Executive Summary

This proposal investigates possible design alternatives and implementation details of Fingerprint Based Authentication System (FBAS). This design will consist of hardware and software implementations. Optimizing the resulting system will only be considered if time permits

The resulting proposed solution involves the Atmel FingerChip Biometric Sensor as well as the purchase of the Evaluation and Development Kit and use of the Bioscrypt, which is included in the development kit. Simple Systems Solutions Consulting is confident that our design team can successfully achieve the desired results to complete this project.

The deadline for this project is December 5, 2005 on this date Simple Systems Solution Consulting will submit a finalized report indicating the approach taken for the design and implementation of the FBAS along with a working prototype. An in-depth evaluation and analysis of the results will be provided in the final report as well. The total estimated cost allotted to implement the proposed design is approximately $758.00, which will be covered by external funding resources.

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

Table of Contents

List of Figures

List of Tables

Introduction

Problem Statement

The requirements of the embedded system are continuously becoming more demanding, with security being proposed as a new design dimension for embedded systems. The safety of information on such devices is important in today's society where unauthorized access can be detrimental. The primary concern should be the security of these embedded devices with the architecture being developed accordingly. Using an embedded system that requires user authentication can be a solution to ensure the security of information transactions. Biometrics can be used to further increase the protection of the information stored in such electronic devices. The biometric approach is generally superior to conventional method of assumed surrogate identity when a higher level of security is required without typical drawbacks of increased inconvenience to users. In this project we will investigate the potential solutions to support secure and efficient fingerprint-based user authentication on an embedded systems.

Objectives

- To research a possible method of implementation of a fingerprint based authentication mechanism with an embedded computing device
- Ensure that this system satisfies the security issues while maintaining principles of an embedded system

Background

To achieve a more secure verification system we should use something that really characterizes the given person. Biometrics offers automated methods of identity verification on the principle of measurable physiological or behavioral characteristics such as a fingerprint or a voice sample. The characteristics are measurable and unique.

Biometric systems can be used in two different modes. Identity *authentication* occurs when the user claims to be already enrolled in the system (presents an *authentication* ID card or login name); in this case the biometric data obtained from the user is compared to the user's data already stored in the database. *Identification* (also *identification* called *search*) occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all. This project will focus on the authentication mode of the biometric system.

The traditional method of obtaining (or enrolling) fingerprints use ink to get the fingerprint onto a piece of paper. Then this piece of paper is then scanned using a traditional scanner. This method is becoming obsolete. Currently fingerprint sensors are now used to obtain fingerprints. These fingerprint sensors are most commonly based on optical, thermal, silicon or ultrasonic principles. Optical fingerprint sensors are based on reflection changes at the spots where the finger papilla lines touch the reader's surface. Thermal fingerprint sensor's measures the temperature differential between the skin ridges and the air caught in the fingerprint valleys. Silicon technologies are based on the capacitance of the finger, which is the measurement of the capacitance between the skin and the silicon sensor. Ultrasonic fingerprint sensors use ultrasound to monitor the finger surface. The user places the finger on a piece of glass and the ultrasonic sensor moves and reads whole the fingerprint.

Most of the biometric fingerprint systems use the fingerprint sensor to provide the bitmap image only, the processing and matching is done by software that runs on a separate system. Fingerprint manufacturers used to provide processing software with the hardware but that is no longer the case. SSSC will determine which type of fingerprint sensor is better suited for this project along with the associated software and hardware if not provided with the sensor itself. The combination of hardware and software can produce a very efficient fingerprint-based user authentication program on an embedded system.

State of the Art

Essentially, Simple System Solutions Consulting is designing an embedded biometric fingerprint based security system that can efficiently identify authorized personnel. Scope of this system includes fingerprint scanning, fingerprint image enhancement, minutiae identification, minutiae-based fingerprint comparison and secure fingerprint template storage.

There is wide range of security products available from multiple companies that revolve around fingerprint-based user identification. Number of products available from Atmel, AuthenTec, Bioscrypt, Verifi and many others but most of them share component design and software algorithms. The main components of a typical fingerprint-based authentication system can be functionally categorized into enrollment and authentication. Schematic diagram of enrollment and authentication systems is shown in Figure 1 and Figure 2.

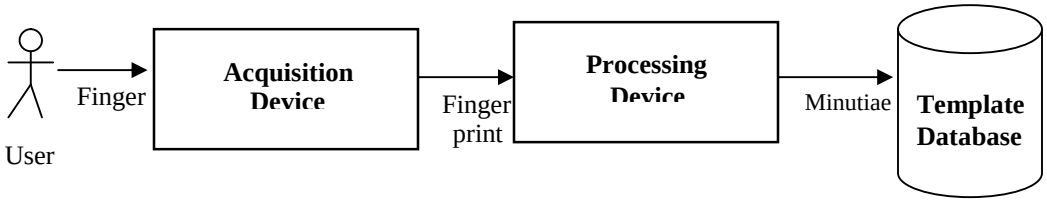

Figure 1: Schematic diagram of user enrollment

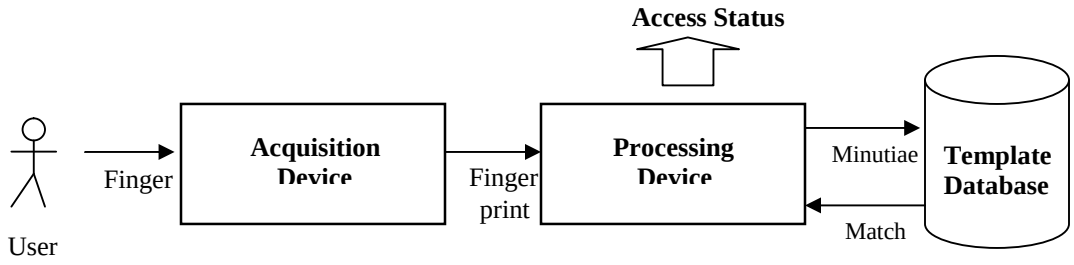

Figure 2: Schematic diagram of user authentication

Majority of commercially available sensors are based on ether optical, thermal, ultrasound or silicon capacitive methods. Optical technology is oldest and least efficient method and currently being replaced by thermal and silicon capacitive sensors. Current implementation of ultrasound sensors is not applicable to embedded devices due to large size and power load requirements. Silicon Capacitive method is based on measurement of the capacitance between the skin and the silicon sensor. Thermal sensors measure the temperature differential between the skin ridges and the air caught in the fingerprint valleys.

Fingerprint image enhancement is required step in order improve minutiae identification. There are number of methods for fingerprint image enhancement. The first one is carried out using local histogram equalization, Wiener filtering, and image binarization. The second method uses a unique anisotropic filter for direct grayscale enhancement.[2]

Fingerprint identification and comparison in most automatic systems are based on minutiae matching. Minutiae characteristics are local discontinuities in the fingerprint pattern, which represent terminations and bifurcations. Alternative method is graph-based. The amount of information needed to be stored and longer processing time for graph-based approach makes it impractical for embedded applications.

Constraints

The proposed design solution must adhere to the following constraints:

- Sensor housing should not be larger than 150x250x50 mm
- System power draw should not be larger than 1A
- Sensor should be capable of operation from –30C to +45C
- System should not generate false positive matches
- System should not generate rejected enrolls

Criteria

The proposed design solution must have the following criterions:

- Efficiency is the most important criteria. One of the main objectives of this project is to increase the efficient of the fingerprint-based authentication on an embedded system.
- Fast and reliable access is another important criterion. As it affect the overall performance of the system.
- Access time should be minimized in order to improve end user productivity cost
- Modularity is an important factor because this design must re-usable to future improvements and upgrades.
- Performance and efficiency should be optimized by the selection of design alternatives
- Intuitive end user interface, minimizing implementation cost
- Time to identify person should be minimized
- System should be modular for ease of upgrade and repair
- Intuitive end user interface
- System should minimize false negatives

Assumptions

- The development kit will be available for the final product given sufficient time to implement
- Power supply will be available on all sites of possible use
- All users will have at least one finger and are physically capable placing it on the sensor

Preliminary Designs Ideas

In this section we will discuss and evaluate different implementations of various parts of the Fingerprint Based Authentication System (FBAS). As shown in Figure 3, FBAS can be separated into few distinct components – fingerprint sensor, processing device, database and various user interfaces. The processing device can be further subdivided into minutiae extraction, matching and storing components – sensor, fingerprint matching algorithm and interface. We will evaluate the implementation of the separate parts of the system by outlining the functionality and evaluating them according to our set of constrains and criteria.

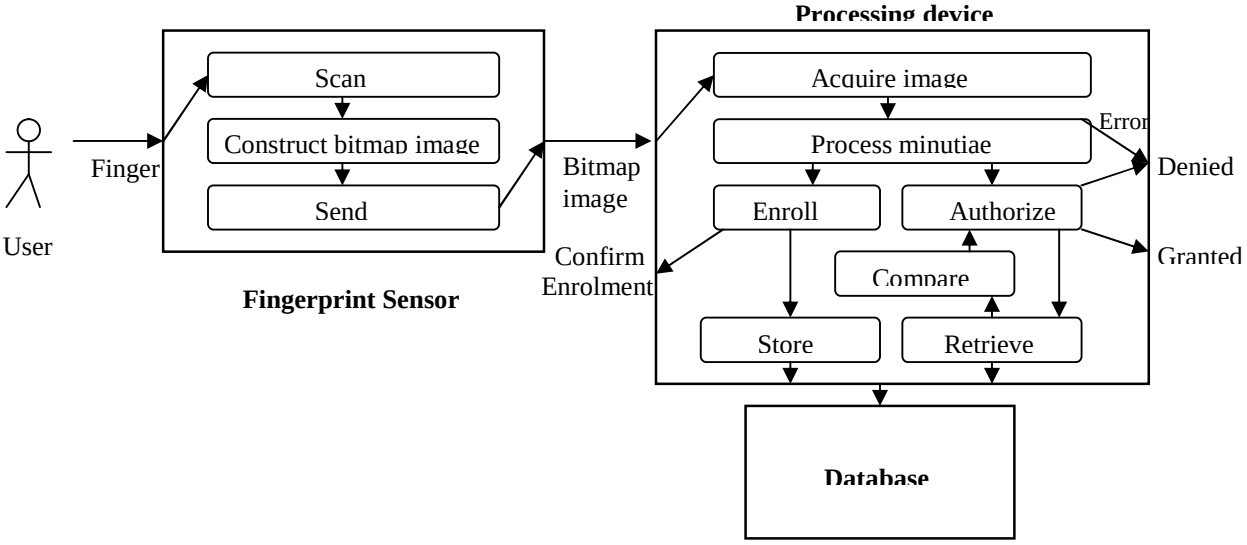

Figure 3: Fingerprint Based User Authentication System

Fingerprint Sensor System

The fingerprints will be acquired as a bitmap image using a biometric sensor. There are few different approaches to scanning fingerprints - optical scanning, surface pressure-sensing and thermal imaging also known as TruePrint technology. Currently thermal imaging is more effective and widespread solution to the problem of scanning fingerprints [3]. All the competitive fingerprint sensors that are currently available use thermal or silicon capacitive methods therefore we will not be considering other types of sensors.

Preliminary Sensor Designs Ideas

Standalone Fingerprint Sensor

There are quite a few standalone sensors available that are capable of producing a bitmap image of a fingerprint. Most of them are designed to work with a server (i.e. PC) connected via USB port. The input biometric signal is captured by the front-end sensor and is sent to the server for processing, matching and storage. Verifi P4000 finger print reader sensor, as shown in *Figure 4*, is one of the better sensors in this category for it uses USB Interface, it is based on Authentec AES 4000 sensor and it has a low cost of $119.00.

Figure 4: Verifi P4000 finger print reader

Advantages of this approach:

- Interface is already implemented
- USB is sufficient to power the sensor
- Easy to interchange components

Disadvantage of this approach:

- Must rely on USB to transfer raw uncompressed data
- Susceptible to identity theft attacks during data transmission
- Image enhancement, fingerprint processing, storage and comparison are not part of the system

Overall this system would have more flexibility, and as a result larger potential for optimization, in implementation of image enhancement, fingerprint processing and storage components of the system. This system is limited in efficiency and security due to the need to transfer large amounts of sensitive data using USB. The use of a USB can be easily breached therefore compromising the data being transferred. Consequently, possible benefits of improved algorithm enhancement will be offset by inefficiency of a data transfer method and additional overhead from drivers. An additional concern is the safety of the biometric information cannot be guaranteed because security might be compromised during data transmission or on the server [1].

Finger print module with embedded microprocessor

An alternative to a *bare-bones* USB sensor is an embedded biometric recognition system that incorporates the signal processing and matching from the server to the embedded device. The biometric signals are processed and matched on the embedded device and only the result is transmitted to the server. Atmel's FingerChip Biometric Module, shown in *Figure 5* is one of the better products in this category. It uses FingerChip fingerprint sensor directly interfaced to ARM9-based microprocessor via 8-bit bus. It comes with all image enhancement, fingerprint processing, comparison and storage as a part of the system. This module cost $130.00 but requires the purchase of an expensive development kit to implement an interface.

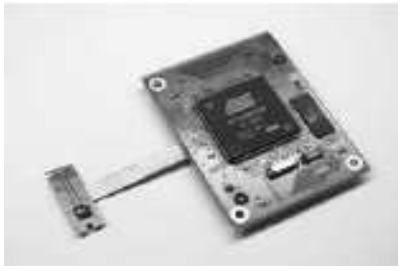

Figure 5: FingerChip Biometric Module AT77SM0101BCB02VKE

Advantages of this approach:

- Embedded standalone system
- All software code is already implemented
- Immune to transmission and server identity theft

Disadvantage of this approach:

- Requires purchase of an evaluation board
- Added difficulty of introducing custom instruction extensions
- Requires encoding or hashing of all fingerprint templates

Overall this approach is a lot more secure and portable. This system can avoid the attacks on communication and server. This system also eliminates the need to transfer and store the biometric data on multiple servers for multiple applications. However, it is very easy to compromise the plaintext storage of the template in the embedded device and it should be encoded [1].

Atmel's Biometric Module includes all necessary hardware and software components and allows immediate functional implementation of the system. ARM9 microprocessor with Linux operating system leaves enough flexibility to evaluate and customize implementation of any of the software components. We recommend this solution as a more secure system with overall better performance.

Alternative evaluation procedures for Sensor Selection

Table 1 is a decision matrix evaluating the possible design solutions for the fingerprint sensor. Each possible design is weighted according to its importance and relevance to the determine project criteria's and constraints. As seen in *Table 1* the most suitable sensor is the sensor with an embedded microprocessor. This type of sensor is provided in the Atmel's FingerChip Biometric Module.

Decision Matrix for Sensor Selection						
Criterion →	**Cost**	**Security**	**Reliability**	**Performance**	**Ease of Implementation**	
Weighting →	**3**	**4**	**3**	**2**	**1**	
Alternatives ↓						**Total**
1. Standalone Sensor	8	5	6	7	9	85
2. Sensor w/ embedded microprocessor	6	9	8	8	7	101

Table 1: Decision Matrix for Sensor Selection

Preliminary Fingerprint Extraction, Enrollment and Matching Algorithms Designs Ideas

There are two types of fingerprint-based authentication techniques - graph-based and minutiae-based. The minutiae based approach is widely believed to be the most discriminating and reliable method of identifying features of a fingerprint. In addition, the amount of information needed to be stored in the template database for fingerprint matching is smaller. The processing time is shorter than that of graph-based algorithms [1].

The algorithm works with the bitmap fingerprint image captured by the sensor, first it normalizes the captured image, determines the image orientation, creates frequency image and region mask [1], filters and binarizes the image and extracts minutiae by examining each pixel and its immediate neighbors [2]. This will identify a fingerprint in such way that it can be stored and compared to other fingerprints in the database.

The minutiae-matching algorithm will compare stored templates against templates in database to determine a match. The 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.

All algorithms are evaluated based on Fingerprint Verification Competition (FVC) [5] evaluation criteria:

1. Number of rejected fingerprints during enrollment
2. Number of rejected fingerprints during genuine matches
3. Average enrollment time
4. Average matching time
5. Maximum template size
6. Maximum amount of memory allocated

In order to evaluate algorithms standardized fingerprint databases and evaluation algorithms used in FVC2004 and available through Handbook of Fingerprint Recognition [7] were used. The tests were executed under Windows XP O.S. on PC AMD Athlon64 (2.01 GHz). The maximum memory that can be allocated by the processes was limited to 4 Mbytes. The enrollment and matching time are platform-dependant and will be significantly less impressive when implemented on embedded system. Still these values can be used for comparison and should scale for final application.

Bioscrypt Algorithm

This algorithm developed by Bioscrypt Inc. and provided with Atmel's FingerChip module. It is also available through Bioscrypt [6] corporate web site for evaluation and licensing.

Number of rejected fingerprints during enrollment – 0%
Number of rejected fingerprints during genuine matches – 0%
Average enrollment time - 0.08 sec
Average matching time - 0.16 sec
Maximum template size - 1.2Kb
Maximum amount of memory allocated - 3044Kb

With perfect values for rejected enrollments and genuine matches, impressive enrollment and matching time and reasonable memory this algorithm is clearly superior product and is our recommendation.

SourceForge's Algorithm

This algorithm developed as an open-source project through SourceForge foundation. It is available through SourceForge [8] website as a source code for free download.

Number of rejected fingerprints during enrollment – 16%
Number of rejected fingerprints during genuine matches – >1%
Average enrollment time - 1.5 sec
Average matching time - 0.2 sec
Maximum template size - 8Kb
Maximum amount of memory allocated – not applicable

This algorithm showed high rejection rate during enrollment due to lack of support to number of image formats. It also has a memory leak that resulted in gradual increase in memory usage.

Alternative evaluation procedures

Table 2 is a decision matrix evaluating the possible design solutions for the software algorithms. Each possible design is weighted according evaluation criteria set out by the Fingerprint Verification Competition. These criterions include 1) The number of rejected fingerprints during enrollment, 2) The number of rejected fingerprints during genuine matches, 3) Average enrollment time, 4) Average matching time, 5) Maximum template size and 6) Maximum amount of memory allocated. As seen in *Table 2* the most suitable is Bioscrypt algorithm.

Decision Matrix for Software Algorithms							
Criterion →	**1.**	**2.**	**3.**	**4.**	**5.**	**6.**	
Weighting →	**5**	**6**	**4**	**3**	**1**	**2**	
Alternatives ↓							**Total**
1. Bioscrypt Algorithm	9	10	8	7	7	8	181
2. SourceForge's Algorithm	4	5	5	6	4	0	92

Table 2: Decision Matrix for Software Algorithms

Methodology

Detailed Design Methodology

The project has been broken into four phases, each focusing on separate and distinct element of FBAS. We propose to implement this project in four sequential phases listed below. The development of this design will follow our Project Development Chart in Appendix A.

Phase 1: Component Identification

During this phase it was imperative to identify and recommend a fingerprint sensor in the early stages of the project. In this case the fingerprint processing hardware and software and all other necessary interfaces can be acquired as soon as possible. This phase was extremely time-sensitive due to being critical section of the project with uncontrollable deadline and unreliable delivery times for the components. This phase has been completed with the selection and actual purchase of the recommended sensor from Atmel. For further information on the sensor selection process refer to the initial proposal in which the recommendations were made in the appendix section. The current proposed solution suggests a specific development kit (Atmel) for the recommended sensor.

Phase 2: Hardware Implementation

Once all of the hardware components become available, the actual implementation of the authentication system can begin. We can then commence to interface the fingerprint sensor with the image-processing device, determine the inefficiencies and determine a course of action. Given there is sufficient time remaining additional hardware might be considered to support benchmarking and additional optimization. However, since the proposed solution requires a development kit to interface the fingerprint sensor with the image-processing device this phase of the project will reschedule for a later date. These changes can be seen in the Project Development Chart in Appendix B.

Phase 3: Software Implementation

This phase was initially schedule to occur once the hardware implementation was already underway. Due to troubles attaining the development kit it has now been decided that software optimization can start immediately and will continue once the kit is attained. When the processing, acquisition and benchmarking systems are set-up and functional the 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. Also in this phase all available source code will be reviewed if applicable combined to further increase software efficiency.

Phase 4: System Optimization

This phase would consist of software algorithms being benchmarked. Within this phase security-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 increase the overall performance of the system. However due to recent setbacks in our project development these will simply be recommended at a later date.

We recognized that this is a time sensitive project and as a result we have re-structured our Project Development Chart to reflect current delays and possible unforeseen circumstances in the future.

Conclusion and Recommendations

It is our belief that using the Atmel FingerChip Sensor is the best option for this project as described earlier in the report. The Atmel FingerChip fingerprint sensor was selected primarily because the system features which consist of the following: image enhancement, fingerprint processing, comparison and storage. This is beneficial, as SSSC will need to design these features from scratch.

For an increase in efficiency software algorithms were also analyzed and narrowed down by the ability to meet or surpass criteria's that were set out by the Fingerprint Verification Competition (FVC) evaluation criteria's. These include the number of rejected fingerprints during enrollment, number of rejected fingerprints during genuine matches, average enrollment time, average matching time, maximum template size and maximum amount of memory allocated. While we recognized that the enrollment and matching time are platform specific the results were as a basis for comparison the actual algorithm performance and we have no doubt that the results will not alter significant to affect the final design performance.

These decisions were a result of an evaluation process that entailed a critique of the proposed solutions attributes against the stated design criteria and constraints for the project. Preceding the evaluation process, an analysis of the most popular available the fingerprint-based authentication systems was completed to further narrow down the choices. That resulted in the two design alternatives being considered for the fingerprint sensor and the software algorithm. As result of our evaluation process we have selected Atmel's FingerChip Biometric Module and Bioscrypt algorithm which is provided in the development and evaluation kit also supplied by Atmel.

SSSC is confident that the selected design option is the most optimal solution for the problem. While we are more than confident this is the best possible solution we are still open to discussion and feedback.

Appendix A: Budget Analysis and Available Funding Resources

The primarily problem Simple System Solutions Consulting (SSSC) has encountered and is continuing to deal with is funding. It was our expectation that we would receive funding from The University of Guelph Undergraduate Engineering Society Equipment Fund. Unfortunately we were unable to secure funding from this source. We have now developed an alternative plans for finding additional resources. However, this has taken more time than expected but SSSC is determined to seek funding for the purchase of the Atmel FingerChip Biometric Evaluation and Development Kit. In this section you will find a budget analysis very similar to the one submitted in the initial proposal and funding that we have secured thus far.

Items	**Estimated Cost**
Fingerprint Authentication Evaluation and Development Kit	$758.00
Fingerprint Biometric Module	$150.00*
Total	**$758.00**

**The Fingerprint Biometric Module has already been purchased and therefore not added in the total. The total only reflects the amount of money required to date.*

Funding Resources	Amount
College of Physical Engineering and Sciences	$158.00
Dr. Shawki Areibi	$100.00
Dr. Ralph Brown	$200.00
Unconfirmed Source	$100.00
Total	**$558.00**
Total Secured Funding	**$458.00**
Total Funding Deficit	**$200.00**

As mentioned above we have explored alternative sources of funding and SSSC believes that we will be able receive enough funding to proceed with the implementation phase of our project.

Appendix B: Project Development Chart

The current Project Development Chart includes amendments made to reflect expected phase completion dates and any possible delays.

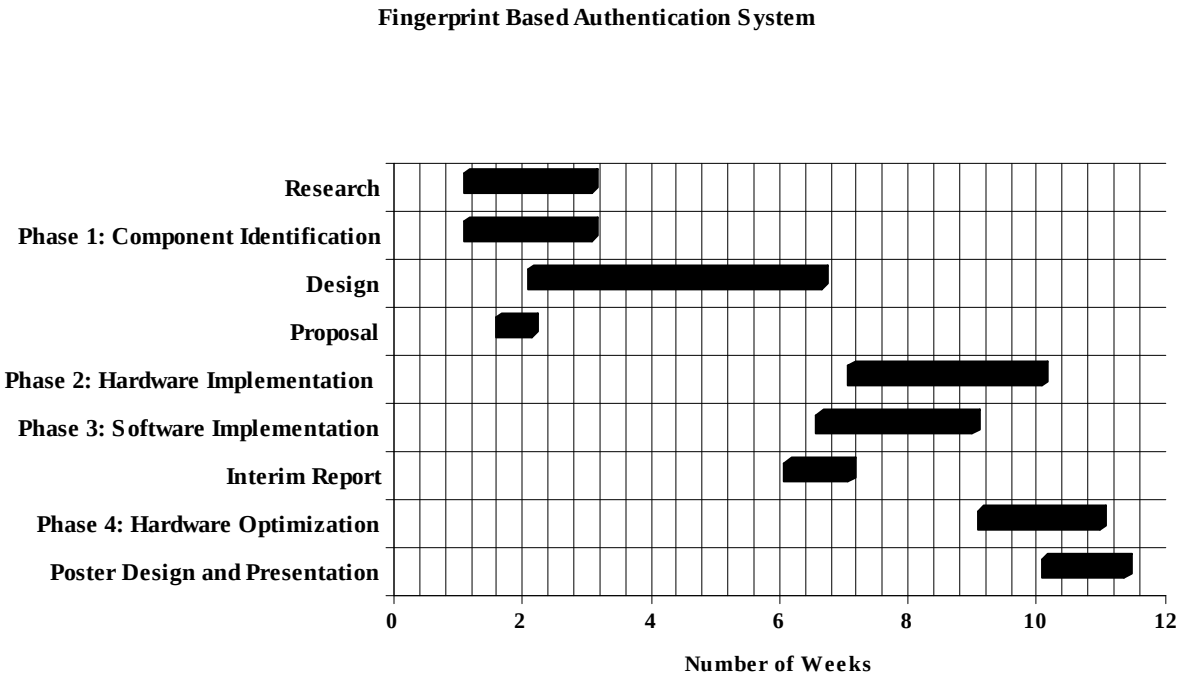

Figure 6: Project Development Chart

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,October 2005

[4] S. Yang, K. Sakiyama, I. M. Verbauwhede, "A Compact and Efficient Fingerprint Verification System for Secure Embedded Devices", http://www.emsec.ee.ucla.edu/pdf/2003asilomar_yang.pdf, October 2005

[5] "FVC2004", http://bias.csr.unibo.it/fvc2004/perfeval.asp, October 2005

[6] "BioscryptCore", http://www.bioscrypt.com/products/bioscrypt_core.shtml, October 2005

[7] "D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York, NY: Springer, 2003.

[8] "FVS website." http://fvs.sourceforge.net, October 2005