Artif Life Robotics (2017) 22:108–112
DOI 10.1007/s10015-016-0323-4

ORIGINAL ARTICLE

Evaluation of feature values of surface electromyograms for user authentication on mobile devices

Hisaaki Yamaba[1] · Akitoshi Kurogi[1] · Shin-Ichiro Kubota[1] · Tetsuro Katayama[1] · Mirang Park[2] · Naonobu Okazaki[1]

Received: 11 April 2016 / Accepted: 17 August 2016 / Published online: 19 September 2016

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 use 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 method that uses a list of gestures as a password is proposed. And also, results of experiments are presented that was carried out to investigate the performance of the method extracting feature values from s-EMG signals (using the Fourier transform) adopted in this research. *Myo*^{TM}, which is the candidate of s-EMG measurement device used in a prototype system for future substantiative experiments, was used in the experiment together with the s-EMG measuring device used in the previous research to investigate its performance.

Keywords Mobile device · User authentication · Shoulder surfing · S-EMG

This work was presented in part at the 21st International Symposium on Artificial Life and Robotics, Beppu, Oita, January 20-22, 2016.

✉ Hisaaki Yamaba
yamaba@cs.miyazaki-u.ac.jp

[1] University of Miyazaki, 1-1, Gakuen Kibanadai-nishi, Miyazaki, Japan

[2] Kanagawa Institute of Technology, 1030, Shimo-ogino, Atsugi, Kanagawa, Japan

1 Introduction

This paper proposes a new user authentication method for mobile devices 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. However, 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-stroke sketch on the screen. People positioned close to the owner of the mobile device 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]. Feature extraction is carried out through the analysis of the s-EMGs. For example, fast Fourier transform (FFT) can be adopted for the analysis. The extracted features are used to differentiate the muscle movement, including hand gestures.

In the previous research [2], we investigate the prospect of realizing an authentication method using s-EMGs through a series of experiments. Specifically, several

gestures of the wrist were introduced, and the s-EMG signals generated for each of the motion patterns were measured. In the research [2], 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. Thus, s-EMGs can confirm one's identification for authenticating passwords on touchscreen devices. We listed the problems to be solved in the paper as follows:

1. Collecting more and more data from subjects of various ages.
2. Proposing a concrete method for user authentication using s-EMG.
3. Exploring a feature value to identify users using a computer program.
4. Measuring s-EMG signals from subjects under various conditions.
5. Developing a prototype system to evaluate the performance of the proposed method under various conditions.

In this paper, 2, 3, and 5 are mainly intended. First, a method that uses a list of gestures as a password is proposed. Next, the results of experiments are presented that were carried out to investigate the performance of the method extracting feature values from s-EMG signals (using the Fourier transform) adopted in this research. *Myo*^{TM}, which is a candidate of a device to measure s-EMG signals used in a prototype system for future substantiative experiments, was used together with the s-EMG measuring device used in the previous research to investigate its performance.

2 Characteristics of authentication method for mobile devices

User authentication of mobile devices has two characteristics.

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

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 thieves to steal passwords or PINs.

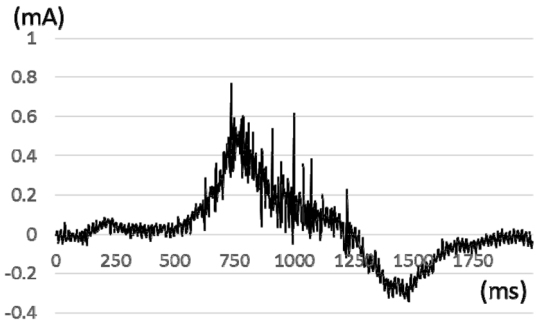


Fig. 1 Sample of an s-EMG signal

To prevent shoulder-surfing attacks, many studies have been conducted. The secret tap method [3] introduces a shift value to avoid revealing pass-icons. 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 [4] relieves the user from looking at the touchscreen when unlocking the device. 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 (Fig. 1) are generated by the electrical activity of muscle fibers during contraction and are detected over the skin surface (Fig. 2). Muscle movement can be differentiated by analyzing the s-EMG. Usually, FFT is adopted for the analysis, and feature extraction is carried out through the 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

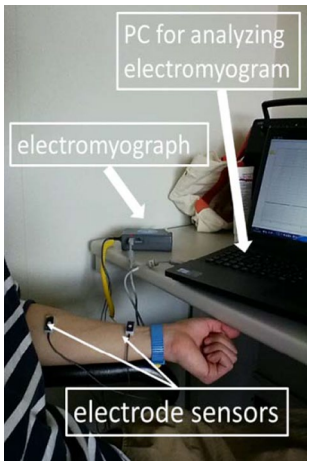


Fig. 2 Measuring an s-EMG signal

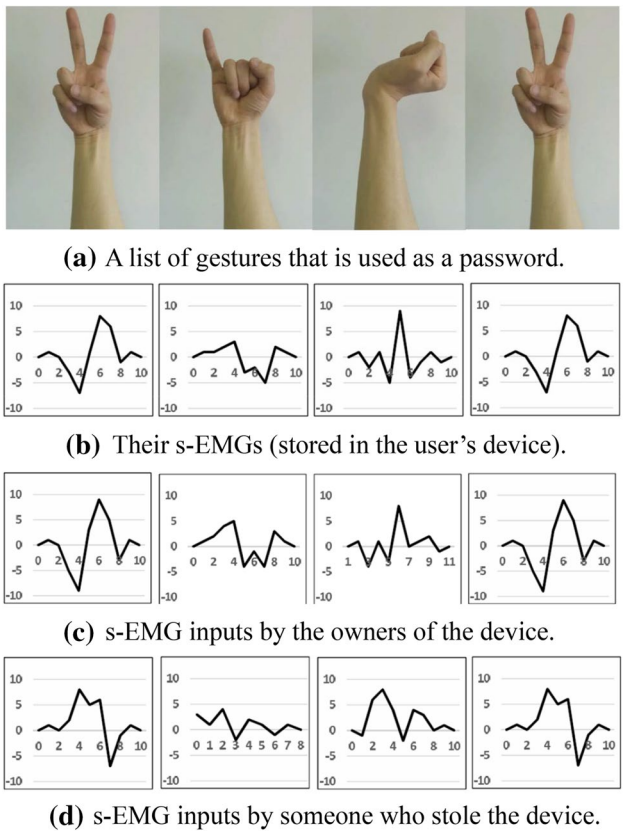
distinguish gestures for everyone is desired. For example, a method that uses the maximum value and the minimum value of raw s-EMG signals was proposed [5].

4 User authentication using s-EMG

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

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

1. At first, pass-gesture registration is carried out. A user selects a list of gestures that is used as a pass-gesture. (Fig. 3a)
2. The user measures s-EMG of each gesture, extracts their feature values, and registers the values into his mobile device. (Fig. 3b)
3. When the user tries to unlock the mobile device, the user makes his pass-gesture and measures the s-EMG.
4. The measured signals are sent to his mobile device.
5. The device analyzes the signals and extracts the feature values.
6. The values are compared with the registered values.
7. If they match, the user authentication will succeed. (Fig. 3c)
8. On the other hand, an illegal user authentication will fail, because a list of signals given by someone who stole the device (Fig. 3d) will not be similar with the registered one.



(a) A list of gestures that is used as a password.

(b) Their s-EMGs (stored in the user's device).

(c) s-EMG inputs by the owners of the device.

(d) s-EMG inputs by someone who stole the device.

Fig. 3 List of gestures used as a password

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.

One of the advantages of our method using an s-EMG signal against other biometrics based methods, such as a fingerprints, an iris, and so on, is that a user can change the list of gestures. When authentication information, a fingerprint or an iris, come out, the user cannot use them, because he/she cannot change his/her fingerprint or iris. However, the user can arrange his/her gesture list again and use the new gesture list.

5 Prototype authentication system

To verify the validity of the proposed method, a prototype system for experimental use is very useful. The authors are

Fig. 4 Myo^{TM} (quoted from http://store.myo.com/)

planning to develop such a system by assembling devices that are easy to get.

Myo^{TM} (Fig. 4) is one of the most promised candidates for electromyogram sensor of the experimental authentication system. Myo^{TM}, which was developed by Thalmic Labs Inc., is a wearable device that equips electromyograph. Myo^{TM} consists of 8 blocks that have an electrode and can measure electronic potentials at the 8 spots at the same time. Myo^{TM} also equips wireless communication mechanism. It can send measured data to PCs using Bluetooth. Myo^{TM} is suitable for the prototype system, because it is inexpensive and easy to measure data and easy to send data to PCs.

6 Experiments

A series of experiments was carried out to investigate the prospect of the authentication method using s-EMGs. Specifically, we investigated whether feature values obtained through the Fourier transform were able to be used for the differentiation of gestures by mobile devices. In addition, we investigated whether feature values obtained from s-EMG signals measured by Myo^{TM} were acceptable or not.

The six hand gestures (1–6) shown in Fig. 5 were introduced in the experiments. The two electromyographs,

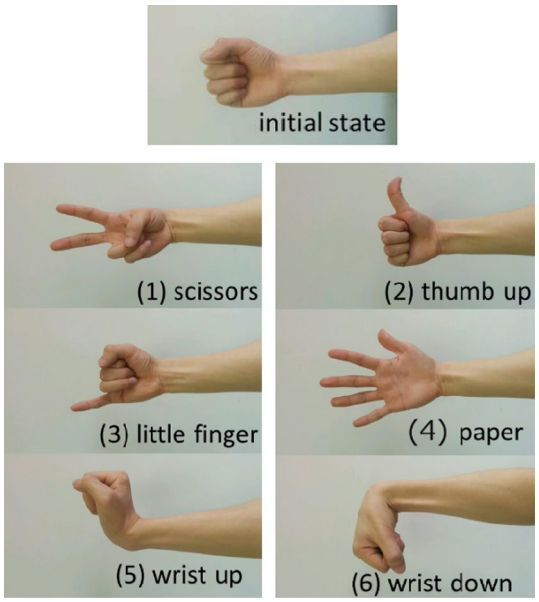


Fig. 5 Gestures used in the experiments

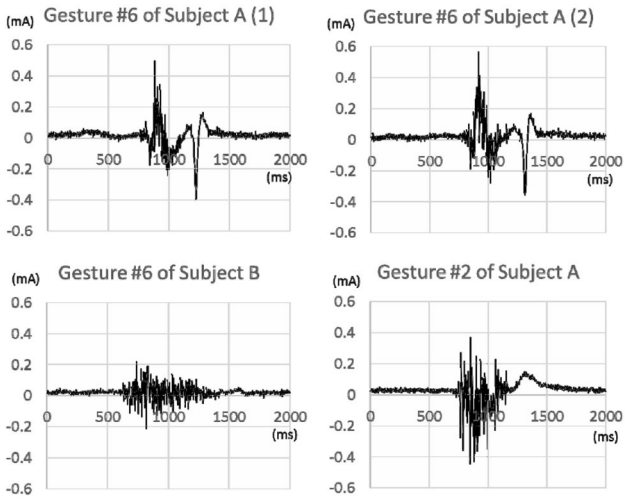


Fig. 6 Comparison s-EMG signals

Myo^{TM} and DL-3100 (S&M Inc.), that were used in the previous research, measured the s-EMG of each movement pattern. 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. To investigate the best performance/the potential to identify users of our method using s-EMG signals, these experiments were carried out under the favorable conditions; the subjects sat still on a chair and the positions of electrodes were decided through the preliminary experiments.

Table 1 Rates of similar s-EMG signal data for 3 gestures

Gesture	(2)	(4)	(6)
Rate	$\frac{484}{500}$	$\frac{481}{500}$	$\frac{489}{500}$

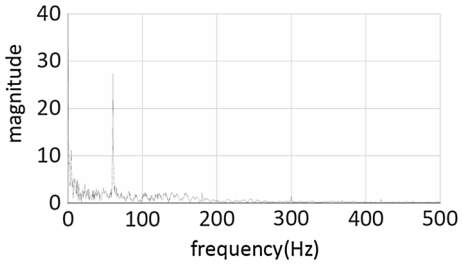


Fig. 7 Result of the Fourier transform on a s-EMG signals measured by DL-3100

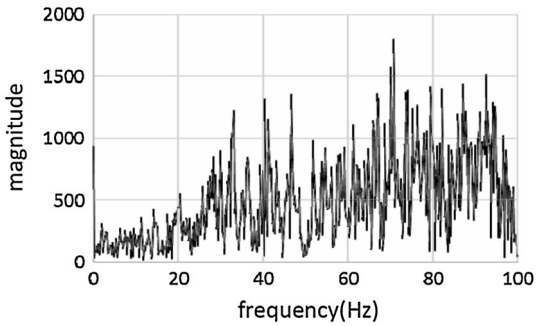


Fig. 8 Result of the Fourier transform on a s-EMG signals measured by Myo^{TM}

First, the s-EMGs of the same gesture made by the same subject were very similar. Two charts in upper row of Fig. 6 show two s-EMGs of the gesture (6) made by the same subject and measured by DL-3100. Table 1 shows the rate of similar signals for three gestures. The decisions were made by one human experimenter. However, s-EMG signals of the gesture (6) made by the different two subjects are not similar. In addition, s-EMG signals of the gesture (2) and the gesture (6) made by the same subject are not similar either.

Next, one of the results of the Fourier transform is shown in Fig. 7. Clear peaks that are expected as feature values are obtained by the Fourier transform. However, we could not find such peaks in frequencies obtained from signals measured by Myo^{TM} (Fig. 8).

These results show that the s-EMG is promising as identification input for a user authentication method. The Fourier transform is expected to obtain feature values from s-EMGs when we use DL-3100 to measure s-EMG. However, s-EMG signals measured by Myo^{TM} are not sufficient to use them as date for user authentication. Then, further improvement is needed to adopt Myo^{TM} as a component of our prototype system that will be used in the future substantiative experiments, which has to be carried out to verify the performance of our method under various realistic conditions.

7 Conclusion

We investigated a new user authentication method that can prevent shoulder-surfing attacks in mobile devices. 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 investigate the performance of candidates of feature values. The results showed that the Fourier transform is promising method to extract feature values from s-EMG signals. We will improve the precisions of feature value extraction method for s-EMG signals obtained by Myo^{TM}. In addition, we will continue collecting s-EMG data from various subjects, and we will study on the performance of our method under various conditions in the future work.

References

1. Tamura H, Okumura D, Tanno K (2007) A study on motion recognition without FFT from surface-EMG (In Japanese). IEICE Part D J90–D(9):2652–2655
2. Yamaba H, Nagatomo S, Aburada K et al (2015) An authentication method for mobile devices that is independent of tap-operation on a touchscreen. J Robot Netw Artif Life 1:60–63
3. Kita Y, Okazaki N, Nishimura H et al (2014) Implementation and evaluation of shoulder-surfing attack resistant users (In Japanese). IEICE Part D J97–D(12):1770–1784
4. Kita Y, Kamizato K, Park M et al (2014) A study of rhythm authentication and its accuracy using the self-organizing maps (In Japanese). Proc DICOMO 2014:1011–1018
5. Tamura H, Goto T, Okumura D et al (2009) A study on the s-EMG pattern recognition using neural network. IJICIC 5(12):4877–4884