INTRODUCTION TO EEG AND ITS USE IN PERSON AUTHENTICATION

Michal Košík

Doctoral Degree Programme (1), FIT BUT

E-mail: xkosik00@stud.fit.vutbr.cz

Supervised by: Martin Drahanský

E-mail: drahansky@fit.vutbr.cz

Abstract: This paper offers an introduction to the topic of electroencephalography and its use in person authentication. It explains principles of encephalograph as a machine as well as various techniques used with authentication via brain waves. Comparison with several other devices for measuring brain activity and comparison with some other biometrics is discussed here as well. Finally, previous research by other scientist in this area is presented.

Keywords: electroencephalograph, electroencephalogram, EEG, brain waves, biometrics, person authentication, authentication using EEG.

1. INTRODUCTION

An authentication system is a system that confirms or rejects the identity claimed by a person. It is a one-to-one matching, unlike an identification system which attempts to identify a given person in a finite pool of N people (one-to-N matching). Both types of systems share the same preprocessing, extraction of features and also a great part of classification unit [5].

However, the use of both systems differs. Identification systems are usually deployed in surveillance applications, where people do not tend to interact with the system directly. On the other hand, authentication systems are used to grant access (e.g. to a computer, building) or rights (transaction authorization), causing that people are supposed to willingly cooperate with them.

Authentication systems use various approaches – some can be based on knowledge of password, others on a possession of item (e.g. a chip) and some on some traits such as face, fingerprints or voice. An interesting approach is use of brain waves for person authentication. This paper offers an introduction to this topic.

The paper consists of three main parts: First, there is an introduction to electroencephalography with explanation of its principles; second part talks about the electroencephalograph from the person authentication perspective; and finally the third part presents research done in this area so far. At the end, all information is summarized and future work is suggested.

2. ELECTROENCEPHALOGRAPHY

Electroencephalography is recording of electrical activity along the scalp that is generated by a collective activity of neurons located mainly in cortex, since signal from deeper (inner) layers of the brains is usually attenuated. In order to be able to record this activity, neurons have to fire synchronously and be oriented towards the surface of the head [9]. These signals then can be recorded by placing voltage sensitive electrodes on the scalp, where each electrode records a stereotyped signal. Device that records these signals is called electroencephalograph and its output is called electroencephalogram (EEG); it is a 2D graph, in which a horizontal axis is of time and vertical is of voltage [6].

2.1. History and Use

The first human EEG was recorded by German physiologist and psychiatrist Hans Berger in 1924 (see Figure 1) who also invented encephalograph giving it its name. Since then, electroencephalograph has been used in medicine in a variety of cases, e.g. in diagnose of epilepsy, loss of consciousness and dementia, or brain death confirmation [11].

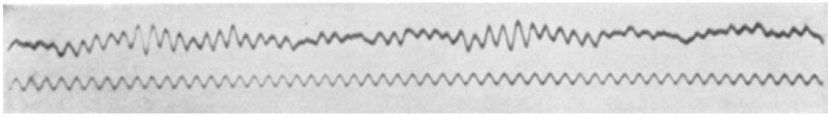

Figure 1: One of the first human EEGs recorded by Hans Berger. The lower tracing is a 10 Hz timing signal. Source: http://en.wikipedia.org/wiki/Electroencephalography

Another use is a brain-computer interface (BCI). BCI can be described as a system that translates brain electrical activity to signals controlling external devices [4]. However, using EEG as BCI usually requires an extensive training prior to active usage [4].

EEG can be also used in person identification and authentication; the use of EEG as a biometric was first proposed by Forsen in 1977 [9].

2.2. Signal Recording

As mentioned above, EEG is recorded by electrodes placed on the scalp. To unify electrode placement and to ease reproduction of results of various experiments, several systems of placing electrodes on the scalp were created and are still in use [7]. The most known is the “International 10-20 system”, where distances between two adjacent electrodes are 10% and 20% of total front-back and right-left distance of the skull respectively. This system allows placing up to 21 electrodes.

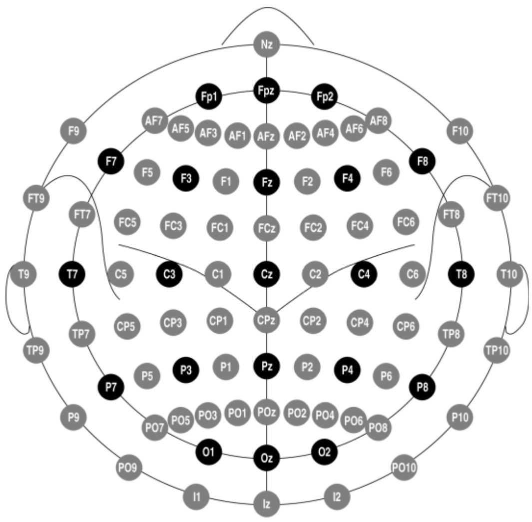

Figure 2: Electrodes positions and labels in 10-20 system (black circles) and in 10-10 extension (black and gray circles) [7]

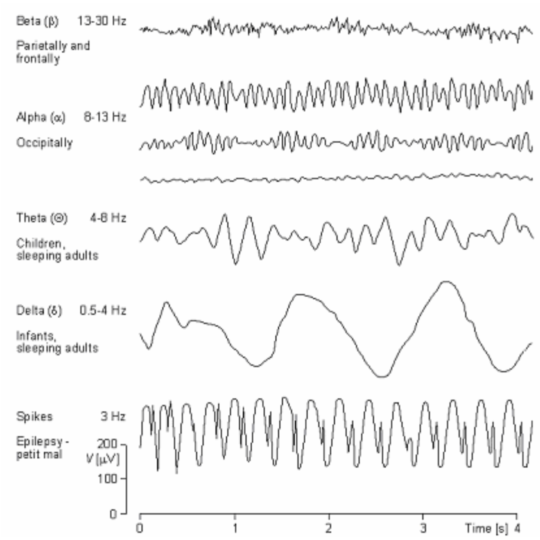

Figure 3: Example of several frequency bands [9]

If more electrodes need to be used, new electrodes are added in between of two left-right adjacent electrodes from 10-20 system; this system of electrodes placement is known as “10% system” or “10-10 system” and allows placing up to 74 electrodes, as Figure 2 shows.

Names of electrodes placed on the same position remain the same in all systems. Each electrode measures electrical potential (measured in mV after amplifying) on the scalp at various frequency bands sampled at various frequencies; for authentication purposes, it is usually between 0.5-1.0 KHz [9]. The signal from electrodes tends to contain noise and various artefacts caused e.g. by eyes movements or teeth clenching [10].

Brain waves have been categorized to several frequency bands according to their frequencies. These bands (also known as rhythms) are: Delta (0.5-4 Hz), theta (4-8 Hz), alpha (8-13 Hz), mu (8-12 Hz), beta (13-30 Hz) and gamma (>30 Hz) [9].

It is important to highlight that none of these waves are ever emitted alone; however, the state of conscious of an individual may result in one frequency to be more prominent as the others [11]. For example, alpha waves are dominant in relaxed state with eyes closed; on the contrary, beta waves are dominant in active calm state, when eyes are open [6]. Figure 3 shows several frequency bands.

2.3. COMPARISON OF EEG WITH OTHER METHODS FOR STUDYING BRAIN FUNCTION

There are several other non-invasive methods for studying brain function, including functional magnetic resonance imaging (fMRI); magnetoencephalography (MEG) that records brain's magnetic fields; positron emission tomography (PET) which observes brain metabolic activity, that is reflected in changes in blood flow; or near-infrared spectroscopy (NIRS).

Each of these devices has certain advantages compared to EEG – for example, they can provide detailed information on the activity of very small brain areas, even in deeper regions of the brain and with much higher signal-to-noise ratio (e.g. fMRI).

On the other hand, there are several disadvantages - hardware costs for most of these devices and their spatial, power or other requirements are much higher than those of EEG. For example, fMRI and MEG require a shielded room, Furthermore, EEG can provide much higher sampling rates than the most of the devices mentioned above (except of MEG; on the other hand, PET is extremely slow in comparison to EEG). Also, EEG does not emit sound and is relatively tolerant to subject's movements. This whole section draws from [5] and [11].

3. ELECTROENCEPHALOGRAM AS A BIOMETRIC

Biometric can be defined as any biological of physiological signal that can be used to identify or authenticate a person [8]. Several biometric-based systems exist, such as systems using fingerprint, retinal or iris scanning, speech matching, 2D or 3D face recognition, hand geometry, etc.

Authentication of a person is a confirmation (or rejection) of the identity claimed by this person based on the information he or she provided. This information is usually one of three categories: knowledge (e.g. a password or PIN); possession (a chip, passport, etc.); or trait (such as fingerprint, retina, or brainwaves) [2]. Person authentication is performed by an authentication system.

Most end user authentication systems implement either knowledge/knowledge (for example username/passport) or possession/knowledge (ATM card/PIN) combinations. However, biometric systems based on intrinsic physical and behavioral traits are being implemented [2].

For a biometric to be used in an authentication system, it must meet several conditions [3]: Universality, uniqueness, permanence, and collectability. Moreover, several other criteria need to be satisfied [3]: Performance (namely recognition accuracy and speed), acceptability (how willing are people to accept this biometric to be used in their daily lives), and circumvention (how difficult it is to fool the authentication system to accept an intruder).

All biometrics used today satisfy the first four conditions. However, they vary in the last three criterions. For example, although fingerprints achieve high performance in person verification and authentication, systems using this biometric have been reported to be circumvented by fake fingers [3]. Furthermore, most of these biometrics are unsuitable for continuous authentication i.e. authentication not only prior to granting access to a system, but during the whole time the user interacts with the system. Face can be used for this purpose, although it can be imitated [6].

EEG can be used for continuous authentication as well. Moreover, it offers several additional advantages: it is confidential (as it usually corresponds to a mental task); it is very difficult to mimic (each person EEG is unique; therefore, even if more people are performing the same mental task, their EEGs differ); and it is very difficult to steal unless the person is voluntarily willing to cooperate (since brain activity is sensitive to stress; therefore the aggressor cannot force the person to reproduce his or her mental state necessary for authentication) [2], [5]. Furthermore, as EEG measures brain activity that happens inside the skull, as biometric it is effective for anti-circumvention (unless a whole model of the brain was created, what would be difficult). Also, brainwaves themselves can be used for liveliness detection.

3.1. AUTHENTICATION METHODOLOGIES

EEG as biometric makes use of several facts known about human brain [4]: Various states of human consciousness are linked to various frequency bands being dominant in various parts of cortex; human brain responds to some stimuli and these responses cannot be willingly suppressed nor controlled; and EEG signals can to some extent be voluntarily brought under control.

As mentioned before, when a mentally healthy adult person is in relaxed state with his or her eyes closed, alpha waves are dominant in this person's posterior regions of the head [6], [10]. A unique pattern occurs in each person's EEG which can be extracted and compared to a sample version.

Another option is to use brain's response to stimuli. These stimuli occur when a rare event occurs in a series of frequent events. Such brain responses belong to a category called event related potentials (ERPs) or evoked potentials (EPs). An ERP is identified by its latency, polarity (P – positive, N – negative) and spatial location. The less probable the elicit event, the larger response signal amplitude e.g. when recognizing a known image in a sequence of other images.

Additionally, a person can be asked to perform some action that is known to result in changes in his or her EEG. Such tasks are (and not limited to), motor movement (real movement of a body part [12]), motor imagery (e.g. imagining hand movements [5]), imagining speech [5], performing mental computation or reading [2], rotating or moving an object [2], or any other suitable task.

4. ONGOING RESEARCH

Experiments with EEG as biometric were usually performed with only several subjects. A number of different approaches have been chosen while experimenting, covering all previously mentioned authentication methodologies.

Paranjape et al [8] recorded several 8.33 seconds long EEGs of 40 subjects with their eyes closed and eyes opened using only a single electroencephalograph's channel – P4, resulting into 100% of subjects being correctly classified. Nahanishi et al [6] used alpha rhythm for authentication by using spectrum analysis on 23 subjects. By comparing subjects' EEGs with their EEGs taken one year before this experiment, he claims the long-term variation of the power spectrum in the alpha band is small. Su et al [10] who used EEG in a covert warning system. If a person clenches his teeth, a secret alert message is sent to authorities. Alert messages were correctly detected in 100% of cases when testing subjects were properly instructed.

Comparison of effectiveness of authentication when performing motor movement and motor imagery tasks was conducted by Yang and Deravi [12]. 18 subjects performed 3 runs of 2 motor movement tasks and 2 motor imagery tasks. The results showed the imagery tasks generally outperform the movement tasks in generating signals for EEG identification and authentication. Marcel and Millán, on the other hand, [5] focused only on imagery tasks. 9 subjects took sessions over three days. They were asked to perform three actions – to imagine a repetitive left hand movement; to imagine a repetitive right hand movement; and to generate words starting with the a random letter. Results showed that motor imagery tasks are better for authentication purposes than word imagining, performance slightly degrades over day although, and that there is a potential for incremental learning.

5. CONCLUSION

In comparison with other brain waves measuring techniques, EEG is cheap, allows fast data collection (in hundreds of Hz and more), and is portable (unlike equipment necessary for fMRI), what may to some extent compensate its lower signal-to-noise ratio.

Compared to other biometrics, EEG offers higher robustness against falsification with built-in liveliness test, possibility of continuous recording and many others advantages. Its main drawbacks are lower signal-to noise ratio, artifacts and the necessity of putting electrodes and gels on scalp.

Previous research in this area focused on various technics used in person identification and authentication using a range of approaches – from recording EEG while the subject is in relaxed state with eyes closed, through imagining words or limbs movement, up to reacting to various stimuli.

EEG is an interesting biometric that still waits to show its full potential. By removing artefacts, improving its signal-to-noise ratio and creating a portable and easy-to-use device, it can be used not only in person authentication, but also as standard human-machine interface device.

REFERENCES:

[1] Abdullah, M., et al: Analysis of Effective Channel Placement for an EEG-based Biometric System. In: IEEE EMBS Conference on Biomedical Engineering & Sciences, 2010, pp 303 – 306

[2] Ashby, C., et al: Low-Cost Electroencephalogram (EEG) based Authentication. In: International IEEE/EMBS Conference on Neural Engineering, 2011, pp 442 – 445

[3] Jain, A., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. In: IEEE Trans. on Circuits and Systems for Video Technology, 2004, pp 4-20

[4] Kubler, A., et al: Brain-Computer Communication: Unlocking the Locked In. In: Psychological Bulletin, 2001, pp 358 – 375

[5] Marcel, S., Millán, R.: Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007, pp 743 – 752

[6] Nakanishi, I, et al: EEG Based Biometric Authentication Using New Spectral Features. In: International Symposium on Intelligent Signal Processing and Communication Systems, 2009, pp 651 – 654

[7] Oostenveld, R., Praamstra, P.: The five percent electrode system for high-resolution EEG and ERP measurements. In: Clinical Neurophysiology, 2001, pp 713 – 719

[8] Paranjape, R., Mahovsky J., Benedicenti, L., Koles, Z.: The electroencephalogram as a biometric. In: Canadian Conference on Electrical and Computer Engineering, 2001, pp 1363 – 1366

[9] Revett, K., Deravi, F., Sirlantzis, K.: Biosignals for User Authentication – Towards Cognitive Biometrics?. In Proceedings of the 2010 International Conference on Emerging Security Technologies, 2010, pp 71-76

[10] Su, F., et al: A biometric-based Covert Warning System Using EEG. In: International Conference on Biometrics, 2012, pp 342 – 347

[11] Tangkraingkij, P., et al: Selecting Relevant EEG Signal Locations for Personal Identification Problem Using ICA nad Neural Networks. In: IEEE/ACIS International Conference on Computer and Information Science, 2009, pp 616 – 621

[12] Yang, S., Deravi, F.: On the Effectiveness of EEG Signals as a Source of Biometric Information. In: International Conference on Emerging Security Technologies, 2012, pp 49 - 52