Consumer grade Brain Computer Interfaces as an augmented security measure for authentication

Ivens Applyrs, Bhaveek Desai, Julian Mendoza, Ernest Williams, Juan E. Gilbert
Computer and Information Science and Engineering Department, University of Florida

Abstract

Brain Computer Interfaces (BCIs) have largely been limited to the medical space. Often to collect the necessary amount of physiological data needed, medical researchers spend thousands to millions of dollars on high end electroencephalogram (EEG) machines. However, with the increased presence of affordable consumer grade BCIs further research questions have developed. One such question is the utilization of consumer grade BCIs as an augmented security measure for authentication. Within this space the increasing demand for more robust and easy to use security measures can be satisfied. Current biometric forms of identification, such as finger print and retinal scans, demonstrate the full capacity of having a user specific authentication system. However recent developments in technology have demonstrated that this may no longer be a viable option. This research aims to incorporate physiological data with current biometric identification practices to analyze if a device or framework can be accessed solely through EEG data correlations.

1 Introduction

Data acquisition through consumer grade brain computer interfaces (BCIs) has grown exponentially. It is now a commonality to apply BCIs outside of the medical space: such as applications in control, education, entertainment, and more (Van Erp, J. B., Lotte, F., & Tangermann, M. (2012, April))[3]. The capabilities of data acquisition in BCIs have developed to the point of reducing a 100+ channel BCI device to less than 15 channels of usable brainwave data. Companies such as Emotiv and Muse have produced affordable devices that collect

electroencephalogram (EEG) data with as little as 7 channels. BCI devices are recognized in two general forms; invasive (surgically implemented) and non-invasive (dry or wet electrodes).

Invasive devices or intracranial EEG devices are deemed the most effective in terms of data acquisition, due to the proximity of the device to the brain and high signal-to-noise ratio. However, due to the increased health risks and ethical concerns this form is limited to medical applications such as ALS and Epilepsy patients [7].

The second form of BCI devices are non-invasive or extracranial EEG devices. Non-invasive devices are generally categorized as a wet or dry electrodes device depending on the setup. This form is often susceptible to negative feedback caused by the increased proximity of the electrodes to the brain. So it generally has a low signal-to-noise ratio. The 10-20 model (Fig. 1) is generally used to map the placement of the BCI electrodes. This aligns each electrode to specific regions of the brain to create the clearest and most accurate channels to extract brain waves. This is currently the most applicable device for research due to safety and setup time.

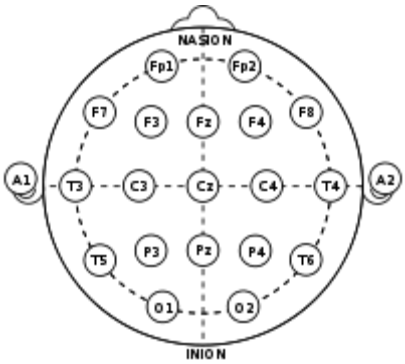

Fig. 1. Electrode placements for the International 10-20 Standard. The placement of a respective BCI electrode corresponds to a location on this map.

In the security space, there has come increased demand for more protection from hackers and identity theft. However, there is also a need for high-end security that is efficient yet easy to

use. Individuals are unwilling to traverse through the endless security questions, multi-character passwords, and hierarchal security walls. The growing area of biometric identification has consistently been the solution to providing high end security with user friendly interface. The current security measures, such as fingerprint and retinal display, have an underlying problem not addressed. Current forms of biometric identifications are not able to be "canceled" [8]. Per [1] hackers are capable of utilizing a high definition photo to reconstruct an individual's finger print. With this potential flaw in fingerprint security, protecting important data has proven more difficult.

This research aims to explore the capabilities of Brain Computer Interfaces (BCIs) in the space of security. Particularly, can consumer based BCIs be used as a form of biometric identification. The proposed testing device for this research will be the Emotiv Insight (Fig. 2). Combined with its robust testing platform, minimal setup time, and attractable design, it presents itself as the most desirable testing tool to for this research. The objective of this research is to apply this consumer grade BCI as an augmented form of security measure for authentication. In doing so, this research hopes to provide viable solutions to current security issues today.

Fig. 2 The Emotiv Insight is the second model released by Emotiv. It provides 5 channels and 2 reference nodes to record brainwaves. It is a non-invasive dry electrode device.

We propose unlocking a device or a predesigned testing framework storing a random set of data. This has varying levels of analysis encompassing data acquisition, pre/post processing, application, and the user interface. It is a developing field of study [4] and based on previous research conducted by [5] and [6], we hypothesize that consumer grade BCIs can be used as a form of authentication with a sleek user interface.

Methods

2 Practicality Testing

Consumer grade BCIs come in several different models with different capabilities. Some are in the shape of headsets while others look like headphones. With such varying levels of performance, design, and usability, each device needed to be analyzed to determine the most viable option for long term use. To initialize the study of whether a consumer grade BCI can be used as an 'augmented security measure for authentication' a testing environment had to be developed. The BCI devices available for testing were the Emotiv Epoc+ (Fig. 3), Emotiv Insight, & Muse (Fig. 4). Each device needed to be examined based on the current technical support provided, its ability to acquire accurate data, and its usability. These areas play a pivotal role in setting up the research as every device may not wield the same results. The breakdown of each specification of these devices is provided by Table 1.

BCI Device	**Channels**	**Type**	**Connectivity**
Emotiv Epoc+	14	Wet Electrodes	Bluetooth
Emotiv Insight	5	Dry Electrodes	Bluetooth
Muse	5	Dry Electrodes	Bluetooth

Table 1. The specification of BCI devices from two leading companies (Emotiv and Muse)

Fig 3. Is the Emotiv Epoc+ a wet electrode consumer grade BCI with 14 channels.

Fig 4. Is the Muse Headband a dry electrode consumer grade BCI with 5 channels.

Each subject was placed in front of a minute and 30 second stimulus while the BCI device was fixed on their head. During each phase of the data acquisition stage, time was logged for preparation and connection. Preparation was considered as anything that needed to be done before the subject was asked to place the device on their head. For the Emotiv Epoch+ this was necessary time required to wet the electrodes or create a testing bench. Connection time was considered as the time between placing the device on the subject's head and acquiring data. We set a threshold of 90% of active channels before acquiring data.

3 Authentication Testing

The next phase of this research is authentication testing. Determining the varying levels of self-similarity and cross-similarity using the pearson product-moment correlation coefficient paired with Matlab.

Pearson product-moment correlation

This is the measure of the linear correlation between two variables A and B. In the augmented sense, the study of the relationship between two random data sets or the extent to which two data sets have a linear relationship. This algorithm is represented below.

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}}$$

Where

- $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$ (the sample mean); and analogously for $\bar{y}$

With the selected BCI Device, users recorded their EEG data using the Testbench suite provided by Emotiv. The record EEG data was collected between four subjects over a three-day span of time. Within each day the subject watched an amended version of the minute and 30 second stimulus utilized in the practicality testing. This stimulus was a count down from 10 to 1 which was watched in the morning, noon, and evening. This created a sample size of nine data sets which were implemented into Matlab. Using pearson's correlation algorithm each recording was compared to other subjects and their own individual sessions.

Bibliography

1. Kleinman, Z. (2014, December 29). Politician's fingerprint 'cloned from photos' by hacker. Retrieved from http://www.bbc.com/news/technology-30623611
2. Chuang, J., Nguyen, H., Wang, C., & Johnson, B. (2013). I Think, Therefore I A m: Usability and Security of Authentication Using Brainwaves. National Science Foundation, 1-16.
3. Van Erp, J. B., Lotte, F., & Tangermann, M. (2012, April). Brain-Computer Interfaces: Beyond Medical Applications. 26-34. doi:0018-9162/12/$31.00 © 2012 IEEE
4. Marcel, S., & Millan, J. D. (2007). Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation. IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 29(4), 743-748. doi:10.1109/TPAMI.2007.1012.
5. Marcel, S., & Millan, J. D. (2007). Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation. IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 29(4), 743-748. doi:10.1109/TPAMI.2007.1012.
6. Thorpe, J., Oorschot, P. V., & Somayaji, A. (2006). Pass-thoughts: Authenticating with Our Minds. 45-56. doi:1-59593-317-4/06/02....$5.00
7. Lal, T. N., Schröder, M., Hill, J. N., Rosenstiel, W., Elger, C. E., Schölkopf, B., et al. (2005). Methods towards invasive human brain computer interfaces. In L. K.Soul, Y.Weiss, & L.Bottou (Eds.), Advances in Neural Information Processing Systems (vol. 17, pp. 737–744). Cambridge, MA: MIT Press.
8. Moore, S. K. (2016, April). “Brainprint” Biometric ID Hits 100% Accuracy. IEEE Spectrum. Retrieved from http://spectrum.ieee.org/biomedical/devices/brainprint-biometric-id-hits-100-accuracy