PAPER *Special Section on Sensing, Wirel. Netw., Data Collection, Analysis and Proc. Techn. for Ambient Intell. with Internet of Things*

Mobile Brainwaves: On the Interchangeability of Simple Authentication Tasks with Low-Cost, Single-Electrode EEG Devices

Eeva-Sofia HAUKIPURO[†], Ville KOLEHMAINEN[†], Janne MYLLÄRINEN[†], Sebastian REMANDER[†], Janne SALO[†], Tuomas TAKKO[†], Le NGU NGUYEN[††], Stephan SIGG[††], *and* Rainhard Dieter FINDLING[††],

SUMMARY Biometric authentication, namely using biometric features for authentication is gaining popularity in recent years as further modalities, such as fingerprint, iris, face, voice, gait, and others are exploited. We explore the effectiveness of three simple Electroencephalography (EEG) related biometric authentication tasks, namely resting, thinking about a picture, and moving a single finger. We present details of the data processing steps we exploit for authentication, including extracting features from the frequency power spectrum and MFCC, and training a multilayer perceptron classifier for authentication. For evaluation purposes, we record an EEG dataset of 27 test subjects. We use three setups, baseline, task-agnostic, and task-specific, to investigate whether person-specific features can be detected across different tasks for authentication. We further evaluate, whether different tasks can be distinguished. Our results suggest that tasks are distinguishable, as well as that our authentication approach can work both exploiting features from a specific, fixed, task as well as using features across different tasks.

key words: *biometrics, classification, EEG, mobile, user authentication*

1. Introduction

Electroencephalography (EEG) is a method to record electric potential, which predicts activity of the brain. Neurons in the brain produce electric voltages that can be measured over the scalp. EEG is commonly used in clinical applications to investigate brain diseases like epilepsy and schizophrenia [1]. Besides these use, EEG signals have been researched for different application scenarios, including biometric authentication, the recognition of a subject being or not being e.g. the authorized device owner, based on biometric stimuli. Recent results indicate that EEG signals are unique to many individuals, which qualifies them as recognition and authentication method [2]. While traditional instrumentations are expensive and stationary, recently less intrusive, mobile, low-cost consumer-grade EEG devices were developed, which enable using EEG signals as means of biometric recognition. Low cost in terms of EEG refers to at the moment devices in the range of 100 EUR becoming available on the market (e.g. the NeuroSky MindWave Mobile+[†] EEG headset), while the price of less recent EEG devices can be higher by orders of magnitude and range in the thousands or even tens of thousands of EUR (from e.g. the Emotiv EPOC device series[††] to e.g. the Brain Vision LLC ActiCHamp[†††]).

Compared to knowledge-based authentication (PIN codes, passwords, graphical patterns), biometric authentication (in constrast to e.g. recall-based authentication such as alphanumeric password or pattern-based) offers several advantages. Knowledge-based authentication demands complex knowledge, which is harder to remember, and requires time and effort to input to mobile devices [3]–[6]. It can further be stolen by an adversary via shoulder surfing and smudge attacks [7]–[9]. In contrast, biometrics need not be remembered but can be extracted from stimuli of the individual itself. A common drawback of biometric features is, however, that they can be easily observed and thus obtained by an active adversary for impersonation attacks (e.g. fingerprints [10], facial images [11], voice recordings [12]). Unlike other biometrics, EEG is not easily exposed to attackers, as it requires physical contact between electrodes and skin. The challenges to realize practical, unobtrusive EEG authentication, are that EEG traditionally utilizes obtrusive, stationary, and expensive hardware. For mobile authentication, however, less obtrusive, low-cost, small, and mobile hardware is required. Only recently, such mobile EEG devices became available and it remains a challenge to extract stable features from such hardware that allow to reliably distinguish individuals [2], [13].

We present an EEG user authentication and task recognition approach that processes signals from a low-cost, consumer-grade, single channel, and mobile EEG device. In our authentication we perform EEG signal analysis, feature extraction, feature selection, and classification of subjects and tasks. In addition, we briefly describe different machine learning methods which can be used for feature extraction and selection to increase classification accuracy. We investigate authentication during the execution of three different tasks, including the stability of EEG features across different tasks (task agnostic), as well as the ability to distinguish different tasks. The tasks have been adopted from typical tasks proposed in the literature [14], [15].

We record EEG signals from 27 subjects performing three tasks with closed eyes in a quiet room. The recording was done in a non-clinical way in an everyday environ-

Manuscript received May 11, 2018.

[†]Authors are with the Department of Computer Science, Aalto University. All authors have contributed equally to the publication.

[††]Authors are with the Ambient Intelligence Group, Department of Communications and Networking, Aalto University.

DOI: 10.1587/trans.E0.??.1

[†]NeuroSky MindWave Mobile+: `https://store.neurosky.com/`

[††]Emotiv EPOC devices series: `https://www.emotiv.com/`

[†††]Brain Vision LLC ActiCHamp: `http://brainvision.com/actichamp.html`

ment to receive realistic authentication data, thus making our approach adaptable to real-life mobile EEG authentication. The evaluation is performed in a comparative way, analyzing the EEG authentication performance in a baseline as well as a task-specific (authentication requires execution of the same task) and a task-agnostic (authentication regardless of the task performed) manner. Furthermore, we evaluate the distinguishability of tasks themselves. In summary, the contributions of this paper are:

- A method to distinguish subjects and tasks with mobile, low-cost, and single channel EEG devices.
- An authentication method from EEG as alternative to alphanumerical or pattern-based mobile authentication.
- An investigation of task-agnostic and task-specific authentication of EEG signals (Can subjects be authenticated from EEG regardless of the task they perform?)
- Evaluation of our method on a self-recorded dataset of 27 subjects.

We find that there are similarities in the signals generated in different tasks, which can be used interchangeably to identify test subjects. Furthermore, tasks are distinguishable in most cases.

2. Related work

EEG-based user authentication has recently been investigated as new biometric authentication [16]. A good overview of EEG authentication is provided in [1], [17].

In contrast to our work, the majority of previous research in EEG authentication was conducted with clinical-grade, multi-channel EEG devices [16], [18], [19], since single-channel EEG devices have become commercially available only in recent years. Some authors study EEG-based person identification with portable devices [2], [15], [20]. The usability and safety of authentication with a commercial single-channel device have been discussed in [14]. Findings indicate that this device class is able to distinguish different subjects but has weaknesses of differentiating between distinct EEG signals of a single subject [14], [15]. Still, single-channel EEG authentication provides an acceptable cost-accuracy tradeoff compared to multi-channel devices [14].

The comprehensive work on person identification with multi-channel EEG devices provides a wide basis of features that can be used also in EEG authentication. Commonly used features include autoregressive (AR) model parameters [13], [16], [18], [20]–[22] and frequency power spectrum features [14], [15], [23]. An overview of recent advances in the domain is given in Table 1.

Summarizing, most previous research focused on finding and tuning suitable EEG based authentication to achieve best possible accuracy amongst different mental and physical tasks. On the level of individual subjects, there is evidence that different EEG related tasks result in different EEG authentication accuracies [15]. However, the task-sensitivity has not been studied. It is unknown if subjects can be authenticated across task boundaries, exploiting subject (not task) specific stimuli. Likewise, it is unknown if EEG authentication is task-sensitive, meaning that authentication succeeds only when a specific set of tasks is used. We shed first light on these questions, respecting the limitations of mobile EEG devices.

3. Our approach

We propose a method for single-channel EEG *authentication* under different scenarios, as well as for *task identification*, i.e. recognizing the underlying task. For this, we exploit EEG signal acquisition, processing, as well as classification. The classifiers used are distinct and trained and evaluated with respect to their specific purpose. Besides this, the processing in our method is common to all scenarios, and includes sensing EEG signals, data preprocessing, and feature extraction (cf. figure 1). The individual steps are discussed in the following sections.

3.1 Data recording

We record data with a commercial, low-cost, mobile and portable single-channel EEG headset: the NeuroSky MindWave Mobile+. The headset has one electrode on the left forehead, and the system is grounded by a clip attached to the left auricle. The wireless headset is connected to a mobile phone or PC by Bluetooth. The device has a built-in filtering mechanism to account for and remove sensed electrical power grid frequencies. The EEG sampling frequency of the device is 512 Hz. We use a baud rate of 57600, which provides 16-bit quantized raw wave recordings[†] and sample raw EEG. The mobile device connected to the headset receives and computes the short time frequency transform power spectrum 8 times a second and covers the range of 0-63.75 Hz with 256 bands of 0.25 Hz bandwidth each. Subjects record data while performing one of three tasks: resting, thinking about a scene they have just seen in an image, or moving their right-hand index finger at predefined pace. Those different types of tasks were chosen based on performance and usability comparisons of similar tasks [14], [15].

3.2 Data preprocessing

Almost all power in EEG signals – and thus the information – is represented in the lower frequencies (see Figure 2) which are linked to psychological states and cognitive brain functions: the delta (δ) band at 0.5-4 Hz, the theta (θ) band at 4-8 Hz, the alpha (α) band at 8-14 Hz, and the beta (β) band at 14-30 Hz [1]. We therefore apply a low-pass filter on the power spectrum to extract the 0-30 Hz band.

[†]NeuroSky communication protocol details are available at `http://developer.neurosky.com/docs/doku.php?id=thinkgear_communications_protocol`.

Table 1: Table of closely related work in terms of objectives and features, partly adapted from [1].

#	Channels	Subjects	Features	Classification	Performance
[22]	1	79	AR	NN	72%-84%
[13]	8	40	AR	Discriminant Functions	About 80%
[18]	1/100	10	AR	NN	80%-95% / 85%-100%
[19]	1/8	203	e.g. MFCC	SVM	35% / 93%
[21]	2/3/5	45	AR	Polynomial classifier	Best 99%
[16]	54	9	AR	Linear classifier	Best 100%
[14]	1	15	Power spectrum	Similarity	99%
[20]	1	13	AR	SVM, LDA	87%
[23]	26	5	Power spectrum	Single space projection (SSP)	Best 92%
[15]	1	12	Power spectrum	SVM	80%
[24]	14	5	e.g. AR, power spectrum	SVM	100%

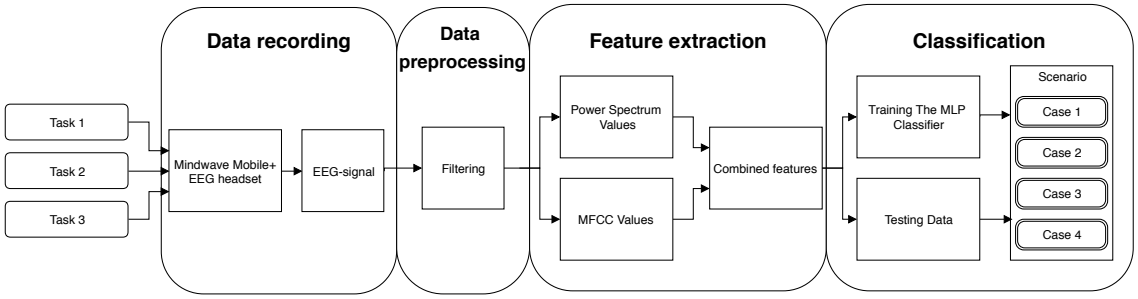

Fig. 1: Overview of our approach (exemplary with 3 tasks). Data is recorded with subjects performing different tasks, before it is preprocessed, features are extracted, combined into feature vectors, and scenario-specific classifiers (subject or task classification) are trained.

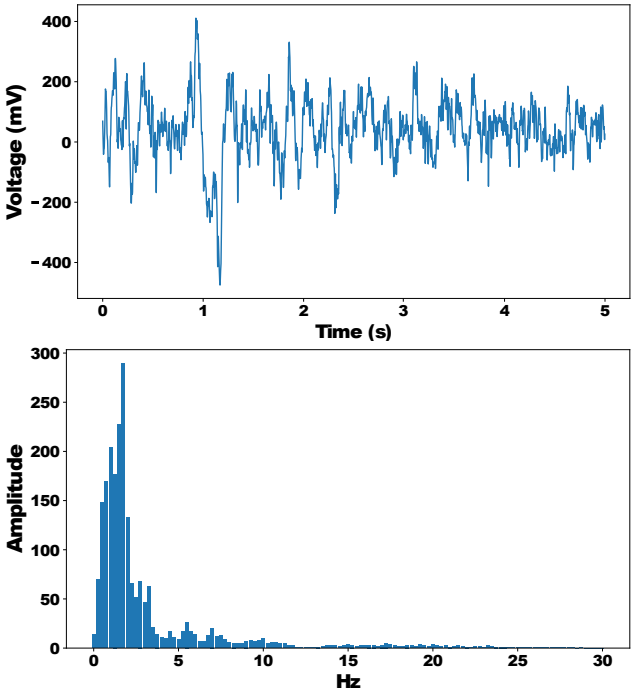

Fig. 2: Raw EEG signal (top) and the corresponding power spectrum from a 5 second excerpt (bottom).

3.3 Feature extraction and selection

We use the compressed power spectrum and its quartiles, as well as Mel-frequency cepstral coefficients (MFCCs) over 121 frequency bins with a width of 0.25Hz in the 0-30Hz range [25]. For each bin, we extract 3 features, namely the 1st, 2nd, and 3rd quartile (which corresponds to the 25% percentile, the median, and the 75% percentile as suggested in [14]). MFCC features are prominently used in audio signal processing, but are also suitable to model logarithmic characteristics in EEG measurements. We compute 39 MFCC components per sample as suggested in [19]. Power spectrum and MFCC features are then combined into a single vector per sample, which results in 402 numeric features.

3.4 Classification

In order to be comparable to previous EEG research, we utilize four types of classifiers that have frequently been used in related research before, and perform a grid search their corresponding parameters. The classifiers we consider are: support vector machine (SVM), k-nearest neighbors (k-NN), random forest (RF), and multilayer perceptron (MLP) classifier. We used the processing and feature extraction as described above, trained a classifier with data from one task at a time, and tested for subject recognition with classification accuracy as performance metric. Note that we evaluated the aforementioned classifiers using four-fold cross-validation and their respective optimal parameters. Table 2 shows the best accuracy of each classification algorithm after the cross-validation process. We thereby found the MLP classifier with a logistic activation function to consistently outperform other classifiers. We therefore conduct the subsequent evaluation

Table 2: Authentication results of different classification algorithms applied to our data (see section 4.1).

	MLP	SVM	k-NN	RF
rest	**0.75**	0.58	0.61	0.74
image	**0.76**	0.62	0.66	0.69
finger	**0.74**	0.61	0.68	0.72

to using only a MLP classifier. However, any classification method could be used in our approach.

We compare four scenarios:task-agnostic authentication, task-specific authentication, and task classification, which are compared to a baseline authentication scenario on the same data. The classification step is scenario dependent. For all authentication scenarios, the device is owned by one person, for which the authentication should allow access, and other people are considered adversaries, hence authentication should deny access. Samples from the device owner thereby become samples of the positive class P, and sample of other subjects become samples of the negative class N.

(1) Baseline authentication

In the baseline authentication scenario we train a binary classifier with data of a single task. The classifier thereby learns to distinguish between owner and attackers when given data of this task. This approach is similar to previous research, e.g. such as in [14], and serves as baseline for comparisons between subsequent scenarios and with previous research.

(2) Task-agnostic authentication

The task-agnostic authentication scenario is based on the baseline authentication, but uses data of different tasks for training the classifier than for the subsequent authentication. For n tasks, training data includes data of $n-1$ tasks, with the authentication using data of the left out task. The purpose of this scenario is to investigate whether single-channel EEG of different tasks are similar enough to be used interchangeably in authentication.

(3) Task-specific authentication

The task-specific authentication is also based on the baseline authentication scenario, but the positive class is formed just by data of one task of the owner. All other data (from other tasks of the same subject and all tasks of from other subjects) constitutes the negative class. It thereby uses data of multiple tasks for training, but requires only data of one task for authentication that was not used during training. The purpose of this scenario is to further investigate possible additional similarity or dissimilarity between signals of different tasks within and across users. We investigate this as a first step towards inter-compatibility of EEG tasks in EEG authentication, with with users could e.g. train their devices with a certain set of EEG tasks, but afterwards authenticate using a different and wider range of EEG tasks than used for training. This would allow for decreasing the user effort connected to training EEG authentication, hence in making EEG authentication more unobtrusive.

(4) Classification of tasks

The task classification scenario does not involve authentication, but aims at distinguishing the tasks. For a scenario with n tasks, we train a n-class-classifier with data of the device owner. The classifier is trained to distinguish the tasks of the device owner. The purpose of this scenario is to investigate whether the same data that is used for authentication can also be used to distinguish between different tasks of the device owner. This task classification is only applied to owner data, as it should only be performed if the preceding EEG authentication already accepted the user as genuine.

4. Evaluation

We investigate if a) different tasks have correlated EEG signals (for authentication), b) if the device owner can be authenticated correctly regardless the underlying task, and c) if EEG signals are task-sensitive, so that device owner authentication and the task itself can be used for authentication at the same time.

For comparability, we use three tasks which have been used in the literature: *rest*, *image*, and *finger* [14], [15]. In the *rest* task, subjects were resting and instructed not to think anything. In the *image* task, subjects were shown an image of a palm beach, and were instructed to think about that image. In the *finger* task, subjects were instructed to tap a table with their right-hand index finger at the pace of the sound of a metronome configured at 120 beats per minute. We acknowledge the limitations the selected tasks cause for the comparison of authentication between the tasks. In particular, differences between the tasks are small, as subjects sit still with eyes closed in all tasks. More dissimilar tasks with more versatility potentially produce more distinct EEG signals. More diverse EEG signals ease classification and discourage cross-task authentication.

4.1 Data recording

In accordance to previous, comparable EEG studies [26]–[28], we recorded data of a total of 27 participants, one at a time, in a quiet room. Recordings were done in university and home environments in Finland, with 44% of subjects being male and 66% of subjects being female, and with a mean subject age of 29 years (std: 11.3 years). In all three tasks, the subjects were sitting still with eyes closed (see Figure 3).

Each participant repeated each task 5 times for 20 seconds. For a realistic recording scenario and to be able to address possible artifacts during recording, the EEG headset was unequipped and re-equipped between all individual 20-second-long recordings. Furthermore, tasks were recorded in mixed order, so that similar tasks did not occur subsequent to each other. Each recording (in total 405 recordings) resulted in one raw, 512 Hz sampled, 20-second-long EEG signal, and the corresponding frequency power spectrum. Subjects were instructed to notify us when they had the

Fig. 3: Subject wearing the wireless EEG headset.

impression that a recording was biased or when they had difficulties to concentrate. This was done to minimize noise in the training data and bias towards non-intended effects.

4.2 Evaluation setup

We use 4-fold cross validation to assess the performance of the baseline and task-specific authentication scenarios. We form cross-validation partitions so that each partition contains data from exactly one task. Hence, during cross validation, classifiers are trained with data of all but one task and tested with data of the left out task. For each fold, a binary classifier was trained for each test subject, based on scenario requirements as described in Section 3.4. Then, we gave each of the signals in the test set to all classifiers to classify as either positive (access granted) or negative (access rejected). For a sample of this specific subject, positive prediction from the classifier counted as *true acceptance* and negative prediction as *false rejection*. Similarly, provided a sample of a different subject was considered as negative prediction (*true rejection*) and else a *false acceptance*.

In authentication, false acceptance is considered the most harmful error type. In our case, a prediction was determined positive if the classifier assigned a probability of greater than 0.5 for the signal belonging to the positive class.

In evaluating the task-agnostic scenario, data from each task was used as test data while the other two tasks were used as training data. Otherwise, the evaluation process of this scenario was identical to the other two authentication scenarios. In measuring the performance of our model in authentication scenarios, we computed the false acceptance rate (FAR), false rejection rate (FRR), and half total error rate (HTER). FAR measures the fraction of times an impostor has been granted access as another subject. FRR is defined as the fraction of times a legitimate subject has been denied access. Those rates indicate the probability of incorrectly accepting or rejecting samples for the positive and the negative classes, independently of the possibly unknown frequency of samples of both classes in real authentication situations. HTER is the mean of FAR and FRR. The error rates were measured individually for each task in each scenario. Also, in task classification, we performed a 4-fold cross validation for each test subject separately. The predicted and actual task labels were recorded and combined over all folds and test subjects. We computed an accuracy score for the classifier and produced a confusion matrix using this information.

A commonality of all authentication and task classification scenarios is that by performing cross validation as stated above, the positive and negative classes are unbalanced, with the positive class (device owner, selected task) always being smaller than the negative class (attackers, other task). As training a classifier with unbalanced data has a tendency to generate a classifier preferring the bigger class, the class distribution was equalized using oversampling of the positive class. Thereby, instances of the positive class were used repeatedly, until both classes were of equal size. This proved to improve classification accuracy for all classification scenarios.

For the implementation we relied on the scikit-learn Python library [29].

5. Results

The error rates in the baseline scenario (see Table 3a) are comparable to related work in the field, suggesting that our method proves the concept of a low-cost, mobile, single-electrode based EEG authentication. False acceptance rates do not vary greatly between tasks. In the *rest* task, the amount of false rejections is noticeably higher (0.311) than in the other two tasks (0.269, 0.252).

In comparison, in the task-agnostic scenario (see Table 3b), results indicate that the false acceptance rates for all tasks are lower when compared to the baseline scenario (0.013-0.017 vs. 0.023-0.031), while false rejection rates of *image* and *finger* tasks are higher (0.313, 0.290 vs. 0.269, 0.252). Results for the *rest* task show a small improvement over the baseline scenario in terms of both FAR and FRR (0.015, 0.265 vs. 0.023, 0.311). This indicates that, though there are differences in signals produced by the tasks, overall they are still similar enough to be used interchangeably in training and authentication situations.

In the task-specific scenario (see Table 3c), we observe a decrease in false acceptances (to 0.004-0.007), but also proportionally bigger increased false rejections (to 0.496-0.576), when comparing to results of the task-agnostic scenario. This is not surprising as the negative class also includes measurements from the same test subject performing a different task, which is not the case in the other scenarios. Results for the task-specific scenario being worse than for the task-agnostic scenario thereby emphasize that there are similarities in EEG signals of the same subject across different EEG tasks.

Results for task classification indicate that identifying the task that is underlying a given EEG signal is possible (see Figure 4 and Table 3d). Overall, correctly identifying tasks was possible with an accuracy of 0.562. Identifying the *rest* task appears to be a little more difficult than identifying

Table 3: Task-agnostic and task-specific authentication.

(a) Baseline authentication

Task	FAR	FRR	HTER
rest	0.023	0.311	0.166
image	0.025	0.269	0.147
finger	0.031	0.252	0.141

(b) Task-agnostic authentication

Task	FAR	FRR	HTER
rest	0.015	0.265	0.140
image	0.013	0.313	0.163
finger	0.017	0.290	0.154

(c) Task-specific authentication

Task	FAR	FRR	HTER
rest	0.006	0.576	0.291
image	0.004	0.522	0.263
finger	0.007	0.496	0.252

(d) Confusion of task classification

Task	Precision	Recall	Accuracy
rest	0.548	0.515	0.698
image	0.543	0.567	0.693
finger	0.594	0.603	0.733

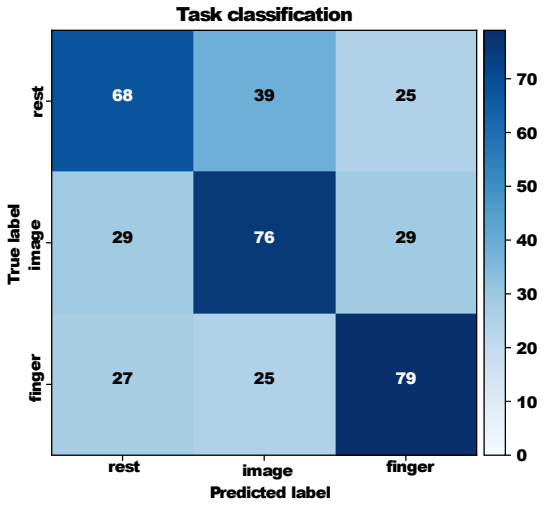

Fig. 4: Confusion matrix for task classification.

the other two tasks, as it is frequently identified as thinking about an image, similar to the *image* task. In comparison to the *rest* and *image* tasks, the *finger* task achieved better results, hence seems more distinguishable from other tasks. This also aligns with intuition about the *rest* and *image* tasks being more similar to each other than to the *finger* task. Another reason why identifying the *finger* task is possible with higher accuracy is that test subjects were able to produce more consistent signals in this task, due to it being more structured by using a rhythmic movement.

To conclude, our task-agnostic results indicate that legitimate users would be denied access in between 13 to 17 out of 1000 times, while attackers would be allowed access in about 265 to 313 times out of 1000 times. This indicates that users do not seem to be required to train all those EEG tasks they later plan on using for authentication. This would furthermore allow for EEG training to become less obtrusive in comparison to users being required to train all tasks. In addition, even with using low-cost hardware and training the system with EEG data in a task-agnostic way, attackers are denied access in at least 68% from EEG alone. For this reason, these results indicate that EEG authentication can be utilized in multi-modal authentication for modern mobile devices, such as in the CORMORANT framework [30]. Multi-modal mobile authentication thereby incorporates a wide range of diverse authentication approaches (cf. [31], [32]), including biometrics, to cover a large body of authentication situations. It can thereby achieve unobtrusive authentication, as users can utilize the one approach that suits a given situation best [33]–[35]. While our our results indicate that EEG can contribute as another biometric authentication approach to such combinations – by lowering success chances of attacks without significantly impeding legitimate access also in task-agnostic scenarios – an evaluation of the corresponding biometric fusion with further authentication approaches is left for future work.

6. Discussion

With biometrics, more subjects will naturally add further noise. With EEG it is still an open question to investigate the size of the password space of EEG based authentication approaches. As we do not address this important aspect in our research this point remains open for future research.

In addition to the approach outlined in section 3, we also investigated further concepts. However, in preliminary experiments those turned out to not contribute to improving authentication and task recognition performance, hence are not used in the presented approach. For filtering sensed raw EEG data we investigated single-channel independent component analysis (SCICA). SCICA is a method to extract independent components from time series data, such as raw EEG signals [36], [37]. However, in preliminary experiments on our data, filtering the sensed EEG signal using SCICA did not improve authentication results, so that we disregard it in the processing. Besides using power spectrum and MFCC features, in preliminary experiments we also utilized autoregressive (AR) models, wavelet decomposition, and power spectral entropy (PSE). With AR models fitted to the raw EEG signal data as in [18], we then used the determined model parameter values as features. With wavelet decomposition we utilized the Debauchies family of wavelets and extracted coefficients and energies as in [38] for each wavelet decomposition level. The PSE values were computed from the extracted frequency power spectrum bins, by first calculating the power spectral density and then further the PSE for each bin, as proposed in [39]. However, none of those features contributed to improved authentication results, which is why the presented processing relies only on a combination of frequency power spectrum features and MFCC features.

7. Conclusions

In this paper we investigated the impact, different tasks and settings have on mobile EEG authentication. We used a low-cost, single-electrode EEG-device to capture EEG signals and have presented a multi-step processing to perform EEG authentication. We collected a dataset of 27 users in a realistic live authentication scenario. In our evaluation we have investigated the effects three tasks have on subsequent authentication. The evaluation included a baseline,

a task-agnostic, a task-specific, as well as a task classification scenario. We also compared which of our results align with performance of previous research. Results for the task-specific scenario indicate that EEG signals of different tasks contain sufficient information about users, hence sufficient similarity within users, to allow for user authentication across tasks to some extent. Additionally, in task classification we tested for distinguishability of EEG tasks. Results indicate that the task underlying a given EEG signal can as well be identified correctly.

Future work should investigate a wider variety of different EEG tasks. Our evaluation results for task recognition indicate that it is possible to distinguish different tasks from a given EEG signal alone. However, further verification would require a larger amount of samples within each task. Future work should therefore investigate whether a larger variety of tasks with a larger sample size within each task is still well distinguishable. Tasks might also involve physical activity, include background noise, or allow subjects to open their eyes. Furthermore, in our evaluation we noticed that the authentication error slightly increased when adding new test subjects, which could indicate an overlap of subjects in the chosen feature space. Future work should therefore investigate the password space for EEG-based authentication and whether a larger amount of test subject is able to address this effect.

References

[1] P. Campisi and D.L. Rocca, "Brain waves for automatic biometric-based user recognition," IEEE Transactions on Information Forensics and Security, vol.9, no.5, pp.782–800, May 2014.

[2] R. Palaniappan and D.P. Mandic, "EEG based biometric framework for automatic identity verification," The Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology, vol.49, no.2, pp.243–250, 2007.

[3] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller, "On the need for different security methods on mobile phones," MobileHCI, pp.465–473, ACM, 2011.

[4] J. Bonnau, C. Herley, P.C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," IEEE SOUPS, pp.553–567, 2012.

[5] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," Workshop on New security paradigms, pp.133–144, ACM, 2009.

[6] L. Zhang-Kennedy, S. Chiasson, and P. van Oorschot, "Revisiting password rules: facilitating human management of passwords," Symposium on Electronic Crime Research, pp.1–10, June 2016.

[7] A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J.M. Smith, "Smudge attacks on smartphone touch screens," USENIX conference on offensive technologies, pp.1–7, 2010.

[8] F. Schaub, R. Deyhle, and M. Weber, "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," Mobile and Ubiquitous Multimedia, pp.1–10, ACM, 2012.

[9] F. Tari, A.A. Ozok, and S.H. Holden, "Comparison of perceived & real shoulder-surfing risks of alphanumeric & graphical passwords," Symposium on Usable privacy and security, pp.56–66, 2006.

[10] E. Marasco and A. Ross, "Survey on antispoofing schemes for fingerprint recogn.," ACM CSUR, vol.47, no.2, pp.1–36, Nov. 2014.

[11] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," International Joint Conference on Biometrics (IJCB 2011), pp.1–7, 2011.

[12] H. Bredin, A. Miguel, I. Witten, and G. Chollet, "Detecting replay attacks in audiovisual identity verification," ICASSP, 2006.

[13] R. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles, "The electroencephalogram as a biometric," Electrical and Computer Engineering, 2001, pp.1363–1366, IEEE, 2001.

[14] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I think, therefore I am: Usability and security of authentication using brainwaves," Financial Cryptography and Data Security, pp.1–16, 2013.

[15] M.T. Curran, J. k. Yang, N. Merrill, and J. Chuang, "Passthoughts authentication with low cost EarEEG," IEEE Engineering in Medicine and Biology Society, pp.1979–1982, Aug 2016.

[16] D.L. Rocca, P. Campisi, and G. Scarano, "On the repeatability of EEG features in a biometric recognition framework using a resting state protocol.," BIOSIGNALS, pp.419–428, 2013.

[17] F. Lotte, M. Congedo, A. Lécuyer, F. Lamarche, and B. Arnaldi, "A review of classification algorithms for EEG-based brain–computer interfaces," Journal of Neural Engineering, vol.4, no.2, p.R1, 2007.

[18] G. Mohammadi, P. Shoushtari, B. Molaee Ardekani, and M.B. Shamsollahi, "Person identification by using AR model for EEG signals," World Academy of Science, Engineering and Technology, pp.281–285, 2006.

[19] P. Nguyen, D. Tran, X. Huang, and D. Sharma, "A proposed feature extraction method for eeg-based person identification," ICAI, 2012.

[20] Z. Dan, Z. Xifeng, and G. Qiangang, "An identification system based on portable EEG acquisition equipment," IEEE Intelligent System Design and Engineering Applications, pp.281–284, 2013.

[21] D.L. Rocca, P. Campisi, and G. Scarano, "EEG biometrics for individual recognition in resting state with closed eyes," Biometrics Special Interest Group (BIOSIG), pp.1–12, Sept 2012.

[22] "Person identification based on parametric processing of the EEG, author=Poulos, M and Rangoussi, M and Chrissikopoulos, V and Evangelou, A, booktitle=IEEE Electronics, Circuits and Systems, volume=1, pages=283–286, year=1999,"

[23] F. Babiloni, F. Cincotti, L. Lazzarini, J. Millan, J. Mourino, M. Varsta, J. Heikkonen, L. Bianchi, and M. Marciani, "Linear classification of low-resolution EEG patterns produced by imagined hand movements," IEEE Transactions on Rehabilitation engineering, vol.8, no.2, pp.186–188, 2000.

[24] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, "Low-cost electroencephalogram (EEG) based authentication," IEEE/EMBS Neural Engineering, pp.442–445, 2011.

[25] S.B. Davis and P. Mermelstein, "Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences," in Readings in speech recognition, pp.65–74, 1990.

[26] P. Campisi and D.L. Rocca, "Brain waves for automatic biometric-based user recognition," IEEE Transactions on Information Forensics and Security, vol.9, no.5, pp.782–800, May 2014.

[27] D. La Rocca, P. Campisi, and G. Scarano, "On the repeatability of eeg features in a biometric recognition framework using a resting state protocol.," Proc. BIOSIGNALS, pp.419–428, 2013.

[28] K. Das, S. Zhang, B. Giesbrecht, and M.P. Eckstein, "Using rapid visually evoked eeg activity for person identification," 2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp.2490–2493, Sept 2009.

[29] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," Journal of Machine Learning Research, vol.12, pp.2825–2830, 2011.

[30] D. Hintze, R.D. Findling, M. Muaaz, E. Koch, and R. Mayrhofer, "CORMORANT: Towards continuous risk-aware multi-modal cross-device authentication," Proc. 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp 2015), Osaka, Japan, pp.169–172, ACM, Sept. 2015.

[31] R.D. Findling, M. Muaaz, D. Hintze, and R. Mayrhofer, "Shake-unlock: Securely transfer authentication states between mobile devices," IEEE Transactions on Mobile Computing (TMC), vol.16,

no.4, pp.1163–1175, April 2017.

[32] D. Schürmann, A. Brsch, S. Sigg, and L. Wolf, "BANDANA - body area network device-to-device authentication using natural gait," 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp.190–196, March 2017.

[33] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," Pattern recognition, vol.38, no.12, pp.2270–2285, 2005.

[34] A.A. Ross, K. Nandakumar, and A.K. Jain, Handbook of Multibiometrics (International Series on Biometrics), Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[35] A. Ross and A. Jain, "Information fusion in biometrics," Pattern recognition letters, vol.24, no.13, pp.2115–2125, Sept. 2003.

[36] M.E. Davies and C.J. James, "Source separation using single channel ica," Signal Processing, vol.87, no.8, pp.1819–1832, 2007.

[37] B. Mijovic, M. De Vos, I. Gligorijevic, J. Taelman, and S. Van Huffel, "Source separation from single-channel recordings by combining empirical-mode decomposition and independent component analysis," IEEE transactions on biomedical engineering, vol.57, no.9, pp.2188–2196, 2010.

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

[39] A. Zhang, B. Yang, and L. Huang, "Feature extraction of EEG signals using power spectral entropy," BioMedical Engineering and Informatics, pp.435–439, May 2008.