APPLIED SCIENCES AND ENGINEERING

A flexible pressure sensor array for self-powered identity authentication during typing

Tongtong Zhang[1], Farid Manshaii[2], Chris R. Bowen[3], Maoyi Zhang[1], Weiqi Qian[1,4], Chaosheng Hu[1,4], Yanan Bai[1,5], Zhijie Huang[1,5], Ya Yang[1,4,5]*, Jun Chen[2]*

The keyboard, a staple tool for information entry and human-machine interaction, faces demands for enhanced information security due to evolving internet technologies. This study introduces a self-powered flexible intelligent keyboard (SFIK) that harnesses the giant magnetoelastic effect to convert the mechanical pressure from key presses into electrical signals. The sensor boasts a wide sensing range (35 to 600 kPa) and a rapid response time (~300 ms), allowing it to record and recognize individual keystroke dynamics. Integrated with machine learning, this keyboard enables identity authentication through both fixed- and dynamic-text inputs. It accurately authenticates fixed passwords of eight characters with a 95.3% success rate and dynamic text from 14 sets of double keys with 100% accuracy. Given its capabilities, the SFIK offers promising applications in artificial intelligence, network security, and access control for computers and networks.

INTRODUCTION

With the rapid development of modern technologies and artificial intelligence, the need for information security has become more critical than ever (*1*–*3*). Information encryption and identity recognition technologies (*4*–*6*) are two main approaches to achieving information security. Among these, identity authentication through passwords is the most widely used method. It verifies authorized users and serves as the first line of defense for information security. However, this traditional method has its limitations when confronted with evolving cyber threats. Identification methods (*7*–*10*) that leverage biophysiological features, including facial recognition and fingerprint scanning, provide improved security. However, the need for specialized equipment often restricts their broad implementation. Moreover, these authentication approaches are verified only at the time of login and do not provide continuous authentication during use. Therefore, there is a need to develop identity authentication systems that are widely available, cost-effective, minimally invasive, and highly interactive for ensuring information security.

The research area of keystroke dynamics (*11*–*14*) studies behavior patterns to identify users according to their unique typing attributes (*15*–*18*), such as keystroke duration, hold time, interval, errors, and force. The advantage of keystroke dynamics lies in its behavioral characteristic, which is difficult to imitate and does not necessarily require additional equipment.

Previous work has explored solutions using flexible materials based on piezo-resistive (*19*, *20*) and capacitance effects (*21*). However, for piezo-resistive and capacitive devices, challenges include hysteresis, robustness, and environmental interference. To reduce device power consumption, self-powered sensing mechanisms, such as those based on triboelectric (*22*–*27*) and piezoelectric effects (*28*, *29*), have unique advantages in developing sustainable portable systems. Yet, the triboelectric signal is affected by humidity (*30*–*32*), which is crucial for skin-interfaced devices exposed to sweat. In addition, there are limitations (*33*, *34*) in mechanical stability, material quality, and chemical stability of the device, restricting its potential for large-scale production. Inspired by the success of these concepts, an in-depth search is underway to create generators that can provide sufficient current with low electrical impedance to power conventional electronics and to monitor key press events, body movements, and other physiological parameters.

In this work, we report a flexible pressure sensor based on a porous, soft magnetoelastic polymer. The sensor's operation is based on the giant magnetoelastic effect recently discovered in the soft polymer systems (*35*–*41*), as shown in Fig. 1A, which converts the keystroke biomechanical activities into high-fidelity electrical signals via a combination of magnetoelastic effect and electromagnetic induction (*35*). The manufacturing process for stretchable pressure sensors is depicted in fig. S1. We designed a flexible electrical circuit (fig. S2) to assemble with the pressure magnetoelastic sensor arrays to create a self-powered flexible intelligent keyboard (SFIK) system; see Fig. 1B. The keyboard buttons are shown in Fig. 1C. For fixed-text identification, useful for initial login authentication via a password, the SFIK uses machine learning (ML) to learn and analyze keystroke characteristics such as input time and stroke force of different users, achieving a recognition accuracy reaches of 95.3%.

Furthermore, for dynamic text identification, we selected 10 groups of double key events representing the most frequent keyboard tapping combinations in English, such as "er" and "en." This enables the identity authentication system to achieve continuous and real-time monitoring of user identity, with a recognition accuracy of 100%. The fixed-text approach provides auxiliary authentication as the user logs in, while the dynamic text approach continuously monitors the identity after logging in; see Fig. 1D. This combination not only ensures information security but also enhances the accuracy of authentication, offering an important direction for data security. Thus, this work could lead to substantial advances in biometric systems, with potential applications in wearable electronics, artificial intelligence, cybersecurity, and human-computer interaction (Fig. 1E).

[1]CAS Center for Excellence in Nanoscience, Beijing Key Laboratory of Micro-Nano Energy and Sensor, Beijing Institute of Nanoenergy and Nanosystems, Chinese Academy of Sciences, Beijing 101400, P. R. China. [2]Department of Bioengineering, University of California, Los Angeles, Los Angeles, CA 90095, USA. [3]Department of Mechanical Engineering, University of Bath, Bath BA2 7AK, UK. [4]School of Nanoscience and Technology, University of Chinese Academy of Sciences, Beijing 100049, P. R. China. [5]Center on Nanoenergy Research, School of Physical Science and Technology, Guangxi University, Nanning 530004, P. R. China.
*Corresponding author. Email: yayang@binn.cas.cn (Y.Y.); jun.chen@ucla.edu (J.C.)

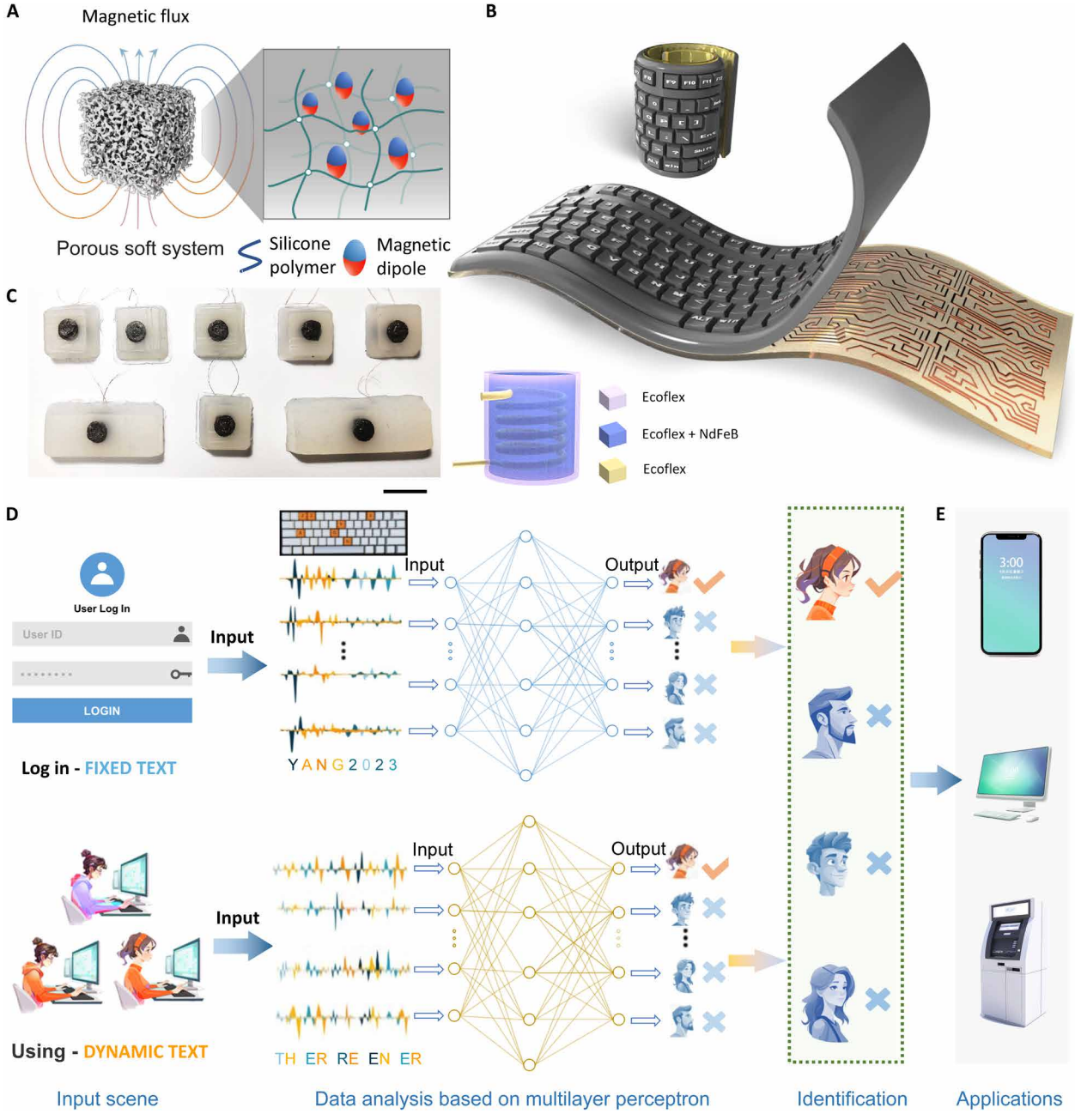

Fig. 1. An overview of the self-powered flexible intelligence keyboard for personalized keystroke dynamics. (**A**) Schematic of SFIK. (**B**) Detailed view of porous, soft magnetoelastic system's internal structure, illustrating the alignment of magnetic dipoles within the soft polymer matrix. The inset provides a detailed view of the composition of the keyboard buttons. (**C**) Photograph of several buttons of the SFIK. The scale bar is 10 mm. (**D**) Architecture and application scenarios of ML algorithms in dual-mode identity authentication systems, enhancing both robustness and universality. This system enables identity verification through both fixed- and dynamic-text inputs. (**E**) System's application in artificial intelligence, network security, and human-machine interaction.

RESULTS

Giant magnetoelastic effect in soft material systems

After incorporating solid magnetic nanoparticles, viscous silicone polymer, and microbubbles, we observed a substantial magnetoelastic effect in the resulting porous, soft polymer (Fig. 1B). By applying a pulsed magnetic field, the embedded magnetic nanoparticles within the polymer are reoriented. Scanning electron microscopy (SEM) images, presented at various magnifications in fig. S3, illustrate the microstructure of the porous soft magnetoelastic polymer, showcasing the even distribution of magnetic nanoparticles within the polymer matrix. To enhance the device's durability, a layer of silicone encases the magnetoelastic composite, with the device's overall structure displayed in fig. S4. By coupling magnetoelasticity with electromagnetic induction, each key unit is inherently waterproof, as magnetic fields can penetrate water. In addition, it remains stable under temperature fluctuations near room temperature. The sensing performance

of each magnetoelastic key unit under varying humidity and temperature conditions is shown in fig. S5.

Subjecting the composition to pulsed magnetization induces the rotation and movement of the magnetic nanoparticles within the polymer, leading to a chain arrangement, as depicted in Fig. 1B, and maintaining a remanent magnetic intensity of 41 emu/g (Fig. 2A). Integrating microbubbles to create a porous structure within the flexible silicone system reduces Young's modulus, facilitating larger mechanical deformation. This improvement enhances the biomechanical-to-magnetic energy conversion efficiency. Figure 2 (A and B) demonstrates that incorporating air microbubbles to increase mechanical compliance results in a significant change in the soft polymer system's remanence (ΔBr) before and after uniaxial compression. By varying the concentration of magnetic nanopowder in the polymer matrix, we can control the mechanical modulus and magnetic strength. A platform was designed to monitor variations in magnetic properties and magnetization intensity under uniaxial pressure (see fig. S6). Figure 2C shows the magnetization change in the porous soft magnetoelastic polymer under vertical stress, and Fig. 2D illustrates the magnetization intensity change during a compression-release process typical of a key press.

Under constant uniaxial pressure, the composite containing 400 weight % (wt %) magnetic nanoparticle concentration (2500 mT) exhibits the largest variation in magnetic flux density, while composites

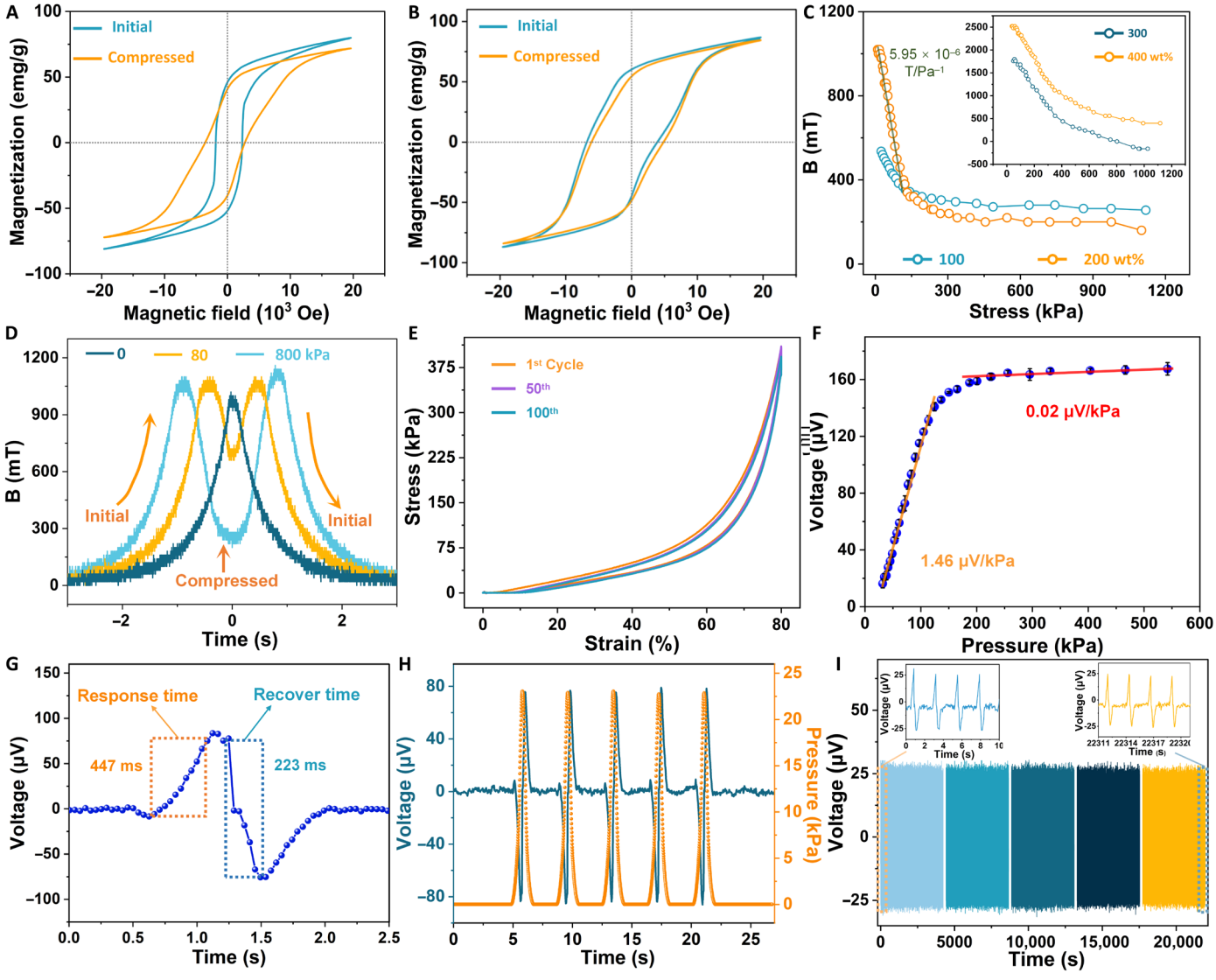

Fig. 2. Pressure sensing evaluation of each magnetoelastic key unit. (**A**) Hysteresis loops of porous and nonporous, soft magnetoelastic polymers, displayed with and without the application of uniaxial stress. (**B**) Hysteresis loop of porous and nonporous, soft magnetoelastic polymers, displayed with and without the application of uniaxial stress. (**C**) Changes in the magnetic field of the porous soft magnetoelastic polymer with different micromagnet concentrations under pressures ranging from 0 to 1200 kPa. (**D**) Magnetic field variation in the polymer during compression. (**E**) Device's cyclic stress-strain response over 100 cycles at 200 wt % micromagnet concentration. (**F**) Graph showing the sensor's pressure sensitivity across different pressures, with error bars indicating SDs from three measurements. (**G**) Voltage (V)–time (T) curve displaying a rapid response time of 447 ms and recovery time of 223 ms. (**H**) Output voltage and external tension waveforms correspond closely with the cyclic loading and unloading process. (**I**) Mechanical durability test results show consistent performance over 10,000 stretch-release cycles at 50 kPa. An inset provides a detailed view of a marked region.

with lower concentrations of 100 wt % (300 mT), 200 wt % (800 mT), and 300 wt % (1800 mT) show reduced variations, decreasing with a lower nanoparticle fraction. As shown in Fig. 2C, the magnetic flux density decreases with increasing applied stress, from 0 to 1200 kPa, achieving a maximum magnetic coupling coefficient of 5.95×10^{-6} T/Pa, which is 476 times greater than that of Fe-Co alloy metal; see table S2 (*36*, *43*). This significant change in magnetization flux intensity during a single compression-release event highlights the material's suitability for keyboard applications. At constant pressure loading, compared to devices with higher doping concentrations (>30 kPa), the difference in the maximum stress required between the first and 100th cycles are smaller when the concentration of the magnetic nanoparticles is 200 wt % (<20 kPa) (see fig. S7). Furthermore, the magnetic coupling coefficient at 200 wt % nanoparticle concentration (5.95×10^{-6} T/Pa) surpasses those at 100 wt % (5.26×10^{-6} T/Pa), 300 wt % (4.19×10^{-6} T/Pa), and 400 wt % (4.73×10^{-6} T/Pa).

The pronounced magnetoelastic effect observed in soft systems arises from changes in the microstructure of magnetic nanoparticle chains under mechanical deformation (*35*). Specifically, when external stress is applied to a magnetoelastic material, its internal magnetic domain structure reconfigures to accommodate the new stress conditions, leading to a variation in magnetic flux density. The giant magnetoelastic effect in this porous soft magnetic polymer originates from mechanisms operating at two physical scales (*35*–*42*, *44*): The first is the magnetic particle-particle interaction (MPPI), which is the interactions among the magnetic nanoparticles that alter their distance and orientation under external pressure. The second mechanism, stemming from magnetic dipole-dipole interaction (MDDI), operates at the atomic scale, resulting from the rotation and motion of magnetic dipoles within nanoparticles due to applied stress. Therefore, the interaction within the connected particle chain is independent of the external magnetic field. Consequently, our experimental results reveal that even a small level of externally applied pressure (9.6 kPa) can lead to significant magnetic field changes (5.95×10^{-6} T/Pa) in the soft polymer composite.

Constructing a soft magnetoelastic sensor

The giant magnetoelastic effect enables the conversion of applied stress into changes in the magnetic field within a porous soft magnetoelastic polymer. These changes in magnetic flux generate an electrical signal. Using this phenomenon, we construct flexible pressure sensors and design circuits to ultimately connect them, forming a sensor array. The core of the sensor unit, as illustrated in fig. S4, consists of a flexible magnet encased in a copper coil and covered by an Ecoflex sleeve. Unlike traditional permanent magnets, this soft magnetoelastic sensor integrates seamlessly with copper coils and withstands high pressures (>600 kPa). The sensor facilitates electromechanical conversion by holding a conductive coil, ensuring the flexible sensing unit maintains high electrical conductivity under high pressure and strain. This enhances the sensing unit's robustness. During an individual compression-release cycle, the magnetic flux through the copper coil changes, inducing an electromotive force. According to Faraday's law of electromagnetic induction, this force is produced in a closed circuit due to changes in magnetic flux. The induced electromotive force (ε) is defined as $\varepsilon = -N\frac{d\varphi}{dt}$, where N is the coil count, φ represents the magnetic flux, and t denotes time. Figure S8 illustrates the device's operating principle and response. To visualize and quantify strain and magnetic flux changes during compression, we simulated the compression process using COMSOL, depicted in fig. S9.

To quantitatively evaluate the electrical performance of the compressed sensing unit, we developed a constant-velocity compression device. The sensor's pressure sensitivity (S) is defined as $S = \frac{\Delta\varphi}{\Delta P}$, where $\Delta\varphi$ signifies the voltage change, ΔP the changing pressure. Figure S10 displays the voltage magnitude of the sensing unit under various pressures. As Fig. 2F and fig. S11 indicate, sensitivity below an applied pressure of 150 kPa reaches 1.46 μV/kPa, declining to 0.02 μV/kPa to in the high-pressure range (150 to 550 kPa). The mass ratio of magnetic powder to silica gel polymer also influences sensitivity (fig. S12), with a 200 wt % magnetic nanoparticle concentration showing peak sensitivity under 150 kPa. Given its application in keyboards and wearable sensors, we selected soft polymer composites with a 200 wt % magnetic particle concentration as the responsive component.

We will now examine the sensor's response time to external forces during compression and release, which is essential for assessing performance in real-time human-computer interaction tasks. The response time is defined as 90% of the duration from the steady-state transition to the final voltage. Similarly, the recovery time is the interval required for the signal to return to 90% of the steady-state value from the maximum response, as shown in Fig. 2G. Figure 2G demonstrates the sensor's rapid response to both loading and unloading, with a response time of ≈447 ms and a recovery time of ≈223 ms. This allows the device to quickly detect changes in mechanical stimuli. With negligible hysteresis (Fig. 2H), the output signal remains consistent at a pressure of approximately 23 kPa. The device's stability during mechanical cycling, as depicted in Fig. 2I, is crucial for long-term operation. After more than 10,000 compression-release cycles at approximately 50 kPa, the sensor output voltage change is minimal, under 2%. The inset in Fig. 2I presents the sensor's output voltage waveforms at the initial and final stages of the compression-release cycle, remaining nearly constant.

Therefore, our sensors exhibit notable advantages over advanced pressure sensors, including high stretchability, excellent mechanical durability, and heightened sensitivity. In addition, each component of the sensing unit is crafted from cost-effective materials (table S3) and can be produced through a scalable manufacturing process. These features enable a rapid and accurate response to pressure through electrical signal production, meeting a wide range of practical application requirements. By harnessing the unique structural features and sensing capabilities of the sensor, we are developing an innovative smart keyboard that seamlessly integrates identity authentication with daily typing.

A magnetoelastic intelligent keyboard

A static keystroke analysis is designed to perform evaluations based on fixed-text inputs, such as combining an account and password during system logins, to facilitate two-factor authentication. The sensor crafted from a flexible material into a compressible structure, can be integrated into a pressure sensor array. We have engineered this sensor array to create a SFIK, as illustrated in Fig. 1A, incorporating an integrated circuit. This design enables the recognition of specific letters and individual key presses throughout the typing process. Figure 3 (A and B) displays the keyboard and the printed circuit board (PCB), respectively, while fig. S2 details the circuit connections of the keyboard. The system's block diagram for identity authentication is depicted in

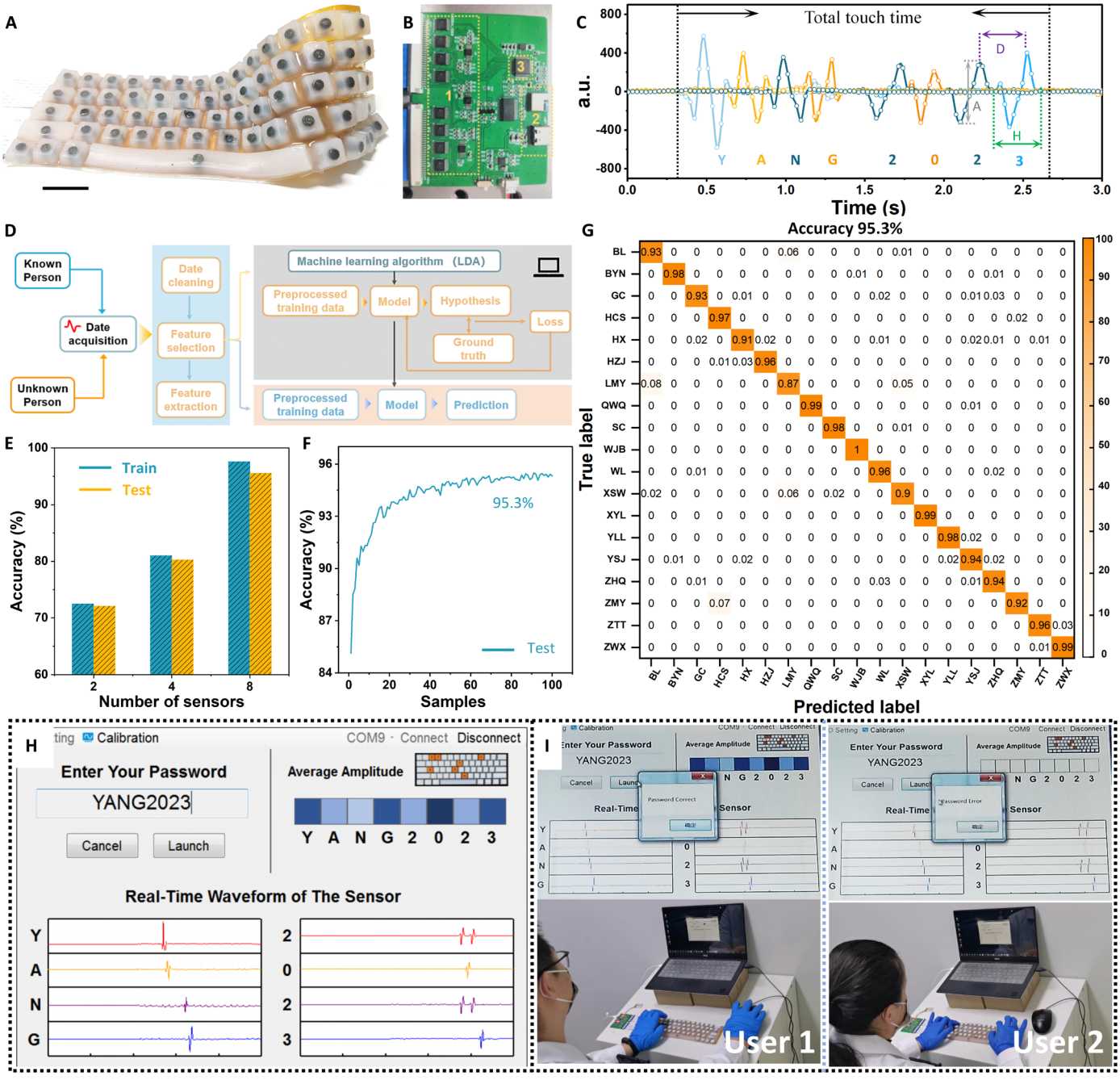

Fig. 3. The magnetoelastic intelligent keyboard based multidimensional identity authentication system. (**A**) Photograph of SFIK. The scale bar is 5 cm. (**B**) Photograph of PCB. (**C**) Graph depicting the waveform generated by a subject entering the password "YANG2023," including metrics such as keystroke force, timing intervals, and duration. (**D**) Flowchart outlining the ML process for the fixed text–based identity authentication system. (**E** to **F**) Graphs showing prediction accuracy variations to the number of sensors used and the sample size, respectively. (**G**) Confusion matrix of ML outcomes for 19 objects using eight channels. (**H**) User interface of the computer for the identity authentication system. (**I**) Photographs of different subjects using the SFIK for login purposes.

fig. S13, which also elucidates the functions and contents of the digital markings on the PCB. The SFIK keyboard is compatible with both standard universal serial bus interfaces and Bluetooth connection. The keyboard is also being developed as part of our proprietary identity authentication system, which allows for real-time input and instant feedback, notably improving the user experience. The software is compatible with computers running the Windows operating system.

The act of pressing a single key is segmented into a "press" and "bounce" process. The system generates a time-current signal curve that represents a comprehensive result derived from multiple data dimensions, including keystroke frequency, keystroke force, and the intervals between keystrokes. Any alteration in the typing conditions will directly influence the shape of this output. Upon a keystroke, various signal processing techniques, such as denoising,

baseline cancellation, and peak detection, are used to extract features (as defined in Fig. 3C) such as typing delay (D), hold time (H), signal amplitude (A), and key force. These features are derived from the electrical signals generated by different individuals using the keyboard, as dynamically recorded and analyzed. Any alteration in the typing conditions will directly influence the shape of this output. For instance, Fig. 3C showcases the waveform for a password input "YANG2023," and fig. S14 illustrates the signals from 19 testers entering eight-digit passwords. We collected data from each tester as they entered their password 120 times.

ML techniques are used to further analyze and distinguish between keyboard users based on the collected features. ML techniques are applied to sift through the time-domain data collected by the SFIK, highlighting the distinct differences between keyboard users. However, direct time series data analysis can be computationally intensive, both in time and memory. Hence, efficient feature extraction through ML requires identifying the most impactful features for prediction accuracy, such as the maximum and minimum values, the range, the intervals between peaks and troughs, and so on. Figure 3D outlines the ML process for identification based on fixed-text input using the SFIK, starting with data preprocessing of known individuals' inputs, followed by principal components analysis for feature extraction. This process leads to a reduction in the dimensionality of the data, eliminates redundant information, extracts key features, and improves our understanding and analysis of the data. We then proceeded to train the ML models, tailoring them with feature engineering based on the training samples. As the training iterations progress, the ML model steadily attains a higher classification accuracy enabling it to achieve identity authentication for fixed-length text. In addressing the challenge of time series classification, we used four algorithms to gauge accuracy: logistic regression, naïve Bayes, random forest, and multilayer perceptron classifiers. The predicted results are presented in table S4. Two channels (sensor count) are noted in Fig. 3E; the data show less distinction and ML classification accuracy stands at merely 73%. However, as the channel count increases, so does the accuracy. Using fixed text comprising eight letters and numbers, reminiscent of standard passwords, elevates the accuracy rate to as high as 95.3%. Furthermore, the sample size plays a critical role in the accuracy of the ML model, showing improvement as the number of samples grows (see Fig. 3F). A confusion matrix for 19 individuals, depicted in Fig. 3G, reveals that all participants achieved over 90% perceptual accuracy.

To explore the practical feasibility of integrating a flexible keyboard with ML for user recognition, we developed an identity authentication system. We conducted multiple experiments using data from various participants, feeding diverse datasets into the trained ML model. However, all attempts failed to achieve successful identity verification. The system integrates the SFIK, a data acquisition module, a transmission module, and a display interface. Displayed in Fig. 3H, the computer terminal's interface for the identity authentication system features a real-time waveform diagram in its lower segment. The top left panel serves as the password input screen, while the top right panel shows a color display calibrated according to the average amplitude strength size of User 1, the approved user, obtained during the ML process, we set the system's login password. Five students were given access to enter the password sequentially to log into the system. Their interactions are documented in Fig. 3I and movie S1. Only the approved User 1 receives a "Password Correct" message upon entering the correct password and clicking "Launch." This highlights the SFIK's capacity to precisely and consistently verify a user's identity, ensuring secure and authorized access.

Personalized keystroke dynamics

Continuous identity monitoring cannot be achieved through a single login event alone. Therefore, a continuous authentication technology is required to protect system security in real time and prevent unauthorized user changes during use. In response to the challenges posed by traditional authentication methods, we have designed an identity authentication technology based on the features of dynamic text keystrokes to continuously monitor user identity in real time. Since a user's input varies over time, a fixed-text keystroke feature extraction approach is impractical. During dynamic text–based keystroke authentication, the irregularity of the user's typing input results in a substantial amount of data. To obtain the necessary data for our experiment, we invited 10 users to participate in data collection, each typing different types of text ranging from approximately 700 to 900 words (fig. S16), extracted from an article (*45*), as shown in fig. S16. To enhance data processing efficiency and reduce data volume, we selected 10 double key entries with the highest frequency in English: "er," "th," "in," "an," "en," "he," "re," "on," "at," and "ed." (For various double-key entries, the quantity across different texts ranges approximately from 50 to 110 instances.) From these, we extracted double bond features such as typing delay (D), hold time (H), total touch time (T), and signal amplitude (A).

We developed a dynamic text predictive voting system to facilitate identity authentication during use. Figure 4A displays the detailed flowchart of the predictive voting system for identity recognition, supported by ML. Initially (Fig. 4A, first step), we extract double-key data from the text, and Fig. 4B shows the waveform and extractable features of five double bonds. After analyzing the data, we determined that the delay time should be short (<0.5 s) due to the high proficiency of users performing high-frequency double-keystrokes. If two adjacent keys form a double-key combination, we select those with an interval time of less than 500 ms. Next (Fig. 4A, second step), after selecting and extracting features for 10 types of double-key data, we establish an ML model between the feature matrix and labels, continuously iterating to create a trust model. We then obtained the confusion matrix of 10 double bonds, as shown in Fig. 4 (C to E) and fig. S15. By choosing double-key entries (two channels) to extract keystroke features, the final accuracy ranged only from 60 to 85%. To further enhance the accuracy of identity authentication, we designed a voting system based on the double keys (Fig. 4A, third step). During keyboard use, when a double click is recognized, the trust model is used for identity recognition with a single double-key entry, and the result is recorded. Then, as more text is input, additional double-key entries are used for identity recognition. We have specified the number of double keys included in the recognition unit within the system. Upon reaching the maximum number, we select the recognition result for each double key and choose the most frequent result as the final character identity. We then compare the voting results with the user identity to determine whether identity authentication is successful.

In the voting system, we explored the impact of different text lengths and types of double-key entries on accuracy. Figure 4F displays the confusion matrices for text with six double-key lengths and three types of double keys, where the accuracy was only 78.5%. However, as the text length increased, the accuracy of the voting

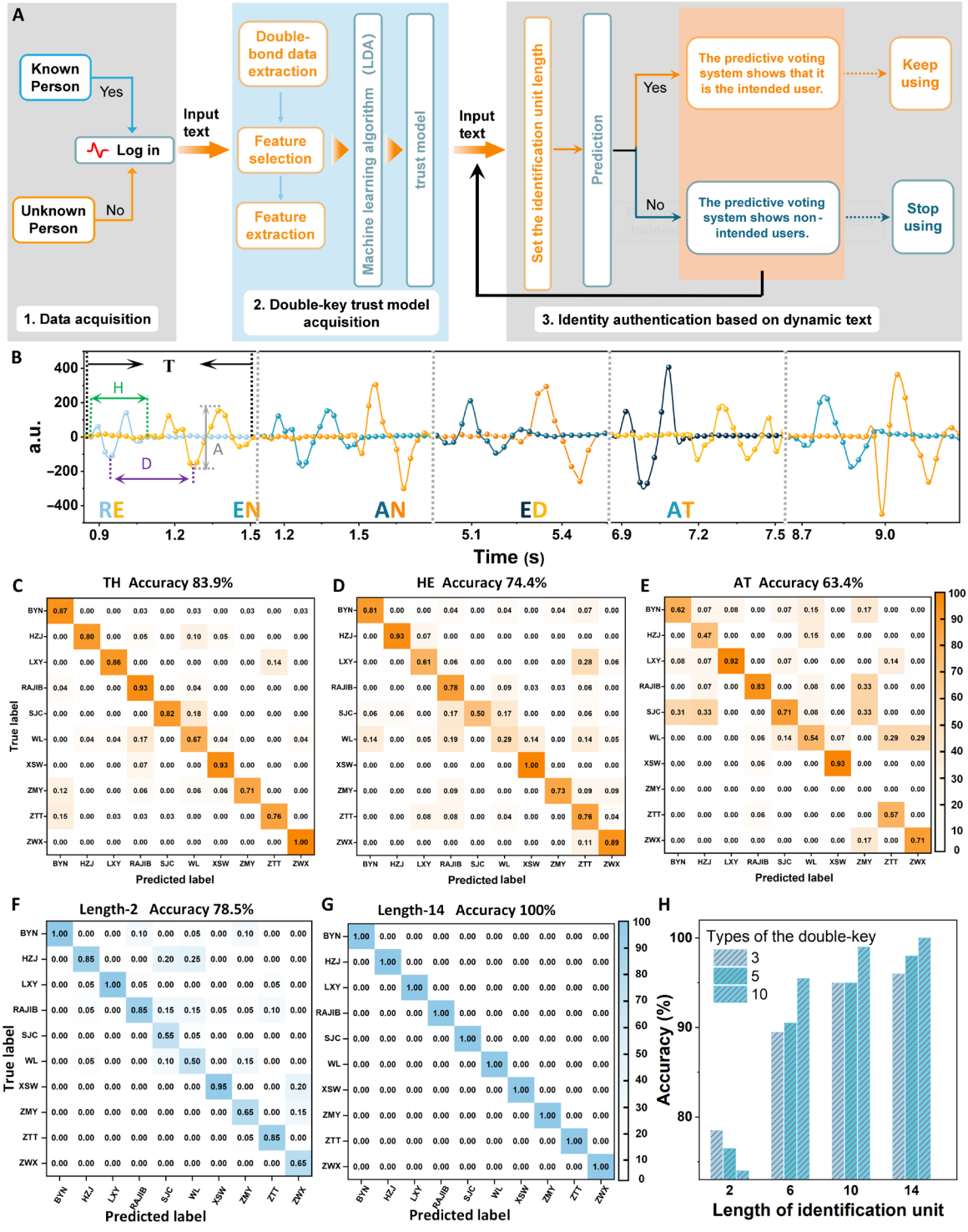

Fig. 4. Personalized keystroke dynamics for multidimensional identity authentication. (**A**) Flowchart describing how the identity authentication system, which relies on ML, processed fixed text. (**B**) Displays the waveforms corresponding to five instances of double bonds. (**C** to **E**) Confusion matrices showing the ML performance for three sets of double bonds across 10 individuals. (**F** and **G**) Confusion matrices for the ML outcomes of 10 individuals analyzed with 10 different types of double bonds, in scenarios where the texts contain six double bonds. (**H**) Illustrates a graph of the system's prediction accuracy, highlighting how it varies with different numbers of double bonds and lengths of text.

system also significantly improved. Figure 4G shows the confusion matrices for text with 14 double-key lengths and 10 types of double-key events, where the accuracy reached 100%. Figure 4H details the effects of double key types, from 3 to 10, and text lengths, ranging from 2 to 14, on the identity authentication system. When entering 10 types of double keys for text containing 14 double keys, the accuracy reached 100%.

DISCUSSION

We have developed an innovative SFIK by integrating the giant magnetoelastic effect with magnetic induction in soft systems. The SFIK comprises a pressure sensor array based on a type of sensor using magnetoelastic soft composite, boasting a range of innovative features: high sensitivity, stable performance under high pressure, low cost, construction from readily available raw materials, and self-powered functionality. In comparison to other authentication systems, the SFIK excels in using keystroke dynamics to identify the personal characteristics of users as they type.

A dual-mode identity authentication system has been implemented, capable of authenticating identities through both fixed- and dynamic-text analysis. The system achieves an identity authentication accuracy of 95.3% for fixed-text logins. For dynamic text, we have introduced a long-text authentication system that focuses on double-key events, the most frequently occurring consecutive keystrokes in English. With the aid of ML techniques, this system can achieve 100% accuracy in identity recognition for long text entries that include 14 sets of double keys, significantly mitigating security risks associated with password leaks.

This method proves more reliable than fingerprint-based authentication, which can be easily replicated. Unlike fingerprint systems that offer only auxiliary authentication at login, our method continuously monitors dynamic text to verify user identity during keyboard usage. Combining these two authentication approaches not only enhances information security but also increases authentication accuracy, offering an important direction for data security.

Given its outstanding features, mechanical flexibility, self-powered sensing, affordability, and high precision, the SFIK holds promising applications in wearable bioelectronics, artificial intelligence, cybersecurity, and human-computer interaction. The SFIK distinguishes itself through its innovative application of keystroke dynamics, offering a promising technology for various use cases. However, scaling this system for real-world implementation presents several challenges. One significant issue is the difficulty in collecting consistent and accurate keystroke data across diverse devices and user interfaces. In addition, it is crucial to prioritize user privacy and security when managing sensitive keystroke information. Effectively addressing these challenges will be vital for the successful deployment and widespread adoption of the SFIK in practical, real-world scenarios.

MATERIALS AND METHODS

Fabrication of NdFeB-Ecoflex composite materials

$Nd_2Fe_{14}B$ magnetic powders hold a particle size of 100 mesh (~150 μm). A silicone elastomer (Ecoflex 0020) was synthesized by combining Part A and Part B in a 1:1 weight ratio. No additional treatments were applied to the chemicals.

Fabrication of stretchable strain sensors

The manufacturing process for stretchable strain sensors is depicted in fig. S1. Initially, a 150-turn copper coil was placed at the center of a 5 mm by 5 mm by 3 mm cube and shaped using a laser engraving machine (fig. S1, A and B). Subsequently, 2 g of both Ecoflex A and B were mixed in a beaker until uniform. An 8-g portion of $Nd_2Fe_{14}B$ magnetic powders was then integrated with the Ecoflex mixture to form a black, homogeneous substance (fig. S1C). This mixture was carefully transferred into the mold of a hollow cube, which was then solidified at 60°C and then postremoval from the mold (fig. S1D). The spring element served as the electrical component, while the $Nd_2Fe_{14}B$ magnetic powders were used as the magnetic constituent. After magnetization in a high-voltage magnetic field along its axial direction, a 5 mm by 5 mm by 5 mm composite magnetoelectric elastic conductor was manufactured (fig. S1E). Last, the sample was encased in an Ecoflex colloid and allowed to cure at room temperature for 1 hour, resulting in a sensor with a 6 mm final outer diameter (fig. S1F).

Characterizations and measurements

The $Nd_2Fe_{14}B$ magnetic powders and their nanocomposites were analyzed using a field-emission scanning electron microscope (SEM, ZEISS GIMINER 300). Samples were prepared using a laser engraving machine (Universal, PLS 4.75). Mechanical tensile tests of the composite materials were performed using a universal testing machine (ESM301-50 N) at a tensile speed of 100 mm/min. Electrical characterization was conducted with a Keithely 2611B system, managed by computer software. A stretcher (Yuelian S81) facilitated the compression-release process.

Supplementary Materials

The PDF file includes:

Supplementary Notes S1 and S2
Tables S1 to S4
Figs. S1 to S16
Legend for movie S1

Other Supplementary Material for this manuscript includes the following:

Movie S1

REFERENCES AND NOTES

1. K. K. R. Choo, The cyber threat landscape: Challenges and future research directions. *Comput. Secur.* **30**, 719–731 (2011).
2. J. Cook, S. U. Rehman, M. A. Khan, Security and privacy for low power IoT devices on 5G and beyond networks: Challenges and future directions. *IEEE Access* **11**, 39295–39317 (2023).
3. S. Kraemer, P. Carayon, J. Clem, Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Comput. Secur.* **28**, 509–520 (2009).
4. J. Kim, P. Kang, Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features. *Pattern Recogn.* **108**, 107556 (2020).
5. I. Hazan, O. Margalit, L. Rokach, Keystroke dynamics obfuscation using key grouping. *Expert Syst. Appl.* **143**, 113091 (2020).
6. C. S. Wu, W. B. Ding, R. Y. Liu, J. Y. Wang, A. C. Wang, J. Wang, S. M. Li, Y. L. Zi, Z. L. Wang, Keystroke dynamics enabled authentication and identification using triboelectric nanogenerator array. *Mater. Today* **21**, 216–222 (2018).
7. B. Li, On identity authentication technology of distance education system based on voiceprint recognition, in *Proceedings of 30th Chinese Control Conference* (Yantai, China, 2011), pp. 5718–5721.
8. J. Chen, J. Chen, Z. Wang, C. Liang, C. W. Lin, Identity-aware face super-resolution for low-resolution face recognition. *IEEE Signal Proc. Let.* **27**, 645–649 (2020).
9. P. Li, L. Prieto, D. Mery, P. J. Flynn, On low-resolution face recognition in the wild: Comparisons and new techniques. *IEEE Trans. Inf. Foren. Sec.* **14**, 2000–2012 (2019).
10. Q. Cao, L. Shen, W. D. Xie, O. M. Parkhi, A. Zisserman, VGGFace2: A dataset for recognising faces across pose and age, in *2018 13th IEEE International Conference on Automatic Face and Gesture Recognition* (2018), pp. 67–74.

11. B. Miller, Vital signs of identity. *IEEE Spectrum* **31**, 22–30 (1994).
12. A. Peacock, X. Ke, M. Wilkerson, Typing patterns: A key to user identification. *IEEE Secur. Priv.* **2**, 40–47 (2004).
13. R. Toosi, M. A. Akhaee, Time-frequency analysis of keystroke dynamics for user authentication. *Future Gener. Comp. Sy.* **115**, 438–447 (2021).
14. H. Ali, W. Wahyudi, M. J. E. Salami, Keystroke pressure based typing biometrics authentication system by combining ANN and ANFIS-based classifiers, in *2009 5th International Colloquium on Signal Processing and Its Applications (CSPA)* (2009), pp. 198–203.
15. C. J. Tsai, P. H. Huang, Keyword-based approach for recognizing fraudulent messages by keystroke dynamics. *Pattern Recogn.* **98**, 107067 (2020).
16. J. Chen, G. Zhu, J. Yang, Q. S. Jing, P. Bai, W. Q. Yang, X. W. Qi, Y. J. Su, Z. L. Wang, Personalized keystroke dynamics for self-powered human-machine interfacing. *ACS Nano* **9**, 105–116 (2015).
17. C. Cortes, V. Vapnik, Support-vector networks. *Mach. Learn* **20**, 273–297 (1995).
18. M. L. Ali, J. V. Monaco, C. C. Tappert, M. K. Qiu, Keystroke biometric systems for user authentication. *J. Signal Process Syst.* **86**, 175–190 (2017).
19. T. Kim, J. Kim, I. You, J. Oh, S. P. Kim, U. Jeong, Dynamic tactility by position-encoded spike spectrum. *Sci. Robot.* **7**, eabl5761 (2022).
20. S. L. Wang, Y. Y. Nie, H. Y. Zhu, Y. R. Xu, S. T. Cao, J. X. Zhang, Y. Y. Li, J. H. Wang, X. H. Ning, D. S. Kong, Intrinsically stretchable electronics with ultrahigh deformability to monitor dynamically moving organs. *Sci. Adv.* **8**, eabl5511 (2022).
21. W. Cheng, X. Y. Wang, Z. Xiong, J. Liu, Z. J. Liu, Y. X. Jin, H. C. Yao, T. S. Wong, J. S. Ho, B. C. K. Tee, Frictionless multiphasic interface for near-ideal aero-elastic pressure sensing. *Nat. Mater.* **22**, 1352–1360 (2023).
22. J. Chen, Z. L. Wang, Reviving vibration energy harvesting and self-powered sensing by a triboelectric nanogenerator. *Joule* **1**, 480–521 (2017).
23. T. Jin, Z. D. Sun, L. Li, Q. Zhang, M. L. Zhu, Z. X. Zhang, G. J. Yuan, T. Chen, Y. Z. Tian, X. Y. Hou, C. Lee, Triboelectric nanogenerator sensors for soft robotics aiming at digital twin applications. *Nat. Commun.* **11**, 5381 (2020).
24. Z. L. Wang, Triboelectric nanogenerators as new energy technology for self-powered systems and as active mechanical and chemical sensors. *ACS Nano* **7**, 9533–9557 (2013).
25. F. R. Fan, W. Tang, Z. L. Wang, Flexible nanogenerators for energy harvesting and self-powered electronics. *Adv. Mater.* **28**, 4283–4305 (2016).
26. X. C. Qu, Z. Liu, P. C. Tan, C. Wang, Y. Liu, H. Q. Feng, D. Luo, Z. Li, Z. L. Wang, Artificial tactile perception smart finger for material identification based on triboelectric sensing. *Sci. Adv.* **8**, eabq2521 (2022).
27. Z. Sun, M. Zhu, X. Shan, C. Lee, Augmented tactile-perception and haptic-feedback rings as human-machine interfaces aiming for immersive interactions. *Nat. Commun.* **13**, 5224 (2022).
28. Q. Q. He, Y. S. Zeng, L. M. Jiang, Z. Y. Wang, G. X. Lu, H. C. Kang, P. Li, B. Bethers, S. W. Feng, L. Z. Sun, P. Sun, C. Gong, J. Jin, Y. Hou, R. J. Jiang, W. W. Xu, E. Olevsky, Y. Yang, Growing recyclable and healable piezoelectric composites in 3D printed bioinspired structure for protective wearable sensor. *Nat. Commun.* **14**, 6477 (2023).
29. Z. L. Wang, J. H. Song, Piezoelectric nanogenerators based on zinc oxide nanowire arrays. *Science* **312**, 242–246 (2006).
30. Y. S. Fang, Y. J. Zou, J. Xu, G. R. Chen, Y. H. Zhou, W. L. Deng, X. Zhao, M. Roustaei, T. K. Hsiai, J. Chen, Ambulatory cardiovascular monitoring via a machine-learning-assisted textile triboelectric sensor. *Adv. Mater.* **33**, e2104178 (2021).
31. W. F. Yang, W. Gong, C. Y. Hou, Y. Su, Y. B. Guo, W. Zhang, Y. G. Li, Q. H. Zhang, H. Z. Wang, All-fiber tribo-ferroelectric synergistic electronics with high thermal-moisture stability and comfortability. *Nat. Commun.* **10**, 5541 (2019).
32. S. L. Zhang, M. Bick, X. Xiao, G. R. Chen, A. Nashalian, J. Chen, Leveraging triboelectric nanogenerators for bioengineering. *Matter* **4**, 845–887 (2021).
33. X. Zhao, Y. H. Zhou, Y. Song, J. Xu, J. Li, T. Tat, G. R. Chen, S. Li, J. Chen, Permanent fluidic magnets for liquid bioelectronics. *Nat. Mater.* **23**, 703–710 (2024).
34. C. M. Boutry, Y. Kaizawa, B. C. Schroeder, A. Chortos, A. Legrand, Z. Wang, J. Chang, P. Fox, Z. N. Bao, A stretchable and biodegradable strain and pressure sensor for orthopaedic application. *Nat. Electron.* **1**, 314–321 (2018).
35. Y. Zhou, X. Zhao, J. Xu, Y. Fang, G. Chen, Y. Song, S. Li, J. Chen, Giant magnetoelastic effect in soft systems for bioelectronics. *Nat. Mater.* **20**, 1670–1676 (2021).
36. X. Zhao, G. Chen, Y. Zhou, A. Nashalian, J. Xu, T. Tat, Y. Song, A. Libanori, S. Xu, S. Li, J. Chen, Giant magnetoelastic effect enabled stretchable sensor for self-powered biomonitoring. *ACS Nano* **16**, 6013–6022 (2022).
37. G. Chen, Y. Zhou, Y. Fang, X. Zhao, S. Shen, T. Tat, A. Nashalian, J. Chen, Wearable ultrahigh current power source based on giant magnetoelastic effect in soft elastomer system. *ACS Nano* **15**, 20582–20589 (2021).
38. J. Xu, T. Tat, J. Y. Yin, D. Ngo, X. Zhao, X. Wan, Z. Y. Che, K. R. Chen, L. Harris, J. Chen, A textile magnetoelastic patch for self-powered personalized muscle physiotherapy. *Matter* **6**, 2235–2247 (2023).
39. Y. Zhou, X. Zhao, J. Xu, G. R. Chen, T. Tat, J. Li, J. Chen, A multimodal magnetoelastic artificial skin for underwater haptic sensing. *Sci. Adv.* **10**, eadj8567 (2024).
40. Z. Che, X. Wan, J. Xu, C. Duan, T. Zheng, J. Chen, Speaking without vocal folds using a machine-learning-assisted wearable sensing-actuation system. *Nat. Commun.* **15**, 1873 (2024).
41. A. Libanori, J. Soto, J. Xu, Y. Song, J. Zarubova, T. Tat, X. Xiao, S. Yue, S. Jonas, S. Li, J. Chen, Self-powered programming of fibroblasts into neurons via a scalable magnetoelastic generator array. *Adv. Mater.* **35**, e2206933 (2023).
42. X. Zhao, Y. Zhou, J. Xu, G. Chen, Y. Fang, T. Tat, X. Xiao, Y. Song, S. Li, J. Chen, Soft fibers with magnetoelasticity for wearable electronics. *Nat. Commun.* **12**, 6755 (2021).
43. J. Liu, C. Jiang, H. Xu, Giant magnetostrictive materials. *Sci. China Technol. Sci.* **55**, 1319–1326 (2012).
44. G. Chen, X. Zhao, S. Andalib, J. Xu, Y. Zhou, T. Tat, K. Lin, J. Chen, Discovering giant magnetoelasticity in soft matter for electronic textiles. *Matter* **4**, 3725–3740 (2021).
45. Y. Yang, *Hybridized and Coupled Nanogenerators: Design, Performance, and Applications* (Wiley-VCH GmbH: Weinheim, Germany, 2020).

Acknowledgments

Funding: Y.Y. acknowledges the National Natural Science Foundation of China (grant no. 52072041), the Beijing Natural Science Foundation (grant no. JQ21007), and the University of Chinese Academy of Sciences (grant no. Y8540XX2D2). J.C. acknowledges the Henry Samueli School of Engineering & Applied Science and the Department of Bioengineering at the University of California, Los Angeles for their startup support. J.C. also acknowledges the Vernroy Makoto Watanabe Excellence in Research Award at the UCLA Samueli School of Engineering. **Author contributions:** Conceptualization: Y.Y. and J.C. Methodology: T.Z. and M.Z. Software: T.Z. and M.Z. Validation: T.Z. and C.H. Formal analysis: T.Z. and M.Z. Investigation: T.Z. and C.H. Visualization: T.Z., W.Q., C.H., Y.B., and Z.H. Resources: Y.Y. and J.C. Data curation: T.Z. and M.Z. Writing–original draft: T.Z. and F.M. Writing–review and editing: T.Z., F.M., C.R.B., Y.Y., and J.C. Supervision: Y.Y. and J.C. Project administration: Y.Y. and J.C. Funding acquisition: Y.Y. and J.C. **Competing interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials.

Submitted 5 August 2024
Accepted 4 February 2025
Published 12 March 2025
10.1126/sciadv.ads2297