On-Demand Biometric Authentication for System-User Management

Isao Nakanishi[0000−0001−9533−9987]

Tottori University, Tottori 680-8552, Japan
nakanishi@tottori-u.ac.jp

Abstract. To realize a secure system-user management, continuous authentication must be implemented in the system. In addition, only limited biometrics that can be measured passively are applicable for continuous authentication. However, continuous authentication is a heavy processing load for the system. In this study, possible methods for conducting a continuous authentication are examined from the viewpoint of reducing the processing load, and two types of on-demand authentication approaches are confirmed to be effective.

Keywords: System-user management · Continuous authentication · Biometrics · On-demand authentication · Processing load.

1 Introduction

In the transport systems involving many human lives, security systems handling confidential information, and online-learning systems for licenses and qualification purposes, it is extremely important to distinguish regular users of the system. In general, user authentication is performed only once when users begin to use a system, such as a log-in authentication using a password. However, if a regular user is replaced by a nonregular user after authentication, the nonregular user can easily use the system.

To prevent such spoofing, continuous authentication, in which users are constantly authenticated while using the system, is required. Therefore, continuous authentication is drawing research attention[1]. However, general passwords and ID cards cannot be used in continuous authentication because it is inconvenient for users to keep presenting them while using the system. Thus, biometrics is expected to be used in continuous authentication. However, if the conscious use of biometrics brings about the same level of inconvenience as passwords and ID cards, the use of only passively detectable biometrics that do not need to be consciously presented will be essential. Continuous authentication can be realized only when passively detectable biometrics are applied. Although such an affinity between biometrics and continuous authentication has also been pointed out in Ref. [2], a concrete proposal has yet to be examined.

Initially, biometrics was expected to be a convenient authentication method because unlike passwords and ID cards, such information is never lost or forgotten[3]. However, passwords and ID cards are still used in our daily lives.

Although there may be several reasons for this, one reason is that passwords and ID cards are sufficient for person authentication. In person authentication, security is always contrary to usability[1]. In ordinary circumstances, security never has a higher priority than usability. Ease of use is important for ordinary people. As an alternative to passwords and ID cards, biometrics must overcome the inconvenience of introducing a new method into people ' s lives, which is an ongoing problem. An aspect unique to biometrics, thereby validating its use, is continuous authentication.

The face, iris, and ear images are applicable as passively detectable biometrics that users are not required to consciously present. However, such features are exposed on the body surface; therefore, it is easy for others to capture them without knowledge of the user, and there is a risk that the authentication system using the modality will be counterfeited through the use of forgeries produced with the captured data. There is also a risk that they can be changed through plastic surgery. Moreover, there is a tendency for the face to be prohibited from use because it directly concerns the issue of privacy[4]. Therefore, the biometric modalities that are exposed on the body surface are ineligible for this study. Any vulnerability or risk has to be excluded in transport systems involving many human lives, security systems handling confidential information, and other areas.

There are also behavioral biometrics that are extracted for human actions such as moving, writing, speaking, and typing. However, biometrics based on actions differing from those applied by the system are excluded because they cannot be unconsciously presented. Assuming the use of a system, although a voiceprint or typing pattern is applicable, they are usable only when speaking or typing.

Therefore, there is no conventional biometrics suitable for contentious authentication. The author has noted continuous authentication as a killer biometrics application[5] and has therefore proposed the use of an intra-body (palm) propagation signal as passively detectable biometrics and evaluated its verification performance[6–10]. Moreover, the author has noticed brainwaves (electroencephalogram, EEG) as passively detectable biometrics and evaluated different verifications of their performance[11–16].

However, with continuous authentication, the authentication process is always being executed; therefore, if the application and authentication processes are executed on the same system, the processing load of the system will become heavy. In Ref. [1], the increase in power consumption from the authentication processing is also pointed out.

Therefore, this study examines what types of methods are effective in realizing continuous authentication through the use of passively detectable biometrics for the purpose of reducing the processing load.

[1] If the threshold for determining whether a user of a system is genuine becomes high, the security of the system increases, whereas the usability is decreased because a user may be rejected many times even if the user is genuine.

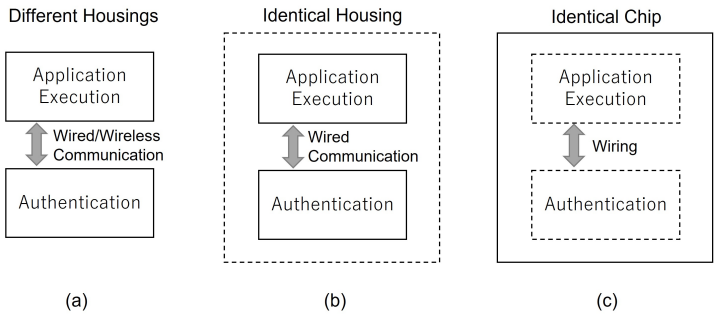

Fig. 1. System configuration.

2 Assumed Authentication System

First, the relationship between the execution of an application and authentication processing is defined. People execute an application in a system, whereas authentication processing has no relation with the application execution. Therefore, it is natural to suppose that application execution and authentication processing are applied in different systems, as shown in Fig. 1(a). However, even if a user is determined to be non-regular by the authentication system, it is impossible to directly prevent a non-regular user from using the application system. The two separate systems exchange information using some means of communication. However, if the communication means are disconnected or a fake signal is inserted into the communication path, the application system cannot know that the user is non-regular. Even if the two systems are installed in a specific case (Fig. 1(b)), the same problem as in (a) may be caused in the inner cable connecting the two systems. To solve this problem, these two systems must be installed on a chip, as shown in (c). However, case (c) is unrealistic because it is necessary to prepare a dedicated chip for each application.

It is easy to realize these systems using software on a general-purpose CPU, and the disconnection problem in the communication path does not arise. Thus, in this study, it is assumed that the application and authentication are processed using software in a CPU. Therefore, less processing load is required for authentication.

3 Authentication of System User

Four types of authenticating users can be assumed in the system, as described in Fig. 2, where the horizontal axis represents the passage of time while using the system and small downward arrows indicate the authentication execution. The larger the number of the arrows, the heavier the processing load becomes.

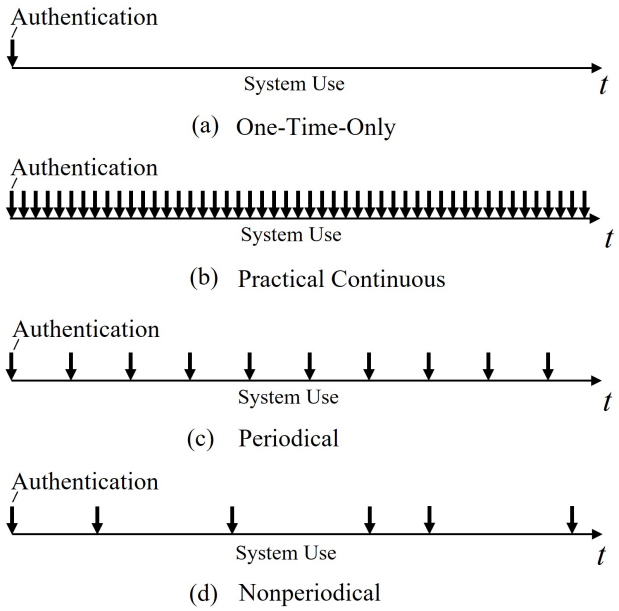

Fig. 2. Four types of authentication of system users.

3.1 One-time-only Authentication

Figure 2(a) shows the one-time-only (one-off) authentication, in which the authentication is executed only once when the user begins to use the system. Log-in authentication when starting the use of a computer or mobile device is a typical example. However, one-time-only authentication never prevents a spoofing in which a regular user is switched to a nonregular user after authentication. This spoofing is also called "section hijacking"[17, 18].

3.2 Continuous Authentication

To prevent such hijacking, continuous authentication, in which the users are continuously authenticated while using the system, is required. However, strictly speaking, the authentication is executed not in a continuous (analog) time but in a discrete time, as shown in Fig. 2(b), for instance, every frame (50 ms)[19], every second[17, 20], or every cycle for an instruction execution of the system[18, 21–23].

As the biometrics, a passively detectable face image and voiceprint were used, along with a fingerprint detected from a sensor equipped on a mouse for computer use[17, 19, 20]. In addition, soft biometrics (skin and clothes colors) extracted from images[18], touching actions on a smartphone display[21, 22], keystrokes

when typing on a keyboard, and voiceprints when calling or conducting a voice-search on a web sites[23] were used.

In these studies, the reason why multiple biometrics were used is to deal with a case in which appropriate biometric data for authentication cannot be obtained when executing authentication. For instance, in authentication using face images, when a face is not facing the camera, an appropriate face image for matching cannot be obtained, and thus alternative biometrics are used. Moreover, when using the keystroke of a keyboard or a mouse operation as biometrics, even if they temporarily stop and their biometric data can no longer be obtained, the prior obtained authentication score (reliability) is maintained despite its decrease over time. When the deceased score is less than the threshold determined in advance, the system usage is prohibited, and the user is re-authenticated.

It is important that the actions applied for using the system and authentication be identical. It is impossible or inconvenient to conduct an action that differs from that when using the system. In the following, it is not assumed that the system usage is interrupted, and biometric data are presented for authentication.

However, in addition to the application execution, a continuous authentication system operates without stopping, and thus its processing load increases. In Ref. [20], it was reported that the system overhead reaches up to 42% when authentication is applied every second.

4 Periodical and Non-periodical Authentication

To reduce the processing load, it is necessary to reduce the number of authentication executions while preventing spoofing.

4.1 Periodical Authentication

Instead of continuous authentication, it is conceivable to authenticate at regular intervals, as shown in Fig. 2(c). For convenience, this is called periodical authentication. In Ref. [24], the authentication using a face image was conducted at 30-s intervals, and thus, it is expected to reduce the processing load. However, the possibility of spoofing during the 30-s period is not considered. In addition, a problem in which the applicable biometric data cannot be obtained when executing the authentication, as mentioned above, is not considered.

4.2 Nonperiodical Authentication

Thus, it is conceivable that authentication is executed only when required and executable. This is called nonperiodic authentication, and can reduce the processing load, as shown in Fig. 2(d). However, the actual amount of reduced processing load depends on the authentication frequency.

To further discuss the reduction in the number of processes in a non-periodic authentication, Fig. 3 is presented, in which, similar to Fig. 2, the horizontal axis represents the passage of time while using the system, and the small downward

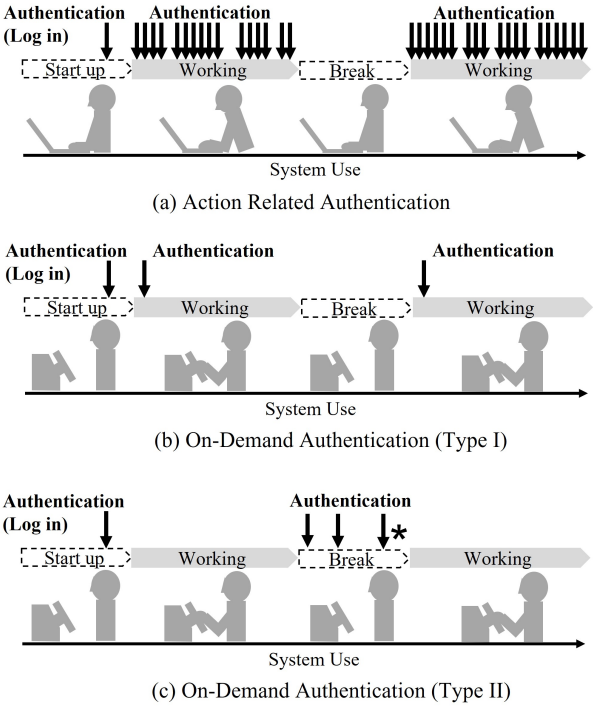

Fig. 3. Nonperiodical authentication.

arrows indicate the authentication execution. In addition, continuous operations in the system usage (for instance, typing or handling) and a break between them are distinguished as "Working" and "Break", respectively.

4.3 Action-Related Authentication

Authentication that is triggered by the operation of a device is called action-related authentication herein, as shown in Fig. 3(a). In Refs. [25–27], the authors assumed operations when applying a keyboard and computer mouse or when touching a smartphone display. Although these studies may be classified as continuous authentication, in this study, they are treated separately because they differ from the way continuous authentication is approached.

Because action-related authentication is applied continuously during an operation, the effect of reducing the processing load depends on the operation frequency, although it is not considered to be high. In addition, there may be temporary breaks during an operation; therefore, a mechanism for maintaining the authentication score obtained before, as described in Sec. 3.2, is provided.

5 On-demand Authentication

The author proposed on-demand authentication [14, 28–31], in which authentication is applied when required and possible. Unlike action-related authentication, the frequency of authentication execution is low, which results in a reduction in the processing load. However, its realization has not actually been discussed. What type of situation describes "when authentication is required"?

5.1 Type I

The author proposed the use of an intra-body (palm) propagation signal [6–10], that is, the signal propagated between two electrode pairs on the body, as a type of biometrics. If the characteristics of the propagated signals differ from each other, the propagated signal can be used as a new biometric modality. Various systems are applied with the user touching or gripping a part of the system. If a detection mechanism of the intra-body propagation signal is equipped in the system, the propagated signal can be detected without any positive action; thus, it is a passively detectable biometric. On-demand authentication using such a biometrics is called Type I, as shown in Fig. 3(b).

Can it be assumed that a driver will be replaced with someone else when turning a handle? In addition, can it be assumed that a computer user will be replaced when typing on a keyboard or moving a mouse? The answer is clearly no. Therefore, it is not necessary to authenticate the user while touching the system[2]. This is an extremely important aspect of the present study.

In the case of action-related authentication, continuous action when using a mobile device is applied as a biometric; therefore, continuous authentication is required, which increases the processing load. By contrast, when not using continuous action as a biometric, it is not necessary to authenticate continuously even when using a system. This is a different aspect between action-related authentication and the proposed Type I authentication. When the use of the system is started, authentication is executed once, after which, or during a break, authentication is not conducted.

5.2 Type II

By contrast, it is possible for a user to be replaced with someone else during a break while at work[3]. Thus, it is proposed to avoid authenticating the user while

[2] Even if the user changes into someone else after authentication, it is possible to deal with the spoofing by authenticating the user nonperiodically while increasing the frequency of the authentication, that is, applying a processing load. The authentication frequency should be determined by considering the increase in the processing load.

[3] The break is assumed to be temporal, for instance, a temporary interruption to think while using a computer, or a temporary stop at a traffic signal while driving. If the user leaves the system, it is considered that the work has been completed and a log-in authentication will be required again.

using the system and instead to authenticate the user when a break is detected. This is considered Type II, as shown in Fig. 3(c).

This type is preferable to biometrics that use cognitive information, such as brain waves[11–16, 28–31]. In brain wave measurements, noise from body movements can be mixed into the waves, which becomes a problem. When using the response to stimulation in brain waves, the mixing of different stimuli must be avoided. As mentioned in the previous subsection, if it is not assumed that the user changes during a work period, it becomes sufficient to apply authentication during a break, which is convenient for preventing noise from being mixed into the brain waves.

However, it is unpredictable when a break will end, and the work will resume. When using passively detectable biometrics such as brain waves, it is unknown when authentication can be conducted. If authentication is applied after spoofing, it is possible to prevent such spoofing. Therefore, Type II has a deterrence against spoofing. However, if authentication is conducted only once during a break, the user is replaced with someone else as a sink-or-swim gamble, and the spoofing is not prevented after authentication. Thus, authentication must be conducted periodically or nonperiodically during a break with the proposed Type II approach.

Even so, the risk of user replacement after authentication just before resuming the work, as indicated by "$*$" in Fig. 3(c), cannot be completely eliminated. To eliminate this risk, a multimodal type combining Type I is required. In this case, authentication is conducted during both work and break periods, which results in an increase in the processing load.

5.3 Reduction of Processing Load

Based on the above discussion, on-demand authentication is the most effective method for reducing the processing load while preventing spoofing. However, the effect of reducing the processing load depends on the length of the work and break times. When the break time is longer than the work time, the processing load of Type II increases. By contrast, a lengthy work time results in a large processing load for Type I. Which type is suitable depends on the application? For instance, when users use an application while occasionally thinking, Type I is suitable. When users do nothing except use the application, then Type II is suitable. However, the above examination is based only on the frequency of the authentication execution. However, a processing load also occurs owing to the authentication itself. The actual processing load must be evaluated by combining the authentication frequency and amount of authentication processing.

5.4 Detection of Start/Break/End-of-work Times

In the proposed Types I and II approaches, it is necessary to accurately detect the start, pause, and end-of-work times. The trigger of the detection is the start, pause, or end of keyboard typing or mouse operation when using a computer. When driving, the start, pause, and end of driving are detected by pressing

an accelerator pedal, pressing a brake pedal, and leaving the seat, respectively. These are detectable using pressure sensors and signal processing techniques, and their processing load is not large. In addition, in the case of driving. These triggers may be obtained from the driving control system of the car.

5.5 Working During Break Period

Next, let us examine a case of working during a break period. In this study, it is assumed that strict user management is required, such as transport systems involving many human lives, security systems handling confidential information, and online learning systems for licenses and qualifications. It is therefore unexpected for users to do the other work during their break period, for instance, when drinking, eating, calling of the phone, or chatting, among other cases. The user concentrates on conducting the original work (application) while using the system. A break is a temporary pause in work and not for carrying out other works. In the proposed Type II approach, it is assumed that the authentication is executed during the break, but it is not assumed that the user will conduct other tasks.

However, body movements are assumable during a break, which results in noise in the brain waves. Therefore, during body movements, authentication using brain waves should be avoided. However, if large body movements occur during a break, it may suggest that a regular user is trying to be replaced with someone else. Thus, by detecting body movements, authentication can be prohibited while the body is in motion. If such movement continues for more than a certain interval, a log-in authentication will be required again, assuming that spoofing has occurred.

6 Processing of On-demand Authentication

Based on the discussion thus far, the processing of the proposed on-demand authentication method is examined.

6.1 Type I

The processing flow of Type I is shown in Fig. 4. At first, the login authentication is performed[4]. After the login authentication, the system usage by the user is started. When detecting the beginning of a work period, authentication using passively detectable biometrics is applied. If the user is regarded as genuine, the user is permitted access to the system until the break period is detected. After the break, if the start of the work is detected again, authentication is resumed. However, if the end of the work is detected, the authentication process also ends.

[4] In on-demand authentication, passively detectable biometrics are also used for a login authentication, whereas action-related authentication requires the user to use other biometrics or a password/ID card for login authentication.

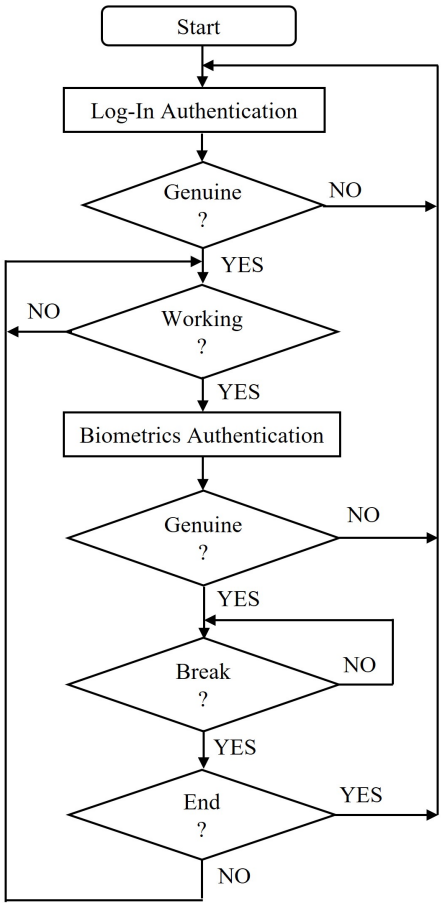

Fig. 4. Processing flow of Type I.

6.2 Type II

The processing flow for Type II is shown in Fig. 5. After login authentication and the start of system use, the user is permitted to use the system unless a break in work is detected. If a work interruption is detected and then the end of the work is also detected, the system use will be ended. If the end of the work is not detected, the interruption is regarded as a work break, and body movement detection is applied. If body-movement is not detected, the authentication is conducted. If the user is regarded as genuine, the user is permitted to use the system, and the interval for applying the next authentication is set, where a nonperiodic authentication is assumed to be conducted during the break. At the time set for the next authentication, the detection of the break restarts. However, if body movement is detected, authentication is not conducted. The detection

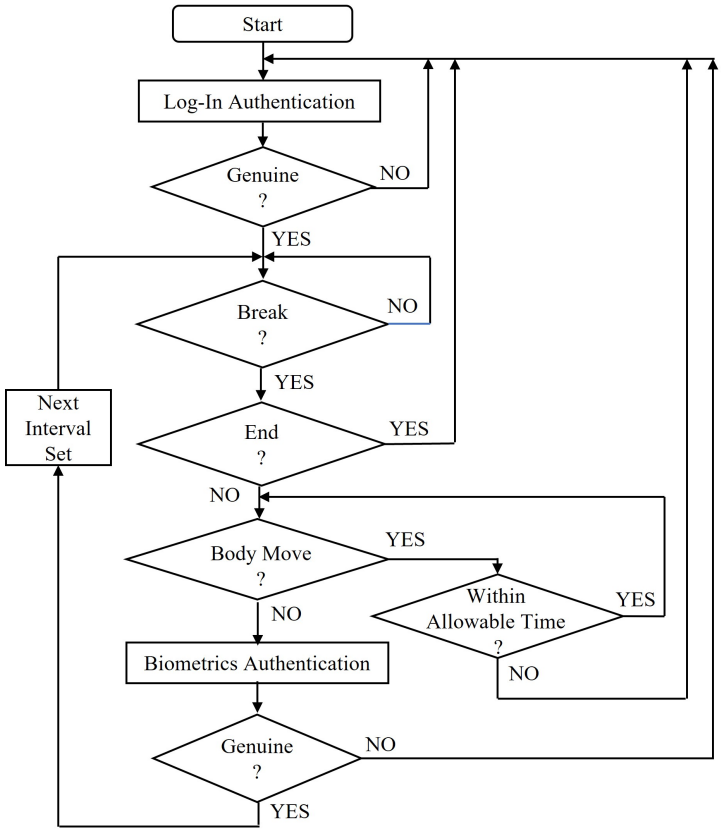

Fig. 5. Processing flow of Type II.

of body-movement is continued within the allowable preset time. If the interval in which the authentication is not performed becomes larger than the allowable time, the system usage of the user is forcibly refused.

7 Conclusions

To prevent spoofing in system-user management, continuous authentication is required; however, this increases the processing load of the system. In addition, only passively detectable (consciously presentable) biometrics are applicable for continuous authentication.

In this study, from the viewpoint of reducing the processing load, we examined what type of method is effective in realizing continuous authentication using passively detectable biometrics. As a result, it was confirmed that the proposed on-demand authentication system is effective. Moreover, Type I, which applies

authentication during work, and Type II, which conducts authentication during a break period, were proposed as on-demand authentication, and their feasibilities were evaluated. In particular, Type II is suitable for cognitive biometrics, such as brain waves.

In this examination, only the frequency of the authentication execution was considered; however, the processing load owing to the authentication process itself should also be included. In the future, it will be necessary to comprehensively evaluate the processing load when considering the authentication frequency and load required for authentication processing. It will also be necessary to build authentication systems and evaluate their processing loads.

References

1. A. F. Baig and S. Eskeland, "Security, Privacy, and Usability in Continuous Authentication: A Survey," Sensors, vol. 21, pp. 1-26, 2021.
2. A. A. Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and Transparent Multimodal Authentication: Reviewing the State of the Art," Cluster Comput, vol. 19, pp. 455-474, 2016.
3. A. Jain, R. Bolle, and S. Pankanti, "BIOMETRICS Personal Identification in Networked Society," Kluwer Academic Publishers, Massachusetts, 1999.
4. "EU privacy watchdogs call for ban on facial recognition in public spaces," Reuters Tech News, 21 June 2021.
5. I. Nakanishi, "Unconscious Biometrics for Continuous User Verification," Proc. of the 8th International Conference on Signal Processing Systems (ICSPS2016), pp. 20-25, 2016.
6. I. Nakanishi, Y. Yorikane, Y. Itoh, and Y. Fukui, "Biometric Identity Verification Using Intra-Body Propagation Signal," Proc. of 2007 Biometrics Symposium, 2007.
7. I. Nakanishi, Y. Sodani, and S. Li, "User Verification Based on the Support Vector Machine Using Intra-Body Propagation Signals," International Journal of Biometrics, vol. 5, nos. 3/4, pp. 288-305, 2013.
8. T. Inada, Y. Sodani, and I. Nakanishi, "Intra-Palm Propagation Signals as Suitable Biometrics for Successive Authentication," Journal of Computer Technology and Application, vol. 7, no. 2, pp. 65-72, 2016.
9. I. Nakanishi, I. Ogushi, R. Nishi, and T. Murakami, "Effect of Propagation Signal and Path on Verification Performance Using Intra-Body Propagation Signals," Proc. of 2017 International Conference on Biometrics Engineering and Application (ICBEA2017), pp. 80-84, 2017.
10. K. Fujita, Y. Ishimoto, and I. Nakanishi, "Person Verification Using Intra-Palm Propagation Signals with A New Phase Spectrum," Proc. of 12th International Conference on Knowledge and Smart Technology (KST2020), pp. 86-90, 2020.
11. I. Nakanishi, C. Miyamoto, and S. Baba, "EEG Based Biometric Authentication Using New Spectral Features, " Proc. of 2009 IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS2009), pp. 651-654, 2009
12. I. Nakanishi, S. Baba, C. Miyamoto, and S. Li, "Person Authentication Using a New Feature Vector of the Brain Wave," Journal of Communication and Computer, vol. 9, no. 1, pp. 101-105, 2012.

13. I. Nakanishi, C. Miyamoto, and S. Li, "Brain Waves as Biometrics in Relaxed and Mentally Tasked Conditions with Eyes Closed," International Journal of Biometrics, vol. 4, no. 4, pp. 357-372, 2012.
14. I. Nakanishi, S. Baba, K. Ozaki, and S. Li, "Using Brain Waves as Transparent Biometrics for On-Demand Driver Authentication," International Journal of Biometrics, vol. 5, nos. 3/4, pp. 321-335, 2013.
15. I. Nakanishi, and T. Yoshikawa, "Brain Waves as Unconscious Biometrics towards Continuous Authentication - The Effects of Introducing PCA into Feature Extraction -," Proc. of 2015 IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS2015), pp. 422-425, 2015.
16. I. Nakanishi, and T. Maruoka, "Biometrics Using Electroencephalograms Stimulated by Personal Ultrasound and Multidimensional Nonlinear Features," Electronics, vol. 9, no. 24, pp. 1-18, 2020.
17. S. Zhang, R. Janakiraman, T. Sim, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," Proc. of International Conference on Biometrics (ICB2006), pp. 562-570, 2006.
18. K. Niinuma, U. Park, and A. K. Jain, "Soft Biometric Traits for Continuous User Authentication," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 771-780, 2010.
19. A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. of 2003 Workshop on Multimodal User Authentication, pp. 207-214, 2003.
20. G. Kwang, R. H. C. Yap, T. Sim, and R. Ramnath, "Usability Study of Continuous Biometrics Authentication," M. Tistarelli and M. S. Nixon (Eds.): ICB2009, LNCS 5558, Springer, pp. 828-837, 2009.
21. M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," IEEE Transactions on Information Forensics and Security, vol. 8, pp. 136-148, 2012.
22. R. Kumar, V. V. Phoha, and A. Serwadda, "Continuous Authentication of Smartphone Users by Fusing Typing, Swiping, and Phone Movement Patterns," Proc. of 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS2016), 2016.
23. H. Crawford, K. Renaud, and T. Storer, "A Framework for Continuous, Transparent Mobile Device Authentication," Computers & Security, vol. 39, pp. 127-136, 2013.
24. D. Crouse, H. Han, D. Chandra, B. Barbello, and A. Jain "Continuous Authentication of Mobile User: Fusion of Face Image and Inertial Measurement Unit Data," Proc. of 2015 International Conference on Biometrics (ICB2015), 2015.
25. V. M. Patel, R. Chellappa, D. Chandra, B. Barbello, "Continuous User Authentication on Mobile Devices: Recent Progress and Remaining Challenges," IEEE Signal Processing Magazine, vol. 33, 2016.
26. S. Mondal, and P. Bours, "A Computational Approach to the Continuous Authentication Biometric System," Information Sciences, vol. 304, pp. 28-53, 2015.
27. S. Mondal, and P. Bours, "A Study on Continuous Authentication Using a Combination of Keystroke and Mouse Biometrics," Neurocomputing, vol. 230, pp. 1-22, 2017.
28. I. Nakanishi, and C. Miyamoto, "On-Demand Biometric Authentication of Computer Users Using Brain Waves," F. Zavoral et al. (Eds.), Networked Digital Technologies in the Communications in Computer and Information Science (CCIS) series of Springer LNCS, vol. 87, pp. 504-514, 2010.

29. I. Nakanishi, S. Baba, and S. Li, "Evaluation of Brain Waves as Biometrics for Driver Authentication Using Simplified Driving Simulator," Proc. of 2011 International Conference on Biometrics and Kansei Engineering (ICBAKE2011), pp. 71-76, 2011.
30. I. Nakanishi, S. Baba, and S. Li, "Driver Authentication Using Brain Waves While Route Tracing as a Mental Task," Proc. of the 6th International Conference on Security and Cryptography (SECRYPT2011), pp. 90-96, 2011.
31. I. Nakanishi, H. Fukuda, and S. Li, "Biometric Verification Using Brain Waves toward On-Demand User Management Systems - Performance differences between divided regions in alpha-beta wave band," Proc. of the 6th International Conference on Security of Information and Networks (SIN2013), pp. 131-135, 2013.