PDHonline Course G522 (6 PDH)

Biometrics

Instructor: Robert P. Jackson, PE

2020

PDH Online | PDH Center

5272 Meadow Estates Drive
Fairfax, VA 22030-6658
Phone: 703-988-0088
www.PDHonline.com

An Approved Continuing Education Provider

ABBREVIATIONS:

	-A-
ABIS	Automated Biometric Identify Systems
AFIS	Automated Fingerprint Identification System
ANSI	American National Standards Institute
ATMS	Automatic Teller Machines
	-B-
BIOAPI	Biometric Application Programming Interface
	-C-
CIA	Central Intelligence Agency
CJIS	Criminal Justice Information System
CTIA	Cellular Telephone Industries Association
	-D-
DARPA	Defense Advanced Research Products Agency
DoD	Department of Defense
DPI	Dots per Inch
DNA	Deoxyribonucleic Acid
	-E-
EBGM	Elastic Bunch Graphic Matching
	-F-
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FERET	Face Recognition Technology Evaluation
FIPS	Federal Information Processing Standards
FRGC	Face Recognition Grand Challenge

FRR	False Recognition Rate
FRVT	Face Vendor Recognition Test

-H-

HSPD	Homeland Security Presidential Directive

-I-

IAFIS	
ICAO	International Civil Aviation Organization
ID	Identification
IDC	International Data Corporation
IEC	International Electric Code
INCITS	International Committee for Information Technology Standards
INSPASS	Immigration and Naturalization Services Passenger Accelerated Service Systems
IS	Identification Services
ISO	International Standards Organization
IT	Internet Technology
ITIC	Intelligence Technology Innovation Center

-L-

LDA	Linear Discriminant Analysis

-M-

MRDT	Machine Readable Travel Documents

-N-

NBS	National Bureau of Standards
NFL	National Football League
NGI	Next Generation Initiative
NIST	National Institute of Standards and Technology

NSTC	National Science and Technology Council

-P-

PC	Personal Computer
PCA	Principal Components Analysis
PIN	Personal Information Number
POS	Point of Sale

-T-

TAG	Technical Advisory Group

-U-

US	United States

TABLE OF FIGURES:

TABLE OF CONTENTS:

INTRODUCTION:

Biometrics may be a fairly new term to some individuals so it is entirely appropriate at this time to define the technology. This will lay the groundwork for the discussion to follow. According to the International Biometric Society:

“Biometrics is used to refer to the emerging field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition.”

The terms “Biometrics” and “Biometry” have been used since early in the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences.

From the Free Dictionary we see the following definition:

- ***The statistical study of biological phenomena.***
- ***The measurement of physical characteristics, such as fingerprints, DNA, or retinal patterns for use in verifying the identity of individuals.***
- ***Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.***

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

The oldest biometric identifier is facial recognition. The dimensions, proportions and physical attributes of a person's face are unique and occur very early in infants. A child will (obviously) recognize a parent, a brother or sister. It is only since the advent of computers and accompanying software that the ability to quantify facial features has become possible.

The FBI has long been a leader in biometrics and has used various forms of biometric identification since the very earliest day. This Federal institution assumed responsibility for managing the national fingerprint collection in 1924. As you know, fingerprints vary from person to person (even identical twins have different prints) and don’t change over time. As a result, they are an effective way of identifying fugitives and helping to prove both guilt and innocence.

We will discuss fingerprints, as well as other modes of identification, later on in this course.

BIOMETRIC APPLICATIONS:

In the last several years, improvements in the technology have greatly increased application. It is expected that in the near future, we will use biometry many times in our daily activities such as getting in the car, opening the door of our house, accessing our bank account, shopping by internet, accessing our PDA, mobile phone, laptops, etc. Depending on where biometric systems are deployed, the applications can be categorized in the following five main groups: 1.) Forensic, 2.) Government, 3.) Commercial, 4.) Health-care, and 5.) Traveling and immigration. However, some applications are common to these groups such as physical access, PC/network access, time and attendance, etc.

Forensic:

The use of biometric technology in law enforcement and forensic analysis applied to law enforcement, has been known and used for quite some time. That technology is used mainly for identification of criminals. In particular, the AFIS (automatic fingerprint identification system) has been used for this purpose. Recently, facial-scan technology or mug shots are being used for the identification of suspects. Another possible application is the verification of individuals considered for arrest as suspects in home and auto break-ins. The typical applications are:

- **Identification of criminals-** Collecting evidence, such as fingerprints, at the scene of a crime makes it possible to compare information relative to an existing database. You often hear in the movies of investigating officers "dusting for fingerprints". This has been and is common practice.
- **Surveillance -**-Using cameras, one can monitor very busy areas such as stadiums, airports, meeting rooms, etc. to determine the presence of criminal suspects or when suspected criminal activity could be a possibility. Based on the face recognition biometric, using images (e.g., mug shots), database files of wanted persons or criminals may be integrated to verify their presence. Since the events of September 11, 2001, the interest in biometric surveillance has increased dramatically, especially for air travel. There are many cameras monitoring crowds at airports for detecting wanted terrorists.
- **Corrections -**This refers to the treatment of offenders (criminals) through a system of penal incarceration, rehabilitation, probation, and parole, or the administrative system by which these are effectuated. In this case a biometric system can avoid the possibility of accidentally releasing the wrong prisoner, or to ensure that people leaving the facilities are really visitors and not inmates.
- **Probation and home arrest -** Biometrics can also be used for post-release programs (conditional release) to ensure the fulfillment of the probation, parole and home detention terms.

Government:

There are many applications of biometric technology operating in the government sector. An AFIS or Automatic Fingerprint Identification System is the primary means for locating duplicate entities enrolled in benefits systems, electronic voting for local or national elections, issuance of driver's license emission, etc. The typical application is:

- **National Identification Cards -** The idea is to include digital biometric information in the national identification card. This is the most ambitious biometric program, since the identification must be performed in a large-scale database, containing hundreds of millions of samples, corresponding to the whole population of one country. These cards can be used for multiple purposes such as controlling the collection of benefits, avoiding duplicates of voter registration and driver's license usage. These applications are primarily based on finger-scan and AFIS technology; however it is possible that facial-scan and iris-scan technology could be used in the future.

- **Voter ID and Elections -** While the biometric national identification (ID) card is still an ongoing project in the United States, many countries already use this mode of biometry to control voting and voter registration. These ID cards are used for national and/or regional elections. During the registration of voters, biometric data is captured and embedded in the card with matching data in a stored database for the later use. The purpose is to prevent duplicate registration and voting.

- **Driver's licenses -** In many countries a valid driver license is used as an identification document; therefore it is important to prevent duplication and use under a different name. Biometrics can eliminate this problem. However, it is important that the data is shared between states, because in the United States, the license is controlled at the state level as opposed to the federal level.

- **Benefits Distribution (social service) -** The use of biometry in benefits distribution prevents fraud and abuse within government benefits programs. This can ensure that legitimate recipients have quick and convenient access to benefits such as unemployment, health care and social security.

- **Employee authentication -** The government use of biometric data for PC, network, and data access is critical for securing buildings and thereby protection of confidential information.

- **Military programs -** The military has long been interested in biometric technology and many of the advancements have come from R&D efforts financed by the government. With this being the case, the technology has enjoyed extensive support from the national security community.

Commercial:

Banking and financial services represent enormous growth areas for biometric technology. Many developments are currently in place with pilot projects initiated frequently. Several applications within the banking sector are:

- **Account access -** Access to a specific personal or commercial account using Biometrics allows the financial institution to keep definitive records of account access by employees and customers. Using biometry, customers can access accounts and employees can log from their workstations or in person.
- **ATMs –**Biometrics allowing ATM access, provides for more secure banking transactions. This access would probably be by virtue of fingerprint, retina or iris scans.
- **Expanded Service Kiosks -** A more receptive market for biometrics may be special purpose kiosks, using biometric verification to allow a greater variety of financial transaction; than are currently available through standard ATMs.
- **Online banking –** Internet-based account access is already widely used in many places. The inclusion of biometric technology will bring about much greater security for these transactions from home. Currently, there are many pilot programs using biometrics in home banking.

- **Telephone transaction -** Voice-scan biometric can be used to secure telephone-based banking transactions. In this application, when the consumer calls to execute a transaction, a biometric system will authenticate the customer's identity based on his or her voice. There will be no need for any additional device.
- **PC/Network access -** The use of biometric login to local PCs or remotely through networks increases the security of the overall system. This definitely insures greater protection of valuable information.
- **Physical access -** Biometric technology is widely used for controlling the access to buildings or restricted areas. This is very common right now.
- **E-commerce -** Biometric e-commerce is the use of any biometric mode to verify the identity of individuals wishing to gain remote access for transaction involving goods or services.
- **Time and attendance monitoring –** Biometrics can be used for controlling the presence of individuals in a given area; for example, for controlling time sheets of employees or the presence of students in a classroom. Hand and palm readers are very prevalent in manufacturing locations for use in clocking in and clocking out.

Health Care:

Applications for this sector include identification or verification of individuals interacting with a health-care entity or acting in the capacity of health-care employees or other professionals. The main purpose being prevention of fraud, protecting patient information, and the control of pharmaceutical products. Typical application are:

- **PC/Network Access** – To control the activity of employees needing to gain access to hospital networks. Used primarily to protect patient information from unauthorized personnel.
- **Access of personal information** - Patient information could possibly be stored on smart cards or secure networks allowing access for patients relative to their personal information.
- **Patient identification** - In cases of emergency and when a patient does not have identification documentation, biometric identification may be a good alternative. The DoD is experimenting with DNA samples carried by the uniformed soldier allowing doctors in emergency situations to access the patient’s records.

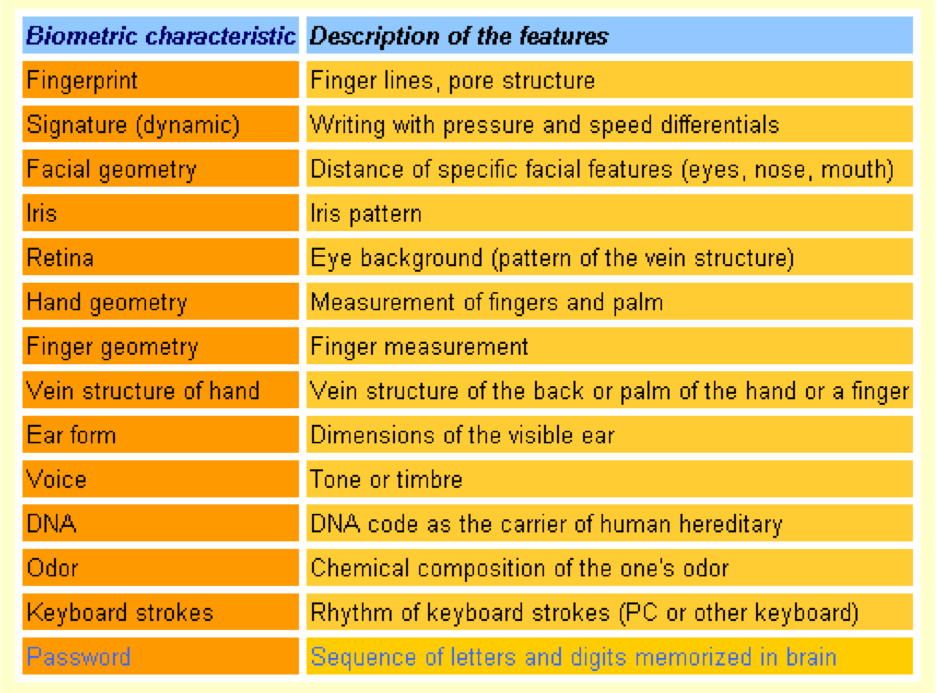
Travel and Immigration

The application in this sector includes the use of biometrics technology to identify or verify the identity of individuals interacting with systems during the course of travel. This, of course, includes immigration entity or acting in the capacity of an immigration employee. Typical applications are:

- **Air travel -** Many airports are already using a biometric system in to reduce inspection processing times for authorized travelers.
- **Border crossing -** The use of biometrics to control the travelers crossing the national or state border is increasing, especially in regions with high volume of travelers or illegal immigrants.
- **Employee access -** Several airports use biometrics to control the physical access of employees to secure areas.
- **Passports -** Some countries already issues passports with biometric information on a barcode or smart chips. The use of biometrics prevents use of multiple passports for the same person and facilitates the identification at the airports and border controls.

BIOMETRIC SUITE:

If we look at all biometric possibilities, we see the following methods of applying the technology:



Biometric characteristic	*Description of the features*
Fingerprint	Finger lines, pore structure
Signature (dynamic)	Writing with pressure and speed differentials
Facial geometry	Distance of specific facial features (eyes, nose, mouth)
Iris	Iris pattern
Retina	Eye background (pattern of the vein structure)
Hand geometry	Measurement of fingers and palm
Finger geometry	Finger measurement
Vein structure of hand	Vein structure of the back or palm of the hand or a finger
Ear form	Dimensions of the visible ear
Voice	Tone or timbre
DNA	DNA code as the carrier of human hereditary
Odor	Chemical composition of the one's odor
Keyboard strokes	Rhythm of keyboard strokes (PC or other keyboard)
Password	Sequence of letters and digits memorized in brain

FIGURE 1: BIOMETRIC SUITE OF CHARACTERISTICS

The methods used, relative to allowing access to information and location, must be determined by careful consideration of 1.) cost, 2.) interface with existing computer equipment and computer code, 3.) level of social intrusion tolerated, 4.) ease in maintenance of equipment and 5.) level of security required by the facility. You would expect entry into a nuclear facility to be more difficult that entry into an NFL locker room. You get the point.

THEFT AND FRAUD:

The possible theft and fraud occurences hit home when we consider the number of identity theft cases each year. Add to that number the instances of fraud and money laundering and you get a difficult picture to believe.

- Approximately 15 million United States residents have their identities used fraudulently each year, with financial losses totaling upwards of fifty billion ($50 B) .

- On a case-by-case basis, that means approximately seven percent (7%) of all adults have their identities misused with each instance resulting in approximately $3,500 in losses.

- Close to one hundred (100) million additional Americans have their personal identifying information placed at risk of identity theft each year when records maintained in government and corporate databases are lost or stolen.

- On average, banks charge nineteen percent (19%) for a returned check and fiver dollars ($5.00) to the depositor. Assuming a combined revenue stream to banks of twenty-four dollars ($24.00) for returning a check, with 300 million returned checks, the annual revenue from returned checks is seven billion dollars ($7billion).

- Ernst & Young reports that more than five hundred (500) million checks are forged annually. The American Banker, an industry magazine, predicts that there will be a twenty-five percent (25%) increase in check fraud in the 2016 year.

- Money laundering has increased over the last ten years. As a result, global efforts to combat this crime have increased. While it is extremely difficult to estimate the amount of worldwide money laundering, one model estimated that in 1998 it was near $2.85 trillion.

- According to Meridian Research, estimated fraud loss for the credit card industry amount to $1.5 billion annually, of which $230 million is estimated to result from online transactions. MasterCard reported a 33.7% increase in worldwide fraud from 1998 to 1999. During the first quarter of 2000, fraud losses increased 35.3% over the last quarter in 1999. VISA reports similar trends. It is estimated that fraud losses for online transactions may exceed $500 million in 2000. Fraudulent credit card activities include the use of counterfeit, stolen, and never received cards, as well as account takeover, mail order and Internet card-not present transactions.

- The FBI estimates losses from check fraud total $18.7 billion annually.

- Health care fraud costs the country tens of billions of dollars a year. It's a rising threat, with national health care expenditures estimated to exceed $3 trillion in 2014 and spending continuing to outpace inflation. Recent cases also show that medical professionals continue, and may be more willing, to risk patient harm in furtherance of their schemes. Medicare has no official estimate of the amount of money lost to fraud each year, but the Federal Bureau of Investigation refers to estimates of three to ten percent of all health care billings. In 2011, Medicare expenditures totaled approximately $565 billion. If the FBI percentages are applied to this amount, the cost of Medicare fraud for the 2011 fiscal year was anywhere from $17-57 billion.

- According to an FBI report on insurance fraud, published on its web site under "The Economic Crimes Unit" section, total insurance industry fraud is $27.6 billion annually. The Coalition Against Insurance Fraud breaks the total down across the insurance industry as follows:

    - · Auto $12.3 billion ·

    - Homeowners $1.8 billion ·

- Business/Commercial $12 billion ·
- Life/Disability $1.5 billion

Economic crimes in this area include those committed both internally and externally. Internal fraud can manifest itself in bribery of company officials, misrepresentation of company information for personal gain, and the like.

- In his testimony to the Senate Subcommittee on Commerce, Justice, State and the Judiciary on March 21, 2000, Chairman Arthur Levitt stated that Internet securities fraud is on the rise. He stated that there will be over 5.5 million online brokerage accounts by year end. The SEC has seen a rapid rise in Internet fraud in this area, with most of it occurring between 1998 and 1999. One recent pyramid scheme raised more than $150 million from over 155,000 investors before it was shut down. Securities fraud takes the form of stock manipulation, fraudulent offerings, and illegal touts conducted through newspapers, meetings, and cold calling, among others. These same scams have been conducted electronically, but are now joined by some newer, more sophisticated fraudulent activity. These include momentum-trading web sites, scalping recommendations, message boards posted by imposters, web sites for day trading recommendations, and misdirected messages. Investors are suffering large losses due to these cyber crimes.
- The U.S. Secret Service estimates that telecommunication fraud losses exceed $1 billion annually. Other estimates range from three ($3) billion to twelve ($12) billion. Subscription or identity fraud involves using false or stolen IDs or credit cards to gain free service and anonymity. It has tripled since 1997, says Rick Kemper, Cellular Telecommunications Industry Association's (CTIA) director of wireless technology and security, a trend he attributes to criminals favoring subscription fraud over cloning, plus increased industry competition to reach a broader and riskier market. The International Data Corporation (IDC: Framingham, MA) stated that, "Fraud remains endemic to the wireless industry, with estimated loses expected to reach a staggering $677 million by 2002…" One of the key reasons is the dramatic increase of subscription fraud which IDC estimates will reach $473 million by 2002.17 Telemarketing fraud resulted in losses to victims of over $40 billion in 1998. In 1996, the FBI estimated that there were over 14,000 telemarketing firms that were involved in fraudulent acts, the majority of which victimized the elderly.
- Intellectual property theft – in the form of trademark infringement, cyber squatters, typo squatters, trade-secret theft, and copyright infringement – has increased as Internet use and misuse has risen. It occurs across the seven industries detailed here, as well as most other businesses. "According to the American Society for Industrial Security, American businesses have been losing $250 billion a year from intellectual property theft since the mid-1990's.

These alarming statistics demonstrate identity theft and fraud may be the most frequent, costly and pervasive crime in the United States and on a global basis. There is also a growing belief that biometrics may be able to lessen to a very great degree identity theft.

OTHER USES:

Other uses of biometrics involve allowing or disallowing access to guarded areas. The options currently available for user authentication fall within three categories: 1.) authentication through information the user knows, such as a PIN or a password, 2.) an item the user has, such as a token with random codes, a flash drive or a proximity card, and 3.) a trait physically unique to the individual.

Today's system security professionals speak of passwords being too weak; this means that authentication, which for years has been the most widely used tool to protect data and systems, has been often proven too easy to break or too impractical to use when systems administrators enforce long, complex and unmemorable alphanumeric passwords. Tokens and other devices have also proved not always effective due to the cost of production and distribution and the possibility of being stolen and used fraudulently. So what are the alternatives? Biometrics, for one, can be used for password replacement. This is an ideal solution for identity-based authentication of computer users as it is for securing a computer facility. Biometrics is often seen today as an additional layer of protection to add to other, more traditional, authentication systems like passwords and PINs. Using a second (or even a third) authentication mechanism may provide a much higher level of security to verify the identity of a user. What the future might hold is a shift from multi-type secure authentication to simply using synergistic multiple biometric systems.

Unimodal and Multimodal Biometric Systems:

Unimodal biometric systems are based on identification through only one trait. This is obviously not as accurate as we could wish and might not be adequate to all applications and uses. Also, if collection of that single data is affected in any way (for example by cream on hands that are fingerprint identified or by noise when collecting voice), accuracy would be limited. In addition, collecting only one type of data could exclude part of the user's population when particular disabilities are present.

The possibility of spoofing a single biometric data is higher than that of compromising more. (NOTE: Spoofing is defined as follows:

(ī-pē spoof´ing) (n.) A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an *IP address* ***indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.)***

Newer routers and firewall arrangements can offer protection against IP spoofing.

This is why a multimodal biometric system using more than one trait for identification can be more reliable and resolve ambiguities and accuracy concerns.

As you can see, the science of Biometrics is an extremely important science and one that has "real-world" significance in today's hectic and fast-moving world.

ADVANTAGES AND DISADVANTAGES:

Biometric technology brings information unique for each individual. The information can identify each individual in spite of time variations. It matters not if the first biometric sample was taken years ago. That information is still very credible relative to the identification process. The pillars of e-learning security are: 1.) authentication, 2.) privacy (data confidentiality), 3.) authorization or access control, 4.) data integrity and 5.) non-repudiation of information. Biometric methodology can present techniques that provide all of these requirements with a great deal of reliability. Biometric technology is considered the most effective and safe method for identification because it is very difficult to falsify. Even with this being the case, we have to bear in mind its disadvantages. Since it is an evolving technology, it is not always completely integrated into PC systems. IT departments need to make a conscious decision before making a purchase and changing structure of existent code. Let's now look at why biometric technology is secure.

- **Unique**: The various biometrics systems have been developed around unique characteristics of individuals. The probability of two (2) people sharing the same biometric data is virtually nonexistent. Fingerprints, iris scans, voice recognition, etc. all presenting very distinctive characteristics relative to specific individuals.

- **Cannot be shared**: Because a biometric property is an intrinsic property of an individual, it is extremely difficult to duplicate or share (you cannot give a copy of your face or your hand to someone!).

- **Cannot be copied**: Biometric characteristics are nearly impossible to forge or spoof, especially with new technologies ensuring that the biometric being identified is from a live person.

- **Cannot be lost**: A biometric property of an individual can be lost only in case of serious accident. Biometric properties "travel well". They are with an individual, for the most part, forever.

Even with these facts, there is a relative down side. Errors can occur. These fall into two distinct categories: recognition errors and compromised data.

Recognition Errors

There are two basic types of recognition errors: 1.) the false accept rate (FAR) and 2.) the false reject rate (FRR). A False Accept is when a non-matching pair of biometric data is wrongly accepted as a match by the system. A False Reject is when a matching pair of biometric data is wrongly rejected by the system. The two errors are complementary. When you try to lower one of the errors by varying the threshold, the other error rate automatically increases. There is therefore a balance to be found, with a decision threshold that can be specified to either reduce the risk of FAR, or to reduce the risk of FRR.

In a biometric authentication system, the relative false accept and false reject rates can be set by choosing a particular operating point (i.e., a detection threshold). Very low (close to zero) error rates for both errors (FAR and FRR) at the same time are not possible. By setting a high threshold, the FAR error can be close to zero, and similarly by setting a significantly low threshold, the FRR rate can be close to zero. A meaningful operating point for the threshold is decided based on the application requirements, and the FAR versus FRR error rates at that operating point may be quite different. To provide high security, biometric systems operate at a low FAR instead of the commonly recommended equal error rate (EER) operating point where FAR = FRR.

Compromised Biometric Data

Paradoxically, the greatest strength of biometrics is at the same time its greatest liability. It is the fact that an individual's biometric data does not change over time: the pattern in your iris, retina or palm vein remain the same throughout your life. Unfortunately, this means that should a set of biometric data be compromised, it is compromised forever. The user only has a limited number of biometric features (one face, two hands, ten fingers, two eyes). For authentication systems based on physical tokens such as keys and badges, a compromised token can be easily canceled and the user can be assigned a new token. Similarly, user IDs and passwords can be changed as often as required. But if the biometric data are compromised, the user may quickly run out of biometric features to be used for authentication. This is BIG!!!!!

Vulnerable Points of Biometric Systems

The first stage of usage generally involves scanning the user to acquire his/her unique biometric data. This process is called enrollment. During enrollment, an invariant template is stored in a database that represents the particular individual. This information is unique to the individual.

To authenticate the user against a given ID, this template is retrieved from the database and matched against the new template derived from a newly acquired input signal.

This is similar to a password and in many cases IS the password. It's just not numeric. You first have to create a password for a new user, and then when the user tries to access the system, he or she will be prompted to enter his or her password. If the password entered via the keyboard matches the password previously stored, access will be granted. I'm saying the obvious, but this must be accomplished properly or access will not be granted.

Attacks

There are seven main areas where attacks may occur in a biometric system:

- Presenting fake biometrics or a copy at the sensor; for instance, a fake finger or a face mask. It is also possible to try to resubmit previously stored digitized biometrics signals such as a copy of a fingerprint image or a voice recording.
- Producing feature sets preselected by the intruder by overriding the feature extraction process.
- Tampering with the biometric feature representation. The features extracted from the input signal are replaced with a fraudulent feature set.
- Attacking the channel between the stored templates and the matcher. The stored templates are sent to the matcher through a communication channel. The data traveling through this channel could be intercepted and modified - There is a real danger if the biometric feature set is transmitted over the Internet.

- Corrupting the matcher. The matcher is attacked and corrupted so that it produces pre-selected match scores.

- Tampering with stored templates, either locally or remotely.

- Overriding the match result.

Typically, the weakest link in a biometric system is the enrollment process. A subject can create a new identity by presenting fake documents (i.e. driver's license and or passport) during the enrollment process in a biometric facility. Once a new fake identity has been accepted, an imposter can board a plane, enter a facility or buy restricted materials. When biometric databases are not interconnected, it is entirely possible to steal a genuine identity by presenting other persons' documents during the enrollment process. It is a known fact that some of the September 11 attackers possessed up to a dozen US valid driver licenses with different identities. If a government cannot guarantee the emission of documents to imposters, then a biometric system will do little or nothing to increase security and/or maintain the integrity of the databases. There is not yet a world-wide acceptance of what quality means in a biometric sample. The International Committee for Information Technology Standards (INCITS) in the USA defines quality by three parameters: 1.) character, 2.) fidelity and 3.) utility. The character of a biometric is mostly related with the intrinsic physical condition of an individual (i.e., an individual whose fingerprints have been deteriorated by abrasives has fingerprints with "poor biometric character"). Fidelity is defined as the accuracy by which physical characteristics are represented in a sample; fidelity is highly dependent on sensors and algorithms that capture the sample. Finally, utility is defined as "how valuable is the sample for a given purpose". INCITS has developed a scale for each of the three parameters. A current problem is that many biometric vendors neither rely on the INCITS quality definitions nor on its scales. Another major problem within the biometric industry is the lack of mature standards. Mature standards ensure that vendors comply with common authentication protocols, use common biometric exchange file formats, share common scales of sample quality and develop a common protocol for equipment conformance testing. International committees on standards like the International Standards Organization (ISO) and the US counterpart (INCITS) have developed the BIOAPI standard aimed to fulfill the lack of industry standardization. By December 2011, only about 50 vendors claim to comply with the BIOAPI standards but the BIOAPI consortium cannot verify if they really comply. Legacy biometric equipment that does not conform to the BIOAPI standard is installed in many facilities in the US. The lack of well-trained personnel to manage biometric facilities, the different accuracy of the vendor' s mathematical algorithms and users not well-informed about biometrics, are a set of problems whose consequences are not yet fully addressed. There is a movement aimed to build databases using legacy databases (i.e. use of the driver' s license photos in legacy databases to build a face recognition application). If a legacy database contains many imposters, their direct use for biometric applications will result in a decrease in security for the US population. Building massive biometric applications in society requires a critical mass of technicians capable of managing the applications properly. Typical activities of these technicians are to collect samples for enrollment using complex sensors, to authenticate identity documents (i.e. passports or birth certificates) of individuals before enrolling them, maintain the biometric facility under proper conditions, follow maintenance protocols properly and judge the quality of the samples collected. Technicians who are not well trained can hinder the expected security level of a facility. There are very few technical and professional schools at this moment capable of training the required quantity of technicians with the expected quality. Most biometric technicians are trained onsite by the vendor's personnel.

SOCIAL AND LEGAL IMPLICATIONS OF BIOMETRIC TECHNOLOGY:

Biometric technology, like any other technology, suffers from unexpected and unforeseen consequences that many other technologies have experienced when implemented in society. Problems can arise when massive implementations are done. What happens when a biometric file is stolen? A password or a credit card can be easily replaced and the stolen information somehow invalidated. A biometric template is nothing more than another binary file in a database; therefore, can be stolen by hackers as any other file. Losing our own biometrics may not be a matter of replacement; “with a biometric it is very difficult, if not impossible, for any individual to disassociate oneself from one’ s biometric”. If biometric databases are not protected properly and information is stolen, the consequences can be permanently devastating. There is no easy way to program the biometric systems to not recognize a legit biometric of an authentic user. Once the standards are in place and biometric systems are interconnected around the world, a stolen biometric can be used improperly (i.e, by using telecommunication channels) with massive damages to the public. What happens when biometric is used for surveillance purposes? Face recognition surveillance may be used for security purposes to monitor well-known criminals. Faces can also be captured from social websites, sporting events, concurred streets or malls and used for nonrelated security purposes without people’ s consent in clear violation to the individual’ s right to privacy: “If there is any law in the history of technology it is that technologies are rarely used in ways that their inventors intended”. Are minorities disadvantaged in biometric applications? It has been seriously suggested that many biometric applications are biased toward certain minorities. The Face Vendor Recognition Test (FRVT), organized by the US government in 2002, showed that identification rates for males were six percent (6%) to nine percent (9%) points higher than that of females and recognition rates for older people were higher than younger people. Based on the FRVT of 2002, Givens also concluded: “Asians are easier (to recognize) than whites, African-Americans are easier than whites, other race members are easier than whites, old people are easier than young people, other skin people are easier to recognize than clear skin people…”. Therefore the multiplicity of algorithms in the market may be designed with inherent and unforeseen biases. If biases are proven, it will make the use of these systems illegal and unethical, especially when social services or access to public facilities (like the right to enter a public park or stadium) are denied to minority groups when falsely rejecting them in higher proportions with respect to other groups based on their race, color or gender. How will population with disabilities (or lacking physical traits) will be enrolled or authenticated in biometric databases? People with just one hand, no iris or retina, no fingers, and in general people lacking physicals characteristics in need of using a biometric facility, may suffer discrimination and unnecessary delays in biometric systems. A well-developed, well-designed biometric system should allow these persons alternative ways to enroll and authenticate, yet delays and processes of bypassing the biometric systems may give them hardships each time they want to access a resource or use a facility which may be an ethical violation of their rights. Finally, lack of mature standards and standardization enforcement may create a different set of results for similar facilities located in different geographic sites requiring similar sets of security requirements. Lack of proper standardization has the potential to discriminate users based on the geographic biometric facility they want to use. A user may be well-recognized in one facility but rejected in another one without major explanation. The US government is promoting contests among vendors in order to motivate them to comply with standards and to improve their equipment accuracies, but so far this is a voluntary activity. Eventually, most vendors in the US will comply with standards. The US government is mostly conducting business with vendors who comply with the BIOAPI standard, yet privates companies are free to install any other system without standard enforcements. Confusion from the public and discrimination in general will be some of the major social consequences when there are no mature standards and/or the adoption of a common standard by most vendors is not enforced.

You can see from this that although much better than PIN numbers and passwords, biometrics are not foolproof. Let's look now at each methodology relative to advantages and disadvantages.

Facial recognition:

Advantages:

a. Non-intrusive to subject

b. Inexpensive technology.

Disadvantages:

a. 2D recognition is affected by changes in lighting, the person's hair, the age, and if the person wears glasses.

b. Requires camera equipment for user identification; thus, it is not likely to become popular until most PCs include cameras as standard equipment. We might mention here that cameras installed as "standard" equipment are becoming the norm. This is due to acceptance of social media.

Voice recognition:

Advantages:

a. Non intrusive. High social acceptability.

b. Verification time is about five seconds.

c. Inexpensive technology.

Disadvantages:

a. A person's voice can be easily recorded and used for unauthorized PC or network.

b. Low accuracy.

c. An illness such as a cold can change a person's voice, making absolute identification difficult or impossible.

Signature recognition:

Advantages:

a. Non-intrusive.

b. Short time for verification (about five seconds).

c. Inexpensive technology.

Disadvantages:

a. Signature verification is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification.

b. Error rate: 1 in 50.

DNA:

Advantages:

a. Very high accuracy.

b. It impossible that the system made mistakes.

c. It is standardized

Disadvantages:

a. Extremely intrusive.

b. Very expensive.

Retinal scanning:

Advantages:

a. Very high accuracy.

b. There is no known way to replicate a retina.

c. The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to be taken with retinal scans to be sure the user is a living human being.

Disadvantages:

a. Very intrusive.

b. It has the stigma of consumer's thinking it is potentially harmful to the eye.

c. Comparisons of template records can take upwards of ten (10) seconds, depending on the size of the database.

d. Very expensive.

Iris recognition:

Advantages:

a. Very high accuracy.

b. Verification time is generally less than five (5) seconds.

c. The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being.

Disadvantages:

a. Intrusive.

b. A significant amount of memory for the data to be stored.

c. Very expensive

Fingerprint:

Advantages:

a. Very high accuracy.

b. Is the most economical biometric PC user authentication technique.

c. It is one of the most developed biometrics

d. Easy to use.

e. Small storage space required for the biometric template, reducing the size of the database memory required

f. It is standardized.

Disadvantages:

a. For some people it is very intrusive, because is still related to criminal identification.

b. It can make mistakes with the dryness or dirty of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly).

c. Image captured at five hundred (500) dots per inch (dpi). Resolution: eight (8) bits per pixel. A 500 dpi fingerprint image at eight (8) bits per pixel demands a large memory space, 240 Kbytes approximately with a compression factor of 10 approximately.

Hand Geometry:

Advantages:

a. Though it requires special hardware to use, it can be easily integrated into other devices or systems.

b. It has no public attitude problems as it is associated most commonly with authorized access.

c. The amount of data required to uniquely identify a user in a system is the smallest by far, allowing it to be used with Smart Cards easily.

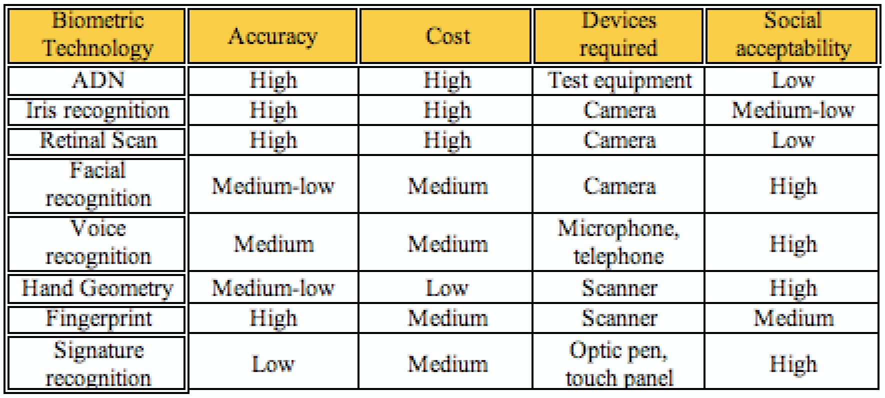
Disadvantages:

a. Very expensive

b. Considerable size.

c. It is not valid for arthritic person, since they cannot put the hand on the scanner properly.

The following table will indicate the biometric mode vs. accuracy, relative cost of devices required and social acceptability.



Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
ADN	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

FIGURE 2: BIOMETRIC TECHNOLOGY VS. DESIRABILITY

HISTORY:

The following is a rather lengthy chronology of history relating to biometrics and how the technology has evolved over the decades to the present point. I think it is very important to detail the evolution of the technology so please bear with me. You will see how the various biometric modes have developed and grown much more important over time.

Obviously, the oldest and most basic example of a characteristic that is used for recognition by humans is facial recognition. Since the beginning of civilization, humans have used faces to identify known and unknown individuals. This simple task became increasingly more challenging as populations increased and as more convenient methods of travel introduced many new individuals into once-small communities. The concept of human-to-human recognition is also seen in behavioral-predominant biometrics such as speaker and gait recognition. Individuals use these characteristics, somewhat unconsciously, to recognize known individuals on a day-to-day basis.

Other characteristics have also been used throughout the history of civilization as a more formal means of recognition. Several examples are:

• In a cave estimated to be at least 31,000 years old, the walls are adorned with paintings believed to be created by prehistoric men who lived there. Surrounding these paintings are numerous handprints that are felt to "have acted as an unforgettable signature" of its originator.

• There is evidence that fingerprints were used as a person's mark as early as 500 B.C. "Babylonian business transactions are recorded in clay tablets that include fingerprints."

• Joao de Barros, a Spanish explorer and writer, wrote that early Chinese merchants used fingerprints to settle business transactions. Chinese parents also used fingerprints and footprints to differentiate children from one another. If you are a parent, you know that footprints are impressed on birth certificates to indicate association.

• In early Egyptian history, traders were identified by their physical descriptors to differentiate between trusted traders of known reputation and previous successful transactions, and those new to the market.

By the mid-1800s, with the rapid growth of cities due to the industrial revolution and more productive farming, there was a formally recognized need to identify people. Merchants and authorities were faced with increasingly larger and more mobile populations and could no longer rely solely on their own experiences and local knowledge. Influenced by the writings of Jeremy Betham and other Utilitarian thinkers, the courts of this period began to codify concepts of justice that endure with us to this day. Most notably, justice systems sought to treat first time offenders more leniently and repeat offenders more harshly. This created a need for a formal system that recorded offenses along with measured identity traits of the offender. The first of two approaches was the Bertillon system of measuring various body dimensions, which originated in France. These measurements were written on cards that could be sorted by height, arm length or any other parameter. This field was called anthropometries.

The other approach was the formal use of fingerprints by police departments. This process emerged in South America, Asia, and Europe. By the late 1800s a method was developed to index fingerprints that provided the ability to retrieve records as Bertillon's method did but that was based on a more individualized metric- fingerprint patterns and ridges. The first such robust system for indexing fingerprints was developed in India by Azizul Haque for Edward Henry, Inspector General of Police, Bengal, India. This system, called the Henry System, and variations on it are still in use for classifying fingerprints.

True biometric systems began to emerge in the latter half of the twentieth century, coinciding with the emergence of computer systems. The nascent field experienced an explosion of activity in the 1990s and began to surface in everyday applications in the early 2000s.

Timeline of Modern Biometrics History:

1858 – First systematic capture of hand images for identification purposes is recorded

Sir William Herschel, working for the Civil Service of India, recorded a handprint on the back of a contract for each worker to distinguish employees from others who might claim to be employees when payday arrived. This was the first recorded systematic capture of hand and finger images that were uniformly taken for identification purposes.

1870 – Bertillon develops anthropometries to identify individuals

Alphonse Bertillon developed "Bertillonage" or anthropometries, a method of identifying individuals based on detailed records of their body measurements, physical descriptions and photographs. Repeat criminal offenders often provided different aliases when arrested. Bertillon noted that although they could change their names, they could not change certain elements of their bodies. Police authorities throughout the world used his system, until its use quickly faded when it was discovered that some people shared the same measurements.

1892 – Galton develops a classification system for fingerprints

Sir Francis Galton wrote a detailed study of fingerprints in which he presented a new classification system using prints from all ten fingers. The characteristics (minutiae) that Galton used to identify individuals are still used today. These details are often referred to as Galton's details.

1894 – The Tragedy of Pudd'nhead Wilson is published

In The Tragedy of Pudd'nhead Wilson, author Mark Twain mentions the use of fingerprints for identification. In the story, a man on trial calls on the comparison of his fingerprints to those left at the crime scene to prove his innocence.

1896 – Henry develops a fingerprint classification system

Sir Edward Henry, Inspector General of the Bengal Police, was in search of a method of identification to implement concurrently or to replace anthropometries. Henry consulted Sir Francis Galton regarding fingerprinting as a method of identifying criminals. Once the fingerprinting system was implemented, one of Henry's workers, Azizul Haque, developed a method of classifying and storing the information so that searching could be performed easily and efficiently. Sir Henry later established the first British fingerprint files in London. The Henry Classification System, as it came to be known, was the precursor to the classification system used for many years by the Federal Bureau of Investigation (FBI) and other criminal justice organizations that perform ten print fingerprint searches.

1903 – NY State Prisons begin using fingerprints

"The New York Civil Service Commission established the practice of fingerprinting applicants to pre-vent them from having better qualified persons take their tests for them." This practice was adopted by the New York state prison system where fingerprints were used "for the identification of criminals in 1903.

In 1904 the fingerprint system accelerated when the United States Penitentiary at Leavenworth, Kansas, and the St. Louis, Missouri Police Department both established fingerprint bureaus. During the first quarter of the 20th century, more and more local police identification bureaus established fingerprint systems. The growing need and demand by police officials for a national repository and clearinghouse for fingerprint records led to an Act of Congress on July 1, 1921, establishing the Identification Division of the FBI."

1903 – Bertillon System collapses

Two men, determined later to be identical twins, were sentenced to the US Penitentiary at Leavenworth, KS, and were found to have nearly the same measurements using the Bertillon system. Although the basis of this story has been subsequently challenged, the story was used to argue that Bertillon measurements were inadequate to differentiate between these two individuals.

1936 – Concept of using the iris pattern for identification is proposed

Ophthalmologist Frank Burch proposed the concept of using iris patterns as a method to recognize an individual.

1960s – Face recognition becomes semi-automated

The first semi-automatic face recognition system was developed by Woodrow W. Bledsoe under contract to the US Government. This system required the administrator to locate features such as eyes, ears, nose and mouth on the photographs. This system relied solely on the ability to extract useable feature points. It calculated distances and ratios to a common reference point that was compared to the reference data.

1960 – First model of acoustic speech production is created

A Swedish Professor, Gunnar Fant, published a model describing the physiological components of acoustic speech production. His findings were based on the analysis of x-rays of individuals making specified phonic sounds. These findings were used to better understand the biological components of speech, a concept crucial to speaker recognition.

1963 – Hughes research paper on fingerprint automation is published

1965 -Automated signature recognition research begins

North American Aviation developed the first signature recognition system in 1965.

1969 – FBI pushes to make fingerprint recognition an automated process

In 1969, the Federal Bureau of Investigation (FBI) began its push to develop a system to automate its fingerprint identification process, which was quickly becoming overwhelming and required many man-hours. The FBI contracted the National Institute of Standards and Technology (NIST) to study the process of automating fingerprint identification. NIST identified two key challenges: (1) scanning fingerprint cards and identifying minutiae and (2) comparing and matching lists of minutiae.

1970s – Face Recognition takes another step towards automation

Goldstein, Harmon, and Lesk used 21 specific subjective markers such as hair color and lip thickness to automate face recognition. The problem with both of these early solutions was that the measurements and locations were manually computed.

1970 – Behavioral components of speech are first modeled

The original model of acoustic speech production, developed in 1960, was expanded upon by Dr. Joseph Perkell, who used motion x-rays and included the tongue and jaw. The model provided a more detailed understanding of the complex behavioral and biological components of speech.

1974- First commercial hand geometry systems become available

The first commercial hand geometry recognition systems became available in the early 1970s, arguably the first commercially available biometric device after the early deployments of fingerprinting in the late 1960s. These systems were implemented for three main purposes: physical access control; time and attendance; and personal identification.

1975 – FBI funds development of sensors and minutiae extracting technology

The FBI funded the development of scanners and minutiae extracting technology, which led to the development of a prototype reader. At this point, only the minutiae were stored because of the high cost of digital storage. These early readers used capacitive techniques to collect the fingerprint characteristics. Over the next decades, NIST focused on and led developments in automatic methods of digitizing inked fingerprints and the effects of image compression on image quality, classification, extraction of minutiae, and matching. The work at NIST led to the development of the M40 algorithm, the first operational matching algorithm used at the FBI. Used to narrow the human search, this algorithm produced a significantly smaller set of images that were then provided to trained and specialized human technicians for evaluation. Developments continued to improve the available fingerprint technology.

1976 – First prototype system for speaker recognition is developed

Texas Instruments developed a prototype speaker recognition system that was tested by the US Air Force and The MITRE Corporation.

1977 – Patent is awarded for acquisition of dynamic signature information

Veripen, Inc. was awarded a patent for a “Personal identification apparatus” that was able to acquire dynamic pressure information. This device allowed the digital capture of the dynamic characteristics of an individual’s signature characteristics. The development of this technology led to the testing of automatic handwriting verification (performed by The MITRE Corporation) for the Electronic Systems Division of the United States Air Force.

1980s – NIST Speech Group is established

The National Institute of Standards and Technology (NIST) developed the NIST Speech Group to study and promote the use of speech processing techniques. Since 1996, under funding from the National Security Agency, the NIST Speech Group has hosted yearly evaluations – the NIST Speaker Recognition Evaluation Workshop- to foster the continued advancement of the speaker recognition community.

1985 – Concept that no two irises are alike is proposed

Drs. Leonard Flom and Aran Safir, ophthalmologists, proposed the concept that no two irises are alike.

1985 – Patent for hand identification is awarded

The commercialization of hand geometry dates to the early 1970s with one of the first deployments at the University of Georgia in 1974. The US Army began testing hand geometry for use in banking in about 1984. These deployments predate the concept of using the geometry of a hand for identification as patented by David Sidlauskas.

1986 – Exchange of fingerprint minutiae data standard is published

The National Bureau of Standards (NBS) – now the National
Institutes of Standards and Technology (NIST) – published, in collaboration with ANSI, a standard for the exchange of fingerprint minutiae data (ANSI/ NBS-I CST 1-1986). This was the first version of the current fingerprint interchange standards used by law enforcement agencies around the world today.

1986 – Patent is awarded stating that the iris can be used for identification

Drs. Leonard Flom and Aran Safir were awarded a patent for their concept that the iris could be used for identification. Dr. Flom approached Dr. John Daugman to develop an algorithm to automate identification of the human iris.

1988 – First semi-automated facial recognition system is deployed

In 1988, the Lakewood Division of the Los Angeles County Sheriff's Department began using composite drawings (or video images) of a suspect to conduct a database search of digitized mug shots.

1988 – Eigenface technique is developed for face recognition

Kirby and Sirovich applied principle component analysis, a standard linear algebra technique, to the face recognition problem. This was a milestone because it showed that less than one hundred values were required to approximate a suitably aligned and normalized face image.

1991 – Face detection is pioneered, making real time face recognition possible

Turk and Pentland discovered that while using the Eigen faces techniques, the residual error could be used to detect faces in images. The result of this discovery meant that reliable real time automated face recognition was possible. They found that this was somewhat constrained by environmental factors, but the discovery caused a large spark of interest in face recognition development.

1992 – Biometric Consortium is established within US Government

The National Security Agency initiated the formation of the Biometric Consortium and held its first meeting in October of 1992. The Consortium was chartered in 1995 by the Security Policy Board, which was abolished in 2001. Participation in the Consortium was originally limited to government agencies; members of private industry and academia were limited to attending in an observer capacity. The Consortium soon expanded its membership to include these communities and developed numerous working groups to initiate and/or expand efforts in testing, standards development, interoperability, and government cooperation. With the explosion of biometric activities in the early 2000s, the activities of these working groups were integrated into other organizations (such as INCITS, ISO, and the NSTC Subcommittee on Biometrics) in order to expand and accelerate their activities and impacts. The Consortium itself remains active as a key liaison and discussion forum between government, industry, and academic communities.

1993 – FacE Recognition Technology (FERET) program is initiated

The FacE Recognition Technology (FERET) Evaluation was sponsored from 1993-1997 by the Defense Advanced Research Products Agency (DARPA) and the DoD Counterdrug Technology Development Program Office in an effort to encourage the development of face recognition algorithms and technology. This evaluation assessed the prototypes of face recognition systems and propelled face recognition from its infancy to a market of commercial products.

1994- First iris recognition algorithm is patented

Dr. John Daugman was awarded a patent for his iris recognition algorithms. Owned by Iridian Technologies, the successor to lriScan, Inc. – this patent is the cornerstone of most commercial iris recognition products to date.

1994 – Integrated Automated Fingerprint Identification System (IAFIS) competition is held

The next stage in fingerprint automation occurred at the end of the Integrated Automated Fingerprint Identification System (IAFIS) competition. The competition identified and investigated three major challenges: (1) digital fingerprint acquisition, (2) local ridge characteristic extraction, and (3) ridge characteristic pattern matching. The demonstrated model systems were evaluated based on specific performance requirements. Lockheed Martin was selected to build the FBI's IAFIS.

1994 – Palm System is benchmarked

The first known Automated Fingerprint Identification Systems (AFIS) system built to support palm prints is believed to have been built by a Hungarian company known as RECOWARE Ltd. In late 1994, latent experts from the United States benchmarked this palm system, RECOderm™, in Hungary and invited RECOWARE Ltd. to the 1995 International Association for Identification (I AI) conference in Costa Mesa, California. The palm and fingerprint identification technology embedded in the RECOderm TM System was bought by Lockheed Martin Information Systems in 1997.

1994 – INSPASS is implemented

The Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) was a biometrics implementation that allowed travelers to bypass immigration lines at selected airports throughout the US until it was discontinued in late 2004. Authorized travelers received a card encoded with their hand geometry information. Rather than being processed by an Immigration Inspector, INSPASS travelers presented their tokens (cards) with the encoded information and their hands to the biometric device. Upon verification of the identity claimed, the individual could proceed to the customs gate, thus bypassing long inspection lines and speeding entry into the US.

1995 – Iris prototype becomes available as a commercial product

The joint project between the Defense Nuclear Agency and lriscan resulted in the availability of the first commercial iris product.

1996 – Hand geometry is implemented at the Olympic Games

A major public use of hand geometry occurred at the 1996 Atlanta Olympic Games where hand geometry systems were implemented to control and protect physical access to the Olympic Village. This was a significant accomplishment because the systems handled the enrollment of over 65,000 people. Over 1 million transactions were processed in a period of 28 days.

1996 – NIST begins hosting annual speaker recognition evaluations

Under funding from the National Security Agency, the National Institute of Standards and Technology (NIST) Speech Group began hosting yearly evaluations in 1996. The NIST Speaker Recognition Evaluation Workshop aims to foster the continued advancement of the speaker recognition community.

1997 – First commercial, generic biometric interoperability standard is published

Sponsored by NSA, the Human Authentication API (HA-API) was published as the first commercial, generic biometric interoperability standard and focused on easing integration of and allowing for interchangeability and vendor independence. It was a breakthrough in biometric vendors working together to advance the industry through standardization and was the precursor to subsequent biometric standardization activities.

1998- FBI launches COOIS (DNA forensic database)

The FBI launched Combined DNA Index System (CODIS) to digitally store, search, and retrieve DNA markers for forensic law enforcement purposes. Sequencing is a laboratory process taking between 40 minutes and several hours.

1999 – Study on the compatibility of biometrics and machine readable travel documents is launched

The International Civil Aviation Organization's (ICAO) Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) initiated a study to determine the "compatibility of currently available biometric technologies with the issuance and inspection processes relevant to MRTDs; and quantifying these compatibilities to determine whether one or more technologies could/should be adopted as the international standard for application in MRTDs."

1999 – FBI's IAFIS major components become operational

IAFIS, the FBI's large-scale ten-fingerprint (open-set) identification system, became operational. Prior to the development of the standards associated with this system, a fingerprint collected on one system could not be searched against fingerprints on another system. The development of this system addressed the issues associated with communication and information exchange between standalone systems as well as the introduction of a national network for electronic submittal of fingerprints to the FBI. IAFIS is used for criminal history background checks and identification of latent prints discovered at crime scenes. This system provides automated ten print and latent search capabilities, electronic image storage of fingerprints and facial images, and electronic exchange of fingerprints and search responses.

2000 – First Face Recognition Vendor Test (FRVT 2000) is held

Multiple US Government agencies sponsored the Face Recognition Vendor Test (FRVT) in 2000. FRVT 2000 served as the first open, large-scale technology evaluation of multiple commercially available biometric systems. Additional FRVTs have been held in 2002 and 2006, and the FRVT model has been used to perform evaluations of fingerprint (2003) and iris recognition (2006). FRVT's primary purpose is to evaluate performance on large-scale databases.

2000 – First research paper describing the use of vascular patterns for recognition is published

This paper describes the technology that was to become the first commercially available vascular pattern recognition system in 2000. The technology uses the subcutaneous blood vessel pattern in the back of the hands to achieve recognition.

2000 – West Virginia University biometrics degree program is established

West Virginia University (WVU) and the FBI, in consultation with professional associations such as the International Association for Identification, established a bachelor's degree program in Biometric Systems in 2000. While many universities have long had biometrics-related courses, this is the first biometrics-based degree program. WVU encourages program participants to obtain a dual-degree in Computer Engineering and Biometric Systems as the biometric systems degree is not accredited.

2001 – Face recognition is used at the Super Bowl in Tampa, Florida

A face recognition system was installed at the Super Bowl in January 2001 in Tampa, Florida, in an attempt to identify "wanted" individuals entering the stadium. The demonstration found no "wanted" individuals but managed to misidentify as many as a dozen innocent sports fans. Subsequent media and Congressional inquiries served to introduce both biometrics and its associated privacy concerns into the consciousness of the general public.

2002 – ISO/IEC standards committee on biometrics is established

The International Organization for Standardization (ISO) established the ISO/IEC JTC1 Subcommittee 37 (JTC1 /SC37) to support the standardization of generic biometric technologies. The Subcommittee develops standards to promote interoperability and data interchange between applications and systems.

2002 – M 1 Technical Committee on Biometrics is formed

The M1 Technical Committee on Biometrics is the US Technical Advisory Group (TAG) to the JTC1 ISC37. This technical committee reports to the InterNational Committee on Information Technology Standards (INCITS), an accredited organization of the American National Standards Institute (ANSI), which facilitates the development of standards among accredited organizations.

2002 – Palm Print Staff Paper is submitted to Identification Services Committee

In April 2002, a Staff Paper on palm print technology and Integrated Automated Fingerprint Identification System (IAFIS) palm print capabilities was submitted to the Identification Services (IS) Subcommittee, Criminal Justice Information Services Division (CJIS) Advisory Policy Board (APB). The Joint Working Group called “for strong endorsement of the planning, costing, and development of an integrated latent print capability for palms at the CJIS Division of the FBI.” As a result of this endorsement and other changing business needs for law enforcement, the FBI announced the Next Generation IAFIS (NGI) initiative. A major component of the NGI initiative is development of the requirements for and deployment of an integrated National Palm Print Service.

2003 – Formal US Government coordination of biometric activities begins

The National Science & Technology Council, a US Government cabinet-level council, established a Subcommittee on Biometrics to coordinate biometrics R&D, policy, outreach, and international collaboration.

2003 – ICAO adopts blueprint to integrate biometrics into machine readable travel documents

On May, 28 2003, The International Civil Aviation Organization (ICAO) adopted a global, harmonized blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs) … Facial recognition was selected as the globally interoperable biometric for machine-assisted
identity confirmation with MRTDs.

2003 – European Biometrics Forum is established

The European Biometrics Forum is an independent European organization supported by the European Commission whose overall vision is to establish the European Union as the World Leader in Biometrics Excellence by addressing barriers to adoption and fragmentation in the marketplace. The forum also acts as the driving force for coordination, support and strengthening of the national bodies.

2004 – US-VISIT program becomes operational

The United States Visitor and Immigrant Status Indication Technology (US-VISIT) program is the cornerstone of the DHS visa issuance and entry I exit strategy. The US-VISIT program is a continuum of security measures that begins overseas at the Department of State's visa issuing posts, and continues through arrival to and departure from the US. Using biometrics, such as digital inkless fingerprints and digital photographs, the identity of visitors requiring a visa is now matched at each step to ensure that the person crossing the US border is the same person who received the visa. For visa-waiver travelers, the capture of biometrics first occurs at the port of entry to the US. By checking the biometrics of a traveler against its databases, US-VISIT verifies whether the traveler has previously been determined inadmissible, is a known security risk (including having outstanding wants and warrants), or has previously overstayed the terms of a visa. These entry I exit procedures address the US critical need for tighter security and its ongoing commitment to facilitate travel for the millions of legitimate visitors welcomed each year to conduct business, learn, see family, or tour the country.

2004 – DOD implements ABIS

The Automated Biometric Identification System (ABIS) is a Department of Defense (DoD) system implemented to improve the US Government's ability to track and identify national security threats. The associated collection systems include the ability to collect, from enemy combatants, captured insurgents, and other persons of interest, ten rolled fingerprints, up to five mug shots from varying angles, voice samples (utterances), iris images, and an oral swab to collect DNA.

2004 – Presidential directive calls for mandatory government-wide personal identification card for all federal employees and contractors

In 2004, President Bush issued Homeland Security Presidential Directive 12 (HSPD-12) for a mandatory, government-wide personal identification card that all federal government departments and agencies will issue to their employees and contractors requiring access to Federal facilities and systems. Subsequently, Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) for Federal Employees and Contractors, specifies the technical and operational requirements for the PIV system and card. NIST Special Publication 800-76 (Biometric Data Specification for Personal Identity Verification) is a companion document to FIPS 201 describing how the standard will be acquiring, formatting and storing fingerprint images and templates for collecting and formatting facial images; and specifications for biometric devices used to collect and read fingerprint images. The publication specifies that two fingerprints be stored on the card as minutia templates.

2004 – First statewide automated palm print databases are deployed in the US

In 2004, Connecticut, Rhode Island and California established statewide palm print databases that allow law enforcement agencies in each state to submit unidentified latent palm prints to be searched against each other's database of known offenders.

2004 – Face Recognition Grand Challenge begins

The Face Recognition Grand Challenge (FRGC) is a US Government-sponsored challenge problem posed to develop algorithms to improve specific identified areas of interest in face recognition. Participating researchers analyze the provided data, try to solve the problem, and then reconvene to discuss various approaches and their results – an undertaking that is driving technology improvement. Participation in this challenge demonstrates an expansive breadth of knowledge and interest in this biometric modality.

2005 – US patent for iris recognition concept expires

The broad US patent covering the basic concept of iris recognition expired in 2005, providing marketing opportunities for other companies that have developed their own algorithms for iris recognition. However, the patent on the IrisCodes® implementation of iris recognition developed by Dr. Daugman will not expire until 2011.

2005 – Iris on the Move is announced at Biometrics Consortium Conference

At the 2005 Biometrics Consortium conference, Sarnoff Corporation (now SRI International) demonstrated Iris on the Move, a culmination of research and prototype systems sponsored by the Intelligence Technology Innovation Center (ITIC), and previously by the Defense Advanced Research Projects Agency (DARPA). The system enables the collection of iris images from individuals walking through a portal.

2008 – U.S. Government begins coordinating biometric database use

Finger image and facial quality measurement algorithms and related toolset development was finalized. An iris quality measurement algorithm was also developed.

The FBI and Department of Defense also started working on next generation databases designed to include iris, face and palm data, in addition to fingerprint records.

The Department of Homeland Security denied an individual entry into the U.S. after cross-matched biometric data identified the individual as a known or suspected terrorist

2010 – U.S. national security apparatus utilizes biometrics for terrorist identification

A fingerprint from evidence collected at the believed 9/11 planning location was positively matched to a GITMO detainee. Other fingerprints were identified from items seized at other locations associated with 9/11.

2011 – Biometric identification used to identify body of Osama bin Laden

Along with DNA, the CIA used facial recognition technology to identify the remains of Osama bin Laden with 95 percent certainty.

2013 – Apple includes fingerprint scanners into consumer-target smartphones

Touch ID is a fingerprint recognition feature, designed and released by Apple Inc., that was made available on the i-Phone 5S, the i-Phone 6 and i-Phone 6 Plus, the i-Pad Air 2, and the i-Pad Mini 3. Touch ID is heavily integrated into i-OS devices, allowing users to unlock their device, as well as make purchases in the various Apple digital media stores (iTunes Store, the App Store, i-Bookstore), and to authenticate Apple Pay online or in apps. On announcing the feature, Apple made it clear that the fingerprint information is stored locally in a secure location on the Apple A7 (in i-Phone 5S and i-Pad mini 3 (APL0698), A8 (in i-Phone 6 and i-Phone 6 Plus), or A8X (in i-Pad Air 2) chip, rather than being stored remotely on Apple servers or in i-Cloud, making it very difficult for external access.

As mentioned earlier, Biometrics is a developing technology and one in which daily usage will continue to increase. The movement to this technology represents an economic classification unto itself. We look at that now.

GLOBAL USAGE OF BIOMETRICS AND FUTURE MARKETS:

The biometrics market is one of the fastest growing sectors of electronic security on the global landscape. Increasing government spending, national ID projects, e-passports and visas, rising crime rates, growing terrorist activities, cybercrimes, and data thefts are the factors that are spurring the market for various biometrics technologies globally.

According to 6Wresearch, the Global Biometrics Market is projected to reach $21.9 billion by 2020. North America leads overall markets, where the United States is the major revenue generating country in this region. Increasing homeland security, government spending, research and development activities are driving the growth of the U.S. in North American biometrics market.

A market projection by Tractica forecasts global biometrics market will increase from US $2bn in 2015 to $14.9bn by 2024, with cumulative revenue for the 10-year period reaching $67.8bn. According to their forecast, "Biometric modalities that are likely to generate the most revenue include fingerprint, iris image and voice recognition," the company says. "Key use cases include consumer device authentication, mobile banking, ATMs, government IT systems, point of sale (POS) transactions, pharmacy dispensing and wearable device authentication." This is illustrated by the following graphic:

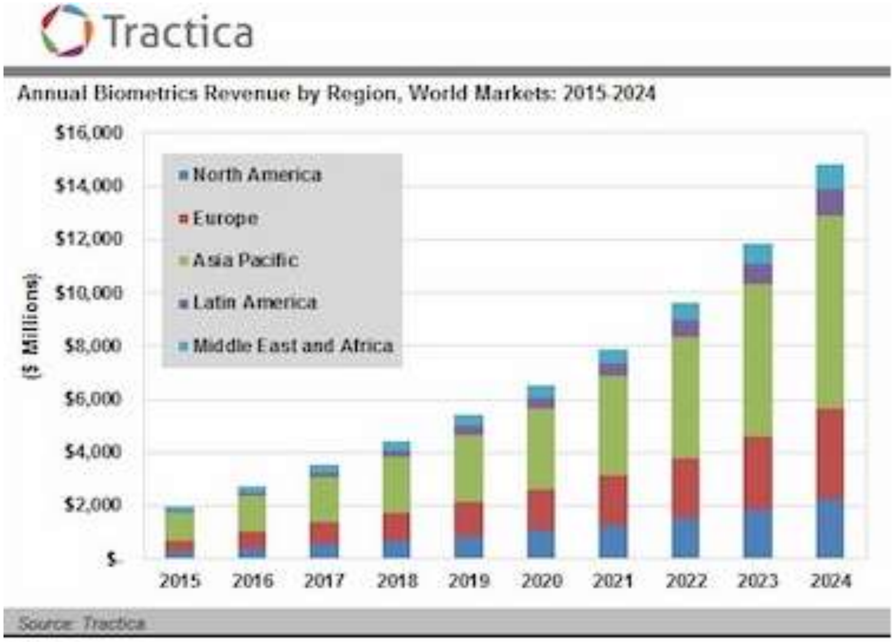


FIGURE 3: ANNUAL BIOMETRICS REVENUE BY REGION

Until 2014, the North American region dominated overall biometrics market; however, by the end of 2015, the share of the region is expected to decline to become second largest in the industry. Growth in Asia-Pacific (APAC) biometrics market is exhibited as the major factor for the declining share of North American region. Surging security spending, introduction of several government projects, increasing IT spending, data thefts, and shift from traditional smart card based systems towards biometric based systems are boosting the growth of Asia- Pacific biometrics market.

Fingerprint biometrics technology accounts for majority of the market share in the overall biometrics market. Ease of usage and affordable in nature have resulted for its market dominance. However, in the forecast period, share of fingerprint technology is expected to decline due to growth in other biometrics technologies such as Face, IRIS, Vein and also the adoption of multimodal biometrics systems.

KEY COMPANIES:

Several key companies in the global biometrics market are given below. Please keep in mind; the names represent only a few of the existing possibilities. Since the United States represents the leading edge relative to biometric usage, it stands to reason there are more U.S. companies to choose from. I would recommend you receive quotes from several sources, including vendors off-shore.

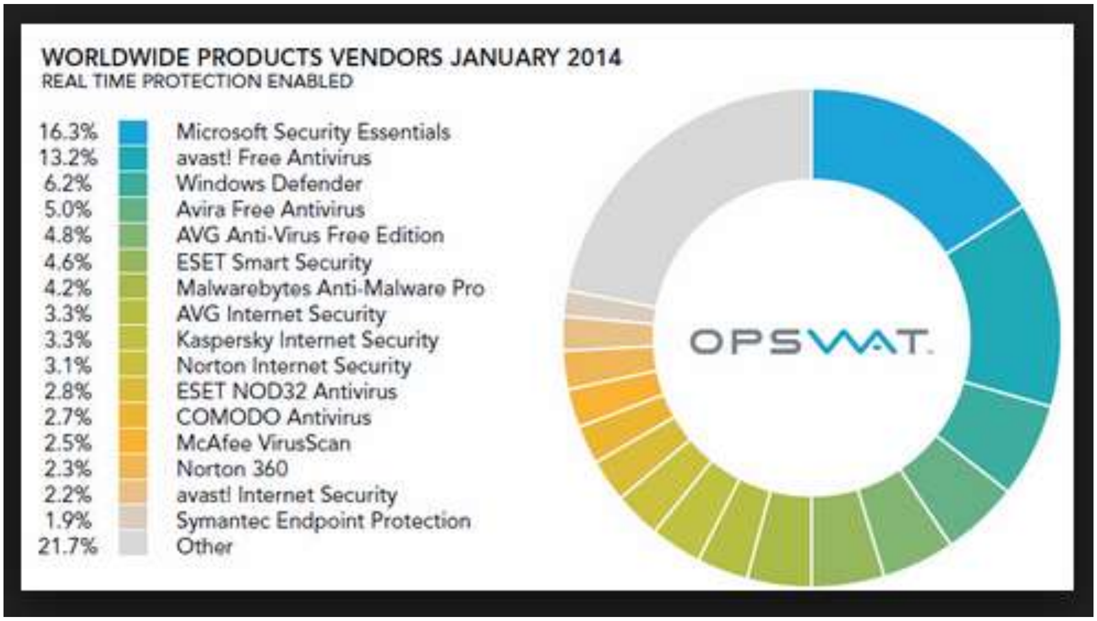


FIGURE 4: POSSIBLE VENDORS

Additional possibilities are:

- Qualcomm
- Crossmatch
- SRI International
- M2SYS
- SecuGen
- Schlage
- MSI Security
- Fujitsu Frontech North America
- e-DATA
- Digital Persona
- Actatek
- 360 Biometrics
- Triad Biometrics
- Integrated Biometrics
- BioLink Solutions (Bio-Metrica)

We definitely recommend you do a data search to discover which vendor is right for you. At end of this course, we list several vendor organizations that will allow additional research relative to the many possibilities.

MARKET SEGMENTS BY TECHNOLOGY:

A quick breakdown of the various segments look as follows:

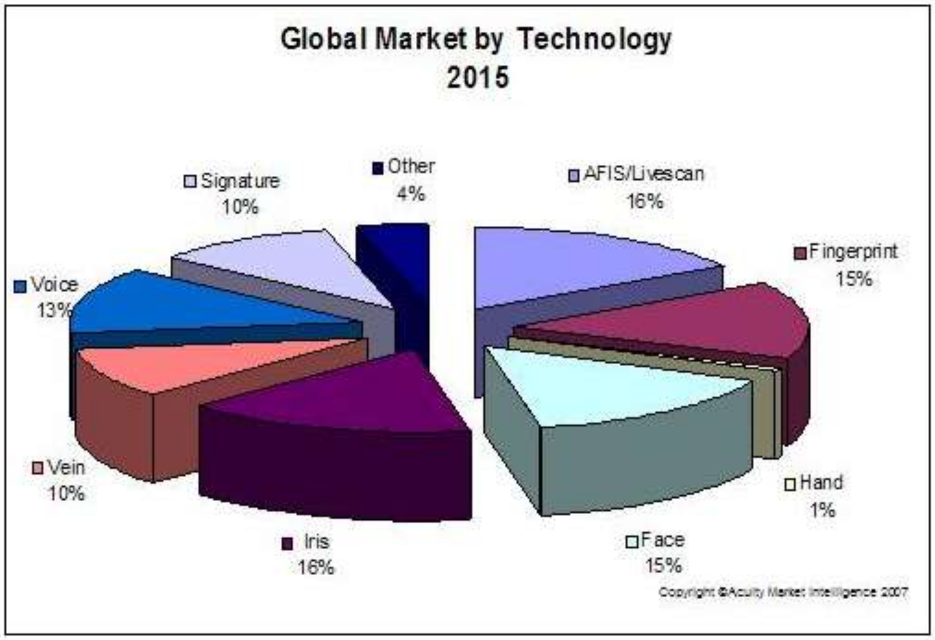


FIGURE 5: GLOBAL MARKET BY TECHNOLOGY SECTOR

As you can see from above, the categories are basically equal in percentages used to identify a specific individual with no one category being significantly better than another.

The figure below will indicate the breakdown for the basic core technology relative to solutions available. Definitions for each solution category are as follows:

Integrated biometric solutions are applications software products or “middleware” software frameworks that utilize multiple types of biometric technologies in a mixed or “multi-modal” context. These solutions may be specifically tailored for vertical industries (like banking or health care) to address a specific business problem within an industry, or they may be more generalized to address a more horizontal range of identification and authentication applications (such as physical access control or network logon). Integrated biometric solutions provide an infrastructure that manages the enrollment, secure storage, communication, and matching functions associated with the use of biometrics. Since no one technology is perfect and there is no single solution that fits all situations, integrated biometric solutions often provide the flexibility to utilize more than one type of biometric technology, individually or in combination, and may include the integration of biometrics with other companion technologies, like smart cards or public key infrastructure (PKI).

Modern day retail **point of sale software systems** have come a long way over the years. Transactional complexities and nuances of the retail industry requires sophisticated technology that performs a myriad of functions and most importantly, assures that safety, security, accountability, reliability and accuracy are paramount. The fast-paced world of today’s POS environments demands user-friendly software that can handle transactions with agility to maximize profits without sacrificing precision.

Every second and every penny counts within POS systems, and end users want to have the faith and peace of mind that the technology they use is going to ensure maximum returns on investment (ROI) and build sustainable profit margins while at the same time minimizing fraud and waste.

Total identification solutions encompass a large-scale application of equipment and software that allows for use of multiple system technology; i.e, fingerprint, iris scans, voice, etc.

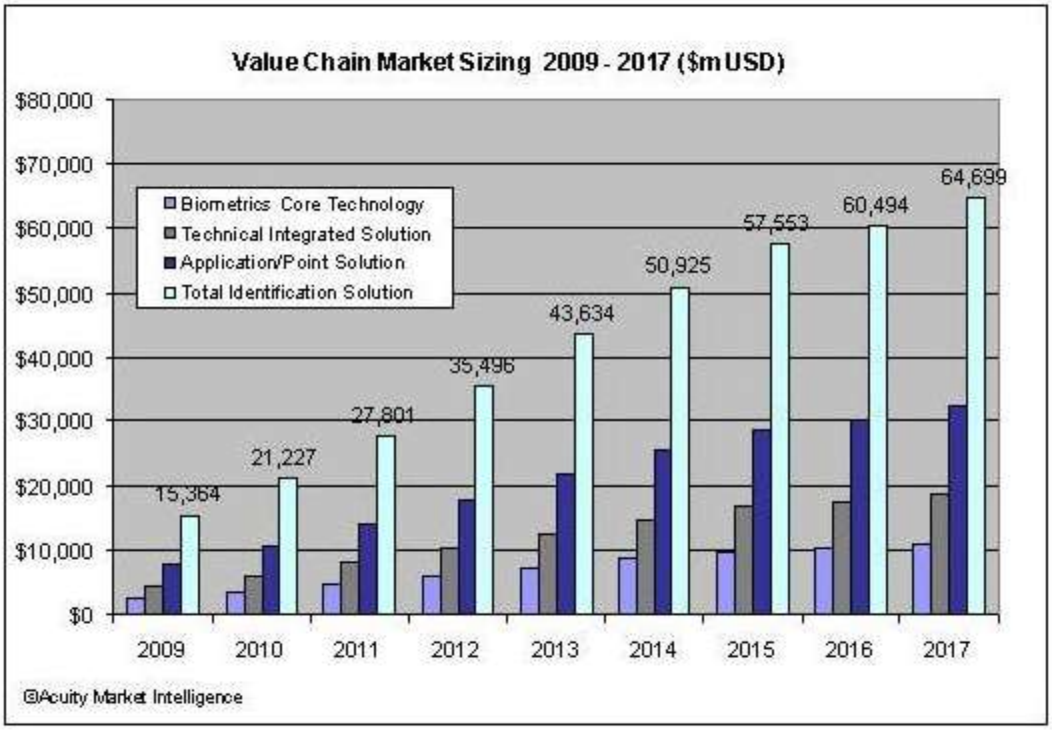
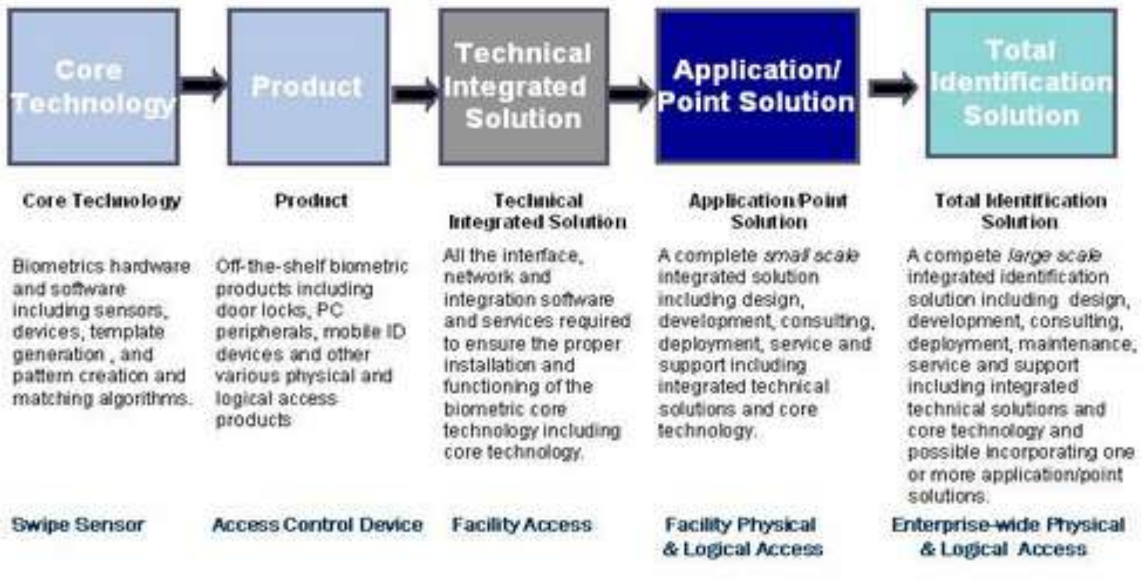


FIGURE 6: VALUE CHAIN MARKET SIZING 2009—2017 (PROJECTED)

A graphic representing the various complexities of biometric solutions and core technology is given below.


Core Technology
Product
Technical Integrated Solution
Application/ Point Solution
Total Identification Solution
Swipe Sensor
Access Control Device
Facility Access
Facility Physical & Logical Access
Enterprise-wide Physical & Logical Access

Core Technology

Biometrics hardware and software including sensors, devices, template generation , and pattern creation and matching algorithms.

Product

Off-the-shelf biometric products including door locks, PC peripherals, mobile ID devices and other various physical and logical access products

Technical Integrated Solution

All the interface, network and integration software and services required to ensure the proper installation and functioning of the biometric core technology including core technology.

Application Point Solution

A complete *small scale* integrated solution including design, development, consulting, deployment, service and support including integrated technical solutions and core technology.

Total Identification Solution

A compete *large scale* integrated identification solution including design, development, consulting, deployment, maintenance, service and support including integrated technical solutions and core technology and possible incorporating one or more application/point solutions.

FIGURE 7: IDENTIFICATION SOLUTIONS

PHYSICAL EQUIPMENT AVAILABLE:

It’s obvious there must be a physical link between the biometric mode used and the data base capturing the information. We now examine the “hardware” used to bring about reading and allowing access for verification and identification.

FINGERPRINT SCANNER

With any fingerprint system, a user will never present exactly the same image to the scanner. There will always be subtle variations, (for instance, dirt, cuts, faulty scanner, etc). Systems match on the basis of confidence intervals, i.e, a fingerprint is 95% similar to the one in the database. When a single fingerprint is presented, that interval needs to be very high, to ensure that other people cannot login as an authorized user. There are several systems, such as the finger PIN, which use multiple fingerprints in a sequence. In this fashion, the interval for each fingerprint is reduced. As long as a user knows the sequence in which the fingerprints were input, there is a massive reduction in the chance of letting a non-authorized user log in.

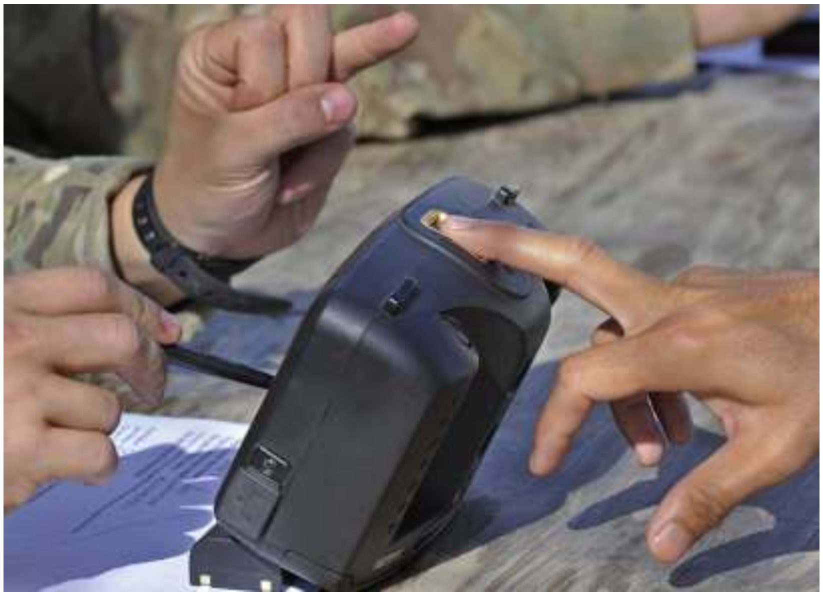


FIGURE 8: FINGERPRINT READER

Other fingerprint readers may look as follows:

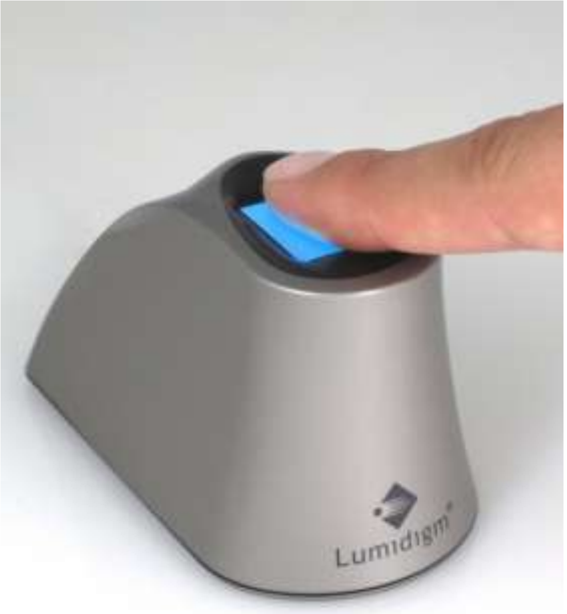


FIGURE 9: FINERPRINT READER

FIGURE 10: FINGERPRINT READER

PALM and VEIN READER:

Unlike other forms of biometric scanners, palm vein readers are robust and scan beneath the surface of the skin demonstrating a high tolerance of skin surface problems such as dryness, roughness, moisture, or scarring.

With an extremely low false acceptance rate (FAR) and false reject rate (FRR), non-intrusive contactless authentication, and the highest reliability of all hand-or finger-based biometric authentication scanners, they represent the ideal biometric recognition device compared to other biometric hardware for all environments.

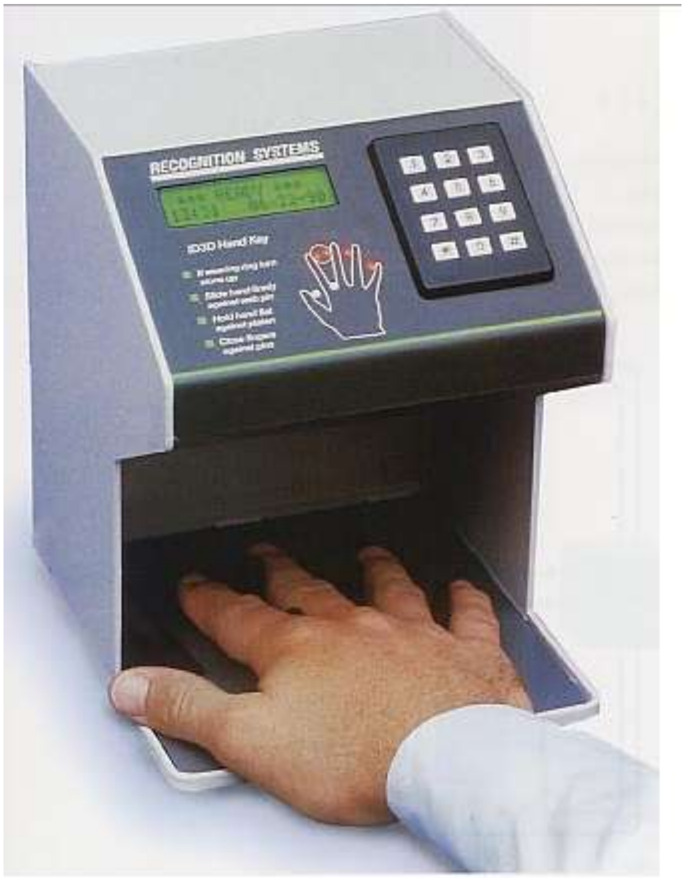


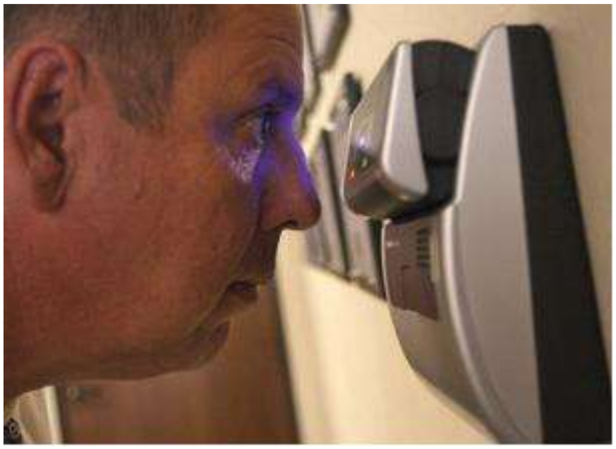
FIGURE 11: PALM AND HAND READER

RETINA AND IRIS SCANNERS:

These devices have become very “high-tech” and functional allowing access for devices as small as i-phones and tablets. The three digitals, given below, will show how advanced the technology has become.

FIGURE 12: RETINA AND IRIS SCAN

Figure 12 above shows application software allowing the owner access. This biometric is becoming much more popular with cell phone users.



FURING 13: RETINA AND IRIS SCANNER

Generally, access using a retina or iris scan is accompanied by a necessary PIN or password. This combination is called a bimodal system. The user chooses the PIN or password. There is a programmed time lapse between scan and entry of PIN or password. Also, most systems will allow two or three tries before the user is locked out. This is a third layer of protection. This type of system is shown by Figure 14 below.

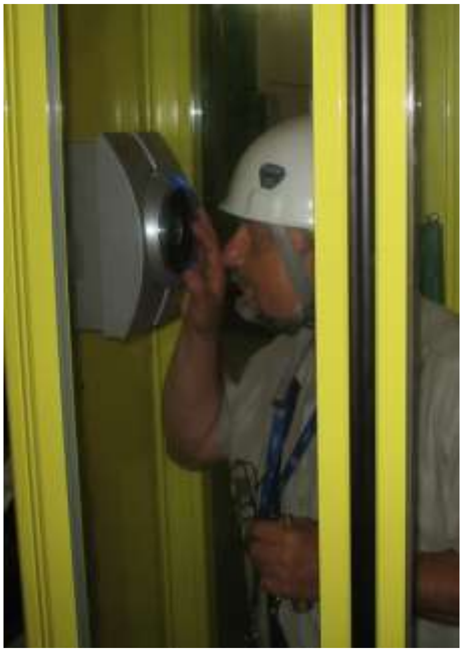


FIGURE 14: RETINA SCAN WITH PIN INPUT

FACIAL RECOGNITION CAMERAS:

As you can imagine, facial recognition is accomplished by using cameras to capture the image. This image is then interrogated by software programs and used for comparison to an existing database. The cameras are remarkably sophisticated as you can see from the following JPEGs. One very desirable feature is the small size of the camera taking the picture. Picture plus PIN or password will allow entry. The time and date of the entry is automatically logged into the system.

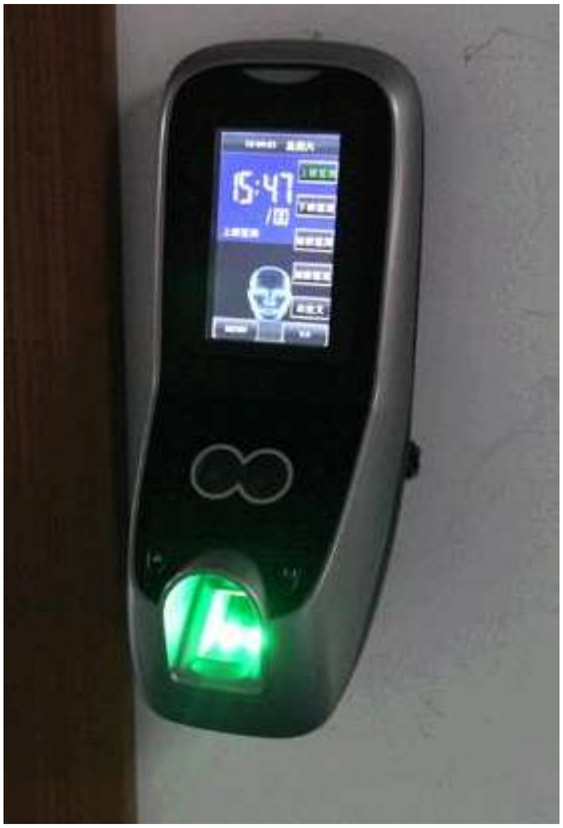


FIGURE 15: FACIAL RECOGNITION CAMERA

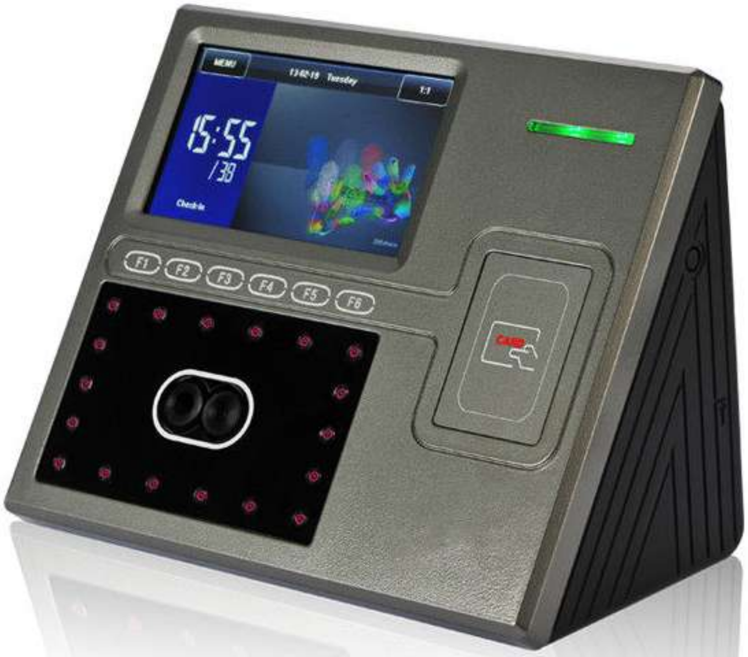


FIGURE 16: FACIAL RECOGNITION CAMERA

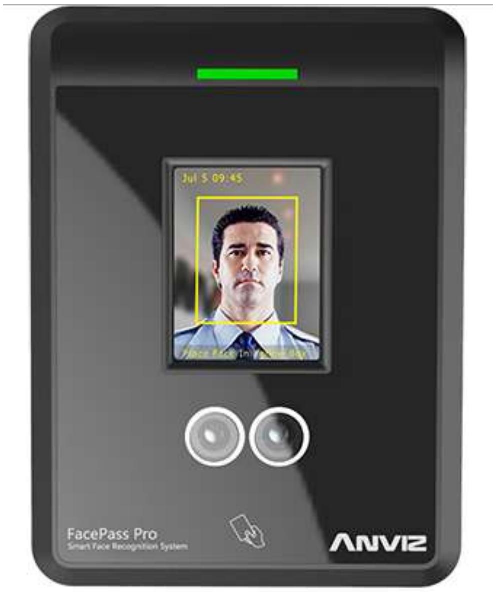


FIGURE 17: FACIAL RECOGNITION CAMERA

EAR LOBE AND EAR CONFIGURATION:

OK this is an unusual one, but the hardware does exist and looks as follows:

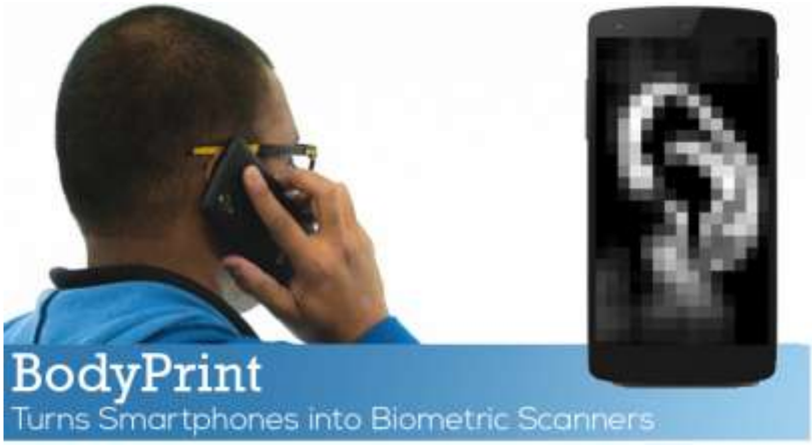


FIGURE 18: EAR LOBE

So, you do not want to wait for giving an authentication by swiping the screen or scanning for fingerprints or typing PIN in order to answer the calls. Just put your smart phone to your ear and let touch screen sensor scan its shape. That is it. If your ear prints match, the call will automatically be answered. There is actually an app for this type of access. Really cool.

VOICE RECOGNITION:

One of the oldest forms of biometric technology, voice recognition, still remains allowable as evidence in courtrooms. It is also used as a tool for allowing admission to classified areas or confidential documents.

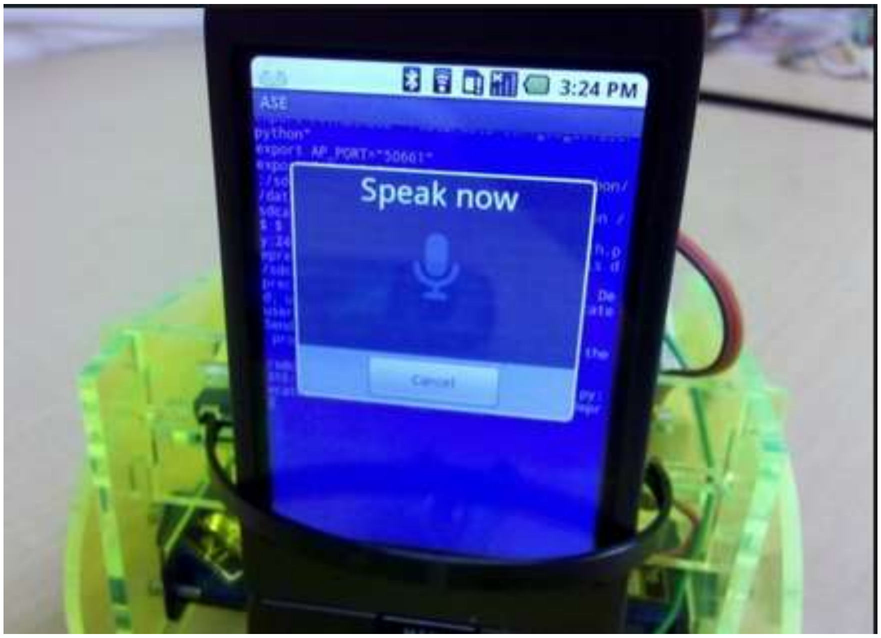


FIGURE 19: VOICE RECOGNITION RECEPTOR

DNA:

DNA access is the most intrusive of the fourteen (14) biometric modes of allowing access. A physical sample must be taken and entered into a database. That DNA sample must be matched each time entry or permission is given relative to accessing a database or area. The sample may be a follicle of hair, saliva or other substance carrying DNA material. The software programs required for matching are expensive, but accuracy is remarkable.

ODOR:

A bleeding edge technology with multiple potential applications is odor biometrics. An individual’s body odor is genetically determined and can be tracked. The idea is to create a sensor that replicates a dog’s nose, which is estimated to be one hundred (100) times better than that of a human. Such a sensor could recognize subtle differences for authentication or identification purposes. Additionally, body odor changes under stress. This could expand the modality to identify individuals and determine if a person is experiencing stress, perhaps due to lying. Biometric sensors capable of detecting odor could be used to find harmful compounds such as explosives and other contraband. They could also be used to detect harmful bacteria or if an individual is carrying a contagion.

There is also the possibility of combining odor and DNA. The odor biometric could locate an individual’s specific skin cells, which are left just about everywhere, and then the DNA could test those same cells.

The device below is a “sniffer” and is capable of detecting odor.

FIGURE 20: SNIFFER

We have looked at hardware necessary for detection and interface so now let’s go deeper into the actual modes and discover the technology behind the usage.

<u>BIOMETRIC MODES:</u>

FINGERPRINT

Fingerprint identification is one of the most well-known and publicized biometrics. Because of their uniqueness and consistency over time, fingerprints have been used for identification for more than a century, more recently becoming automated (i.e., a biometric) due to advancements in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (10 fingers) available for collection, and their established use and collections by law enforcement and immigration.

A fingerprint is made of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points: ridge endings (where a ridge ends) and ridge bifurcations (where a ridge splits in two). Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other).

The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. There are five basic fingerprint patterns: arch, tented arch, left loop, right loop and whorl. Loops make up 60% of all fingerprints, whorls account for 30%, and arches for 10%.

Fingerprints are usually considered to be unique, with no two fingers having the exact same dermal ridge characteristics.

There are two main algorithm families to recognize fingerprints:

- Minutia matching compares specific details within the fingerprint ridges. At registration (also called enrollment), the minutia points are located, together with their relative positions to each other and their directions. At the matching stage, the fingerprint image is processed to extract its minutia points, which are then compared with the registered template.

- Pattern matching compares the overall characteristics of the fingerprints, not only individual points. Fingerprint characteristics can include sub-areas of certain interest including ridge thickness, curvature, or density. During enrollment, small sections of the fingerprint and their relative distances are extracted from the fingerprint. Areas of interest are the area around a minutia point, areas with low curvature radius, and areas with unusual combinations of ridges.

A variety of sensor types — optical, capacitive, ultrasound, and thermal — are used for collecting the digital image of a fingerprint surface. Optical sensors take an image of the fingerprint, and are the most common sensor today. Other fingerprint sensors capture images by employing high frequency ultrasound or optical devices that use prisms to detect the change in light reflectance related to the fingerprint. Thermal scanners require a swipe of a finger across a surface to measure the difference in temperature over time to create a digital image.

SIGNATURE

Biometric signature recognition systems will measure and analyze the physical activity of signing, such as the stroke order, the pressure applied and the speed. Some systems may also compare visual images of signatures, but the core of a signature biometric system is behavioral, i.e, how it is signed rather than visual, i.e, the image of the signature.

FACIAL RECOGNITION

Humans often use faces to recognize individuals, and advancements in computing capability over the past few decades now enable similar recognitions automatically. Early facial recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes. Major advancements and initiatives in the past 10 to 15 years have propelled facial recognition technology into the spotlight. Facial recognition can be used for both verification and identification (open-set and closed-set).

Biometric facial recognition systems measure and analyze the overall structure, shape and proportions of the face: Distance between the eyes, nose, mouth, and jaw edges; upper outlines of the eye sockets, the sides of the mouth, the location of the nose and eyes, the area surrounding the cheekbones.

Predominant Approaches to Facial Recognition

There are two predominant approaches to the facial recognition problem: geometric (feature based) and photometric (view based). As researcher interest in face recognition continued, many different algorithms were developed, three of which have been well studied in face recognition literature: Principal Components Analysis (PCA), Linear Discriminant Analysis (LDA), and Elastic Bunch Graph Matching (EBGM). PCA: Principal Components Analysis (PCA) PCA, commonly referred to as the use of eigenfaces, is the technique pioneered by Kirby and Sirivich in 1988. With PCA, the probe and gallery images must be the same size and must first be normalized to line up the eyes and mouth of the subjects within the images. The PCA approach is then used to reduce the dimension of the data by means of data compression basics2 and reveals the most effective low-dimensional structure of facial patterns. This reduction in dimensions removes information that is not useful and precisely decomposes the face structure into orthogonal (uncorrelated) components known as eigenfaces. Each face image may be represented as a weighted sum (feature vector) of the eigenfaces, which are stored in a 1D array. A probe image is compared against a gallery image by measuring the distance between their respective feature vectors. The PCA approach typically requires the full frontal face to be presented each time; otherwise the image results in poor performance. The primary advantage of this technique is that it can reduce the data needed to identify the individual to 1/1000th of the data presented.

At enrolment, several pictures are taken of the user's face, with slightly different angles and facial expressions, to allow for more accurate matching. For verification and identification, the user stands in front of the camera for a few seconds, and the scan is compared with the template previously recorded.

To prevent an image / photo of the face or a mask from being used, face biometric systems will require the user to smile, blink, or nod their head. Also, facial thermography can be used to record the heat of the face (which won't be affected by a mask).

A grid is constructed of “surface features”; those features are then compared with photographs located in data bases or archives. In this fashion, positive identification can be accomplished.

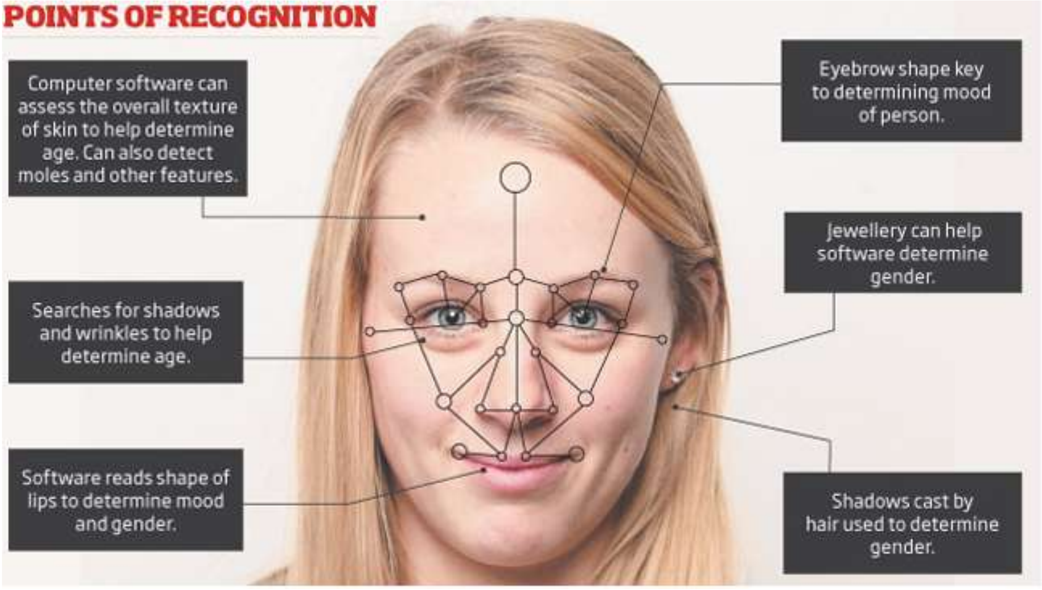

POINTS OF RECOGNITION
Computer software can assess the overall texture of skin to help determine age. Can also detect moles and other features.
Eyebrow shape key to determining mood of person.
Jewellery can help software determine gender.
Searches for shadows and wrinkles to help determine age.
Software reads shape of lips to determine mood and gender.
Shadows cast by hair used to determine gender.

FIGURE 21: POINTS OF RECOGNITION

Cameras are definitely required to initiate the identification process. These cameras may be full-face or scanning. The JPEG below will indicate the process for a scanning camera.

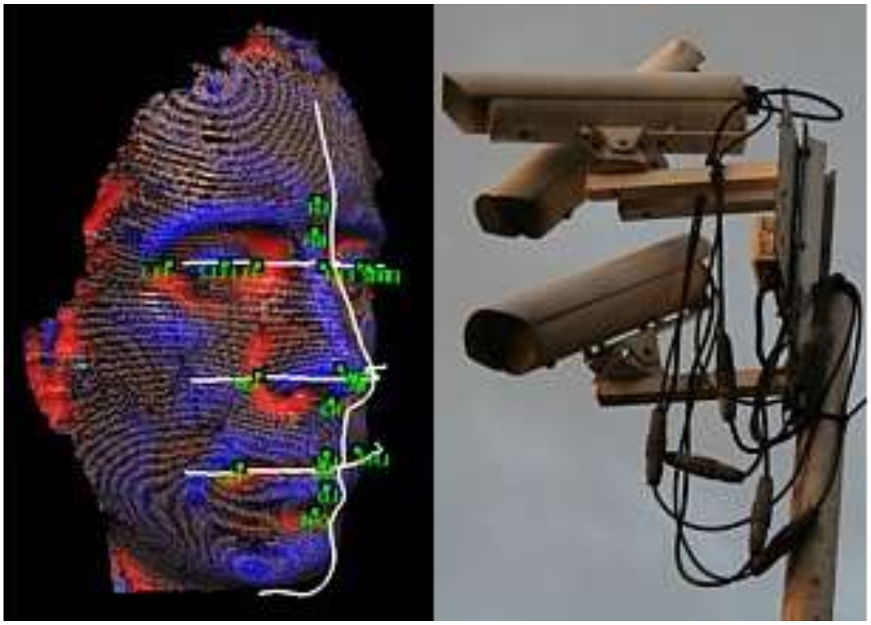


FIGURE 22: MACHINE VISION CAMERAS

IRIS SCAN

FIRUER 23: IRIS SCAN

The iris is the elastic, pigmented, connective tissue that controls the pupil. The iris is formed in early life in a process called morphogenesis. Once fully formed, the texture is stable throughout life. It is the only internal human organ visible from the outside and is protected by the cornea. The iris of the eye has a unique pattern, from eye to eye and person to person. An iris scan will analyze over 200 points of the iris, such as rings, furrows, freckles, and the corona and will compare that scan to a previously recorded template.

Glasses, contact lenses, and even eye surgery does not change the characteristics of the iris.

To prevent an image / photo of the iris from being used instead of a real "live" eye, iris scanning systems will vary the light and check that the pupil dilates or contracts.

Of all the biometric technologies used for human authentication today, it is generally conceded that iris recognition is the most accurate. Coupling this high confidence authentication with factors like outlier group size, speed, usage/human factors, platform versatility and flexibility for use in identification or verification modes - as well as addressing issues like database size/management and privacy concerns - iris recognition has also shown to be exceedingly versatile and suited for large population applications.

Iris recognition is the best of breed authentication process available today. While many mistake it for retinal scanning, iris recognition simply involves taking a picture of the iris; this picture is used solely for authentication. But what makes iris recognition the authentication system of choice?

- Stable - the unique pattern in the human iris is formed by 10 months of age, and remains unchanged throughout one's lifetime
- Unique - the probability of two irises producing the same code is nearly impossible
- Flexible - iris recognition technology easily integrates into existing security systems or operates as a standalone
- Reliable - a distinctive iris pattern is not susceptible to theft, loss or compromise
- Non-Invasive - unlike retinal screening, iris recognition is non-contact and quick, offering unmatched accuracy when compared to any other security alternative, from distances as far as 3" to 10"

Iris recognition is an attractive technology for identity authentication for several reasons.

1. The smallest outlier population of all biometrics. Few people can't use the technology, as most individuals have at least one eye. In a few instances even blind persons have used iris recognition successfully, as the technology is iris pattern-dependent, not sight-dependent.
2. Iris pattern and structure exhibit long-term stability. Structural formation in the human iris is fixed from about one year in age and remains constant (barring trauma, certain rare diseases, or possible change from special ophthalmologic surgical procedures) over time. So, once an individual is enrolled, re-enrollment requirements are infrequent. With other biometric technologies, changes in voice timbre, weight, hairstyle, finger or hand size, cuts or even the effect of manual labor can trigger the need for re-enrollment.
3. Ideal for Handling Large Databases. Iris recognition is the only biometric authentication technology designed to work in the 1-n or exhaustive search mode. This makes it ideal for handling applications requiring management of large user groups, such as a National Documentation application might require. Large databases are accommodated without degradation in authentication accuracy. Iris Access platforms integrate well with large database back ends like Microsoft SQL and Oracle 9i.
4. Unmatched Search Speed in the one to many search mode is unmatched by any other technology, and is limited not by database size, but by hardware selected for server management. In a UK Government-commissioned study, Iris ID's Iris Access platform searched

records nearly 20 times faster than the next fastest technology. Iris ID has developed a high speed matching engine, Iris Accelerator™, designed to deliver 10 million+ matches per second.

5. Versatile for the One to Many, One to One, Wiegand and Token Environments. While initially designed to work in one-to-many search mode, iris recognition works well in 1-1 matching, or verification mode, making the technology ideal for use in multifactor authentication environments where PINs, or tokens like proxy or smartcards are used. In a token environment, many privacy issues related to biometric database management are moot, as the user retains control of biometric data – a small template of 512 bytes per iris.

6. Safety and Security Measures in Place. Iris recognition involves nothing more than taking a digital picture of the iris pattern (from video), and recreating an encrypted digital template of that pattern. 512-byte iris templates are encrypted and cannot be re-engineered or reconstituted to produce any sort of visual image. Iris recognition therefore affords high level defense against identity theft, a rapidly growing crime. The imaging process involves no lasers or bright lights and authentication is essentially non-contact.

7. Convenient, Intuitive User Interface. Using the technology is an almost intuitive experience, requiring relatively little cooperation from subjects. Proximity sensors activate the equipment, which incorporates mirror-assisted alignment functionality. Audio auto-positioning prompts, automated image capture, and visual and audio authentication decision-cueing completes the process.

RETINA SCAN

FIGURE 24: RETINA SCAN

The blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person. Retina scans require that the person removes their glasses, place their eye close to the scanner, stare at a specific point, and remain still, and focus on a specified location for approximately 10 to 15 seconds while the scan is completed. A retinal scan involves the use of a low-intensity coherent light source, which is projected onto the retina to illuminate the blood vessels which are then photographed and analyzed. A coupler is used to read the blood vessel patterns.

A retina scan cannot be faked as it is currently impossible to forge a human retina. Furthermore, the retina of a deceased person decays too rapidly to be used to deceive a retinal scan.

A retinal scan has an error rate of 1 in 10,000,000, compared to fingerprint identification error being sometimes as high as 1 in 500.

HAND GEOMETRY

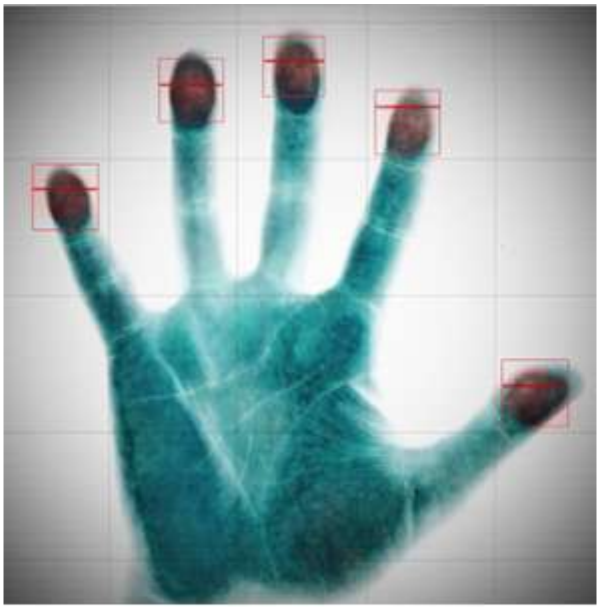


FIGURE 25: HAND GEOMETRY

Palm print recognition inherently implements many of the same matching characteristics that have allowed fingerprint recognition to be one of the most well-known and best publicized biometrics. Both palm and finger biometrics are represented by the information presented in a friction ridge impression. This information combines ridge flow, ridge characteristics, and ridge structure of the raised portion of the epidermis. The data represented by these friction ridge impressions allows a determination that corresponding areas of friction ridge impressions either originated from the same source or could not have been made by the same source. Because fingerprints and palms have both uniqueness and permanence, they have been used for more than a century as a trusted form of identification. However, palm recognition has been slower in becoming automated due to some restraints in computing capabilities and live-scan technologies.

An individual's hand does not significantly change after a certain age. Unlike fingerprints, the human hand isn't unique. Individual hand features are not descriptive enough for identification. However, hand biometric recognition systems are accurate for verification purposes when combining various individual features and measurements of fingers and hands.

Biometric hand recognition systems measure and analyze the overall structure, shape and proportions of the hand, e.g., length, width and thickness of hand, fingers and joints; characteristics of the skin surface such as creases and ridges. Some hand geometry biometrics systems measure up to 90 parameters.

As hand biometrics rely on hand and finger geometry, the system will also work with dirty hands. The only limitation is for people with severe arthritis who cannot spread their hands on the reader.

The user places the palm of his or her hand on the reader's surface and aligns his or her hand with the guidance pegs which indicate the proper location of the fingers. The device checks its database for verification of the user. The process normally only takes a few seconds.

To enroll, the users place his or her hand palm down on the reader's surface.

To prevent a mold or a cast of the hand from being used, some hand biometric systems will require the user to move their fingers. Also, hand thermography can be used to record the heat of the hand, or skin conductivity can be measured.

Even though total error rates are decreasing when comparing live-scan enrollment data with live-scan verification data, improvements in matches between live-scan and latent-print data are still needed. Data indicates that fully integrated palm and fingerprint multi-biometric systems are widely used for identification and verification of criminal subjects as well as in security access applications. However, there are still significant challenges in balancing accuracy with system cost. Image matching accuracy may be improved by building and using larger databases and by employing more processing power, but then purchase and maintenance costs will most certainly rise as the systems become larger and more sophisticated. Future challenges require balancing the need for more processing power with more improvement in algorithm technology to produce affordable systems to all levels of law enforcement.

VEIN GEOMETRY

FIGURE 26: HAND GEOMETRY

As with irises and fingerprints, a person's veins are completely unique. Twins don't have identical veins, and a person's veins differ between their left and right sides. Many veins are not visible through the skin, making them extremely difficult to counterfeit or tamper with. Their shape also changes very little as a person ages.

To use a vein recognition system, you simply place your finger, wrist, palm or the back of your hand on or near the scanner. A camera takes a digital picture using near-infrared light. The hemoglobin in your blood absorbs the light, so veins appear black in the picture. As with all the other biometric types, the software creates a reference template based on the shape and location of the vein structure.

Scanners that analyze vein geometry are completely different from vein scanning tests that happen in hospitals. Vein scans for medical purposes usually use radioactive particles. Biometric security scans, however, just use light that is similar to the light that comes from a remote control.

FINGER GEOMETRY

We can actually include finger geometry with hand geometry. The process is really the same. One very interesting twist to enhance security is using multiple fingers on the same hand in a given sequence. Each finger, as described above in the “hardware” section, would be presented for reading.

EAR FORM

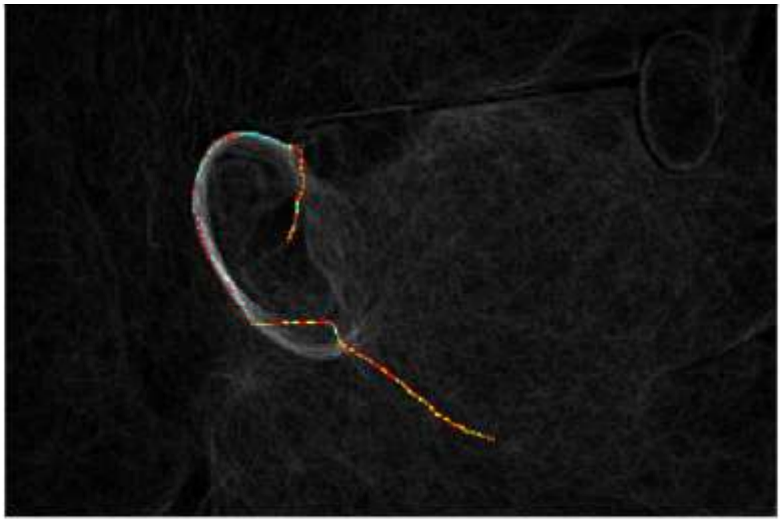


FIGURE 27: EAR LOBE IDENTIFICATION

A new class of biometrics based upon ear features was introduced for use in the development of passive identification systems by Alfred Iannarelli. Identification by ear biometrics is promising because it is passive like face recognition, but instead of the difficulties to extract face biometrics, it uses robust and simply extracted biometrics like those in fingerprinting. The ear is a unique feature of each human. Even the ears of “identical twins” differ in some respects. People working in crime laboratories assume that human external ear characteristics are uniquely individual and unchanging during the lifetime of an adult. Over the years, suggestions have been made in occasional literature that the shapes and characteristics of the human ear are widely different and it may be possible to differentiate between the ears of all individuals. Unfortunately, this “individuality” has apparently been taken for granted but has never been empirically established. Techniques that allow computers to understand the shape of a human ear in images and video sequences can be used in a wide range of applications. In certain domains it suffices to recognize a few different shapes, observed always from the same viewpoint.

VOICE RECOGNITION

FIGURE 28: VOICE RECOGNITION

Speaker, or voice, recognition is a biometric modality that uses an individual's voice for recognition purposes. It is a different technology than "speech recognition," which recognizes words as they are articulated, which is not a biometric. The speaker recognition process relies on features influenced by both the physical structure of an individual's vocal tract and the individual's behavioral characteristics.

A popular choice for remote authentication due to the availability of devices for collecting speech samples (e.g., telephone network and computer microphones) and its ease of integration, speaker recognition is different from some other biometric methods in that speech samples are captured dynamically over a period of time, such as a few seconds. Analysis occurs on a model in which changes over time are monitored, which is similar to other behavioral biometrics such as dynamic signature, gait, and keystroke recognition**.**

Speaker recognition is the identification of a person from characteristics of voices (*voice biometrics*). It is also called voice recognition. There is a difference between *speaker recognition* (recognizing **who** is speaking) and *speech recognition* (recognizing what is being said). These two terms are frequently confused, and "voice recognition" can be used for both. In addition, there is a difference between the act of authentication (commonly referred to as speaker verification or speaker authentication) and identification. Finally, there is a difference between *speaker recognition* (recognizing **who** is speaking) and *speaker diarisation* (recognizing when the same speaker is speaking). Recognizing the speaker can simplify the task of translating speech in systems that have been trained on specific person's voices, or it can be used to authenticate or verify the identity of a speaker as part of a security process.

Speaker recognition has a history dating back some four decades and uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). Speaker verification has earned speaker recognition its classification as a "behavioral biometric".

DNA

Genes make up five (5) percent of the human genome. The other 95 percent are non-coding sequences, which used to be called junk DNA. In non-coding regions there are identical repeat sequences of DNA, which can be repeated anywhere from one to 30 times in a row. These regions are called variable number tandem repeats (VNTRs). The number of tandem repeats at specific places, called loci, on chromosomes varies between individuals. For any given VNTR loci in an individual's DNA, there will be a certain number of repeats. The higher the number of loci that are analyzed, the smaller the probability to find two unrelated individuals with the same DNA profile.

DNA profiling determines the number of VNTR repeats at a number of distinctive loci and uses it to create an individual's DNA profile. The main steps to create a DNA profile are: isolate the DNA from a sample such as blood, saliva, hair, semen, or tissue; cut the DNA up into shorter fragments containing known VNTR areas; sort the DNA fragments by size; and compare the DNA fragments in different samples.

The benefit of using DNA as a biometric identifier is the level of accuracy offered: the chance of two individuals sharing the same DNA profile is less than one in 100 billion with 26 different bands studied.

Humans have 23 pairs of chromosomes containing their DNA blueprint. One member of each chromosomal pair comes from their mother; the other comes from their father. Every cell in a human body contains a copy of this DNA. The large majority of DNA does not differ from person to person, but 0.10 percent of a person's entire genome would be unique to each individual. This represents 3 million base pairs of DNA.

ODOR

Human odor can be very different between individuals and can therefore be seen as a biometric to identify a specific person. Dogs have been trained to identify objects held by an individual from the beginning of the twentieth century. Advancing technology has made it possible to identify humans based on headspace analysis of objects they have handled, opening the route to the use of odor as a biometric.

Odor Biometrics attempts to identify individuals based on a unique chemical pattern. Their applications are used to identify individuals in airports by virtue of detecting different components in the human body.

The researchers write, "Body odor identification is not a new idea considering the technique has been used for over a century. Police forces use bloodhounds which trained for such a task. The ability of these dogs to follow the trail of a person from a sample of his or her's personal odor is well known and proves that using body odor is effective as an effective biometric identifier."

The system used by the researchers has not yet achieved the accuracy of a dog's nose, but achieved an error rate of 15% in analysis of 13 people during 28 sessions. The researchers claim that the system has enormous potential.

KEYBOARD STROKES

The behavioral biometric of Keystroke Dynamics uses the manner and rhythm in which an individual types characters on a keyboard or keypad. The keystroke rhythms of a user are measured to develop a unique biometric template of the user's typing pattern for future authentication. Raw measurements available from almost every keyboard can be recorded to determine Dwell time (the time a key pressed) and Flight time (the time between "key up" and the next "key down"). The recorded keystroke timing data is then processed through a unique neural algorithm, which determines a primary pattern for future comparison. Similarly, vibration information may be used to create a pattern for future use in both identification and authentication tasks.

Data needed to analyze keystroke dynamics is obtained by keystroke logging. Normally, all that is retained when logging a typing session is the sequence of characters corresponding to the order in which keys were pressed and timing information is discarded. When reading email, the receiver cannot tell from reading the phrase "I saw 3 zebras!" whether:

- that was typed rapidly or slowly
- the sender used the left shift key, the right shift key, or the caps-lock key to make the "i" turn into a capitalized letter "I"
- the letters were all typed at the same pace, or if there was a long pause before the letter "z" or the numeral "3" while you were looking for that letter
- the sender typed any letters wrong initially and then went back and corrected them, or if they got them right the first time.

STANDARDS:

The success of biometric applications is particularly dependent on the interoperability of biometric systems. Deploying these systems requires both national and international biometric standards. Programs supporting the development of open system standards for biometrics and promoting innovation and industrial competitiveness is absolutely critical. Although a number of standards have been developed, innovations in biometrics technologies, personal recognition systems, and new customer's needs are leading to additional standards developed by individual vendors and companies. The purpose of this development is to add technical functionality to existing published standards and to reflect these technology innovations and new customers' needs. In the biometric arena, NIST stands alone as an impartial developer of standards and it is considered a leading testing organization. NIST/ITL is currently involved in many capacities related to personal authentication activities (technology research, metrology, and standardization). Under this program, we work in close partnership with other NIST/ITL experts, managers and experts from other U.S. Government agencies and other users, industry and academic institutions to support development of formal national and international biometric standards of high relevance to the nation.

Base standards, such as biometric data interchange formats and technical interface standards do not usually contain the conditions to demonstrate that products meet the technical requirements specified in the standards. Conformance testing captures the technical description of a specification and measures whether an implementation faithfully implements the specification. We will now take a look, by virtue of the following lists, those standards, international and domestic, that are being used at the present time. I will not go into the process involving the development of standards not third-party testing to insure compliance. That is a discussion beyond the scope of this course.

ISO (INTERNATIONAL STANDARDS ORGANIZATION)

The body of ISO standards is huge so I'm simply giving the web site from which all documents may be obtained. That site is:

http://www. ISO/IEC JTC 1/SC 37 Biometrics

UNITED STATES STANDARDS FOR BIOMETRICS

These standards may be found by accessing:

http://www.nist.gov/standardsgov/biometrics.cfm

I would now like to recommend to you the following web sites for "best practices and recommendations".

- ***Best Practices for Privacy-Sympathetic Biometric Deployment , www.bioprivacy.org/best_practices_main.htm***
- **Biometrics Institute – www.biometricsinstitute.org**
- **Biom BioPrivacy Initiative – www.bioprivacy.org**
- **Biometrics.gov Standards – http://www.biometrics.gov/Standards/Default.aspx**
- **FBI Biometric Center of Excellence (BCOE) – http://www.biometriccoe.gov/**
- ***Mobile ID Device Best Practice Recommendation, Version 1.0, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=903169***
- **National Biometric Security Project (NBSP) Enterprise – www.nationalbiometric.org**
- **National Institute of Justice (NIJ) Sensors, Surveillance, and Biometric Technologies Center of Excellence –www.biometricgroup.com/Center/**
- **National Institute of Standards and Technology (NIST) Information Technology Laboratory's Identity Management Systems Program – http://www.itl.nist.gov/ITLPrograms/IDMS/external/**
- ***Privacy guidance for the electronic sharing of corrections photographs* –** The International Justice and Public Safety Network

INDUSTRY GROUPS:

The following lists represent a summary of the industry groups formed to promote and discuss Biometric Technology. Each of these entities has important information relative to "breaking news", standards, new products, applications, advantages and disadvantages of use, costs and projects underway.

- International Biometric Association
- Association of Automatic Identification and Mobility
- Biometric Consortium
- British Security Industry Association (BSIA)
- Biometric Research Center, Hong Kong Polytechnic University
- Center for Biometric and Security Research (CBSR)
- International Biometric Industry Association (IBIA)
- International Association for Identification
- International Association for Biometrics (IAFB)
- International Professional Security Association (IPSA)
- Joint Research and Development Laboratories for Advanced Communication and Community Technologies (JDL)
- SMARTEX
- Swedish National Biometrics Association (SNBA)
- The International Biometrics Society
- The Security Industry Association (SIA)
- The International Biometric Foundation
- The Security Institute
- Biometric API Consortium
- National Biometric Security Project (NBSP)
- Biometric Identity Management Agency (BIMA)
- American National Standards Institute(ANSI)
- Biometric Testing Services
- Intellect Association for Biometrics

- Biometrics Institute (London)
- Danish Biometric Research
- European Biometrics Forum
- European Privacy Institute
- Nordic Biometrics Forum
- Swedish National Biometrics Association
- Center for Biometrics and Security Research (CBSR)
- Center for Forensic Sciences, Beijing Genomics Institute
- Asia Pacific Smart Card Association
- Singapore Biometrics Working Group
- Biometrics Institute (Australia)
- ASIS, New Zealand

CONCLUSIONS:

I hope you can see from this brief course on Biometric Technology the importance of the subject and how biometrics can and will fit into our daily lives. Identify theft and fraud are ever-increasing problems on a global basis. Biometrics is certainly one possible solution to this problem. As with any game-changing or disruptive technology, it is evolutionary and revoluntionary.

APPENDIX

- **GLOSSARY**
- **REFERENCES**

APPENDIX

GLOSSARY:

Active Impostor Acceptance– when an access control system incorrectly recognizes and accepts a biometric sample which has been altered, modified, or cloned.

Algorithm– a sequence of instructions that instructs a biometric system on how to solve a problem. It could have a finite number of steps in the instruction to use in computing whether the sample and the template are matched.

Application Program Interface (API)– a set of protocols used to standardize an application by a developer. For example, an API may be added or interchanged by an application developer into any biometric system.

Application Developer– an application programmer or manufacturer that develops and applies any software

Artificial Neural Network– an artificial intelligence system which allows learning to take place in the system. it may use past experiences and compute whether a biometric sample is a match with a template

ASIC or Application Specified Integrated Circuit-a silicon chip for a biometric system which is specifically produced to enhance performance

Attempt– the moment a biometric sample is being submitted for verification. An "attempt" may happen more than once in cases where it is denied or rejected.

Authentication– biometric data is considered to be correct and valid. "Validation" is the preferred term.

Behavioral Biometric– pattern of biometrics that is established after a given amount of time. It is not necessarily a physiological trait.

Biometric– a physical trait or pattern which is unique to every individual. It often used to verify and authenticate a person's identity who is enrolled into a system. Biometric patterns can be anything from fingerprints, iris scans, facial recognition or even voice recognition.

Biometric Application– the implementation of any system that involves biometric data.

Biometric data– a sample taken from an individual which is unique to their own person. Common biometric data are: fingerprint, voice and iris scans, palm vein patterns and even facial patterns.

Biometric Engine– the portion of the biometric software system that processes the gathered data. It can start to operate from the data capture, extraction, and comparison down to the matching.

Biometric Identification Device– gathers, reads and compares biometric data. Biometric System is the term more often used.

Biometric Sample Data- the data captured by a system collected from a person of interest or a user.

Biometric System– an automated system which:

1. Collects or captures biometric data via a scanner
2. Extracts the data from the actual submitted sample
3. Compares the scanned data from those captured for reference
4. Matches the submitted sample with the templates
5. Determines or verifies whether the identity of the biometric data holder is authentic.

Biometric Taxonomy– a method of classification using gathered biometric data. It can also be the classification of biometric data according to their use in a given system such as:

- Cooperative versus Non-cooperative User
- Overt vs. Covert Biometric System
- Habituated vs. Non-habituated user
- Supervised vs. Unsupervised User
- Standard Environment vs. Non-standard Environment

Biometric Technology– A system or application which is designed to employ biometric data. It can also be classified further according to the type of biometrics being used in the system.

Capture– the process of collecting biometric data from the end user or enrollee. Most biometric data is "captured" by use of an image scanner in cases of fingerprints, palm vein patterns or a camera to collect facial an iris scans.

Certification– testing gathered biometric data against a system or software to verify its ability to perform. The application will be then tested according to set standards for certification. Testing organizations are the ones that issue certifications.

Comparison– comparing a biometric sample with previously gathered samples or against a template or templates for verification of the identity

Claimed Identity– a biometric sample of an enrolled user of the system

Claimant– person who submits his biometric sample for identity verification. Claimants may either have true or false identities.

Closed Set Identification-users need to be enrolled into a biometric system and verified for access to be granted

CMOS or Complementary Metal Oxide Semiconductor-a kind of circuit (integrated) used by some biometric systems due to its low power consumption

D Prime– statistical measure which grades the ability of a system to distinguish between biometric samples or individuals. The higher D prime number means that the system is more capable of distinguishing between samples.

Degrees of Freedom– the number of independent features in a biometric system

Encryption-the conversion of any biometric data into a code which cannot be easily read. A password may be used to decrypt or decode the data

End User– an enrolled or about to enroll individual who has his biometric data submitted for verification

End User Adaptation-users of a biometric system are able to adjust accordingly to it after being familiar with the test

Enroll-the user who has his biometric template entered into the system

Enrolment-gathering and processing of biometric data with the intent of storing them into a database

Enrollment Time-time spent the moment biometric data is collected and successfully processed

Equal Error Rate– the rate in which the rate of false rejection is almost equal to the rate of false acceptance

Extraction– the moment a biometric sample is converted into data after which it compared to a biometric template.

Failure to Acquire– a biometric system failing to capture, extract and store the data.

Failure to Acquire rate-the number of times that a failure to acquire occurs

False Acceptance– the biometric system accepts either a false identity or incorrectly identifies a wrong identity against a claimed one

False Match Rate-the moment a match between enrollee and submitted data is done which in turn results to a rejection

False Rejection– occurs when an enrolled identity is rejected by the system or when it fails to verify a legitimate identity

False Rejection Rate– the probability that a biometric system will fail to identify a legitimate identity

The equation is:

FRR=NFR/NEIA or FRR=NFR/NEVA

- FRR is the false rejection rate
- NFR- number of false rejections

• NEIA number of enrollee identification attempts
• NEVA-number of enrollee verification attempts

Field Test– a sample trial done in the outside or Real-world

Goats Biometric System– pattern of activity done by system end-users which varies beyond the specified range allowed. Consequently, it may be rejected by the system.

Hamming Distance-a measure of dissimilarity. It is actually the disagreeing bits between two binary vectors.

Identification or Identity– biometric sample which is matched against templates and other biometric references

Impostor– a person who poses as a verified user by submitting his own biometric sample

In House Test– series of testing done in a closed facility or laboratory. It may or may not involve the use of external participants or subjects.

Live Capture– the actual process of gathering biometric sample from a live user using a biometric system

Match or Matching– the process of matching a template versus a submitted biometric sample. It is then rejected or accepted based on whether the score has met the threshold or not.

Open- Set Identification– identifying users who are not enrolled in the system. Opposite of closed set identification

Original Equipment Manufacturer or Module-an organization which assembles a biometric system from different parts or an independent module which can be integrated into a biometric system

Passive Impostor Acceptance– when an impostor's submitted sample is verified and accepted by the system.

Personal Identification Number (PIN)-usually a four digit number is entered into a system to gain access

Performance criteria– a set of standards or criteria which is used to evaluate the performance of the system

Physiological or Physical Biometric– a physical characteristic used as biometric data. This includes: fingerprints, face recognition, ear shape, iris recognition, palm and retina scans.

Receiver Operating curves– a graph showing how the false rejection and false acceptance rates varies with one another

Recognition– widely used term is identification

Response Time– the amount of time in which a biometric system analyzes a sample and returns with a decision

Template or Reference Template Data– a biometric measurement which is used to verify succeeding biometric data

Third Party Test-a test done by an independent party in a controlled environment

Threshold or Decision Threshold– acceptance level of any given biometric system. it may be tightened or widened accordingly to make the system meet certain requirements. If the data falls above or below the threshold, it is rejected. If the sample falls within the acceptable range, it is accepted.

Throughput Rate– the number of users a biometric system can successfully process within a given time

Type 1 error– See "false rejection"

Type 2 Error– See "false acceptance"

User– the client of any biometric vendor. Essentially, they are the clients that purchase the technology but may or may not enroll themselves into the system. End-users are those who enroll their biometric data into the system.

Validation-the process of comparing a biometric sample whose identity is claimed with the biometric data in the system.

Wavelet Transform/Scalar quantization or WSQ-a compression algorithm used to compress reduce the size of reference templates

Zero Effort Forgery-an impostor uses the actual biometric sample of an enrolled user

REFERENCES:

1. **"Fingerprints and Other Biometrics",** The Federal Bureau of Investigation.
2. **"Biometrics: Today's Choice for the Future of Authentication",** The Infosec Institute, March 6, 2015.
3. **"Global Biometrics Market (2014-2020): Market Forecast By Technologies, Applications, End Use, Regions and Countries"**, PR NEWSWIRE, New York, January 19, 2015.
4. **"History of Biometrics",** Biometric Update.com, January 14, 2015
5. **"There is No Easier Way to Integrate Fingerprints",** Bromba Biometrics, December 24, 2014
6. **"Identity Theft",** Wikipedia, 2015
7. **"Biometric Applications",** Griaule Biometrics, 2014
8. **"The Current and Future Applications of Biometric Technologies",** John C. Mears, Director, International Biometrics and Identification Association, May 21, 2013.
9. **"Introduction to Biometric Technologies and Applications",**Prof. Marios Savvides**,** ECE & CyLab, Carnegie Mellon University, 2015.
10. **"ID Theft, Fraud & Victims of Cybercrime",** CyberSecurity Alliance, 2015
11. **"Intellectual Property Theft: A Threat to U.S. Workers, Industries, and Our Economy"**, Department for Professional Employees-AFLCIO, Fact Sheet 2014.
12. "**Intellectual Property Theft: Get Real",** National Crime Prevention Council, 2015.
13. "**Protection From Hackers: Computer Fraud and Cyber Liability Insurance",** *Charlie Morriss on* June 1, 2014 *in Cyber Security, Management Liability*
14. **"The Underground Hacking Economy is Alive and Well",** Dell Secure Works, Inc, 2015
15. "**DNA",** Federal Bureau of Investigation, Biometrics Center of Excellence, 2015
16. **"Facial Recognition",** Federal Bureau of Investigation, Biometrics Center of Excellence, 2015.
17. **"Palm Print ",** Federal Bureau of Investigation, Biometrics Center of Excellence, 2015.
18. **"Mandatory National IDs and Biometric Databases",** Electronic Frontier Foundation, 2014
19. **"The History of Biometric Security and How It's Being Used Today",** Technology Explained, Bryan Clark, March 4, 2015.
20. "**Iris Scan",** Federal Bureau of Investigation, Biometrics Center of Excellence, 2015.

21. **“Biometrics: Facial Recognition and Iris Scanning”,** PrivacySOS, ACLU of Massachusetts, 2015.

22. **“Iris Recognition Technology”,** IRIS Access, 2015.

23. **“Iris Recognition”,** Find Biometrics—Global Identity Management, 2014

24. **“**Biometric Standards Program and Resource Center”, Information Technology Laboratory, March 19, 2015

25. **“Biometrics and standards”, ITU** News, January—February, 2010.

26. **“Bio Buoyed by Government Projects, Global Biometrics Market is Projected to Touch $21.9 Billion by 2020; Asia-Pacific (APAC) to Acquire Leadership in the Forecast Period** – 6Wresearch”, December 2014.

27. “**Global Biometrics Market to Reach US$14 Billion by 2015”,** BioMed Trends,

28. **“Biometrics: Market Shares, Strategies, and Forecasts, Worldwide, 2013 to 2019”,** IT & IT Communications, November 2013.

29. “**Biometrics: Technologies and Global Markets”,** BCC Research, November 2010

30. “**GLOBAL BIOMETRICS TECHNOLOGY MARKET IS EXPECTED TO EXCEED USD 23 BILLION BY 2019”,** Biometrics Technology Watch, 2015

31. “Use of Biometric Technology in Developing Countries”, World Bank.org, Xavier Gine, Jessica Goldberg, University of Michigan, Shalini Sankaranarayanan, IFC, Peter Sheerin, IFC, Dean Yang, University of Michigan, 2014.

32. **“Voice Recognition”,** Federal Bureau of Investigation, Biometric Center of Excellence, 2015.

33. **“Biometrics of Next Generation: An Overview”,** Anil K. Jain and Ajay Kumar, Department of Computer Science and Engineering, Michigan State University. 2010.

34. **“Advantages and disadvantages of technologies”,** PB Works, 2007.

35. **“AC 2012-3789: Ethical and Social Consequences of Biometric Technologies”,** Dr. Rigoberto Chinchilla, Eastern Illinois University, American Society for Engineering Education, 2012.

36. **“Emerging Biometrics”,** Federal Bureau of Investigation, Biometrics Center of Excellence, 2015.

37. **“The Growing Global Threat of Economic and Cyber Crime”, National** Fraud Center, December 2000.