Development of a Low Cost Biometric Hand Vein Scanner

Using near infrared imaging

Presented By
Jason Forté

Prepared for:
Dr A. van der Byl
Dept. of Electrical and Electronics Engineering

November 2014

This project report is submitted in partial fulfilment of the requirements for the degree of Bachelor of Science in Mechatronics

(Keywords: Biometrics, Image Processing, Infrared)

Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the IEEE convention for citation and referencing. Each contribution to, and quotation in, this report from the work(s) of other people has been attributed, and has been cited and referenced.
3. This report is my own work.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as their own work or part thereof.

Signature: (J. C. Forté)

Date:

Acknowledgements

To

Abstract

- Open the **Project Report Template.tex** file and carefully follow the comments (starting with %).
- Process the file with **pdflatex**, using other processors may need you to change some features such as graphics types.
- Note the files included in the **Project Report Template.tex** (with the .tex extension excluded). You can open these files separately and modify their contents or create new ones.
- Contact the latex manual for more features in your document such as equations, subfigures, footnotes, subscripts & superscripts, special characters etc.
- I recommend using the **kile** latex IDE, as it is simple to use.

Table of Contents

Glossary

AHE Adaptive Histogram Enhancement. 23

API Application Programming Interface. 26

Biometric Template Biometric information that is usually stored and compared to biometric queries during a biometric recognition operation. 5

CBEFF Common Biometric Exchange File Format. 26

CLAHE Contrast Limited Adaptive Histogram Enhancement. 23

DET Detection Error Trade-off. 17

EER Equal Error Rate. 17

FAR False Accept Rate. 16, 17

FMR False Match Rate. 16, 17

FNMR False Non-Match Rate. 16, 17

FRR False Reject Rate. 16

FTA Failure to Acquire Rate. 16

IEC International Electro-technical Commission. 5

IR Infra-red. 32, 37

ISO Internation Organisation for Standardisation. 5

NFC Near Field Communication. 9

PET Privacy Enhancing Technologies. 6, 7

ROC Receiver Operation Characteristic. 17

ROI Region of Interest. viii, 14, 20–22, 24

SIFT Scale Invariant Feature Transform. 14

Soft Biometrics The use of non discriminatory features to aid in reducing the search space during a biometric identification process. 5

Three factor security system The method of identifying a subject based on something they know something they possess and something they are. 4, 8, 9

TV Total Variation. 25

UML Unified Modelling Language. vi, 42

UX User Experience. 30

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background to the study

A very brief background to your area of research. Start off with a general introduction to the area and then narrow it down to your focus area. Used to set the scene.

1.2 Objectives of this study

1.2.1 Problems to be investigated

Description of the main questions to be investigated in this study.

1.2.2 Purpose of the study

Give the significance of investigating these problems. It must be obvious why you are doing this study and why it is relevant.

1.3 Scope and Limitations

Scope indicates to the reader what has and has not been included in the study. Limitations tell the reader what factors influenced the study such as sample size, time etc. It is not a section for excuses as to why your project may or may not have worked.

1.4 Plan of development

Here you tell the reader how your report has been organised and what is included in each chapter.

I recommend that you write this section last. You can then tailor it to your report.

Chapter 2

Literature Review

In order to get an understanding of the concepts and best practises involved in the field of biometric, it is important to review currently available literature on the topic. This section of the project is aimed at building up a good understanding of the state-of-the-art with regards to biometrics and more specifically the biometrics for hand vein verification. Some aspects addressed in this section include the biometric ecosystem; acquisition and processing techniques; acceptability of biometric systems and typical biometric system architectures. While there is a tendency towards the technical aspects, slight consideration of the social, environmental and ethical issues in relation to biometrics have been included in the review. The technical measures to be taken with regard to using personal information will also be considered in this section.

2.1 Biometrics as an Identification Technique

Over the past few decades there has been a gradual shift into the virtual domain. As more people go online, there becomes a greater incentive for companies to integrate their conventional systems with those of the web. Internet banking and e-commerce services are becoming prolific throughout the digital world. However this reallocation of processes into the digital space comes at a cost. Keeping track of a large online user-base is becoming harder. By allowing remote access to a system (via the internet protocols), the inherent risk of malicious activity is increased. It is therefore, sometimes vitally, important to verify the identity of any person who wished to access a system or service. A subtle difference exists between biometric verification and biometric identification which has large implications on the architecture of the biometric system. This difference will be clarified later in the chapter.

It is natural to suggest that better methods be investigated to reliably identify users. The most simple of access control systems is the key-value system (namely username plus password value to allowed access). But the rise in high speed computation means that systems such as these are easily hacked by brute force attacks. A suitable alternative would be to identify people based on physiological characteristics that are harder for the layman to extract, measurable and most importantly non-varying characteristics.

Systems such as the key-value paradigm are a considered to be a subset of a greater class of systems called Three factor security systems. Three factor security makes use of a combination of: something a subject knows, something a subject possesses and something a subject is. In commercial applications two out of three is usually considered adequate [1].

2.1.1 Selecting Useful Biometrics

It is because of the need to correctly identify people that biometrics exists as a field of study. Conversations on the topic will often lead with the most ubiquitous of biometrics - fingerprints. The availability and uniqueness of an individuals finger print makes it a useful biometric characteristic. However, because of the legacy of fingerprints, there are a number of methods that have been found to fool fingerprint systems that don't have built in vitality detection[2].

So because of this, the fingerprint has started to lose it's lustre as a viable security option. It is suspected that DNA analysis would provide the greatest strength in terms of biometric security. But the time taken to develop a DNA analysis means that it too would not be suitable as part of a regularly used biometric security system. Indeed, the choice of which biometric characteristic to use is also dependent on the situation. A fingerprint capture system may be viable for the front door of an office block where the flow of users is small but in a system with a high flow of users - such as a subway station - the fingerprint scanner may be damaged or become a hygienic concern.

The randomness inherent in the human evolutionary system allows for random fluctuations in DNA. This means that on a most fundamental scale every person is unique and therefore in order for uniqueness to arise there must exist a means of categorically identifying every individual (whether we know of that means or not). Without going too far into biology or philosophy the essence is that uniqueness must arise within the physiology - and indeed it does - of an individual.

Of the most unique physiological traits, DNA is the most discriminatory feature available. The crown prosecution service which is in charge of DNA matching guidelines in the UK gives the DNA-17 test a match probability of 1 in 1 billion between two subjects - this also takes into account the effect of laboratory error[3]. Although the precision of DNA tests is high it is fairly cumbersome as a biometric characteristic because of the cost, effort and time required to process the sample.

Biometric Feature Traits

In order that a biometric feature be deemed appropriate for use in a biometric recognition system; it is necessary that the traits of a good biometric be defined[4]:

- Universality: The feature must be available in all subject.

- Distinctiveness: The feature must be suitably discriminatory to be able to successfully identify any two subjects as being different.
- Invariance: The feature must not degrade over time. In cases where the feature does degrade slowly, a suitable re-enrolment procedure should be designed.
- Collectibility: The feature must be able to be collected relatively easily. This trait may extend to encompass social considerations such as when using face detection in a region where religion dictates the wearing of a headdress.
- Performance: The system must perform well in terms of accuracy and speed. Biometrics for use in unlocking a mobile device may gradually destroy the appeal of a product if there is a delay in the performance.
- Acceptability: This trait is to do with the ability for a population to adopt the biometric system. Users may need to be taught about how biometric recognition works and the stigmas within the area need to be addressed
- Circumvention: Any trait that is considered for a biometric security system must be hard to circumvent. This is not necessarily only to to with the trait. For instance if a biometric validation sub-system produces a one-number output to represent the match of a comparison then optimisation techniques can be applied the sub-system to reverse engineer the algorithm and hence break the system.

Soft Biometrics

Although there is little prospect for identifying a subject based on such things as skin tone, markings or tattoos. These features do have uses in the field of Soft Biometrics. Soft biometrics aims to reduce the search space of biometric templates by bagging templates of subjects with similar soft biometric features. This is usually helpful when there is a 1:N relationship between the biometric query and the Biometric Templates. For instance the skin color of an individual such as African or Caucasian could be used to narrow the search space to only consider one group.

2.1.2 Biometric System Acceptance

The Internation Organisation for Standardisation (ISO) have compiled guidelines on the requirements for an acceptable biometric system. The International Electro-technical Commission (IEC) and ISO standards are in place to guide the field to standards that are to this point still materialising. The official criteria in order to be considered is that the standard is accepted by 75% of the registered members of the organisations. The ISO 24714 standard deals with the treatment, vocabulary and acceptability of biometrics and biometric systems. The ISO 24712-1 deals with jurisdictional and societal considerations in the biometric landscape. Some of the factors which impact acceptability of a biometric system are outlined in the standard[1]:

- Privacy and Data Protection

It is important that the privacy of the subjects' data is stored in a means that is secure. Certain requirements such as minimising the time that a biometric capture device stores the raw input measurement and the means of encoding the data is all usually stated in the ISO standards.

Because the choice of biometric characteristics is based on it's ability to remain constant over a subjects lifetime, biometric features are considered as part of Privacy Enhancing Technologies (PET). PET features are required to maintain a comprehensive and correct privacy regime. (Details of the social issues are covered more extensively in 2.1.3)

- Convenience It has been deemed necessary that for maximum acceptability any biometric system being developed for public use needs to offer the greatest tangible benefit for the subjects. This usually comes with any system that reduces physical and mental workload on subjects according to the standard.

- Reliability and Performance The biometric recognition system needs to offer reliability and performance to avoid mismatches that could deplete the security of the access point. Sluggish performance may cause slower adoption of the system.

- Consumer-friendly and Legal Considerations It is obvious that a biometric system be able to perform recognition tasks in a means that is legal within the jurisdiction it operates. It may also be that in legal terms a biometric characteristic submitted alone to a system is not evidence for use and it might be that the three factor strategy be supported (See Section 2.1 on three factor security). The scepticism of a system may be countered by suitable demonstrations of system accuracy.

- Invasiveness Invasiveness relates to the ease with which the biometric is accessible. For instance gait recognition which measures a persons stride technique is minimally invasive because it can be implemented with cameras. Iris recognition could be deemed more invasive because the of the subjects' close-up engagement with capture device. This may also detract from the system if the subjects using the system are not familiar with the concept of biometric identification.

- Health and Hygiene Of course health and hygiene become issues when there is a mass flow of users. The factors in this regard would help decide on cleaning schedules for the device. A system may be deemed discriminatory if the demographic of users is not adequately considered. A person with compulsive-obsessive conditions may not be comfortable using a hand palm detector. Also in the context of hospitals it may be necessary to consider disease or contamination issues.

It is conveyed in the above list that there is much complexity in designing and implementing a biometric system furthermore there are ethical, social and religious issues that require consideration before developing a biometric system. Some of these aspects are discussed in the next section.

2.1.3 Privacy and Social Considerations for Biometric Recognition Systems

Privacy and Ethics forms for the Project

As with implementing any new system into an environment where it will be used by humans; there needs to be considerable effort int trying to avoid discrimination of potential users. Along with that there needs to be extreme care put towards the way in which the information is handled.

Section 2.1.2 refers to biometric features as a PET. Which means that any breach of a system could be considered a breach of privacy and therefore implicate the designers in legally enforced privacy lawsuits. The ISO standard[1] outlines the generally accepted rules with regard to ensuring the integrity of the public information in PETs:

- Use no personal data or as little as possible
- Use encryption if using personal data
- Destroy raw data as soon as possible
- Anonymize personal data wherever possible
- Do not use central databases where not required
- Give subjects control over there personal information
- Use a means of certification and evaluation to verify that the application delivers a guarantee of an appropriate level of trust

The International Covenant on Civil and Political Rights states[5]

> Article 17
>
> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

It is therefore imperative that privacy be considered whole heartedly with regard to any biometric system. in terms of the University of Cape Town policy on the use of human test subjects the required ethics forms have been submitted to the required authorities. The purpose of the forms is to give outlines as to how the integrity of any test subjects data will be kept. The process of collecting personal information requires certain requirements such as opt-in only fields, the ability of the subject to deny access to the data at a later stage and the assurance that private data will not be used for an intent not expressly consented to by the individual.

Social and Religious Issues

As mentioned in a few of the above sections, there needs to be consideration of the users foremost when designing a biometric system. Designing a system that is at a height no reachable by someone in a wheelchair is considered unacceptable. There are nuances within this section of biometrics that are often overlooked. Thoughts must be contributed towards such situations as[1]:

- Individuals with conditions that prevent the accurate use of the system. Examples include a person with missing fingers trying to access a fingerprint based biometric system.
- Religious reasons such as religious attire can affect the adoption of biometric systems. Also cultures that have a personal space mentality may not react well to a biometric system involving touching the capture device.
- Regional situations where a Latin based signature system is used against users who's language is not complimentary with Latin are also interesting.
- Reputation of an individual could be degraded if a the individual is rejected by a biometric system where there is no foul play. This could cause emotional stress on the users which could deter other future users.

As there are many aspects to consider in a biometric system it is up to the system designers to decide on the suitable demographic of users and then implement suitable alternatives where necessary to avoid discrimination.

This concludes this section on the introductory issues of biometrics. It was seen that there is merit in pursuing the development of a hand vein biometric system because of the accuracy in the comparisons. Research into the ISO standards has also illuminated some issues to take forward in the next chapter. The next section will begin to delve more deeply into the technical aspects of biometric identification and authentication.

2.2 Identification, Verification and Biometric Modalities

When it comes to biometric systems it is important to make the distinction between two main areas in the field - these are identification and verification[4]. The two system definitions mainly differ in the way that the biometric is processed but can also have implications for such things as the degree of accuracy required during acquisition and the speed at which the user experiences the recognition procedure. There are also system architecture issues for each use.

2.2.1 Biometric Identification

Biometric identification is a method by which a user is identified based solely by a biometric feature. This goes against the Three factor security system method discussed in Section 2.1.

The main use for identification systems is when there is a 1:N recognition problem to be solved. Biometric identification is mainly used in the criminal investigation sector where biometric features such as fingerprints need to be compared to an entire database of biometric templates. It is because of the number of searches that need to be carried that biometric identification becomes computationally intensive. It is important in these contexts to make use of optimisation techniques such as soft biometrics (Section 2.1.1) to decrease the search space of the template database[4].

Included in the search problem is the fact that for biometric identification, the database of templates can be very large. This can often void the idea of an entirely localised system. Network connections to a database will therefore increase the cost and security implications of such a system.

Other applications of this type of recognition are: border control points, drivers licenses and ID documents.

2.2.2 Biometric Verification

Biometric verification requires fewer technological resources compared to identification. Although the biometric capture process is usually the same, verification usually involves a user submitting additional information to the system as well. This extra information is usually something that the user possesses or something the user knows (See Section 2.1 on Three factor security system)). In either case the biometric feature is compared with a template related to the external information. This means that the comparison is usually 1:1 where the system either gets a comparison match to verify the user or a miss-match to lock the system.

The extra information can be in the form of something such as an access card or Near Field Communication (NFC) device[4]. Items of knowledge could be things like an email address, telephone number, ID number or a number sent to the user int the process of prime factorisation encryption[6].

Some common uses for a system such as this would be: ATMs, E-Commerce and user access control on mobiles.

Although the computational intensity of verification is less than that of identification, the use of a centralised database to store the biometric templates will always raise security concerns. If access cards are used then the biometric template can be stored in the card and in some cases information from the card or token can be combined with the captured feature to produce a more secure system.

While there is merit in improving either field the focus of this report will be geared more towards a verification system. This negates the need for implementation of network resources and allows more focus on the biometric capture sub system and the preprocessing aspects.

2.2.3 Biometric System Modalities

There are a number of biometric modalities established within the field each with it's own pros and cons[4]. A brief introduction to some of them is presented here.

Choice of Hand Vein Modality

Contactless hand vein biometric capture devices are perceived as less intrusive than for instance iris capture[7]. It is for this reason - in conjunction with the accuracy rates - that a vein capture device will be designed in this project.

Disadvantages of Using Hand Vein Modalities

A list of common biometric traits are indicated in Table 2.1 along with the percentage accuracy of the modality

Table 2.1: A subset of the most common Biometric Modalities and their associated accuracy scores[4]

Biometric Feature	Accuracy Level
Finger Print	99.9%
Palm Print	> 95%
Hand Geometry	>95%
Vein Pattern	99%
Face	95%
Ear	> 95%
Iris	99.9%
Retina	99%
Voice	90%
Keystroke Dynamics	> 90%
Gait	>90%
Signature	>90%

2.2.4 Multi-modal Systems

Multi-modal biometric systems, make use of multiple processes in order to increase the complexity of the biometric template. The aim of this is to improve the circumvention trait (Section 2.1). There are many ways in which this is accomplished.

Multiple Uncorrelated Feature Technique

The first method of increasing the security level of a system is to capture two biometric features. This proves to be useful only if the two features are uncorrelated - such as iris and fingerprint or gait and face. Although the security of the system can be improved, it is usually at the expense of the user who may find it tedious to have to enter two biometrics features. But, in the same breath, this can improve the perceived security of a system which in the contexts of banking applications can improve the appeal to users[8]. Added convenience can be achieved by making use of a non intrusive biometric. If the gait of a subject approaching a door is analysed via camera before they supply a finger print the security of the system can be enhanced with minimal cost to the user. This scheme may not work for high volume access points though.

Multiple Algorithm Techniques

Multiple algorithm techniques use two or more algorithms to perform the comparison task between the query and the template. The results of all the algorithms is then combined to form a final decision on the match of biometric feature to the template[4]. Although a method like this could help circumvent malicious reverse engineering of the systems it also proves an issue in high traffic environments if the algorithms used don't take the same amount of time to execute.

Feature Combination Techniques

A third technique to improve the security of a system is to combine two captured features into one query and then perform comparison. In the case where only one feature is captured the user may hold a key card or password that is used to encrypt the biometric feature before the comparison is performed.

Fusion Levels The idea of fusing more than biometric together raises a consideration of when the features should be combined. The two features could be combined at the capture level or in some cases the result of the first comparison is fed, in combination with the next feature into the second comparison operation. Adding these fusion levels can dramatically increase the robustness of a system.

It has been discussed that there are many techniques used to improve the robustness of a biometric system towards fraud. The improvements may however hinder the speed of operation of the system. In terms of the project objectives it seems reasonable that a vascular hand capture, while already quite robust (Table 2.1) can be even further enhanced by the use of a multi-modal approach. The technical details behind the comparison of different biometric systems are considered in the next section. The common architectures used in the biometric field will also be elaborated upon.

2.3 Biometric System Architecture and Performance Metrics

In order to prepare for the design and implementation of a biometric capture device, it is important that the architectures of such systems be researched. The review will begin to focus in on the task of a biometric vascular hand scanner while still trying to give a broad review of the material where necessary. Before this, however, some time will be allocated to discuss the metrics used in comparing biometric recognition systems.

2.3.1 Technical Requirements of a Biometric System

In most implementations of biometric systems it is important that the system is able to perform to a certain standard. The performance of a system is usually based on the requirements listed in Section 2.1.2. The technical aspects are mainly:

- The system cost
- The speed of capture, comparison and decision making of the entire system
- The accuracy of the system towards detecting matches and rejecting false matches
- More prevalently the computational requirements are a factor, especially for in low power applications such as mobile phones[9].

2.3.2 Basic System Architecture

Over the past few years the standards for biometric systems have been primarily developed by international consortiums such as the International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC) and then further by their individual members [10]. There is still a sluggish global adoption rate on these standards. Hand vein recognition, for instance, has only been recognised by ISO since 2007. The standards provide a guideline to the correct way of implementing biometric systems and how such things as data and communication is handled with regard to biometric systems. As well as this the standards provide a vocabulary that eases understanding within the field[11].

Transactions

In the area of biometric verification (rather than identification) the word **transaction** is used to express an operation that is performed by the biometric system. A transaction could be a capture transaction where the system does one or more **capture attempts** with the intent of acquiring all of the biometric data from a **biometric capture subject** to produce either a **biometric reference** or a **biometric probe**.

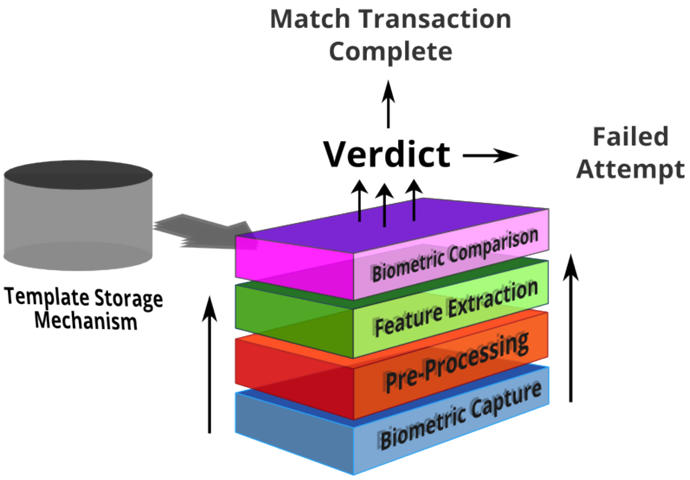


Figure 2.1: Basic biometric system stack model and the procedure towards the completion of a transaction.

A verification transaction is one or more verification attempts resulting in the resolution of a **biometric claim**.

Enrolment

The transaction of enrolment is one where a **biometric applicant** (a subject seeking to enrol in the biometric database) is first admitted to the system. When this first enrolment happens it is important that the quality of the captured feature is acceptable for storage. The stored biometric information is called a **biometric template** or **biometric reference**.

It is the biometric reference that is compared with a biometric probe (also reffered to as a **biometric query**) during a verification attempt.

Re-enrolment It is worthwhile to note that certain biometric modalities require regular re-enrolment in order to ensure the effectiveness of the system. Modalities such a facial recognition may not work for a person who has aged; or a child who enrols in a hand geometry system may grow up and need re-enrolment. It is therefore important that these things are taken into consideration during design.

Feature Capture

The entry point for most biometric systems is the feature capture device. This is a sub-system of the overall biometric system. This could be a retina scanner, fingerprint detector, a signature pad etc. In this project the capture will be via a contactless vascular hand scanner.

It is identified from the ISO standard[1] that the raw data from the capture device be converted to an encrypted biometric query as quickly as possible and then the raw data must be deleted to ensure safety of the personal information as discussed in Section 2.1.3. This quick deletion is usually inherent in real time or high frame rate capture devices because of the data storage constraints imposed on them.

Image Optimisation and ROI extraction

Occasionally the ambient conditions and noise within the detection subs-system can cause in acquiring the feature. In this regard it is important to normalise the data and enhance any features of use[12]. Other procedures contained in this part of the model are ROI extraction. Certain visual based feature extraction methods (such as the Scale Invariant Feature Transform (SIFT)[12]) can be used without having to adjust the illumination of the acquired signal or the orientation. This can improve the performance of the match but can degrade the speed of the system due to a more complex computational load. Details of optimisation and pre-processing techniques will be covered in section 2.5.

Feature Extraction

Depending on the optimised image and the biometric comparison technique, certain features may need to be extracted from the pre-processed sample. It is after the feature extraction stage that the sample is then referred to as a **biometric query**. The query is then sent on to the biometric comparison system. Once the query has been extracted, the raw data that was captured is destroyed or erased from memory in terms of the ISO standards[1].

Biometric Comparison

The biometric recognition algorithms then compare the supplied query to a template. The template is either supplied via a database or via data stored on a physical token. The comparison operation is the most important factor in determining the effectiveness of the overall system.

The most common of hand vein methods make use of a euclidean distance[13] or basic pixel comparison between the template and query (Hamming Distance). Other more robust methods make use of the positions of features such as line endings and bifurcations[14]. There are even more complex and robust methods using support vector machines[7]; nearest neighbour classifiers; manifold learning [15] and probabilistic neural networks[16] to name a few (Details are in Section 2.6).

Biometric Verdict

Usually the final subsystem is a comparison on the match results of the biometric transaction. The match could be in the form of a committee decision applied in a multi-mode biometric system or another such scoring method. When decisions are produced by the biometric recognition operation there is usually a threshold that is applied as the minimum score which constitutes as a match. This threshold value usually introduces a trade-off between accuracy of the match and number of rejected samples that are genuine users as will be seen in the following section.

There is, however, a down side to the one number output scoring mechanism. If, for instance, a biometric system is being used for authentication and it is commandeered by someone with intent to hack the system, the one number output means that the system could be tricked into believing that it is receiving inputs and will subsequently produce an output which could guide the hacker to an input combination that maximises the match score. These optimised inputs could then be used to compromise other similar systems.

A method to avoid this is to decentralise the verification process; introduce hard-wired lockouts for multiple attempts, and introduce delays between subsequent attempts. Good encryption standards will also avoid this.

2.3.3 System Performance

In order to facilitate the evaluation of different biometric comparison systems, there needs to be a generally accepted means of quantifying the accuracy with which the system matches correct queries and rejects fraudulent ones. The Encyclopaedia of Biometrics states the following as fundamental performance measures for any biometric system under consideration[17].

FTE (Failure to Enrol Rate)

The failure to enrol rate is the portion of the population for whom the system fails to complete the enrolment process i.e. the feature can be used because of bad quality or missing features such as lost fingers. This rate is usually governed by a threshold that determines the acceptable sample quality. High quality gives better matches but there is usually higher failure to enrol rates.

FTA (Failure to Acquire Rate)

This rate differs from the failure to enrol rate in the fact that a failure to enrol doesn't contribute to the failure to acquire. The failure to acquire is the measure of the number of samples where they are of acceptable quality but the system cannot extract meaningful biometric signatures from the sample. This is usually in the comparison stage of the recognition process

FNMR (False Non-match Rate)

This is the number of genuine attempt samples that are rejected by the system as being a non match to a template that is of the same characteristic and from the same user submitting the sample.

FMR (False Match Rate)

This is the proportion of zero effort attempts that provide match verdicts when the template is from a different user. This is usually the least desirable rate for a system.

The False Match Rate (FMR) and False Non-Match Rate (FNMR) can usually be adjusted by a threshold that is present on the verdict of a biometric comparison. It is most often the case that an increase in the FMR leads to a decrease in the FNMR and vice versa. These metrics are however not good measurable performance metrics because they do not take into account multiple attempts by the same user. In biometric recognition a transaction is the unit of measure but can encompass one or many re-attempts by the same user. The following measures are therefore more telling of the overall performance[17].

FRR (False Reject Rate)

The false reject rate is a metric in verification defined as the number of truthful claims that are incorrectly denied. When a transaction consists of a single attempt then the False Reject Rate (FRR) includes the Failure to Acquire Rate (FTA) and FNMR:

$$FRR = FTA + FNMR \times (1 - FTA)$$

FAR (False Acquire Rate)

This is the proportion of zero effort wrongful claims of identity that are incorrectly confirmed. The false accept rate is given by:

$$FAR = FMR \times (1 - FTA)$$

FRR and False Accept Rate (FAR) don't include failures occurring in enrolment. To accommodate for this the failure to enrol is considered to be a transaction but then further transaction by or against the enrollee fail.

GFRR (Generalised False Reject Rate)

This is the proportion of genuine users who fail to enrol, whose sample is submitted but cannot be acquired or users who are enrolled, sample acquired but are falsely rejected.

$$\begin{aligned} GFRR &= FTE + (1 - FTE) \times FRR \\ &= FTE + (1 - FTE) \times FTA + (1 - FTE) \times (1 - FTA) \times FMR \end{aligned}$$

GFAR (Generalised False Acceptance Rate)

This is the number of imposters who are enrolled, samples acquired and falsely matched

$$\begin{aligned} GFAR &= (1 - FTE) \times FAR \\ &= (1 - FTE) \times (1 - FTA) \times FMR \end{aligned} \tag{2.1}$$

ERR (Equal Error Rate)

Because the thresholds within a system interact in an inversely proportional way - namely increases in FMR cause decreases in FNMR - there is a value of the threshold called that produces an equal error rate where the FNMR equals the FMR (In an overall system this would be $FRR = FAR$). This is one of the most often used metrics in comparing biometric systems.

DET Curves

Detection Error Trade-off (DET) curves are Receiver Operation Characteristic (ROC) curves that are used widely in comparing biometric system performance (especially vascular recognition applications). The DET curves are produced by varying the threshold value that accounts for the FAR and Glsfrr. This usually produces a hyperbolic-like graph where the $y = x$ line represents the Equal Error Rate (EER). A typical DET curve is shown in Figure 2.2.

Other Performance Metrics

The following other performance measures are of relevance to this project [17]:

- Average Enrol Time - The average CPU time taken for a single enrol operation.

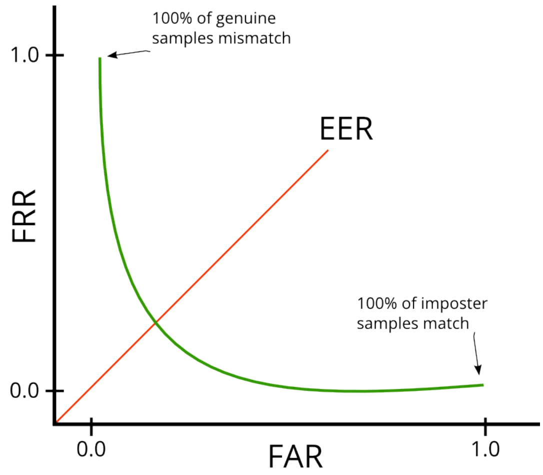


Figure 2.2: This image shows the typical shape of a DET curve. The biometric system will operate at a point on the line which is governed by the thresholds that are imposed on system.

- Average Match Time - The average CPU time taken to perform a comparison match between a template and a query.
- Throughput rate - This is the time it takes for a user to complete a transaction; including operating the device via the interface.

There are similar performance measures for identification systems too. These are outside of the scope and so are not considered here.

In the context of the a biometric hand vein capture device the most important metrics to consider would be the FTE and FTA rates. Because the matching aspect is outside the scope of this project, it will form a minor role in the evaluation. The next section goes into more detail about the specific components of biometric systems.

2.4 Acquisition via near-field infra-red

This section addresses research done on the use of near-field infra-red radiation for detection of vascular patterns in the hand. The section starts by outlining the basic anatomy of the hand and what traits are available for use as the biometric feature set. The methods of capturing a sample and the means to improve the sample (pre-processing) are discussed in the final subsection.

2.4.1 Basic Hand Anatomy[17] and Detection

Veins in the hand are generally hidden under the skin. This makes them invisible to naked-eye inspection. The pattern of veins is also said to be unique and fairly stable from the ages of 20 - 50 years[17]. The veins are responsible for the supply of blood to different body parts. Because the blood is warmer, there is a notable heat gradient that surrounds the veins. This means the vein pattern can be captured using an infra-red camera set up to detect heat signatures. The use of heat signatures presented by the heat gradients allows for far-field infra-red imaging. The use of near-field infra-red is another alternative method of imaging the subcutaneous veins. The two methods are outlined next.

Far-field Infra-red Imaging

The first method makes use of far-field infra-red (with wavelengths of $6 - 14\,\mu m$). This method of imaging actually picks up on the heat signatures of the veins. The heat data captured by the infra-red camera is then processed by a computer. The fact that it is the heat signature being imaged, means that there can be fluctuations that occur based on external conditions such a temperature of the room or whether someone is sick.

The imaging of the heat signature means that the recognition system needs to be more robust to random noise brought on by the heat of the hand.

Near-field Infra-red Imaging

The other method for infra-red imaging leverages on the fact that, because the veins are actually carrying a percentage of de-oxygenated blood, the reduced haemoglobin content makes the veins absorb infra-red light. Pair this with the fact that infra-red can penetrate biological tissue to a depth of about $3\,cm$ means that if incident light is imposed upon the hand the reflected light will show the vascular pattern of the bigger veins as darker regions. The effect of near-field infra-red (with wavelengths $750 - 2000\,nm$) can be picked up by most inexpensive cameras as they don't make use of infra-red filters to block out the near infra-red spectra.

The most effective wavelength for imaging according to the review literature is in the region of $800 - 900\,nm$ wavelengths. By only imaging in this band, the effect of body heat is largely neglected. more focus can then be put towards feature extraction.

Palm vs. Dorsum

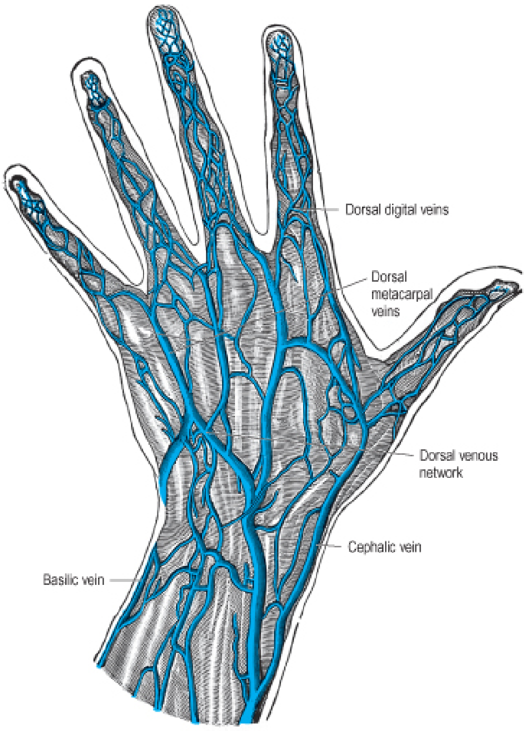
Each of the above infra-red modes can be used to image the palm or the dorsum (back of hand). The dorsum contains two types of veins: Cephalic veins which originate from the base of the hand by the wrist and Basilic veins which are on the back of the hand towards the fingers (as shown in figure).

The back of the hand is used more often in near-field infra-red imaging due to the fact that the ridges and markings on the palm are sometimes visible to the camera operating on the edge of the visible wave band. The palm vein pattern is also far more complex but potentially contains more information.

The back of the hand will be used in this project.

Some methods also make use of through light imaging where laser diodes are used to shine infra-red light through the hand[18]. An infra-red camera on the other side captures the image for processing.

It is usually the hand vein endings and bifurcations that are used as feature points for the matching system. The extraction of these feature points means that, the ROI needs to be accurately extracted.



© Elsevier Ltd 2005. Standring: Gray's Anatomy 39e - www.graysanatomyonline.com

Figure 2.3: Basic vascular patterns within the human hand.

2.4.2 Image Capture

The capture of infra-red light can be accomplished by most low cost cameras. The camera sensors are generally capable of capturing the near-field band. some cameras even use the technology for such things as auto focus. In more high end cameras, the IR is blocked out using filters.

2.4.3 IR Radiation Optimisation

In order to provide illumination of the hand surface it is necessary to use an appropriate source of near-infra-red light. One paper[19] tested a number of array geometries including double line, rectangular and concentric circles. All arrays had the camera centred in the centre of the array (Figure 2.4). It was found that the LED array offering the best uniformity of illumination was the concentric circle array.

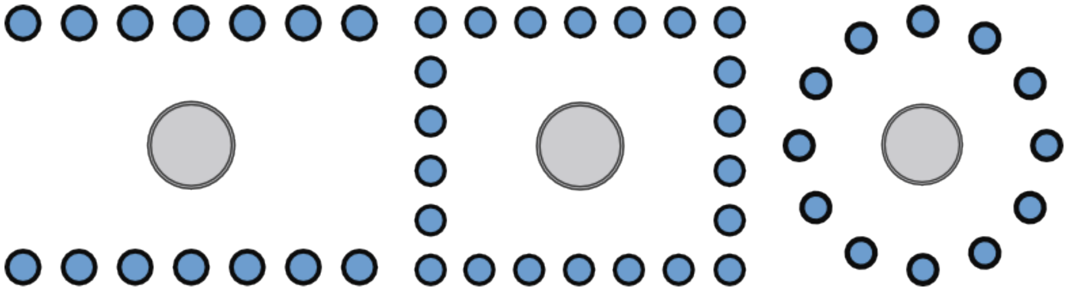


Figure 2.4: Three types of LED geometries were tested by Crisan et al. [19]. One outcome of the paper concluded that the concentric circle layout gave the best uniformity when illuminating the ROI. (Left) Double line layout. (Center) Rectangular layout. (Right) Concentric Circle layout

Further research into the LED array was carried out. A number of papers [20] [21] aim to calculate the distance away from an geometric LED array where there is optimal uniformity of the light. Both papers are based on the assumption that the LEDs are lambertian emitters. Moreno et al. Investigates in detail the illumination of a number of array patterns. For the concentric circle with number of LEDs, $N \geq 3$, the irrandiance $E(x,y,z)$ at a point (x,y,z) away from the origin which is at the center of the LED array is given by[20].

$$E(x,y,z) = z^m A_{LED} L_{LED} \sum_{n=1}^{N} \left\{ \left[x - \rho \cos\left(\frac{2\pi n}{N}\right)\right]^2 + \left[y - \rho \sin\left(\frac{2\pi n}{N}\right)\right]^2 + z^2 \right\}^{\frac{-(m+2)}{2}} \tag{2.2}$$

ρ is the radius of the LED array with area A_{LED} and radiance L_{LED} in units of $W.m^{-2}.sr^{-1}$. The variable m is defined as a function of $\theta_{1/2}$ of the LEDs. This is usually specified by the manufacturer and is the angle at which the illuminance is half that of the illuminance in the direction the LED is pointing. The relation between $\theta_{1/2}$ and m is given in[20] as:

$$m = \frac{-\ln 2}{\ln\left(\cos\theta_{1/2}\right)} \tag{2.3}$$

By computing the second partial derivative, a relationship was found between the distance ρ_0 of optimum uniformity and radius of the LED array. It was found to be [20].

$$\rho_0 = \sqrt{\frac{2}{m+2}}\, z \tag{2.4}$$

It was noted that the relationship was independent of the number of LEDs, N, in the circle.

2.4.4 Filtering and Diffusion

A number of papers reviewed made use of filters and diffusion to improve the contrast of the resulting image. While most used filters to filter out the entire visible spectrum[22]. One paper reported using a combination of two filters - one in front of the camera and one in front of the light source - orientated at 90° to each other. This arrangement reduced reflections from other light sources other than the incidence IR [19].

In order to improve the images without using a filter, a darker environment could be built in-which the hand would be imaged. Although an implementation like this would be cheaper, the idea of placing your hand inside a scanner is less acceptable to users (See Section 2.1.3).

Diffusion was another option used to improve the uniformity of the incident light. This is because non-uniform light causes fluctuations between subsequent images that could prove detrimental to the matching capability of the system.

2.5 ROI Extraction & Preprocessing

ROI extraction was performed in a number of ways. The method of extraction mainly depended on the type of matching algorithm that was used.

Some techniques used for ROI extraction are outlined below. Only three methods were considered.

2.5.1 Method 1: Wang et al. [12]

This method proposed by Wang et al. uses the following steps to optimise the captured images:

ROI Extraction

This method finds the centroid of the image using the formula:

$$x_0 = \frac{\sum_{i,j} i \times I(i)}{\sum_{i,j} I(i,j)}; \;\; y_0 = \frac{\sum_{i,j} j \times I(i)}{\sum_{i,j} I(i,j)} \tag{2.5}$$

This is equivalent to a center of mass calculation. Once the centroid (x_0, y_0) is found the image $I(x, y)$ is cropped on either side to a 360×360 image.

Contrast Limited Adaptive Histogram Enhancement (CLAHE)

The method uses CLAHE to enhance the vein pattern. This method compares the histogram of a local region of the image to the histogram of the entire region. This is in comparison to Adaptive Histogram Enhancement (AHE) which is a more generalised method than CLAHE which has the undesirable effect of increasing the noise too. The following steps are taken to perform CLAHE [23]

1. Choose a grid size for the local histogram (8 x 8 used by Wang et al.)
2. Find the normalised histogram of the local window
3. Find the normalised histogram of the entire image excluding the window
4. Transform the old region to a new region defined by

   $$h_L(r) = \alpha h_w(r) + (1-\alpha)h_B(r) \tag{2.6}$$

   $h_L(r)$ is the final local histogram, $h_w(r)$ is the normalised histogram of the window, $h_B(r)$ is the normalised histogram of the remaining image.

Where $0 \leq \alpha \leq 1$ is a factor that changes the relative importance of local information compared to global information.

To lessen the computational time required, the histogram can be calculated for a grid of points and then the intermediate points are interpolated from the grid using bilinear interpolation [24].

Bilinear Interpolation The points between two pixels can be reconstructed using the 4 neighbouring points. To perform bilinear interpolation the rows can be processed first and then the columns can be processed from the results of the rows. To compute the grey value $I(p', q')$ of a point (p', q') based on the 4 neighbours [25]:

$$I(p', q') = (1-a)\Big[(1-b)I(p,q) + bI(p,q+1)\Big] + a\Big[(1-b)I(p+1,q) + bI(p+1,q+1)\Big] \tag{2.7}$$

Where a and b are the distances from point $I(p,q)$ in the y and x direction respectively (Origin top left with positive x right and positive y down).

The value of a will obviously be quantised in the implementation.

Post Enhancement Filtering & Sauvola Method for Segmentation

After CLAHE, a 15 x 15 Weiner filter is applied to further reduce overall noise.

To segment the vein patterns, the Sauvola method is used [12]

For the $r \times r$ neighbourhood of every point the mean $m(x, y)$ and deviation $s(x, y)$ are calculated:

$$m(x, y) = \frac{1}{r^2} \sum_{i=x-\frac{r}{2}}^{x+\frac{r}{2}} \sum_{y-\frac{r}{2}}^{y+\frac{r}{2}} I(i, j) \tag{2.8}$$

$$s(x, y) = \sqrt{\frac{1}{r^2} \sum_{i=x-\frac{r}{2}}^{x+\frac{r}{2}} \sum_{y-\frac{r}{2}}^{y+\frac{r}{2}} \Big(I(i, j) - m(x, y)\Big)^2} \tag{2.9}$$

From the mean and standard deviation a threshold value can be obtained using:

$$T(x, y) = m(x, y) + k \times s(x, y) \tag{2.10}$$

Where k is defined as the coefficient of correction. If the center pixel is below the threshold then it is part of the vein domain.

Normalisation

Once the ROI has been found the image is normalised to the range 0 - 255. The mapping is as follows;

$$y = \Big(x - min(x) \times 255\Big) \,/\, \Big(max(x) - min(x)\Big) \tag{2.11}$$

2.5.2 Method 2: Crisan et al.[19]

This method presented by Crisan et al. are outlined below:

ROI Extraction

The problem of region extraction was controlled by minimising the allowable positions of the hand in the scanner. This meant that all images were correctly orientated and that the entire capture area was used for processing.

Filtering

In order to reduce computational efficiency a simple 3 x 3 kernel smoothing filter was applied to the image. To implement this the center pixel is replaced by the average of the neighbourhood.

Contrast Adjustment

In this method the contrast is adapted to fit the entire region 0 - 255. It is performed in a similar way to that of Wang et al. in 2.11

Segmentation

The method of segmentation used in this method also makes use of a kernel method. The exception is that this method only uses the mean of a sliding 25 x 25 kernel to compare against the center pixel. The value of the center is then altered accordingly. The authors note that the resulting veins are enlarged considerably by the size of the kernel. This is not a huge issue because of the thinning process they use.

2.5.3 Measuring the Noise in an Image

In order to quantitatively measure the noise in an image a method called Total Variation (TV) was used**Wang2010** The method involves finding the euclidean distance between a pixel and it's four nearest neighbouring pixels, then summing over the entire image. Namely:

$$TV(I) = \sum_i \sum_j \begin{pmatrix} \Big(I(i,j) - I(i-1,j)\Big)^2 \\ + \Big(I(i,j) - I(i+1,j)\Big)^2 \\ + \Big(I(i,j) - I(i,j-1)\Big)^2 \\ + \Big(I(i,j) - I(i,j+1)\Big)^2 \end{pmatrix}^{\frac{1}{2}} \tag{2.12}$$

2.6 Biometric Comparison Techniques

The most important section of any biometric system is the matching technique. The matching section is not explicitly covered in the scope of this project but it is necessary to garner an understanding of how the segmented images will be used in order to optimise the inputs to those functions.

[TODO: Complete Section]

2.7 Other System Aspects

These aspects of biometric systems are only minor with regard to the scope of this project. Each of these aspects could have varying impacts on the security and the cost of the system being developed.

2.7.1 Biometric Storage

In order to use an enrolled template for verification it is necessary that the template be stored. Storage can be in the form of a database, information in a 2D barcode or other token or hardened templates that are embedded in the hardware of a device such a smart-phone.

The specifications on how to store images is stipulated in specifications such as the BioAPI which is an Application Programming Interface (API) that allows for easier interconnection between a broad range of biometric systems in a common way. The BioAPI base is written in C and offers a layer of abstraction that can be used interchangeably between different modalities (however not multi-modal systems). It offers methods to perform enrolment, verification and many other operations[26].

It also had functions that allow storage of data in standard Common Biometric Exchange File Format (CBEFF) format which is recommended by the ISO standards[27].

2.8 Prospects for Vascular Acquisition via IR and Preprocessing

[TODO: Consider Prospects of Vascular Acquisition technology for the future]

Chapter 3

Methodology

LED array and detector enrolment process verification process failure to enrol test failure to accept test method of matching output images

method of recording results of acquisitions i.e. FTE, FTA

3.1 Vascular Detector for use in Biometrics

3.2 Software API to interface to Detector

NOTE: Timing considerations

This is what I did to test and confirm my hypothesis.

You may want to split this chapter into sub chapters depending on your design. I suggest you change the title to something more specific to your project.

This is where you describe your design process in detail, from component/device selection to actual design implementation, to how you tested your system. Remember detail is important in technical writing. Do not just write I used a computer give the computer specifications or the oscilloscopes part number. Describe the system in enough detail so that someone else can replicate your design as well as your testing methodology.

If you use or design code for your system, represent it as flow diagrams in text.

Chapter 4

Top Level Design

Some available literature has been reviewed in Chapter 2 and a strategy for developing and testing the system has been outlined in Chapter 3. In this section, the top level and detailed design of the hardware and software subsystems will be presented. As well as the hardware and software aspects; the interfacing will also be addressed to allow good integration with internal and external systems. The entire system will therefore be considered in relation to the three components:

- Hardware System
- Software System
- System Interfaces

For each element the top-level design will be considered in section 4.1 and then detailed design will be laid out in Chapter 5 with the top level design used as scaffolding for the detailed design.

4.1 Introduction to the Top Level Design

In order to develop the top level design for a biometric vein capture device, the first thing to consider is the context in which it will operate. How the system will be used and the goals of each stakeholder will have great influence on the final design. Identification of individual goals and stakeholder motives is carried out in section 4.2. After the needs of the system have been identified the technical requirements of the project need to be formed so as to conform to the needs of the stakeholders. The technical requirements in section 4.3 will give guidance to the detailed design in section 5. The final top level design element is the environmental issues surrounding the implementation of the project (4.4). The aim of including environmental considerations is to provide a humanistic due diligence on any adverse environmental consequences that could derive from this project and address any potential issues.

As a start point to the top level design, the most important factor to consider is the user level experience. In the current technological environment it is potentially unwise to create products that do not have usability in mind. Any product that in not usable is usually quickly replaced by one that is. If there is any possibility for the system to be used in future applications, whether commercial or otherwise, it is important to make good User Experience (UX) a pillar to the design process. It was seen in 2.1.2 that the there are many complex factors that govern the acceptability of a biometric system. It is important that these factors be considered so that the system is accepted within it's target environment.

4.2 Stakeholders, Goals and Use Cases

In order to garner an understanding of the system usage, the first task is to identify stakeholders that are involved with the system. Once the stakeholders have been identified, the respective use cases for each stakeholder needs to be considered. While there could be a number of use cases for each stakeholder, this project only aims to satisfy a small portion of use cases. This is due to time constraints and the scope of the project as laid out in Section 1.3.

Some of the stakeholders considered in this project are:

- **The Users**. More specifically the users who make use of the biometric system as a proxy to access some other external service. This could be a member of the public who aims to use an ATM or someone performing a verification purpose to access public transport. For this stakeholder, the goal is usually not the verification process but what comes after. These users are not interested in the mechanics of biometrics and only care that the process is quick and inconvenient.
- **The Owners**. This is the stakeholders that employ the system in order to make some other function more secure. They are interested in such things as: how the system performs and how many people pass through the system. They may also require that the technology integrates easily with other technologies that they already in use. Reliability of verification is a major concern for these stakeholders.
- **The maintainers and developers**. If the biometric system breaks, then these stakeholders will need to somehow diagnose the problem or fix it. Added to this stakeholder category are the developers who may need to integrate the device into another system. These stakeholders may not necessarily care for the end goal of the user but they require more access to the system functions in order to diagnose issues. These functions must be easy to understand and relevant. In this project these stakeholder concerns will carry a dual function when the system is being showcased. In order to adequately present the system access to these functions may be needed.

Other possible stakeholders that are not considered in this project are:

- **Enrolment Assistants**. These could be people in charge of helping people to perform the enrolment procedure, such as a bank teller who needs to enrol a user. They need to be able to know whether an enrolment has been successful and need to know how to delete badly enrolled feature sets.

- **Secondary Users**. In the case of verifying users on a bus, the bus driver is considered as a secondary user. They are not involved with the verification procedure directly, but care for whether a person getting on the bus is verified successfully or not. Breaks in this system may cause delays or frustration.

4.2.1 Users

It is expected that the users of the system are not interested in the mechanics of the biometric verification process. They are more likely using biometric verification as a proxy to some other service.

Requirements & Goals

Convenience The main concern to this user is the convenience of the system. As seen in section 2.1.2, convenience can relate to a reduction in mental or physical workload on the user. Paired with this any user interface should be self-explanatory and useful. The flow of information to the user should be fluid and give feedback that lets the user know that the process is still running. If a problem arises there should be contingencies that are in place to allow a retake of the information or to cancel the operation. The user also needs to be presented with such details of where to place their hand, and how to begin the scan procedure. This must be simple so as to allow use by even those who battle with English comprehension. This can be measured by having a high FRR too.

Hygiene In order for quick adoption the system needs to be hygienic. A system that involves touching of a surface must be cleaned regularly or allow the user the material (such as disinfectant towels) to clean before use. A system with regular touching of the device will not be useful in such areas such as hospitals and clinics where hygienic concerns are paramount. For this project a non-touch based system will be the goal.

Accessibility The accessibility by users who do not have the physiological trait because of loss of limb may need to make use of an alternative method of enrolment and verification. In this project the accessibility issue could be handled by allowing PIN based verification as an alternative. In a real system this may compromise the users security but due to scope an alternative biometric modality may not be implementable for this category of users.

Security of Information It is of great importance to the user that by introducing the biometric verification process, their data or information will be more secure than without. In some instances, such as e-commerce it may be that a reduction in convenience can be offset with an improved perception of security. The security of the system can be judged by a low FAR.

Use Cases & Storylines

A typical use case for the user is shown in Figure 4.1. This presents an idealised use case where the user undergoes a verification process. Figure 4.2 shows a use case for a basic self-enrolment procedure. Self enrolment assumes that the user is performing the enrolment unassisted with the use of a computer interface to guide them through the process.

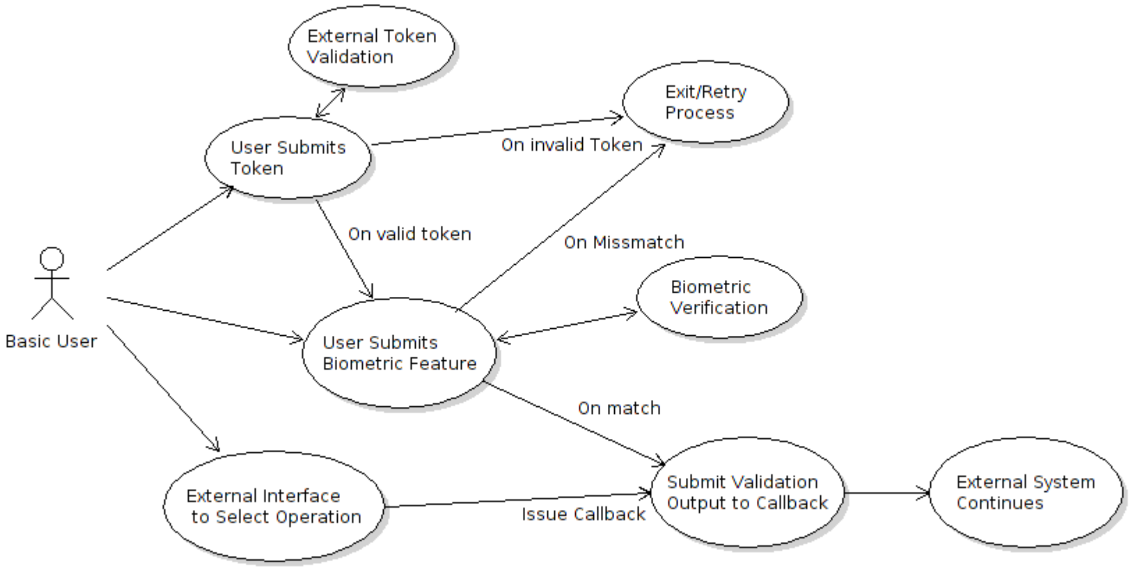

External Token Validation
Exit/Retry Process
User Submits Token
On invalid Token
On valid token
On Missmatch
Biometric Verification
Basic User
User Submits Biometric Feature
On match
External Interface to Select Operation
Issue Callback
Submit Validation Output to Callback
External System Continues

Figure 4.1: Basic use case for a simple verification operation. Here it is assumed that operations such as token submission & validation, operation choice and retry operations are carried out by the external system. It must also be noted that each operation bubble can only be activated when all inputs have been presented i.e. The user can only present a biometric feature once the token has been validated.

Project Demonstration Paired with this project is a demonstration of the final product. This could be to promote the system and it's functionality. For this specific case, a user storyline has been designed to be used for demo purposes.

During the demonstration, two operations will be shown. The first is enrolment. Where the system is presented with a token and then a biometric feature (re-entry of the biometric feature will be disabled to speed up the process). The system will perform a very basic feature extraction and store the results. The main focus of this project is image extraction and vein enhancement so to demo this the original image of the vein pattern captured by the camera will be shown alongside that of the final processed and enhanced image. A graphical animation will be shown to please the user that the information has been stored. Further information will be presented stating that the data will be deleted within a certain time frame (approx. 45 min).

Once the system is back in a normal state a token can be presented and then the biometric feature.

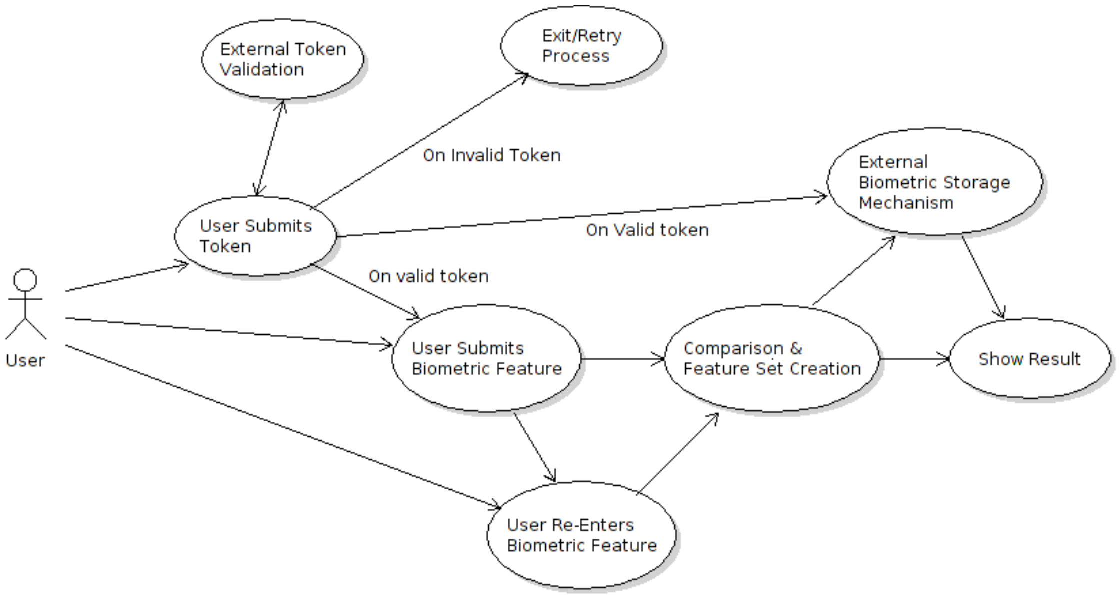

External Token Validation
Exit/Retry Process
On Invalid Token
External Biometric Storage Mechanism
User Submits Token
On Valid token
On valid token
User
User Submits Biometric Feature
Comparison & Feature Set Creation
Show Result
User Re-Enters Biometric Feature

Figure 4.2: Basic use case for a simple user self-enrolment operation. Note that each operation bubble is only activated when all inputs have been presented i.e. The user can only present a biometric feature once the token has been validated.

The system will perform an enhancement and then attempt to match the query with the template. A score will be presented to the user to see the match percentage. Then a final verdict will be presented to the user as to whether there has been a match or not.

One idea for the token is a business card. On the one side will be information about the author and a website to access more information. Included on this side is QR code which can direct to the project website but also contains a random number to be used as the token. On the reverse side the user can draw an image that they can present to the system to store. When a verification is successful, the system will present the user with the image stored on the back of the card.

4.2.2 Owners

The owners are considered to be those stakeholders that provide the service to their customers for the improvement of security. Like the users these stakeholders may not be interested in the workings of the device but care that it is secure and that it is easy to integrate with existing systems. The following concerns are presented for the owners.

Requirements & Goals

Security As with the users, security is important, this includes the FAR. Also important to the owners is the FTA metric so that they can see how effectively the system can capture the users data without needing to re-enter data. This could be important to prevent bottlenecks in certain environments where the system is placed.

Integration For the owners it is important that the system be able to integrate with many other pre-existing systems. This lowers the cost of future upgrades and guarantees the availability of people who understand how to maintain and implement the system. It must also be easy for owners to extract the data that is necessary (via a Graphical User Interface (GUI) or web interface).

Cost Most projects require that the system be cheap to install and implement. However, a high cost may be offset for a system that is more secure. While the security is important this trade-off with cost is sometimes unavoidable.

Robustness It is important that systems installed in public places be robust to such things as vandalism. The system components must be easy to replace if they are broken and the system should have contingencies if the biometric system fails.

Access Control This aspect will relate to some application more than others. This is the process of revoking, or admitting access to a subset of the enrolled users. This feature will not be fully implemented in this project.

Use Cases & Storylines

Some possible use cases are presented here. The first basic use case is the hypothetical scenario where the owner wishes to view the number of users who have passed through the system. This is an external system to the users' system. The recording of accesses is implemented in most access control applications so this service may not need to be implemented. The information such as FRR, FAR, EER etc. however will need to be accessible by this stakeholder. The use case diagram for this stakeholder is very simplistic in this project (Figure 4.3).

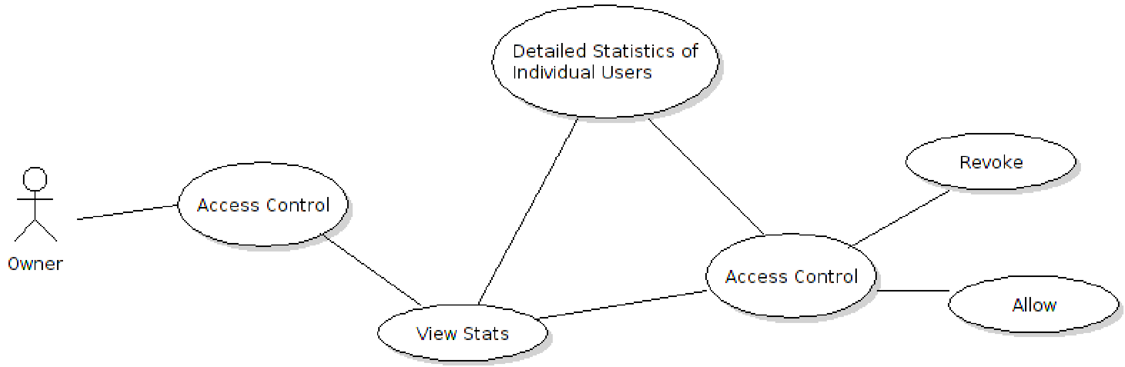


Figure 4.3: Simplified use case for an owner accessing the system. The owner may need to access information about how many users have accessed the system and the efficiency with which it has operated.

4.2.3 Maintainers

The maintainers are the stakeholders who generally have the most control of the system. They perform maintenance on the equipment and are also responsible for integrating the system with any existing systems. While there are potentially many goals for this stakeholder below are a few of the ones considered in this project. The goals of the maintainer is easy access to the system test suites and sub components. Offering a platform to test the system is also a good way to avoid unintended breaks in the system functionality.

Requirements & Goals

Access to Sub-Systems The maintainer may require access to the subsystems such as camera module, lighting module and the matching functionality. However in a commercial context it is important to ensure that while the maintainers have enough access to diagnose issues; they must not be able to access details of the matching or filtering procedures. Successful abstraction will allow for a secure system with easy access to component. Due the the scope of the project, there are only a few sub-systems that are part of the system. This will mean that good development practice such as using abstraction and coding to an interface will allow for this future functionality to be implemented easily.

Access to a Testing Suite There may be a need to include certain tests in the implementation of the project in order to allow easy debugging. During the development stage it is expected that good testing practice will be considered and good tests will be built to keep the system running in an expected way.

Access to Simulation It is common is most systems for simulations to be run on the system to ensure the chosen settings perform in the correct way. Once the functioning of the system is reviewed, the new settings are applied to the actual system. This avoids unnecessary implications that can occur from accidentally accessing or changing critical thresholds or variables.

Modular Hardware Architecture In order to address physical faults it is important that the hardware be easy to fix and replace. One method of hardware access control that could be used is to have unusual screw shapes (such as hex screws) which will prevent the layman from opening the system.

Change Threshold settings It may be necessary to set the threshold settings of the biometric verification system based on the implementation. This option may also be presented to the owners in a more user friendly way.

Use Cases & Storylines

The use case in Figure 4.4 presents the proposed usage of the system by a maintainer. They have tools that allow access to different functions but are not allowed access to information such as specific details of users. This is to improve the security of the system.

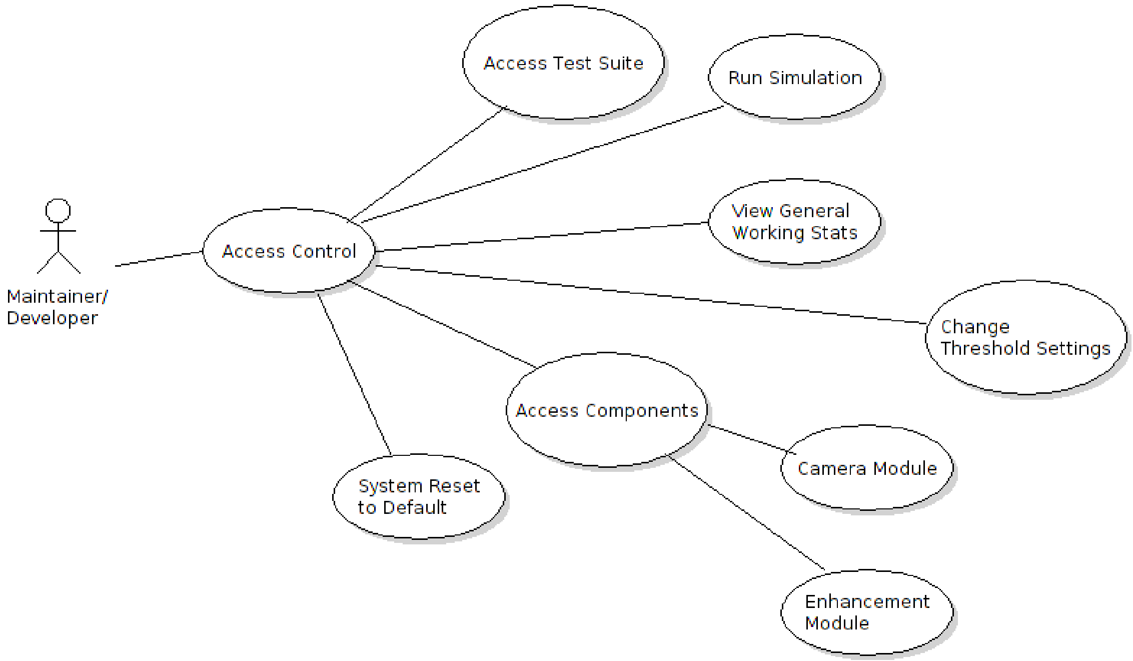


Figure 4.4: Simplified use case for system maintainer or developer. The maintainer has access to the inner workings of the system in general but may not be allowed access to the matching or enhancement algorithm. They can perform simulations and tests but may not be able to view the information of the users in the way that the owners can.

4.2.4 Summary of Stakeholder Requirements

The list below shows a summary list of the stakeholder requirements.

- **Users**
  - The system must be convenient to use. Even without prior use of the system,
  - The system must be as fast as possible without degrading performance,
  - The system must access the biometric feature in a means that is biometric,
  - The use of the biometric system must limit the number of users that are excluded from using the system based on physiological reasons,
  - The system must be secure or at least give the perception of security,
- **Owners**
  - The system must be able to be integrated with a number of other subsystems such as a token validator, biometric storage and system interface. The use of the system must not compromise the existing system,

  - The system must be relatively cheap to produce and run,
  - The system must be robust to use and be active in preventing crashes. It must also allow easy cancellations and reset if necessary,
  - The system usage records must be stored effectively and be easy to access. Access to the system must be easy to administer (revoke or affirm users),

- **Maintainers**
  - There must be relatively easy access to the sub-systems without giving too much access to the matching and enhancing algorithms,
  - There should be adequate testing and/or simulation environments to ensure new code added to the software doesn't cause bugs,
  - The hardware needs to be modular and compact to allow for easy replacement of parts that break or become faulty,
  - Thresholds within the system need to be accessible and changeable.

These are some of the requirements that will be used to assess the system during the design phase. In the next section some of these aspects will be considered in more depth and some new aspects will be added.

4.3 Technical Design Criteria

4.3.1 Hardware

4.3.2 Software

4.3.3 Interface

4.3.4 Summary of Technical Design Criteria

4.4 Environmental Considerations

4.4.1 Summary of Environmental Design Criteria

4.5 Summary of Top Level Design Specifications

Chapter 5

Detailed Design & Implementation

This section is geared towards explaining the steps that were taken during the design and development stages of the project. The hardware and software were designed and built with the final goals of the project in mind. While some aspects of the project could be designed in terms of a waterfall like plan, this project was geared towards a more agile approach. The agile method of development is more iterative, with each iteration ending in a final delivered product or version. In order to set up the initial structure of the project the first iteration will use the waterfall method and further iterations will adopt a more agile style of development as the project changes focus to the software.

5.1 Hardware

5.1.1 LED Camera Array

The design of the LED array was a core part of the project. It was necessary to build an Infra-red (IR) source that would be able to illuminate the subject region adequately. The main specifications in the design of the LED array are:

- The array must be able to provide uniform illumination to the subject of interest,
- Low cost components should be used to avoid delays in the project timeline,
- The wavelength used should be able to be absorbed by the veins enough to produce a visible contrast,
- The device should be user friendly and incorporate the camera in a convenient way

5.1.2 Choice of Materials

5.2 Software: Programming and Development Environment

This section contains details of the software design and implementation.

5.2.1 Python for Development

In order to produce a system quickly, it is necessary that the right programming language be chosen. For this project, python has been chosen to this aim. Python is a highly flexible programming language for prototype development. Here are some of the advantages:

Advantages of Python

- Python is Object Orientated. This means that it can make use of classes and subclasses. This will make the system easier to code because commonly used functions can be abstracted and used many times.
- Python has mutable data types. This means that a variable doesn't need to be specifically linked to one type. This makes it easy to implement functions without having to care too much about the data types being passed too and from it.
- Attributes of objects can be directly referenced. This means there is no need for implementing getter and setter methods to handle data access to private variables.
- The numpy[1] package extends python to allow Octave like matrix computation.
- Python can hand complex mathematics natively.
- A python-opencv package is available through the linux apt-get package manager. This means that installation of opencv will be very simple.

Disadvantages

- Python is a scripting language and not a compiled language. This means that the programs created are not as efficient at run time. But as a prototype development language it is flexible. At a later stage, python methods can be implemented in a more robust language such as C++ or Java.

Python 2 vs Python 3

[1] http://www.numpy.org/

Python 3 is a newer version of python 2 but due to a number of technical reasons, python 3 is not always fully backward compatible with python 2 script. Although Python 2 is considered the legacy version there is still a large community that still use it even for new projects. Because of the legacy, the opencv library for python is written mainly for the python 2 style and for this reason, Python 2 will be used.

Python Version 2.7.6 was used in this project.

5.2.2 Eclipse as IDE

For this project, Eclipse Luna 4.4.0[2] was used as the IDE. Eclipse is a free development environment that was chosen because of familiarity. The PyDev add-on was also used to allow development of python scripts.

5.2.3 Git Version Management

https://github.com/DustioDesign/Palmetto.git

Git version management was used to ensure that any working software was secure from further edits. The eclipse git add-on made it easy to control the branches and the development flow. The entire software base was pushed to GitHub[3] to allow for remote access by future developers.

5.2.4 OpenCV

[TODO:]

5.2.5 GNU Octave

[TODO:]

5.2.6 Project Structure

The structure of the project describes how the actual project folder is organised.

[2] https://projects.eclipse.org/releases/luna

[3] http://www.github.com

- Palmetto - Project Root
    - package: **demo**

      This package contains the scripts that are used to demonstrate the system. This is not meant to be an integral part of the software but and is not referenced by any of the other packages.
    - package: **experiments**

      The experiments package contains scripts that were used throughout the development process to aid in the design of the final system. Some scripts in this package run optimisation routines to find constants for operations such as CLAHE and Suavola Thresholding. This package also contains some initial implementations to test the functionality of different operations.
    - package: **functions**

      This package contains useful functions that could aid in further development or debugging of the system. Modules to draw histograms and perform optimisations are in this package.
    - package: **operations**

      This package contains modules that perform operations on the images. The operations package contains the final versions of the CLAHE, AHE etc. operations.
    - package: **structure**

      The structure package controls the program execution and contains non-business rules - such as interfacing to the camera and editing persistent configuration variables. It contains base classes for other subclasses within the program and contains the main entry point for the Palmetto project.

      [TODO: Enter entry point destination]
    - package: **tests**

      The test package contains unit test classes that can be used to test whether the system is still functioning as intended. See Section 5.8

5.3 Software: Program Structure

For the first iteration of the design process the program flow was drawn up in VioletUML as shown in figure 5.1. The program flow basic but can be adapted to in the future.

5.3.1 Programming to an Interface

Referring to figure 5.1, the ”Get Enhance Operations” and ”Get Matching Operations” retrieve operations to perform which are passed to the program. Each operation such as Adaptive Histogram Enhancement or Median Filter will be applied by accessing a class which performs that operation. To ensure extensibility an interface will be created for the enhance operations and the matching operations. Programming to an interface will enforce certain methods that will be used by other parts of the program.

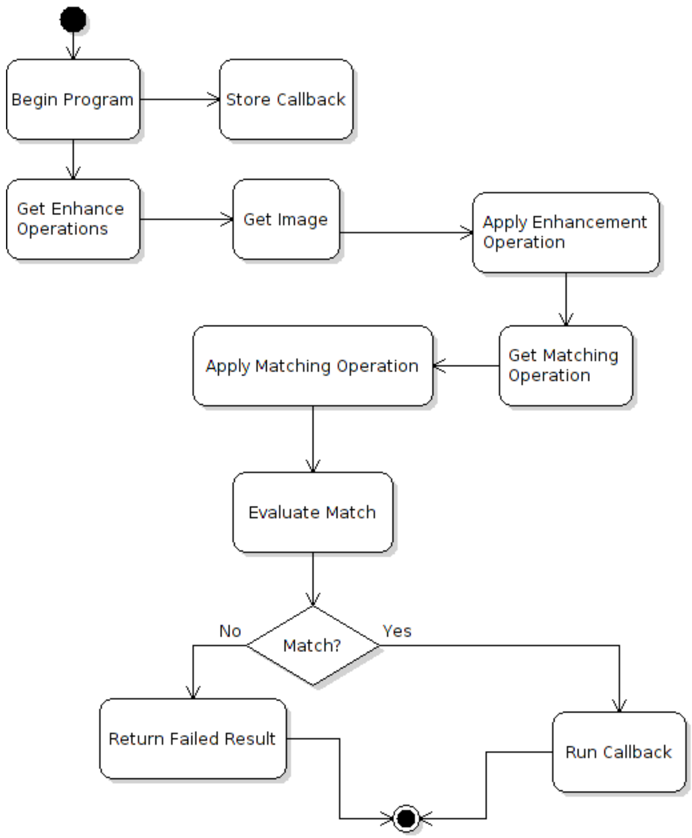


Figure 5.1: Sample Caption

5.4 Software: Computational Operations

This section contains the detailed design of some of the custom built operations used in processing the input image. Ideally, the aim of these operations is to transform the input image into a binary image with the vein pattern emphasised. In each of the sub-sections that follow the heading represents the operation that is being developed. Below that is the python import that is required in order to use the module. This import also serves as a reference to the module location in the python project. Below that is the design process that was followed.

Modularisation: All the implementations described below are able to be imported by other python scripts. Some scripts can be executed individually in which case there is a main condition that runs an example useage of the module.

Documentation: All python modules are documented as far as possible (See Section 5.9.2)

5.4.1 Optimisation Method using BGA

```python
from functions.fminbga import fminbga
```

5.4.2 Grayscale Normalisation

```python
from operation.graynorm import GrayNorm
```

This operation performs gray-scale normalisation [25]. Gray-scale normalisation dims the effect of saturation due to the illumination of the hand. Each pixel in the original image is mapped via the following formula

$$y = \frac{\left(x - min\right) * 255}{max - min}$$

Where max and min are the maximum and minimum gray-scale values in the original image.

5.5 User Experience

5.6 Expected Product Lifecycle

5.7 Integration Design

How will the system interact with other systems already in place.

5.8 Testing Infrastructure

How will the system be tested during production and during further developments.

5.9 Maintenance Design

5.9.1 Hardware Maintenance

5.9.2 Software Maintenance

Documentation

5.10 Environmental Impact Assessment

A brief description of any foreseeable environmental issue that are directly or indirectly to related to this product.

5.11 Summary of Tools Used

Within this section is a list of all the tools that were used in the design of this product. As far as possible the design has focused on the use of open source tools. The listed tools below are accompanied by a brief reason for selection this is ancillary to any reasons discussed in above sections.

5.11.1 Hardware Tools

5.11.2 Software Tools

[4]

5.11.3 Miscellaneous Tools Needed for Assembly and Development

[4] http://www.google.com

Chapter 6

Results & Outcomes

A number of tests were performed on the components of the biometric system. The results are presented within this section. The tests performed were either in the form of a software simulation or a experimental experiment. The experiments and results covered in this section are:

- **Simulation of LED Array Setup (6.1)**

  A simulation was run in order to check the validity of the LED specifications designed in section 5.1.1.

-
-
-

6.1 Simulation: Simulation of LED Array Setup

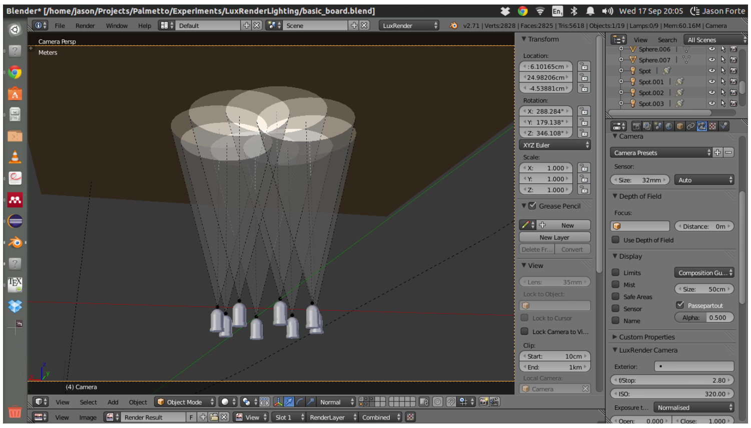
Aim This simulation is in reference to section 5.1.1 where the design for the LED layout was considered. The appropriate distribution of the LED array was calculated. Within this experiment, an attempt is made to validate this configuration. In order to fully test the proposed setup it was necessary to find software that could accurately simulate the ray traces emitted from the LEDs. Finding such software proved a challenge and non scientific software was on hand (not cheaply at least) to perform this test. As an alternative, an open source 3D animation rendering program was used.

Blender[1] is an open-source application geared to the animation industry. The program can perform modelling, rigging, texturing and as well as a wide range of other functions. Importantly for this simulation, the program makes use of complex ray trace and scattering algorithms

[1] http://www.blender.org

to produce the rendered scenes and are of similar type to those used in
GPU rendering of games. The accuracy of the models was a concern but as a baseline they were sufficient to the aims.

Method The scene was set up with eight (8) LEDs placed on the XY plane of the 3D scene. A flat plane representing the incidence surface was placed parallel to the XY plane at a distance z away from the origin. Each LED was modelled as a spotlight source with cubic falloff and $30°$ viewing angle. Figure 6.1 shows the constructed scene.



Blender* [/home/jason/Projects/Palmetto/Experiments/LuxRenderLighting/basic_board.blend]

v2.71 | Verts:2828 | Faces:2825 | Tris:5618 | Objects:1/19 | Lamps:0/9 | Mem:60.16M | Camera

Location: :6.10165cm, 24.98206cm, -4.53881cm

Rotation: X: 288.284°, Y: 179.138°, Z: 346.108°, XYZ Euler

Scale: X: 1.000, Y: 1.000, Z: 1.000

Lens: 35mm

Clip: Start: 10cm, End: 1km

Sensor: Size: 32mm, Auto

Depth of Field – Focus: Distance: 0m; □ Use Depth of Field

Display: □ Limits, □ Mist, □ Safe Areas, □ Sensor, □ Name; Composition Gu...; Size: 50cm; ☑ Passepartout; Alpha: 0.500

LuxRender Camera – f/Stop: 2.80; ISO: 320.00; Exposure t... Normalised; Open: 0.000; Close: 1.000

Figure 6.1: Blender Lighting Simulation. Circular LEDs are placed on the XY plane and a surface is placed at a distance z from the LEDs. The light profiles are set to have cubic falloff. The resulting overlapping distribution on the flat plane is then observed

6.2 Initial Comparison of Images

6.3 Simulation Results

6.4 Experimental Results

Chapter 7

Discussion

Here is what the results mean and how they tie to existing literature...

Discuss the relevance of your results and how they fit into the theoretical work you described in your literature review.

Chapter 8

Conclusions

8.1 Project Conclusions

Thisefaf fdafsdaf fda These are the conclusions from the investivation and how the investigation changes things in this field or contributes to current knowledge...

Draw suitable and intelligent conclusions from your results and subsequent discussion.

8.2 Recommendations for Future Work

Make sensible recommendations for further work.

Appendices

Appendix A

Software Resources

A.1 UML Design (VioletUML)

The UML diagrams were created using Violet UML Version 2.0.1 [1]

A.2 Image Editing

A.2.1 Vector Image Creation (Inkscape)

Vector image creation was done using Inkscape[2] Version 0.48. Inkscape is an open source alternative to Adobe Illustrator.

A.2.2 Image and Photo Editing (GIMP)

Pixel base photo and image editing was performed using GIMP [3]. Version 2.8 was used in this project.

[1] http://http://alexdp.free.fr/violetumleditor/

[2] http://www.inkscape.org

[3] www.gimp.org

References

[1] T. Report, "ISO/IEC 24714-1 Information Technology - Biometrics - Jurisdictional and societal considerations for commercial applications," International Organisation for Standardisation (ISO), Geneva, Tech. Rep., 2008.

[2] M. Espinoza, C. Champod, and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks.," *Forensic science international*, vol. 204, no. 1-3, pp. 41–9, Jan. 2011, ISSN: 1872-6283. DOI: 10.1016/j.forsciint.2010.05.002. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0379073810002331.

[3] The Forensic Science Service, *Guide to DNA: for Lawyers and InvestigatingOfficers*. Crown Prosecution Services, 2004.

[4] J. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern Recognition*, vol. 47, no. 8, pp. 2673–2688, Aug. 2014, ISSN: 00313203. DOI: 10.1016/j.patcog.2014.01.016. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S003132031400034X.

[5] *International Covenant on Civil and Political Rights*. [Online]. Available: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[6] LearnCryptography.com, *Learn Cryptography — Prime Factorization*, 2014. [Online]. Available: http://learncryptography.com/prime-factorization/.

[7] G. K. O. Michael, T. Connie, and A. B. J. Teoh, "A contactless biometric system using multiple hand features," *Journal of Visual Communication and Image Representation*, vol. 23, no. 7, pp. 1068–1084, Oct. 2012, ISSN: 10473203. DOI: 10.1016/j.jvcir.2012.07.004. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1047320312001216.

[8] F. Deane, K. Barrelle, R. Henderson, and D. Mahar, "Perceived Acceptability of Biometric Security Systems," *Computers & Security*, vol. 14, no. 3, pp. 225–231, 1995.

[9] P. Harsha and C. Subashini, "A real time embedded novel finger-vein recognition system for authenticated on teller machine," *2012 International Conference on Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM)*, pp. 271–275, Dec. 2012. DOI: 10.1109/ICETEEEM.2012.6494494. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6494494.

[10] R. Ryan, “The importance of biometric standards,” *Biometric Technology Today*, vol. 2009, no. 7, pp. 7–10, Jul. 2009, ISSN: 09694765. DOI: `10.1016/S0969-4765(09)70114-6`.

[11] I. Standard, *ISO/IEC 22537 - Information Technology - ECMAScript for XML (E4X) specification*, Geneva, 2006.

[12] Y. Wang, Y. Fan, W. Liao, K. Li, L.-K. Shark, and M. R. Varley, “Hand vein recognition based on multiple keypoints sets,” *2012 5th IAPR International Conference on Biometrics (ICB)*, pp. 367–371, Mar. 2012. DOI: `10.1109/ICB.2012.6199778`. [Online]. Available: `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6199778`.

[13] M. H.-. M. Khan, N. Ali, and M. Khan, “A New Method to Extract Dorsal Hand Vein Pattern using Quadratic Inference Function,” vol. 6, no. 3, pp. 26–30, 2009.

[14] Anil K. Jain and Patrick Flynn and A. A. Ross, *Handbook of Biometrics*. New York: Springer, 2008, ISBN: 9780387710402.

[15] Z. Liu, Y. Yin, H. Wang, S. Song, and Q. Li, “Finger vein recognition with manifold learning,” *Journal of Network and Computer Applications*, vol. 33, no. 3, pp. 275–282, May 2010, ISSN: 10848045. DOI: `10.1016/j.jnca.2009.12.006`. [Online]. Available: `http://linkinghub.elsevier.com/retrieve/pii/S1084804509001428`.

[16] S. G. Wu, F. S. Bao, E. Y. Xu, Y.-X. Wang, Y. Chang, and Q.-L. Xiang, “A Leaf Recognition Algorithm for Plant Classification Using Probabilistic Neural network,” in *IEEE International Symposium on Signal Processing and Information Technology*, 2007, pp. 11–16.

[17] S. Z. Li and A. J. Jain, Eds., *Encyclopedia of Biometrics*. New York: Springer, 2009, ISBN: 978-0-387-73002-8.

[18] N. Mahri, S. A. Sundi Suandi, and B. A. Rosdi, “Finger Vein Recognition Algorithm Using Phase Only Correlation,” *2010 International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics*, pp. 1–6, Aug. 2010. DOI: `10.1109/ETCHB.2010.5559283`. [Online]. Available: `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5559283`.

[19] S. Crisan, I. G. Tarnovan, and T. E. Crisan, “Radiation optimization and image processing algorithms in the identification of hand vein patterns,” *Computer Standards & Interfaces*, vol. 32, no. 3, pp. 130–140, Mar. 2010, ISSN: 09205489. DOI: `10.1016/j.csi.2009.11.008`. [Online]. Available: `http://linkinghub.elsevier.com/retrieve/pii/S0920548909001007`.

[20] I. Moreno, M. Avendaño-Alejo, and R. I. Tzonchev, “Designing light-emitting diode arrays for uniform near-field irradiance.,” *Applied optics*, vol. 45, no. 10, pp. 2265–72, Apr. 2006, ISSN: 0003-6935. [Online]. Available: `http://www.ncbi.nlm.nih.gov/pubmed/16607994`.

[21] J. Muñoz, “Uniform illumination of distant targets using a spherical light-emitting diode array,” *Optical Engineering*, vol. 46, no. 3, p. 033 001, Mar. 2007, ISSN: 0091-3286. DOI: `10.1117/1.2715562`. [Online]. Available: `http://opticalengineering.spiedigitallibrary.org/article.aspx?doi=10.1117/1.2715562`.

[22] S. Zhao, Y. Wang, and Y. Wang, "Extracting Hand Vein Patterns from Low-Quality Images: A New Biometric Technique Using Low-Cost Devices," *Fourth International Conference on Image and Graphics (ICIG 2007)*, pp. 667–671, Aug. 2007. DOI: `10.1109/ICIG.2007.97`. [Online]. Available: `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4297166`.

[23] H. Zhu, F. H. Chan, and F. Lam, "Image Contrast Enhancement by Constrained Local Histogram Equalization," *Computer Vision and Image Understanding*, vol. 73, no. 2, pp. 281–290, Feb. 1999, ISSN: 10773142. DOI: `10.1006/cviu.1998.0723`. [Online]. Available: `http://linkinghub.elsevier.com/retrieve/pii/S1077314298907238`.

[24] S. M. Pizer, R. E. Johnston, J. P. Ericksen, B. C. Yankaskas, and K. E. Muller, "Contrast-Limited Adaptive Histogram Equalization: Speed and Effectiveness Stephen M. Pizer, R. Eugene Johnston, James," 1990.

[25] W. K. Pratt, *Digital Image Processing*, 3rd Editio. Los Altos, California: John Wiley & Sons, 2001, vol. 5, pp. –471, ISBN: 0471374075.

[26] C. Tilton, "BioAPI Presentation," W3C Workshop on SIV, Reston, VA, Tech. Rep. March, 2009.

[27] F. L. Podio, J. S. Dunn, C. J. Tilton, L. O. Gorman, and M. P. Collier, *Common Biometric Exchange File Format*, 2001.