

**Hybrid Multi-Modal Biometric Authentication System**

**James Finglas**

**B00094138**

Department of Informatics

School of Informatics and Engineering

Technological University Dublin

Submitted to Technological University Dublin in Partial Fulfilment of the requirements for the degree of:

Bachelor of Science (Honors) in Computing

Course: Biometrics & Forensics Applications

Lecturer: Arnold Hensman

Submission Date: 22/11/2019

Word count (Introduction to Conclusions): 3682

# Project Submission/Declaration Form

Submitted by: James Finglas

Course Coordinator: Stephen O'Shaughnessy

Module Name: Biometrics & Forensics Applications

Course Code: H4016

Lecturer: Arnold Hensman

Submission Date: 22/11/2019

I declare that the work contained in this report which I now submit on the program of study leading to the award of Degree of Honors B.Sc. in Computer Science in Technological University for Dublin is my own work and has not been taken from the work of others. Any sources which have been referenced or analyzed have been cited using the Harvard/IEEE standard within the body of this report. It is entirely my own work except where otherwise stated and has not been submitted for assessment for an academic purpose at this or any other academic institution other than in partial fulfilments of the requirements stated above.

I have read and understood the Technology University Dublin’s policy regarding plagiarism.

X

James Finglas

# Abstract

This report lays out the development process of my multimodal biometric system for my Biometrics and Forensics Applications course, 2019. The purpose of this assignment was to develop a framework from which we could build a multimodal biometric application later, which lays out the methodology, design considerations, application design process including design and technical specifications. Also included is a preliminary testing phase followed by my conclusions on my design template.

In In order to facilitate the production of my design template, I conducted and document some basic research into the primary biometric options I felt I had available to me, as laying out my reasons for the methods I ultimately selected and reasons for why discarded the others.

Contents

[Project Submission/Declaration Form 2](#_Toc24914069)

[Abstract 3](#_Toc24914070)

[Table of figures: 5](#_Toc24914071)

[1.0 Introduction 6](#_Toc24914072)

[2.0 Summary 8](#_Toc24914073)

[2.1 Requirements Specification 8](#_Toc24914074)

[2.2 Methodology 9](#_Toc24914075)

[2.3 Design Considerations 10](#_Toc24914076)

[2.3.1 Signal versus Non-Signal 10](#_Toc24914077)

[2.3.2 Fingerprint 10](#_Toc24914078)

[2.3.3 Facial Recognition 10](#_Toc24914079)

[2.3.4 Voice Recognition 11](#_Toc24914080)

[2.3.5 Iris Recognition 11](#_Toc24914081)

[3.0 Application Design 12](#_Toc24914082)

[3.1 Design Specification 12](#_Toc24914083)

[3.2 Technical Specification 13](#_Toc24914084)

[4.0 Testing 15](#_Toc24914085)

[4.0 Conclusions 16](#_Toc24914086)

[6.0 Glossary 18](#_Toc24914087)

[7.0 References 19](#_Toc24914088)

# Table of figures:

[Figure 1 Here we see the Irishield-USB BK 2121U. 9](#_Toc24914060)

[Figure 2 My simple Use Case Breakdown of my Biometric system. 13](#_Toc24914061)

[Figure 3 Extended Use Case Diagram for Option 1: Enrollment, with basic error correction documented. 14](#_Toc24914062)

[Figure 4 Extended Use Case Diagram for Option 2: Identification / Verification, with basic error correction documented. 14](#_Toc24914063)

[Figure 5 The 7 Characteristics of Biometrics, taken from the chapter Introduction to Biometrics and Biometric Security Systems’ [6]. 16](#_Toc24914064)

[Figure 6 Visual samples of Iris at distance low interaction technology in action. 17](#_Toc24914065)

# Introduction

Biometrics; The science of extracting human characteristics for conversion to metric data points. This can be used for identification purposes, as in law enforcement a suspect may be fingerprinted for the purposes of attempting to match a given set of prints against a known database of prints. If a match is found, the suspect can be said to have been identified. A company may use biometrics too for identification of who is on the premises or access restricted areas. Similarly, biometric data can be used for authentication and access purposes. This is where a potential user or client claims to have access or be someone, and biometrics are used to compare against a known user database to confirm the user is who they say they are refute the attempt to authenticate.

In biometrics, most common systems will have known potential flaws which can be reduced in frequency by adjustment of a threshold of acceptance; as discussed by Neri Merhav, such as a failure to enroll rate (FTE) [1]. This is the given rate at which users might try to enroll on the system and the attempt will fail erroneously due to bad data input or system malfunction or incorrect use of scanners by the user attempting to enroll. A system might also have known level of failures to reject (FTR). This is where a system will mistakenly identify or authenticate a user who is not enrolled. And a system may also have a known false rejection rate (FRR). Lastly a system have a high rate of false acceptance (FAR), whereby a user is accepted who is not enrolled or has been misidentified by too low a threshold. This is where the system fails to authenticate a user who is enrolled and should be authenticated. Each type of biometric system, be it fingerprint, voice, facial will have acceptable and unacceptable levels of each of these failure types. As well as adjustable levels of threshold at which a detected input is considered acceptable by the system or rejected.

Each system might also incorporate a ‘liveness’ detection method as discussed by Anita Babu, et al [2]. This is where a system is designed to detect the presence of a living human. This is a pure security strengthening addition and has no input on the identification or authentication algorithm except in that the user will either pass or fail and be allowed to proceed on to identification/verification, or not.

Some systems would be deemed more secure or less secure than others. For example, A silicone-based fingerprint scanner would be considered less secure than a capacitive scanner. While a capacitive scanner would be considered less secure than a capacitive scanner incorporating near infra-red vein detection/recognition technology. And Again, Facial or Voice biometrics, might both be considered more secure than any fingerprint biometrics simply because the circumvention of Facial and voice biometrics is cumbersome and awkward and obvious, whereas fingerprint circumvention is far less so.

For this reason, multimodal biometrics systems were developed. Where one system might fail, it is less likely that two will fail. Where one system might be circumvented, multiple systems will be much harder to circumvent, and finally, should any one system fail, you will be left with one method of obtaining and checking biometrics. So, a multi-modal system can, depending on placement and context of use; be said to increase security, decrease the likely hood of circumvention, while reducing the likely hood of total system FTE, FTR, FAR or FRR.

This is the area in which this paper is focused. Our challenge was to design a multimodal biometric system. Primarily we focused on developing an application. I elected to institute a self-imposed scope limitation, whereby choices were limited to available college hardware or hardware owned or purchased by me (Optional). Furthermore, we were not asked to design algorithms or script new API’s To handle the actual biometrics. We are simply tasked with comparing the pros and cons of various types of biometric systems. Then we must select a minimum of two types and implement these two via freely available API’s.  
We must firstly, demonstrate an understanding of general biometric pros and cons, and secondly with a minimum amount of scripting and coding implement a system that can enroll, identify and authenticate with our chosen biometric methods.

# Summary

I began by laying out the methodology of my design approach and the goals of my research. Next, I analyzed the pros and cons Each type of Biometric method available, both singularly and when combine with other types to construct a multimodal system. Following on from this I planned out the design of my multi-modal implementation and its basic use case functionality. I laid out a minimal testing phase. I expect the testing phase to be expanded during implementation, but having no testing planned at all would be a gross over-site on the part of any developer. I then

## 2.1 Requirements Specification

The goal of this project is to display a clear understanding of the pros and cons of the various types of biometrics systems available to us. We also aim to demonstrate our ability to design a system that will be capable of multi-modal biometric enrollment, identification and verification. We shall seek to create a design template for a program that can handle a database enrollment system for enrollment of large sample enrollment files as well biometric manual enrollment and identification/verification. We shall also outline a limited testing plan to display our understanding of the potential problems our system could run into regarding FTE, FAR and FRR rates, threshold adjusting and lack of error handling.

The system require will be as follows:

Mandatory functions –

1. Manual single user enrollment in both facial database via facesAlogrithimDemo.exe, coupled with manual enrollment in iris database via irisesAlgorithimDemo.exe to complete platform enrollment.
2. Manual single user identification in facial database via facesAlogrithimDemo.exe, coupled with manual verification in iris database via irisesAlgorithimDemo.exe to complete platform verification.

Optional functions –

1. Automatic Enrollment of many users from file in both facial database via facesAlogrithimDemo.exe, coupled with manual enrollment in iris database via irisesAlgorithimDemo.exe to complete platform enrollment.
2. Automatic identification of many users from file in facial database via facesAlogrithimDemo.exe, coupled with automatic verification in iris database via irisesAlgorithimDemo.exe to complete platform identification/verification for testing purpose by looping through users and complete testing/verification a preset number of times.
3. Addition of a Authorization level attribute and table. We would have access via identification. If the user is not in the facial database, access is denied. Verification is achieved via iris scan. And authorization could be achieved by use of an authorization attribute. This attribute could also be gated behind the addition of a password which would be required before the system would check for an authorization attribute. If no password is entered, an authorization of least privilege could be assigned for a given session. At a later date, logging could be added for completion of a ‘AAA’ system.

## 2.2 Methodology

Due to the restrictions in available hardware, I elected to restrict my selection choices to silicone or capacitive finger print scanner, facial recognition. iris scanning, and voice recognition. We must conduct research into the pros and cons of each, and finally outline a design template for their implementation. Limited testing will be outlined although this may be extended during implementation.

My Program will be CLI based and written in the visual basics IDE, using the C (C+ or C#) language family or Java and it will be based on implementation the Neurotechnology API’s. This is due to compatibility with Visual basics which allows for C language, Java and JavaScript languages. As I have determined to use Facial recognition and Irish recognition, my hardware will be my Laptop onboard webcam, and my iris scanner will be an Irishield-USB BK2121U as seen below in figure 1.

The use of MySQL may be required to meet some optional requirements I have set myself, and I reserve the right to include this program in the design template.

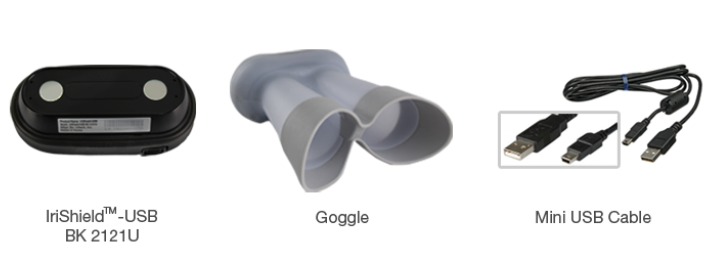


Figure Here we see the Irishield-USB BK 2121U.

For Software I will incorporate the Neurotechnology SDK API’s for both FaceAlgorithimDemo.exe and IrisesAlgorithimDemo.exe.

## 2.3 Design Considerations

### 2.3.1 Signal versus Non-Signal

Since I have limited myself to the technology available within the college this restricts to fingerprint, iris and face scanning as well as voice pattern analysis. Of these 4 methods, one is signal based, meaning voice. As I must college a sequence of data to analyze, because one signal phenom from a voice sample cannot be used to create a pattern match. So, a user must speak for say 10 seconds and record a phrase. This creates a map which can be used for verification via phenom pattern recognition. This phrase must then be repeated matching phenoms and speech pattern / tone. For this reason, I have determined that signal-based biometrics in this case are not what I consider to be acceptable as the collection and verification methods require too much rigidity from the user. User comfort must be considered when designing a biometric system.

Facial, Iris and fingerprint can all be said to be image-based biometrics methods. Each method simply requires the user to remain relatively still and either present their finger, face or iris for scanning and the user must only hold-still for a few seconds. I feel this is a much more acceptable level of data collection providing a greater level of user comfort, which makes these three methods of Biometrics more favorable regarding my system.

### 2.3.2 Fingerprint

Where fingerprint scanning is concerned, I have two options available to me. Silicone and capacitive scanning. The first, silicone present a relatively simple form of circumvention. These can be fooled simply by creating a latex mold of a finger and presenting it to the scanner.

A capacitive scanner while affording a highly of security due to its liveness detection, can be fooled by a similar method, by simply ensuring a small piece of the user’s actual real finger contacts the scanners positive/negative transistor-based scanning surface and closes the circuit. Other types of finger print scanners can be bypassed with much simply methods, be it by breathing on the surface, using a plastic bag containing hot water to simulate the heat of the human body etc. These circumvention techniques are discussed in detail by Tom Fladsrud in his scholarly paper titled ‘circumvention of fingerprint scanners [3]. For this reason, I have ruled out fingerprint scanners and fingerprint biometrics as being too insecure.

### 2.3.3 Facial Recognition

Facial Recognition is a relatively low interaction biometric affording relative comfort to the user. It has a high level of acceptability in my opinion. However, it does have a somewhat negative aspect. It is relatively simple to bypass a facial recognition scanner if there are no humans overseeing the verification process. As facial recognition is based in identification of large areas of the face and the eyes are only use for liveness detection, a simple picture can be used to simulate the presence of a face and the live detection related to the eyes can be easily fooled. My system will be designed as low interaction biometric system, meaning no humans will be present. This may present a problem if Facial can be bypassed relatively easily in this case. The issues surrounding the circumvention of facial technology are addressed here by Security Researcher Curtis Franklin Jr. [4].

### 2.3.4 Voice Recognition

Voice Recognition is an interesting signal based biometric. Being signal based it means that a single image or frame of data cannot be used to create a map of the user’s identification. This makes Vocal circumvention reasonably difficult which require high tech technology. However, it is reasonable to say that the average user might find recording their voice and having to speak back a specific sequence of words for a specific period of time somewhat uncomfortable. This make sit a high interaction biometric with a relatively low acceptability score. In fact, Voice has been found, in some white papers; to be one of the strongest biometrics, though not un-hackable, in their testing, as conducted by Nuance [5].

### 2.3.5 Iris Recognition

Irish recognition is a strong Biometric. Due to its use of high amounts of data sampling, it is very difficult to circumvent, as noted by Vanaja Roselin E. Chirchi, in the 2011 paper titled ‘Iris Biometric Recognition for Person Identification in Security Systems’ [6]. It retains a high level of acceptability, performance and permanence.

# Application Design

## 3.1 Design Specification

I have Elected to adopt a 2-stage facial and iris-based biometric system. I have chosen this system as they lend themselves together quite nicely in my opinion. As previously mention, Facial recognition does have what can be considered an Achilles heel, meaning that if no human observance is involved, a facial recognition system can be fooled without too much technical difficulty. This is largely due the eye liveness detection being flawed.

However, when coupled with an iris biometric scan which is very hard to circumvent, this flaw is removed. Therefore, my system will require a user to first be identified by a facial scan, to verify that the user in question exists on the system. Should the user not exist on the system, no further validation is required, and the user is deemed to not be authorized for access. Should the user pass a facial scan, the user is then passed on to the second stage, verification. This is where the user claims a specific identity within the database and an Irish scan is used to verify the user identity. The option to add in a third element, authorization, is reserved here. For example, a database table could be added to allow a user to be assigned an authorization score during enrollment, such as 0 for user and 1 for admin.

Version 2019 of visual basics community edition will be used to attempt to maintain future compatibility if possible, without having to re-encode the system in a new version of visual basics. If I adopt the java program language, the Java SE Development kit 13 will be used; again, to main maintain future compatibility. However, should the Neurotechnology SDK’s suffer any compatibility issue with the newer versions of the visual basics IDE, or the program language I adopt, I reserve the right to downgrade this to older versions to remove any potential compatibility issues with the Neurotechnology SDK’s.

My program will be designed to enroll users from file and individually. Individual enrollment will be handled manually. The program will also offer identification with facial recognition via the FacesAlgorithimDemo.exe application and finally Verification with the IresesAlgoritimDemo.exe program. Verification will only be complete if a user is found and verified.

The threshold for facial recognition may be increased slightly for added security, and the threshold for iris will be increased slightly for heightened security. The exact numbers will need to be tested during implementation to balance usability and acceptability while maintaining relatively low FTE and FAR numbers.

Finally, should time allow for it, the optional requirements, such as the addition of an authorization attribute could be investigated. This will necessitate the use of a relation database system such as MySQL to create a authorization attribute table. Should the attribute be gated behind a password requirement a second password table will be required with passwords being hashed and salted,

## 3.2 Technical Specification

My application will be built upon the Visual Basics Platform. The system will be an ‘AND’ based system within my code. This means that for a user to be deemed to be fully verified and access authorized, the user must have been identified via facial biometrics AND verified via iris biometrics.

This will be performed with either a C family programming language or the Java language. I reserve the right to make this decision later, depending on the fullness of compatibility of java within the visual basics IDE platform.

The Biometrics will be carried out via the Neurotechnology FacesAlgorithimDemo.exe and IrisesAlgorithimDemo.exe.

Any testing will be Carried out either in Visual Basics or Eclipse for extended unit testing. White box testing will be carried out by myself, and black box testing will be carried out by a fellow student who will not get to see my code before testing.

The basic system structure will be as follows:

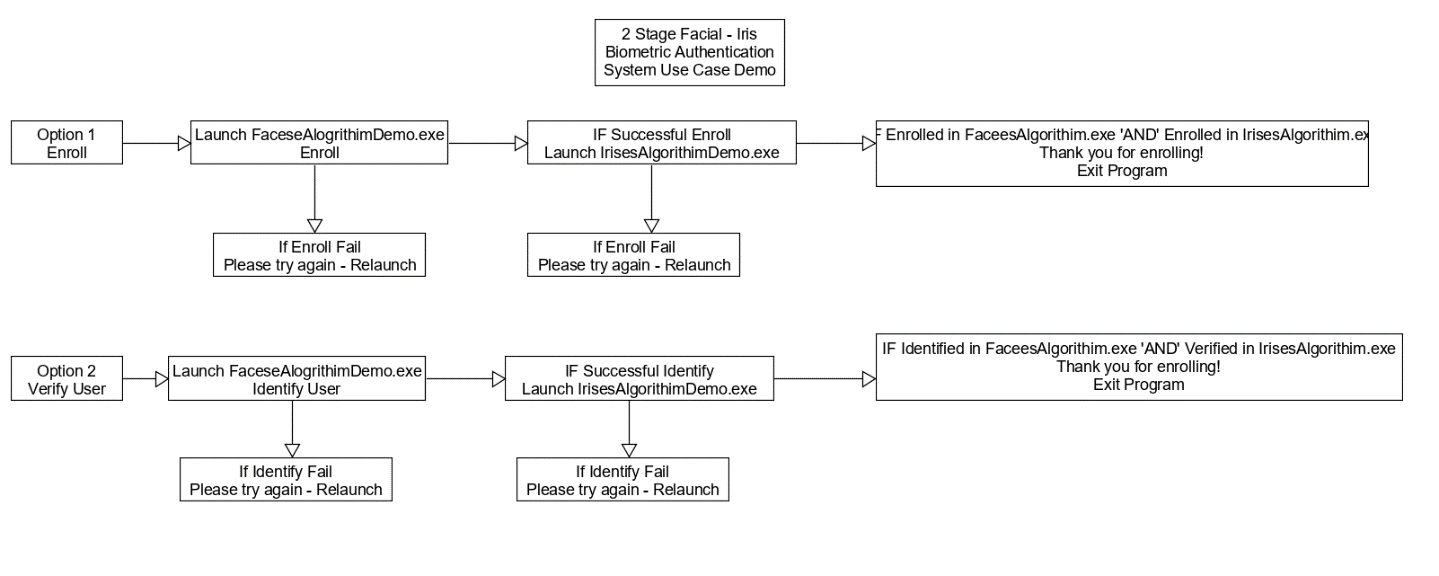


Figure My simple Use Case Breakdown of my Biometric system.

So, as we can see above, the user will have 2 options. Option 1: Enrollment & Option 2: Verification.

Should the User select option 1, the user will attempt to Enroll with FacesAlgorithimDemo.exe. If the user fails to enroll with FacesAlgorithimDemo.exe, the process will be restarted.

If this enrollment initial enrollment is successful, the user will then attempt to enroll with IrisAlgorithimDemo.exe. Should this second enrollment be unsuccessful the second enrollment process will begin again.

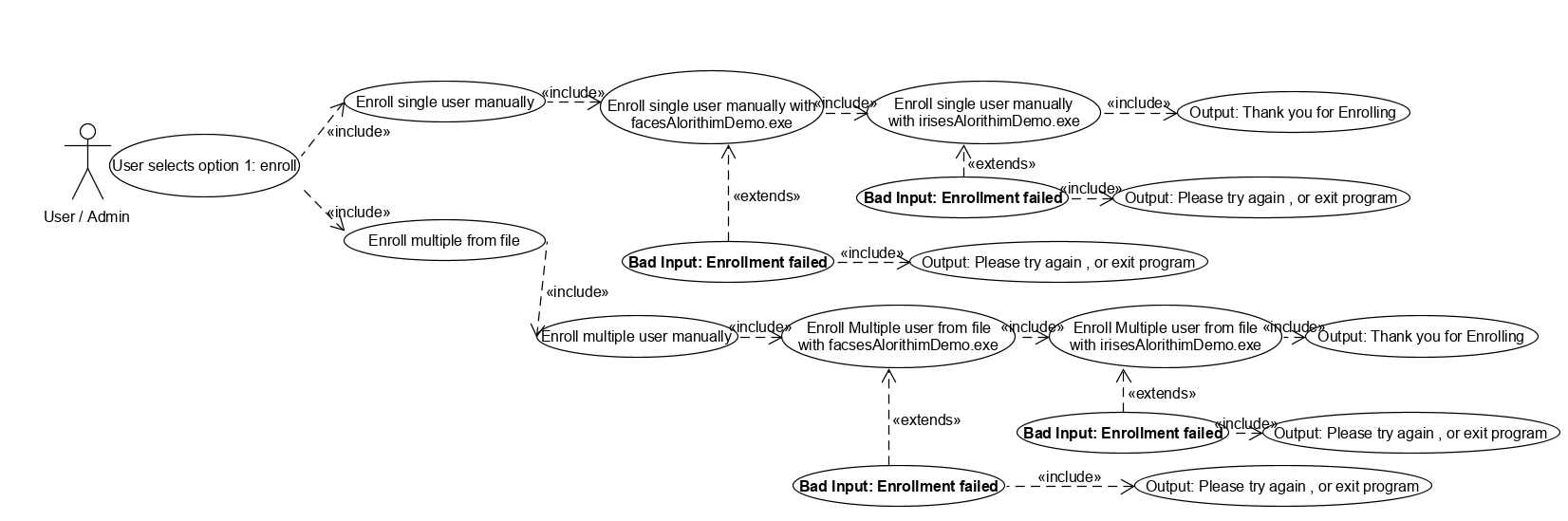


Figure Extended Use Case Diagram for Option 1: Enrollment, with basic error correction documented.

Should both enrollments be successful, the user is deemed enrolled on the database and the program is exited.

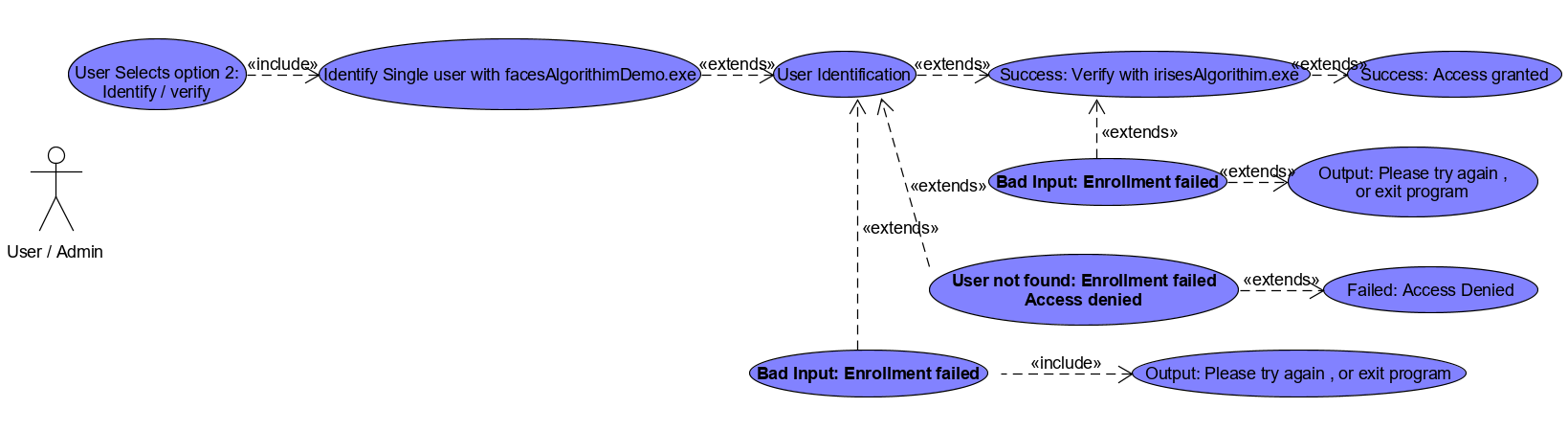


Figure Extended Use Case Diagram for Option 2: Identification / Verification, with basic error correction documented.

Should the User select option 2, the user will attempt to Identify with FacesAlgorithimDemo.exe. If the user fails to Identify with FacesAlgorithimDemo.exe, the process will be restarted.

Should the User not be found in the Database, the entire verification is rejected, and access is denied.

If this identification is successful, the user will then attempt to verify with IrisAlgorithimDemo.exe. Should this verification attempt be unsuccessful the verification process will begin again.

If the verification fails, the identify/verification is rejected, and access is denied.

Should both identification ‘AND’ verification be successful, the user is verified, and access is granted.

# 4.0 Testing

Testing will be done in sections, screening each mode of the multimodal system for levels of FTE, FAR & FRR. This will also involve the uploading of sample databases for the purposes of enrollment and identification / verification testing. The thresholds may need to be adjusted to reach a suitable level of each.

A limited amount of white and black box testing will be performed as well as some unit testing to determine that each function of the program and error handling is working correctly. API implementation testing will be conducted on an ongoing basis during development with final testing be conducted during FTE/FAR/FRR testing. This may involve taking a sample of our database (for example, 100 users) and attempting to identify/verify each of these users a preset number of times, for example 500 times each and preparing a table of individual biometric mode scores as well combined multimodal scores to determine if our FTE/FAR rates are acceptable.

Optional:

For testing purposes, a script may be written, or added that will conduct extensive tests by attemptingto enroll, identify and verify multiple users, multiple times, from a file. Or these tests may be conducted manually, depending on what time allows for during the development life cycle implementation phase of the program design.

# Conclusions

When designing a biometric system, we must consider firstly the 7 main characteristics of any biometric system, as discussed by Chen le; as well as the functionality of the system [7].

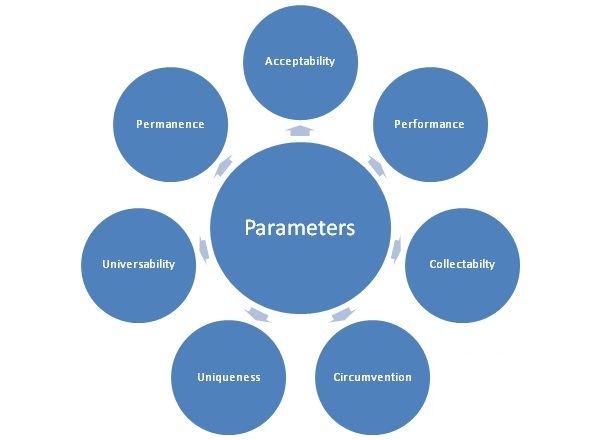


Figure The 7 Characteristics of Biometrics, taken from the chapter Introduction to Biometrics and Biometric Security Systems’ [6].

As we can see above, we must consider acceptability. I believe that in combining Face recognition and Iris Recognition I have chosen two biometrics that have the same level of acceptability and complement each other. Next, we must consider performance. Again, both systems have a very good level of performance, and even adding some extra conditional checks of my own code will not impede the performance of these two biometrics operating side by side.

In terms of collectability, Facial data is easy to collect. However, with my available technology, it is fair to say that Iris reduces the level of collectability somewhat, by having the user hold the scanner up their eyes. More modern technologies do remove this small issue however, reducing the level of interaction to a bare minimum. So, while my available technology does reduce collectability by a small factor, modern technology would negate this, in fact, modern technology affords Iris recognition on mobile devices, as discussed by Peter Corcoran (et al) in is 2015 paper, ‘Iris authentication in handheld devices - considerations for constraint-free acquisition’, as well as Irish at distance [8].

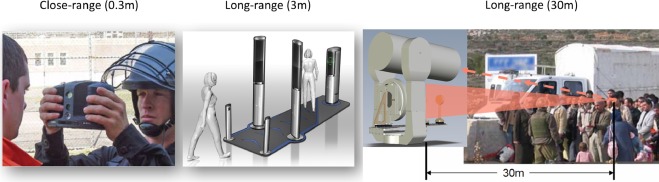


Figure Visual samples of Iris at distance low interaction technology in action.

As discussed earlier, facial biometrics do have a somewhat dimple circumvention factor, but this is negated by the complex circumvention factor of Iris biometrics. Similarly, this same interaction is reflected in uniqueness. While face biometric data is unique, Irish data biometric data is more intricate while also being unique. This affords a high level of confidence in security where both circumvention and uniqueness are considered.

As funny as it may be to say, everybody has a face, and everybody has eyes. But what about in cases where a user may have facial disfigurement due to medical complications, an accident or other factors. While this will of course contribute to uniqueness, it will cut down confidence in facial matches due to less acceptable data being available. In such cases, the iris would act as a failsafe fallback putting confidence back into verification. This could also work in cases where a user is blind or suffers from another form od visual ailment that may discolor or otherwise inhibit the collection of data from the iris, in such cases, Facial data acts as the fallback.

Universality is an interesting factor. And one I think yet again adds feasibility and validity to my choices. The human face is normally universal. But what about Identical twins? Well here we run into a problem in facial recognition. However, since facial recognition is only being used for Identification, twins do not present a problem in my system. Since I would expect both twins to have identified separately, but potentially be identified as both twins, I only require them to be found in the database. Iris on the other hand is fully universal. With so much data in the Iris, it is almost an incredibly low likelihood that two irises will be even close enough to be a match, where a match should not be found. For this reason, I feel my system removes a known problem, all be it a small argument, against using facial recognition; and this negation supports my multimodal system.

Neither the face, nor the Iris are permanent. Over extended periods of time we would expect to see changes. Perhaps a discoloration of the Iris. And of course, the face will age. However, since the Iris is converted into greyscale, this discoloration will have a minimal affect of the validity of Iris data. And the Face will, under normal conditions taken many years to age to the point where data will not be viable. For these reasons I feel that facial and Iris data can be considered permanent with a recommendation for re-enrollment every 5-10 years.

I believe my system is viable, feasible and solves some known issues with simple biometric systems who affording a comfortable level of acceptability, reliability, and security.

# 6.0 Glossary

FTE: Failure to enroll.

FAR: False acceptance rate.

FRR: False rejection rate.

Threshold: The level of acceptable data upon which a biometric match can be made, after which a scan attempt is rejected.

Multimodal: A biometric system involving more than 1 mode of biometrics.

API: Advanced programming Interface.

IDE: Integrated Development Environment.

SDK: Software Development Kit.

# 7.0 References

1. N. Merhav, ‘False–Accept/False–Reject Trade–offs for Ensembles of Biometric Authentication Systems’, IEEE Xplore Digital Library - IEEE International Symposium on Information Theory, 2019, [ONLINE] Vol 1, issue 1, page 1 – ‘Introduction’, 2019, Available at: https://ieeexplore.ieee.org/document/8849726?arnumber=8849726&SID=EBSCO:edseee [Accessed Nov 14th, 2019]
2. A. Babu (et al), ‘An investigation of biometric liveness detection using various techniques’, IEEE Xplore Digital Library - International Conference on Inventive Systems and Control (ICISC) 2017, [ONLINE] Vol 1, Issue 1, page 1-3 – ‘Introduction’, 2017, Available at: https://ieeexplore.ieee.org/document/8068745?arnumber=8068745&SID=EBSCO:edseee [Accessed Nov 14th, 2019]
3. T. Fladsrud & R. Sollie, ‘Circumvention of ﬁngerprint scanners’, ResearchGate January 2005, [ONLINE] Vol 1, Issue 1, page 5 – 9, ‘Counterfeiting Fingerprints’, December 15, 2004, Available at: https://www.researchgate.net/profile/Tom\_Fladsrud/publication/228939679\_Circumvention\_of\_fingerprint\_scanners/links/0deec52822d2d8a08e000000/Circumvention-of-fingerprint-scanners.pdf [Accessed Nov 14th, 2019]
4. C. Franklin Jr., ‘Researchers Show Vulnerabilities in Facial Recognition’ DARK READING, July 8th, 2019, [Online] Available at: https://www.darkreading.com/vulnerabilities---threats/researchers-show-vulnerabilities-in-facial-recognition/d/d-id/1335471 [Accessed: Nov 14th, 2019]
5. Nuance, ‘The Security Value of Voice Biometrics’, July 8th, 2019, [Online] Vol 1, Issue 1, pages 6 – 10, ‘Why voice biometrics provides a superior security solution over PINs or agent security questions’ July 8th, 2019, [Accessed Nov 14th, 2019]
6. V. R. E. Chirchi (et al), June 2011, ‘Iris Biometric Recognition for Person Identification in Security Systems’, [Online] Internation journal of Computer Applications Vol 24, page 1, ‘Introduction’ - Iris Scan, June 2011, [Accessed: Nov 14th, 2019]
7. C. le, under the guidance of Prof. R. Jain., November 28th, 2011, ‘A survey of Biometrics Security Systems’, [ONLINE] Vol 1, Issue 1, page 2, ‘Introduction to Biometrics and Biometric Security Systems’, November 28th, 2011, [Accessed: Nov 14th, 2019]
8. P. Corcoran (et al), May 2015, ‘Iris authentication in handheld devices - considerations for constraint-free, [Online] Vol 1, Issue 1, page 1, ‘Introduction’, May 2015, [Accessed: Nov 14th, 2019].