

About Fingerprint Technology¹

Gerik Alexander v.Graevenitz

von Graevenitz - Biometrics, Bonn, Germany

May, 23rd 2004

Overview about Biometrics

Biometrics refers to the automatic identification of a living person based on physiological or behavioural characteristics. There are many types of biometric technologies on the market: face-recognition, fingerprint recognition, finger-geometry, hand geometry, iris recognition, vein recognition, voice and signature recognition.

The method of biometric 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. The identification based on biometric techniques obviates the need to remember a password or carry a token or a smartcard.

With the rapid increase in use of PINs and passwords occurring as a result of the information technology revolution, it is necessary to restrict access to sensitive/personal data. By replacing PINs and passwords, biometric techniques are more convenient in relation to the user and can potentially prevent unauthorised access to or fraudulent use of ATMs, Time & Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, and computer networks.

¹ published in A&S International under the title "Sensing Fingerprints", Volume 52, Taipei, 2003, pp. 102-104

PINs and passwords may be forgotten, and token based methods of identification, like passports, driver's licenses and insurance cards, may be forgotten, stolen, or lost.

Various types of biometric systems are being used for real-time identification; the most popular are based on face recognition and fingerprint matching. Furthermore, there are other biometric systems that utilise iris and retinal scan, speech, face, and hand geometry.

Fingerprint Technologies

Fingerprint recognition represents the oldest method of biometric identification. Its history is going back as far as at least 2200 BC. The use of fingerprints as a personal code has a long tradition and was already used by the Assyrians, the Babylonians, the Chinese and the Japanese. Since 1897, dactyloscopy (synonym for non-computer-based fingerprint identification) has been used for criminal identification. A fingerprint consists of ridges (lines across fingerprints) and valleys (spaces between ridges). The pattern of the ridges and valleys is unique for each individual.

There are two major methods of fingerprint matching: Minutiae matching and global pattern matching. The first approach analyses ridge bifurcations and endings, the second method represents a more macroscopic approach. The last approach considers the flow of ridges in terms of, for example, arches, loops and whorls. As the equal-error-rate is low, therefore fingerprint recognition is very accurate. The prices of such systems compared to other biometric systems are quite low and the user acceptance is very high. The strength of fingerprint identification is, that it can be deployed in a varied range of environments. It is a proven core technology and, the ability of enrolling multiple fingers can increase the system accuracy and the flexibility dramatically.

Optical Fingerprint Sensors

The optical method is one of the most common methods. At the heart of the optical scanner, a CCD-Camera (charged coupled device) is used.



DELSY CMOS-Sensor

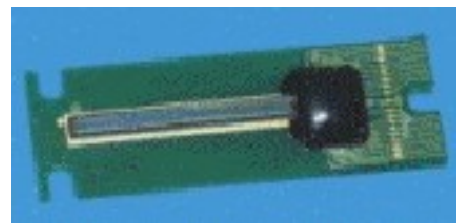
A CCD-Camera is simply an array of light sensitive diodes called photosites. In general the finger will be placed on a glass plate and the CCD camera takes the picture. The CCD system has an array of LEDs (light-emitting diodes) to illuminate the ridges and valleys of the finger. The advantage of optical systems is the very low price; the disadvantage of optical systems is that they are quite easy to fake. Another problem are latent fingerprints, which are remaining fingerprints from the previous finger that was placed on the sensor surface.

Leading manufacturers of optical fingerprint scanners are Delsy, Dermalog, Smiths Heimann Biometrics (spin-off of Jenoptik / Rheinmetall)

Thermalelectric Sensors

The thermal-electric method is less usual. Currently there exists only the Atmel FingerChip™ with thermal-electric technology on the market.

The FingerChip utilizes a unique method for imaging the entire finger by "sweeping" it across the sensor. Sweeping captures successive images (slices), then uses a special software to reconstruct the fingerprint image. This method allows the FingerChip™ to return a large, high quality, 500 dots per inch image of the fingerprint with 256 grayscales.



Atmel FingerCHIP™

The sensor measures the temperature differential between the skin ridges and the air caught in the fingerprint valleys. This method provides a high quality image even on poor quality fingerprints such as ones that are dry or worn with little depth between the peaks and valleys of the fingerprint. The thermal technology also operates well under extreme environmental conditions, like extreme temperatures, high humidity, dirt, oil and water contamination.

In addition to providing a small form factor, the sweeping method also has the benefit of self-cleaning the sensor, which avoids latent fingerprints. Latent fingerprints are prints left behind on a non-sweeping sensor which not only can cause problems with future reads but also leaves an image that can be copied and possibly used to gain access to a system. In fact, the sweeping method utilizing thermal based technology allows the FingerChip to be resistant of many other technologies. The fingerchip works in low-temperature and high humidity environments, too.

Another benefit of this technology is a very big image of good quality, and an always clean sensor. The disadvantage is, that the image quality depends a little bit from the users skill in using the scanner. The second disadvantage is the heating of the sensor array which increases the power-consumption of the sensor. The heating of the sensor is necessary to avoid the possibility of a thermal equilibrium between the sensor and the fingerprint surface.

In high volume the design of the scanner leads to lower prices because the manufacturing process needs less silicon.

Capacitive Sensors

The capacitive method is one of the most popular methods. Like the other scanners the capacitive fingerprint scanner generates an



Veridicom 5th sense™



Infineon FingerTIP™

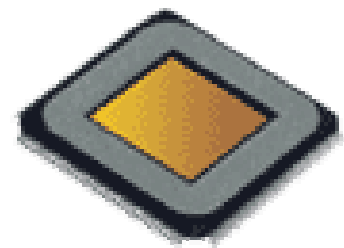
image of the ridges and valleys that make up a fingerprint. The capacitive sensor uses capacitors with electrical current for measuring the fingerprint. A capacitive sensor is made up of an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer.

The main advantage of capacitive sensors is that they require a real fingerprint. Capacitive sensors have problems with wet and dry fingers. With wet fingers the users sometimes get black images, whilst dry fingers make the image pale.

Leading manufacturers of capacitive sensors are Infineon, Veridicom, Sony and ST Microelectronics.

E-Field Sensors

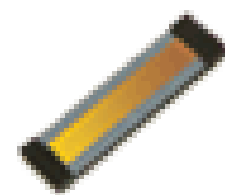
The E-Field sensor works with an antenna array and measures the electric field beyond the surface layer of the skin where the fingerprint begins. The E-field technology claims that it is capable of working for everyone, under tough real-world conditions such as dry, worn, or dirty skin.



Authentec AES4000

E-Field technology creates a field between the finger and the adjacent semiconductor that mimics the shape of the ridges and valleys of the finger's epidermal layer. An under-pixel amplifier is used to measure the signals. The sensors operate together to a clearer image that accurately corresponds to the pattern of the fingerprint and results in a clearer image than optical or DC capacitive technologies produce. This allows E-Field Technology to acquire fingers that other technologies cannot.

With E-Field technology, antenna arrays measure the skin's subsurface features by generating and detecting linear field



Authentec AES2500

geometries the live layer of skin cells is originated beneath the skin's surface.

This is in contrast to the spherical or tubular field geometries generated by simple capacitive sensor, which only read the very top surface of the skin. As a result, fingers that are difficult or impossible to acquire using capacitive sensors can be successfully acquired with E-field Technology.

Recently there exists also a swipe sensor with E-field technology, which is due to be announced for release within the next few months.

One disadvantage is the low resolution of the images and the small image area, what is leading to a higher Equal-Error-Rate (EER).

Touchless Sensors

A touchless sensor works similar to an optical sensor. In general there is a precision glass optic with a distance of 2-3 inches from the fingerprint while the finger is scanned. The fingerprint is put on an area with a hole. One disadvantage can be considered is that dust and dirt may fall through the hole onto the glass optic with the possible result of bad images. Another point is that the scanned fingerprints are spherical which leads to more complex matching algorithms.

Surface Pressure Sensor

The principle of pressure sensing is that when a finger is placed over the sensor area, only the ridges of the fingerprint come in contact with the sensor piezo array.

The valleys in contrast have no contact with the sensor cells. A main difference for the further recognition and

matching to other sensors we have is pressure sensors generate a 1-bit binary image. A 1-bit image has less information than an 8-bit gray-scale image.

A surface pressure sensor can be considered as allowing clearly to sense both dry and wet fingers. Furthermore it has a large sensing area, which enables it to capture

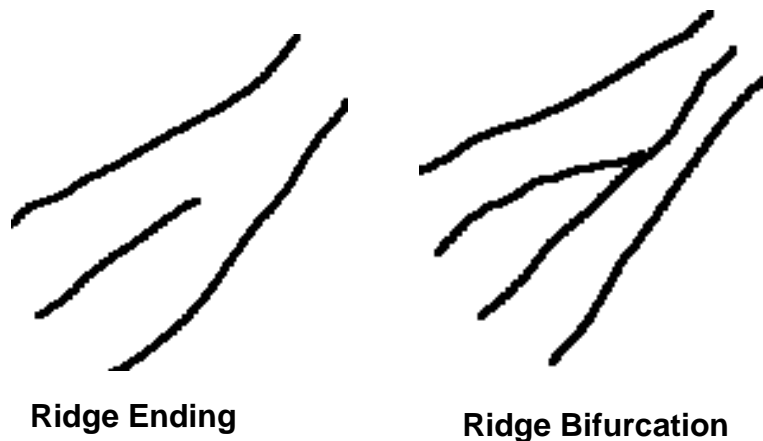


BMF BLP100-Sensor

a complete fingerprint for better accuracy of recognition that leads to a lower EER (Equal Error Rate.)

Fingerprint recognition

Fingerprint-based identification can be placed into two categories: Minutiae-based matching (analysing the local structure) and global pattern matching (analysing the global structure). Currently the computer aided fingerprint recognition is using the minutiae-based matching. Minutiae points are local ridge characteristics that appear as either a ridge ending or a ridge bifurcation.



The uniqueness of a fingerprint can be determined by the pattern of the ridges and the valleys a fingerprint is made of. A complete fingerprint consists of about 100 minutiae points in average. The measured fingerprint-area consists in average of about 30-60 minutiae points depending on the finger and on the sensor area.

These minutiae points are represented by a cloud of dots in a coordinate system. They are stored together with the angle of the tangent of a local minutiae point in a fingerprint-code or directly in a reference template. A template can consist of more than one fingerprint-code to expand the amount of information and to expand the enrolled fingerprint area. In general this leads to a higher template quality and therefore to a higher similarity value of the template and the sample.

The template sizes varies from 100 bytes to 1500 Bytes depending on the algorithm and the quality of a fingerprint. Nevertheless, very rarely there are fingerprints without any minutiae-points that leads to a failure to enroll (FER = Failure to Enroll Rate). It is also difficult to extract the minutiae points accurately when the fingerprint has got a low quality.

Conclusion

Choosing a biometric technology respectively a fingerprint sensor seems to be very difficult. Every sensor technology has got its advantages and disadvantages. Therefore it is not possible to make a general recommendation for a special technology. It is shown that choosing a fingerprint scanner depends on the kind of application the customer wants biometric technology to be implemented. This is strongly depending on the environment. The ensemble playing of the algorithms and the fingerprint sensor is very important in relation to the equal-error-rate.