Alechenu Iyoko
University of Hull

Face recognition systems with Unmanned Ground Vehicles

Table of Content

Table of Content..1
Abstract..1
Keywords/Concepts...2
1. Introduction..2
2. Literature Review..4
2.1 History and Evolution...4
2.2 Face Recognition Systems...6
Definition...6
Steps in Face Recognition Systems...6
Deep learning and face recognition..7
2.3 Face recognition on UGVs...9
2.4 Ethical Considerations.. 11
2.4 Challenges, limitations and suggested improvements..13
2.5 Security and Safety Applications of Face Recognition Technology:................................. 15
2.7 Application of Face Recognition Technology in UGVs:..16
2.8 Analysis of Face recognition for Biometric Authentication..16
Suggested improvements.. 19
3. Methodology.. 20
Face Recognition Model Development...20
Model Deployment..23
Model Integration with UGV..24

Abstract

Facial recognition technology (FRT) has undergone significant advancements since its inception, evolving into a promising biometric authentication tool with applications in various domains, including social media, healthcare, and security and safety measures. This project explores the potential of face recognition in security applications by levaring transfer learning techniques to train a MobileNetV2 model for face recognition. The system is then deployed on an unmanned ground vehicle, specifically the Limo AgileX. Utilising virtual environments such as Google Colab and the Robot Operating System (ROS), the project aims to seamlessly integrate the facial recognition system with the capabilities of the UGV.

The primary focus lies in exploring functionalities such as individual identification, access control, and perimeter patrol. By leveraging deep learning techniques, the project aims to evaluate the performance of the developed face recognition system and identify its potential applications in enhancing security and safety measures.

Furthermore, this project endeavours to address how face recognition systems can be integrated into unmanned ground vehicles and the responsible and effective implementation of FRS in real-world settings. With a comprehensive assessment of the processes involved with the integration and the UGVs capabilities and limitations, it aims to contribute to the ethical and practical considerations surrounding the deployment of face recognition technology on UGVs.

Overall, this project seeks to shed light on the opportunities and challenges associated with face recognition system implementation, ultimately aiming to pave the way for its responsible adoption in diverse environments.

Keywords/Concepts

Biometric authentication, deep learning algorithms, unmanned ground vehicles, security and safety applications.

1. Introduction

Face recognition is the process of automatically identifying or verifying the identity of an individual by analysing facial patterns .It encompasses two primary subfields: face identification and face verification. Face identification determines the identity of an individual, whereas face verification confirms or denies a claimed identity (Peng et al., 2022). Ensuring accurate face recognition is integral for granting access to services, as permissions should only be accorded following correct identification or verification.

Facial recognition technology has emerged as a powerful tool in the realm of biometric authentication, offering an efficient means of identifying individuals based on their unique features. With advancements in deep learning algorithms and the availability of sophisticated computing platforms, the potential applications for face recognition have expanded across various sectors, including security, law enforcement, and access control systems.

Unmanned Ground Vehicles are

In recent years, there has been a growing interest in leveraging FRS to enhance security and safety measures within institutions and public spaces. The ability to accurately identify individuals in real-time and automate access control processes has the potential to streamline operations, improve security protocols, and mitigate risks associated with unauthorised access.

The objectives of this project are as follows: **(1)** Investigate current research and advancements in facial recognition technology, focusing on aspects such as accuracy, robustness, privacy, security, bias, fairness, and emerging applications, to inform the development of facial recognition systems (FRS) tailored for the integration with unmanned ground vehicles (UGVs). **(2)** Evaluate best practices associated with implementing facial recognition technology in the context of UGVs, considering factors such as accuracy, computational resources, real-time performance, and seamless integration with autonomous systems. **(3)** Analyse deep learning algorithms for facial recognition, with a specific focus on pre-trained Convolutional Neural Networks (CNN) models, architectures suitable for computationally constrained devices, and performance comparisons with MobileNetV2, aiming to identify the most suitable algorithm for deployment in the context of the project. **(4)** Examine the challenges and the future directions of facial recognition technology, including privacy concerns, security vulnerabilities, ethical considerations and potential research avenues for improved accuracy, security, and ethical development, with to mitigating risks and enhancing the reliability of the deployed FRS. **(5)** Develop a comprehensive methodology for conducting research on facial recognition systems in the context of UGVs, encompassing data collection, processing, analysis, evaluation metrics, ethical considerations limitations, and timeline to ensure the systematic and rigorous investigation of the project objectives.

This project aims to explore the capabilities and limitations of facial recognition technology within the context of security and safety applications, with a specific focus on its integration with autonomous systems. By utilising transfer learning to develop an FRS using a state-of-the-art deep learning algorithm, MobileNetV2, and virtual environments, we seek to assess the feasibility of deploying facial recognition systems in conjunction with unmanned ground vehicles (UGVs) for enhanced security and surveillance purposes.

In the following section, we delve into the theoretical foundations of facial recognition technology, explore relevant literature and research studies in the field, and critically analyse existing methodologies and approaches employed in similar projects. Additionally, we will review the ethical considerations, privacy concerns, legal frameworks and user acceptance factors associated with the implementation of the facial recognition systems. Through an extensive review of the existing body of knowledge, we aim to provide a comprehensive understanding of the subject matter and inform the project's methodology and conclusions.

2. Literature Review

This section serves as a comprehensive analysis of existing research pertinent to the deployment of face recognition systems for biometric authentication, particularly in the context of unmanned ground vehicles (UGVs) for biometric authentication.

2.1 History and Evolution

Facial recognition technology has come a long way since its humble beginnings. Here we delve into the fascinating journey of this technology, highlighting key milestones and advancements.

Early Beginnings (1960s): The seeds of facial recognition were sown in the 1960s, when pioneering researchers like Woodrow Bledsoe, Helen Chan Wolf, and Charles Bisson embarked on the ambitious task of teaching computers to recognize faces. Their system relied on manually identifying specific facial features like eyes, nose, and mouth. While revolutionary for its time, this method faced limitations. The lack of readily available computing power at the scale needed for complex algorithms, coupled with the inherently high dimensionality of facial data (requiring a vast amount of data points to represent a face) made the system impractical for real-world applications[1].

Biometric Boom: The latter half of the 20th century witnessed exponential growth in biometric research. Semi-automated facial recognition methods emerged in the 1960s, followed by automated processes funded by the FBI in 1969. The 1990s saw the emergence of real-time facial detection technology. By the 2000s, biometric authentication became commonplace, with hundreds of algorithms patented within the USA and widespread commercial adoption (Moen, 2021).

The Eigenface Revolution (1991): A significant breakthrough came in 1991 with the introduction of Eigenfaces by researchers Matthew Turk and Pentland. This technique utilised the power of linear algebra and Principal Component Analysis (PCA) to address the challenge of high dimensionality of facial images. Eigenfaces captured the most prominent gestures in a set of faces, creating a compressed representation. This innovation significantly improves processing efficiency, paving the way for more advanced algorithms[1].

DARPA and the Rise of Commercial Applications (1990s): The 1990s witnessed a surge in facial recognition development. The Defense Advanced Research Projects Agency (DARPA) initiated the face recognition technology program FERET, specifically designed to evaluate automated facial recognition capabilities for security applications. This program played a crucial role in fostering the creation of commercially viable facial recognition systems. This program challenged researchers to develop algorithms with greater accuracy and robustness, ultimately leading to the creation of systems that could be adapted for real-world security needs. The success of the FERET spurred significant investment in facial recognition technology, paving the way for its transition from research labs to the commercial market[6].

*Deep learning Revolutionised Accuracy. The dawn of the 21st century ushered in a new era for facial recognition, marked by a dramatic leap in accuracy and robustness. This transformation was fueled by two key advancements, Advancements in computer processing power and the rise of deep learning.

*Deep Learning Techniques: The rise of deep learning, particularly Convolution Neural Networks (CNNs), revolutionised the field. CNNs excel at feature extraction from images, allowing them to learn intricate patterns and variations within facial data. This learning capability significantly improved the accuracy and reliability of face recognition algorithms

*Increased Computing Power: The exponential growth of computing power provided the necessary muscle for running complex algorithms that could effectively analyse facial data.

** History of face recognition on UGVs

Present Day and Beyond: Governments worldwide are heavily invested in facial recognition technology. In the US, airports are enhancing security with facial recognition systems , and some states allow law enforcement to search databases using facial recognition (Dharaiya & Davies, 2020)

2.2 Face Recognition Systems

Definition

Face recognition systems are a type of biometric technology that automatically identifies or verifies a person’s identity based on their facial characteristics. These systems capture and analyse a person's facial features (e.g., distance between their eyes, shape of nose) and compare them to a database of known faces (Buolamwini & Gebru, 2024). In this section we will delve into the overview of face recognition systems and its application in unmanned ground vehicles

Steps in Face Recognition Systems

These systems are usually composed of three main steps. **(1) Face detection, **(2)** Feature Extraction, and **(3)** Facial recognition as shown in figure…**

Face detection, the process of a face recognition system begins with detecting the presence of a face within an image. Face detection algorithms are employed to determine whether an image contains one or more faces and to pinpoint their locations.

Once a face is detected, the next step involves extracting its features. Feature extraction, this is crucial for tasks such as recognizing facial expressions and animated faces. Feature extraction entails generating a feature vector, known as a signature, from the detected face. This signature serves as a representation of the face, possessing properties of uniqueness and discrimination between individuals. Importantly, feature extraction can be integrated into the face detection process.

Finally, the face recognition phase encompasses authentication and identification. Authentication entails comparing a face with another to verify the claimed identity, while identification involves comparing a face with multiple others to determine its identity among several possibilities (Chihaoui, 2016).

Deep learning and face recognition

Deep learning has emerged as a pivotal field within computer vision research and machine learning, revolutionising image processing and identification capabilities. Its architecture, comprising numerous non-linear transformations, enables efficient problem-solving across diverse domains. Face recognition, in particular, benefits from a deep learning approach, with techniques like Convolutional Neural Networks (CNNs) offering robust solutions. CNNs, adept at identifying image characteristics, employ convolutional layers to extract features crucial for classification tasks. *Image of CNN layers*

Deep learning algorithms: Prior to the rise of deep learning algorithms, traditional face recognition methods typically followed a two-step approach. Initially, these methods involved the extraction of shallow hand-crafted features from facial images using techniques such as Local Binary Pattern (LBP), Scale Invariant Feature Transform (SIFT), and Histogram of Oriented Gradients (HOG). Subsequently the extracted features were trained and identities were classified using algorithms like Support Vector Machines (SVMs) or Nearest Neighbors(Ahonen et al., 2006)(Geng & Jiang, 2010) (F. De la Torre et al., 2011).

Advantages of deep learning for facial recognition

Despite their computational complexity, CNNs offer advantages such as

Efficient Implementation: CNNs are adaptable to various image resolutions and boost detailed computing capabilities, minimising error rates.

Handling Complexity: CNNs excel in solving high-complexity problems by efficiently processing numerous parameters.

Face recognition: CNNs can accurately classify both known and unknown faces, making them invaluable in biometric authentication. (Setiowati et al., 2018)

Suitable DL architectures for resource constrained devices

In response to the need for computationally efficient CNN architectures suitable for resource-constrained environments, various models have been introduced. EffNet, ShuffleNet, and MobileNet are among the notable examples. L-CNN (Light-weight CNN) was proposed as a trainable version of the BCONV-ELM architecture, which uses binary weight convolution neural networks for low-complexity implementations. This model optimises binary kernels while maximising accuracy through an extreme learning machine approach (Felea, I & Dogaru, R., 2020).

MobileNet proposed by (Howard, 2017) utilises depthwise separable convolutions to create lightweight networks. This involves breaking down standard convolutions into depthwise and pointwise convolutions, significantly reducing the number of parameters while maintaining accuracy comparable to larger models like VGG-16. MobileNetV2, proposed by (Sandler, 2018) further improves upon MobileNet by introducing inverted residuals bottleneck structures and layer expansion. Despite these advancements, challenges remain in effectively running deep learning frameworks on CPUs (Duong, 2020).

Image of MNV2 architecture

Challenges using DLMs on resource constrained devices

2.3 Face recognition on UGVs

Optimising facial recognition algorithms for real-time performance on resource-constrained platforms like unmanned ground vehicles (UGVs) presents several challenges. This section explores key considerations and potential solutions for deploying face recognition models on UGVs effectively.

Considerations:
Model complexity: Given the limited computational resources, choosing or designing lightweight models is crucial. These models should achieve a balance between accuracy and complexity. We can consider the lightweight models proposed earlier

Effnet arch

Shufflenet arch

Mobile net arch

Under considerations we've discussed how models can be too computationally...for deploying face recognition models on UGVs here are some... to go

Alternatives for running models in Resource-constrained Environments

While model complexity plays a significant role, other strategies can be employed for deploying face recognition on UGVs:

Model Conversion: The field of model quantization in convolution neural networks (CNNs) has emerged due to the need for the mobile-friendly models that prioritise computational efficiency and small model sizes. The necessity arises from the deployment of CNNs on mobile platforms such as smartphones, augmented and virtual reality devices, drones(Unmanned Aerial Vehicles) and UGVs, which require limited device memory and low latency. Methods on model quantization can be broadly categorised into two approaches: The design of new network architectures from 32-bit floating-point to lower bit-depth representations. TensorFlow, initially developed as distbelief by Google Brain in

2010. TensorFlow was created to simplify and restructure the code base, resulting in a faster and more robust application-level code. Abreakthrough led by Hinton’s research team significantly reduced errors in neural networks, particularly in Google”s speech-recognition software. In May 2017, Google introduced TensorFLow Lite, dedicated to Android development, allowing the deployment of lightweight machine learning algorithms on resource constrained edge devices like smartphones and microcontrollers. TensorFlow Lite offers the flexibility to run various algorithms on different edge devices while maintaining computational efficiency (Junyan Dai, 2020).

- Cloud platform

Edge TPU’s: The Edge TPU, a machine learning ASIC developed by Google offers fast TensorFlow Lite model inference with low power consumption. It continuously adds new operations and updates, maintaining a constant ratio of known limitations to all supported operations. With a power consumption of only two watts, the Edge TPU is suitable for low-power environments and outperforms other hardware accelerators in terms of images processed per second per Watt. In classification tasks, the Edge TPU consistently outperforms other hardware accelerators in terms of latency and power efficiency. However, comparisons of accuracy between Edge TPU models with int8 precision and competitors with float32 precision is limited. For object detection, the Edge TPU is used in applications such as face mask detection. The deployment of deep neural networks (DNNs) to Edge TPU involves converting TensorFlow or Keras models to TFLITE format, quantizing the model, and compiling it using the Edge TPU compiler. Transfer learning can be achieved through methods such as retraining the last layer or weight imprinting (Yipeng Sun & Andreas M. Kist, n.d.).

Model Comparison

The overall architecture of MobileNetV2 employs 3x3 kernels for spatial convolution, with parameters including the expansion factor (t), the number of output channels ©, the repeating number (n), and the stride(s). The network's computational cost ranges from 300 million to 585 million multiply-adds, with a model size varying between 1.7 million and 6.9 million parameters. Training is conducted using 16 GPUs with a batch size 96.

Image of overall architecture

In Image Net classification, MobileNetV2 achieves superior performance compared to MobileNetV1 and ShuffleNet, even with comparable model size and computational cost. With a width multiplier of 1.4, MobileNetv2 outperforms ShuffleNet (x2) and NASNet, while maintaining faster inference time across various input resolutions and width multipliers. (Sik-Ho Tsang, 2019)

*Image of comparisons**

2.4 Ethical Considerations

Face recognition technology offers a powerful tool for security and identification, but its widespread adoption raises significant ethical concerns. These concerns touch upon fundamental rights and freedoms and necessitate careful consideration before implementing this technology. This section will explore the key ethical considerations surrounding the use of facial recognition technology for security and biometric authentication, they include:

Privacy concerns: Biometric data usage spans authentication, identification, and surveillance across various sectors, posing both benefits and concerns. While biometric data offers universal, unique, and permanent identification, concerns arise regarding data security, privacy breaches and regulatory gaps. Addressing these concerns necessitates robust security measures, transparent data handling practices, and legislative updates to safeguard individual privacy rights (Miller, 2022). Biometric data, due to its unique and sensitive nature, poses significant privacy risks, including unauthorised access, re-identification, and lack of individual control. To mitigate these risks, stringent security measures, encryption techniques, and transparent consent mechanisms are essential for responsible biometric data handling (*GDPR and Biometric Data: Privacy Implications and Regulatory Compliance*, n.d.). In addition, new methods such as The federated learning and privacy protection in impact detection have been developed to address privacy issues in facial recognition (Farooq & Borghesi, 2023). What does the method entail?

Data Collection and Storage: The converted collection of biometric information, without individuals' knowledge or consent, raises serious privacy concerns. This practice can infringe on personal data privacy and national security measures, exposing individuals to cyber threats and identity theft. Moreover, gathering secondary information alongside primary identifiers, in this case, facial features can increase the risk of privacy infringement misuse. To mitigate these risks, explicit consent from individuals is crucial, ensuring transparency and accountability in data collection. Additionally, handling sensitive biometric data securely and complying with relevant privacy laws, such as the Illinois Biometric Information Privacy Act (BIPA), is essential for protecting personal privacy rights. Responsible use of biometric data requires robust security measures, transparent policies, regular privacy impact assessment, and stakeholder involvement in governance. Overall, safeguarding personal privacy in the context of biometric security demands a proactive approach to address privacy concerns and ensure ethical data handling practices (Radwan, 2024).

Bias and Discrimination: Face recognition technology's increasing use worldwide has brought attention to its uneven performance across races, raising concerns about bias and discrimination. Researchers at The University of Texas at Dallas School of Behavioural and Brain Sciences identified factors contributing to these disparities and offered guidelines for evaluating algorithms as technology advances. The study outlined two types of bias, data-driven and operationally defined, which influence algorithm performance and user decisions, respectively. While there's no one-size-fits-all solution, the research suggests specific approaches to improve accuracy. However, addressing bias requires caution and understanding the complexity of the issue, as algorithms may exhibit bias in different ways. Despite advancements, there's still much work to be done to mitigate bias and ensure fair and ethical use of these algorithms (Fontenot, 2020).

Security risks: The security risks associated with biometric authentication encompass various threats, including spoofing attacks, data breaches, false positives and negatives, and function creep. Spoofing attacks involve replicating or imitating biometric traits to gain unauthorised access, challenging conventional biometric systems (K, 2023). Data breaches pose serious security implications, potentially leading to identity theft and impersonation if biometric databases are compromised (Morais, 2020). False positives and negatives can occur due to factors like poor lighting conditions or changes in physical appearance, undermining system accuracy. Function creep blurs the line between legitimate use and privacy intrusion by using biometric data in unintended ways (*Biometrics Questions: Privacy, Consent, Function Creep*, n/a). To address these risks, companies can adopt local or device-based authentication mechanisms, such as smartphone-based readers, to avoid storing biometric data centrally. Tokenization or encryption methods can also be utilised as in this approach sensitive biometric data, in this case facial images are converted into unique codes or encrypted hashes. These codes are then used for authentication instead of storing the raw biometric data on servers. This method enhances security by reducing the risk of misuse or unauthorised access to the original biometric information (Morais, 2020).

Lack of transparency and Explainability: Face recognition systems are often employed without proper consent or notification. Users should understand how these systems work to make informed decisions about participating in authentication processes, the inner workings of these systems will be discussed in a later section. Transparency fosters trust and ensures that users are aware of how facial recognition operates, so they can better assess its impact on their privacy and rights (Gray, 2022). An example of this would be a recent audit of UK police deployments of facial recognition technology found that all three cases failed to meet minimum ethical and legal standards. Lack of transparency and accountability were key concerns, making it difficult to evaluate whether the tools perpetuated racial profiling (The University of Cambridge, 2022).

2.4 Challenges, limitations and suggested improvements

While this technology offers promising potential for biometric authentication, several technical challenges and limitations need to be carefully considered when implementing such systems. These challenges can directly impact the ethical implications discussed earlier, particularly regarding accuracy, fairness, and user trust. Here, we explore the key challenges and limitations that need to be addressed to ensure the responsible and effective use of facial recognition for individual identification, access control, and perimeter control.**

Accuracy and Robustness: Facial recognition accuracy can be significantly influenced by various factors, including lighting variations, facial expressions (such as glasses or masks), pose variations, and image quality. These challenges are particularly relevant in real-world deployments like access control systems, where controlled environments might only sometimes be feasible. For instance, variations in lighting conditions outdoors could potentially lead to misidentification. Researchers have developed a novel deep neural network framework that enhances facial recognition accuracy. This framework incorporates techniques from FaceNet and Includes atrous spatial pyramids pooling and squeeze-excitation modules. The approach achieves superior accuracy surpassing 99% even under challenging conditions, such as lighting variations and facial position discrepancies (Ul Ghani et al., 2024). This framework could be integrated into lightweight architectures like MobileNet to improve the facial recognition systems accuracy on resource-constrained devices.

Data Sufficiency: Training face recognition algorithms require a large and diverse dataset of facial images, limited data can lead to inaccurate identification, especially for individuals with underrepresented facial features[35]

Computational Requirements: Running facial recognition algorithms, especially deep learning models, demands significant computational power. Resource-constrained deployments (e.g. on unmanned ground vehicles) face challenges due to computational requirements. Model quantization is a suggested approach that compresses deep neural networks (DNNs) by reducing the number of bits required to represent each weight. This is achieved by using lower precision formats, such as 4-bit or 8-bit signed integers, instead of full-precision floating-point (FP). These methods have been successful in reducing computation costs and are supported by most deep-learning accelerators. Quantization enables performance gains by reducing model size and improving inference speed. For example, applying 8-bit quantization on ResNet100 reduces the model size from 261.2MB to 65.3 MB. Deep learning accelerators like PyTorch can run quantized models 2-4 times faster and reduce memory bandwidth by 2-4 times compared to FP models. However, the exact performance improvements depend on the underlying hardware. After quantization, model weights and parameters need to be tuned and calibrated, which may require access to training data. Face recognition networks also rely on large-scale training datasets like MS1M and VGGFace2. While most recent face datasets are collected from the web, further collection may be limited due to legal privacy issues and regulations like GDPR, which allow individuals to withdraw consent for data usage (Damer et al., 2022).

Security Vulnerabilities: These systems could pose significant security risks due to the use of biometric data, which can be exploited for identity theft and other malicious purposes. To overcome security challenges in FRT, several methods can be employed: **(1)** Conduct white-box or black-box security assessments to improve security. **(2)** Leverage cloud storage for data, as it offers encryption and redundancy, making it more secure (Javaid, 2024)

2.5 Security and Safety Applications of Face Recognition Technology:

Face recognition technology has become a powerful tool for security and safety in various applications. Here's a breakdown of some key areas:

Access Control

Facial recognition systems are widely used for secure access control in buildings, data centres, and restricted areas. Users can gain entry by presenting their face to a camera, eliminating the need for physical keys or cards which can be potentially misplaced or forgotten.

Surveillance

Face recognition is used in public safety and security applications like identifying missing children and disoriented adults, Identifying and finding exploited children, identifying and tracking criminals, and supporting and accelerating investigations[17].

While this can be beneficial for the public safety, concerns exist regarding potential misuse and privacy concerns

Individual identification

Facial recognition is used by law enforcement agencies to identify suspects from surveillance footage or mugshots. It can also be used for facial verification during identity checks[15]

Border Security

Face recognition is increasingly used at border checkpoints to verify traveller identities and expedite immigration processes.

2.7 Application of Face Recognition Technology in UGVs:

Facial recognition is being explored for various applications in robotics, focusing on safety and security applications some examples are:

Security and Monitoring

Robots can use facial recognition to patrol restricted areas, identify authorised personnel, or detect intruders. This can enhance security in warehouses, factories, or other sensitive locations[21]. To go into further details these robots can be deployed autonomously in remote locations or be controlled wireless using a pc or mobile phone where the camera stream can be displayed, reducing the workload of security guards at inconvenient times like night shifts and assisting them in monitoring restricted locations.

Object Recognition and Manipulation

Facial recognition can be combined with object recognition to enable robots to identify and interact with specific people or objects in their environment. This has the potential applications in logistics, manufacturing, and other automated tasks[22]. For instance, in a warehouse setting, train stations, etc, robots could be deployed to locate and retrieve designated items based on the identity of the person.

It’s important to note that the use of facial recognition technology in robotics is still at its early stage. While it holds promise for various applications, challenges regarding accuracy, reliability, and ethical considerations need to be addressed for widespread adoption.

2.8 Analysis of Face recognition for Biometric Authentication

Face recognition technology offers a range of advantages for security and safety applications. However, it also comes with limitations and ethical concerns that need to be critically evaluated.

Advantages:

- **Convenience and speed:** Facial recognition offers a contactless and relatively fast method for access control, identification, and verification. mUsers don't need to carry physical keys or cards, streamlining security procedures.
- **Enhanced Security:** Facial recognition can potentially tighten security by providing a unique biometric that is not as easy to forge in comparison to traditional methods like passwords, keycards, or tickets
- **Improved Efficiency:** In applications like border control, facial recognition can expedite processing times and improve overall efficiency.

Disadvantages

- **Accuracy and Reliability:** Facial recognition accuracy can be affected by factors like lightning, pose, and facial expressions. Additionally, bias on training datasets can lead to inaccurate results for certain demographics.
- **Privacy Concerns:** The collection, storage, and use of facial recognition data raise significant privacy concerns. Potential misuse of this data by governments or corporations requires careful regulation
- **Security Risks:** Facial recognition systems can be vulnerable to hacking or spoofing attacks with masks or deep fakes. Robust security measures are crucial to protect user data and prevent unauthorised access.
- **Ethical Consideration:** The widespread use of facial recognition technology raises ethical concerns, these could **

Biometric Authentication vs Other Authentication Methods

Here a comparison of authentication techniques based on the provided metrics by (Gaber, 2014) :

Usability:

Face Recognition: High usability as it utilises the mobile's camera, requiring minimal user effort.

Fingerprint: High usability, as it involves simply scanning a finger.

Iris Recognition: Medium usability due to the additional step of capturing the iris, which might be less intuitive for users.

Voice Recognition: Medium usability, as it involves speaking a password, which may not be as convenient in noisy environments.

Keystroke: Low usability on touchscreen devices due to the difficulty in capturing keystroke dynamics accurately.

Signature Recognition: Medium usability, depending on the device used (e.g., touchscreen vs. signature pad).

Cost:

Face Recognition: Low cost as it utilises the mobile's built-in camera.

Fingerprint: Low cost as it requires only a fingerprint sensor.

Iris Recognition: Medium cost due to the need for specialised iris scanning hardware.

Voice Recognition: Low cost as it utilises the mobile's microphone.

Keystroke: Low cost as it requires only software implementation.

Signature Recognition: Low cost as it typically utilises existing touchscreen hardware.

Performance:

Face Recognition: Medium performance, depending on lighting conditions and image quality.

Fingerprint: High performance in accuracy and speed.

Iris Recognition: High performance in accuracy but may have longer authentication times.

Voice Recognition: Medium performance, affected by factors such as background noise.

Keystroke: Medium performance, may suffer from accuracy issues on touchscreen devices.

Signature Recognition: Medium performance, accuracy affected by variations in signature style.

Explicit or Implicit Technique:

All techniques except for Keystroke are explicit, requiring direct user interaction.

Robustness against Eavesdropping:

All biometric techniques are generally robust against eavesdropping compared to traditional password-based methods.

Circumvention:

Biometric techniques are susceptible to mimicry or circumvention, especially if the biometric data is compromised.

Traditional techniques may be more susceptible to password sharing or theft.

Continuous Authentication:

All techniques can potentially be used for continuous authentication, depending on implementation.

Please note that how optimal a type of authentication is depends on various factors like location and its specific security requirement.

While limitations exist, facial recognition offers a potentially more secure and convenient alternative to traditional methods in specific scenarios. For instance, in high-security environments where robust access control is necessary, facial recognition could be a valuable tool alongside other security measures (multi-factor authentication). **However, the decision to implement facial recognition should be carefully considered, taking into account specific needs, potential risks, and ethical implications.

Suggested improvements

Multi-Factor Authentication: Combining different authentication methods like passwords, tokens, and fingerprint scanners can offer a more secure alternative than relying solely on facial recognition.

Iris Recognition: Iris recognition offers potentially higher accuracy compared to facial recognition, but it can be less user-friendly due to the need for specialised scanners.

Behavioural Biometrics: Analysing gait, typing patterns, or voice can provide additional security layers without relying on facial features.

The choice of security or safety technology should ultimately depend on the specific context and the level of risk involved. A combination of approaches might often be the most effective solution.

3. Methodology

Face Recognition Model Development

- Data Acquisition and Pre-processing
- Model selection and Training
- Model Evaluation
- Model Conversion

The methodology adopted for training the face recognition system involves utilising transfer learning techniques to retrain a pre-trained MobileNetV2 model. This process integrates a custom dataset with the online dataset, WIDER Face obtained from Kaggle. The aim is to tailor the model to meet the project's objectives for the face recognition software, focusing on individual identification and its access control.

Installing Dependencies: We start by installing necessary dependencies using pip, including TensorFlow for deep learning, OpenCV for image processing, Albumentations for data augmentation, Matplotlib for visualisation, and DropBox for accessing datasets.

Loading Datasets and Annotations: Acquiring and preparing the datasets is crucial for training the face recognition model as it allows the model to learn from a diverse set of facial features and conditions, improving its ability to recognize faces accurately. The model uses images from a custom dataset and the online dataset, WIDER Face stored in a Dropbox folder retrieved using the dropbox API along with their annotations(why use dropbox). The custom dataset was annotated using an online annotation platform Computer Vision Annotation Tool (CVAT).

Data Pre-processing: This step involves preparing the data for training. It includes tasks such as resizing images to a uniform size, normalisation to scale pixel values between 0 and 1, and applying data augmentation techniques like rotation, shifting, shearing, zooming, and flipping are commonly used to artificially increase the variability of the training data and improve the models ability to recognize unseen data.

Model Selection and Definition: The face recognition model architecture is defined using MobileNetV2, alongside being a lightweight convolutional neural network (CNN) architecture its known for its balance between accuracy and efficiency which is why it is carefully selected to achieve the projects objectives of model deployment on a resource-constrained device like an unmanned ground vehicle

Adding Layers: Custom classification layers are added on top of the MobileNetv2 base model. These additional layers are responsible for adapting the features learned by the pre-trained MobileNetV2 model to the specific task of face recognition. Typically, these layers include global averaging pooling, fully connected (dense) layers, and dropout layers to prevent overfitting.

Data Augmentation: Data augmentation techniques are applied to increase the variability of the training data and improve the model’s robustness. These techniques include random rotations, shifts, shears, zooms, and flips applied to the input images. Data augmentation helps the model learn invariant features and reduces the risk of overfitting to the training data.

Model Training : The model is trained using the filtered training image paths. During the training, the model learns to recognize faces by adjusting its parameters (weights) based on the input images and corresponding labels. The training process involves feeding batches of images through the pipeline, computing the loss (error) between the predicted outputs and the ground truth labels, and using optimization algorithms (e.g., Adam Optimizer) to update the model parameters to minimise the loss.

Model Evaluation: The trained model is evaluated on a separate set of validation data to assess its performance. Evaluation metrics such as accuracy and loss are computed to measure how well the model generalises to unseen data. This step helps in determining if the model is overfitting to the training data and provides insights into potential improvements.

Model Deployment: Now that we have a trained and evaluated model, the model can be deployed for real-world applications, This involves integrating the model into a software or hardware system that can process live video streams, detect faces, and recognise individuals in real-time in this case an unmanned ground vehicle that could be used for, individual identification, access control or perimeter control.

Challenges and Fixes developing the model

Accessing Data from DropBox: Initially, there were issues storing images and annotation data as the WIDER Face dataset was too large and attempting to upload this into google drive was tedious. The alternative used was to utilise a cloud storage to store the large files, DropBox in this case and gain access to DropBox storage Dropbox's API the access token.

Other challenges involved correcting image format incompatibility by converting all images to the same file format and navigating image and annotation directories from dropbox, to solve this the images and annotations stored in DropBox were downloaded onto Google Colabs storage system to facilitate easier directory navigation.

Model Deployment

Model Deployment

- Model conversion
- Model Export
- Cloud Deployment
- Edge Deployment

Model Conversion

The face recognition model was trained using a deep learning framework, TensorFlow. TensorFlow the popular open-source machine learning framework developed for building and deploying machine learning models. However, TensorFlow models are not optimal lightweight devices, such as those with resource constrained environments due to their computational complexity and memory footprint. To address this issue the model is converted from a tensorflow model to a tensorflow lite model which is optimised for deployment on devices with the ARM64 architecture.

This guide outlines the process of converting the TensorFlow Keras face recognition model “face_recognition_model.keras” to TensorflowLite and deploying it on a limo device with an ARM64 architecture.

Model Download: The model "face_recognition_model.keras" is saved in Google colab storage environment, to use it it is downloaded into a directory in the limo. Replace with correct code

```
from tensorflow.keras.models import load_model
model = load_model('face_recognition_model.keras')
```

Convert to TFLite: Import the TFLiteConverter class and use it to convert your model:

```python
import tensorflow as tf

converter = tf.lite.TFLiteConverter.from_keras_model(model)
tflite_model = converter.convert()

# Optionally, save the converted model:
with open("converted_model.tflite", "wb") as f:
    f.write(tflite_model)
```

Facial Recognition Algorithms: The project adopts MobileNet, a carefully selected and customised facial recognition algorithm tailored to meet the specific requirements of the project. MobileNet offers a balance between computational efficiency and accuracy, making it suitable for deployment on resource-constrained platforms such as the Raspberry Pi for the UGV.

Virtual Environment: Google Colab and ROS (Robot Operating System) are employed to create a virtual environment that simulates real-world deployment scenarios. This virtual environment enables comprehensive testing and refinement of the facial recognition system, ensuring its robustness and reliability in dynamic operational settings.

User Interface: A user-friendly interface is developed to display individuals' verification results on the Limo AgileX’s touchscreen display. This interface provides actionable insights for system operators, enhancing the usability and effectiveness of the deployed facial recognition system.

Model Integration with UGV

Integration with UGV

- Model Inference
- Camera Integration
- Prediction Display
- User Interaction

Key Challenges:

The project encounters several challenges in its implementation journey, including:

Selection of an efficient and accurate facial recognition algorithm suitable for resource constrained platforms, such as raspberry pi for the UGV, ultimately leading to the adoption of MobileNet.

Seamless integration with ROS to ensure cohesive system functionality.

Addressing data security and privacy concerns associated with the storage and processing of facial data within the system.

Optimizing for the system for real-time performance on the UGV, balancing computation efficiency with accuracy and reliability

Handling challenges such as varying lighting conditions, diverse poses, and occlusion in facial images

-

References

Ahonen, T., Hadid, A., & Pietikäinen, M. (2006, October 30). *Face Description with Local Binary Patterns: Application to Face Recognition*. ieeexplore.ieee.org. Retrieved April 20, 2024, from https://ieeexplore.ieee.org/document/1717463

Biometrics questions: privacy, consent, function creep. (n/a, n/a n/a). Thales. Retrieved April 16, 2024, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometrics-questions

Buolamwini, J., & Gebru, T. (2024, February 28). *Facial recognition system*. Wikipedia. Retrieved April 20, 2024, from https://en.wikipedia.org/wiki/Facial_recognition_system

Chihaoui, M. (2016, September 28). *Computers | Free Full-Text | A Survey of 2D Face Recognition Techniques*. MDPI. Retrieved April 20, 2024, from https://www.mdpi.com/2073-431X/5/4/21

Damer, N., Kuijper, A., & Boutros, F. (2022, June 21). arXiv. Retrieved April 16, 2024, from https://arxiv.org/pdf/2206.10526.pdf

Dharaiya, D., & Davies, R. (2020, March 10). *Face Recognition Technology Past, Present, and Future*. ReadWrite. Retrieved April 17, 2024, from https://readwrite.com/history-of-facial-recognition-technology-and-its-bright-future/

Dharaiya, D., & Good, O. (2020, March 10). *Face Recognition Technology Past, Present, and Future*. ReadWrite. Retrieved April 16, 2024, from https://readwrite.com/history-of-facial-recognition-technology-and-its-bright-future/

Duong, C. K. (2020, September 03). *MobiFace: A Lightweight Deep Learning Face Recognition on Mobile Devices*. IEEE. Retrieved April 25, 2024, from https://ieeexplore.ieee.org/abstract/document/9185981

Farooq, E., & Borghesi, A. (2023, n/a n/a). *A Federated Learning Approach for Anomaly Detection in High Performance Computing*. IEEE Xplore. Retrieved April 16, 2024, from https://ieeexplore.ieee.org/document/10356584

F. De la Torre, J. Salido, G. Bueno, & O. Déniz. (2011, January 20). *Face recognition using Histograms of Oriented Gradients*. Science Direct. Retrieved April 20, 2024, from https://www.sciencedirect.com/science/article/pii/S0167865511000122

Felea, I, & Dogaru, R. (2020). *Improving Light-weight Convolutional Neural Networks for Face Recognition Targeting Resource Constrained Platforms*. Retrieved April 25, 2024, from https://www.esann.org/sites/default/files/proceedings/2020/ES2020-185.pdf

Fontenot, S. (2020, December 4). *Study Outlines What Creates Racial Bias in Facial Recognition Technology*. News Center. Retrieved April 20, 2024, from https://news.utdallas.edu/science-technology/racial-bias-facial-recognition-2020/

Gaber, T. (2014, February). *Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues*. Research Gate. Retrieved April 25, 2024, from https://www.researchgate.net/publication/268388162_Biometric_and_Traditional_Mobile_Authentication_Techniques_Overviews_and_Open_Issues

GDPR and Biometric Data: Privacy Implications and Regulatory Compliance. (n.d.). gdpr-advisor.com. Retrieved April 17, 2024, from https://www.gdpr-advisor.com/gdpr-and-biometric-data-privacy-implications-and-regulatory-compliance/

Geng, C., & Jiang, X. (2010, February 17). *Face recognition using sift features*. ieeexplore.ieee.org. Retrieved April 20, 2024, from https://ieeexplore.ieee.org/document/5413956

Gray, P. (2022, August 31). *Ethical issues of facial recognition technology*. TechRepublic. Retrieved April 16, 2024, from https://www.techrepublic.com/article/ethical-issues-facial-recognition/

Howard, A. (2017, April 17). *1704.04861v1 [cs.CV] 17 Apr 2017*. arXiv. Retrieved April 25, 2024, from https://arxiv.org/pdf/1704.04861

Javaid, S. (2024). *Top 4 Facial Recognition Challenges & Solutions in 2024*. Research AIMultiple. Retrieved April 16, 2024, from https://research.aimultiple.com/facial-recognition-challenges/

Junyan Dai. (2020). *Real-time and accurate object detection on edge device with TensorFlow Lite*. iopscience. Retrieved April 25, 2024, from https://iopscience.iop.org/article/10.1088/1742-6596/1651/1/012114/pdf

K, S. (2023, September 6). *What is BIometric Spoofing and How To Prevent It*. Facia.ai. Retrieved April 16, 2024, from https://facia.ai/blog/biometric-spoofing/

Miller, S. (2022, July 20). *The basics, usage, and privacy concerns of biometric data*. Thomson Reuters. Retrieved April 17, 2024, from https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data

Moen, A. (2021, December 8). *A Brief History of Biometrics*. BioConnect. Retrieved April 16, 2024, from https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/

Morais, L. (2020, May 6). *Biometric Data: Increased Security and Risks | 2020-05-06*. Security Magazine. Retrieved April 16, 2024, from https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks

Peng, J., Wang, X., Guo, Y., Wang, Y., Bihui Chen, & Zhang, S. (2022, December 26). *A Survey of Face Recognition*. arxiv. Retrieved 04 17, 2024, from https://arxiv.org/abs/2212.13038

Radwan, A. (2024, April 2). *The Rise of Biometric Security: Implications for Personal Privacy The Rise of Biometric Security*. Internet Safety Statistics. Retrieved April 20, 2024, from https://www.internetsafetystatistics.com/biometric-security-risks/

Sandler, M. (2018, December 16). *IEEE*. MobileNetV2: Inverted Residuals and Linear Bottlenecks. Retrieved April 25, 2024, from https://ieeexplore.ieee.org/document/8578572

Setiowati, S., Zulfanahri, Franita, E. L., & Ardiyanto, I. (2018, January 11). *A review of optimization method in face recognition: Comparison deep learning and non-deep learning methods*. ieeexplore. Retrieved April 25, 2024, from https://ieeexplore.ieee.org/abstract/document/8250484

Sik-Ho Tsang. (2019, May 19). *Review: MobileNetV2 — Light Weight Model (Image Classification) | by Sik-Ho Tsang*. Towards Data Science. Retrieved April 25, 2024, from https://towardsdatascience.com/review-mobilenetv2-light-weight-model-image-classification-8febb490e61c

Ul Ghani, M. A. N., She, K., & Saeed, M. U. (2024, March 21). *Enhancing facial recognition accuracy through multi-scale feature fusion and spatial attention mechanisms*. AIMS press. https://www.aimspress.com/article/doi/10.3934/era.2024103?viewType=HTML#b31

The University of Cambridge. (2022, October 27). *UK police fail to meet 'legal and ethical standards' in use of facial recognition*. University of Cambridge. Retrieved April 20, 2024, from https://www.cam.ac.uk/research/news/uk-police-fail-to-meet-legal-and-ethical-standards-in-use-of-facial-recognition

Yipeng Sun, & Andreas M. Kist. (n.d.). *DEEP LEARNING ON EDGE TPUS*. arxiv. Retrieved April 25, 2024, from https://arxiv.org/pdf/2108.13732.pdf