A User Authentication Enabled Piezoelectric Force Touch System for the Internet of Things

Anbiao Huang[1], Shuo Gao[1,2,*] and Arokia Nathan[3,*]
[1]School of Instrumentation Science and Optoelectronic Engineering, Beihang University, Beijing, 100191, China
[2]Beijing Advanced Innovation Center for Big Data-Based Precision Medicine, Interdisciplinary Innovation Institute of Medicine and Engineering, Beihang University, Beijing, 100191, China
[3]Cambridge Touch Technologies Inc., 154 Cambridge Science Park Milton Rd, Milton, Cambridge, CB4 0GN, UK
*shuo_gao@buaa.edu.cn; anathan@camtouch3d.com

***Abstract*—In Internet of Things (IoT) applications, secure access to smart systems, e.g., smartphones, is important for protecting private information. Among various authentication techniques, keystroke authentication methods based on touch behavior of the user have received increasing attention. This is due to the unique benefits, such as no additional hardware component and the ease of use in most smart systems. In this paper, we present a technique for obtaining high user authentication accuracy by utilizing a user's touch time and force information, which are obtained from a piezoelectric touch panel. After combining artificial neural networks with the user's touch features, an equal error rate (EER) of 1.09% is achieved, validating the feasibility of the proposed technique for achieving highly secure user authentication, hence advancing the development of security techniques potentially deployable in the field of IoT.**

Keywords—Keystroke; user authentication; piezoelectric touch panel; Internet of Things security

I. INTRODUCTION

With the rapid rise in use of mobile devices, access security is becoming a global concern. As the most widely used and accepted method, password-based identity authentication [1] has many security loopholes, such as brute force cracking and smudge attacks [2]. Keystroke authentication can be a good alternative as it not only solves the insecurity of passwords but also has other advantages, such as low cost, high flexibility, and simpler hardware structure as compared to other biometric authentication methods [3-5], such as fingerprint and face identification.

Research on traditional keystroke authentication is mainly based on computer keyboards [6-8], in which the system only identifies users by time-related characteristics, limiting the expression of individual keystroke habits. Research on keystroke authentication based on mobile devices has emerged in recent years [9-11], but existing mobile devices, such as phones, have a limited ability to sense a user's force of touch. For example, the iPhone X can only classify force touches into two levels [12], which does not satisfy the need for accurate force sensing, but is important for keystrokes [13-14].

Based on the above considerations, this paper proposes a piezoelectric force touch system for keystroke authentication. The piezoelectric effect is used for high force detection accuracy, based on which the features of a user's touches are extracted and processed by a machine learning algorithm—an artificial neural network (ANN) [15]—for user authentication.

This work was supported in part by the National Natural Science Foundation under Grant 61803017 and Grant 61827802, and in part by the Beihang University under Grant KG12090401 and Grant ZG216S19C8.

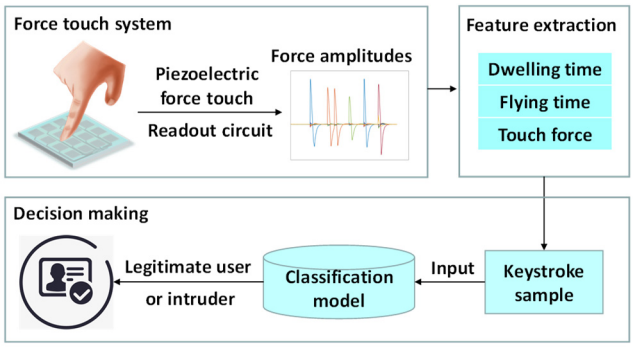

Fig. 1: The overall route of the paper.

With the developed technique, a low equal error rate (EER) of 1.09% is achieved, demonstrating its feasibility in user authentication. The procedure of implementing the proposed technique is depicted in Fig. 1.

II. METHODOLOGY

A. Sensor and System Design

The piezoelectric touch panel is designed as shown in Fig. 2 a and consists of four layers. The first layer is a glass substrate functioning as a protective cover. Below the glass cover is a layer of patterned (4×4) Indium tin oxide (ITO) electrodes. ITO was chosen as the electrode material due to its good light transmittance and low resistivity [16]. The side length of each electrode element is 10 mm, with spacing at 3 mm (shown in Fig. 2 b). The third layer is a PVDF based force sensing layer [17], which offers high light transmittance, high flexibility, good mechanical properties, and high force-voltage responsivity (d_{33} = 30 pC/N), making it sensitive to a user's touch force. The bottom layer is a continuous ITO electrode, which acts as the ground reference. The thickness of each layer is illustrated in Fig. 2 c, and each layer is laminated with an optically clear adhesive (OCA).

Fig. 2 d shows the equivalent circuit of the piezoelectric sensor, based on which the readout system is designed and shown in Fig. 2 f. The force induced charge is collected and amplified through a 16-channel charge amplifier, which is sent to the micro-control unit (MCU) after analogue-to-digital conversion (ADC), STM32 (115,200 Baud rate) is used due to its high sampling rate. Finally, the force related voltage information is uploaded to the computer where data analysis and processing are performed.

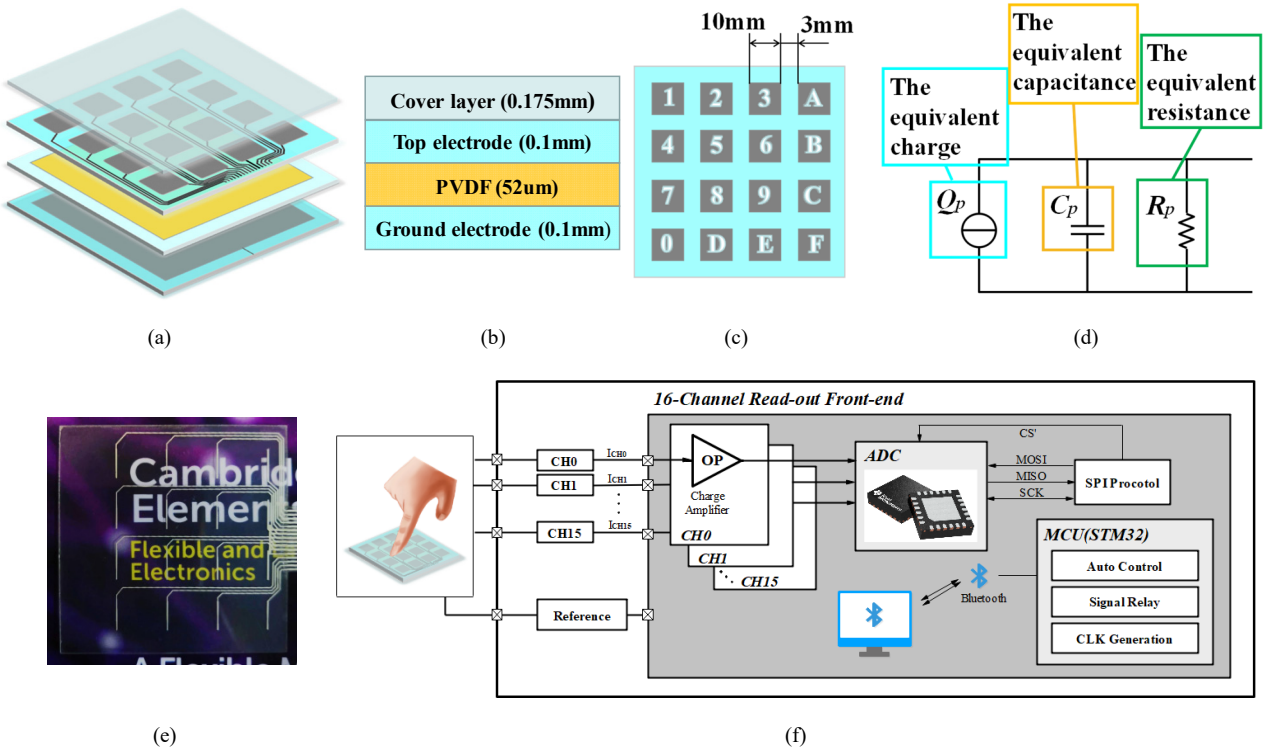

Fig. 2: (a) Schematic of the structure of the piezoelectric touch panel. (b) Schematic of the thickness of each layer. (c) Schematic of the geometry and key configuration. (d) Equivalent circuit of the piezoelectric sensor. (e) Photograph of the experimental testbed. (f) Block diagram of whole data acquisition system.

B. Data Collection

To train the ANN model, datasets were made by ten students (six males and four females) from Beihang University. They were asked to enter the same six-digit password (199517). The purpose of authentication is to distinguish legitimate users from intruders. Thus, one participant was designated as the legitimate user, while the rest were "intruders". Within a month, we collected a dataset containing 150 positive samples from the legitimate user and 50 negative samples from each intruder.

C. Feature Extraction

The voltage response obtained from one password input is shown in Fig. 3 a. A complete touch event consists of two processes, a finger press and a finger lift, which are reflected by the piezoelectric effect as two opposite voltage responses. The collected raw voltage response data cannot directly reflect the main keystroke characteristics, which are dwelling time (*DT*), flying time (*FT*), and touch force amplitude (*F*). *DT* represents the time interval from finger press to finger lift in one touch event, and *FT* is the time interval from the finger lift of the first touch event to the finger press of the next touch event. To clearly explain these important features, we show them in Fig. 3 b. *DT* is the time interval from the first positive peak to the first negative peak, *FT* the time interval from the first negative peak to the second positive peak, and the positive peak of each touch represents the touch force (*F*). Hence, a six-digit password consists of six *DT*s, five *FT*s, and six *F*s, as described in Eq. 1.

$$P=[DT_1,DT_2,...,DT_6,FT_1,FT_2,...,FT_5,F_1,F_2,...,F_6] \quad (1)$$

To provide high quality data for extracting accurate touch features, a pre-processing algorithm (explained in Fig. 3 c) is used on the raw data. First, the 50 Hz common mode noise is filtered out. Second, the direct current (DC) offset of each channel is removed. Third, peak detection is performed. Finally, the feature information is extracted according to the above method.

D. Feature Analysis

Keystroke authentication is always based on the premise that the keystroke habits of one person maintain a certain stability and independence from those of others. We used the following differential scoring method to assess the stability of the legitimate user's multiple keystroke characteristics and their differences from those of the simulated "intruders".

Take the average feature vector $\overline{P}$ of multiple keystrokes of the legitimate user as the keystroke template. Let the predicted feature vector be X; then, the difference between X and $\overline{P}$ can be described by Eq. 2. The smaller the value of D, the closer the X vector is to the $\overline{P}$ vector, that is, the more likely the feature vector X to be predicted comes from the legitimate user.

$$D(X,\overline{P})=\sum_{i=1}^{n}\left|\frac{X_i-\overline{P}_i}{\sigma_i}\right| \quad (2)$$

Where X_i , $\overline{P}_i$ donate the i-dimensional feature of X and $\overline{P}$, and σ_i donates the standard deviation of the i-dimensional feature of $\overline{P}$.

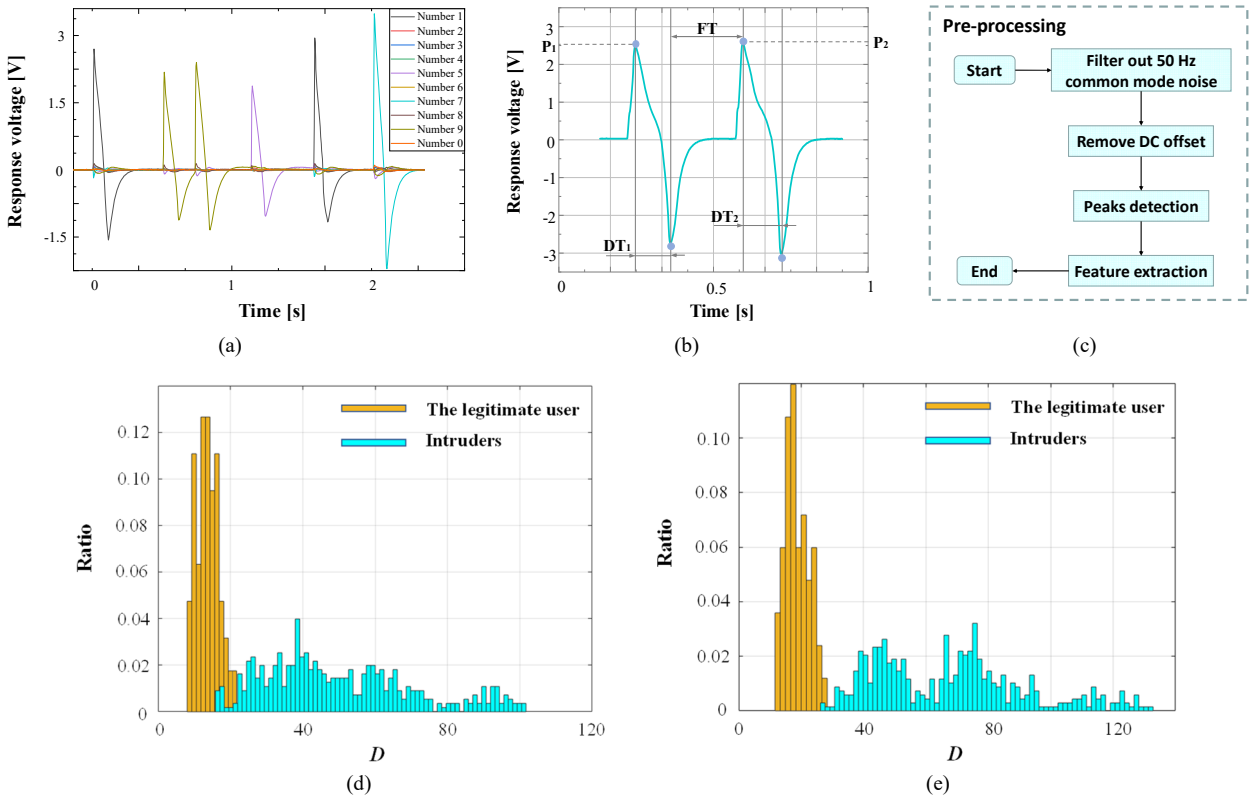

Fig. 3: (a) The voltage response obtained from one password input. (b) The method of feature extraction. (c) Flow chart for the data pre-processing. (d) The value of the D distribution of samples (DT, FT) from the legitimate user and intruders. (e) The value of the D distribution of samples (DT, FT, F) from the legitimate user and intruders.

III. Results and Discussion

The results of Eq. 2 are illustrated in Fig. 3 d and e. Fig. 3 d demonstrates the results using only the time related features (DT and FT), while Fig. 3 e shows the result utilizing all features (DT, FT, and F). It can be observed that, on the one hand, in either case, all keystroke vectors from the legitimate user are concentrated in the region with a lower D value, while the keystroke vectors from simulated intruders are scattered in the region with a higher D value. This result is consistent with our previous assumption. On the other hand, the overlap represents data that could be misclassified. It is clear that if the feature of the touch force is added, the data that can be misclassified will be significantly less than if only the time feature is used.

As shown in Fig. 1, the system architecture of our method also has a decision module, whose function is to use the existing dataset to train the classifier, finally recognize the predictive keystroke vector, and output the decision whether the keystroke vector is from a legitimate user or from an intruder.

Fig. 3 d and e provide a direct view of the effect of using force information for user authentication. Below, we show the quantitative classification results using the ANN algorithm.

To feed the ANN, the collected data are divided into two datasets. Each has 200 training samples and 400 test samples. In the training set, 50 positive samples and 150 negative samples are contained, and the remaining samples all serve as the test set. For dataset 1, only time associated features are used, while time and force features are both considered in dataset 2. EER is used as an indicator for evaluating the comprehensive performance of biometric authentication systems.

The result in Table I shows that the EER of dataset 2 is almost half of the EER of dataset 1. This proves that taking accurate force features into consideration is of great significance to improve the accuracy of keystroke authentication compared to merely using time features.

IV. Conclusion

Keystroke authentication offers an efficient way to solve the security problems of current IoT devices. We reported here a piezoelectric force touch system capable of detecting a user's touch time and force information. After analysing the time and force information, a low EER of 1.09% was achieved. The developed technique allows smart end terminals, such as smartphones and tablets, to provide secure access for users, thereby protecting the users' private information and enhancing the interactivity in devices for the IoT.

TABLE I. EER for Two Datasets

Dataset	*Features*	*Training set*	*Test set*	*EER (%)*
Dataset 1	*DT*, *FT*	200[a]	400[a]	**2.17**
Dataset 2	*DT*, *FT*, *F*	200[a]	400[a]	**1.09**

[a] The fourth and fifth columns represent the sample sizes for training and test, respectively.

References

[1] Z. Shuo and H. Tao, "Design and implementation of password-based identity authentication system," *2010 International Conference on*

Computer Application and System Modeling (ICCASM 2010), Taiyuan, 2010, pp. V9-253-V9-257.

[2] X. Bultel *et al*., "Security analysis and psychological study of authentication methods with PIN codes," *2018 12th International Conference on Research Challenges in Information Science (RCIS)*, Nantes, 2018, pp. 1-11.

[3] D. K. Anguiano Cervantes, Ghouri Mohammad Saaduddin, Y. Li and M. Xie, "Comparison between fingerprint and behavioral biometric authentication using 2D and 3D gestures," *2016 IEEE Conference on Communications and Network Security (CNS)*, Philadelphia, PA, 2016, pp. 372-373.

[4] S. Kang, J. Lee, C. Kim and H. Yoo, "B-Face: 0.2 MW CNN-Based Face Recognition Processor with Face Alignment for Mobile User Identification," *2018 IEEE Symposium on VLSI Circuits*, Honolulu, HI, 2018, pp. 137-138.

[5] Q. Zhang, H. Li, Z. Sun and T. Tan, "Deep Feature Fusion for Iris and Periocular Biometrics on Mobile Devices," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2897-2912, Nov. 2018.

[6] F. Monrose, A. D. Rubin, "Keystroke dynamics as a biometric for authentication," in *Future Generation Computer Systems*, vol. 16, no. 4, pp. 351-359, Feb. 2000.

[7] E. Vural, J. Huang, D. Hou and S. Schuckers, "Shared research dataset to support development of keystroke authentication," *IEEE International Joint Conference on Biometrics,* Clearwater, FL, 2014, pp. 1-8.

[8] C. Shen, H. Xu, H. Wang and X. Guan, "Handedness Recognition through Keystroke-Typing Behavior in Computer Forensics Analysis," *2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin, 2016, pp. 1054-1060.

[9] F. Alshanketi, I. Traore and A. A. Ahmed, "Improving Performance and Usability in Mobile Keystroke Dynamic Biometric Authentication," *2016 IEEE Security and Privacy Workshops (SPW)*, San Jose, CA, 2016, pp. 66-73.

[10] D. El Zein and A. Kalakech, "Feature Selection for Android Keystroke Dynamics," *2018 International Arab Conference on Information Technology (ACIT)*, Werdanye, Lebanon, 2018, pp. 1-6.

[11] K. Tse and K. Hung, "Behavioral Biometrics Scheme with Keystroke and Swipe Dynamics for User Authentication on Mobile Platform," *2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Malaysia, 2019, pp. 125-130.

[12] J. Park, C. Nam, J. Lee and D. R. Shin, "Analysis of Task Success Rate for Classifying 2D-Touch and 3D-Touch through Threshold," *2019 21st International Conference on Advanced Communication Technology (ICACT)*, PyeongChang Kwangwoon_Do, Korea (South), 2019, pp. 334-338.

[13] K. Krombholz, T. Hupperich and T. Holz, "May the Force Be with You: The Future of Force-Sensitive Authentication," in *IEEE Internet Computing*, vol. 21, no. 3, pp. 64-69, May-June 2017.

[14] H. Saevanee and P. Bhattarakosol, "Authenticating User Using Keystroke Dynamics and Finger Pressure," *2009 6th IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, 2009, pp. 1-2.

[15] T. H. Oong and N. A. M. Isa, "Adaptive Evolutionary Artificial Neural Networks for Pattern Classification," in *IEEE Transactions on Neural Networks*, vol. 22, no. 11, pp. 1823-1836, Nov. 2011.

[16] J. R. McGhee, J. S. Sagu, D. J. Southee and K. G. U. Wijayantha, "Humidity Sensing Properties of Transparent Sputter-Coated Indium–Tin Oxide and Printed Polymer Structures," in *IEEE Sensors Journal*, vol. 18, no. 18, pp. 7358-7364, 15 Sept.15, 2018.

[17] A. Kimoto, N. Sugitani and S. Fujisaki, "A Multifunctional Tactile Sensor Based on PVDF Films for Identification of Materials," in *IEEE Sensors Journal*, vol. 10, no. 9, pp. 1508-1513, Sept. 2010.