# Evaluation of Brain Waves as Biometrics for Driver Authentication Using Simplified Driving Simulator

Isao Nakanishi, Sadanao Baba and Shigang Li
*Graduate School of Engineering*
*Tottori University*
*Tottori, Japan*
*Email: nakanishi@ele.tottori-u.ac.jp*

***Abstract*—The brain wave is able to present biometric data unconsciously, so that it enables continuous or on-demand authentication which is effective in user management. In this paper, assuming an application to driver authentication, we evaluate verification performance of the brain wave using a simplified driving simulator. In addition, dividing the $\alpha$-$\beta$ band to several partitions, we propose to extract the difference between a mean value of the power spectrum at each partition in relaxed condition and that in mental-tasked condition as an individual feature. Fusing the differences from higher partitions in verification, the EER of 24% is obtained among 10 subjects.**

***Keywords*-Biometrics, Driver Authentication, Brain Wave, Simplified Driving Simulator**

## I. Introduction

In ubiquitous networked society, non face-to-face communication is necessary, so that the person authentication technique which verifies whether users are genuine or not becomes important. Until now passwords and/or ID cards are used for such a case. But there is a problem that they are at a risk for being forgotten or stolen.

Thus, the person authentication using biometrics attracts attention [1]. As the biometrics, a physical or behavioral characteristic such as the fingerprint, iris, vein, face, ear, voice, signature and keystroke are utilized. They are never forgotten or stolen; therefore, they are effective in usability. However, they assume one-time-only authentication since they are considered as alternatives of the passwords or the ID cards.

On the other hand, from a viewpoint of user management, the one-time-only authentication is low-security. After authentication by a genuine user, even if he/she is switched to an imposter, the one-time-only authentication could not detect such an identity thief.

In order to cope with the problem, continuous or on-demand authentication is needed. Figure 1 shows conceivable styles for authentication, in which it is assumed that the authentication process and the execution of applications are simultaneously performed in a single system.

where (a) is the one-time-only, (b) is the continuous, and (c) is the on-demand authentication.

As mentioned above, in the one-time-only authentication, the authentication is achieved only at the start of using the applications; therefore, the authentication requires the system little load but there is no security after the authentication.

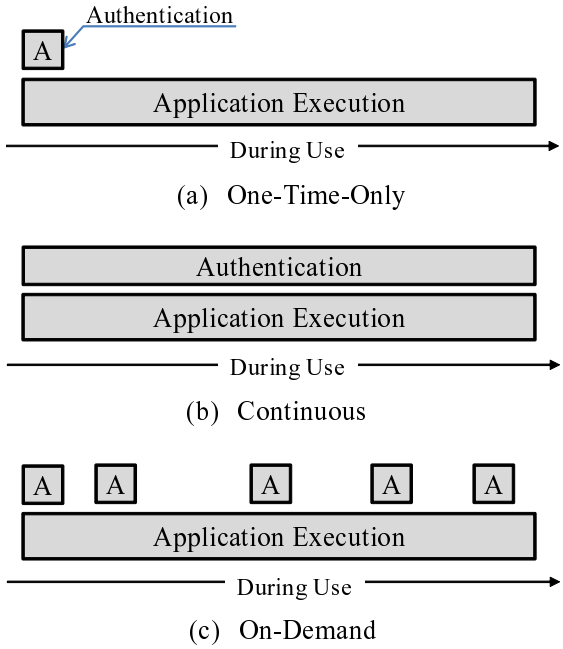


Figure 1. Authentication styles.

On the other hand, the continuous authentication is actively studied [2], [3]. The authentication is always achieved while the applications are being executed; therefore, the security is also guaranteed the while but it brings heavy load on the system. It was reported that the overhead of 42% in computational time was caused in a continuous authentication system [3].

We have proposed the on-demand authentication, where a user is authenticated on a regular or nonregular schedule on demand of authentication from a system [4]. The on-demand authentication does not require the system to authenticate the user at all times, so that it could reduce the load on the system.

However, in the on-demand authentication, the user is required to present biometric data every time the system attempts to authenticate and so it is not inconvenience. Resultingly, unconscious biometrics is needed.

As the unconscious biometrics, the 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.

In fact, conventional biometric modalities mostly have a problem that to make their artifacts is easy so that they are revealed on the body surface. It is well known that consumer authentication systems using the fingerprint were circumvented by fake fingers [5].

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 the artifacts but it also needs additional sensors or systems.

For these reasons mentioned above, we have focused attention on the brain wave as biometrics [6], [4], [7]. The brain wave is generated by the activities of neurons in the cerebral cortex; therefore, it is hidden in the body and so effective for anti-circumvention. If the function of liveness detection is possible by using the brain wave, no additional sensor or system is needed. Moreover, the brain wave is generated autonomously and unconsciously; therefore, it enables the on-demand authentication. The brain wave is the best biometrics on accessibility since it is detectable even if the user has any physical defect.

It has been already studied by other researchers to use the brain wave as biometrics [8]-[17]. However, it is not clear what applications of authentication using the brain wave are. Of course, the brain wave is not suitable for applications based on the one-time-only authentication such as the room entering management and the passport control since users are required to wear sensors every time they are authenticated. Approaches using visual stimuli are very interesting [12], [17] but they are not applicable in unconscious authentication. In order to make the authentication using the brain wave fit for practical use, it is necessary to argue not only the performance but also the utilization style.

We consider that the brain wave as biometrics is the most suitable for the on-demand authentication as previously mentioned. Users are authenticated on demand from a system while using it. Figure 2 shows examples of the utilization style which assume drivers of a public transportation system such as a train, bus, aircraft, ship and so on which involve many human lives, operators of a computer with sensitive information, students in a remote education system which gives them some academic degree or public qualification, and operators of a military weapon.

In this paper, assuming an application to driver authentication, we evaluate verification performance of the brain wave while a user is operating a simplified driving simulator.


Figure 2. Utilization styles of authentication using the brain wave.

If the detection of catnapped and/or drunkard drivers using the brain wave is possible, it is expected to be integrated with the driver's on-demand authentication and will become valuable protection against having accidents.

In this paper, we assume driver authentication as one of applications which need the on-demand authentication and propose simple feature extraction and verification methods of the brain wave and then evaluate them in experiments using a simplified driving simulator.

## II. Verification Using Brain Waves

### A. 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, $\delta$ (0.5-3Hz), $\theta$ (4-7Hz), $\alpha$ (8-13Hz), and $\beta$ (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 $\alpha$ and/or $\beta$ waves are applicable for person authentication.

### B. Feature Extraction and Verification

Most of the conventional approaches used medical-use brain wave sensor systems (electroencephalographs), which required users to set a number of electrodes on their scalp. It was inconvenience when assuming practical applications. In addition, such multichannel measurement increases the amount of processing data, so that it needs heavy computational load. It is also unsuitable for the practical use while it could provide higher authentication accuracy.

For removing the burden of wearing the brain wave sensor and reducing the computational load, we use a consumer-use brain wave sensor system which has only one electrode (single-channel). In addition, we adopt feature extraction and verification methods as simply as possible.

Concretely, dividing $\alpha - \beta$ band into several partitions, the difference between a mean value of the power spectrum in tasked condition and that in relaxed condition at each partition are utilized as an individual feature. Figure 3 shows the case of 4 partitions. The reason why the $\alpha - \beta$ band is divided is that spectral distribution is not a uniform state and depends on an individual; therefore, each partition has different effects on verification Therefore, to find and utilize distinguishable partitions might be effective for the verification.

The block diagram of the proposed verification system is described in Fig. 4. In advance of the verification,

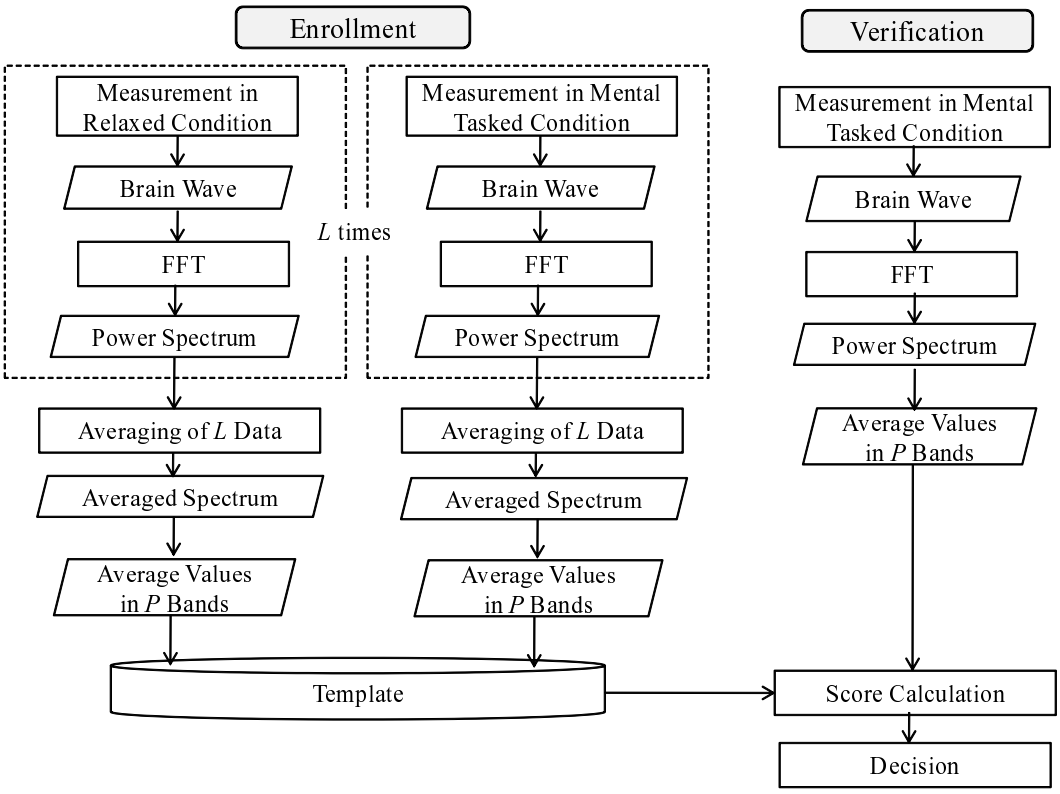


Figure 4. A block diagram of the proposed verification system.

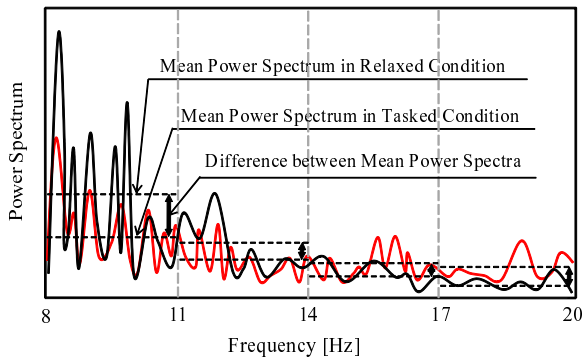


Figure 3. Extraction of Individual features (4 partitions).

the enrollment of templates is performed. The enrollment has two stages. Firstly, an EEG of each user in relaxed condition are measured several ($L$) times and then an ensemble mean value of $L$ power spectra in each partition is calculated. Next, in tasked condition, similar measurements and processing are done and then an ensemble mean value of power spectra in each partition is obtained. The mean values in all partitions in both conditions are stored as templates in the system.

In the verification, an EEG is measured once from a user verified in the tasked condition and the verification score $S$ is calculated by

$$S = \sum_{p=1}^{P} ||s_t^r - s_t^m| - |s_t^r - s^m||_p \quad (1)$$

where $P$ is the number of partitions, $s_t^r$ and $s_t^m$ are templates in the relaxed and tasked conditions, respectively and $s^m$ is a mean value of each partition in the tasked condition at the verification stage.

If $S$ is less than a threshold, the user is authenticated genuine.

## III. Driver Authentication Using a Simplified Driving Simulator

It is fair to measure EEGs of drivers while really driving but it carries risk slightly. There is a way to introduce a special training simulator for driving but it has an issue of cost. Resultingly, we introduce a simplified driving simulator which is mainly composed of gaming machines.

### A. Simplified Driving Simulator

Simulated driving scenes are generated by PlayStation 3 (PS3) as hardware and Gran Turismo 5 Prologue (GT5P) as software produced by Sony Computer Entertainment Inc.. However, the GT5P is for a racing game and so the following settings are applied.

- Set the manual transmission to first gear to limit the maximum speed of a car to 65km/h
- Set the driving course to the urban road in London to drive the car in a general road

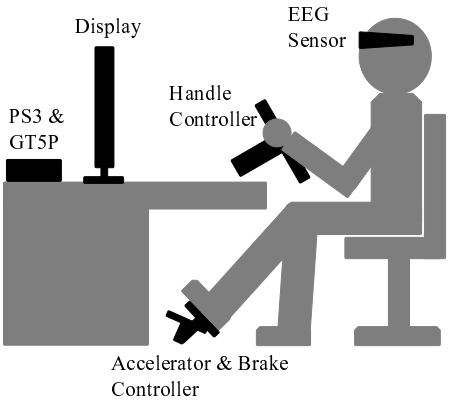


Figure 5. An arrangement plan of the simplified driving simulator.

- Set the racing mode to the time trial, that is, solo drive to avoid accidents with other cars

The driving scenes are displayed on a 24 inch wide-monitor through HDMI, which prevents their image quality from being degraded. A handle, accelerator and brake are equipped by imitated controllers: Driving Force GT produced by Logitech. Figure 5 shows an arrangement plan of the simplified driving simulator.

A measurement scene and a still image of the driving scenes are shown in Fig. 6.

### *B. Measurement of EEGs*

The number of subjects was 10. All were male around 20 years old and each had a driver's license. They wore an EEG sensor and then watched the driving scene and handled the controllers.

The EEG sensor was a consumer single-channel electroencephalograph. By using the 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. The specifications are summarized in Table I.

Table I
SPECIFICATIONS OF THE EEG SENSOR.

| | |
|---|---|
| Frequency Range | 1-24 Hz |
| Minimum Voltage | 5 $\mu V_{p-p}$ |
| Maximum Voltage | 80 $\mu V_{p-p}$ |
| Sampling Frequency | 128 Hz |

Before the measurement, the subjects were required to make two rounds to adapt themselves to maneuvering feeling of the controllers. If there was some accident, for instance, a car hit against a wall, the measurement was redone.

Each measuring time was three minutes. The measurement was carried out twice a day and it was repeated five days and so 10 EEGs were obtained from each subject and 100 EEGs were obtained in total. In addition, for generating templates, five EEGs were obtained from each subject in relaxed condition by measuring once a day for five days.

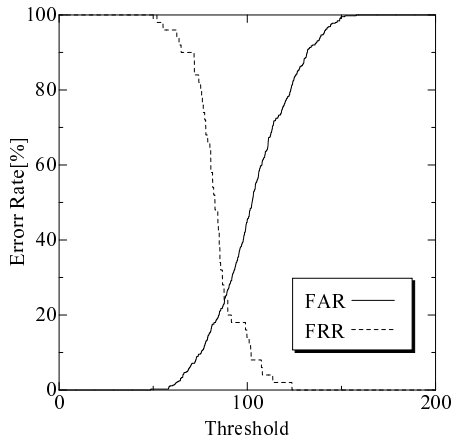


Figure 7. Error curves.

## IV. VERIFICATION EXPERIMENTS AND RESULTS

In verification experiment, we used the data of middle one minute from three minute data measured of each EEG. The average number $L$ was set to five, that is, five EEGs of each subject were used for generating his/her templates. The rest five data of each subject were used for the verification and all other subjects' data were used as imposters ones.

In this paper, the number of partitions was 4, that is, 8-11, 11-14, 14-17 and 17-20 Hz. Verification performance was evaluated by using an equal error rate (EER) at which a false acceptance rate (FAR) was equal with a false rejection rate (FRR). As a result, the EER was 28%.

Next, we evaluated the EER at each partition. The results are summarized in Table II. Comparing these results, the EER at 8-11 Hz is larger than others.

Table II
EER AT EACH PARTITION

| Frequency Band (Hz) | 8-11 | 11-14 | 14-17 | 17-20 |
|---|---|---|---|---|
| EER (%) | 46 | 36 | 36 | 38 |

In this paper, power spectra used in calculating the score were not normalized. The spectrum at the $\alpha$ band is relatively larger than that at the $\beta$ band, so that the difference between the spectrum at the $\alpha$ band in the relaxed condition and that in the tasked condition is larger than that at the $\beta$ band. Resultingly, the large variation might influence on the error rate and degrade the performance.

Finally, excepting the band of 8-11 Hz and fusing scores from remaining three bands, we evaluated the verification performance. Error curves are described in Fig. 7. The EER was 24% and improved by 4%.

This is not high enough to conclude that driver authentication using the brain wave has a practical use but it can be confirmed that there are any possibilities.


(a) A measurement scene

(b) A still image of the driving scenes

Figure 6. Measurement using the simplified driving simulator.

## V. Conclusions

In this paper the brain wave as biometrics was evaluated in the application to driver authentication. While subjects were using a simplified driving simulator, their brain waves were measured. The difference between the power spectrum at the $\alpha - \beta$ band in the relaxed condition and that in the tasked condition was extracted as an individual feature and then verification performance was evaluated. As a result, the EER of 24% was obtained among 10 subjects.

To evaluate the performance using large number of subjects and to adopt more powerful verification method are problems to be overcome. In the future, we would like to develop an on-demand authentication system using the brain wave and evaluate the performance of not only verification but also usability.

## Acknowledgements

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

## References

[1] A. Jain, R. Bolle and S. Pankanti, BIOMETRICS Personal Identification in Networked Society, Kluwer Academic Publishers, Massachusetts, 1999.

[2] A. Altinok and M. Turk, Temporal Integration for Continuous Multimodal Biometrics, Proc. of 2003 Workshop on Multimodal User Authentication, pp. 131-137, Dec. 2003.

[3] G. Kwang, R. H. C. Yap, T. Sim, and R. Ramnath, An Usability Study of Continuous Biometrics Authentication, M. Tistarelli and M. S. Nixon (Eds.): ICB2009, LNCS 5558, Springer, pp. 828-837, 2009.

[4] I. Nakanishi, S. Baba, and C. Miyamoto, On-Demand Biometric Authentication of Computer Users Using Brain Waves, F. Zavoral et al. (Eds.): NDT2010, Part I, CCIS 87, Springer, pp. 504-514, 2010.

[5] 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.

[6] I. Nakanishi, S. Baba, and C. Miyamoto, EEG Based Biometric Authentication Using New Spectral Features, Proc. of 2009 IEEE International Symposium on Intelligent Signal Processing and Communication Systems, pp. 651-654, Dec. 2009.

[7] I. Nakanishi, S. Baba and M. Inoue, Driver Authentication Using Brain Waves While Route Tracing as a Mental Task, Proc. of 2011 International Conference on Security and Cryptography, pp. 90-96, Jul. 2011.

[8] M. Poulos, M. Rangoussi, V. Chrissikopoulos, and 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] G. Mohammadi, P. Shoushtari, B. M. Ardekani, and 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.

[16] 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.

[17] 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.