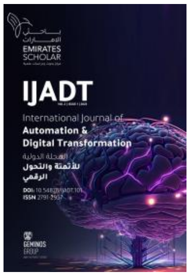


International Journal of Automation and Digital Transformation
Vol 1 Issue 1 (2024)
Pages (19 – 35)

Available at www.emiratesscholar.com

ARIF: Autonomous Recognition in the Field

Enhancing National Security with Computer Vision-Based Facial Recognition

Abubakr Osama Abubakr Osman

Bachelors of Computer Science, University of Medical Science & Technology

Abstract

Through a novel research approach that employs a mix of Convolutional Neural architectures & Siamese Neural Nets, we propose a viable mechanism that focuses on leveraging these groundbreaking advancements, through the utilisation of deep learning algorithms we were able to effectively & accurately identify and authenticate individuals based on unique facial features derived from machine learnt embeddings.

In The ARIF Project we implement the proposed architecture models through utilisation of developer friendly modules like the python facial recognition library, the OpenCV framework & Jupiter Notebooks, performing the necessary product development, market research and product analysis throughout the development process, finally deliver a refined & minimalistic solution that not only fills market gaps but also serves as a solid foundation for rapid adoption & deployment.

Keywords: *biometrics, facial recognition, AI, ML, Computer Vision, Identification, Security, National Security, Homeland Security, Siamese Neural Networks, Convolutional Neural Networks*

Email Address: mrabubakrosama@gmail.com

1. Chapter 1: Introduction

1.1. Introduction

Over the past few years Sudan has experienced unprecedented growth in terms of local crime rate, these crimes range from petty to violent crime [1]. It's underdeveloped and under-equipped nations like Sudan that continue to witness surges in criminal activity [2].

In aims of combating such negative phenomena, we address the existing drawbacks of traditional security procedures and propose alternative digital approach techniques to achieve effective and scalable Security.

Driven by Recent developments within the field of Machine Learning, Facial Recognition systems have come to play a crucial role in ensuring & improving security & effectively combating such negative phenomena [3], through the accurate identification and authentication of personnel, the field of biometrics has been able to experience significant progress.

We provide an in-depth overview of our computer vision-based facial recognition system, it's implications for security & particularly it's role in the enhancement of both private & national security.

Utilising advanced Machine Learning algorithms our system is able to extract, analyse, and match distinctive facial features through an in-house recognition protocol, producing both reliable & fast results. Through employment our proposed approach we were able to achieve improved accuracy and reliability in contrast to traditional systems positioning our technique as both a viable and more effective alternative to current systems.

We begin our initial phase through integration of modern facial recognition techniques, where it is our core belief that the integration of computer vision-based facial recognition & biometrics in general into modern security frameworks & particularly national security offers applicants several advantages. Through the enablement of accurate, efficient & rapid identification, our system allows the designated authorities to effectively identify potential threats or people of interest, improving the overall quality of security services [4]. Furthermore, through inhouse Facial indexing, we provide law enforcement agencies & security personnel control over their data, allowing them maintain their privacy while still being able to rapidly identify & neutralise bad actors.

In conclusion, this project will not only go in-depth into what it takes to implement such systems but will also assess their overall validity & applicability.

1.2. Problem Statement

The Nation of Sudan currently faces major security challenges represented by rising crime rates & poor national security. As an under developed nation, Sudan is burdened with limited resources and poor overall infrastructure, it is for those reasons that we find traditional security measures inadequate at efficiently addressing those issues. Moreover, we find that the heavy reliance on human personnel in these traditional security systems is both resource-intensive and time-consuming, not to mention the increased risks involving humanintroduced errors and inefficiency, these factors together act as hinderances to operational performance, scalability and overall effectiveness, resulting in an overall poor delivery of security services.[5]

1.3. Research question

How can the integration of facial recognition technology into modern Sudanese security frameworks address the challenges posed by rising crime rates and poor security measures?

1.4. Research Aims

In this project our primary aim is to propose an effective & scalable security framework, providing all the supporting documentation which highlights the transparent investigation of the proposed systems & it's potential benefits, furthermore in this project we lay a solid foundation for the systematic integration of facial recognition technology into modern Sudanese security frameworks.

Specifically, it is our ultimate aim to address the challenges posed by rapid rise of crime rates and poor security protocols through the following framework:

1. Analysis of the current state of security in Sudan: This research aims to assess the existing security landscape in Sudan, including the nature and extent of crime rates, the shortcomings of traditional security measures, and the specific challenges faced by law enforcement agencies and security personnel.
2. Explore the capabilities of facial recognition technology: The research aims to examine the capabilities and limitations of facial recognition technology, particularly in the context of improving security measures. This includes understanding the underlying algorithms, data

requirements, accuracy rates and the potential applications of these facial recognition systems.

3. Evaluate the feasibility of facial recognition integration: This research aims to determine the technical feasibility and practical considerations of integrating facial recognition technology into the Sudanese security framework. It explores factors such as infrastructure requirements, data privacy concerns, training and deployment of the technology, as well as potential interoperability with existing systems.
4. Assess the impact on crime prevention and national security: This research aims to assess the potential impact of facial recognition technology on crime prevention and overall national security in Sudan. This includes evaluating its effectiveness in identifying potential threats, enhancing investigative processes, reducing response times, and improving the overall quality of security services.
5. Examine the projects possible Ethical and Legal Implications: This research aims to examine the ethical and legal implications associated with the use of facial recognition technology in security procedures. This includes considerations related to privacy, data protection, potential biases or discrimination, and compliance with relevant laws and regulations.
6. Provide recommendations for implementation: Based on the findings from the research, this study aims to provide practical recommendations for the successful implementation of facial recognition technology into the Sudanese security framework. These recommendations will consider the identified challenges, feasibility assessments, and ethical considerations, aiming to guide policymakers, law enforcement agencies, and relevant stakeholders in adopting effective and responsible practices.

By addressing these research aims, this study aims to contribute to the knowledge and understanding of how facial recognition technology can be effectively utilised to address the challenges faced by the current Sudanese security systems, ultimately leading to improved crime prevention and enhanced national security.

1.5. Methodology

The methodology for this project involves utilising tools such as Python, OpenCV, and Jupyter Notebooks. Various Techniques such as facial recognition, data pre-processing, post-processing, secure storage, motion detection and data encryption & not to mention their effective employment.

The importance of our proposed project lies in several factors like enhancement of security protocols, prevention of crime and effective investigation & followup, improved border control and immigration management & last but not least facilitation of efficient travel procedures. The projects has several expected outcomes including improved security measures, reduced crime rates, enhanced security procedures both on a national level & private level, improved efficiency and effectiveness and a transparent & critical assessment of the system validity & applicability.

This project scope also encompasses development, deployment, and evaluation of the proposed facial recognition-based techniques, providing relevant documentation and sharing the project schematics with the scientific community and public.

1.6. Research Importance

1. Enhancement of Security Protocols: As a primary goal, this research aims to provide a contribution to the enhancement of national security. Providing a guideline to the implementation & deployment of machine-based facial recognition systems, allows the proper authorities to accurately and efficiently identify individuals, detect potential threats and take appropriate actions promptly, improving overall security both at a national & private level.
2. Crime Prevention and Investigation: Our system provides law enforcement agencies the crucial aid they need to better prevent crime and investigate criminal activity. Through fluent comparison of facial recognition metrics against existing databases, our system is able to rapidly facilitate suspect identification and assistance.
3. Border Control and Immigration Management: In the context of border control and immigration, facial recognition technology plays a vital role, expediting personnel identification & providing autonomous border surveillance. Through the accurate identification of individuals for example, immigration authorities can better manage immigration procedures and ensure only authorised individuals may enter or exit.
4. Efficient Travel Procedures: The integration of facial recognition into the national security framework can also significantly expedite travel

procedures & protocols. Possibly Eliminating the need for legal documents in the future & reducing queue wait times through automated customer response systems. Deployment of our proposed system holds huge potential in the elimination of lengthy manual identity checks and allows travellers to experience a streamlined travel experience.

5. Technological Advancement: Research into FRT and their implementations allows those who adopt it to contribute to the advancement of technological & security. Steps like this Led to the development of more accurate, reliable, and efficient algorithms and systems, benefiting the various sectors that adopt & work on these systems.

1.7. Expected Outcomes

- Improved security measures: Through careful integration of Advanced Facial Recognition Technology into existing security systems, we are able to enhance the overall security process, accurately identify and authenticating personnel & evidently leading to improved security measures.
- Reduction in crime rates: Through improving the performance of our current security systems, we anticipate a marginal reduction in crime rates, this would be due to the improved accuracy of personnel identification and the overall improvement in system responsiveness .
- Enhanced national security: The integration of facial recognition technology into national & private security frameworks would provide several advantages on a national level. Aiding law enforcement agencies and security personnel alike in rapid identification and neutralisation of potential threats, strengthening border control procedures, improving immigration procedures and expediting travel all together.
- Improved system efficiency and overall effectiveness: The implementation of advanced machine learning algorithms in the field and the process of in-house recognition leads to an improvement in overall accuracy, reliability, and speed. This results in more efficient security operations and improved resource utilisation.
- A Transparent & Critical Assessment of System Validity and applicability: Conclusively our research explores the validity and applicability of the proposed system in context of crime prevention & security, providing a comprehensive evaluation of the proposed system, a look into its benefits, limitations & implementation strategies.

1.8. Project Scope

This project's focuses mainly on the develop and deployment of comprehensive facial recognition-based security initiatives, both for private and public use cases, our main aim is to address drawbacks in traditional security procedures through leveraging modern facial recognition technology and machine learning algorithms.

Specifically, the project will focus on the following objectives:

1. Construction of a digitally driven security system for the identification and neutralisation of bad actors: The proposed system would utilize facial recognition technology to accurately identify and authenticate individuals, enabling law enforcement agencies and security personnel alike to both detect and neutralise potential threats effectively.
2. Development of secure system to aid border control and immigration affairs: In this project we deploy facial recognition technology to expedite personnel identification and provides autonomous surveillance. Helping the targeted authorities manage immigration procedures more efficiently and ensure authorisation policies are enforced.
3. Development of a system to expedite and oversee travel procedures: The integration of our proposed facial recognition technology into our preexisting national security frameworks allows us to streamline travel procedures, reducing queue wait times through automated systems. It would even eliminate the need for physical documents in the near future.

2. Chapter 2: Literature Review

2.1. Introduction

In this Chapter, we conduct a comprehensive literature review to explore the existing body of knowledge related to security systems & facial recognition systems along with their applications in the field of security. This literature review serves as a foundation for understanding the current state of research, identifying gaps, and informing the development of facial recognition-based security initiatives like this one.

2.2. Overview

Facial recognition technology has garnered significant attention in recent years due to its potential to revolutionise security practices. Numerous studies have investigated the effectiveness of facial recognition systems in various domains, including law enforcement, border control, and public safety agencies. By analysing these studies, we aim to gain insights into the strengths, limitations, and practical considerations associated with implementing facial recognition technology for crime prevention and national security enhancement.

This literature review begins by examining the theoretical foundations of facial recognition technology, delving into the underlying principles of face detection, feature extraction, and matching algorithms. We explore the advancements in machine learning techniques, such as convolutional neural networks (CNNs)[6] & Siamese Neural Networks[7], which have significantly contributed to the accuracy and efficiency of facial recognition systems. Moreover, we investigate the role of biometrics, including facial landmarks and unique facial features, in enhancing the identification and authentication processes.

Next, we explore real-world applications of facial recognition systems in security frameworks. This includes an examination of case studies where facial recognition technology has been successfully deployed in law enforcement agencies, airports, and other critical infrastructure facilities. We also analyse the impact of these systems on crime prevention, suspect identification, and overall security operations.

Additionally, we assess the ethical and privacy considerations surrounding the use of facial recognition technology [8]. As facial recognition involves the collection and processing of sensitive personal data, it is crucial to address concerns related to privacy infringement, bias, and potential misuse. By reviewing existing literature on these topics, we aim to develop an ethical framework and privacy guidelines for the implementation & deployment of our facial recognition-based security initiative in Sudan.

This literature review concludes with a synthesis of key findings and a discussion of the gaps and limitations in the current body of knowledge. By identifying these gaps, we lay the groundwork for our research contributions and provide insights into areas that require further investigation.

Overall, this literature review serves as a critical examination of the existing research on facial recognition systems and their applications in security. It provides a comprehensive understanding of the theoretical foundations, real-world applications and ethical considerations associated with implementing facial recognition technology for crime reduction, national security enhancement, and improved security procedures.

2.3. Current System

The current traditional security system in Sudan relies heavily on human actors and conventional security protocols. However, this system poses several key drawbacks that hinder its effectiveness and scalability.

The resource-intensive and time-exhaustive nature of traditional security procedures pose several challenges in combating the growing crime rates in the country.

Moreover, relying solely on human intervention introduces the possibility of human error and inefficiency, which can compromise the overall performance and capability of the security process.

Traditional security protocols in Sudan also lack the integration of advanced technological solutions and rely heavily on manual identification and authentication techniques, this often leads to delays in the identification of potential threats or people of interest, hindering the timely response of concerned authorities.

Additionally, the absence of a comprehensive national databases and the lack of an efficient data management system limits the nation's ability to effectively track and monitor criminal activities.

Due to this factors & the underdeveloped and under-equipped nature of Sudan's security infrastructure, the existing traditional security system faces difficulties in ensuring the safety and security of both private and public entities, further contributing to the heavy struggle to address the rising rate of crimes that have been plaguing the nation in recent years.

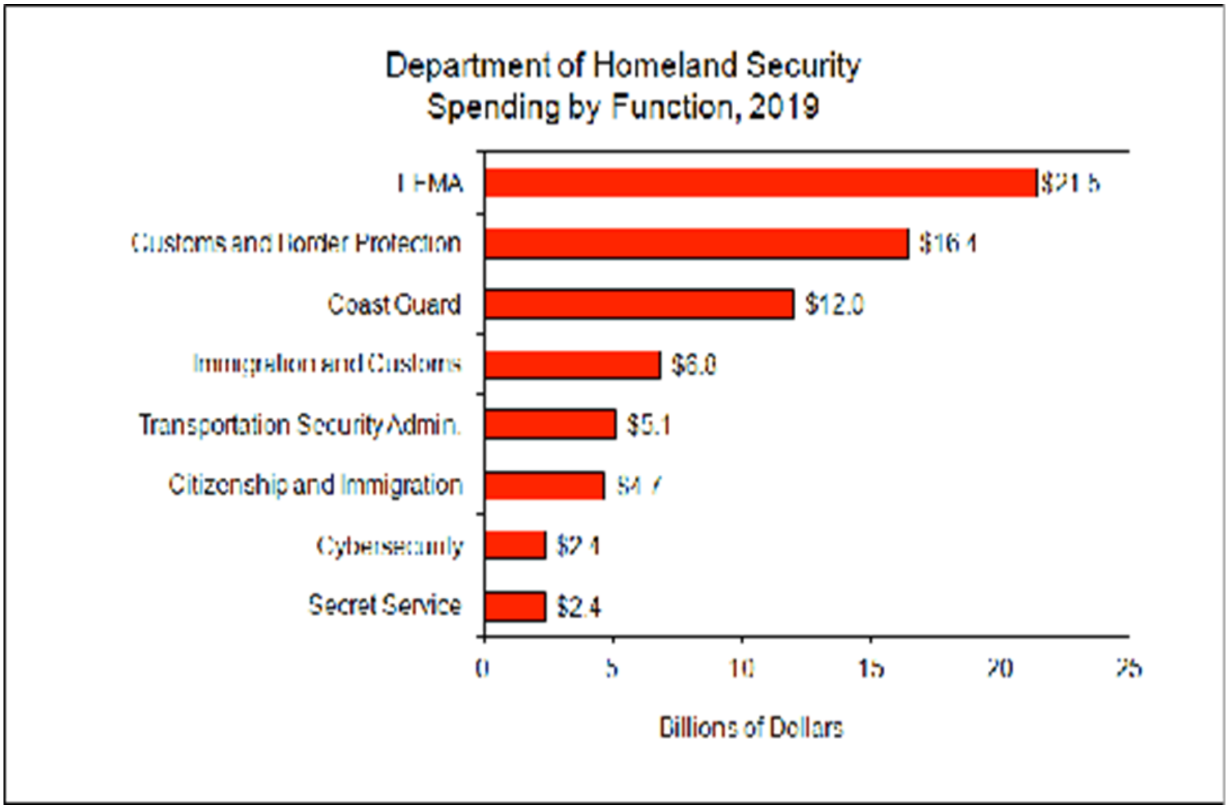


Fig 2.1 Shows the US Department of Homeland Security's annual spending report for the year 2019[9].

2.4. System Benefits

1. Enhanced Security: By integrating facial recognition technology into existing security frameworks, the system enhances overall security measures. It enables the accurate identification and authentication of individuals, helping authorities detect and neutralise potential threats effectively & rapidly. Improving security both at a national and private level.
2. Crime Prevention and Investigation: The proposed system provides much needed aid to local law enforcement agencies in the prevention and investigation of crime. Through fluent comparison of facial recognition metrics against in-house databases, it allows for the facilitation of rapid suspect identification and provision of valuable assistance to criminal investigations.
3. Efficient Border Control and Immigration Management: Facial recognition technology plays a vital role in border control and immigration management. It not only expedites personnel identification & automates border surveillance but also assists immigration authorities in efficient management procedures. It primarily ensures that only authorised individuals enter or exit controlled border,
4. strengthening the overall border control mechanisms & measures. Streamlined Travel Procedures: Integration of facial recognition mechanisms into national security frameworks can significantly expedite travel procedures and protocols. Its a key initiative that holds significant potential for the elimination of physical documents in the future, it also promotes a reduction in overall queue wait times through customer-response system automation, providing travellers with streamlined and hassle-free travel experiences, while serving security purposes.
5. Technological Advancement: Research and implementation of facial recognition systems contributes first and foremost to the advancement of technology not only in the field of security but in the field of computer vision itself. Leading to the development of more accurate, reliable, and efficient algorithms and systems, this is a factor that not only benefits the security sector but also the various other sectors that adopt and deploy on these systems.

6. Improved System Efficiency and Effectiveness: The system's utilisation of advanced machine learning algorithms and in-house recognition protocols leads to improved accuracy, reliability, and speed. This translates into more efficient security operations, optimised resource utilisation, and enhanced overall effectiveness in identifying and responding to security threats.
7. A Transparent & Comprehensive Assessment: This project also provides a critical assessment of the validity and applicability of the proposed facial recognition system. Through clear evaluation of system benefits, limitations, and implementation strategies, this research contributes to the betterment of understanding of these systems and their potential, helping guide future advancements in this vast field.

2.5. Related work

- **FaceFirst:**

FaceFirst is an operator of a facial recognition software platform designed to prevent fraud, security risks and public safety threats. The company's platform offers surveillance, mobile and desktop forensic face detection capabilities to detect and deter stalkers, corporate spies, known criminals and disgruntled employees, thereby enabling retailers, law enforcement agencies, transportation hubs, militaries and corporations to maintain security and privacy.

- **OpenCV:**

OpenCV is a great python library that allows developers to integrate image processing and computer vision algorithms into their programs. It is completely open-sourced and allows developers to incorporate various features like face detection, objection tracking, landmark detection, and much more.

- **Siamese Neural Networks:**

In a nutshell, a Siamese neural network is a type of neural network architecture that is designed to compare or measure similarity between pairs of inputs. It gains its name from the famous concept of Siamese twins, as the network is usually composed of two identical subnetworks that share the same weights and architecture.

The main purpose of a Siamese network is to learn a similarity metric between these inputs. Taking in pairs of inputs & passing each input through one of it's subnetworks, it then combines the outputs to compute a similarity score or distance metric. A Siamese Neural Network is trained on labeled pairs of inputs, where the desired output is a known similarity or dissimilarity between the pairs.

Siamese networks are commonly used in tasks such as facial recognition, signature verification, image retrieval, and natural language processing. Through learning a similarity metric, the network can effectively determine if the two inputs belong to the same class or category.

Overall, Siamese neural networks offer a powerful approach for learning and comparing similarities between pairs of inputs, enabling various applications in pattern recognition and similarity-based tasks.

- **Convolutional Neural Networks:**

Convolutional Neural Networks or CNNs in short, are a type of deep learning model commonly used in facial recognition tasks. CNNs are particularly wellsuited for image processing tasks due to their ability to autonomously learn and extract meaningful features from raw pixel data.

In the context of facial recognition, CNNs can be trained to analyse facial images and extract important features such as the shape of a face, presence of specific facial landmarks (e.g., eyes, nose, mouth) and textural patterns. These extracted features can then be used for classification or identification of individuals.

The architecture of a CNN consists of multiple layers, including convolutional layers, pooling layers, and fully connected layers. In the initial layers, CNNs apply convolutional filters to input images, this helps detect local patterns and features. The subsequent pooling layers reduce spatial dimensions of feature maps, making the network more computationally efficient. Finally, the fully connected layers process the high-level features and make predictions regarding the identity of the person in the image.

During the models training phase, CNNs learn to recognise facial features and discriminate between different individuals by adjusting the weights of their layers using a process known as back-propagation and gradient descent. Training data typically includes large numbers of labeled facial images, allowing the network to learn patterns and generalise to unseen examples.

Once trained, CNNs can be used for facial recognition by feeding them with input images and obtaining predictions about the identity of the person/people depicted. This may be achieved by comparing the extracted features from the input image with the features of known individuals stored in a database.

Overall, CNNs have proven to be highly effective in facial recognition tasks, achieving state-of-the-art performance and enabling various applications such as biometric identification, surveillance systems, and access control.

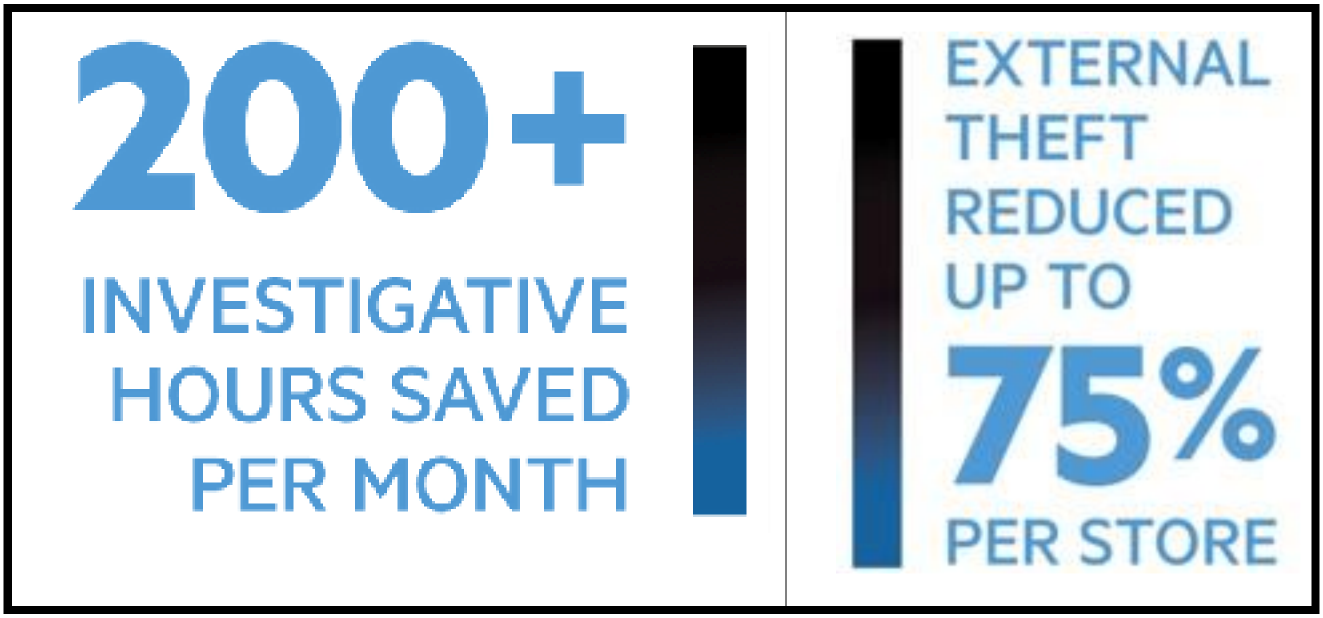


Fig 2.2 Shows the Impact of FaceFirst on current security ecosystem according to it's website[10].

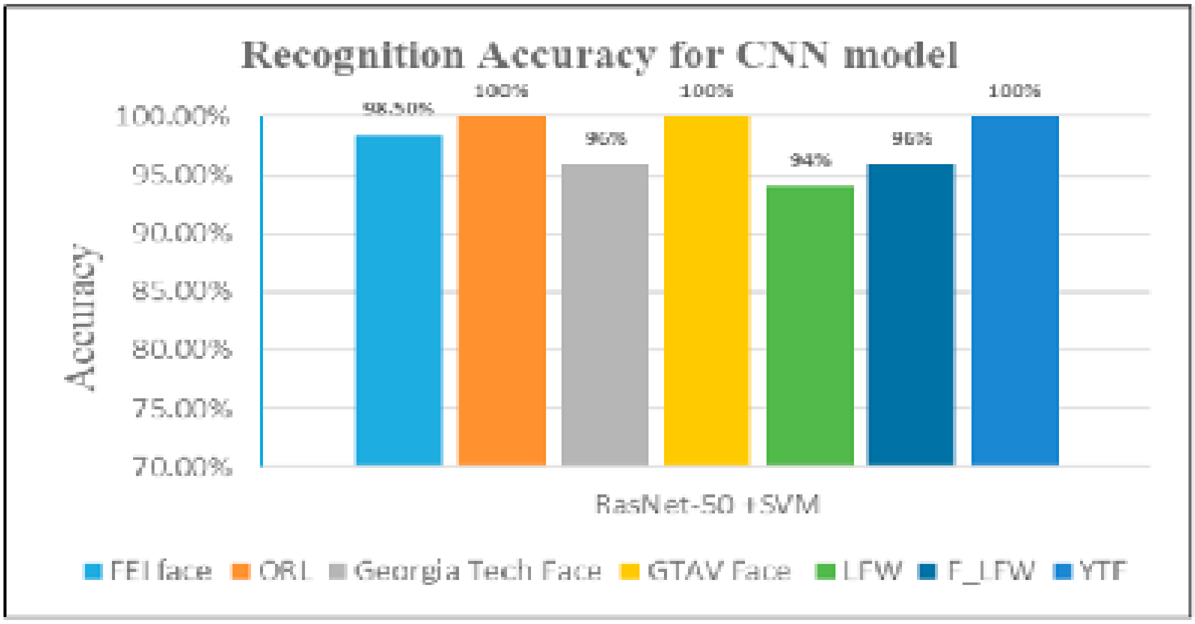


Fig 2.3 Shows the Accuracy of the ResNet-50 +SVM model on facial recognition databases[11]

- **face_recognition**

face_recognition is a simple & intuitive python library that allows developers to recognise and manipulate faces from Python or from the command line. The library was built using dlib's state-of-the-art face recognition algorithms. The model touts an accuracy of 99.38% on a popular benchmark known as Labeled Faces in the Wild.

- **ClearViewAI:**

ClearviewAI is an American facial recognition company, providing facial recognition software to companies, law enforcement agencies, universities, and individuals alike. The company's algorithm matches faces to a database of more than 20 billion images indexed from the various Internet sites, including but not limited to social media applications & blogs.

- **PimEyes:**

PimEyes touts itself as online facial search engine, it operates by going through the Internet to find pictures containing given faces. PimEyes uses face recognition search technologies to perform reverse image searches. Find faces and checking where the images appear online.

Project Name	Functionality
Face First	The operator of a facial recognition software platform designed to prevent fraud, security risks and public safety threats.
OpenCV	An Open Sourced python library that allows developers to integrate image processing and computer vision algorithms into their programs.
Siamese Neural Networks	A type of neural network architecture that is designed to compare or measure similarity between pairs of inputs.
Convolutional Neural Networks	A type of deep learning model that employ convolutions and are commonly used in facial recognition tasks.
face_recognition	A python library that allows developers to recognise and manipulate faces from Python or the command line.
ClearViewAI	A company providing facial recognition software to companies, law enforcement agencies, universities, and individuals alike.
PimEyes	An online facial search engine, that scrapes the web to find picture matches.

3. Chapter 3: Methodology

3.1. Introduction

This Chapter describes the projects research design, data collection methods and analytical techniques employed to address the research objectives outlined in chapters 1 & 2. Our methodology revolves around providing a systematic approach for investigating the various potential benefits and effectiveness of integrating facial recognition techniques into a modernised Sudanese security framework.

3.2. Research Design

This research adopts a mixed-methodical approach, combining both quantitative and qualitative research procedures to gather comprehensive data and insights. Choosing this approach allows for a more holistic understanding of the research topic discussed and facilitates the triangulation of said findings.

3.2.1. Data Collection

Quantitative Data

Quantitative data will be collected through a combination of primary & secondary sources. Primary data will be obtained through surveys and questionnaires administered to law enforcement agencies, security personnel, and relevant stakeholders involved in the Sudanese security management process. The survey questions will be designed to gather information on crime rates, existing security measures, challenges faced, and perceptions regarding the integration of facial recognition technology. The sampling technique will involve purposive sampling to ensure representation of different regions and security agencies within Sudan.

Secondary data will also be collected from official reports, government publications, academic journals and databases related to crime rates, security policies and advancements in facial recognition technology. This data will provide a contextual understanding of the current state of security in Sudan and serve as a basis for the comparison and validation of primary data.

Qualitative Data

Qualitative data will be collected through interviews with key informants, including representatives from law enforcement agencies, security experts, policymakers, and civil society organisations. Semi-structured interviews will be conducted to explore their perspectives, experiences, and opinions regarding the integration of facial recognition technology. The interviews will be audio-recorded with the participants' consent and transcribed verbatim for analysis.

3.2.2. Data Analysis

The collected data will be analysed using the appropriate quantitative and qualitative methods.

Quantitative data analysis will involve descriptive statistics, such as frequencies and percentages, to summarise survey responses. For Statistical Analysis we have chosen Excel as our employed tool, which we will use for data management and analytics. We will then present our results in the form of tables, charts and graphs for better & improved visualisation and interpretation.

Qualitative data analysis will involve thematic analysis, where interview transcripts will be coded and categorised to identify recurring themes and patterns. This analysis will allow for a deeper understanding of the participants' perspectives and insights related to the integration of facial recognition technology. Software, such as NVivo & ATLAS.ti, will be used for organising and analysing qualitative data.

3.2.3. Ethical Considerations

Ethical considerations will be given the utmost importance throughout the research process. Informed consent will be obtained from all participants involved in surveys and interviews, ensuring their anonymity and confidentiality. The research will follow ethical guidelines & regulations regarding data protection, privacy, and informed consent set by relevant institutions and governing bodies.

3.2.4. Limitations

It is important to acknowledge certain limitations that may arise during the research process. These limitations include potential biases inherent in the survey responses, limited availability of comprehensive secondary data and various constraints associated with time and resource limitations. However, efforts will be made to mitigate these limitations by employing rigorous data collection methods and conducting thorough analysis.

3.3. Technical Requirements:

In this section we will outline the various tools, languages, functional and nonfunctional requirements associated with this project's undertaking.

3.4. Tools:

- **Python:**

Python is a popular high-level programming language known for its simplicity and readability. It has a wide range of applications, including web development, data analysis, artificial intelligence, machine learning, and automation. Python's extensive libraries and frameworks make it versatile and suitable for various tasks, which is why we will be basing our core functionality around the python language.

- **OpenCV:**

OpenCV (Open-Source Computer Vision Library) is an open-source computer vision and machine learning software library. It provides a set of tools and functions that help developers and researchers in image and video processing, object detection, facial recognition, and more. OpenCV supports multiple programming languages, including Python, C++, and Java.

- **Google Collaboratory:**

Google Colab is a cloud-based integrated development environment (IDE) provided by Google. It allows users to write and execute Python code directly in their web browser. Colab offers free access to computing resources, including GPUs and TPUs, making it popular among data scientists and machine learning practitioners. It also enables collaboration by allowing users to share notebooks with others.

- **Jupiter Notebook:**

Jupyter Notebook is an open-source web application that allows interactive computing in several programming languages, including Python. It provides an environment where users can create and share documents called "notebooks" containing live code, equations, visualisations, and explanatory text. Jupyter Notebook supports data exploration, prototyping, and data analysis workflows.

- **Microsoft Excel:**

Microsoft Excel is a widely used spreadsheet program that allows users to organise, analyse, and visualise data. It offers a variety of features, including formulas, functions, charts, pivot tables, and macros.

- **NVivo:**

NVivo is a qualitative data analysis software developed by QSR International. It assists researchers and analysts in organising, coding, and analysing unstructured data, such as text, audio, video, and images. NVivo provides tools for data exploration, text mining, thematic analysis, and visualisation, making it valuable in social sciences, market research, and other qualitative research domains.

- **Apple Pages:**

Apple Pages is a word processing and desktop publishing software developed by Apple. It is part of the iWork productivity suite and is available on macOS, iOS, and iPadOS. Pages offers a range of features for creating and formatting documents, including templates, styles, graphics, and collaboration tools. It supports importing and exporting files in various formats, making it compatible with other popular word processing software.

3.5. Components:

- The Core Face Recognition Program.
- Our Own Custom In-House DataBase Software.
- An Encrypted Facial Encodings Dataset
- An Encrypted Face Images Dataset.

3.6. Programming Languages:

- HTML, CSS & Javascript.
- Python.
- XML.
- Git.
- JSON.
- Bash.

3.7. Functional requirements:

Defines the various expected components, functionalities, components, architectural designs & interactions:

- Easy Setup.
- User Login.

- User Accesses the DataBase.
- User Performs a Query.
- Administrator Manages the Database.
- Administrator checks the Action Logs.
- Administrator Registers & Manages Users & DataBase Access.
- Each User is issued a secure Username & Password.
- Administrator Manages Security.

3.8. NON-FUNCTIONAL REQUIREMENTS

- The Service should be Up 24/7 & Should be Backed up and Secured.
- The Software Should be easy to setup, use & manage.
- Should be able to handle several requests simultaneously.
- Requesting process should be fast.
- Login & Data Queries should be fast.
- The database & software should be highly secure bnmand provide a high level of encryption.

3.9. UML DIAGRAMS:

The unified modelling language provides a general purpose, developmental, modelling language within the field of software engineering, this language is intended to provide a standard way to visualise system design.

3.11. UML Use Case Diagram:

The purpose of a use case diagram in UML is to demonstrate the different ways that a user's might interact with our proposed system model.

3.10. Flow Chart Diagram:

A flowchart diagram depicts the processes, system interactions or computational algorithms used in a project implementation. Flow Chart Diagrams are widely used in multiple fields for the purposes of documentation, studies, planning, improvement and communication, outlining complex processes in clear, easy-tounderstand diagrams.

Flowcharts, sometimes spelled as flow charts, use rectangles, ovals, diamonds and potentially numerous other shapes to define the types of steps used in a project implementation, they are often used along with connecting arrows to define process flow and sequencing. FC diagrams range from simple & hand-drawnchartsto comprehensive computer drawn diagrams that depict multiple steps and routes in a project sequence

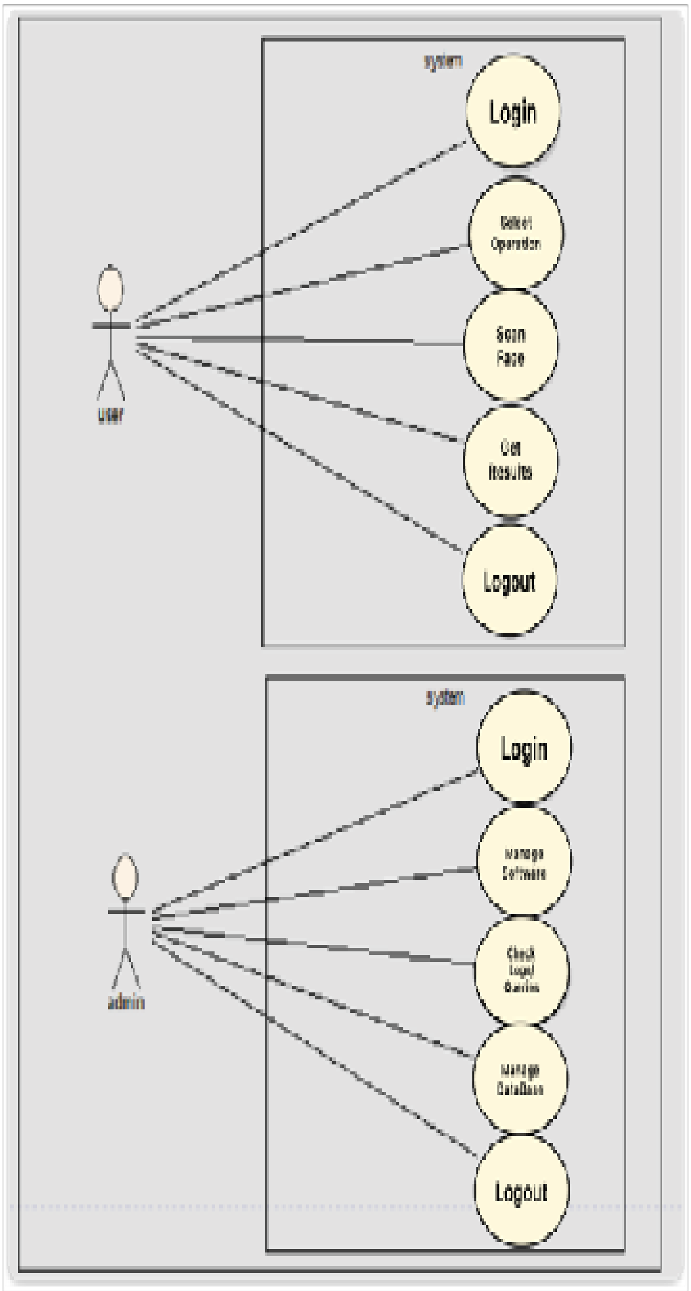


Figure 3.1 Shows the use case diagram for the proposed system

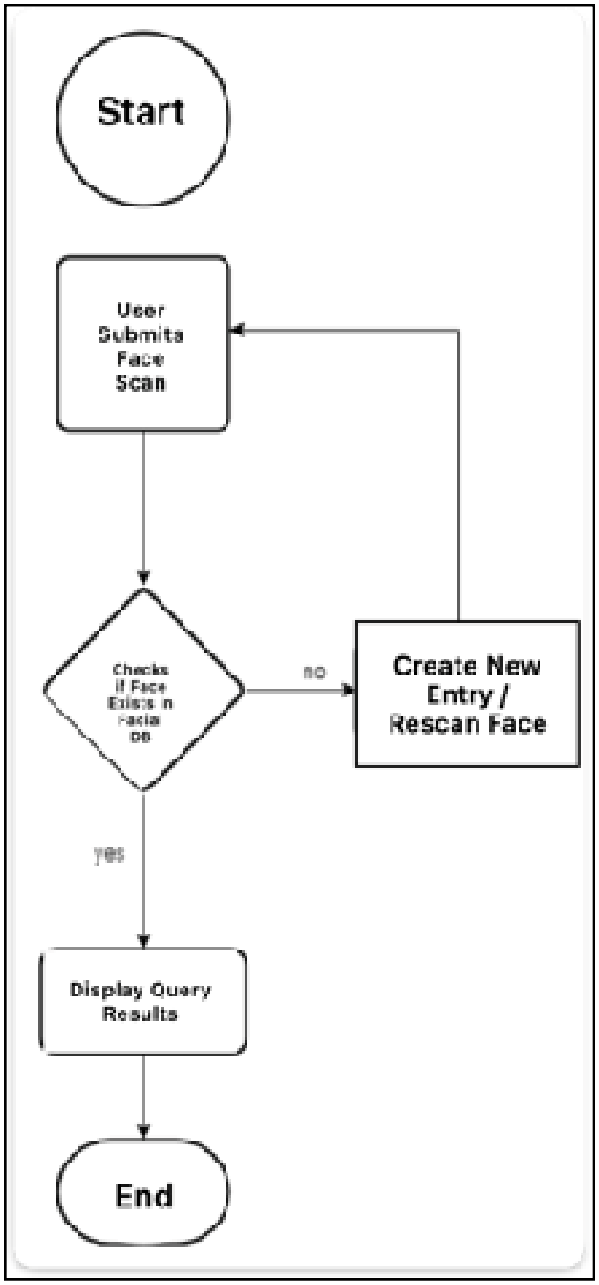

Start
User Submits Face Scan
Checks if Face Exists in Facial DB
no
Create New Entry / Rescan Face
yes
Display Query Results
End

Figure 3.2 Shows the End-User FC diagram

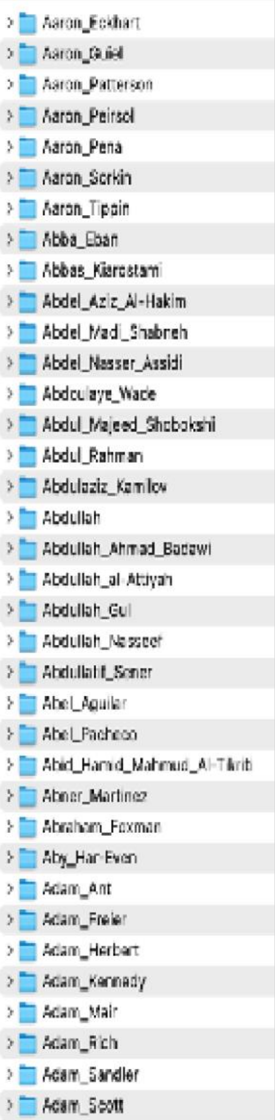
4. Chapter 4: Implementation

4.1. Introduction:

In this chapter, we will display data description tables and data schema, and then we will work on a screenshot of the entire application and simplified description of it.

4.2. System Screenshots:

Figure 4.2 Shows the internal Facial Recognition system's file vsstructure.



Aaron_Eckhart
Aaron_Guiel
Aaron_Patterson
Aaron_Peirsol
Aaron_Pena
Aaron_Sorkin
Aaron_Tippin
Abba_Eban
Abbas_Kiarostami
Abdel_Aziz_Al-Hakim
Abdel_Madi_Shabneh
Abdel_Nasser_Assidi
Abdoulaye_Wade
Abdul_Majeed_Shobokshi
Abdul_Rahman
Abdulaziz_Kamilov
Abdullah
Abdullah_Ahmad_Badawi
Abdullah_al-Attiyah
Abdullah_Gul
Abdullah_Nasseef
Abdullatif_Sener
Abel_Aguilar
Abel_Pacheco
Abid_Hamid_Mahmud_Al-Tikriti
Abner_Martinez
Abraham_Foxman
Aby_Har-Even
Adam_Ant
Adam_Freier
Adam_Herbert
Adam_Kennedy
Adam_Mair
Adam_Rich
Adam_Sandler
Adam_Scott

Figure 4.3 Shows the Labelled Faces In The Wild Dataset which we used in the training of this dataset.

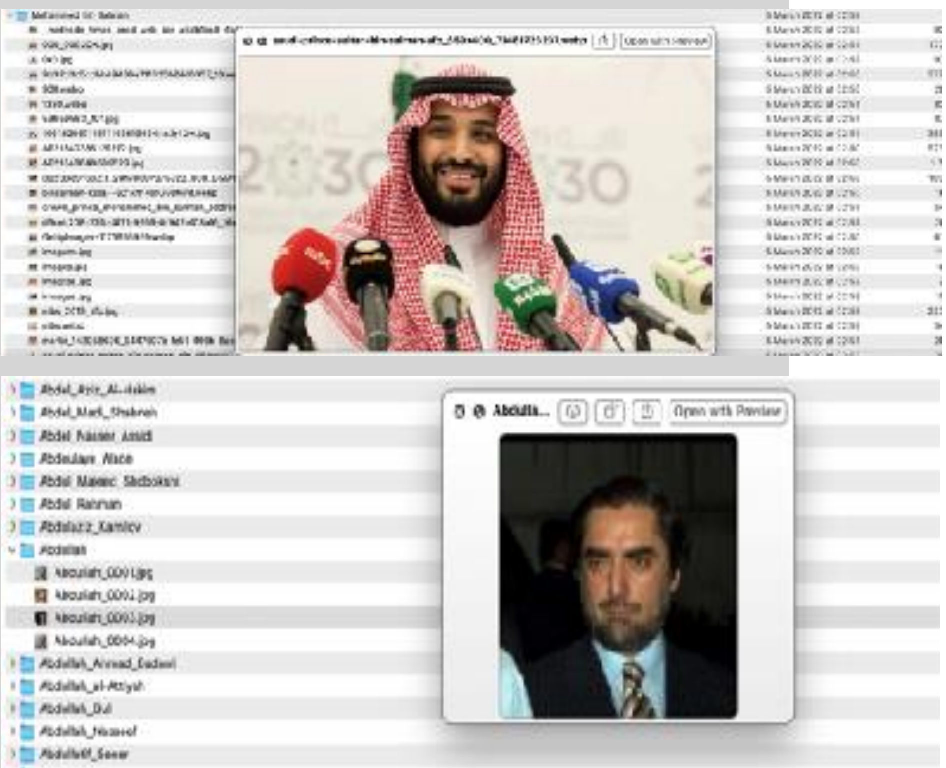
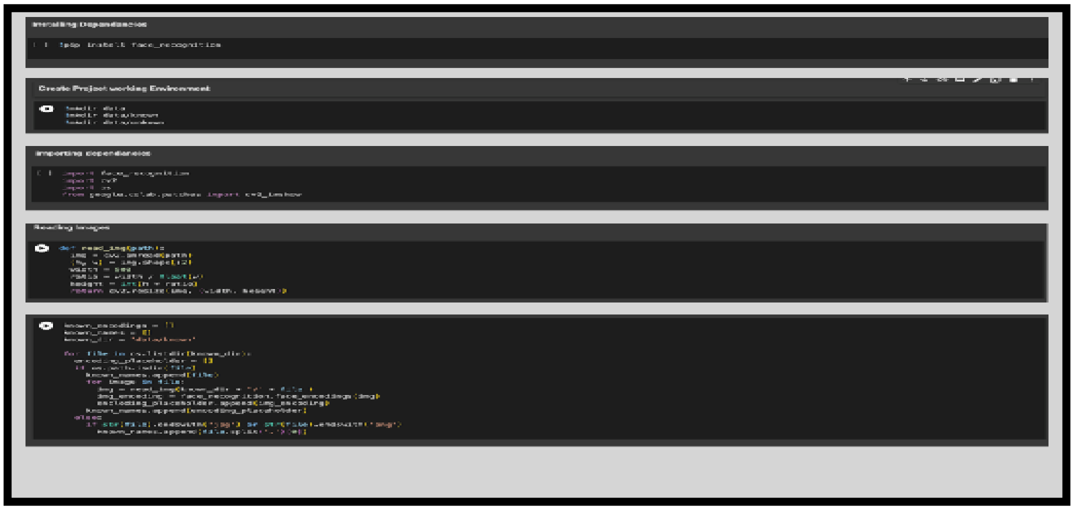


Figure 4.4 Shows a sample from the entries we used to train & evaluate the model.

4.3. Source Code:



Installing Dependancies

```
[ ] !pip install face_recognition
```

Create Project working Environment

```
!mkdir data
!mkdir data/known
!mkdir data/unknown
```

Importing dependancies

```
[ ] import face_recognition
    import cv2
    import os
    from google.colab.patches import cv2_imshow
```

Reading Images

```
def read_img(path):
    img = cv2.imread(path)
    (h, w) = img.shape[:2]
    width = 500
    ratio = width / float(w)
    height = int(h * ratio)
    return cv2.resize(img, (width, height))
```

```
known_encodings = []
known_names = []
known_dir = 'data/known'

for file in os.listdir(known_dir):
  encoding_placeholder = []
  if os.path.isdir(file):
    known_names.append(file)
    for image in file:
      img = read_img(known_dir + '/' + file )
      img_encoding = face_recognition.face_encodings(img)
      encoding_placeholder.append(img_encoding)
    known_names.append(encoding_placeholder)
  else:
    if str(file).endswith('.jpg') or str(file).endswith('.png')
      known_names.append(file.split('.')[0])
```

Figure 4.5 shows the source code of a simple & minimalistic Jupiter notebook Implementation, it served as both our initial project draft & as a viable proof of Concept demo for the project.

4.4. Project Demo:

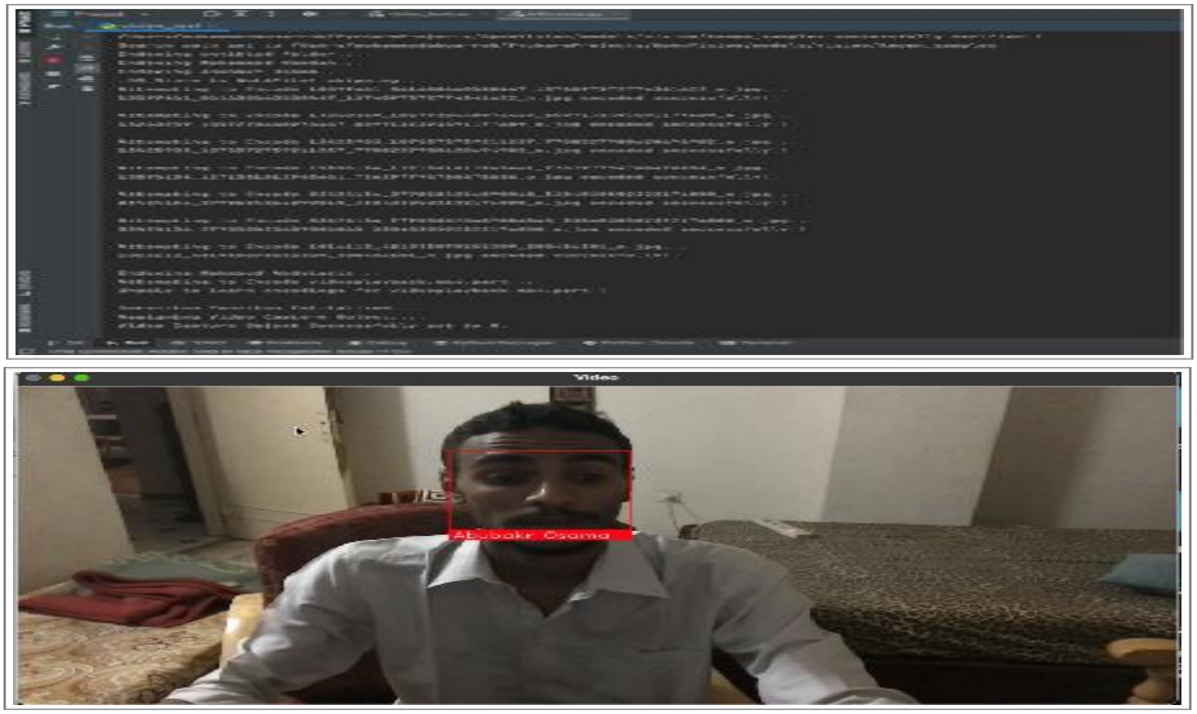


Figure 4.6 The Above image show the inference run console & system operation. Where Inference is Top & A Positive Face Match during an inference session is displayed below.

5. Chapter 5: Conclusion

5.1. Project Summary

This project focuses on addressing the issue of rising crime rates in countries like Sudan through the proposition of a digital initiative that utilises facial recognition technology for effective and scalable security. Our research aims to develop and deploy a facial recognition-based security initiative for both private and public use cases, utilising state-of-the-art machine learning algorithms and computer vision techniques.

The primary focus of this project is to enhance security protocols, prevent and investigate crime, improve border control, aid immigration management and expedite travel procedures.

The methodology involves the utilisation of tools such as Python, OpenCV, and Jupiter Notebooks, along with other techniques including facial recognition, data pre-processing and post-processing, secure storage, motion detection, and data encryption. The expected outcomes include improved security measures, a reduction in crime rates, enhanced national security, improved system efficiency and effectiveness, not to mention the provision of a transparent and critical assessment of the proposed system's validity and applicability.

The project scope encompasses the development, deployment and evaluation of facial recognition-based techniques, with a focus on constructing a comprehensive security system for identification and neutralisation of potential threats, aiding border control and immigration affairs and expediting travel procedures. The project also emphasises sharing the results and documentation with the scientific community and the public.

Overall, this research contributes to the advancement of security protocols, crime prevention, border control, and technological innovation, through leveraging facial recognition technology and machine learning algorithms, the proposed system offers a promising solution to combat crime and enhance overall security measures in Sudan & other countries like it.

5.2. Conclusion:

We have created a service that helps users and organisations to integrate Facial Recognition technology into their existing security framework, additionally we have also released an open source developer friendly API both in Notebook format on Google Colab for research purposes & as a standalone python program on Github[5].

The importance of this research lies in the quantitative & qualitative analysis of the existing system conducted through the development of this project, as well as the final product which aims to improve existing security systems and address some of the setbacks faced by those systems.

This document includes in-depth quantitative research, where data was collected through various methods (Research Papers, Journals, Interviews & Questionnaires).

The conducted research using two types of diagrams; Use Case Diagram and FlowChart.

5.3. Future enhancement:

In the future we hope to create a better and more friendly user interface for our base system, as well as a commercial product in the form of specialised software to serve the above-mentioned use-cases within this research. We also hope to enhance our existing security mechanism & improve overall performance by stay up-to date with the latest state-of-the-art Computer Vision based Facial Recognition techniques.

Finally, we also hope to deploy our proposed system in a real-life test environment and assess its performance against the old system, to measure how well it performs & include said findings in our paper.

References:

1. Criminality in Sudan - the organized crime index. The Organized Crime Index | ENACT. (n.d.-a). https://ocindex.net/country/sudan
2. Crime rate by country 2023. (n.d.-a). https://worldpopulationreview.com/country-rankings/crime-rate-by-country
3. Raposo, Vera Luacutecia. “The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal - European Journal on Criminal Policy and

Research." SpringerLink, 1 June 2022, link.springer.com/ article/10.1007/s10610-022-09512-y.

4. Aware, Inc. (2023, February 22). Facial Recognition & law enforcement – The Value Proposition. https://www.aware.com/blog-facial-recognition-used-in-lawenforcement/
5. Blog-manager. (2018, October 9). Traditional vs automated security systems in the Philippines: Elid Blog. ELID Technology Intl., Inc. https://elid.com.ph/blog/ traditional-vs-automated-security/
6. O'Shea, Keiron, and Ryan Nash. "An Introduction to Convolutional Neural Networks." arXiv.Org, 2 Dec. 2015, arxiv.org/abs/1511.08458.
7. G Koch. "Siamese Neural Networks for One-shot Image Recognition". cs.cmu.edu, , https://www.cs.cmu.edu/~rsalakhu/papers/oneshot1.pdf.
8. Gangarapu, Katam Raju. "Ethics of Facial Recognition: Key Issues and Solutions." Learn Hub, learn.g2.com/ethics-of-facial-recognition. Accessed 5 Aug. 2023.
9. Downsizinggovernment.org. (n.d.). https://www.downsizinggovernment.org/ homeland-security
10. Stop retail violence, theft with face matching, video analytics. FaceFirst. (n.d.). https://www.facefirst.com/
11. Almabdy, S., & Elrefaei, L. (2019, October 17). Deep convolutional neural network-based approaches for face recognition. MDPI. https://www.mdpi.com/ 2076-3417/9/20/4397
12. [MementoDeAMor. "Mementodeamor/OpenSecurity: An Open-Source Framework for Computer Vision Based Tasks." GitHub, github.com/ MementoDeAMor/OpenSecurity. Accessed 5 Aug. 2023.
13. "Criminality in Sudan." The Organized Crime Index, ocindex.net/country/ sudan. Accessed 5 Aug. 2023.