Simple System Solutions Consulting
School of Engineering
University of Guelph
Guelph, Ontario N1G 2W1

Background Information

This project focuses on the problem of supporting efficient biometric fingerprint-based user authentication in embedded systems. Biometric user authentication is the process of verifying the identity of a user by distinctive physiological characteristic such as fingerprint, voice or facial features. Biometric approach is generally superior to conventional method of assumed surrogate identity (e.g. passwords, access cards) when a higher level of security is required without typical drawbacks of increased inconvenience to users. Fingerprints are the most widely used biometric features for personal identification.

In the scope of this project fingerprint-based approach will be explored. Implementing fingerprint authentication system requires realizing finger print scanning, processing, storing and matching algorithms that are capable of supporting efficient fingerprint-based user authentication in embedded system. Most automatic systems for fingerprint comparison are based on identifying local discontinuities in the fingerprint pattern, called minutiae [1]. In order to reliably identify minutiae image must be enhanced and in order to match fingerprints minutiae must be identified. Both image enhancement and matching algorithms can be greatly optimized by using custom instruction set [2].

Proposed Solution

This project focuses on implementation and optimization of Fingerprint Authentication System (FBAS) according to listed constrains and criteria. As shown in Diagram 1, FBAS can be separated into few distinct components – fingerprint sensor, processing device, database and various user interfaces. Processing device can be further subdivided into minutiae extraction, matching and storing components.

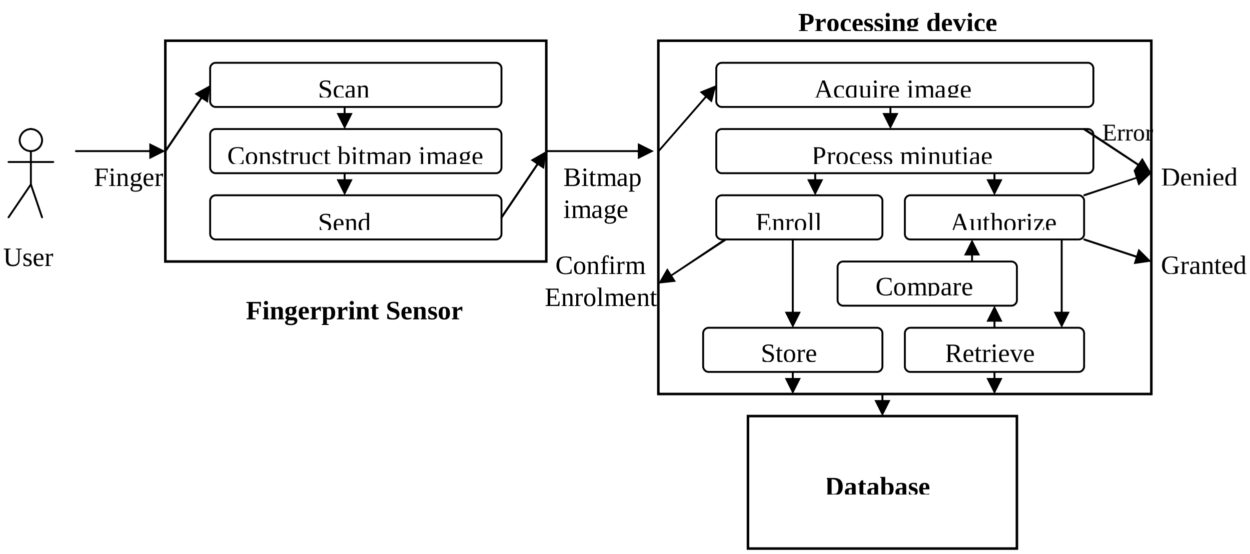

Diagram 1: Fingerprint Based User Authentication System

Fingerprints will be acquired as a bitmap image using biometric sensor. There is wide variety of different approaches to scanning fingerprint, from optical scanning, surface pressure-sensing to RF imaging also known as TruePrint technology. Since RF imaging provides superior results [3] we will be using RF imaging sensor, such as Atmel AT77C101B- FingerChip or Verifi P4000 with AuthenTec AES4000 sensor.

After acquisition fingerprint bitmap image will be transmitted to microprocessor processing hardware for enchantment, minutiae extraction, matching and storage. The processing device will directly interface with a sensor and will run minutiae extraction, matching and storage algorithms. As such it should have sufficient memory and processing power to perform these tasks in reasonable time. For this purpose we will be using Atmel AT91RM9200 or as a last resort Motorola 68HC12 microcontroller evaluation board.

Our minutiae extraction algorithm will be based on open-source algorithm or Atmel BioCore software. These algorithms work functionally in the same way using these basic concepts; using the bitmap image to normalize the captured image, determine image orientation, create frequency image and region mask[1], filter and binarize image and extract minutiae by examining each pixel and its immediate neighbors [2]. This processor-intensive task will identify fingerprint in such way that it can be stored and compared to other fingerprints in database.

Minutiae matching algorithm will compare it against templates in database to determine a match. This algorithm compares minutiae positional matrixes and determines matching score, if it exceeds a given threshold it declared as a match. [2]. All minutiae positional matrices are stored in the database along with the clearance status.

Overall there is great variety of different components fingerprint authentication system can based on but only one functional way it can work – acquire, process and compare fingerprint image.

Constraints

- Tamper resistance. Authentication system should be resilient to tampering to prevent unauthorized access.
- Sensor should be resistant to abrasion, more than 0.5 million finger sweeps
- System should not generate false positives

Criteria

- Low fingerprint sensor cost. Single site is likely to include multiple fingerprint sensors per single processing device, as a result sensor cost should be minimized
- Compact Size. Due to possible versatile installations on vehicles and portable devices authentication system should be limited in size.

- Intuitive end user interface. Due to wide range of possible users authentication system interface should aim at being easy too use with very fast learning curve.
- Fast and reliable access. Access time should be minimized in order to improve end user productivity.

Resources

Below is a list of items that will be required for the implementation for the proposed solution.

- Lab facilities with locker for storing the prototype once completed.
- Computer with internet connection (must have USB port, Window 2000/XP operating system, compiler depending on the programming language used in the software from the development kit)
- FGPA Motorola 68HC12 (or alternative DSP board)
- Embedded LCD Module

Upon consultation with Dr Areibi all other equipment will be requested, if it is determine necessary.

Budget Analysis and Schedule

Budget

A majority of the cost will be the acquisition of the development kit including the correct sensors for the FBAS. Wherever possible all attempts will be made to reduce cost as much as possible. This includes using equipment provided by the engineering department at University of Guelph. The items that will have to be purchased can be found in the list of materials below. These costs will be covered by Engineering Lab Fund and only if necessary external sponsorship.

Items	***Estimated Cost***
Fingerprint Authentication Development Kit	$350.00
Fingerprint Biometric Module	$125.00
Fingerprint Matching Software	$50.00
Emergency Fund	$25.00
Total	**$550.00**

Schedule

The project has been broken into four phases, each focusing on separate element of FAS. We propose to implement this project in four sequential phases listed below, each phase focusing on distinct element of the system.

Phase 1: Component Identification
During this phase it will be imperative to identify and recommend acquiring of the necessary hardware- fingerprint sensor, fingerprint processing hardware and software and all necessary interfaces. This phase is extremely time-sensitive due to being critical section of the project with uncontrollable deadline due to unreliable delivery times for the components.

Phase 2: Hardware Implementation
Once all of the hardware components become available work on implementing authentication system can begin. This phase focuses on getting fingerprint sensor and image processing hardware interfaced and ready for scanning fingerprints. Since focus of this project is to develop and optimize embedded authentication system, additional hardware to support benchmarking and optimization might be added. These devices if necessary will be determined within this phase allotted time.

Phase 3: Software Implementation
Once processing, acquisition and benchmarking systems are set-up and functional software algorithms for fingerprint minutiae image processing, minutiae comparison and storage will be implemented. Implementation of these algorithms will be closely based on available open source code.

Phase 4: System Optimization
During this phase software algorithms will be benchmarked and limiting components will be identified and optimized using custom instruction set with embedded functionality.

We expect that by optimizing some of the limiting components we will be able to greatly speed up overall performance of the system.

As this is a time sensitive project, the figure below will illustrate the time required to achieve the desired results, with consideration for possible delays due to unforeseen circumstances.

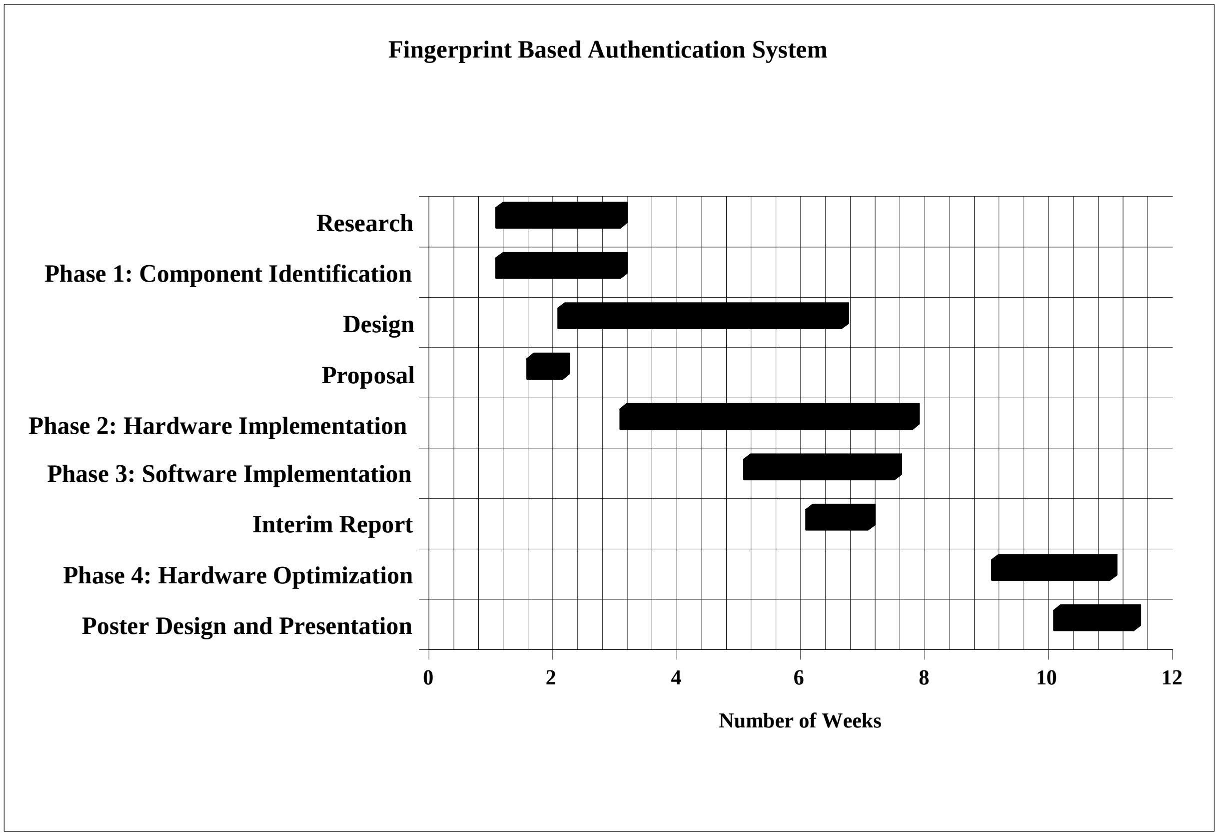

Figure 2: Fingerprint Based Authentication System Project Gantt chart

Deliverables

Sensor Recommendations --September 15, 2005
Proposal --September 19, 2005
Interim Report--- October 21, 2005
Final Design Report and Memo ---December 5, 2005
Poster Presentation ---December 2, 2005

Appendix A

Sensor Justification

As mentioned throughout the proposal, this is a time sensitive project. The date of completion is a firm date, one of which can not be adjusted or postponed by any means. With that in mind decisions regarding the design have to be made in the earlier stages which would not be normally recommended. One of these decisions included the type of sensor to be used. The reason for this early decision is that the sensor needs to be purchased from an outside contractor and the delivery dates are unreliable. This section will give a brief analysis on the different sensors, detailing the advantages and disadvantages of each. Our decision to purchase a particular type of sensor was based on this information.

Atmel FingerChip Module

Advantages
- Readily available through DigiKey
- Includes image processor, pre-processed and already embedded
- Module includes all the hardware and software needed for operation
- Memory Supply SDRAM and DataFlash (allows for direct programming)
- Software development kit allows for database management through high-level functions
- Price: Evaluation/Development Kit $623.72. This includes demo kit board with an integrated biometric module, power supply with adapters for international power outlets, crossed Ethernet cable, serial cable, "Quick Start" guide, CD-ROM comprising all the necessary tools and Documentation

Disadvantages
- Operating system: Linux (kernel 2.4.19)
- Requires the purchase of the Evaluation/Development Kit to develop the user interface of the final application.

AuthenTec

Advantages
- Includes software and verification demo
- Sensor specific image capture
- DSP evaluation board with specific software

Disadvantages
- Have to special order it through Texas Instrument which in turn can not confirm delivery date
- Minimal pre-processing

- Difficult to interface with embedded system as it is meant to be PC based
- Price: Fingerprint Authentication Development Tool $403.59. This includes Daughter Card (expansion board) with AuthenTec AFS8600 sensor, "Fingerprint development support for TI DSPs" software CD, Bioscrypt fingerprint verification demo (GUI for demo on PC) with capture, enroll and verify functions, evaluation version of Bioscrypt's core verification algorithm for C6713 DSP, schematics of sensor board with interface to DSP, hardware and software user guides and Quick Start Guide.

Spectrum Digital

Advantages
- Operating system: Windows© 98, Windows 2000 and Windows XP
- Code Composer Studio which is an efficient optimizing C/C++ compiler assembler, linker, debugger, an a advanced editor with Code Maestro™ technology for faster code creation, data visualization, a profiler and a flexible project manager

Disadvantages
- This is simply just a development platform not specific to fingerprint recognition but has the capabilities to support it
- Price: DSP Starter Kit $553.14 approximately ($395.01 US). This includes C5510 DSP Development Board, C5510 DSK Code Composer Studio™ v2.12 IDE, Power Analyzer and Power Scaling Library, Quick Start Guide, Technical Reference, Customer Support Guide, USB Cable, Universal Power Supply, AC Power Cord(s)

Based on the above information SSS Consulting has selected Atmel as our first choice as it is the only development kit that provides all software and hardware necessary. Due to financial constraints the module can be purchase on its own which includes the sensor and the evaluation board with software as well. This option still works out to be a better decision with the price being roughly $99.95 CAD. While it does operate in a Linux platform, the development kit provides plenty of support for advanced and novice developers.

References

[1] S. Yang and I. M. Verbauwhede, "A secure fingerprint matching technique", in Proc. Wkshp. Biometrics Applications & Methods, Nov. 2003, pp. 89–94.
[2] P.Gupta, S.Ravi, A. Raghunathan, N. Jha, "Efficient Fingerprint-based User Authentication for Embedded Systems", ACM Press, 2005, pp. 244 - 247
[3] "Authentec website, Technology", http://www.authentec.com, September 2005
[4] "Texas Instruments", http://www.ti.com, September 2005