Biometric Recognition: Sensor Characteristics and Image Quality

Salil Prabhakar, Alexander Ivanisov, and Anil Jain

Biometric recognition, or simply biometrics, refers to recognizing a person based on one or more of his anatomical or behavioral characteristics. A good biometric trait should be measurable, distinctive (different for every person) and stable over time. The sensing method should not be intrusive or socially unacceptable, and the system should be easy to use. A biometric system based on this trait should be accurate, fast, robust and inexpensive. In this article, we discuss the signal acquisition aspects of fingerprint and iris biometrics—two of the most widely used biometric traits.

Introduction

Personal recognition of people is necessary to conduct many social and economic activities. Figs. 1a-c show examples of biometric systems. Besides visual recognition of acquaintances, checking a person's government issued photo ID is the most common procedure. In electronic access or transactions, passwords and security tokens are commonly used. These credentials are surrogates of a person's identity. Their major shortcoming is that they can be easily compromised by being lost, stolen, or given to someone else. For better security, it is necessary to link the digital identity of a person to his body's characteristics.

A Biometric System

A biometric system may be viewed as a signal detection system with a pattern recognition architecture that senses a biometric signal, processes this signal to extract a salient set of features, compares these features against the feature sets residing in the database (templates), and makes a decision about the identity of the person providing the input biometric signal. Fig. 2 shows a fingerprint recognition system. A biometric system can operate either in *verification* mode, where a claim of identity is submitted together with the captured biometric data or in *identification* mode, where the biometric data is submitted without any claim of identity. The claim of identity may be a *positive claim*, where a subject claims that he is enrolled in the system. This is typically the case when a person wants to enter a secure facility. The claim of identity can be a *negative claim*, where a subject claims that he is not enrolled in the system. This is typically the case in government entitlement applications, where the subject claims that he has not been previously enrolled in the program. In such applications, there is no substitute for biometrics to detect "multiple enrollments" or "double dippers". For more details of the biometric system, their components and processes, see [1].

Every authentication system makes some errors. For example, verification using a 4-digit PIN has a 1 in 10,000 chance of being guessed (*false positive error*). There is also a small but finite chance that the subject will forget or mistype his PIN (*false negative error*). The errors made by a biometric system are numerous because of the nature of interaction between the human body and the biometric sensor as well as the variability in the biometric signal of the same trait captured at different times. The main types of errors are referred to as *Failure to Enroll*, *False Match*, *False Non-Match*, *False Negative Identification* and *False Positive Identification*. Some of the errors in a biometric system are interrelated. For example, there is typically an inverse relationship between the false non-match rate (FNMR) and false match rate (FMR). It is also important to emphasize that the biometric system's performance depends on the demographics of the population, the characteristics of the sensor, and the environmental conditions. In evaluations conducted by NIST at a false accept rate (FAR) of 0.1%, the false reject rate (FRR) of fingerprint and iris were 0.25% [2] and 1.1% [3], respectively.

In a recent evaluation performed by UIDAI in India, at an FPIR of 0.0025%, an FNIR of 0.5% on two-irides, 0.25% on 10-fingerprints, and 0.01% on a combination of 2-irides and 10-fingerprints was reported on a gallery size of 20,000 records [4].

This research was supported by the WCU (World Class University) program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (R31-2008-000-10008-0).

1094-6969/11/$25.00©2011IEEE

(a)

(b)

(c)

Fig. 1. Examples of biometric systems. (a) A fingerprint scanner used at US borders by US-VISIT in a border control program. Photo: Courtesy of Crossmatch, Inc. (b) An iris sensor used in an expellee program, DubaiDesk, at the UAE borders. Photo: Courtesy of Prof. John Daugman. (c) A sensor used in India's Unique Identity Program that provides identity to every resident in India.

Fingerprint

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of

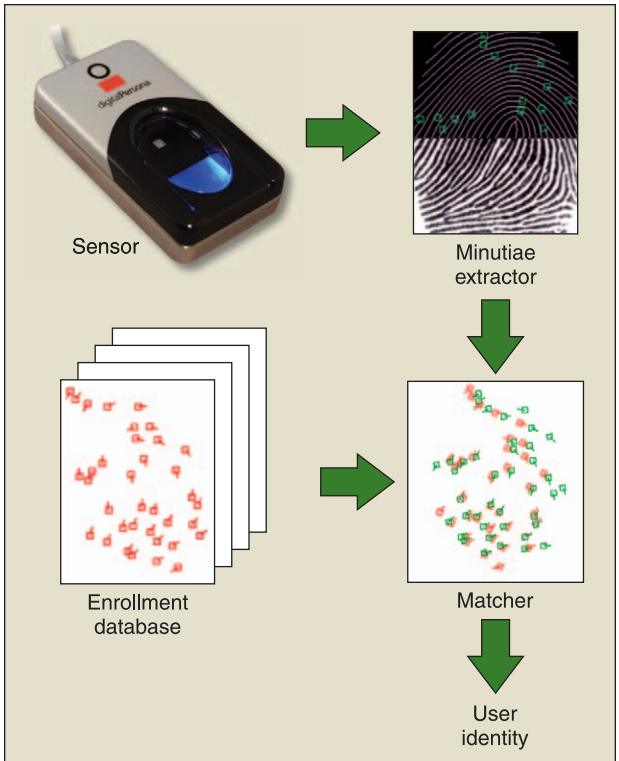

Fig. 2. Fingerprint recognition system.

identical twins are different and so are the prints on each finger of the same person. While fingerprints have been used in law enforcement for over 100 years, civil identification and commercial applications are currently the most popular markets for fingerprint biometric technology. Fingerprint matching is extremely accurate and all ten fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities. In this section, we provide details of fingerprint sensing technology. Note that while the rolled-ink method of fingerprinting is still practiced in law enforcement, our focus here is on live scan technology which directly provides a digital image of a fingerprint.

Fingerprint Sensors

The most common live scan fingerprint sensing method is the frustrated total internal reflection (FTIR) method. Direct optical imaging methods are gaining popularity and methods based on optical fibers and light emitting polymers also exist.

FTIR: When a finger touches the top side of a glass or plastic prism (imaging surface), the ridges make contact with the imaging surface while the valleys do not. One side of the prism is typically illuminated with a diffused light source (a bank of light-emitting diodes or a film planar light). The light entering the prism is reflected at the valleys and randomly scattered at the ridges. The light rays exit from the other side of the prism and are focused through a lens onto a CMOS image sensor as Fig. 3a shows. The valleys appear bright due to reflection and ridges appear dark due to lack of reflection. Different geometries of the prism such as a micro-prism array

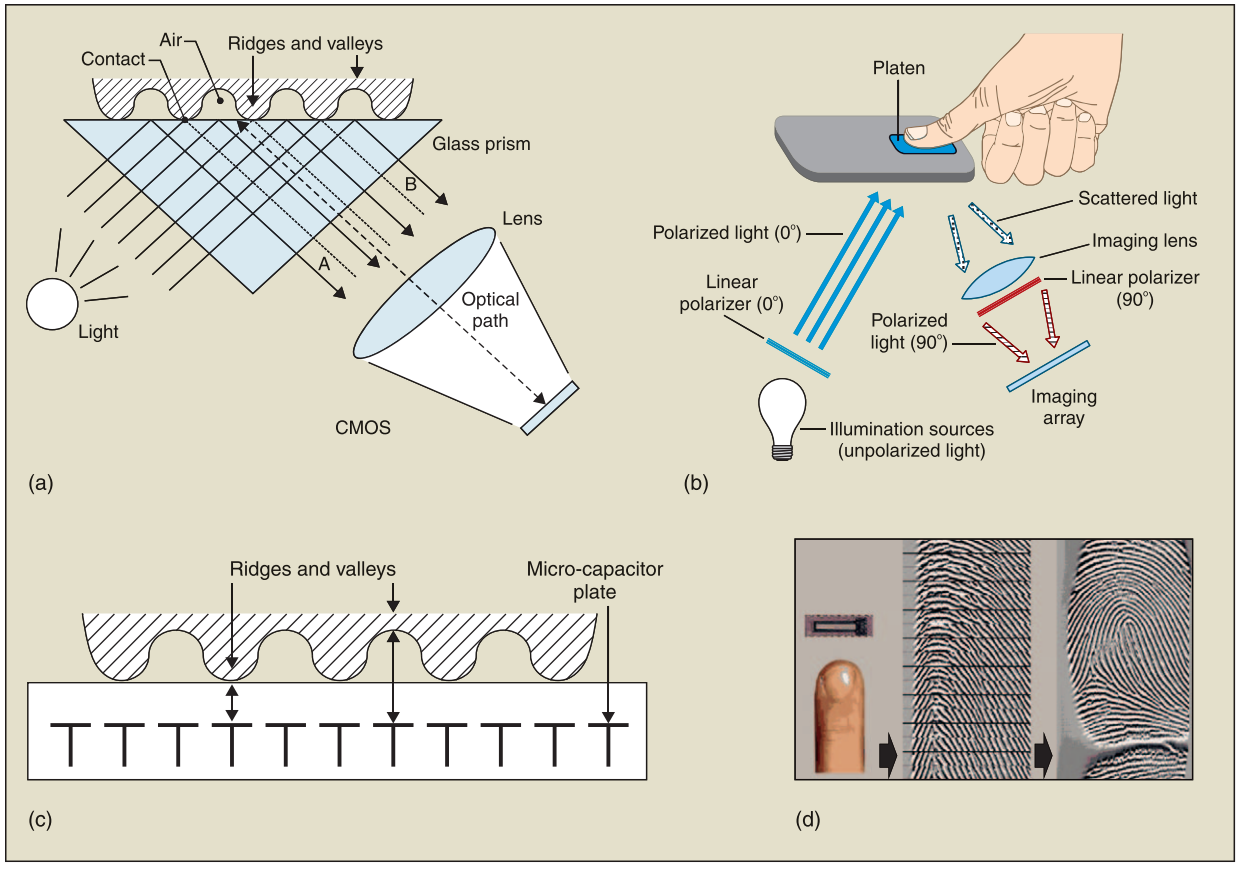

Fig. 3. Fingerprint sensing technologies. (a) FTIR fingerprint sensing. (© 2009 Springer, used with permission from [1].) (b) Direct optical imaging fingerprint sensing. (Courtesy of Lumidigm Inc. from [5].) (c) Capacitive fingerprint sensing. (©2009 Springer, used with permission from [1].) (d) Sweep sensor. (©2009 Springer, used with permission from [1].)

and dark-field imaging approach have been used to reduce the size and cost of the scanner.

Direct imaging: In this approach a camera is directly focused on the fingertip. The finger does not need to be in contact with any surface (touchless acquisition), and the scanner may be equipped with a mechanical support to facilitate the user in presenting the finger at a uniform distance as Fig. 3b shows. One variation of direct imaging is to capture multiple images of the finger under different illumination schemes (wavelength, illumination orientation, polarization, etc.) and then to combine them into a single image using an algorithm. Direct imaging is believed to be more robust for acquiring images of fingers with non-ideal conditions, e.g., dry fingers. However, obtaining well-focused and high-contrast images with the touchless methods is challenging.

Three-dimensional imaging: A 3D fingerprint image can be obtained by using multiple cameras that acquire images from different viewpoints and then fusing them. In another variation, a structured light source is used to illuminate the finger with a specific pattern.

Solid-State Sensors

Solid-state sensors have gained popularity due to their small size and low cost. Solid state sensors are part of live-scan fingerprint scanners and measure some physical property of the fingerprint and convert it to a digital fingerprint image. Two of the most popular types of solid-state fingerprint sensors are capacitive and electric field.

Capacitive sensor: A capacitive sensor is a two-dimensional array of micro-capacitor plates embedded in a chip as Fig. 3c shows. The other plate of each micro-capacitor is the finger skin itself. Small electrical charges are created between the surface of the finger and each of the silicon plates when a finger is placed on the chip. The magnitude of these electrical charges depends on the distance between the fingerprint surface and the capacitance plates [1]. Thus, fingerprint ridges and valleys result in different capacitance patterns across the plates.

Electric field sensor: The sensor consists of a drive ring that generates an RF signal and a matrix of active antennas that receives a very low amplitude signal transmitted by the drive ring and modulated by the derma structure (subsurface of the finger skin). The finger must be simultaneously in contact or close proximity with both the sensor and the drive ring. To image a fingerprint, the magnitude of the RF signal is measured for each pixel element [1].

Touch Versus Sweep Sensors

Most of the fingerprint sensors available today use the touch method: the finger is placed on the scanner, and the finger

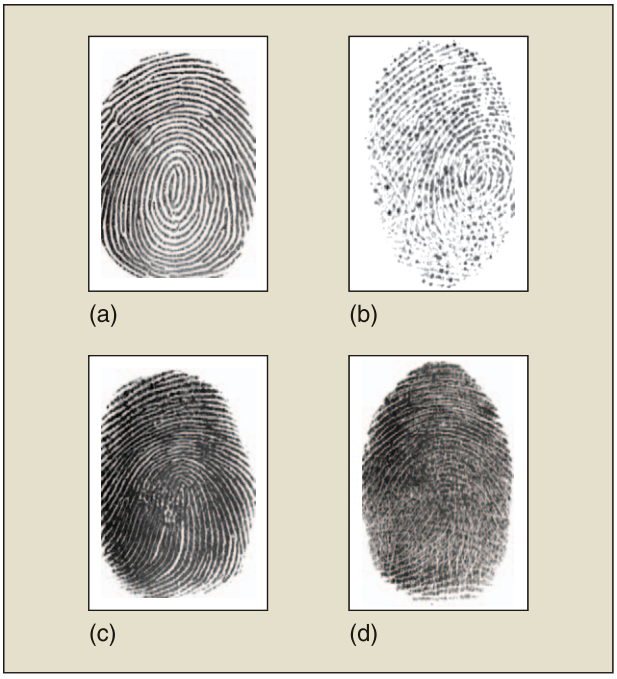

Fig. 4. Examples of fingerprint images acquired with an optical scanner. (a) A good quality fingerprint. (b) A fingerprint of a dry finger. (c) A fingerprint of a wet finger. (d) An intrinsically poor quality fingerprint. (© 2009 Springer, used with permission from [1].)

is not moved during the acquisition process. The main advantage of this method is its simplicity and small user effort. However, in mobile authentication applications (e.g., laptops and cell phones), where the cost and footprint of the sensor are critical, sweep sensors are used, which require the subject to move the finger over the sensor. Since the finger only moves vertically, the sensor needs to be only as wide as the finger, and the height of the sensor can be very small. A reconstruction algorithm forms the full fingerprint image from multiple slices formed as the finger moves as Fig. 3d shows.

Basic Parameters of Fingerprint Scanners

One of the main objectives of fingerprint sensing is to obtain a good quality image of the ridge pattern. However, it is not easy to precisely define the quality of a fingerprint image, because it is coupled with the sensor characteristic and the intrinsic finger surface condition. In fact, if the ridge prominence is very low (especially for workers engaged in heavy manual work), or if fingers are too moist or dry or if they are incorrectly presented to the sensor, most of the scanners produce poor quality fingerprint images irrespective of the quality of the sensor (see Fig. 4). Therefore, applications that require minimum image quality need to specify some range of values for the basic parameters of the fingerprint.

There are two major Standards, EFTS [6] and PIV [7], that define the basic parameters for fingerprint scanners (see Chapter 2 in [1]). The most critical and sensitive parameter is the acquisition area, followed by spatial resolution, geometrical accuracy, signal-to-noise ratio, and gray scale range.

Challenges in Fingerprint Scanner Design

While the EFTS and PIV sensor specifications assure a basic level of image quality output by the fingerprint sensors, they are not sufficient. There are a number of other challenges and tradeoffs facing fingerprint sensing technologies.

Dry finger: Dry fingers do not make good contact with the sensor surface. In optical sensors, manufacturers attempt to counter this problem by: heating the scanner surface to cause the fingers to sweat making them less dry, but this increases power consumption; by applying a silicone coating that improves the optical contact between the dry finger and the sensor, but this coating is not very durable; and by recommending the subjects to moisten their fingers by rubbing moisturizer on their hands.

Wet finger: optical FTIR as well as solid-state sensors produce "blobs" when a finger is too wet. Water fills the valleys, and the ridges and valleys merge together in the image to form blobs. Vendors recommend that the subjects wipe their fingers to get rid of the excess moisture. Some vendors use "water discriminating optics" in FTIR sensors based on the fact that skin has a higher refractive index than water. This design, together with using a wet cloth to moisten the finger, helps to address the dry finger problem as well.

Durability: optical sensors that have glass or plastic surfaces are reasonably durable, but any sensor that uses silicone membrane coating is not very durable. Solid state sensors also have surface durability problems – the silicon chip needs to be protected from chemical substances (e.g., sodium in perspiration) as well as physical scratches and wear and tear. A thick coating increases the distance between the pixels and the finger making it difficult to distinguish between a ridge and a valley.

Electro-static discharge (ESD): Solid state sensors are inherently more sensitive to ESD than optical sensors. The ESD problem is addressed through surface coating, grounding, and design that protect the critical components from ESD.

Motion blur: motion blur and smear can result if the finger is moving on the surface of an area sensor and the sensor has a slow frame rate. In swipe sensors, if the finger is swiped too quickly, the resulting image is blurred.

Whether a sensor works for all users in all operating conditions is called *generalization.* This is where the major differences show up in fingerprint sensors from various manufactures. The real challenge is whether the sensor works for dry, wet and dirty fingers with different skin colors and with varying skin conditions (e.g., cuts and abrasion). Further, the ergonomics and usability aspects are extremely important, often more important than the sensor parameters discussed above.

There are a number of other challenges and tradeoffs facing fingerprint sensing technologies.

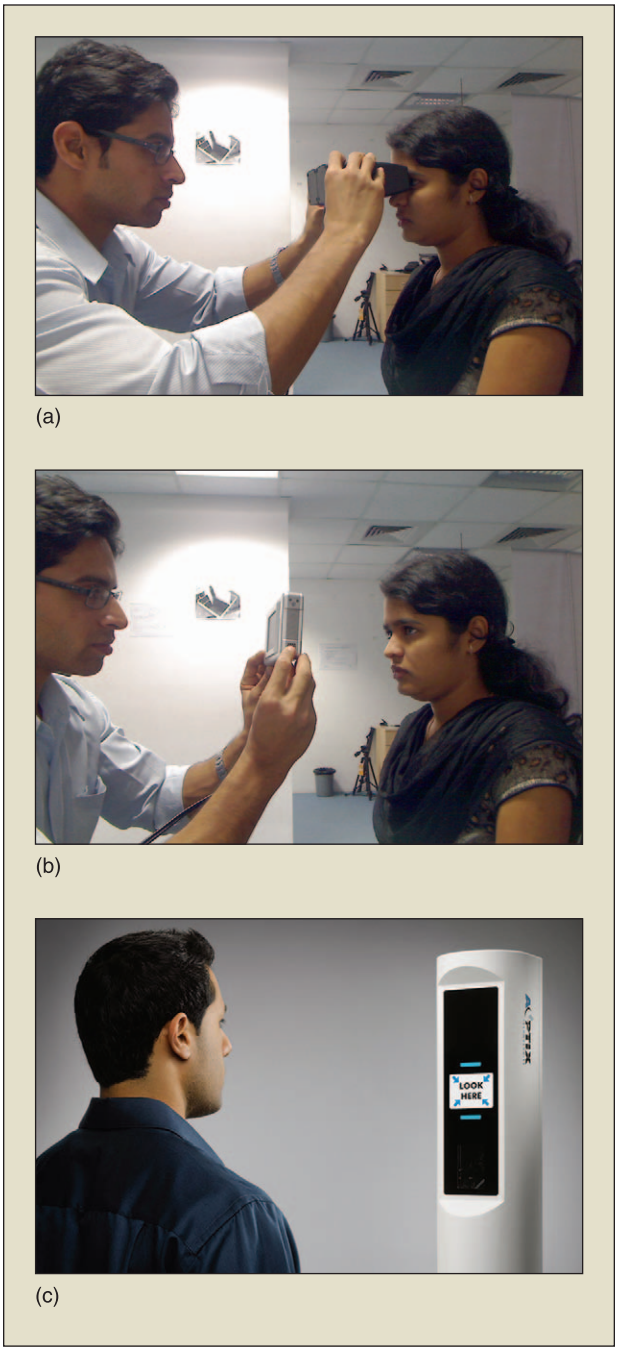

Fig. 5. Iris scanners for different distances. (a) Very close distance. (b) Medium distance. (c) Long distance. (Courtesy of AOptix Technologies [9].)

The Iris Biometrics

The iris is the annular region of the eye bounded by the pupil on the inside and the sclera (white of the eye) on the outside. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information and is useful for personal recognition. Each iris is distinctive, and even the irises of identical twins are different [8]. It is extremely difficult to surgically tamper with the texture of the iris, and it is possible to detect artificial irises (e.g., designer contact lenses). The iris texture has been shown to be stable and discriminative, and a large number of commercial iris recognition systems have demonstrated their value.

Iris recognition technology is not as mature as fingerprint technology, especially in image acquisition. An iris needs to be acquired at a high resolution and be imaged under near infra-red lighting, which is better than visible light in acquiring the texture of dark irises. Iris recognition devices are not as user friendly as fingerprint scanners and often require an attendant.

The iris cameras on the market can be divided into three types based on the standoff distance (see Fig. 5): very close, medium, and long distance cameras. The very close distance cameras are typically used with the assistance of an operator, although self-use is also possible. Medium distance cameras (typically used at a distance of 50-100 cm) are mounted on a wall or tripod and can be used by the subjects in unattended applications. However, they still require a lot of effort on the part of subjects in correctly aligning themselves in the field of view and at a specific distance from the camera. Long distance cameras (typically at up to 2 meters) are relatively new devices that have not yet been widely deployed. Some of these devices require the subject to be reasonably stationary while some can acquire an image even if the subject is moving. They are implemented as a portal or a lane and typically involve more than one camera within the acquisition system. One camera finds the face and eyes, and the other camera pan-tilt-zooms onto the eyes to acquire the iris.

Basic Parameters of Iris Scanners

The parameters of iris sensors are not as well understood as those of fingerprint sensors due to two factors: Iris sensor technology is less mature and the "signal" needed from the iris for recognition is not as well defined as the minutiae that are used in fingerprint scanners.

For consistency in capturing an iris image, the cameras must function within certain parameters. The main parameters of iris cameras and their minimum requirements are defined in the ISO/IEC 19794-6 Annex A (referred to as ISO below) [10]. The parameters are:

- *Illumination:* the wavelength of light used for illuminating the iris should be between 700 nm and 900 nm. The pigment in the iris is melanin and it absorbs much less light in near infra-red light than in the visible spectrum which makes the texture more defined in the image that is captured using near infrared illumination.
- *Contrast:* according to ISO, the iris image captured should have a minimum separation of 70 gray levels between iris and sclera and 50 gray levels between the iris and pupil.
- *Occlusion:* there should be no more than 30% occlusion (obstruction of the iris). At least 70% of iris area should be visible. Occlusion, which usually is from eyelids and depends on anatomy and gaze, is determined more by the acquisition process and less by the iris camera. However, the device should detect occlusion and provide instruction to the operator or the subject to correct it.

- *Ambient light and reflections must be avoided:* strong reflections from ambient light on the iris or on the camera can severely degrade the image quality. Often iris cameras use a visor or hood to block strong light. It is also helpful to use a narrow band-pass filter at the wavelength of the infra-red light source to block the ambient light.
- *Pupil size requirement:* a pupil dilates and contracts depending on the amount of ambient light. Excessive pupil dilation can degrade the quality of the acquired iris image. According to ISO, the pupil's size should be 7 mm or less. This can be achieved by adding a visible light source in addition to the infra-red light as brighter visible light will cause the pupil to contract and the iris to dilate.
- *Signal-to-noise (SNR) ratio:* The SNR ratio should be no less than 40 db. However, the test methodology to measure SNR is not clearly defined yet by the ISO.
- *Motion blur:* a significant contributor to the lack of image sharpness is motion blur. This can be mitigated by using imagers with global shutter and fairly high shutter speed. For example, assuming the camera is moving with respect to the iris at a speed of 10 cm/sec, the shutter speed should be no longer than 1 ms. This can be used in conjunction with synchronized pulse-mode illumination. Use of a visor that touches the forehead can reduce head movement and therefore reduce shutter speed requirement significantly.
- *Optical resolution:* according to ISO, to ensure high quality, iris diameter should be 200 pixels or more with pixel resolution of 16.7 pixels/mm and contrast ratio of at least 60% at 4 line pairs per mm. The pixel resolution and contrast transfer function are determined by the imager and the lens design. There is an inherent tradeoff between the optical resolution and the depth of field (DOF). In practice, this means that a fixed-focus camera needs to be positioned with respect to the eye within a tolerance of a few millimeters along the optical axis, which is fairly difficult to achieve. Some cameras capture multiple frames as the camera is moved towards the eye and select the frame with the best focus. Other cameras employ auto-focus, which is preferred but increases the camera cost. Contact lenses are transparent and do not cause any problem with imaging of the iris. However, there are some designer contact lenses on the market that have printed color texture on them – these will pose a problem.

Challenges in Iris Scanner Design

The biggest challenge is to optimize the cost and usability of an iris camera while meeting specifications on the basic parameters. To understand the usability and cost tradeoff, let us consider the medium-distance camera for illustrative purposes.

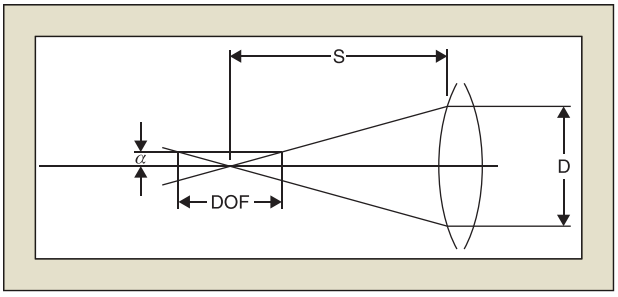

Fig. 6. Lens design for an iris scanner showing the depth-of-field.

One of the main factors affecting usability of iris cameras is the relationship between depth of field (DOF) and maximum achievable camera resolution. A small depth-of-field requires the subject to be precisely aligned with the camera. To understand this relationship, let us assume that the imaging optics are perfect and the system is only diffraction limited. Due to diffraction, the light is not collected from a single point but from an Airy disk (the central bright circular region of the pattern produced by light diffracted when passing through a small circular aperture) having a central spot with radius to first null $a = 1.22\lambda S/D$, where λ is the wavelength of the light, S is the distance from the object (iris) to the input pupil/lens of the imaging optics, and D is the diameter of the input pupil of the imaging optics.

The biggest challenge is to optimize the cost and usability of the iris camera while meeting specifications on the basic parameters.

It is straightforward to show that $DOF = 4aS/D$ (Fig 6). Substituting S/D from the Airy disk formula, $DOF = 4a^2/1.22\lambda = 3.4a^2/\lambda$. Hence, DOF does not depend on the parameters of the imaging optics and thus cannot be addressed by the lens design!

Even though the exact relationship between the resolution of the iris camera and the recognition accuracy is not well known, ISO considers iris image quality to be high if the annular diameter is over 200 pixels, low if it is between 100 and 149 pixels, and unacceptable if it is below 100 pixels. Assuming an annular diameter of 10 mm and assuming that the radius of the Airy disk should be comparable to the pixel size, we expect the spot radius, a, to be in the range from 0.05 mm to 0.1 mm. Assuming a wavelength of 860 nm, we can calculate the depth-of-field to be in the range from 10 mm (for borderline high quality) to 40 mm (worst acceptable). This means that a fixed focus iris camera should be positioned with respect to a subject's iris within ±5 mm from the optimal imaging position to obtain a high-quality iris image.

Due to the small depth-of-field, a subject then needs to move his head back and forth with respect to the camera to get his iris in focus (the so called "iris dance"), which is not only user-unfriendly but also increases the chance of motion blur. To avoid motion blur, the eye should not move by more than two pixels (0.1mm) during the capture. To get such a quick capture, an imager that has global shutter is required. Global

shutter means that all pixels in the image are integrated during the same period of time, and such imagers are more expensive as compared to most roller shutter CMOS imagers, where each line is integrated right before readout. Further, the imager frame rate should be high enough that a head moving at a reasonable practical speed will have a chance to be at the correct distance from the iris camera to capture a high-quality frame. A camera running at 30 frames per second (FPS) will work if the head is moving at a speed of 15 cm/sec or less. Assuming the same lateral speed, the shutter speed should be no longer than 1/1500 sec. While this can be achieved by using certain expensive imagers and by using illumination infrared LEDs in the high power output pulse mode, it illustrates the challenges in achieving a balance between usability and cost in iris camera design, especially when combined with other basic parameter requirements and the quality of imaging optics.

Summary and Future Directions

Fingerprint and iris recognition systems account for a substantial majority of deployed biometric systems. As such, system integrators are increasingly choosing fingerprint and iris scanners based on the requirements of the specific application. For example, forensic and civil applications are using optical slap-fingerprint scanners and dual-eye iris cameras which are compliant with the EFTS [6] or ISO [10] specifications. However, existing image quality specifications (IQS) from ISO and other standards bodies do not cover all the relevant aspects of a scanner (e.g., the ability of a scanner to acquire dry or wet fingers is not covered by any image quality specifications), so these standards are "necessary but not sufficient". Commercial applications (e.g., logical access control in laptops and mobile phones or physical access control in health-clubs) use biometric scanners that may not meet the standard IQS specifications. These scanners optimize other parameters such as cost, size, or usability. However, some of them sacrifice image fidelity and recognition accuracy in favor of small size and lower cost. We believe that the trend of using application-specific biometric scanners will continue. Designing biometric scanners is a challenge because humans come in all shapes and sizes, and their physiological factors are different due to hereditary, lifestyle, and environmental factors. Furthermore, the human factors (e.g., ergonomics, hygiene, perception of invasiveness, behavior, etc.) are extremely important in biometrics and bring an element of art into the science of biometric scanner design.

References

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd Edition, Springer, 2009.

[2] C. Wilson, A. R. Hicklin, M. Bone, H. Korves, P. Grother, B. Ulery, R. Micheals, M. Zoepfl, S. Otto, and C. Watson, "Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report," NIST, *Technical Report NISTIR 7123*, June 2004.

[3] P. J. Phillips and W. T. Scruggs, A. J. O´ Toole, P. J. Flynn, K. W. Bowyer, C. L. Schott, and M. Sharpe, "FRVT 2006 and ICE 2006 Large-Scale Results," NIST, *Technical Report NISTIR* 7408, March 2007.

[4] UID enrollment Proof-of-Concept report, [Online] Available: http://uidai.gov.in/images/FrontPageUpdates/uid_enrolment_poc_report.pdf.

[5] "Schematic of a multispectral imaging fingerprint biometric sensor," Lumidigm Inc., [Online] Available: http://www.lumidigm.com/multispectral-imaging/.

[6] "Electronic Fingerprint Transmission Specification (EFTS),"Version 9.1, Appendix F, 2010, [Online] Available: https://www.fbibiospecs.org/.

[7] "Personal Identity Verification (PIV) Image Quality Specifications for Single Finger Capture Devices," 2006, [Online] Available: https://www.fbibiospecs.org/.

[8] J. Daugman and C. Downing, "Epigenetic randomness, complexity, and singularity of human iris patterns" *Proc. of the Royal Society*, B, 268, Biological Sciences, pp. 1737 – 1740, 2001.

[9] "High Throughput Iris Recognition Biometrics. The Revolution in Air Transport Security.", (photo of Fig. 5c), AOptics Technologies, [Online] Available: http://www.aoptix.com/irisrecognition.

[10] ISO/IEC 19794-6:2005 Information technology – Biometric data interchange formats –Part 6: Iris image data, Annex A, 2005.

Salil Prabhakar (SalilP@digitalpersona.com) is an expert on biometrics and large scale national identity systems. He is the chief scientist and director of R&D at DigitalPersona Inc., California. He recently designed the biometric system for UIDAI in India as a volunteer. He has been an associate editor for four international journals including IEEE TPAMI; co-chaired several IEEE and SPIE conferences; is a senior member of IEEE and VP Finance for the IEEE Biometrics Council.

Alexander Ivanisov has an M.S. degree in optoelectronic instruments from Kyiv Engineering Technical Institute and is currently distinguished engineer at DigitalPersona Inc., California. He has a wide variety of skills and interests in design and development of hardware instruments as well as software systems.

Anil K. Jain is a University Distinguished Professor in the Department of Computer Science & Engineering at Michigan State University and an Adjunct Professor in the Department of Brain & Cognitive Engineering at Korea University. His research interests include pattern recognition, computer vision and biometric recognition. He is a Fellow of the ACM, IEEE, AAAS, IAPR and SPIE.