Development of a Mobile EEG-based Biometric Authentication System

Klonovs, Juris; Petersen, Christoffer Kjeldgaard; Olesen, Henning; Hammershøj, Allan Dyhr

Publication date:
2012

Document Version
Early version, also known as pre-print

Development of a Mobile EEG-based Biometric Authentication System

J. Klonovs[1,2], C. Kjeldgaard Petersen[1], H. Olesen[1], A. Hammershøj[1]

[1] Center for Communication, Media and Information Technologies (CMI),
[2] Department of Mechanical and Manufacturing Engineering
Aalborg University Copenhagen
A. C. Meyers Vænge 15, DK-2450 Copenhagen, Denmark
e-mail: juris@m-tech.aau.dk, christoffer@sappy.dk, {olesen, allan}@cmi.aau.dk

***Abstract*—In recent years the need for greater security for storing personal and business data or accessing corporate networks on mobile devices is growing rapidly, and one of the potential solutions is to employ the innovative biometric authentication techniques. This paper presents the development of a mobile biometric authentication system based on electroencephalogram (EEG) recordings in combination with already proven technologies such as facial detection and near-field communication (NFC). The overall goal of this work is to fill the gap between mobile web technologies and wireless EEG devices and to develop a new authentication technique and a feasible application. Therefore, we review the relevant literature, conduct several EEG measurement experiments and discuss their procedure and results with experts in the EEG and digital signal processing (DSP) fields. Based on these results we build and present a mobile prototype system capable of authenticating users based on the uniqueness of their brainwaves. Furthermore, we implement a novel authentication process, which leads the authentication system to be more secure. We also give suggestions for future improvements of the system.**

***Key words*—EEG, Biometric Authentication, Mobile Communication**

I. Introduction

Electroencephalogram (EEG) systems capable of measuring brainwaves of an individual have received a lot of attention in recent years. These brainwaves measured as electric activity on the scalp can reveal various information about a person. Traditionally, EEG has been used in clinical contexts to diagnose a patient in different areas; including testing for brain death [1] or coma, distinguishing between epileptic seizures, movement disorders, or migraine variants [2], or testing for the depth of anaesthesia [3].

EEG signals of an individual are just as unique as fingerprints [4]. The uniqueness of EEG signals is particularly strong when a person is exposed to visual stimuli, and the visual cortex area of the brain on the backside of the head is the best place to measure brainwaves, related to the visual sense [5].

The brain is a highly complex and continuously active organ that receives and processes signals from the body and the environment, generates responses accordingly and recalls the stored information when it is needed. It is a known fact, that our brains represent both behavioural and physiological information at the same time [6] [7] and therefore reveal a big potential value for biometric purposes. The brain activity produces several types of signals, including electrical, magnetic and metabolic signals [8, p. 87]. This activity can be registered using different approaches, and EEG recording is considered to be the fastest. EEG characteristics are highly dependent on the degree of activity of the cerebral cortex [9, pp. 2–5], which represents a very complex neural wiring, and therefore are unique for each person [10, p. 18]. The most familiar classification uses EEG waveform frequency bands (alpha, beta, theta, delta and gamma waves) [11, p. 211], which can be decomposed using different mathematical approaches. In general, EEG signals represent a combination of waveforms. They are classified according to their frequency, amplitude, wave morphology, spatial distribution and reactivity [12].

Speaking of authentication and security terms, three different and clearly distinct concepts are essential: Identification, Authentication and Authorization [13]. Authentication systems, which are the main topic of this paper, are in general based on three fundamental classes, “something you know”, “something you have” and “something you are”. Each of the classes authenticates a person in different ways:

1. *Something you know:* Could for instance be a textual password. The overall idea is that you have a secret that only you know.
2. *Something you have:* Could for instance be a smart card. The overall idea is that the person authenticating into a system must have some kind of object to do so.
3. *Something you are:* Could for instance be a fingerprint. The overall idea is to base the authentication on something “built-in” in the person trying to authenticate.

It has been shown that the more of the three classes that can be verified in an authentication system, the better the system is from a security point of view [39, p. 7]. At least two classes and preferably all three should be used. Authentication systems based on multiple classes are harder for an attacker to compromise.

II. Related Work

One of the early ideas about combining EEG with authentication systems was presented by Thorpe et al. [14]. In 2005, they presented their novel idea for an authentication system using thoughts (calling them pass-thoughts) and described the design for such system. They argued that such a system is feasible and could work since brain signals from an individual might be unique even when thinking about the

same thought as others. The paper also briefly mentions the need for an open debate about the ethical considerations for such systems.

Processing brainwaves evoked from visual stimuli for the purpose of authentication has been described by Zúquete et al. [15]. They argued that visual stimulations lead to very focused brain activities known as Visual Evoked Potentials (VEP), and present an EEG authentication system using a picture set of black-and-white line drawings made by Snodgrass and Vanderwart [16] - the latter originally conceived to investigate the differences and similarities in the processing of pictures. This is similar to our approach, since we are also using visual stimuli to build an authentication system. Furthermore, we are aiming for using a limited number of sensors placed on the occipital lobe of a person.

Ashby et al. proposed an EEG based authentication system based on a low cost EEG headset [17]; specifically a 14-sensor Emotiv Epoc EEG headset, which is also used in our prototype. They argued that a low-cost EEG headset might pave the way for mass adoption in consumer applications.

III. Methods

Methodically, we performed a number of experiments, where we gathered EEG data by recording brainwave signals from subject persons. The purpose was to have a data collection that could be analysed with the intent to find unique features, which can be used for authentication purposes. In order to interpret the obtained data material, we carried out a qualitative interview session with neurologist Jesper Rønager from the national hospital of Denmark, Rigshospitalet in Copenhagen [18]. We use these data for the purpose of defining an initial approach on how an EEG-based authentication system could technically be developed. The outcome of this work is then used to validate whether our approach is plausible.

Finally, we assess the different possible usage scenarios, where EEG-based authentication systems could be put to use, and analyse the security aspects related to such systems in order to evaluate, whether using EEG in authentication systems gives better security than in current systems.

IV. Technical Setup

In general the prototype is divided into two major parts (in addition to the EEG headset); a front-end part located on an Android smartphone responsible for user interaction and a back-end part located on a remote server responsible for processing EEG data and handling the authentication algorithms. The overall architecture is a client-server model, and in the following sections we refer to the client as front-end, and the server as back-end.

The overall biometric authentication system architecture from the hardware and communication perspective is illustrated in Fig. 1.

A. Smartphone Device

As the system is tailored for mobile use, it is necessary to implement it in a modern smartphone environment with access to various context triggers like web, camera and accelerometer among others. According to Gartner, the worldwide market share of smartphone systems in the second quarter of 2012 is dominated by the Android system from Google (68.1 %) and iOS from Apple (16.9 %) [19]. Besides having the biggest market share, the Android system is also relatively easily accessible from a development point of view, since a Software Development Kit is provided free of charge and the system itself is open source [20].

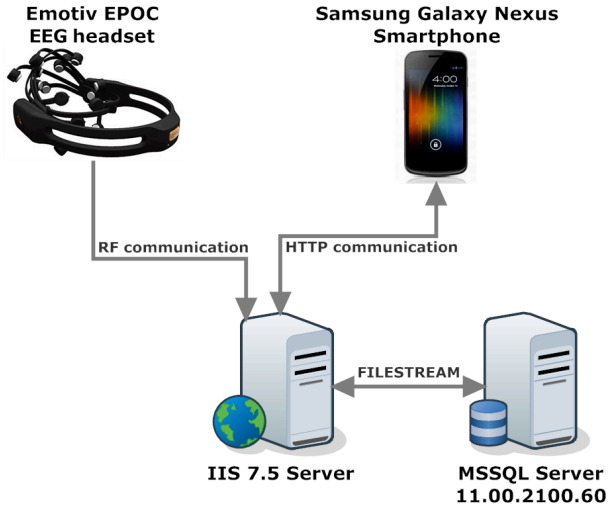

Fig. 1: System architecture diagram. The Emotiv EPOC headset is responsible for EEG signal transmission. The Samsung Galaxy Nexus Smartphone is running the front-end part, which communicates with an IIS 7.5 server running the back-end part responsible for data exchange with a MSSQL database.

These circumstances formed the decision to base the front-end part of the prototype on the Android platform. Specifically, a Samsung Galaxy Nexus smartphone running Android version 4.0.4 (Ice Cream Sandwich) is used as the main testing device. This device features a 1.3-megapixel front camera as well as a 5-megapixel rear camera. The front camera can be used to unlock the phone using facial recognition software, which is built in natively in the new Android 4.0 version. Besides that, the device also includes support for Near Field Communication (NFC), capable of establishing a radio connection between the device and an item or endpoint with a RFID tag [21, p. 3].

B. EEG Headset

Based on our previous research [22], we have chosen the Emotiv EPOC EEG neuroheadset to use for the development of our prototype solution. The Emotiv EPOC EEG headset has 14 saline electrodes with two reference sensors and is recognized as a high-fidelity EEG device designed for practical consumer applications [23]. As all incoming data from the Emotiv EPOC headset are encrypted, it must first be decrypted before applying further digital signal processing techniques.

C. Technical Front-end Setup

The front-end of the prototype is implemented as a native Android application aimed for minimum API level 14 (Android 4.0 and upwards). Even though the application is developed as native (thus written in Java with user interface files written in XML), a significant part of the app is written in standard web technologies like HTML, CSS and JavaScript. The web code is built on top of jQuery Mobile, which is a framework optimized for mobile devices with touch interfaces, it is in itself based on the jQuery framework. A screenshot of the front page styled with jQuery Mobile can be seen in Fig. 2.

The reason for choosing to implement most of the graphical user interface with web technologies is the rapid prototype capabilities of current web technologies. Also, it makes

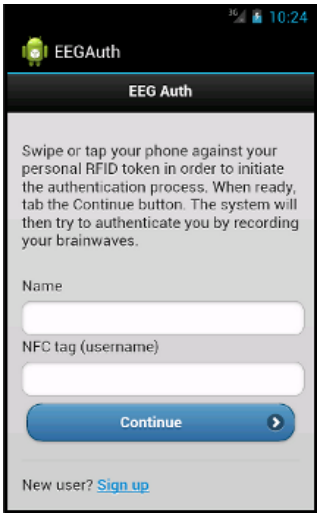

Fig. 2: Screenshot of the EEGAuth frontpage styled with jQuery Mobile.

the code more portable, if one should decide to implement the system on a different platform.

Prior to recording the user's brainwaves in order to authenticate him or her, several steps must be carried out. Since the prototype system is an authentication system with the sole purpose of answering the question "Is the user actually who he or she claims to be?", the system should initially allow users to make such claim. As explained earlier, the more of the three classes, something you know, have or are, a system can incorporate, the more secure the system is. The "something you have" class can be applied by demanding that the user verifies his or her identity with an item containing a chip the system can read. Such an item could be a smart card, ID card or even a wristband or finger ring containing an electronic chip. By taking advantage of the NFC technology built into the Android device, the user must swipe his or her personal item containing an RFID tag against the device in order to initiate the authentication process. Besides knowing other significant credentials of the user, an intruder also has to steal this item in order to bypass the authentication system. The entire front-end system flow from the perspective of the user is illustrated in Fig. 3.

To start the authentication process, the user must swipe an RFID tag against the phone. The front-end will then ask the back-end whether a user profile matching this RFID tag exists. This is synonymous to making a claim about a user identity. If a user profile exists, the process continues, otherwise it stops here with an error dialog. If the RFID tag corresponds to a known user, the system proceeds with face and motion detection flows, in order to validate if there is actually a user in front of the camera, standing relatively still. The remainder of Fig. 3 shows the flow for authenticating the user with EEG.

1) Facial Detection

The next couple of steps are implemented to make sure that the optimal circumstances and conditions of the user are met when recording EEG data from the headset. The prototype system requires that the subject person should sit in a comfortable and relaxed position, stay relatively still, and concentrate his or her mind on a photograph of a person [18]. Therefore we take advantage of the camera built into the smartphone to detect whether there is a person in front of the display or not. Specifically, the system shows a page containing a live camera preview stream alongside with a text asking the user to place his or her face in front of the camera. The system continuously scans the camera preview for faces, and in the moment when one face is detected, the user is redirected to a new page where the authentication process continues. In addition to detecting a face, the camera could also be used for logging purposes in the authentication part of the system. The system could capture a picture of the person in front of the camera, when someone tries to authenticate. This photo could be used in case of disputes, or when an intruder is trying to gain unauthorized access after theft of an RFID token, further improving the overall security of the system.

2) Motion Detection

When a face has successfully been detected, it is time to check, if the user is standing relatively still. As mentioned earlier, the best EEG data are measured from subject persons, who are standing still [18]. Thus, the prototype system uses the built-in accelerometer to detect the movement level of the smartphone. The idea behind is that it should not be possible to continue with the authentication process, if the phone (and, consequently, the headset) is shaken too much, or if the user is currently moving from one spot to another.

D.Authentication Process

When the NFC-, face detection- and motion detection-steps are completed, it is time for the actual authentication process. The back-end server will provide a photograph showing a person, which will stimulate the user's visual cortex while recording brainwaves. Before showing the photo to the user, the system should vibrate the smartphone for a short period of time to further prepare the user for paying attention to the shown image. By sensing this "touch" from the phone, the alpha waves will be lowered, setting the user in a ready-state [18].

The image will be shown for a total of five seconds, and when five seconds have passed, the front-end will immediately prompt the back-end server for a result of the authentication. Based on the answer from the back-end, the front-end will either show a "Congratulations" page, if the authentication was successful or an "Access denied" page, if it wasn't (as illustrated in Fig. 3).

E. System Flow Considerations

The process of authentication as shown in Fig. 3 is the end result of a number of iterations including changes and improvements to the flow and system design. Originally, the plan was to develop a system based on secret password images for EEG authentication, as Thorpe et al. proposed [14]. In this setup users would choose their own personal password image. This image would be shown to the user when authenticating, and the measured EEG signals would be analysed in order to confirm that the user is who he or she claims to be and currently looking at the correct password image. This is different from the final setup, where the images are only used for visual stimulation, and what they are depicting is not essential for the authentication reasoning.

In other words, the most crucial in the final prototype is that some image depicting a known face will be shown to the user while authenticating, but it is not essential that the image is kept secret or belonging to the user in question. The use of this approach was due to advice received from Jesper Rønager on the way EEG functions. EEG is not a tool to read the exact thoughts of a brain, but can outline the results of certain tasks from within the brain. The spatial resolution of EEG is relatively low and the most informative

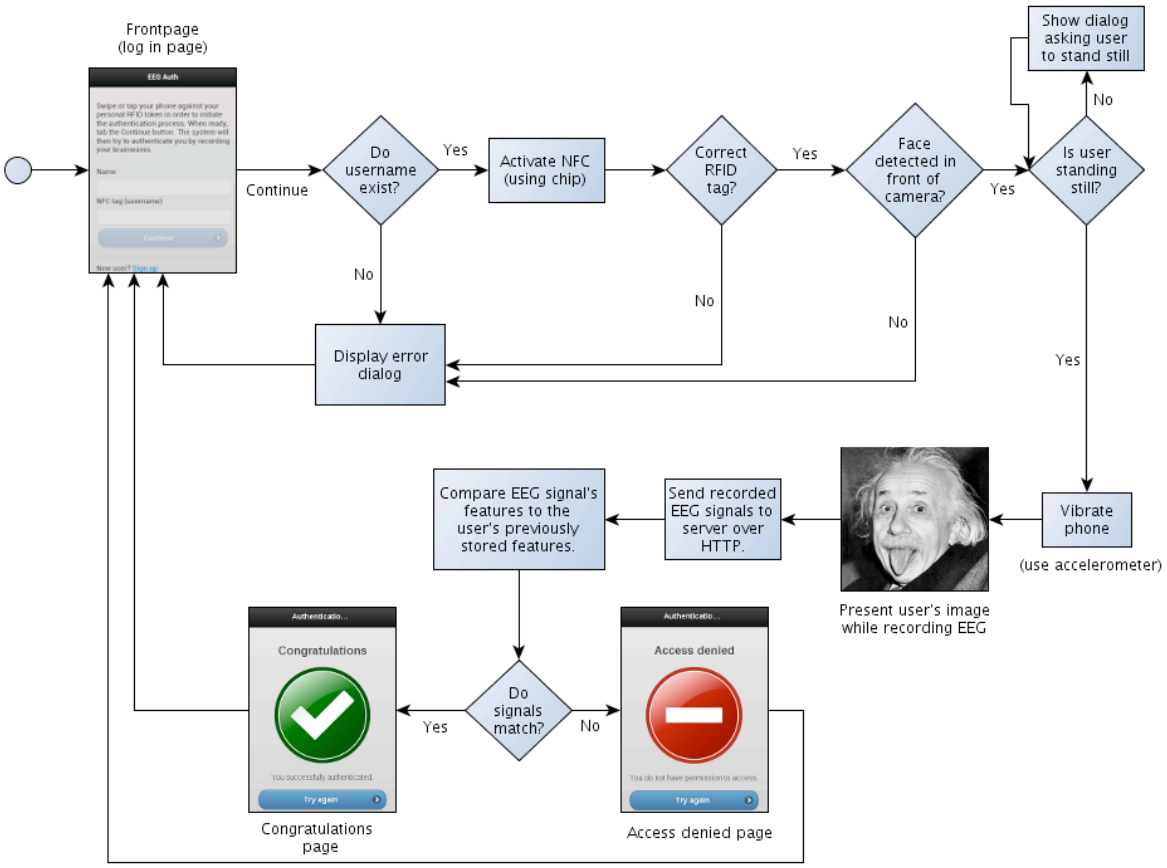

Fig. 3: Flowchart representing the authentication steps in the front-end. The diagram centers on a front page and shows how the user can try to authenticate using an existing user profile.

signals that contains data necessary to build an authentication system based on thought images, is carried out by gamma waves, which are filtered out in the brain tissues. The electrical activity of the brain sources is propagated through the anatomical structures and the resulting EEG is a linear mixture (with unknown or difficult to model parameters) of brain sources and other electro-physiological disturbances, often with a low signal to noise ratio (SNR) [24].

If brainwaves should be interpreted, it would be necessary to conduct a Structural MRI (Magnetic Resonance Imaging) and Functional MRI at the same time as measuring EEG, but this would be way costlier than the proposed system.

Taking these circumstances into account, it is still possible to identify a subject person using visual based EEG, but the process cannot stand alone for authentication purposes. Therefore there was a need to incorporate an additional step that the user must carry out in order to successfully authenticate. We chose to add the RFID validation step, hence making a two-factor system by requiring “something you have” in addition to “something you are” (the EEG).

The face and motion detection steps and vibration of the phone are not by themselves improving the security of the systems, but were added to take advantage of the most relevant context triggers on the phone, that could help ensure that the person trying to authenticate is as relaxed as possible and ready to concentrate.

F. Technical Back-end Setup

Based on our previous investigation [22], we proposed that the system should be able to carry out heavy DSP calculations on a server side, which ensures lowering the smartphone's processor load as well as giving several benefits in terms of security and scalability of the system. For this purpose, we set up an IIS 7.5 server, which operates the back-end part intended for processing the EEG data packages and extracting unique user features for the purpose of authentication. The back-end is also responsible for communication between the server and the EEG headset, as well as it responds to the front-end requests (see Fig. 5), and finally it exchanges the user specific data with the SQL database. The XML-based web interface is written in ASP.NET, and functionality is implemented with C# .NET, and for the data storage we use a Microsoft SQL 2012 server, which enables a cloud-ready information platform.

The back-end part consists of two main modules: 1) the Signal Acquisition and Pre-processing module and 2) the Feature Extraction and Classification module. The advantage of such division is that the system can adapt to any EEG hardware by adjusting only the Signal Acquisition and Pre-processing module. The main purpose of this module is to deliver the selected raw EEG data in a compact and organized form to the Feature Extraction and Classification module, which is responsible for calculating and delivering the final authentication results to the front-end.

The entire back-end system flow from the perspective of the EEG signal handling is illustrated in Fig. 4.

The Signal Acquisition and Pre-processing module is built using the OpenVIBE software platform [25], which is dedicated to designing, testing and employing brain-computer interfaces and it can be used to acquire, filter, process, classify and visualize brain signals in real time.

Based on the experiment results and the literature review [26][15], the most significant features can be extracted from the visual parietal-occipital cortex of the brain. Therefore the Channel Selector is created and set to obtain the data

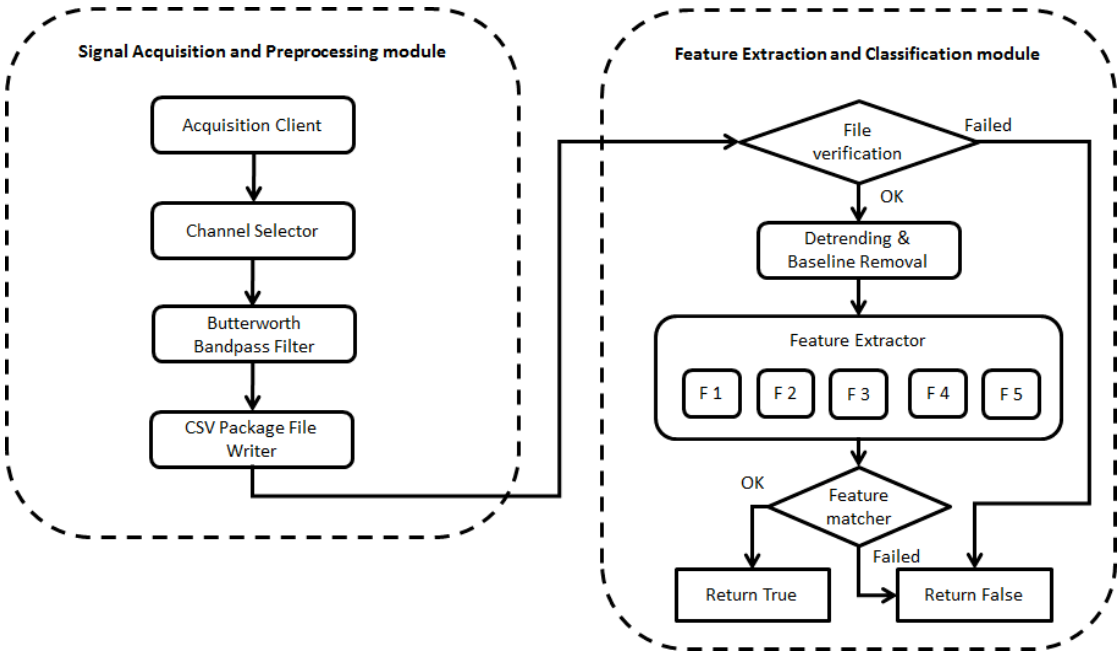

Fig. 4: Flowchart representing the EEG signal handling steps divided in two main modules. The first module represents the actual signal acquisition module, which should be implemented on the particular environment connected directly to the EEG measuring device. The second part is responsible for feature extraction and matching the extracted features to the database records on the server side.

from the following four EEG sensor locations: P7, P8, O1, O2, based on the international 10-20 system [27, p. 140]. The Butterworth band-pass filter was applied in order to reject frequencies, which are lower than 0.5 Hz and higher than 40 Hz, because these frequencies were not informative enough for further feature extraction. The CSV Package File Writer is responsible for generating EEG data packages by the request from the front-end and it logs six second EEG signal values including half a second before and after the famous face picture image is shown to the subject.

1) EEG Data Package Verification

The package file verification procedure is necessary to ensure that the signal is acquired correctly and that it can be further used for the extraction of unique biometric features. First of all it checks that the package exists and that it contains non-zero content, which is formatted correctly. This also reveals one of the reasons, why the De-trending and Baseline Removal part is not applied in the Signal Acquisition and Pre-processing module. In our system, the baseline itself is used to verify the package data, thus it is stored in a temporary buffer. For example, if there is a high fluctuation of the baseline, which exceeds the 100 μV value, it means that the EEG signal is too noisy and is not reliable for further feature extraction. This usually happens if the subject person is not adjusted the EEG headset properly, or if he or she is on-the-go. So if it happens, the back-end will automatically respond with false to the front-end request, so that the user will not be authenticated and will be asked to retry the authentication procedure.

2) Detrending and Baseline Removal

For easier feature extraction, it is necessary to remove the baseline of the raw EEG dataset for each electrode measurements individually, and the simplest way is to subtract the centred moving average of one-second time period from the six second recording. This step ensures that the signal is distributed around 0 and the valid remaining signal is five seconds long (rejecting a half of a second from each end) ranging from 1 Hz to 40 Hz frequency signal for the further processing.

Another reason, why this step was not applied in the Signal Acquisition and Pre-processing module, is that the baseline itself can potentially represent a unique biometric feature [28, p. 2], as it represents micro voltage values of the scalp. Therefore, it might be necessary to store the baseline of a 5-second-long EEG signal in the database as an extra component for further feature extraction.

3) Feature Extraction

We have revised and tested several EEG feature extraction techniques, which were suggested by EEG and DSP professionals as well as found in the literature as potentially unique. Before the feature extraction procedures, it was necessary to prepare signals and to enhance the signal-to-noise ratio and to reduce the configuration space we must evaluate by applying band-pass filters and Independent Component Analysis [29]. One of the simplest features, which proved the uniqueness from subject to subject, was zero-crossing rate, however it was not efficient enough to rely the whole authentication decision making on this one method only.

To improve the system reliability, several additional techniques were employed, such as power spectral density [30][31][32] and Wavelet analysis, based on 1) Morlet and 2) “Mexican hat” wavelets [33][34], where the feature output was multidimensional coefficient matrices. Therefore, it was relatively hard to distinguish differences between subjects from a large set of extracted data and at the same time to present the stationary of these features. From the power spectral density we were able to find the similarities in the histogram of the spectrogram image, and the wavelet analysis was beneficial to measure latencies of visual-evoked potentials at the occipital lobe area. This is a valuable finding for biometric authentication application, since these measures are more likely unique for a larger number of subjects, since nobody has the same neural-wiring of the brain. Finally, as a potentially beneficial feature for biometric au-

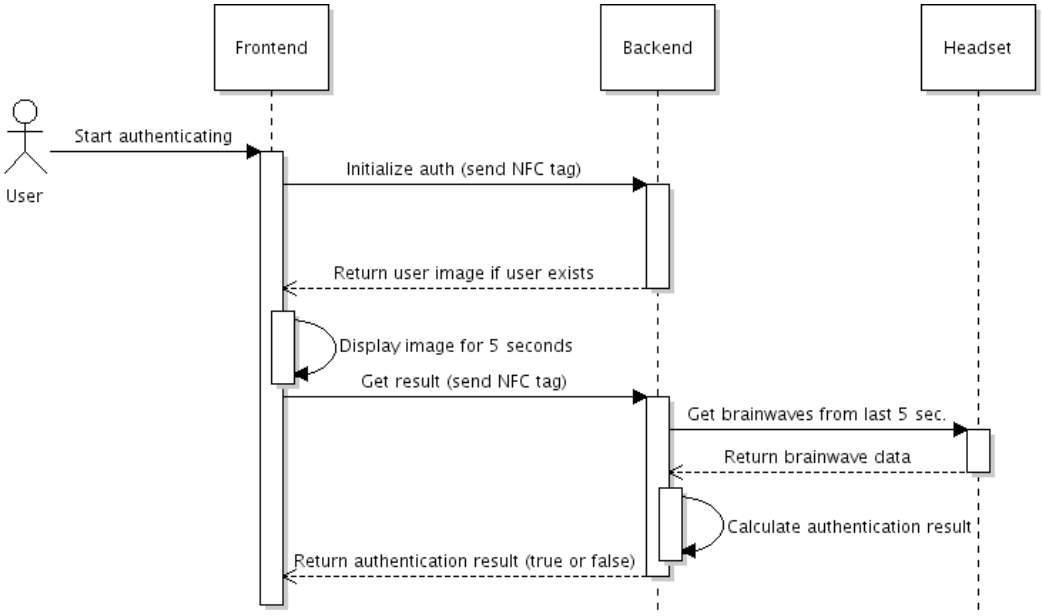

Fig. 5: Sequence diagram showing interaction between front-end, back-end and headset. Communication between front-end and back-end is carried out in a RESTful approach, with the front-end querying the back-end with GET parameters, and the back-end server responding with XML files.

thentication, we proposed to use eye artifact related signals and facial expressions.

G.Front-end-Back-end Communication Protocol

The front-end and back-end communicate with each other by means of a RESTful web interface. Simply put, REST (Representational state transfer) is an architectural style where data is exchanged over HTTP, for example in a client-server model [35]. In the prototype the front-end and back-end communicate over a WiFi connection, with the front-end querying data from the back-end by sending HTTP requests with additional GET parameters. The back-end will in return respond with data in XML format. As the front-end is simply a web application built with HTML, CSS and JavaScript, communication with the back-end server is done through AJAX calls using the JavaScript XMLHttpRequest API. Fig. illustrates the flow of data in the exchange protocol.

As it can be seen in the figure, the communication between front-end and back-end is initiated after the user has swiped a NFC tag against the smartphone, and the face- and motion-detection steps has been completed. The front-end will then send a request to the back-end containing the NFC tag as a GET parameter. If the NFC tag matches an existing user profile, the back-end responds with an XML file containing an image path. The front-end displays this image to the user while recording his or her brainwaves, and when the 5 seconds have elapsed, the front-end will send a new HTTP request to the server (sending the NFC tag as a GET parameter once more, as the exchange protocol is stateless). The intention of this second request is to get the result of the authentication process, and once calculated by the back-end server, it will be returned to the front-end in a simple XML file containing either true (for a positive authentication result) or false (for a negative authentication result).

V. Discussion & Conclusion

This paper has demonstrated the development of a new mobile EEG-based biometric person authentication system. We proposed that the short EEG recordings can be transformed to represent unique biometric identifiers, including both: behavioural and physiological characteristics. Sensor condition and adjustments of the EEG headset were critically important for successful system usage, however the exact sensor positioning was not so crucial.

As the system presented in this project is mobile based, it is especially suited for scenarios, where there is a sudden or unexpected need to prove an identity or authenticate, but that doesn't prevent it from being used more statically.

Based on our experience and feedback from the subjects we have tested, the comfortability of the Emotiv EPOC neuroheadset varies from subject to subject and some people finds it relatively uncomfortable to wear for a longer period of time. As our proposed system requires wearing the EEG headset for only a few seconds, this problem does not apply to our prototype. However, it might take relatively long time (up to approximately 10 minutes) for adjusting procedures of the Emotiv EPOC headset, which potentially makes the EEG authentication service impractical. These procedures are moisturising the EEG sensors and adjusting sensors on the correct locations by avoiding hair. The individuals with bushy hair have more problems in adjusting the sensors. To solve this issue, it is necessary to investigate further how the EEG hardware should be build, and as mentioned before, the dry sensor electrodes might be more appropriate and reliable.

We have seen a positive side-effect security-wise of basing the system on brainwave recordings from relaxed subject persons, since it makes it impossible for an intruder to directly force a user to authenticate. If stress signals are present in the measured brainwaves it will result in a denial of access.

VI. Future Work

In a future version of the system, it would be relevant to use more unique features, which are complementary to each other, and cover all of the five EEG characteristics (frequencies, amplitudes, wave morphology, spatial distribution, reactivity), so that behavioural and physiological data is

covered for authentication reasoning. Furthermore, we suggest using emotional states (which can be extracted from the Emotiv research package) as an extra context, in order to avoid emotional states influencing the authentication result, by adjusting features accordingly. We also believe that facial expressions detected from the brainwaves and the smartphone camera can be beneficial for increasing the security level of the system, since they can be used as an extra context trigger.

REFERENCES

[1] R.J. Wilkus, "The EEG as confirmatory evidence of brain death: Previous and current approaches," *Journal of Medical Humanities*, vol. 2, Mar. 1980, pp. 39–45.

[2] S. Akben, A. Subasi, and D. Tuncel, "Analysis of EEG Signals Under Flash Stimulation for Migraine and Epileptic Patients," *Journal of Medical Systems*, vol. 35, Jun. 2011, pp. 437–443.

[3] L. Jameson and T. Sloan, "Using EEG to monitor anesthesia drug effects during surgery," *Journal of Clinical Monitoring and Computing*, vol. 20, Dec. 2006, pp. 445–472.

[4] Q. Zhao, H. Peng, B. Hu, Q. Liu, L. Liu, Y. Qi, and L. Li, "Improving Individual Identification in Security Check with an EEG Based Biometric Solution," *Brain Informatics*, Y. Yao, R. Sun, T. Poggio, J. Liu, N. Zhong, and J. Huang, eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 145–155, Available online: http://www.springerlink.com.zorac.aub.aau.dk/content/g53n47235k5u5542/, (Accessed: January 31, 2012).

[5] J. Ales, T. Carney, and S.A. Klein, "The folding fingerprint of visual cortex reveals the timing of human V1 and V2," *NeuroImage*, vol. 49, Feb. 2010, pp. 2494–2502.

[6] N. Reefmann and T. Muehlemann, "Simultaneous measurement of brain activity, physiology & behavior in large animals," *Proceedings of the 7th International Conference on Methods and Techniques in Behavioral Research*, 2010, Available online: http://www.agroscope.admin.ch/publikationen/einzelpublikation/index.html?lang=en&aid=22334&pid=22962, (Accessed: May 31, 2012).

[7] A.F. Mirsky and P.V. Cardon Jr., "A comparison of the behavioral and physiological changes accompanying sleep deprivation and chlorpromazine administration in man," *Electroencephalography and Clinical Neurophysiology*, vol. 14, Feb. 1962, pp. 1–10.

[8] K. Li, V. Narayan Raju, R. Sankar, Y. Arbel, and E. Donchin, "Advances and Challenges in Signal Analysis for Single Trial P300-BCI," *Foundations of Augmented Cognition. Directing the Future of Adaptive Systems*, D. Schmorrow and C. Fidopiastis, eds., Springer Berlin / Heidelberg, 2011, pp. 87–94, Available online: http://www.springerlink.com/content/n1302838231852x2/abstract/, (Accessed: June 3, 2012).

[9] E.G. Jones, "Cortical and Subcortical Contributions to Activity-Dependent Plasticity in Primate Somatosensory Cortex," *Annual Review of Neuroscience*, vol. 23, 2000, pp. 1–37.

[10] L. Graziano Breuning, "How Your Brain Wires Itself," *Meet Your Happy Chemicals: Dopamine, Endorphin, Oxytocin, Serotonin*, CreateSpace, 2012, p. 210.

[11] E. Ackerman and L.C. Gatewood, *Mathematical Models in the Health Sciences: A Computer-Aided Approach*, University of Minnesota Press, 1979.

[12] J. Klonovs and C.K. Petersen, "Development of a Mobile EEG-Based Feature Extraction and Classification System for Biometric Authentication," Aalborg University Copenhagen, 2012.

[13] J. Harper, *Identity Crisis: How Identification is Overused and Misunderstood*, Cato Institute, 2006.

[14] J. Thorpe, P.C. van Oorschot, and A. Somayaji, "Pass-thoughts: authenticating with our minds," *Proceedings of the 2005 workshop on New security paradigms*, New York, NY, USA: ACM, 2005, pp. 45–56, Available online: http://doi.acm.org/10.1145/1146269.1146282, (Accessed: May 18, 2012).

[15] A. Zúquete, B. Quintela, and J.P.S. Cunha, "Biometric Authentication using Brain Responses to Visual Stimuli.," *BIOSIGNALS*, Aveiro, Portugal: Institute of Electronics and Telematics Engineering of Aveiro (IEETA), 2010, pp. 103–112, Available online: http://www.ieeta.pt/~avz/pubs/BIOSIGNALS10.pdf, (Accessed: February 22, 2012).

[16] J.G. Snodgrass and M. Vanderwart, "A standardized set of 260 pictures: norms for name agreement, image agreement, familiarity, and visual complexity," *Journal of Experimental Psychology. Human Learning and Memory*, vol. 6, Mar. 1980, pp. 174–215.

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

[18] J. Rønager, *Interview and Meeting about EEG and authentication.*, Aalborg University Copenhagen: 2012.

[19] "IDC: Android jumps to 68.1% global market share, iOS slips to 16.9%," *Android Authority* Available online: http://www.androidauthority.com/idc-android-jumps-to-68-1-global-market-share-ios-slips-16-9-106446/, (Accessed: October 5, 2012).

[20] Google Inc., "Philosophy and Goals," *Android Open Source* Available online: http://source.android.com/about/philosophy.html, (Accessed: May 3, 2012).

[21] "Identification and authentication" Available online: http://publib.boulder.ibm.com/infocenter/cicsts/v3r1/topic/com.ibm.cics.ts31.doc/dfht5/topics/dfht5ni.htm, (Accessed: May 27, 2012).

[22] J. Kļonovs and C.K. Petersen, *Mobile Mind State Detection Services*, Denmark: Aalborg University Copenhagen, 2011.

[23] Emotiv, *Emotiv SDK Research Edition Specifications*, Available online: http://www.emotiv.com/upload/manual/sdk/Research%20Edition%20SDK.pdf, (Accessed: May 13, 2012).

[24] D.M. Goldenholz, S.P. Ahlfors, M.S. Hämäläinen, D. Sharon, M. Ishitobi, L.M. Vaina, and S.M. Stufflebeam, "Mapping the Signal-To-Noise-Ratios of Cortical Sources in Magnetoencephalography and Electroencephalography," *Human brain mapping*, vol. 30, Apr. 2009, pp. 1077–1086.

[25] Y. Renard, F. Lotte, G. Gibert, M. Congedo, E. Maby, V. Delannoy, O. Bertrand, and A. Lécuyer, "OpenViBE: An Open-Source Software Platform to Design, Test, and Use Brain–Computer Interfaces in Real and Virtual Environments," *Presence: Teleoperators and Virtual Environments*, vol. 19, Feb. 2010, pp. 35–53.

[26] A. Zúquete, B. Quintela, and J.P.S. Cunha, "Biometric Authentication with Electroencephalograms: Evaluation of Its Suitability Using Visual Evoked Potentials," *Biomedical Engineering Systems and Technologies*, A. Fred, J. Filipe, and H. Gamboa, eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 290–306, Available online: http://www.springerlink.com.zorac.aub.aau.dk/content/g6878412401753n5/, (Accessed: January 31, 2012).

[27] E. Niedermeyer and F.L. da Silva, eds., *Electroencephalography: Basic Principles, Clinical Applications, and Related Fields*, Lippincott Williams & Wilkins, 2004.

[28] I. Damousis, D. Tzovaras, and E. Bekiaris, "Unobtrusive Multimodal Biometric Authentication: The HUMABIO Project Concept," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Jan. 2008, p. 265767.

[29] L. Zhukov, D. Weinstein, and C. Johnson, "Independent component analysis for EEG source localization," *IEEE Engineering in Medicine and Biology Magazine*, vol. 19, Jun. 2000, pp. 87 –96.

[30] F. Cona, M. Zavaglia, L. Astolfi, F. Babiloni, and M. Ursino, "Changes in EEG Power Spectral Density and Cortical Connectivity in Healthy and Tetraplegic Patients during a Motor Imagery Task," *Computational Intelligence and Neuroscience*, vol. 2009, 2009, pp. 1–12.

[31] M. Zavaglia, L. Astolfi, F. Babiloni, and M. Ursino, "The effect of connectivity on EEG rhythms, power spectral density and coherence among coupled neural populations: analysis with a neural mass model," *IEEE transactions on bio-medical engineering*, vol. 55, Jan. 2008, pp. 69–77.

[32] R. Palaniappan, "Two-stage biometric authentication method using thought activity brain waves," *International Journal of Neural Systems*, vol. 18, Feb. 2008, pp. 59–66.

[33] "Methodological Framework for EEG Feature Selection Based on Spectral and Temporal Profiles - Springer," Available online: http://link.springer.com/chapter/10.1007/978-0-387-88630-5_3?no-access=true, (Accessed: October 5, 2012).

[34] C.S. Herrmann, M. Grigutsch, and N.A. Busch, "EEG oscillations and wavelet analysis," *Event-related potentials: a methods handbook*, T. Handy, ed., Cambridge: MIT Press, 2005, pp. 229 – 259, Available online: http://wase.urz.uni-magdeburg.de/cherrman/pdfs/MIT-Bookchapter.pdf, (Accessed: January 21, 2010).

[35] A. Rodriguez, "RESTful Web services: The basics," *IBM.com Developerworks page REST*, Nov. 2008 Available online: http://www.ibm.com/developerworks/webservices/library/ws-restful/, (Accessed: May 8, 2012).