タイトル Title	On-Demand Biometric Authentication of Computer Users Using Brain Waves
著者 Auther(s)	Nakanishi, Isao; Miyamoto, Chisei
掲載誌・巻号・ページ Citation	Networked Digital Technologies. NDT 2010. Communications in Computer and Information Science , 87 : 504 - 510
刊行日 Issue Date	2010-07
資源タイプ Resource Type	会議資料 / Conference Paper
版区分 Resource Version	著者版 / Author
権利 Rights	© Springer-Verlag Berlin Heidelberg 2010
DOI	10.1007/978-3-642-14292-5_51
URL	http://repository.lib.tottori-u.ac.jp/6285

On-Demand Biometric Authentication of Computer Users Using Brain Waves

Isao Nakanishi[1] and Chisei Miyamoto[1*]

Graduate School of Engineering, Tottori University
4-101 Koyama-minami, Tottori, 680-8552 Japan
nakanishi@ele.tottori-u.ac.jp

Abstract. From the viewpoint of user management, on-demand biometric authentication is effective for achieving high-security. In such a case, unconscious biometrics is needed and we have studied to use a brain wave (Electroencephalogram: EEG). In this paper, we examine the performance of verification based on the EEG during a mental task. In particular, assuming the verification of computer users, we adopt the mental task where users are thinking of the contents of documents. From experimental results using 20 subjects, it is confirmed that the verification using the EEG is applicable even when the users are doing the mental task.

1 Introduction

In networked society, non-face-to-face communications are performed through computer networks; therefore, it is quite important to verify identity. For such a person authentication method, magnet cards, IC cards, or passwords have been used but the cards have forgery or robbery concerns, and the password tends to be forgotten. Consequently, the person authentication using biometrics gains public attention.

Among biometric modalities, a fingerprint and an iris achieve higher performance and are already used in consumer security systems. However, it has been reported that the authentication systems using them were circumvented by fake fingers or printed iris images [1, 2]. The reason is that the fingerprint and iris are revealed on the body surface.

Veins are kept in the body; therefore, it is expected to have tolerability to the circumvention. However, it is also reported that even the authentication system using the vein accepted artifacts in enrollment and verification [3]. This is due to lack of the function of liveness detection which examines whether an object is a part of a living body. The liveness detection scheme is necessary for protecting biometric authentication systems from spoofing using artifacts.

On the other hand, conventional biometrics systems mainly assume the applications based on one-time-only authentication such as access control, banking, passport control, and so on. However, from the viewpoint of user management,

* Presently at the NEC Corporation, Tokyo, Japan

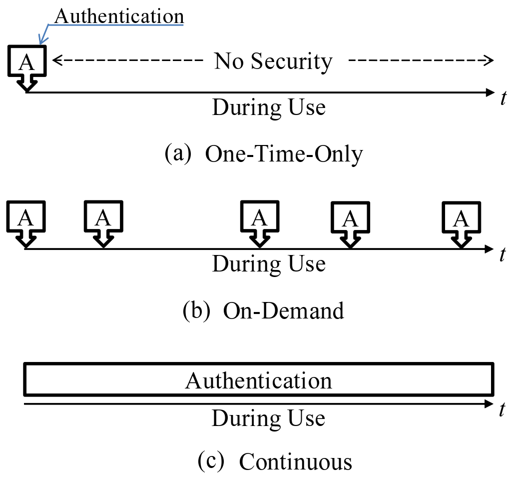

Fig. 1. Styles of authentication

the one-time-only authentication is low-security. After authenticating by a genuine user, even if he/she is switched to an imposter, the one-time-only authentication system could not detect such spoofing. In order to cope with this problem, some other style of authentication is needed.

Figure 1 shows conceivable styles of authentication where (a), (b) and (c) are one-time-only, on-demand and continuous authentication, respectively. The term: "continuous" was used in [4] and the continuous authentication was realized by using multimodal biometrics. However, the continuous authentication cannot be realized by using a single biometric modality unless it adopts optical processing.

Instead, we define "on-demand" authentication as a new style. In the on-demand authentication, users are verified on a regular or nonregular schedule on demand of authentication from the systems.

By the way, the fingerprint and the iris are not suitable for the on-demand authentication because they ask users to present their biometric data every authenticating. In other words, the on-demand authentication needs unconscious biometrics. As the unconscious biometrics, a face, ear, voice, keystroke and gate are applicable but the face and the ear are easily imitated using artifacts and the voice, keystroke and gate limit applications.

It has been proposed to use a brain wave as the biometrics [5]-[11]. We have also studied the authentication using the brain wave [12]. The brain wave is generated by the activities of neurons in the cerebral cortex; therefore, it is kept in the body and so it is effective for anti-circumvention. Of course, the brain wave possesses the function of liveness detection because it is generated only by live human beings. Moreover, the brain wave is generated autonomously and unconsciously; therefore, it enables the on-demand authentication. Conversely,

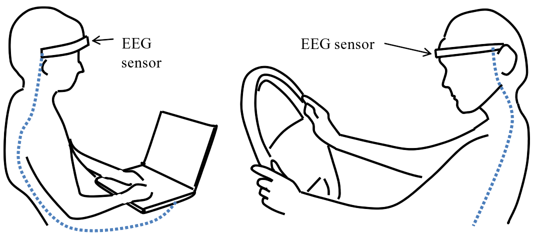

Fig. 2. Authentication of operators using brain waves

since users are required to put sensors on their scalp every authentication under present technologies, the brain wave is not suitable for the one-time-only authentication. It will be solved if contactless sensors for detecting brain waves are invented in the future.

Considering these facts, we assume operator verification of systems such as computers and vehicles as shown in Fig.2. The operators wear brain wave sensors and they are verified on demand while using the systems. For example, in the remote education system students should be authenticated while learning. It is even more so for the students who are trying to obtain some academic degree or public qualification. Also, operators of public transportation systems should be authenticated while operating since thousands of human lives depend on them. There are other examples: pilots of aircrafts, drivers of emergency vehicles, operators of military weapons and so on. Additionally, if the detection of catnapped and/or drunkard operators using the brain wave is possible, it is expected to be integrated with the operator's on-demand authentication and will be valuable protection against having accidents.

However, it is not easy to implement the proposed on-demand authentication in a single step. We must consider step by step which band of the brain wave we use and how we reduce the noise in the brain wave caused by the eye-blink. We have already confirmed the verification performance using the α band in the case where users are relaxed in eye-closed condition [12]. This is the first step. However, such a condition is not appropriate for practical applications. As the second step, we assume that users are not relaxed but concentrating on some mental task with closed eyes. At the final step, we will assume eye-opened users while doing some mental task. If the effectiveness of the authentication using brain waves is confirmed, we will build up the on-demand system using the proposed authentication method.

This paper is at a point of the second step. We assume to construct an authentication system of which user has the authority to use his/her own personal computer; therefore, not the identification (one-to-many matching) but the verification (one-to-one matching) is assumed. Also, we adopt a mental task in which the user is mentally making sentences. Through experiments, we confirm that the authentication using the brain wave is possible even during the mental task.

2 Verification Using EEG in Mental Task

2.1 Brain Wave

Electrical changes from large number of synapses (neurons) in the cerebral cortex are accumulated and then detected as a brain wave (Electroencephalogram: EEG)@on scalp using an electrode. Because of spatiotemporal dispersiveness of neurons, there are not distinct patterns in the EEG in general. However, when the activity of the cerebral cortex becomes low, brain waves partially become synchronous and thereby some distinctive wave is observed. As such waves, δ (0.5-3Hz), θ (4-7Hz), α (8-13Hz), and β (14-30Hz) are well known and detectable when human beings are during deep sleep, getting sleepy, relaxed with closed eyes, and in some mental activity, respectively. In particular, the α and/or β waves are applicable for the person authentication.

2.2 Mental Task

Several authentication methods using the EEG in mental activities have been proposed [13]-[15]. The mental tasks are, however, invented from a viewpoint of brain sciences: mental arithmetic, mental rotation of a three-dimensional block and so on. In the case of on-demand authentication, if actual tasks (works) are different from mental ones, users are required to perform the mental task every authentication and thereby it makes the authentication conscious. The mental task should be related with the actual one for keeping the authentication unconscious.

In this paper, we assume the authentication of computer users who are making sentences mentally. For convenience, we call this task mental composition hereafter. The mental composition is a supposable task for the computer users; therefore, it enables unconscious authentication.

2.3 Feature Extraction

We have confirmed that the spectral distribution in the α band is an important feature for distinguishing individuals [12]. It is, however, known that when some mental activity is being done, the α wave is suppressed while the β wave becomes detectable. In this paper, we add a spectral feature in the β band to the conventional ones.

Spectral Smoothing. Since the EEG spectrum has large intra-individual variation, all spectral data for feature extraction are pre-processed by smoothing. Concretely, by using spectral values at five adjacent frequency bins, we obtain an averaged spectral value

$$|X_k| = \frac{1}{5} \sum_{n=-2}^{2} |X_{k-n}| \qquad (1)$$

where k is a frequency index and X_k is a discrete Fourier transform (DFT) of an EEG signal.

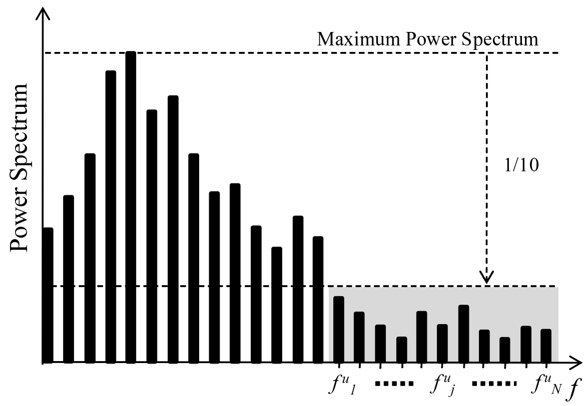

Fig. 3. Definition of the concavity of spectral distribution

Feature Extraction in α Band. In the α band, we have utilized two spectral features [12]. The one is spectral variance and the other is the concavity of spectral distribution.

Assuming the spectrum in the α band is normally-distributed, its spectral variance is calculated by

$$v = \frac{1}{T}\sum_{k=1}^{T}(s_k - \bar{s})^2 \tag{2}$$

where T is the number of frequency bins in the α band. s_k $(k = 1, 2, \cdots, T)$ are power spectral values and $\bar{s}$ is their mean one.

The definition of the concavity of spectral distribution is shown in Fig. 3. First, the maximum value of the power spectrum is detected and then its tenth part is calculated and adopted as a criterion. Next, frequencies of which power spectral values are under the criterion are squared and then summed as

$$F_u = \sum_{j=1}^{N}(f_j^u)^2 \tag{3}$$

where $f_j^u(j = 1, 2, \cdots, N)$ is frequencies under the criterion. F_u is regarded as a feature representing the concavity of spectral distribution.

Feature Extraction in β Band. The spectrum in the β band is relatively uniformly-distributed and thus the features described above are undetectable in the β band. In this paper, we propose to use the difference between the spectrum in relaxed condition and that during mental composition as the feature in the β band.

First, the spectrum in the β band is measured L times in the relaxed condition and then their ensemble mean $\overline{\beta_k^l}$ is found at each frequency bin. Next, the

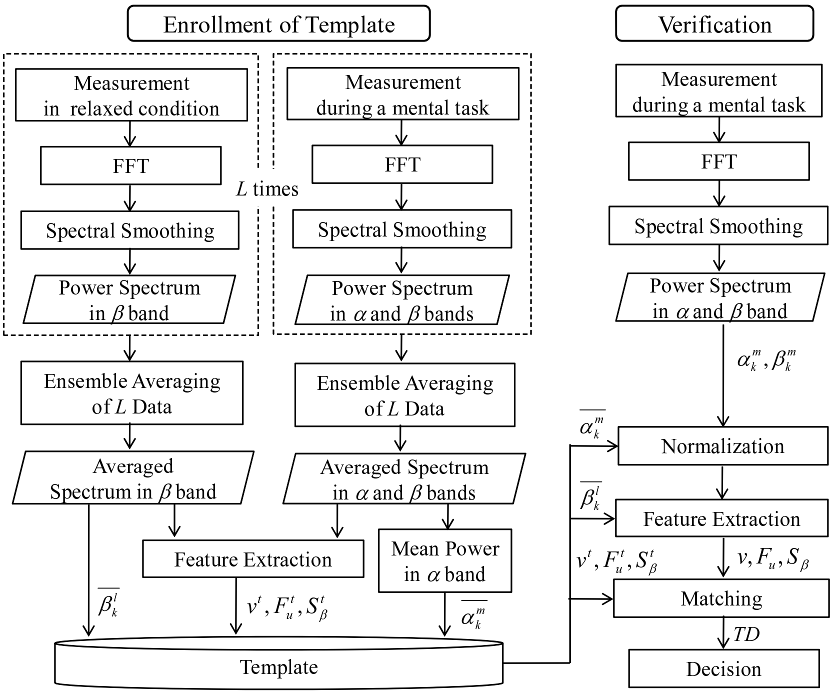

Fig. 4. Block diagram of the proposed verification system

spectrum in the β band during the mental composition is also measured as β_k^m and then the Euclidean distance from the mean value of the spectrum in the relaxed condition is calculated and all distances are accumulated as a feature.

$$S_\beta = \sqrt{\sum_{k=1}^{N} (\beta_k^m - \overline{\beta_k^l})} \tag{4}$$

where N is the number of frequency bins in the β band.

2.4 Verification

The block diagram of the proposed verification system is described in Fig. 4. The details of each block are explained in the following sub-sections.

Enrollment of Template. In advance of the verification stage, spectral features of all users are enrolled as templates. The EEG of each user is measured in relaxed condition and then its power spectrum in the β band is calculated by Fast Fourier transform (FFT). After that, the spectral smoothing described in Sect. 2.3 is performed. These processes are repeated L times and then the ensemble mean of L spectra in the β band is found as $\overline{\beta_k^l}$ and it is stored as a template.

In the same way as the relaxed condition, the spectrum during the mental composition is measured L times and then ensemble mean values of L spectra in both α and β bands are respectively found as $\overline{\alpha_k^m}$ and $\overline{\beta_k^m}$.

In the averaged spectrum $\overline{\alpha_k^m}(k = 1, 2, \cdots, M)$ where M is the number of frequency bins in the α band, the spectral variance and the concavity of spectral distribution are extracted as features and registered as templates: v^t and F_u^t, respectively. Also, the mean value of the averaged power spectrum in the α band is stored simultaneously. This is used for the normalization described later.

The template in the β band is given by

$$S_\beta^t = \sqrt{\sum_{k=1}^{N}(\overline{\beta_k^m} - \overline{\beta_k^l})} \tag{5}$$

Normalization and Matching. In the verification stage, each user declares who oneself is by giving his/her name or ID number to the system, which specifies his/her template. And the spectrum of the user during the mental composition is found and then smoothed, and only spectral elements in the α and β bands are used as verification data: α_k^m and β_k^m, respectively.

By the way, the features in the α band are based on the absolute amount of the spectrum; therefore, they tend to be influenced by intra-individual variation. For suppressing such variation, the normalization is performed in advance of the feature extraction. Concretely, the mean value of the $\alpha_k^m(k = 1, 2, \cdots, M)$ is calculated and then the α_k^m is adjusted (normalized) so that the mean value may become equal to that of the template: $\overline{\alpha_k^m}$ stored in the system.

After that, the features in the α and β bands: the spectral variance, the concavity of spectral distribution and the spectral distance are extracted as v, F_u and S_β, respectively. The difference between the extracted features and their templates are calculated and then normalized because they have deferent dimensions. Total distance (TD) is given by

$$TD = x \cdot |v - v^t| + y \cdot |F_u - F_u^t| + z \cdot |S_\beta - S_\beta^t| \tag{6}$$

where x, y and z are coefficients for combining features and $x + y + z = 1$. If TD is less than a threshold which is preliminary determined, the user (declarer) is regarded as a normal user. If not so, he/she is rejected as an imposter.

3 Experiments

In order to examine the verification performance of the proposed method, we carried out experiments.

3.1 Conditions

The number of subjects was 20. All were healthy male around twenty and seated at rest with closed eyes in a silent room.

In advance of launching measurements, we presented the subjects five themes: a letter for parents, a self-introduction, hometown PR, memories of college life, and a brief description of own researches.

While measuring, they were required to make sentences about these themes mentally. The EEG signals were recorded using a consumer single-channel electroencephalograph during continuous one minute. By using a headband, a single electrode (sensor) was set on the frontal region of head which corresponded to the frontal pole (Fp1) defined by the international standard: 10/20 method. 10 EEG signals were obtained from each subject on the same day and 200 EEG signals were obtained in total. The average number L was set to five; therefore, five data of each user were used for generating his/her templates. The rest five data of each subject were used for verification and all other subjects' data were used as those of imposters.

3.2 Results

Verification performance was evaluated by the equal error rate (EER) where the false rejection rate (FRR) was equal with the false acceptance rate (FAR). The EERs in several ratios of coefficients x, y, z for combining features are summarized in Table 1.

Table 1. EERs at various coefficients for combining features

Ratio ($x : y : z$)	EER (%)
0.2 : 0.3 : 0.5	16
0.3 : 0.2 : 0.5	16
0.3 : 0.4 : 0.3	16
0.4 : 0.3 : 0.3	13
0.3 : 0.5 : 0.2	17
0.5 : 0.3 : 0.2	13

From these results, it is confirmed that the EER in the mental composition was about 15 %.

For reference, we also examined the verification performance using only the features of the α wave and thereby obtained the EER of 15%. This suggests that the proposed feature of the β wave was not valid in this experiment.

Moreover, we examined the verification performance during mental arithmetic which is generally used in the brain science. The number of subjects was 10 and they imagined to calculate $7 \times 10,\ 7 \times 11, 7 \times 12, \cdots$ with closed eyes until the end of measurement. The EER was about 11 %. Since the number of subjects is not equal to that in the mental composition, it is not accurate to compare these results but the effect of using the feature of the β wave could be confirmed in the case of mental arithmetic.

The difference between two cases might be due to the degree of mental activity, that is, the content of the mental task. In the mental arithmetic, the contents were clearly defined and they were not relatively easy to perform. On the other hand, in the case of the mental composition some themes were given as rough guidelines but actual contents depended on the subjects. Some subjects might make simple sentences, and others might make difficult ones. These had an influence on the degree of mental activity.

Base on the above discussion, it is supposed that the harder the mental activity became, the better the verification performance became. On the other hand, it was worried that verification performance might be degraded because it is generally known that the mental activity suppresses appearance of the α wave while it makes the β wave detectable. But such degradation was not confirmed in this experiment. As a result, it is concluded that the verification using brain waves is possible even during the mental task.

4 Conclusions

From the viewpoint of user management, one-time-only authentication is low-security; therefore, on-demand authentication is necessary but it requires an unconscious biometrics. We had studied the brain wave (EEG) as a powerful unconscious biometrics. However, in order to apply the authentication using the EEG to practical applications, we had to examine the verification performance during mental tasks. In addition, the mental task should be related with an actual one for keeping the authentication unconscious.

In this paper, assuming the verification of computers users, we adopted mental composition in which the users were mentally making sentences. It was a supposable task for the computer users. Moreover, introducing the mental task required to add a new spectral feature in the β band, that is, the Euclidean distance between the spectrum in the relaxed condition and that during the mental task to conventional ones, that is, spectral variance and the concavity of spectral distribution in the α band. Verification was simply performed by combining the differences between the extracted features and their templates.

In experiments using 20 subjects, the EER of about 15 % was obtained, so that we conclude that the verification using the EEG was possible even during the mental task. In addition, from the comparison with the results in mental arithmetic, it was confirmed that the degree of mental activity had influence on the verification performance.

In this paper, since we cared about the influence of eye-blinks on the EEG, we assumed eye-closed condition. But in our exploratory experiments, we already confirmed that the noise in the EEG caused by the eye-blink did not have great influence on verification performance as long as individual features were extracted from the spectrum of the EEG. The frequency of eye-blink was different from that of the α or β band. We are now examining the proposed authentication method at the final stage where users drive vehicles in eye-opened condition. Results will be available in the near future.

5 Acknowledgement

A part of this work was supported by the Support Center for Advanced Telecommunications Technology Research, Foundation (SCAT) in Japan.

References

1. T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, “Impact of Artificial ”Gummy” Fingers on Fingerprint Systems,” Proc. of SPIE, vol. 4677, pp. 275-289, Jan. 2002.
2. T. Matsumoto, T. Kusuda, J. Shikata, “On the Set of Biometric Test Objects for Security Evaluation of Iris Authentication Systems -Part 2- (in Japanese),” Proc. of the 9th IEICE Technical Report of Biometrics Security Group, pp. 60-67, 2007.
3. T. Matsumoto, “Security Design and Security Measurement for Biometric Systems (in Japanese),” Proc. of the 7th IEICE Technical Report of Biometrics Security Group, pp. 57-64, 2006.
4. A. Altinok and M. Turk, “Temporal Integration for Continuous Multimodal Biometrics,” Proc. of 2003 Workshop on Multimodal User Authentication, pp. 207-214, Dec. 2003.
5. M. Poulos, M. Rangoussi, V. Chrissikopoulos, A. Evangelou, “Person Identification Based on Parametric Processing of the EEG,” Proc. of the 9th IEEE International Conference on Electronics, Circuits and Systems, vol. 1, pp. 283-286, 1999.
6. M. Poulos, M. Rangoussi, and N. Alexandris, “Neural Networks Based Person Identification Using EEG Features,” Proc. of 1999 International Conference on Acoustic Speech and Signal Processing, pp. 1117-1120, 1999.
7. M. Poulos, M. Rangoussi, V. Chissikopoulus, and A. Evangelou, “Parametric Person Identification from the EEG Using Computational Geometry,” Proc. of the 6th IEEE International Conference on Electronics, Circuits and Systems, pp. 1005-1008, 1999.
8. R. B. Paranjape, J. Mahovsky, L. Benedicent, and Z. Koles, “The Electroencephalogram as a Biometric,” Proc. of 2001 Canadian Conference on Electrical and Computer Engineering, vol. 2, pp. 1363-1366, 2001.
9. K. V. R. Ravi and R. Palaniappan, “Recognition Individuals Using Their Brain Patterns,” Proc. of the 3rd International Conference on Information Technology and Applications, 2005.
10. R. Palaniappan, “Identifying Individuality Using Mental Task Based Brain Computer Interface,” Proc. of the 3rd International Conference on Intelligent Sensing and Information Processing, pp. 239-242, 2005.
11. G. Mohammadi, P. Shoushtari, B. M. Ardekani, M. B. Shamsollahi, “Person Identification by Using AR Model for EEG Signals,” Proc. of World Academy of Science, Engineering and Technology, vol. 11, no. 2, pp. 281-285, Feb. 2006.

12. C. Miyamoto, S. Baba, and I. Nakanishi, "Biometric Person Authentication Using New Spectral Features of Electroencephalogram (EEG)," Proc. of 2008 IEEE International Symposium on Intelligent Signal Processing and Communication Systems, pp. 312-315, Dec. 2008.
13. S. Marcel and J. R. Millan, "Pearson Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaption," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 743-748, Apr. 2007.
14. R. Palaniappan and D. P. Mandic, "Biometrics from Brain Electrical Activity: A Machine Learning Approach," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 738-742, Apr. 2007.
15. R. Palaniappan, "Multiple Mental Thought Parametric Classification: A New Approach for Individual Identification," International Journal of Signal Processing, vol. 2, no. 1, pp. 222-225, Sep. 2005.