Ztitch
Solutions

September 23rd, 2010

Dr. Andrew Rawicz
School of Engineering Science
Simon Fraser University
Burnaby, British Columbia
V5A 1S6

Re: ENSC440 Project Proposal for a Mobile Facial Identification System for Nokia Devices

Dear Dr. Rawicz:

The attached document, *Proposal for a Mobile Facial Identification System for Nokia Devices*, is a run through of our project for ENSC440/ENSC305. The purpose of this project is to implement a security system to provide secured mobile log-in based on facial match of the user. The project, which requires extensive knowledge in image processing and hardware design, will act as a proof-of-concept system (prototype) that can provide Nokia with expertise and insight for any future implementation. Nokia has already agreed to partially sponsor this project by providing us with a single N96 device.

This project proposal will outline the potential of such a system in today's market, the mathematical computations and algorithms required for facial detection and facial matching, the hardware and software tools that we will be using, the challenges faced by this project, a tentative projected budget, and information on project scheduling and team organization.

Ztitch Solutions consists of three motivated fifth-year engineering students: Andrew Au (computer engineering), George Liao (electronics engineering), and Ching-Hsin Chen (computer engineering). Being a past employee of Nokia, I will be leading this team in bringing life to this project. If you have any question or concern about our project proposal, feel free to contact me by phone (778-322-7928) or by e-mail (aau1@sfu.ca).

Sincerely,

Andrew Au

Fifth-year Computer Engineering Student

Enclosure: *Project Proposal for a Mobile Facial Identification System for Nokia Devices*

Ztitch Solutions

Proposal for a

Mobile Facial Identification System for Nokia Devices

Project Team:	Andrew Au George Liao Ching-Hsin Chen
Contact Person:	Andrew Au aau1@sfu.ca
Submitted to:	Dr. Andrew Rawicz – ENSC 440 Michael Sjoerdsma – ENSC 305 School of Engineering Science Simon Fraser University
Issued date:	September 23rd, 2010
Revision:	2.4

Executive Summary

As the number of mobile subscribers continues to rise, so has the number of stolen or missing mobile devices. Since 2002, mobile subscribers already exceed fixed-line subscribers globally. According to Gartner [1], an information technology research and advisory firm, cell phone sales across the world are expected to exceed one billion handsets a year by 2010, making mobile phones the most widespread consumer electronics device above personal computers and televisions. In comparison, the research group Gartner found that 674 million phones were sold in 2004 and 779 million in 2005.

The technological capabilities of cell phones are improving rapidly. More personal data are being stored in a cell phone than ever before. For example, mobile users are constantly using their mobile phones to access their internet banking accounts, and as such, they may have their account numbers and passwords cached in the phone. In countries like Japan, cell phones can be used as a credit card to purchase items by simply swiping the phone over a scanner. Clearly, today's mobile devices offer much more than the ability to make a simple telephone call, but at the same time, there has been no dramatic enhancement in mobile security. A stolen or missing mobile device can lead to dire consequences, including identity theft and unauthorized access into personal accounts.

Currently, there is one common preventative measure in place - a cell phone that has been reported missing or stolen can have its IMEI number blocked by the cellular provider (IMEI is an *International Mobile Equipment Identity* that is unique to each device). When a phone's IMEI has been blocked, the phone can no longer make calls in the network, but in most cases, any personal data stored on the phone is still openly available to the thief. Some phones have a feature which will automatically delete its content once an IMEI has been blocked by the cellular provider; however, this security system can be bypassed by certain ways, such as removing any connection hardware (i.e. the 3G chip) inside the device before the IMEI has been blocked.

Nokia, being the current largest mobile phone maker in the world (followed by Samsung, then LG), is committed to enhancing mobile security by implementing a facial identification security system. The feature will be an active security system that can grant secured mobile log-in quickly and seamlessly compared to other plausible methods such as password log-in or fingerprint identification. The major advantage of this system is the fact that it can be implemented on many Nokia phones that are already sold. The only requirement is that the phone must be running on S60 (the latest Symbian operating system), and that the phone must have the secondary camera. The implementation cost is thus very low – no hardware changes will be needed on currently released models or any future models, as a software update is sufficient.

The system will make use of the phone's secondary camera to recognize the user's face. As opposed to the main camera on the back of the phone, the secondary camera is on the front of the phone, and is often used for making video calls. Ideally, a quick scan to the user's face is sufficient to allow the phone to recognize the user as the phone's authentic user.

If all goes well, the system may be able to see light in the market within a few years. Several Nokia teams around the world have been assigned to this task, and we have been fortunate enough to have the opportunity to extend this exciting project into our ENSC440/ENSC305 capstone project course, which will include research, design, and actual implementation of a prototype system. Such a prototype system can provide Nokia with valuable insight and expertise for their actual implementation.

The project will span a 13-week period with early December of 2009 as the scheduled completion date, and the projected budget is approximately $730 CAD, with most of the cost stemming from the phone itself, but it is expected that Nokia will provide us with the device.

Table of Contents

Executive Summary… ii

1. Introduction … 1

2. System Overview … 2

3. Other Security Solutions … 4

3.1. Log-in using Password… 4

3.2. Fingerprint Identification… 4

3.3. Eye Iris Identification… 4

3.4. GPS Tracking… 5

3.5. IMEI Blocking… 5

4. Proposed Design Solution… 6

5. Concepts of Facial Identification…7

5.1. Eigenface… 7

5.2. Fisherface… 8

5.3. Summary… 8

6. Budget and Funding… 8

6.1. Budget… 8

6.2. Funding… 8

7. Schedule… 9

8. Team Organization…10

9. Conclusion…10

10. Sources and References…11

1. Introduction

Modern mobile devices contain so much personal information that, when stolen, can lead to dreadful consequences such as identify theft and fraudulent entry into personal accounts. In some countries, a cell phone can even be used as a credit card or pre-paid cash card. It seems that the technological capability of the once simple telephone device has become much more than just that. The number of features is still increasing rapidly, which means that more and more personal privacy continues to be at risk. Unfortunately, despite all the technological enhancements of the mobile phone, one capability that has seen no dramatic improvement in the past decade is the device's active security system.

Security approaches can always be broken down into two different types: *active* or *passive*. An *active* approach to security covers all actions designed to prevent a breach of your system's security model. A *passive* approach to security refers to the actions taken to monitor the security of your system based on that security model. Active security systems have never been popular on a mobile device because it defeats the purpose of simplicity. Users do not want to enter a password to log-in to their mobile phone, and companies do not want to implement a fingerprint scanner because it is extremely costly, not to mention that the hardware module is relatively bulky for a cell phone. Therefore, it seems that the best solution is one which can be quick and easy for the user, and cheap to implement for the manufacturer.

Nokia, being the world leader in the mobile phone industry, is committed in finding the solution. One suggested method of active security system for Nokia phones is a facial identification system which grants mobile log-in based on the facial match of the user. This idea is still new, and largely in the research and development stage, but our group has been given the opportunity to incorporate this research and development process as part of our capstone project.

Since most Nokia Smartphones have two cameras – one primary camera on the back for high-quality photo shoots, and a secondary camera on the front for video calls – it is possible to implement this facial identification system without any hardware modifications to the phone. The goal is to develop a software-based computational method of facial matching that can quickly identify the user's face using the secondary camera, then either give or deny log-in rights to the user. Another benefit of this approach is that existing Nokia users can acquire this new security feature by only a software update – they do not need to buy a new device. After all, there are currently more than 80 million Nokia Smartphone users globally.

A number of facial matching algorithms exist. Some algorithms rely on extracting landmarks or features, from an image of the subject's face. By analyzing the relative position, size, and shape of key features on the face, such as the eyes, nose, cheekbones, and jaw, a mathematical matrix calculation can be used to search for other images with matching features. Other algorithms normalize a gallery of face images, compressing the face data to save only the data in the image that is functional for face detection. A probe image is then contrasted with the compressed face data. One early successful system is built on template matching methods applied to a set of prominent facial features, providing a encoded face representation. Existing mathematical algorithms include "eigenface," "fisherface," "eigenfeatures," the "Hidden Markov model," and the "neuronal motivated dynamic link matching."

This document is a proposal to outline our product, by providing an overview of design considerations, a summary of other security solutions, the hardware and software tools that we will be using, the associated mathematical algorithms, project scheduling and budget, and team organization.

2. System Overview

Figure 1 demonstrates the idea in action. The user must first take several images of his or her face at a direct angle, preferably in the same lighting environment, and in the same relative position. These images will be uploaded and stored in the online server's database. Figure 2 displays an example of a face image collection.

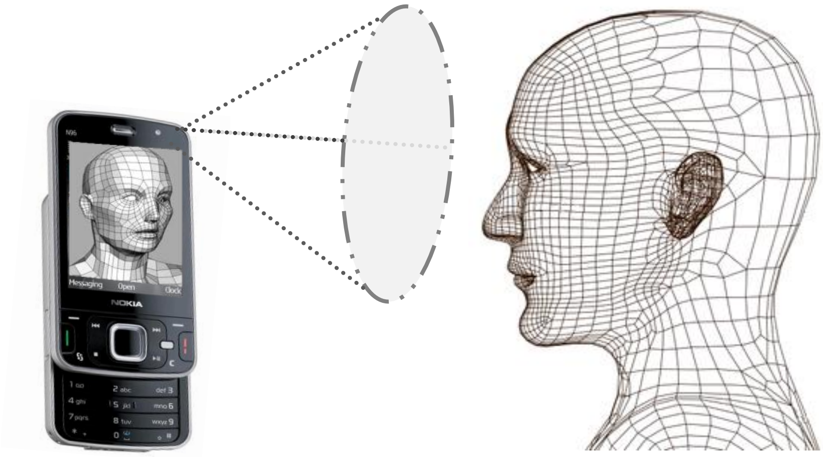

Figure 1. Scanning the user's face with the secondary camera

The challenge is to access and analyze the unique facial features to create a key to identify the user. Every time the user attempts to access secured areas of the phone (such as logging into an HTTPS secure network), authentication will be required. This is done by using the secondary camera (figure 1), on the front of the device, to scan the user's face. The secondary camera is much like a web camera of a computer, and it faces the user while allowing the user to monitor his or her face on the LCD screen. This allows the user to ensure that a complete facial capture is attained. It would be difficult to do this using the primary camera which is on the back of the phone.

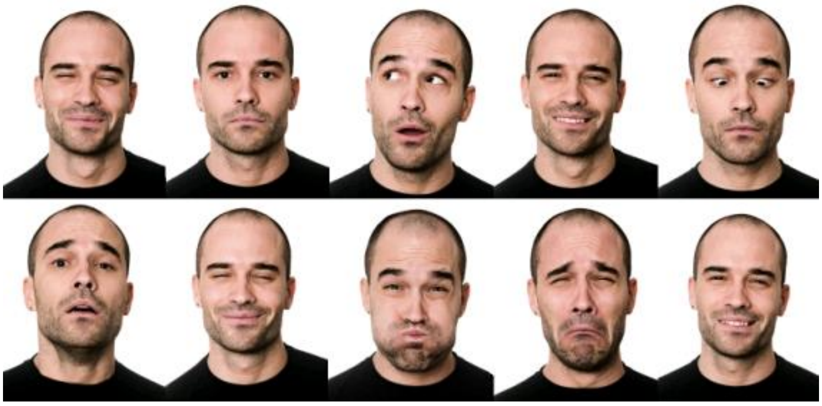

Figure 2. Example collection of face images for processing

Once the system recognizes a face has been captured, it will try to distinguish this face against the one(s) in the database. If successful, the phone's secured area will be unlocked and can become accessed, but if authentication fails, the area will continue to be locked. Two optional security enhancements may be set by the user: (1) email notification is sent to the owner when a log-in fails, along with a picture attachment of the intruder, and (2) log-in password requirement in case the owner has an identical twin sibling. Figure 3 shows the system block diagram.

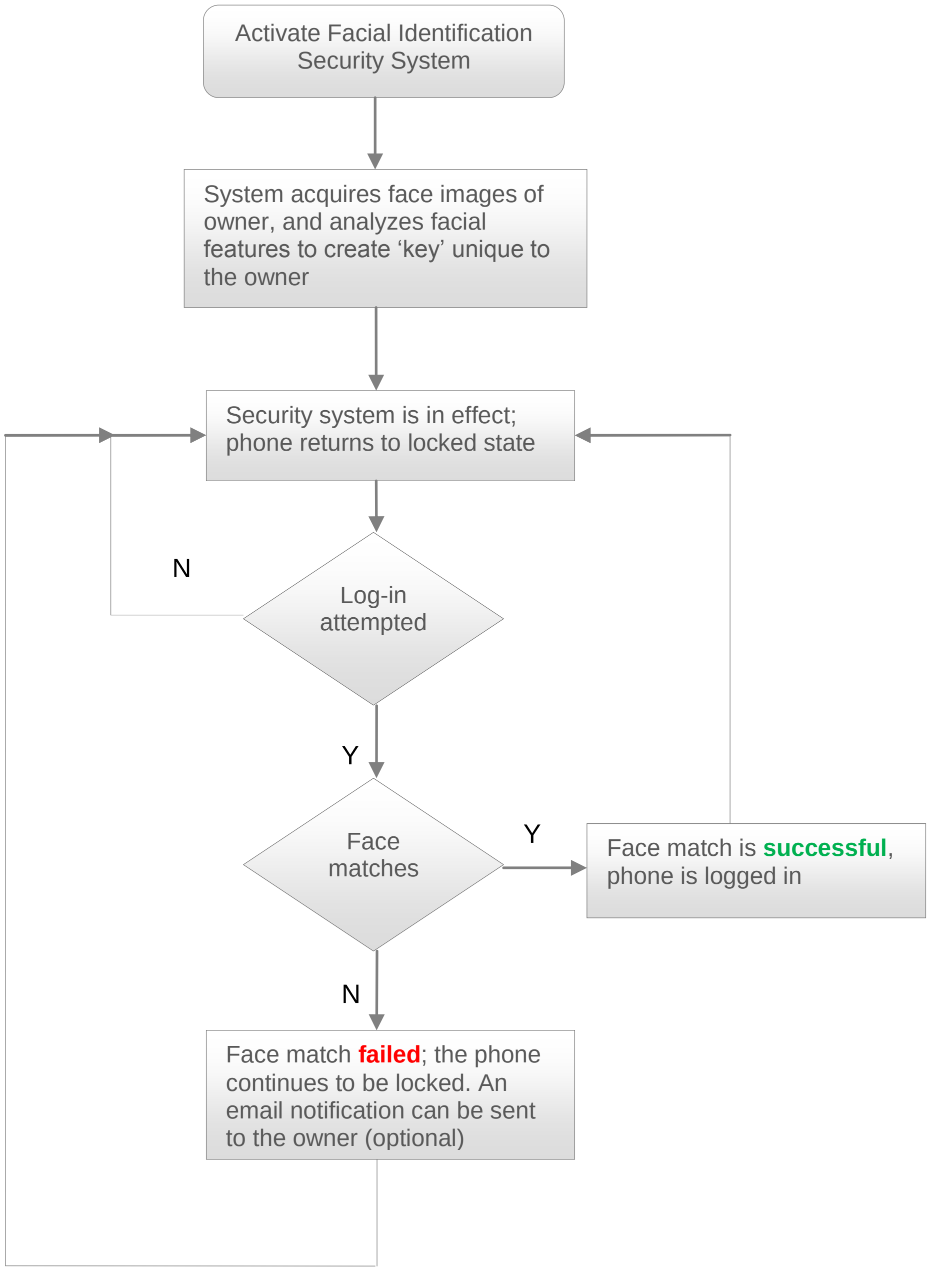
Activate Facial Identification Security System
System acquires face images of owner, and analyzes facial features to create 'key' unique to the owner
Security system is in effect; phone returns to locked state
N
Log-in attempted
Y
Face matches
Y
Face match is successful, phone is logged in
N
Face match failed; the phone continues to be locked. An email notification can be sent to the owner (optional)

Figure 3. System Block Diagram

3. Other Security Solutions

Different methods of security solutions are possible, and some of them have already been attempted. However, none of them prove to be particularly successful in either preventing mobile phone theft, or stealing personal data stored in a cell phone. This section will outline four of these major security systems by describing their advantages and disadvantages.

3.1. Log-in using Password

A password-based login system already exists on most cell phones – it can be enabled as an option. However, most phones have it disabled from the factory, knowing that most users will not want to use it.

Advantages:

- Easy to implement, as the technology has been established for decades
- The least expensive authentication method available

Disadvantages:

- For a mobile phone with numeric keypad, only numerical passwords are supported
- Not impossible to bypass, thieves can automate brute force attacks
- A hassle to use for mobile phones: defeats the purpose of ease and simplicity
- Alternate bypass needed for the forgetful users

3.2. Fingerprint Identification

Fingerprint authentication system is popular among laptop computers, but the innovation has not made it to any cell phone on the market.

Advantages:

- A proven technology in both commercial and law-enforcement uses
- Impossible to reproduce fingerprint, except for genetically identical twins
- Quick and easy to gain access for mobile users

Disadvantages:

- Susceptible to the quality of the skin: dirty or marked is difficult to image properly
- The scanner increases the size, weight, and cost of the mobile device
- The same fingerprint can be difficult to identify after years of certain types of manual labor
- Not unique for about 0.2% of the human population with a genetically identical twin

3.3. Eye Iris Identification

Eye iris authentication is possible, but it requires an iris scanner or a high-quality camera with specific features. So far, this system has only been deployed to facilitate airports, border crossings, and various high-security facilities around the world.

Advantages:

- Extremely secure: even genetically identical twins have different iris textures
- Using John Daughman's IrisCode, the false rate match is better than 10^{-11}

Disadvantages:

- Still a new technology, it is expensive to implement in terms of both hardware and software
- Difficult to perform at large distances; susceptible to poor image quality

3.4. GPS Tracking

At least one mobile phone company, DoCoMo from Japan, has begun to offer GPS tracking of lost or stolen mobile phones.

Advantages:

- Most smart phones already have an integrated GPS, so no additional hardware required
- GPS tracking is a proven to well with law-enforcements in snaring car thieves

Disadvantages:

- The technology has not been proven useful to track lost or stolen mobile devices
- The GPS pointed position can be off by up to 100 feet: useless in tracking small objects
- Thieves can easily disable the GPS tracking by dismounting the GPS chip

3.5. IMEI Blocking

IMEI, short for International Mobile Equipment Identity, is a code unique to each mobile device that exists. When a cell phone has been reported missing or lost, the owner can request to have the IMEI blocked, which will prevent the phone from connecting to any cellular network. In some cases, depending on the phone, data stored on the device can be automatically deleted once an IMEI has been blocked.

Advantages:

- To a certain extent, prevents the misuse of lost or stolen devices
- Serves well as a preventative measure that makes mobile phone theft less attractive

Disadvantages:

- Delayed response time: it takes time for the owner to report a lost or stolen device
- Before the IMEI is blocked, the thieve can use the device freely
- Unable to protect any personal data stored on the device

4. Our Proposed Design Solution

Section 3 analyzed some of the other potential security solutions, but as pointed out, they all have many disadvantages in cell phone application. In this section, we will demonstrate why our proposed solution of facial identification is a worthy candidate, by outlining both the advantages and disadvantages in an unbiased manner.

Advantages:

- No additional hardware required, as most Nokia devices come with an integrated secondary camera
- No hassle, as a quick scan to the face is sufficient
- Can outperform humans in identifying faces, and could uniquely identify some twins
- Extremely good false rate match; more secure than password based login

Disadvantages:

- Battery drainage of an active camera
- Processing speed will depend on the phone's processing capabilities, the data connection speed, and the server's processing speed
- Susceptible to poor image quality and different lighting conditions
- Must be able to distinguish between a real human face and a picture (solution for this will be discussed)

Undoubtedly, there are still a number of disadvantages surrounding the facial authentication system that must be carefully considered. The issue of battery life is an important consideration for many mobile phone customers, and having a camera constantly in its active mode can vastly reduce the battery life. Processing speed is another issue, but our system has its processing done by the server for maximum security. All that is required by the device is to upload a compressed bitstream (under 10 kB) to the server via the phone's data transmission protocol (i.e. 2G/3G/HSPA+), which will relay back a 128-bit key to unlock the phone, or an instruction to lock it.

Susceptibility to image quality and lighting conditions is a foreseeable problem as well [4]. Fortunately, all Nokia phones have a light sensor to detect the amount of light there is in the external environment, and it is synchronized with the camera in a feedback loop to increase the camera's light sensitivity in a dark environment, and reduce its light sensitivity in a bright environment. Therefore, the camera can make adjustments to different lighting conditions. In a completely dark environment with absolutely no light, the camera's LCD screen can automatically increase its brightness to reflect more light to the user's face.

Most critics of the facial authentication system argue that intruders can always use a picture of the owner's face to attempt fraudulent access. One solution is to have the system detect the blinking of an eye as a way to verify that it is a real person, and not a picture. In our prototype system, we will not have this feature given the complexity of motion sensing and our time constraint.

5. Concepts of Facial Identification

There are currently at least five different methods or algorithms available for facial matching: eigenface, fisherface, eigenfeatures, the Hidden Markov model, and the neuronal motivated dynamic link matching. They all have their advantages and disadvantages, but all share the same characteristic which is that they turn the human face into a mathematical space. In this section, we will briefly detail the first two methods listed above; these approaches are more practical for our purpose.

5.1. Eigenface

Eigenfaces are a set of eigenvectors derived from the covariance matrix of the probability distribution of the "high-dimensional vector space of possible human faces" [2]. To generate a set of eigenfaces, a set of digital images of the same human face must be taken under the same or similar conditions (both lighting and position wise). The images are then re-sampled to the same resolution, and the eigenfaces can be extracted using a mathematical tool called PCA (principal component analysis).

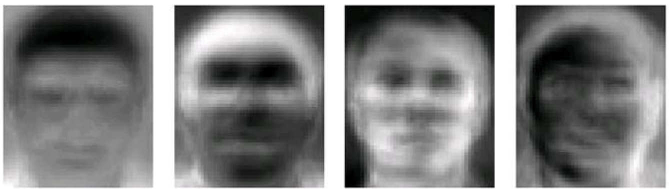

Figure 4. Some eigenfaces from the AT&T Cambridge Laboratories

The steps to implement eigenface are briefly listed below (excruciating details are skipped for this proposal). After eigenface is applied, the face is no longer recorded as a digital photograph, but as a list of values.

1. Prepare a set of images, taken under the same lighting condition, and aligned as best as possible in the same position. By concatenating the rows of pixels, each image is seen as one vector. A grayscale image with *r* rows and *c* columns is represented as a vector with *r* x *c* elements. All images are stored in a single matrix, **T**, where each row of **T** is an image.

2. From matrix **T**, calculate an average image **a**, and subtract it from each original image in **T**.

3. Calculate the eigenvectors and eigenvalues of the covariance matrix **S**. The eigenvectors of **S**
are called eigenfaces. They are the directions in which the images in the set differ from the mean image **a.** The challenge is to efficiently find **S** without actually computing **S** explicitly.

4. Choose the **principal components.** The *D* x *D* covariance matrix will result in *D* eigenvectors, each representing a direction in the image space. Keep the eigenvectors with the largest associated eigenvalue.

5.2. Fisherface

The fisherface method is similar to the eigenface method, but it is more successful and requires more computation, as well as more image sets. Compared with Eigenface, which extracts Most Expressive Features (MEFs), Fisherface is designed to extract features more suitable for classification purpose, so called Most Discriminating Features (MDFs). Therefore, Fisherface method is proved to outperform Eigenface method in most cases. The major advantage of fisherface for the application of cell phone security is that it is much less sensitive to lighting. For this proposal, we will skip the mathematical steps of fisherface.

5.3. Summary

	Fisherface	**Eigenface**
Computational Complexity	Slightly more complex	Simple
Effectiveness Across Pose	Good, even with limited data	Good, with enough data
Sensitivity to Lighting	Less	More

Table 1. Comparing eigenface to fisherface [3]

Even though fisherface yields better result, we cannot decide which method to use yet. We have very limited time to complete this project, and we do not want to get bogged down by the more complex fisherface method.

6. Budget and Funding

Table 2 outlines a tentative budget for the Facial Identification Security System.

Item	**Cost (CAD, includes tax)**
Nokia N96 smart phone	$600
Active SIM card plus subscription	$-
Various electronic components	$100
Nokia Tools and SDKs	$0
Cases, stands, and miscellaneous accessories	$30
Total Cost	**$730**

Table 2. Tentative budget

- The Nokia N96 is pricey, but comes with a 640x480 pixel camera. The less expensive alternative is the Nokia N95 which comes with only a 320x240 pixel camera. For development and testing, the higher pixel camera is the better option.
- An active SIM card must be available for testing.
- We wish to modify the device to be compatible with special connections, and achieve automation of the phone.
- Nokia tools and SDK's (Software Development Kits), including licensed Microsoft Visual Studio 2010, will be free to use.

The phone will be provided solely by Nokia as agreed upon.

7. Schedule

Figure 5 shows the Gantt chart of our tentative project schedule. As can be seen, most time will be spent on research, and also on development. Development, integration, and testing will overlap each other. We will be beginning this project before the semester has begun to give us a head start. Due dates of submissions can be found in table 3.

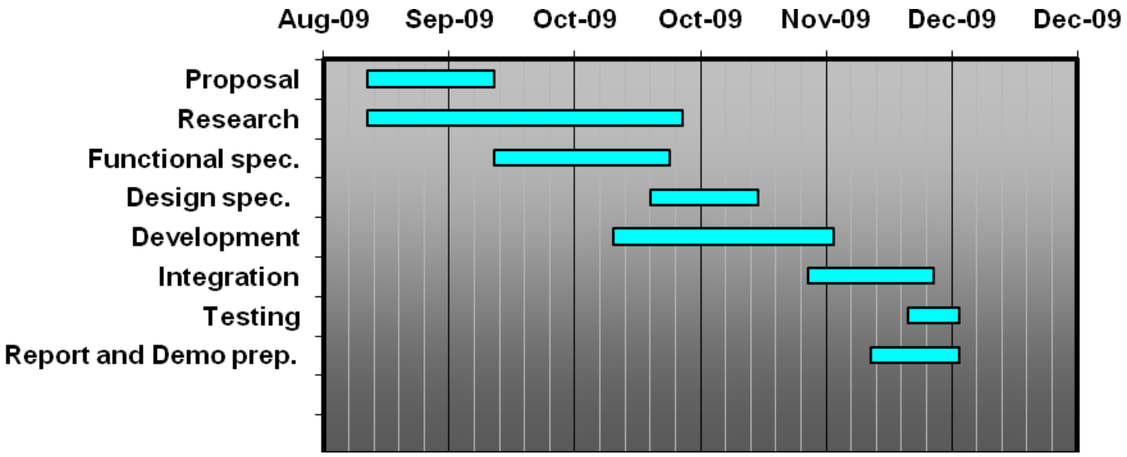

Figure 5. Tentative project schedule.

Sept 23	Project Proposal
Early Oct	Oral Progress Reports
Oct 14	Functional Specification
Nov 14	Design Specification
Nov 18	Written Progress Report
Mid Dec	Group Presentation/Demo
Mid Dec	Lab Journal/Project File
Mid Dec	Post-Mortem

Table 3. Important due dates for ENSC305

8. Team Organization

This team consists of three highly motivated engineering students: Andrew Au, George Liao, and Ching-Hsin Chen. All members are 5th year undergraduate engineering students, with diverse abilities from past taken courses and co-op experiences. Each member will contribute to the research of the project, but development and integration roles will be divided as equally as possible. Being past employees of Nokia, Andrew and Ching-Hsin are experienced in developing both software and simple hardware components for mobile devices.

Being an undergraduate research assistant for Professor Jie Liang as part of the NSERC program, and having taken ENSC424 multimedia communications engineering, Andrew is quite familiar with image and video processing. Programming and scripting in Nokia's QT language is also part of Andrew's diverse skills coming from the workplace that can contribute to the project. Andrew was responsible for sketching and putting together the concept of this project, and will lead the team in developing the mathematical algorithms to be used for facial matching.

George and Ching-Hsin will be responsible for assisting in the development of the facial matching algorithm, the GUI, and modifying the device (Nokia N96) to meet special requirements. For example, special connections will be needed in order to be able to establish a communication gateway between the device and an external computer. Also, after working at Broadcom and being well equipped with both software and hardware qualification, Ching-Hsin will be responsible for integrating the team's work together.

9. Conclusion

Mobile device security has become increasingly important as the capabilities of the personal device have reached new heights. Personal data stored on phones has become such a big risk that consumers can no longer ignore it. As such, there is a huge market potential for the facial identification security system.

If everything goes according to plan at Nokia, the system may be able to surface in the market within a four to five year timeframe. However, for this course, the major challenge of this project is developing the facial matching techniques and integrating them into the phone to successfully produce a prototype system. The end result is gaining valuable expertise and insight for the team at Nokia Canada in developing an actual system that can protect consumer privacy, and help raise the Nokia brand image among a tough, competing market. The purpose of this document is to serve as a proposal only, outlining some of the major components of the project. More detailed explanations can be found in future documents.

10. Reference

[1] Gartner Press Release. 2005. Gartner Says Mobile Phone Sales Will Exceed One Billion in 2009. http://www.gartner.com/press_releases/asset_132473_11.html [Accessed: September 10, 2010]

[2] SourceForge. 2003. Eigenface-based facial recognition. http://openbio.sourceforge.net/resources/eigenfaces/eigenfaces-html/facesOptions.html [Accessed: September 11, 2010]

[3] Daily Burito. 2004. Face Recognition: Eigenface and Fisherface Performance Across Pose. http://dailyburrito.com/projects/facerecog/FaceRecReport.html#refs [Accessed: September 14, 2010]

[4] Top Bits Technology Community. 2010. Facial Recognition System. http://en.wikipedia.org/wiki/Facial_recognition_system [Accessed: September 15, 2010]

[5] Department of Computer Science, Colombia University. 1997. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection: http://www1.cs.columbia.edu/~belhumeur/journal/fisherface-pami97.pdf [Accessed: September 20, 2010]