DSP for Smart Bio-Metric Solutions

Maddineni Rakesh Chowdari

[1]SRM University, Bharathi Salai, Ramapuram, Chennai-600089, India

Abstract: ***Biometrics is the science of measuring and statistically analyzing biological data. In information technology, biometrics refers to the use of a person's biological characteristics for personal identification and authentication. Fingerprint, iris-scan, retinal-scan, voiceprint, signature, handprint and facial features are some of the most common types of human biometrics. Digital signal processors (DSPs), which are specially designed single-chip digital microcomputers that process electrical signals generated by electronic sensors (e.g., cameras, fingerprint sensors, microphones, etc.), will help to revolutionize this world of biometrics. The core of the biometric authentication process is made up of image processing and pattern matching or minutiae comparison algorithms. And the programmable DSP, with architecture well-suited for implementing complex mathematical algorithms, can efficiently address all the processing needs of such a system. The following information introduces the concept of a complete biometrics system solution based on semiconductor components, development tools, and software solutions. Additionally, the various concepts that outline the inherent advantages of a DSP in a biometric system - better accuracy, faster recognition and lower cost, all leading to smarter biometrics - will also be covered.***

Keywords: Application of DSP in Bio-Technology.

1. Introduction

Imagine how convenient it would be to activate the security alarm at your home with the touch of a finger, or to enter your home by just placing your hand on the door handle. How would you like to walk up to a nearby ATM which will scan your iris so you can withdraw money without ever inserting a card or entering a PIN . You will basically be able to gain access to everything you are authorized to, by presenting yourself as your identity.

This scenario might not be as far off as we might expect. In the near future, we may no longer use passwords and PIN numbers to authenticate ourselves. These methods have proven to be insecure and unsafe time and time again. Technology has introduced a much smarter solution to us: Biometrics.

Biometrics, the use of a person's unique biological characteristics (such as face, voice, or fingerprints) for personal identification. The advantages of biometrics are becoming more apparent with the increasing use of computers in our daily life. As cyber crime increases, the need for security against identity theft becomes more and more apparent. Add to this the ever-increasing threat to personal, corporate and government assets, the need for better forms of security is obvious.

Biometric authentication will help in enhancing the security infrastructure against some of these threats. After all, physical characteristics are not something that can be lost, forgotten or passed from one person to another. They are extremely hard to forge and a would-be criminal would think twice before committing a crime involving biometrics.

2. Biometrics System

The four basic elements of a typical biometric system are: sensing, processing, storage and interface to an existing infrastructure.

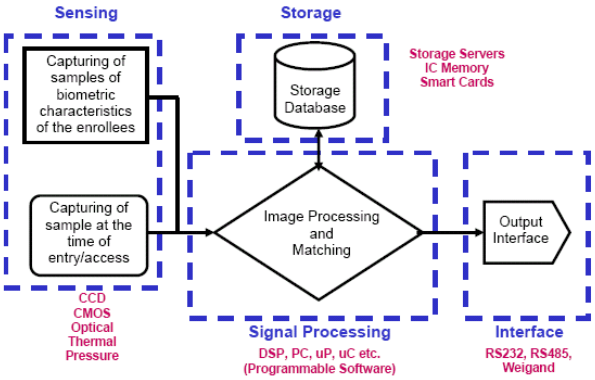

Figure 1: Biometric Systems Element

2.1 Sensing Element

The *sensing element*, or the input interface element, is the hardware core of a biometrics system and converts human biological data into digital form. This could be a complementary metal oxide semiconductor (CMOS) imager or a charge coupled device (CCD) in the case of face recognition, handprint recognition or iris/retinal recognition systems; a CMOS or optical sensor in the case of fingerprint systems; or a microphone in the case of voice recognition systems. These sensors capture the biometric information and convert it into a digital form that can be processed by the next stage

2.2 Processing Element

The *processing element* is generally a microprocessor, digital signal processor or computer that processes the data captured from the sensors. The processing of the biometric image generally involves image enhancement, normalization, template extraction, and matching/ comparison of the biometric template during enrollment and authentication of the users.

A programmable processor like the DSP from TI can address all the processing needs of a biometric system while providing the most viable path to standards and feature upgrades. A DSP allows the product to be small and portable while maintaining power-efficient performance — all at a low overall system cost.

The DSP architecture is built to support complex mathematical algorithms that involve a significant amount of multiplication and addition. The DSP executes the multiply/add feature in a single cycle (compared to multiple cycles for RISC processors) with the help of the multiply/accumulate (MAC) hardware inside the arithmetic logic unit. In addition, the Harvard architecture of the DSP (multiple busses) allows instruction and operand fetches in the same cycle for increased speed of operation.

Developers of biometrics systems can take advantage of this architecture to enhance the resolution of the captured image with the use of two-dimensional Fast Fourier Transforms and finite IR filters. Because the accuracy of a system is as much dependent on the input image as it is on the processing algorithm, this helps in improving the overall accuracy and error rate of the biometrics system - a key performance metric. With the high performance capabilities of the DSP, the total recognition time of the system can be reduced without an increase in power consumption generally associated with faster processors. This low-power consumption in TI DSPs is achieved with hardware enhancements and leading-edge process technology.

2.3 Storage Element

The function of the *storage element* is to store the enrolled template that is recalled to perform a match at the time of authentication. For most identification solutions (1:N), the storage element would be random access memory or flash EPROM or some other form of memory IC, and in some other cases it could be a data server. In the case of verification (1:1), a removable storage element like a contact or contact less smart card can be used.

2.4 Interface Element

Finally, there is the output *interface element*, which will communicate the decision of the biometric system to the interfaced asset to enable access to the user. This can be a simple serial communication protocol like RS232, or the higher bandwidth USB protocol. It could also be the TCP/IP protocol via a wired medium like 10/100 Ethernet or through a wireless medium using either the 802.11b protocol, ISM RF band, RFID, Bluetooth, or one of the many cellular protocols.

3. Complete System Solution

Add software solutions and development tools to the broad spectrum of DSP and analog components available from TI and you have a supplier with the most complete system solution offering (see Figure 2). A wide array of eXpress. DSP™-compliant software and hardware development tools are available for all DSP platforms.

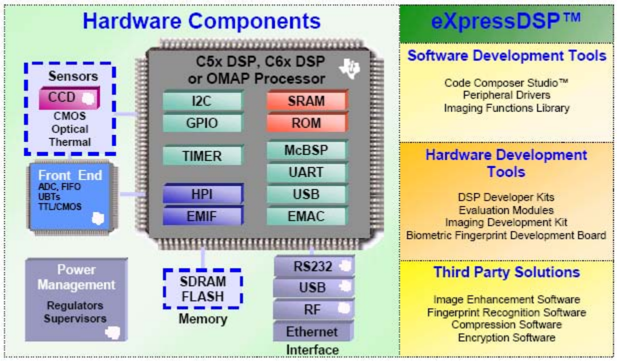

Figure 2: Complete Biometric System Solution

For biometrics, specific developments tools like fingerprint development kits, software drivers and multiple algorithms for fingerprint verification, speaker verification and signature verification are available today from third parties.

4. DSP for Secure and Trusted Biometrics

Today's biometric systems are based mainly on interfacing the sensing element with a personal computer. The sensors are generally networked to a computer server to service unlimited users and multiple access points. The cost of using PCs is prohibitive and the communication link between the sensor and the PC/server could be a major cause for concern with regards to security and privacy. A biometrics solution based on DSPs can function both as a *secure standalone device* for recognition (1:1 or 1: few) and as a *trusted network device* for identification (1: many).

4.1 Secure Standalone Device

A *secure standalone device* is one where all the functions of authentication are carried out within the confines of the embedded processor and the result is communicated or displayed along with control signals to deny or grant access to the secured asset. The original enrolled template or pattern is either stored in the memory within the product or on a smart card which is carried on the user's person.

In a secure standalone device, the captured image is transferred to the embedded processor (DSP) which then converts/encodes the analog video stream into a digital image for camera based biometrics like facial, and iris/retinal recognition. The encoding can then be done on the DSP using off-the-shelf encoding software available for the TI DSP (MPEG2, JPEG, etc). With fingerprint recognition, no encoding is required as the output of the sensor module is a grayscale bitmap image. In the case of optical sensors, analog front-end components like amplifiers and analog-to-digital converters may be needed to generate the bitmap.

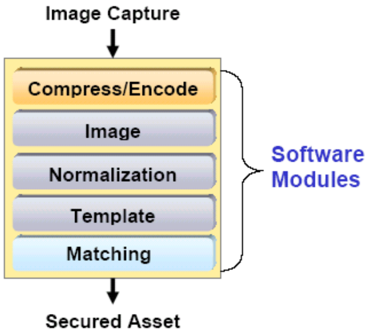

Figure 3: Use of DSP as a secure standalone device

After the capture (and encoding), the image can then be enhanced with one or more functions like histogram equalization, filtering, edge correction, etc. The enhancement process results in a higher resolution image, which can then be normalized. Normalization is the process of creating standard input images with appropriate pixel information independent of the sensor used for image capture. This normalized image is then processed using the core algorithm to extract the template information. This template can then be stored in a memory module and recalled to perform the match against another live biometric data presented at the time of authentication (this live biometric data also goes through the same stages described above). The matching could be an image data comparison or a pattern matching function, which has additional information on the location of the reference, angle of rotation, scale, etc.

All of the functions mentioned above can be better implemented by using software on a programmable DSP while maintaining the flexibility of adjusting the parameters of the system as per the application requirements.

4.2 Trusted Network Device

A *trusted network device* is one in which the captured biometric can be extracted into a template (in the case of minutiae) or encoded and compressed (in the case of image patterns) and then encrypted before being transmitted to a computing server on which the matching against a database of templates/patterns is carried out as part of the identification process. In the case of a networked identification system (like access to PCs in a LAN or WAN or POS terminals connected to a credit processing network), there are multiple access points and the user needs to be identified amongst a database of users as an authorized user. To secure such a network, the access point that is the source of the live biometric data being presented needs to be a trusted point of access.

First, encrypting the extracted template or the captured image and transmitting this encrypted data to the remote server using a public key infrastructure can help establish this trust. This can help ensure that the biometric data presented for a match is not a digital file of a bitmap image being fed into the system by hacking or breaking into the communication link between the access point and the database server.

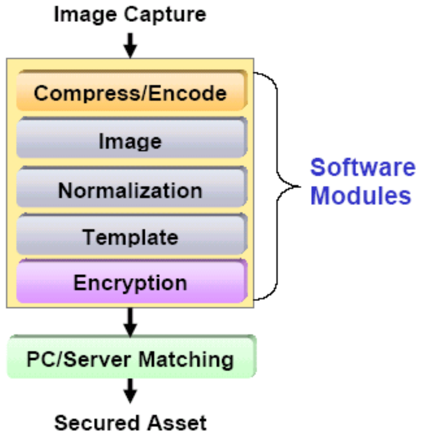

Figure 4: Use of DSP as a Trusted Network Device

With the use of an embedded DSP in the trusted network device, all the functions of a secure standalone device mentioned above can be implemented excluding the matching step and still have performance headroom to execute software encryption (e.g., 3DES, RSA1024, etc.) algorithms.

5. Biometric System Examples

The following sections provide examples of the TMS320C5509 DSP-based biometric fingerprint solution and the TMS320DM642™ DMP-based biometric smart camera.

5.1 TMS320VC5509 DSP-Based Biometric Fingerprint Solution

An example fingerprint biometric system based on TMS320C5509 DSP is shown in Figure 6

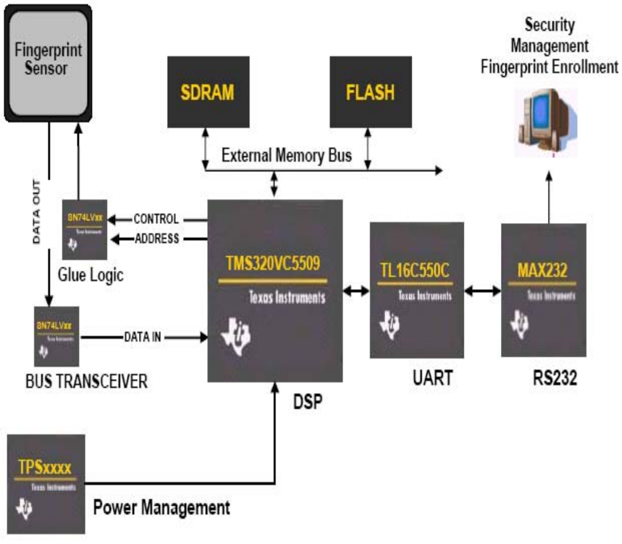

Figure 5: TMS320C5509 DSP based fingerprint biometric solution

In addition to the DSP, the TPSXXX power management, TL16C550C UART, MAX232 serial driver (RS232), standard linear and logic components like universal bus transceivers and NAND gates are the other hardware components from TI used to build a standalone fingerprint system with serial interface. Additionally, third party software solutions for image enhancement and matching are available to complete the system solution.

If this design is used in a computer mouse or keyboard, the internal USB slave port can be used as the interface to the PC. If it is networked to a server managing multiple fingerprint access modules, the designer can make use of the RS485 component (SN65XXX and SN75XXX) or use a 10/100 Ethernet interface connected to the external memory bus on the DSP. If the application requires wireless connectivity then the system developer can opt to use an RFID component (low frequency, Tag-It™ high frequency and encrypted transponders and readers) for contact less smart card solutions.

5.2 TMS320DM642 DMP-Based Biometric Smart Camera

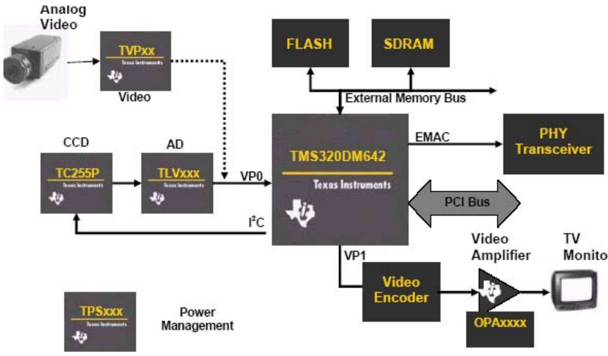

Figure 6: TMS320DM642 DMP-Based Biometric Smart Camera

Figure 6 illustrates a Biometric Smart Camera module that can be used as a digital surveillance camera or as part of a facial recognition system based on the TMS320DM642 digital media processor. The DM642 processor is made up of the C64x DSP core coupled with video ports, 10/100 EMAC controller and a 66 MHz PCI bus in addition to standard peripherals.

The facial image capture can be carried out either from a snapshot (CCD combined with data converter) or streaming video image (external camera source via TVPXXXX video decoders) as the video ports on the DM642 are configurable. One of the three video ports on the DM642 can be configured to output the image to a display/monitor.

In addition to the on-chip 10/100 Ethernet MAC controller and the 66 MHz PCI bus that provide flexibility in terms of interface options, TI supports independent or integrated FireWire™ IEEE1394 ICs (TSB43XXXX - integrated, TSB12XXXX - link layer and TSB14XXXX – physical layer).

6. Conclusion

Using DSP as the embedded processor of choice for enabling smart biometric systems can provide the following advantages:

- Fast, accurate, secure and trusted authentication
- Enable new applications with one scalable design
- Reduce overall cost of development

References

[1] Digital Signal Processing: Principles, Algorithms, and Applications by J. G. Proakis and D. G. Manolakis.
[2] Multi-rate Digital Signal Processing by R. E. Crochiere and L. R. Rabiner.
[3] Theory and Application of Digital Signal Processing by Rabiner and Gold. A comprehensive, industrial-strength DSP reference book.
[4] Biometrics by John D. Woodward, Jr., Nicholas M. Orlans, Peter T. Higgins
[5] Biometric Technologies and verification systems by John R.Vacca
[6] Guide to Biometrics by Ruud Bolle.

Author Profile

Maddineni Rakesh Chowdari is currently studying his B. Tech (ECE) in SRM University, Ramapuram, Chennai, India