Biometric technologies automate the process of using a physiological or behavioral characteristic to prove someone's identity. The chance of two people—even identical twins—having the same fingerprint is probably less than one in a billion. Fingerprint comparison is the most widely used method of biometric authentication—and the most cost-effective.

Fingerprint recognition compares a user’s fingerprint to a previously stored template and determines validity or authenticity based on this comparison. The template is created from tiny points called minutiae—based on the position of end points and junctions of print ridges—extracted from the fingerprint during enrollment, and comparison of attributes are carried out using complex algorithms during verification.

Total biometric revenues, including law enforcement and large-scale public sector usages, have grown rapidly, reaching an estimated one billion dollars in 2005. Much of this growth is attributable to PC/network access and e-commerce, although large-scale public sector deployments, such as airports, military installations and other secure facilities, continue to be an essential part of the industry.

Biometrics has moved from unconventional specific technological applications to more mainstream applications.

**Overview**

**Design Challenges**

Corporations and institutions considering biometric deployments must investigate a range of questions including costs, compatibility, scalability and user acceptance.

Utilizing fingerprint biometrics can result in many variations in system design, ranging from the basic, stand-alone verification system used for restricted access areas, to the multi-unit networked system with a central hub and many remote scanning units, such as in an airport setting. The stand-alone system would consist of the fingerprint sensor, a microprocessor running the algorithms, a user interface and Flash for the template storage.

An ATM-style system would incorporate a card reader, with the smart card becoming the storage for the fingerprint template. The networked remote scanning system would add a network interface such as USB or Ethernet to provide communication from the scanner to the central hub. A security device could be used by all these systems to encrypt the data before transmission or storage, allowing increased security levels. The challenge is to ensure that the basic solution is versatile enough to be incorporated into the more complex systems as well, with minimal modifications for enhancements.
The MCF5249 ColdFire device interfaces directly to the fingerprint sensor using the integrated queued serial peripheral interface (QSPI) module. Once the fingerprint scan is complete, the data is transferred from the sensor to the MCF5249 over the serial peripheral interface (SPI), before the algorithms are executed. The 96 KB of internal SRAM allows increased performance by running the algorithms in the internal memory, while the enhanced Multiply-Accumulate (eMAC) unit enables the algorithms to be executed efficiently and quickly. The MCF5249 supports external SDRAM and Flash memory modules through a glueless interface. The Flash is used to store the fingerprint templates after enrollment and is accessed for template retrieval during verification. The low power consumption of the MCF5249 allows it to fit into power-critical fields such as in battery-powered applications and does not significantly add to the battery drain of the product. The user display is based around an LCD panel. The general-purpose input/output (GPIO) available on the MCF5249 is used to control the generation of messages on the LCD. The display will inform the user that enrollment is complete as well as display a verified fingerprint message and a rejected fingerprint message subsequent to enrollment. The I²C module on the MCF5249 provides a glueless interface to the card reader in an ATM style system. This allows quick template retrieval from the smart card and reduces user delay. If enhanced data security is required, then a security processor can be attached via the bus interface providing data encryption for storage or transmission purposes. The network interface, i.e., Ethernet or USB, is also attached to the bus interfaces allowing communication between the remote unit and the central hub when this is required.