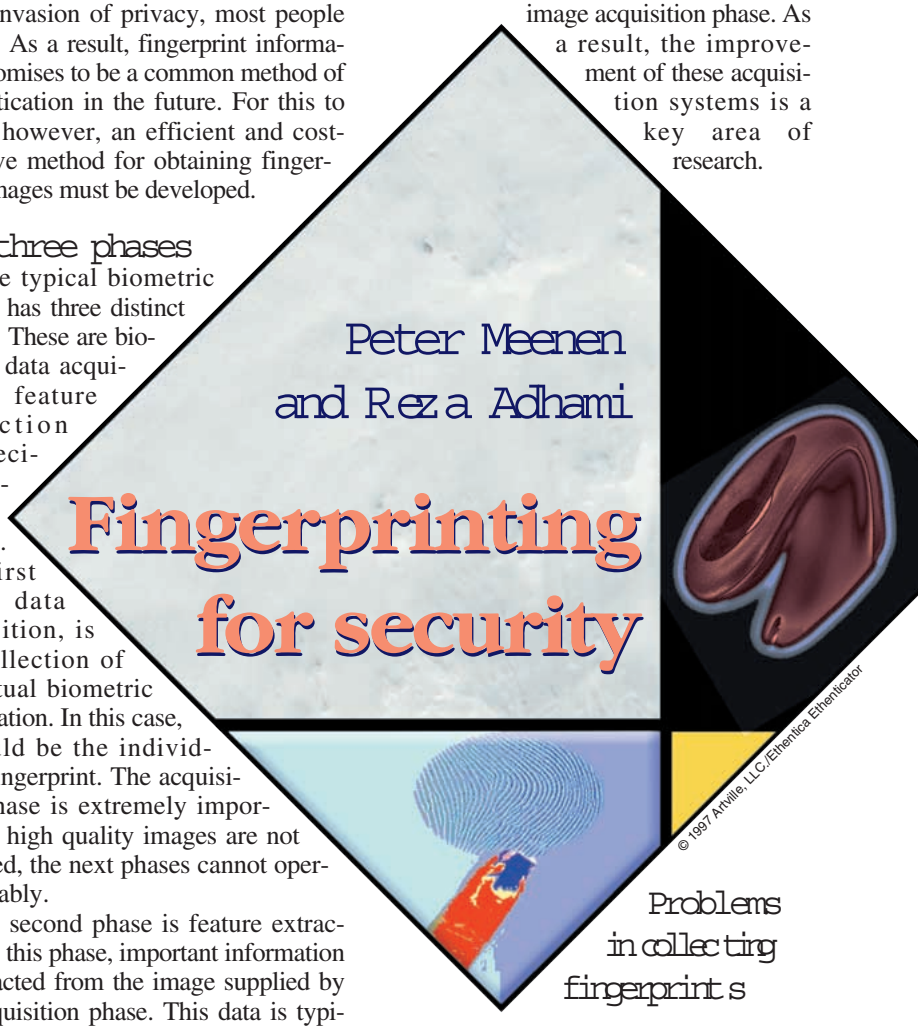
Fingerprinting for security

Peter Meenen and Reza Adhami



The convenience of current electronic applications has led to an explosive increase in their use. E-banking, electronic fund transfer, online shopping and virtual auctions are just some applications prevalently used by the public. Trust, as a result, has become more of an issue.

As expected, there is an element of security when performing transactions in person. When using electronic services, however, this element is removed. In an electronic environment, it is easy for a person to pose as someone else. As a result, the verification of an individual's identity is vitally important. No one wants automatic teller machines (ATMs) or credit card companies to authorize fraudulent transactions made by someone else. To try to prevent illegal transactions, electronic security methods are employed.

Most methods rely on one of two basic security methodologies: token-based security and secret-based security. Token-based security relies on the user's possession of a special item or token. Often, this token is an access or ID card such as a credit card or security access badge. Secret-based security, on the other hand, relies on an individual's secret ID number like a computer password or a PIN number that only that person would know. This information is then supplied to verify his or her identity.

Both methodologies have one major flaw. Neither can accurately determine if the individual that possesses a token or knows some secret information is actually the individual it represents. Tokens can be stolen, and secret information can be guessed or fraudulently obtained. Once a person has the token or secret password, it is easy to pose as the original owner.

A third security methodology that seeks to solve the problem of positive identification is biometrics. Biometrics is the practice of using people's physical or behavioral traits to confirm their identities. People have been using biometrics for a long time without even realizing it. Most people identify others based upon physical traits such as their body shapes, facial features or voices. This is the same principle behind modern biometric identification. Physical traits such as facial structure, retina pattern, hand geometry, iris pattern and fingerprints are all used by biometric systems to try to verify an individual's identity.

One trait of particular interest, since it is easily collected and universal is fingerprints. The law enforcement community has been using fingerprint identification for many years. Although a segment of the public views fingerprinting as an invasion of privacy, most people do not. As a result, fingerprint information promises to be a common method of authentication in the future. For this to occur, however, an efficient and cost-effective method for obtaining fingerprint images must be developed.

The three phases

The typical biometric system has three distinct phases. These are biometric data acquisition, feature extraction and decision-making. The first step, data acquisition, is the collection of the actual biometric information. In this case, it would be the individual's fingerprint. The acquisition phase is extremely important. If high quality images are not obtained, the next phases cannot operate reliably.

The second phase is feature extraction. In this phase, important information is extracted from the image supplied by the acquisition phase. This data is typically a pattern of features or landmarks that allows a given individual to be uniquely identified. For fingerprint recognition, these features are typically minutia points such as ridge endings (the termination points of fingerprint friction ridges) and ridge bifurcations. (The points where a ridge splits to form a Y shape.) Figure 1 shows examples of ridge endings and bifurcations. The coordinate pattern of these features is unique to a given individual; thus, it can serve as his or her identification.

The final phase of a biometric system is the decision-making phase. In this phase, the feature pattern that was extracted from the image is compared to a previously known example. A decision is then made regarding the identity of the individual. If the patterns are close enough, the individual's identity is verified; otherwise, the claimed identity is rejected.

So if an accurate image is not obtained in the first phase, the rest of the process will be inaccurate. In fact, most difficulties in accurately identifying an individual can be traced back to the image acquisition phase. As a result, the improvement of these acquisition systems is a key area of research.

Problems in collecting fingerprints

There are five major problems in current fingerprint acquisition technology. The first challenge is inconsistent contact. Most fingerprint collection systems require that the finger come into contact with a surface. This is often a glass platen or another kind of sensing plate.

By placing the finger on a surface, the three dimensional finger is being mapped onto a two dimensional plane. As a result distortions occur. The skin on the finger will stretch when pressed against the surface. This stretching causes slight changes in the distances between features on the fingerprint. In most cases, different levels of pressure will be used each time the individual's finger is scanned. This results in slightly different images as well.

The second challenge is non-uniform

 0278-6648/01/$10.00 © 2001 IEEE

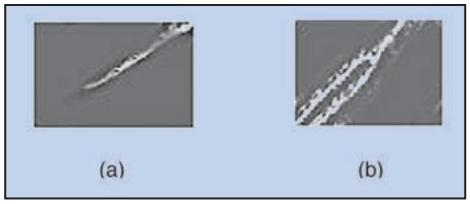


Fig. 1 An example of a) a ridge ending and b) a ridge bifurcation

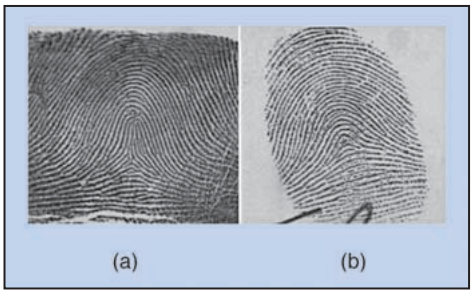


Fig. 2 Examples of inked fingerprints. a) illustrates the "rolling" technique, while b) illustrates the "dabbing" technique. Both images are taken from the NIST 4 database.

contact. The non-uniform contact occurs due to minor inconsistencies in the surface of the finger. For a fingerprint-scanning device to capture the whole fingerprint, it is necessary for the whole print to be in contact with the scanning surface. But ridges worn down or dry in comparison to surrounding ridges will often not come in contact with the scanning surface. Other factors that can interfere include sweat, dirt, grease and skin disease.

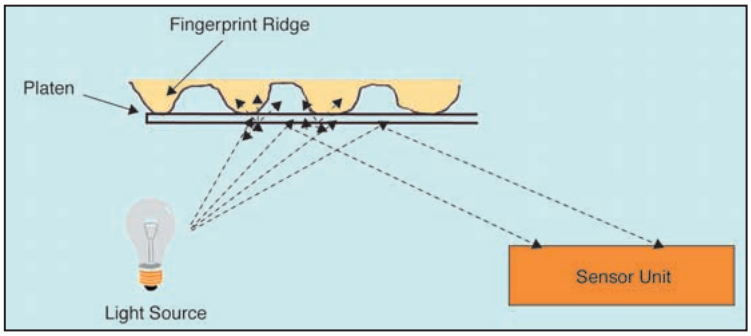


Fig. 3 An illustration of frustrated total internal reflection. Incident light is scattered by the glass/ridge intersections while it is reflected by the glass/air boundaries in the valley regions.

Irreproducible contact is another major problem for fingerprint acquisition systems. Irreproducible contact occurs when the captured image changes from session to session. For example, an individual could have their fingerprint altered through accidental injury. Cuts, scratches, scars and ridges that are worn down all contribute to changes in a fingerprint image. These changes cause problems for the recognition algorithms.

When dealing with electronic sensors and scanners, in many cases different parts of the fingerprint are imaged during each session. Most scanners are not large enough to capture the entire surface of the finger. As a result, only a piece of the total fingerprint is captured. By imaging different portions of the finger each time, additional minutia features are inserted and some previously measured features are removed. This change from session to session is an additional problem for identification algorithms.

Another challenge is noise. Noise can be introduced into the system through the acquisition process. This noise can be caused by electromagnetic radiation, excessive ambient light, or imperfections in the scanning equipment. Another type of noise that can be introduced is residual noise. This is noise that enters that image due to residual portions of previous prints. For example, an impression of the previous fingerprint is often left behind on the scanner surface. The impression, usually an oily residue, can interfere with the next scanned fingerprint. The previous impression may just add excess grease to the next scan, or it may result in a ghost image of the previous fingerprint. In either case, the unwanted information causes serious problems.

The final major problem is with the feature extraction system. In many cases, some of the signal processing algorithms used to enhance an acquired image can leave irregularities in the image causing problems for the feature extraction stage. These signal-processing algorithms may be implemented in software as part of the feature extraction stage, or in hardware as part of the acquisition system. In either case, the irregularities that they introduce cause additional problems when trying to find a match to a given print.

Ink-based fingerprinting

The oldest and most common method for obtaining fingerprints is using ink and paper. It has been used by law enforcement agencies for years and is probably the method most people think of when the topic is mentioned.

The process of performing ink and paper-based fingerprinting is relatively simple. First, the finger must be evenly coated with a layer of ink done by rolling the finger on an ink-covered surface. Once the finger is coated with ink, there are two methods that are typically used to acquire an image of the print. The first and most common method is called "rolling." To obtain a print using the rolling method, the ink-coated finger is rolled on a piece of paper starting with the edge of the fingernail on one side and continuing to the edge of the fingernail on the other. Figure 2 shows a fingerprint acquired using the rolling technique.

This process provides an impression of a large portion of the finger surface. Having such a large portion of the finger surface available is a major benefit of this particular method. The larger area allows more useful information to be gathered from the print. A larger number of usable minutia points in the image allow for easier matching with future copies of the fingerprint. This is especially useful when the later print captures may only contain a portion of the finger surface. Unfortunately, the act of rolling the finger tends to cause distortion in the resulting image. The pressure applied to the finger stretches the skin causing small distance changes.

The second method is called "dabbing." As the name suggests, the dabbing method involves simply pressing the inked finger onto the paper. Since the finger is not rolled, less of the fingerprint surface is captured. However, the dabbing method causes less distortion in the fingerprint image because stretching is minimized.

When fingerprinting is performed by law enforcement agencies, all ten fingers are typically done. The resulting images are placed on cards and stored for later identification. In the past, law enforcement agencies needed to perform time-consuming visual comparisons between an unknown print and sets of prints stored in their card database. In recent years, however, many agencies have switched to more computerized systems. The cards containing the fingerprints are scanned into a computer using a flatbed scanner or CCD camera. Once in the computer, the number of possible matches can be limited by applying special processing and match-searching algorithms. This limited set of possible matches can then be searched manually

in much less time.

Even with computer matching systems, ink and paper-based fingerprinting is not a very practical solution. Since the inked print must be scanned into the computer, the time required to verify would prohibit timely authentication. In addition, the requirement of placing ink on the fingers is not typically acceptable for an application that requires frequent sampling of the fingerprint. Not many people would want to get their fingers inked every time they want to log into their computer or make a withdrawal from their ATM. As a result, ink and paper-based fingerprinting will most likely remain a practice only within the law enforcement community. However, the larger surface that ink and paper-based methods provide is a desirable feature. It may be that the initial print for a biometric system taken during the enrollment phase should be done using ink and paper. This would allow a much larger set of minutia points for future comparison.

Optical methods

The remaining technologies described can all be grouped into a category called "livescan." This term means that the fingerprint images are captured by the computer directly from the individual's finger. These technologies typically capture a smaller portion of the finger surface than ink and paper-based methods, but they are much quicker and do not have unwanted side effects like ink-covered fingers.

The most common technique used by optical fingerprint scanners is that of frustrated total internal reflection. The typical scanner design consists of a glass platen or prism, a light source and a light detector. The frustrated total internal reflection technique works by using some basic principles of optics. When a finger is placed on the glass plate or prism, the ridges of the fingerprint come into direct contact with the glass material. The valleys, however, do not directly touch the surface. The behavior of the glass plate relative to the incident light is changed due to the contact with the ridges. When no ridge is present, the light that hits the glass plate at an angle is reflected back where it strikes the sensor unit. The light that strikes the portions of the platen where a ridge is present diffracts and the ridges appear black. Figure 3 demonstrates the basic operation of frustrated total internal reflection.

The benefits are that the scanners are inexpensive to manufacture and are capable of relatively high resolutions. On the other hand, optical scanners are very sensitive to ambient light. If there is too much light in the area where the scanner is being used, it can lead to poor image quality since stray light can confuse the detector. In addition, optical fingerprint scanners tend to suffer from a lack of contrast. The images can be extremely light which makes them more difficult to process. In many cases, additional signal processing is required to darken the images so that accurate feature extraction can occur. The signal processing algorithms often serve to introduce image artifacts and amplify the noise in the image.

There are two types of optical scanners that are less often utilized, but show a great deal of promise. The first one is based on hologram reflection. These devices are similar to those using frustrated total internal reflection, except that the light passes through a light diffractive grating contained within a hologram. The light is then modulated by the ridge structure of the finger. The modulated light then returns through the diffractive grating and is analyzed by a detector. Scanners based on this technology can overcome some of the distortions introduced by the detector arrays within standard optical scanners. They can also be built within much smaller packages. This would make them practical for inclusion within portable devices.

The final type of optical scanner discussed here is a scanner that uses a CCD camera to capture the fingerprint. The finger does not have to be pressed against a platen. Systems utilizing this no contact technology usually consist of a CCD camera that has been focused on a specific point. A guide, or finger rest, is typically placed so that the user will position their finger at the correct photographic point. The CCD camera captures an image of the target finger. This image is then processed to enhance the ridge structure of the finger. There are several benefits to this type of design. First, there is no distortion due to skin stretching from pressing against a surface. This helps to make successive images more reproducible. Also, there is no platen that can be scratched. This lowers the required system maintenance.

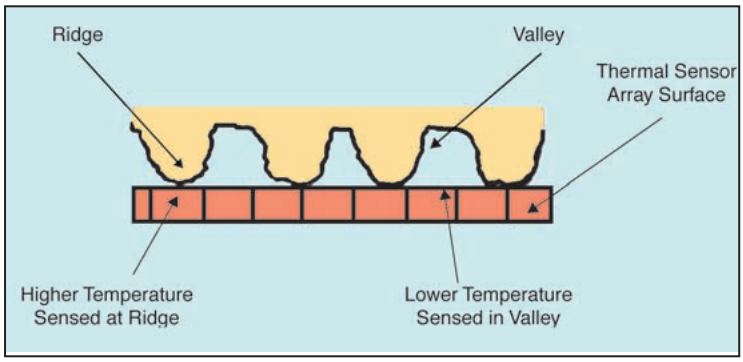


Fig. 4 A depiction of the interaction between the ridges and valleys of a fingerprint and the thermal sensors in a thermal fingerprint scanner. A higher temperature is sensed where the ridge directly touches the surface, and a lower termperature is detected in the valleys where there is an air gap.

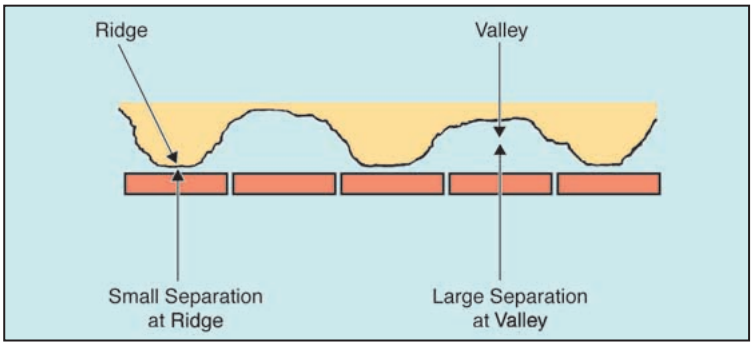


Fig. 5 An illustration of a typical electromagnetic fingerprint sensing device. The sensor plates are close to the finger at the ridges, but separated at the valleys. This causes different capacitance values for the different sensor plates.

Still, high ambient light is likely to be a problem. In addition, even these optical scanners are still limited to scanning the surface layer of the skin, which may be worn and unusable.

Thermal imaging

Thermal imaging uses body heat to create an image of the fingerprint. A pyroelectric substance is used within a

sensor to create an electrical signal that relies on the heat applied to the sensor. An array of these sensors is employed to detect the temperature of the finger at various positions. When a finger is placed on the sensor array, the ridges of the fingerprint come into direct contact with the sensor surface. Since the ridges touch the sensor and the valleys do not, the ridges will be sensed at a higher temperature than the valleys. These sensed temperature values are then converted into an eight-bit grayscale image. The number and density of the sensors within the array determines the resolution of the resulting image. Figure 4 displays the interaction between the ridge and valley pattern of a fingerprint and the thermal sensor array of a thermal fingerprint scanner.

Thermal scanners have some benefits over the others. Thermal sensors are less influenced by the condition of the finger. Whether the finger is wet, dry or greasy makes very little difference to the scanner. The primary concern of the scanner is that the temperature variations are sufficient. Therefore, as long as the ridge structure is well defined, a good image can be obtained. (However, it does not solve the problem of dirty or worn fingerprints.) In addition to its tolerance to finger conditions, thermal scanners are not affected by ambient light, and they are often capable of obtaining an image through a thin film such as a latex glove. As long as the heat pattern of the fingerprint is preserved through the film, a thermal scanner can obtain an image.

The major problem with a thermal scanner is obviously its sensitivity to environmental heat. The best images are acquired when the scanner and the finger are at very different temperatures. If the scanner is in an environment that could cause its temperature to approach that of the finger, the thermal scanner is not a good choice. In addition, if the ridge pattern is not distinct enough, a thermal scanner cannot determine the difference between the temperature of a ridge and the temperature of a valley. This will result in poor image quality.

Electromagnetic field imaging

Fingerprint scanning based on electromagnetic fields is a relatively new area. Most electromagnetic field sensors are based on the principles behind the capacitor. A typical capacitor consists of two conducting plates separated by an insulating dielectric material. The capacitance of the capacitor is based on the charge on the plates, the size of the plates, and the distance by which the two plates are separated. In a typical electromagnetic fingerprint sensor, the sensor's surface consists of a large number of small conductive plates. The finger is then used as the second plate in the capacitor arrangement. When the finger is placed on the surface, it comes into contact with a conduction ring that surrounds the sensor array. This conduction ring passes a charge onto the finger. This charge is propagated by the highly conductive layer of newly formed cells beneath the outer layer of skin. The scanner then senses the capacitance on each of the tiny plates within the sensor array and converts this value into an eight-bit grayscale value. The values generated by each of the small plates in the array are collected to form an image of the fingerprint.

The reason that this works is actually quite simple. The finger acts as the second plate of the capacitor. It is charged by the conductive ring. The distance of the finger from the sensing plates is determined by the shape of the fingerprint. The ridges will be much closer to the sensor plates and, thus, will yield a capacitance that is reflective of two plates separated by a small distance. The charge at the valleys, however, is separated from the sensing plates by a much larger distance and will yield a capacitance that reflects this fact. Figure 5 depicts the arrangement of an electromagnetic scanning device.

One major advantage to using electromagnetic scanning is that it will return an image of the cells below the outer layer of skin. As a result, electromagnetic scanning is far less influenced by surface conditions and worn finger surface ridges.

Another advantage of electromagnetic sensors is their size. Since they are solid state devices, they can be made very small. Typical electromagnetic sensors are about the size of a postage stamp. This feature makes them ideal for inclusion in portable devices.

A weakness of electromagnetic scanners is their susceptibility to damage from electrostatic discharge. Since the finger is acting as a plate in the capacitor, the electronics in the scanning device must be developed so that it can come into contact with the finger. This makes the chip very open to problems from static electricity that tends to build up on the human body. A sufficient discharge could destroy an electromagnetic sensor. Developing a design that would ground the individual before allowing them to touch the chip would solve this problem.

Ultrasound imaging

Ultrasound involves, as the name suggests, the use of sound waves generated at frequencies higher than the human ear can hear. Many people are probably familiar with the use of ultrasound in medical applications. It has a proven track record in obtaining images of the human body without the ill effects of radiation. Ultrasound fingerprint scanning is simply an extension of this proven medical technique. An ultrasound scanner requires that the user place his or her finger on a glass plate. Once the finger is in place, a transmitter, and ring of receivers, is mechanically moved along the length of the glass plate. As the assembly is moved, the transmitter emits pulses of sound. As this sound comes into contact with objects, some of the

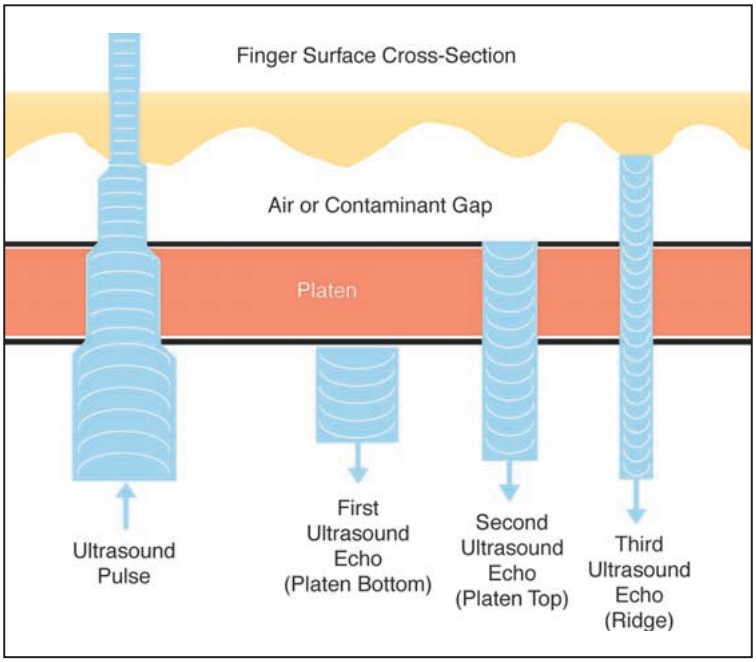


Fig. 6 An illustration of the transmission and reflection of sound waves in an ultrasound scanner.

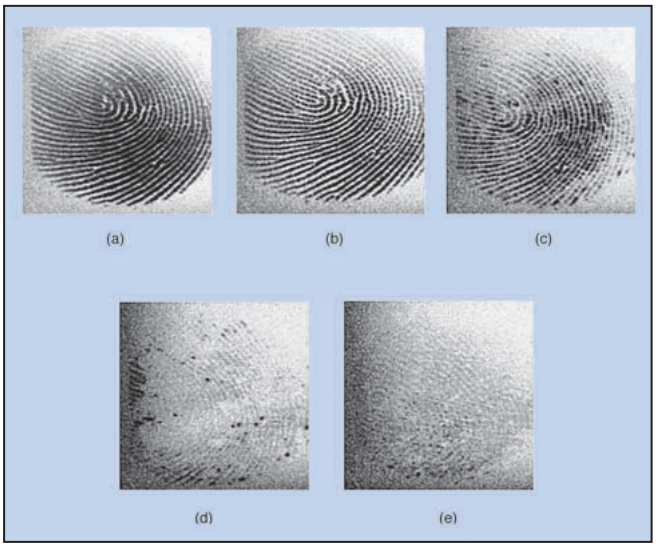


Fig. 7 The test results of the optical scanner. a) The normal finger yields a good scan. b) The wet finger also yields a good scan. c) The dry finger: The optical scanner yields poor quality and begins to deteriorate. d) The scan of the dirty finger yields very low quality. e) The scan with the glove shows a ghost print because of oil deposits on the scanner surface.

Table 1 Quality of images acquired by scanning technologies under various conditions

CONDITIONS	Optical	Thermal	Ultrasound
Normal	Good	Good	Excellent
Wet	Good	Good	Fair
Dry	Fair	Good	Good
Dirty	Poor	Fair	Fair
Glove	None	Poor	Fair

sound waves are transmitted through the object and some are reflected back. Figure 6 shows the transmission and reflection concept of an ultrasound scanner. The waves reflected back are received by the ring of receivers. These echoes, and the measured delays in their return, are then transformed into an image using signal-processing techniques used in medical computer tomography.

Ultrasound imaging obtains images from the layers of skin slightly beneath the surface of the finger. As a result, much like electromagnetic imaging, ultrasound imaging is less susceptible to the finger's surface conditions. It is also capable of imaging through items covering the finger, such as latex gloves. These benefits make ultrasound scanning attractive.

The main drawbacks of ultrasonic scanning are speed, size and cost. Ultrasound scanners require mechanical movement of the transmitter and receiver assemblies. As a result the scanner package must include all of the necessary mechanical equipment. In addition, the mechanical movement is slow in comparison with the time required for the other scanners, which is often measured in milliseconds. Finally, the cost of the components is high making the overall imaging cost much higher than other types. Thus, it is unlikely that ultrasound scanners will be seen in portable devices anytime soon. However, they do seem to be an attractive scanner when high accuracy and security are requirements that outweigh speed and size.

Comparison testing

Now let's try comparing the performance of these technologies by testing some actual units. The technologies involved are optical, thermal and ultrasound. The optical scanner that was used was the Finger Imaging System manufactured by Polaroid. The thermal scanner was the Sweepe manufactured by Thomson CSF, and the ultrasound scanner was a series 500 scanner from Ultra-Scan, Inc. The same finger was scanned on each of the three scanners under five different finger conditions. Figures 7 through 9 display the results of the scans. Table 1 displays a ranking of the quality of the images in each case. These conditions consisted of the following:

1. Normal—no special action was taken
2. Wet—The finger was moistened with a wet rag before scanning.
3. Dry—The finger was dried out thoroughly.
4. Dirty—The finger was rubbed in soil and then wiped with a dry cloth before scanning.
5. Gloved—The finger was placed in a latex glove and then scanned.

As can be seen from the results, each scanner performed close to what would be expected based upon its described strengths and weaknesses. By looking at the results, a few interesting comments can be made. First in the case of the optical scanner, the resulting images displayed in this article were contrast-enhanced after scanning so that they would show up in printing. All the images from the optical scanner were very light and difficult to see before enhancement. The optical scanner also had a great deal of trouble with the dirty finger. Finally, there is a ghost image in the glove scan. The optical scanner should not have any results for a scan through a glove. However, at the time of scanning there was an oily residual print left on the scanner from a previous scan. The presence, of this residue resulted in the ghost image, seen in Fig. 7(e).

With the thermal scanner, we see that it can actually sense a print through a

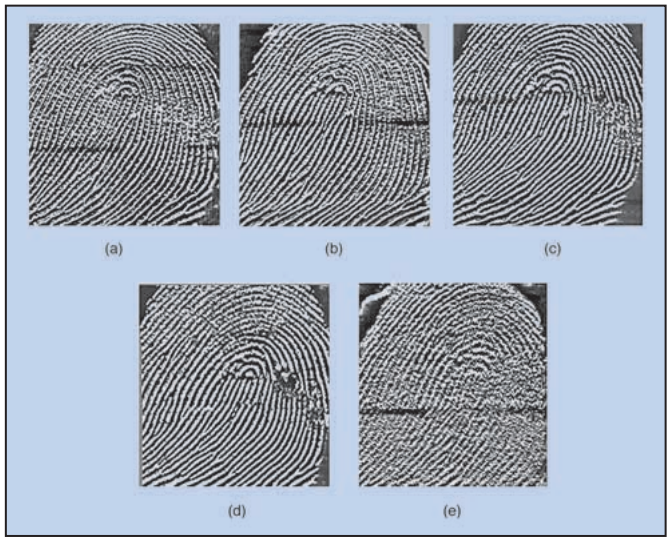


Fig. 8 The test results of the thermal scanner. a) The normal finger yields a good scan. b) The wet finger is not that different from the normal scan. c) The dry finger is also not that different from the normal scan. d) The scan of the dirty finger is not as good as the others, but still quite good. e) The glove scan provides a fairly good scan considering that it is scanning through a glove.

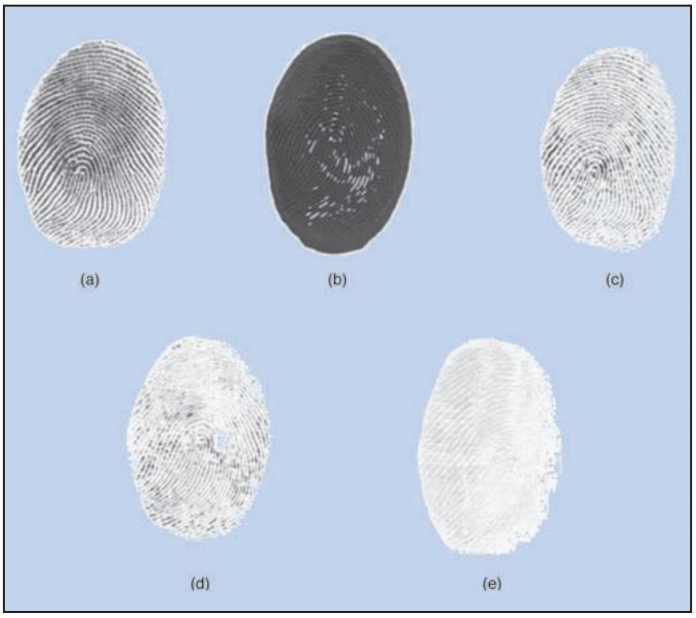


Fig. 9. The results of the testing on the ultrasound scanner. (a) The normal finger: yields a very good scan. (b) The wet finger: a dark image since the excess water confused the scanner. . The fingerprint is still evident within the image. (c) The dry finger: still a good scan. (d) The dirty finger: This scan is not great, but it is still quite good. (e) The glove: The best results of the three technologies.

glove. However, the resulting print is not of the same quality attained in the other scans. Some distortion can also be noted in all of the thermal scans due to the fact that it is a sweep-style scanner. In other words, the image is dependent upon the sweeping of the finger across a sensing strip. Changes in speed during the scanning causes the horizontal distortions that can be seen in the results. Also, the thermal scanner, too, had some trouble with the dirty finger. While there was trouble with the dirty finger, the quality of the scan was higher than that of the optical scanner in the same situation.

Finally, the ultrasound scanner performed relatively well. The scans are of high quality in most of the cases. It had slight problems with the dirty finger. While the image is not of the highest quality, it would most likely still be of high enough quality to identify the individual. The wet fingerprint is very dark on the ultrasound scanner. This is because the excess water confused the scanner. While it is dark, the fingerprint can still be seen as a series of black lines within a dark background. Finally, the ultrasound scanner provided the best image of the finger through the latex glove. This was to be expected based upon the technology that was used. While the print is light, it is still readable and some information could likely be extracted from it.

Conclusions

While the scanners performed at levels close to expectations, there obviously is substantial room for improvement. The scanning technology implemented in the scanners on the market today is adequate for the current tasks; but, for biometrics to become more widely accepted and implemented, improvement is necessary. Fingerprint scanners need to be able to produce useful results under a wide range of situations. Scanning technology will remain a hot field for research until these problems are solved.

Read more about it

• A. K. Jain, L. Hong, and S. Pankanti. (2000)."Biometrics: Promising Frontiers for Emerging Identification Market." [Online]. Available:http://*www.ese.msu.edulpublicationsltechITPIMSU-CSE-00*-2.ps.gz.

• A. K. Jain and S. Pankanti, "Biometrics Systems: Anatomy of Performance," *IEICE Trans. Fundamentals, vol.* E00-A, no. 1, Jan. 2001.

• A. K. Jain, S. Pankanti, and A. Ross, "Fingerprint Matching: Data Acquisition and Performance Evaluation," March 1999. [Online]. Available: http*://www.ese.msu. edu/publications/techITPIMSU-CPS-99*-14-ps-4.

• A.K. Jain and S. Pankanti, "Automated Fingerprint Identification and Imaging Systems," *Advances in Fingerprint Technology,* 2nd ed. (H.C. Lee and R.C. Gaensslen). New York: Elsevier Science, 2001.

• *Ultra-Scan Homepage*.[Online]. Available: http://www.ultra-scan.org .

• W. Bicz, D. Banasiak, P. Bruciak, Z. Gumienny, S. Gumuli_ski, D. Kosz, A. Krysiak, W. Kuczy_ski, M. Pluta, and G. Rabiej"Fingerprint Structure Imaging Based on an Ultrasound Camera." 1997. [Online]. Available: http://www.optel.com.pl/article/english/article.htm.

• M. Metz, C. Flatow, N. Phillips, and Z. Coleman, *Device for forming and detecting fingerprint images with valley and ridge structure*. (1999, Oct. 26). U.S. Patent: 5,974,162 [Online]. Available: http://www.uspto.gov.

• Biometric Partners homepage. [Online]. Available: http://www.biometricpartners.com.

• Atmel Inc., *Atmel Thermal Fingerprint Sensor Databook* Atmel Inc. Nov. 2000. [Online]. Available: http://www.atmel.com/atmel/acrobat/doc1962.pdf• Infineon, *Fingertip Scanner Databook 3.3*. . . Infineon Inc. 2000.

• Veridicom homepage. [Online]. Available: http://www.veridicom.com.

• W. Bicz, Z. Gumienny, D. Kosz, M. Pluta"Ultrasonic Setup for Fingerprint Patterns Detection and Evaluation." [Online]. Available: http://www.optel.com.pl/article/english/article2.htm.

• Polaroid Biometrics Group homepage.[Online].Available: http://www.polaroid.com/products/id/id systems/biometrics.html.

About the authors

Reza Adhami is chairman of the Department of Electrical and Computer Engineering at the University of Alabama in Huntsville. Dr. Adhami has nearly 20 years of industry and academic experience in the areas of digital signal processing, digital image processing, biometrics, pattern recognition, and speech recognition. He has contributed to many applications of the wavelet transform including vibration analysis, mammography lesion classification, computed tomography, and data compression. He has been a consultant to many industries and Government agencies.

Peter Meenen is a graduate student in the Electrical and Computer Engineering Department of the University of Alabama in Huntsville. He has an MSEE in Signal Processing from UAH and a BS in Physics and Computer Science from Berry College. He is currently doing research in the Engineering Department's Integrated Biometrics Laboratory in the areas of biometric fingerprint recognition and analysis.