Biometric Authentication Systems

This article provides a broad overview of the subject of biometrics mentioning about the different types of methods, how they are used, how their performance is measured and how beneficial can they prove to be. A biometric system is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user.

PROF. A. C. SUTHAR & DR. G. R. KULKARNI

Biometrics is best defined as measurable physiological and / or behavioral characteristics that can be utilized to verify the identity of an individual. They include fingerprints, retinal and iris scanning, hand geometry, voice patterns, facial recognition and other techniques. They are of interest in any area where it is important to verify the true identity of an individual. Initially, these techniques were employed primarily in specialist high security applications; however we are now seeing their use and proposed use in a much broader range of public facing situations.

But what was wrong with cards and pins?

With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data.

This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- The person to be identified is required to be physically present at the point-of-identification.
- Identification based on biometrics techniques obviates the need to remember a password or carry PINs, biometrics techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

PINs and passwords may be forgotten, and token-based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Thus biometric systems of identification are enjoying a renewed interest.

Types of Biometrics

Various types of biometric systems are being used for real-time identification. Out of the number of biometrics, some of them are rather impractical even if technically interesting. The 'popular' biometrics seem to gravitate at present around following methodologies:

- Fingerprint identification,
- Hand scan,
- Iris recognition,
- Retina scan,
- Face recognition,
- Speaker identification,
- Signature scan,
- Multimodal

Fingerprint Biometrics

Fingerprint Verification: Among all the biometrics techniques, fingerprint-based identification is the oldest method, which has been successfully used in numerous applications.

Everyone is known to have unique, immutable

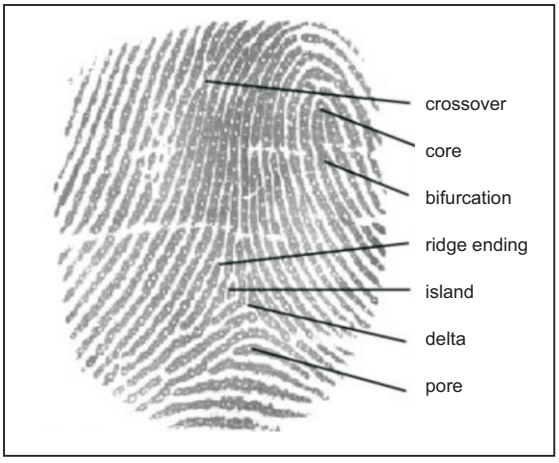

Fig.1.

fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending as seen in fig. 1.

Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. The basic idea is to measure the relative positions of minutiae, in the same sort of way you might recognize a part of the sky by the relative positions of stars.

However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. The most common procedure was the ink-and-roll method. Fingerprint identification through biometrics is the computerized process of manual fingerprint acquisition and storage.

Classification: Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, etc. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database (FBI database contains approximately 70 million fingerprints!).To reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner so that the input fingerprint is required to be matched only with a subset of the fingerprints in the database.

An algorithm has been developed to classify fingerprints into five classes, namely, whorl, right loop, left loop, arch, and tented arch as shown in figures 2, 3,4,5,6.


Fig.2: Whorl


Fig. 3: Right Loop

Fig. 4: Left Loop


Fig. 5: Arch


Fig. 6: Tented Arch

The algorithm separates the number of ridges present in four directions (0 degree, 45 degree, 90 degree, and 135 degree).

Fingerprint technology: The capture device analyzes a fingerprint image to determine the location of the fingerprint core and the pattern type (i.e., right loop, left arch, etc.).

The algorithm estimates the quality of the ridgelines and then extracts the points in which the ridges split, intersect or end (minutia).

The software locates a standard axis over the print, positioned so that the center of the axis is on the core of the print and the axis is aligned so that it runs along the centerline of the print as seen in fig. 7.

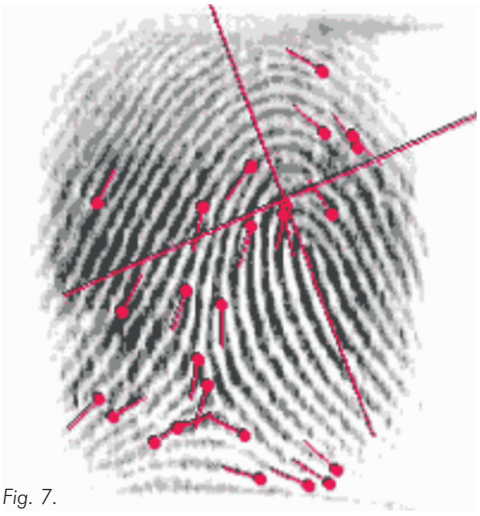
Fig. 7.

Finally, the mapping of the minutia points is converted into a mathematical code called a template. Matching two minutiae-based templates does not require that all extracted minutiae match. In fact very strong matches can be made when as few a one third of the total minutiae match. Because minutia points do not change over time and due to the fact that not all minutia must be present in order to verify identity, minutia based systems are the preferred method underlying most fingerprint biometric systems. For example, cuts and scars may not affect all minutia points and even partial prints left behind at crime scenes may yield sufficient amount of minutia points to run a comparison against a database. One of the largest criminal databases in the world, the FBI's IAFIS system with over 40 million records, uses minutia based fingerprint templates.

Image Capture: A fingerprint scanner system has two basic jobs -- it needs to get an image of your finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images.

A fingerprint image can be captured using one of three scanners as explained below:

Optical Scanner: The heart of an optical scanner is a charge-coupled device (CCD), the same light sensor system used in digital cameras and camcorders. A CCD is simply an array of light-sensitive diodes called photosites, which generate an electrical signal in response to light photons. Each photosite records a pixel, a tiny dot representing the light that hit that spot. Collectively, the light and dark pixels form an image of the scanned scene (a finger, for example). Typically, an analog-to-digital converter in the scanner system processes the analog electrical signal to generate a digital representation of this image. The scanning process starts when you place your finger on a glass plate, and a CCD camera takes a picture. The scanner has its own light source, typically an array of light-emitting diodes, to illuminate the ridges of the finger. The CCD system actually generates an inverted image of the finger, with darker areas representing more reflected light (the ridges of the finger) and lighter areas representing less reflected light (the valleys between the ridges). Before comparing the print to stored data, the scanner processor makes sure the CCD has captured a clear image. It checks the average pixel darkness, or the overall values in a small sample, and rejects the scan if the overall image is too dark or too light. If the image is rejected, the scanner adjusts the exposure time to let in more or less light, and then tries the scan again. If the darkness level is adequate, the scanner system goes on to check the image definition (how sharp the fingerprint scan is). The processor looks at several straight lines moving horizontally and vertically across the image. If the fingerprint image has good definition, a line running perpendicular to the ridges will be made up of alternating sections of very dark pixels and very light pixels. If the processor finds that the image is crisp and properly exposed, it proceeds to comparing the captured fingerprint with fingerprints on file.

Capacitance Scanner: Like optical scanners, capacitive scanners generate an image of the ridges and valleys that make up a fingerprint. But the capacitors sense the print using electrical current. The fig. 8 shows a simple capacitance scanner. The sensor is made up of one or more semiconductor chips containing an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer. The surface of the finger acts as a third capacitor plate, separated by

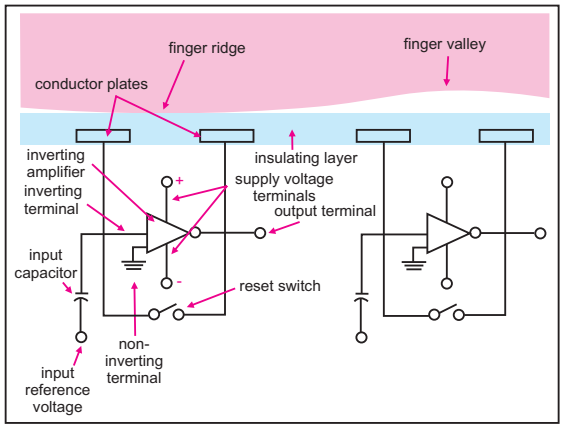

Fig. 8.

the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air. The sensor is made up of one or more semiconductor chips containing an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer. The cells are tiny -- smaller than the width of one ridge on a finger.

The sensor is connected to an integrator, an electrical circuit built around an inverting operational amplifier. Like any amplifier, an inverting amplifier alters one current based on fluctuations in another current. Specifically, the inverting amplifier alters a supply voltage. The alteration is based on the relative voltage of two inputs, called the inverting terminal and the non-inverting terminal. In this case, the non-inverting terminal is connected to ground, and the inverting terminal is connected to a reference voltage supply and a feedback loop. The feedback loop, which is also connected to the amplifier output, includes the two conductor plates.

As you may have recognized, the two conductor plates form a basic capacitor, an electrical component that can store up charge. The surface of the finger acts as a third capacitor plate, separated by the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air. Varying the distance between the capacitor plates (by moving the finger closer or farther away from the conducting plates) changes the total capacitance (ability to store charge) of the capacitor. Because of this quality, the capacitor in a cell under a ridge will have a greater capacitance than the capacitor in a cell under a valley.

To scan the finger, the processor first closes the reset switch for each cell, which shorts each amplifier's input and output to "balance" the integrator circuit. When the switch is opened again, and the

processor applies a fixed charge to the integrator circuit, the capacitors charge up. The capacitance of the feedback loop's capacitor affects the voltage at the amplifier's input, which affects the amplifier's output. Since the distance to the finger alters capacitance, a finger ridge will result in a different voltage output than a finger valley. The scanner processor reads this voltage output and determines whether it is characteristic of a ridge or a valley. By reading every cell in the sensor array, the processor can put together an overall picture of the fingerprint; similar to the image captured by an optical scanner.

Ultrasound Scanners: Ultrasound technology, though considered perhaps the most accurate of the fingerprint technologies, is not yet widely used. It transmits acoustic waves and measures the distance based on the impedance of the finger, the platen, and air. Ultrasound is capable of penetrating dirt and residue on the platen and the finger, countering a main drawback to optical technology.

Even with a few significant drawbacks, but lots of advantages, fingerprint scanners are an excellent means of identification and still have great scope for improvement in the near future.

Hand Scan

This biometric approach uses the geometric form of the hand for confirming an individual's identity. Because human hands are not unique, specific features must be combined to assure dynamic verification. Some hand-scan devices measure just two fingers; others measure the entire hand.

These features include characteristics such as finger curves, thickness and length; the height and width of the back of the hand; the distances between joints and overall bone structure. It should be noted that although the bone structure and joints of a hand are relatively constant traits, other influences such as swelling or injury can disguise the basic structure of the hand. This could result in false matching and non-false matching, however the amount of acceptable distinctive matches can be adjusted for the level of security needed.

To register in a hand-scan system a hand is placed on a reader's covered flat surface. This placement is positioned by five guides or pins that correctly situate the hand for the cameras as seen in fig 9. A succession of cameras captures 3-D pictures of the sides and back of the hand. The attainment of the hand-scan is a fast and simple process. The hand-scan device can process the 3-D images in 5 seconds or less and the hand verification usually takes less than 1 second. The image capturing and verification software and hardware can easily be integrated within standalone units. Hand-scan applications that include a large number of access points and users can be centrally administered, eliminating the need for individuals to register on each device.

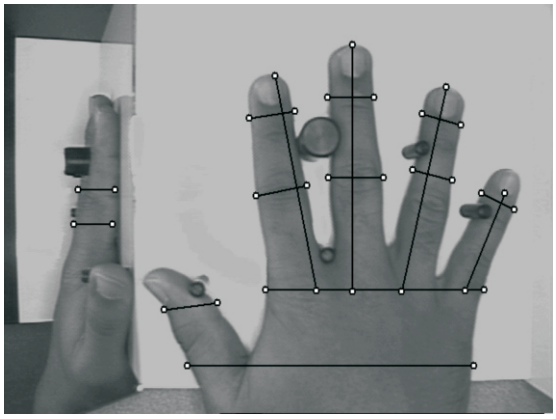

Fig. 9.

Iris Recognition

Iris recognition leverages the unique features of the human iris to provide an unmatched identification technology. So accurate are the algorithms used in iris recognition that the entire planet could be enrolled in an iris database with only a small chance of false acceptance or false rejection.

Iris recognition is based on visible (via regular and/or infrared light) qualities of the iris. A primary visible characteristic is the trabecular meshwork as shown in fig. 10. (permanently formed by the 8th month of gestation), a tissue which gives the appearance of dividing the iris in a radial fashion.

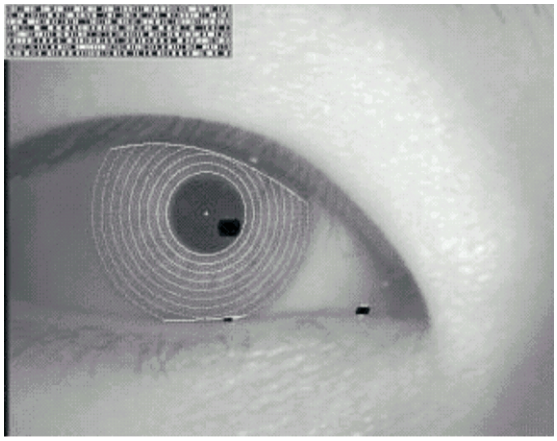

Fig. 10.

Other visible characteristics include rings, furrows, freckles, and the corona, to cite only the more familiar. Expressed simply, iris recognition technology converts these visible characteristics into a 512 byte IrisCode(tm), a template stored for future verification attempts. 512 bytes is a fairly compact size for a biometric template, but the quantity of information derived from the iris is massive. From the iris' 11mm diameter, Dr. Daugman's algorithms provide 3.4 bits of data per square mm. This density of information is such that each iris can be said to have 266 unique "spots", as opposed to 13-60 for traditional biometric technologies.

The Algorithms: The first step is location of the iris by a dedicated camera no more than 3 feet from the eye. After the camera situates the eye, the algorithm narrows in from the right and left of the iris to locate its outer edge. This horizontal approach accounts for obstruction caused by the eyelids. It simultaneously locates the inner edge of the iris (at the pupil), excluding the lower 90° because of inherent moisture and lighting issues. The monochrome camera uses both visible and infrared light, the latter of which is located in the 700-900nm range.Upon location of the iris, as seen above, an algorithm uses 2-D Gabor wavelets to filter and map segments of the iris into hundreds of vectors (known here as phasors).Understanding in detail the 2-D Gabor phasor encoders requires a degree in advanced mathematics, but they can be summarized as follows:

The wavelets of various sizes assign values drawn from the orientation and spatial frequency of select areas, bluntly referred to as the "what" of the sub-image, along with the position of these areas, bluntly referred to as the "where."

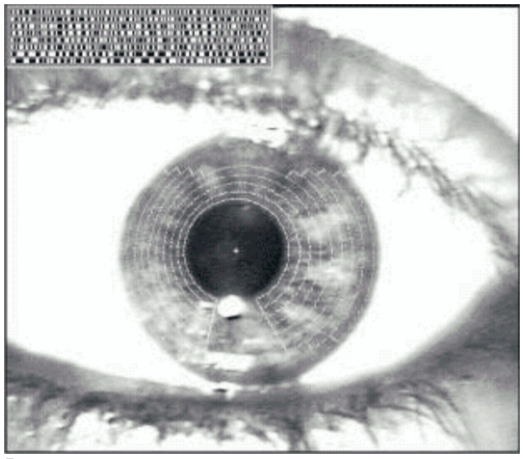

Fig. 11.

The "what" and "where" are used to form the IrisCode. Not the entire iris is used: a portion of the top, as well as 45° of the bottom, are unused to account for eyelids and camera-light reflections. Refer fig. 11.

Essential to the understanding of the technology is that it provides exceptional detail, well beyond what any pictorial or point-based representation could provide (some filters actually span as much as 70° of the iris). Remember also that for future identification, the database will not be comparing images of irises, but rather hexadecimal representations of data returned by wavelet filtering and mapping.

Retinal Scanning

Retinal scanning analyses the layer of blood vessels at the back of the eye. Scanning involves using a low-intensity light source and an optical coupler and can read the patterns at a great level of accuracy. It does require the user to remove glasses, place their eye close to the device, and focus on a certain point. Whether the accuracy can outweigh the public discomfort is yet to be seen.

How it works: The user looks through a small opening in the device at a small green light.

The user must keep their head still and eye focused on the light for several seconds during which time the device will verify his identity. This process takes about 10 to 15 seconds total. There is no known way to replicate a retina, and a retina from a dead person would deteriorate too fast to be useful, so no extra precautions have been taken with retinal scans to be sure the user is a living human being.

Uses: Contrary to popular public misconceptions, and reflective of what is seen in the movies, retina scan is used almost exclusively in high-end security applications.

It is used for controlling access to areas or rooms in military installations, power plants, and the like that are considered high-risk security areas.

Evaluation: Retina scan devices are probably the most accurate biometric available today. The continuity of the retinal pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high-security option.

Unfortunately, the cost of the proprietary hardware, as well as the inability to evolve easily with new technology make retinal scanning devices a bad fit for most situations. It also has the stigma of consumer's thinking it is potentially harmful to the eye, and in general not easy to use.

To be continued in the next issue...