Designing an autonomous drone infrastructure for surveillance with facial recognition

Stephen Rerri-Bekibele

School of Computer Science

UNIVERSITY OF LINCOLN

Introduction

The use of drones in the modern world has been increasing. From the little drones children play with in their backyard and parks to their distant cousins in warfare, movie making, nature observing, and the list continues to increase. As the uses of drones becomes more normalized in everyday life there has been a demand for harsher laws to prevent unlawful uses of our beloved toys. These laws mean there are restrictions on who can fly certain drones and where drones can be operated. One aim of this research paper is to challenge the question: if we can't fly the drones, can we make the drones fly themselves and achieve meaningful results? One such application of this question is to design infrastructure that would allow law enforcement agencies and search and rescue agencies to employ the help of autonomous drones with facial recognition for law keeping and searching for people of interest in urban areas.

According to research by PwC there could be 76,000 drones in the UK by 2030

Aims & Objectives

Implement infrastructure for drone surveillance with facial recognition

The objectives of my project is to:

1. Create a solid and secure infrastructure for the communication of personal data to a remote server.
2. To build a system that can receive images and act based on the received images during a live video feed
3. To safely navigate to an individual in a crowded place
4. To accurately navigate to the correct individual in a crowded place
5. For the drone to be able to learn the best heights to be at for and accurate monitoring of a target.
6. To introduce a novel and appropriate use of drone and facial recognition technology for the aid of law keeping and search and rescue operations.

Research Methods

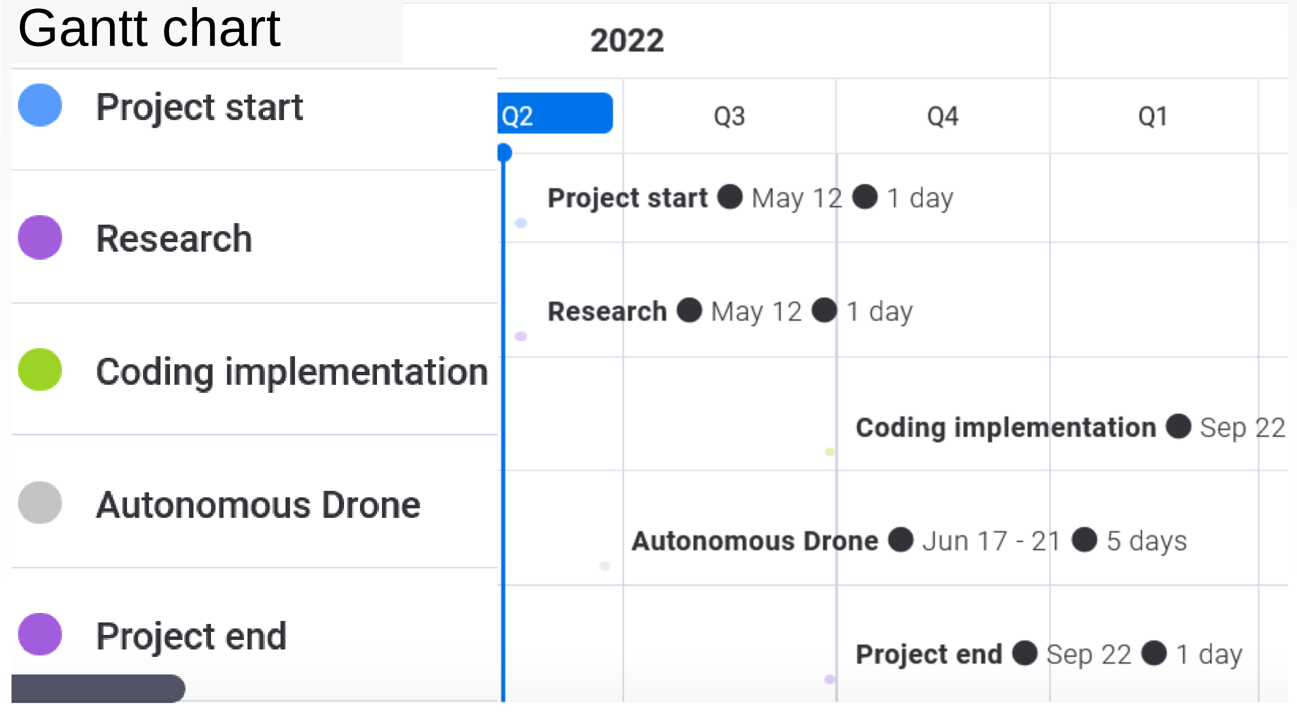
The research will be carried out through the use of experiments in simulation and with a VM to simulate the presence of a raspberry pi, the VM will run the facial recognition code as well as the file receiver python code simultaneously. Images of targets will then be sent to the VM as the code is running to test the stability of the code. To simulate a drone, a third party software, Droidcam, able to use mobile phones as computer cameras will be used to connect a phone to the VM. Another device will then run the python script used to send a target image to the VM.

The accuracy and performance of different facial recognition libraries will be tested and the most suitable algorithm will be chosen.

Asides from this, the ability of the algorithms to work in different lighting conditions will also be tested via speed of detection and confidence value.

The ability of the drone to seek and follow a target safely will also be tested. As a measure of the deployability of the drone in a real world scenarios.

Gantt chart

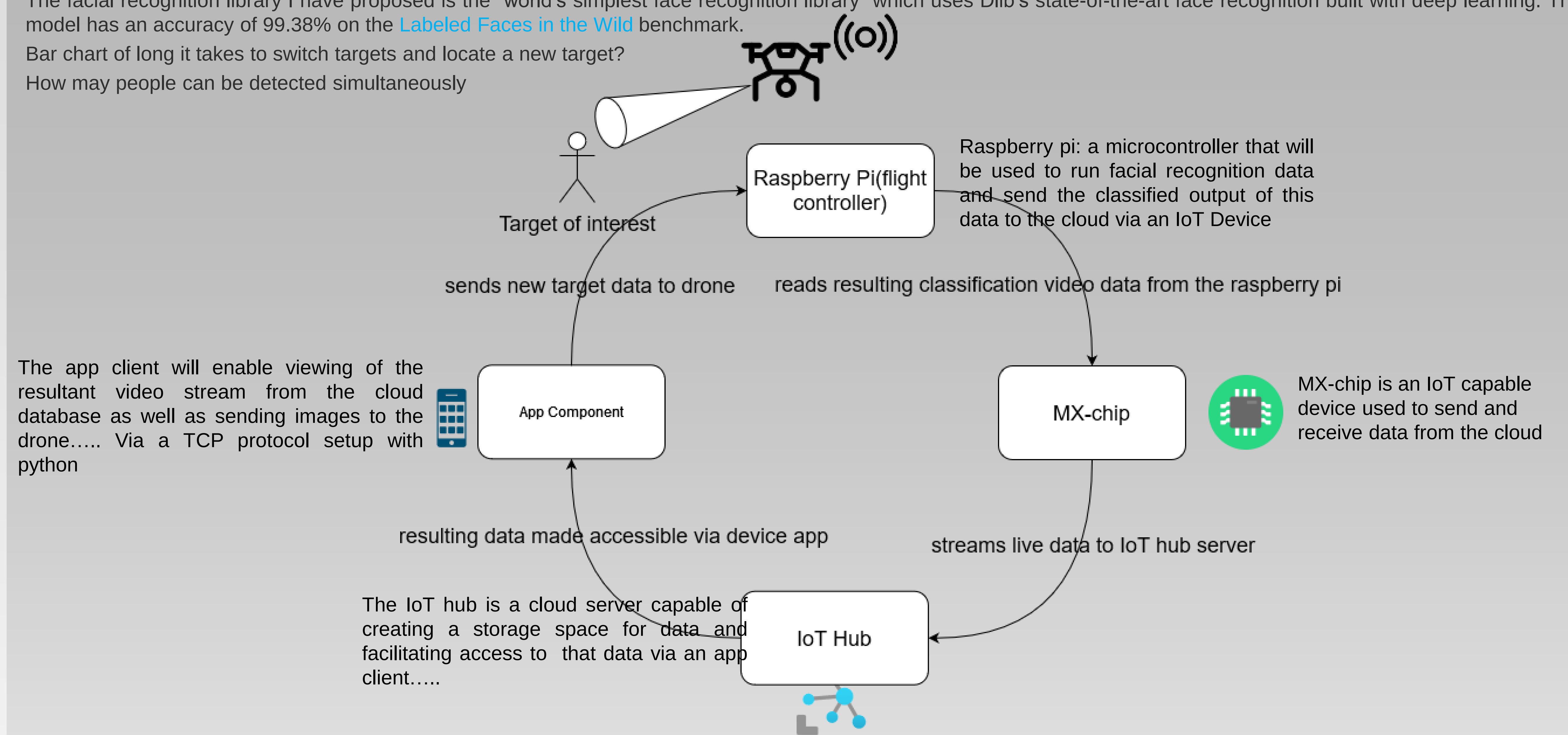


Research Plan

The facial recognition library I have proposed is the "world's simplest face recognition library" which uses Dlib's state-of-the-art face recognition built with deep learning. The model has an accuracy of 99.38% on the Labeled Faces in the Wild benchmark.

Bar chart of long it takes to switch targets and locate a new target?

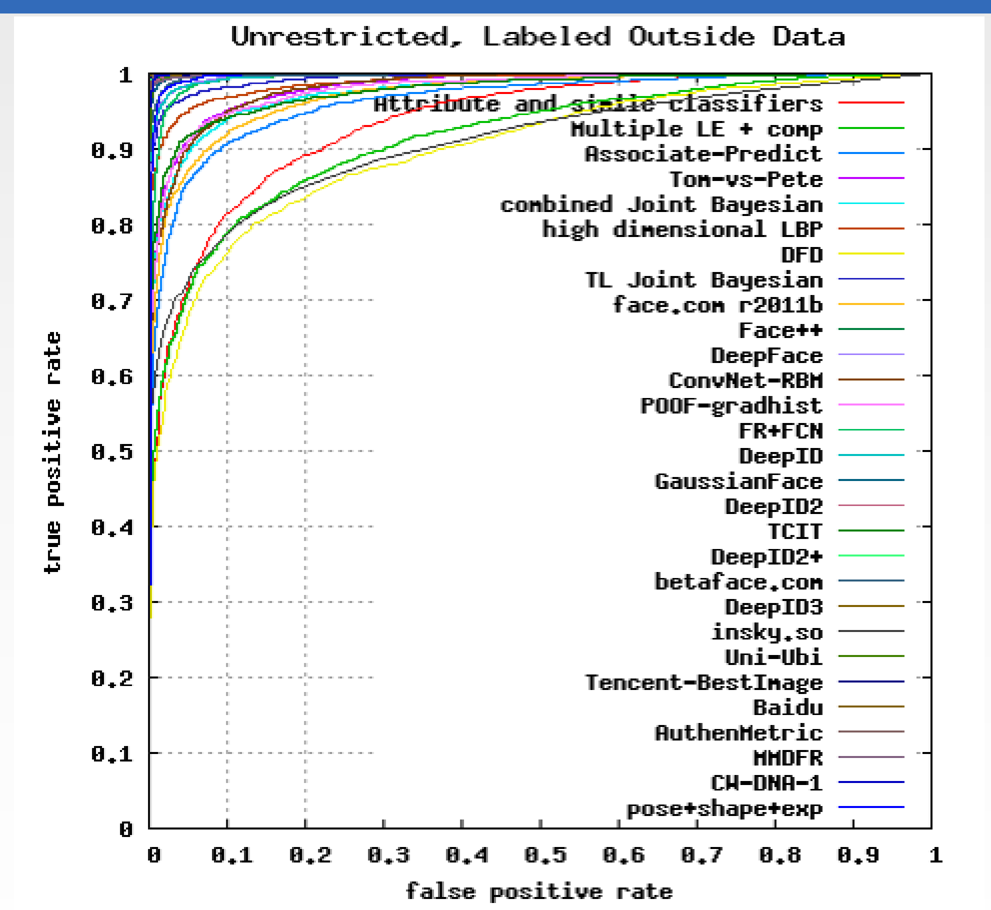
How may people can be detected simultaneously



The Local device sends pictures of targets to the autonomous drone which adds these images to an "unknown" folder. On board the drone also has a "known" folder which contains pictures of known targets with labels. These known pictures are then matched against the unknowns to verify if a match is found.

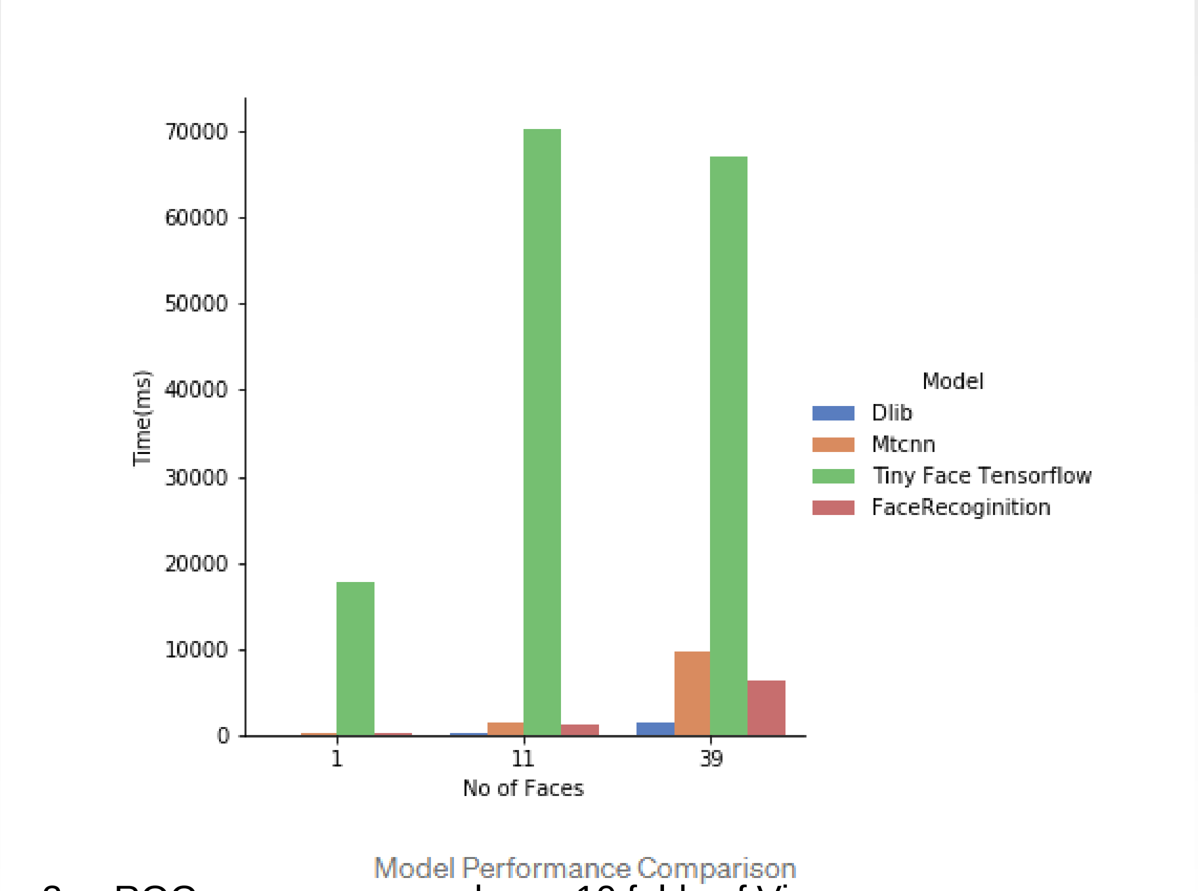
To test the application 2 virtual machines were setup, one to simulate a drone with a raspberry pi and another to simulate a device sending target information to the drone. This was done via two python scripts one to act as a sender and the other, a receiver.

Research Results



1. ROC curves averaged over 10 folds of View 2.

Figure 1 is a graph showing the performance of different algorithms based on the Labelled Faces in the wild benchmark. These are all different implementations of Dlib's state of the art face recognition built using deep learning.



2. ROC curves averaged over 10 folds of View 2.

Figure 2 is a comparison between Dlib's library and other known face recognition libraries. Tiny Face model is best compared to Dlib because it offers higher accuracy with low-quality images. However it takes more computational time

Risk Analysis

Risk items (Potential future problems derived from Brainstorming)	Likelihood of Risk Item Occurring	Impact to project if Risk item does occur	Solution
Fail to get an autonomous drone	L:5, C:2	The project will have to be entirely simulation based without a drone	I am using VMs to simulate the raspberry pi a phone to simulate the drone
Fail to safely secure user data	L:2,C:5	The project will not be able to go on without secure encryption	The images will be sent over the internet via a secure port and then will encrypted.
Fail to compare other face recognition libraries	L:3,L:2	This will mean a better face recognition library I do not test may provide better results in the future	The main objectives of implementing facial recognition into a drone and being able to switch targets will be possible
Fail to get raspberry pi but get suitable drone	L:5, C:1	Without a raspberry pi the project will have to be done with VMs	Facial recognition will have to be on the computer after the video is streamed

L: Likelihood, C: Consequence, high numbers mean more likely

Conclusions

In conclusion the project has demonstrated that facial recognition for use on drones is very reliable and accurate but when used on drones various constraints have to be considered for the drone's camera to operate as well as a camera in an isolated environment such as the optimal height of the drone and angle of the camera for accurately detecting the faces of people.

In addition, the project also highlighted the dangers of drone usage for surveillance and the vulnerability of drones for surveillance operating at street level making them conspicuous and thus unable to be applied as a means of covert surveillance unlike UAVs to some degree due to the abilities to operate at higher altitudes and safe from target retaliation such as people trying to shoot them down.

Furthermore, the drones can be limited by how long they can operate for and the conditions they can be applied in due to their small sizes making them susceptible to the wind and small battery capacity.

References

A webpage comparing an explaining the best face recognition models and their performance:

https://rupeshthetech.medium.com/face-detection-models-and-their-performance-comparison-eb8da55f328c

Labelled Faces in the wild:

http://vis-www.cs.umass.edu/lfw/results.html

Dlib: http://dlib.net/

Acknowledgements

Dr Miao Yu