Biometric Solutions By Classification

Other biometrics technology on the market today depends on modifications to existing hardware, or the addition of new hardware to the system. BioPassword is the only biometrics technology that does not rely on modifications to the existing hardware available on a standard computer system. BioPassword is software based, it does not rely on special scanners to measure and record the information that the user gives to the system. In the areas of user verification, the general methods to verify a person's identity are through the use of physical objects (tokens), through the use of knowledge items (codes, passwords), and through the use of physical characteristics that are part of the person or a person's actions or behavior (keystroke dynamics, fingerprints, voice patterns, signature dynamics).

Keystroke Dynamics

Typing biometrics is more commonly referred to as keystroke dynamics. Keystroke dynamics looks at the way in which a person types or pushes keys on a keyboard. This method is based on the typing characteristics of the individuals such as durations of keystrokes, and latencies between keystrokes, inter-keystroke times, typing error frequency, force keystrokes etc. Specifically, keystroke dynamics measures two distinct variables: "dwell time" which is the amount of time you hold down a particular key and "flight time" which is the amount of time it takes a person to travel between keys.

The original technology was derived from the idea of identifying a sender of Morse code using a telegraphy key known as the "fist of the sender", whereby operators could identify senders transmitting a message by the rhythm, pace and syncopation of the signal taps.

During World War II, the Army Signal Core identified that an individual keying rhythm on a telegraph key was unique. In the early-'80s the National Science Foundation and the National Bureau of Standards in the United States conducted studies establishing that typing patterns contain unique characteristics that can be identified.

Keystroke dynamics works by monitoring both the rate of typing and intervals between letters when typing in a password.

- Benefits: Verification is based on the concept that how a person types, in particular their rhythm, is distinctive. Even if intruders guess the correct password, they cannot type it in with the proper rhythm.
- Drawbacks: If someone is in the lab with you, for example, they could possibly observe someone's key clicks when typing in a password. However, once an imposter is removed from the environment, (causing a lapse in memory), the imposter is unable to replicate the legitimate biometric template.
- Applications: BioPassword technology was recently introduced commercially for User Authentication and Access Control when logging on to the Windows NT operating system.

Biometrics keystroke dynamics technology utilizes - the manner and rhythm in which each individual types passwords and logon codes - to create a biometric template. It measures the keystroke rhythm of a user in order to develop a template that verifies the authorized user.

Fingerprint Verification

The patterns and geometry of fingerprints are different for each individual and they are unchanged with aging. The classifications of fingerprints are based on certain characteristics (arch, loop, whorl). The most distinctive characteristics are the minutiae, the forks, or endings found in the ridges and the overall shape of the ridge flow.

Fingerprint systems are among the most widely used biometric technologies. However, fingerprint systems available for recognizing these characteristics can be complex. Some systems are not capable of differentiating a fingerprint from a live user or a copied fingerprint. Finger surgery, injury, condition of hands might affect the performance of the systems. In some cultures, stigmatizing faces the problem of public acceptance, as it is considered intrusive or stigmatizing.

Facial Analysis

The premise of this approach is that face characteristics (e.g. size of nose, shape of eyes, chin, eyebrows, mouth) are unique revealing individuals identity. The facial applications are well suited for a one-to-many compare to identify a person when presented to a reader.

Hand Geometry

This biometric method is based on the distinct characteristics of the hands; these include external contour, internal lines, and geometry of hand, length and size of fingers, palm and fingerprints, blood vessel pattern in the back of the hand. They work by comparing the image of the hand with the previously enrolled sample. The user enters his identification number on a keypad and places his hand on a platter. A camera captures the image of the hand and then software analyzes it. Other systems use cards where the user's hand is recorded. This technology is mostly used in physical access control, law and order areas.

Speech Analysis

There are various characteristics of the sounds, phonetics, and vocals by which an individual can be identified. Vocal characteristics such as mouth, nasal cavities, vocal tract make the production of speech different for each individual.

Handwritten Signature Verification

This biometric method is based on the fact that signing is a reflex action, not influenced by deliberate muscular control, with certain characteristics (rhythms, successively touches the writing surface, number of contracts, velocity, acceleration).

Summary

The most widely deployed biometric security technologies are face recognition, finger scanning, finger and hand geometry, iris and retina recognition, palm-print recognition, voice recognition, and signature (the handwritten type) recognition. Each requires special equipment and ongoing maintenance and calibration procedures of one kind or another. For example, voice recognition calls for a microphone and a PC sound card. Fingerprint scanners and eye scanners require specialized network and desktop hardware (though some vendors are starting to offer fingerprint-scanning keyboards and panels for laptops). For face recognition, you need a digital camera.

BioPassword, as a software-only solution, our biometric can integrate with any of these other biometrics. Because it is software-only, it also requires no additional hardware, replacement or maintenance costs traditionally associated with other biometrics. It is easy to deploy and inexpensive to install: no new keyboards, or fingerprint/scanner readers with which to contend and no expensive/time consuming employee training required.