INVITED PAPER *Special Section on Advanced Log Processing and Office Information Systems*

Toward More Secure and Convenient User Authentication in Smart Device Era

Yasushi YAMAZAKI[†a)] ***and*** **Tetsushi OHKI**[††], ***Members***

SUMMARY With the rapid spread of smart devices, such as smartphones and tablet PCs, user authentication is becoming increasingly important because various kinds of data concerning user privacy are processed within them. At present, in the case of smart devices, password-based authentication is frequently used; however, biometric authentication has attracted more attention as a user authentication technology. A smart device is equipped with various sensors, such as cameras, microphones, and touch panels, many of which enable biometric information to be obtained. While the function of biometric authentication is available in many smart devices, there remain some problems to be addressed for more secure and convenient user authentication. In this paper, we summarize the current problems with user authentication on smart devices and propose a novel user authentication system based on the concept of context awareness to resolve these problems. We also present our evaluation of the performance of the system by using biometric information that was acquired from smart devices. The evaluation demonstrates the effectiveness of our system.

key words: *smart device, user authentication, biometrics, context awareness, environment recognition*

1. Introduction

Smart devices, such as smartphones and tablet PCs, are considered to be the most influential information and communication devices from the viewpoint of their growing number and the data traffic they produce in the Internet of Things (IoT) era [1]. Moreover, they are also the most familiar and interactive devices in our daily life. For such smart devices, the implementation of information security functions, such as encryption and user authentication, is indispensable because various kinds of data concerning user privacy, such as lifelogs, are frequently processed within them. At present, password-based authentication is primarily used for smart devices; however, active utilization of biometric authentication [2], [3], which has advantages over password-based authentication in terms of security and convenience, should also be taken into account considering the possibility of developing various smart-device-specific user services in the near future. Recently, the function of biometric authentication, such as fingerprint recognition, has been provided for many smart devices; however, its use is still limited compared with password-based authentication. To further spread the use of biometric authentication on smart devices, we should solve the following technical problems.

The first problem is that the variation in usage environments influences the authentication performance when using a biometric authentication function on smart devices. The characteristics of biometric information fluctuate even in the same person, so various algorithms that allow for this fluctuation have been proposed. However, comparing smart devices with other devices, the former has a tendency of showing more obvious variation in biometric information. For example, in the case of handwritten signatures, which are one biometric modality, the capture environment, such as the input means, e.g., fingers or a pen, writing posture, e.g., standing position or sitting position, and device position, e.g., held in the hand or put on a table, can frequently fluctuate in user authentication. Our recent study [4] revealed the fact that such variation in usage environments in the authentication process has no small effect on authentication performance. High flexibility in usage environments is one of the most attractive characteristics of smart devices; however, the variation in usage environments, which is difficult to control on the system side, seriously affects the performance of biometric authentication, so the consideration of effective countermeasures becomes increasingly important.

The second problem is security issues that occur when using biometric information on smart devices. Nowadays, one of the biggest problems is the leakage of personal information from smart devices whose users are not always highly security conscious. Unlike password-based authentication, biometric authentication, the security strength of which is not affected by a user's security awareness, is an appropriate means of protecting personal information on smart devices. However, biometric information itself is the ultimate personal information, and once leaked, it cannot be changed unlike passwords, which is a biometric-specific vulnerability. Therefore, various methods for establishing the security of biometric templates [5] have been proposed. However, many of them are based on sophisticated cryptographic algorithms that require a high computational complexity or high communication cost. As far as we know, few template protection methods have been proposed that are suitable for smart devices in which the computational complexity or memory capacity is limited. Therefore, there is an urgent need to develop a technology for protecting biometric information that is suitable for smart devices.

The third problem is that smart devices have various limitations compared with conventional PCs in terms of

Manuscript received February 3, 2017.
Manuscript revised June 9, 2017.
Manuscript publicized July 21, 2017.

[†] The author is with The University of Kitakyushu, Kitakyushu-shi, 808–0135 Japan

[††] The author is with Shizuoka Univerisy, Hamamatsu-shi, 432–8011 Japan

a) E-mail: y-yamazaki@kitakyu-u.ac.jp

DOI: 10.1587/transinf.2016OFI0002

available resources, such as processor performance, memory size, battery capacity, and physical size. In conventional PC-based biometric authentication, biometric data are usually obtained from the stand-alone sensors and processed by using a PC. Small numbers of discussions have been made on the sizes of the sensors or the resources required for authentication processing. This discussion is inevitable when biometric authentication is applied to smart devices. It is controversial whether the conventional technologies can be applied to smart devices as they are. In some biometric authentication technologies that have already been provided for smart devices, it is true that the above problem has been partially cleared; however, more discussion on the resources of smart devices is needed to provide various biometric authentication functions to smart devices.

It is indispensable to address all these problems to establish more secure and convenient user authentication for the coming smart device era; however, this would exceed the scope of this paper since the problems cover a very broad range of research topics. Therefore, in this paper, we primarily pay attention to how to balance security and convenience in smart-device-specific user authentication, which is mainly related to the first problem, and propose a novel user authentication system. An overview of our proposal is illustrated in Fig.1. We call it a "context-awareness-based multifactor authentication system." In our approach, we focus on the concept of "context awareness," which is detailed in the subsequent section, and develop a multifactor user authentication system by combining different kinds of authentication factors, such as passwords and a few kinds of biometric information. As shown in Fig.1, the system recognizes its surrounding environment autonomously by using multiple sensors in the system and authenticates a user by selecting an appropriate authentication method adaptively, which enhances not only the security but also the convenience of the system. The proposed system, detailed in the subsequent section, is an extension of our work [6], [7] and improves it in several ways.

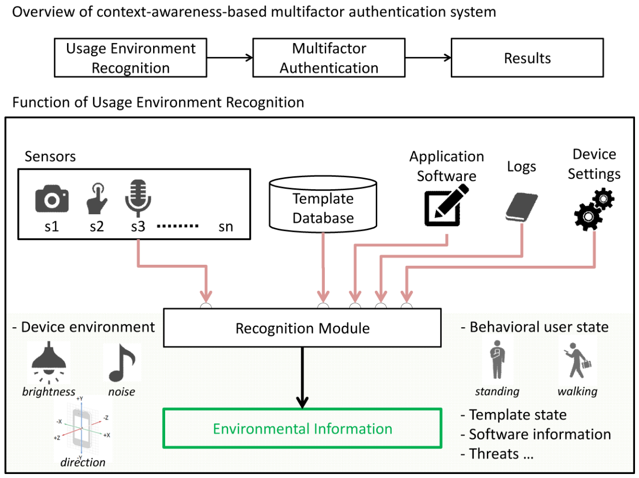

Fig. 1 Overview of context-awareness-based multifactor authentication system

The remainder of the paper is organized as follows. Related work is introduced and discussed in Sect. 2. Our approach is described in Sect. 3. Experimental results are shown in Sect. 4. We then conclude our work in Sect. 5.

2. Related Work

This section is a review of related work on context awareness, the main concept of our system.

To the best of our knowledge, the first appearance of the term "context awareness" dates back to the 1990's in [8] by Schilit et al. They defined context as the knowledge on a user's and IT device's state, including the surroundings, situation, and, to a lesser extent, location. They classified context in terms of where you are, who you are with, and what objects are around you. Subsequently, many researchers have given various definitions to the term, as shown in [9]–[12]. For example, Dey et al. [11] defined it as follows. "Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves." They classified context in terms of location, identity, activity, and time.

The term "context awareness" is also defined in the above pieces of literature. Schilit et al. [8] defined it in terms of proximate selection, automatic contextual reconfiguration, contextual information and commands, and context-triggered actions. Dey et al. [11] defined that a system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task. Chen et al. [12] defined it in terms of active and passive context awareness.

After the proposal by Schilit et al. [8], the main target of research on context awareness continued to be context recognition, whose purpose is to provide user services according to the context. Here, it should be noted that an application of context awareness for user authentication in terms of information security was not found until around 2005. After the appearance of smartphones that contain sophisticated sensors such as accelerometers and global positioning system (GPS) functionality, the trend of applying context awareness in the research field of user authentication began to take place. Typical examples are shown in the application of recognizing gait with an accelerometer on a smartphone while considering the position the smartphone is being held in [13]–[16]. In these examples, the difference in authentication accuracy was evaluated in specific usage environments, namely, different holding positions; however, the idea of the context awareness shown in [12], where an authentication algorithm is adjusted in accordance with a user's context, has still yet to be reached. Some examples of authentication algorithms that consider context awareness are shown in [17], [18]. Primo et al. [18] focused on 55 features that can be obtained from an accelerometer on a smartphone and clarified the effective features corresponding to the holding positions of the smartphone and showed that highly reliable authentication can be achieved by selecting the appropriate features for each holding position. Moreover, Hayashi et al. [17] proposed a scheme for selecting an appropriate authentication method to meet security demands. They focused on an authentication system that requires a user to input not a short PIN but a long password when he/she uses the system in a different place than usual or is in a crowd and defined it in a probabilistic framework.

Our approach to context awareness is related to the work of [17] and [18]. In particular, in the work of Hayashi et al. [17], they proposed context-aware scalable authentication (CASA), which is not a specific but a general authentication framework, where the authentication methods are changed depending on the context. Their concept partially includes our idea; however, there are some differences as follows.

- Only the change of authentication methods is considered, and an extension to multifactor authentication has yet to be done.
- The framework is proposed; however, experiments are conducted by using only PINs, passwords, and coarse positioning information as the context, and extension to biometric authentication is not discussed.
- As for security issues, only having the information on the context is discussed, yet security risks due to the invalid input of context or biometric information are not discussed.

Our approach is also related to current user authentication methods, such as multifactor authentication, multimodal biometric authentication, and risk-based authentication, each of which is focused on enhancing security under the assumption of threats of forgery. In user authentication on smart devices that are highly portable and user oriented, it is important to maintain convenience while enhancing security. Stable authentication even during vast changes in usage environments is considered to be an important factor in deciding the level of convenience. However, in many cases, users are prone to use the same predetermined authentication method regardless of the usage environment, which means that current methods are not always appropriate for user authentication on smart devices in terms of coping with changes in usage environments. The originality of our approach especially lies in selecting an optimal authentication method while enhancing convenience as well as security.

3. Context-Awareness-Based Multifactor Authentication [6], [7]

In this section, we give an overview of our proposed method. The proposed context-awareness-based multifactor authentication system is illustrated in Fig.2.

In our proposal, the concept of context awareness is included in the module of usage environment recognition shown in the same figure. The function of this recognition is detailed as follows.

- Recognition of device environment
  The environment surrounding the device, e.g., brightness and noise, or the environment of the device itself, e.g., the direction the device is facing, is recognized by using sensors in the device. The recognition results are used, for example, as the information used by the system to decide that voice should not be used as authentication information when the device is used in a noisy place.
- Recognition of behavioral user state
  The behavioral user state, e.g., resting state or walking state, is recognized by using sensors on the device. The recognition results are used, for example, as the information used by the system to decide that handwriting should not be used as authentication information when the user is walking because it would be difficult to write while walking.
- Acquisition of template state information
  Information on the kind and number of biometric templates registered in the system database or a lapse of time from the registration or the last update of a template is acquired. The acquired information is used, for example, by the system to decide that the system requires the user to update biometric information when a period of time has passed since the last update.
- Acquisition of application software information
  Information on the application software used or being used is acquired. The acquired information is used, for example, by the system to decide whether the system should conduct voice-based continuous user authentication [3] when the user is activating verbal communication software, such as voice chat.
- Acquisition of operation, usage, and behavioral logs
  Information on the operation log of a device, the usage log of application software, and the behavioral log of a user is acquired for the purpose of demanding user authentication when the user operates the device in a different manner than usual.
- Detection of threats
  Threats against the device by a malicious third party, e.g., the invalid operation against sensors, are detected. The detected information is used, for example, by the system to decide whether the system should stop using a face image temporarily for authentication information when it is clear that an attacker has tried to alter the measurement value of illuminance around the device invalidly by shading a brightness sensor intentionally in the authentication process.
- Acquisition of security/usability level
  Information is acquired on the desired preset security level for each piece of application software and on the usability level regarding the level of convenience in authentication, which is set by a user. The acquired information is used, for example, by the system to decide the appropriate authentication method for a device unlock application, a money transfer application, and so on.

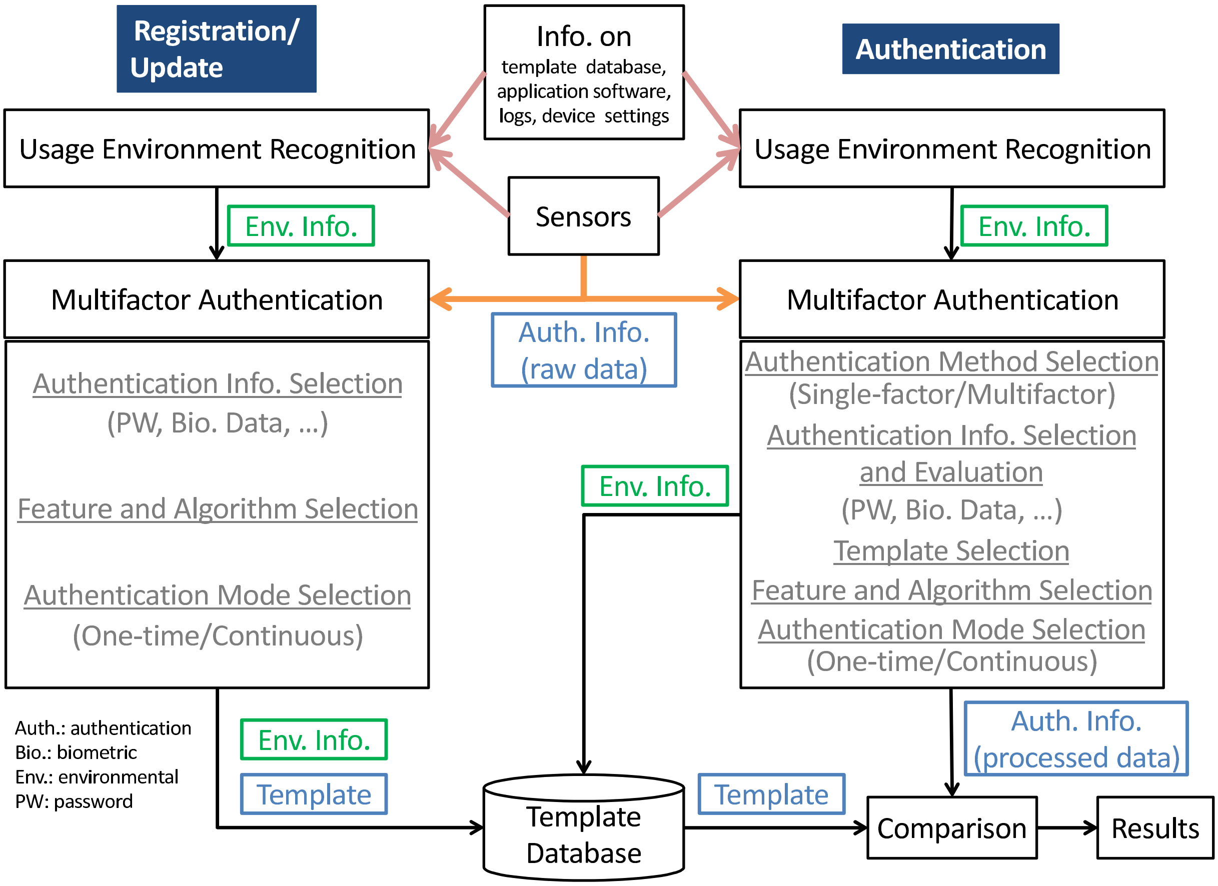
Registration/ Update
Info. on
template database, application software, logs, device settings
Authentication
Usage Environment Recognition
Sensors
Usage Environment Recognition
Env. Info.
Env. Info.
Multifactor Authentication
Multifactor Authentication
Auth. Info. (raw data)
Authentication Info. Selection
(PW, Bio. Data, ...)
Feature and Algorithm Selection
Authentication Mode Selection
(One-time/Continuous)
Authentication Method Selection
(Single-factor/Multifactor)
Authentication Info. Selection and Evaluation
(PW, Bio. Data, ...)
Template Selection
Feature and Algorithm Selection
Authentication Mode Selection
(One-time/Continuous)
Env. Info.
Auth.: authentication
Bio.: biometric
Env.: environmental
PW: password
Env. Info.
Template
Template Database
Template
Auth. Info. (processed data)
Comparison
Results

Fig. 2 Context-awareness-based multifactor authentication system

In the proposed method, the registration/update process and authentication process are conducted by using environmental information that is generated by using the above function of usage environment recognition.

In the registration/update process, authentication information is selected and input, and templates are registered or updated. In this paper, we call such information that is input by a user and used for authentication "authentication information." A password or a piece of biometric data are both examples of authentication information. Moreover, authentication information, especially that for registration in a template database, is called a "template." In the initial registration, a user inputs his/her authentication information, the type of which is selected by the system on the basis of the environmental information. The system registers both the template and the corresponding environmental information in the template database. For example, when the type of authentication information is a face image, the extracted features of a user's face image are regarded as a template, and the measurement value of the illuminance around the system at the moment the face image is input is regarded as the environmental information. Here, it should be noted that when the type of authentication information is biometric data, the feature and the algorithms of preprocessing and feature extraction are also selected on the basis of the environmental information with a view toward enhancing the verification accuracy. After the initial registration, the user conducts an additional registration and update of templates upon notification by the system when the system decides that those are necessary on the basis of the result of recognizing the usage environment. As mentioned above, the system requests the user to input the least amount of authentication information during the initial registration and also requests him/her to add and update the templates on a timely basis in the process of using the system, which avoids degrading convenience by letting the user input all the authentication information at the same time.

In the authentication process, authentication information is selected and input, then the information and templates are compared. First, on the basis of the result of recognizing the usage environment, the system selects the authentication method. In this process, the system decides on either single-factor authentication, which uses a single kind of authentication information, or multifactor authentication, which uses multiple different kinds of authentication information. Moreover, in the case of multifactor authentication, the system also evaluates the types and reliability (weights) of the authentication information used. With these mechanisms, the system tries to keep the authentication accuracy high in various usage environments and optimize the amount of authentication information needed. Next, the user sequentially inputs the authentication information that was requested by the system, and the system selects the optimal template that corresponds to the most similar environmental information from the template database with a view toward enhancing the verification accuracy and outputs the authentication results by comparing the authentication information with the selected template.

Furthermore, the proposed system can be operated in a continuous authentication mode [3] as well as a conventional one-time authentication mode. Currently, most smart devices employ a one-time user authentication scheme in which an authentication system only authenticates a user when he/she tries to login or unlock the device. However, this scheme is not always good enough for securing smart devices when we consider that various kinds of data concerning user privacy are frequently processed within them. To overcome this problem, many continuous authentication methods that continuously authenticate a user the entire time that the user is operating a device have been proposed [3]. In continuous authentication, acquiring authentication information while the user is unaware is a key requirement; however, in the case of smart devices, this is often difficult due to the variation in usage environments, which causes the verification accuracy to degrade. To address this problem, we tried to extend our former system to be able to conduct continuous authentication with a view toward enhancing the verification accuracy by using the function of usage environment recognition [19].

4. Experiments

In this section, we present our evaluation of the performance of the proposed system, especially focusing on the effectiveness of recognizing the usage environment in terms of context awareness.

4.1 Template Selection

First, we evaluated the effectiveness of selecting an appropriate template on the basis of the result of recognizing the usage environment. In this subsection, we briefly quote our main results described in [7]. In the experiment, we regarded face, signature, and voice, which can be acquired with most smart devices, as authentication information and assumed that such templates that correspond to different usage environments have already been registered along with environmental information in the template database shown in Fig.2. Moreover, the system selects the template that corresponds to the most similar environmental information and compares the authentication information with the selected template. Table 1 lists the experimental conditions, and Table 2 lists the usage environments we evaluated.

Table 3 lists the verification accuracies of multifactor authentication in various usage environments. The left part of the table shows the combination of usage environments used in the authentication process. The right part shows the verification accuracies in terms of the equal error rate (EER). Both shown in the same table are the EER with and without usage environment recognition and the EER with a weight that corresponds to the verification accuracy in a certain modality. The best cases (No.1–No.5) and the worst (No.6–No.10) in terms of EER are extracted from all of the

Table 1 Experimental conditions 1

	Face auth.	Writer auth.	Speaker auth.
Device	Apple iPad Air, MD789J/A		
# of subjects	10		
Specification	Face image from front	Japanese signature	Japanese speech
Input means	Built-in camera (1.2 Mpixel)	Finger (200 Hz, 0.01 mm)	Built-in mic. (44.1 kHz, 16 bit)
Features	LBP [20], ILBP [21]	(x,y) time series, # of pen-ups	MFCC [22]
Comparison	Bhattacharyya distance	DTW [23], Δ # of pen-ups	Euclidean distance
# of intrap. comparison	150		
# of interp. comparison	1620		
Fusion	Z-score		

auth.: authentication, mic.: microphone
LBP: local binary pattern, ILBP: improved LBP
MFCC: mel-frequency cepstrum coefficients, DTW: dynamic time warping
intrap.: intrapersonal, interp.: interpersonal, Δ: difference

Table 2 Usage environments 1

Face authentication	
• Illumination	
Bright room (B)	Illuminance: 850 ± 10 lx
Semi-dark room (S)	Illuminance: 80 ± 10 lx
Dark room (D)	Illuminance: 15 ± 5 lx
• Holding state of device	
Perpendicular (P)	Getting image of face from front
Natural (N)	Getting image of face from below
Writer authentication	
• Writing time	
Usual (U)	Usual writing time
Fast (F)	$\frac{2}{3}$usual writing time
Very fast (V)	$\frac{1}{2}$usual writing time
• Holding state of device	
Put on desk (Pu)	Writing at desk
Held in hand (He)	Writing while standing
Speaker authentication	
• Location of use	
Anechoic chamber (AC)	
Bus, SNR = 10 dB (Bu10)	Using on bus
Bus, SNR = 20 dB (Bu20)	Using on bus
Station, SNR = 10 dB (St10)	Using at station
Station, SNR = 20 dB (St20)	Using at station

Table 3 Verification accuracy of multifactor authentication

Usage environment				EER (%)		
No.	Face	Writer	Speaker	W/o recog.	With recog.	With weight
1	BP	HeV	AC	0.00	1.38	0.00
2	BP	PuU	Bu20	0.00	1.38	0.00
3	BP	HeU	St20	0.00	1.35	0.06
4	BP	PuV	Bu10	0.00	1.35	0.00
5	BP	PuF	Bu20	0.00	1.35	0.00
6	DN	PuF	St10	26.39	1.31	0.00
7	DN	HeF	St10	27.28	1.35	0.00
8	DN	HeV	St10	27.52	1.35	0.00
9	DN	PuV	St10	28.20	1.31	0.00
10	DP	HeV	St10	27.92	0.12	0.00
Avg. of all 180 environments				9.90	0.72	0.09
Max. of all 180 environments				28.20	2.72	1.44
Min. of all 180 environments				0.00	0.00	0.00

recog.: recognition

results. As shown, the proposed system improved the verification accuracy by selecting an appropriate template and weighting on the basis of using the function of environment recognition.

4.2 Feature/Algorithm Selection

Next, we evaluated the effectiveness of selecting an appropriate feature and algorithm on the basis of the result of recognizing the usage environment. As clarified in the former subsection, selecting an appropriate template improves the verification accuracy; however, more improvement can be expected by selecting an appropriate feature and algorithm on the basis of the recognition result. In this subsection, we briefly quote our main results described in [24]. The following was clarified from preliminary experiments. For face authentication, there was a tendency for the verification accuracy to be high when using the local binary pattern (LBP) [20] as the feature under the condition that there exist some templates that were generated in a similar usage environment. In contrast, the verification accuracy was high when using an improved LBP (ILBP) [21] as the feature under the condition that there exists no template that was generated in a similar usage environment. Since ILBP can further emphasize the edges of an image compared with LBP, it is considered that the verification accuracy was high when the difference in luminance between two images was large, and the verification accuracy was low when the difference in luminance was small. Therefore, in the experiment, we calculated the difference in luminance between a template and a piece of authentication information input in the authentication process, and we used LBP when the difference was not greater than 0.1, or we otherwise used ILBP. In comparison, in speaker authentication, there was a tendency for the verification accuracy to be improved when spectral subtraction (SS) [25], which is a typical method for noise reduction in speech engineering, was applied to speech data including human voice as background noises. Therefore, in the experiment, we calculated the rate of spectral intensity ranging from 0.4 to 4 kHz, which corresponds to the voice frequency band. We used SS when the rate was not less than 0.2; otherwise, we did not apply noise reduction. In the experiment, we regarded face and voice as authentication information. Table 4 lists the experimental conditions, and Table 5 lists the usage environments we evaluated. As shown in the table, there existed a combination of usage environments, such as “bright room” and “dark room,” whose luminances were quite different, and also some usage environments, such as “station square” and “department store,” which included human voice as background noises.

Table 6 lists the verification accuracies of authentication with feature/algorithm selection in terms of the EER averaged over different usage environments. As shown in the table, the proposed system improved the verification accuracy by selecting an appropriate feature and algorithm on the basis of environment recognition.

Table 4 Experimental conditions 2

	Face authentication	Speaker authentication
Device	Apple iPad Air, MD789J/A	
# of subjects	10	
Specification	Face image from front	Japanese speech
Input means	Built-in camera (1.2 Mpixel)	Built-in microphone (44.1 kHz, 16 bit)
Features	LBP, ILBP	MFCC
Comparison	Bhattacharyya distance	Euclidean distance
# of intrap. comparison	150	90
# of interp. comparison	1620	810

Table 5 Usage environments 2

Face authentication	
• Illumination	
Bright room (B)	Illuminance: 725 ± 95 lx
Semi-dark room (S)	Illuminance: 344 ± 64 lx
Dark room (D)	Illuminance: 14 ± 6 lx
Speaker authentication	
• Location of use	
Anechoic chamber (AC)	
Car, SNR = 5, 10, 20 dB (Ca)	Using in car
Construction site, SNR = 5, 10, 20 dB (Co)	Using around construction site
Station square, SNR = 5, 10, 20 dB (St)	Using near station square
Department store, SNR = 5, 10, 20 dB (De)	Using in department store

Table 6 Verification accuracy of authentication with feature/algorithm selection

Modality	Feature/algorithm	EER (%)
Face	LBP (fixed)	16.1
	ILBP (fixed)	8.4
	proposal	7.5
Voice	w/o noise reduction (fixed)	8.1
	SS (fixed)	8.2
	proposal	6.8

4.3 Continuous Authentication

Finally, we evaluated the possibility of continuous authentication on the basis of the result of recognizing the usage environment. In this subsection, we briefly quote our main results described in [19]. In the experiment, we regarded face, flick operation, and voice as authentication information. Table 7 lists the experimental conditions, and Table 8 lists the usage environments we evaluated. The biometric data in Table 7 were collected in a manner much similar to a real continuous authentication scenario.

Table 9 lists the recognition and verification accuracies for continuous authentication under various usage environments. For face authentication, the recognition rate was the highest when a user was standing and holding the device naturally and the lowest when the user was sitting and placing the device on the desk. Apparently, one of the reasons for the former case being outperformed lies in the distance between the face and the device. In the former case, the distance was large to some extent, which enabled a whole face image to be captured clearly. In the latter case, however, the distance was small in some cases, which lead to failure in capturing the whole face image. These results suggest that, if the system recognizes the behavioral user state and

Table 7 Experimental conditions 3

	Face auth.	Writer auth.	Speaker auth.
Device	Asus Zenfone 2 Laser	Arrows NX F-04G	Asus Zenfone 2 Laser
# of subjects	10		
Specification	Face image from front (6 times every 2 sec.)	Flick operation (10 times upward)	Japanese speech (6 times, $\sim$2.4 sec. per sentence)
Sensor	Built-in camera (5.0 Mpixel)	Touch panel (1440 × 2560 pixels)	Built-in mic. (44.1 kHz, 16 bit)
Features	LBP, ILBP	Features in [26]	MFCC
Comparison	Bhattacharyya distance	Normalized Euclidean distance	Euclidean distance
# of intrap. comparison	90	150	360
# of interp. comparison	540	3240	3240

Table 8 Usage environments 3

Face authentication	
• Holding state of device	
Sitting (Si)	Sitting and holding naturally
Placing (Pl)	Sitting and placing on desk
Standing (St)	Standing and holding naturally
Walking (Wa)	Walking and holding naturally
Writer authentication	
• Application software information	
WWW browser (W)	Browsing web pages
Photo viewer (P)	Browsing photos
Speaker authentication	
• Holding state of device	
Sitting (Si)	Sitting and holding naturally
Walking (Wa)	Walking and holding naturally

Table 9 Recognition/verification accuracy for continuous authentication

Modality	Environment	Performance	
		Recog. rate (%)	EER (%)
Face	Si	71.7	—
	Pl	35.0	—
	St	88.3	—
	Wa	75.0	—
Flick	W	—	8.0
	P	—	4.6
Voice	Si	—	14.9
	Wa	—	20.2

selects a stable usage environment, such as (St) in Table 8, by using the function of usage environment recognition, the verification performance is expected to be improved. For writer authentication, the verification accuracy was higher when a user was browsing photos than when the user was browsing web pages. We believe that this is because the flick operation is prone to being more constant and stable in photo browsing than in web browsing because the types of content are different; the former contains only photos, and the latter contains various kinds of characters and pictures, which may further affect the finger movement of the user. These results also suggest that, if the system acquires information on application software being used and selects a stable usage environment, such as (P) in Table 8, by using the function of usage environment recognition, the verification performance is expected to be improved. For speaker authentication, the verification accuracy was more degraded when a user was walking than when the user was sitting. The reason is considered to be that stable collection of voice was difficult when the user was walking due to the oscillation of the device. Again, these results suggest that, if the system recognizes the behavioral user state and selects a stable usage environment, such as (Si) in Table 8, by using the function of usage environment recognition, the verification performance is expected to be improved.

5. Conclusion

In this paper, we summarized the current problems with user authentication on smart devices and proposed a novel user authentication system based on the concept of context awareness to address these problems. We also presented our evaluation of the performance of the system by using biometric information that was acquired from smart devices. The evaluation demonstrated the effectiveness of our system. The full realization of a context-awareness-based multifactor authentication system that satisfies all the requirements described in the first section will be our principal area of study.

Acknowledgments

Part of this work was supported by JSPS KAKENHI Grant Number JP16K00190. The authors would like to thank the laboratory students for their support.

References

[1] T. Barnett Jr., A. Sumits, T. Khurana, U. Andra, and R. Pepper, "Cisco visual networking index: Global mobile data traffic forecast update, 2015–2020," Cisco Public, 2016.

[2] L.M. Mayron, "Biometric authentication on mobile devices," IEEE Security & Privacy, vol.13, no.3, pp.70–73, 2015.

[3] V.M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices — Recent progress and remaining challenges," IEEE Signal Process. Mag., vol.33, no.4, pp.49–61, 2016.

[4] S. Onoda, Y. Goubaru, and Y. Yamazaki, "A study on the performance of a mobile terminal-based signature verification system under different writing environments (in Japanese)," IEICE Trans. Fundamentals (Japanese Edition), vol.J98-A, no.12, pp.664–667, 2015.

[5] K. Nandakumar and A.K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," IEEE Signal Process. Mag., vol.32, no.5, pp.88–100, 2015.

[6] R. Okabe, T. Higashi, Y. Yamazaki, and T. Ohki, "A smart device-based multifactor authentication system based on context awareness (in Japanese)," IEICE Technical Report, BioX2015-47, pp.37–42, 2016.

[7] R. Okabe, T. Higashi, Y. Yamazaki, and T. Ohki, "A study for a context awareness-based multifactor authentication system using smart devices (in Japanese)," IEICE Trans. Fundamentals (Japanese Edition), vol.J99-A, no.12, pp.467–470, 2016.

[8] B. Schilit, N. Adams, and R. Want, "Context-aware computing applications," IEEE Workshop on Mobile Computing Systems and Applications, pp.85–90, 1994.

[9] P.J. Brown, J.D. Bovey, and X. Chen, "Context-aware applications: From the laboratory to the marketplace," IEEE Pers. Commun., vol.4, no.5, pp.58–64, 1997.

[10] N. Ryan, J. Pascoe, and D. Morse, "Enhanced reality fieldwork: The

context-aware archaeological assistant," Computer Applications in Archeology, 1997.

[11] A.K. Dey and G.D. Abowd, "Towards a better understanding of context and context-awareness," Workshop on the What, Who, Where, When, and How of Context-Awareness, as part of the 2000 Conference on Human Factors in Computing Systems (CHI 2000), 2000.

[12] G. Chen and K. David, "A survey of context-aware mobile computing research," Dartmouth Computer Science Technical Report, TR2000-381, 2000.

[13] E. Vildjiounaite, S.M. Mäkelä, M. Lindholm, R. Riihimäki, V. Kyllönen, J. Mäntyjärvi, and H. Ailisto, "Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices," 4th Intl. Conf. on Pervasive Comput., pp.187–201, 2006.

[14] J.R. Kwapisz, G.M. Weiss, and S.A. Moore, "Cell phone-based biometric identification," 2010 Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), pp.1–7, 2010.

[15] T. Kobayashi, K. Hasida, and N. Otsu, "Rotation invariant feature extraction from 3-D acceleration signals," 2011 IEEE Intl. Conf. on Acoustics, Speech, Signal Process. (ICASSP), pp.3684–3687, 2011.

[16] J.X. Felix, C. Bhagavatula, A. Jaech, U. Prasad, and M. Savvides, "Gait-id on the move: Pace independent human identification using cell phone accelerometer dynamics," 2012 Fifth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), pp.8–15, 2012.

[17] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, "CASA: Context-aware scalable authentication," Symposium on Usable Privacy and Security (SOUPS) 2013, pp.1–10, 2013.

[18] A. Primo, V.V. Phoha, R. Kumar, and A. Serwadda, "Context-aware active authentication using smartphone accelerometer measurements, CVPR 2014, pp.98–105, 2014.

[19] T. Higashi, T. Agawa, R. Okabe, Y. Yamazaki, and T. Ohki, "A study on continuous user authentication for smart devices considering usage environment (in Japanese)," SCIS2017, 3D4-2, 2017.

[20] T. Ojala, M. Pietikäinen, and D. Harwood, "A comparative study of texture measures with classification based on feature distributions," Pattern Recognit., vol.29, no.1, pp.51–59, 1996.

[21] H. Jin, Q. Liu, H. Lu, and X. Tong, "Face detection using improved LBP under Bayesian framework," Proc. Third International Conference on Image and Graphics (ICIG'04), pp.306–309, 2004.

[22] L. Rabiner and B.H. Juang, "Fundamentals of speech recognition," Prentice Hall, 1993.

[23] H. Sakoe and S. Chiba, "Dynamic programming algorithm optimization for spoken word recognition," IEEE Trans. Acoust., Speech, Signal Process., vol.26, no.1, pp.43–49, 1978.

[24] T. Higashi, R. Okabe, Y. Yamazaki, and T. Ohki, "A study on improving authentication accuracy for a multifactor authentication system considering usage environment (in Japanese)," IEICE Technical Report, BioX2016-29, pp.67–72, 2016.

[25] S. Boll, "Suppression of acoustic noise in speech using spectral subtraction," IEEE Trans. Acoust., Speech, Signal Process., vol.27, no.2, pp.113–120, 1979.

[26] Y. Matsubara, H. Nishimura, T. Samura, H. Yoshimoto, and R. Tanimoto, "A new biometrics technique with flick operation on electronic device (in Japanese)," IEICE Technical Report, BioX2015-39, pp.91–96, 2015.

Yasushi Yamazaki received the BE and ME degrees in electronics and communication engineering from Waseda University, Tokyo, Japan, in 1993 and 1995, respectively, and the PhD degree in electronics, information and communication engineering from Waseda University in 1998. He is currently an associate professor in the Department of Information and Media Engineering at the University of Kitakyushu, Fukuoka, Japan. His research interests include biometrics, information security, and pattern recognition.

Tetsushi Ohki received the BE and ME degrees in electronics and communication engineering from Waseda University, Tokyo, Japan, in 2002 and 2004, respectively, and the PhD degree in engineering from Waseda University in 2010. He is currently a lecturer in the Faculty of Informatics, Shizuoka University, Japan. His research interests include biometrics, pattern recognition, information security and privacy.