Journal of Robotics, Networking and Artificial Life, Vol. 2, No. 1 (June 2015), 60-63

An Authentication Method Independent of Tap Operation on the Touchscreen of a Mobile Device

[1]Hisaaki Yamaba, [1]So Nagatomo, [2]Kentaro Aburada, [1]Shinichiro Kubota, [1]Tetsuro Katayama, [3]Mirang Park, [1]Naonobu Okazaki

[1]University of Miyazaki, 1-1, Gakuen-kibanadai nishi, Miyazaki, 889-2192, Japan

[2]Oita National College of Technology, 1666, Maki, Oita, 870-015, Japan

[3]Kanagawa Institute of Technology, 1030, Shimo-ogino, Atsugi, Kanagawa, 243-0292, Japan

yamaba@cs.miyazaki-u.ac.jp, hf11036@student.cs.miyazaki-u.ac.jp,

aburada@oita-ct.ac.jp, kubota@cs.miyazaki-u.ac.jp, kat@cs.miyazaki-u.ac.jp,

mirang@nw.kanagawa-it.ac.jp, oka@cs.miyazaki-u.ac.jp

Abstract

At the present time, mobile devices such as tablet-type PCs and smart phones have widely penetrated into our daily lives. Therefore, an authentication method that prevents shoulder surfing is needed. We are investigating a new user authentication method for mobile devices that uses surface electromyogram (s-EMG) signals, not screen touching. The s-EMG signals, which are generated by the electrical activity of muscle fibers during contraction, are detected over the skin surface. Muscle movement can be differentiated by analyzing the s-EMG. In this paper, a series of experiments was carried out to investigate the prospect of an authentication method using s-EMGs. Specifically, several gestures of the wrist were introduced, and the s-EMGs generated for each motion pattern were measured. We compared the s-EMG patterns generated by each subject with the patterns generated by other subjects. As a result, it was found that each subject has similar patterns that are different from those of other subjects. Thus, s-EMGs can be used to confirm one's identification for authenticating passwords on touchscreen devices.

Keywords: mobile device, user authentication, shoulder surfing, electromyogram.

1. Introduction

This paper proposes a new user authentication method for mobile devices by using surface electromyogram (s-EMG) signals, not screen touching.

At the present time, mobile devices such as tablet type PCs and smart phones have widely penetrated into our daily lives. Therefore, an authentication method that prevents shoulder surfing is needed. Shoulder surfing is the direct observation of a user's personal information, such as passwords. Authentication operations on mobile devices are performed in many public places, so we have to ensure that no one can view our passwords. But it is not an easy task. Many mobile devices have no keyboards, so the authentication method must use a touchscreen. When using a touchscreen, the owner of the mobile device inputs his or her authentication information through simple or multi-touch gestures. These gestures include, for example, designating his/her passcode from displayed numbers, selecting registered pictures or icons from a set, or tracing a registered one-

Published by Atlantis Press

stroke sketch on the screen. People positioned close to the mobile device owner can easily grasp these actions and obtain the user's authentication information.

The s-EMG signals, which are generated by the electrical activity of muscle fibers during contraction, are detected over the skin surface. These s-EMGs have been used to control various devices, including artificial limbs and electrical wheelchairs. Muscle movement can be differentiated by analyzing the s-EMG[1]. For example, fast Fourier transform (FFT) can be adopted for the analysis. Feature extraction is carried out through the analysis of the s-EMGs. The extracted features are used to differentiate the muscle movement, including hand gestures.

In this paper, a series of experiments was carried out to investigate the prospect of realizing an authentication method using s-EMGs. Specifically, several gestures of the wrist were introduced, and the s-EMG signals generated for each motion pattern were measured. We compared the s-EMG signal patterns generated by each subject with the patterns generated by other subjects. As a result, it was found that the patterns of each individual subject are similar but they differ from those of other subjects. From these results, it is expected that s-EMGs is used to confirm one's identification for authenticating passwords on touchscreen devices.

2. Characteristics of authentication method for mobile devices

User authentication of mobile devices has two characteristics.

One is that an authentication often takes place around strangers. An authentication operation is performed whenever a user wants to start using their mobile devices. Therefore, the strangers around the user can possibly see the user's unlock actions. Some of these strangers may scheme to steal information such as passwords for authentication.

The other characteristic is that much user authentication of mobile devices is now performed on a touchscreen. Many current mobile devices do not have hardware keyboards, and so it is not easy to input long strings into such mobile devices. When users unlock mobile touchscreen devices, they input passwords or personal identification numbers (PINs) by tapping numbers or characters displayed on the touchscreen. In many cases, the user moves only one finger. Since users have to look at their touchscreens while unlocking their devices, strangers around them can easily see the unlock actions, and so it becomes very easy for such strangers to steal passwords or PINs.

To prevent shoulder-surfing attacks, many studies have been conducted. The secret tap method introduces a shift value to avoid revealing pass-icons[2]. The user may tap other icons in the shift position on the touchscreen, as indicated by a shift value, to unlock the device. By keeping the shift value secret, people around the user cannot know the pass-icons, although they can still watch the tapping operation. The rhythm authentication method relieves the user from looking at the touchscreen when unlocking the device[3]. In this method, the user taps the rhythm of his or her favorite music on the touchscreen. The pattern of tapping is used as the password. In this situation, the users can unlock their devices while keeping them in their pockets or bags, and the people around them cannot see the tap operations that contain the authentication information.

3. Surface electromyogram signals

The s-EMG signals are detected over the skin surface and are generated by the electrical activity of muscle fibers during contraction. Muscle movement can be differentiated by analyzing the s-EMG. Usually, FFT is adopted for the analysis, and feature extraction is carried out through analysis of the s-EMG.

However, since measured s-EMG signals vary by subject, the extracted features do not show enough performance to correctly differentiate the muscle movement in multiple subjects. Therefore, researchers have explored other methods to improve the performance of feature extraction. Since some methods demonstrate good performance for some subjects but other methods show better performance for other subjects, a feature that can be used to distinguish gestures for everyone is desired. For example, a method that uses the maximum value and the minimum value of raw s-EMG signals was proposed[4].

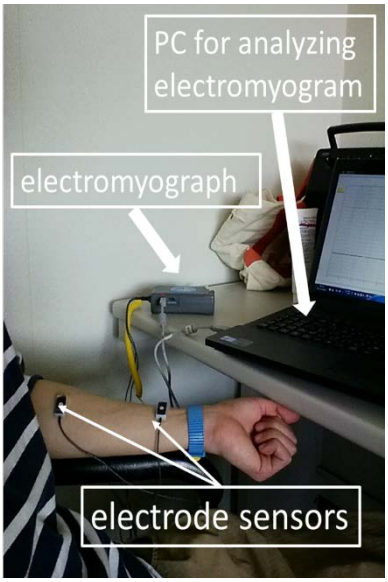

Figure 1 Experimental System

4. User authentication using s-EMG

In this section, the method of user authentication by using s-EMGs, which do not require looking at a touchscreen, is presented.

The s-EMG signals are measured, and the features of the measured raw signals are extracted. We estimate gestures of a user of a mobile device from the extracted features. Next, combinations of the gestures are converted into a code for authentication. These combinations are inputted into the mobile device and used as a password for user authentication.

Adopting s-EMGs for authentication of mobile devices has two advantages. First, the user does not have to look at his/her device. Since the user can make a gesture that is used as a password on a device inside a pocket or in a bag, it is expected that the authentication information can be concealed. No one can see what gesture is made. In addition, it is expected that if another person reproduces a sequence of gestures that a user has made, the authentication will not be successful, because the extracted features from the s-EMG signals are usually not the same between two people.

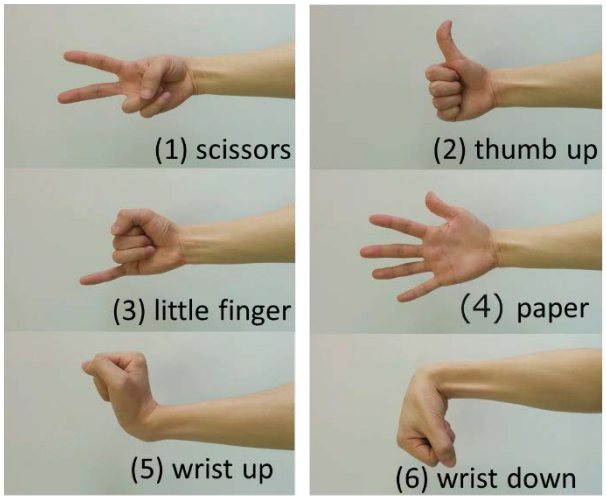

Figure 2 Gestures used in the experiments

5. Experiments

A series of experiments was carried out to investigate the prospect of the authentication method using s-EMGs. Specifically, we investigated whether the measured s-EMG signals of one experimental subject were similar and whether the signals of different subjects were different from each other.

Figure 1 shows the experimental system used in these experiments. An electromyograph measured the s-EMG of each movement pattern with two electrode sensors. The measured data were stored and analyzed on a PC. Ten healthy persons whose ages were in the twenties (students of University of Miyazaki) participated as experimental subjects (Subjects A–J). The six hand gestures (1–6) shown in Figure 2 were introduced in the experiments. First, each subject made each gesture ten times in succession and their s-EMG signals were recorded (Exp. #1). Approximately one week later, the same experiment was carried out again (Exp. #2).

Some of the results are shown in Figure 3. The raw s-EMG signals of gesture 1 made by experimental subjects A and B are displayed. The signals of Exp. #1 and #2 are similar for each subject. On the other hand, the signals of subjects A and B are not similar to those

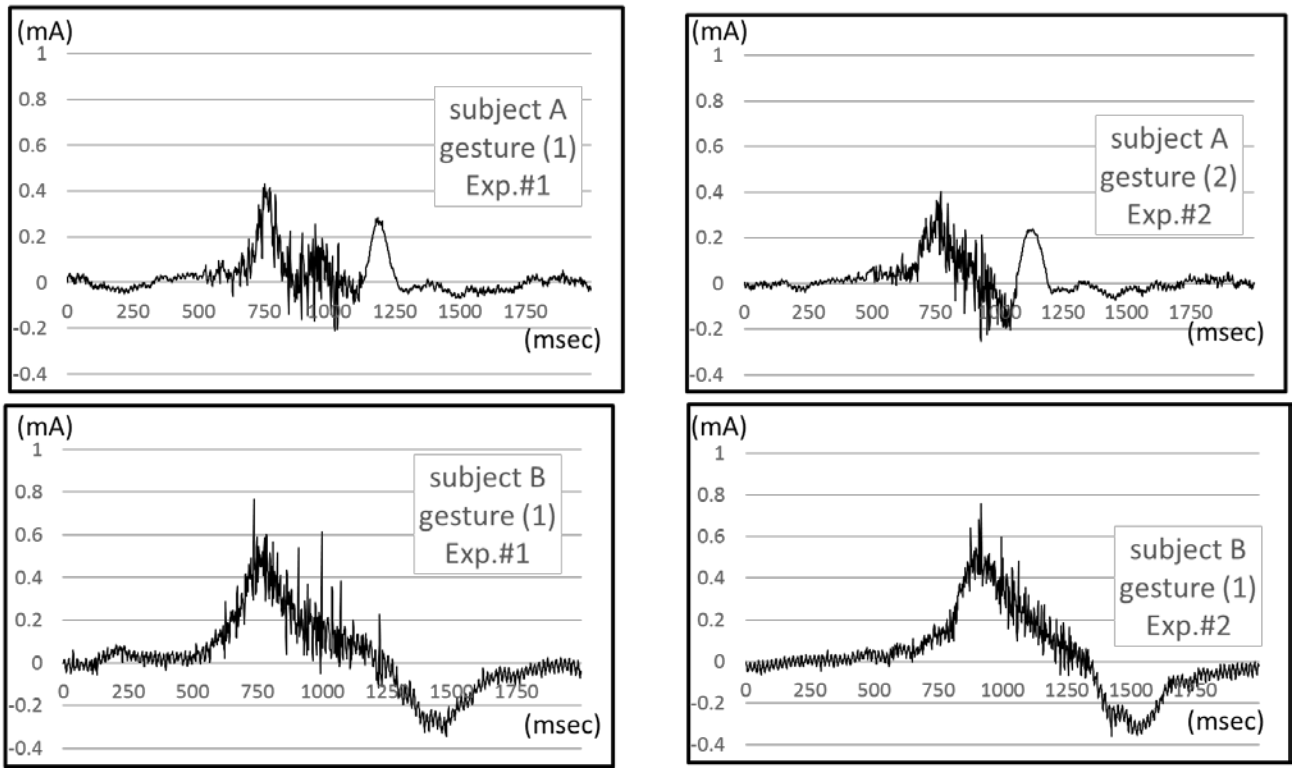

Figure 3 Obtained s-EMG signals

of the other subject. The same results were obtained for every pair of subjects and all gestures.

These results show that the s-EMG is promising as identification input for a new user authentication method.

6. Conclusion

We investigated a new user authentication method that can prevent shoulder-surfing attacks in mobile devices. We know that the unlocking operations of mobile devices such as tablet-type PCs or smart phones can often be viewed by other people. Users can hide such operations from others by not looking at the touchscreen of a mobile device while unlocking it. To realize such an authentication method, we assigned a set of gestures to obtain the s-EMG signals. A series of experiments was carried out to confirm that the s-EMG signals of each person are similar for that person and the signals of different people are not similar to other people's signals. These results showed that s-EMG signals can be used as input for a new user authentication method. We will conduct a quantitative evaluation of this approach in future work.

Acknowledgements

Useful advice and the experiment system were offered by Prof. K. Tanno, Prof. H. Tamura and Mr. K. Nagatomo of University of Miyazaki.

References

1. H. Tamura, et al., A study on motion recognition without FFT from surface-EMG, IEICE-part D, J90-D(9), (2007) 2652-2655.
2. Y. Kita, et al., Implementation and evaluation of shoulder-surfing attack resistant users (In Japanese), IEICE-part D, J97-D(12), (2014) 1770-1784.
3. Y. Kita, et al., A Study of Rhythm Authentication and its Accuracy using the Self-Organizing Maps (In Japanese), Proceedings of DICOMO 2014, (2014) 1011-1018.
4. H. Tamura, et al., A study on the s-EMG pattern recognition using neural network, IJICIC, 5(12) (2009) 4877-4884.