A Study on the Feasibility of Using EEG Signals for Authentication Purpose

Tien Pham[1], Wanli Ma[1,2], Dat Tran[1], Phuoc Nguyen[1], and Dinh Phung[1]

[1] Faculty of Education, Science, Technology and Mathematics,
University of Canberra, Australia
[2] Department of Computer Science, University of Houston Downtown, USA
{tien.pham,wanli.ma,dat.tran,phuoc.nguyen,
dinh.phung}@canberra.edu.au

Abstract. Authentication is to verify if one is who he/she claims. It plays an important role in security systems. In this paper, we study the feasibility of using Electroencephalography (EEG) brain signals for authentication purpose. In a general sense, there are three types of authentications including password based, token based, and biometric based. Each of them has its own merit and drawback. Technology advancing makes it possible to easily obtain EEG signals. The evidences show that finding repeatable and stable brainwave patterns in EEG data is feasible. The prospect of using EEG signals for authentication is promising. An EEG based authentication system has the combined advantages of both password based and biometric based authentication systems, yet without their drawbacks. Therefore, it makes an EEG signal based authentication suitable for especially high security system. Through the analysis and processing of EEG signals of motor imagery from BCI Competition, our experiment results confirm the theories stated in this paper.

Keywords: EEG, machine learning, pattern recognition, authentication, security.

1 Introduction

Authentication is the fundamental function of a security system to verify if one is who he/she claims. In general, there are three means of authentications: password based (something the individual knows), token based (something the individual possesses), and biometric based authentication (something the individual is). Each of them has its own vulnerabilities [3]. A password can be guessed or stolen by an imposter. Similarly, a token can be duplicated or stolen. Biometric information, such as voice, face, iris, retina, and finger print, can be recorded or photographed. Recently, EEG (Electroencephalography) signal emerges as a potential biometric modality with advantages of difficult (close to impossible) to fake, impossible to observe or intercept, unique, un-intrusive, and alive [7]. An EEG signal is a measurement of the electrical field which is generated when neurons are activated. There are a lot of studies on EEG based biometric recognition including person identification and person verification by

M. Lee et al. (Eds.): ICONIP 2013, Part II, LNCS 8227, pp. 562–569, 2013.

applying machine learning [2, 6, 8, 11-13, 15-17, 18, 21]. The purpose of study so far is mainly on person recognition [5]. Although person recognition is related to authentication, the focus is different. An authentication system requires accuracy and stability, minimum risk of being faked or information disclosure, nonintrusive, easy to implement and operate, and having different credentials for different levels of security. In addition, the same person may want to set different levels of "EEG password" to the systems of different levels of security. EEG can have all those characteristics. The experimental results of these studies are very high at true positive rate that means the existing of repeatable and stable brainwave patterns correspond to mental tasks is potential. Inspired by these results, in this paper we study the feasibility of an EEG based authentication system.

The rest of the paper is organized as follows. We first introduce EEG and the application of machine learning in processing signals in Section 2. Section 3 presents using EEG for person recognition. In Section 4 and Section 5, we highlight the drawbacks of conventional types of authentication, and study the feasible to use EEG for authentication. Experiments and results are presented in Section 6. We conclude the paper with a discussion and our future work in Section 7.

2 EEG and Its Applications

An EEG signal is a measurement of the electrical field which is generated when neurons are activated [19]. EEG signals contain the information about brain activities, and they are usually recorded by placing electrodes on the scalp of a person. In this paper, we concern only human EEG.

EEG signals are divided into five major bands, delta (0.5-3 Hz), theta (4-7 Hz), alpha (8-13 Hz), beta (14-30 Hz), and gamma (>30 Hz). Delta waves are mainly associated with deep sleep and may also be observed in a waking state while theta waves are associated with creative inspiration and deep meditation. Alpha waves are the most popular in the brain activities. They appear in both relaxed awareness without attention and with concentration. Beta waves are the usual waking rhythms in the brain associated with active thinking, active attention, or solving problems. Gamma waves usually have low amplitudes, rare occurrence, and relate to left index finger, right toes, and tongue movement [19].

EEG signals have been playing an important role in health and medical applications. Epileptic seizure detection is one of the most well-known applications. Another common usage of EEG signal in health is the study of sleep disorders. In additional, the relations between EEG signals and brain diseases have been investigated [19].

Recording EEG signals is non-invasive with a portable device; therefore, EEG is widely used in Brain Computer Interface (BCI) which can provide a link between the human subject and the computer without physical contact [19]. Affective computing is also an attractive area with many researchers trying to understand the states of human minds, emotion etc. [20]. In addition, EEG is used to reveal concealed information for forensics, for example, lie detection [4].

In recent years, researchers start to establish the fact that brain-wave patterns are unique to every individual, and thus EEG signals can be used in biometrics [8].

3 Using EEG for Person Recognition

Machine learning is a branch of computer science, artificial intelligent, and pattern recognition. It has been found wide application in processing EEG signals particular in BCI [19] and also EEG-based person identification. An EEG-based person recognition system usually has two phases training and testing. There are two main components in the each of the phases feature selection and classification. First of all, the biometric information of a user is acquired from his or her brainwave signals. Next, in the training phase, EEG data pre-processing is conducted to reduce noise. Afterwards, features are extracted by a feature selection algorithm to select only useful features. Finally, these extracted feature vectors are used to train a classifier to build a model of the EEG signal patterns of the person. In the testing phase, the same feature extraction algorithm processes EEG signals of a person, and those features are compared to the models created during the training phase.

A variety of models have been used for person recognition purpose. Linear support vector machine with cross validation was employed for the classification in [2]. Neural network with spectral features was used in [16]. In [8], a Gaussian mixture model with maximum a posteriori adaptation was applied for person verification. AR (Auto Regression) coefficients with PCA (Principle Component Analysis) were used in [15]. Fisher's Linear Discriminant (FLD) was first deployed in [21] to reduce the dimensions of AR and power spectrum density (PSD) feature vectors, and then a k-Nearest Neighbours (kNN) classifier was applied.

Some more studies in applying machine learning algorithms for EEG based recognition can be found in [6, 11, 12]. Multi-sphere Support vector data description (MSSVDD) is used in [11]. MSSVDD is also used with universal background model (UBM) in [12]. In [6], J.Hu tried to analysis EEG signals for person authentication based on an ARMA (Auto-Regressive and Moving Average) model.

All this research work is concentrating on person recognition. We will review authentication in next section again, very briefly here.

4 A Review on Authentication Systems

Authentication is the foundation of any security system, in which a person is verified to be timely who he or she claims. There are 3 means of authentication: (i) something a person knows, for example, password and PIN (personal identity number), (ii) something a person has, for example, physical keys, smart cards etc., and (iii) something a person is and does – so called biometric authentication, such as voice recognition, fingerprints matching, and iris scanning etc. [9].

Authentication by something a person knows, also known as password based authentication, is the most popular authentic mechanism, where a user has to provide not only ID but also a password [3]. The system is simple, accurate, and effective. It will continue to be the working horse for authentication for many years to come [9]. However, password based authentication is not immune from malicious attacks. The popular ones are offline dictionary attack, popular password attack, exploiting user mistakes, and exploiting multiple password use [3]. The dilemma now is that with ever increasing computer power, which can crack even longer password with shorter time, the memorability of human brain or the length password stays the same. Therefore, a feasibility alternative is extreme desirable.

Authentication by something a person has, also known as token based authentication, is an authentic mechanism that bases on objects a user possesses such as a bank card, a memory card, a smart card, and a USB Dongle [3]. This kind of authentication requires users always bringing and providing tokens when accessing the system. Presenting a token, which is not a part of a human body, can cause inconvenient. Another inconvenient of token based authentication is that all the tokens require special reader. In additional, tokens can be physically stolen, be duplicated, as well as be hacked by engineering techniques [3]. Securing the tokens is itself a challenge.

Authentication by something a person is and does, also known as biometric based authentication, tries to authenticate users based on their biometric characteristics. User characteristics can be divided into two classes including physiological characteristics such as fingerprint, face recognition, print, hand geometry, and iris recognition, and behavioral characteristics, such as hand writing, and voice etc. [3, 18]. Although biometric authentication can avoid some disadvantages of password based and token based authentication, the conventional biometrics modalities have some security disadvantages. Face, fingerprint, and iris information can be photographed. Voice could be recorded, and hand writing may be mimicked [5, 10]. Moreover, individuals can be lost or changed their biometric characteristics such as finger or face. These disadvantages require a better biometric modality for security systems.

5 Using EEG for Authentication Purpose

While the conventional types of authentication have their own shortcomings as above, EEG emerges as a potential modality for authentication because of following advantages, yet without shortcomings of the conventional types:

1. EEG is confidential because it corresponds to a mental task;
2. It is very difficult to mimic because similar mental tasks are person dependent;
3. It is almost impossible to steal because the brain activity is sensitive to the stress and the mood of the person, an aggressor cannot force the person to reproduce his or her mental pass-phrase [8]; and
4. EEG exists in every person and requires the alive person recording [1].

Therefore, we propose an authentication system using EEG signals. The system can be regarded as authentication by something a person thinks. An EEG based authentication system has two phases: enrollment and verification. In the enrollment phase, a person is asked to do some tasks, for example imagining moving a hand, a foot, a finger or the tongue, and EEG signals are recorded. For authentication purpose, which is different from person recognition purpose, the imagery tasks themselves are also a part of the credential and could not be seen by a third party. The number of tasks can be flexible and depends on the security of the system. After collecting the data, the EEG signals of each task corresponding to the user are pre-processed, extracted features, and are used to train and build the model which is kept securely in a database.

In the verification phase, when a user wants to access the system, he or she has to provide EEG signals by repeating the tasks which he/she did in the enrolment phase. These input EEG data are processed the same as in the enrolment. The obtained vector features are then fed into the classifier as testing data to match the model of the individual who he or she claims to be.

The number of tasks need to repeat depends on the requirement of the security policy. It can be just a single match or multi-match policy. A single match means the user can perform a few tasks while the verification is done by, and at least one task is matched. On the other hand, multi-match requires the EEG patterns of more than one tasks are matched for the person to be authenticated.

To use EEG for authentication purpose, EEG patterns of an individual have to be repeatable and stable on the one hand, and distinguishable from an individual to another. In this section, we study the feasibility of using EEG for authentication purpose, i.e., if EEG signals indeed have aforementioned characteristics. From the research that has been done so far on person recognition, stable patterns are feasible with motor imagination, and motor imagination is repeatable [12-14].

Therefore, we can confident that EEG patterns are stable enough for person recognition. However, more is needed to use EEG for authentication purpose than just simple person recognition. EEG based authentication system uses EEG based "password" that is the combination of personal characteristics of EEG patterns and secret task performed as seen in Table 2. The analogy can be seen in the voice based authentication system where a person can be identified from the voice, but only specific voice phrases can be used as "password", e.g., saying a special sequence of words.

6 Experiments and Results

6.1 Data Set

The Graz dataset B in the BCI Competition 2008 comes from the Department of Medical Informatics, Institute of Biomedical Engineering, Graz University of Technology for motor imagery classification problem in BCI Competition 2008 [7]. The Graz B 2008 dataset consists of EEG data from 9 subjects. The subjects were right-handed, had normal or corrected-to-normal vision and were paid for participating in the experiments. The subjects participated in two sessions contain training data without feedback (screening), and three sessions were recorded with feedback. It consisted of two classes: the motor imagery (MI) of left hand and right hand. Three bipolar recordings (C3, Cz, and C4) were recorded at sampling frequency of 250 Hz.

6.2 Feature Extraction

The signals from electrodes C3, C4, Cz were selected to extract features. The autoregressive (AR) linear parameters and power spectral density (PSD) components from these signals are extracted as features. In details, the power spectral density (PSD) in the band 8-30 Hz was estimated. The Welch's averaged modified periodogram method was used for spectral estimation. Hamming window was 1 second 50% overlap. 12 power components in the frequency band 8-30 Hz were extracted.

Besides PSD features, autoregressive (AR) model parameters were extracted. In AR model, each sample is considered linearly related with a number of its previous samples. The AR model has the advantage of low complexity and has been used for person identification and authentication [16] [17]. Burg's lattice-based method was used with the AR model order 21, as a previous study [16] suggested when there were many subjects and epochs. The resulting feature set consists of 3*(12+21) = 99 features.

6.3 Results

The Support Vector Data Description (SVDD) method was used to train person EEG models. Experiments were conducted using 5-fold cross validation training and the best parameters found were used to train models on the whole training set and test on a separate test set. The RBF kernel function $K(x - x') = e^{-\gamma||x-x'||^2}$ was used. The parameters for SVDD training are γ and ν. The parameter γ was searched in $\{2^k$: $k = 2l + 1$, $l = -8, -7, \ldots, 2\}$. The parameter ν was searched in {0.001, 0.01, 0.1}. The best parameters found are $\nu = 0.1$, $\gamma = 2^{-3}$ for left and right hand motor imagery for each subject.

Table 1. Dataset description

Dataset	#subjects	#tasks	#trials	#sessions	Length(secs)
Graz 2008 B	9	2	120	5	7.5

Table 2. Recognition rates of 9 subjects B01-B09 using the left and right motor imagery tasks

Task Subject	Left hand (L)	Right hand (R)	(L ∨ R)	(L ∧ R)
B01	95.3%	95.3%	99.8%	90.8%
B02	95.0%	96.3%	99.8%	91.5%
B03	96.9%	98.9%	99.9%	95.8%
B04	90.9%	92.6%	99.3%	84.2%
B05	83.0%	93.8%	98.9%	77.9%
B06	91.4%	95.9%	99.6%	87.7%
B07	94.7%	93.1%	99.6%	88.2%
B08	92.5%	93.2%	99.5%	86.3%
B09	92.6%	99.8%	99.9%	92.4%

Due to the levels of security system, tasks matched can be any of a few, e.g. $(T_1 \vee T_2 \vee T_3)$, or all of them in the right order, e.g. $(T_1 \wedge T_2 \wedge T_3)$. Let T_1 and T_2 be the events of correct classification of Task 1 and Task 2, respectively, we will have the probability of successfully classifying at least one of the tasks as $P(T_1 \vee T_2) = P(T_1) + P(T_2) - P(T_1 \vee T_2)$.

Two designated motor imagery tasks were to cue left hand and right hand as seen in Table 1. If the system is more important, all sequence tasks must be matched, so with 2 tasks T_1 and T_2 the probability of successful access will be $P(T_1 \vee T_2) = P(T_1) * P(T_2)$. Table 2 summarizes the two figures $P(L \vee R)$ and $P(L \wedge R)$ for 9 subjects for authentication with tasks.

Table 2 shows that the probability of successful access is very high when the single match policy is applied with only two tasks ($L \vee R$). It is also seen that security is considerable strengthened when the authentication system applies the multiple match policy ($L \wedge R$).

7 Discussion and Future Work

Using EEG signals for authentication has the advantages of both password based and biometric based authentications, yet without their drawbacks. Firstly, EEG signals are biometric information of individuals, and have the advantages of biometric based authentication, yet EEG based authentication can overcome the disadvantages of conventional biometric based authentication.

On the other hand, EEG based authentication brain patterns correspond to particular mental tasks, and they are considered as passwords. As the result, EEG based authentication has all the benefits of password based authentication, yet without the vulnerabilities.

Moreover, security systems may have a multiple security levels with EEG based authentication because it can be adjusted by the number of matched tasks. If a system is of a lower security level, an individual can perform a few tasks, and the system only requires that at least one task is matched. If a system is of a high security level, all tasks in the sequence also in the right order must be matched, so it helps to strength the security system.

Using EEG for authentication purpose is feasible, and also desirable. In the near future, we will investigate the EEG based authentication on a large dataset. The impact of different individuals performing the same task and the same single person performing different tasks will also be studied. Repeatable and stable EEG patterns also remind us a research direction in which EEG based biometric is combined with cryptography effectively for information security applications, and we will study the possibility of using the task sequence as the key for encryption.

References

1. Allison, B.: Trends in BCI research: progress today, backlash tomorrow? The ACM Magazine for Students 18, 18–22 (2011)
2. Ashby, C., Bhatia, A., Tenore, F., Vogelstein, J.: Low-cost electroencephalogram (EEG) based authentication. In: 2011 5th International IEEE/EMBS Conference on Neural Engineering (NER), pp. 442–445 (2011)
3. Brown, L.: Computer Security: Principles and Practice. William Stallings (2008)

4. Grubin, C., Madsen, L.: Lie detection and the polygraph: A historical review. The Journal of Forensic Psychiatry & Psychology 16, 357–369 (2005)
5. He, C., Chen, H., Wang, Z.: Hashing the MAR Coefficients From EEG Data For Person Authentication. In: IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2009, pp. 1445–1448 (2009)
6. Hu, J.: Biometric System based on EEG Signals by feature combination. In: 2010 International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), pp. 752–755 (2010)
7. Leeb, R., Brunner, C., Muller-Putz, G., Schlogl, A., Pfurtscheller, G.: BCI Competition 2008 - Graz data set B, `http://www.bbci.de/competition/iv/`
8. Marcel, S., Millán, J.R.: Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(2007), 743–752 (2007)
9. Ma, W., Campell, J., Tran, D., Kleeman, D.: Password Entropy and Password Quality. In: 2010 4th International Conference on Network and System Security (NSS), pp. 583–587 (2010)
10. Matyáš, V., Řiha, Z.: Security of biometric authentication systems. In: 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM), pp. 18–28 (2010)
11. Nguyen, P., Tran, D., Le, T., Hoang, T.: Multi-sphere support vector data description for brain-computer interface. In: 2012 Fourth International Conference on Communications and Electronics (ICCE), pp. 318–321 (2012)
12. Nguyen, P., Tran, D., Le, T., Huang, X., Ma, W.: EEG-Based Person Verification Using Multi-Sphere SVDD and UBM. In: 17th Pacific-Asia Conference, pp. 289–300 (2013)
13. Nguyen, P., Tran, D., Huang, X., Sharma, D.: A Proposed Feature Extraction Method for EEG-based Person Identification. In: The International Conference on Artificial Intelligence (ICAI 2012), USA (2012)
14. Nguyen, P., Tran, D., Huang, X., Ma, W.: Motor Imagery EEG based Person Verification. In: Rojas, I., Joya, G., Cabestany, J. (eds.) IWANN 2013, Part II. LNCS, vol. 7903, pp. 430–438. Springer, Heidelberg (2013)
15. Palaniappan, R.: Two-stage biometric authentication method using thought activity brain waves. International Journal of Neural Systems 18 (2008)
16. Poulos, M., Rangoussi, M., Alexandris, N.: Neural network based person identification using EEG features. In: Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing ICASSP 1999, pp. 1117–1120 (1999)
17. Poulos, M., Rangoussi, M., Alexandris, N., Evangelou, A.: Person identification from the EEG using nonlinear signal classification. Methods of Information in Medicine 41(1), 64–75 (2002)
18. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security (2011)
19. Sanei, S., Chambers, J.: EEG signal processing. Wiley-Interscience (2007)
20. Schaaff, K., Schult, S.: Towards emotion recognition from lectroencephalographic signals. In: 3rd International Conference on Affective Computing and Intelligent Interaction and Workshops, ACII 2009, pp. 1–6 (2009)
21. Yazdani, A., Roodaki, A., Rezatofighi, S.H., Misaghian, K., Setarehdan, S.K.: Fisher linear discriminant based person identification using visual evoked potentials. In: 9th International Conference on Signal Processing, ICSP 2008, pp. 1677–1680 (2008)