

## BIOMETRICS

FINGERPRINT  
MATCHING

Anil K. Jain, *Michigan State University*  
 Jianjiang Feng, *Tsinghua University, Beijing*  
 Karthik Nandakumar, *Institute for Infocomm Research*

Fingerprint matching has been successfully used by law enforcement for more than a century. The technology is now finding many other applications such as identity management and access control. The authors describe an automated fingerprint recognition system and identify key challenges and research opportunities in the field.

**T**he skin on our palms and soles exhibits a flow-like pattern of ridges and valleys. These papillary ridges on the finger, called *friction ridges*, help the hand to grasp objects by increasing friction and improving the tactile sensing of surface textures. The “Friction Ridge Patterns” sidebar describes the nature and origin of these characteristics.

Another important use of friction ridges is person identification. The pattern of friction ridges on each finger is unique and immutable, enabling its use as a mark of identity. In fact, even identical twins can be differentiated based on their fingerprints. Superficial injuries such as cuts and bruises on the finger surface alter the pattern in the damaged region only temporarily; the ridge structure reappears after the injury heals.

Henry Faulds, Francis Galton, and Edward Henry, among others, established the scientific basis for using fingerprints as a method for person identification in the late 19th century. Since then, law enforcement agencies worldwide have employed fingerprint recognition for two main purposes:

- establish the identity of a suspect (or victim) based on partial prints, or *latents*, left at a crime scene; and
- identify repeat offenders based on prints of all of their fingers (using 10 prints improves matching accuracy).

One of the world's largest fingerprint recognition systems is the Integrated Automated Fingerprint Identification System, maintained by the FBI in the US since 1999. The IAFIS currently contains fingerprints of more than 60 million persons, with corresponding demographic information, providing both latent-print search for crime scene investigation and 10-print ID for suspect identification and general-population background checks. In 2008, the FBI began updating the IAFIS to the Next Generation Identification (NGI) system, which will support other biometric traits such as palmprint, iris, and face.

Due to rising concerns about security and fraud, government<sup>1</sup> and commercial organizations have substantially increased their own deployment of fingerprint-based recognition systems in several nonforensic applications, including physical and logical access control, ATM transactions, border control, and consumer device access. The fingerprint is the dominant biometric trait in these applications compared to other common traits such as face, iris, and voice, and new emerging traits, including gait, ear, and palm-vein.<sup>2</sup>

The main reasons for the popularity of fingerprint recognition are

- its success in various applications in the forensic, government, and civilian domains;
- the fact that criminals often leave their fingerprints at crime scenes;
- the existence of large legacy databases; and
- the availability of compact and relatively inexpensive fingerprint readers.

A fingerprint recognition system can be used for both verification and identification. In *verification*, the system compares an input fingerprint to the “enrolled” fingerprint of a specific user to determine if they are from the same finger (1:1 match). In *identification*, the system compares an input fingerprint with the prints of all enrolled users in the database to determine if the person is already known under a duplicate or false identity (1:N match). Detecting *multiple enrollments*, in which the same person obtains multiple credentials such as a passport under different names, requires the *negative identification* functionality of fingerprints.

The US Department of Homeland Security's US-VISIT program ([www.dhs.gov/usvisit](http://www.dhs.gov/usvisit)) provides visa-issuing posts and ports of entry with fingerprint recognition technology that enables the federal government to establish and verify the identity of those visiting the US. This large-scale automated fingerprint recognition system has processed more than 100 million visitors to the US since 2004. The system identifies terrorists,

## ➔ FRICTION RIDGE PATTERNS

**V**olar skin—derived from *vola*, an ancient Roman term for the palm of the hand and the sole of the foot—is different from the skin covering other parts of the body. Continuously corrugated with narrow ridges, it contains no hairs or oil glands.<sup>1</sup> Volar skin is not unique to humans; all primates have this regular pattern of interweaving ridges and valleys on their palms and soles. Because friction ridges appear on the epidermis layer of the skin, they are also called epidermal ridges. In fact, the inner layer of the epidermis also has a ridge pattern similar to the surface layer.

Embryology research has shown that the process of friction ridge pattern formation is preceded by the formation of volar pads at about the sixth week of fetus development. Friction ridges appear in about the fourth month of gestation as a result of the stresses during growth of the fetus; the ridges are not elevated on the skin until about the 18th week. Minutiae are formed as ridges separate and create space for forming new ridges due to the growth of the finger surface.

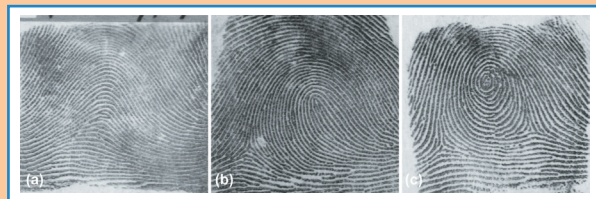


Figure A. Major fingerprint pattern types: (a) arch, (b) loop, and (c) whorl.

The overall pattern of the fingerprint is governed by the shape, size, and placement of volar pads.<sup>2</sup> Higher and symmetric volar pads tend to generate *whorls*, flatter and symmetric volar pads tend to generate *arches*, and asymmetric volar pads tend to generate *loops* as Figure A shows. Identification of the pattern type can facilitate faster search in large-scale fingerprint-recognition applications.

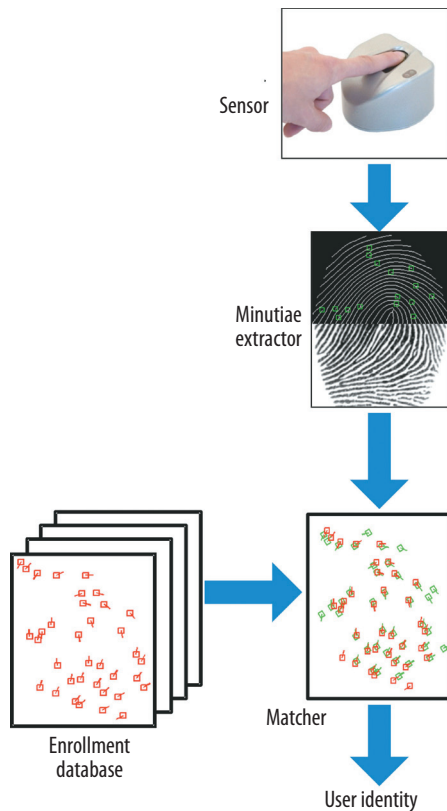
It is generally understood that friction ridge patterns are influenced not just by genetic factors but also by random physical stresses and tensions during fetal development. These random effects in the formation of fingerprints provide their uniqueness.

### References

1. H. Cummins and C. Midlo, *Finger Prints, Palms and Soles: An Introduction to Dermatoglyphics*, Dover, 1961.
2. M. Kücken and A.C. Newell, “Fingerprint Formation,” *J. Theoretical Biology*, vol. 235, no. 1, 2005, pp. 71-83.

criminals, and immigration violators by comparing a visa applicant's fingerprints with those in watch-list databases and also verifies that a visitor at a port of entry is the same person to whom the visa was issued.

The growing list of commercial and government applications for fingerprint recognition, coupled with the advent of compact and inexpensive sensors and powerful processors, have increased demand for fully automated, highly accurate, real-time systems. Developing these next-generation systems presents both challenges and opportunities.



**Figure 1.** A typical automated fingerprint recognition system. The system determines the user's identity by comparing the match score to a threshold.

### AUTOMATED FINGERPRINT RECOGNITION

Figure 1 outlines a typical automated fingerprint recognition system.

During the *enrollment phase*, the sensor scans the user's fingerprint and converts it into a digital image. The minutiae extractor processes the fingerprint image to identify specific details known as *minutia points* that are used to distinguish different users. Minutia points represent locations where friction

ridges end abruptly or where a ridge branches into two or more ridges. A typical good-quality fingerprint image contains about 20-70 minutiae points; the actual number depends on the size of the sensor surface and how the user places his or her finger on the sensor. The system stores the minutiae information—location and direction—along with the user's demographic information as a template in the enrollment database.

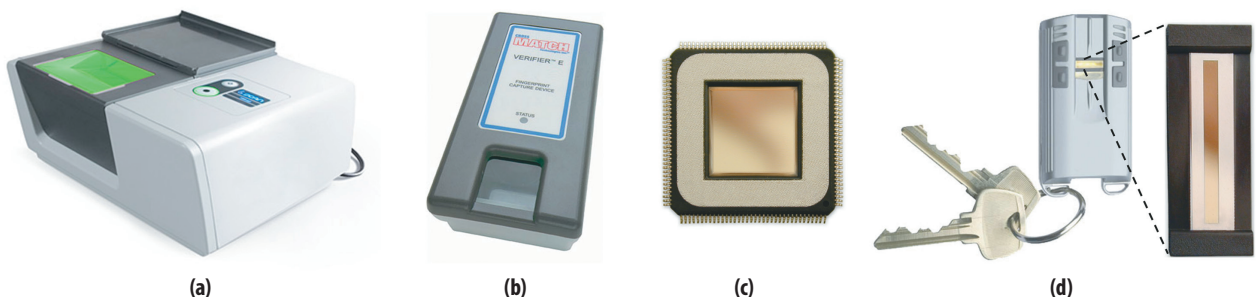
During the *identification phase*, the user touches the same sensor, generating a new fingerprint image called a *query print*. Minutia points are extracted from the query print, and the matcher module compares the query minutia set with the stored minutia templates in the enrollment database to find the number of common minutia points. Due to variations in finger placement and pressure applied on the sensor, the minutia points extracted from the template and query fingerprints must be aligned, or registered, before matching. After aligning the fingerprints, the matcher determines the number of pairs of matching minutiae—two minutia points that have similar location and directions. The system determines the user's identity by comparing the match score to a threshold set by the administrator.

### Sensing

Fingerprints can be sensed using numerous technologies.

The traditional “ink and paper” method, still used by many law enforcement agencies, involves applying ink to the finger surface, rolling the finger from one side of the nail to the other on a card, and finally scanning the card to generate a digital image.

In the more popular *live-scan* method, a digital image is directly obtained by placing the finger on the surface of a fingerprint reader as shown in Figure 2. Optical sensors based on the frustrated total internal reflection (FTIR) technique are commonly used to capture live-scan fingerprints in forensic and government applications, while solid-state touch and sweep sensors—silicon-based



**Figure 2.** Fingerprint readers: Cross Match ([www.crossmatch.com](http://www.crossmatch.com)) optical (a) 10-print and (b) single-print scanners; AuthenTec ([www.authentec.com](http://www.authentec.com)) solid-state (c) touch and (d) sweep sensors embedded in Privaris plusID ([www.privaris.com](http://www.privaris.com)) devices.

devices that measure the differences in physical properties such as capacitance or conductance of the friction ridges and valleys—dominate in commercial applications.

Latent fingerprint impressions left at crime scenes require manual “lifting” techniques like dusting.<sup>3</sup>

The most significant characteristics of fingerprint readers are their resolution and capture area. The standard fingerprint image resolution in law enforcement applications is 500 pixels per inch (ppi), but some readers now have dual-resolution capability (500 and 1,000 ppi). The sensing surface of readers used by law enforcement tends to be large so that they can capture palmprints and all four fingers simultaneously—such sensors are referred to as 10-print scanners.

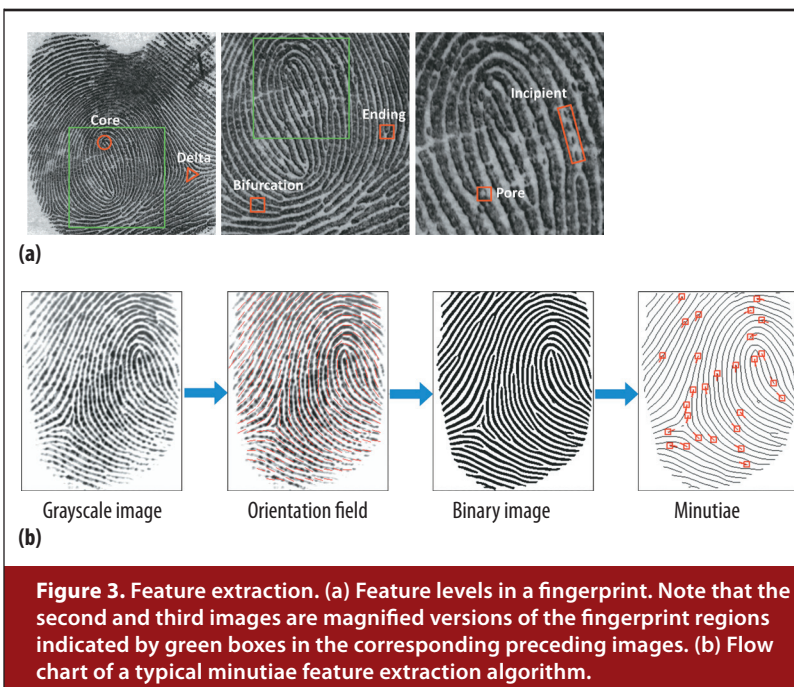
Low-resolution and small-area readers are preferred in commercial applications so that they can be easily embedded in consumer devices. Sweep sensors are popular in mobile phones, PDAs, and laptops because of their small size (for example, 14 mm × 5 mm) and low cost (under \$5). However, such sensors require users to sweep their finger across the sensing surface; the reader fuses overlapping image slices obtained during sweeping to form a full fingerprint. Fingerprint sensors embedded in mobile phones or PDAs are also used to support navigation and hot-key functions, with each finger assigned to a specific functionality.

## Feature extraction

Features extracted from a fingerprint image are generally categorized into three levels, as shown in Figure 3a. Level 1 features capture macrodetails such as friction ridge flow, pattern type, and singular points. Level 2 features refer to minutiae such as ridge bifurcations and endings. Level 3 features include all dimensional attributes of the ridge such as ridge path deviation, width, shape, pores, edge contour, and other details, including incipient ridges, creases, and scars.

Level 1 features can be used to categorize fingerprints into major pattern types such as arch, loop, or whorl; level 2 and level 3 features can be used to establish a fingerprint’s individuality or uniqueness. Higher-level features can usually be extracted only if the fingerprint image resolution is high. For example, level 3 feature extraction requires images with more than 500-ppi resolution.

Figure 3b shows the flow chart of a typical minutiae feature extraction algorithm. First, the algorithm estimates the friction ridge orientation and frequency from the image.



**Figure 3. Feature extraction. (a) Feature levels in a fingerprint. Note that the second and third images are magnified versions of the fingerprint regions indicated by green boxes in the corresponding preceding images. (b) Flow chart of a typical minutiae feature extraction algorithm.**

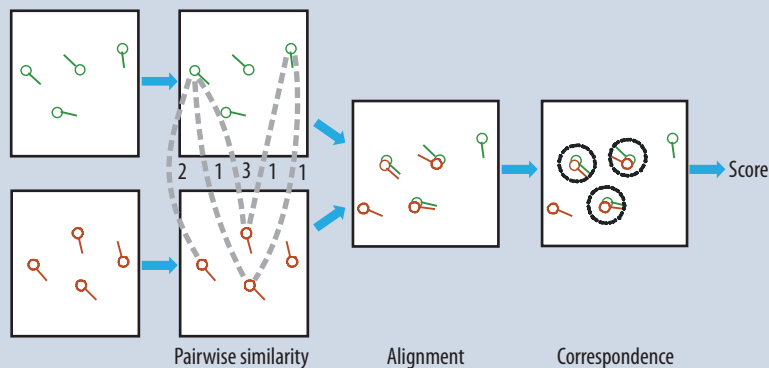
Based on these values, it then performs contextual filtering to improve the image quality and facilitate ridge extraction. The algorithm then obtains binary ridge skeletons from the enhanced image by tracing the ridge lines. Ridge endings and bifurcation points are obtained from the ridge skeleton and referred to as minutiae. The algorithm employs some heuristic rules to detect and remove spurious minutiae resulting from an imperfect skeleton image.

## Matching

A fingerprint matching module computes a match score between two fingerprints, which should be high for fingerprints from the same finger and low for those from different fingers. Fingerprint matching is a difficult pattern-recognition problem due to large intraclass variations (variations in fingerprint images of the same finger) and large interclass similarity (similarity between fingerprint images from different fingers). Intraclass variations are caused by finger pressure and placement—rotation, translation, and contact area—with respect to the sensor and condition of the finger such as skin dryness and cuts. Meanwhile, interclass similarity can be large because there are only three types of major fingerprint patterns (arch, loop, and whorl).

Most fingerprint-matching algorithms adopt one of four approaches: image correlation, phase matching, skeleton matching, and minutiae matching. Minutiae-based representation is commonly used, primarily because

- forensic examiners have successfully relied on minutiae to match fingerprints for more than a century,
- minutiae-based representation is storage efficient, and



**Figure 4.** Typical minutiae-matching algorithm. The algorithm first uses local minutiae descriptors to coarsely align two fingerprints and then computes a global match score based on minutiae correspondences.

**Table 1.** Sample accuracy results from three fingerprint technology evaluations.

Evaluation	Data	Best reported accuracy
NIST FpVTE 2003 (MST)	10,000 plain fingerprints	FNMR = 0.6% at FMR = 0.1%
FVC2006	140 fingers × 12 images Electric field sensor (250 ppi) Optical sensor (569 ppi) Sweep sensor (500 ppi)	FNMR = 15% at FMR = 0.1% FNMR = 0.02% at FMR = 0.1% FNMR = 3% at FMR = 0.1%
NIST ELFT 2008 (Phase II)	835 latent prints, 100,000 rolled fingerprints	FNIR = 8% at FPIR = 1%

- expert testimony about suspect identity based on mated minutiae is admissible in courts of law.

The current trend in minutiae matching is to use local minutiae structures to quickly find a coarse alignment between two fingerprints and then consolidate the local matching results at a global level. This kind of matching algorithm<sup>4</sup> typically consists of four steps, as Figure 4 shows. First, the algorithm computes pairwise similarity between minutiae of two fingerprints by comparing minutiae *descriptors* that are invariant to rotation and translation. Next, it aligns two fingerprints according to the most similar minutiae pair. The algorithm then establishes minutiae correspondence—minutiae that are close enough both in location and direction are deemed to be corresponding (mated) minutiae. Finally, the algorithm computes a similarity score to reflect the degree of match between two fingerprints based on factors such as the number of matching minutiae, the percentage of matching minutiae in the overlapping area of two fingerprints, and the consistency of ridge count between matching minutiae.

### Performance

A fingerprint matcher can make two types of errors: a *false match*, in which the matcher declares a match between images from two different fingers, and a *false nonmatch*, in which it does not identify images from the

same finger as a match. A system's false match rate (FMR) and false nonmatch rate (FNMR) depend on the operating threshold; a large threshold score leads to a small FMR at the expense of a high FNMR. For a given fingerprint matching system, it is impossible to reduce both these errors simultaneously.

Fingerprint identification system performance is measured in terms of its *false positive identification rate* (FPIR) and *false negative identification rate* (FNIR). A false positive identification occurs when the system finds a hit for a query fingerprint that is not enrolled in the system. A false negative identification occurs when it finds no hit or a wrong hit for a query fingerprint enrolled in the system. The relationship between these rates is defined by  $FPIR = 1 - (1 - FMR)^N$ , where  $N$  is the number of users enrolled in the system. Hence, as the number of enrolled users grows, the fingerprint matcher's FMR needs to be extremely low for the identification system to be

effective. For example, if an FPIR of 1 percent is required in a fingerprint identification system with 100 million enrolled users, the FMR of the corresponding fingerprint matcher must be on the order of 1 in 10 billion. Such a stringent FMR requirement can usually be met only when fingerprints from all 10 fingers of a person are used for identification. This explains the need to continuously decrease the error rates of fingerprint matchers employed in large-scale identification systems.

The National Institute of Standards and Technology (NIST) has conducted several fingerprint technology evaluations (<http://fingerprint.nist.gov>), such as the Fingerprint Vendor Technology Evaluation (FpVTE), the Minutiae Interoperability Exchange Test (MINEX), Proprietary Fingerprint Template (PFT) testing, and the Evaluation of Latent Fingerprint Technologies (ELFT), which use operational data collected in forensic and government applications. The University of Bologna conducts FVC-onGoing (<https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx>), which is an evolution of the international Fingerprint Verification Competitions (FVCs) organized between 2000 and 2006.

Table 1 summarizes FpVTE 2003 Medium-Scale Test (MST), FVC2006, and ELFT 2008 (Phase II) results. Clearly, system performance varies widely depending on fingerprint data characteristics used in the evaluation. However, while these evaluations are useful, the performance of

different biometric systems cannot always be directly compared. In addition, technology evaluations do not always reflect operational performance due to differences in data characteristics, operating environments, and user interactions with the fingerprint reader.

A fingerprint recognition system's operational performance is based on several factors, including sensor characteristics, the number and demographic distribution of the population enrolled in the system, and various environmental factors—indoor versus outdoor, temperature, humidity, and so on. Moreover, the required FMR and FNMR depend on the specific application—for example, Disney World's fingerprint-based entry system operates at a low FNMR, so as not to upset paying customers, at the expense of a higher FMR. On the other hand, an ATM fingerprint verification system may require low FMR at the expense of higher FNMR.

In some cases, a fingerprint recognition system may not even successfully capture the user's fingerprint. *Failure to enroll* (FTE) and *failure to acquire* (FTA) refer to the fraction of users who cannot be enrolled or processed by a particular system due to the poor quality of their fingerprints—for example, people such as manual laborers or the elderly with “worn-out” fingers. In practice, FTE can be rather high (a few percentage points) depending on the target population and the occupation of users in the population.

## OPEN RESEARCH OPPORTUNITIES

Numerous challenging problems in fingerprint recognition are yet to be solved. The ever-increasing demand for reducing the error and failure rates of automated fingerprint recognition systems and the need for enhancing their security have opened many interesting research opportunities that encompass multiple domains such as image processing, computer vision, statistical modeling, cryptography, and sensor development.

### New sensors

The physical shape of fingers makes it difficult to capture a complete fingerprint pattern using touch-based sensors. In law enforcement applications, multiple impressions of the same finger are often recorded to obtain good-quality complete images of all the fingers. As most touch-based sensors are based on directly measuring the finger surface, they have difficulty sensing the fingerprints of elderly persons, whose fingerprints tend to be flattened, and manual laborers, whose fingerprints may contain many cuts. Rolling and improper pressure while using touch-based sensors also introduce distortion in the sensed images.

New sensor technologies are being developed to overcome these drawbacks. For instance, Lumidigm ([www.lumidigm.com](http://www.lumidigm.com)) has developed readers that use multispec-

tral technology to scan a fingerprint pattern directly from just below the skin's surface; this technique may provide better-quality fingerprints from dry, wet, or dirty fingers. Researchers at TBS ([www.tbsinc.com](http://www.tbsinc.com)) are investigating touchless 2D and 3D fingerprint imaging, which could obtain complete fingerprint information without the distortion introduced by rolling and other pressure variations.

However, more work is still needed to improve the quality of acquired images of difficult fingers with as little imaging constraint as possible. Even touchless fingerprint imaging requires users to place their finger(s) within close proximity of the sensor. Existing touchless sensors cannot be used in surveillance applications. The feasibility of acquiring fingerprints from a distance is still an open question, and any solution is likely to revolutionize the field and lead to numerous new applications for fingerprints.



**The actual problem of estimating the error rate of latent fingerprint identification is not yet solved.**

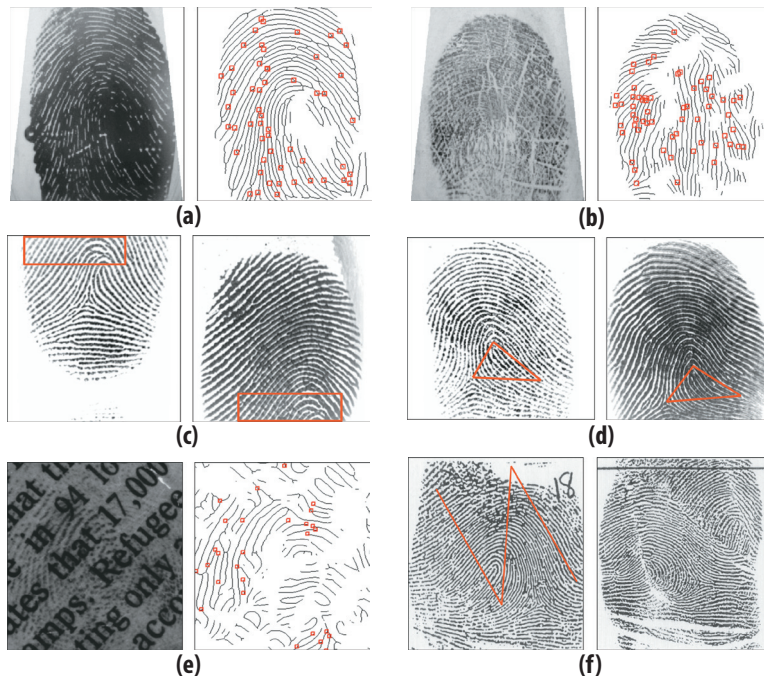
### Low-quality images

Due to nonideal skin conditions, inherently low-quality fingers, and sensor noise, a significant percentage of fingerprint images are of poor quality. Extracting features from and matching low-quality fingerprints, like those shown in Figures 5a and 5b, is a challenging problem that will require significant research.

In many government and forensic applications, human experts are available to encode low-quality fingerprints and verify associated hits found by the automated fingerprint recognition systems. In situations where human intervention is expensive or inconvenient, or fingerprints are unusable, a possible solution is *multibiometrics*<sup>5</sup>—the fusion of multiple biometric traits such as fingerprint, palmprint, face, iris, and voice. However, the seamless integration of different biometric traits remains a difficult research problem both at the acquisition stage (how to acquire the multiple traits simultaneously) and processing stage (how to combine the information from multiple traits effectively).

### Small overlapping area and nonlinear distortion

Fingerprint sensors embedded in consumer electronic devices tend to have a smaller sensing area. This factor, combined with users' improper placement of their finger on the sensor, results in a limited overlapping area between two impressions of the same finger, as Figure 5c shows. Given the very small number of minutiae in the overlapping area, it is difficult to determine if two fingerprints are from the same finger.



**Figure 5.** Challenges in automated fingerprint processing: (a) wet fingerprint (left) and extracted features (right); (b) fingerprint with many cuts (left) and extracted features (right); (c) small overlapping area as marked by rectangles; (d) large nonlinear distortion in fingerprint patterns as indicated by the corresponding triangles; (e) latent fingerprint with overlapping letters (left) and the extracted features (right); (f) altered fingerprint: a criminal made a Z-shaped incision into each of his fingers (left), switched two triangles, and stitched them back into the finger (right).

One way to alleviate this problem is to utilize level 3 features to improve the matching accuracy in cases where there is only a small overlapping area between the two impressions. However, level 3 features may not be suitable for commercial applications because the sensors used in such applications usually provide only low-resolution images. A more feasible solution may be *fingerprint mosaicking*, which combines multiple smaller images into a larger image, and more ergonomic and intuitive interfaces that can guide users to properly place the central (pattern) area of their finger on the sensor.

Pressing soft finger skin on a sensor always introduces some distortion, which is generally not repeatable. Matched fingerprints may appear very different under severe distortion, as Figure 5d shows. Ergonomic sensors and appropriate feedback to users can alleviate this problem. Another option is to match fingerprints locally—for example, using local minutiae descriptors<sup>4</sup>—before aggregating these local matches globally.

### Latent fingerprints

Latent fingerprints generally suffer from low image quality, small overlapping area, and nonlinear distortion as well as the presence of a complex background, as Figure 5e shows. To overcome this challenging problem, current automated fingerprint ID systems require extensive manual intervention in latent encoding (feature extraction) and in verifying a candidate list returned by the system.

With the increase in latent matching transactions for civilian, law enforcement, and homeland security applications, automated latent processing and matching are receiving more attention.

Latent fingerprint evidence was accepted as infallibly accurate in US courts of law for almost a century. In recent years, however, it has been repeatedly challenged under the *Daubert* standard, a rule of evidence regarding the admissibility of scientific testimony largely derived from a 1993 Supreme Court case (<http://cfr.law.cornell.edu/supct/html/92-102.ZS.html>). The *Daubert* standard has two basic requirements for expert opinions: The underlying scientific basis should be accepted widely, and the error rate should be known.

Match/nonmatch decisions are made subjectively by human experts whose error rates are difficult to estimate and can vary significantly from person to person. Although many researchers have attempted to estimate the inherent individuality of fingerprints,<sup>6</sup> the actual problem of estimating the error rate of latent fingerprint identification,<sup>7</sup> which involves human factors in many stages—latent development, encoding, matching—is not yet solved. The only viable solution in the near term may be to keep improving automated fingerprint systems' performance and ultimately replace human experts with automated systems.

### Altered/fake fingerprints

People may alter their fingerprints in different ways for many reasons. For example, an unauthorized user may use a fake finger that imitates a legitimate user's fingerprint template to access a computer system. Criminals may cover their fingers with fake fingerprints made of substances like glue or they may intentionally mutilate their fingers to avoid being identified by automated systems or even human experts, as Figure 5f shows.

An essential countermeasure to thwart the use of inanimate or fake fingers is *liveness detection*—checking if the finger is “live” by measuring and analyzing various vital signs of the finger such as pulse, perspiration, and deformation. While software-based liveness detection solutions that complement existing fingerprint scanners

may be more cost-effective, they have not yet shown much promise.

To deal with mutilated fingers, a mutilation detector should be added, and, once mutilation is detected, effort should be made to identify the subject either by restoring the original fingerprints or using only the unaltered areas of the fingerprint. With the adoption of multiple biometric traits in large-scale identification systems such as the FBI's NGI, multibiometrics will be a powerful tool to handle altered fingerprints.

### Interoperability

Interoperability problems can occur in all three main modules of a fingerprint recognition system: sensor, feature extractor, and matcher. Different sensors may output images that exhibit variations in resolution, size, distortion, contrast, background noise, and so on. Different encoders may extract different features or adopt varying definitions of the same feature. This diversity makes it difficult to build a fingerprint system with principal components sourced from different vendors.

To improve interoperability among multiple fingerprint systems, international standardization organizations have established standards for sensors, templates, and system testing—for example, image quality specifications for fingerprint sensors and data exchange formats for minutiae templates.<sup>8</sup> However, the superiority in matching accuracy of proprietary templates compared to standard templates in NIST MINEX testing shows that existing standards must be improved by, for example, including extended features.

Fingerprint matchers pose a less-noticeable interoperability challenge. Different matchers can have different score distributions, which may pose a problem during the fusion of multiple algorithms or multiple biometrics. Limited work has been done in standardizing the output of matchers.

### System on device

An important security issue in fingerprint recognition systems is the tampering or modification of the hardware/software components and interception of fingerprint data passing through the communication channels—for example, the wireless interface between a passport reader and the chip on a passport that contains the user's fingerprint template. This problem can be overcome by employing system-on-device technology in which the sensor, feature extractor, matcher, and even the templates reside on a tamper-resistant device such as the Privaris plusID product shown in Figure 2d. The advantage of this technology is that the information about a user's fingerprint never leaves the device; it is only the matching result that is securely transmitted. Moreover, well-known cryptographic tools can be leveraged to prevent interception and alteration of fingerprint information.



**Figure 6. Cancellable fingerprint.** Applying a noninvertible mathematical transformation to the fingerprint template on the left produces the template on the right. Even if the transformed template is revealed, the real fingerprint cannot be gleaned easily.

### Template security

While system-on-device technology may be a useful security measure in verification applications, fingerprint ID systems require centralized storage of fingerprint information in large enrollment databases. The unauthorized use or disclosure of fingerprint template information from such databases constitutes a serious security and privacy threat. Not only can a stolen fingerprint template be reverse-engineered to construct a fake finger<sup>9</sup> or replayed into the system, it can be used for cross-matching across different databases to covertly track people without their consent, thereby compromising their privacy.

Another issue is that unlike credentials such as passwords or ID cards that can be easily revoked and reissued, people cannot arbitrarily replace their fingerprint template—disclosure of fingerprint information results in permanent loss. Merely encrypting the fingerprint is insufficient because the template remains secure only as long as the decryption key is held secretly. Most of the reported attacks on biometric passports issued in European countries have tried to exploit this vulnerability by intelligently sniffing the decryption key.

Two strategies have been proposed to secure fingerprint templates. One is to apply a noninvertible mathematical transformation to the fingerprint template and store only the transformed template. In this way, even if the transformed template is revealed, the real fingerprint cannot be gleaned easily. Since the same fingerprint can be used to generate a new template using a different transformation, it is referred to as a *cancellable fingerprint*, as Figure 6 shows. Another promising solution is to use *biometric cryptosystems* and generate cryptographic keys based on biometric samples.

The problem with both approaches is that there is some loss of information during the transformation/key generation process that adversely affects the fingerprint

recognition system's accuracy. However, researchers are exploring ways to minimize this degradation in accuracy without compromising template security.

**A**utomated fingerprint identification systems have been successfully deployed around the globe for both law-enforcement and civilian applications, and new fingerprint-matching applications continue to emerge. The fingerprint will continue to be the dominant biometric trait, and many identity management and access control applications will continue to rely on fingerprint recognition because of its proven performance, the existence of large legacy databases, and the availability of compact and cheap fingerprint readers. Further, fingerprint evidence is acceptable in courts of law to convict criminals.

While fingerprint recognition technology has been under development for nearly half a century, new research problems have accompanied the wide deployment of fingerprint technology. These include extraction of level 3 features, liveness detection, and automated latent fingerprint identification. Issues such as fingerprint recognition at a distance, real-time identification in large-scale applications with billions of fingerprint records, developing secure and revocable fingerprint templates that preserve accuracy, and scientifically establishing the uniqueness of fingerprints will likely remain as grand challenges in the near future.

Although fingerprint recognition is one of the earliest applications of pattern recognition, the accuracy of state-of-the-art fingerprint-matching systems is still not comparable to human fingerprint experts in many situations, particularly latent print matching. Significant advances require not only a deeper understanding of friction ridge formation, but also adaptation of new developments in sensor technology, image processing, pattern recognition, machine learning, cryptography, and statistical modeling. While successful commercial applications have driven fingerprint-matching technology, more breakthroughs could be achieved with greater investment in fundamental research.<sup>10</sup> Active collaboration among academic and industrial research groups will also stimulate rapid progress in fingerprint matching. ■

## References

1. National Science and Technology Council Subcommittee on Biometrics and Identity Management, *Biometrics in Government Post-9/11: Advancing Science, Enhancing Operations*, Aug. 2008; [www.ostp.gov/galleries/NSTC%20Reports/Biometrics%20in%20Government%20Post%209-11.pdf](http://www.ostp.gov/galleries/NSTC%20Reports/Biometrics%20in%20Government%20Post%209-11.pdf).
2. A.K. Jain, P. Flynn, and A.A. Ross, eds., *Handbook of Biometrics*, Springer, 2007.
3. H.C. Lee and R.E. Gaensslen, eds., *Advances in Fingerprint Technology*, 2nd ed., CRC Press, 2001.
4. J. Feng, "Combining Minutiae Descriptors for Fingerprint Matching," *Pattern Recognition*, Jan. 2008, pp. 342-352.
5. A.A. Ross, K. Nandakumar, and A.K. Jain, *Handbook of Multibiometrics*, Springer, 2006.
6. S. Pankanti, S. Prabhakar, and A.K. Jain, "On the Individuality of Fingerprints," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Aug. 2002, pp. 1010-1025.
7. D.R. Ashbaugh, *Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology*, CRC Press, 1999.
8. D. Maltoni et al., *Handbook of Fingerprint Recognition*, 2nd ed., Springer, 2009.
9. R. Cappelli et al., "Fingerprint Image Reconstruction from Standard Templates," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Sept. 2007, pp. 1489-1503.
10. National Research Council of the National Academies, *Strengthening Forensic Science in the United States: A Path Forward*, National Academies Press, 2009.

**Anil K. Jain** is a University Distinguished Professor in the Department of Computer Science and Engineering and the Department of Electrical and Computer Engineering at Michigan State University. He is also affiliated with the WCU project in the Department of Brain and Cognitive Engineering at Korea University, Seoul, South Korea. His research interests include pattern recognition, computer vision, and biometric recognition. Jain received a PhD in electrical engineering from the Ohio State University. He is a Fellow of the ACM, the IEEE, the American Association for the Advancement of Science, the International Association of Pattern Recognition (IAPR), and SPIE. Contact him at [jain@cse.msu.edu](mailto:jain@cse.msu.edu).

**Jianjiang Feng** is an assistant professor in the Department of Automation at Tsinghua University, Beijing. His research interests include image processing, pattern recognition, and biometric recognition. Feng received a PhD in communication engineering from Beijing University of Posts & Telecommunications. Contact him at [jfeng@tsinghua.edu.cn](mailto:jfeng@tsinghua.edu.cn).

**Karthik Nandakumar** is a research fellow at the Institute for Infocomm Research, A\*STAR, Singapore. His research interests include statistical pattern recognition, computer vision, image processing, and biometric recognition. Nandakumar received a PhD in computer science and engineering from Michigan State University. He is a member of the IEEE, the IEEE Computer Society, and IAPR. Contact him at [knandakumar@i2r.a-star.edu.sg](mailto:knandakumar@i2r.a-star.edu.sg).



Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.