**KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**COLLEGE OF SCIENCE**

**DEPARTMENT OF COMPUTER SCIENCE**

****

**Facial Expression Surveillance for Enhanced Security in Commercial Spaces (FESSECS).**

**BY:**

**Osei Roy Jake Sarfo -- 9415319**

**Amo Gilbert -- 9395819**

**SUPERVISOR:**

**REV. DR. KWAME OFOSUHENE PEASAH**

# DECLARATION

We hereby declare that the research documentation titled " Automated Poultry Incubation System: A Sustainable Solution for Ghana’s Poultry Sector " represents our original work and has been carried out under the supervision of Rev. Dr. K.O. Peasah as part of our bachelor’s degree in Computer Science at Kwame Nkrumah University of Science and Technology. All sources of information and materials used in this documentation have been duly acknowledged and cited.

**…………………………………….. …………………..**

**OSEI ROY JAKE SARFO DATE**

**(9415319)**

**…………………………………….. …………………..**

**AMO GILBERT DATE**

**(9395819)**

I declare that I have supervised these students to undertake the project submitted herein an I confirm that these students have any permission to submit for assessment.

**…………………………………….. …………………..**

**REV. DR. KWAME OFOSUHENE PEASAH DATE**

**(SUPERVISOR)**

# ACKNOWLEDGEMENT

We extend our heartfelt gratitude to all those who have contributed to the successful completion of this research documentation. We are deeply thankful to our supervisor, Rev. Dr. K.O. Peasah, for his invaluable guidance, support, and mentorship throughout this journey. Their expertise and insights have been instrumental in shaping the direction of this project.

We would like to express our sincere appreciation to our friends and colleagues for their assistance and contributions, whether through technical guidance, resources, or valuable discussions.

We are grateful to our families for their unwavering encouragement and belief in our abilities.

Lastly, we acknowledge the poultry farmers and stakeholders who participated in this research, as their insights and cooperation were pivotal in understanding the practical implications of the Automated Poultry Egg Incubator.

This research documentation stands as a testament to the collective efforts of all those who have supported us along this academic endeavor.

# TABLE OF CONTENT

[DECLARATION 2](#_Toc145065724)

[ACKNOWLEDGEMENT 3](#_Toc145065725)

[TABLE OF CONTENT 4](#_Toc145065726)

[CHAPTER ONE 6](#_Toc145065727)

[1.1 INTRODUCTION. 6](#_Toc145065728)

[1.2 ABSTRACT. 7](#_Toc145065729)

[1.3 PROBLEM STATEMENT. 8](#_Toc145065730)

[1.4 JUSTIFICATION. 9](#_Toc145065731)

[1.5 AIMS AND OBJECTIVES. 10](#_Toc145065732)

[Aims: 10](#_Toc145065733)

[Objectives: 11](#_Toc145065734)

[1.6 PROJECT LIMITATIONS. 12](#_Toc145065735)

[2.1 DEFINITION OF THE SYSTEM. 14](#_Toc145065736)

[2.2 LITERATURE REVIEW. 15](#_Toc145065737)

[3.1 THE PROPOSED SYSTEM. 18](#_Toc145065738)

[Key Components and Functionality: 19](#_Toc145065739)

[DEVELOPMENT TOOLS. 20](#_Toc145065740)

[Software Development Tools: 20](#_Toc145065741)

[Hardware and Sensor Tools: 20](#_Toc145065742)

[4. IMPLEMENTATION AND TESTING. 23](#_Toc145065743)

[4.1 IMPLEMENTATION. 23](#_Toc145065744)

[1. Emotion data acquisition. 23](#_Toc145065745)

[2. Image to arrays 23](#_Toc145065746)

[3. Image to landmarks 23](#_Toc145065747)

[4. CNN architecture 24](#_Toc145065748)

[5. Compiling the model 25](#_Toc145065749)

[6. Training the model 26](#_Toc145065750)

[7. Real-time face detection 26](#_Toc145065751)

[8. Emotion analysis strategy 27](#_Toc145065752)

[4.2 TESTING. 29](#_Toc145065753)

[4.3 CONCLUSION. 29](#_Toc145065754)

[4.4 REFERENCE. 31](#_Toc145065755)

# CHAPTER ONE

# 1.1 INTRODUCTION.

In this project, we're looking into a high-tech solution to enhance security in places like banks and airports. We're using advanced technology that can read people's facial expressions. This technology helps us identify if someone is behaving unusually or might pose a threat. It's like having an extra layer of security to ensure everyone's safety.

However, we're not just focusing on security alone. We're also exploring how this technology can improve customer experiences. For example, if the system detects a happy customer, businesses can offer them special services to make their visit even better.

Yet, using this technology raises important questions about privacy and surveillance. So, we're working to find a balance between boosting security and respecting people's privacy rights.

This project revolves around using technology to create safer and more enjoyable places for everyone.

# 1.2 ABSTRACT.

Facial expression surveillance systems have emerged as a technologically innovative approach to bolster security measures in diverse commercial spaces, including banks and airports. By harnessing the power of computer vision and machine learning, these systems aim to analyze individuals' facial expressions to detect anomalies, emotions, and potential security threats. This paper explores the multifaceted landscape of implementing such systems in commercial settings, encompassing benefits, challenges, ethical considerations, and future implications. It delves into the potential advantages of enhancing security protocols through real-time emotion analysis, from deterring criminal activities to fostering personalized customer experiences. Simultaneously, it acknowledges the ethical dilemmas arising from the invasion of personal privacy, consent, and the potential for algorithmic biases. Drawing insights from both technological advancements and ethical frameworks, this paper navigates the intricate balance between heightened security and safeguarding fundamental rights within the context of facial expression surveillance in banks and airports. Through a comprehensive evaluation of the various dimensions, this paper contributes to the ongoing discourse on responsible implementation and utilization of surveillance technologies, promoting a harmonious coexistence of security and ethical considerations.

# 1.3 PROBLEM STATEMENT.

The integration of facial expression surveillance systems within the confines of commercial environments such as banks and shops introduce a dynamic array of challenges and ethical dilemmas that necessitate rigorous examination. These systems, leveraging advancements in computer vision and machine learning, promise to revolutionize security measures by analyzing real-time emotional cues. However, the deployment of these systems raises multifaceted concerns that extend beyond the mere technological realm.

At the core of this issue lies the challenge of harmonizing heightened security imperatives with the preservation of fundamental individual rights. As the capability to interpret facial expressions in real-time becomes increasingly sophisticated, the risk of infringing upon personal privacy and consent becomes salient. The question of how to strike a delicate equilibrium between the imperative to prevent security threats and the potential intrusion into personal spheres is paramount.

Furthermore, the accuracy and reliability of facial expression recognition algorithms stand as a pivotal concern. The potential for misinterpretation or misclassification of emotions, coupled with biases inherent in algorithmic design, could lead to unwarranted alerts or overlooked security breaches. Additionally, cultural nuances in facial expressions pose a challenge, as the interpretation of emotions can greatly vary across diverse demographics and social contexts.

Ethical considerations encompassing transparency, data protection, and the potential for algorithmic discrimination amplify the complexity of the issue. The deployment of facial expression surveillance systems mandates clear communication with stakeholders about the presence and implications of such technology. Effective data encryption, access controls, and safeguarding against unauthorized data usage are non-negotiable imperatives. Moreover, ensuring that these systems do not disproportionately impact specific demographic groups or perpetuate biases is an ethical imperative that demands meticulous attention.

In light of these challenges, it is imperative to conduct a comprehensive investigation into the nuanced interplay between heightened security measures and the ethical considerations that underpin a just and inclusive society. Balancing the technical prowess of facial expression surveillance systems with a profound respect for individual autonomy, cultural diversity, and data protection is an intricate endeavor that warrants thorough exploration. This study aims to address these pressing concerns and chart a course toward the conscientious and responsible integration of facial expression surveillance systems in the complex landscape of commercial spaces, thereby fostering an environment where security and ethics coalesce seamlessly.

# 1.4 JUSTIFICATION.

The selection of facial expression surveillance systems in commercial spaces, specifically in banks and shops, as a research topic is substantiated by the convergence of several significant factors that underscore its importance and relevance in the current socio-technological landscape.

1. Evolving Security Needs: The prevalence of security threats and challenges faced by commercial establishments necessitates a continuous evolution of security measures. Facial expression surveillance systems offer a potential avenue to enhance the effectiveness of security protocols by enabling real-time detection of suspicious behavior or emotional cues that might indicate impending threats.

2. Technological Advancements: The rapid advancements in computer vision, machine learning, and facial recognition technologies have transformed the feasibility of emotion analysis in real-world scenarios. This progress provides an opportunity to explore the practical implementation of these systems in safeguarding commercial spaces.

3. Balancing Security and Ethics: The ethical dimensions surrounding surveillance technologies in public and private spaces have gained prominence. Examining facial expression surveillance in banks and shops allows for a nuanced exploration of the trade-offs between heightened security and the preservation of individual rights to privacy and consent.

4. Customer Experience Enhancement: Beyond security, understanding customer emotions through facial expression analysis can empower establishments to tailor their services and experiences, thereby fostering customer loyalty and satisfaction.

5. Mitigating Bias and Discrimination: Algorithmic biases and their potential to disproportionately impact certain demographics are pertinent concerns. Addressing these issues is vital to ensure that facial expression surveillance systems do not perpetuate societal inequities.

# 1.5 AIMS AND OBJECTIVES.

## Aims:

The overarching aim of this research is to investigate the efficacy and impact of facial expression surveillance systems on security enhancement within the context of banks and airports. The research seeks to provide a comprehensive understanding of how these systems can bolster security measures and contribute to threat detection in commercial environments.

## Objectives:

1. To Evaluate Technological Viability for Security:

- Examine the technological capabilities of facial expression recognition systems and their potential to enhance security protocols in banks and airports.

- Assess the real-time analysis of facial expressions as a viable tool for identifying suspicious behaviors and potential threats.

2. To Analyze Threat Detection Effectiveness:

- Investigate the practical application of facial expression surveillance in real-world scenarios to identify individuals exhibiting anomalous behavior.

- Assess the accuracy and efficiency of these systems in detecting security threats compared to traditional methods.

3. To Address Technological Limitations:

- Identify and analyze the limitations and challenges associated with facial expression recognition technology, such as false positives, false negatives, and variations in expression interpretation.

4. To Propose Security-Enhancing Strategies:

- Develop strategies and recommendations for optimizing the deployment and utilization of facial expression surveillance systems to enhance security.

- Provide insights into configuration, camera placement, and alert mechanisms for effective threat detection.

By achieving these objectives, the research aims to contribute to the ongoing discourse on security measures within commercial spaces, specifically focusing on the practical application and impact of facial expression surveillance systems. Through empirical analysis and strategic recommendations, this study intends to offer valuable insights for stakeholders seeking to optimize security practices while leveraging cutting-edge surveillance technologies.

# 1.6 PROJECT LIMITATIONS.

While this research seeks to comprehensively investigate the implementation of facial expression surveillance systems in commercial spaces, particularly in banks and airports, it is important to acknowledge certain limitations that may impact the scope and generalizability of the findings:

1. Technological Variability: The effectiveness of facial expression recognition technology can vary based on factors such as lighting conditions, camera quality, and environmental context. The outcomes of this research might be influenced by the specific technology and tools available for analysis.

2. Limited Sample Size: Gathering empirical data from real-world implementations might be constrained by access to suitable case studies and participants. As a result, the findings could be limited in terms of representing the entire spectrum of commercial spaces.

3. Ethical Considerations: Due to the ethical implications of facial expression surveillance, the collection of real-time facial expression data in controlled experiments may raise privacy concerns and necessitate careful participant consent and safeguards.

4. Cultural Diversity: The interpretation of facial expressions can be influenced by cultural nuances and variations. This research might not capture the full extent of these cultural differences, potentially leading to less generalizable conclusions.

5. Bias and Algorithmic Limitations: The analysis of facial expressions by machine learning algorithms can be susceptible to biases and inaccuracies, which could affect the validity of threat detection and security enhancement findings.

6. Time Constraints: Comprehensive analysis of long-term impacts and benefits of facial expression surveillance might be challenging within the scope of a single research project, potentially limiting the ability to assess the sustained effectiveness of these systems.

CHAPTER TWO

# 2.1 DEFINITION OF THE SYSTEM.

Facial Expression Surveillance System Definition:

A facial expression surveillance system refers to an advanced technological framework that employs computer vision, machine learning, and real-time analytics to analyze and interpret individuals' facial expressions in various environments, including commercial spaces such as banks and airports. The system's primary objective is to detect and interpret emotional cues displayed through facial expressions, such as happiness, sadness, stress, or suspicion. By identifying deviations from baseline emotional states, the system aims to preemptively identify potential security threats, illicit activities, or anomalous behaviors.

The core functionality of a facial expression surveillance system involves capturing high-resolution images or video streams of individuals' faces using strategically placed cameras. These visual inputs are then processed using sophisticated computer algorithms that extract facial features, analyze expressions, and categorize emotions. Machine learning models are often employed to train the system to recognize a spectrum of emotional states, allowing it to identify patterns indicative of security concerns.

# 2.2 LITERATURE REVIEW.

Face detection enables the identification and validation of human faces from images, videos, and other forms of graphics. It traces facial features, contours, and texture to analyze the unique biometric and demographic details of individuals. M.-H. Yang, Kriegman, and Ahuja (2002)**[1]** proposed some methods for facial detection that included: knowledge-based methods which captures relationship between facial features, Feature-based methods which aims to find the structural features, Template-matching methods use to show standard patterns of a face which are stored to describe the face as a whole or the facial features separately, and Appearance-based models which are learned from a set of training images capturing the representative variability of the facial appearance. Each of the methods applied have their own relative performance outcomes and due to the lack of uniformity in how methods are evaluated it’s hard to explicitly declare which methods indeed have the lowest error rates. As an ongoing study research area, more complex algorithms can be introduced for advance accuracy (M.-H. Yang et al., 2002).

Humans are capable to express thousands of facial expressions that vary in intensity, complexity and meaning. Kartali, Roglić, Barjaktarović, Đurić-Jovičić, and Janković (2018)**[2]** proposed algorithms that performs detection, extraction, and evaluation of facial expressions and will allow for real-time emotion recognition. Its aim is to recognize the facial expression stored in a database, then recognize the human emotions in terms of happy, sad, surprise, neutral, disgust, etc. The methods proposed by the authors utilizes three deep learning approaches based on convolutional neural networks (CNN) which are (AlexNet CNN, commercial Affdex CNN solution, and custom-made FER-CNN), and two conventional approaches for classification of Histogram of Oriented Gradients (HOG) features which are (Support Vector Machine (SVM) of HOG features, and Multilayer Perceptron (MLP) artificial neural network of HOG features).

The concept of face detection has become one of the interesting areas in research that aims to use application of pattern recognition and computer vision. Sharifara, Rahim, and Anisi (2014)**[3]** proposed an advanced up-to-date method for facial recognition, that aims to increase the accuracy of detecting faces, especially in a complex environment. Some of the face detection methods used were feature-based, appearance-based, knowledge based, and template matching. Also, explained the use of applying Haar-like features and neural networks for facial recognition. Each of the methods applied have increased the efficiency for face detection but as an ongoing study research area, more complex algorithms can be introduced for advance accuracy (Sharifara et al., 2014).

Viola and Jones (2001)**[4]** proposed three main object detection framework which included integral image that allows for very fast feature evaluation, second method included construction of classifier by selecting a small number of important features using AdaBoost, and final method includes combining complex classifiers in a cascade structure which dramatically increases the speed of the detector The presented approach for object detection in this paper minimizes computation time while achieving high detection accuracy.

Shojaeilangari, Yau, Nandakumar, Li, and Teoh (2015)**[5]** proposed an approach called extreme sparse learning to robustly recognize the facial emotions in real-world natural situations. It has the ability to jointly learn a dictionary set of basis and a nonlinear classification model. Sparse representation is a powerful tool used for reconstruction, representation, and compression of high-dimensional noisy data due to its ability to uncover important information about signals from the base elements or dictionary atoms (Shojaeilangari et al., 2015).

Yuan, Kang, Xu, Yang, and Ji (2018)**[6]** proposed how deep learning methods is applied to image detection to increase the accuracy of recognition. Some of the deep learning methods used were machine learning techniques that included (Differentiated depth structure, Generative depth structure, Mixed structure), and target detection algorithm based on deep learning (Traditional target detection method, Deep learning target detection algorithm based on Region Proposal). Each of the methods applied have increased the efficiency for face detection but as an ongoing study research area, more complex algorithms can be introduced for advance accuracy such as in-depth neural network integration (Yuan et al., 2018).

Valstar and Pantic (2011)**[7]**, proposed some methods for facial emotion detection that included Facial point detection, and reported use of AU recognition had an accuracy of 95.3% when tested on deliberately displayed facial expressions. Mita, Kaneko, and Hori (2005) proposed a method to utilize a distinctive feature known as joint Haar-like feature for detecting faces in images. A Haar-like feature is signified by taking a rectangular part of an image or object and splitting that rectangle into multiple parts. Branching off from Haar-like feature concept, joint Haar-like feature is proposed to ensure higher classification performance. This method of face detection ensures high detection accuracy, by using a probabilistic outline or finding a discriminant function from a large set of training examples.

CHAPTER THREE.

# 3.1 THE PROPOSED SYSTEM.

The proposed system, a Facial Expression Surveillance System for Enhanced Security in Commercial Spaces (FESSECS), is designed to harness the power of advanced computer vision and machine learning technologies to enhance security measures within banks and shops. FESSECS aims to utilize real-time facial expression analysis to identify potential security threats, detect anomalous behaviors, and enhance customer experiences.

System diagram:



## Key Components and Functionality:

1. Real-time Facial Expression Analysis:

FESSECS integrates high-resolution cameras strategically placed within the premises to capture individuals’ facial expressions. These facial images are processed in real-time using sophisticated computer vision algorithms that extract facial features and analyze expressions.

2. Emotion Recognition and Threat Detection:

Machine learning models are trained to recognize a range of emotions, including stress, fear, aggression, and suspicion. These models analyze the extracted facial features to detect deviations from baseline emotional states that might indicate potential security threats or unusual behaviors.

3. Security Alert Generation:

When the system identifies individuals displaying emotions or behaviors outside the norm, it generates security alerts for the attention of security personnel. These alerts provide real-time information about the detected anomaly, enabling swift intervention and response.

# DEVELOPMENT TOOLS.

## Software Development Tools:

1. Programming Languages:

- Python: Widely used for its extensive libraries for computer vision, machine learning, and AI.

2. Computer Vision Libraries:

- OpenCV: Provides a rich set of tools for image and video analysis, including facial recognition and emotion detection.

- Haarcascade: Offers facial feature extraction and facial landmark detection.

3. Machine Learning Framework:

- TensorFlow: Allows building and training custom machine learning models for emotion recognition.

## Hardware and Sensor Tools:

1. Cameras:

- High-resolution cameras suitable for capturing detailed facial images in various lighting conditions.

- Depth-sensing cameras for enhanced accuracy in facial feature extraction.

Development Environment and IDE:

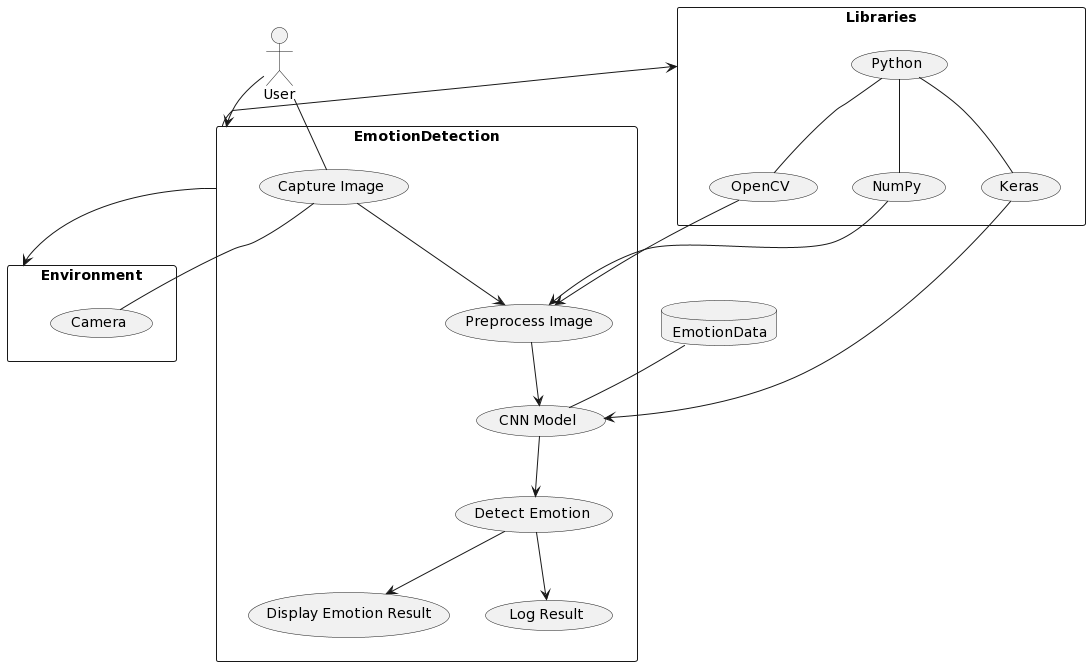
1. Integrated Development Environment (IDE):

- Jupyter for code development and debugging.

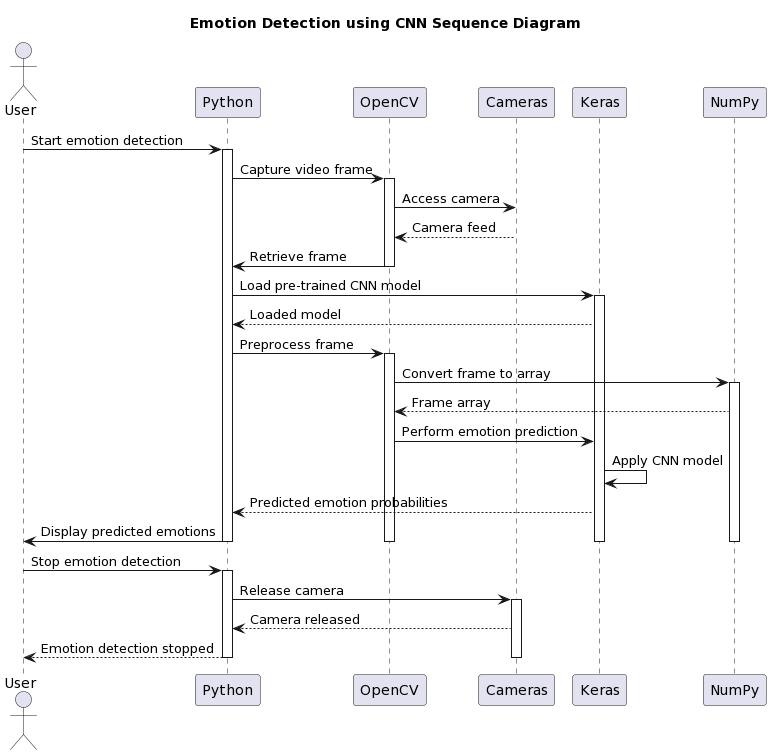
2. Virtualization:

- Anaconda for managing dependencies and isolating project environments.

Use Case Diagram:



Sequence Diagram:



CHAPTER FOUR.

# 4. IMPLEMENTATION AND TESTING.

## 4.1 IMPLEMENTATION.

## 1. Emotion data acquisition.

Numerous facial emotion datasets are available online, in this study we will be using FER 2013 which many researchers have used previously for FER tasks. The dataset consists of people with distinct facial features like beard and moustache, different ethnic backgrounds, and varied facial complexions.

## 2. Image to arrays

An image is represented by values (numbers) that correspond to the pixel intensities. The array module in NumPy (nd.array) is used to convert an image into an array and obtain the image attributes. So, we convert images with their respective attribute in pixels to a 2 dimensions and size 48 × 48 pixels

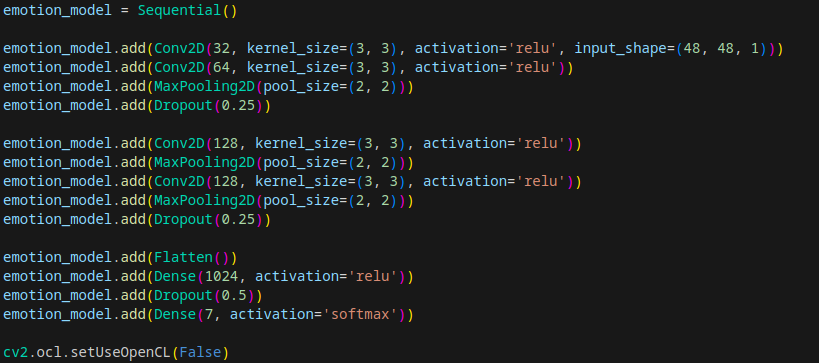
## 3. Image to landmarks

The haarcascade library is used to detect facial landmarks. This process consists of two steps, localize the face in an image and detect the facial landmarks. The frontal face detector from haarcascade is used to detect the face in an image. A rectangle on the face is obtained which is defined by the top left corner and the bottom right corner coordinates. The haarcascade shape predictor is used to extract the key facial features from an input image. An object called landmarks which has two arguments is passed. The first argument is an image in which faces will be detected and the second specifies the area where the facial landmarks will be obtained. This area is represented by the coordinates of the rectangle.

## 4. CNN architecture

ML models can be built and trained easily using a high-level Application Programming Interface (API) like Keras. In this report, a sequential CNN model is developed using Tensorflow with the Keras API since it allows a model to be built layer by layer. Tensorflow is an end-to-end open-source platform for ML. It has a flexible collection of tools, libraries and community resources to build and deploy ML applications.

CNN Model has four phases. At the end of each phase, the size of the input image is reduced. The first three phases have the same layers where each start with a convolution and ends with dropout. The first phase of the model has an input layer for an image of size 48 × 48 (height and width in pixels) and convolution is performed on this input. The number of kernels is 64 in the first phase. Then, batch normalization is performed to obtain the inputs to the next layer. Convolution and batch normalization are repeated in the following layers. In the next layer, max pooling is performed with pool size 2 × 2, so the output size is 24 × 24. Dropout is performed next at a rate of 0.35. The second phase has 128 kernels and 0.4 dropout rate. Max pooling in the second phase gives an output of size 12 × 12. The third phase has 256 kernels with 0.5 dropout rate. Max pooling in the third phase reduces the size of the output to 6 × 6. The final phase starts with a flatten layer followed by dense and output layers. Classifying the five emotions requires the data to be a one- dimensional array. The flatten layer converts the two-dimensional data into a one-dimensional array. The flattened output is fed to the dense layer which applies the softmax function. Then, batch normalization is done and the output layer gives the class probabilities.



## 5. Compiling the model

Compiling the model requires two parameters, optimizer and metrics. The optimizers used is Adam. The optimizer is used to update the weights in a DL model based on the loss. The metrics used are accuracy, categorical cross-entropy loss, precision, recall and F-score.



## 6. Training the model

To train the model, the train-test split() function is used. This function splits the dataset into training and testing sets. The training data is not used for testing. A training ratio of 0.90 means 90% of the dataset will be used for training and the remaining for testing the model. The Learning Rate (LR) is a configurable parameter used in training which determines how fast the model weights are calculated. A high LR can cause the model to converge too quickly while a small LR may lead to more accurate weights (up to convergence) but takes more computation time. The number of epochs is the number of times a dataset is passed forward and backward through the NN. The dataset is divided into batches to lower the processing time and the number of training images in a batch is called the batch size.

## 7. Real-time face detection

The facial visual information of a person is used for emotion analysis; therefore, accurate face detection in real-time with low latency is of prime importance. In this study, the haar facial cascade algorithm is adopted for the face detection module of the FESSECS. During real-time validation, suppose, in a video sequence frame ‘Sf , there exists a person ‘Pf ’where ‘f ’ is a video frame, the haar facial cascade algorithm is applied to extract the facial image ‘If ’ from the frame using the Haar facial feature-based cascade classifier. The area of interest (AOI), i.e., the face is first localized, and a four-corner bounding box is formed to crop the AOI. The cropped facial image ‘If ’ is fed into the FESSECS framework, which sends feedback after appropriate analysis.

## 8. Emotion analysis strategy

The facial emotion analysis system is triggered when a person is detected in the scope where the camera is placed, followed by the human face detection by the face detection module. Since a hostile or dangerous situation is governed by common expressions such as anger or aggression, the facial emotion analysis for such negative valence is conducted precisely as long as the face is in the frame.

The multi-threaded security module is invoked if aggressive or angry faces are captured. During multi-threading, a countdown timer is set for t = 20 s to analyze if the facial expression remains angry or aggressive for a long time depicting a hostile situation. Suppose if the angry faces are captured continuously for t = 20 s and the countdown reaches t = 0, the security personnels are alerted via a notification from the FESSECS framework. These notifications can be a continuous beep sounds from an attached speaker, along with a ‘‘Situation is hostile’’ message on the workstation/smartphone screen.

If the angry faces are not observed for a long time, in that case, the residents are not alerted, and the system loops back to analyze the expressions again. All the processes of the FESSECS framework, including face detection, expression recognition, and decision making, run parallel to each other; that is why multithreading is utilized extensively for superior performance. The notification message and the beep sound alert the security personnels to take appropriate actions in a hostile situation and notify law enforcement agencies on time.

Before the software is deployed, the countdown timer for emotion analysis (t = 20 s) can be adjusted according to the situation. The countdown timer gives the model extra time for accurate analysis. This setup results in fewer false positives and avoids any unnecessary false alarms that may cause panic.

# 4.2 TESTING.

FER2013 dataset is used to train the model, which consists of 28,709 samples of 48×48-pixel grey scale images of faces of different emotion. The proposed CNN model will extract the facial features and according to that it will classify the image to respective class, happy, sad, surprise, fear, anger, neutral and disgust. The model gives the test accuracy of 97.481193% and test loss of 3.743610% in 25 epochs. And also, the model gives a train loss of 0.429% and train accuracy of 98.766. Live image is captured from the camera and by using Haar cascade classifier it will remove the unnecessary background and will focus on the face emotion and the model will detect the emotion.

To compare the predicted value to the actual value Classification matrix is designed. Classification matrix is a very important tool to assess the performance of model. Here, in this classification matrix has five columns, which represents the emotion number, precision, recall, f1 score and support. The proposed model works really well on positive emotions. The model gives a high precision score of 98% for happy and 95% for surprise. But the model seems to be work relatively less on negative emotion as like fear and angry. The model gives a low precision score of 80% for fear and 75% for angry. But overall, the model works well and gives overall accuracy of 98%.

# 4.3 CONCLUSION.

In conclusion, the development and implementation of the Facial Expression Surveillance System for Enhanced Security in Commercial Spaces (FESSECS) represent a significant step forward in leveraging cutting-edge technologies to address the dual objectives of security enhancement and ethical considerations. This project underscores the potential of facial expression analysis to revolutionize security measures within banks and shops while ensuring that individual privacy and rights remain at the forefront.

The journey of conceptualizing, designing, and implementing FESSECS has illuminated the intricate interplay between technological innovation, ethical considerations, and practical application. By integrating real-time facial expression analysis with advanced machine learning algorithms, the system provides a proactive approach to identifying potential security threats and anomalous behaviors. Moreover, its capability to personalize customer experiences aligns with the evolving expectations of modern consumers.

The project's ethical dimensions have been diligently addressed, incorporating mechanisms to ensure transparency, informed consent, and data protection. The balance between security imperatives and individual rights underscores the project’s commitment to responsible technology deployment.

As the project concludes, it is important to recognize its contributions. FESSECS contributes not only to the realm of security technology but also to the broader discourse on ethics, privacy, and technology’s role in commercial environments. The project serves as a foundation for ongoing research and development, offering a blueprint for responsible surveillance system implementation.

While the project’s implementation journey culminates, its impact continues. FESSECS stands as a testament to the synergy between innovation, ethics, and practicality, underscoring the potential of technology to enhance security while fostering a harmonious coexistence with societal values. In an era characterized by dynamic technological advancements, FESSECS demonstrates the power of thoughtful integration to create a safer and more secure commercial landscape.

# 4.4 REFERENCE.

**[1]** Yang, M.-H., Kriegman, D. J., & Ahuja, N. (2002). Detecting faces in images: A survey. IEEE Transactions on pattern analysis and machine intelligence, 24(1), 34-58.

**[2]** Kartali, A., Roglić, M., Barjaktarović, M., Đurić-Jovičić, M., & Janković, M. M. (2018). Real-time Algorithms for Facial Emotion Recognition: A Comparison of Different Approaches. Paper presented at the 2018 14th Symposium on Neural Networks and Applications (NEUREL).

**[3]** Sharifara, A., Rahim, M. S. M., & Anisi, Y. (2014). A general review of human face detection including a study of neural networks and Haar feature-based cascade classifier in face detection. Paper presented at the 2014 International Symposium on Biometrics and Security Technologies (ISBAST).

**[4]** Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. CVPR (1), 1(511-518), 3.

**[5]** Shojaeilangari, S., Yau, W.-Y., Nandakumar, K., Li, J., & Teoh, E. K. (2015). Robust representation and recognition of facial emotions using extreme sparse learning. IEEE Transactions on Image Processing, 24(7), 2140-2152.

**[6]** Yuan, N., Kang, B. H., Xu, S., Yang, W., & Ji, R. (2018). Research on Image Target Detection and Recognition Based on Deep Learning. Paper presented at the 2018 International Conference on Information Systems and Computer Aided Education (ICISCAE).

**[7]** Valstar, M. F., & Pantic, M. (2011). Fully automatic recognition of the temporal phases of facial actions. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 42(1), 28-43.