The Emerging Role Of Biometrics

Alan S. Horowitz

Introduction

The ancient Egyptians determined which workers were entitled to monthly provisions by keeping records of each person's physical appearance, such as his height and weight, and distinctive marks and traits, including whether he had a limp or was missing a finger, his demeanor and other such anatomical and behavioral identifiers.

At the beginning of the nineteenth century, the discipline of phrenology developed, which tried to relate behavior with physical and biological characteristics. This included using characteristics of the surface of the skull as indicators of behavior, such as claiming those with convex foreheads tended to be benevolent.

Interest in fingerprints dates back to as early as the 1680s, but it wasn't until around the start of the Twentieth Century that much attention to them began. An Argentine police official was the first to establish fingerprint files in 1891, and the New York State Prison system was the first agency to use fingerprints in a systematic way in the U.S. in 1903.

The Twentieth Century's development of powerful computers permitted the melding of biological characteristics with the ability to automate the process of identity verification. This has led to the today' promising field of biometrics, the subject of our presentation.

While biometrics was used to give passengers entry to various parts of the Enterprise space ship of Star Trek fame, it this no longer a subject of science fiction. Fingers were recently pointed at the technology when the Tampa, Florida, police photographed attendees at the Super Bowl 35 in January 2001, hoping to find criminals by using facial matchups. Some thought this was an invasion of privacy since the football fans were not told they would be photographed. It may be but, in fact, almost every business will at some point use biometrics, either internally with its employees, or externally with its customers or as a customer of another company.

Though in limited use today, biometrics will help us in the near future control access to a company's computer system, to authenticate Internet transactions and to provide secure access to physical locations, as well as other uses. The promise of biometrics is it will be easier to use and administer, and be more accurate than the technologies in use today. While you shouldn't throw away your keyring just yet, the days may be numbered for such security technology as user names and passwords, keys and locks, identification badges and personal identification numbers, photos and signatures.

I'm XXX and this is "The Emerging Role of Biometrics," which looks at the technologies, the uses, the benefits and the challenges of biometric technologies. From this presentation, you will learn what is biometrics and how to decide if it is right for your company. This program will cover:

. What is biometrics?

. Basic Biometric Technical Workings
. Types of Biometric Technology
    . Fingerprints
    . Hand geometry
    . Iris scans
    . Voice scans
    . Signature scans
    . Facial scans
    . Other biometric technology
. The Market And Costs
. Benefits
. A Case Study
. The Future

The information in this program comes from variety of print and online sources, and industry experts.

What Is Biometrics?

Biometrics encompasses a wide variety of technologies, making it a difficult term to define. But one can say biometrics is the computer-based, automated use of an individual's unique physical characteristics to authenticate or verify identity.

Biometrics takes advantage of certain facts. One of these is that we all have characteristics which are unlike those of anyone else. The patterns of our fingerprints, irises, retinas, voices, faces, even our ears, are ours alone. Even identical twins have different iris patterns. Also, these characteristics tend to be highly stable over time. Fingerprints taken years ago can be accurately matched to fingerprints from the same person taken today. There may be some wear-and-tear, but generally, the ridge patterns on our finger tips remain largely the same over our lifetimes. The same holds true for other physical characteristics.

That said, there are inconsistencies in our physical characteristics from moment to moment, which significantly complicates the job facing biometric technology. Raj Nanavati, a partner in the New York-based biometric consulting firm, International Biometric Group or IBG, comments about this fact:

Nanavati: "The exact image that's captured will vary substantially each time you take an image. If you take a picture of someone in your family sitting in a chair today and then again tomorrow, it's the same person. Their height hasn't changed. Their looks haven't changed. Nothing really has changed, but the picture will be a little bit different. For the same general reasons, the overall pattern of a biometric will vary. If you're studying the pattern of a person's iris, there may be dust in their eye or they may be looking at the camera from a different angle, which will cause variations. So each image is a little bit different, but within a given person, it varies within a very narrow range."

Basic Biometric Technical Workings

Biometric products make a template of a physical characteristic, such as your fingerprint or iris pattern, and then use an algorithm to match the template taken at a given moment with one on file, in an attempt to make a match. Generally, the user first provides identification, such as a personal identification number or password, or a token like a smart card, to call up their template. This simplifies the process because now the biometric system needs to match just one template -- the one identified by the user -- with another, the one provided by the user at that moment in time.

A more complex scenario is when a person, each time he or she wants to use the system, provides a template, such as a fingerprint or iris scan, and the system has to match that against all the templates in its database to make a verification. This is a much more complex problem for the system though it eliminates the user's need to provide any identification other than the live biometric.

Biometric methods come in a wide variety of flavors, such as fingerprint, iris scan, voice recognition and others, which we will discuss shortly. But the underlying configuration of biometric systems are similar.

First, a user must be enrolled. This involves capturing an image of whatever the biometric source is -- face, voice, handprint, retina, etc. -- and encrypting it in a template which is then stored. Often, this image is stored in a central database located on a server, personal computer or other storage system. But it may also be stored within the biometric reader device or on a token, such as a smart card.

A number of biometric samples are usually captured during the enrollment process, with three being commonplace. This is done because each image will likely differ slightly, as we noted before. By employing several images, the system can average them and create a representative image. Once the template is created, it is referenced against an identification source, such as a PIN number or card. This allows the template to be called up every time the user attempts to access the system. In any biometric system, the accuracy of the enrollment template is critical because it is used from then on as the baseline by which to verify the user.

After the enrollment, when the user logs on, a new template is created of a live image. The system then compares this new template with that of the existing one in the database. Since, as noted already, the two templates will not exactly match, algorithms are used to compare the templates and determine if there is a match.

For this reason, the user is often allowed a certain number of attempts before being rejected. In fact, some thought needs to be given this variable when you set up your biometric system. You want legitimate users to have access to the system and don't want to quickly reject them, called a false rejection, but you also don't want impostors to have the opportunity to experiment and gain access, called a false acceptance. Generally, systems allow for relaxing or tightening the criteria for matching the templates. When relaxed, the system is easier to use but carries the cost of there likely being more false acceptances. When the criteria are tightened, you decrease the likelihood of false acceptances but at the cost of more false rejects.

Bill Rogers, editor of *The Biometric Digest*, has some thoughts on this aspect of biometrics: Rogers: “Virtually all of the biometrics products now available allow end users to set the parameters of accepting or rejecting a live biometric. I know of a some credit unions that have used biometrics and they set up their system, initially, at a mid range, and then with trial-and-error adjusted it. How stringent or lenient you are depends on what you are dealing with. In a college meal program where the student pays for his meals with a fingerprint, if a mistake is made and the student is passed and should not have been, you’re talking about the cost of a meal. It’s nominal. On the other hand, if you’re too lax on an automobile and somebody gains access, you lost a car.”

More than in many other areas of information technology, external factors play a role in biometrics. How well users engage the system affects the system’s accuracy and performance. An improperly placed fingertip in a biometric reader can increase the probability of their being false rejects. The same is true for those with a sore throat who are trying to access a system using voice recognition. Such difficulties can affect the system’s performance as well as create user frustration. The system’s external environment may also be a factor. A system that uses hand geometry to allow access to a building may be affected by temperature or rain. Likewise, background noise can limit the effectiveness of a voice recognition system. As a result, consideration must be given to user training and the system’s environment.

Types of Biometric Technology

Fingerprints
Fingerprints are perhaps the best known biometric technology, as well as the most widely used. The technology matches the ridges and valleys that make up our fingerprints. While fingerprinting has been around for years -- as we noted, it’s been used by law enforcement for over a century -- it is not entirely straightforward. Getting a good fingerprint image can be compromised by the position of the finger on the scanner, temperature of the air, sweat on the skin and other factors. Because of all the variables involved, some systems limit the size of the area the print that’s used for matching, which reduces the chances that extraneous data, such as cuts or dirt, can cause difficulties.

IBG estimates that, by revenue, fingerprint scanning accounted for 34 percent of the biometric market in 1999. Uses for fingerprints include providing access to physical facilities, network security and e-commerce. The IBG rates various biometric technologies by cost, the effort and time required on the part of the user, accuracy at identifying individuals and intrusiveness -- how intrusive users perceive the system to be. It calls this its Zephyr Analysis, a trademarked name. Finger scanning is rated about in the mid-range for all of these variables.

Fingerprint vendors include AuthenTec (whose products include FingerLoc and EntrePad), Biometric Access (and its SecureTouch product), Mytec Technologies (which makes the BioScrypt product) and BIO-key (whose product is called WEB-key).

Hand geometry
Hand geometry, also called hand scans, involve the scanning of a person’s hand, rather than just the fingertips. The system takes a three dimensional image of a hand, focusing on finger length,

height and other characteristics. In his book, *Biometrics: Advanced Identity Verification*, Julian Ashbourn reports that some hand scanning systems measure as many as 90 parameters.

IBG says hand scans accounted for 28 percent of the biometric market as measured by revenue in 1999. It rates the intrusiveness of hand geometry as in the mid range, accuracy and cost a bit higher than average, and effort, higher still.

The Recognition Systems division of Ingersoll-Rand makes the HandReader, a hand recognition product.

Iris-scan
The iris is the colored part of the eye and is made up of a fibrous and elastic structure that's quite complex. Not only is the pattern of your iris unique to you, but your right iris has a different pattern than your left. Even the irises of identical twins differ. Irises, like fingerprints, do not to change with age.

So rich in details is the iris, IBG says the technology can identify 266 unique "spots," so to speak, as compared with 13 to 60 for some of the other biometric technologies. For this reason, iris scanning is considered the most accurate biometric technology -- and the most costly. It also, says IBG, requires a relatively high degree of effort on the part of users, while being relatively non-intrusive. John Daugman, in his article, "Recognizing Persons By Their Iris Patterns," says that the patterns of irises can be encoded from distances of almost a meter away or about three feet.

IBG reports that iris scans, in 1999, accounted for 9 percent of the biometric market as measured by revenue. Uses for iris scans include ATM machines, Internet security, entry into buildings and other spaces, computer login validation and electronic commerce.

Iridian Technologies (formerly IriScan) is a vendor of iris scanning technology, which it calls KnoWho..

Voice Scans

This is a technology that seems to labor under an unusual number of different names, including speech recognition, voice recognition, speaker authentication and talker verification. Our voices have a distinctiveness which is the result of both behavioral and physiological qualities. This technology is one of the least accurate among the major biometrics. It is subject to a number of verification errors, including misspoken words, sickness such as a sore throat, the speaker's emotional state -- stress, for example, can alter a person's voice -- environmental difficulties such as echos in a room and generally variable acoustics, and aging.

IBG says voice scans accounted for 11 percent of the biometric market by revenue in 1999, and notes that this is the least intrusive of the biometric technologies, is among the cheapest and requires only a moderate amount of effort. Uses for the technology include access control, e-commerce, automated call center applications and other situations involving remote identification verification.

Technology for voice scans is sold by T-NETIX, whose product is called SpeakEZ, and Veritel Corp. of America and its VoiceCheck product.

Signature Scans

No, this is not handwriting analysis. It is measuring how someone signs his or her name. Some of the variables measured include stroke order, speed and pressure.

Let's let Bill Rogers describe a signature scan demonstration that greatly impressed him: Rogers: "I was at a trade show last year. A gentleman signed his name to a paper on a pad that had a biometric identifier and then handed me the paper and pad, plus a clean sheet of paper over the one he wrote on, and asked me to trace his signature. I did so and when I held the two pieces of paper in my hands and looked up at them in the light, they were basically identical. However, the computer rejected my signature of his name. Why? Because I did not sign with the speed that he wrote it and I didn't use the same pressure. If a bank teller compared these signatures, with one on a check and the other on a signature ID card, the teller would have passed it, no question about it. But the computer system rejected it."

IBG reports that signature scans' market share was 3 percent in 1999 by revenue. This is considered among the least accurate of the major biometric technologies, it does not require much effort, it involves moderate cost and is relatively non-intrusive. It is useful anyplace signatures are required, such as the banking industry.

PenOp is a vendor of this technology and calls its technology PenOp Siganture Series. Communication Intelligence Corp. has a product called InkTools.

Facial Scans

Facial scanning technology really came out in the open in January 2001 when it was used by police to compare the faces of 72,000 fans who attended the Super Bowl in Tampa with mugshots of known badguys. The surveillance system, based on an algorithm originally developed at the Massachusetts Institute of Technology, was based on software from Viisage [SPELLED WITH TWO "i"s] Inc. of Littleton, Mass. As fans entered the stadium, they were videotaped and the tape was digitalized and fed into a computer. These images were then compared to thousands of faces in the database of the police. The technology measures 128 distinct facial features and translates the characteristics of a face into a unique set of numbers, which is a profile specific to each face. The National Football League knew the surveillance was going on, but the fans didn't, creating concerns among a number of observers regarding issues of privacy. The system made 19 positive IDs, but there were no arrests. The system is also used in casinos around the country to spot cheats and card counters.

While the typical person cannot consistently match finger prints or irises or even signatures, all of us make face matches virtually every day. Consider: We essentially identify who is a stranger and who is not by matching people's faces to those in our database of faces -- which resides in our brains -- and trying to make a match.

Facial scans make use of distinctive facial features or characteristics, and can overcome such distractions as facial hair and eye glasses by avoiding those parts of the face where hair and eye glasses are found. Instead, the technology focuses on those areas of the face which are less susceptible to alteration. These include the upper parts of the eye sockets, the cheekbones and the sides of the mouth.

Facial scanning, according to IBG, involves a somewhat high degree of intrusiveness and cost, a moderate amount of accuracy, while requiring relatively low efforts on the part of users. Face scans made up about 15 percent of the biometric market by revenue in 1999.

In addition to Viisage and its FacePASS product, other facial scanning vendors include BioID and its BioID Client/Server product, and Visionics, whose product is called FaceIt.

Other Biometric Technology

Biometrics include a number of other technologies, too numerous to cover here in any detail. Many are more developmental than currently practical. However, it is worth being aware of what these other technologies are. One is retina scans, which look at patterns found in the back portion of the eye where light hits. Another area, keystroke dynamics, is somewhat like signature scans, in that it looks at patterns of how people do things -- write their signature or type. With keystroke dynamics, typing rythms are studied.

It turns out that our ears have unique patterns, making them also the object of biometric measurements. Smell is one of our five senses, so it is probably logical that some work is being done on pattern recognition based on odors. Finally, the fact that some aspects of our bodies which we use for biometrics, such as our face, eyes, hands and ears, may be obscured, has helped spur interest in gait recognition. After all, people usually have to walk, and when they do, their gait is apparent and can be measured.

The Market And Costs

The size of the biometric market, like many other emerging, rapidly growing technologies, is subject to different interpretations. IBG estimates that total revenue for biometrics in 1999 were $58.4 million, and is projected to grow to $594.0 million by 2003, an annual compound growth rate of 78.6 percent. In 1999, Lehman Brothers said the industry at the time was less than $100 million, and it expected it to grow at an annual rate of 30 percent to 35 percent and to reach $400 million in five years, which would be 2004.

We spoke with Richard Norton, executive director of the International Biometric Industry Association in Washington, D.C. He told us that biometric sales at the device level with software support was about $20 million five years ago and is just under $200 million now. With growth at an annual rate of about 50 percent, he predicts biometrics will be a $2.5 billion to $3 billion industry by the end of the decade.

Costs range widely, depending on the technology. Iris recognition requires fairly sophisticated

hardware and software, while fingerprints do not. Some of the technologies require a camera, while voice requires a microphone. Norton says the industry is selling 450,000 devices a year at an average cost is $400.

Bill Rogers, how much do you think these various technologies cost?

Rogers: “From what I’ve seen, fingerprint costs vary from $100 to $1,000 per workstation. This range includes hardware and software. The hardware is pretty inexpensive. Finger scanners today are about $100. When I started my publication six years ago, they were $1,200. Voice technology will go from $75 to $500 per workstation. Signature is pretty cheap, about $50 to $500. The most expensive is iris scan which will range from $5,000 to $20,000 per workstation. I think facial recognition costs between $200 and $1,000 per workstation, with hand geometry being about the same.”

Benefits

A widely agreed upon benefit of biometrics is that it can make life easier for users. They don’t have to remember passwords and the like. But there are other benefits. Raj Nanavati, what benfits do you see biometrics delivering?

Nanavati: “For one thing, administrators can more effectively keep track of when people log on because they know that it is that person logging on. Also, you don’t have to worry about resetting passwords, and you don’t have to worry about re-administering smart cards or tokens, or anything like that.

Bill Rogers, you have some statistics on the costs of the security systems now in use. What are they?

Rogers: Today we all use security codes and PIN numbers. That raises two points: 1. What is the cost to issue PIN numbers and security codes? What does it cost to maintain passwords?. The numbers I’ve seen say that the cost of maintaining passwords ranges from $200 to around $500 per employee per year. In fact, studies of call centers have found that 70 percent of the calls they receive are password related. We can’t eliminate all of the passwords, but if we could reduce that number from 70 percent to 10 percent, that’s a substantial drop in manpower and cost.

Biometrics promises a number of benefits, including enhanced security, easier administration by companies, easier use for end-users and lower costs.

A Case Study

We spoke with Donald Smith, program coordinator in the UGA Card Support Services department at the University of Georgia, in Athens, about the university’s biometrics program. Amazingly, the university has been using biometrics, specifically hand readers, since 1972. Today, the university uses four biometrics applications.

The first of these uses hand readers with the university’s food services, a program which has

been running for nearly 30 years. Students on the meal plan are allowed to come to the food services' cafeteria and eat as much as they want and come back to the cafeteria as often as they want, making it necessary to have fairly stringent access security. Currently, over 5,000 students are on the meal plan.

The university, several years back, built a large physical activity center. It attracts between 5,500 and 6,000 users a day. It's lobby has six hand readers in its lobby, which provide access to the building via turnstiles. Donald notes that if biometrics weren't used, this building would need six attendants to check IDs, which is costly.

Over 5,000 students live in residence halls, and these facilities are also accessed only with hand readers. Finally, the statistics department recently instituted a program whereby those taking computerized tests must be verified via hand readers.

The older models of the hand readers were costing $2,100, but the new ones run about $1,600, while an outdoor model is priced at $3,200. These are all run off an RS 6000, and all the code was custom written by the university. Donald has no dollar figures for the cost of the entire system, but the campus has about 50 hand readers. The university's database contains templates of the hands of about 30,000 students, faculty and staff. Smith notes that accuracy improves when templates are matched one-to-one, rather than requiring the system to sort through all 30,000 templates, which is why a PIN number or ID card is required.

In places where security isn't very critical, such as the physical activity center, users can type in their PIN number or use their university ID card which contains a bar code to call up their template. Other places on campus where security is more of an issue, such as resident halls, students must use their ID cards. Donald estimates that, in terms of accuracy, the system is 99.5 percent accurate when it comes to false positives, which is when someone is allowed access who should not have. When it comes to false negatives -- when users are rejected by the system though they should not be -- the accuracy rate is 98.5 percent to 99 percent. Put another way, about 1 percent to 1.5 percent of those using the system are rejected when they should be accepted. It takes about two seconds for a person to use the system and gain entrance.

He notes that the enrollment procedure is critical for the system to work efficiently. If you take a little more time to get a good template and to explain the system to the user and let them try it, acceptance of the system is very good. You can do the enrollment in less than a minute, he says, but the university has decided it is worth spending a little time at the beginning, so its enrollment process takes about three minutes per person.

The Future

Bill, biometrics has been touted as becoming a major technology for some time. So far, it's still a pretty small market. You've said you think the market is almost at the point of entering the mainstream. What makes you think so?

Bill Rogers: "Several things are pushing it into the mainstream. One is that the big players are moving to create biometrics standards. When this happens, the whole business community will

sit up and take note. The first big one was Microsoft, which has announced it will introduce biometrics as a standard feature of a future Windows release.

Question: Isn't true they haven't released anything yet?

Bill Rogers: Yes, but I can't help but think they'll do something by the end of this year.

Question: What else will drive the market in the future?

Bill Rogers: Another driver is the credit card companies. They've all been running pilots using biometrics on their cards the last couple of years, Mastercard, Visa, Discover, American Express. As soon as those players come out and say, 'If you want our credit card, we need to put a biometric identifier on it,' the technology will become mainstream.

Question: What do you see as the biometrics industry will use in the beginning?

Bill Rogers: Logically, I think the credit card industry will use fingerprints, though the fingerprint will be converted to a scrambled bar code which will be on the back of the card. The next industry will be automotive. General Motors has already announced it will use biometrics, such as fingerprints to gain access to a car. I think those are the big ones who will first promote biometrics.

Question: Anything else you see driving the market?

Bill Rogers: "The Internet continues to explode and more e-commerce is going through the Internet, and financial transactions, and that's also helping to drive biometrics. And the last thing is fraud, stolen identity. That continues to grow at a fairly decent pace.At the same time, the cost of the technology has dropped dramatically. When all this comes together, biometrics will become really mainstream and I think a lot of people will sit up and say, 'When did all this happen?"

<u>Sources</u>
Raj Nanavati, International Biometric Group, 212 809-9491
Bill Rogers, The Biometric Digest, 314 892-8632
Donald Smith, University of Georgia, 706 542-5110
Richard Norton, International Biometric Industry Association, 202 783-7272