Everything You Need to Know About Biometrics

By Erik Bowman, Identix Corporation

January 2000

A technology that has been around

Chances are this is not your first exposure to the field of biometric identification. After all, the first modern biometric device was introduced on a commercial basis over 25 years ago when a machine that measured finger length was installed for a time keeping application at Shearson Hamil on Wall Street. In the ensuing years, hundreds of these hand geometry devices were installed at high-security facilities operated by Western Electric, Naval Intelligence, the Department of Energy, and the like. There are now over 20,000 computer rooms, vaults, research labs, day care centers, blood banks, ATMs and military installations to which access is controlled using devices that scan an individual's unique physiological or behavioral characteristics.

While you would expect sensitive access control applications to be the first uses of a new high-security technology, biometric technologies also are being used increasingly in computer and communications systems, hospitals, airports, and even homes. In some cases, it is the convenience of the devices more so than the security level that motivates adoption. Still, the "biometric revolution" that has been forecast since the mid-1970s has not occurred. Instead, there has been a steady evolution under way that is being led by a new generation of more reliable, less expensive and better-designed biometric devices.

The most dramatic evidence of the evolution is the falling price of biometric verifiers. In 1999, the average price per access point protected was just under $500 compared with a figure of over $6,000 six years ago. Voice and signature verifiers are now available for under $1,000, and highly secure fingerprint and hand geometry devices are available for $300 to $1,200. But the rate of price drops has slowed recently, since major technological improvements already have been implemented by most manufacturers, including custom chip design and solid-state image acquisition. But reductions in end-user costs will continue as production volume increases and manufacturers improve production. Just this year, the industry experienced price declines in fingerprint devices - some available for as little as $100 per access point protected. Reduced prices have lead to increased awareness of biometric technologies; this coupled with lower overall prices will certainly bode well for this industry as we move through the new millennium.

Biometrics 101

Biometric technologies are defined as "*automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic*." Let's extract the key words from this definition and examine each.

Automated Methods

The term biometric device in the access control industry implies that three major components are present: 1) a mechanism to scan and capture a digital or analog image of a living personal characteristic; 2) compression, processing and comparison of the image; and 3) interface with applications systems. These pieces can be configured in a variety of ways for different situations. A common issue is where the stored images (reference templates) reside: on a card, in the device or at a host. The word "automated" is necessary for our definition because without it, we also would describe a variety of very common, but significantly less reliable, identification techniques such as a photo or inked fingerprint on an ID badge. Figure 1 shows the typology of identification techniques based on human characteristics, including the major automated biometric technologies that we will address in more detail later.

Identification and Authentication

This is arguably the most important aspect of the definition of biometrics, because the products associated with each category are vastly different.

- *Identification*: Identification occurs when an individual's characteristics are being selected from a group of stored images. Called a "one-to-many" search, the question put to the machine is "Do I know you?" The search algorithm will search a database and return a likely list of candidates in a matter of minutes. These types of products can cost between $40,000 and $1 million depending on the configuration. The most popular application for identification devices is law enforcement. These AFIS (automated fingerprint identification system) systems can perform over 100,000 fingerprint match attempts in a second.

- *Authentication*: Authentication occurs when an individual makes a claim of identity by presenting a code or a card. Called a "one-to-one" search, the question put to the machine is "Are you who you claim to be?" In this sense, the individual's characteristics are being measured against an enrolled image that is stored on a token or in a local database with the image presented. These types of products cots between $100 and $3,000 and are used in applications including physical access control and logical access control for example. Because the person presenting him or herself for authentication presents a PIN or password as an index, the search time and subsequent authentication are much faster than its counterpart where 100,000 matches are made in a second; an authentication occurs in a millisecond.

Living Person

While this term appears obvious, it is important to the definition. One of the first questions newcomers to the field ask is "What about a latex finger, digital audio tape, plaster hand, prosthetic eye, etc.'" The answer is that many but not all devices include methods of determining whether there is a live characteristic being presented. The methods are sometimes ingenious and usually simpler than would be expected. The term "living" also separates the biometric industry from the forensic identification field, although basic principles transcend both areas.

Physiological and Behavioral Characteristics

A final point about the definition is the difference between physiological and behavioral characteristics. A physiological characteristic is a relatively stable physical characteristic, such as a fingerprint, hand silhouette, iris pattern, or blood vessel pattern on the back of the eye. This type of measurement is basically unchanging and unalterable without significant duress. A behavioral characteristic is more a reflection of an individual's psychological makeup, although general physical traits, such as size and sex, have a major influence. The signature is the most common behavioral trail used in identification in this hemisphere. Other behaviors that can be used are how one types at a keyboard and how one speaks. Because of the variability over time of most behavioral characteristics, many of these machines update their enrolled biometric reference template each time they are used. After many successful accesses, the template may be significantly different than the original data. The machine will also have become more proficient at identifying you. Generally, behavioral biometrics work best with regular use.

The differences between physiological and behavioral methods are important for several reasons. First, the degree of intrapersonal variation in a physical characteristic is smaller than a behavioral characteristic. Barring injury, your fingerprint is the same day-in and day-out. A signature, however, is influenced by both controllable actions and less controllable psychological factors. Developers of behavior-based systems, therefore, have a tougher job adjusting for intrapersonal variation. For example, it is easier to build a machine that guides you to place your hand in the same position every time than it is to build algorithms that take into account emotional states or the sniffles. The down side to machines which measure physical characteristics is that they tend to be larger, more expensive and may be seen as threatening to users. Behavior-based biometrics often excel in these areas. Both techniques provide a significantly higher level of identification and accountability than passwords or cards alone.

Because of these differences, no one biometric will serve all needs. A company may even decide to use different techniques in different parts of the same access control system. For example, voice verification may be used on executive suites, and fingerprints may be used on computer rooms.

Performance Measures

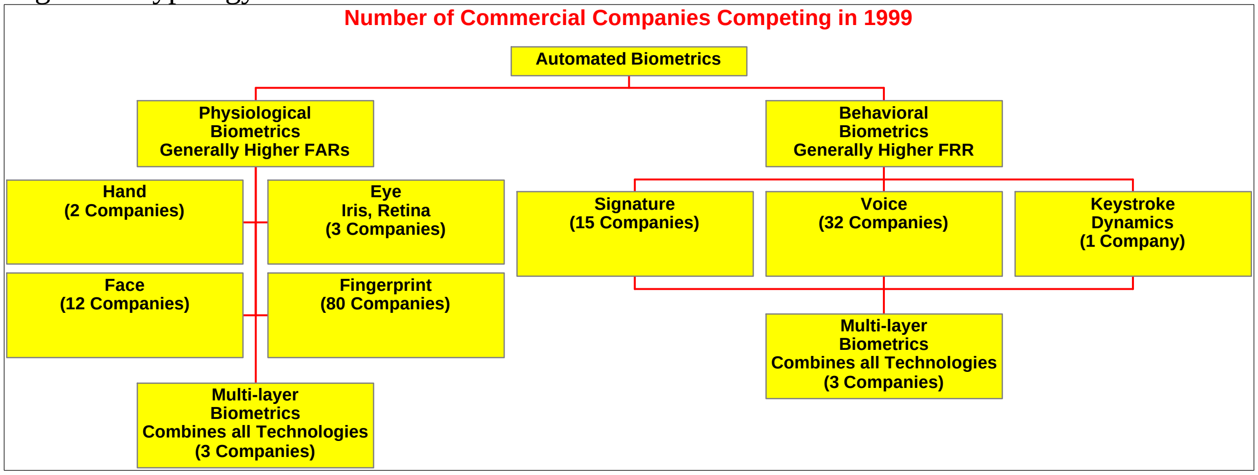
The most commonly discussed performance measure of a biometric is its Identifying Power. The terms that define ID Power are a slippery pair known as False Rejection Rate (FRR), or Type I Error, and False Acceptance Rate (FAR), or Type II Error. While these are important terms, the rates themselves are often overemphasized, and not enough attention is given to their meaning. Many machines have a variable threshold to set the desired balance of FAR and FRR. If this tolerance setting is tightened to make it harder for impostors to gain access, it also will become harder for authorized people to gain access (i.e., as FAR goes down, FRR rises). Conversely, if it is very easy for rightful people to gain access, then it will be more likely that an impostor may slip though (i.e., as FRR goes down, FAR rises). Traditionally, the industry has battled over whose rates are the best, while hardly mentioning that cards and passwords have much worse faults from a security perspective (such as being forgotten, lost, counterfeited, or stolen). Today, a user has to sacrifice up to 4% FRR on first attempts to get near-perfect protection against impostors. But this measure is an aggregate for a large population, and most of the false rejections occur repeatedly to a small subset of the total population. Developers continue to work on techniques to reduce FRR; however, the improvements become more difficult as the percentage of problem cases falls. Most early adopters of biometrics have found that good user training is the best way to reduce false rejections. Most have found that false reject rates drop markedly after two weeks of use. The most balanced biometric device available today, the ID-3D hand geometry machine, has FRR-FAR crossover of less than 0.2%.

Now that you have a good general knowledge of biometrics, let's examine each major type of device on the market.

How is the industry structured?

Segmentation of the biometric industry can first be done by technology, then by the vertical markets and finally by applications these technologies serve. Generally, the industry can be segmented, at the very highest level, into two categories: physiological and behavioral biometric technologies. Physiological characteristics, as stated before, include those that do not change dramatically over time. Behavioral biometrics, on the other hand, change over time and some times on a daily basis. The following chart depicts the easiest way to segment the biometrics industry. In each of the technology segments, the number of companies competing in that segment has been noted.

Figure 1: Typology of Biometric Methods


Number of Commercial Companies Competing in 1999
Automated Biometrics
Physiological Biometrics Generally Higher FARs
Behavioral Biometrics Generally Higher FRR
Hand (2 Companies)
Eye Iris, Retina (3 Companies)
Face (12 Companies)
Fingerprint (80 Companies)
Multi-layer Biometrics Combines all Technologies (3 Companies)
Signature (15 Companies)
Voice (32 Companies)
Keystroke Dynamics (1 Company)
Multi-layer Biometrics Combines all Technologies (3 Companies)

Source: CardTech/SecurTech 1999

Fingerprints

The stability and uniqueness of the fingerprint are well established. Upon careful examination, it is estimated that the chance of two people, including twins, having the same print is less than one in a billion. Many devices on the market today analyze the position of tiny points called minutiae, the end points and junctions of print ridges. The devices assign locations to the minutiae using x, y and directional variables. Another technique counts the number of ridges between points. Several devices in development claim they will have templates of fewer than 100 bytes depending on the application. Other machines approach the finger as an image-processing problem. The fingerprint requires one of the largest data templates in the biometric field, ranging from several hundred bytes to over 1,000 bytes depending on the approach and security level required; however, compression algorithms enable even large templates fit into small packages.

Today, the largest application of fingerprint technology is in automated fingerprint identification systems (AFIS) used by police forces throughout the U.S. and in over 30 foreign countries. These multi-million dollar installations have been responsible for thousands of criminal apprehensions and increasingly are being used for non-law enforcement applications, such as welfare benefits and border crossings.

Increasingly fingerprints, as well as handprints, are also being used to identify welfare recipients who apply for benefits under different identities. Programs in California, New York and many other states have already led to millions of dollars of savings.

Fingerprints are gaining popularity in general security and access control applications. As might be expected, fingerprint verifiers are installed at military facilities, including the Pentagon and government labs. Banks also have been early adopters, protecting computer rooms and computer tape vaults. But, machines tend to reject over 3% of authorized users while maintaining false accept rates of less than one in a million. More than 30 companies are working on new fingerprint ID systems using such technologies as neural network, fuzzy logic and ultrasound scanning.

MasterCard and Visa as well as many other financial institutions have both begun long term efforts to incorporate biometric devices in the bank card environment when smart cards become more common. This kind of endorsement, while not actually resulting in significant sales yet, has bolstered the level of innovation by vendors trying to satisfy demanding requirements. Leading the list are a number of smaller, less expansive machines. Some of the seeds of recent R&D promise to bear fruit. Several companies have produced fingerprint capture units smaller than a deck of cards. Perhaps the most interesting developments are VLSI chips onto which a finger can be directly placed. It is still to be seen if this approach will hold up in field tests, but if it does future fingerprint capture devices will be small enough to install into any ATM, POS terminal or even a mouse. The cost dynamics of chip production could also result in devices priced under $100 in large volume.

Eye Patterns

Both the pattern of flecks on the iris and the blood vessel pattern on the back of the eye (retina) provide unique bases for identification. Only one company, EyeDentify, Inc., produces retinal scan products, and no others are expected to enter the field. There are, however, two companies working on devices that examine the human iris; the most notable, IrisScan, owns the patent. The technique's major advantage over retina scans is that it does not require the user to focus on a target, because the iris pattern is on the eye's surface. In fact, the video image of an eye can be taken from several up to 3 feet away, and the user does not have to interact actively with the device. Sensar, a company that has licensed the iris scanning technology from IriScan hopes to position its IrisIdent product into ATMs in the coming years.

Retina scans, performed by directing a low-intensity infrared light through the pupil and to the back part of the eye, have been available commercially since 1985. The retinal pattern is reflected back to a camera, which captures the unique pattern and represents it using less than 35 bytes of information. Most installations to date have involved high-security access control, including numerous military and bank facilities. Retina scans continue to be one of the best biometric performers on the market with low false reject rates, a nearly 0% false accept rate, small data template, and quick identify confirmations. The toughest hurdle for the technologies continues to be user resistance.

Hand Scans

Hand geometry is the granddaddy of biometrics by virtue of a 20-year history of live applications. There have been six different hand-scanning products developed over this span, including the most commercially successful biometric to date, the ID-3D Handkey from Recognition Systems, Inc. The Handkey looks at both the top and side views of the hand using a built-in video camera and compression algorithms. The reference template is under 10 bytes, the smallest in the industry. Dirt and cuts do not detract from performance, and the hand can be guided easily into the correct position for scanning. Hand geometry is employed at over 8,000 locations, including the Colombian legislature, San Francisco International Airport, day care centers, a sperm bank, welfare agencies, hospitals and immigration facilities for the INSPASS frequent international traveler system.

Devices that look at other hand features are also under development by several companies, including BioMet Partners, Palmetrics, and BTG. The BioMet strategy, for its two-finger Digi-2 scanner is interesting. The company only supplies OEM components to partners for integration into access control, time and attendance, ATMs and other equipment. The company itself does not sell any end-user configured products.

Signature Dynamics

Because of its long-term potential for automating signature verification in the financial community, signature dynamics has been one a hot area of biometric development. Over 100 patents have been issued in this field, including several each to IBM, NCR and VISA. Several companies currently have commercial products available. Each company uses a technique based on a slightly different principle and looks at a different aspect of the dynamic process of making a signature. The key in signature dynamics is to differentiate between the parts of the signature that are habitual and those that vary with almost every signing. Several devices also factor in the static image of the signature, and some can capture a static image of the signature for records or reproduction. In fact, static signature capture is becoming quite popular for replacing pen and paper signing in bankcard, PC and delivery service applications. Generally, verification devices use wired pens, sensitive tablets or a combination of both. Devices using wired pens are less expensive and take up less room but are potentially less durable. To date, the financial community has been slow in adopting automated signature verification methods for credit cards and check applications, because they demand very low false reject rates. Therefore, vendors have turned their attention to computer access and physical security. Anywhere a signature is used already is a candidate for automated biometrics. The first biometric to retail for under $1,000 was the Sign/On product introduced in 1986. Today products are available from Communication Intelligence, AEA Technology, CheckMate Electronics, InfoRite and others.

Voice Verification

Voice verification is a very attractive biometric approach because of its acceptability to users. There are several approaches to analyzing the voice, although all systems are rooted in broader-based speech processing technology. Several large organizations, including AT&T, ITT, France Telecom, Bellcore, Texas Instruments, and Siemens, have developed verification algorithms for communications applications. A common question about voice systems is impersonations. This is not a serious problem, because the devices purposely focus on different characteristics of speech than people do. Impersonators concentrate on the same characteristics as human hearing and do a poor job with the rest. Speech patterns are formed by a combination of physiological and behavioral factors. Voice verification is being used in access control for medium-security or high-throughput situations such as offices and labs as well as in remote banking applications.

Major corporations, including Martin Marietta, GM and Hertz, are protecting computer facilitates with this technology. Voice also is being used increasingly to protect dial-up computer links and terminal access. Five providers of home confinement systems, used to control the whereabouts of early parolees, use voice verification to confirm that prisoners are at home.

There are two basic approaches to voice verification: 1) dedicated hardware and software at the point of access and 2) dial-up of a PC host using regular phones. The former is designed for general access control situations and costs over $1,000 per door protected. The PC-based systems are currently more popular, because the $20,000 to $40,000 of the base system can reduce the per door cost of the technology in large applications.

Keystroke Dynamics

Keystroke dynamics, also called typing rhythms, is one of the most eagerly awaited of all biometric technologies in the computer security arena. As the name implies, this method analyzes the way a user types at a terminal by monitoring the keyboard input 1,000 times per second. The analogy is made to the days of telegraph when operators would identify each other by recognizing "the fist of the sender." The modern system has some similarities, most notably that the user does not realize he is being identified unless told. Also, the better the user is at typing, the easier it is to make the identification. Both the National Science Foundation and National Institute of Standards and Technology have conducted studies establishing that typing patterns are quite unique. The advantages of keystroke dynamics in the computer environment are obvious. Neither enrollment nor verification detract from the regular workflow, because the user would be entering keystrokes anyway. Since the input device is the existing keyboard, the technology costs less. Keystroke dynamics also can come in the form of a plug-in board, built-in hardware and firmware or software. Still, technical difficulties abound in making the technology work as promised, and a half dozen efforts at commercial technology have failed. Differences in keyboards, even of the same brand, and communications protocol structures are challenging hurdles for developers.

Facial Features

One of the fastest growing areas of the biometric industry in terms of new development efforts is facial verification and recognition. And no less than a dozen organizations are working on systems using advanced object recognition techniques including the MIT Media Lab, Harvard University, a slew of defense contractors, and several Japanese firms. Most of these efforts are stimulated by the fast rise in multimedia video technology, which is placing more and more cameras in the workplace, and eventually the home.

Many of the efforts employ neural either network technology or statistical correlations of the face’s geometric shape. The allure of facial recognition is obvious. It is the method most akin to the way that we as humans identify people and the facial image can be captured from several meters away using today's video equipment. But most developers have had difficulty achieving high levels of performance when database sizes increase into the ten's of thousands or higher. Still, interest from government agencies and even the financial sector is high, stimulating the high level of development efforts. Given this pace of development, it is likely that in the future your multimedia PC will recognize you via a camera built into your monitor for teleconferencing on the electronic superhighway. More specific applications such as screening welfare databases for duplicates and airport lounges for terrorists are also likely to advance with time.