Facial Recognition Access Control System
Research Manual
by

Hoda Ahmed;
Student ID: C00214991

April 17, 2020

Abstract

Companies and organizations often overlook the importance of physical security to equipment rooms due to the increase of cybercrime and the emphasis that cybersecurity industries put on cybercrime. This report discusses the importance of physical security to equipment rooms and proposes a solution to fix this flaw: The Facial Recognition Access Control System. Facial recognition is the future, and it has already started being implemented in most places for security, criminal identification, law enforcements and even social media where users can upload photos of other people and tag them.

Contents

1 Introduction **1**

2 Topic Area **2**
2.1 Overview of Biometrics 2

3 Types of Physiological Biometric Authentication **3**
3.1 Facial Recognition Technology Through History [19][20][21][22] 6
3.2 Artificial Intelligence, Machine Learning & Neural Networks 8
3.2.1 Usage in Facial Recognition Technology 10

4 Similar Applications **13**

5 Technology Stack **14**
5.1 Software Technologies 14
5.1.1 Face Recognition API 14
5.1.2 Desktop Application[44] 14
5.1.3 Web Application, Server & Database 16
5.1.4 SMS Authentication (Twilio) 16
5.1.5 Mobile Application 17
5.2 Hardware Technologies 17

6 Conclusion **18**

1 Introduction

"Face recognition is one of the newer developments of biometric identifiers that doesn't require as much time or intrude on the person its verifying." [1]. This research report focuses on the research carried out to design, implement, and display the Facial Recognition Access Control System project. With the increase of cybercrime, companies are often overlooking the threats of insecure physical access to equipment rooms (e.g. server rooms). Physical security helps "protect assets, including IT infrastructure and servers [of companies], that make their businesses run and that store sensitive and critical data" [2]. Not only does it also "encompasses measures and tools like gates, alarms and video surveillance cameras, but [it] also includes another central element: an organization's personnel". Essentially, fostering a culture of physical security is just as crucial as investing in technology to help secure the company from the cybersecurity perspective.

This project focuses on securing equipment rooms in companies by limiting access to them with the help of facial recognition. Only authorized persons should be allowed to enter equipment rooms and all access to these rooms should be logged to be examined by administrators when needed. This research report explains the idea behind the Facial Recognition Access Control System in minute details, focusing in on motivation behind using this method for authentication, the purpose of the project and the final solution to it.

The report also examines the different technologies that were researched and the finalized decisions on which technologies to use, both in the hardware, the software, the frontend and the backend categories. It also examines some applications that exist in the industry that are similar to the Facial Recognition Access Control System project. The report finally concludes with a clear set of requirements and an unambiguous understanding of the project's implementation and design.

2 Topic Area

"Biometrics is a growing technology, which has been widely used in forensics, secured access and prison security" [3]. As mentioned in the previous section, companies are focusing more on securing their digital systems against recently rising cybercrime and attacks, like ransomwares or DDoS attacks, that they often disregard the significance of keeping their equipment rooms secure.

2.1 Overview of Biometrics

Biometric (Bio-Life and metrics-measure) [4] -based authentication systems are believed to be more reliable than traditional systems that use the common 'username-password' combination or even keys or ID cards that can easily be lost or stolen or forgotten. This is because the performance of biometric-based systems operates based on a person's physiological and behavioural characteristics, which are secure and authentic for most of the time. [5]

There are two types of biometric attributes: physiological and behavioural. physiological biometric attributes are essentially derived from a physical attribute of a person [6]. Face is an example of physiological biometric attribute, and there are many other physiological biometric methods through which authentication can take place, like fingerprint, retinal/iris scans, voice or even finger vein geometry. Sometimes even a person's heartbeat can be used for biometrics, and in fact it is believed to be a more efficient authentication mechanism as it can't be faked, unlike other biometric authentication methods [7].

In contrast to physiological biometric attributes, behavioral biometric attributes depend on a person's action to habits to uniquely identify that person. Examples of behavioral biometrics include signature recognition, keystroke dynamics, gait (the unique way a person walks) and general physical human gestures [8].

3 Types of Physiological Biometric Authentication

This section will focus on 3 types of physiological biometric authentication mechanisms and will outline why they were not the chosen biometric for this project, and why facial recognition was chosen instead.

- **Fingerprints:** Because of a fingerprint's uniqueness, universality and accuracy, it is currently in the lead in most biometric authentication systems[9]. Fingerprints are tiny ridges, whorls and valley patterns on the tip of each finger. The formation on these fingerprints depend on the initial conditions of the embryonic mesoderm from which a human develops. Because of its widespread usage and its un-novelty, it was not chosen as the biometric authentication mechanism for this project.

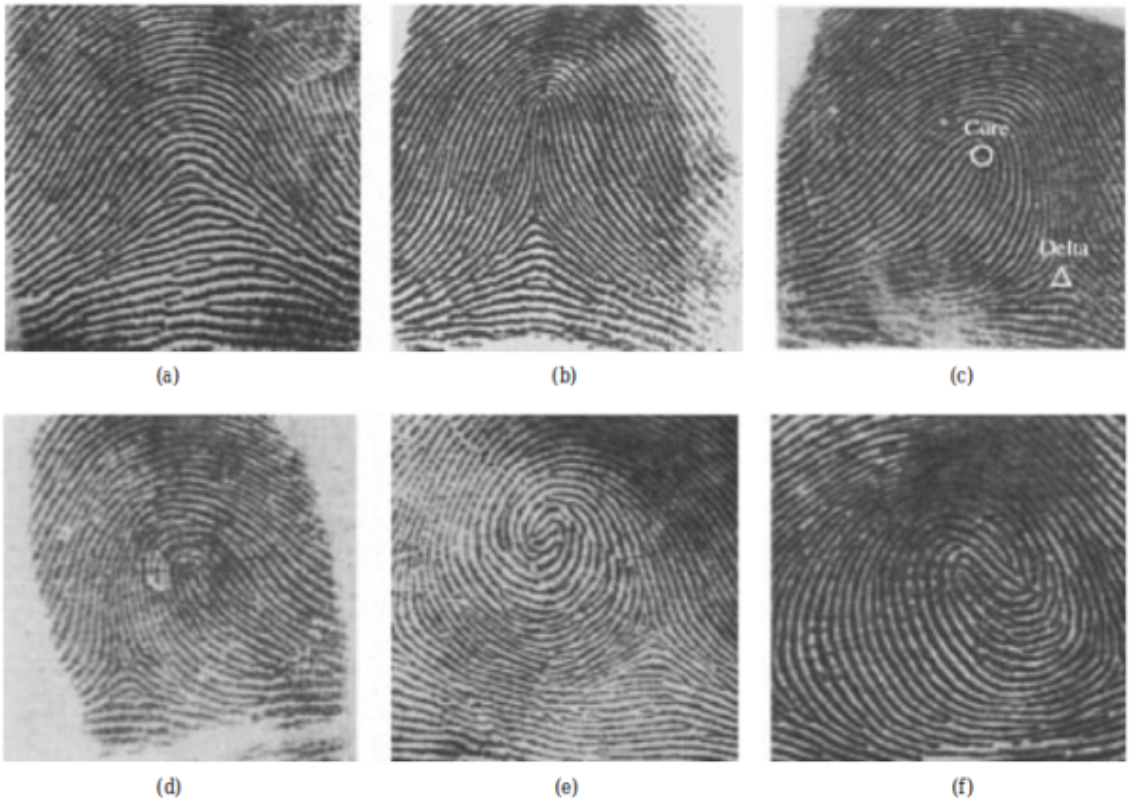


Figure 1: Fingerprints and a fingerprint classification schema of 6 categories: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop. Critical points in a fingerprint, called core and delta, are marked on (c) [10]

- **Finger Vein:** This is a new hidden biometric trait that can be used for authentication. This method works by passing an infra-red light through the finger, which is absorbed by the haemoglobin of the blood, displaying dark black lines (the vein) [11]. An advantage to this method is that finger vein structure is not seen by normal human sight, so it is very hard to forge or manipulate [12].

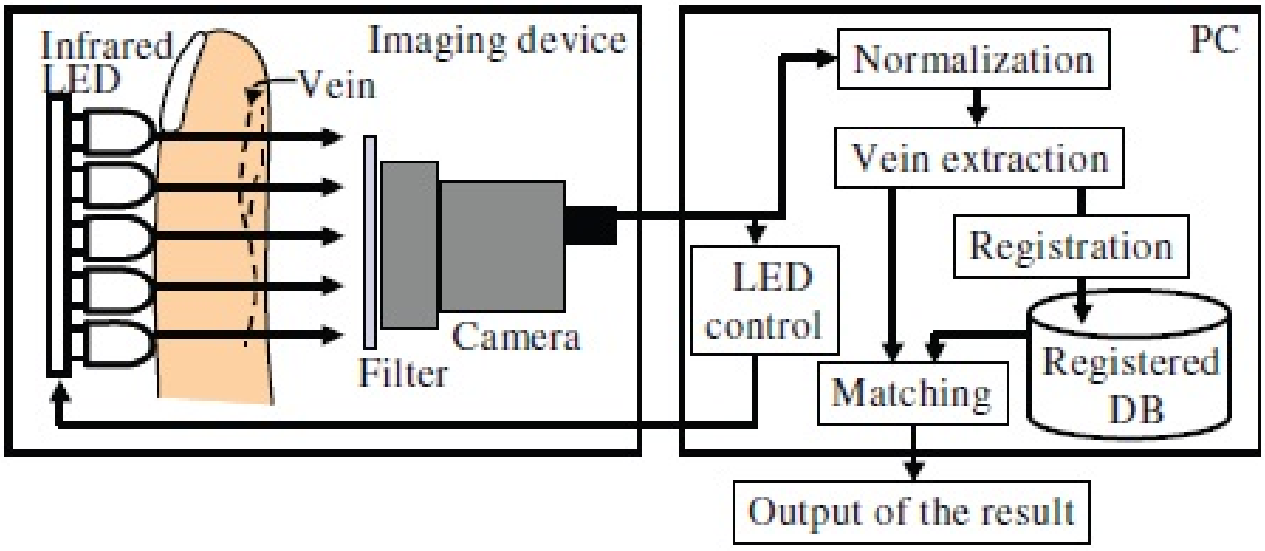


Figure 2: Process by which finger vein authentication takes place [13]

- **Retinal Scan:** Although retinal scans are one of the most efficient methods for biometric authentication it is still one of the least deployed for several reasons, with the most obvious reason is the concern regarding health exposure. Retinal scans can reveal information regarding a human's illnesses, hereditary diseases and sometimes even pregnancy, so people tend to view this scan as very intrusive for an authentication mechanism [14]. Retinal scans are performed by casting an unperceived beam of low energy infrared light into a person's eye as they look through the scanner's eyepiece. This beam of light traces a standardized path on the retina, which helps the scanner device capture a retinal image which then assists with compiling the unique features of the retinal blood vessels networks into a template [15].

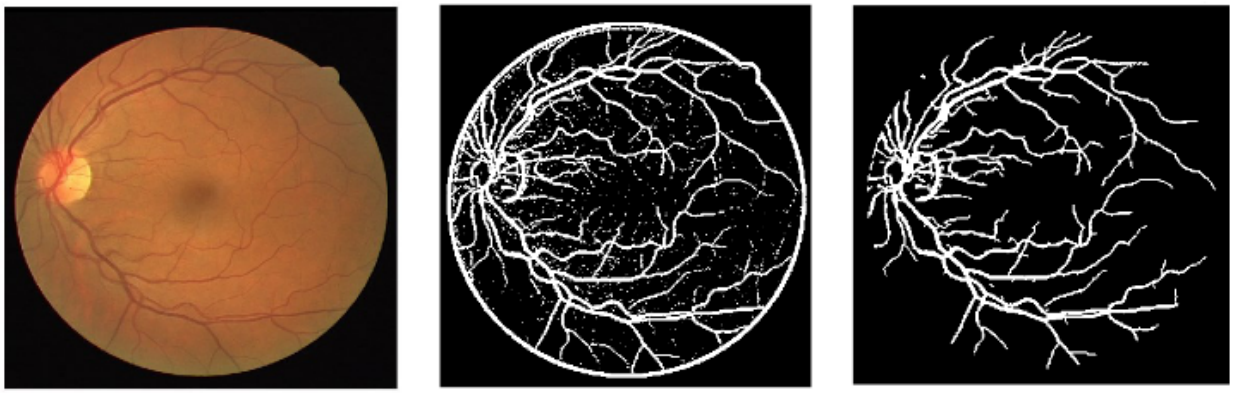


Figure 3: Retinal scan process: (a) Original image; (b) Edge detection in noisy image; (c) Noise removal. [16]

While researching the above 3 types of biometric authentication I have learned of their advantages, but I also learned of some disadvantages or limitations that discouraged me to implement them in my biometric access control project. These advantages and disadvantages are outlined in the table [17] below.

Table 1: Comparison of Various Biometric Authentication Methods

Biometric Measure	Advantages of Use	Disadvantages of Use
1. *Fingerprint*	• Easy to use • Non-intrusive • Low cost • High accuracy	• Affected by skin condition • Sensor might get dirty/unhygienic
2. *Finger Vein Structure [18]*	• Non-invasive • Reliable and highly accurate	• Complex procedure • High cost
3. *Retinal Scan*	• Very high accuracy • Long-term stability, therefore, user only needs to enrol once	• Very intrusive - state of health can be detected/exposed • High cost • Limited Applications

Researching the above methods encouraged me to do more research on face recognition access control systems, as they are the secure solution that is non-intrusive and hygienic at the same time, and not very costly when compared to other biometric solutions.

3.1 Facial Recognition Technology Through History [19][20][21][22]

The very beginning of facial recognition technology was in 1964 when the mathematician and computer scientist Woodrow Wilson Bledsoe developed a system that could classify photos digitized by hand using a RAND tablet [See Fig. 4 below]. This was a device that could be used to input vertical and horizontal coordinates on a grid using a stylus that emitted electromagnetic pulses. Coordinate locations of several facial features were manually recorded in this system, then they would be stored in a database. After this, once a user provided the system with a new picture of an individual, it was able to get the image from the database that most resembled the provided picture.

Although the technology at that time was limited and computer processing power was not as great, it was still a very important step in facial recognition technology.

Figure 4: RAND Tablet[1]

A few years after, 21 facial markers were introduced to assist the automated face recognition. Computer scientists Goldstein, Harmon and Lesk used 21 specific subjective markers that included lip thickness and hair color to help automate the recognition. The locations and measurements still needed to be manually put into the computer, causing the program to require a lot of labor time. Regardless of the issue, the accuracy was still better when compared to the RAND Tablet technology.

Nearly a decade later, in 1988, scientists Sirovich and Kirby started implementing the use of linear algebra for facial recognition [23], and this is known today as the Eigenface approach. The two scientists were able to show that the feature analysis on a group of facial pictures could establish a set of basic features.

Later, in 1991, Turk and Pentland extended the study of the Eigenface approach and discovered how to detect faces within images. This was revolutionary as this was the step that led to the first instances of automatic facial recognition [24].

From 1993 to the start of the 2000s, the Defense Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology introduced the Face Recognition Technology (FERET) program to help encourage face recognition in the commercial market. The goal of this program, according to NIST, "was to develop automatic face recognition capabilities that could be employed to assist security, intelligence, and law enforcement personnel in the performance of their duties."[2]

[1] https://www.wired.com/wp-content/uploads/2015/01/rand.jpg
[2] https://www.nist.gov/programs-projects/face-recognition-technology-feret

Following the FERET program, other institutes started developing and improving automatic facial recognition algorithms for commercial availability. For example, NIST began Face Recognition Vendor Tests (FRVT) in early 2000s, which were built on top of FERET [25].

From there onwards, several facial recognition algorithm tests were evaluations and were becoming available for further development by other institutes and technological companies (e.g. FRGC). In 2010, facial recognition was implanted in social media platforms, especially Facebook and its photo tagging feature. This feature allowed users to tag a photo and the system will automatically recognize the face of everyone in the photo, only if they exist on the Facebook platform.

After further developments in the facial recognition sector in Facebook, the photo tagging photo was improved so that the Facebook system would be able to identify a person in a picture even if they're not tagged [26] This development is due to the implementation of machine learning and neural networks in facial recognition technology. In fact, Facebook has a dedicated system for deep learning facial recognition, called DeepFace. This system employs a nine-layer neural network with over 120 million connection weights and was trained on four million images uploaded by Facebook users [27].

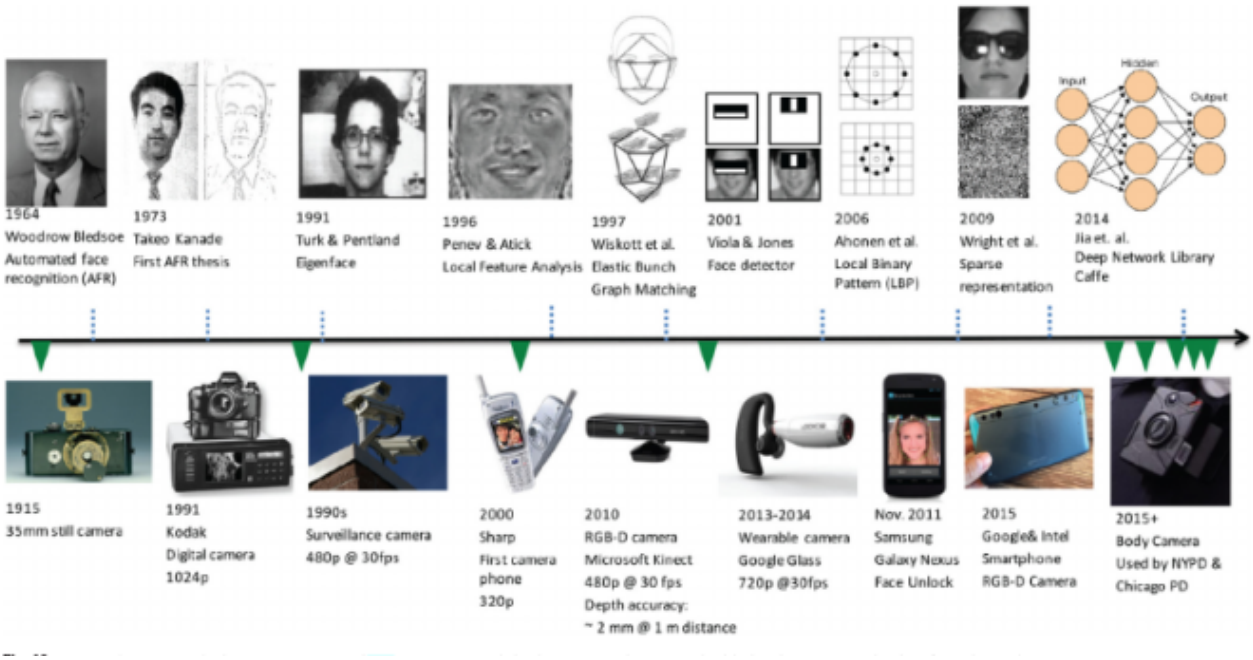


Figure 5: Facial Recognition Technology Timeline [28]

3.2 Artificial Intelligence, Machine Learning & Neural Networks

When Machine Learning (ML) or Artificial Intelligence (AI) are mentioned, Neural Networks (also known as Artificial Neural Networks or ANN) come to mind. Essentially, AI is the bigger picture of this whole technological sector, and only a subpart of it is ML, and a subpart of ML is ANN.

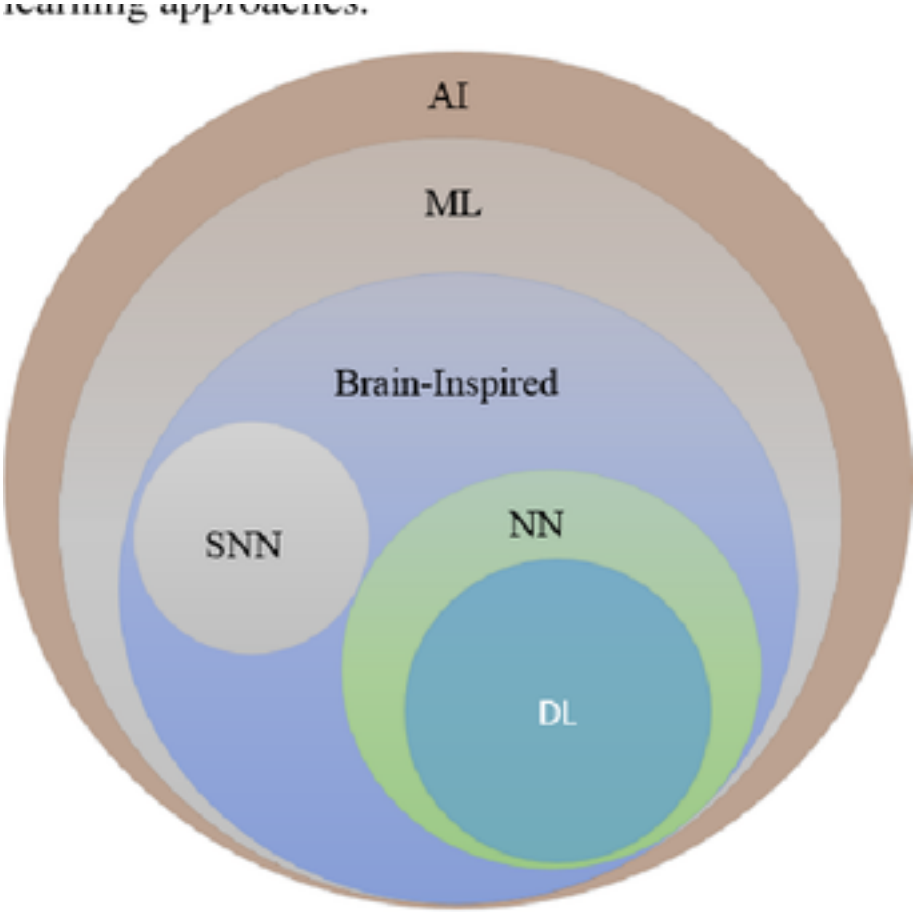


Figure 6: Relationship between AI, ML & ANN [29]

There are 4 types of learning in machine learning: supervised, unsupervised, semi-supervised and reinforcement, However, for facial recognition, the type of learning that is used is supervised. "Supervised learning is when the model is getting trained on a labeled dataset." [30]. It is a method used to enable machines to classify object, problems or situation based on related data "fed" into the machine. These machines are fed with "data such as characteristics, patterns, dimensions, color and height of objects, people or situations repetitively until the machines are able to perform accurate classifications." [31].

ANN are computers whose architecture is designed after the human brain. They typically consist of hundreds of simple processing nodes that are wired together in a complicated network of communication. Each node or unit is a simplified model of a real human brain neuron that send off a new signal or fires if it receives a sufficiently strong input signal from the other nodes or units to which it is connected [32].

To understand neural networks further, we can consider them to be classifiers (which is a type of supervised learning) [30]. Their main aim is to sort objects that are taken in (inputs) and place them in their corresponding classes that were predetermined, which is the output (terminology not to be confused with Object-Oriented programming classes). This classification is used in many applications, for example, this project; image processing. Specifically, for this project, we seek to

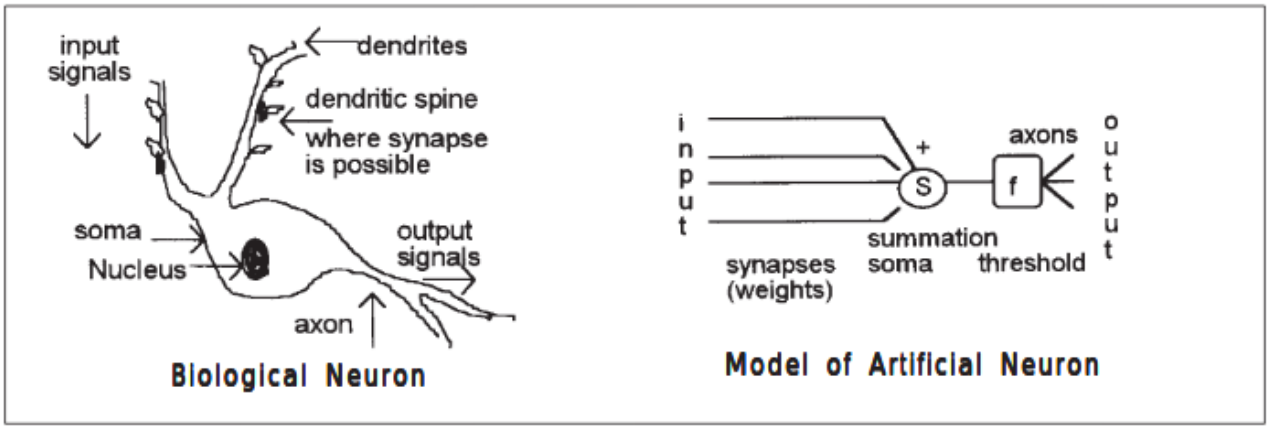


Figure 7: Similarities Between An Artificial Neuron and a Real Brain Neuron [33]

distinguish images depicting different persons. Other applications include natural language processing (NLP), where we may seek to classify texts into categories (e.g. talks about politics, sports, music etc.), or even email classification (Gmail classifying mails in classes like social, promotion, updates etc.) [34] [35].

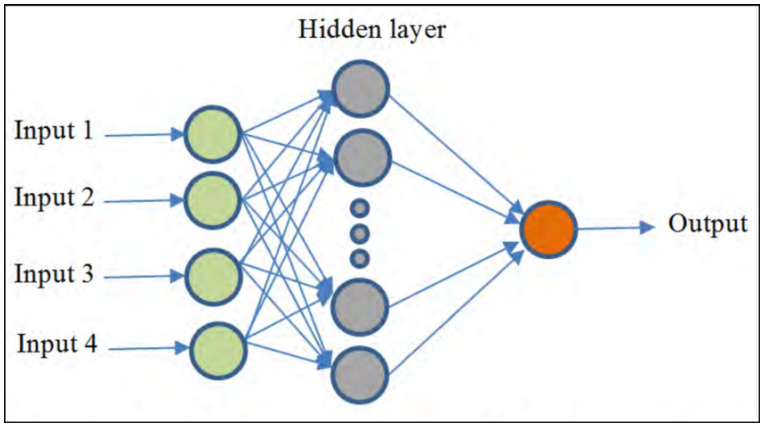


Figure 8: Example of a simple artificial neural network [36]

These networks are beneficial as they are learning to perform tasks that the human brain can carry out. For the sake of this project, an example would be training a neural network to identify heads in a picture. The system is trained by manually marking heads in pictures and "feeding" the system with images that contains no head, and then using the trained network to identify whether heads exist in other images or not.

3.2.1 Usage in Facial Recognition Technology

The following figure summarises how neural networks are used in facial recognition technology:

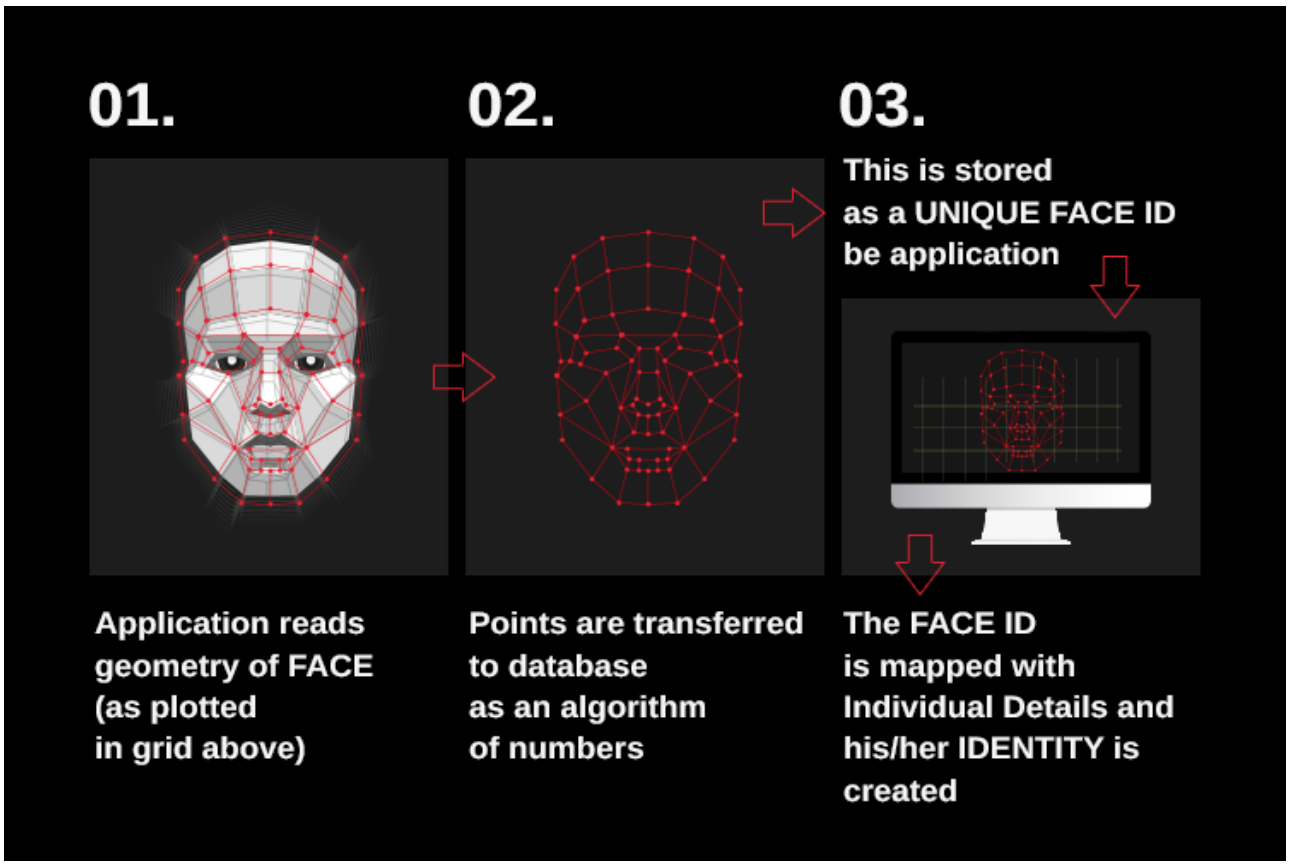


Figure 9: Process of Facial Recognition Algorithm [37]

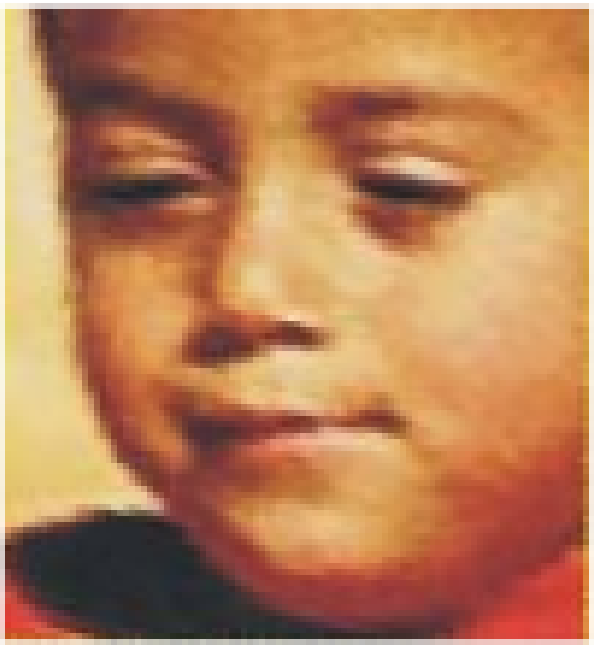
The first step in using machine learning in facial recognition technology, is the machine's ability to detect a face in an image. Provided with an image (or even a videostream), the algorithm must detect[38] the face(s) in that image. This step is not necessarily machine-dependent, meaning a human can carry out this step.

The second step is face alignment, where the face is "normalized" to be consistent with the database. For example, geometric normalization forces the face to be aligned vertically (see Figure 10 below). There is more than one normalization type e.g. light normalization, head rotation normalization, face expression normalization and even elimination of occlusions like glasses/beards or other obstacles that may cover the face.

(a) Original Image

(b) Face Detected

(c) Face Geometrically Normalized



(d) Result

Figure 10: Geometrical Normalization Process [39]

Normalization usually prepares the face(s) for the next step in the process: facial extraction. "The goal of normalization is to change the values of numeric columns in the dataset to a common scale, without distorting differences in the ranges of values. For machine learning, every dataset does not require normalization. It is required only when features have different ranges." [40]

Facial extractions and extract its/their features. These features can be - but not limited to - the following characteristics: [41]

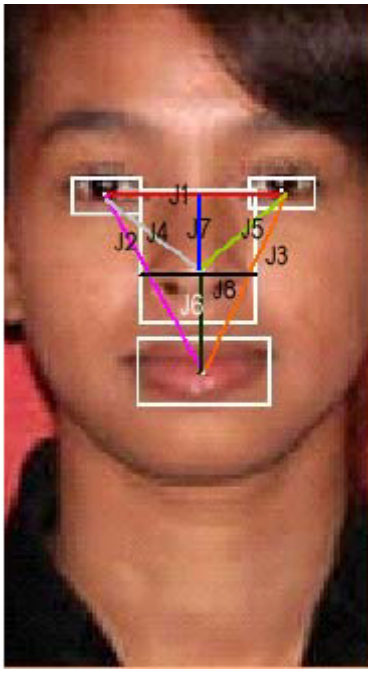


Figure 11: Facial Features Extraction[41]

- J1 - distance between middles of the eyes
- J2 - distance between middle of the left eyes and middle point of mouth
- J3 - distance between middle of the right eyes and middle point of mouth
- J4 - distance between middle of the left eyes and middle point of nose
- J5 - distance between middle of the right eyes and middle point of nose
- J6 - distance between middle point of mouth and middle point of nose
- J7 - distance of middle point of J1 and middle of nose
- J8 - width of nose

These features are then transferred to a database as an algorithm of numbers, where actual facial recognition methods can be carried out on the face e.g. face matching, similarity, verification & identification [42].

For the purpose of this project, only a brief understanding of neural networks should suffice. Due to the nature of limited time for the project's implementation, a self-implemented neural network model is not possible. Therefore, the use of existing facial recognition APIs will take place instead (a comparison of existing facial recognition APIs is included in the Backend Technologies section below).

4 Similar Applications

This project is not the first to implement the idea of securing physical access using facial recognition. In fact, there are a few applications that already exist in the market that companies can implement. The following table examines each application and outlines what it offers.

Table 2: Similar Applications That Provide Facial Recognition Access Control Systems

Application	**What is being offered**
FaceFirst[3]	• Facility security • Authentication • Event access • Surveillance
ActionFirst[4]	• Access control • Building security • Loss prevention • Security audit trails
Herta (BioAccess)[5]	• User management at runtime • Allows users to be enrolled on-the-fly by video capture
FaceKey[6]	• Automatic light correction • Centralized enrollment

The only difference between the mentioned existing systems and the one I will be creating is that scope. The existing systems offer facial recognition access control as part of a whole monitoring suite, whereas in my project, only room access control will be designed and completed.

It is also worth noting that the existing systems in the market store the images that are captured by the systems for logging, monitoring and statistical purposes. This is not the case for my facial recognition access control system, as no images are stored beyond the point of confirmed authentication (i.e. whether the person is authorized to enter room or not). The image is stored only for the duration of the facial detection, analysis and feature extraction. After this, the image is erased completely so that no personally identifiable information (PII) is kept for longer than required, and for respecting the privacy of the users as well.

5 Technology Stack

A lot of different technologies are encapsulated together to produce the facial recognition access control system. It is also worth mentioning that there will be both software and hardware technologies used in the project, they are all examined in the sections below.

5.1 Software Technologies

5.1.1 Face Recognition API

As mentioned above, a facial recognition API will be used. After a lot of research for face recognition API, the options were limited to only 3, Kairos Facial Recognition, Amazon AWS Rekognition API and Microsoft Azure Face API. The table below shows a comparison between the two and the finalized decision on which API will be used.

Table 3: Comparison of Different Facial Recognition APIs

	Kairos Facial Recognition [43]	**AWS Rekgonition**	**Microsoft Azure Face**
Cost	No free option - Cheapest option (Student Offer): $19 /month + 0.02 /transaction	Free option for • Analyzing first 5,000 images /month and • Storing 1,000 metadata /month	Free option for 30,000 transactions /month.
No. of Faces Allowed (Analyzing & Storing)	Not shown, but not unlimited	• Analyzing: 5,000 • Storing: 1,000	Depends on the 30,000 transactions per month
Ease of Integration	API documentations found online	API documentations found online	API documentations found online

5.1.2 Desktop Application[44]

A desktop application will be designed which the users will interact with to use the system. This desktop application will be installed on the hardware device (Raspberry Pi or Arduino) which the API calls will be made from.
Many desktop applications can be created using C/C++, Java, Python and even JavaScript. Determining the language used to design the desktop application will depend on the operating system running on the hardware device. After doing research, it seems that Python is the most suitable language to use to design the desktop application. This is for a number of reasons:

- Python is a lightweight programming language, which is useful as a very small application is needed to be used on the hardware device.[45]
- Python is cross-platform and can run on any operating system.
- Python provides a lot of UI frameworks and toolkits that can be helpful for designing the user interface.

There are a number of available frameworks that can be used to develop desktop application using Python. The most common of these are PyQt, wxPython and TKinter.
A quick comparison of the three frameworks is outlined in the table below.

Table 4: Comparison of Different Python Desktop Application Development Frameworks

Framework	**Description**
PyQt[46]	• Many learning resources available • Stable - used in many large-scale applications • Has a steep learning curve, but very flexible • Has a UI Builder available • Cross-platform
wxPython[47]	• Large library of widgets • Very flexible. • Requires downloading and installing (not included with Python). • No reliable UI builder available (equiv. to Qt Designer)
TKinter[48]	• Included in the standard Python library • Fast • Easy to learn and learning curve not as steep as other frameworks • No reliable UI builder available (equiv. to Qt Designer) • No advanced widgets (e.g. date picker)

After examining the above table, I have come to the conclusion that PyQt is the best framework to be used to develop the desktop application. Although it has a steep learning curve, the various learning resources available and the UI builder can help me overcome this and make learning it more fun and enjoyable.

5.1.3 Web Application, Server & Database

Since there will be a user login functionality and a logging functionality in the project, there needs to be a database to store user information, logging information and a portal for administrators to view and access these logs. Hence, web application development technologies will be used. To get the most value out of the project, the web application (website) will be designed from scratch. As the web application will also be running on the hardware device, it is important that it is lightweight and suitable for the chosen device. This means that, like the desktop application, the web application will be designed using a Python web development framework. There are a number of Python web development frameworks that can be used for the development of the facial recognition access control system website. This includes Django, Flask and Pyramid. A comparison table is outlined below to examine the advantages and disadvantages of each and a conclusion as to which one will be used is provided.

Table 5: Comparison of Different Python Web Development Frameworks

Framework	**Description**
Django	• Released in 2005 • Designed for large, complex and high-load web apps • Has a steeper learning curve • Has lots of built-in features & modules, making it quite heavy and not as flexible
Flask	• Released in 2010 • More suited to small, light-weight & less complicated web apps • Minimalist & simple, offers better flexibility & control
Pyramid	• Released in 2008 • Suited for later-to-be complex web apps • Very easy to customize • The most complicated of the three web development frameworks

Looking at the above comparison table, it is obvious that **Flask is the best choice** of the three, for more than one reason. Flask is lightweight, which is perfect for running on the hardware device. Bootstrap, a simple and flexible HTML, CSS, and JS for popular UI components and interactions, will be used with Flask in order to design the frontend of the web application and make it as catchy as possible.

As for the backend database, MySQL will be used for the database connections and queries. This is because of the previous experience I have with MySQL and how easy it is to implement. The device will have a MySQL server and database running so that both the web server and the desktop application can interact with it, retrieve and insert data from and into it.

5.1.4 SMS Authentication (Twilio)

An additional layer of authentication will be used for admins attempting to register users into the system. This additional layer is an SMS authentication method, where the admin will receive an code via SMS, and they have to enter that code into the system to be able to register new users.

The perfect service for this is Twilio, which is a cloud communications platform as a service (PaaS). It provides a means for software developers to make/receive phone calls and send/receive SMS messages. This service is harnessed through Twilio's web API.

5.1.5 Mobile Application

If time allows, there will also be a mobile application for the admins. This will be an alternative method of viewing logs, aside from the website. The mobile application will be based for Android, so Android Studio and Java will also be used.

5.2 Hardware Technologies

There are two options to choose from for the hardware device on which the desktop application will be installed: a Raspberry Pi or an Arduino. After doing my research (shown in Table 4 below), I have concluded that Raspberry Pi will be used.

Table 6: Comparison of Raspberry Pi and Arduino[49][50]

Raspberry Pi	**Arduino**
A mini computer with Raspbian OS. It can run multiple programs at a time.	A microcontroller (which is a part of the computer). It runs only one program again and again.
Requires complex tasks like installing libraries and software for interfacing sensors and other components	Very simple to interface sensors and other electronic components to Arduino.
Can be easily connected to the internet using Ethernet port and USB Wi-Fi dongles.	Requires external hardware to connect to the internet and this hardware is addressed properly using code.
Does not have storage on board. It provides an SD card port.	Can provide onboard storage.
Has 2 - 4 USB ports (depending on model) to connect different devices.	Has only one USB port to connect to the computer.
The recommended programming language is Python but C, C++, Python & Ruby are pre-installed.	Uses Arduino programming language or C/C++.

An LCD touchscreen will also be needed, so that the users can enter their credentials and be able to interact with the Raspberry Pi. A Raspberry Pi Camera module will be used to capture the user's face trying to access the room.

Additionally, a physical lock will be needed to operate the locking/unlocking of the door. The lock will be attached to the Raspberry Pi as a source of power to operate properly when given the signal.

6 Conclusion

This project is focused on using facial recognition technology to secure physical access to equipment rooms in companies. Amazon AWS Rekognition API will be used for this implementation, and a Raspberry Pi will be used to operate the camera and a physical lock which is responsible for locking and unlocking the door once a user is authorized to enter the room. There is a logging functionality that will log the user that accessed the room, what time they accessed it at and a list of all the other times at which they accessed the room. Other biometric authentication factors for this project might be considered (e.g. finger vein authentication) for future implementation. For a user to enter the room, they have to provide their credentials by entering it into the Raspberry Pi desktop application and verify themselves using facial recognition, otherwise, they are denied access to the room and this will also be logged.

The web application will be used by admins to view the logs and user information. It can also be used by normal users to modify their information, e.g. change password, enter their phone number/email etc.

References

[1] TechFunnel. *Future of Face Recognition Technology*. 2018. URL: https://www.techfunnel.com/information-technology/future-of-face-recognition-technology/.

[2] Phil Goldstein. *Why Physical Security Should Be as Important as Cybersecurity*. 2016. URL: https://biztechmagazine.com/article/2016/10/why-physical-security-should-be-important-cybersecurity.

[3] Renu Bhatia. "Biometrics and Face Recognition Techniques". In: *International Journal of Advanced Research in Computer Science and Software Engineering* 3.5 (2013). URL: https://pdfs.semanticscholar.org/a7cf/ede8225c99f6e1883d4ae14c66fb20191117.pdf.

[4] Olufemi Sunday Adeoye. "A Survey of Emerging Biometric Technologies". In: *International Journal of Computer Applications* 9.10 (Sept. 2010), pp. 213–218. DOI: 10.5120/1424-1659. URL: https://pdfs.semanticscholar.org/2c6c/4f84046be0a9b317f398bf1783e32e5ad771pdf.

[5] Long Tran and Thai Le. "Person Authentication Using Relevance Vector Machine (RVM) for Face and Fingerprint". In: *Modern Education and Computer Science* 5 (2015), pp. 8–15. DOI: 10.5815/ijmecs.2015.05.02. URL: http://www.mecs-press.org/ijmecs/ijmecs-v7-n5/IJMECS-V7-N5-2.pdf.

[6] Elakkiya Ellavarason, Richard Guest, and Farzin Deravi. "A Framework for Assessing Factors Influencing User Interaction for Touch-Based Biometrics". In: *Kent Academic Repository* (2018). DOI: 10.23919/EUSIPCO.2018.8553537. URL: https://kar.kent.ac.uk/68945/7/20180903%20Elakkiya%20Ellavarason%20A%20Framework%20for%20Assessing%20Factors%20Influencing%20User%20Interaction%20for%20Touch-based%20Biometrics%281%29.pdf.

[7] D Ramli, M Hooi, and K Chee. "Development of Heartbeat Detection Kit for Biometric Authentication System". In: *20th International Conference on Knowledge Based and Intelligent Information and Engineering Systems* 96 (2016), pp. 305–314. DOI: 10.1016/j.procs.2016.08.143. URL: https://reader.elsevier.com/reader/sd/pii/S1877050916319445.

[8] T Pandikumar et al. "Enhancing Performance and Usability of Keystroke Dynamics Authentication on Mobile Touchscreen Devices Using Features Extraction Scheme". In: *International Journal of Engineering Science and Computing* 7.6 (2017). URL: https://pdfs.semanticscholar.org/b6a3/5194a686adfb4075a9b942fd3af7c07fb981.pdf.

[9] Anil Jain, Arun Ross, and Salil Prabhakar. *Fingerpring Matching Using Minutiae and Texture Features*. 2001, pp. 282–285. URL: https://www.cse.msu.edu/~rossarun/pubs/RossMinTexture_ICIP01.pdf.

[10] A.K. Jain et al. "An Identity-Authentication System Using Fingerprints". In: *Proceedings of the IEEE* 85.9 (Sept. 1997), pp. 1365–1388. DOI: 10.1109/5.628674. URL: http://biometrics.cse.msu.edu/Publications/Fingerprint/JainEtAlIdentityAuthUsingFp_ProcIEEE97.pdf.

[11] Miyuki Kono, Hironori Ueki, and Shin-ichiro Umemura. "Near-Infrared Finger Vein Patterns for Personal Identification". In: *Applied Optics* 41.35 (Dec. 2002), p. 7429. DOI: 10.1364/ao.41.007429. URL: http://svsu.edu/library/archives/public/follett/documents/144_151/KFP148_69e.pdf.

[12] Sujata Kulkarni, R.D. Raut, and P.K. Dakhole. "A Novel Authentication System Based on Hidden Biometric Trait". In: *Procedia Computer Science* 85 (2016), pp. 255–262. DOI: 10.1016/j.procs.2016.05.229. URL: https://core.ac.uk/download/pdf/81219055.pdf.

[13] Seminars Only. Feb. 2019. URL: https://www.seminarsonly.com/computer%20science/finger-vein-recognition-seminar-report-ppt.php.

[14] John Trader. *4 Difference between Iris and Retina for Biometric Identification*. May 2016. URL: http://www.m2sys.com/blog/iris-recognition-2/difference-iris-retina-important-biometric-identification/.

[15] Rawlson King. *Explainer: Retinal Scan Technology*. May 2013. URL: https://www.biometricupdate.com/201307/explainer-retinal-scan-technology.

[16] Parth Panchal, Ronak Bhojani, and Tejendra Panchal. "An Algorithm for Retinal Feature Extraction Using Hybrid Approach". In: *Procedia Computer Science* 79 (2016), pp. 61–68. DOI: 10.1016/j.procs.2016.03.009. URL: https://core.ac.uk/reader/82033941.

[17] Sushil Chauhan, Ajat Arora, and Amit Kaul. "A survey of emerging biometric modalities". In: *Procedia CS* 2 (Dec. 2010), pp. 213–218. DOI: 10.1016/j.procs.2010.11.027.

[18] Dana Hejtmánková et al. "A New Method of Finger Veins Detection". In: *International Journal of Bio-Science and Bio-Technology* 2009 (Dec. 2009), pp. 11–15.

[19] Dhairya Parikh. *Advancements in Computer-Based Facial Recognition Systems*. June 2018. URL: https://medium.com/coinmonks/from-the-rand-tablet-to-differentiating-identical-twins-aa4ba6031bb0.

[20] Jesse Davis West. *History of Face Recognition and Facial Recognition Software*. Mar. 2019. URL: https://www.facefirst.com/blog/brief-history-of-face-recognition-software/.

[21] Yoram Boccia et al. 2019. URL: https://www.doc.ic.ac.uk/~hh4017/History.

[22] Neil Lydick. *A Brief Overview of Facial Recognition*. URL: https://www.eecs.umich.edu/courses/eecs487/w07/sa/pdf/nlydick-facial-recognition.pdf.

[23] L. Sirovich and M. Kirby. "Low-Dimensional Procedure for the Characterization of Human Faces". In: *Journal of the Optical Society of America A*. 4.3 (Mar. 1987), p. 519. DOI: 10.1364/josaa.4.000519. URL: https://www.osapublishing.org/josaa/abstract.cfm?uri=josaa-4-3-519.

[24] Matthew Turk and Alex Pentland. "Eigenfaces for Recognition". In: *Journal of Cognitive Neuroscience* 3.1 (Jan. 1991), pp. 71–86. DOI: 10.1162/jocn.1991.3.1.71.

[25] Mei Ngan and Patrick Grother. "rFace Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms". In: *NIST 8052* (Apr. 2015). DOI: 10.6028/nist.ir.8052. URL: https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8052.pdf.

[26] Facebook App. *An Update about Face Recognition on Facebook*. Sept. 2019. URL: https://about.fb.com/news/2019/09/update-face-recognition/.

[27] Yaniv Taigman et al. *DeepFace: Closing the Gap to Human-Level Performance in Face Verification*. URL: https://research.fb.com/wp-content/uploads/2016/11/deepface-closing-the-gap-to-human-level-performance-in-face-verification.pdf.

[28] Anil K. Jain, Karthik Nandakumar, and Arun Ross. "50 years of biometric research: Accomplishments, challenges, and opportunities". In: *Pattern Recognition Letters* 79 (2016), pp. 80–105.

[29] Md. Zahangir Alom et al. "The History Began from AlexNet: A Comprehensive Survey on Deep Learning Approaches". In: (Mar. 2018).

[30] Mohit Gupta. May 2018. URL: https://www.geeksforgeeks.org/ml-types-learning-supervised-learning.

[31] Techopedia. 2019. URL: https://www.techopedia.com/definition/30389/supervised-learning.

[32] Sonali B. Maind and Priyanka Wankar. *International Journal on Recent and Innovation Trends in Computing and Communication Research Paper on Basic of Artificial Neural Network*. 2014. URL: https://pdfs.semanticscholar.org/cb22/b35b740a79ce710f7471c0bc01e570092480.pdf.

[33] Jitendra R Raol and Sunilkumar S Mankame. *Artificial Neural Networks - A Brief Introduction*. Feb. 1996.

[34] Jason Elder. *Exploring neural networks for facial recognition – Saratoga*. July 2019. URL: https://www.saratoga.co.za/exploring-neural-networks-for-facial-recognition/.

[35] Aris Papadopoulos. *An Intuitive Explanation for Neural Networks — aris.onl*. July 2016. URL: http://aris.onl/intuitive-neural-nets/.

[36] Ashok Kumar et al. *Experimental Modeling of NOx and PM Generation from Combustion of Various Biodiesel Blends for Urban Transport Buses*. Aug. 2016.

[37] Igor. *Facial Recognition and Neural Networks: The Technology Marches Forward*. Nov. 2019. URL: https://gbksoft.com/blog/neural-networks-for-facial-recognition/.

[38] Jason Brownlee. *How to Perform Face Detection with Deep Learning*. June 2019. URL: https://machinelearningmastery.com/how-to-perform-face-detection-with-classical-and-deep-learning-methods-in-python-with-keras/.

[39] Michal Kawulok. URL: http://sun.aei.polsl.pl/~mkawulok/stud/fr/lect/05.pdf.

[40] Urvashi Jaitley. *Why Data Normalization Is Necessary for Machine Learning Models*. Oct. 2018. URL: https://medium.com/@urvashilluniya/why-data-normalization-is-necessary-for-machine-learning-models-681b65a05029.

[41] Jovana Stojilkovic. 2012. URL: http://neuroph.sourceforge.net/tutorials/FaceRecognition/FaceRecognitionUsingNeuralNetwork.html.

[42] Jason Brownlee. *A Gentle Introduction to Deep Learning for Face Recognition*. May 2019. URL: https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/.

[43] Kairos. 2016. URL: https://www.kairos.com/docs/api/.

[44] codesharedot. *Best Python framework for building a desktop application and GUI*. DEV Community, Oct. 2019. URL: https://dev.to/codesharedot/best-python-framework-for-building-a-desktop-application-and-gui-58n5 (visited on 04/12/2020).

[45] Python. Aug. 2019. URL: https://www.python.org/about/.

[46] PyQt Wiki. *PyQt - Python Wiki*. wiki.python.org, 2019. URL: https://wiki.python.org/moin/PyQt (visited on 04/12/2020).

[47] The wxPython Team. *Welcome to wxPython!* wxPython, Dec. 2019. URL: https://www.wxpython.org/ (visited on 04/12/2020).

[48] *TkInter - Python Wiki*. Python.org, 2013. URL: https://wiki.python.org/moin/TkInter (visited on 04/12/2020).

[49] Elktros. *What are the differences between Raspberry Pi and Arduino?* Dec. 2017. URL: https://www.electronicshub.org/raspberry-pi-vs-arduino/.

[50] Paul Albinson. *Computing in Education: A Study of Computing in Education and Ways to Enhance Students' Perceptions and Understanding of Computing*. 2013. URL: https://eprints.bournemouth.ac.uk/21331/1/msc-dissertation.pdf.

List of Figures

1 Fingerprints . . . 3
2 Finger Vein Authentication Process . . . 4
3 Retinal Scan Process . . . 5
4 RAND Tablet . . . 6
5 Facial Recognition Technology Timeline . . . 7
6 Relationship Between AI, ML & ANN . . . 8
7 Artificial Neuron & Brain Neuron . . . 9
8 Simple Artificial Network . . . 9
9 Facial Recognition Algorithm Process . . . 10
10 Geometrical Normalization Process . . . 11
11 Facial Features Extraction . . . 12

List of Tables

1 Comparison of Various Biometric Authentication Methods . . . 5
2 Similar Applications That Provide Facial Recognition Access Control Systems . . . 13
3 Comparison of Different Facial Recognition APIs . . . 14
4 Comparison of Different Python Desktop Application Development Frameworks . . . 15
5 Comparison of Different Python Web Development Frameworks . . . 16
6 Comparison of Raspberry Pi and Arduino . . . 17