AT&T | EMERGING DEVICES

12.18.09

Biometrics

Emerging Devices Technical Brief

Biometrics

Emerging Devices Technical Brief

Definition

Biometrics is the use of physiological and/or behavioral characteristics to recognize or verify the identity of individuals through automated means.

Description

Physiological biometrics is based on data derived from direct measurements of parts of the human body. Fingerprints, iris scans, retina scans, hand geometry, and facial recognition are all leading physiological biometrics.

Behavioral characteristics are based on a person's actions. Behavioral biometrics, in turn, are based on measurements and data derived from an action, thus indirectly measuring characteristics of the human body. Voice recognition, keystroke scans, and signature/sign scans are leading behavioral biometric technologies. One of the defining characteristics of a behavioral biometric is the incorporation of time as a metric, i.e., the measured behavior has a beginning, middle, and an end.

Although behavioral biometrics are based on an individual's actions, those actions are in turn influenced by physiological attributes such as the size of a person's hand (in a signature scan) or the shape of their vocal chords (in voice recognition).

Uses

While no one biometric technology is perfect for all situations, certain biometric technologies will be ideally suited for specific applications based on factors such as security, ease of use and cost. For mobile devices, the most often used

biometric technologies are fingerprints. A significant number of voice and face recognition phones have also shipped recently in Japan. Use of other biometrics (such as iris scans or vein recognition) in mobile devices is not currently feasible due to the size and cost of the associated biometric capture devices. Fingerprint biometrics offer high security levels at relatively low cost but require a sensor on the device. Signature/Sign, and voice recognition input can be added to mobile devices using software and so their costs are less. Fingerprint biometrics offer private and personal characteristics as do Signature/Sign biometrics, while voice recognition can be overheard or recorded and facial recognition is a difficult use model that forces you to take a picture of yourself with your mobile phone. Moreover, both voice and face recognition have a high False Reject Rate due to personal changes (perhaps from a cold, haircut, glasses, etc.). Over 7 million mobile phones have shipped with biometric fingerprint sensors which are generally used to protect private and confidential information content such as e-mail, SMS, photos, contact lists as well as money and banking data on M-commerce enabled mobile phones.

Process

All biometric systems follow the same general process of enrollment, comparison, and identification. The particular biometric component must first be enrolled in order to extract its unique identifying features, which in turn are used in the creation of a biometric template. The biometric template will then be used during a real-time comparison of a new biometric action in determining a successful match. Matching occurs via a processor- based mathematical algorithm of feature extraction and template comparison. As a result, biometric decision-making is very rapid, and in most cases a match/non-match decision occurs in one second or less.

Comparing Biometrics

Biometric technologies are often compared based on several factors including;

1. Universality — How commonly a biometric characteristic is found in each individual.

2. Uniqueness — How well the biometric matching process separates one individual from another.
3. Consistency — How close the biometric measurements are to each other each time they are derived.
4. Permanence — How well a biometric template resists aging.
5. Intrusiveness — How easy it is to acquire a biometric sample for measurement with minimal user interaction.
6. Reliability — Typically measured by the False Reject Rate (FRR), or the rate at which an enrolled user is not accurately identified.
7. Security — Typically measured by the False Accept Rate (FAR), or the rate at which a different person is incorrectly matched to an enrolled individual.
8. Ease of Use (Convenience) — Indicating the time, intuitiveness, ergonomics and general use model by an individual interacting with a biometric system (enrolling and verifying).
9. Circumvention — The ability to fool or "spoof" a biometric system with a non-genuine biometric sample.
10. Integration — The general set of factors which are involved with integrating a biometric technology, such as the biometric capture device's:
    1. size
    2. cost
    3. power requirements
    4. aesthetics
    5. durability
    6. other physical or technical attributes

Security

The main reason to use biometrics on your mobile device is to protect the data on the device and to provide secure yet convenient access to the device and to the network it may be connected to. Unfortunately, mobile device theft is on the

rise and insurance plans are becoming more expensive. It is very common to lose your mobile phone or have it stolen. The use of biometrics protects the data on the device and serves as a theft deterrent since the device is useless to others when it is protected with biometric security. A good biometric solution makes security convenient.

Convenience

The main use case is one of convenience, replacing the use of a password to protect personal and confidential information. Passwords are often easy to hack (guess) and can be hard for users to remember. Significant IT dollars (over $10 per user per year) are spent by IT departments resetting lost or forgotten user passwords. Longer passwords are too cumbersome for users to enter on the mobile phone or QWERTY keypad. The biometric system allows for a convenient way for users to unlock their device.

Personalization

The use of Signature/Sign on PDA's, phone-enabled PDA's and Tablet PC's allows users, to release their electronic signatures to electronic documents and release the significant productivity associated with the use of electronic documents. The use of different secret sign or fingerprint biometric samples allows users to set up hot keys and speed dial numbers. Since each sample is unique, users can launch different frequently used applications. For example, your right index finger can launch your e-mail, while your left index finger can launch your music player. This allows different fingers to quick launch different applications without having to go through detailed menu structures and allows users to personalize their mobile devices.

This same concept can be applied to secure web sites and VPNs. Different biometric samples can be used to not only launch the website, but also to provide a secure log-in. The use of a biometric sensor delivers another factor of authentication which is important for VPN, corporate access, intranet and mobile banking applications.

Finally, fun applications such as speed calling friends, showing favorite photos, and launching favorite songs can be delivered and personalized using different biometric samples.

Navigation

The fingerprint sensor can also be used as a touch pad input device for the phone. Similar to the touchpad on a laptop PC, the fingerprint sensor can detect finger motion across the surface and move the cursor or mouse in response to the finger motion. This replaces mechanical buttons with a smooth electronic solution similar to the way the mouse replaced cursor keys on early personal computers (PCs). Using this type of electronic input device greatly improves menu navigation and the mobile gaming user experience since the finger is not fatigued from an electronic input as it is from a mechanical input. Also, additional commands are added such as tap, double tap, tap and hold and tap and drag which allows for new functions when interacting with new mobile devices. Scrolling through long lists of items such as contacts, e-mail, music and pictures is significantly improved with features such as scrolling, turbo-scrolling and acceleration which allows you to move through items either one at a time, or at various speeds depending on how long (how many) the item list and where the user wants to go. This type of electronic menu navigation also improves the overall mobile web surfing experience when the amount of content for a specific web page is larger than the device screen.

Biometrics Resources

For more information on biometric solutions for mobile applications, visit:

AuthenTec: http://www.authentec.com

Crypto-Sign: http://www.crypto-sign.com