DRIVER AUTHENTICATION USING BRAIN WAVES WHILE ROUTE TRACING AS A MENTAL TASK

Isao Nakanishi[1] Baba Sadanao[1] and Masahiro Inoue[2]

[1]*Graduate School of Engineering, Tottori University, 4-101 Koyama-minami, Tottori, Japan*
[2]*Faculty of Engineering, Tottori University, 4-101 Koyama-minami, Tottori, Japan*

Keywords: Biometrics, Driver Authentication, Brain Wave, Route Trace, Mental Task.

Abstract: From the viewpoint of user management, continuous or on-demand biometric authentication is effective for achieving higher security. In such a case, the biometrics which is able to present biometric data unconsciously is needed and we have proposed to use the brain wave as the unconscious biometrics. In this paper, assuming driver authentication, we measure brain waves of drivers when they are tracing routes as a mental task. And we evaluate verification performance using the difference between the mean power spectrum at α-β band in relaxed condition and that in mental-tasked condition as an individual feature. As a result, the EER of 31 % is obtained among 12 subjects.

1 INTRODUCTION

For secure networked society, person authentication using biometrics gains public attention. Among biometric traits, the fingerprint and the iris achieve higher performance and are already used in consumer security systems. However, it has been reported that authentication systems using them were circumvented by using fake fingers or printed iris images (Matsumoto et al., 2002; Matsumoto et al., 2007). The reason is that the fingerprint and iris are revealed on body surfaces. The vein is 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 (Matsumoto, 2006). 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 biometric systems mainly assume applications based on one-time-only authentication such as access control, banking, passport control, and so on. However, from the viewpoint of user management, 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.
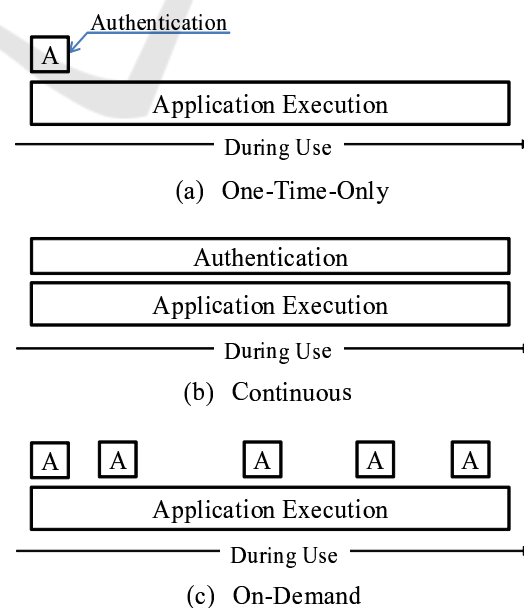

Figure 1: Styles of authentication.

Figure 1 shows conceivable styles of authentication where (a) is the one-time-only authentication. Assuming that both authentication and application execution are simultaneously achieved in a single system, the one-time-only authentication is not a heavy load since the authentication is achieved only once at the start of the application while security is not guaranteed after the authentication.

In order to cope with this problem, continuous authentication is proposed (Altinok and Turk, 2003; Kwang et al., 2009), which is shown as (b) in Fig. 1. The security is guaranteed all the while that the application is executed but the continuous authentication brings a heavy load for the system. In fact, it was reported that overhead of 42% was yielded in a continuous authentication system (Kwang et al., 2009).

On the other hand, we have proposed on-demand authentication, where users are authenticated on a regular or nonregular schedule on demand of authentication from the system (Nakanishi et al., 2010). It is illustrated as (c) in Fig. 1 and makes the system load lighter.

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 continuous or on-demand authentication needs unconscious biometrics. 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.

It has been proposed to use the brain wave as the biometrics (Poulos et al., 1999c; Poulos et al., 1999a; Poulos et al., 1999b; Paranjape et al., 2001; Ravi and Palaniappan, 2005; Palaniappan, 2005b; Mohammadi et al., 2006; Marcel and Millan, 2007; Palaniappan and Mandic, 2007; Singhal and Ramkumar, 2007; Riera et al., 2008). The brain wave is generated by 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, 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[1].

Considering these facts, operator verification of systems such as computers and vehicles are suitable for the authentication using the brain wave as shown in Fig. 2. The operator wears a brain wave sensor and he/she is verified on demand while using the system. For instance, in remote education systems, 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 hundreds of hu-
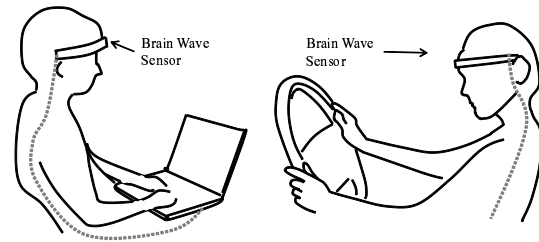

Figure 2: Authentication of operators using the brain wave.

man lives depend on them. There are other examples: pilots of aircrafts, drivers of emergency vehicles, operators of military weapons and so on.

We had confirmed verification performance using the α band in the case where users were relaxed in eye-closed condition (Nakanishi et al., 2009). Also, assuming user authentication of computers, we evaluated the verification performance when users were concentrating on the mental composition with closed eyes (Nakanishi et al., 2010). The mental composition was a mental task in which the user was mentally making sentences. However, these were in eye-closed condition. For applying the authentication using the brain wave in practical environments, it is needed to evaluate verification performance in eye-opened condition.

In this paper, assuming driver authentication, users (drivers) are authenticated by using brain waves while virtual-driving. As a mental task in eye-opened condition, we adopt route tracing in which the drivers verify actual routes with memorized ones.

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 become valuable protection against having accidents.

2 VERIFICATION USING BRAIN WAVES

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 hu-

---

[1]It will be solved if contactless sensors for detecting brain waves are invented in the future.
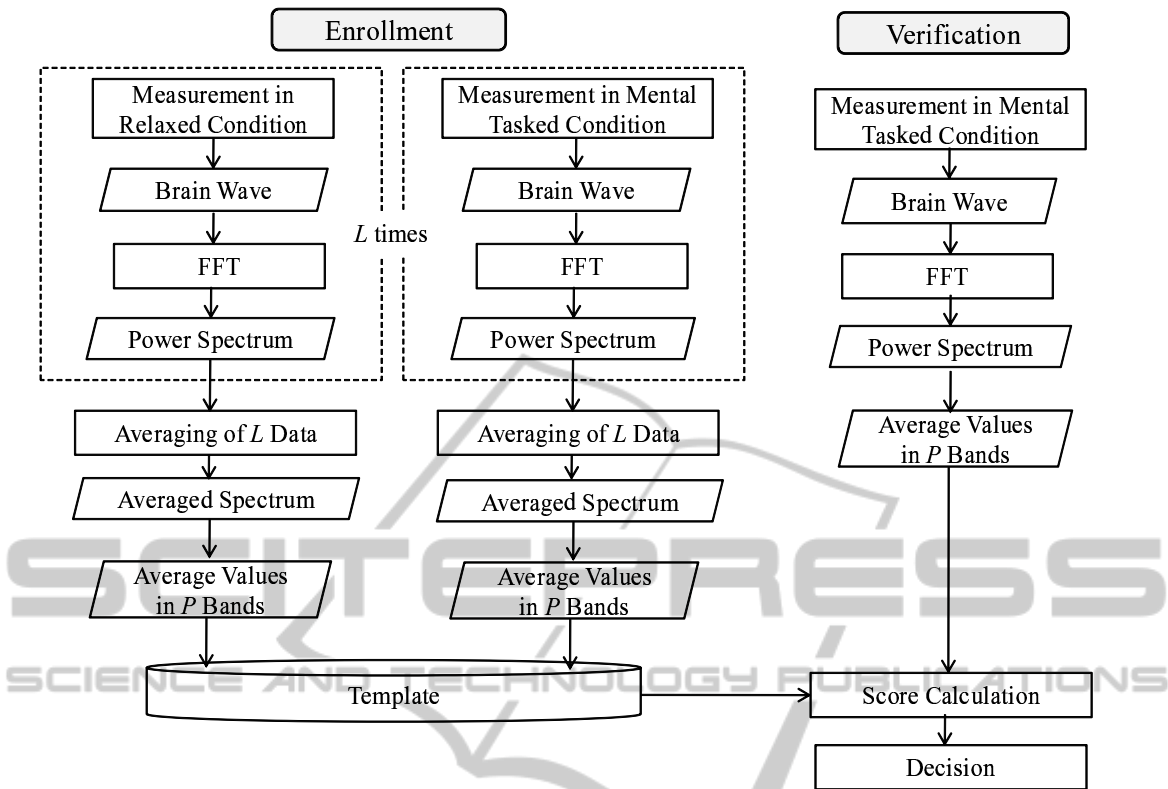
Figure 3: Block diagram of the proposed verification system.

man 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 person authentication.

2.2 Feature Extraction and Verification

In order to actualize the authentication using the EEG, architecture for feature extraction and verification must be as simple as possible.

We have confirmed that the spectral distribution in the α band is an important feature for distinguishing individuals (Nakanishi et al., 2009). It is, however, known that when some mental activity is being done, the α wave is suppressed while the β wave becomes detectable. Also, for verification in mental-tasked condition, we proposed to fuse an individual feature in the β band with those in the α band (Nakanishi et al., 2010).

In this paper, dividing α-β band into several partitions, the difference between a mean value of power spectra in tasked condition and that in relaxed condition at each partition are utilized as an individual feature.

The reason why the α-β band is divided is that the distribution of spectra in the α-β band depends on an individual; therefore, each partition has differ-

ent effect on verification Distribution of spectra at α-β band is not a uniform state. Therefore, to find and utilize distinguishable partitions might be effective for verification.

The block diagram of the proposed verification system is described in Fig. 3. In advance of the verification, the enrollment of templates is performed. The enrollment has two stages. Firstly, EEGs of a user in relaxed and eye-opened condition are measured several (L) times and then an ensemble mean value of L power spectra in each partition is calculated. Next, in mental-tasked condition, similar measurements are done and then each ensemble mean value of power spectra is obtained. The mean values in all partitions are stored as templates in the system.

In the verification, an EEG is measured once in the mental-tasked condition and the verification score S is calculated by

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

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

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

3 DRIVER AUTHENTICATION WHILE ROUTE TRACING

Several authentication methods using the EEG in mental activities have been proposed (Palaniappan, 2005b; Marcel and Millan, 2007; Palaniappan, 2005a). 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 the authentication of computer users, we measured EEGs during a mental task where subjects are making sentences mentally (Nakanishi et al., 2010). This task was called the mental composition. In this paper, we assume authentication of drivers and measure EEGs when subjects are driving.

3.1 Route Trace

Drivers control their cars by processing audio-visual information and then moving four limbs. Additionally, the information processing and the motion are repeated in no time; therefore, it is difficult to extract only the mental task in practical driving. On the other hand, it carries a risk of having some accident in experiments for subjects to drive cars actually. As a result, it is necessary to define what a mental task is with risk-free in driving.

In this paper, we define a new mental task where drivers are checking landmarks in view with their memorized ones. For convenience, we call this task route trace hereafter. The route trace is a supposable task for the drivers; therefore, it enables unconscious authentication.

3.2 Making of Driving Scenes

In order to perform the route trace in a laboratory environment, we prepared driving scenes which were presented to subjects. They were captured by a digital video camera which was put on a dashboard in the forward direction of a car. A still image of the scene is indicated in Fig. 4.

The car was driven to turn at as many intersections as possible in order to give the subjects a heavy mental load in verifying landmarks in view with their memorized ones. Captured scenes are loaded in a computer and scenes with poor visibility and/or out-of-focus are

Figure 4: A driving scene.

eliminated and as a result, we prepared a driving scene of three minutes long.

3.3 Measurement of Brain Waves

The number of subjects was 12. All are male around 20 years old and had driver's licenses. Firstly, the driving scene was presented to them while they were requested to memorize landmarks. Next, a brain wave sensor was worn on them and the same driving scene was presented again. The subjects were requested to trace a route by checking the landmarks.

The brain wave sensor was a consumer single-channel electroencephalograph. 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. The specifications are summarized in Table 1.

Table 1: Specifications of the brain wave sensor.

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

An experimental scene is shown in Fig. 5. Distance between the subjects and a display was about 1 m.

The measurement was carried out twice a day and it was repeated five days and so 10 EEGs were obtained from each subject and 120 EEGs were obtained in total. In addition, for making templates, five EEGs in relaxed condition for each subject were obtained by measuring once a day for five days.

Figure 5: An experimental scene.

3.4 Verification Experiments

EEGs of one minute long were used in verification. 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 those of imposters.

For reference, spectra of two subjects at $\alpha-\beta$ band in relaxed and mental-tasked condition are shown in 6. Additionally, frequencies which caused these variations depend on the subjects; therefore, it is expected that the difference between the power spectra in relaxed and in mental-tasked condition becomes an individual feature.

In this paper, setting the number of partitions in α-β band: P to 4, that is, 8-11 Hz, 11-14 Hz, 14-17 Hz and 17-20 Hz, we evaluated verification performance at each partition by using the equal error rate (EER) where the false acceptance rate (FAR) is equal with the false rejection rate (FRR). The results are summarized in Table 2. It is interesting that each band has

Table 2: Verification performance.

Partition (Hz)	EER (%)
8-11	41
11-14	37
14-17	32
17-20	34

a different EER. In particular, the EER of 8-11 Hz is the biggest. As shown in Fig. 6, the discriminative spectra in α band in the relaxed condition were not observed in the mental-tasked condition. Such a large variation might have an influence on increasing the error rate since normalization was not performed in this verification.

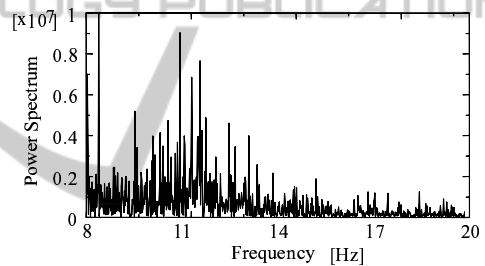Next, we evaluated the performance by combin-
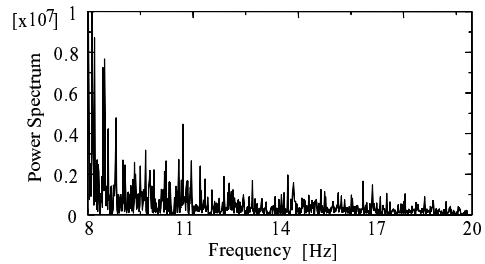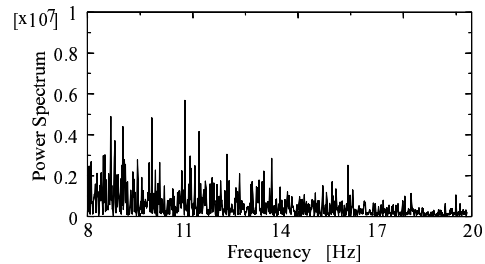

(a) Relaxed Condition
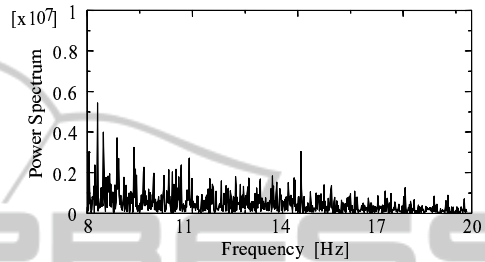
(b) Mental-Tasked Condition

(a) Subject A

(a) Relaxed Condition

(b) Mental-Tasked Condition

(b) Subject B

Figure 6: Spectra of two subjects, in (a): relaxed condition and (b): mental-tasked condition.

ing scores in three partitions except the 8-11 Hz. The variation of the FAR and FRR with the threshold in the final decision are plotted by the solid line and the dashed one, respectively in Fig. 7. The intersection of these curves corresponds to the EER and it was 31 % in this case.
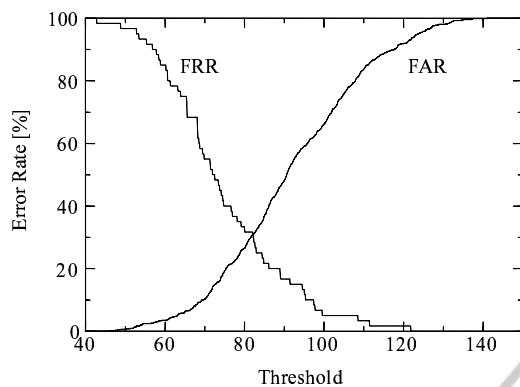
Figure 7: Error rate curves.

4 CONCLUSIONS

Assuming driver authentication as one of applications based on on-demand operator authentication, we measured EEGs of drivers when they were route-tracing. And we evaluated verification performance using the difference between the power spectrum at α-β band in relaxed condition and that in mental-tasked condition as an individual feature. Using 12 subjects, we obtained the best EER of 31 % when the scores in 11-14 Hz and 14-17 Hz are combined.

However, the performance is not high enough to conclude that the authentication using the brain wave is ready for practical use. There are many problems to be overcome. We are now assembling the database of the brain wave using large number of subjects and evaluating the verification performance. It is also a problem to introduce more powerful method into verification. In the future, it is necessary to evaluate not only verification performance but also usability in the on-demand authentication system using the brain wave.

ACKNOWLEDGEMENTS

REFERENCES

Altinok, A. and Turk, M. (2003). Temporal integration for continuous multimodal biometrics. In *Proc. of 2003 Workshop on Multimodal User Authentication*.

Kwang, G., Yap, R. H. C., Sim, T., and Ramnath, R. (2009). Usability study of continuous biometrics authentication. In *Tistarelli M. and Nixon M. S. (Eds.): ICB2009, LNCS 5558*. Springer.

Marcel, S. and Millan, J. R. (2007). Pearson authentication using brainwaves (eeg) and maximum a posteriori model adaption. In *IEEE Trans. on Pattern Analysis and Machine Intelligence*.

Matsumoto, T. (2006). Security design and security measurement for biometric systems (in japanese). In *Proc. of the 7th IEICE Technical Report of Biometrics Security Group*.

Matsumoto, T., Kusuda, T., and Shikata, J. (2007). On the set of biometric test objects for security evaluation of iris authentication systems -part 2- (in japanese). In *Proc. of the 9th IEICE Technical Report of Biometrics Security Group*.

Matsumoto, T., Matsumoto, H., Yamada, K., and Hoshino, S. (2002). Impact of artificial 'gummy' fingers on fingerprint systems. In *Proc. of SPIE*.

Mohammadi, G., Shoushtari, P., Ardekani, B. M., and Shamsollahi, M. B. (2006). Person identification by using ar model for eeg signals. In *World Academy of Science, Engineering and Technology*.

Nakanishi, I., Baba, S., and Miyamoto, C. (2009). Eeg based biometric authentication using new spectral features. In *Proc. of 2009 IEEE International Symposium on Intelligent Signal Processing and Communication Systems*.

Nakanishi, I., Baba, S., and Miyamoto, C. (2010). On-demand biometric authentication of computer users using brain waves. In *Zavoral F. et al. (Eds.): NDT2010, Part I, CCIS 87*. Springer.

Palaniappan, P. (2005a). Multiple mental thought parametric classification: A new approach for individual identification. In *International Journal of Signal Processing*.

Palaniappan, R. (2005b). Identifying individuality using mental task based brain computer interface. In *Proc. of the 3rd International Conference on Intelligent Sensing and Information Processing*.

Palaniappan, R. and Mandic, D. P. (2007). Biometrics from brain electrical activity: A machine learning approach. In *IEEE Trans. on Pattern Analysis and Machine Intelligence*.

Paranjape, R. B., Mahovsky, J., Benedicent, L., and Koles, Z. (2001). The electroencephalogram as a biometric. In *Proc. of 2001 Canadian Conference on Electrical and Computer Engineering*.

Poulos, M., Rangoussi, M., and Alexandris, N. (1999a). Neural networks based person identification using eeg features. In *Proc. of 1999 International Conference on Acoustic Speech and Signal Processing*.

Poulos, M., Rangoussi, M., Chissikopoulus, V., and Evangelou, A. (1999b). Parametric person identification from the eeg using computational geometry. In *Proc. of the 6th IEEE International Conference on Electronics, Circuits and Systems*.

Poulos, M., Rangoussi, M., Chrissikopoulos, V., and Evangelou, A. (1999c). Person identification based on parametric processing of the eeg. In *Proc. of the 9th*

IEEE International Conference on Electronics, Circuits and Systems.

Ravi, K. V. R. and Palaniappan, R. (2005). Recognition individuals using their brain patterns. In *Proc. of the 3rd International Conference on Information Technology and Applications.*

Riera, A., Soria-Frisch, A., Caparrini, M., Grau, C., and Ruffini, G. (2008). Unobtrusive biometrics based on electroencephalogram analysis. In *EURASHIP Journal on Advances in Signal Processing.*

Singhal, G. K. and Ramkumar, P. (2007). Person identification using evoked potentials and peak matching. In *Proc. of 2007 Biometric Symposium.*