Biometric Identification Systems

Homi Limbuwala, *VP Business Development, SkandSoft Technologies.*
homi@skandsoft.com, homilimbu@hotmail.com

Biometrics (ancient Greek: bios ="life", metron="measure") is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Examples of biometric characteristics include fingerprints, retinas and irises, facial recognition patterns and hand measurements.

Biometric technologies have become the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

As technology advances, and time goes on, more and more private companies and public utilities will use biometrics for safe, accurate identification. However, these advances may raise privacy and security related concerns throughout society and must be addressed.

Despite the misgivings, biometric systems have the potential to identify individuals with a very high degree of certainty. The three biometric identification technologies, internationally standardized by ICAO (International Civil Aviation Organization) for use in future passports are fingerprint, iris and face recognition.

The United States government has become a strong advocate of biometrics with the increase in security concerns in recent years, since September 11, 2001.

In a speech made by President Bush on May 15, 2006, live from the Oval Office, it was very clear, from then on, anyone willing to go legally in the United States in order to work there will be card-indexed and will have to communicate his fingerprints while entering the country.

"A key part of that system [for verifying documents and work eligibility of aliens] should be a new identification card for every legal foreign worker. This card should use biometric technology, such as digital fingerprints, to make it tamper-proof," said President George W Bush.

The US Department of Defense (DoD) has already issued more than 10 million Common Access Card, which is an ID card issued to all US Service personnel and contractors on US Military sites. This card contains biometric data and digitized photographs. It also has laser-etched photographs and holograms to add security and reduce the risk of falsification.

Operation of a Biometric System

In any biometric system, a person has to first be registered into the system with one or more of their physical and behavioral characteristics saved. This information is then processed by a numerical algorithm, and entered into a database. The algorithm creates a digital representation of the obtained biometric.

Each subsequent attempt to use the system, or authenticate, requires the biometric of the user to be captured again, and processed into a digital template. That template is then compared to those existing in the database to determine a match.

The process of converting the acquired biometric into a digital template for comparison is completed each time the user attempts to authenticate to the system. The comparison process involves the use of a Hamming distance. The measurement of how similar two bit strings are is called Hamming distance.

The Hamming distance measures the percentage of dissimilar bits out of the number of comparisons made. Current technologies have widely varying Equal Error Rates, varying from as low as 60% and as high as 99.9%.

Performance

Performance of a biometric measure is usually referred to in terms of the false accept rate (FAR), the false reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted as genuine users, while the FRR measures the percent of valid users who are rejected as impostors.

In real-world biometric systems the FAR and FRR can typically be traded off against each other by changing some parameter. One of the most common measures of real-world biometric systems is the rate at which both accept and reject errors are equal: the equal error rate (EER), also known as the cross-over error rate (CER). The lower the EER or CER, the more accurate the system is considered to be.

Some of the Biometric Authentication Technologies are:

- Biometric Fingerprint System
- Biometric Face System
- Biometric 3D Face System
- Biometric Iris System
- Biometric Retina System

Fingerprint Recognition System

The fingerprint is the most prevalent biometric system used for personal identification systems to date. One reason for this is that fingerprints have been (for many years) the primary means of identification used by law

enforcement agencies the world over. It's not surprising then that fingerprint based identification is the most active area of biometric research, development, and applications. Finger-scan technology has matured to the point where it is relatively inexpensive, easy to integrate, manage, and use.

Furthermore, newer finger-scan technology called live-scan, is today's replacement of the messy ink-and-roll fingerprint acquisition procedure has reduced the criminal stigma associated with fingerprints.

A person's fingerprints will remain essentially constant throughout their life unless their hands are exposed to excessive or repetitive abrasions such as those encountered by people who perform certain kinds of manual labor.

A fingerprint is the pattern of ridges and valleys on the surface of the finger. The two primary template matching technologies used in fingerprint based PI are minutia (also called Galton features) matching (minutia are local ridge discontinuities) and global matching (correlation of global ridge patterns).

Fingerprint based identification systems work well in user "identification mode," although the manageable template database volume may be smaller than eye-scan based technologies.

Fingerprint technology is flourishing and making personal identification implementation's cheaper, faster, and easier. So much so that it has expanded beyond corporate to personal use.

Before a significant investment is made, application specific performance capability should be verified.

Biometrically Enabled Smart Card – the Way Ahead

A smart card is a plastic card, which holds a processing chip – like those found in computers. The chip on the card is designed to protect the information stored on it using various security mechanisms.

IDsmart, a US based biometric security system provider (www.id-smart.com), has designed a unique new smart card that combines smart card technology with an on-card fingerprint sensor, enabling stand alone biometric fingerprint identification and authorization solutions.

With the IDsmart Capture-Store-Match (CSM) process, the user's fingerprint image is captured, stored and matched directly on the card itself. This process enables IDsmart to decentralize security risks by eliminating the need to store and retrieve biometric information in a database for authentication.

By decentralizing the process, ID-Smart creates a highly secure solution that is easy to use and extremely scalable. This approach also allows a high degree of system customization to meet client's unique business rules and

requirements, like being able to provide a high degree of authentication in remote locations where database connectivity is a problem.

When a fingerprint image is stored to the IDsmart card, the image cannot be extracted from the card. It can only be used internally within the card to "match" the fingerprint of the user. In addition, there is no need to employ separate hardware to capture fingerprint images through sensor-enabled terminals. Existing electronic hardware locks, can be modified to accept this system with minimal changes.

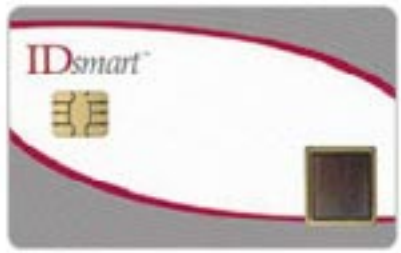
The high performance system design enables IDsmart products to achieve fast processing speeds as well as storage of more than 30 fingerprint templates. One of the IDsmart products utilizes a Fujitsu MBF200 AFIS compliant Fingerprint Touch Sensor providing resolution of 500 dpi.

The IDsmart Enrollment Process

- Finger is placed on the sensor
- The sensor "captures" an "image" of the fingerprint
- The image data is transferred from the sensor to a processor on the card
- The processor examines the image data and computes a template representation of the image (template allows comparisons to be performed)
- The template is then stored directly on the card
- The fingerprint is captured again and matched with the stored template to confirm that the template is valid

The IDsmart Verification and Matching Process

The fingerprint is processed into smaller features, referred to in fingerprint biometrics as minutiae (also called Galton features). Capacitive fingerprint sensors such as one used by IDsmart generate an image of the ridges and valleys that make up a fingerprint by use of electrical current. The processor uses complex algorithms to recognize and analyze these minutiae.



The processor measures the relative positions of minutiae, in the same way you might recognize a part of the sky by the relative positions of stars. A simple analogy is to consider the shapes that various minutiae form when you draw straight lines between them. If two prints have three ridge endings and two bifurcations, forming the same shape with the same dimensions, there is a high likelihood they are from the same print.

Based on the result of the matching process, a secure confirmation message is generated and then interpreted by the controlling device/terminal to make the appropriate decision (i.e. open the door, or allow the transaction).

IDsmart's Superior Security

IDsmart products provide superior authentication and security capabilities to new and existing systems. IDsmart enabled systems benefit from the advantages of the latest biometric authentication technologies, high performance processors, secure data storage, and strong cryptographic systems, all encapsulated in a convenient ISO standard smartcard form factor.

IDsmart's biometric smart cards and related products can be used for secure facility access, secure financial transactions, and a variety of identification confirmation and control systems.

Beyond biometric images, other personal data can also be securely stored and accessed on the card, creating a wide range of options for personal identity tokens such as driver's licenses, credit cards, health cards and more.

"Two-factor" or "Multi-Factor" security solutions requires something you know plus something you have; for example, a debit card and a personal Identification Number (PIN) or biometric. The IDsmart cards can also store other Biometric information like Iris scans or facial recognition patterns, etc. that can then be sent to the Iris scan systems for an added layer of authentication.

AFIS – Automated Fingerprint Identification System

Automated Fingerprint Identification System (or AFIS) is a system to automatically match one or many unknown fingerprints against a database of known prints. This is done for various reasons, not the least of which is because the person has committed a crime. Systems like AFIS have been used in civil identification projects. The intended purpose is to prevent multiple enrollments in an election, welfare, DMV (Depart of Motor Vehicles – Drivers license) or similar system.

IAFIS, the 'I' meaning 'integrated', holds all fingerprint sets (called tenprints) collected in the US, and is managed by the FBI.

Technology

The machine used to scan fingerprints into AFIS is called the LiveScan

Device. The process of obtaining the prints by way of laser scanning is called LiveScan. The process of obtaining prints by putting a tenprint card (prints taken using ink) is occasionally called DeadScan or CardScan. The most common method of acquiring fingerprint images remains the inexpensive ink pad and paper form. Scanning forms ("fingerprint cards") in forensic AFIS complies with standards established by the FBI and NIST.

To match a print, a fingerprint technician scans the print in question, and the computer marks all minutiae points according to an algorithm. In some systems, the technician then goes over the points the computer has marked, and submits the minutiae to a one-to-many (1:n) search. Increasingly, there is no human editing of features necessary in the more sophisticated commercial systems.

US-VISIT (United States Visitor and Immigrant Status Indicator Technology)

US-VISIT is a U.S. immigration and border management system, which has the ability to verify that travelers are who they say they are and do not pose a threat to the United States. The U.S. Department of Homeland Security's (DHS) US-VISIT program supports the U.S. government's efforts to establish the identity management capability that supports that system. The system calls for a layered approach where cross-border travel and U.S. immigration activities are simple and convenient for eligible, low-risk travelers.

US-VISIT is advancing the security of the United States and worldwide travel through information sharing and biometrics solutions for identity management.

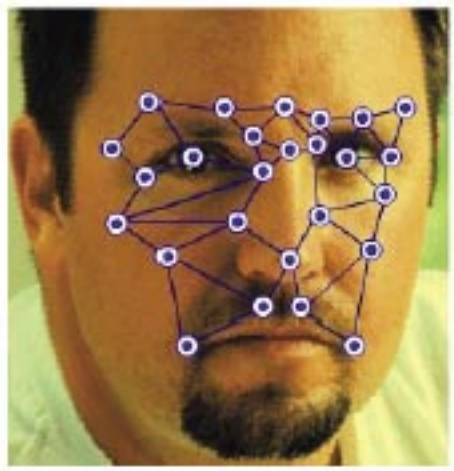
According to the US-VISIT policy, certain non-U.S. citizens who wish to enter the United States have their two index fingers digitally scanned and a digital photograph taken at the U.S. port of entry. Immigration officials have the ability to instantly check the criminal background using ADIS of the person seeking entry.

Visitors to the US, who required a visa inserted in their passport as well as visitors who are eligible for the Visa Waiver Program (VWP) have also been required to use the US-VISIT program.

U.S. citizens are not required to be digitally finger scanned or photographed when they enter United States territory.

Facial Recognition System

Facial recognition is one of the most common methods of personal identification used. Because facial recognition is non-invasive, usually passive, and fairly inexpensive, people generally do not have a problem accepting it as a biometric authentication system. It is probably for these reasons that face recognition has been one of the most active areas of biometric research.



Current facial recognition technology works well in "user verification" mode. For smaller databases, it works well in "user identification" mode.

A facial recognition system is a computer-driven application for automatically identifying a person from a digital image. It does that by comparing selected facial features in the live image and a facial database.

It is typically used for security systems and can be compared to other biometrics such as fingerprint or iris recognition systems.

Popular recognition algorithms include eigenface (or principle component analysis - PCA), fisherface, the Hidden Markov model, and the neuronal motivated Dynamic Link Matching. A newly emerging trend, claimed to achieve previously unseen accuracies, is three-dimensional face recognition. Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images.

Privacy Concerns

Despite the potential benefits of this technology, many citizens are concerned that their privacy will be invaded. Some fear that it could lead to a "total surveillance society," with the government and other authorities having the ability to know where you are, and what you are doing, at all times.

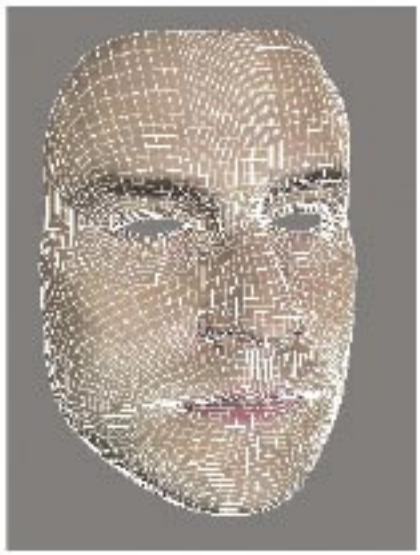
Comparative Study

Among the different biometric techniques facial recognition may not be the most reliable and efficient but its great advantage is that it does not require aid from the test subject. Properly designed systems installed in airports, multiplexes, and other public places can detect presence of criminals among the crowd. Other biometrics like fingerprints, iris, and speech recognition cannot perform this kind of mass scanning.

Some users of this system are:

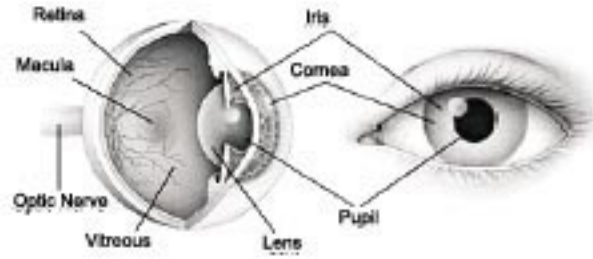
- The German Federal Police use a facial recognition system to allow voluntary subscribers for EU or Swiss citizens to pass fully automated border controls at Frankfurt Rhein-Main international airport.
- Griffin Investigations is famous for its recognition system used by casinos to catch card counters and other blacklisted individuals.

Three-dimensional Face Recognition



Three-dimensional face recognition (3D face recognition) is a modality of facial recognition methods in which the three-dimensional geometry of the human face is used. It has been shown that 3D face recognition methods can achieve significantly higher accuracy than their 2D counterparts, rivaling fingerprint recognition.

3D face recognition achieves better accuracy than its 2D counterpart by measuring geometry of rigid features on the face. This avoids such pitfalls of 2D face recognition algorithms as change in lighting, different facial expressions, make-up and head orientation. Another approach is to use the 3D model to improve accuracy of traditional image based recognition by transforming the head into a known view.



The main technological limitation of 3D face recognition methods is the acquisition of 3D images, which usually requires a range camera. This is also a reason why 3D face recognition methods have emerged significantly later (in the late 1980s) than 2D methods. Recently, commercial solutions have implemented depth perception by projecting a grid onto the face and integrating video capture of it into a high resolution 3D model. This allows for good recognition accuracy with low cost off-the-shelf components.

Iris Recognition System

Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the irides (the tinted annular portion of the eye bounded by the black pupil and the white sclera) of an individual's eyes. Not to be confused with another less prevalent ocular-based technology, retina scanning, Iris recognition uses CCD camera technology to capture an image of an eye, and subtle IR illumination to reduce specular reflection from the convex cornea to create images of the detail-rich, intricate structures of the iris. These unique structures converted into digital templates, that offer exceptional matching performance for both FAR and FRR, provide mathematical representations of the iris that yield unambiguous positive identification of an individual.

The iris is mostly flat and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae), which control the diameter of the pupil. The human iris is composed of elastic connective tissue called the trabecular meshwork. The trabecular meshwork is completely developed by the eighth month of gestation. It consists of a host of visible features namely rings, furrows, freckles, etc. This makes the iris shape far more predictable than, for instance, that of the face.

Iris recognition is rarely impeded by glasses or contact lenses. Iris technology has the smallest outlier (those who cannot use/enroll) group of all biometric technologies. The only biometric authentication technology designed for use in a one-to many search environment, a key advantage of iris recognition is its stablity, or template longevity as, barring trauma, a single enrollment can last a lifetime.

A remarkable fact about the iris (and one of the reasons that the iris image makes an excellent biometric) is that each possesses a highly detailed and unique visible texture.

The texture of the iris, like fingerprints, is determined randomly during embryonic gestation. Even genetically identical individuals have completely independent iris textures.

An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away.

Operating Principle

An iris-recognition algorithm first has to identify the approximately concentric circular outer boundaries of the iris and the pupil in a photo of an eye. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images. The mathematical methods used resemble those of modern lossy compression algorithms for photographic images.

Another thing to consider is the eyelid. Most Westerners have the eyelid directed to forward or upward, but most from the Orient have eyelid downward, interfering with the iris image data.

Iris has 266 points of comparison data while fingerprints have 40, and in theory it has 1078 over 1 error rate. But since the theory assumes that the full iris image is taken without any eyelid interferences in the registration mode, and the same kind of iris image is taken in authentication process, in actual application there are lot more things to consider and rate goes far less down.

Less than 40 percent of the whole iris image can only be used for the iris authentication process. In order to reduce the false-reject risk in such cases, additional algorithms are needed to identify the locations of eye lids and eye lashes, and exclude the bits in the resulting code from the comparison operation.

IRIBIO Protector – Iris Authentication System

Arcturus Innovation's (http://www.arcturusInnovation.com), IRIBIO Protector Authentication System, is an Iris authentication system that's small enough to be fit inside of mouse, yet powerful enough to perform Iris Authentication process by one tiny chip and not by the computer. IRIBIO Protector has an embedded Iris Authentication engine board that operates independently from the computer.

IRIBIO Protector's powerful software protects your PC from illegal attempt to access your computer. It also provides higher security features such as Iris File Encryption, Iris Folder Encryption and Drive / Folder Security (IRIBIO Protector Pro, Enterprise versions).

Now with this powerful, accurate, portable and reasonably priced Iris Authentication Solution, you can finally be free from worrying about unauthorized access to your computer.

Match-on type Iris Authentication System

IRIBIO Protector Authentication System uses "Match-on-type" method of authenticating. In other words, the registration and identification process of your iris is all done by IRIBIO Protector Authentication System, not by your PC. This implies that the Iris Authentication System can be applied to almost any solution. Thanks to the super efficient algorithm, it is now possible to create accessibly priced Iris Authentication System. With existing algorithm, the impossible-to-break barrier for public use of Iris Authentication System is finally over!

Specially Developed Image Sensor

They have a specially designed CMOS image sensor for Iris Scanning system. It clearly and sharply captures the iris for maximum performance. Also incorporates a Concave Mirror Guide system. The 15mm sized concave mirror reflects your iris when you look at the mirror. It tells you where to look at, and lets you see if your iris is focused or not. It is the compact yet very effective iris guiding system which makes the system very compact.

Retinal Scan System

A retinal scan is a biometric technique that exploits the uniqueness of the vascular pattern of the retina to identify them. Typically a retina scanner illuminates, through the pupil, an annular region of the retina (the retina is located inside and at the rear of the eye) with infrared (IR) light and records the reflected vasculature contrast information. The human retina is stable from birth to death, making it one of the most accurate biometric to measure.

It has been possible to take a retina scan since the 1930s, when research

suggested that each individual had unique retina patterns. The research was validated and we know that the blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person. Barring disease and severe injury, the retina's vascular patterns are stable throughout one's lifespan.

A retinal scan involves the use of a low-intensity IR light source and coupler that are used to read the blood vessel patterns, producing very accurate biometric data. It has the highest crossover accuracy of any of the biometric collectors, estimated to be in the order of 1:10,000,000.

Development of the technology has taken longer than expected and for many years the process of taking a retinal scan was measured in tens of seconds. New technology is capable of capturing a retinal scan in less than 1 second.

Some biometric identifiers, usually the less expensive fingerprint scanners, can be fooled. This is not the case with a retina scan. The retina of a deceased person quickly decays and cannot be used to deceive a retinal scan. It is for this reason that retina scan technology is used for high end access control security applications.

Retina scanning possesses each of the four characteristics that make up a good biometric. It works well in both user verification and user identification modes. Additional advantages include small template size and good operational speed.

Retina scanning is considered an exceptionally accurate and invulnerable biometric technology and is established as an effective solution for very high security environments. Some parts of the American Department of Energy were using retinal scanners for identification purposes.

For personal identification system's that requires user "identification mode" over large template databases, this technology may be one of only two options (the other is iris scanning).

Despite these misgivings, biometric systems have the potential to identify individuals with a very high degree of certainty. As technology advances, and time goes on, more and more private companies and public utilities will use biometrics for safe, accurate identification. However, these advances will raise many concerns throughout society, where many may not be educated on the methods.

* Information for the article was gathered from various sources, including Wikipedia. ■