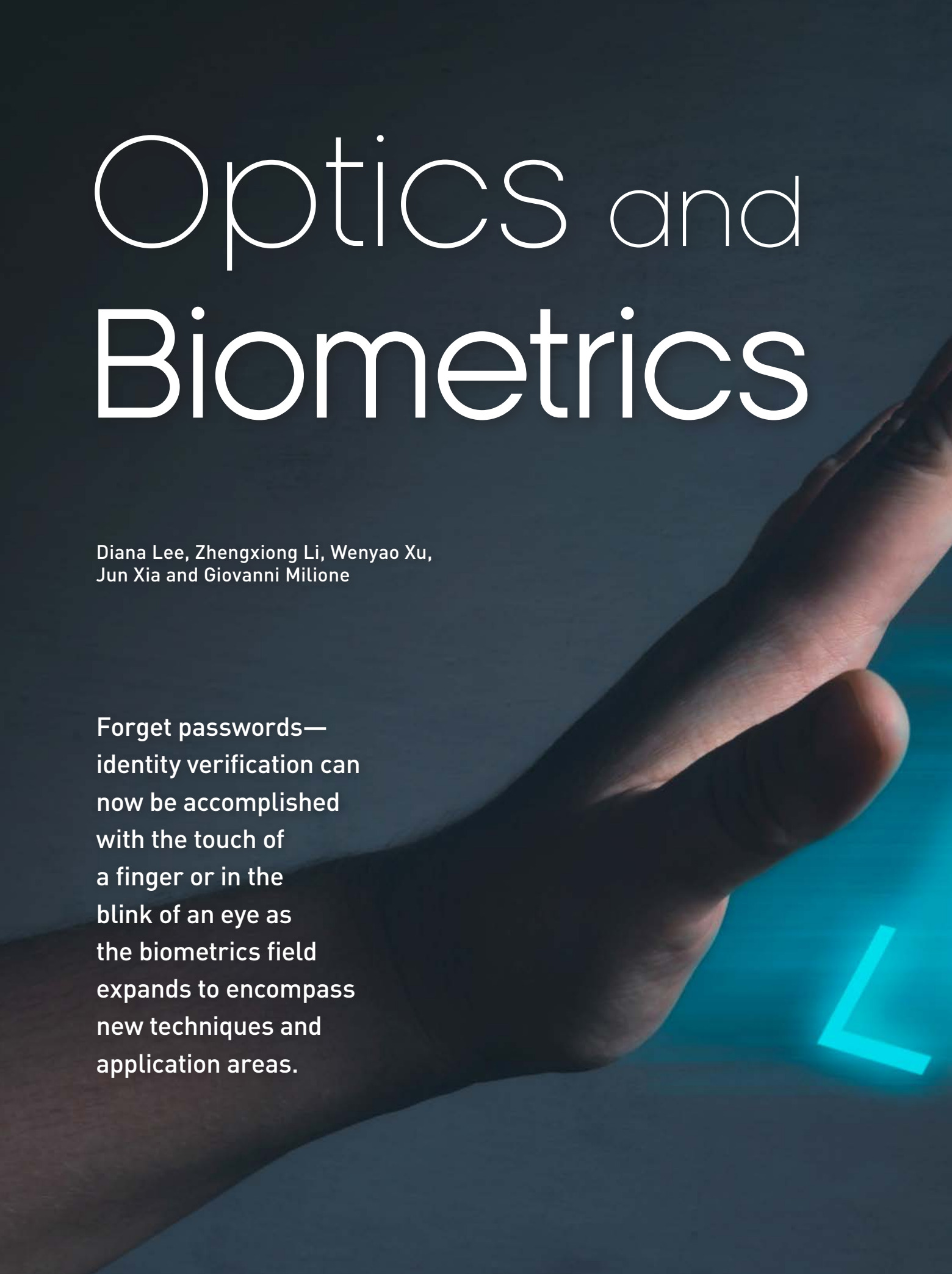
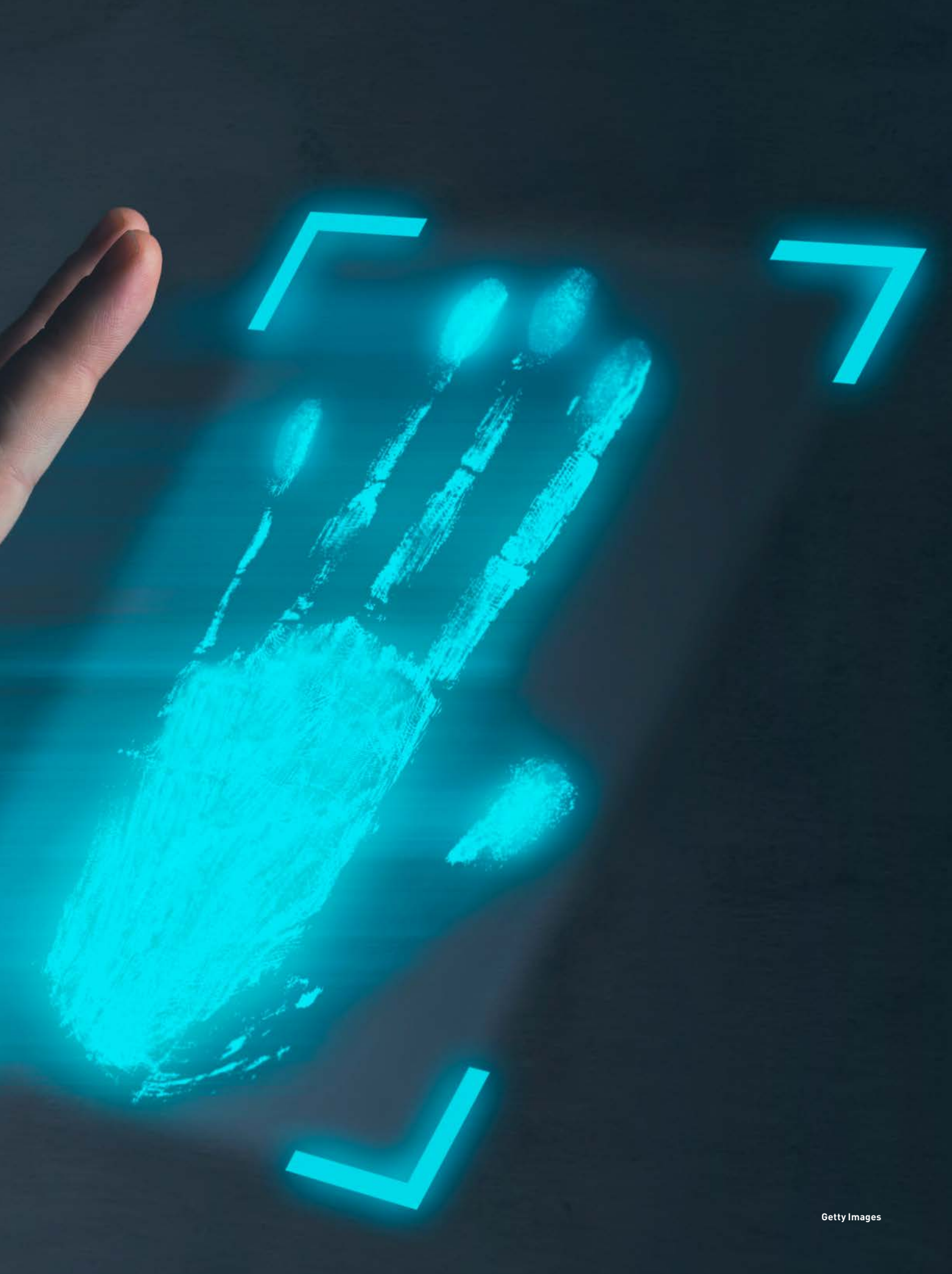
Optics and Biometrics

Diana Lee, Zhengxiong Li, Wenyao Xu,
Jun Xia and Giovanni Milione



Forget passwords—identity verification can now be accomplished with the touch of a finger or in the blink of an eye as the biometrics field expands to encompass new techniques and application areas.



Getty Images

Getty Images

Since the dawn of the Information Age in the mid-20th century, digital information has become ubiquitous in modern society. Some 60% of the global population now actively uses the internet—engaging in personal banking, making purchases and accessing sensitive personal and work information, all from the convenience of a smartphone or personal laptop. Of course, the ability to access such sensitive data at the touch of a button raises serious security issues; thus reliable identity authentication is important to safeguard against fraud and theft.

Enter biometrics—unique, anatomical, human features used to authenticate human identities. The most widely used biometrics are faces, fingerprints and irises; other prevalent biometrics include finger veins, palm prints and palm veins. Other biometrics garnering attention, albeit currently used on a more limited scale, include heartbeat, voice, ear canal and gait. Regardless of the feature being authenticated, compared with token-based and knowledge-based forms of identification like passports and passwords, biometrics are unmatched. And optics-based acquisition of biometrics has the advantage of being noncontact, high resolution and harmless.

In general, biometrics should have a few key properties: universality (possessed by everyone), distinctiveness (different for different people), permanence (unchanged over time), collectability (quantifiable), performance (identity authentication is achievable), acceptability (people are willing to use them) and circumvention (difficult to spoof). Optics enables competitive performance, acceptability and circumvention, which is why optics-based biometrics can be found in almost every personal smartphone and why fingerprint biometrics has become a law-enforcement standard. Optics is also exploited for more advanced biometrics, such as finger-vein imaging, and today, novel methods like optical coherence tomography and photoacoustic tomography enable advances beyond even that.

Whether for banking, immigration control or recreational ticket monitoring, biometrics help to secure information and protect privacy. This article explores a few of the most common optical biometric technologies and their real-world applications.

How are biometrics used?

The use of biometrics can be divided into three steps. Generally, the first consists of *acquiring* the raw data from the sensor for the biometrics, at a particular sampling rate, while ensuring proper placement and low environmental noise. Next, *feature-extraction* techniques reduce noise in the signal and pull out multiple features for matching. Finally, the obtained features are leveraged to classify the input signal with previously trained data, and thereby *authenticate* the individual.

Acquisition

Acquiring a specific biometric signal depends on different sensors with varying hardware configurations, placement locations, sampling frequencies and other technical constraints. The aim of the acquisition module is to capture individuals' unique characteristics, ensure that sufficient features can be extracted from the acquisition signal and minimize the inevitable accumulated noise during the measurement.

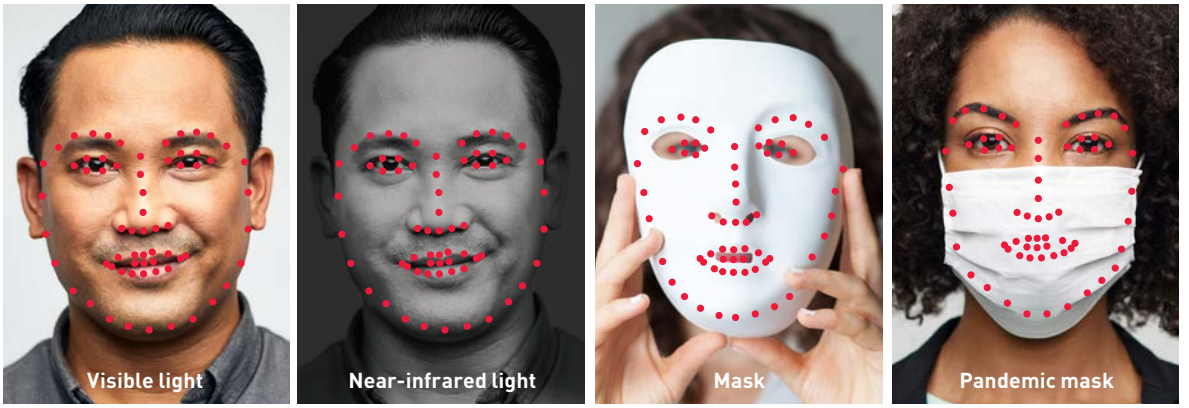
The selection criteria for an acquisition technique significantly rely on the application and overall domain, and choosing the optimal technique is essential to achieve exceptional performance from the biometric system. From the perspective of sensor placement, there are two main types of biometrics acquisition. Contact surface sensing transduces the distinct bioelectric activity within the body into a measurable electrical signal for biometrics via electrodes, stethoscopes or on-body sensors. Noncontact and remote sensing, on the other hand, monitor the unique characteristics of an individual's motions or exterior appearance for biometrics through, for example, conventional cameras and lidar.

Feature extraction

Comparing the biometric signals of different individuals for classification requires extracting features relative to a domain, time or frequency dimension. While a comprehensive selection of multiple features can increase the accuracy of the biometric model, it may also lead

1047-6938/21/05/36/8-$15.00 © OSA

Optics enables competitive performance, acceptability and circumvention, which is why optics-based biometrics can be found in almost every personal smartphone.



In facial-recognition systems, unique features are extracted from visible or near-infrared images by marking the faces with nodal or key points. While a mask replica of a face can spoof a facial-recognition system, systems that focus on facial features in the unobscured area of the eyes can achieve high recognition accuracy even when people are wearing pandemic masks.
NEC/Getty Images

to higher computational cost. Currently, there are four representative types of feature extraction for biometrics authentication: domain-based features, statistical-based features, frequency-based features and wavelet-based feature-extraction techniques.

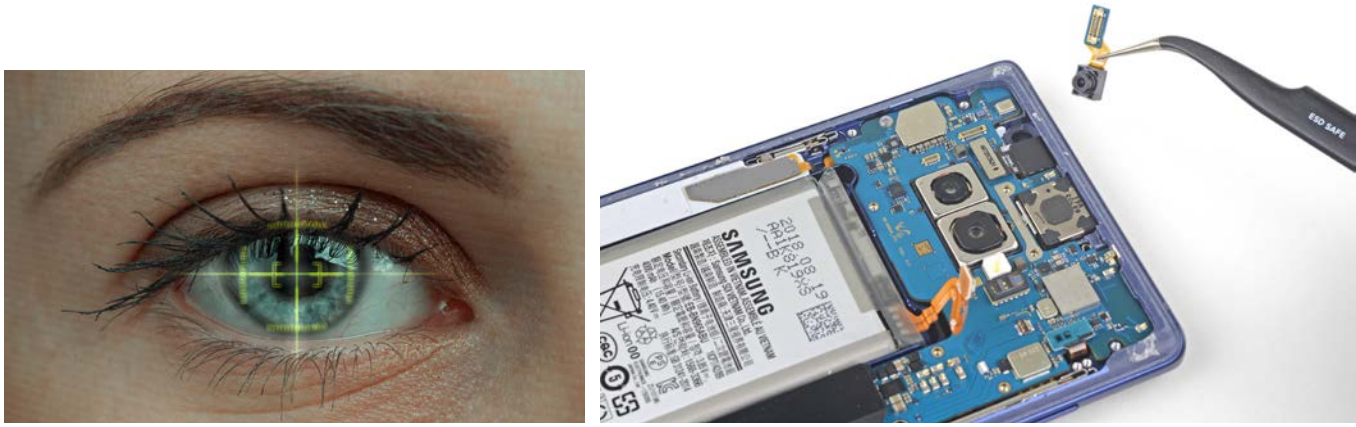
Domain-based features rely on the specific biometric domain's overall knowledge and are often based on fiducial points of biometrics-related signals. Meanwhile, statistical-based features are coherent with the time series of the signal, typically with no dependency on its domain; they represent the mean, median, standard deviation, maximum and minimum value of a segment. Frequency-based features are computed from the fast Fourier transform (FFT) of the signal, which includes spectral roll-off, spectrum energy, spectral centroid and other features depending on the power-spectral density. Finally, wavelet-based features offer valuable insights by decomposing the time-series biometric signals into multilevel coefficients at different frequency sub-bands.

Authentication

Upon receiving the optimized feature vector consisting of the domain, statistical or frequency features, a matching algorithm is implemented to finalize a decision. In the biometric authentication system, the classification will result in either an authorized user or an imposter. The location of the feature extraction and classification model is essential for a secure biometric system. The matching algorithms employed for biometric authentication can be broadly categorized into signal-matching and machine-learning techniques. Signal-matching techniques—like Euclidean distance, Karl Pearson's correlation or dynamic time warping—compare the signals obtained by the sensor through distance and correlation measures. On the other hand, machine-learning techniques—such as convolutional neural networks, support vector machines and K-nearest neighbor—are more data-driven, meaning they rely on collecting a large scale of user data for training and test.

Facial recognition

Every individual has unique facial features that can be used as biometric signatures for facial recognition—an omnipresent application in daily life. Traditional facial recognition uses 2D images obtained by visible or near-infrared (NIR) light. For 2D imaging with visible light (380 nm to 750 nm), most cameras are sufficient to capture a facial image. These images are then marked with nodal points to highlight unique features and geometry, such as distance between the eyes. Although the geometry of the nodal points is unique, this biometric signature is still vulnerable to spoofs—or the presentation of a biometric replica to a biometric authentication system, such as a mask or a photo ID.



Samsung's iris-recognition technology inside the Samsung Galaxy Note9 smartphone. An infrared source illuminates the eye while a sensor captures an image of the iris for authentication. Getty Images /iFixit

NIR cameras, on the other hand, can overcome some of these challenges for better anti-spoofing. These cameras capture NIR light waves (750 nm to 1700 nm) reflected from the human face. To spoof an IR camera, a face replica like a mask or photo would have to be made to have the same NIR reflectivity as human tissue. Compared with visible-light camera systems, NIR cameras can detect faces in the dark and are less sensitive to facial expression and different environmental conditions, such as rain, snow and fog.

However, NIR cameras like the ones found in laptops or smartphones for facial recognition come with their own set of challenges. For example, NIR cameras are less susceptible to illumination, so they produce lower-resolution images, which can make facial recognition less accurate. Eyeglasses can also pose a problem for NIR cameras, as the differing reflectivity for NIR and visible light can obscure facial features.

Even more accurate than 2D facial recognition is 3D facial recognition, which traditionally uses at least two cameras to capture the front and the side views of the face, allowing for more unique features with depth geometry that is harder to forge. This technique also overcomes the illumination-variation and facial-expression challenges that plague 2D facial-recognition systems. In recent years, commercial 3D facial-recognition systems have been integrated into our smartphones for improved security, such as Apple's TrueDepth camera system.

COVID-19 has created new challenges for facial recognition, namely the widespread adoption of face masks, which obscure canonical face features like the positions, shapes and sizes of noses and mouths. One solution is to focus on the extraction and analysis of facial features that are not covered by masks, like the areas surrounding eyes, which is what multinational information technology and electronics company NEC has done. At the U.S. Department of Homeland Security's 2020 Biometric Technology Rally, NEC's mask solution achieved a 98.7% "true identification rate"—19% higher than the median performance of other mask solutions. Such a technique could enable easier check-in at airports and passport verification at borders, mitigating some of the travel problems caused by the pandemic.

Iris recognition

Another unique human attribute that is used as a biometric is the iris. High-resolution visible-light cameras can produce detailed images of the unique patterns and color of the iris; however, images captured with visible light are more vulnerable to reflections and environmental noise, so NIR camera systems are preferred for iris imaging.

Similar to facial recognition, smartphones also employ iris-recognition technology—for example, the Samsung S8, which features iris-recognition technology designed by the small U.S. biometric security company, Princeton Identity, based in New Jersey. Located in the front of the smartphone is a front camera and an LED sensor (with a proprietary pulse rate) that illuminates the face with NIR light. These waves reflect off of the eyes and are captured by the front-facing camera, which has built-in filters to detect NIR waves while blocking out visible light—resulting in a higher-contrast image of the iris. The iris-recognition software then maps out over 200 unique features of the iris that serve as reference points to unlock the smartphone.

To increase the accuracy of the scanning system, obtaining the highest-quality initial iris image is crucial. Although ordinary digital cameras work for iris-image acquisition, higher-resolution cameras like the LG IrisAccess 4000 edge ahead. These special iris-imaging systems comprise four important components:

Even more accurate than 2D facial recognition is 3D facial recognition, which traditionally uses at least two cameras to capture the front and the side views of the face.

illuminators, lens, sensor and the control unit. When controlled, illumination can enhance textural information of the iris, providing more unique features of an individual's eye and in turn boosting biometric security and accuracy. However, over illumination can increase reflection, which interferes with the image quality. The lens—typically an autofocusing lens in these systems—focuses the image onto the sensor, which must be placed within the focal length to get a clear image.

Image quality depends on the camera system's sensor, which can be divided into two categories—CCD-based sensors, which outputs analog signals that must then be converted to digital, and CMOS-based sensors, which outputs digital signals. Most iris-imaging systems favor CMOS sensors for their low power consumption and higher sensitivity. Lastly, the control unit processes the captured image. To improve image quality after acquisition, some systems may preprocess these images—for example, by adding filters to eliminate the background noise and amplify the signal from important iris features.

Although there are many methods to improve image acquisition and image resolution for iris recognition, the technology still faces some challenges. Blinking can cause motion artifacts, like blurring, and other factors such as poor illumination and light reflections may also affect the image quality. Eyelashes and eyelid occlusions are another hurdle—for those with smaller eyes, the imaging system may not be able to capture the entire iris—and glasses or color contacts can cause a false-negative authentication. Image-process algorithms, however, can overcome some of these challenges.

Finger and palm prints

One of the most popular biometrics, integrated in many consumer electronic devices, is fingerprint or palm recognition. A human fingerprint and palm print have many unique patterns that help to identify the individual, and incorporating various sensors—including optical, capacitive and ultrasonic sensors—into a scanner can detect these patterns.

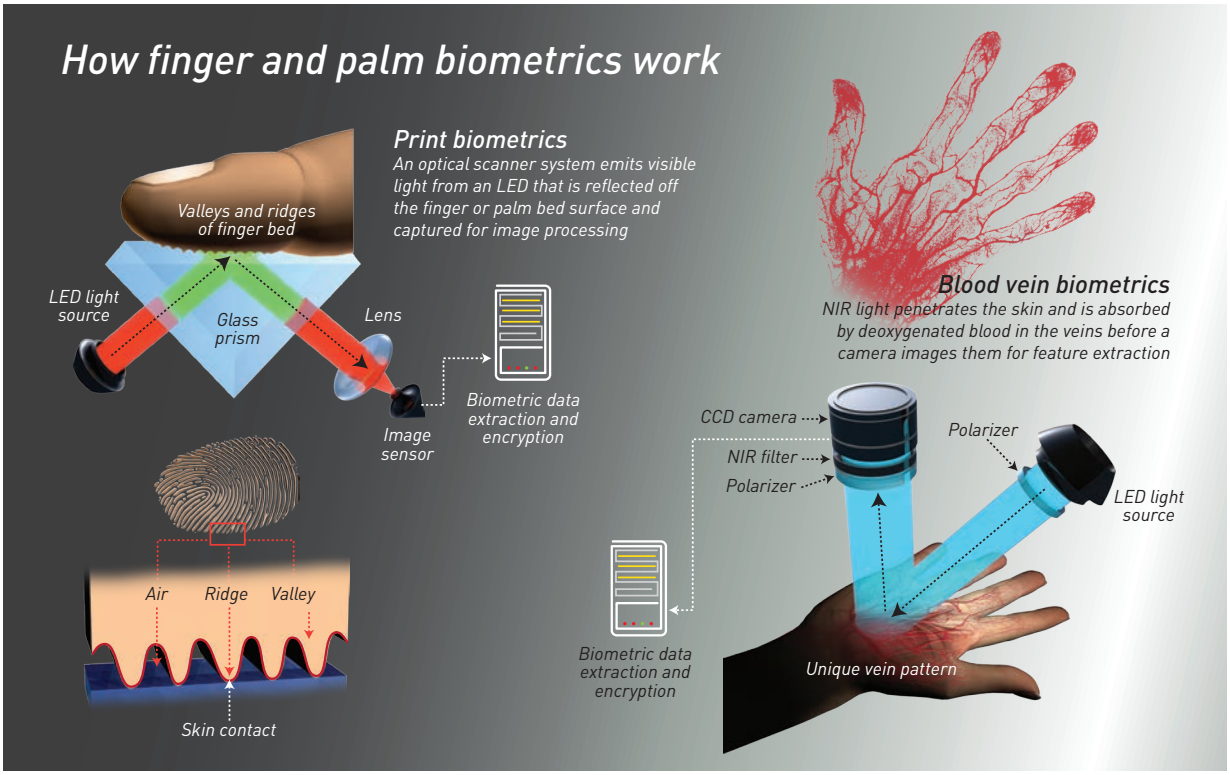


Illustration by Phil Saunders

Amazon recently unveiled its own version of palm-recognition technology, Amazon One, which uses custom-built algorithms and hardware to "create a unique palm signature."
Amazon

Traditional fingerprint- and palm-print-recognition technologies are based on frustrated total internal reflection, similar to seeing fingerprints on the inside of a glass of water that's been held. Visible light from an LED is incident on the finger–glass interface. Because the ridges of the finger bed are in contact with the glass, the light is transmitted. In contrast, the air gap between the valleys of the finger bed and the glass reflect light. A lens focuses and magnifies the signal, which is captured by a CCD or CMOS imaging sensor. The fingerprint or palm-print image is then reconstructed into a 2D image and fed into an image-processing system to filter and improve the resolution for feature extraction. Although these systems are perfectly functional, optical scanners can be bulky and easy to spoof using fake fingerprints that have the same optical properties as human tissue.

As smartphones slimmed down and became even more portable, a smaller fingerprint-scanning system based on capacitive sensors gained traction. Unlike the optical scanning system, the capacitive system employs a 2D array of micro-capacitor plates integrated on the smartphone. By placing the finger on top of the micro-capacitor plate, the ridges and valleys induce electrical charges, which are stored in the micro-capacitors. In these systems, the ridges in the finger skin induce a charge while the valleys leave the capacitors relatively unchanged. An op-amp integrator tracks the electrical changes, and an analog-to-digital converter records the signals, which are then analyzed to extract the fingerprint's distinctive characteristics.

Compared with the optical fingerprint-scanning system, the capacitive system is harder to spoof—a replicated 2D image or a fake prosthetic finger would not be able to completely imitate the electrical charges. Additional security comes at greater expense, however, as more capacitors are needed to capture more detailed fingerprints. Capacitive sensors are also vulnerable to hackers, who can bypass the recognition system.

The latest fingerprint-recognition system, like the one sold by U.S. company Qualcomm, depends on ultrasonic sensors to capture 3D fingerprints. This system comprises two main components, the transmitter and the receiver. The transmitter emits high-frequency acoustic waves that are reflected by the ridges and the valleys of the finger skin—the difference in acoustic impedance of the skin (ridges) and air (valleys) causes the reflected acoustic waves to differ as well. Then the receiver can detect the different mechanical stress intensities induced by the reflected acoustic waves. The distinctiveness of the ridges and valleys will produce different intensities unique to each individual, and in this way, a 3D image of the fingerprint can be mapped out.

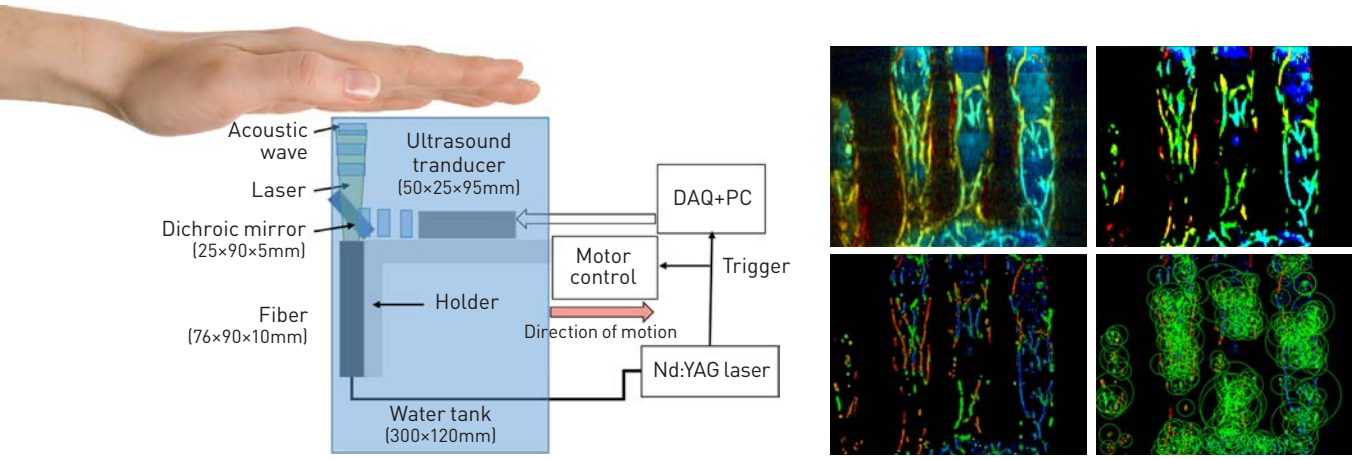
Compared with 2D images obtained from the optical and capacitive systems, the 3D fingerprint ultrasonic system is more secure; by imaging depth, the system extracts more unique features, making it harder to spoof. Although the scan time of the ultrasonic system is slightly longer, the scanner still functions efficiently regardless of screen thickness—a major advantage in the smartphone industry.

Finger and palm veins

Just as the prints on a person's fingers and palms form a unique biometric, so too do the vein structures underneath the skin—each individual has a unique blood vessel pattern in their fingers and palms that others cannot mimic. Traditionally, optical methods scanning the venous structures in a person's hand use NIR light and polarization. NIR light can penetrate through biological tissue of a few milimeters where it's absorbed at a specific rate by the deoxygenated blood in veins, creating a darker shadow in the image that effectively maps the venous vasculature in the palm or the finger.

There are two main methods of palm-vein imaging: reflection or transmission. The reflection method, which relies on light absorption and reflection to reconstruct the vascular image, is most common. In this method, the illuminating component (the light source) and the capturing component (the sensor or camera) are on the same side of the target—the front. The transmission method, however, places the target in the middle, sandwiched between the illuminating and capturing components. Of course, this requires a stronger light penetration and is therefore less common.

Just as the prints on a person's fingers and palms form a unique biometric, so too do the vein structures underneath the skin.



A recently reported, compact photoacoustic imaging platform (left) creates 3D finger vein images (right) that are then processed to extract biometric features (green circles). Adapted from Y. Zhan et al., Appl. Opt., doi: 10.1364/AO.400550 (2020)

These biometric systems frequently use CCD cameras to capture the palmar or finger veins. NIR CCD cameras provide higher resolution; however, the equipment can be expensive. Most vein-imaging modalities use LED light sources emitting in the 800-nm-to-900-nm range for an optimal image. Adding polarizers or NIR filters boosts the resolution of the vascular structures in the biological tissue. A polarizer projects a light wave to only vibrate in a single plane, like how polarized sunglasses block glare. Similarly, polarizers block light reflected from the skin's surface, the polarization of which is unchanged, from light that penetrates deeper and scatters in the skin, becoming depolarized. This provides better contrast between vascular structure and surrounding tissue.

The captured venous image is then uploaded into an image-processing algorithm for feature extraction followed by authentication. The authentication protocol includes two modes: the registration and enrollment mode, which registers the individual's biometric into the database, and the authentication process, which verifies the person's identity. Once enrolled, the system can then recognize the individual with the biometric authentication protocol as a legitimate or an adversary drone.

Just as 3D facial recognition is more secure than 2D systems, 3D vein imaging biometrics is harder to spoof than 2D techniques. Photoacoustic tomography is a burgeoning imaging modality that can overcome the light-scattering limits in human tissue that make 3D biometrics difficult to obtain. In this technique, a laser illuminates and is absorbed by blood vessels in human tissue, creating an ultrasonic shockwave, which is subsequently detected by an ultrasonic transducer array. Then, using a physics-based acoustic source localization algorithm, a 3D image of the blood vessels is reconstructed. Just last year, our team at NEC Laboratories America and the University at Buffalo, USA, demonstrated accuracies greater than 99% and false acceptance rates as low as 0% with this system.

Key advantages of optical-based biometric technologies are non-invasiveness, harmlessness and the ability to obtain biometrics at a distance. Research that will see rapid growth in the near future will address the persistence of those advantages amidst requirements of the "new normal," such as contact-freedom, preservation of privacy and equity and anti-spoofing. That includes the biometric application of advanced imaging modalities, such as photoacoustic tomography, optical coherence tomography and lidar. OPN

Diana Lee and Jun Xia are with the Department of Biomedical Engineering and Zhengxiong Li and Wenyao Xu are with the Department of Computer Science & Engineering, University at Buffalo, NY, USA. Giovanni Milione (gmilione@nec-labs.com) is with NEC Laboratories America, Inc., NJ, USA.

For references and resources, go online: **www.osa-opn.org/link/biometric**.

References and Resources

- X. Chen et al. "IR and visible light face recognition," Comput. Vision Image Understanding **99**, 332 (2005).
- M. M. H. Ali et al. "A review: Palmprint recognition process and techniques," Int. J. Appl. Eng. Res. **13**, 7499 (2018).
- Y. Wang et al. "A Robust and Secure Palm Vessel Biometric Sensing System Based on Photoacoustics," IEEE Sens. J. **18**, 5993 (2018).
- J.J. Winston and D.J. Hemanth. "A comprehensive review on iris image-based biometric system," Soft Comput. **23**, 9361 (2019).
- Y. Zhan et al. "3D finger vein biometric authentication with photoacoustic tomography," Appl. Opt. **59**, 8751 (2020)
- S. Marcel Uhl, C. Busch and R.N.J. Veldhuis. *Handbook of Vascular Biometrics*, Springer, (2020).