Analysis and Intelligent Design
1428 Elm Street
Soeville, ON
N1L 2H0
(519) 767-0115

January 15, 2007
Project No. 07-01

S. Areibi
School of Engineering
University of Guelph
Guelph, ON,
N1G 2W1

Subject: Fingerprint Based User Authentication

Dear: Dr. Areibi

Enclosed please find a copy of *Analysis and Intelligent Design's* proposal for the embedded fingerprint based user authentication system. We are currently looking at 3 different designs to investigate the issue of supporting efficient fingerprint based user authentication in an embedded system. These range in price from about $125.00 to $765.00. An interim report will be delivered to you on February 16th with more detail on these three design and a recommendation as to the best design to proceed with and a final report on the chosen design will be delivered on April 9th, with a poster presentation on April 5th. We look forward to working with you further on this project.

Sincerely,

Wade Milton

Jay Hilliard

Breanne Stewart

Executive Summary:

This project looks at issues of supporting efficient biometric fingerprint-based user authentication in embedded systems. There are two different forms of fingerprint sensors that can be used; swipe and area sensor. To identify between fingerprints the minutiae are most commonly used. These are the terminations or ridge endings and the bifurcations where ridges fork or diverge. They are thought to be the most discriminating feature of the fingerprint.

We are currently looking at 3 different designs to investigate the issue of supporting efficient fingerprint-based user authentication in an embedded system. The designs we are currently looking at are: to purchase a development kit that provides a complete hardware system which includes the fingerprint sensor interfaced with a DSP microprocessor, examining the feasibility of attempting to interface preexisting hardware which we have access to and implementing freeware fingerprint analysis software, or to examine manufactured data and provide insight into how to develop an embedded fingerprint system with free software to create and analyze fingerprint minutiae data. These range in price from about $125.00 to $765.00.

An interim report will be delivered to you on February 16th with more detail on these three design and a recommendation as to the best design to proceed with and a final report on the chosen design will be delivered on April 9th, with a poster presentation on April 5th.

Background:

The focus of this project is to look at biometric fingerprint-based user authentication in an embedded system. Biometric identification can be used to provide security access based on physiological characteristics such as a fingerprint, voice, iris, or facial features [1]. This type of identification has advantages over the traditional password or swipe card method because the person has to be physically present at the time of identification and it also removes the need for the user to carry a card or remember a password or PIN [1].

The fingerprint is the most widely used biometric trait. To use fingerprint-based user authentication in an embedded system the user will provide a sample of their fingerprint through the use of a fingerprint sensor. There are two basic types of fingerprint sensors; swipe and area sensors. As implied the swipe sensor takes an image of their fingerprint as a finger is swiped past it and the area sensor takes an image as a finger is pressed on the sensor. In both cases the resulting data that represents the fingerprint image is stored in a matrix of pixels to show the characteristics of the fingerprint.

There are two different methods of fingerprint matching; graph-based and minutiae-based. The minutiae-based fingerprint matching is very popular because it is considered to be the most discriminating feature on the finger. It also has a smaller template size than the graph-based matching and processes at a higher speed [2]. For these reasons minutiae-based fingerprint analysis will be used for this project. Minutiae-based fingerprint analysis involves matching the local discontinuities or minutiae of the fingerprint. Discontinuities in a fingerprint include terminations or ridge endings and the bifurcations where ridges fork or diverge [3]. The information for a fingerprint is then stored as a point pattern of minutiae instead of a complete image of a fingerprint [4]. Once a fingerprint has been scanned, it can then be saved for future reference or compared to a previously saved point pattern. The global structure of the minutiae and how they relate to each other is used to determine the uniqueness of a fingerprint [3].

Figures 1 and 2 below [5] provide examples of how minutiae information is extracted from a fingerprint and then how this relates to a matrix that represents the extracted image.

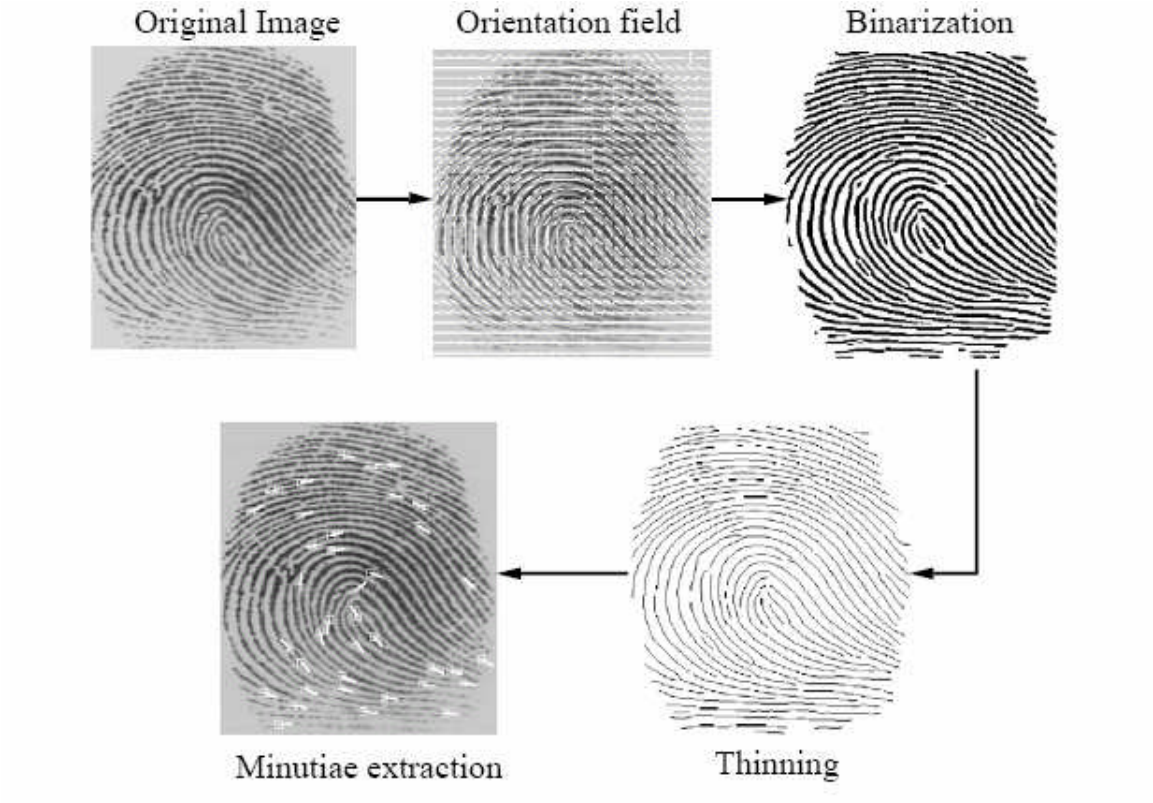


Figure 1. The various stages of minutiae fingerprint extraction

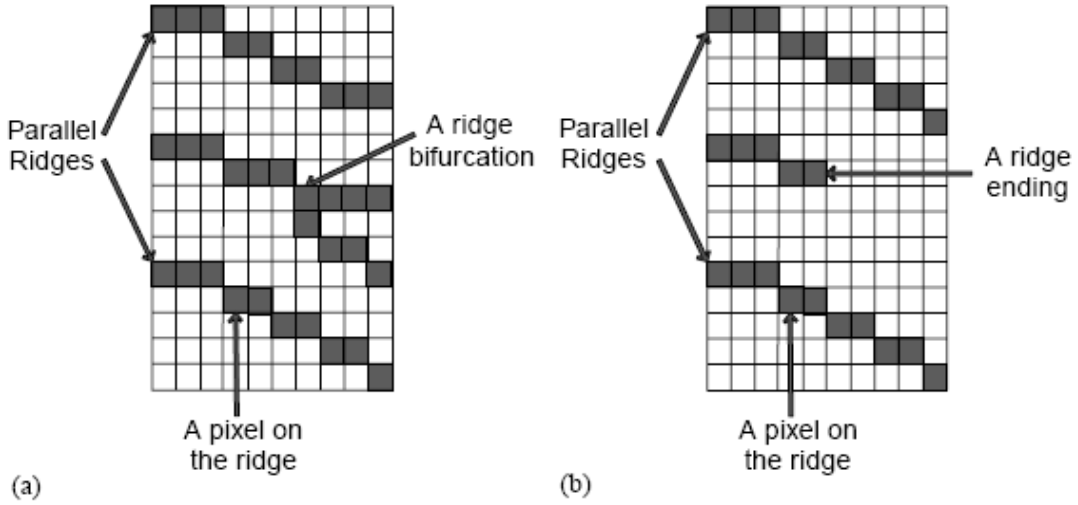


Figure 2. Example of minutiae fingerprint data stored as a matrix of pixels

The basic authentication process using fingerprints is shown in the following flow diagram.

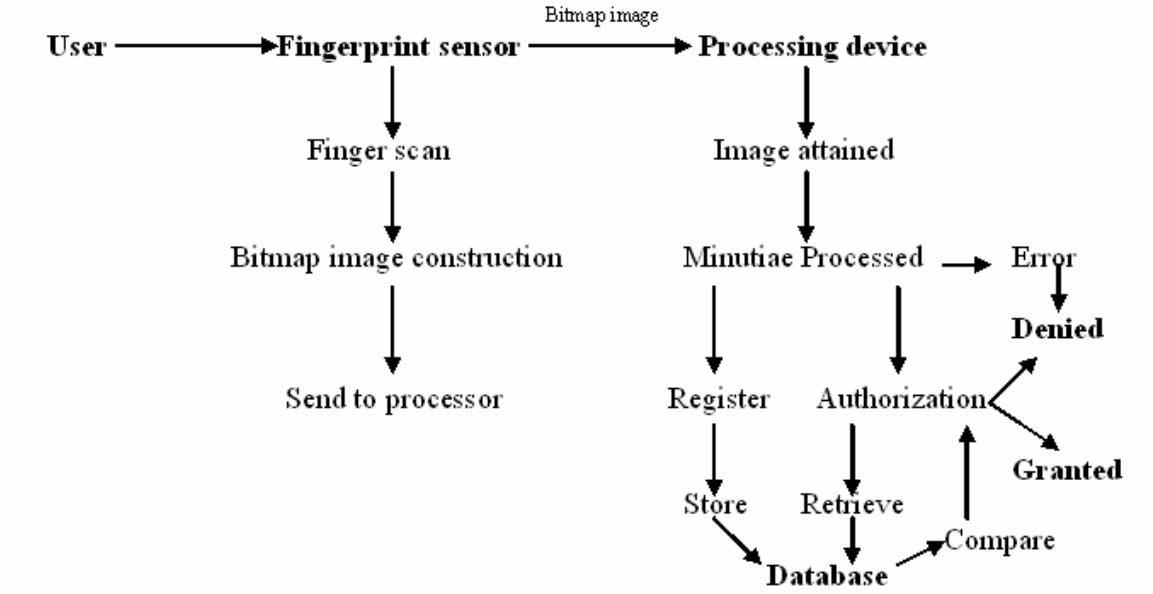


Figure 3. Example of minutiae fingerprint data stored as a matrix of pixels

Constraints:

- The processor must be secure from interference and tampering that could lead to unauthorized entry.
- The sensor should be able to withstand a minimum of 500,000 samples per year.
- The system must have a minimum accuracy of 99.99%.
- The system must not allow unauthorized entry.

Criteria:

- Minimize the cost of design
- Minimize the size for compatibility and mobility
- Maximize the simplicity of the user interface
- Maximize the speed of authentication

Proposed work:

Analysis and Intelligent Design proposes to investigate the issues of supporting efficient fingerprint-based user authentication in embedded systems and to suggest a direction towards developing fingerprint security measures for embedded devices. There are two main issues that relate to an implementation of a fingerprint-based security system. The hardware required to sample, store, and manipulate fingerprint data and software that is used to analyze, create and compare the fingerprint minutiae points.

Analysis and Intelligent Design will investigate and compare three different methods to implement a fingerprint-based security system for embedded systems.

The first method that will be investigated is to purchase a development kit that provides a complete hardware system. This would include the fingerprint sensor interfaced to a DSP microprocessor along with the software routines that capture and analyze the data. The ability to fully achieve this aspect of the project will depend on *Analysis and Intelligent Design*'s ability to obtain funding to cover the high cost of the development kit.

The second method will involve examining the feasibility of attempting to interface preexisting hardware that *Analysis and Intelligent Design* has access to and implementing freeware software which performs the analysis of fingerprint data. This hardware is the Atmel AT77C101B - FingerChip sensor and the Motorola MC68HC11 microcontroller evaluation board. Although this hardware would not be exactly the hardware chosen to implement an actual design, it would provide valuable insight to the issues involved in creating a real implementation. The software that would be used for this method would be based on freeware software that can be used to create and analyze fingerprint minutiae data.

A third possible method to examine the issues involved in supporting efficient fingerprint-based user authentication in embedded systems is to use the knowledge that all fingerprint sensors will essentially provide the same data being a matrix of pixel data. Using this information the software required to analyze and compare fingerprint minutiae data could be examined in a general way using manufactured data and still provide insight into how to develop an embedded fingerprint security system. The software that would be used for this method would be based on freeware software that can be used to create and analyze fingerprint minutiae data.

Requirements:

The items that will be required for this project are:

- Access to Lab 2307 in the engineering building for computer and technical support.
- Computer access.
- Use of the devices or adequate funding for whichever idea is used as described above.

A DSP is a device that is powerful and fast enough to handle a host of different applications. The function of a digital signal processor is to specialize in real-time computations which are critical to the integrity of a system. One specific application which may be highlighted is fingerprint/pattern recognition which makes this development tool an ideal platform for designing a cost-efficient embedded system.

Another key advantage of a DSP is its ability to interface to many different pieces of hardware depending on a user's need. This allows a developer to test several different biometric authorization techniques or several different devices which provide similar data. For example, using several different fingerprint scanners as inputs a developer could determine which product actually provides the most reliable data when working in concert with the DSP.

Other applications which may be useful and feasible with a DSP include voice recognition, wireless communication, and general biometrics.

The team working on this design is made up of 3 engineering students: Wade Milton – Project Manger, Jay Hilliard – Software specialist, and Breanne Stewart – Biometric consultant.

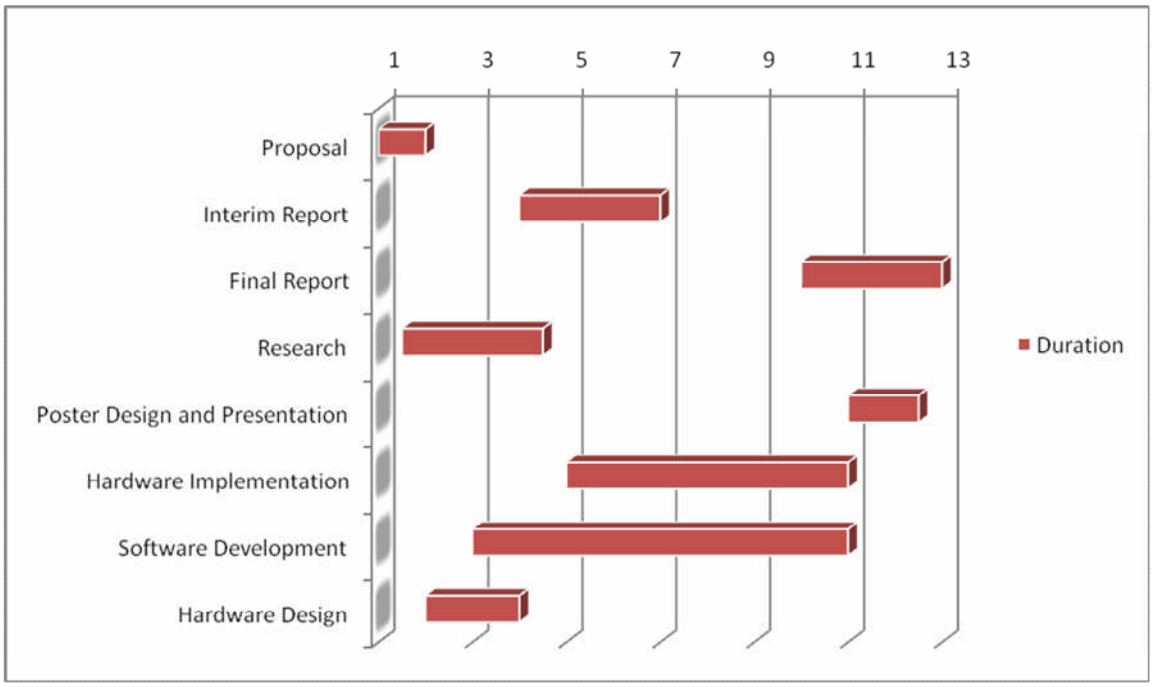
Budget:

To acquire the funding for one of the designs we will be applying to the Engineering Lab Fund for the bulk cost which is taking place on January 31st. The application forms are due one week before the meeting. For any other cost that might not be covered by our lab fund request we will ask for funds from the 41X budget which can be up to $150.00.

Items	Cost
Design 1	
Fingerprint Sensor Interfacing Device	$290.00
DSP Board	$475.00
Total	$765.00
Design 2	
Fingerprint Sensor	$5.00
Microcontroller	$20.00
PCB Fabrication & Assembly	$110.00
Total	$135.00

** All prices are estimated in Canadian funds.

Time schedule:



Deliverables:

Proposal……..January 15, 2007
Interim Report……..February 16, 2007
Final Design Report……..April 9, 2007
Poster Presentation……...April 5, 2007

Reference:

[1] “An Overview of Biometrics”, http://biometrics.cse.msu.edu/info.html. January 2007.

[2] S. Yang and I. M. Verbauwhede, “A secure fingerprint matching technique”, in Proc. Wkshp. Biometrics Applications & Methods, Nov. 2003, pp. 89–94.

[3] M. Aladjem, I. Dimitrov, S. Greenberg and D. Kogan, “Fingerprint Image Enhancement using Filtering Techniques,” Pattern Recognition, 2000. Proceedings. 15th International Conference, Vol. 3, pp. 322-325, 2000.

[4] X. Jiang, and W. Yua, “Fingerprint Minutiae Matching Based on the Local And Global Structures”, 15th International Conference on Pattern Recognition (ICPR'00). Vol.2. 2000. pp. 1038-1401.

[5] S. Prabhakar, A. K. Jain, and S. Pankanti, "Learning Fingerprint Minutiae Location and Type", *Pattern Recognition*, Vol. 36, No. 8, pp. 1847-1857, 2003.