numbers or extend your palm across a scanner when you can simply smile at a camera?

Facial recognition will also be central to enhancing our travel and financial experiences. Unlocking and driving your car, renting a vehicle, being picked up in a taxi, opening the door to your hotel room or your apartment – all will come to use the technology. In fact, the era of paperless and ticketless travel will become a reality in a surprisingly short period of time. Moving through the green channels at airports based on stand-off biometric identifiers, or having a family group recognised in one frame at immigration, can all be achieved today using existing technology.

Beyond travel and accommodation, financial transactions will also be secured by a mobile phone being detected in range, combined with successful facial recognition. This kind of two-part authentication will reduce the likelihood of fraud to practically nil. The result is, the more we grow to use and trust these technologies, the safer that society will become. So perhaps the only remaining barrier to widespread deployment is public confidence. Step forward Apple, Google, Careem and others. Facial recognition unlocking our hardware is progressively convincing people that it can provide higher levels of security and efficiency.

Putting this futurism to once side, the ability to use facial recognition live from a body-worn camera exists and works today. And it is getting ever more accurate every day that machine learning algorithms are beavering away. This technology has a major part to play in ensuring the safety of first responders and civilians alike. And so it is vital that governments invest in it sooner rather than later, particularly in the face of the growing terrorist threat to our security and way of life.

About the author

Fernande van Schelle is the product manager for facial recognition at Digital Barriers. Before working at Digital Barriers, she held numerous project, analysis and product management roles, several of which were in the defence, security and aerospace industries. She has an MBA from INSEAD, a Masters in the History of International Relations from LSE, and a BSc in Biochemistry from Newcastle University.

Reference

1. Lizzie Dearden. 'Met Police to stop investigating some 'low-level' crimes in response to £400m funding cuts'. The Independent, 16 October 2017. Accessed March 2018. http://www.independent.co.uk/news/uk/crime/met-police-spending-cuts-400-million-funding-london-crimes-not-investigated-burglary-assault-a8002746.html

Good vibrations: accessing 'smart' systems by touching any solid surface

Jian Liu, Chen Wang and Yingying Chen, Rutgers University and Nitesh Saxena, University of Alabama


Jian Liu


Chen Wang


Yingying Chen


Nitesh Saxena

The process of people authenticating themselves to verify their identity is now commonplace across many areas of our daily life. It's no longer just users of touchscreen devices like mobile phones – the growing use of smart systems means people need to identify themselves to access many other devices and daily activities, like entering their apartment, driving a vehicle and using smart appliances.

All this calls for a more flexible authentication process: and a new prototype system called VibWrite could extend finger-input authentication beyond touchscreens to any solid surface using vibrations. This system integrates passcode, behavioural and physiological characteristics and surface dependency to potentially offer a low-cost, tangible and enhanced security solution.

The need for more innovation in this area is clear. Research by MarketsandMarkets shows that the deployment of smart security access systems is set to grow at nearly 6.5% annually to reach a market value of $10bn by 2023[1]. Yet the current authentication process in smart security access systems mainly relies on traditional solutions supported by intercom, camera, card or fingerprint-based techniques. These approaches involve expensive equipment, complex hardware installation and diverse maintenance needs.

Meanwhile, there is a growing industry trend to use low-cost, low-power tangible user interfaces (TUIs) to support user authentication for various facility entrances, apartment doors and vehicles. For example, token devices (such as a smart ring, glove or pen) could be used for associating identities to their touch interactions[2, 3], and an ultra-thin sensing pad can be deployed in vehicles to perform driver authentication[4]. In addition, isometric buttons are appearing on new models of microwave ovens, stove tops and rotary inputs (eg, used by iPods) to replace the usual physical buttons and provide better functionality and flexibility.

These new approaches appear promising in terms of carrying out user authentication and operating appliances/devices in smart systems via capacitive sensing. However, these techniques require the touched surface to have electric conductivity and an electric field

that produces/stores electrical energy, which significantly limits the deployment of these solutions.

To address this area, we began researching a low-cost general user authentication approach via vibrations, called VibWrite[5], which is able to work with any solid surface for smart access systems. The convenience of executing user authentication by touching any surface is appealing. For instance, a driver could simply place their palm against the side window to enter and start a vehicle. In fact, that's already been visualised in the movie *Mission Impossible 5*, where Tom Cruise instantly unlocks the featured BMW car by pressing his palm against the window. In another example, an individual could place their hand on the door panel of their apartment to identify themselves and unlock the door, without a card or key.

"User authentication by touching any surface is appealing. A driver could place their palm against the side window to enter a vehicle. In fact, that's already been visualised in the movie Mission Impossible 5"

Again, there is a growing need for electronic appliances in smart homes to provide customised services for advanced safety – such as prohibiting children from operating risky appliances like an oven or dryer, adjusting the room temperature or lighting conditions and recommending TV content. A low-cost solution of tangible user authentication enabled on any solid surface could eliminate the need to install touchscreens on such electronic devices and make the customised services easier to deploy. Toward this end, we set out to develop a general-user authentication solution with smart access capability that can work with any solid surface (like a door, table or vehicle window), not limited to touchscreens, and with minimum hardware and maintenance cost.

Vibration-based sensing

So how does this new approach work? Physical vibration is a phenomenon that creates a mechanical wave, transferring the initial energy through a medium. Similar to the way wireless signals are transmitted, when a vibration signal travels through a medium, it experiences attenuation along the propagation path, and reflection/diffraction when the signal hits the boundary of two different media

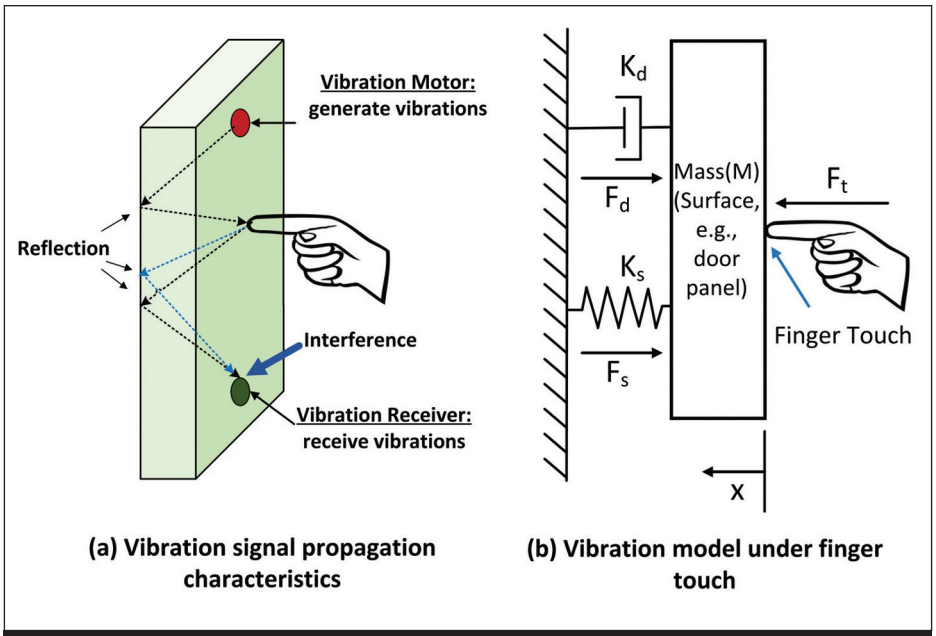

Figure 1: This shows the propagation characteristics of vibration signals on a solid surface.

(eg, the contacting area between a finger and a medium).

Figure 1 (a) shows the reflection and diffraction of a vibration signal propagating in a solid surface, when a finger touches the area between the vibration signal generator and receiver. What happens is that when the vibration signal hits the contacting area of the finger, part of the signal reflects back to the surface and the rest of it propagates into the finger (it's absorbed) and bounces back to the surface along a different propagation path. The vibration signal is affected by the touching location of the finger and traverses different paths before reaching the receiver (the vibration sensor). So, the touching location information is embedded in the various interference effects captured at the receiver. What's more, when a finger touches the surface of an object (like a table), the flexibility of the object is affected not only by the touching location but also the strength of touch.

To mathematically model the vibration effect on the object under an external force caused by the finger touch, we considered a spring-mass-damper system, as shown in Figure 1 (b). This indicated that the finger touching force could be captured by analysing the received vibration signals and used as a biometric-associated feature in VibWrite. In an empirical study, we found that the frequency response of the same user's fingerpress resulted in a higher correlation than those of different users when they touched the same location on a surface. This important observation suggested that the vibration propagation properties are strongly influenced by unique human physical traits embedded in finger touches, such as contacting area, touching force, etc – which could support ubiquitous user authentication with a passcode on any surface beyond touchscreens.

System deployment

To enable touching and writing on any surface during the authentication process, VibWrite builds on a touch-sensing technique that uses vibrations, is resistant to environmental noise, and can operate on surfaces constructed from a broad range of materials. As shown in Figure 2 (a), when a vibration motor actively excites a surface, resulting in an alteration of the shockwave propagation, the presence of the object or finger touching the surface can be sensed by analysing the vibrations received by the sensor.

"The vibration response of an office door differs from a house door. Unique behavioural information is embedded in the surface being touched, making the system harder to be hacked by attackers"

VibWrite supports generalised vibration sensing based on a low-cost single sensor prototype that can be attached to a solid surface (such as a door, table or appliance) to sense user touches and perform authentication flexibly from anywhere. By relying on the vibration signals in a relatively high frequency band (over 16kHz), the system is hardly audible or

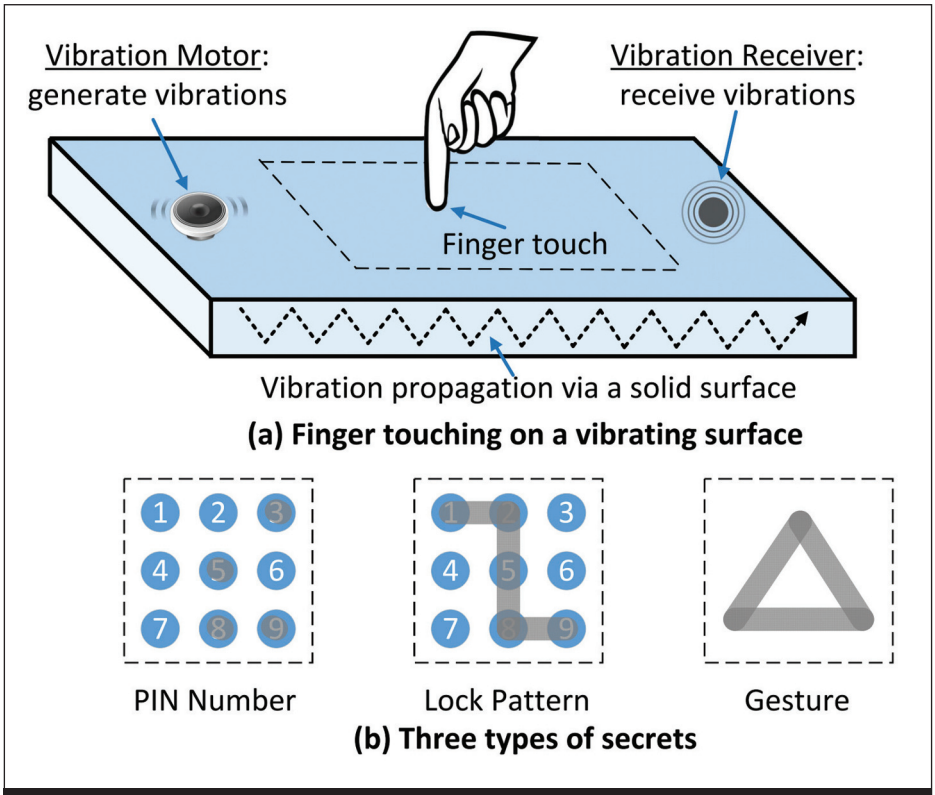

Figure 2: Illustration of a finger touching on a solid surface under physical vibration, and three independent types of passcodes for pervasive user authentication.

distracting to the user, and is less susceptible to environmental interference from acoustic (ie, mainly within a lower frequency band) or radio-frequency noise.

"Many environmental factors may affect system performance. A car door panel's vibration response may vary due to changes in temperature, humidity, wind, wetness and dirt"

More importantly, vibration propagation is highly dependent on the surface material and shape in specific scenarios. So VibWrite provides enhanced security by integrating location/surface uniqueness through such low-cost and tangible vibration-based user interfaces. As an example, the vibration response of an office door differs from that of a house door. This unique behavioural information is embedded in both the behavioural biometrics as well as the surface being touched – the specific door in the office – making the system harder to be hacked by attackers.

VibWrite enables users to choose from three different forms of passcodes, including PINs, lock patterns and gestures – and signatures in the future – to gain secure access, as shown in Figure 2 (b). The authentication process can be enabled on any solid surface beyond touchscreens and without the constraint of the limited screen size. It is resilient to side-channel attacks, such as when an adversary places a hidden vibration receiver on the authenticating surface or a nearby microphone to capture the received vibration signals. It is also resistant to various adversarial activities, including the seemingly powerful ones that observe the legitimate user's input multiple times to learn the passcode.

VibWrite can authenticate the legitimate user and thwart attacks because of the following insights: (1) the vibration signals can perform cm-level location discrimination; and (2) unique features are embedded in a user's finger pressing at different locations on a solid surface. Such unique features reflect the characteristics of the user's finger touching on the medium (eg, a door panel or desk surface), including the locations of touching, contacting area, touching force, etc. This makes them capable of determining different touching locations by the same user and different users when touching the same location.

Comparison to existing work

So how does VibWrite compare with other solutions when it comes to ensuring that the secret inputs used to authentication a person are physically from that legitimate user:

- Biometric-based systems such as fingerprints, iris patterns, retina patterns and face have clearly become prominent in achieving authentication. However, physiological biometrics are sensitive personal information that may involve privacy concerns and may not be not widely accepted.
- A compromise approach that reduces privacy concerns is to authenticate users based on their behavioural characteristics, including unique keystroke dynamics[6], mouse movements[7] and gait patterns[8]. But while these approaches are less sensitive in terms of privacy, they are designed for continuous user verification when the user operates the keyboard, moves a mouse or takes a walk, rather than one-time authentication.
- To provide authentication to the emerging smart access systems being introduced in corporate facilities, apartment buildings, hotel rooms and smart homes, techniques involving intercoms, cameras, access cards and fingerprints have been explored. For example, KinWrite[9] uses Kinect, a vision-based platform, to capture the user's 3D handwriting patterns for authentication. But these approaches usually involve expensive hardware, a complex installation process and diverse maintenance efforts.
- Recent studies have successfully combined 2D handwriting and behaviour features such as corresponding writing pressure, writing speed and correlation between multiple fingers on touchscreens to provide enhanced security[10, 11, 12]. But the limitation here is that the authentication relies on touchscreens, which may suffer from smudge attacks[13] and are not always available in smart access systems.

Limitation and future work

In summary, as a starting point for a vibration-based authentication system, VibWrite offers a low-cost and easily deployed solution that has a high potential to work in various locations – such as apartment buildings, hotel rooms and smart homes. However, the current prototype is still not ready for industrial deployment in terms of its authentication/false accept rates, and there is much room for us to improve the system. The current VibWrite system remains far from practical deployment, as a legitimate user may

need to try a few times to successfully access the system.

To improve system performance, we plan to explore the deployment of multiple sensor pairs, hardware refinements, and authentication algorithm improvements. Specifically, more than one pair of vibration transmitters and receivers can be used to help increase the dimension of the surface sensing features, which can better represent each individual's behavioural and physiological characteristics.

In addition, we noticed that the uniqueness of the features is affected by the stableness of the hardware components, since the weak analogue signals extracted by the piezoelectric sensor can be easily distorted when passing through electronic components (eg, amplifier and ADC). So we could build a higher standard hardware signal processing component (eg, an ultra-low noise signal amplifier) to enhance the system. Meanwhile, improving the vibration motor in terms of its power level, stableness and frequency response could become another topic to explore.

Also, when it comes to practical deployment, there are many environmental factors that need to be taken into consideration that may affect system performance. For instance, if the surface (say a car door panel) is exposed to an outdoor environment, its vibration response may vary on different days due to changes in temperature, humidity, wind, wetness, dirt, etc. Again, the temporary presence of objects placed on the surface – such as a book placed on the desk – could alter the received vibrations to be slightly different from the trained one. The effects of these factors might be reduced through further filtering or directional sensing techniques.

More robust machine learning methods grounded on deep learning can also be built in our future work to deal with various environment-related elements. In addition, future work should include more/diverse population samples, longer time periods and more influential factors to improve system robustness. But VibWrite offers a route forward in finding a low-cost, secure and practical way to access smart systems by touching any solid surface.

About the authors

Jian Liu is pursuing a PhD degree with the Department of Electrical and Computer Engineering at Rutgers University. His research interests include cyber-security/privacy, mobile computing/sensing and vehicular systems. He received the Best Paper Award from IEEE SECON 2017 and is currently working in the Data Analysis and Information SecuritY (DAISY) Lab with Prof Yingying Chen.

Chen Wang is also pursuing a PhD degree in Rutgers' Electrical and Computer Engineering Department. His research interests include mobile computing, cyber-security and privacy, and smart healthcare. He received the Best Paper Award from the ACM Conference on Information, Computer and Communications Security (ASIACCS) 2016 and the Best Paper Award from the IEEE Conference on Communications and Network Security (CNS) 2014.

Yingying (Jennifer) Chen is Professor of Electrical and Computer Engineering at Rutgers, a member of the Wireless Information Network Laboratory (WINLAB) and leads the DAISY Lab. Her research interests include smart healthcare, cyber-security and privacy, IoT and mobile sensing. She has published over 100 journals and referred conference papers in these areas. She is serving on the editorial boards of IEEE TMC and IEEE TWireless.

Nitesh Saxena is an Associate Professor of Computer Science at the University of Alabama at Birmingham (UAB), and founding director of the Security and Privacy in Emerging Systems (SPIES) group/lab. He works in the areas of computer and network security, and applied cryptography, with a keen interest in wireless and mobile device security, and the emerging field of user-centred security.

References

1. 'Access Control Market worth 10.03 Billion USD by 2023'. MarketsandMarkets. Accessed March 2018. https://www.marketsandmarkets.com/PressReleases/access-control.asp
2. Phuc Nguyen, Ufuk Muncuk, Ashwin Ashok, Kaushik R Chowdhury, Marco Gruteser and Tam Vu. 'Battery-Free Identification Token for Touch Sensing Devices'. In Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM, 2016; ACM, 109–122.
3. Tam Vu, Akash Baid, Simon Gao, Marco Gruteser, Richard Howard, Janne Lindqvist, Predrag Spasojevic and Jeffrey Walling. 'Distinguishing users with capacitive touch communication'. In Proceedings of the 18th annual international conference on Mobile computing and networking, 2013; ACM, 197–208.
4. Raja Bose, Synaptics. 'How to implement fingerprint authentication in automobiles', Electronic Products, 25 January 2017. Accessed March 2018. https://www.electronicproducts.com/Sensors_and_Transducers/Sensors/How_to_implement_fingerprint_authentication_in_automobiles.aspx
5. Jian Liu, Chen Wang, Yingying Chen and Nitesh Saxena. 'VibWrite: Towards Finger-input Authentication on Ubiquitous Surfaces via Physical Vibration'. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2017; pp. 73-87.
6. Kenneth Reve. 'A bioinformatics based approach to user authentication via keystroke dynamics'. International Journal of Control, Automation and Systems, 2009; 7, 1, 7–15.
7. Nan Zheng, Aaron Paloski and Haining Wang. 'An efficient user verification system via mouse movements'. In Proceedings of the 18th ACM conference on Computer and communications security, 2011; 139–150.
8. Yanzhi Ren, Yingying Chen, Mooi Choo Chuah and Jie Yang. 'User Verification Leveraging Gait Recognition for Smartphone Enabled Mobile Healthcare Systems'. IEEE Transactions on Mobile Computing, 2015; 14, 9, 1961–1974.
9. Jing Tian, Chengzhang Qu, Wenyuan Xu and Song Wang. 'KinWrite: Handwriting-Based Authentication Using Kinect'. In Proceedings of Network and Distributed System Security Symposium (NDSS), 2013.
10. Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner and Heinrich Hussmann. 'Touch me once and I know it's you!: implicit authentication based on touch screen patterns'. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2012; 987–996.
11. Yanzhi Ren, Chen Wang, Yingying Chen, Mooi Choo Chuah and Jie Yang. 'Critical segment based real-time E-signature for securing mobile transactions'. In Proceedings of the IEEE Conference on Communications and Network Security (CNS). 2015; 7–15.
12. Michael Sherman, Gradeigh Clark, Yulong Yang, Shrida Sugrim, Aru Modig, Janne Lindqvist, Ani Oulasvirta and Teemu Roos. 'User-generated freeform gestures for authentication: Security and memorability'. In Proceedings of the 12th annual international conference on Mobile systems, applications and services, 2014; ACM, 176–189.
13. Adam J Aviv, Katherine L Gibson, Evan Mossop, Ma Blaze and Jonathan M Smith. 'Smudge Attacks on Smartphone Touch Screens', 2010; Woot 10, 1–7.