



Faculty of Business, Law, and Digital Technologies.

MSC Applied AI and Data Science (MAIDS).

Isaac Otu Arhinful

**Impact of Artificial Intelligence facial recognition on
Maritime Piracy.**

*This project is submitted towards the fulfilment of the
MSc (Master of Sciences) degree in Applied AI and Data
Science at Solent University.*

2nd -September-2022

DECLARATION

I hereby declare that this submission is my own work for the MSc in Applied AI and Data Science degree at Solent University, and that, to the best of my knowledge, it does not contain any materials that have been previously published by another person or materials that have been accepted for the award of any other degree by the University, with the exception of those instances where appropriate acknowledgement has been made in the text.

Date: 2nd September -2022

Signature: ...Isaac Arhinful.

Table of Contents

DECLARATION	2
CHAPTER ONE	5
INTRODUCTION.....	5
1.1 Background to the Study.....	5
1.2 Problem Statement.....	9
1.3 Objective of the Study.....	12
CHAPTER TWO	12
LITERATURE REVIEW	12
2.1 Introduction	12
2.2 Conceptual Review	12
2.3 Theoretical Review.....	17
2.4 Empirical Review.....	19
CHAPTER THREE	30
RESEARCH METHODOLOGY	30
3.1 Introduction	30
List of libraries, files, and requirements.	30
Running process.....	31
Data collection and processing process.	32
OpenCV-Python.....	33
Data_generate.py	35
Train_classifier.py	36
Detect_face.py	40
GUI.....	41
SQL Database.....	41
CHAPTER FOUR	42
4.1 Research Analysis and findings.....	42
CHAPTER FIVE	44
5.1 Limitation.	44
CHAPTER SIX	45
6.1 Conclusion.	45
Reference (Harvard Style).....	46
Appendix.....	49

Table of Figures.

Figure 1. Gui.SOURCE: (Arhinful, 2022)	32
Figure 2. Sample of Haar cascade classifier features. SOURCE. (Behera, 2021)	34
Figure 3. Haar cascade classifier mathematical calculations: SOURCE. (Behera, 2021)	35
Figure 4. generating dataset. SOURCE:(Arhinful,2002)	36
Figure 5. LBPH procedure. SOURCE (Prado. 2017).....	38
Figure 6.Training the classifier . SOURCE: (Arhinful,2022).....	39
Figure 7.Confidence level formular . SOURCE.(Prado. 2017).....	40
Figure 8.Detect face. SOURCE. (Arhinful,2022)	41
Figure 9.Tkinter GUI.SOURCE.(Arhinful,2022).....	41
Figure 10.SQL Database Table . SOURCE: (Arhinful.2022)	42
Figure 11.SQL Database Code. SOURCE:(ARHINFUL,2022)	42
Figure 12.Confidence level parameter. SOURCE (Arhinful.2022)	43
Figure 13. Real world test results. SOURCE(Arhinful, 2022).....	43
Figure 14. Test with two participants. SOURCE(Arhinful , 2022).....	44
Figure 15.Test with two participants2 (SOURCE(Arhinful , 2022)	44
Figure 16.Participant Questionnaire form 1.	50
Figure 17.Participant Questionnaire form 2	51
Figure 18.Participant Questionnaire form 3	52
Figure 19.Participant Questionnaire form 3	53

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

The United Nations (UN) Agenda 2030 for Sustainable Development has become one of the major targets confronting the world leaders today. The Goal 14 – “Life below Water” seeks to conserve, sustainably use the oceans, seas, and marine resources for sustainable development. In view of this goal, governments and heads of states have mounted various strategies to protect their territorial waters. One of the key issues obstructing marine resources utilization is piracy. To response to this obstruction, the current study is proposed to design model to facially recognize the pirates (Liu et al., 2021; Boo and Chua, 2022).

In respect of the direction taken by the researcher, it should be emphasized herein that the concept of piracy has changed throughout history depending on the act itself, the perpetrator's modus operandi, and the era (Hashting and Philips 2022). The definition of piracy has evolved over time and depended on circumstances. The evolution of the definition reflects the politics of the time, which was characterized by a distinction between pirates and privateers (Langfitt, 2011). In ancient times, piracy referred to those who attacked others at sea.. A pirate society was a community that plundered people and

goods en masse without an official declaration of war (Goodwin, 2006).

There are many applications that recognize faces. Manufacturers of digital cameras, camcorders and surveillance cameras claim that their products recognize faces and smiles and behave accordingly. Facial recognition is then defined as a subset of visual pattern recognition. Humans are constantly recognizing visual patterns and receiving visual information from their eyes. The brain recognizes this information as meaningful concepts (Lander et al., 2018). Face recognition in the broadest sense encompasses the methods used to design face recognition systems. Face recognition algorithms determine the coordinates of all faces in an image (Li et al., 2010). How can this be achieved? How do modern systems that require more accurate facial recognition work? The potential of facial recognition is huge, including for security and various applications. There is no official definition of face recognition. We can say that face recognition is a system that recognizes faces from camera images, compares them with data from a face database using a specific algorithm, and draws conclusions based on this information.

In general, facial recognition can be divided into two categories: Face recognition and face matching. The goal of face recognition is to find a specific face in an image or video, while the goal of verification methods is to confirm that a person is indeed who he or she claims to be (Ahonen, 2008; Lehmussola, 2008). Face recognition systems have developed due to the simultaneous

development of computer image processing. This includes the use of automatic recognition and learning methods from video data and improvements in camera technology. For example, facial recognition technology works by calculating facial features captured by digital cameras (Rossion and Michael, 2018). This image is then compared with previously analysed faces and stored in a database.

There are several studies on unmanned aerial vehicle in maritime piracy. For instance, Tahir et al. (2019) analysed the main features of drone havens and assessed how they are perceived by the public. To achieve their goals, they argue the features, challenges, and importance of drones. The report also presents the results of a pilot study with researchers, which shows that drone platforms will be an important issue in the future and will eventually become mainstream.

Also, Li and Fung (2019) investigated whether the concept of autonomous ships brings a breakthrough to the maritime industry by improving ship safety and local development opportunities. This study uses the example of Norway, which developed the first autonomous vessel and initiated autonomous operations in the region by establishing the Advanced Autonomous Watercraft (AAWA) program.

Again, Keshtgar et al. (2019) investigated whether orthognathic surgery affects facial recognition in the automated border control system of airports and whether it is useful to update the photographic identification of patients after surgery. A total of 50 patients responded to

the survey, 35 of whom travelled by air after the intervention. Of these, six had immigration problems (two human, four automatic), but were able to travel safely after additional security checks; four had undergone double tongue surgery, one a mandibular frontal surgery, and one a mandibular frontal surgery. Orthognathic surgery affects identification at border control and most of our patients had problems at the automatic screening because the biometric data on the chip of the electronic passport did not match the scanned biometric data. These results may improve the information provided to patients before surgery, but further studies are needed to increase the sample size and reliability.

Moving on, Liu et al. (2021) analysed the confidentiality of facial recognition and the factors affecting it. The results show that users are more concerned about privacy if they think their personal information can be compromised by facial recognition. Henderson et al. (2018) examined how cross-cultural responsiveness affects the ability of service providers to recognize the faces of black and white consumers; two experiments were conducted to understand how cross-cultural responsiveness affects the face recognition of black and white consumers. It was found that the more cross-cultural responsiveness the respondents showed toward blacks, the better they were able to distinguish between black and new regular customers in the same experience.

This research then focusses on the artificial intelligence algorithm used in facial recognition by using Neural

Network in deep learning to be incorporated in drones in efforts to tackle Maritime Piracy.

1.2 Problem Statement

Maritime have already been confronted with piracy. Over time, the law of the sea has changed. Numerous regions of the world, the practice has deep cultural roots, so that what is often considered illegal is recognised and upheld in some places (Caplan et al., 2010; Randrianantenaina 2013; Hashtings and Philips, 2022). The definition of piracy and non-piracy has changed over time (Ali, 2014; Atole et al., 2017). The prevalence of piracy fluctuates and decreases over time due to several factors. Therefore, piracy is a complex issue, and its causes must be considered. International transportation security has always been a crucial concern. The core of global trade is the movement of products. Investors and shippers both want their cargo to arrive intact. Markets make trade easier, and trade makes transportation easier. The risks are very different at sea. There are two distinct accident kinds to think about: accidents involving marine safety and security (Warren, 2011; Ruiz et al., 2021).

Security incidents are unintentional events such as accidents caused by natural phenomena, crew members or third parties. These include fires, equipment damage and collisions. Safety incidents also include navigation accidents caused by weather and geographical conditions. Modern piracy is a criminal activity that threatens the lives and livelihoods of many seafarers. Piracy and armed robbery have increased significantly in recent years and

thousands of seafarers have been killed, injured, robbed, or threatened (Jones, 2014; Julius et al., 2022). However, the adoption of international anti-piracy laws has changed these penalties, with pirates being tried by national courts rather than politicians. This means that convicted pirates can be rehabilitated. Unlike the pirates of the Golden Age, who lived on the sea, today's pirates are mostly on land and attack with speedboats. Pirate tactics have changed, and weapons are now more common than swords. However, their objectives have remained the same. They threaten, rob, attack, and sometimes abandon the crews of other ships.

Although there have been studies on maritime piracy, for instance, Khan et al. (2021) developed a system for real-time accurate detection of sprayed areas, which is very important for unmanned aerial spraying: they developed a two-stage target detection system using Deep Learning from drone images. Consider creating a cilantro nursery to determine areas to be sprayed with the classifier. The developed deep learning system had an average F1 value of 0.955 and an average computation time of 3.68 milliseconds to locate the classifier. The developed deep learning system can be implemented in a real-time drone-based delivery system to make a trade-off between delivery accuracy and computational complexity and overcome the computational limitations associated with drones.

Also, Zhang et al. (2018) proposed a pheromone-based method for monitoring drone interference against hacking attacks. In this approach, the environment is modelled

using a pheromone map, and drone movements are detected based on pheromone intensity. Considering the interaction between pirates and merchant ships, an on-board detection mechanism is proposed to increase the probability of detecting pirates. To eliminate the disadvantages of the indirect distribution mechanism, a prediction and redirection mechanism using an ascending collection mechanism was proposed. Simulation experiments were conducted to test the effectiveness of the proposed method. The results show that the proposed method reduces the success rate of hacking attacks by 8% compared to the alternate method, and that the indirect collection mechanism is more effective than the indirect intent propagation mechanism, especially in the presence of many drones.

Moreover, Ruiz et al. (2021) reported the results of a study on the use of unmanned aerial vehicles (UAVs) as a visual data collection tool to investigate anomalous phenomena on building facades in the fields of architecture, engineering, construction, and facilities management. The methodology used is an experimental field study with three medium and tall buildings as case studies. The results show that digital aerial photos are more effective in detecting damage than 3D models and orthophotos created with digital photogrammetry software, demonstrating the technical feasibility and effectiveness of unmanned inspections.

However, there have not been enough studies on facial recognition in maritime piracy, for this purpose this study aims in incorporating Artificial intelligence face

recognition software to be used in an Unmanned Aerial Vehicles to optimise Maritime Piracy safety.

1.3 Objective of the Study

The main Objective of the study is to assess the impact of facial recognition in Maritime Piracy. The study will specifically focus on the following objective.

- 1.2 Detect faces; facial recognition software which can be used by third party business, companies, or Governments in an Unmanned Area vehicles in improving Maritime Piracy.
- 1.2 Recognize faces by comparing them to previously taken images.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents review on the topic, the impact of facial recognition in maritime piracy. Specifically, the chapter has been categorized into four sections, the conceptual review, the theoretical review, the empirical review, and the conceptual framework.

2.2 Conceptual Review

- ***Facial Recognition***
Recognizing faces seems like a simple task for the human brain. However, it is difficult for a computer system to do

so (Ahonen, 2008). Today, however, there are many applications that recognize faces. Manufacturers of digital cameras, camcorders and surveillance cameras claim that their products recognize faces and smiles and behave accordingly. How can this be achieved? How do modern systems that require more accurate facial recognition work? The potential of facial recognition is huge, including for security and various applications. There is no official definition of face recognition. We can say that face recognition is a system that recognizes faces from camera images, compares them with data from a face database using a specific algorithm, and draws conclusions based on this information. In general, facial recognition can be divided into two categories: Face recognition and face matching. The goal of face recognition is to find a specific face in an image or video, while the goal of verification methods is to confirm that a person is indeed who he or she claims to be (Ahonen, 2008; Lehmussola, 2008). The scientific definition of RFS is not straightforward, but RFS can be divided into two different categories (recognition and verification), which represent the main research areas. Recognition methods, for example, involve recognizing a selected person in a crowd. A digital image of the person must be stored in a database to compare different data. In authentication, a person's face is like a card or password. Kamarinen (2008) notes that many systems use authentication methods in which a person with the correct face is granted access to a restricted area controlled by the SRF.

Facial recognition is a subset of visual pattern recognition. Humans are constantly recognizing visual patterns and

receiving visual information from their eyes. The brain recognizes this information as meaningful concepts (Lander et al., 2018). In a computer, an image or video is a chain of several pixels. The machine must decide which concept the data set represents. This is the problem of approximate classification in visual pattern recognition. In face recognition, for each data set that contains a face, the machine must distinguish to whom that face belongs. This is a problem that has several parts (Hu et al., 2010). Face recognition in the broadest sense encompasses the methods used to design face recognition systems. This includes face recognition, face localization, identity recognition and image pre-processing. Face recognition algorithms determine the coordinates of all faces in an image (Li et al., 2010). In this process, the entire image is scanned to determine whether a potential area is a face. The face coordinate can be derived from a square, rectangle, etc. Face position is the position of the face coordinate in the face recognition coordinate system (Lander et al., 2018; Li et al., 2020). Deep learning systems mainly use advanced methods to detect good positions. The computation time of face localization algorithms is much shorter than that of face recognition algorithms.

Face recognition systems have developed due to the simultaneous development of computer image processing. This includes the use of automatic recognition and learning methods from video data and improvements in camera technology. These databases store many faces, their names and other personal information. Face recognition systems work by computer analysis of the shape of the face, or geometric coordinates of position

and distance. These coordinates include the centres of the pupils of both eyes, the back of the nose and the eyebrows (Amato et al.). Since each person has unique facial features, the features of the captured image can be compared with a database of previously identified images to match the image to the identified face. Facial recognition and related methods have been developed to analyse and read facial expressions and determine a person's mood, emotions, and current state. Biometric technologies aim to measure and enhance human characteristics. Current technologies are like iris recognition, voice recognition and fingerprint recognition (Cook et al., 2019).

- ***Maritime Piracy***

The word "pirate" comes from the Latin word "peirate," from which the word "pirate" is derived, and the Greek word "peirātés" is a noun derived from the verb "peiran," meaning "to try" or "to attack" (Julius et al. 2022). Since its inception, the concept of piracy has included the terms "attempt" and "actual infringement." The concept of piracy has changed throughout history depending on the act itself, the perpetrator's modus operandi, and the era (Hashting and Philips 2022).

For a long time, piracy was associated only with maritime transportation, but it has since expanded into other fields, such as aviation, intellectual property, and broadcasting. More recently, piracy has become a popular topic in aviation, computers, radio, and television. As a result, the

term "piracy" is often used to refer to illegal or unauthorized activities. Although today the term "piracy" is sometimes used in different meanings, its original meaning was related to maritime transportation, where it denoted warlike, plunderous, and violent actions at sea against ships, their cargo, and the people (crew and passengers) on board. The codification of customary international law on piracy in the 1958 Law of the Sea Convention and the 1982 United Nations Convention on the Law of the Sea led to the development of an internationally recognized definition of piracy (Ayto, 2005; Amirel, 2009).

The definition of piracy has evolved over time and depended on circumstances. The evolution of the definition reflects the politics of the time, which was characterized by a distinction between pirates and privateers (Langfitt, 2011). In ancient times, piracy referred to those who attacked others at sea. The Greeks and Romans distinguished between pirates and pirate societies. A pirate society was a community that plundered people and goods en masse without an official declaration of war (Goodwin, 2006). In the Middle Ages, piracy was seen as simple theft at sea. To avoid wars, looting between kingdoms was masked by unconstitutional charters and treaties organized by civil society. By the 17th century, pirates were no longer accepted by pirate society. Pirates were seen as individuals who banded together to commit evil, and these groups did not form a state (Rubin, 2006).

2.3 Theoretical Review

- ***Global Anomie Theory***

Global Anomie Theory (TAG), developed by Nikos Passas (1999, 2000), describes the impact of globalization and neoliberalism on the state and the conditions within the state that create anomalies that lead to deviance. It also analyses global cultural structures and forces that affect societies and individuals. The theory is holistic in that it incorporates anomalies and other criminological approaches, as well as relevant insights from the social sciences; TGA aims to provide an integrated macro-theory of the social context of deviance (Twyman-Ghoshal, 2021).

According to the comprehensive approach to dysfunction, neoliberal globalization is one source of dysfunction and disharmony that creates an environment conducive to crime and social harm. According to this theory, the spread and intensification of neo liberalization increases the asymmetry of crime and leads to a disconnect between cultural goals and the legitimate means used to achieve them. The interconnectedness resulting from globalization leads to greater social mobility, better international communication and increased international trade. This process is spreading across the globe and emphasizing the importance of a free and unrestricted market to promote material goals, growth, and consumption. In this increasingly interconnected environment, there are more and more reference groups that influence people's preferences and are increasingly oriented toward economic goals.

At the same time, the processes of globalization accentuate inequality, stratification, exclusion, and marginalization, which hinder the achievement of desired material goals and lead to absolute and relative deprivation (Twyman-Ghoshal, 2021). Drawing on Merton's work, Paz argues that this sense of alienation leads to organizational disillusionment when aspirations are not met. All people adapt differently to stress, and some behave differently. In such a structural situation, deviant behaviour is rationalized and, if successful and not punished, perpetuates itself in society as the norm for those who have not experienced the original stress. The theory also highlights the impact of neoliberal globalization on governance. Regulatory norms and control mechanisms are being dismantled to reduce state intervention and control. Among other things, social measures to support privatized markets are being dismantled. The ability of governments to act effectively is further reduced when adjustment problems become persistent and create a non-economic environment (Twyman-Ghoshal, 2021).

The strength of the theory is that it describes social processes that explain the broader effects of globalization that contribute to the emergence and perpetuation of deviance. Before explaining the various elements and concepts of global anomaly theory, it is important to review the literature on the genesis of piracy. The existing literature on piracy provides a list of factors that are considered concomitant with piracy. Opportunity is the most cited causal factor of piracy in the literature. In the

context of piracy, the concept of opportunity includes favourable geographic conditions as well as legal and jurisdictional loopholes (Murphy, 2007). Favourable terrain refers to physical features (e.g., narrow waterways, numerous islands and bays that are ideal hiding places) and the presence of potential targets in high-traffic areas (Caplan, Moreto and Kennedy, 2010).

2.4 Empirical Review

- ***Unmanned Aerial Vehicle in Maritime Piracy***

Tahir et al. (2019) analysed the main features of drone havens and assessed how they are perceived by the public. To achieve their goals, they argue the features, challenges, and importance of drones. The report also presents the results of a pilot study with researchers, which shows that drone platforms will be an important issue in the future and will eventually become mainstream.

Li and Fung (2019) investigate whether the concept of autonomous ships brings a breakthrough to the maritime industry by improving ship safety and local development opportunities. This study uses the example of Norway, which developed the first autonomous vessel and initiated autonomous operations in the region by establishing the Advanced Autonomous Watercraft (AAWA) program. Another goal of the paper is to compare ship launching with air and land vehicle automation. The idea for the paper came from meetings and discussions with experts in the shipping industry, including captains, senior marine engineers, and ship designers. Developments in autonomy

and technology have been studied and analysed in various international journals. Due to the practical nature of the dissertation, a qualitative research method was used to collect and analyse data. The conclusions of the study are as follows. It highlights the great potential of unmanned ships and their competitive advantage over existing cargo ships.

Grote et al. (2022) worked with the civil aviation community to raise concerns and questions about the concept of shared airspace as a first step toward future shared airspace planning. The methodology was to conduct an interactive webinar with (n=80) participants from the UK aviation community. The collected data (oral and written) was qualitatively analysed using thematic analysis, and conclusions were drawn by grouping the identified questions into several themes and three main topics: 1) operational environment, 2) technical and regulatory environment, and 3) legislation and the broader community. Nearly a quarter (27%) of participants' comments relate to the idea that airspace sharing is only possible if aircraft are equipped with electronic identification (EID) systems based on collision detection and avoidance (CAD). These results indicate that an inclusive airspace management policy is needed to create an appropriate technical and regulatory environment for the creation of shared airspace, with the main goal of involving the civil aviation community (and all other stakeholders) in the development process.

Yu et al. (2022) focus on developing a wing segmentation system that combines vision-based sensors and deep

learning-based segmentation techniques. The semantic segmentation model of the encoding and decoding system is closely coupled with convolutional modules that support matrix blocks, each with two different degrees of expansion, to efficiently classify wings of different types and sizes. To train the proposed network, images of different types of wings were collected and expanded, and their performance was compared with conventional segmentation models. Finally, the trained network was applied to drone images and was able to successfully segment wings even in images that differed in shape and colour.

Atole et al. (2017) provide detailed observations on commercial drones or unmanned aerial vehicles (UAVs), including their uses and features, based on various secondary data, mainly reference materials, network logs and key informant interviews. Quantitative methods were used to compile the data. Today, drones are used in agriculture, real estate, film and television, oil and gas exploration, construction, fishing, wildlife control, water management and security. Of the 30 applications in the sample, 23.33% were for public and/or civil security. This was followed by agriculture, wildlife photography and monitoring with 16.67%, 3 (10%) were related to real estate, 2 (6.67%) to fisheries and 1 (3.33%) to oil and gas, construction, and water.

Khan et al. (2021) developed a system for real-time accurate detection of sprayed areas, which is very important for unmanned aerial spraying: they developed a two-stage target detection system using Deep Learning

from drone images. Consider creating a cilantro nursery to determine areas to be sprayed with the classifier. The developed deep learning system had an average F1 value of 0.955 and an average computation time of 3.68 milliseconds to locate the classifier. The developed deep learning system can be implemented in a real-time drone-based delivery system to make a trade-off between delivery accuracy and computational complexity and overcome the computational limitations associated with drones.

Zhang et al. (2018) propose a pheromone-based method for monitoring drone interference against hacking attacks. In this approach, the environment is modelled using a pheromone map, and drone movements are detected based on pheromone intensity. Considering the interaction between pirates and merchant ships, an on-board detection mechanism is proposed to increase the probability of detecting pirates. To eliminate the disadvantages of the indirect distribution mechanism, a prediction and redirection mechanism using an ascending collection mechanism was proposed. Simulation experiments were conducted to test the effectiveness of the proposed method. The results show that the proposed method reduces the success rate of hacking attacks by 8% compared to the alternate method, and that the indirect collection mechanism is more effective than the indirect intent propagation mechanism, especially in the presence of many drones.

Al Abqal et al. (2020) evaluated the advantages and disadvantages of drones to improve port and border

security in Kuwait and the United States. The main research question was how drones can be effectively used to improve port security. Primary and secondary data were collected. Primary data was collected using qualitative and quantitative methods. Primary data was collected through an online questionnaire sent to 66 port stakeholders and five semi-structured telephone interviews with selected respondents. However, there are risks involved in implementing such a system, especially about terrorist organizations and cyber security threats.

Ruiz et al. (2021) report the results of a study on the use of unmanned aerial vehicles (UAVs) as a visual data collection tool to investigate anomalous phenomena on building facades in the fields of architecture, engineering, construction, and facilities management. The methodology used is an experimental field study with three medium and tall buildings as case studies. The results show that digital aerial photos are more effective in detecting damage than 3D models and orthophotos created with digital photogrammetry software, demonstrating the technical feasibility and effectiveness of unmanned inspections.

- ***Facial Recognition and Maritime Piracy***

Keshtgar et al. (2019) investigated whether orthognathic surgery affects facial recognition in the automated border control system of airports and whether it is useful to update the photographic identification of patients after surgery.⁸² Patients underwent orthognathic surgery between August 2013 and June 2017. Data were collected

from 82 patients. They were asked by telephone whether they had experienced problems with automatic or human intervention at border controls or with other identification documents such as driver's licenses. All questions related to the experience prior to the intervention. A total of 50 patients responded to the survey, 35 of whom travelled by air after the intervention. Of these, six had immigration problems (two human, four automatic), but were able to travel safely after additional security checks; four had undergone double tongue surgery, one a mandibular frontal surgery, and one a mandibular frontal surgery. Orthognathic surgery affects identification at border control and most of our patients had problems at the automatic screening because the biometric data on the chip of the electronic passport did not match the scanned biometric data. These results may improve the information provided to patients before surgery, but further studies are needed to increase the sample size and reliability.

Liu et al. (2021) analysed the confidentiality of facial recognition and the factors affecting it. In this study, 518 online questionnaires were collected, SPSS 25.0 was used to analyze the questionnaire data, and the Cronbach's alpha coefficient (α coefficient) was used to determine the reliability of the data. The results show that users are more concerned about privacy if they think their personal information can be compromised by facial recognition. Henderson et al. (2018) examined how cross-cultural responsiveness affects the ability of service providers to recognize the faces of black and white consumers; two experiments were conducted to understand how cross-

cultural responsiveness affects the face recognition of black and white consumers. It was found that the more cross-cultural responsiveness the respondents showed toward blacks, the better they were able to distinguish between black and new regular customers in the same experience.

Boo and Chua (2022) attempted to explain how Singaporean hotel guests' attitudes toward facial recognition technology are shaped by combining the technology acceptance model (TAM), computational privacy theory, and individual innovation. Guests of four- and five-star hotels in Singapore were selected using a systematic random sampling method. The results showed that hotel guests made cognitive calculations when weighing the benefits and risks of using facial recognition.

Julius et al. (2022) studied piracy and armed robbery in the Gulf of Guinea and its impact on transportation costs and economic growth in Nigeria. Data were taken from a statistical report of the Nigerian Maritime Safety Agency (NIMASA). For statistical, forecasting and modelling purposes, EViews 12 software and one-way regression analysis were used to model the relationship between the dependent and independent variables of the research hypotheses, tested at a 5% significance level. The results of the analysis show that piracy is inversely related to economic growth in Nigeria. A significant relationship was also found between piracy and armed robbery and the cost of insurance premiums against piracy on ships.

Hustings and Phillips (2015) examine how these local institutions shape and constrain the complex linkages and behaviours associated with piracy. Following the literature on state failure and piracy, they argue that norms and institutions also impose constraints on criminal organizations such as pirates. In the Somali Peninsula, piracy is structurally and ideologically influenced by the Somali right-wing economy, informal clan rules, rent-based economic activities, and collective security arrangements. In West Africa, sophisticated piracy depends on the formal economy, particularly the international oil industry. Findings show that piracy networks often reflect and interact with the formal institutions that regulate and protect Nigeria's oil production, as well as oil production, refining, distribution, and transportation facilities.

Ringsberg and Cole (2020) examine the perceived barriers to compliance with the ICS. To test the conceptual framework, a mixed method of empirical data collection was used, which included interviews with national experts and a survey in 47% of Swedish cargo ports. Based on the proposed framework, Swedish ports believe that the barriers to compliance are related to cooperation within the Swedish network of maritime security stakeholders, available resources, and the development of a security culture. The barriers identified by smaller ports relate to the alignment of the IHSS at different levels and the lack of specific measures to manage maritime security. Given the growing interest in international shipping, this paper is one of the few to address the barriers to meeting the demands of multi-sectoral road transport.

Choudhury (2019) calls for a discussion of the threat to national security posed using fake e-passports. National security must be strengthened to combat cross-border crime and terrorism. The verification process is inadequate as there are no identification methods such as physical, biometric, and electronic verification. This paper focuses on facial recognition to improve biometric authentication of e-passports and describes the identification of permanent markings such as makeup or fake faces and bags. An algorithm is proposed for detecting permanent markings on the face caused by cosmetics, such as moles, freckles, birthmarks, and pigmentation. A shape model is applied to the active appearance model using principal component analysis to detect facial marks; permanent facial marks can be detected using the edge detector and directional gradient histogram. The results provide face recognition algorithms and recommendations for secure biometric identification of passports for national security.

Dang et al. (2022) examined key issues and implications for consumer attitudes toward this innovative payment method. The study used a survey to collect data from 795 Chinese retail customers. The results showed that perceived usefulness, perceived ease of use, and perceived innovativeness have a positive effect on consumers' attitudes toward MFIs, while perceived risk has a negative effect on these attitudes.

Moungsouy et al. (2022) proposed a solution for face recognition using a mask. The lower part of the face is

hidden and cannot be used for face recognition training. Thus, they developed a solution for face recognition where parts of the face can change depending on whether the mask is on or off. The proposed solution is based on FaceNet and aims to improve performance in masked and unmasked situations by modifying existing face recognition models. A simulated masked face image is then computed from the original face image for use in face recognition training. In addition, a heat map is generated that allows the user to almost visually view the parts of the face image that are relevant to masked face recognition. The proposed method has been validated using several test scenarios. The results show that the accuracy of face recognition with mask is 99.2%. From the feature heat map, unmasked parts of the face such as the eyes and nose are more important for face recognition than the lower part of the face, which can be masked.

Yao and Qiu (2021) built a CNN model to learn local features of eyes, eyebrows, and mouth. These features were then sent to a support vector machine (SVM), which extracted the probabilities of each feature. Finally, the model's outputs were identified and combined to produce the final recognition results. Experimental results showed that the improved conventional neural network structure improved facial expression recognition performance by 0.06% for the ER2013 dataset and by 2.25% for the CK+ dataset.

Zaqout and Al-Hanjori (2018) focus on efficient facial expression recognition and show that the recognition speed and accuracy of the proposed method are

comparable to other methods such as principal component analysis and linear discriminant analysis using the same dataset. From the Olivetti Research Laboratory (ORL) dataset, 150 faces were selected with a recognition rate of 95.6% and accuracy of 85%, and from the Yale University (YU) dataset, 165 faces were selected with a recognition rate of 95.5% and accuracy of 84.4%. Thus, the ENT dataset had a recognition rate of 95.6% and accuracy of 85%, while the Yale dataset had a recognition rate of 95.5% and accuracy of 84.4%.

Jones (2014) determined the nature and extent of the global piracy threat. The cost of piracy is estimated at 15-25 billion euros globally. The global cost of piracy is estimated at \$15 billion, reaching a record high in 2011, and continues to threaten global trade by driving up commodity prices. Based on a literature review including official and unofficial publications, this study aims to provide a comprehensive overview of the extent of piracy worldwide, including global piracy activities and shipowner responses, as well as global trends and temporary economic impacts. Although the overall conclusions are not definitive due to incomplete and unreliable data, piracy affects goods transported by sea worldwide.

Chang and Khan (2019) seek to explain why maritime development and maritime security are important to Pakistan and what China's concerns are. Using qualitative criteria, this study analyses the impact of China's CPEC ambitions on strategic regional Deepwater management and maritime regulation, with a focus on the port of

Gwadar. The paper argues that the Gwadar port makes a significant contribution to maritime security throughout the region. It also analyses legal, national, and international security issues related to the CPEC project.

Warren (2011) analyses the dilemmas shipowners face in dealing with the threat of piracy off the Somali coast from a virtue ethics perspective. Drawing on virtue theory, she analyses the ethical dilemmas facing shipowners in relation to the threat of piracy off the coast of Somalia. In particular, he talked about the ethical problems faced by shipowners sailing in dangerous areas and the dilemma of whether shipowners should pay ransom to pirates when their ships are attacked by pirates. It was shown that although individual shipowners can take various initiatives and security measures, it was concluded that piracy can only be reduced through international cooperation between shipowners and states.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the research approaches and methods. In this study, it should be noted that the following factors were considered: Data collection process, Data analysing, training , Data visualisation, connecting to SQL database and finally creating GUI.

List of libraries, files, and requirements.

```
future~=0.18.2
opencv-python~=4.6.0.66
numpy~=1.23.1
scikit-learn~=1.1.2
pillow~=9.0.1
setuptools~=60.8.1
matplotlib~=3.5.1
tqdm~=4.62.3
```

Please note the requirements and libraries needed for this project to run maybe be installed automatically depending on the user settings.

Running process.

To run the software, the user must first run the gui.py,

- Click on capture 'Generate Pirate Dataset' if the user wants to collect new pirate images (data) . The training of the dataset (images) function code has been incorporated into the "Generate Pirate Dataset" function. This means just one click captures images, trains the classifier, and saves it.
- The user can then click the 'Detect Pirate Face' to identify already trained and saved data (Images).



Figure 1. Gui.SOURCE: (Arhinful, 2022)

Data collection and processing process.

According to the Data Protection Act of 1998, images of people constitute personal data and must be handled per data protection rules. This means that personal data must be used properly and legally, with the consent of the person. Images of the 4 participants used in this research was approved and signed by the participant (See Appendix A).

Participants	Gender	Ethnicity
Xavi	Male	Black – Caribbean
Jen	Female	Black – Caribbean
Abbie	Female	Black – African
Isaac	Male	Black – African
Lorraine	Female	White – British

OpenCV-Python

The dataset was generated with OpenCV-Python which was created to resolve issues with computer vision.

OpenCV-Python has over 2500 optimised machine learning algorithms for facial and many objects detection.

It's important to mention the difference between face detection and face recognition. Face detection detects only faces in video or picture while face recognition identifies the face of the person in a picture or video. For this research, OpenCV-Python will be used to detect only faces from the images or videos which is captured by the external image/video capture device.

The purpose of using OpenCV-Python for this project is to identify faces in a video or images captured from the device's internal or external camera. After the face detection (How many faces are there in the video or picture) has been completed, the image will be cropped and pass on to the Neural Network for face recognition (To know the name of the person).

For OpenCV-Python to be able to detect a face in a picture or video, it uses an algorithm called Haar feature-based cascade classifier. There are many Haar feature-based

cascade classifiers algorithms to detect specific objects in an image or video. Examples are like cars, bikes, number plates and many different objects. Since our focus is on face detection, we will focus on the Haarcascade frontalface.

The Haarcascade frontalface algorithm classifier first requires many both positive (pictures of faces) and negative (images without faces). After that, we must draw features from it. The Haar features in the image below are utilised for this. They resemble our convolutional kernel exactly. Each feature is a single value that is obtained by deducting the sum of the pixels under the white and black rectangles.

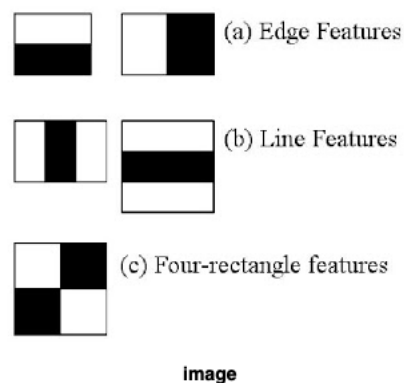


Figure 2. Sample of Haar cascade classifier features. SOURCE. (Behera, 2021)

To calculate and match features, the haar features move in window-sized across the image.

A classifier is used in the Haar cascade. Positive data points that are a part of our observed item are classified differently from negative data points that are not.

In the Figure 2 below, an example depiction of a picture with pixel values ranging from 0.0 to 1.0 is shown on the left in the rectangle. A haar kernel, which has all the bright pixels on the left and all the dark pixels on the right, is represented by the rectangle in the centre. The haar computation is performed by comparing the average pixel values at the lighter and darker regions, and then calculating the difference. The haar feature will detect an edge if the difference is near to 1. Basically, the Haar travels in a rectangle from left to right pattern covering the entire image or video a face.

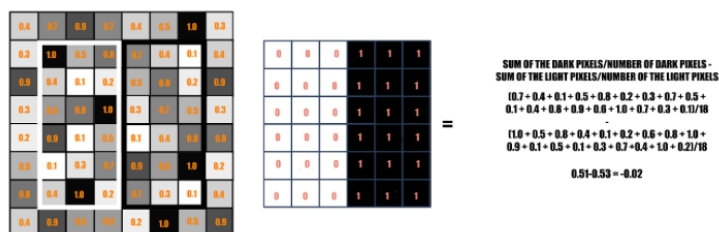


Figure 3. Haar cascade classifier mathematical calculations: SOURCE. (Behera, 2021)

Data_generate.py

The Data_collection.py file is coded to use a webcam to capture images, convert the image to grey and detect faces in the image.

After which the image will be cropped and converted from Red, Green, and Blue (RGB) to greyscale because grayscale is 3 channel image which reduces the complicity for face detection by the Haar cascade algorithm.

```
def generate_dataset():
    # pass camera to face-classifier
    face_classifier = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")

    def face_cropped(img):
        gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
        faces = face_classifier.detectMultiScale(gray, 1.3, 5)
        # scaling factor = 1.3
        # minimum neighbor = 5

        if faces is ():
            return None
        for (x, y, w, h) in faces:
            cropped_face = img[y:y+h, x:x+w]
            return cropped_face

    cap = cv2.VideoCapture(0)
    id = 1
    img_id = 0

    while True:
        ret, frame = cap.read()
        if face_cropped(frame) is not None:
            img_id += 1
            face = cv2.resize(face_cropped(frame), (288, 288))
            face = cv2.cvtColor(face, cv2.COLOR_BGR2GRAY)
            file_name_path = "images/user." + str(id) + "." + str(img_id) + ".jpg"
            cv2.imwrite(file_name_path, face)
            cv2.putText(face, str(img_id), (50, 50), cv2.FONT_HERSHEY_COMPLEX, 1, (0, 255, 0), 2)

            cv2.imshow("Cropped face", face)
```

Figure 4. generating dataset. SOURCE:(Arhinful,2002)

The next step is to connect (With OpenCV-Python) to the webcam to take images, the images will be stored into a folder called images. The images are stored in a folder called images.

After each image is collected from the participant, the webcam will be closed with a printed message “collecting samples completed....”

Train_classifier.py

Before we get into details of how to train the classifier, we will just have detailed explanation of the algorithm.

LBPH is a machine learning algorithm. The Local Binary Pattern (LBP) texturing operator labels each pixel in an image by thresholding its immediate surroundings and treating the result as a binary number.

Since its initial description in 1994 (LBP), it has emerged as a potent characteristic for texture categorization. Additionally, it has been found that using LBP in

conjunction with the HOG descriptor significantly enhances detection performance on specific datasets.

We can express the images of faces using a straightforward data vector by using the LBP in conjunction with histograms.

As a visual descriptor, LBP can also be utilised for face recognition tasks, as demonstrated in the steps that follow.

Let's continue and examine the steps of the algorithm now that we have a better understanding of facial recognition and the LBPH:

LBPH has 4 parameters.

Radius: Shows the areas surrounding the pixel for circular binary pattern , which stands for the region around the centre pixel. Mostly, it is set to 1.

Neighbors: The number of sample points used to create the local binary pattern in a circle.

Grid X: The quantity of cells arranged horizontally.

Grid Y: The quantity of cells arranged vertically.

The initial computational phase of the LBPH is to produce an intermediate image that, by emphasising the face features, more accurately describes the original image. The method does this by utilising a sliding window idea depending on radius and neighbours.

The illustration below demonstrates this process:

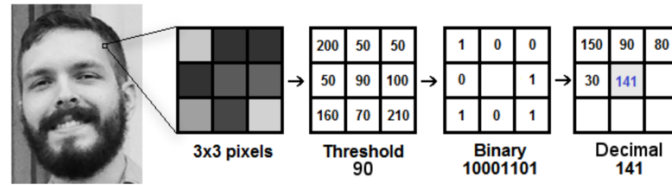


Figure 5. LBPH procedure. SOURCE (Prado, 2017)

Let's break it down into a few simple steps based on the illustration above so we can easily grasp it:

Let's say we have a grayscale image of a face.

- A 3x3 pixel window will give us a portion of this image.
- A 3x3 matrix with the intensity of each pixel (0–255) can likewise be used to represent it.
- The matrix's central value must then be used as the threshold, which is what we must do next.
- The new values from the eight neighbours will be defined using this value.
- We establish a new binary value for each neighbour of the threshold value. For values that are equal to or higher than the threshold, we set 1; for values that are lower, we set 0.
- The matrix will now only have binary values (ignoring the central value). Each binary value from each place in the matrix must be concatenated line by line to create a new binary value (e.g., 10001101). Note that while various authors concatenate the binary values in different ways (such as in a clockwise direction), the outcome will be the same.
- The central value of the matrix, which is a pixel from the original image, is then set to this binary value after being converted to a decimal value.

The algorithm needs to be trained with a dataset containing the facial photographs of the persons we wish to identify. For each image, we must additionally include an ID (which may be a number or a person's name), which the algorithm will use to identify an input image and provide an output. The same ID must appear on all images of the same person. the training set is already built.

To achieve this, the name of the images will be converted in a NumPy array. After training the classifier, it will be saved as a .xml file.

```
def generate_dataset():
    # pass camera to face-classifier
    face_classifier = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")

    def face_cropped(img):
        gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
        faces = face_classifier.detectMultiScale(gray, 1.3, 5)
        # scaling factor = 1.3
        # minimum neighbor = 5

        if faces is ():
            return None
        for (x, y, w, h) in faces:
            cropped_face = img[y:y+h, x:x+w]
            return cropped_face

    cap = cv2.VideoCapture(0)
    id = 1
    img_id = 0

    while True:
        ret, frame = cap.read()
        if face_cropped(frame) is not None:
            img_id += 1
            face = cv2.resize(face_cropped(frame), (200, 200))
            face = cv2.cvtColor(face, cv2.COLOR_BGR2GRAY)
            file_name_path = "images/user." + str(id) + "." + str(img_id) + ".jpg"
            cv2.imwrite(file_name_path, face)
            cv2.putText(face, str(img_id), (50, 50), cv2.FONT_HERSHEY_COMPLEX, 1, (0, 255, 0), 2)

            cv2.imshow("Cropped face", face)
```

Figure 6. Training the classifier . SOURCE: (Arhinful,2022)

The algorithm has already been trained at this point. Each histogram produced serves as a representation of one of the training dataset's images. To build a histogram that accurately depicts an image, we repeat the process for a fresh image after receiving an input image.

Therefore, we only need to compare two histograms to find the image that matches the input image.

- The distance between two histograms can be calculated using a variety of methods, such as the Euclidean distance, chi-square, absolute value, etc. Based on the following formula, we can apply the well-known Euclidean distance in this example:

$$D = \sqrt{\sum_{i=1}^n (hist1_i - hist2_i)^2}$$

Figure 7. Confidence level formular . SOURCE.(Prado. 2017)

Thus, the "confidence" measurement is the algorithm's output. The algorithm's accuracy in identifying the image can then be automatically determined using a threshold and "confidence." If the confidence is greater than the threshold specified, we can assume that the algorithm has correctly recognised the object.

Detect_face.py

The detect face.py file contains a function which draws boundaries over the image in the webcam. The code loads pre-saved images from the saved classifier.xml file and makes a prediction based on the stored images. If the images are not matched in the images folder, it will display "unknown"


```

def draw_boundary(img, classifier, scaleFactor, minNeighbors, color, text, clf):
    gray_img = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
    features = classifier.detectMultiScale(gray_img, scaleFactor, minNeighbors)

    for (x, y, w, h) in features:
        cv2.rectangle(img, (x, y), (x + w, y + h), color, 2)

        id, pred = clf.predict(gray_img[y:y + h, x:x + w])
        confidence = int(100 * (1 - pred / 300))

        if confidence > 79:
            if id == 1:
                cv2.putText(img, "Isaac", (x, y - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.8, color, 1, cv2.LINE_AA)
            if id == 2:
                cv2.putText(img, "xavi", (x, y - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.8, color, 1, cv2.LINE_AA)
            if id == 3:
                cv2.putText(img, "mana_africa", (x, y - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.8, color, 1, cv2.LINE_AA)
            else:
                cv2.putText(img, "UNKNOWN", (x, y - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.8, (0, 0, 255), 1, cv2.LINE_AA)

    return img

# loading classifier
faceCascade = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")

clf = cv2.face.LBPHFaceRecognizer_create()

```

Figure 8. Detect face. SOURCE. (Arhinful, 2022)

GUI.

A simple GUI was created with tkinter with 2 buttons, one for data generation and training. The other button is for face detection. The function in the GUI will connect to the webcam or external camera, generate dataset, train model, and predict images.

```

window = tk.Tk()
window.title("Pirate Face Recognition system")
# window.config(background=' ')
l1 = tk.Label(window, text="Name", font=("Algerian", 20))
l1.grid(column=0, row=0)
t1 = tk.Entry(window, width=50, bd=5)
t1.grid(column=1, row=0)

l2 = tk.Label(window, text="Age", font=("Algerian", 20))
l2.grid(column=0, row=1)
t2 = tk.Entry(window, width=50, bd=5)
t2.grid(column=1, row=1)

l3 = tk.Label(window, text="Address", font=("Algerian", 20))
l3.grid(column=0, row=2)
t3 = tk.Entry(window, width=50, bd=5)
t3.grid(column=1, row=2)

```

Figure 9. Tkinter GUI. SOURCE. (Arhinful, 2022)

SQL Database.

The final part of the project is to create an SQL database to store all the information from the pirates. This database will serve as source of information on the suspected pirates.

The database can be access on a local network. Below is the URL address.

http://localhost/phpmyadmin/index.php?route=/sql&db=Authorised_user&table=my_table&pos=0

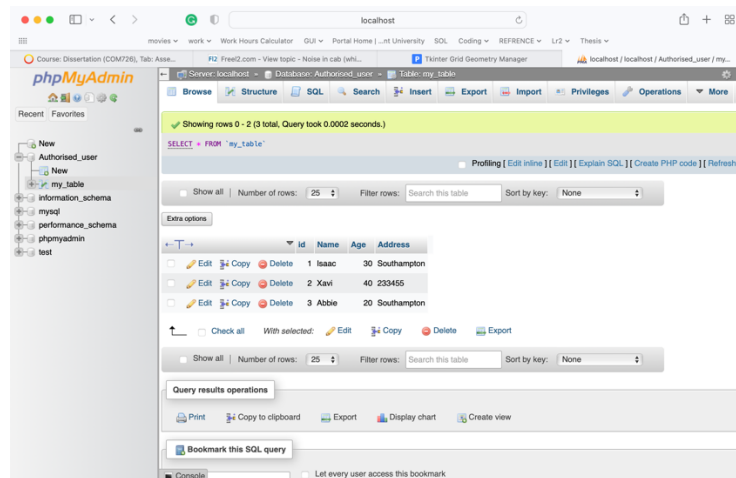


Figure 10. SQL Database Table. SOURCE: (Arhinful,2022)

```
mydb = mysql.connector.connect(
    host="localhost",
    user="root",
    passwd="",
    database="Authorised_user"
)
mycursor = mydb.cursor()
mycursor.execute('select name from my_table where id=' + str(id))
s = mycursor.fetchone()
s = '' + ''.join(s)

if confidence > 74:
    cv2.putText(img, s, (x, y - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.8, color, 1, cv2.LINE_AA)
else:
    cv2.putText(img, "UNKNOWN", (x, y - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.8, (0, 0, 255), 1, cv2.LINE_AA)

coords = [x, y, w, h]
return coords

def recognize(img, clf, faceCascade):
    coords = draw_boundary(img, faceCascade, 1.1, 10, (255, 255, 255), "Face", clf)
    return img
```

Figure 11. SQL Database Code. SOURCE:(ARHINFUL,2022)

Project conversion to application.

The project was converted to .exe file to be used on windows operating system.

CHAPTER FOUR

4.1 Research Analysis and findings.

From the software results, we noticed the software was able to identify each participant in the research. What we also noticed was, the 'confidence' level parameter needed a little adjustment during night mode.

The background light had a significant impact on the confidence level which is an important parameter for accurately making the identifications.

```

if confidence > 79:
    cv2.putText(img, s, (x, y - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.8, color, 1, cv2.LINE_AA)
else:
    cv2.putText(img, "UNKNOWN", (x, y - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.8, (0, 0, 255), 1, cv2.LINE_AA)

    coords = [x, y, w, h]
return coords

def recognize(img, clf, faceCascade):
    coords = draw_boundary(img, faceCascade, 1.1, 10, (255, 255, 255), "Face", clf)
return img

```

Figure 12. Confidence level parameter. SOURCE (Arhinful,2022)

The software was able to identify all participants during day light but failed to identify one black male participant in the living space ambient light conditions. With an increase in the confidence level to 82, it was able to recorrect its error and identified the last (all) participant.

	Daylight with about 2300 footcandles (confidence 79)	Living space ambient with about 5 footcandles (confidence 80)
Number of participants identified correctly.	5	4

Figure 13. Real world test results. SOURCE(Arhinful, 2022)

The figure below shows the first test with two participants at the same time.

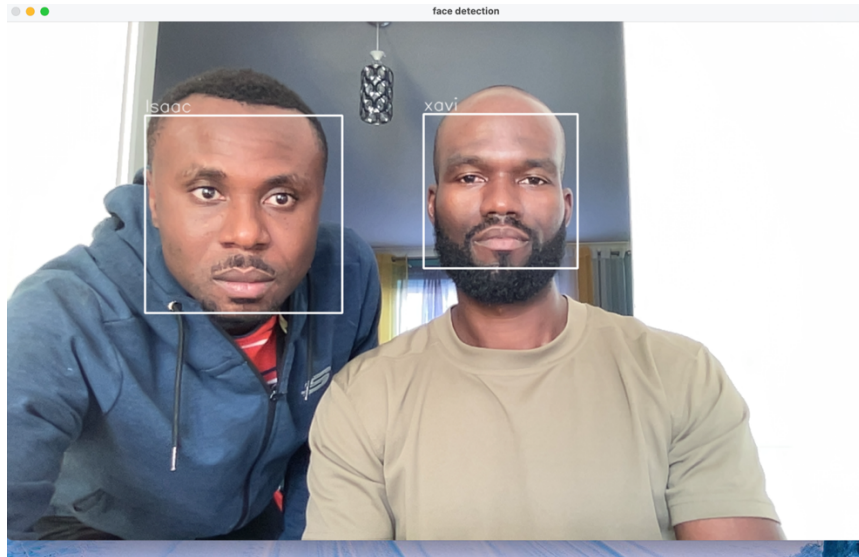


Figure 14. Test with two participants. SOURCE(Arhinful , 2022)

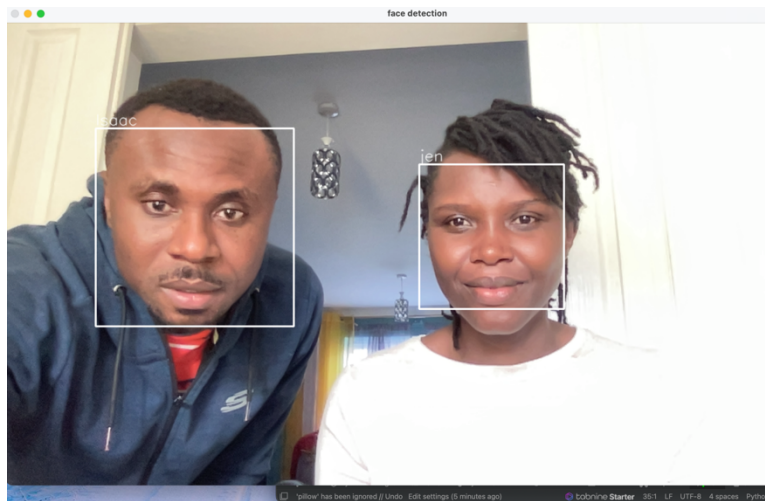


Figure 15. Test with two participants2 (SOURCE(Arhinful , 2022)

This software can be incorporated into microprocessors like raspberry pie or UAV for combating Maritime Piracy

CHAPTER FIVE

5.1 Limitation.

The software was not tested on UAV to test its robust capabilities due to lack of UAV hardware. In this situation, the software will rely on the integrity of the UAV camera

for accurate facial detection. Most cameras are fitted with gimbles and can pick up objects from long range. The Technology is available, which makes this research pragmatic.

Another limitation is the model evaluation which is a crucial part of AI modelling. Since the LBPH algorithm is already defined and takes its testing source live from the camera, the researcher must use different techniques to get the model score which was unsuccessful at that time due to minimum time. But the PyCharm IDE shows evidence of several attempts to get the actual model performance figures. This will be worked on in the future.

CHAPTER SIX

6.1 Conclusion.

Today, property safety and Maritime operations security have grown to be major global concerns. Many security control methods, such as video surveillance and alarm monitoring, have been deployed, but contemporary security requirements call for advanced technology.

This study used human facial detection and recognition techniques to create a cooperative software for UAV for surveillance in an open environment. These body detection and facial recognition algorithms function effectively under controlled conditions, according to

experimental observations. The focus of future study will be on performance enhancement, such as expanding the facial recognition ranges in various locations and under diverse circumstances.

Reference (Harvard Style).

AHONEN, T. (2008). *The interview of research scientist Timo Ahonen on 13.5.*

AL ABKAL, TALAS,R, SHAW,S and ELLIS ,E(2020). *The application of unmanned aerial vehicles in managing port and border security in the US and Kuwait: Reflections on best practice for the UK, IJMCS* , Vol. 01 Issue 01, <https://doi.org/10.24052/IJMCS/V01IS01/ART-3>

ALI, K-D. (2014). *Maritime security cooperation in the Gulf of Guinea: prospects and challenges, Doctor of Philosophy thesis, Australian National Centre for Ocean Resources and Security (ANCORS), University of Wollongong, 2014.* <https://ro.uow.edu.au/theses/4095>

AMATO, G., CARRARA, F., FALCHI, F., GENNARO, C., & VAIRO,C. (2018, October). *Facial-based intrusion detection system with deep learning in embedded devices. In Proceedings of the 2018 International Conference on Sensors, Signal and Image Processing* (pp. 64-68). <https://dl.acm.org/doi/pdf/10.1145/3290589.3290598>

AMIREL, S.E. (2009). La piraterie maritime en Afrique contemporaine, ressort locaux et internationaux des activités de piraterie au Nigeria et en Somalie. *Politique Africaine*, 116, pp. 97-120

ATOLE, R. R. BELLO, L. C. S and LIRAG, J. R. S. (2017). Eyes in the Sky: A Review of Civilian Unmanned Aerial Vehicles (UAVs). *International Journal of Computer Applications*. Vol. 173, Issue 6, pp.36-41. doi:10.5120/ijca2017915349

AYTO, J. (2005). *Word origins: The hidden histories of English words from A to Z. London: A & C Black Publishers Ltd.*

BANIK, D., IBNE HOSSAIN, N.U., GOVINDAN, K., NUR, F. AND BABSKI-REEVES, K. (2022) A decision support model for selecting unmanned aerial vehicle for medical supplies: context of COVID-19 pandemic, *The International Journal of Logistics Management*, <https://doi.org/10.1108/IJLM-06-2021-0334>

BOO, H.C. AND CHUA, B.-L. (2022).An integrative model of facial recognition check-in technology adoption intention: the perspective of hotel guests in Singapore, *International Journal of Contemporary Hospitality Management*, <https://doi.org/10.1108/IJCHM-12-2021->

BROWNLIE , J. 2020. Train-Test Split for Evaluating Machine Learning Algorithms. [Online]. [26 August 2022]. Available from: <https://machinelearningmastery.com/train-test-split-for-evaluating-machine-learning-algorithms/>

CAPLAN, J., MORETO, W., & KENNEDY, L. (2010). *Forecasting global maritime piracy utilizing the risk terrain modeling approach to spatial risk assessment.* Unpublished.

CHANG, Y.-C. AND KHAN, M.I. (2019).China–Pakistan economic corridor and maritime security collaboration: A growing bilateral interests, *Maritime Business Review*, Vol. 4 No. 2, pp. 217-235. <https://doi.org/10.1108/MABR-01-2019-0004>

CHOUDHURY, Z. H. (2019). Cosmetic Applied Based Face Recognition for Biometric Passport. *International Journal of Intelligent Unmanned Systems*.

COOK, C. M., HOWARD, J. J., SIROTIN, Y. B., TIPTON, J. L., & VEMURY, A. R. (2019). Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 1(1).

DANG, V.T., NGUYEN, N., NGUYEN, H.V., NGUYEN, H., VAN HUY, L., TRAN, V.T. AND NGUYEN, T.H. (2022). Consumer attitudes toward facial recognition payment: an examination of antecedents and outcomes, *International Journal of Bank Marketing*, Vol. 40 No. 3, pp. 511-535. <https://doi.org/10.1108/IJBM-04-2021-0135>

GIRIJA SHANKAR , B. 2020. *Face Detection with Haar Cascade*. [Online]. [26 August 2022]. Available from: <https://towardsdatascience.com/face-detection-with-haar-cascade-727f68dafd08>

GOODWIN, J. (2006). Universal jurisdiction and the pirate: Time for an old couple to part. *Vanderbilt Journal of Transnational Law*, 39, 973-1011.

GROTE,M,PILKO,A, SCANLAN,J, CHERRETT, DICKSON, J,SMITH,A, OAKLEY,A AND MARSDEN,G (2022).Sharing airspace with Uncrewed Aerial Vehicles (UAVs): Views of the General Aviation (GA) community. *Journal of Air Transport Management*, Vol.102.<https://doi.org/10.1016/j.jairtraman.2022.102218>

HASHTINGS, J. V. AND PHILIPS, S. G. (2022). Maritime piracy business networks and institutions in Africa. *African Affairs*, Vol. 114, Issue 457, pp. 555–576,<https://doi.org/10.1093/afraf/adv040>

HENDERSON, G.R., RANK-CHRISTMAN, T., WHITE, T.B., GRANTHAM, K.D., OSTROM, A.L. AND LYNCH, J.G. (2018). Intercultural competence and customer facial recognition, *Journal of Services Marketing*, Vol. 32 No. 5, pp. 570-580. <https://doi.org/10.1108/JSM-07-2017-0219>

HU, Y. AN, H. GUO, Y. ZHANG, C. AND LI, Y. (2010). The development status and prospects on the face recognition. In *Bioinformatics and Biomedical Engineering (ICBBE)*, 2010 4th International Conference on, 2010

IBM. 2020. *Convolutional Neural Networks*. [Online]. [26 August 2022]. Available from: <https://www.ibm.com/cloud/learn/convolutional-neural-networks>

INBRIEFCO.UK. 2022. *Image rights in UK law*. [Online]. [26 August 2022]. Available from: <https://www.inbrief.co.uk/human-rights/image-rights/>

JONES, S. (2014). Maritime piracy and the cost of world trade*, *Competitiveness Review*, Vol. 24 No. 3, pp. 158-170. <https://doi.org/10.1108/CR-02-2013-0008>

JULIUS, A. O. EKO-RAPHAELS, M. U. CHIMMA, O. C. DANIEL, O. B. AND EME, O. N. (2022). Sea Piracy and Armed Robbery in the Gulf of Guinea and Its Effect on Shipping Cost and Nigeria's Economic Growth, *Oceanography & Fisheries*. Vol. 14 Issue 4 - February 2022 DOI:10.19080/OFOAJ.2021.14.555894

KÄMÄRÄINEN, J. (2008). The interview of Doctor (D.Sc) Joni Kämäräinen on 9.6.

KESHTGAR, S. KESHTGAR, A. MISTRY, P. AND SHAKIB, K. (2019). Assessing facial recognition after orthognathic surgery at automated border controls in airports, Vol. 57, Issue 6, pp.536-538, DOI:<https://doi.org/10.1016/j.bjoms.2018.12.021>

KHAN S, TUFAIL M, KHAN MT, KHAN ZA, IQBAL J, WASIM A (2021) Real-time recognition of spraying area for UAV sprayers using a deep learning approach. *PLoS ONE* .Vol.16,Issue 4.. <https://doi.org/10.1371/journal.pone.0249436>

LANDER, K. BRUCE, V. AND BINDEMANN, M. (2018). Use-inspired basic research on individual differences in face identification: Implications for criminal investigation and security. *Cognitive research: principles and implications*, 3(1):1–13,

- LANGFITT, F. (2011). Somaliland struggles in effort to fight piracy. National Public Radio. Retrieved from <http://www.npr.org/2011/04/13/135345974/somaliland-strugglesin-effort-to-fight-piracy>
- LEHMUSSOLA, A. (2008). The interview of forensic engineer Antti Lehmussola on 12.5.
- Li, L. Mu, X. Li, S. and Haipeng, P. (2020). A review of face recognition technology. *IEEE Access*, (4)99, 1-12
- LI, S. AND FUNG, K. S. (2019). Maritime autonomous surface ships (MASS): implementation and legal issues. *Maritime Business Review*, Vol. 4 No. 4, 2019 pp. 330-339 .7 DOI 10.1108/MABR-01-2019-000
- LIU, T. YANG, B. GENG, Y. and DU, S. (2021). Research on Face Recognition and Privacy in China—Based on Social Cognition and Cultural Psychology. *Front. Psychol.* <https://doi.org/10.3389/fpsyg.2021.80>
- MOUNGSOUY, W. TAWANBUNJERD, T. LIAMSOMBOON, N. AND KUSAKUNNIRAN, W. (2022). Face recognition under mask- wearing based on residual inception networks. *Applied Computing and Informatics*. DOI 10.1108/ACI-09-2021-0256
- MURPHY, M. (2007). Contemporary piracy and maritime terrorism: The threat to international security. London, UK: Routledge.
- OPEN-SOURCE COMPUTER VISION. 2022. *Cascade Classifier*. [Online]. [26 August 2022]. Available from: https://docs.opencv.org/3.4/db/d28/tutorial_cascade_classifier.html
- OPENCVORG. 2022. *Opencv*. [Online]. [26 August 2022]. Available from: <https://opencv.org/about/>
- OPENGENUSORG. 2021. *Local Binary Patterns Histogram (LBPH)*. [Online]. [23 August 2022]. Available from: <https://iq.opengenus.org/lbph-algorithm-for-face-recognition/>
- PADRO, K. 2017. *Face Recognition: Understanding LBPH Algorithm*. [Online]. [1 September 2022]. Available from: <https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b>
- PASSAS, N. (2000). Global Anomie, dysnomie, and economic Crime: Hidden consequences of neoliberalism and globalization in Russia and around the world. *Social Justice*, 27(2), 16-44.
- Passas, N. (1999). Globalization, criminogenic asymmetries, and economic crime. *European Journal of Law Reform*, 1(4), 399-423.
- PROGRAMMATICALLYCOM. 2021. *What is Pooling in a Convolutional Neural Network (CNN): Pooling Layers Explained*. [Online]. [26 August 2022]. Available from: <https://programmatically.com/what-is-pooling-in-a-convolutional-neural-network-cnn-pooling-layers-explained/>
- RANDRIANANTENAINA, E. J. (2013). Maritime piracy and armed robbery against ships: Exploring the legal and the operational solutions. The case of Madagascar. The United Nations – Nippon Foundation
- RINGSBERG, A. H. AND COLE, S. (2020). Maritime security guidelines: a study of Swedish ports' perceived barriers to compliance, *The flagship journal of international shipping and port research*, Vol. 47, 2020 - Issue 3 <https://doi.org/10.1080/03088839.2020.171197>
- ROSSION, B., & MICHEL, C. (2018). Normative accuracy and response time data for the computerized Benton Facial Recognition Test (BFRT-c). *Behavior research methods*, 50(6), 2442-2460. <https://link.springer.com/article/10.3758/s13428-018-1023-x>
- RUBIN, A. (2006). The Law of Piracy. Honolulu, HI: University Press of the Pacific.
- RUIZ, R.D.B., LORDSLEEM JR., A.C., ROCHA, J.H.A. AND IRIZARRY, J.(2021). Unmanned aerial vehicles (UAV) as a tool for visual inspection of building facades in AEC+FM industry, *Construction Innovation*. <https://doi.org/10.1108/CI-07-2021-0129>

TAHIR, A. BOLING, J. HAGHBAYAN, M. H. TOIVOVEN, H. T. AND PLOSILA, J. (2019). Swarms of Unmanned Aerial Vehicles — A Survey, *Journal of Industrial Information Integration*, Vol. 16. <https://doi.org/10.1016/j.jii.2019.100106>

TEMI, B. 2018. The Mathematics of Neural Networks. [Online]. [20 March 2022]. Available from: <https://medium.com/coinmonks/the-mathematics-of-neural-network-60a112dd3e05>

TWYMAN-GHOSHAL, A. (2021). Global anomie theory. *Criminology and Criminal Justice*,

WARREN, R.C. (2011). Piracy and shipowners' ethical dilemmas, *Society and Business Review*, Vol. 6 No. 1, pp. 49-60. <https://doi.org/10.1108/174656811111105832>

WU, J. 2017. *Introduction to Convolutional Neural Networks*. [Online]. [6 August 2022]. Available from: <https://cs.nju.edu.cn/wuj/paper/CNN.pdf>

YAO, F AND QIU, L. (2021) Facial Expression Recognition Based on Convolutional Neural Network Fusion SIFT Features of Mobile Virtual Reality, <https://doi.org/10.1155/2021/5763626>

YU, B, JEON, H, YI, S, S AND MIN, J (2022). Fender segmentation in unmanned aerial vehicle images based on densely connected receptive field block. *International Journal of Naval Architecture and Ocean Engineering*. <https://doi.org/10.1016/j.ijnaoe.2022.100472>

ZAQOUT, I. AND AL-HANJORI, M. (2018). An improved technique for face recognition applications, *Information and Learning Sciences*, Vol. 119 No. 9/10, pp. 529 544. <https://doi.org/10.1108/ILS-03-2018-0023>

ZHANG, R. HOLVOET, T. SONG, B. AND PEI, Y. (2018). UAVs versus Pirates: A Pheromone-based Swarm Monitoring Method. *2018 IEEE International Conference on Robotics and Biomimetics (ROBIO)*, pp. 2253-2258, doi: 10.1109/ROBIO.2018.8665067

Appendix

Participant questionnaire forms.

Research Participant Consent Form

Title of Project: Impact of Artificial Intelligence facial recognition on Maritime Piracy

Name of Researcher: Isaac Arhinful

> I have been given the opportunity to ask questions (face to face, via telephone and e-mail)

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

> I agree for the data and image collected from me to be used for the research.

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
---	-----------------------------	-----------------------------

> I agree to the interview being tape recorded

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
---	-----------------------------	-----------------------------

> I agree to digital images being taken during the research exercises

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> NA
---	-----------------------------	-----------------------------


> I understand that my participation is voluntary and that I can withdraw from the research at any time **without giving any reason**

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

> I agree to take part in the above study

<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
---	-----------------------------

Name of participant Sharnaz Khan

Signature 

Date 22/08/22

Name of researcher taking consent Isaac Arhinful

Researchers e-mail address Germplus@paho.com

©G / Gastronominplanungs GmbH

Figure 16. Participant Questionnaire form 1.

Research Participant Consent Form

Title of Project: Impact of Artificial Intelligence facial recognition on Maritime Piracy

Name of Researcher: Isaac Arhinful

> I have been given the opportunity to ask questions (face to face, via telephone and e-mail) Yes No

> I agree for the data and image collected from me to be used for the research. Yes No NA

> I agree to the interview being tape recorded Yes No NA

> I agree to digital images being taken during the research exercises Yes No NA

> I understand that my participation is voluntary and that I can withdraw from the research at any time **without giving any reason** Yes No

> I agree to take part in the above study Yes No

Name of participant Jane Odwibo

Signature [Signature]

Date 12/8/22

Name of researcher taking consent Isaac Arhinful

Researchers e-mail address germplus@yahoo.co

Figure 17. Participant Questionnaire form 2

Research Participant Consent Form

Title of Project: Impact of Artificial Intelligence facial recognition on Maritime Piracy

Name of Researcher: Isaac Arhinful

> I have been given the opportunity to ask questions (face to face, via telephone and e-mail)

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
---	-----------------------------

> I agree for the data and image collected from me to be used for the research.

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>	NA <input type="checkbox"/>
---	-----------------------------	-----------------------------

> I agree to the interview being tape recorded

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>	NA <input type="checkbox"/>
---	-----------------------------	-----------------------------

> I agree to digital images being taken during the research exercises

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>	NA <input type="checkbox"/>
---	-----------------------------	-----------------------------


> I understand that my participation is voluntary and that I can withdraw from the research at any time **without giving any reason**

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
---	-----------------------------

> I agree to take part in the above study

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
---	-----------------------------

Name of participant ABIGAIL ARHINFIL

Signature 

Date ✓

Name of researcher taking consent Isaac Arhinful

Researcher's e-mail address Gemplus@yahoo.com

Figure 18. Participant Questionnaire form 3

Research Participant Consent Form

Title of Project: Impact of Artificial Intelligence facial recognition on Maritime Piracy

Name of Researcher: Isaac Arhinful

> I have been given the opportunity to ask questions (face to face, via telephone and e-mail)

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
---	-----------------------------

> I agree for the data and image collected from me to be used for the research.

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>	NA <input type="checkbox"/>
---	-----------------------------	-----------------------------

> I agree to the interview being tape recorded

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>	NA <input type="checkbox"/>
---	-----------------------------	-----------------------------

> I agree to digital images being taken during the research exercises

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>	NA <input type="checkbox"/>
---	-----------------------------	-----------------------------

> I understand that my participation is voluntary and that I can withdraw from the research at any time without giving any reason

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
---	-----------------------------

> I agree to take part in the above study

Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
---	-----------------------------

Name of participant LOREKINE BIGGS

Signature L Biggs

Date 07-09-2022

Name of researcher taking consent Isaac Arhinful

Researchers e-mail address germylusa@yahoo.com

Figure 19. Participant Questionnaire form 3