WHITE PAPER

Milind Borkar,
Marketing Manager, Singlecore DSP,
Texas Instruments

TEXAS INSTRUMENTS

User identification systems leverage smarter biometrics technologies

Introduction

Various means of identity authentication, such as signatures, personal identification numbers (PINs) and passports have been used to ensure security and control access to buildings, financial accounts, electronic devices and many other aspects of everyday life. Now though, the need for faster, more convenient and accurate identity authentication and identification has never been so great. Constant mobile connectivity, the ubiquity of the Internet, the growing popularity of e-commerce and many other factors all accentuate how critical and difficult it can be to authenticate someone's identity.

Modern biometric systems powered by advanced processing architectures are moving identity authentication beyond yesterday's methods toward fast, accurate and secure systems that identify individuals based on unique characteristics. Technology from Texas Instruments Incorporated (TI) is making today's biometric systems more reliable and convenient, while ensuring greater overall protection.

Key links:

www.ti.com/biometrics
www.ti.com/irishield
www.ti.com/dsp

Knock, knock. Who's there?

The world is a complex place. Knowing who is on the other side of the door before opening it is no longer as simple as looking through a peep hole. It's much more difficult to authenticate the identity of someone involved in an online interaction or transaction, which can occur hundreds of thousands of times a day. Many of the older identity authentication methods (keys, PIN numbers, badges) can be lost, forged or stolen leading to false authentication and resulting implications. Instead of relying on external objects or memorized codes, biometric systems determine an identity from the individual's intrinsic qualities, a fingerprint, the pattern of an iris, even DNA. A biometric identification system is able to quickly recognize and analyze these anatomical characteristics, match them against data sets of approved or disapproved persons and either grant or deny access.

Virtual mobility across the Internet and physical mobility around the world only highlight the need for biometric identification systems. Every point of entry – whether into a computer, communications applications, building, campus or country – must be protected.

The basic structure of biometric systems

Fingerprint matching applications were the first and still are the most commonly deployed type of biometric system. The basic architecture (Figure 1) of all such systems is virtually

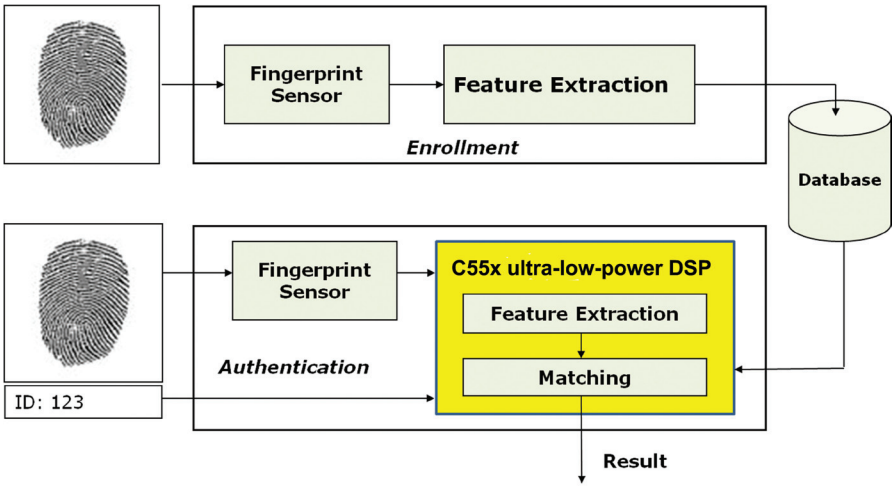

Figure 1. Block diagram of fingerprint recognition system.

the same. Typically, a biometric system is comprised of four major subsystems: sensing, feature extraction, template matching and output.

- **Sensing**

  The sensing or input element scans and captures the subject's anatomical characteristics and then converts this image into digital information. The sensing element might incorporate a camera, CMOS or optical sensor, or one of TI's high-performance charge coupled device (CCD) sensors. Microphones would be deployed in voice-based identification systems while other types of sensors such as thermal and capacitive sensors are used as well.

- **Feature extraction**

  Since many biometric systems are based on computationally intense algorithms, such as image and voice processing, the demands on the system's processing capabilities can be quite challenging. The processor takes data from the sensor, for example, the image of a face during a facial scan, and extracts data points to construct a "template" or a model of the person's unique biometric characteristics. Digital signal processors (DSPs), like TI's **OMAP-L13x DSP+ARM9™ processor**, **TMS320C674x DSP** and **TMS320C55x™ DSP** are ideal for processing the computationally intense algorithms required for feature extraction in biometric systems. As biometrics continue to evolve in the future into smaller form factors, including more battery-powered handheld authentication devices, TI's low-power DSPs will continue to provide the processing capabilities required for critical biometric functionality. TMS320C6000™ DSPs, for example, feature a parallel architecture that enables fast processing of up to 3648 million multiply accumulates (MMACs) while consuming less than 600 mW of power. Key benchmarks on Discrete Fourier Transforms (DFT) as well as corner detection functions show that TI's C674x DSP core provides more than five times improvement in performance over an ARM® Cortex™-A8 core operating at the same frequency.

- **Template matching**

  In an access control application, for example, the biometric system might compare the template of a fingerprint presented at an authentication station with those stored in a database of templates of people who are allowed admittance. If the template is not in the database, the person cannot be identified and is not granted access. Depending on the size of the database, storage can be accomplished in solid state memory located in the authentication station, either integrated with the DSP processor or external to it, or the database might be stored on a remote server that is accessed through a secure communications link. For embedded solutions, key benchmarks for commonly used matching functions, like correlation, show that TI's C674x DSP provides more than eight times improvement in performance over an ARM Cortex-A8 processor operating at the same frequency. To protect the identities contained in storage, biometric

templates are typically encrypted with a state-of-the art encryption algorithm, most of which require mathematically intense computations. Again, TI's DSP platform gives system designers a wide range of scalable and pin-for-pin compatible processors (within product platforms) to meet the specific needs of each particular biometric application.

- **Output**

  Once the biometric system's processor has completed its template search and comparison algorithms, it must output the results. Based on the system's findings, some action is likely to occur. For example, the output might be connected directly to a mechanical apparatus which unlocks a door or the results might be sent through a wireless connection and displayed on a screen for review by a border-crossing guard.

Biometrics today and tomorrow

Biometric identification technology has evolved considerably from the days when digital fingerprint systems were a marvel. Over the last decade, the computational abilities, cost effectiveness and overall capabilities of DSPs as well as processors featuring DSP and general-purpose processing (GPP) cores have continued to advance by leaps and bounds. For example, the DSP and ARM9™ cores integrated into TI's OMAP-L138 processor deliver tremendous performance for high-end biometric systems. At the same time, cost-per-processing cycle has dropped precipitously, making DSPs and DSP/GPPs ideal solutions for computationally intense applications like biometrics. With increasingly more powerful and cost-effective processors at their disposal, designers are empowered to implement more demanding algorithms while decreasing the relative price point of the system.

An extensive example of a sophisticated multimodal biometric system is being implemented in India, one of the most populous countries in the world. India has undertaken a User Identification (UID) initiative and is enrolling all of its citizens in a biometric identity database. The UID program, which began in 2009, is being spearheaded by a cabinet-level minister who expects that half of India's 1.2 billion citizens will be enrolled by 2014. Some one million new biometric identities are being added every day from 20,000 sites across the country. One of the main objectives of the UID program is to improve the government's distribution of approximately 60 billion USD in welfare support to India's poor and rural areas where many residents do not have proper identity documentation and therefore have difficulty opening bank accounts. With biometric identities, the poor will be better able to open bank accounts so that the government can deposit welfare support directly into their accounts. Like other contemporary biometric systems that place emphasis on robustness and accuracy, India's UID program is multimodal. Data is gathered and stored on all 10 fingerprints and both irises. A digital photograph of the face is also recorded.

In the U.S., several government initiatives using biometrics are underway. The Department of Homeland Security has instituted the Visitor and Immigrant Status Indicator Technology (US-VISIT) program which collects digital fingerprints and facial images of international visitors to the country for use for in a biometric

identification system at the border. This database is shared with a number of governmental agencies to authenticate individual identification. In addition, the Federal Bureau of Investigation established the Biometric Center of Excellence in 2007, a program for exploring and advancing the use of new and enhanced biometric technologies and capabilities for integration into operations.

Figure 2. Biometric passports have now been adopted by many countries, including the U.S. In the United Kingdom and other European countries, a digital template of the bearer's face is stored in the passport.

Some newer so-called "soft biometric" systems do not even attempt to match individual identities, but rather general demographics such as gender and age. Certain retail chains are evaluating the use of high-definition, large-screen displays to provide advertisements to their patrons as they shop. In some stores, such systems are complemented by a soft biometric application that uses cameras to determine the general demographics of individuals as they approach each display. Following the execution of biometric and other algorithms, age and gender appropriate ads are displayed so viewers see only those advertisements that might interest them.

The future of biometrics identification

An increasingly broad and very versatile selection of processing elements on which to base biometric systems as well as stronger safeguards for biometric databases ensures that this technology will continue to be adopted throughout society. Distributing a biometric system's processing load across a computationally powerful DSP/GPP platform can increase the processing efficiency of the system, allowing for the deployment of less costly processing platforms or providing the added processing capabilities needed for more sophisticated biometric algorithms.

Many of TI's DSPs and DSP/GPP embedded processors have a proven track record in embedded biometric applications. At the value end of the spectrum, TI's C55x™ ultra-low-power DSPs are cost and power optimized for small- to medium-sized systems with hundreds of identities stored in the biometric database.

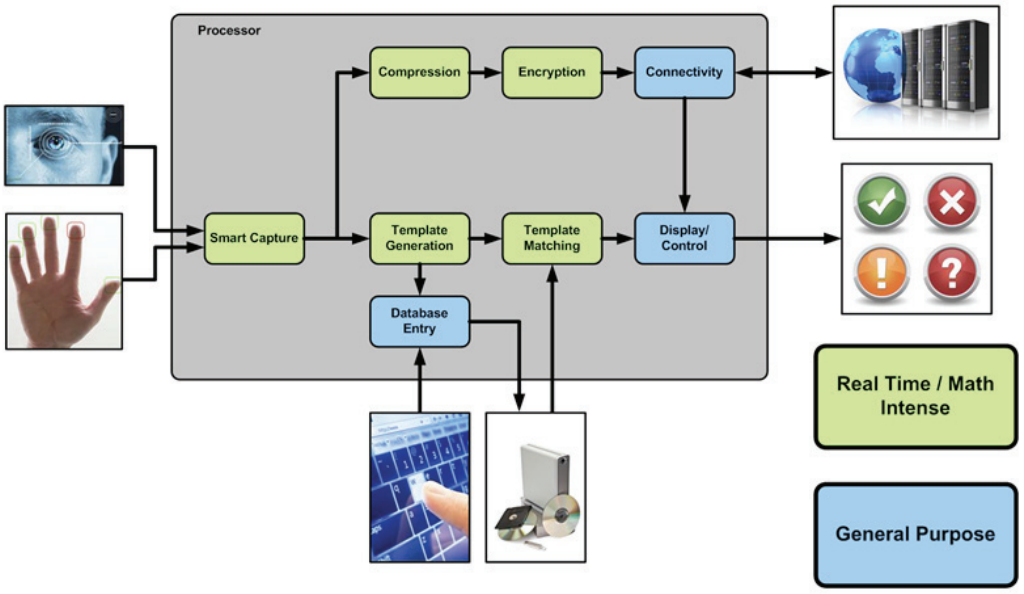

Figure 3: Processing load distribution in typical biometrics applications. Key mathematical and real-time functions are better suited to a DSP, others are better suited to a general-purpose processor.

TI's C674x DSPs provide higher performance for greater imaging resolution and a larger database of identities. For top-end systems, TI's OMAP-L13x DSP+ARM9™ processors support advanced connectivity options, high-level operating systems for graphical user interfaces and optimized performance capabilities.

In addition, TI offers a broad range of support assistance across the entire system. On the power side, Power Management Units (PMUs) designed for optimized support of the DSPs are available to allow the system designer to focus on the business of creating biometric applications without having to worry about getting it powered properly. On the DSP side, this includes hardware kits and sophisticated software development tools. Moreover, several companies in **TI's third-party Design Network** have been actively developing biometric, image-processing and voice-processing subsystems that could be integrated into full-blown biometric applications. TI Design Network member IriTech, Inc.'s fully embedded iris recognition solution, **IriShield™**, is based on TI's C6748 DSP. The module is able to match 1:1000 templates in less than 750 ms and has the capability to store up to 10,000 user templates. IriShield runs on USB power and comes with an application programming interface that allows customers to easily integrate IriShield into their systems without the need to be experts in iris recognition technology.

For more information on TI's DSPs for biometrics, visit **ti.com/dsp**.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components which meet ISO/TS16949 requirements, mainly for automotive use. Components which have not been so designated are neither designed nor intended for automotive use; and TI will not be responsible for any failure of such components to meet such requirements.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265