The Development of a Pressure-based Typing Biometrics User Authentication System

by

Chen Change Loy
Adv. Informatics Research Group
MIMOS Berhad
Malaysia

Assoc. Prof. Dr. Chee Peng Lim
Associate Professor
Sch. of Electrical & Electronic Eng.
University of Science Malaysia,
Malaysia

Dr. Weng Kin Lai
Adv. Informatics Research Group
MIMOS Berhad
Malaysia

Products Used:

National Instruments PCI6251™ Multifunction Data Acquisition (DAQ)
National Instruments BNC2110™
National Instruments LabVIEW™ 7 Express

The Challenge:

To develop a low-cost, high-performance force measurement system for pressure-sensitive keyboards using National Instruments Hardware and Software Solutions.

The Solution:

Keyboard typing force is acquired from the pressure sensors using real-time acquisition and processing board from National Instruments. Data capturing module, features extraction module, and the user-friendly graphical user interface are developed using ***LabVIEW***. An intelligent classification program based on neural networks that is written in C, was integrated with ***LabVIEW*** to authenticate the individual's typing pattern.

Abstract

In this paper, the development of a pressure-based typing biometrics user authentication system is presented. Studies have shown that identity of a user can be recognized based on his/her keystroke timing pattern [1-2]. However, instead of using conventional typing timing characteristics, the work presented in this paper investigates the applicability of using a different approach to ascertain the identity of a user – the user's typing force. In the following sections, the hardware architecture, including all the constituent components and the software development will be elaborated.

Introduction

Typing biometrics or sometimes also known as keystroke dynamics is the analysis and recognition of a user's distinct keystroke pattern. The underlying assumption is that each of us has a unique way of using the keyboard to enter a password. This may come in the form of the different pressures exerted on the individual keys on the keyboard or it may be the different timing delays when entering the character pairs. At present, most of the works done are commonly based on keystroke latencies and durations.

A typing biometrics system is essentially operated in two modes which are the "enrolment mode" and the "verification mode". In the enrolment mode, a user enrolls by typing a few samples of his/her password. The samples are then used to construct the reference profile. In the verification mode, a user has to provide his/her username and password. The system checks the login information and compares the typing pattern with the reference profile for that individual. A user will gain access if his/her typing pattern closely matches with the reference profile, otherwise he/she will be denied entry.

To date, there has not been a widespread adoption of typing biometrics to complement existing password-based authentication as they may not be as secure as other biometrics systems, e.g. fingerprint systems and iris scanning systems. Therefore, in order to strengthen the system security, this study investigates the use of combined keystroke pressure and latency for the authentication process. We have done some work earlier to investigate the use of typing biometrics based on keystroke latencies [3] and we want to improve the authentication accuracy by combining the latency data with those from the keystroke pressure.

Typing pressure signal acquisition with high resolution and high sampling rate becomes our primary concern because system accuracy would drop if the acquired signal cannot reflect the users' actual typing behaviors. Higher sampling frequency acquires more data in a given time and thus forms a better representation of the original pressure signal. The higher the resolution, the higher the number of divisions the signal range is broken into, and therefore, the smaller the detectable value changes.

Using a specialized force measurement system is not cost-effective, since it cost us nearly $1000 for only 6 kS/s of sampling rate. Additionally, the specialized system requires an individual sensor handle and RS232 port for each sensor. These requirements are clearly unacceptable for the pressure-based typing biometrics system that uses about 20 sensors. Besides, it would be time consuming to integrate this system with the authentication system based on neural network as well as the signal processing analysis.

The alternative solution to develop this system from ground up may be less costly financially, but the amount of time needed to design, develop and debug the system is something that we cannot afford due to the tight time schedules that was given. In addition, the system must be able to accommodate changes in the sampling rates as we work towards improving the authentication accuracy of the system by optimizing the sampling rates.

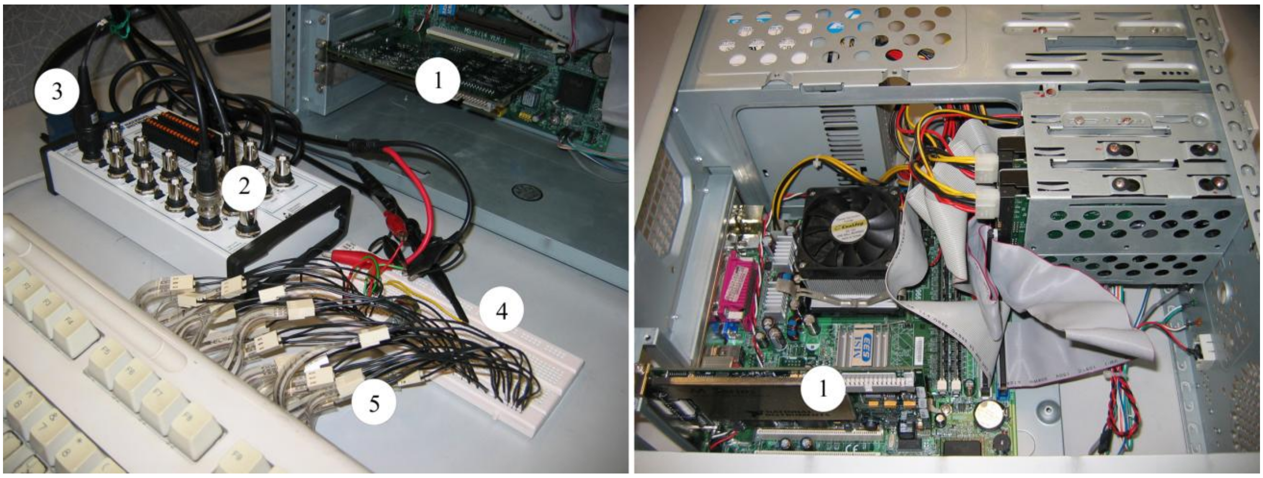
Hardware Set-up

In order to measure the forces exerted during typing, a pressure-sensitive keyboard is developed. The keyboard is modified from a 104-key Windows keyboard by placing the sensors at optimal locations below each keyboard key by adhering them between the keyboard matrix and keyboard plate. The pressure sensor used is an ultra-thin and flexible printed circuit which is constructed of two layers of polyester film. A conductive material is applied on each layer, and this is followed by a layer of pressure-sensitive ink. Analogously, the pressure sensor acts like a variable resistor where its resistance changes in accordance to the amount of force that each user applies when he/she types.

The sensors are extended to the rear of the keyboard through narrow openings on the plate and connected to a signal conditioning circuit. This circuit uses an inverting operational amplifier arrangement to amplify the signal to an acceptable input range for the DAQ card. A low pass filter is added on the circuit to eliminate high frequency components/noise before the pressure signals are processed by the intelligent authentication system.

The signal conditioning circuit is connected to the ***BNC2110*** shielded connector block. The connector block simplifies the connection of the signal conditioning circuit to the DAQ card. Differential Analog Input Channel 0 (AI 0) is used to log the output voltage from signal conditioning circuit, while the Analog Output Channel 0 and 1 (AO 1, AO 2) are used to provide ±10 volts respectively to the operational amplifier on the signal conditioning circuit.

The ***BNC2110*** connector block is connected to the DAQ card through a noise rejection ***SH6868EPM*** cable. The 16 bit, 1.25 MS/s high-speed M series ***PCI6251*** DAQ card is selected because of its high resolution and fast sampling rate. At present, the sampling rate is set to 0.6 MS/s. Keystroke pressure data is acquired indefinitely into the DAQ card buffer and stored in template files. The data acquisition is repeated until the user terminates the program or the enrolment/verification process is completed. The keystroke pressure data are stored in the desktop computer for further analysis.



(a) Connections between the keyboard and the processing unit

(b) Location of the PCI6251 within the processing unit

Figure 1: Pressure-based typing biometrics user authentication system. (1) PCI6251, (2) BNC2110, (3) SH6868EPM, (4) Signal Conditioning Circuit, (5) Pressure Sensors

Software Development

The software is divided into four components, i.e., data capture module, feature extractor, data classifier, and graphical user interface.

For the data capture module, an event-driven module is developed by using the ***LabVIEW*** event structure. The module can responds synchronously to the keyboard value changes. In contrast to traditional polling technique, where the computer is required to continuously poll the keyboard inputs, the event structure remains idle (sleeps) when there are no events of interest during run time. This is important as it eliminates the execution overhead. On the other hand, when the event structure detects the occurrence of “key-down” and “key-up” events, it reacts by executing the code to capture the typing pattern.

Another advantage of using ***LabVIEW*** is that we can also capture the keystroke latencies at the timing resolution of 1ms via the ***LabVIEW*** system timer. The keystroke pressure is measured in volts ranging from 0 to 10 volts in the form of time discrete signal. The pressure discrete time signals are then transformed into the frequency domain by using Fast Fourier Transform (FFT). Features to be extracted from the frequency domain signal include mean, root mean square, peak value, signal in noise and distortion, total harmonic distortion, fundamental frequency, energy, kurtosis, and skewness. The FFT and the features are computed using the inbuilt Spectral Measurements Express VI and Statistics Express VI in ***LabVIEW***.

For the data classifier, Fuzzy ARTMAP (FAM) neural network which is developed in C, is used to match the typing pattern captured with the reference profile stored. The code is executed by calling its executable from ***LabVIEW*** using System Exec VI. In the future we would like to re-code the FAM using ***LabVIEW***.

A user-friendly graphical interface is developed to simulate the actual login environment. The interface displays a dialog box to alert the users if they have entered a wrong password during the enrolment mode. A special administrative panel is designed to enable the user to adjust the system security level and manage the database.

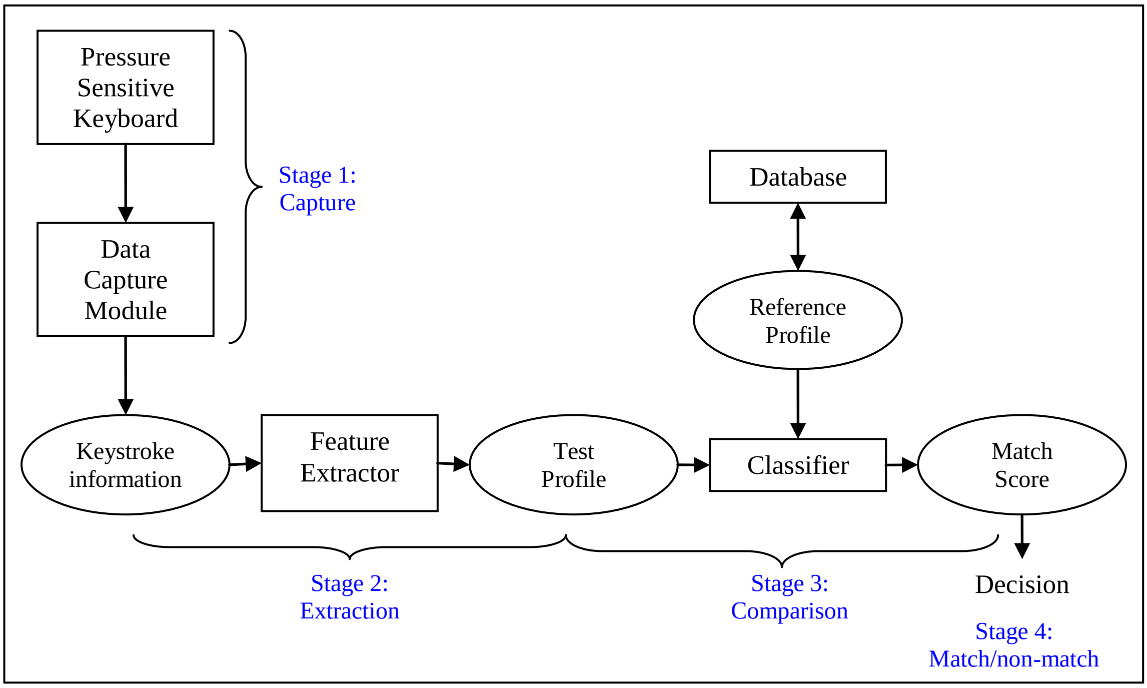
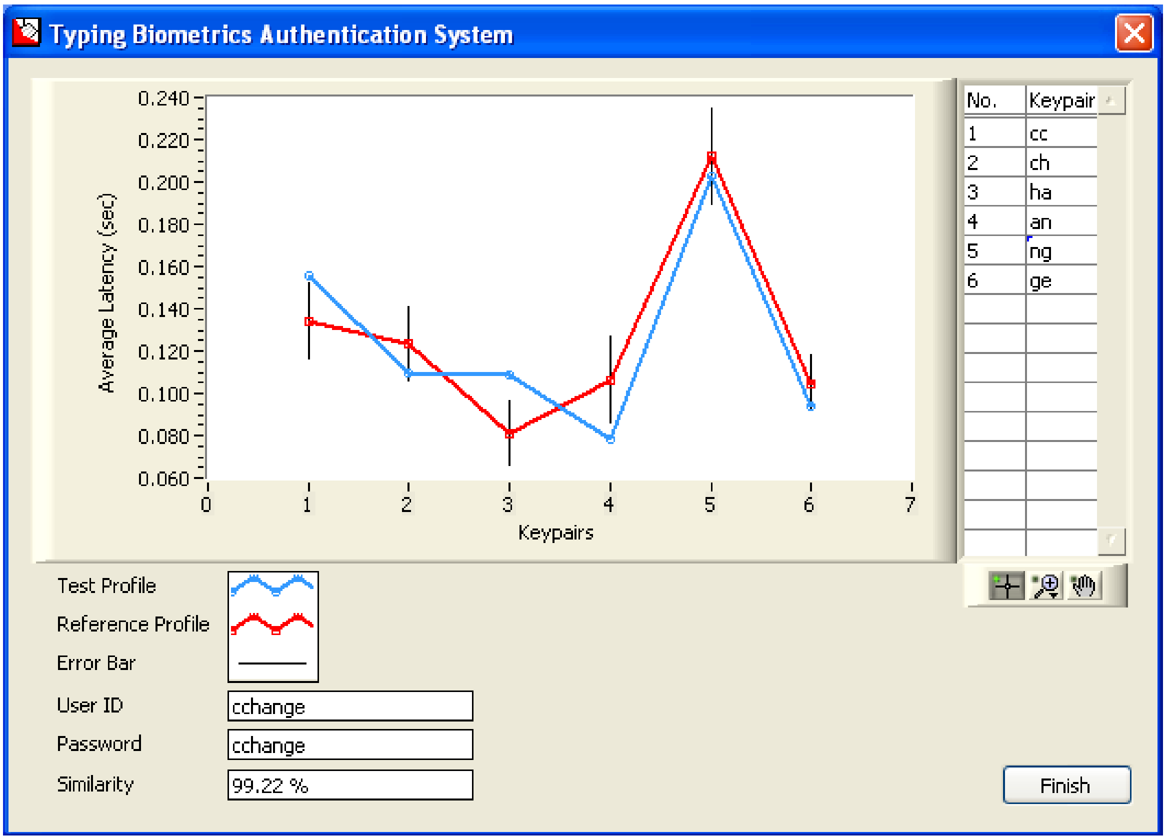


Figure 2: System block diagram.



No.	Keypair
1	cc
2	ch
3	ha
4	an
5	ng
6	ge

User ID: cchange

Password: cchange

Similarity: 99.22 %

Figure 3: User interface window for viewing pattern matching result.

Experiment

A series of experiments has been conducted to find the

- False Acceptance Rate (FAR) – the rate that an imposter's typing pattern is falsely identified as belonging to a legitimate user.
- False Rejection Rate (FRR) – the rate that a legitimate user's typing pattern is incorrectly identified as belonging to an imposter.

The ideal situation is for both these parameters to be as close to zero as possible.

Conclusions

Using the NI DAQ card and ***LabVIEW***, a complex system for capturing typing pressure, analyzing measurement data, recognizing typing pattern, and storing results was simplified into a single, unified system. Besides, the development effort and time is reduced. The experimental results are encouraging. Using keystroke latency alone gives FAR of 2.63% and FRR of 14.6%. However, by combining both keystroke latency and keystroke pressure together yielded improvement of up to 70%, i.e., FAR of 0.87% and FRR of 4.4%. The study reveals the potential of using high precision keystroke pressure to improve the security of conventional typing biometrics system.

References

[**1**] R. Joyce, and G. Gupta, "*Identity authentication based on keystroke latencies*," Comm. ACM, vol. 33, pp. 168–176, February 1990.

[**2**] F. Monrose, and A. Rubin, "*Authentication via keystroke dynamics*," Proc. of the Fourth ACM Conference on Computer and Communications Security, Zurich, Switzerland, pp. 48–56, 1997.

[**3**] Fadhli Wong Mohd Hasan Wong, Ainil Sufreena Mohd. Supian, Ahmad Faris Ismail, Lai Weng Kin, and Ong Cheng Soon, "*Enhanced User Authentication Through Typing Biometrics With Artificial Neural Networks and K-Nearest Neighbor Algorithm*", Proc. of the 35th Asilomar Conference on Signals, Systems & Computers, California, November 2001.