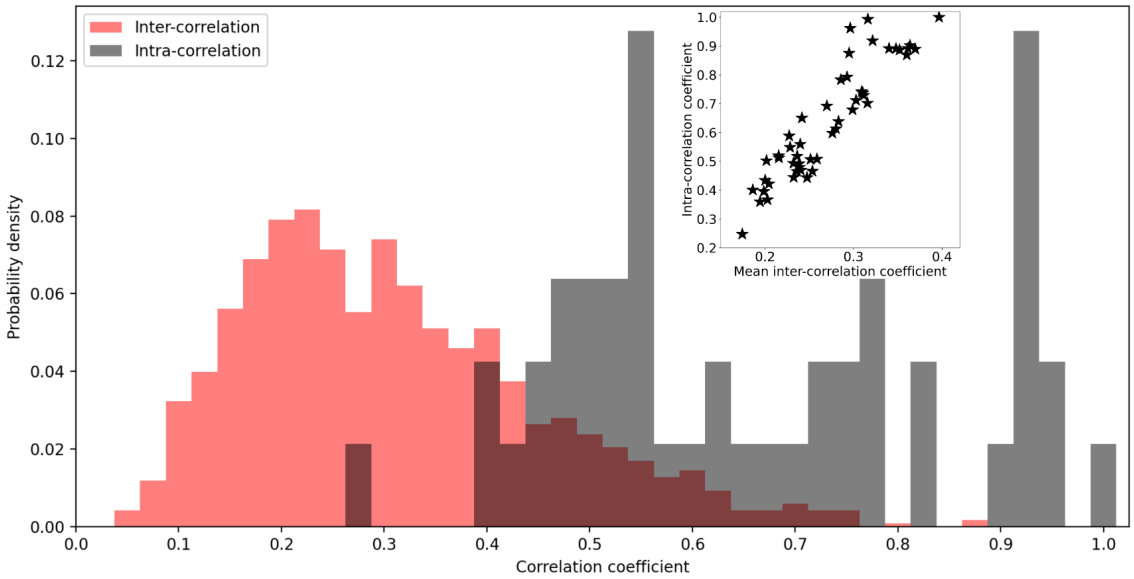
Ethics declarations

All authors are employees of Arctop Inc.

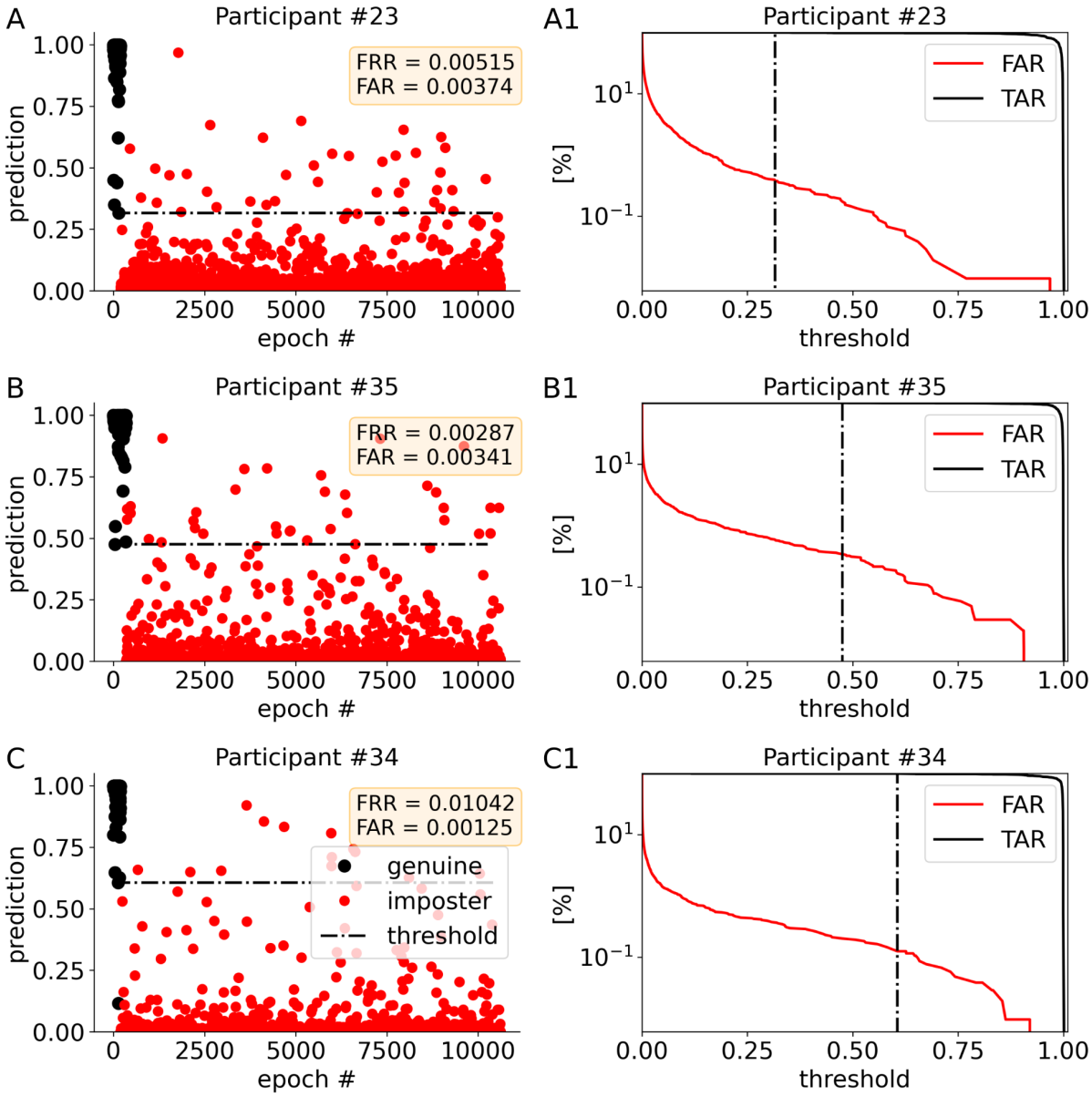
SUPPLEMENTARY MATERIALS



Supp. Fig. 1. Brain biometric ID cluster tree. The mean overall training events were calculated for each participant. Mean event correlation matrix between participants was then calculated by pairwise correlation. Using this matrix, hierarchical cluster tree (dendrogram) algorithm creates the linkage distance between participants (y-axis).



Supp. Fig. 2. Histograms of intra-participant and inter-participants events correlations. Intra-participant events correlation is the mean of pairwise correlation between all training events of a participant with themselves. Inter-participant correlations are the mean of pairwise correlation of all training events of a participant with the events of another participant. The diagonal elements in the event correlation matrix (Fig. 2E), represents the intra-participant correlations while the inter-participants correlations are the off-diagonal elements of the matrix. It is clearly seen that intra-participant correlations are generally higher than the inter-participants correlation. Meaning, a higher similarity within intra events patterns compared with inter-participants events. Although there is an overlap between the two histograms, it does not necessarily mean that perfect separability at the authentication event level is not feasible, as suggested by the inset.



Supp. Fig. 3. Epoch predictions and threshold determination. Three sessions per participant are contributing to the training data. Out of it, 30% are devoted for model validation, and to determine the model threshold. In panels **A**, **B**, **C** the prediction of three models trained for three participants (sub #23, # 35, #34 respectively) are presented for the validation data. Here, epochs predictions of genuine identity are marked in black dots, and epochs predictions of imposters are marked in red. The threshold (black dashed line), discernmenting between genuine and imposter epochs is determined by an optimization algorithm. The algorithm finds a threshold probability in which the false acceptance rate (FAR) is minimal while the true acceptance rate (1-FRR) is maximal. This is under the condition for TAR>90%, and FAR<3%. This is demonstrated in panels **A1**, **B1**, **C1.** FAR, TAR functions are plotted in red and black respectively, the threshold which was found is marked in black dashed-dot line, y-axis is in logarithmic scale.

Subject #	True rejection rate (TRR)	True acceptance rate (TAR)	False acceptance rate (FAR)	False rejection rate (FRR)
0	0.81	0.83	0.19	0.17
1	0.95	1.00	0.05	0.00
2	0.82	1.00	0.18	0.00
3	0.93	1.00	0.07	0.00
4	0.86	1.00	0.14	0.00
5	0.86	1.00	0.14	0.00
6	0.87	0.60	0.13	0.40
7	0.95	1.00	0.05	0.00
8	0.85	1.00	0.15	0.00
9	0.78	1.00	0.22	0.00
10	0.92	1.00	0.08	0.00
11	0.92	1.00	0.08	0.00
12	0.76	1.00	0.24	0.00
13	0.84	0.83	0.16	0.17
14	0.97	1.00	0.03	0.00
15	0.95	0.83	0.05	0.17
16	0.92	1.00	0.08	0.00
17	0.94	0.17	0.06	0.83
18	0.96	1.00	0.04	0.00
19	0.91	1.00	0.09	0.00
20	0.90	1.00	0.10	0.00
21	0.89	1.00	0.11	0.00
22	0.84	0.33	0.16	0.67
23	0.99	1.00	0.01	0.00
24	0.96	1.00	0.04	0.00
25	0.91	1.00	0.09	0.00
26	0.99	0.50	0.01	0.50
27	0.93	1.00	0.07	0.00
28	0.95	1.00	0.05	0.00
29	0.97	1.00	0.03	0.00
30	0.81	1.00	0.19	0.00
31	0.94	1.00	0.06	0.00
32	0.75	1.00	0.25	0.00
33	0.93	0.33	0.07	0.67
34	1.00	1.00	0.00	0.00
35	0.98	1.00	0.02	0.00
36	0.94	1.00	0.06	0.00
37	0.94	0.83	0.06	0.17
38	0.96	1.00	0.04	0.00
39	0.95	1.00	0.05	0.00
40	0.85	1.00	0.15	0.00
41	0.94	0.00	0.06	1.00
42	0.96	1.00	0.04	0.00
43	0.92	1.00	0.08	0.00
44	0.86	1.00	0.14	0.00
45	0.98	0.17	0.02	0.83
46	0.95	0.25	0.05	0.75
47	0.89	1.00	0.11	0.00
48	0.96	1.00	0.04	0.00
Average	0.91	0.87	0.09	0.13

Supp. Table 1. A detailed performance of the authentication system for each participant. The coefficients of the confusion matrix per each participant is presented.

Supp. Video 1. Rapid Serial Visual Presentation (RSVP) Stimuli. Example of a stream of images watched by participants while brain signals were recorded by their headband. https://youtu.be/TWUzbX3Q8sk

Supp. Video 2. Brain-based Authentication: Living Room Demo. Microsoft HoloLens 1, retrofitted with BCI sensors, delivers passwordless authentication. https://youtu.be/n6v9z3lNs2M