ELSEVIER

Keystroke dynamics enabled authentication and identification using triboelectric nanogenerator array

Changsheng Wu [1,†], Wenbo Ding [1,†], Ruiyuan Liu [1,†], Jiyu Wang [1], Aurelia C. Wang [1], Jie Wang [2,3], Shengming Li [1], Yunlong Zi [1], Zhong Lin Wang [1,2,3,*]

[1] School of Materials Science and Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA
[2] Beijing Institute of Nanoenergy and Nanosystems, Chinese Academy of Sciences, Beijing 100083, PR China
[3] School of Nanoscience and Technology, University of Chinese Academy of Sciences, Beijing 100049, PR China

Cyber security has become a serious concern as the internet penetrates every corner of our life over the last two decades. The rapidly developing human–machine interfacing calls for an effective and continuous authentication solution. Herein, we developed a two-factor, pressure-enhanced keystroke-dynamics-based security system that is capable of authenticating and even identifying users through their unique typing behavior. The system consists of a rationally designed triboelectric keystroke device that converts typing motions into analog electrical signals, and a support vector machine (SVM) algorithm-based software platform for user classification. This unconventional keystroke device is self-powered, stretchable and water/dust proof, which makes it highly mobile and applicable to versatile working environments. The promising application of this novel system in the financial and computing industry can push cyber security to the next level, where leaked passwords would possibly be of no concern.

Introduction

Keystroke dynamics, first proposed by Spillane in 1975 [1], is a behavioral biometric based on people's typing attributes. Its ballistic nature [2] and non-invasive monitoring characteristics [3,4] have fostered its applications in multi-factor authentication [5] for enhanced cyber security, especially after the establishment of its singularity to the typist by both the National Science Foundation and National Institute of Standards and Technology in the 1980s [6]. However, most academic and industrial efforts [2] utilize only the features of keystroke latency and key hold time, without taking into account the typing force, typing speed and/or finger size of individuals [7–10]. Here we developed a two-factor authentication and identification system composed of a triboelectric keystroke device that can continuously collect a user's intrinsic behavior reflected in keystroke dynamics, a customized signal processing scheme for feature extraction, and a support vector machine (SVM) algorithm-based platform for user classification. The triboelectric keystroke device can transduce the typing motion including the effects of typing force and contact area into the electrical signals, and its touch-proof feature offers an improved signal-to-interference-plus-noise ratio (SINR) compared to previous active sensing devices based on triboelectrification [11–13]. The SVM-based platform [14], with a rationally designed training stage and the capability of handling nonlinear features in keystrokes, is much more advanced than previously used statistical-based approach [13]. This one-stop, hardware-plus-software security system is capable of authenticating and even precisely identifying users through their unique typing behaviors at the terminals, with an accuracy up to 98.7%. The promising application of this novel system in the financial and computing industry can push cyber security to a new level, where leaked passwords would possibly be of no concern.

* Corresponding author at: School of Materials Science and Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA.
E-mail address: Wang, Z.L. (zhong.wang@mse.gatech.edu).
† These authors contributed equally to this work.

 https://doi.org/10.1016/j.mattod.2018.01.006

Results and discussion

The proposed system consists of two processes, the training process and the authentication/identification process (Figure 1a). During the training process, users will input a string of characters through the keystroke device, followed by the acquisition of the induced electrical signals. Pre-defined features will then be extracted from the acquired signals and used to construct a profile database. During the authentication/identification process, a test profile will be built following the same procedures and cross-referenced with the existing profile database to either determine if the test subject is an authorized user (authentication) or identify who the test subject is (identification). The design of our triboelectric key is depicted in Figure 1b. Its structure was made of silicone, and it had three electrodes – a shield electrode, a top electrode, and a bottom electrode. As a proof-of-concept demonstration, a numeric keypad consisting of 16 triboelectric keys similar to those commonly seen in financial institutions was fabricated in this work. It is stretchable and conforms to rounded surfaces (Figure 1c), making it more adaptable for today's highly mobile society. From the perspective of working mechanism, the triboelectric key consists of a shield electrode and a contact-separation-mode triboelectric nanogenerator (CS-TENG) [15–17]. The enclosed CS-TENG is responsible for transducing the typing behavior into analog electrical signal for data acquisition [18,19], while the shield electrode is to minimize undesirable components in output signals originating from inadvertent touch or variations in working conditions, such as wet or dirty fingers. The detailed working principle is illustrated in Supplementary Figure S1 and discussed in Supplementary Note 1.

To reveal the practical shielding effect, the electrical outputs from our triboelectric key and a reference key without shield electrode as a human finger slowly approaches, presses, releases, and leaves the keys, were tested, with the results plotted in Figure 2a. For our triboelectric key, the undesired voltage components induced from touch, denoted by T1 and T2, were greatly reduced and hence the SINR was improved from around 2 dB to nearly 10 dB, where SINR is defined as $10\log_{10}(V_{press}/(V_{touch} + V_{noise}))$ [20]. Therefore, the rationally designed triboelectric key can hugely diminish the effects of inadvertent touch from the fundamental physical level. Furthermore, the pressure-sensitive signal from the fabricated triboelectric key device makes it possible to introduce factors such as typing force and finger size into keystroke dynamics without the necessity of conventional pressure sensors. Figure 2b presents the maximum output voltage of the device under various typing forces with a contact area of 1 cm^2. Three different response regions were observed and can be attributed to the different contact statuses between the top and bottom parts. The first transition occurs when the typing force enables

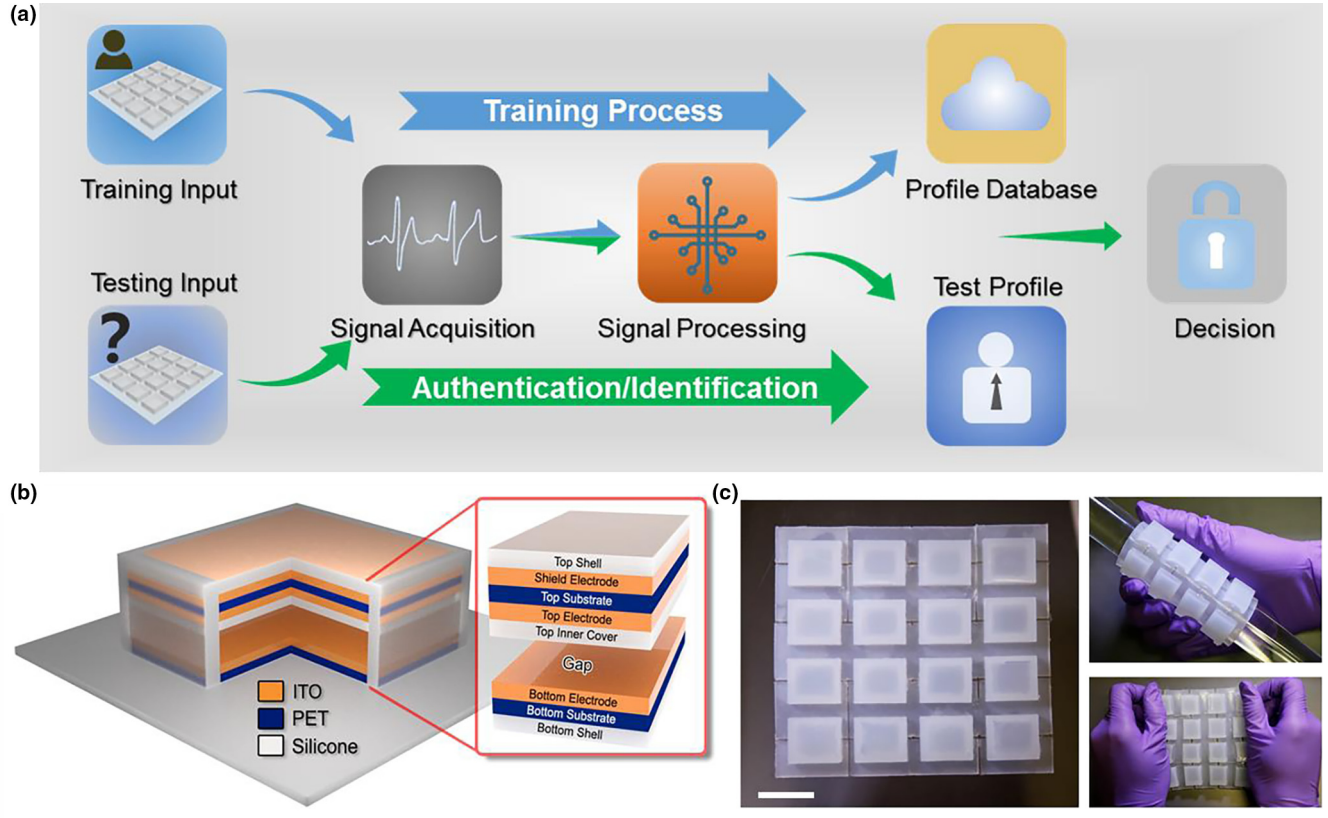


FIGURE 1

The two-factor authentication and identification system. (a) The system outline consisting of the training process and the authentication/identification process. (b) Schematic and exploded view of a single triboelectric key. The shield electrode and the top electrode were embedded into the top silicone shell of the key, while the bottom electrode was attached on the bottom silicone layer and exposed to the inner gap of the key. PET films were used as the supporting substrates for all electrodes. (c) Photographs of the proof-of-concept triboelectric numeric keypad consisting of 16 keys at different mechanical states (Scale bar: 2 cm).

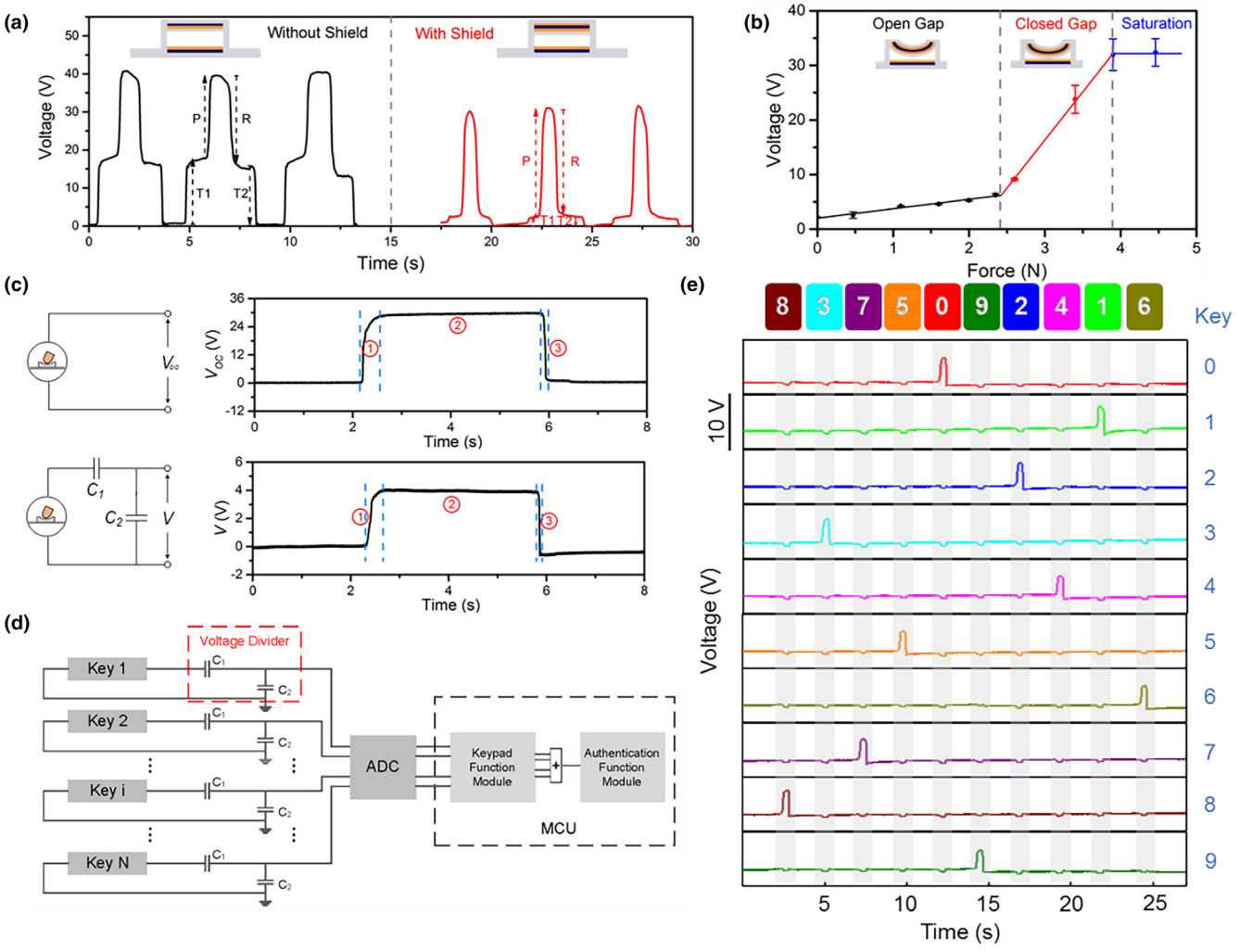


FIGURE 2

The triboelectric-key-based numeric keypad. (a) Comparison of electrical outputs from our triboelectric key and a reference key without shield electrode. Our key with shield electrode yields a one-magnitude-larger SINR. (b) The relationship between the maximum output voltage from our triboelectric key and the typing force. The responses can be categorized into three different regions, open-gap, closed-gap, and saturation, depending on the different contact statuses between the top and bottom parts of the key. (c) The capacitor-based voltage-dividing scheme to transform the key output signals to be compatible with common ADCs. Three labeled stages correspond to the pressing, hold and releasing of the key during normal typing. (d) Equivalent electrical circuit for a keystroke device consisting of multiple triboelectric keys. (e) Electrical signals from the fabricated numeric keypad by sequentially inputting the digits "8-3-7-5-0-9-2-4-1-6.

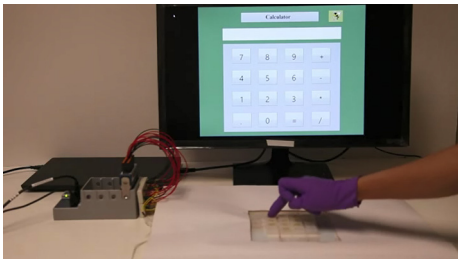
the contact between the two parts, while the second one is due to the saturation of the contact area. The increase in contact area can induce a more significant increase in output voltage than the decrease in gap distance, which explains why the closed-gap region has a steeper slope (17.63 *V/N*) than that of the first open-gap region (1.72 *V/N*). The durability of the key device was also tested (Figure S2a) and proved to be fully functional even after eight thousand typing cycles under the same stimulated conditions. The gradual decrease of the voltage output would not affect the system accuracy after long-term usage since normalized values instead of absolute ones are adopted for analysis. The surface of the device was chemically treated as well to make it hydrophobic with a contact angle of 126° (Figure S2b) and more resistant to moisture and dirt, further improving device stability.

The detection of keystrokes on a keypad/keyboard is realized through multichannel measurement, which is typically handled by a multichannel analog-to-digital converter (ADC) with a limited range of operation voltage – for instance, within ±10 V for most National Instrument DAQ devices. However, active open-circuit-voltage (V_{OC}) signals from CS-TENG tend to be tens to hundreds of volts [15], as further evidenced by the top plot in Figure 2c for our key, and thus a voltage divider is required before connecting triboelectric devices to portable multichannel measurement systems. Considering that the functioning element in a triboelectric key, the CS-TENG, has an equivalent electrical circuit consisting of a voltage source and a serial variable capacitor (Figure S3a), we proposed a capacitor-based voltage-dividing scheme, with its equivalent electrical circuits and typical voltage outputs from normal typing plotted in the bottom of Figure 2c. Two capacitors with rationally selected capacitance (C_1: 330 pF, C_2: 660 pF) are connected to the triboelectric key and

only the voltage across C_2 is measured as the output signal, which can be represented by

$$V = \left(\frac{V_{OC}(t)}{1/C_{TENG}(t) + 1/C_1 + 1/C_2}\right) \Big/ C_2 \quad (1)$$

The divided voltage signal has been lowered to about 5 V while keeping the shape of the OCV as well as retaining all the keystroke information such as applied typing force and hold time. This voltage-dividing scheme is superior to previously reported resistor-based one [11,13], with detailed comparison presented in Figure S3 and Supplementary Note 2. The consequent equivalent electrical circuit for a keystroke device consisting of multiple triboelectric keys is illustrated in Figure 2d. The analog voltage signals are measured by the ADC module and then sent to the Microprogrammed Control Unit (MCU) for subsequent processing and analysis, including the digital filtering, denoising, baseline elimination, feature extraction, and so on. The electrical signals from the fabricated numeric keypad by sequentially inputting the digits "8-3-7-5-0-9-2-4-1-6" are plotted in Figure 2e. Each typed digit is clearly recorded by the voltage change in the corresponding channel, while the induced noise in other channels are negligible, demonstrating the successful implementation of the triboelectric device as a numeric keypad. In Supplementary Movie 1, its application as an active keypad and an arithmetic calculator is recorded, with the outputs correctly shown on a customized interface (Figure S5a).



Supplementary Movie 1.

A customized SVM-based software platform (Figure 3) was developed and integrated with the triboelectric numeric keypad to construct a two-factor authentication/identification system (Figure 4a). Analog voltage signals transduced from keystrokes is firstly converted to digital signals by the hardware circuits consisting of voltage dividers and an ADC. Subsequently, the keystroke features (defined as in Figure 4b and Supplementary Note 3), such as typing latencies (L), hold time (H) and signal magnitudes (M), are extracted using specific signal processing techniques, e.g., denoising, baseline elimination, and peak detection. For an exemplary number sequence consisting of six digits, "8-0-7-3-4-5", a total of 17 features can be obtained accordingly, and the radar plot of their normalized mean values of five users after they typed the number sequence for 150 times each shows

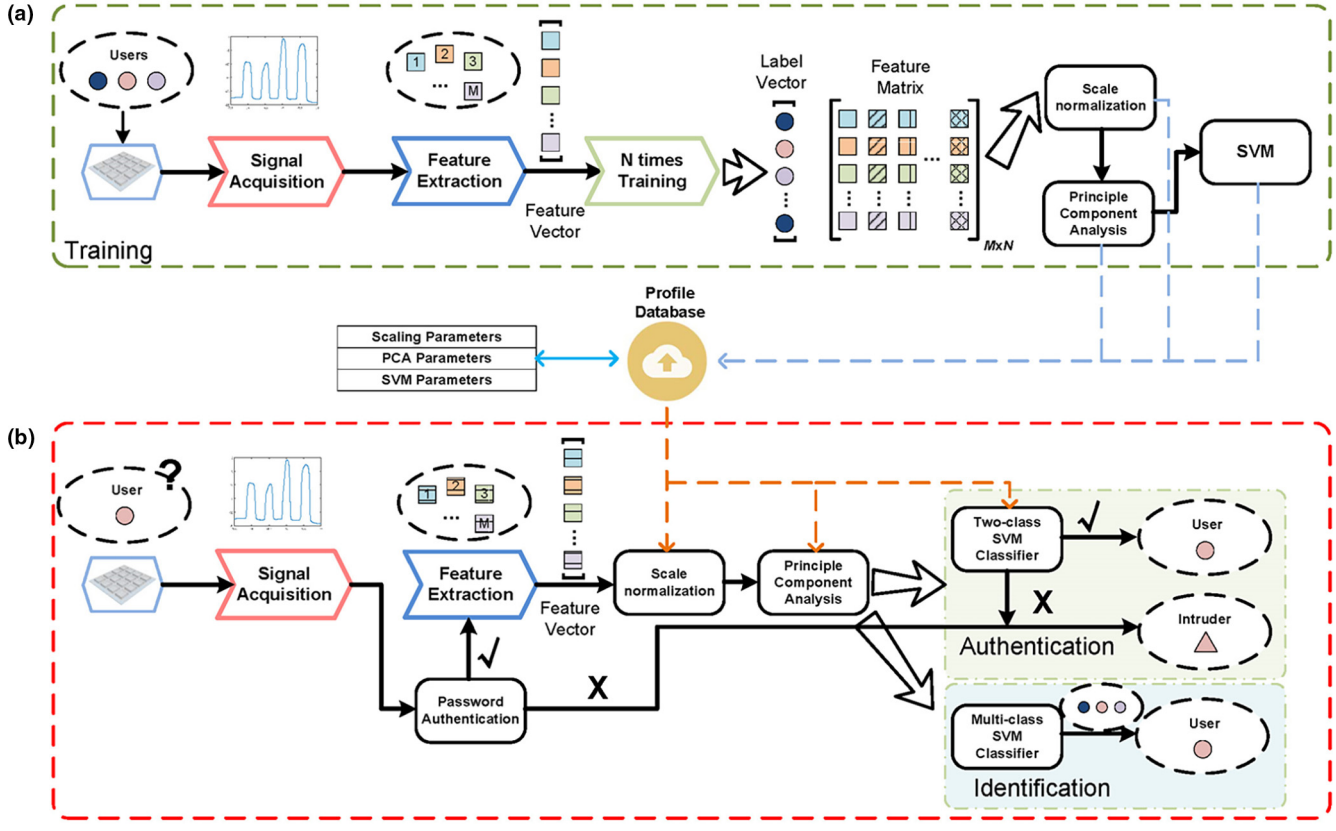


FIGURE 3

The process flow of the proposed authentication and identification system combined with the classification algorithm. (a) The training process. (b) The authentication and identification process.

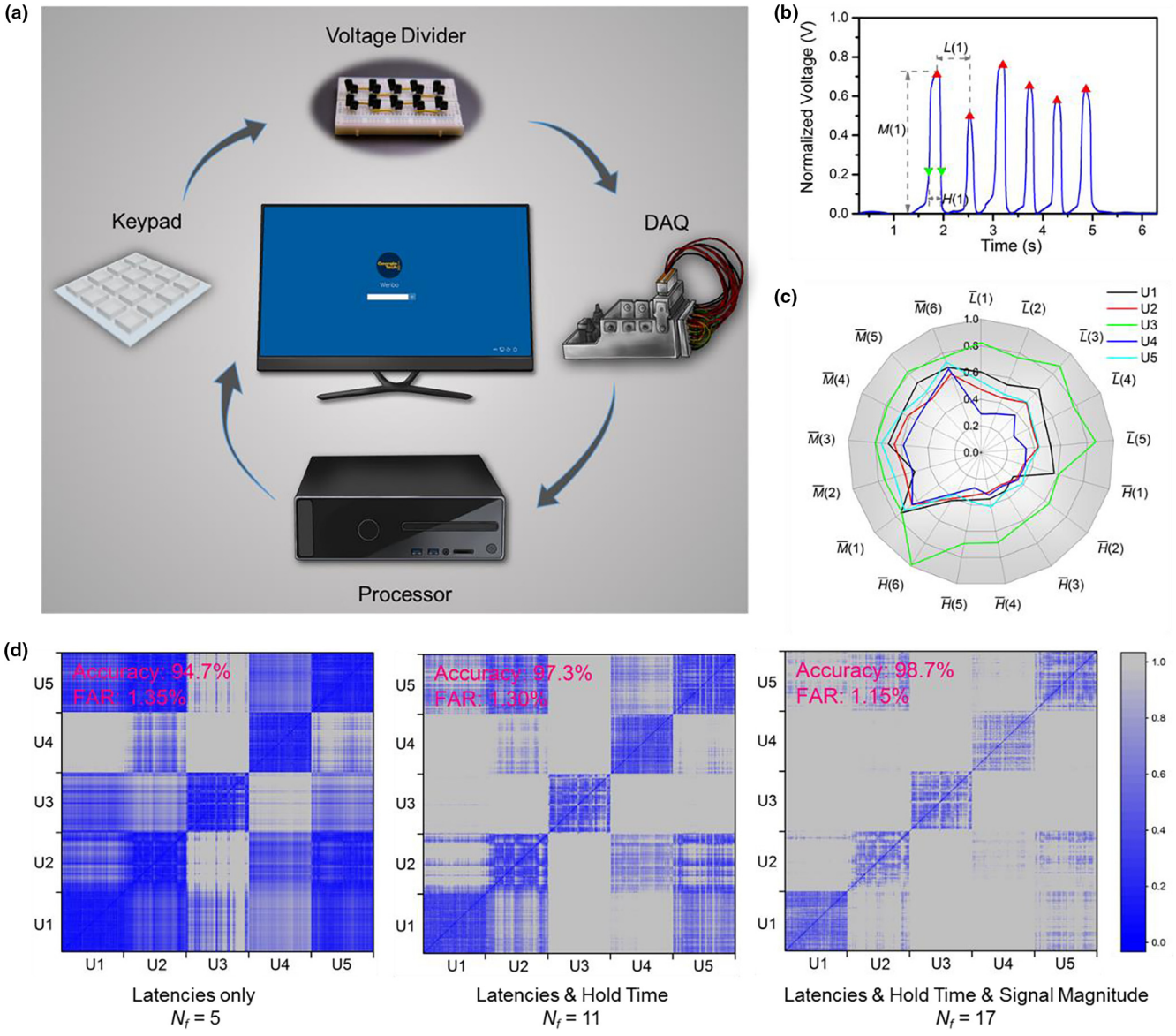


FIGURE 4

The two-factor authentication and identification system built upon the triboelectric keystroke device. (a) The hardware schematic of the experimental system. (b) The keystroke features defined to construct user profile models. Typing latencies, hold time, and signal magnitudes are denoted as *L*, *H*, and *M* respectively. (c) The radar plot of the normalized mean feature values of five users after they typed the number sequence "8-0-7-3-4-5 for 150 times each. A total of 17 features, 5 typing latencies, 6 hold time and 6 signal magnitudes can be extracted from the 6-digits sequence. (d) The difference score matrices across user inputs with varying combinations of feature types.

distinctive typing behaviors among them (Figure 4c). In the training process, these normalized feature vectors are then used to build user profile models via supervised learning with the help of principle component analysis (PCA) [21] and SVM. For the implementation of the authentication and identification, a similar process is carried out and the test user profile is cross-referenced with the existing profile database for decision making through a pre-trained classifier. The classifier is built upon a customized classification algorithm modified from the LibSVM toolbox [22,23] (Supplementary Note 4), which achieves a satisfactory tradeoff between computational complexity and prediction accuracy, and fits the scenario of a large number of users well. Moreover, it can be analyzed theoretically with a precise probability model and avoid the over-fitting issue of the training sets. The classical two-class (binary) SVM classifier is adequate for authentication while the multi-class SVM classifier [24] is adopted for identification, with the latter extended from the former through the one-against-all strategy.

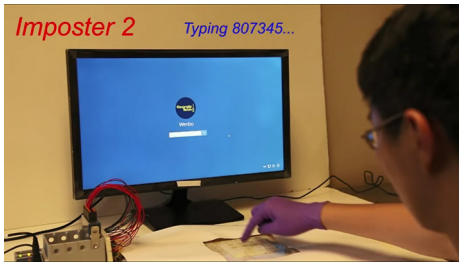
The 150 sets of data from each user were randomly split into two halves, one for training and the other for testing. The classifier performance was optimized by tuning the decision threshold value and comparing the resulting false rejection rate (FRR) and false acceptance rate (FAR). With the optimal decision threshold of 0.75, the tradeoff between a low FRR and a low FAR can be well satisfied so that an equal error rate (EER) as low as 1.15% can be achieved (Figure S4a). A standardized receiver operating

characteristic (ROC) curve (Figure S4b), defined as the plot of the true positive rate (TPR) against the FAR at various threshold settings, is calculated and gives an enclosed area of 0.9967, indicating a very good classifier.

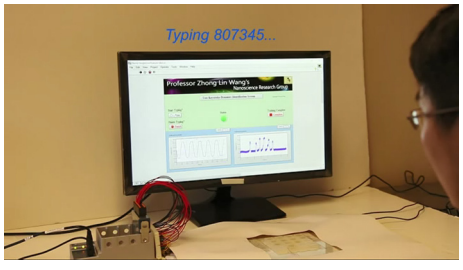
To quantify the difference of users' typing patterns with varying combinations of feature types, a difference score between two typing inputs is introduced based on the normalized interval distance [25,26]. It is defined as

$$S = \sum_{i=1}^{N_f} S_{f^1(i),f^2(i)} = \sum_{i=1}^{N_f} \left| \frac{f^1(i) - f^2(i)}{f^1(i)} \right| \quad (2)$$

where $f(i)$ is the value of feature i, N_f is the total number of features, and $S_{f^1(i),f^2(i)}$ is the contribution to the difference score from the feature i. The difference score between inputs from the same user and different users is plotted in Figure 4d. Ideally the scores across the diagonal should be much lower (more blue) compared to the rest to indicate that the inputs from the same user differ significantly less than those across users. Clearly the introduction of more features such as the hold time and signal magnitudes could produce more ideal score matrices, i.e., only inputs from the same user have the lower score (more blue), suggesting that the typing patterns between different users are more distinctive. The same conclusion can also be drawn from the perspective of system accuracy, i.e., by integrating the features of hold time and the features of signal magnitudes, the system accuracy can be improved and the FAR rate can be reduced compared to only adopting the features of typing latencies. By replacing standard input devices like commercial keyboards with the triboelectric keystroke system, an imposter knowing the correct password still could not log onto the computer system unless his/her typing dynamics matches the information stored in the system, as demonstrated in Supplementary Movie 2 (Figure S5b). By switching the customized classifier in the system from the binary mode to the multi-class mode, the system can serve for identification purposes and identify different users even if they typed the same codes, as in Supplementary Movie 3 (Figure S5c).



Supplementary Movie 2.



Supplementary Movie 3.

Conclusion

The two-factor authentication and identification system built upon the triboelectric keystroke device and the SVM-based platform offers a facile and reliable solution for enhanced keystroke dynamics. It provides a higher level of cyber security by integrating the influence of typing force while excluding the effects from undesirable sources, such as inadvertent touch and changes on typing surfaces. Security concerns about password leaking can be greatly alleviated. The approach can be even more reliable than fingerprint based authentication that can be easily replicated. Meanwhile, the rationally designed, unconventional keystroke device is flexible, stretchable and water/dust proof, which makes it highly mobile and applicable to versatile working environments. Hence, its application as input devices in the financial and computing industry is promising and meaningful for user identification and information protection.

Methods

Fabrication of the triboelectric keystroke device

Pre-cured silicone rubber (Ecoflex 00-50, Smooth-On) was prepared by mixing the two components in a 1:1 volume ratio., and acrylic molds for top and bottom silicone shells are fabricated using a laser cutter (PLS6.75, Universal Laser Systems). The prepared silicone rubber was casted into the acrylic molds and cured at 50 °C for 6 h. The top and bottom silicone shells of the triboelectric keystroke device were then peeled off from the molds. Thin films of PET were coated with ITO using magnetron sputtering (PVD75, Kurt J) and laser-cut into the size of a single key. Two-sided coated PET films were placed onto the top silicone shell and covered with another layer of silicone, i.e., the top inner cover; One-sided coated PET films were pasted onto the bottom silicone shell with the ITO layer facing up. Finally, the top and bottom parts of the triboelectric keystroke device were assembled together using the pre-cured silicone rubber as the glue. A superhydrophobic coating (Rust-Oleum® NeverWet®) was facilely sprayed onto the device to achieve a water and dust resistant surface and the contact angle was measured using a ramé-hart Model 250 Standard Goniometer.

COMSOL® simulation of the potential distribution

A 1-cm wide, 200-μm thick silicone layer with a uniform negative charge density of 100 μC/m^2 on the top surface was first constructed in COMSOL®. Then the potential distribution was numerically calculated for the case without the shield electrode. In the case with the shield electrode, a grounded electrode was placed below the charged silicone, followed by the calculation of the potential distribution.

Electrical output measurements

The open-circuit voltage and short-circuit current from the triboelectric key were measured by a Keithley 6514 system electrometer. Reduced voltage outputs after the capacitor/resistor-based voltage division were measured by an ADC (NI 9220, 16-Channel Voltage Measurement Module, ±10 V, National Instrument), which was also used for the

multichannel measurement. For the voltage-force and durability testing in Figures 2b and S2a the typing motion was stimulated using a 1-cm × 1-cm acrylic covered by a nitrile glove and driven by a programmable linear motor. All other signals were from human typing.

Signal processing and software interface

The signal acquisition, timing synchronization, and the graphical user interface were implemented using LabVIEW 2016. The signal processing including denoising, feature extraction, and classification was implemented with MATLAB® 2016b. Some core algorithms are accelerated with C++. Please refer to Supplementary Notes for the details of the proposed algorithm for feature extraction and SVM based classification.

Acknowledgements

Research was supported by the Hightower Chair foundation, and the "thousands talents" program for pioneer researcher and his innovation team, China, the National Key R & D Project from Minister of Science and Technology (2016YFA0202704), National Natural Science Foundation of China (Grant Nos. 51432005, 5151101243, 51561145021). Patents have been filed based on the research results presented in this manuscript.

Appendix A. Supplementary data

Supplementary data associated with this article can be found, in the online version, at https://doi.org/10.1016/j.mattod.2018.01.006.

References

[1] R.J. Spillane, Tech. Discl. Bull. 17 (1975).
[2] S.P. Banerjee, D.L. Woodard, J. Pattern Recognit. Res. 7 (2012) 116–139.
[3] M.L. Ali et al., J. Signal Process. Syst. 86 (2017) 175–190.
[4] F. Monrose, A.D. Rubin, Future Gener. Comput. Syst. 16 (2000) 351–359.
[5] W.E. Burr et al., NIST Special Publication 800-63-2, National Institute of Standards, 2011.
[6] R.S. Gaines et al., Authentication by Keystroke Timing: Some Preliminary Results, RAND Corporation, 1980.
[7] A. Sulong, Wahyudi, M.U. Siddiqi, 2009 5th Int. Colloq. on Signal Process. & Its Appli. (2009) 151–155.
[8] H. Ali, Wahyudi, M.J.E. Salami, 2009 5th Int. Colloq. on Signal Process. & Its Appli. (2009) 198–203.
[9] C.C. Loy, W. Lai, C. Lim, ASEAN Virtual Instrum. Appli. Contest Submiss. (2005).
[10] S.S. Shen, et al. 2016 Int. Conf. on Appl. Syst. Innov. (ICASI) (2006) 1–4.
[11] Y. Yang et al., ACS Nano 7 (2013) 9213–9222.
[12] G. Zhu et al., Nano Lett. 14 (2014) 3208–3213.
[13] J. Chen et al., ACS Nano 9 (2015) 105–116.
[14] C. Cortes, V. Vapnik, Mach. Learn. 20 (1995) 273–297.
[15] Z.L. Wang, J. Chen, L. Lin, Energy Environ. Sci. 8 (2015) 2250–2282.
[16] S. Niu et al., Energy Environ. Sci. 6 (2013) 3576–3583.
[17] F.-R. Fan, Z.-Q. Tian, Z.L. Wang, Nano Energy 1 (2012) 328–334.
[18] S. Li et al., ACS Nano 10 (2016) 7973–7981.
[19] X. Pu et al., Sci. Adv. 3 (2017) e1700694.
[20] F. Baccelli, B. Błaszczyszyn, Found. and Trends® in Netw. 4 (2010) 1–312.
[21] I.T. Jolliffe, Principal Component Analysis, Springer, New York, 2002, pp. 111–149.
[22] C.-C. Chang, C.-J. Lin, ACM Trans. Intell. Syst. Technol. 2 (2011) 1–27.
[23] R.-E. Fan, P.-H. Chen, C.-J. Lin, J. Mach. Learn. Res. 6 (2005) 1889–1918.
[24] C.-W. Hsu, C.-J. Lin, IEEE Trans. Neural Netw. 13 (2002) 415–425.
[25] H. Wang, D. Lymberopoulos, J. Liu, Wirel. Sens. Netw.: 12th Eur. Conf. Proc. (2015) 168–185.
[26] R.G. Gallager, Discrete Stochastic Processes, Springer, US, 1996, pp. 31–55.