Applications

Editor: Michael J. Potel
http://www.wildcrest.com

Graphics and Security: Exploring Visual Biometrics

Kirk L. Kroeker

Biometrics is the science of recognizing a person on the basis of physical or behavioral characteristics. Things you can carry, such as keys or ID badges, can of course be lost, stolen, or duplicated. The same goes for things that you know, such as passwords or personal ID numbers. Biometrics relies on who you are—on one of any number of unique characteristics that you can't lose or forget.

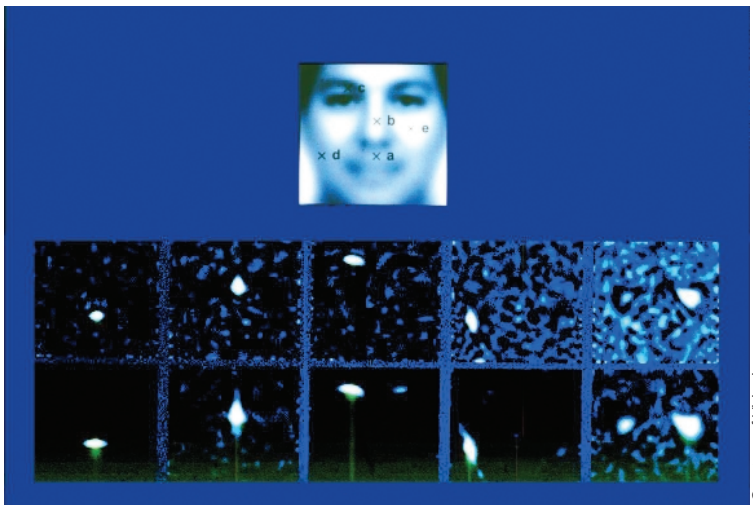
Most biometric systems can be set to varying degrees of security, which gives you more flexibility to determine access levels. Increasing security in biometric systems sometimes makes them more restrictive, resulting in an increased false rejection rate. The net effect of false rejection rates is usually nothing more than inconvenience. However, if security is set too low, the false acceptance rate might increase, which turns out to be potentially far more serious since it involves an unauthorized person gaining access to protected resources.

Furthermore, many companies use biometric security in addition to standard passwording systems—as a layer of additional identity verification. Of course, many biometric systems are expensive and sacrifice some measure of personal privacy. To verify your face, finger, or iris, you must have some personal data on file in the verifying system—personal data that can be stolen or made public. But biometric systems are becoming increasingly popular both as standalone security systems and as added security largely because of one trait: convenience. You can easily forget a password, but you'll never forget to bring your face, finger, or eye.

Face-recognition technology

As Figure 1 shows, all face-recognition technologies share certain commonalities, such as emphasizing those sections of the face that are less susceptible to alteration, including the upper outlines of the eye sockets, areas surrounding the cheekbones, and sides of the mouth.[1] Facial-scan technology works well with standard PC video capture cameras and generally requires cameras that can capture images at least at 320×240 resolution and at least 3 to 5 frames per second. More frames per second, along with higher resolution, will lead to better performance in verification or identification, but higher rates typically aren't required for basic one-to-one verification systems that compare your face scan to a template you've previously stored on the verifying system.

Because such cameras cost as little as $50.00, and demo versions of leading vendors' software are freely available, facial recognition is one of the few biometrics with which you can experiment on a limited budget. For facial recognition at long distances—especially for crowd recognition systems (see Figure 2)—a strong correlation exists between camera quality and system capabilities.[2] And for large-scale one-to-many searches—where you might be comparing a face scan to several thousand face templates to discover somebody's identity—processor speed is critical. But getting started doing one-to-one verification can be almost as cost effective as a standard passwording system.



Courtesy of Visionics

1 Visionics' FaceIt face-recognition biometric system creating a face template.

Face-recognition process

As with all biometric technologies, sample capture, feature extraction, template comparison, and matching define the process flow of facial-scan technology. The sample capture process will generally consist of 20 to 30 seconds during which a facial-recognition system will take several pictures of the subject's face. Ideally, the series of pictures will incorporate slightly different angles and facial expressions to allow for more accurate searches. After entering a sub-

ject's general face scan, the system—no matter what vendor—will typically extract the subject's distinctive features and create a graphic template.

The exact algorithm any given commercial system uses to create and then later verify the templates is typically a closely guarded secret. The template is much smaller than the image from which it's drawn. Whereas quality facial images generally require 150 to 300 Kbytes, templates will only be approximately 1 Kbyte. Visionics, one of the most prominent biometric vendors, uses an even smaller 84-byte template to help accelerate one-to-many searches.

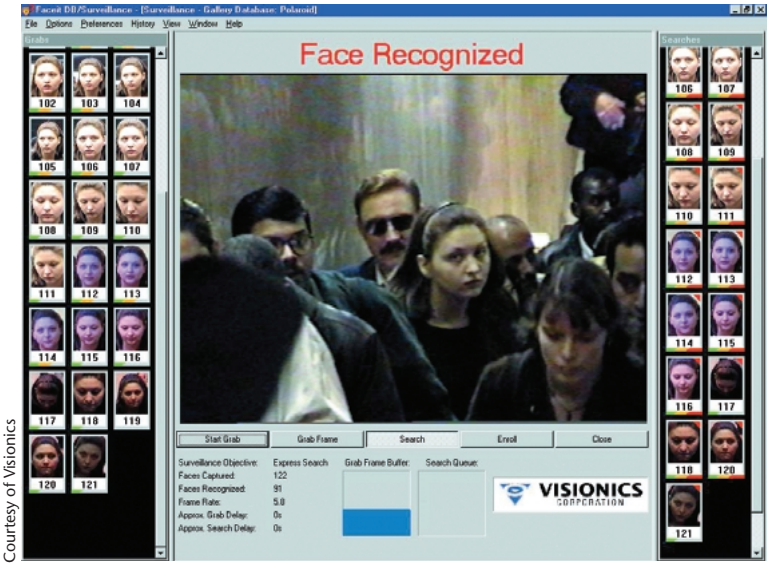
Authentication follows the same protocol. Assuming your user is cooperative, he or she stands or sits in front of the camera for a few seconds and is either verified or rejected. This comparison is based on the similarity of the newly created template against the template on file. One variant of this process is the use of facial-scan technology in forensics. The templates come from static photographs of known criminals and are stored in large databases. The system performs a one-to-many search of these records to determine if the detainee is using an alias. If the database has only a handful of enrollees, this kind of search isn't terribly processor intensive. But as databases grow large, into the tens and hundreds of thousands, this task becomes more difficult. The system might only narrow the search to several likely candidates and then require human intervention at the final verification stages.

Another variable in identification is the dynamic between the target subjects and capture device. Standard verification typically assumes a cooperative audience, one consisting of subjects motivated to use the system correctly. Facial-scan systems, depending on the exact type of implementation, might also have to be optimized for uncooperative subjects. Uncooperative subjects are unaware that a biometric system is in place, or don't care, and make no effort to be recognized. Facial-scan technologies are more capable of identifying cooperative subjects.

Visionics' FaceIt technology

Visionics FaceIt technology is a face-recognition biometric system that can automatically detect human presence, locate and track faces, extract face images, and perform identification by matching against a database of people it has seen before. The technology is typically used for one-to-many searching, verification, monitoring, and surveillance. To determine someone's identity in identification mode, FaceIt computes the degree of overlap between the live face print and those associated with known individuals stored in a database of facial images. The system can return a list of possible individuals ordered in diminishing score or it can simply return the top match and an associated confidence level.

In verification mode, the face print can be stored on a smart card or in a computerized record. FaceIt matches the live print to the stored one. If the confidence score exceeds a certain threshold, then the match is successful and the system verifies the user's identity. FaceIt can find human faces anywhere in the field of view and at any distance—depending on the quality of the video capture device being used—and it can continuously track them and crop them out of the scene, matching the face against a watch list. FaceIt can also compress a face print into the 84-byte template for use in smart cards, bar codes, and other limited-size storage devices.



Courtesy of Visionics

2 Face-recognition software used to recognize individuals in a crowd—like the kind used in Las Vegas or at high-security events—typically scans crowds actively and tries to match the scans with a large database of known criminals. Crowd scanning technology, like Visionics' FaceIt software shown here, requires high-end video capture devices and fast processors.

FaceIt uses what the company calls local-feature analysis to represent facial images in terms of local building blocks. Visionics developed this mathematical technique based on the understanding that all facial images can be synthesized from an irreducible set of elements, not what you might assume to be the basic elements of the face, such as the eye, nose, or mouth. These elements are derived from a representative ensemble of faces using statistical techniques that span multiple pixels and represent universal facial shapes but aren't commonly known facial features.

According to Visionics, more facial building elements exist than facial parts. However, synthesizing a given facial image to a high degree of precision requires only a small subset (12 to 40 characteristic elements) of the total available set. Identity is determined not only by which elements are characteristic but also by the manner in which they're geometrically combined—that is, by their relative positions. FaceIt maps an individual's identity into a mathematical formula—which the company calls a face print—that the system can match and compare to others. According to Visionics, the face print resists changes in lighting, skin tone, eyeglasses, facial expression, and hair variations. The face print contains the information that distinguishes a face from millions of others.

Fingerprint-recognition technology

For decades, fingerprinting was the common ink-and-roll procedure used when booking suspects or conducting criminal investigations. Today, forensic scientists use fingerprint applications in large-scale one-to-many searches on databases of up to millions of fingerprints. In

Fingerprint Features

The human fingerprint consists of ridge patterns that are traditionally classified according to the decades-old Henry system: left loop, right loop, arch, whorl, and tented arch. Loops make up nearly two thirds of all fingerprints, whorls are nearly one third, and perhaps 5 to 10 percent are arches. These classifications are relevant in many large-scale forensic applications but are rarely used in biometric authentication. The discontinuities that interrupt the otherwise smooth flow of ridges are the basis for most fingerprint authentication techniques (see Figure A).

Courtesy of Kinetic Science

A Fingerprint scan produced by Kinetic Sciences' optical fingerprint scanning technology.

Codified in the late 1800s as Galton features,[1] many types of minutiae reside in a fingerprint, including

- dots (very small ridges),
- islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges),
- ponds or lakes (empty spaces between two temporarily divergent ridges),
- spurs (a notch protruding from a ridge),
- bridges (small ridges joining two longer adjacent ridges), and
- crossovers (two ridges that cross each other).

Other features are essential to finger-scan authentication. The core is the inner point, normally in the middle of the print, around which swirls, loops, or arches center.

Reference

1. A.K. Jain and F. Farrokhnia, "Unsupervised Texture Segmentation Using Gabor Filters," *Pattern Recognition*, vol. 24, no. 12, 1991, pp. 1167-1186.

fact, fingerprint technology is the most common biometric technology on the market.[3] And there's good reason this popularity. Naeem Zafar, president of Veridicom, a prominent biometric systems vendor, points out that "fingerprint biometric provides a level of security at a price point and form factor that makes it most convenient for portable devices and IT applications."

Although finger-scanning technology can be used on large databases, it's frequently used for one-to-one verification to provide system access to individual users.[4] Zafar suggests that "fingerprint authentication delivering security, disguised as convenience, will start entering our lives over the next two to five years." Initially, he says, the technology will manifest itself in government projects, aviation security, and fraud-reduction programs but ultimately it will capture consumer attention by freeing people from the password jungle.

Fingerprint-recognition process

Once a fingerprint-recognition system captures a high-quality image, it takes several steps to convert the fingerprint's features into a compact template (see the sidebar "Fingerprint Features" for more information). This process, typically known as feature extraction, is at the core of most finger-scanning technology.[5] Much like the face-recognition companies, each of the primary finger-scan vendors has a proprietary feature-extraction mechanism they typically guard because it distinguishes them from their competitors. Generally, once a fingerprint-recognition system captures a quality image, it converts the image into a usable format. If the image is grayscale, the system discards areas lighter than a particular threshold and it makes darker areas black. It then thins the ridges to one pixel for precise location of endings and bifurcations.

The point at which a ridge ends, and the point where a bifurcation begins, are the most rudimentary minutiae and are used in most fingerprint-recognition applications. Once the point has been situated, its location is commonly indicated by the distance from the core, with the core serving as the center point on an x–y axis. In addition to using the location of minutiae, some vendors classify minutiae by type and quality. The advantage of this is that searches can proceed more quickly, as a particularly notable minutia might be distinctive enough to lead to a match. A vendor can also rank high- versus low-quality minutia and discard the latter.

Getting good images of these distinctive ridges and minutiae is a complicated task. The fingerprint presents only a small area to take measurements and the wear of daily life, which ridge patterns show most prominently. Vendors have developed increasingly sophisticated mechanisms to capture the fingerprint image with sufficient detail and resolution. The main fingerprint-scanning technologies in use today include optical, silicon, and ultrasound.

Optical technology is the oldest and most widely used. To do an optical scan, the user typically places his or her finger on a clear scanning platform, such as the one shown in Figure 3. In most cases, a device simply converts the image of the fingerprint with dark ridges and light valleys into a digital signal and adjusts the contrast automatically.

Silicon technology has gained considerable acceptance since its introduction in the late 1990s. Most silicon technology relies on direct-current capacitance. The silicon sensor acts as one plate of a capacitor and the finger is the other. The software then converts the capacitance between platen and finger into a digital image. Silicon generally produces better image quality than optical technology. Because the silicon chip comprises discrete rows and columns—typically between 200 and 300 lines in each direction on a 1-cm wafer—it can

return detailed data. Silicon chips are small enough to be integrated into many devices that can't accommodate optical technology.

Ultrasound technology, although considered perhaps the most accurate of the finger-scan technologies, isn't yet widely used. Ultrasound can penetrate dirt and residue, countering a main drawback to optical technology. However, implementing ultrasound scans is still more expensive than other fingerprint-scan technologies. In ultrasound scanning, a device sends a short ultrasonic pulse from several different directions toward a finger surface and then measures the response. This pulse response results from the contact scattering of the ultrasonic wave on the surface of the fingertip. Based on a set of such responses, the scanning system reconstructs an image of the finger's surface structure.

Veridicom's silicon technology

Finger-recognition software and silicon sensors like the one shown in Figure 4—both based on technology originally developed at Bell Labs—work together to capture and match your fingerprint in Veridicom's OpenTouch technology. The technology offers a modular hardware and software system for collecting, enhancing, processing, and verifying fingerprint images.

Veridicom's silicon fingerprint sensor provides 500-dpi resolution. The compact sensor is, according to Veridicom, hard and resistant to scratches, abrasion, chemicals, corrosion, and impact. The sensor's surface consists of a silicon chip containing an array of 90,000 capacitor plates with sensing circuitry at 500 dpi. The capacitor-sensing plates create an 8-bit raster-scanned image of the ridges and valleys of the finger pressed against the chip. Software converts this information into a video signal. Typically, a scan takes from one-tenth to one-half a second to complete, depending on the processor's speed.

Veridicom's software then creates a template from the scanned image. The system instantly erases the actual fingerprint image and stores the minutia data, which becomes a unique digital fingerprint template of that person. Future fingerprint readings for that individual are compared against it using the fingerprint-verification module in Veridicom's verification suite. To verify an individual's identity and to authorize transactions, the fingerprint-verification module compares a live reading from a finger placed on the sensor with the minutia data template stored for that individual. If the data match, the individual's identity is verified and the transaction is authorized. If the data don't match, the transaction is rejected.

SecuGen's optical technology

At the most basic level, all optics-based fingerprint systems translate illuminated images of fingerprints into digital code for further software processing. SecuGen devices use the company's proprietary Surface Enhanced Irregular Reflection technology to capture high-contrast, high-resolution fingerprint images. A series of SEIR algorithms developed by SecuGen extract data from the image, mapping the distinguishing characteristics of fingerprint ridge ends, splits, dots, and arches. The algorithms then convert this data into a 400-byte digital template and store it in memory or on disk.

Like many fingerprint-biometric technologies, the actual fingerprint image is never stored and can't be constructed from templates. To identify or verify a fingerprint, a proprietary SEIR matching algorithm compares the extracted minutiae points from the input fingerprint on the optical module to a previously stored sample. The entire matching process takes roughly 1 second. Authentication takes place either locally or on a server, depending on system configuration.

SecuGen embeds its core technology in optical modules that work with the set of extraction and matching algorithms developed for use with the company's SEIR optical method. For example, the company embeds each module in its line of fingerprint PC peripheral devices and standalone devices produced by original equipment manufacturers for various applications.

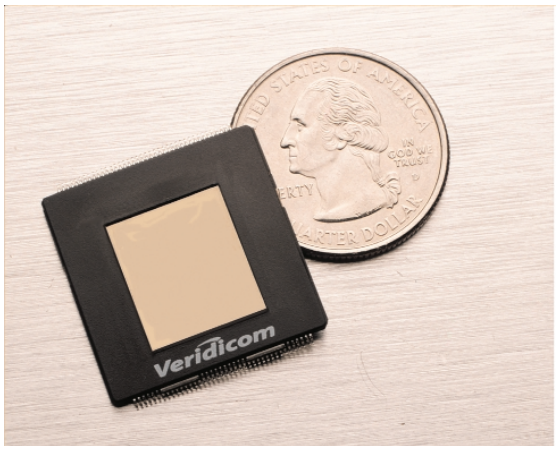
Courtesy of Guardware Systems

3 The high-grade glass used in Guardware's optics makes the scanners scratch-resistant. This also allows SystemsGuard, the company's fingerprint-scanning technology, to be built into a front desk or other work areas where the front of the PC might be difficult to access or there's little room for a desktop unit.

Iris recognition

The holders of the major iris-recognition patents—Leonard Flom, Aran Safir, and John Daugman—founded Iridian Technologies. Since commencing operations in 1993, they've dominated the iris recognition field.[6] Iridian has historically focused on access control, but its current emphasis has been shifting to e-commerce, medical records, network identification, and online banking. So accurate are the algorithms used in iris recognition that, according to the company, the entire planet could be enrolled in an iris database with only a small chance of false acceptance or false rejection.

Iris recognition is of course based on the visible qualities of the human iris (see Figure 5, next page). Visible characteristics include rings, furrows, freckles, and the iris corona. Iridian's iris-recognition technology converts these visible characteristics into an IrisCode, a template stored for future verification attempts. From the 11-mm



4 Veridicom's FPS200 is the latest generation of silicon-based fingerprint sensors. It's designed for integration into the smallest wireless or computing device.

Courtesy of Iridian Technologies

5 The human iris. The primary visible characteristic of the iris is the trabecular meshwork, the tissue that gives the appearance of dividing the iris radially.

Courtesy of Iridian Technologies

6 One of Iridian Technologies' iris recognition products called IrisAccess

diameter iris, Daugman's algorithms provide 3.4 bits of data per square millimeter. This information density means that each iris can have 266 unique spots—compared to 10 to 60 unique spots for traditional biometric technologies.[7]

The first step in scanning an iris is locating it with a dedicated camera no more than three feet from the eye (see Figure 6). After the camera situates the eye, Iridian's algorithm locates the outer and inner edges of the iris and then proceeds to analyze it. Iridian's algorithm uses 2D Gabor wavelets[8]—transforms used typically in visualization applications—to filter and map iris segments into hundreds of vectors. The wavelets assign values drawn from the orientation and spatial frequency of select areas of the iris and they then form an IrisCode. According to Daugman, the equal-error rate (the point at which the likelihood of a false accept and false reject are the same) is one in 1.2 million for IrisCodes.

When the pupil expands and contracts—something that occurs naturally with any change in lighting—it skews and stretches the iris. Iridian's algorithms account for such alteration after locating the iris boundaries at the outer and inner edges. Daugman draws the analogy to a homogenous rubber sheet that, despite its distortion, retains certain consistent qualities. Regardless of the iris' size at any given time, the algorithm draws on the same amount of data, and its resultant iris code is stored as a 512-byte template.

The entire iris-scanning process is brief. The camera normally locates the iris in a quarter second and generates the iris code within 1 second. Database search times are quick, with hundreds of thousands of records analyzed per second, depending on the computer's speed. The iris-capture process does run into the limitations of grayscale imaging technology, where the darkest shades of iris colorations are difficult to distinguish from the pupil. But according to Iridian, the algorithm's robustness actually allows for significant variations in image quality. The same iris might at different times produce iris codes that vary by as much as 25 percent, which might sound like a flaw. But according to Daugman, the odds of a randomly selected iris code coming close to another match are exceptionally small.

Already several iris recognition and verification applications exist. Many companies license the technology from Iridian to create their own products. One such product, Panasonic's Authenticam (see Figure 7), uses Iridian's Private ID iris-recognition technology and comes with I/O Software's SecureSuite to let multiple users access PCs, files, folders, applications, and password banks. In addition to providing security for standard information-access applications, you can use Panasonic's camera to authenticate users for videoconferencing and online collaboration.

Conclusion

Biometrics technology has come a long way from simpler forms of systems security. But are biometrics-based systems more secure or do they simply require crackers to become more proficient at breaking into systems? To recognize your fingerprint requires that a template of your fingerprint actually be present in the system that verifies your access. If you want to pass as somebody else, presumably you'd have to either have that person's finger with you or you'd need to change the verifying template residing in the system that verifies your print.

Cracking into a system and replacing a legitimate print with your own isn't easy to do unless the system's security is poor. While biometric proponents stress the strength of their proprietary technologies or biometrics in general, no system is ever completely secure. Bruce Schneier once pointed out that all computer security is like putting a wooden stake in front of your house and hoping that tresspassers will run into it.[9] Contrary to what many biometric proponents would have us believe—that biometric security outclasses traditional forms of security—all biometric systems are, after all, another form of computer security with its own set of strengths and weaknesses.

Biometrics effectively trade some amount of privacy and cost effectiveness for ultimate convenience—and these systems are certainly no less secure than standard passwording systems. Passwording systems are cheap. Complex biometric scanning equipment is usually expensive. But biometrics seems to be where the indus-

try is headed. Aside from the Orwellian connotations, biometrics systems offer an enormous amount of convenience to users. And, in the present political climate, it's hard to counter the argument that we should adopt biometric systems simply as additional layers of security on top of traditional passwording systems. ■

Courtesy of Panasonic

7 Panasonic's Authenticam uses Iridian Technologies' Private ID software to offer one-to-many identification for applications such as information access or even videoconferencing.

References

1. H. Wechsler et al., *Face Recognition: From Theory to Application*, Springer-Verlag, Berlin, 1998.
2. P.J. Phillips et al., *The Feret Evaluation Methodology for Face-Recognition Algorithms*, NISTIR 6264, Nat'l Inst. of Standards and Technology, Gaithersburg, Md., 1998, http://www.itl.nist.gov/iaui/894.03/pubs.html#face.
3. A.K. Jain et al., "An Identity-Authentication System Using Fingerprints," *Proc. EuroSpeech 97*, IEEE CS Press, Los Alamitos, Calif., 1997, pp. 1348-1388.
4. N. Ratha et al., "A Real-Time Matching System for Large Fingerprint Databases," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 18, no. 8, Aug. 1996, pp. 799-813.
5. K. Karu and A.K. Jain, "Fingerprint Classification," *Pattern Recognition*, vol. 29, no. 3, 1996, pp. 389-404.
6. L. Flom and A. Safir, *Iris Recognition System*, US patent 4,641,349, Patent and Trademark Office, Washington, D.C., 1987.
7. J.D. Daugman, "High-Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, Nov. 1993, pp. 1148-1160.
8. D. Gabor, "Theory of Communication," *J. Institute of Electrical Engineers*, vol. 93, no. 26, Nov. 1946, pp. 429-457.
9. B. Schneier, "Cryptographic Design Vulnerabilities," *Computer*, vol. 31, no. 9, Sept. 1998, pp. 29-33.

Contact Kirk L. Kroeker at kirk@kroeker.net.

Contact editor Michael Potel at potel@wildcrest.com.

For more articles on biometrics, see the July 2002 issue of *Computer*.

Biometric Resources Online

For more information on biometrics, check out these online resources:

- **Association for Biometrics, UK (http://www.afb.org.uk)**: The AfB is a nonprofit organization that aims to be an international forum for research and development, system design and integration, application development, market development, and other issues surrounding biometrics.
- **Automatic Identification Manufacturers Global (http://www.aimglobal.org)**: The AIM Global network is a trade association for the Automatic Identification and Data Capture (AIDC) industry, representing those involved in technologies that include barcode, radio frequency identification, card technologies, biometrics, radio frequency data communications, and their associated industries.
- **BioAPI Consortium (http://www.bioapi.org)**: The BioAPI Consortium was formed to develop a widely available and widely accepted application programming interface for various biometric technologies.
- **Biometric Consortium (http://www.biometrics.org)**: The Biometric Consortium serves as the US Government's focal point for research, development, test, evaluation, and application of biometric-based personal-identification technology.
- ***Biometric Digest* (http://www.biodigest.com)**: *Biometric Digest* is a guide to the companies and people providing and using biometric technology for identification, fraud prevention, security, convenience, customer service, and other applications.
- ***Biometric Technology Today* (http://www.biometrics-today.com)**: *Biometric Technology Today* is a monthly newsletter covering the international biometrics industry. It contains news analysis, case studies, commentary, and regular monthly surveys.
- **Biometrics in Human Services User Group (http://www.dss.state.ct.us/digital/faq/dihsug.htm)**: The focus of BHSUG is to provide a platform for sharing ideas and innovations, distributing findings, identifying best practices, and recommending and creating useful standards for human services users and technology developers.
- **Biometrics Institute (http://www.biometricsinstitute.org)**: The Biometrics Institute is an independent organization engaged in research, analysis, and education for biometric users, vendors, and government agencies.
- **International Biometric Society (http://www.tibs.org)**: The International Biometric Society is an international society devoted to the mathematical and statistical aspects of biometrics. Biologists, mathematicians, statisticians, and others interested in its objectives are invited to become members.
- **John Daugman (http://www.cl.cam.ac.uk/~jgd1000)**: John Daugman's personal Web page offers an excellent overview of the history and present use of iris-recognition technology, including hundreds of reference sources and in-depth studies.