Wearable Authentication Interface

Technology Reports

Proposal of New Input Systems

Although mobile phones are becoming a big part of our daily lives, its interface mechanism based on keyboards and small screens is still difficult to operate not in a few situations such as during walking or driving. If mobile phones were to become easier to use in all aspects of daily life, it would be possible for us to be continuously connected to the Internet and lead our lives with access to an infinite amount of information as if it was our own body of knowledge.

This article introduces the latest topics in human interface research that aims to enable mobile phone operations in all kinds of situations and expand the ways for using mobile phones.

(1) Insensible Input Based Authentication: AwareLESS Authentication

To increase the security of mobile devices, we propose awareLESS authentication. Since insensible input prevents the leakage of the key information, it can provide more secure authentication scheme. Experiments that used a pressure sensor show that users can input a preset rhythm by insensible finger motion, and the boundary between insensible and sensible is extended by adding vibration while input.

Hiroyuki Manabe
and Masaaki Fukumoto

1. Introduction

Mobile terminals have been expanded to support various functions in recent years, and the risk of abuse is increasing. For example, they now hold a lot more private information within it, such as IDs for credit/banking access. Since users always walk around with mobile terminals and they are often used in public environments, mobile terminals pose a lot of risk. One major risk is theft and loss. User authentication is important to prevent their abuse after being stolen.

Various authentication techniques have been implemented in mobile terminals. The user can be authenticated by several factors, possession such as IC card and ID tag, biological/behavioral characteristics such as fingerprint and gesture, or knowledge such as a password or a Personal Identification Number (PIN). Possession-based techniques are not secure against theft or loss. Since it is reported that artificial fingers can fool existing authentication systems [1], biological characteristic-based techniques are not the perfect solutions. The other risk of mobile terminals is the leakage of both information on the display and input operation. The knowledge-based and behavioral characteristic-based techniques are weak against leakage.

Since some sensors have high sensitivity, the user may enter the password or PIN with insensible input. If insensible input can be used, much more secure authentication systems would become possible. We propose the use of insensible input to create leakage resistant authentication.

2. Related Works

There are a few approaches that can be used to improve robustness against leakage, i.e. observation by a malicious party. One approach is to make it impossible to guess the key of authentication even if input leaks. The challenge-response scheme can conceal the key, however it is an annoying procedure.

Other approach is using gestures, for example using keystrokes [2], signature [3], and 3D motion of the terminal [4]. Reports suggest that they make it difficult to imitate the key, however the gesture is easy to observe. The third approach is to use insensible input.

MindDrive [5] detects minute motions to extract the user's "thought." There are some insensible inputs that are not based on motion, for example, the use of biological signals such as ElectroEncephaloGraphy (EEG).

3. AwareLESS Input / Authentication

In conventional authentication scheme, the issue is how to prevent the leakage or duplication of the key. Our approach is hiding not only the key but also the input action itself, and we introduce an input process which can not be noticed by surrounding people, we call it "awareLESS input." The opposite word is "awared input," which can be noticed. "AwareLESS" corresponds to insensible, "awared" to sensible in general terms. Though conventional input interfaces, such as keyboard and dial key, are commonly awared inputs, there are some awareLESS inputs such as [5] or Brain Computer Interface (BCI). The main aims of these interfaces are to improve input performances, such as input speed or accuracy, so that the input style has not been much discussed, whether awareLESS or awared. AwareLESS authentication is authentication process based on awareLESS input. This approach makes it hard for anyone to notice the key of authentication, which factor was used to authenticate the user, and when he was authenticated. So it is possible to make authentication more secure. AwareLESS input can yield input interface for knowledge-based techniques, for example, an input rhythm can be used as a password.

It can also be combined with existing techniques, such as keystroke and gesture based authentication.

4. Finger Pressing Force Based Input

As a first trial of awareLESS authentication, we implemented and tested a system with a pressure sensor to detect finger motion. The system consisted of a PC, a small case (representing a handheld device), a pressure sensor (AC coupled), and a vibrator. The sensor was mounted directly under the tip of index finger when the case was held in the left hand. So when the user makes a finger motion, a peak corresponding to it is found in the sensor output. We used only the input timing (rhythm) of finger motions to simplify processing. If the input rhythm matched the preset one, the authentication was succeeded. In this implementation, the pressing force value is not used as the key of authentication.

5. AwareLESS Input by Finger Motions

The first question is whether the user can make awareLESS input by finger motions. An experiment was performed with six subjects, all of who were trained in inputting a preset rhythm in advance.

5.1 Experiment Setups

One subject (operator) tried to input the preset rhythm consisting of four motions. The other subjects (observers) gazed at the operator in an attempt to notice the finger motions and the input rhythm. The input accepted as the preset rhythm (the operator was authenticated) was judged by the observers. Each accepted input was judged to three categories; no finger motion of the four motions was noticed, any finger motion(s) were noticed but the rhythm was not noticed, or the input rhythm was noticed. The first category indicates awareLESS input, the inputs in the second category are awared input but prevent the leakage of the key (the first and second categories corresponds to key protected input), and the third category corresponds to awared and key leakage inputs. The final judgment of the input was taken as the worst category in all the observers classified. So even if the motion (the rhythm) was noticed by only an observer, the input is judged to the second (the third) category.

The operator tried to input the preset rhythm after a beep, which sounded every 5 sec., until 30 input rhythms were accepted or 6 minutes had elapsed (72 trials). All subjects performed the operator role once in this experiment.

This setup is a severe test for the operator. The setup provides the observer with many clues not available in.

Regular use; the observer already knows the preset rhythm (the key of authentication), the index finger is used for input, the authentication scheme, and the timing of the start of input (beep), and the key for authentication is quite simple.

5.2 How Small Input the User Can Make?

Figure 1 shows an example of an input rhythm and a pressure sensor output when a user tried to input the preset rhythm by awareLESS input. The finger motions appear as pressure peaks of about 1 gfp-p. The system can detect such small peaks, and successfully accept when the input rhythm matched the preset one. It is noted that the pressures generated varied greatly with the operator (from 1 to 30 gfp-p).

5.3 Are AwareLESS Inputs by Finger Motions Reproducible?

Figure 2(a) shows the results of successfully accepted input rhythms (accepted inputs / trials), the rate of awareLESS input, and the rate of key protected input with "normal mode." Though the accepted rate depends on the operator, over 50% of the trials were accepted. The rate of awareLESS input is 16-55% with an average of 37%, which is the rate of awareLESS input against all the accepted inputs (same as the rate of key protected input). And the rate of key protected input is 50-100% with an average of 86%. Though these rates may appear low, they indicate excellent performance given the many disadvantages of the operator. These results show that the operator can input the authentication key by awareLESS input by finger motion, and that the leakage of the key can be prevented. Moreover it is found that these rates are correlated to the accepted rate, which is discussed below.

5.4 Discriminating Awared Input

First experiment indicates that users can input the authentication key by awareLESS input, however there still remains the possibility that input motion will be captured by an outsider. Thus it is important to clarify the difference of awareLESS and awared to create countermeasures. Our hypothesis was that awared input was due to excessive pressure changes. **Figure 3** and **4** shows, for each accepted input captured in the first experiment, the maximum pressure within the input (x axis), the maximum difference of the pressure within the input (y), and whether the input was awareLESS or awared. In many cases, awareLESS inputs have small difference while awared have large differences. Whether the input is awareLESS or awared is basically inde-

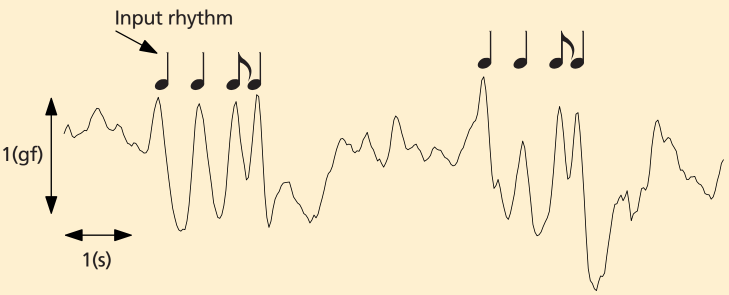
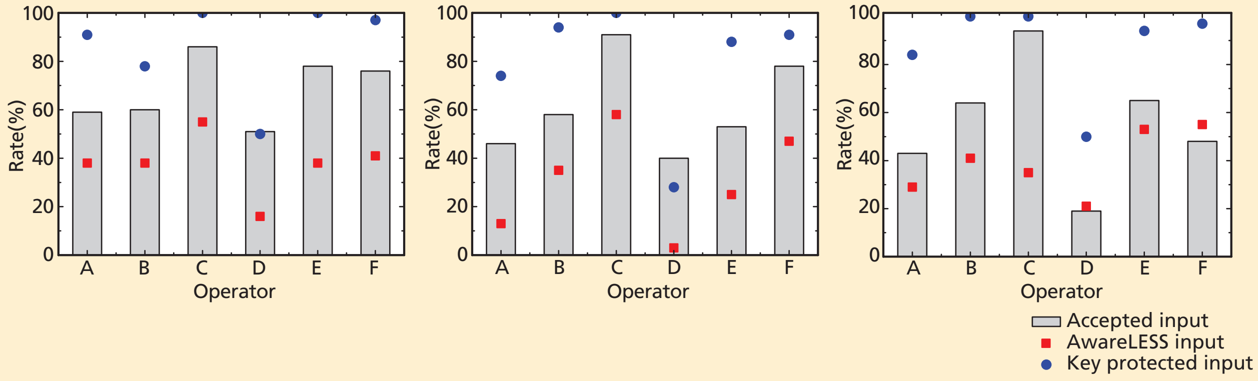


Figure 1 Input rhythm and a pressure sensor output



(a) Normal mode

(b) Response mode

(c) Random mode

Figure 2 The results of accepted input, awareLESS input, and key protected input

pendent of the actual pressures. The dotted line shown in the middle of Fig. 3 and 4 represents a manually set boundary. Input likely to be awared can be detected by the boundary. It has to be noted that for some operators the boundary can not be set well, because whether awareLESS or awared does not seem to be related to pressure. Whether the input is awareLESS or awared depends on various factors, such as the pressure (both AC and DC components), grasping posture, pressing point (fingertip or finger cushion), and so further research is needed to fully resolve this issue. Though the pressure data does not provide an absolute guarantee that the input is awareLESS, it does provides useful information. At least, by using pressure data, the input that is likely to be awared can be identified and countered.

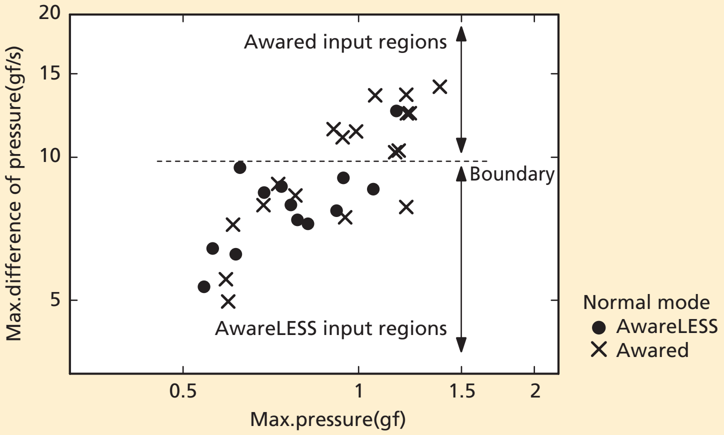


Figure 3 AwareLESS/awared input regions with normal mode

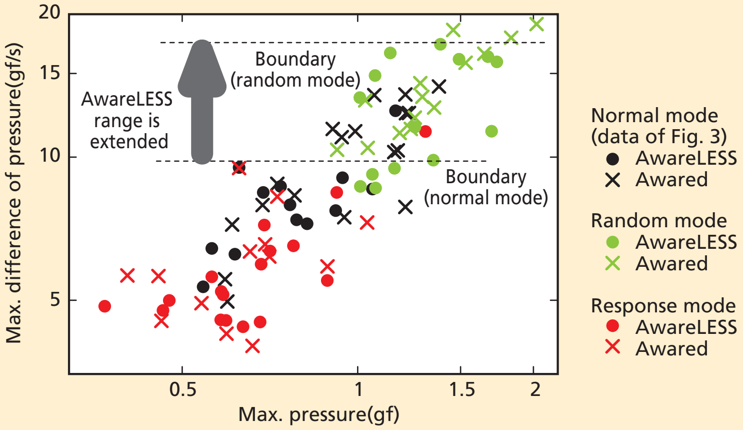


Figure 4 The distribution of awareLESS/awared input and expansion of awareLESS-input regions

6. Input with Vibration

One solution to counter the input

likely to be awared is to mask the input by physically vibrating the terminal. The vibration is made by a motor rotating an eccentric weight (about 10 g) at 15 cycle/s, and this vibrator is used in game controllers as a haptic output device. When the vibrator is switched on, the terminal and the finger visibly vibrate.

6.1 Continuous Vibration

The graph in **Figure 5** shows an example of sensor output with continuous vibration. The influence of the vibration on the sensor output is small. This is because the finger and the sensor are vibrated synchronously, and vibrating frequency (15 Hz) is much higher than input frequency.

6.2 Vibration Only for an Input Likely to be Awared

The first idea is to add vibration only when a big finger motion that is likely to be awared input. This detection is performed by the threshold of the difference of pressing force which we heuristically set from the results of the first experiment, as in Fig. 4. The vibration continued for 500 ms upon detection of a big finger motion. The results of using this mode ("respose mode") are shown in Figures 2 (b) and 4. In this mode, input force becomes smaller than normal mode. And this approach improved the performance of four operators and reduced it for the other two operators.

6.3 Random Vibration

The second idea is random vibration. This mode aims to hide all motions. Since it is difficult to find out the unsteady motion in random vibration rather than in continuous vibration, the high efficiency is expected. The vibration was switched on/off after some random time (40-140 ms). Figures 2(c) and 4 show the results of "random mode." The results show that this mode yielded the highest pressure values and the boundary between awareLESS and awared also becomes higher. It improved/degraded the performance (in the rate of awareLESS input) of 2/4 operators.

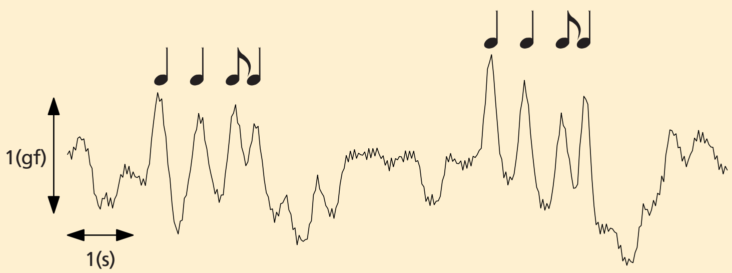


Figure 5 Sensor output with continuous vibration

7. Discussion on the Effects of Vibration

The normal mode is basic and may represent the skill of the operator. In the response mode, we expected that some input would exceed the boundary and thus be masked by vibration. The actual result, however differed from our expectation. In the response mode, the user tried to make motions smaller than those made in the normal mode. Since the boundary was set from the result of normal mode, many inputs fell under the boundary. The result also showed that the improvement in the rate of awareLESS input was small. This means that making smaller motions does not improve the performance. Our explanation of this result is that the response mode has two effects; hiding awared input and increasing the concentration level of the user in order to make smaller motions. The latter effect becomes mental pressure; he feels that he must consciously make smaller finger motions. The operators who could accept this mental load simply made smaller motions and so improved the rate of awareLESS input. The others were disturbed by the mental pressure and their rates declined. The random mode was intended to hide all motions. However, the results show that it increased the leakage. We believe that the random vibration has also two effects; leading the operator to increase the finger pressures due to the additional mental load, and moving the boundary between awareLESS and awared. The ultimate performance is decided by the balance of the two effects. For the two operators who saw improvements in the rate of awareLESS input, the boundary movement outweighed the additional mental loads. For the others, the reverse was true. Since Fig. 5 shows that this system can detect small pressures even with vibration, the random mode would hide input effectively if the operator could make motions as small as normal.

8. Remaining Issues

For some users, probably experts, the experimental awareLESS authentication system can provide an input system that is robust against leakage. However, there are issues that must be resolved in order to make this method acceptable to more people. It is necessary to clarify the factors that make the input awared and how they can be countered. Considering that it is not desirable to install other sensors, a more effective approach is to rely on training; Fig. 2 shows that the rate of awareLESS input is related to the accepted rate which implies that training to improve the accepted rate leads to an increase in the rate of awareLESS input. Moreover effective approaches to masking the input should be examined. Vibration is one approach, however it is not only noticed by the surrounding people but also it attracts their interest.

9. Conclusion

We proposed awareLESS authentication. A pressure sensor based experiment showed that users can use awareLESS input by finger motions for authentication, and that vibration affects system performance. We will try other sensors for capturing awareLESS input, and expand this approach to general operation of information systems.

References

[1] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino: "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," Proc. SPIE, Vol.4677, pp. 275-289, 2002.

[2] W.E. Eltahir, M. J. E. Salami, A. F. Ismail and W. K. Lai: "Dynamic keystroke analysis using AR model," Proc. IEEE ICIT'04, pp.1555-1560, 2004.

[3] D. Sakamoto, H. Morita, T. Ohishi, Y. Komiya and T. Matsumoto: "On-line signature verification algorithm incorporating pen position, pen pressure and pen inclination trajectories," Proc. IEEE ICASSP'01, pp. 993-996, 2001.

[4] S. Ishihara, M. Ohta, E. Namikata and T. Mizuno: "Individual authentication for portable devices using motion of the devices," IPSJ Journal, Vol. 46, No. 12, pp. 2997-3007, 2005 (In Japanese).

[5] MindDrive by The OTHER90% Technologies, Inc.
http://www.other90.com/.2566