Optical Engineering

OpticalEngineering.SPIEDigitalLibrary.org

Line-scan system for continuous hand authentication

Xiaofeng Liu
Lingsheng Kong
Zhihui Diao
Ping Jia

SPIE.

Xiaofeng Liu, Lingsheng Kong, Zhihui Diao, Ping Jia, "Line-scan system for continuous hand authentication," *Opt. Eng.* **56**(3), 033106 (2017), doi: 10.1117/1.OE.56.3.033106.

Line-scan system for continuous hand authentication

Xiaofeng Liu,[a,b,c,*] Lingsheng Kong,[a] Zhihui Diao,[a] and Ping Jia[a]
[a]Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Science, Changchun, China
[b]University of Chinese Academy of Sciences, Beijing, China
[c]Carnegie Mellon University, Department of Electrical and Computer Engineering, Pittsburgh, Pennsylvania, United States

Abstract. An increasing number of heavy machinery and vehicles have come into service, giving rise to a significant concern over protecting these high-security systems from misuse. Conventionally, authentication performed merely at the initial login may not be sufficient for detecting intruders throughout the operating session. To address this critical security flaw, a line-scan continuous hand authentication system with the appearance of an operating rod is proposed. Given that the operating rod is occupied throughout the operating period, it can be a possible solution for unobtrusively recording the personal characteristics for continuous monitoring. The ergonomics in the physiological and psychological aspects are fully considered. Under the shape constraints, a highly integrated line-scan sensor, a controller unit, and a gear motor with encoder are utilized. This system is suitable for both the desktop and embedded platforms with a universal serial bus interface. The volume of the proposed system is smaller than 15% of current multispectral area-based camera systems. Based on experiments on a database with 4000 images from 200 volunteers, a competitive equal error rate of 0.1179% is achieved, which is far more accurate than the state-of-the-art continuous authentication systems using other modalities. [DOI: 10.1117/1.OE.56.3.033106]

Keywords: continuous authentication; palm print; contact image sensor; ergonomics.

Paper 161898 received Dec. 7, 2016; accepted for publication Mar. 7, 2017; published online Mar. 22, 2017.

1 Introduction

The authentication system is used to confirm the identity of a user based on one or more specific credentials.[1] Traditionally, it is merely performed at the initial interaction with the user and does not require reauthentication for continuous access.[2] Although this mechanism has dominated for decades,[3] it is insufficient for securing sensitive resources throughout the session, leaving the system vulnerable to misuse and hijacking.[4] With this concern, continuous authentication to consecutively ensure that the identity of the user is not switched, forged, displaced, or interrupted by verifying the participation or presence of the granted user has been investigated.[5] Initial efforts regarding this concept simply terminate the operating session after an inactive period. This scheme still leaves a vulnerable window and easily annoys the users.[6,7] An option to realize continuous authentication is to utilize biometrics. Compared with the passwords (what you know) and tokens (what you have), biometrics are commonly acknowledged as the most secure and convenient solution.[8] Various physiological or behavior traits associated with identity have been studied. A rapidly growing body of literature on the usage of the physiological modalities, e.g., voice, face, iris, finger, fingernail bed, earlobes, or body odor,[9–11] as well as some implicitly detectable behavioral modalities, such as signature, mouse, keystroke, and movement dynamics, have emerged for continuously monitoring in the last decade.[7,12,13] Among them, facial authentication systems,[7,14–16] mouse-/keyboard-based behavior metrics authentication systems,[12,13,17–20] and biomedical signals [electroencephalogram (EEG)[21] and electrocardiograph (ECG)[22,23]] are the most promising. Facial authentication systems are useful for tablets, laptops, and mobile phones since the user typically looks straight at a built-in, low-cost webcam in these cases. However, their accuracy is easily impacted by the expression, pose, and illumination variations.[14] Additionally, in practice, face images are unavailable when the operator or driver turns his head away. Despite some mouse dynamics-based systems that do not offer satisfactory accuracy,[12] previously proposed keyboard-based systems provide user authentication in an unobtrusive manner and exhibit promising results.[13] However, they still have several defects that limit their pervasive use. Their performance is not robust to those changes in software environments, input devices, tasks, or interaction modes.[12,24] The dataflow is often discontinuous, e.g., when the user is watching a movie on his computer and the systems need a long session of active involvement, e.g., several minutes,[13] to reach an acceptable accuracy level. The use of biomedical traits, e.g., EEG[21] and ECG[22,23] signals, has shown high discriminatory power. Although they have shown promising results, they are unable to produce a long-term, convenient sampling. The emergence and development of noninvasively wearable medical devices will be the hope in the future. In addition to the authentication performance, the usability of a specific application scene is also important. The merits and limitations of the mobile-based continuous user authentication approaches are explicitly investigated in a recent survey.[25] These techniques, however, are not suitable for in-car authentication, especially during driving.

Continuous authentication of the driver or operator is a topic that has been increasingly attracting attention for several reasons and within different application fields, e.g., the

*Address all correspondence to: Xiaofeng Liu, E-mail: liuxiaofeng@cmu.edu

0091-3286/2017/$25.00 © 2017 SPIE

heavy machinery, military, and transportation domains.[26] This issue ensures that the driver has a valid driving license and is granted permission to drive a certain category of vehicles. Furthermore, it can also be used to verify that truck drivers are not exceeding the working hour limits, bind insurance rates with drivers and their personal skills instead of the car, and even improve driving experience (by setting personal seat and air-conditioning settings).[27,28]

Vehicle driving is one of the most complex scenes involving user interaction. The usability issue has arisen regarding asking for characteristics that may lead to safety risks, e.g., distraction and interruption. One of the interaction mediums between the operator and equipment or vehicle is the operating rod. Since the operating rod is occupied throughout the driving period, it can be a possible solution for recording personal characteristics unobtrusively and consecutively via hand scanning. Hand recognition using the hand shape and texture has many advantages compared with other modalities in terms of accuracy, stability, passiveness, and cost.[29] Moreover, this system does not restrict the head pose to take the frontal face or iris images. Thus, the hand is an available source of characteristics for the operating scene. Some robust features, such as the principal lines, wrinkles, textures of palm, hand geometry, and knuckle print, can be easily extracted from the low-resolution multispectral hand images, which are highly reliable for matching.[30–32] The current hand or palmprint recognition systems have not been designed in a user-friendly way, especially for the size and the constrained poses. The palmprint recognition is limited mainly because of the dimensions of the devices.[33,34] Moreover, in current biometrics designs, the human factors, to some extent, have been neglected, despite the well-addressed collectability and the recognition-related performance.[35,36]

The key contributions of this paper can be summarized as follows. (1) We propose an end-to-end design of a continuous authentication system for providing a nonrepudiation security solution for engineering machinery or vehicles that uses the hand characters, especially the palmprint. (2) The proposed line-scan solution is 85% smaller than the current multispectral area-based camera systems, while achieving competitive accuracy. (3) Ergonomics are well considered to design a system under the operating rod-like shape constraints. (4) The authentication accuracy of the proposed system is superior to the state-of-the-art continuous systems with other modalities, which is supported by experiments on our database of 4000 images from 200 people.

The rest of the paper is organized as follows. Section 2 describes the prototype design of our system. The ergonomics are considered in Sec. 2.1. A contact image sensor (CIS) module is used to acquire the panorama image of a hand, reducing more than 85% volume of the conventional area sensor-based systems; it is described in Sec. 2.2. A controller unit is designed to solve the motion-synchronizing problem that occurs with a line-scan sensor. With this unit, the CIS module could capture hand images adaptively when rotating with the motor; it is described in Sec. 2.3. The competitive coding scheme and hamming distance are used for feature extraction and matching, respectively, following the best practice of area array sensor-based system's convention and is described in Sec. 2.4. The verification performance of the proposed system is compared with current area-based ones, which is supported by experiments on a database of 4000 images from 200 people, in Sec. 3.

2 Prototype System Design

After carefully considering the requirements of the operating and driving scene, we proposed an operating rod hand authentication system based on the CIS, an integrated CMOS line-scan sensor. The resolution and quality of images are similar to those of the current area-based system,[30] which enables a fair comparison of recognition performance. Figure 1 shows the three-dimensional (3-D) design model of our proposed hand images acquisition system, which is composed of a highly integrated customized CIS, a controller unit, a motor with an encoder, a slip ring, and a glass cover. The system framework is illustrated in Fig. 2. The controller unit, which is implemented based on a field-programmable gate array (FPGA), is used to capture the panorama hand images adaptively to the motion of the motor in real time. The synchronizing signals, captured images, and electric power of the CIS are transferred by the slip ring. Moreover, a universal serial bus (USB) interface is utilized to communicate between this system and either a desktop computer or an embedded platform. The two interfaces connected to the device are the 12-V power supply and

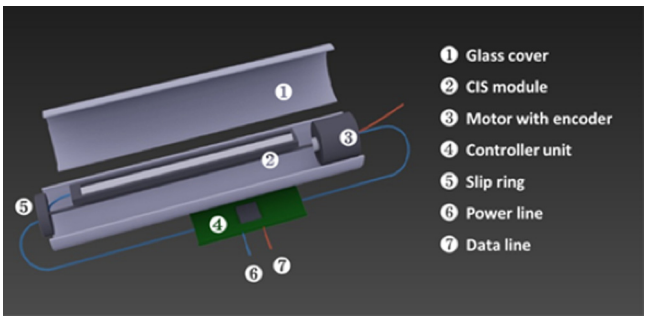

Fig. 1 Design model of the proposed acquisition system.

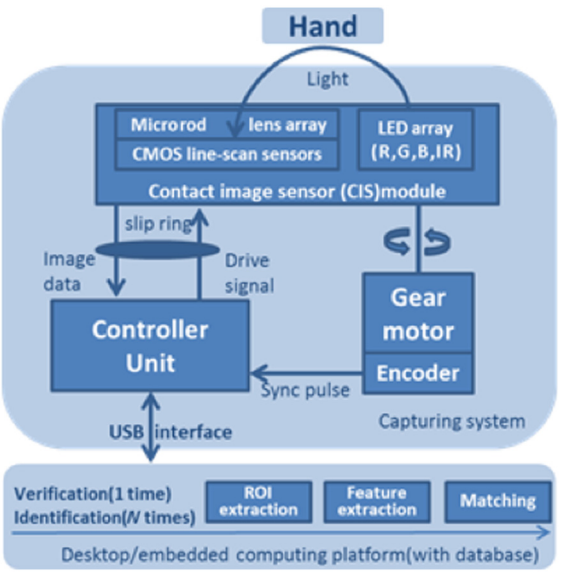

Fig. 2 Diagram of the system framework.

the USB mini-B plug. The highly integrated structure makes it easy to integrate the rod-like parts into conventional machinery. Examples of the desirable and available application parts are listed in Fig. 3.

2.1 *Concept of Design*

Ergonomics in biometrics also include physical and cognitive factors. The collectability might fall into the area of physical ergonomics, while the usability and acceptability could be categorized as cognitive ergonomics. In an ideal ergonomic biometric system, the user should barely notice the authentication process.[37] Otherwise, the system would have difficulty collecting high-quality samples.[37,38] As per early research, the natural and everyday motions are the most readily accepted way for users, which conforms with both physical and cognitive ergonomic principles.[39] We designed our ergonomic authentication system based on a systematic view in which the ergonomics were considered in the stage of characteristics selection, sample-collecting, imaging equipment design, feature extraction, and classification.

First, the finger geometry, knuckle print, and palmprint are some promising characteristics for the continuous and nondisruptive operator or driver authentication. The performance of face and iris recognition obviously degrades when the users move their heads to look at the surroundings and their instrument panels. At present, the methods based on behavior are impractical in actual working conditions and exhibit low accuracy. As for the hand, drivers are required to grab the operating rod during most of the manipulation period, which offers some robust characteristics for reliable and accurate biometrics.

Second, the imaging unit of our system is integrated into a traditional operating rod, which is the most acceptable modification in the driving and operating scene. As a standard operating part of cars, planes, ships, and heavy engineering machines, its structure and appearance have been optimized for several decades to fit the hand and operating habits. Meanwhile, grabbing the operating rod has become a typical action for daily driving and operating. Thus, the standard operating rod appearance would be an ideal physical ergonomic design. Furthermore, considering that the authentication performance is one of the major targets for our system, which requires high-quality images with sufficient features, a CIS imaging module is used to capture the hand skin surface to a panorama image under the constraints of the rod-like appearance.

Finally, the method of feature extraction and classification adopted should be robust to dislocations and fast to process. The dislocations of the hand are inescapable in a physical device design with weak guiding mechanisms, especially in our continuous biometric system where the hand is hard to keep in a fixed position for the entire session.

2.2 *Imaging Module*

The optical path of a conventional area image sensor needs two cone-shaped spaces, as shown in Fig. 4(a). With a constant field of view, the imaging area captured by this scheme is proportional to the square of the object distance. In the hand image acquisition system, this distance should be large enough to cover the whole hand. A longer optical path, however, occupies more space, which is a limitation of current capturing devices. Moreover, the off-axis interference light enters into the optical system easily, which could result in aberrations.

On the contrary, as shown in Fig. 4(b), the line-scan sensor captures a line image with a single row or a linear array of photodiodes, instead of a matrix of them. The field of view in the vertical direction is only one pixel, which is merely one of the thousands of the horizontal directions in our system. The optical path is a thin plane in 3-D space and could be greatly shortened by the rod lens array (RLA). Thus, the line-scan sensor requires a much smaller space for the optical path than that of an area image sensor.

The line-scan sensor takes sharp pictures of objects passing the camera at high speed in a vertical direction. The frames are continuously fed to a computing platform where they are jointed with each other to form an image. Instead of conventional line-scan sensors, the highly integrated CMOS line-scan sensor module—CIS—which consists of the light-emitting diode (LED) lights, microlenses, and several CMOS line-scan sensors, is customized for our system. These parts are integrated into one package, and all the control signals are pinned out through one common connector. This CIS module is equipped with an RLA, which is an array of highly polished cylindrical rod lenses with small diameter rods. The typical working distance of this kind of lens is about several millimeters. In the customized module, it is 1 to 7 mm. There are four types of LEDs deployed in our CIS module: 630 nm for red, 520 nm for green, 465 nm for blue, and 940 nm for infrared spectra. Typical palmprint features lay in the visible spectrum, from 380 to 780 nm. They make a hybrid of white with the color temperature of 6500 K. Recent research has discovered that multispectral palmprint images are better than

Fig. 3 Similar rod-like parts of (a) flight yoke used in Boing 737, (b) side stick used in Airbus A320, (c) voltage lever used in factories, (d) operating stick used in excavator, and (e) motorcycle grip type throttle control.

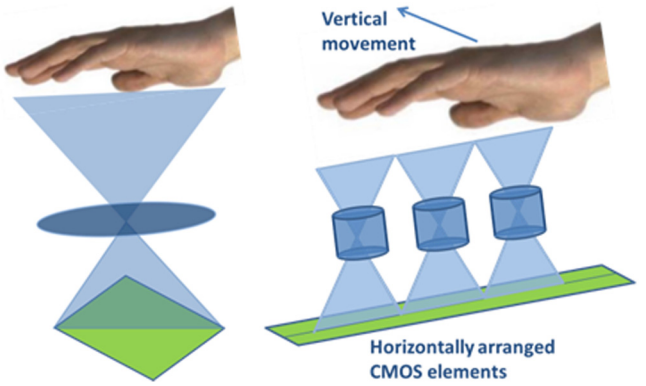

Fig. 4 Comparison of optical path space between (a) area array sensor-based imaging system and (b) line array sensor-based imaging system.

traditional palmprint recognition using the visible spectrum only.[40] In the proposed CIS module, near-infrared LEDs are deployed with the same intensity as the white light. Then the CMOS line-scan sensor records the overall light intensity of these four types of reflection rays from the hand and outputs a grayscale image. We showed the different imaging results of the regions of interest (ROIs) under six kinds of lighting conditions in Figs. 5(a)–5(f). The combination of visible and infrared illumination is good for antispoofing.

The line-scan sensor is 150 mm in length to capture the whole hand, which is the same as the horizontal length of the sampling area, while the vertical length of the sampling area is related to the diameter of the operating rod. According to the previous survey, the average width of the palm, which is also the hand width, is 84 mm for male and 74 mm for female, and the average hand length is 189 mm for a male and 172 mm for a female.[41] Although some parts of the palm near the wrist are easily lost for the grab pose, this part is out of our ROIs and has little influence on our authentication. The imaging area of our system is sufficient for capturing the finger and palm ROIs for most masculine and feminine hands.

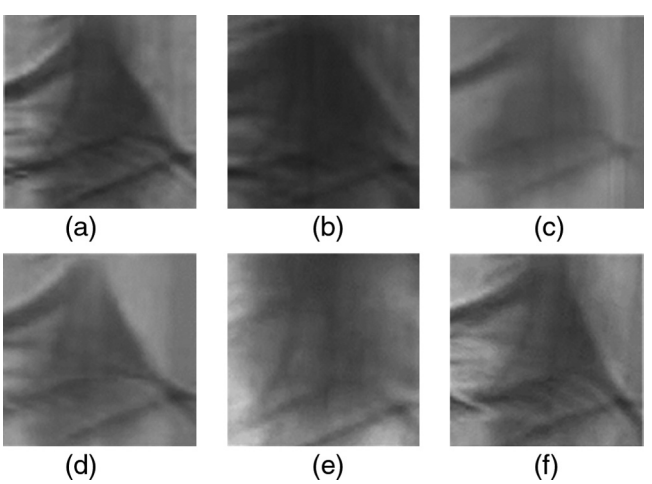

Fig. 5 Best quality palmprint ROIs of the left hand from the same volunteer, sampled with different illuminations: (a) only used the red light, $\lambda p = 630 \pm 15$ nm; (b) only used the green light, $\lambda p = 520 \pm 15$ nm; (c) only used the blue light, $\lambda p = 465 \pm 15$ nm; (d) only used the red, green, and blue light; (e) only used the infrared light, $\lambda p = 940 \pm 20$ nm; and (f) used all of the red, green, blue, and infrared light.

According to former studies, the default resolution of this customized CIS module is 100 dpi, the optimal physical resolution of palmprint features.[30] This parameter determines the horizontal resolution of the captured hand image and further affects the authentication performance. This CIS sensor scans at a speed of 45 μs per line in 100 dpi mode. Thus, it could capture 500 lines within 23 ms, theoretically. The gear motor only needs 1 s to drive the CIS for one round to get 500 lines of the full hand image in our system. The imaging speed guaranteed that the processing time would not be delayed by the sensor. Therefore, the entire processing time depends on the movement of the motor. The material of the shell, acrylic glass, is transparent to over 90% energy and to a large spectrum, including both the visible light and near-infrared light. We used the antifingerprints and antireflective multilayer coatings to keep the outside surface free from dust and oil. Meanwhile, the thickness of cylindrical glass shell is 1 mm, which keeps the hand skin 2 to 7 mm above the rod lens. Finally, the calibration of the pixel is implemented to reduce the interference of the noises. The gray value of the captured standard white images is distributed from 240 to 255 randomly, while the captured black images range from 0 to 10. We captured the white paper and the completely dark environment twenty times to get the average gray value $I\_$ white and $I_$black, respectively. Then, for the gray value I_0 of the point in the row image of the hand, the calibrated gray value I is calculated as follows:

$$I = \frac{I_0 - I\_\text{black}}{I\_\text{white}} \times 255. \tag{1}$$

2.3 *Controller Unit*

To capture images with high quality and high speed, the system should maintain a stable and accurate resolution in both vertical and horizontal directions. Figure 6 is the block diagram of the controller unit. A double-layered printed circuit board was built as the controller unit to regulate all the device

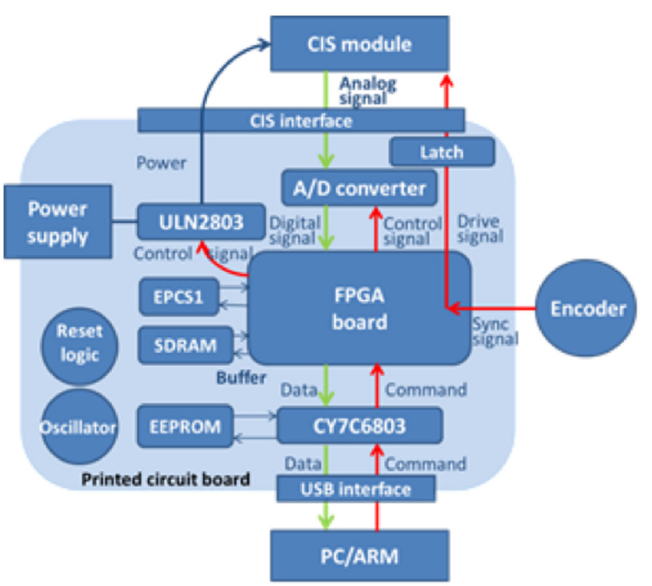

Fig. 6 Block diagram of the controller unit.

parts of our system and communicate with the computation platform through a universal interface. The FPGA board, which controls a synchronizing driver of CIS, an A/D controller, a data buffer, and a USB interface, is the core of the system.

The front side (a) and back side (b) of the printed circuit board are shown in Fig. 7. The Cypress USB CY7C68013A is used as the USB interface engine. EEPRROM and EPCS1 are used to store the firmware program of the CY7C68013A and the FPGA, respectively. The ULN2803 with 8-Darlington transistor array is the ideal equipment to link the low-voltage logic level digital circuit with the high-voltage, high-current circuit, and it is used to control the time of exposure of the LED in the CIS module as a switch. The latches recreate the digital signal to stabilize the voltage and increase the current, which makes the CIS get more stable signals.

The motion of the rotary shaft in the motor is digitized by the photoelectric encoder as synchronizing pulses output. Then, an affiliated gear set of the motor is used to drive the rotary CIS module steadily. The controller unit receives the synchronizing pulse from the photoelectric encoder of the motor and sends out the drive signal to the CIS. When the CIS module is ready for one line, the FPGA demands the AD9822 A/D converter to start reading analog pixel signals. Then the digitized 8-bit image signals are transferred out and stored in the synchronous dynamic random-access memory buffer. The input synchronizing signals, electricity, and output image data of the rotary CIS module are transferred by the slip ring. Finally, the data are sent to a computing platform through the USB interface.

The image resolution in the motion direction is defined by the perimeter of the rod and the imaging times per round. Given the reduction gear ratio R of the gear motor, the encoder sends out P pulse per round and the diameter of the cover's external surfaces D. If the CIS module rotates for one round, the axis of the encoder rotates $1/R$ rounds and sends out P/R pulses correspondingly. Then the synchronizing driver of CIS filters the pulses with a ratio R_0 and sends out one drive signal when it receives $1/R_0$ synchronizing pulses from the encoder. An inch is an imperial unit of length, approximately equal to 25.4 mm. The resolution S (in dpi) can be computed as follows:

$$S = 25.4 \times \frac{P/R}{\pi D} R_0. \tag{2}$$

In our prototype devices, the photoelectric encoder sends 40 pulses per round ($P = 40$). The R is 1/12.5, and the D is 40 mm, while the R_0 is 1. In this configuration, the vertical resolution (along the rolling direction) is 101 dpi, similar to the horizontal resolution of the CIS module (100 dpi). In real-world applications, the gear ratio and filter ratio need to be adjusted to maintain the vertical resolution for the rods with different diameters.

The imaging speed of the system is limited by the slowest part of the data flow. Hence, each part should be optimized to maximize the speed. First, the synchronizing unit should generate accurate synchronizing pulses according to the movement of the motor to minimize the lag. Second, the sensor needs to be fast enough for real-time image capturing to minimize the data waiting time in the buffer. Third, the speed of the A/D converter is required to be faster than the output of the pixels. A buffer could help cache the data while waiting for transfer through the interface. With this setting, the data flow speed only depends on the rotation of the motor.

Recently, biometric applications using the acquisition systems deployed in handheld or mobile platforms are very popular.[42] A framework in which both the desktop computation platform and the embedded platform are compatible with the same image-capturing device is proposed. The CY7C68013A works in Slave FIFO mode for the highest transferring speed and with minimum latency. Continuous transmission speed is over 18 MB/s in a dummy data test. Both the desktop computer and embedded advanced reduced instruction set computing machine platform drivers are implemented.

2.4 *Feature Extraction and Classification*

The recognition is separated into two phases. The first phase is a one-time identification to identify a person from a set of enrolled people, which is a $1:N$ (number of the registered users) classification task. Subsequently, in the second phase, the 1:1 authentication runs continuously to determine whether the user is changed. The difference between these two phases is the scale of the database of matching, which means identification requires the extracted features of all the

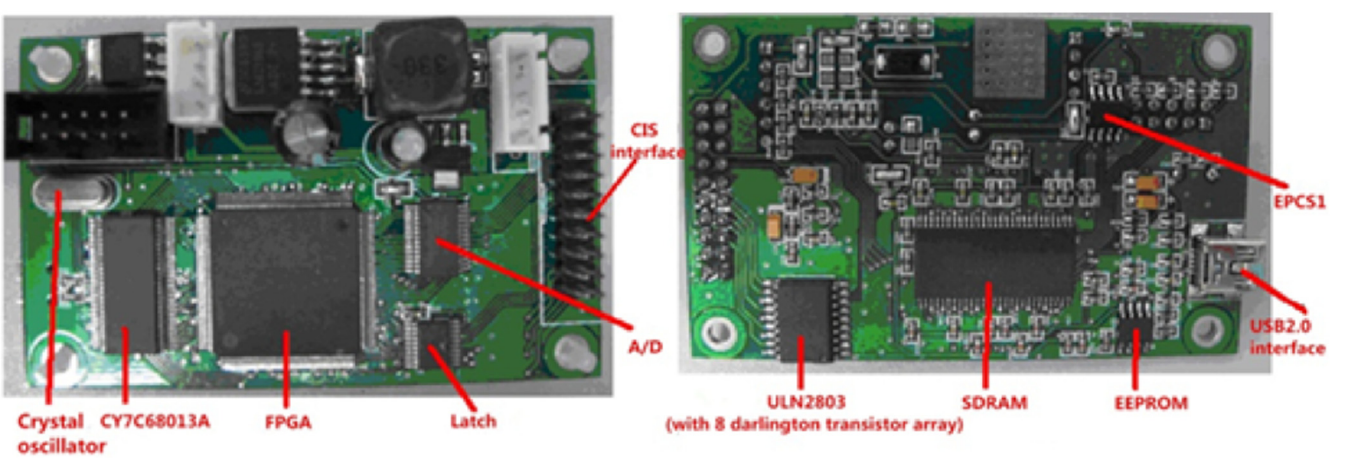

Fig. 7 Pictures of (a) the front side and (b) the back side of the PCB.

enrolled palms, while the authentication only needs the palm that matched in the first phase.

The sampling area of the hand surface includes the fingers and palm. However, the skin of those hand areas is subjected to varying amounts of extruding. Thus, the features that could be extracted from the high-resolution images, such as the ridges, singular points, and minutia points, are not reliable for the corresponding deformation. Fortunately, almost all palmprint recognition research focuses on low-resolution images (≤150 dpi) for commercial and civil applications in recent years, and the effect was tested.

A series of hand images captured along with the rotation of the motor by the operating rod system and processed to extract the ROIs are shown in Fig. 8. The imaging quality of the vertical direction was well uniformed throughout the session, while the rotating speeds of the motor do not need to be uniform with the help of the synchronization unit. It is hard to define an initial point of one hand in this peg-free system. Thus, at least two rounds of rotation are required for recognition to offer at least one integral hand image. Then, this image was filtered by the two-dimensional Gaussian low-pass filter and binary transformed by Otsu algorithm[43] to track the boundary of the hands. The largest connectivity area is an integral hand image. Finally, the ROIs location is computed based on the work of Guo et al.,[44] which is also utilized in the previous systems.[40,45,46] The extracted ROIs of a hand for four times sampling with our system are shown in Fig. 9(b) and compared with the former database captured by the area-base system[46] in Fig. 9(a). Our results show clear texture and deeper principal lines for the bending of the hand. The nonuniform gray distribution could be introduced by refracting and reflecting of the glass cover and the limited imaging distance of the micro-RLA. This could be rectified using the histogram equalization without degrading the recognition quality.

For online feature extraction, competitive coding is implemented. The images convolve with the Gabor filters to extract the orientation information of the palm lines.[47] The Gabor function has the following form:

$$\psi(x,y,x_0,y_0,\omega,\theta,\kappa)=\frac{-\omega}{\sqrt{2\pi}\kappa}e^{-\frac{\omega^2}{8\kappa^2}(4x\prime^2+y\prime^2)}\left[\cos(\omega x\prime)-e^{-\frac{\kappa^2}{2}}\right], \tag{3}$$

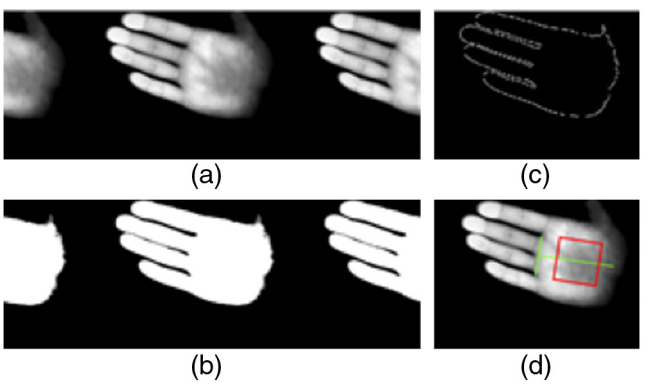

Fig. 8 ROIs extraction: (a) palmprint sample, (b) binary image processing, (c) contour extraction, and (d) located ROIs.

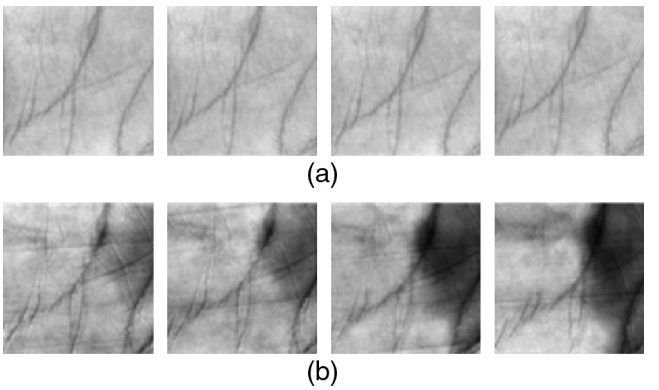

Fig. 9 Extracted ROIs of palmprint: (a) captured by the conventional area-based system[46] and (b) captured by the proposed system.

$$\kappa=\sqrt{2\ln 2}\left(\frac{2^{\delta}+1}{2^{\delta}-1}\right), \tag{4}$$

where the $x'=(x-x_0)\cos\theta+(y-y_0)\sin\theta$, $y'=-(x-x_0)\sin\theta+(y-y_0)\cos\theta$, (x_0,y_0) is the center of the Gabor function, ω is the radial frequency in radians per unit length, and θ is the orientation of the functions in radians. When the standard deviation σ and the half-amplitude bandwidth of the frequency response δ are fixed, ω can be calculated from $\omega=\kappa/\sigma$. Thus, the parameter settings of the σ and the δ have an effect on the performance. These neurophysiology-based Gabor functions are approximate to the general Gabor functions, while the choices of parameters are limited by neurophysiological findings. Moreover, the direct current of the function is removed. These Gabor functions will be used to extract orientation information from palm lines. Three bits were used to represent an element and one bit for the mask. Thus, the four bit-planes could constitute a competitive code.[47] The total size of the proposed feature, including the mask and the competitive code, is 384 bytes.

Then, the Hamming distance is utilized for feature matching, which is efficient in conventional area camera systems.[46] Based on the generally accepted method for feature extraction and matching, it is more persuasive to compare the performance of our system to other palm recognition devices.

3 System Testing

3.1 *Dataset*

In our hand image database, 4000 images were equally collected from 400 hands of 200 people in one session. Considering that squeezing the skin will introduce additional intraclass differences, five of ten images rather than one for each hand were randomly selected for the enrollment, and the others were used for testing. The volunteers were trained for 2 to 5 times before the sampling to grab the operating rod slightly and keep more than three periods of rotation for a hand image sequence with at least one complete hand image. In the capture stage, grasping was implemented 10 times for each hand for 10 image sequences. Then, one of the complete hand images in each sequence was selected to our database manually. The thumb was advised to be placed against the basal plane of the rod to avoid the connection with the other four fingers for those long-handed

people. The samples captured from our system are 1000×600 in size with a resolution of 100 dpi grayscale images.

3.2 *Experiment Result*

The performance is the major concern of a recognition system in which the equal error rate (EER) and the receiver operating characteristic (ROC) curves are provided for evaluation. The EER is the cross point of the false rejection rate (FRR) curve and the false acceptance rate (FAR) curve, widely adopted to briefly evaluate the accuracy of a biometric. The ROC can also depict the overall performance with the FAR against the genuine attempts accepted rate (GAR, equal to $1 - \mathrm{FRR}$), which is independent of the distant threshold.

The EER largely depends on the parameter setting of the σ and the δ in the feature extraction. Based on the rough validation of our system, the σ from 4.0 to 6.0 and the δ from 2.0 to 4.0 can be more effective. Then we tested 400 settings of σ and δ more precisely with the step size of 0.1 to find the best setting. The relationship of the EER and the σ and δ is illustrated in Fig. 10. The EER ranges from 0.1179% to 1.9418% and reaches the minimum value when the σ is 4.2 and the δ is 2.9. Five parameter settings with relatively small EER and corresponding distance threshold are listed in Table 1.

Then, the 4.2, 2.9, and 0.3852 for the σ, δ, and the distance threshold, respectively, are selected for our system with the 0.1179% of the EER. The corresponding distributions of imposter and genuine are shown in Fig. 11(a). The ROC is shown in Fig. 11(b); even when the FAR is as low as 10^{-2}, the GAR is still above 98.5%.

The output of the continuous authentication system in a period T is a decision sequence of reject or accept at each time point. The false acceptance worst (FAW)-case interval and false rejection worst (FRW)-case interval are two recently suggested parameters that present the longest time interval over which an imposter/a legitimate user might be falsely accepted as a legitimate user/falsely rejected and marked as an imposter.[48] We obtained these two metrics of our system with a half hour continuous operating test for 20 times by different operators. The output of each test is a sequence of 1800 decisions, which is calculated in every second. Then we used the largest FAW (2 s) and FRW (5 s) among 20 tests as a conservative choice, which means that the system may falsely reject two successive requests of a legitimate user or falsely accept an imposter as a legitimate user in four consecutive trails in the worst case. It is noteworthy that two successive false decisions may depend on a continuous pose or squeezing, which makes us fail to calculate the probability from the FAR or FER statistically.

However, simply logging out a user based on one reject decision will introduce inconvenience and even danger during operating or driving. A trust level (TL)-based real-time adaptive authorization scheme can be used to alleviate this issue.[49] The TL quantizes how much we trust a user based on previous decisions, making it a value between 0 and 100, where the higher numbers indicate a higher level of trust. Our starting value of TL is 100 after the user was authorized in the initial time. We then continuously update the TL by a

Table 1 EER and distance threshold of parameter settings.

Parameter setting	EER (%)	Distance threshold
$\sigma = 4.2\ \delta = 2.9$	0.1179	0.3852
$\sigma = 4.1\ \delta = 3.1$	0.1213	0.3794
$\sigma = 4.2\ \delta = 3.0$	0.1281	0.3819
$\sigma = 4.4\ \delta = 2.6$	0.1281	0.3993
$\sigma = 4.2\ \delta = 2.7$	0.1292	0.3974

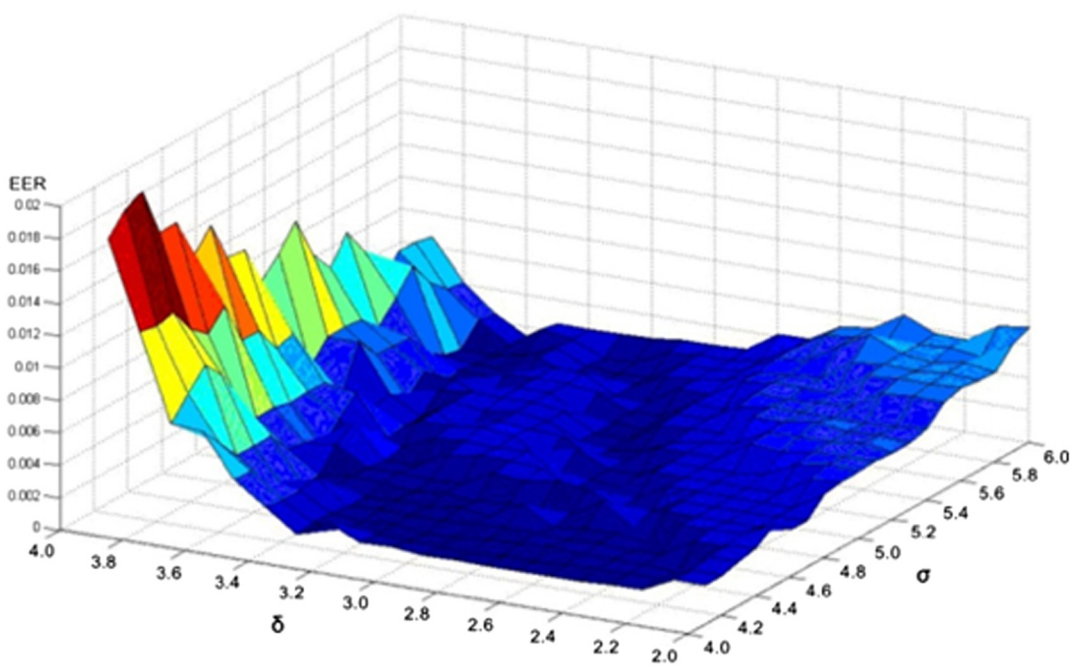

Fig. 10 Distribution of EER for different σ and δ.

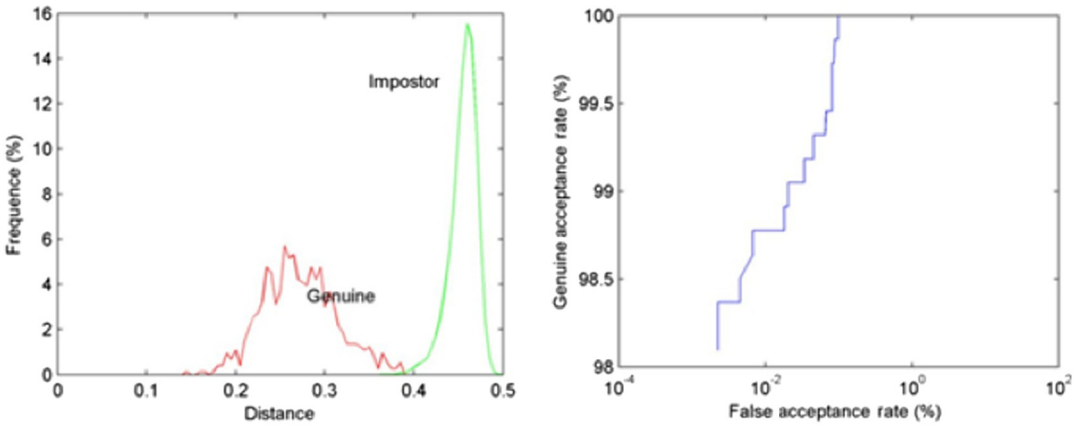

Fig. 11 Performance curve when the $\sigma = 4.2$, $\delta = 2.9$. (a) Imposter and genuine distributions and (b) the ROC curve.

constant step after each decision, e.g., add a C_{Accept} to the TL if the decision is to accept, else minus a C_{Reject}. The value of C_{Accept} and C_{Reject} should be chosen to make TL become 100 when we confidently verify that the user is legitimate and becomes 0 as soon as we detect the presence of an impostor. According to the values of FAW and FRW mentioned above, if we receive more than two accept decisions, TL should become 100, while we can be confident to detect an imposter (TL = 0) with six reject decisions. Hence, we can set the $C_{\text{Accept}} = \frac{100}{\text{FAW}+1} = \frac{100}{3} \approx 34$ and $C_{\text{Reject}} = \frac{100}{\text{FRW}+1} = \frac{100}{6} \approx 17$ for our system. Different thresholds of the TL should be set for different operation devices and levels.

3.3 *Discussion*

As the first continuous authentication system using the palmprint, our proposed system outperforms traditional continuous authentication systems regarding accuracy and efficiency for driving and operating scenes. As mentioned in Sec. 1, several physiological or behavior trait-based continuous authentication systems have been proposed. Table 2 compared our system to the other state-of-the-art continuous authentication systems based on keyboard, mouse, face, and biomedical signal streams. Benefiting from the fast decision process, both the FAR and FRW are less than 5 s, which is much shorter than the latest biomedical signal-based system (FAR = 4 min and FRW = 3 min). Unlike most continuous authentication systems mentioned above compatible for personal computers and laptops, the proposed system can also support an embedded system to follow the trend of mobile devices general purpose computing unit.

The minimum EER our system achieved is 0.1179% in the recognition test, which is slightly larger than that of conventional multispectral area-based palmprint recognition system, but still competitive compared with the recognition of fingerprint and face. The performance of this device also enables it to be a good one-time recognition system for more applications, e.g., door handle and any desk/embedding computing systems. A detailed comparison between the proposed device and the conventional area-based scan palmprint recognition system is shown in Table 3. What must be mentioned is that the values of EER are validated on four different databases captured by four kinds of equipment, respectively. Our database size is close to those systems;[40,45,46] the EERs are given in Table 3 as a reference for system assessment.

The ergonomics-optimized form of the rod encourages a natural hand posture for operation. The skin of the hand is not flattened in a grab posture, making it a challenge for traditional systems. In our proposed system, however, a better performance than our expectation was achieved. One of the main reasons could be the fixed curvature of the rod and the hand. Another explanation is that the gesture or even the action of a person could be persistent after thousands or even millions of repetitions in a long period, which is also the foundation of many behavior biometrics.

There are still three limitations of this system. First, the dataset covers only the adult Chinese in our institution; different skin colors of different races might require different

Table 2 Comparison between different continuous authentication systems.

Systems	Passiveness	Stability	Available in car	EER (%)	Decision time
Keyboard based[24]	+++	+	–	0.5 to 17.6	≈4 min
Mouse based[12]	+++	+	–	2.5 to 26.8	≈1 min
Face based[50]	++	++	++	2.4 to 20	≤1 s
Biomedical based[38]	++	++	++	1.9	1 min
Proposed	+++	+++	+++	0.1179	1 s

Table 3 Comparison between the hand scan systems.

Items	Proposed	System[46]	System[45]	System[40]
Sensor type	CIS	Area CCD	Area CCD	Area CCD
Hand pose	Bended	Stretched	Stretched	Stretched
Resolution	100 dpi	75 dpi	75 to 150 dpi	<100 dpi
Illumination	Multispectrum	Fluorescent	Fluorescent	Multispectrum
Cold start time	40 ms	90 ms	90 ms	90 ms
ROI extract time	212 ms	538 ms	538 ms	138 ms
Feature extract	36 ms	84 ms	36 ms	36 ms
Matching time	0.06 ms	1.7 ms	0.06 ms	0.06 ms
EER	0.1179%	0.6%	0.107%	0.052%
Dimensions (cm^3)	$\pi \times 2^2 \times 25$ (288)	$32 \times 16 \times 19$ (9728)	$32 \times 16 \times 19$ (9728)	$34 \times 28 \times 26$ (23,296)
Platforms	Desktop/embedded Windows/Linux	Desktop windows	Desktop windows	Desktop windows

illumination parameters, which have not been tested. In addition, more than two sessions of sampling across years are expected for a mature biometric system. Second, four fingers (index, middle, ring, and little) are well imagined in our system but have not been utilized for matching. The four fingers are often too close in our dataset, making it hard to separate them accurately with low computation cost and then extract the finger geometry (mean width, length, and N-dimension finger shape vectors) and the knuckle print location trait. The abundant features in the fingers deserve a further exploration.

4 Conclusions

In this paper, we present a CIS-based continuous hand authentication system to expand the application of palmprint biometrics. A customized and highly integrated CIS, a self-adaptive motion synchronizing controller unit, and a cross-platform USB interface are featured in our system. We designed a biometric system with a small size and considering previous ergonomics constraints without compromising authentication performance, which is more efficient and effective for the particular application of people using the rod operator than the current continuous biometrics. Furthermore, inspired by the proposed system, more practical and applicable hand biometric systems could be invented. In addition to the palmprint characteristics we used, other discriminative information in the image, e.g., hand shape, finger print, and knuckle print, are worth studying.

Future research will optimize the structure of the current design and integrate the controller unit into the rod. By choosing a more compact gear motor and battery,[51,52] an even smaller system could be made. Moreover, with further study on behavior biometrics, an irregular cover might be designed to offer a more comfortable grab feel.

Acknowledgments

This work was supported by the Youth Innovation Promotion Association, Chinese Academy of Sciences (CAS) (No. 2017264) and Innovative Foundation of the Changchun Institute of Optics, Fine Mechanics and Physics, CAS under Grant No. Y586320150, and Youth Innovation Promotion Association, CAS, (2017264). In particular, we want to give thanks to Professor Vijayakumar Bhagavatula for his support and guidance of revision. The authors thank the anonymous referees who made useful comments on the work. The authors declare no conflict of interest.

References

1. S. P. Miller et al., "Kerberos authentication and authorization system," in *Proc. Project Athena Technology Plan* (1987).
2. T. Sim et al., "Continuous verification using multimodal biometrics," *IEEE Trans. Pattern Anal. Mach. Intell.* **29**(4), 687–700 (2007).
3. J. Bonneau et al., "The quest to replace passwords: a framework for comparative evaluation of web authentication schemes," in *Proc. IEEE Symp. Security Privacy*, pp. 553–567 (2012).
4. C. Ma, D. Wang, and S. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," *Int. J. Commun. Syst.* **27**(10), 2215–2227 (2014).
5. A. Al Abdulwahid et al., "A survey of continuous and transparent multi-biometric authentication systems," in *European Conf. on Cyber Warfare and Security*, Hatfield, pp. 1–10 (2015).
6. S. Egelman et al., "Are you ready to lock?" in *Proc. ACM Conf. Computer and Communications Security*, pp. 750–761 (2014).
7. K. Niinuma, U. Park, and A. K. Jain, "Soft biometric traits for continuous user authentication," *IEEE Trans. Inf. Forensics Secur.* **5**(4), 771–780 (2010).
8. M. L. Gavrilova and M. Monwar, *Multimodal Biometrics and Intelligent Image Processing for Security Systems*, IGI Global, Hershey (2013).
9. I. B. Barbosa, T. Theoharis, and A. E. Abdallah, "On the use of fingernail images as transient biometric identifiers," *Mach. Vision Appl.* **27**(1), 65–76 (2016).
10. A. S. Anwar, K. K. A. Ghany, and H. ElMahdy, "Human ear recognition using SIFT features," in *IEEE 2015 Third World Conf. on Complex Systems (WCCS)*, pp. 1–6 (2015).
11. S. K. Jha, C. Liu, and K. Hayashi, "Molecular imprinted polyacrylic acids based QCM sensor array for recognition of organic acids in body odor," *Sens. Actuators B* **204**, 74–87 (2014).
12. C. Shen, Z. Cai, and X. Guan, "Continuous authentication for mouse dynamics: a pattern-growth approach," in *Proc. IEEE Int. Conf. Dependable Systems and Networks*, pp. 1–12 (2012).
13. P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," *Sci. World J.* **2013**, 1–24 (2013).
14. K. Niinuma and A. K. Jain, "Continuous user authentication using temporal information," *Proc. SPIE* **7667**, 76670L (2010).
15. D. Crouse et al., "Continuous authentication of mobile user: fusion of face image and inertial measurement unit data," in *Proc. IEEE Int. Conf. Biometrics*, pp. 135–142 (2015).
16. P.-W. Tsai et al., "Interactive artificial bee colony supported passive continuous authentication system," *IEEE Syst. J.* **8**(2), 395–405 (2014).

17. J. Roth, X. Liu, and D. Metaxas, "On continuous user authentication via typing behavior," *IEEE Trans. Image Process.* **23**(10), 4611–4624 (2014).
18. S. Mondal and P. Bours, "Context independent continuous authentication using behavioural biometrics," in *Proc. IEEE Int. Conf. Identity, Security and Behavior Analysis*, pp. 1–8 (2015).
19. I. Traore et al., "Dynamic sample size detection in learning command line sequence for continuous authentication," *IEEE Trans. Systems Man Cybern.* **42**(5), 1343–1356 (2012).
20. P. Bours and S. Mondal, "Performance evaluation of continuous authentication systems," *IET Biom.* **4**(4), 220–226 (2015).
21. J. Sohankar et al., "E-bias: a pervasive EEG-based identification and authentication system," in *Proc. 11th ACM Symp. QoS and Security for Wireless and Mobile Networks*, pp. 165–172 (2015).
22. Z. Zhao et al., "A human ECG identification system based on ensemble empirical mode decomposition," *Sensors* **13**(5), 6832–6864 (2013).
23. R. D. Labati, R. Sassi, and F. Scotti, "ECG biometric recognition: permanence analysis of QRS signals for 24 hours continuous authentication," in *Proc. IEEE Int. Wkshp. Information Forensics and Security*, pp. 31–36 (2013).
24. S. P. Banerjee and D. L. Woodard, "Biometric authentication and identification using keystroke dynamics: a survey," *J. Pattern Recognit. Res.* **7**(1), 116–139 (2012).
25. V. M. Patel et al., "Continoius user authentication on mobile devices: recent progress and remaning challenges," *IEEE Signal Process. Mag.* **33**(4), 49–61 (2016).
26. A. Riener, "Sitting postures and electrocardiograms: a method for continuous and non-disruptive driver authentication," in *Continuous Authentication Using Biometrics: Data, Models, and Metrics*, I. Traore, Ed., pp. 137–168, IGI Global (2011).
27. A. Riener and A. Ferscha, "Supporting implicit human-to-vehicle interaction: driver identification from sitting postures," in *Proc. of the 1st Int. Symp. on Vehicular Computing Systems*, pp. 1–10, Trinity College Dublin, Ireland (2008).
28. I. Traore, Ed., *Continuous Authentication Using Biometrics: Data, Models, and Metrics*, IGI Global, Hershey (2011).
29. A. Morales, E. González, and M. A. Ferrer, "On the feasibility of interoperable schemes in hand biometrics," *Sensors* **12**(2), 1352–1382 (2012).
30. A. Kong, D. Zhang, and M. Kamel, "A survey of palmprint recognition," *Pattern Recognit.* **42**(7), 1408–1418 (2009).
31. C. M. Travieso, J. C. Briceño, and J. B. Alonso, "Transformation of hand-shape features for a biometric identification approach," *Sensors* **12**(1), 987–1001 (2012).
32. L.-Q. Zhu and S.-Y. Zhang, "Multimodal biometric identification system based on finger geometry, knuckle print and palm print," *Pattern Recognit. Lett.* **31**(12), 1641–1649 (2010).
33. D. Zhang et al., "An online system of multispectral palmprint verification," *IEEE Trans. Instrum. Meas.* **59**(2), 480–490 (2010).
34. W. Li et al., "A novel 3-D palmprint acquisition system," *IEEE Trans. Syst. Man Cybern. Part A Syst. Humans* **42**(2), 443–452 (2012).
35. L. Shen et al., "Embedded palmprint recognition system using OMAP 3530," *Sensors* **12**(2), 1482–1493 (2012).
36. M. G. K. Ong et al., "A single sensor hand geometry and palmprint verification system," in *Proc. ACM SIGMM Workshop Biometrics Methods Appl.*, Berkeley, pp. 100–106 (2003).
37. T. Dunstone and N. Yager, Eds., *Biometric System and Data Analysis—Design, Evaluation, and Data Mining*, Springer, New York (2009).
38. F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "Quality measures in biometric systems," *IEEE Secur. Privacy Mag.* **10**(6), 52–62 (2012).
39. A. Albrecht, "Understanding the issues behind user acceptance," *Biom. Technol. Today* **9**(1), 7–8 (2001).
40. A. K. Jain and J. Feng, "Latent palmprint matching," *IEEE Trans. Pattern Anal. Mach. Intell.* **31**(6), 1032–1047 (2009).
41. Jillian, "Average hand size—your resource for hand size, palm size and finger length averages," http://www.theaveragebody.com/average_hand_size.php (4 November 2012).
42. Y. K. R. Sánchez and S. A. Demurjian, "Towards user authentication requirements for mobile computing," in *Innovative Solutions for Access Control Management*, A. K. Malik, Ed., pp. 160–196, IGI Global, Hershey (2016).
43. N. Otsu, "A threshold selection method from gray-level histograms," *IEEE Trans. Syst. Man Cybern.* **9**(1), 62–66 (1975).
44. Z. Guo et al., "Palmprint verification using binary orientation co-occurrence vector," *Pattern Recognit. Lett.* **30**(13), 1219–1227 (2009).
45. M. Wong et al., "Real-time palmprint acquisition system design," *IEEE Proc. Vis. Image Signal Process.* **152**(5), 527–534 (2005).
46. D. Zhang et al., "Online palmprint identification," *IEEE Trans. Pattern Anal. Mach. Intell.* **25**(9), 1041–1050 (2003).
47. A. W.-K. Kong and D. Zhang, "Competitive coding scheme for palmprint verification," in *Proc. 17th Int. Conf. Pattern Recognition*, Cambridge, Vol. **1**, pp. 520–523 (2004).
48. A. Mosenia et al., "CABA: continuous authentication based on bioaura," *IEEE Trans. Comput.* **PP**(99), 1 (2016).
49. I. Deutschmann, P. Nordstrom, and L. Nilsson, "Continuous authentication using behavioral biometrics," *IEEE IT Prof.* **15**(4), 12–15 (2013).
50. D. V. Jadhav, P. K. Ajmera, and N. S. Nehe, "Real time human face location and recognition system using single training image per person," in *Proc. Annual IEEE India Conf.*, pp. 1–5 (2011).
51. S. Li et al., "Yolk-Shell Sn@C eggette-like nanostructure: application in lithium-ion and sodium-ion batteries," *ACS Appl. Mater. Interfaces* **8**(30), 19438 (2016).
52. S. Li et al., "Carbon fiber cloth@ VO 2 (B): excellent binder-free flexible electrodes with ultrahigh mass-loading," *J. Mater. Chem. A* **4**(17), 6426–6432 (2016).

Xiaofeng Liu received his BEng degree in automation and BA degree in communication from the University of Science and Technology of China, Hefei, China, in 2014. He is currently pursuing his PhD at the University of Chinese Academy of Sciences (CAS), Beijing, and is a visiting PhD student in the Department of Electrical and Computer Engineering, Carnegie Mellon University. His research interests include image processing, computer vision, and pattern recognition.

Lingsheng Kong received his bachelor's degree from the University of Science and Technology of China in 2007 and his PhD in optical engineering from the Graduate University of the CAS in 2012. He is currently an associate researcher at Changchun Institute of Optics, Fine Mechanics and Physics, CAS. His current research interests include optical engineering, three-dimensional (3-D) imaging, light field, and virtual reality.

Zhihui Diao received his bachelor's degree from Harbin Engineering University in 2010 and his PhD from the University of the CAS in 2015. He is currently an assistant researcher with Changchun Institute of Optics, Fine Mechanics and Physics, CAS. His current research interests include optical engineering and 3-D imaging.

Ping Jia obtained his MSc degree in computer science from the University of Science and Technology of China and his PhD from the Graduate University of the CAS. He is currently the president at Changchun Institute of Optics, Fine Mechanics and Physics, CAS. His current research interests include image processing, computer vision, and optical engineering.