findBIOMETRICS.com
complete identification verification resource

About Fingerprint Scanning

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable 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.

What is Fingerprint Scanning?

Fingerprint scanning is the acquisition and recognition of a person's fingerprint characteristics for identification purposes. This allows the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual.

There are basically two different types of finger-scanning technology that make this possible.

1. One is an optical method, which starts with a visual image of a finger.
2. The other uses a semiconductor-generated electric field to image a finger.

There are a range of ways to identify fingerprints. They include traditional police methods of matching minutiae, straight pattern matching, moiré fringe patterns and ultrasonics.

back to top

Practical Applications for Fingerprint Scanning

There are a greater variety of fingerprint devices available than any other biometric. Fingerprint recognition is the front-runner for mass-market biometric-ID systems.

Fingerprint scanning has a high accuracy rate when users are sufficiently educated. Fingerprint authentication is a good choice for in-house systems where enough training can be provided to users and where the device is operated in a controlled environment. The small size of the fingerprint scanner, ease of integration - can be easily adapted to keyboards, and most significantly the relatively low costs make it an affordable, simple choice for workplace access security.

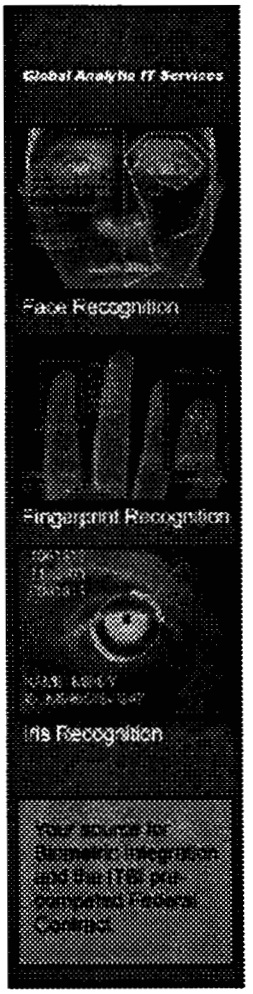
Plans to integrate fingerprint scanning technology into laptops using biometric technology include a single chip using more than 16,000 location elements to map a fingerprint of the living cells that lay below the top layers of dead skin. Therefore, the reading is still detectable if the finger has calluses, is damaged, worn, soiled, moist, dry or otherwise hard-to-read finger surfaces--a common obstacle. This subsurface capability eliminates any attainment or detection failures.

back to top

Accuracy and Integrity

With any security system, users will wonder,... can fingerprint recognition system be beaten? In most cases, false negatives (a failure to recognize a legitimate user)

Showcases
Fingerprint
Iris Recognition
Hand & Finger
Facial Recognition
Voice/Speaker
Consultants
Smart Cards/Multimodal
Signature/Keystroke
2D Bar Codes



are more likely than false positives. Overcoming a fingerprint system by presenting it with a "false or fake" fingerprint is likely to be a difficult deed. However, such scenarios will be tried, and the sensors on the market use a variety of means to circumvent them. For instance, someone may attempt to use latent print residue on the sensor just after a legitimate user accesses the system. At the other end of the scale, there is the gruesome possibility of presenting a finger to the system that is no longer connected to its owner. Therefore, sensors attempt to determine whether a finger is live, and not made of latex (or worse). Detectors for temperature, blood-oxygen level, pulse, blood flow, humidity, or skin conductivity would be integrated.

Unfortunately, no technology is perfect--false positives and spoiled readings do occur from time to time. But for those craving to break free from the albatross that the password has become as both a security and time-management issue fingerprint scanners are worth looking into. It is estimated that 40 percent of helpdesk calls are password related. Whether incorporated into the keyboard or mouse, or used as a standalone device, scanners are more affordable than ever, allow encryption of files keyed to a fingerprint, and can, perhaps most importantly, help minimize stress over that stolen laptop.

back to top

Conclusion

The bottom line advantage of biometrics is this; a biometric template is unique to the individual from whom it is created. Unlike a password, PIN, or smart card, it cannot be forgotten, misplaced, lost, or stolen. Biometrics ensures that a person trying to access your network and applications is actually a sanctioned user, and not in possession of a stolen smart card or someone who found, hacked or cracked a password.

back to top

back

authentication using fingerprints. The solutions replace keys, PINs and passwords in three areas: IT security, physical access and embedded solutions.

Targus

Targus offers two of the most popular Biometrics devices on the market today: The DEFCON Authenticator with USB Hub and the DEFCON Authenticator PC Card Fingerprint Reader.