13

Biochemical Surveillance

Biometrics

1. Introduction

Humans have many unique attributes. Our fingerprints are unique and remain the same throughout our lives, as do our toe prints. Our voices have unique characteristics that can be charted and analyzed through computer processing. The retinas in the back of our eyes have unique patterns, as do the irises at the front of our eyes. As we mature, our faces take on recognizable features and proportions that remain reasonably constant through most of our lives. Each of these sets of features can be measured, stored, compared, and retrieved using computer technologies. With improvements in image processing and databases and transmission through computer networks, it becomes possible to use these characteristics in surveillance applications.

A Royal Canadian Mounted Police (RCMP) officer examines a gun for fingerprints while a large handprint adorns the wall behind his desk. [Canadian National Archives, copyright expired.]

© 2001 by CRC Press LLC

Biometric surveillance is the detection, identification, and tracking of individuals based on their unique physical characteristics or attributes such as their proportions, size, color, fingerprints, iris patterns, or voice patterns. Biometrics is an emerging technology which, with the exception of fingerprints, has only recently become commercially reliable and practical due to computer processing.

Biometric surveillance is closely allied with chemical surveillance. When investigators dust for fingerprints, they are actually depending on the adhering chemical qualities of the oils and sweat in the fingerprints to hold onto the dust to reveal the latent prints. The chemical aspects of biometrics are gradually being extended and almost superseded by visual surveillance and electronic scanning and processing systems. Fingerprint identification cards used to be created by rolling a finger in ink and pushing it against a card. New systems in which a camera or graphics scanner takes a digital image of the fingerprint and processes it directly into a database are being developed, however, and may eventually supersede traditional inking methods. Methods of dusting for prints may change as well. There may be a day when a special ultraviolet scanner locates and processes prints without dust, sending the data immediately to a central law enforcement database and transmitting back a picture of the person who left the prints.

This chapter describes some of the most common biometrics technologies that are used in surveillance and the advances in computer technology in recent years that have enhanced their effectiveness.

2. Types and Variations

The most common biometric technologies that are used for detection and identification in surveillance include

finger, thumb, and hand prints - Widely used in law enforcement and are now used for some types of banking transactions as verification systems. They are also used for certain types of federal ID cards, including Permanent Residence cards (more commonly known as green cards), and entry and exit systems in some prisons.

toe and foot prints - Used in some hospitals to provide records of newborn babies. They may occasionally be used as a substitute for fingerprints for a subject who may not have hands due to accidents or birth defects.

iris scans - Visual scans of the colored portion of a person's eye. Iris scanners can now recognize an iris at a distance of up to two or three feet from the scanning camera. The iris pattern remains constant, for the most part, from infancy to old age. These tend to be used for entry access systems.

retina scans - Visual scans of the structures at the back of the eye and generally require that the subject stand near the camera, usually with the eye resting against an eye cup. These tend to be used for entry access systems.

voice prints - Assessments of the complex patterns and characteristics unique to each person's voice. While voices create unique patterns, the variations that are possible within an individual's modes of speaking may change slightly. Excitement tends to make voices higher, illnesses may make voices scratchier or softer. While recent improvements in voice print processing have made them more practical and reliable, they are sometimes used in conjunction with other biometrics or visual identification for confirmation. Voice analysis is also used in some types of lie detector systems, to indicate stress that might indicate lying.

© 2001 by CRC Press LLC

face prints - Assessments of the complex proportions, colors, and individual features that uniquely identify a face. There are also specialized face printing systems that rely on thermography, a means of scanning the face for infrared 'signatures' rather than characteristics that can be seen with the unaided eye. Face prints tend to be used for entry access systems and are beginning to be used for video tracking systems and for transaction verification systems. Thermographic systems tend to be more expensive than visible light scanning systems. More information about thermal emissions in general is provided in the Infrared Surveillance chapter.

DNA profiles - Unique genetic profiles of a person's biological makeup that can indicate gender, familial relationships, and race, and can sometimes also provide medical estimates and other intimate information. This is such a broad and important topic that it is discussed separately in the Genetics Surveillance chapter rather than being discussed further in this chapter.

other measures - Other physiological aspects are sometimes used for detection such as height, weight, patterns of movement, and general proportions. Heart rate, respiration rate, and perspiration sometimes are also used, as is handwriting analysis. These tend to be used in more specialized scientific studies, although some retail outlets are using them to tailor clothes to the proportions of an individual using laser scans to map the shape of a body. These measures are sometimes also used to study movement in dancers and athletes and to map a person's form for the fitting of prosthetic devices.

There are two primary means of generating a biometric print, by *contact* and by *image scanning*. There are also some less common means of measuring biometrics by various attributes of a person's physiology, including electrical or magnetic characteristics, or temperature and moisture. The most common biometric indicators used in surveillance include

contact prints - Traditionally, fingerprints have been acquired by contact. The finger is inked and pressed against a surface. The same method can be used with thumb, hand, toe, and footprints. It can even be done, to some extent, with facial prints, although the process would be objectionable for most practical applications.

image scanning - This method is becoming more practical and reliable due to advances in computer technology. By scanning a retina, iris, face, or finger, it is possible to electronically measure and analyze the components that make up the person's unique features and compare the data with known parameters or individual listings in a database. The majority of new products use some type of image scanning technology.

physiological indicators - This encompasses a wide variety of biological and chemical indicators that occur as a result of a person's individual physiological characteristics and responses. Lie detector tests, for example, measure a person's stress levels by assessing heart rate, breathing, galvanic skin response, and sometimes other measures. Since physiological indicators are highly variable with a person's mood and health and since their measurement requires special instruments and trained experts to interpret the results, they are not widely used for basic identification systems. However, lie detector tests are used at times in law enforcement to confirm confessions or the veracity of evidence. *Voice stress analyzers* have been built into some software programs to provide indicators as to whether a person might be lying. While they are only somewhat reliable and are subject to expert interpretation, business negotiators have expressed interest in using these types of products for corporate surveillance.

© 2001 by CRC Press LLC

3. Context

The most common contexts in which biometrics are used for surveillance are for criminal and suspect identification (fingerprints and mug shots), entry access, and transaction verification. Thus, biometrics are primarily used in law enforcement, in the workplace, and in retail and financial centers. They are also used in more specialized laboratory studies involving anthropology, kinesthetics, and medicine which are outside the scope of this introduction but which often yield new technologies that are used in the following contexts:

law enforcement - Biometrics are used to identify suspects or individuals who may have a warrant out for their arrest. They are used to determine if a person was present at a crime scene or had contact with key items such as guns, vehicles, or valuables. They are further used to try to locate and identify kidnap victims, hostages, runaways, and victims of suicide or homicide. Forensics professionals use biometrics to reconstruct crime scenes and examine documents for fraud and forgery.

national security - Biometrics are used by customs and immigration officials and intelligence agents to identify refugees, illegal aliens, foreign spies, and potential terrorists. They are also used to facilitate border crossings and to verify authorized entrants.

entry security - Biometrics are being increasingly used to control access to restricted or hazardous areas, to special high security areas (e.g., for athletes at major sports events), to members-only areas, and to workplace buildings. They are also being used by entertainment services to expedite access for season ticket holders.

transaction verification - Biometrics are being increasingly used to double-check the identity of a person before granting permission for them to make financial transactions, such as bank machine withdrawals or purchases at a retail store with a check or credit card. This practice is particularly objectionable to many privacy advocates since an individual may have no control over what the company may try to do with personal information.

4. Origins and Evolution

The two oldest biometric identification technologies are fingerprints and mug shots. Fingerprinting have been used for over 100 years in organized law enforcement. In fact, fingerprinting may have been used for hundreds of years in Asia and was perhaps even used in ancient Egypt. It is still one of the most important verification tools in the justice system today. Mug shots have been in regular use since about the time of the Civil War.

Mug Shots

Since photography is a relatively new technology, the practice of taking mug shots is not as old as the practice of taking fingerprints. However, mug shots appear to have been introduced to western law enforcement as a regular practice a little earlier than fingerprints and 'wanted posters' with hand-drawn mug shots were being created by portrait artists long before photographic mug shots were available.

As has been described in the introductory chapter to this book, Allan Pinkerton, the founder of Pinkerton's Detective Agency, was the first to develop an extensive collection of mug shots based on drawings, descriptions, posters, newspaper clippings, and any other sources Pinkerton's agency could find that would aid in identifying the subjects of their investigations or criminal suspects. Pinkerton was active in President Lincoln's secret service during the

© 2001 by CRC Press LLC

Civil War and returned to his private practice after the War, continuing to extend and expand his manual database of criminal suspects. Soon many law enforcement agents were actively adopting the practice of using mug shots, and by the middle of the 20th century, the practice was widespread and routine.

The Origins of Prints as Identification Marks

In 1880, an influential article appeared in Nature magazine, a reputable scientific journal. The article titled "On the Skin-Furrows of the Hand" was written by Henry Faulds and describes how he noted impressions in pottery that led him to examine the fingertips of humans and monkeys. Faulds reported on how he began collecting fingerprints from people of different nationalities and of both genders, looking for contrasts and similarities. The article also described how to take a basic print. When he was in China, he heard that criminals there had "from early times" been made to provide impressions of their fingers "just as we make ours yield their photographs." He reported that "Egyptians caused their criminals to seal their confessions with their thumbnails, just as the Japanese do now...." He describes his initial observations as a "rich anthropological mine for patient observers." Faulds article was a catalyst for further discovery and many modern practices.

Faulds was not the only observer intrigued by fingerprints. W. J. Herschel responded to Faulds' article by publishing a response in the 25 November 1880 issue of Nature magazine describing how he had been taking 'sign-manuals' comprising 'finger-marks' for over 20 years and introduced them "for practical purposes in several ways in India with marked benefit." Herschel reports having introduced fingerprints for pensioners lacking in vitality and for prisoners entering the jail. Reported Herschel, "The ease with which the signature is taken and the hopelessness of either personation or repudiation are so great that I sincerely believe that the adoption of the practice in places and professions where such kinds of fraud are rife is a substantial benefit to morality." Herschel further pointed out that fingerprints remained unchanged over time.

It took a while for fingerprinting concepts and methods to become firmly established in law enforcement, but by the 1920s, the Federal Bureau of Investigation was collecting fingerprints, and by the 1930s there were good references describing the art and science of taking prints and the practice was rapidly spreading.

Polygraphs

Humans have long tried to find ways to get people to tell the truth. In earlier times, beatings and torture were sometimes used in attempts to extract information or truths. By the early 1900s, inventors were looking for more humane and effective ways to harness new technologies to determine if people were telling the truth.

Different aspects of a person's physiology were studied, including breathing, heartbeat, and perspiration and sensors were developed that could detect and measure these phenomena. The polygraph machine, which incorporates these physiological sensors and creates a visual readout on a piece of paper or, on modern versions, on a computer screen, was first developed by John Larson and Leonard Keeler.

Using the readouts in a structured situation, with general questions asked at the beginning to establish a baseline, a person's reaction to the target questions can be evaluated by a qualified examiner.

Modern Fingerprint Methods

Since dark, clear prints were desired in most instances, fingerprints were taken with a variety of types of inks (sometimes using conventional stamp pads). Ground carbon particles

© 2001 by CRC Press LLC

in a fluid medium were commonly used. These were effective in creating a clear print, but were somewhat objectionable to the person providing the print.

Dusting for fingerprints is an art that takes special fine dusts, high quality brushes, patience, practice, and skill. Inventors were looking for means to find and image prints that didn't require dust and gradually, as technology improved, were beginning to have some success. By the late 1970s, scientists were beginning to explore lasers as a means of finding latent fingerprints and by the 1980s, they had discovered ways to reveal 'difficult' prints, prints on paper and other materials that could not be readily revealed with traditional methods.

Many people object to the mess and inconvenience of getting ink all over their hands when providing finger or handprints and for many years, scientists had been seeking ways to get clear fingerprints without the staining and odor associated with traditional carbon-based inks. Some low-carbon systems had been developed over time, but these were not yet truly 'inkless' systems. However, new methods of using light scattering were being developed that would begin to supersede traditional methods in the 1980s and 1990s.

As video technologies improved, the quality and resolution of charge-coupled devices (CCDs) made it more practical to implement fingerprint scanners based on the reflectance and/or scattering of light from the image of a finger pressed against an image sensor. Some systems even incorporated the unique pressure patterns of a person's finger in addition to the ridges and groove patterns.

The 1980s - The Development and Testing of New Technologies

In the late 1970s and early 1980s, new miniature electronics and microcomputer technologies enabled many new inventions to be developed and some of these technologies were applied to the development of innovative biometric detection devices and database systems.

Some specific examples of new technologies that were introduced around this time include

- In 1977, Robert Hill of Washington State, submitted a patent for identifying individuals according to the vascular patterns inside their retinas. The system was based on scanning the eye in a selected pattern and analyzing the light that was reflected off the retina, thus revealing the patterns of blood vessels at the back of the eye, which are unique to each person and to each eye.
- In 1981, Feix and Ruell of Siemens Corporation submitted a patent for a combination voice signature and facial recognition system in which a key word spoken into a microphone could be compared to a pattern matcher in a database to form a 'familiarity score' aiding in identification.
- In the early 1980s, the Japanese National Police Agency established a computerized retrieval system for fingerprint files which has been used as a model by a number of American police agencies. Various state agencies in the United States were implementing similar systems.
- By the mid-1980s, some law enforcement agencies were beginning to switch over from manual fingerprint systems to automated fingerprint systems that scanned or otherwise electronically imaged or recognized a fingerprint. Palmprint systems were starting to become practical around the same time. Computerized systems could be linked to a central electronic database.
- In 1985, Leonard Flom and Aran Safir submitted a patent application for an iris iden-

© 2001 by CRC Press LLC

tification system in which an image of the iris and the pupil could be compared against stored image information. This appeared to have several advantages over retinal identification. Not only was the iris pattern not as dependent on pupil size that could obscure the retina, but it was not necessary to put the eye as close to the scanner as in retinal scans.

- In 1988, Laurence Lambert, in association with the U.S. Secretary of the Air (Washington, D.C.) submitted a patent for an autonomous face recognition machine. This was a design for a system capable of locating faces in video scenes with mixed/random content and of identifying those faces. This automated system could function without human input or intervention and was not disrupted by scale, brightness, or general discrepancies in focus. The system could be interfaced with motion detection features to improve recognition time to within about a minute.

In the early 1980s and through the 1990s increasingly sophisticated ways of processing latent fingerprints have been described in the scientific literature. In the past, prints on paper or other rough or absorbent materials were difficult or impossible to reveal. Now it was becoming possible to bring out prints in new ways. New magnetic and fluorescing powders were gradually being developed.

The 1990s - Proliferation of Biometrics Systems

Biometrics systems became practical and less expensive in the 1990s and companies began heavily promoting the products to government agencies, financial institutions, corporations, and retailers.

The 1990s is characterized by the improvement of many of the basic technologies developed in the previous two decades and by commercialization. It was also a time when organizations such as the FBI, NIST, and others began to develop standards for fingerprint digitization and compression. Some examples of improvements and practical applications include the following:

- In 1991, John Daugman of Iri Scan Incorporated submitted a patent for an iris analysis system based on using the eye as an 'optical fingerprint,' thus introducing biometric identification systems that were more resistant to forgery than traditional systems. This system improved on previous systems and provided greater automation.
- In 1993, the Immigration and Naturalization Services (INS) began establishing a *Passenger Accelerated Service System* (INSPASS). This program used biometric technology to inspect frequent travelers who carry a special card after enrolling in the program.
- In the mid-1990s, traditional and electronic identification programs were upgraded or enhanced by the U.S. Department of Justice (DoJ). These included the INS *Automated Fingerprint Identification System* and the *Computer-Aided Detection and Reporting Enhancement System*, initially installed in Texas and California. These upgrades were put into effect to improve remote-sensing capabilities and electronic surveillance of the southern border.
- In the mid-1990s, a number of entertainment complexes were beginning to use hand scanners to expedite admissions and to monitor employees and season pass holders.
- At a hospital in Temple, Texas, a new system was put in place so that physicians could access the hospital's electronic medical record system and other computer applications by using a biometric fingerprint scanner. Users indicated that the bio-

© 2001 by CRC Press LLC

metric access was more convenient than remembering a password. The system also provided tighter security and accountability, since the identity of the person typing a password could not be traced as readily to a specific individual as a biometric identifier.

- Iris scanners were also beginning to be used at high-level sports events, like the Nagano, Japan, Winter Olympics where they were used to control access to the rifles used in the biathlon competition.
- Throughout the 1990s, U.S. Customs and Immigration Services continued to explore the use of a number of biometrics systems to expedite border access, including voice recognition and hand scanning and several systems have been tested and some implemented for these purposes. In some cases systems are used together, such as a hand-scan verified by a voice print.
- In 1996, Penine Katz from MCI Communications filed a patent for a telephone-based personnel tracking system which could detect personal identification codes and automatic number identification on incoming telephone calls. The system is designed to create a report of the incoming calls that includes the location of the calling telephone and the person making the call. One of the stated objects of the invention was to use voice recognition to recognize a caller's voice and spoken commands and to match the voice to the caller's identity through voice print matches. The intention of the system was to monitor and record the arrival and departure of field-based employees but clearly the technology is generic enough to be used in many types of telemarketing and technical support applications.
- In the U.K., some automated teller machines (ATMs) have been equipped with iris scanners. These are generally less objectionable to users than retinal scans, as it is not necessary to put the eye against an eye cup in some iris systems. Some of the newer systems can register an iris up to a couple of feet.
- In 1998, the U.S. Immigration and Naturalization Service (INS) installed hand scanners in a number of airports in the United States and Canada. These systems scan a hand and match it with entries in an INS database, expediting passage through the checkpoint.
- In June 1998, the National Highway Traffic Safety Administration (NHTSA) issued proposed regulations to require all states to include social security numbers and security features like biometric identification on drivers' licenses by a specified deadline.

The Motivation for Biometrics Surveillance

Fraud was one of the biggest reasons why the demand for biometrics identification systems increased. The fact that the technology was becoming more powerful, more reliable, and less expensive was also a motivating factor.

Check fraud losses to retailers and financial institutions were estimated to be around $10 billion a year by the mid-1990s. Welfare and insurance fraud was also prevalent, particularly medical insurance fraud. One of the ways in which people were defrauding welfare and insurance providers was by using multiple identities. The use of advanced copier machines to counterfeit negotiable notes (checks, food stamps, coupons, etc.) was also increasing. Discovery and conviction rates for these crimes had traditionally been low.

Signature verification has traditionally been used to verify contracts, documents, and ne-

© 2001 by CRC Press LLC

gotiable items, but signature verification and handwriting analysis are hit-and-miss. Not everyone is good at interpreting or recognizing signatures, not everyone writes his or her signature consistently, and many cashiers simply fail to check the signatures on checks and credit cards.

Biometrics was seen as a way to deter fraud, as well as a way to detect it once it had occurred, to apprehend the perpetrators, and to prove the fraud.

By the late 1990s, a number of banks began using fingerprint identification systems for noncustomers depositing or cashing checks.

A further reason for promoting biometrics identification was the increasing prevalence of electronic transactions. Through computer networks, it was possible to create contracts and enact financial transactions, but it was difficult to authenticate the source and signer of these documents. Because of the potential for profit that is inherent in being able to conduct transactions very quickly, business agents wanted ways to bypass signatures that had to be sent by courier or postal service. Developers and e-business proponents saw biometrics as a possible solution to these problems.

One final motivation for the promotion of biometrics technologies was simple entrepreneurial opportunity. If new products became available and sales representatives could convince companies to buy them, there were opportunities to make a profit.

Concerns About Privacy and the Potential Abuse of Data

The three biggest concerns of privacy advocates are loss of freedom and anonymity, commercial exploitation of intimate knowledge about an individual without his consent or knowledge, and changes in the purpose for which data were originally collected. In the 1990s, there were many, many examples of apparent abuse and overstepping of the original mandate for collecting biometric information, giving genuine cause for concern.

There isn't space to detail the many examples of privacy rights violations which are associated with biometrics or computer databases that have occurred over the last few years. Some of these have been mentioned in other chapters and others can be referenced from the resources listed at the end of this chapter. For the purposes of illustration, just one example is given here, and a few others are mentioned in Section 9 (Implications).

In June 1997, the Secretariat for Criminal Justice Coalition in Australia sent a strongly worded complaint to the New South Wales (NSW) Ombudsman Office entitled "Against Department of Corrective Services Biometric Scanning of Visitors, Workers & Children." The complaint was specific to the "Implementation of Biometric Fingerprint Scanning in NSW Maximum Security Prisons." NSW had implemented the biometrics security system in all maximum security prisons after reviewing voluntary visual identification systems while engaging with discussions with the Privacy Committee in 1995.

Without further substantial discussion or endorsement from the Privacy Committee, however, biometrics scanning technologies were introduced into the prison system in 1996. This incident is illustrative of many political and institutional developments in which systems are installed with a minimum of public interaction or approval or in which the stated objections and the discussion process are bypassed or overridden in favor of installing the technologies. Part of the controversy surrounding this case stems from the fact that the system was initially stated to be a voluntary means of facilitating the visitation process, but it was found that once the units were installed, the emphasis appeared to have shifted to using it as a means of preventing escape.

There have been many situations in which the original intention and mandate in installing

© 2001 by CRC Press LLC

a system changed after installation without a process of discussion or approval. Thus, privacy advocates are not so much opposed to the technologies themselves as they are to the ways in which they are sometimes used.

5. Description and Functions

Fingerprints as a Preferred Identity Tool

Fingerprint technologies form the greatest proportion of biometric identification and surveillance devices. Fingerprints are considered to be unique and essentially unchanging throughout a person's life (except for changes in size during the growth period of childhood) and stable except for unusual accidents or dismemberment. It is difficult to remove or fabricate fingerprints and those who make the attempt usually fail or cause themselves unnecessary pain or disfigurement. For these reasons, fingerprints are favored by many organizations as an identity marker or tool of surveillance.

Fingerprints can provide information about a person's whereabouts, activities, and identity. This information has been used to verify identity for drug testing, financial transactions, insurance applications, scholarship exams, or job applications. It has also been used for locating and convicting criminals, finding missing persons (especially young children or individuals with amnesia or mental illnesses), or detecting and verifying tampering or fraud.

The primary means of detecting fingerprints at crime scenes is with specialized dust. The primary means of using fingerprints for verification or access is with inked systems, but inkless systems and computer image scanning systems are becoming more prevalent.

Fingerprint Acquisition and Identification

Fingerprinting is an important investigative tool and means of documenting a person's presence at a particular location. Because fingerprints are widely used in security and crime investigation, there are many products for processing prints and even some that increase the likelihood of prints being left behind.

Human skin is constantly excreting fluids and moisturizing itself with body oils (oils may also adhere from touching hair) and these fluids and any dirt or residues from the hands (or feet) may stick to surfaces when they are touched. The prints are often found on doorknobs, windows, flashlights, electronics devices, and steering wheels. Glass and metal surfaces tend to hold prints better than coarser, more porous surfaces like fabric or paper.

There are five general aspects of fingerprinting: 1) acquisition, 2) detection, 3) matching/identification, 4) preservation, and 5) database indexing (for storage and retrieval). Chemicals are particularly important in acquisition and detection, and somewhat important in preservation (usually in cases where manual rather than computerized systems are used).

acquisition - Fingerprints are commonly acquired for routine records, for ID cards, for preventive identification records, and for investigations. Examples include bonded and security personnel databases; passports, visas, or resident identification cards; police booking procedures; tampering evidence; those at-risk for child kidnapping or elderly wandering. For acquisition, the emphasis is on getting good quality prints that are clean and clear and which last long enough for the application at hand. 'Inkless' systems are now available as well. Specially designed chemical fingerprint pads, inks, and papers are available for this.

detection - Fingerprint detection commonly occurs when investigating tampering and crime scenes and, to a lesser extent, when checking ID against the person carrying it.

© 2001 by CRC Press LLC

Fuming may also be carried out to reveal latent fingerprints. In the case of tampering or crime investigation, ultraviolet lights, detection powders, photographs, and fingerprint dusting are commonly used with appropriate chemicals and chemical sensors.

matching/identification - In the case of fingerprints, matching and identification are usually carried out visually or with computerized surveillance aids. Chemicals are less important than visual surveillance technologies for this step in the process.

preservation - The preservation of fingerprints provided voluntarily or taken during bookings ideally requires good quality, permanent, indelible inks stamped on acid-free archival papers or cards kept in storage facilities that are temperature-regulated and safe from fire and moisture. In the case of ID cards that are renewed every few years, lamination is usually sufficient to preserve the prints. The preservation of prints found in an investigation may involve photographing the source of the prints, dusting them for better visibility, acquiring them with tape, bagging specific objects that hold prints (guns, phones, knives), sealing the prints with a plastic coating, and photographing the prints themselves or scanning them into a computer matching system/database. Chemicals are most often used in coating and storing the sources of the prints if they are to be held for some time and, of course, in any photographic processes associated with recording the prints.

indexing, search, and retrieval - Traditionally, fingerprints were kept on cards or in files containing objects and envelopes in banks of filing cabinets. One national repository alone includes about 34 million sets of prints stored this way. Increasingly, however, prints are being scanned into computers and retrieved electronically. Sometimes computer matching and identification software is included to aid in narrowing down searches or developing candidate lists. Chemicals are not a direct aspect of computer databanking, but the quality of the prints created with chemical inks and latent print processes will influence the quality of the images available in the computer database and should be processed with the utmost attention to quality. It is also important, whenever possible, to preserve the original evidence in case computer data are compromised or destroyed.

Patent prints are those which are somewhat obvious and *latent* prints are those which are difficult to see or detect without technological aids such as chemicals or image-processing systems.

Because fingerprint analysis is central to many crimes, criminals have sought many ways over the decades to remove prints or to prevent their impressions in the first place. The most common and obvious way is to wear gloves. Sometimes thieves will wipe down surfaces to remove prints and some, like auto thieves, will take what they want and then burn the rest to remove evidence such as prints, hair, and skin. Some people have attempted to hide their prints by attaching 'fake prints' made from flexible molded materials. Others have worn 'chemical gloves' to reduce the chance of leaving prints. Some have even taken extreme measures by surgically or chemically removing the skin on the tips of their fingers. This doesn't always work. The cracks and indentations peculiar to scar tissue, in cases where surgery didn't work well, can be just as unique as an actual print.

Inked and Inkless Systems

Fingerprinting has traditionally been carried out with carbon-based inks, usually supplied in the form of specialized stamp pads. The disadvantage to this system is the objectionable soiling that occurs on the body part subjected to printing, especially in the case of hand and foot prints.

© 2001 by CRC Press LLC

Other types of 'inks' in the form of leuco dyes have been tried; they prevent staining, but are not as permanent of some sorts of traditional black inks.

Inkless systems now exist. Most of these require two steps to process the prints. In the first the fingers (or other body parts) are coated with a chemical reagent, then a developing reagent is applied to the medium on which the prints have been applied to darken the surface. This involves more work for the person collecting the prints, but is still favored where good taste or diplomacy in the matter of soiled limbs is considered best. Unlike inked prints, the person being printed must wait until the processing is complete to make sure the prints are good and don't need to be repeated. There is a higher chance of chemical allergies by sensitive individuals taking the prints than with inked systems.

Inkless systems that use a thermal rather than a chemical process have also been developed. Thermal systems have some drawbacks. Specialized paper must be used, to some it has an irritating texture, and it tends to curl and fade, depending on the brand. Some people are sensitive to the slight odor that occurs during thermal processing.

Visual scanning systems now also exist. These are similar to the image scanners that are used for computer graphics applications. Software to detect and analyze the prints varies widely in the ways in which prints are analyzed, but some analyze up to as many as three dozen characteristics of an individual print.

In September 1998, D. Arndt filed for a patent on behalf of Identicator, Inc. for an inkless system based on alcohol-soluble dyes dissolved in fatty acid esters, which could be produced in a variety of colors. This very-low-stain fingerprinting ink can be made resistant to fading.

Computer Analysis and Identification Systems

Computerization of fingerprint databanking and analysis is an important evolution in the technology of fingerprint science.

There have been a number of computerized systems suggested and developed to speed up the process of finding matches between a reference fingerprint and prints stored in an electronic database. With databases increasingly being linked across the country, the number of possible matches greatly increases and it is not humanly possible to individually search millions of prints, even when they are broken down into categories. Given that there may eventually be a national electronic database of prints that exceeds 50 million entries, obviously some type of automation is desirable.

Computer imaging and the cataloging of visual information have a lot of things in common with robotic vision systems. Image recognition is based on different ways of analyzing the data, including an assessment of attributes such as:

- the proportion of light and dark,
- the complexity of the overall image or parts thereof,
- the direction of the lines, and
- the proportion of verticals to horizontals (or diagonals).

Some computer systems even measure the amount of pressure exerted from the finger being printed.

The process of recognizing a print can be mathematically symbolized with numbers that are based on these attributes. If the numbers are the same, or nearly the same, a list of close matches can be generated. The process is similar to using a search engine. If the user is getting too few near-matches and is not finding the desired data, the search can be expanded to generate more 'hits.'

© 2001 by CRC Press LLC

Similar computer algorithms are used in fingerprint (or handprint) identification systems for access surveillance in which the person gains authorized access by placing part or all of the hand in a computerized scanning device that checks the print against a list of authorized users before allowing a doorway to be entered or exited.

There are two basic ways to store visual information as computer image files, *raster* and *vector*. There are electronic fingerprint systems based on both formats. Some systems will delete the image file, for security reasons, after it has been mathematically coded.

A raster image is typically displayed as dots, pixels, or discrete units of information. In raster storage formats, there is no data relationship assumed between one pixel and those which are adjacent (except for purposes of compression). However, the relationship of dark and light pixels *is* of interest for matching purposes because it aids in determining a pattern or similarity. Raster images of sufficient resolution to provide a really good image of a print can vary from 500 kilobytes to 2-3 Mbytes of data storage.

Lossless compression formats (those which don't average or extrapolate the data when being compressed or decompressed) are preferred for data storage of images that must be exactly the same each time they are retrieved or analyzed. Tag Image File Format (TIFF) is a robust, well-supported, lossless professional graphics format that is preferred for many types of raster image storage and display applications. TIFF files can be reduced in size using LZH compression without loss of visual information when it is decompressed. Lossy compression formats (those that lose information) are sometimes used, with wavelet algorithms appearing to provide some of the best 'recovery' from lossy data. Raster formats do not magnify well due to their structure. Grayscale images are usually preferred over black and white (line) images because they improve the 'perceptual' resolution of the image. Scanners and printers typically use raster systems.

A vector image is one that is composed of lines that are mathematically defined. If you take a circle defined in a raster file and magnify it, it will look coarse and blocky, because there is no information in the file to explain how to fill in the extra pixels when there are more of them. In contrast, if you take a circle defined mathematically and display it at 600 dpi (the resolution of most commercial printers) it looks pretty good. If you double the size, it looks even better. If you blow it up to the size of a room (assuming you have a big enough plotter or printer), it still looks smooth and round. This is because the program is generating the circle 'on the fly' from a mathematical formula for a circle at whatever is the best resolution of the output device, no matter whether it is a handheld electronic notepad or a 20-foot billboard.

Mathematical comparison of vector-format prints can sometimes be more efficient than raster-format prints for quicker search and retrieval. It depends on the system and the nature of the data. Adobe PostScript is an example of a vector format which is used to render images and fonts. CAD programs for design and drafting also use vector formats. Plotters typically use vector systems such as PostScript or HPGL.

Both raster and vector systems exist for computerized fingerprint identification and matching systems. Each method has its advantages. The jury is still out on which will eventually be found to be most practical and powerful for the job, but it's possible that vector systems may have a slight edge in the long run for actual search and retrieval and data storage, and raster systems may continue to be used for printing or displaying the images.

© 2001 by CRC Press LLC

6. Applications

6.a. Examples

A few examples of biometrics systems were described earlier in the chapter, in Section 4 (Origins and Evolution). Some others in current use include

- In Texas and Arizona, public assistance and food stamp applicants are fingerprinted using a computerized electronic finger imaging system. The scanner records the finger image of the index finger of each hand and compares them to images stored in the client database. Portable versions exist to service homebound clients. The program was instituted to deter multiple enrollments.
- In Canada, Citibank and Metro approved a finger scanning system called the Client Identification and Benefits System (CIBS) for business transactions and secure access to benefits. This system takes a finger scan, converts it to digital format, encrypts the data and stores the biometric record, destroying the original image scan to secure the data from visual 'snooping' or duplication.
- Since 1990, the Cook County, Illinois, Sheriff's Department has been using retinal scans to scan prisoners for identification and monitoring purposes. The scanning system is linked with a database of more than a quarter million reference patterns.
- In 1997, initiatives for developing computer-based generic biometric applications programming interfaces (APIs) resulted in the announcement of the Human Authentication Application Program Interface (HA-API), developed by the National Registry and the U.S. Department of Defense.
- In 1999, Fairfax County, Virginia, police and sheriff's officers began using technology that combined electronic fingerprint identification with digital facial image. The system is intended in part to help identify suspects who use numerous aliases and also to cut down on lengthy searches through manual 'mug shot' books.

The FBI has been working with West Virginia University to offer degree programs in forensic identification, in areas such as fingerprint and biometric technologies. The *International Association for Identification* will require that persons employed in forensic identification have a bachelor's degree, to take effect by the year 2005.

6.b. Equipment

There are hundreds of commercial products for providing biometric access to buildings, machines, and services. Here is just a small sampling to provide an introduction to the depth and range of commercial products.

Finger Imaging Recognition

APrint™ *HoloPass*™ - Advanced Precision Technology Inc. uses patented holographic optics to produce images for one-to-one verification and one-to-many matching.

Fingerprint Identification Unit™ (FIU) - Sony software with 56 and 128-bit encryption Third-party vendors have used the system as a basis for developing computer logon systems, smart card terminals, and physical access controllers.

IriScan and GTE are creating biometrically secured electronic commerce transactions. They are working on prototypes of Iris Certificate Security (ICS).

Puppy™ *Secure Biometric Logon System* - A Windows NT™-based biometric fingerprint logon system.

© 2001 by CRC Press LLC

In order to effectively capture the fine details of a fingerprint, they are usually scanned at resolution of at least 500 dots per inch and saved in compressed formats.

Fingerprint scanners use a variety of software algorithms to analyze and identify the users. Some even measure the pressure of the finger against the scanning mechanism. Hand scanners (shown here as a conceptual drawing) are less common than fingerprint scanners. [Classic Concepts photos ©2000, used with permission.]

Voice Recognition

SpeakEZ Voice Print℠ - A voice verification technology which can be used with financial systems, building access devices, and wireless and wired telephone services.

biometric border control system - This is installed at Scobey, Montana, on the Canadian border uses a magnetic stripe card to identify themselves combined with a voice verification through a telephone handset.

The Rensselær Polytechnic Institute has developed a voice-activated lock for doors for high-security areas.

Face Recognition

FaceIt™ - by Visionics Corporation. This is facial recognition software that can be built into a variety of applications to rapidly detect and recognize faces. It is a software development tool designed to be scalable and adaptable to a range of software products. It is capable of recognizing single or multiple faces and functions in one-to-one matching or one-to-many matching modes. It is also capable of following faces and isolating them for tracking purposes. FaceIt creates a digital template unique to an individual and compresses the data down to about 84 bytes for storage and retrieval and degree of similarity to images in a stored database.

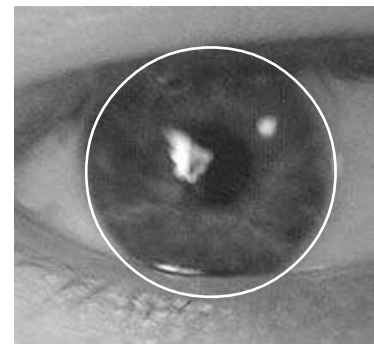
TrueFace™ Access - by Miros, a division of eTrue.com This is facial recognition software certified by the International Computer Security Association. TrueFace ID identifies a person's face from image files or surveillance video when compared to images in a database. TrueFace Network is client-server software that provides secure access to server data using face and/or finger verification.

The Central Intelligence Agency (CIA) has been involved in the development of a number of biometric identification systems for use by federal agencies. Much of the information on these technologies is classified, as is biometrics technology developed by the U.S. Department of Defense.

© 2001 by CRC Press LLC

Eye Recognition

The human iris, the colored portion of the eye surrounding the pupil, is unique to each individual and to each eye and remains stable from infancy to old age, thus making it suitable as a biometric identification tool.



The human iris, the colored portion of the eye surrounding the pupil, is unique to each individual and to each eye and remains relatively stable from infancy to old age, thus making it suitable as a biometric identification tool. Looking into an iris-scanning device is less inconvenient, in most cases, than looking into a retina-scanning device as the subject doesn't have to be as close to the scanning mechanism. Newer systems that use narrower wavelength light beams can be designed to be less disrupted by reflections that may be caused by glasses or contact lenses. [Classic Concepts ©2000 photo, used with permission.]

eyescanning ATM technology - Sensar was demonstrated at the 1997 Banking Administration Institute Conference. When a banking customer puts in an ATM card, the stereo camera locates the face, finds the eye, takes a digital image of the iris at distances up to three feet, compares the captured image to one on file with the bank, and rejects access if there isn't a match. It works with glasses, contact lenses, and at night. No beam is shone in the clients' eyes, passive technology in the form of a zooming camera is used.

Motion Recognition

IBM - Clients sign with a pen measuring speed, pressure, and direction of movement which goes beyond just the shape of the signature (which can be forged) to measure several attributes, making forgery virtually impossible.

There are also systems which will monitor eyeblinks to determine if a subject may be lying or evasive or to determine if an employee is getting fatigued and should perhaps be rotated on a production line or removed if working with dangerous equipment.

Multiple Features Recognition

Digital Justice Solution™ - By Printrak International Inc. combines realtime automated fingerprint identification, computerized criminal history, a mug shot, and document storage and retrieval capabilities. The system can also be used to identify latents prints lifted from crime scenes, comparing them against almost a million records on file in the Louisiana system.

© 2001 by CRC Press LLC

*e*PICS*™ - By Electronic Identification, Inc., this uses a digital camera and ultrasonic fingerprint read integrated into a Web-enabled workstation. The data are converted into a digital signature using proprietary, patented software compression technology and burned into a chip to create an ID card with the digital profile printed on the face of the card. The card works with e*PICS authentication readers.

layered biometric ATM - Diebold, Keyware Technologies, and Visionics - Uses speaker verification and face recognition to process transactions without the use of a PIN or password.

SPIKE™ *Suspect and Prisoner Identification Key Evaluation System* - Combines face recognition, voice verification, and AFIS (Automated Fingerprint Identification System) fingerprint verification. Developed for use by law enforcement agencies. Incorporates a computer, high-resolution digital camera, directional microphone, and fingerprint scanner. Integrates with SPIKENET™ Internet connectivity.

Traditional lie detectors are systems which are designed to monitor a number of features including galvanic skin response, heart rate, etc.

Fingerprint Collection and Detection

Fingerprint kits vary in portability, quality, and ease of use. They are also somewhat dependent on the skill of the person taking the prints. Consequently, practice cards and training videos are supplied by many of the major vendors. Kits may be intended for printing just a single finger (as in the ones often used by banks), or may be designed for printing all digits or even palm or foot prints. When printing larger areas, it is sometimes necessary to have a thin foam layer under the printing card in order for the surface area to evenly contact the card. This is supplied with many of the kits for palm or foot prints. The cards used for storing the prints are designed accordingly.

Fingerprint kits are commonly of inked (stamp-pad style) or inkless types. Inkless kits are convenient to the fingerprintees since most people find ink on their fingers objectionable. Many systems require cartridges or inking pads to be periodically replaced, usually about every 500 to 1500 inkings or so.

The Collection of Fingerprints

A basic stamp pad system and archival card can be as inexpensive as a few dollars and may be suitable for ID cards or temporary records, but might not meet standards for crime investigation evidence.

Specialized inks, designed to provide a finely textured, detailed, dark print are sold in containers of various sizes and shapes. Federal bureaus use them for ID cards and banks sometimes use the small round ones for signature ID prints on negotiated checks, usually third-party checks or checks cashed by customers without accounts at the cashing agency (banks, casinos, money depots). These vary in price from a few dollars to $80 or so, depending on the quality of the ink, the number of impressions, and the types of ink.

Compact inkless fingerprint pads are about $600 with replacement cartridges about $80 to $200 each depending on the number of impressions.

Identification kits, sometimes called portable fingerprinting stations, containing cards, ink or inkless chemicals, sealers, and other accessories can be purchased in various configurations for about $120 to $300.

Special-purpose kits, designed to take prints from people with arthritic or differently shaped fingers, or from cadavers, are also available in about the same price ranges as regular kits.

© 2001 by CRC Press LLC

The main difference is that there is usually a spatula or spoon-like implement included for rubbing against a curved surface to get the print.

Shoe kits to record shoe tread patterns (or telltale shapes in other objects) are sold for about $200 and are valuable for scanning into a computer or saving in a file so that the original shoe doesn't have to be pulled out each time and so that unimpounded shoes (e.g., other suspects) can be referenced later, if needed.

Latent Prints

There is a lot of chemical science involved in the acquisition and processing of prints and they can't be covered in detail, but a sampling of chemicals and techniques is described here. (If you want more information on this important and interesting aspect of biochemical surveillance, there are numerous bibliographic references at the end of the chapter and a good reference Web site at SCAFO mentioned in Section 10.e. Media Resources.)

There are now a variety of types of fingerprint dusts that are used to reveal latent prints on windows, jewelry, firearms, the handles of cars and other objects, including magnetic dusts, colored dusts, and dusts that fluoresce when exposed to ultraviolet light. Sometimes chemical fuming helps to bring up prints. Some of the more recent innovations include lasers to reveal latent prints without dust. [Classic Concepts ©2000 photos, used with permission.]

'Dusting for prints' is the aspect of fingerprint detection most familiar to the general public as it is frequently shown in TV shows and newscasts.

Latent fingerprints may not be visible to the unaided eye. The use of dusts, magnifying glasses, and fuming agents may aid in revealing or further developing prints so they can be seen and processed.

Dusting Powders

Fingerprint detection and collection are intrinsic aspects of crime scene investigation. Many convictions have been based on fingerprint evidence.

Fingerprint dusting powders come in nonmagnetic and magnetic varieties. When they are being photographed, prints on a dark background show up better with a light dust and prints on a light background show up better with a dark dust. To accommodate differing needs, powders are available in a variety of colors, commonly black, white, and metallic shades. For prints that are going to be lifted with tape and placed on a card for examination and filing, dark powders are favored. Bichromatic™ is a commercial product that combines black and sliver-gray powder which tends to look lighter on dark surfaces and vice versa and is a practical solution for some types of situations.

© 2001 by CRC Press LLC

Powders are typically applied with soft, wide, hair or fiberglass brushes that resemble makeup brushes. Powders should be fine and loose, designed for the purpose. Dessicant packets or rice grains can be used to help prevent moisture from clumping the powder. Small ball bearings are sometimes used to help break up the clumps. Powder is built up gradually in fine layers, as it is hard to remove it, if there is too much, without damaging a print. A light touch is important. It is also important not to spread too much powder around as it might contaminate other aspects of a crime scene.

Magnetic powders are less often used but are suitable for use on shiny glossy coatings, plastic containers, and bags, etc. A special applicator is used with magnetic powders. The applicator is lightly moved over the surface with the prints without touching the surface being dusted. Excess particles can be returned to the container.

Tapes

Specialized clear tapes are used to 'lift' and preserve many types of evidence including blood smears, paints, spills, and fingerprints. Once a print has been made more visible with a powder, adhesive tape or precut strips can be placed over the print, pressed gently, and placed over a non-acidic card or paper to protect the image on the tape. This takes practice. The tape must be large enough to cover the area to be lifted and must be laid down gently and evenly so as not to create creases in the tape or distort the image by adhering part of it and then accidentally pulling on it. Then the correct amount of pressure must be applied. Too much pressure can 'squash' a print. Too little can cause some of it to remain on the original surface and the odds of correctly lining up the tape a second time to get the rest of the print are almost zero.

Graphic artists who have done a few years of 'table work,' that is, a lot of drawing, ruling, inking, and film handling, usually have the hand-eye expertise to dust and lift prints. It requires patience and a steady hand for best results and considering the importance of this type of evidence, it should be handled by an expert.

Print-Gathering Supplies

Fingerprint Dusts and Brushes

Camel-hair and fiberglass brushes are preferred by most professionals. Take care not to use a poorly bound brush that loses bristles. Wide, soft brushes are preferred. The bristles of the brush should not be handled, to avoid picking up oily finger residues. Tap excess powder into a dish or the powder container before applying to the surface and build up layers gently, taking care not to apply too much (it's difficult to remove without harming the print). Photograph the print as soon as it is visible. Don't try to overwork the dust to improve the print. Tap the brush gently to shake out excess residue and keep it dry. Use separate brushes for dark and light powders.

Latent Print Developers

The term 'latent' refers to phenomena or objects that are present but not visible. Latent prints are those which are not easily seen or otherwise detected and chemicals are often used to reveal or further 'develop' the prints to make them visible for the use of investigators, attorneys, and juries. There are many ways to develop latent prints and the research is ongoing. Lasers, UV light, image processing, fuming, and chemical development are all options with no clear superiority of any one approach.

Since these chemicals must be stored and used by people, nontoxic, nonflammable brands are preferred. However, some effective chemicals have toxic or irritating effects and are still used, in which case appropriate ventilation and precautions must be observed. Export restric-

© 2001 by CRC Press LLC

tions exist on some chemical developers. These are some common techniques:

- *Ninhydrin* mixed with a number of different fluids can give results ranging from adequate to excellent in revealing latent prints.
- *Gentian violet* is generally purchased as a powder. For use, it is dissolved in distilled water with pH adjustments with a very small quantity of ammonia. Tape with a latent print is soaked in the solution, rinsed, and examined under the microscope where stained cells that make up the ridges can be seen as a distinct violet color. Sometimes prints are transferred from the tape to photographic or other papers before processing with gentian violet. Whenever possible, it is desirable to make as few transfers as possible. Like a photocopy of a photocopy, a little information and clarity are lost each time minute particles are transferred. If a print must be transferred, it is usually accomplished with a chemical reagent or with heat.
- *Powder-detergent suspensions in water* are also used. A thick, iridescent dark or light mixture (depending on what is needed for contrast) is created which is applied to an adhesive surface. The tape is rinsed, pulled through the mixture, or the mixture applied carefully with an implement, and then rinsed again.

Sometimes fingerprints include contaminating traces of blood. Protein dyes that respond to the proteins in the blood stain can be used to stain the blood without affecting the latent print. Protective gear is recommended when using these types of products.

Backing Cards

Blank and printed cards are used for marking or storing evidence. Lifted prints, stains, and other evidence are often lifted with specialized tapes which may then be adhered to a card and labeled. Since chemical analysis of the stains is often carried out, it is important to use cards that do not interfere with the chemicals and which last a long time. Acid-free *archival* cards are preferred. Preprinted cards sometimes simplify the task of labelling and may aid in reducing the number of inadvertent omissions. They may also be numbered for file references to other documents. Numbers may further reduce the chance of fraudulent evidence.

Evidence Tapes

Clear tape, poly tape, Handi-Lifts™, Lightening Lifts™ pre-cut strips are all used to lift prints. The best tapes, in most cases, are those that are clear, that don't wrinkle easily, and have the least intrusive chemicals in the adhesive itself.

7. Problems and Limitations

Forensic Identification of Fingerprints

Some of the difficulties in using computerized matching systems are related to differences between traditional reference fingerprints and the fingerprints left at a scene. In most cases, reference fingerprints are made by the print-taker grasping the individual's finger, exerting light pressure and rolling the finger back and forth to get a print that clearly shows the broadest possible area. The prints left at scenes, however, usually only show part of the finger that protrudes the most, or those parts that come in contact with an object when it is being grasped. The computer software must be able to analyze the prints in such a way that differences in the outer edges stemming from the means of procuring the prints do not interfere with the possibility of a match. This can be done, mathematically, but may require methods different from those which are used in access surveillance applications (e.g., interpreting an image from the center and outward).

© 2001 by CRC Press LLC

Optimizing Iris and Retina Scans

Iris and retinal scan systems tend to require clear, well-focused images that may be hindered, in some instances, by contact lenses or eyeglasses. Earlier systems that shine a light source at the subject's eye tend to have greater problems with incidental reflections than passive light scanning systems. Removal of eyeglasses, and particularly of contacts, is considered inconvenient or intrusive.

Retinal images usually require that the subject be very close to the scanner. Sometimes an eye cup is used to position the eye, which may be inconvenient for the user and brings up some issues of sanitation, since eyes are a source of mucous and bacteria that can be passed from one person to the next.

In recent years, narrow bandwidth light sources have been used to overcome some of the problems of glasses and contacts and the reflectance associated with these accessories.

In a general sense, related to all biometric technologies, injuries and illnesses sometimes cause physical changes that can prevent access or recognition. Some individuals are lacking limbs or eyes due to accidents or birth defects and thus might be denied rightful access to workplaces or transaction machines unless special provisions are made.

Reliability

Electronic biometrics devices were, in many cases, somewhat unreliable until the 1990s at which time many of them began to improve and become commercially practical. However, the reliability is not just a factor of the electronics and the software. Some systems tend to be more reliable due to physical characteristics and changes of a person's body over time. Some types of processing are more difficult than others and some physical aspects are more variable from day to day (if you've ever had laryngitis you're aware of how much a voice can change under certain circumstances). Voice systems tend to fail more often than fingerprinting or facial recognition systems.

In general, reliability is improving as systems and software improve and multiple-input systems can sometimes overcome problems.

Identical twins can fool some biometric systems. If the twins are not mirror twins (with opposite features) and close relatives of the twins can't tell them apart, it's possible that the biometric systems can't tell them apart either on the basis of facial or voice recognition. However, other aspects, such as handwriting style and iris patterns may differ. When multiple sensors are used, it becomes slightly easier to distinguish identical twins. Mirror twins are easier to identify since imperfections and irregularities will be on opposite sides and will tend to aid in identification.

8. Restrictions and Regulations

Protection of Personal Information

Biometric surveillance is a relatively new field. Some aspects of it, such as fingerprinting and mug shots, have become standard law enforcement tools, but new technologies that allow any organization or retailer to use biometrics to monitor employees or customer profiles are now widely available and few restrictions are currently associated with their use.

In some aspects of law, biometric information is regarded as 'personal information.' In a number of codes, personal information is defined as any information that

> "... describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual including, but no limited to,

© 2001 by CRC Press LLC

his education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or his presence, registration, or membership in an organization or activity or admission to an institution."

Legal Force of Biometric Signatures

On 16 June 2000, the *Electronic Signatures in Global and National Commerce Act* was passed unanimously by the U.S. Senate. This made electronic signatures as legal and binding as traditional written signatures, providing a means to authenticate electronic transactions. The definition of *electronic signature* is broad enough to include biometrics:

> "The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

FBI Support Materials

The Federal Bureau of Investigation publishes a number of standards related to evidence which are relevant to chemical/biological surveillance as they relate to crime scene investigation and forensics such as the *Electronic Fingerprint Transmission Specification* (24 August 1995).

General Orders

On a broader scale, *Executive Order 13083* called "Federalism" was signed by President Clinton on or about 14 May 1998 (revokes Order 12612). Its passage was quiet, but it has since become a controversial document which some claim has reduced rather than expanded the divisions of power within the U.S. constitutional system by slanting primary lawmaking functions toward the President and away from Congress.

9. Implications of Use

Many concerns over biometrics identification systems have been raised, most of which relate to administrative changes and use of the technologies rather than the technologies themselves. The most prevalent concerns include reduction of boundaries between restricted and free citizens, changes in administration and use, lies, profit motives, and centralization due to economics.

Reduction of Boundaries and Database Errors

The trend for standardized, centralized databases is increasing. In these databases, a criminal who is incarcerated for murder looks much the same as a law-abiding private citizen. The computer puts the picture in one part of the screen, the name and address in another, and the personal information in a third. The electronic distinction between the criminal and the honest person may be as small as a single checkbox in the bottom right corner.

This may not seem to be a likely occurrence or problem, but you have to examine some of the dynamics of these computerized systems and how they are developed and sold. Databases are structured to demand certain information in certain ways. Anyone who has done data entry is aware that certain data entry fields require inputs before the program will let you continue or before it will perform certain types of processing tasks. When systems designed to record the fingerprints, mug shots, and other personal identities are developed, they are often marketed initially to law enforcement agencies and other bodies that have the resources to purchase them. Then, with a few small modifications (or no modifications), the companies that design these systems seek to broaden their markets, increase their profits, and offset their

© 2001 by CRC Press LLC

development costs, by selling them to other agencies. These could be government agencies (e.g., authorities issuing drivers' licenses), private companies, or retail establishments. In many cases, the database structure is essentially the same. In fact, with the possibility of connecting through the Internet, the pressure on developers to create standardized systems has increased. Once the institutions adopt the software for use with the general public, there is new pressure on the public to provide the same types of information that a criminal must supply when being incarcerated. This homogenization of biometric identities has already occurred in some prison and government database systems. Since it has been found that database entry operators make errors from 10% to 30% of the time, depending on how carefully they are supervised and crosschecked, the potential for misinformation to be rapidly spread through computer systems is great.

Changes in Administration

One of the biggest concerns in the protection of rights and privacy comes with changeovers in executive or governmental administrations. There are thousands of historical examples that show that data collected for one purpose are often used later for another purpose, without the permission or knowledge of the person originally supplying the data. This may be by the administration collecting the data or by a subsequent administration with very different political views and motives. Since computer information is easy to duplicate and transmit, there is no guarantee if one file is deleted, that it does not exist in multiple copies elsewhere.

Profit Motives

Many retail stores and supermarkets are now issuing 'member cards' or 'loyalty cards' that reward frequent and regular customers with discounts and other percs. Some of these companies sell your personal information to other companies and once it is out of their hands, they have no control whatsoever over who has it or how they use it. As biometric data are added to identification and member cards and as computer networks make it possible to amass substantial information on individuals through 'data mining,' very intimate information profiles can be developed on individuals.

Since anyone can purchase these data lists on the open market, they can also be purchased by secret service agencies, foreigners, and marketing professionals.

It's not difficult to configure a computer to analyze the data and figure out how many children you have, what schools they attend, how much money you make, and what types of products you like to buy. This type of intimate information can be used by unscrupulous employees or gray market business owners to stalk, coerce, or defraud.

Even government agencies have been known to enter into deals with private companies. In some states, drivers' license information has been sold to private companies. In some states the sales were blocked, but in another, the court ruled that drivers' license information was not private and that the sale was legal, in spite of public protests.

Lies

Some organizations and individuals simply lie. In the United States alone, it is estimated that $40 billion a year is lost to telemarketing scams. In the course of being defrauded, people often give out personal information that can be sold to others or distributed through computer networks more readily than ever before.

Cost-Effective Deployment and Change of Use

Economic factors often drive administrative decisions that result in loss of privacy. Many organizations install biometric identification systems with the promise that the information

© 2001 by CRC Press LLC

will not be shared with other departments or organizations. However, by the time the systems are installed, the cost of individual stations using the technology is often found to be cost prohibitive, resulting in gradual expansion of the system to spread the cost out over more stations and thus reduce individual costs. With time, these systems become centralized and the initial promise of data security and compartmentalization is broken without due process or public input.

As has been stated about other technologies described in this book, biometric technology is not inherently good or bad, but it is a powerful technology with a high potential for abuse when placed in the wrong hands, used for the wrong purpose, or redistributed without the owner's knowledge or consent. Using a face scan or electronic fingerprint system is not the same as presenting a driver's license photo. The driver's license data supposedly reside in only one database (although previous comments indicate this is not always the case), whereas a facial recognition system, if used by retailers or less accountable organizations, for example, resides in multiple databases that can be sold and swapped and accessed by employees at will. There is very little protection in this type of system.

Some privacy rights advocates are concerned that iris or retinal scans might be used to assess health. An employer who uses iris or retinal scans (or both) might be tempted to analyze data for diabetes, glaucoma, cataracts or other signs of ill health when deciding on medical insurance benefits, raises, promotions, or who to lay off. There are even some types of fingerprint patterns that can indicate certain genetic characteristics or health conditions. In order to try to prevent these types of abuse, some companies have developed systems which delete the original reference image after it has been coded into an electronic pattern, but there is no guarantee that all programmers and vendors will do this, especially if buyers express a willingness to pay for systems that do not add this security layer.

It appears to be only a matter of time before someone begins lobbying for biometrics to be used to verify registered voters when they step into voting booths.

It is hoped that all the issues regarding biometrics are discussed before systems are put in place and that the convenience of some of these systems doesn't overshadow good judgment in evaluating all the factors associated with their use.

10. Resources

Inclusion of the following companies does not constitute nor imply an endorsement of their products and services and, conversely, does not imply their endorsement of the contents of this text.

10.a. Organizations

American Chemical Society (ACS) - Provides members with technical and educational information resources, professional development assistance, industry advocacy, awards, and insurance programs. Supports over 30 specialty divisions, including Analytical Chemistry (ANYL) and Chemical Toxicology (TOXI) which have their own publications in addition to the ACS publications.
http://www.acs.org/

American Society for Investigative Pathology (ASIP) - A society for biomedical scientists who investigate the mechanisms of disease. The discipline uses a variety of structural, functional, and genetic techniques, applying the research results to the diagnosis and treatment of disease. ASIP supports professional development and education of its members. http://asip.uthscsa.edu/

© 2001 by CRC Press LLC

Association for Biometrics (AfB) - A nonprofit organization providing services to government, academic, and industry members, while promoting technologies related to biometrics. http://www.afb.org.uk/

Biometric Consortium - A U.S. government group of over 200 academic, private sector, and government members involved in research, developing, testing and evaluating biometric technologies. http://www.biometrics.org/

Biometric Systems Lab - A biometrics research lab located at the University of Bologna, Cesena, Italy. http://www.csr.unibo.it/research/biolab/bio_home.html

Center for International Security and Cooperation (CISAC) - A multidisciplinary community within Stanford University's Institute for International Studies dedicated to research and training in issues of national security. http://www.stanford.edu/group/CISAC/

Center for Security Systems - This is a research-development-applications center for creating technologies that aid in national security. It includes dedicated laboratories for sensors, image processing, alarms, communications, and biometrics. http://www.sandia.gov/

Chemical Science and Technology Laboratory (CSTL) - Within the U.S. Department of Commerce, the CSTL is one of seven NIST measurement and standards laboratories. It works to promote U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. It includes five divisions: analytical chemistry, biotechnology, physical and chemical properties, process measurements, and surface and microanalysis science. http://www.cstl.nist.gov/

European Association for Biometrics (EAB) - This organization joined a consortium with the National Computer Security Association in 1997.

Federal Bureau of Investigation (FBI) - The FBI provides many print resources and services for law enforcement, along with a number of federal databases. The National Crime Information Center (NCIC) 2000 provides single fingerprint matching and mug shot data available to more than 80,000 criminal justice agencies. http://www.fbi.gov/

International Association for Identification (IAI) - A nonprofit, professional organization for professionals engaged in forensic identification and scientific examination of physical evidence. The IAI provides a range of education and certification programs including latent fingerprint examination, crime scene certification, forensic artist, etc. Descended from the International Association for Criminal Identification, founded in 1915. http://www.theiai.org/

International Biometric Industry Association (IBIA) - This is a nonprofit trade organization established in 1998 to advance, advocate, defend, and support the international biometrics industry. IBIA also publishes newsletters and bulletins. http://www.ibia.org/

International Biometric Society (IBS) - Founded in 1947, the IBS advances the subject-matter sciences related to biometrics. Members include biologists, statisticians, and others applying statistical techniques to research data. http://stat.tamu.edu/Biometrics/

Lightning Powder Company, Inc. Supplies chemicals, including powders, to crime scene investigators and provides informational articles on their Web site on fingerprint technology. http://www.redwop.com/

National Institute of Standards and Technology (NIST) - NIST is an agency of the U.S. Department of Commerce's Technology Administration, established in 1901 as the National Bureau of Standards and renamed in 1988. It aids industry in developing and applying technology, measurements, and standards through four major programs. The Chemical Science and Technology Laboratory is one of seven NIST measurement and standards laboratories. http://www.nist.gov/

Southern California Association of Fingerprint Officers (SCAFO) - A nonprofit organization founded in 1837 to support professional identifiers. It now includes members in more than 50 law enforcement agencies. The Web site has an excellent fingerprint bibliography. http://www.scafo.org/

© 2001 by CRC Press LLC

SWGFAST - The Scientific Working Group on Friction Ridge Analysis, Study, and Technology was founded as the result of a 1995 FBI meeting of latent print examiners. SWGFAST (formerly TWGFAST) provides guidelines, discussions of analysis methods and protocols, and support for the latent print professional community. Information is available through the FBI Laboratory. http://www.fbi.gov/

U.S. Army Biometrics - This is within the Office of the Secretary of the Army Director of Information Systems C4. http://www.army.mil/biometrics/

10.b Print

The author has endeavored to read and review as many mentioned resources as possible or to seek the recommendations of colleagues. In a few cases, it was necessary to rely on publishers' descriptions on books that were very recent, or difficult to acquire. It is hoped that the annotations will assist the reader in selecting additional reading.

These annotated listings may include both current and out-of-print books and journals. Those which are not currently in print are sometimes available in local libraries and second-hand book stores, or through interlibrary loan systems.

Bace, Rebecca Gurley, "Intrusion Detection," Indianopolis: MacMillan Technical Pub., 2000, 339 pages. History and developmental treatment of intrusion detection devices, legal issues, and other concepts. It is not a how-to book but rather an aid in making administrative decisions.

Bodziak, W., "Footwear Impression Evidence," New York: Elsevier, 1990 and Boca Raton: CRC Press, 2000. The CRC Press edition includes added information on barefoot evidence and the O. J. Simpson trial.

Elashoff, Robert, "Perspectives in Biometrics," New York: Academic Press, 1975.

Jain, Anil; Boole, Ruud; Pankanti, Sharath, Editors, "Biometrics, Personal Identification in Networked Society: Personal Identification in Networked Society," from the Kluwer International Series in Engineering, Kluwer Academic Publishers, 1999.

Jain, L. C.; Halici, U.; Hayashi, I.; Lee, S.B., Editors, "Intelligent Biometric Techniques in Fingerprint and Face Recognition," Series on Computational Intelligence, Boca Raton: CRC Press, 1999, 480 pages. This book has received mixed reviews.

Kovacich, Gerald L.; Boni, William C., "High Technology Crime Investigator's Handbook," Butterworth-Heinemann, 1999, 350 pages. Not specifically on biometrics but a good general reference and practical guide to forensics with new technologies.

Articles

Adcock, J. M., "The Development of Latent Fingerprints on Human Skin: The Iodine-Silver Plate Transfer Method," *Journal of Fingerprint Science,* 1977, V.22(3), pp. 599-604.

Almog, Joseph; Hirshfeld, Amiram; Klug, J. T., "Reagents for the Chemical Development of Latent Fingerprints: Synthesis and Properties of Some Ninhydrin Analogues," *Journal of Fingerprint Science,* Oct. 1982, V.27(4), pp. 912-917. Almog has written a series of articles in JFS on this topic.

Ashbaugh, David R., "Ridgeology - Modern Evaluative Friction Ridge Identification," *JFI,* 1991, V.41(1), pp. 16-64. Ashbaugh has written a series of articles in JFI on ridge patterns and identification.

Augibe, Frederick T.; Costello, James T., "A New Method for Softening Mummified Fingers," *Journal of Fingerprint Science,* April 1985, V.31(2), pp. 726-731.

Baniuk, Krystyna, "Determination of Age of Fingerprints," *Forensic Science International,* 1990, V.46, pp. 133-137.

Blank, Joseph P., "The Fingerprint That Lied," *Reader's Digest,* Sept. 1975, pp. 81-85.

© 2001 by CRC Press LLC

Brooks, Andrew J., Jr., "Techniques for Finding Latent Prints," *Fingerprint and Identification Magazine,* Nov. 1972, pp. 3-11.

Burt, Jim A.; Menzel, E. Roland, "Laser Detection of Latent Fingerprints: Difficult Surfaces," *Journal of Fingerprint Science,* April 1985, V.13(2), page 364-370.

Candela, Gerald T.; Grother, Patrick J.; Watson, Craig I.; Wilkinson, R. Allen; Wilson, Charles L., "Public Domain PCASYS: PCASYS–A Pattern-level Classification Automation System for Fingerprints," *National Institute of Standards and Technology.*

"Chemical Formulas and Processing Guide for Developing Latent Prints," *FBI Training Material,* 1994 (revised).

Chen, Hans H., "Bio-Code Systems Promise New Age in Security: But Are They a Threat to Privacy," *APBnews.com,* 10 Oct. 1999. Details some of the uses and surprising abuses of biometrics and computer databases.

Chen, Hans H., "Machines that Mesaure Your Body Parts," *ABPnews.com,* 10 Oct. 1999. Describes basic biometric devices with illustrations of some common systems.

Couto, Joe, "Ontario farmer challenges government over photo ID," *Christian Week,* V.13(10). Describes Ontario's identification which includes the capability to transmit over networks and wireless communications systems.

Creer, Ken, "Operational Experience in the Detection and Photography of Latent Fingerprints by Argon Ion Laser," *Forensic Sciences International,* 1983, V.23, pp. 149-160.

Duff, J. M.; Menzel, E. R., "Laser-Assisted Thin-Layer Chromatography and Luminescence of Fingerprints: An Approach to Fingerprint Age Determination," *Journal of Forensic Science,* 1978, V.23(1), pp. 129-134.

Faulds, Henry, "On the Skin-Furrows of the Hand," *Nature,* 28 Oct. 1880.

Feldman, M. A.; Meloan, C. E.; Lambert, J. L., "A New Method for Recovering Latent Fingerprints from Skin," *Journal of Forensic Science,* Oct. 1982, V.27(4), pp. 806-811.

Fincher, Jack, "Lifting 'latents' is now very much a high-tech matter," *Smithsonian,* Oct. 1989, pp. 201-218.

German, Edward R., "The Admissibility of New Latent Print Detection Techniques in U.S. Courts," *Identification News,* Oct. 1986, pp. 12-13.

Grimoldi, Giuliana; Lennard, Christopher J.; Margot, Pierre A., "'Liquid Gloves' and Latent Fingerprint Detection," *JFI*, 1990, V.40(1), pp. 23-27.

"Here's looking at you: One hospital's experience with biometrics," *HIPAA and Health Information Security.* Describes how biometric technology and access to electronic medical records may be integrated.

Lee, Henry C.; Gaensslen, R. E., "Cyanoacrylate Fuming," *Identification News,* June 1984, pp. 8-14.

Menzel, E. Roland, "Pretreatment of Latent Prints for Laser Development," *Forensic Science Review,* June 1989, V.1(1), pp. 44-66. Menzel has written several articles for a variety of publications including Analytical Chemistry and Journal of Forensic Science.

Nutt, Jim, "Chemically Enhanced Bloody Fingerprints," *FBI Bulletin,* Feb. 1985, pp. 22-25.

"Putting Your Finger on the Line: Biometric Identification Technology," *Framed,* Dec. 1997, Issue 34. Describes biometric technology and the controversy over the implementation of biometrics in the NSW prison system.

Scroggins, Steve, "National ID card system threatens freedom," 18 July 1998. Describes the controversy surrounding a 1996 Department of Public Safety announcement to collect fingerprints for drivers' licenses and the implications of such practices.

Waver, David E., "Photographic Enhancement of Latent Prints," *JFI*, 1988, V.38(5), pp. 189-196.

© 2001 by CRC Press LLC

Wellborn, Stanley N., "Foolproof ID: Opening Locks With Your Body," *U.S. News & World Report*, 17 Dec. 1984. Describes a variety of types of biometric systems and where and how they are used.

Woodward, John D., "Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint," *University of Pittsburgh Law Review, 1997.*

Journals

"The Biometric Digest," a weekly email publication.

"Biometric Technology Today," an Elsevier Advanced Technology publication.

"Biometrics," a journal of the International Biometric Society. http://stat.tamu.edu/Biometrics/

"Biometrics Bulletin," published by the American Statistical Association.

"Biometrics in Human Services User Group Newsletter," provides biometric news, findings, and ideas.

"Chemical Formulas and Processing Guide for Developing Latent Prints," FBI Training Material, 1994 (revised).

"Framed," A quarterly magazine of justice action.

"HIPAA and Health Information Security," a publication for health care professionals tasked with information security.

"The Print," the professional journal of the Southern California Association of Fingerprint Officers (SCAFO). Six issues per year are available to members of SCAFO.

"Voice ID Quarterly," information available through *jmarkowitz@pobox.com*.

10.c. Conferences and Workshops

Many of these conferences are annual events that are held at approximately the same time each year, so even if the conference listings are outdated, they can still help you determine the frequency and sometimes the time of year of upcoming events. It is very common for international conferences to be held in a different city each year, so contact the organizers for current locations.

Many of these organizations describe the upcoming conferences on the Web and may also archive conference proceedings for purchase or free download.

The following conferences are organized according to the calendar month in which they are usually held.

"2000 Biometrics Summit," Implementing Practical Applications in BIometrics for the Next Millenium, Miami, Fl., 7-9 Feb. 2000.

"SmartCard 2000," 13th annual conference, London, England, 8-10 Feb. 2000.

"Experimental Biology 2000," annual meeting of the American Society for Investigative Pathology (ASIP), San Diego, CA, 15-18 April 2000.

"California State Division International Association for Identification," 84th Annual Training Seminar, Laughlin, Nevada, 8-11 May 2000.

"2001: A Speaker Odyssey," The Speaker Recognition Workshop, Jerusalem, Israel, 18-22 Jun. 2001.

"International Association for Identification," annual professional education conference on forensic identification and investigation, Miami, Florida, 22-28 July, 2001.

"Biometric Consortium Conference," Gaithersburg, Md., 13-14 Sept. 2000.

"Biometrics 2000," London, U.K., 6-8 Nov. 2000.

"Defending Cyberspace 2000," CardTech SecurTech conference, Washington, D.C., 11-13 Dec. 2000.

"Carnahan Conference on Electronic Crime Countermeasures," covers a variety of topics including fingerprint technologies and publishes the proceedings.

© 2001 by CRC Press LLC

10.d. Online Sites

The following are interesting Web sites relevant to this chapter. The author has tried to limit the listings to links that are stable and likely to remain so for a while. However, since Web sites do sometimes change, keywords in the descriptions below can help you relocate them with a search engine. Sites are moved more often than they are deleted.

Another suggestion, if the site has disappeared, is to go to the upper level of the domain name. Sometimes the site manager has simply changed the name of the file of interest. For example, if you cannot locate http://www.goodsite.com/science/uv.html *try going to* http://www.goodsite.com/science/ *or* http://www.goodsite.com/ *to see if there is a new link to the page. It could be that the filename* uv.html *was changed to* ultraviolet.html*, for example.*

Department of Social Services - The Connecticut Department of Social Services has information on the DSS Biometric Identification Project and many links to biometric publications. http://www.dss.state.ct.us/digital/dipubs2.htm

Fingerprinting Identification - This is an illustrated FBI educational site that introduces concepts and procedures related to fingerprinting technologies. There are also links to other pages, including polygraph testing. http://www.fbi.gov/kids/crimedet/finger/finger.htm

Southern California Association of Fingerprint Officers (SCAFO) - A nonprofit organization founded in 1837 to support professional identifiers. The Web site has an excellent, extensive fingerprint publications bibliography which, in some cases, includes links to the full text of articles. There is also general educational information about fingerprint science. http://www.scafo.org/

Note: If you don't enjoy typing in long Web addresses (URLs), you can access the links on the support site set up by the author for your convenience. http://www.abiogenesis.com/surveil

10.e. Media Resources

"FBI Files," a weekly television series on the *Discovery Channel* that follows FBI investigations and describes various forensic techniques used in the solving of crimes.

"Forensic Science," from the *History Channel* Modern Marvels Series. This shows traces the history of forensic sciences using fingerprints, DNA profiles, fiber analysis and other technologies. VHS, 50 minutes. Cannot be shipped outside the U.S. and Canada.

"Mission Impossible," a 1996 Paramount Pictures feature film starringa Rason: Tom Cruise as Ethan Hunt. A thriller that illustrates a few biometric technologies, including voice recognition and finger imaging.

"Police Technology," from the *History Channel* Modern Marvels Series. This show traces the history of the police department, from breakthroughs like fingerprint technology to modern forensic methods. VHS, 50 minutes. Cannot be shipped outside the U.S. and Canada.

"Scene of the Crime," from the *Arts & Entertainment* Scene of the Crime series. This shows follows Crime Lab personnel as they gather evidence of a crime including fingerprints and other physical evidence. VHS, 50 minutes. Cannot be shipped outside the U.S. and Canada.

© 2001 by CRC Press LLC

11. Glossary

Titles, product names, organizations, and specific military designations are capitalized; common generic and colloquial terms and phrases are not.

AFIS	Automated Fingerprint Identification System
assay	to analyze for one or more specific components
ATM	automatic teller/transaction machine
BAAPI	Biometric Authentication Application Programmers Interface, proprietary product of TrueTouch which is used by a number of third parties developing biometrics identification products
BIT	biometric identification technology
CCH	computerized criminal history
DSV	dynamic signature verification
extraction	the assessment and processing of information or characteristics that are relevant to detection or identification
goats	individuals who, by lack or cooperation, eccentricity, or personal characteristics tend to not be recognized by a detection or identification system
IAFIS	Integrated Automated Fingerprint Identification System, standardized FBI system
IQS	image quality specifications (see IAFIS)
iris	the colored portion at the front of the eye surrounding the pupil but inside the whites of the eye which contains a unique pattern that is retained throughout life as long as there are no serious health problems or accidents
latent	hidden, not immediately or obviously discernible as faint stains or fingerprint oils
minutiae	the small details found in finger images which include ridges, patterns, valleys, and branching structures (bifurcations)
MIU	Mobile Imaging Unit, as is used in squad cars for mobile identification and verification
PARIS	Pennsylvania Automated Recipient Identification System
PIN	personal identification number
platen	a surface on which a body part is placed in order to be imaged or otherwise scanned or detected
retina	the imaging portion of the back of the eye on which light is directed by the structures at the front of the eye, which contains a unique pattern of blood vessels
speech recognition	the capability to recognize the content of a spoken communication (see voice recognition)
voice recognition	the capability to recognize the presence of a voice or a voice that belongs to a particular individual, but not the content of a communication (see speech recognition)

© 2001 by CRC Press LLC