**AIGS 1010**

**COMPUTER VISION**

**FINAL PROJECT REPORT**

**GROUP 4**

**PROJECT TITLE: SECURE ACCESS WITH FACE RECOGNITION**

**Team Members:**

**1) Ilan Goldfarb**

**2) Nehal Vinubhai Vadoliya**

**3) Ninu Basheer**

**4) Rohit Lovers**

**5) Sonjeet Kaur**

**Submission Date: March 17th, 2024**

**TABLE OF CONTENTS**

**1. Introduction**

**2. Technical Analysis**

**3. Literature Review**

**4. Technologies and Libraries Used**

* 4.1 OpenCV (CV2)
* 4.2 SIFT (Scale-Invariant Feature Transform)
* 4.3 Haar Cascade Classifier

**5. Limitations and Challenges**

**6. Visualizations**

**7. Applications**

**8. Conclusion**

**9. References**

**1. Introduction**

The evolution of biometric technologies has significantly transformed the landscape of security and authentication systems. Among these technologies, face recognition stands out due to its non-intrusiveness and the ability to accurately identify individuals. This paper delves into the development of a face recognition system that leverages the advancements in image processing and machine learning to authenticate individuals by comparing facial features extracted from images. The process is divided into training and testing phases, where the system learns from a set of images and then tests its ability to identify faces in a new set. The goal is to create a system that can accurately identify individuals and operate effectively in real-world scenarios.

**2. Objectives**

* Build a python program that will successfully extract features from inputted pictures of faces and approve access only to users whose face is in the database.
* Test the accuracy of the model by comparing the face of a person wishing to enter the system with the person for whom the accesses permitted.
* Train the model on a selected number of faces.

**3. Technical Analysis:**

In this project uses “cv2.CascadeClassifier” and “cv2.SIFT\_create()”, open-source Python libraries developed by OpenCV [1].

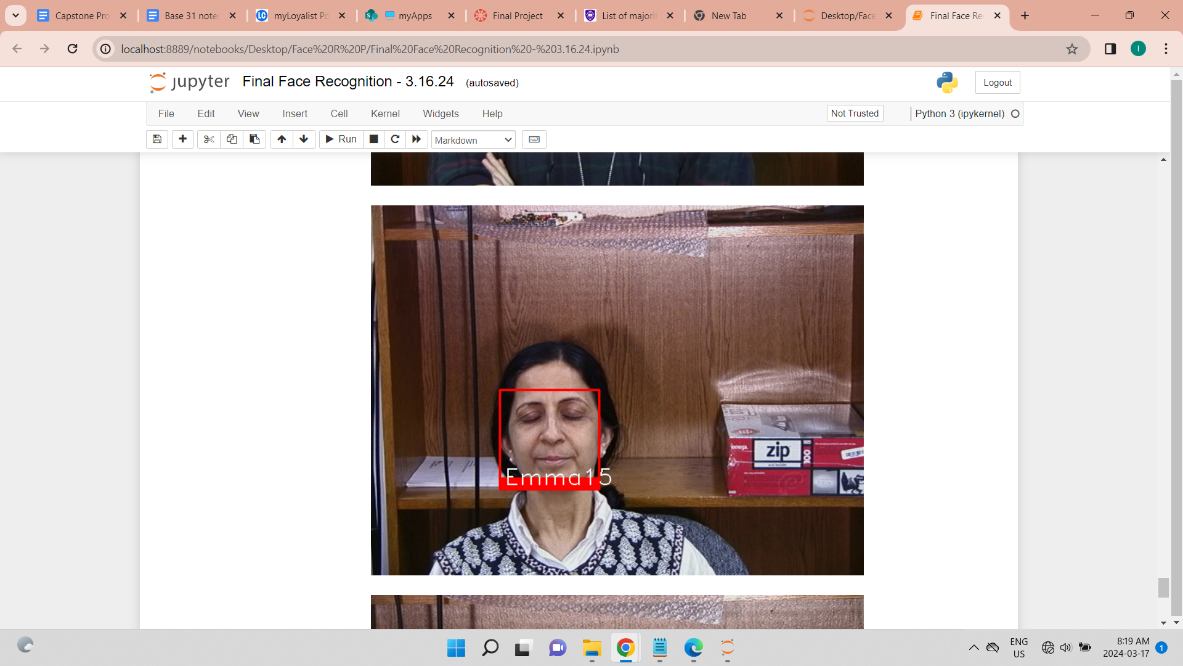
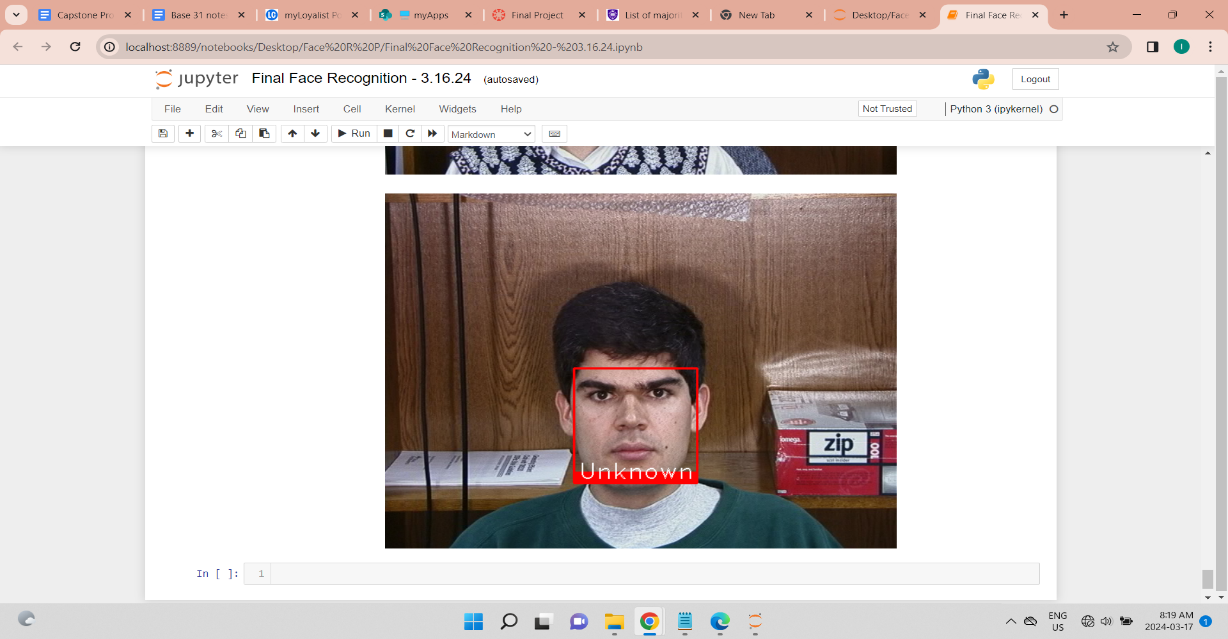
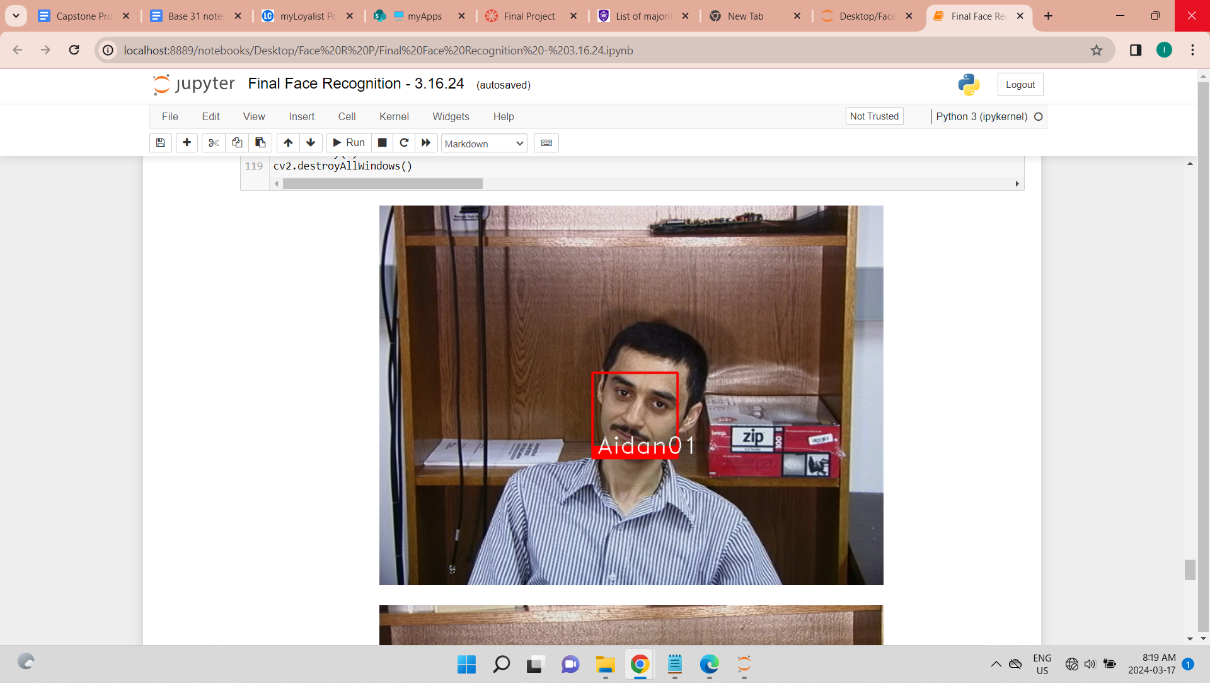
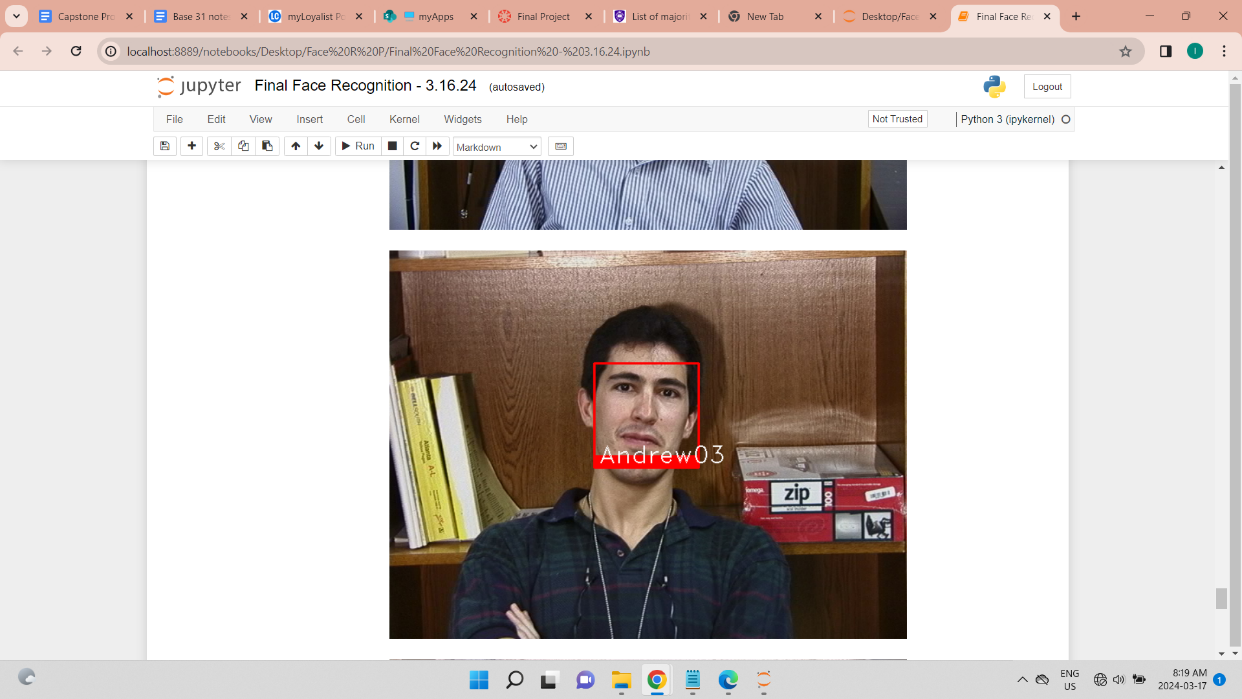
Cv2.CascadeClassifier detects the faces in the images inputted to the program, and “sift.detectAndCompute” detects the common key points between two set of pictures, picture 1 to picture 2, and then picture 2 to picture 1. This processes keep going whit a comparison of picture 1 to picture 3 and picture 3 to picture and so on. After all the relevant picture in the database have been iterated through.

Every set of faces has several common key points and by dividing both pairs to each other, adding them up and dividing by 2, we arrive at a small value, usually around 1. Mathematically it is: (x/y + y/x)/2 for every pair, and for the full set: sum((x/y + y/x)/2)/n, where n is the number of faces n the full set.

The value derived from this process will be the training value. For testing we use compare faces from two different people, and the result is less common key points, and thus a larger overall value. When the values of the testing phase are the same or lower than the training phase, this means that the person is the same for testing and training, and entry to the secure system is granted. If the testing value is larger than the training, this means that the person in testing is a different one than in training, and access is denied.

Among testing of this pars of the program, we ran into some issues suggesting that the mathematical calculation is not sufficient. The program requires a large number of pictures to get a correct result. This is properly due to the using of averages, that by nature, represent reality better as the number of samples get larger. Another issue is that Sift would on occasion classify parts of images as faces, when in fact they are not faces.



The second approach our program uses is a pre trained neural net called “face recognition”. This is a Python module that has been pretrained of faces and will detect weather a person wishing to accesses is in the database or not. This approach offers more accurate results than the first approach but is less “transparent” and comes along with the problems that using deep neural nets have. One problem can be a miss classification of a person, and because we have no access to the trained model, it will be hard to correct this type of issue.  

**4. Literature** **Review**

Image processing has gained popularity as the algorithms used became more effective and computing power grew. Approaches to Image processing vary, but the focus and interest are common. Facial Recognition is an applications of image processing technology. Below are the two different research papers from the field of image processing which uses Facial Recognition.

**4.1 Integrated Biometric Access Control System:**

The "Integrated Biometric Access Control System" project explores the amalgamation of various biometric technologies—specifically, facial recognition, fingerprint identification, and barcode detection—to create a robust and secure access control system. This literature review reflects on the significant strides made in image processing and biometric authentication, highlighting their crucial role in enhancing security measures within digital and physical spaces.

The foundation of facial recognition technology, as discussed, is heavily reliant on the efficacy of Principal Component Analysis (PCA), an insight first introduced by Turk and Pentland in 1991 [2]. This technique simplifies the complexity of facial images by reducing their dimensionality, thus retaining only the most essential features necessary for accurate identification. This method not only boosts the efficiency of facial recognition systems but also minimizes errors in identification processes. The review further mentions the integration of RFID technology with facial recognition, a hybrid approach that strengthens the security framework by requiring dual authentication, thus significantly reducing potential breaches.

Fingerprint recognition, another cornerstone of biometric authentication, has been lauded for its high accuracy and cost-effectiveness. The review acknowledges the contributions of Jordi Sapes and Francesc Solsana, who developed a low-cost fingerprint recognition system tailored for the Raspberry Pi platform. Their work exemplifies the adaptability of fingerprint biometrics in access control systems, further evidenced by its near-perfect accuracy rate. This technology's intrinsic security feature lies in the uniqueness of fingerprints, making it nearly impossible for unauthorized entities to duplicate or forge access.

Barcode identification, while not biometric in essence, plays a complementary role in the integrated system. Saurabh Kumar's implementation of barcode identification using Raspberry Pi showcases the versatility of combining traditional and biometric security measures. This method enhances the system's functionality by allowing additional actions upon user authentication, such as logging attendance or accessing personal records, thus broadening the scope of applications beyond mere access control.

It also navigates through the theoretical underpinnings of image processing methodologies critical to the development of biometric systems. It elaborates on the PCA's role in image compression and enhancement, emphasizing its importance in processing and recognizing biometric data with precision. Additionally, the review touches upon Independent Component Analysis (ICA) and neural network algorithms as potential areas for future research, suggesting these could offer more sophisticated solutions for biometric recognition by capturing higher-order relationships among pixels and improving training methodologies.

In conclusion, the "Integrated Biometric Access Control System" project underscores the pivotal role of image processing and biometric technologies in fortifying security systems. It reflects on the past achievements in the field, the current state of technology, and looks forward to future advancements that promise to enhance the reliability, efficiency, and scope of biometric access control systems. ([Paper1](https://www.researchgate.net/publication/346943788_INTEGRATED_BIOMETRIC_ACCESS_CONTROL_SYSTEM)).

**4.2 Face Recognition and Gender Detection Using SIFT Feature Extraction, LBPH, and SVM**

In the realm of computer vision and machine learning, face recognition and gender detection are pivotal areas of research, owing to their extensive applications in security, authentication systems, and beyond. The study by Alamri et al. (2022) delves into these domains, leveraging the Scale Invariant Feature Transform (SIFT) for feature extraction, combined with the Local Binary Pattern Histogram (LBPH) and Support Vector Machine (SVM) for classification, to enhance the precision of face recognition and gender detection algorithms. This review aims to encapsulate the essence of their findings, relate them to previous works, and underscore the implications and potential for future research.

The cornerstone of Alamri et al.'s methodology is the utilization of the LFW (Labelled Faces in the Wild) database to train and evaluate the efficiency of SIFT alongside SVM and LBPH classifiers in recognizing faces and detecting gender. The SIFT algorithm, renowned for its robustness against transformations and its ability to extract distinctive local features, was pivotal in generating a descriptive feature set for each image. Coupled with SVM's capacity for high-dimensional classification, the study sought to construct a reliable face recognition model. Furthermore, the incorporation of LBPH aimed to harness its computational simplicity and discriminative power, especially in face recognition scenarios. The juxtaposition of these methods aimed to ascertain the most efficacious approach for both recognition and gender detection, with a notable emphasis on LBPH for its superior performance in preliminary tests.

Notably, studies have also explored the efficacy of traditional algorithms like SIFT and SURF, emphasizing their adaptability across a spectrum of tasks. Moreover, the pursuit of gender detection through ocular images and the application of textural descriptors in mobile environments signify the expanding horizons of biometric classification research.

Alamri et al.'s experiments demonstrate the viability of integrating SIFT feature extraction with SVM and LBPH classifiers in a machine learning framework for face and gender recognition. Their results indicate a notable accuracy of 88% in face recognition using LBPH and a commendable gender detection accuracy of 91% with the same method. These findings are instrumental in showcasing LBPH's potential over SVM when applied to the LFW dataset, marking a significant contribution to the literature on biometric recognition technologies.

In conclusion, the study by Alamri et al. provides a comprehensive examination of the synergistic potential of SIFT, LBPH, and SVM in the realms of face recognition and gender detection. Their findings not only contribute to the advancement of machine learning applications in biometric recognition but also open avenues for future research to explore the intricate balance between feature extraction techniques and classification algorithms for optimized performance. The evolution of these technologies holds promise for more secure, reliable, and efficient authentication systems, pushing the boundaries of what is achievable in computer vision and machine learning disciplines. [Paper2](https://www.researchgate.net/publication/359859039_Face_Recognition_and_Gender_Detection_Using_SIFT_Feature_Extraction_LBPH_and_SVM)

**5. Technologies and Libraries Used:**

* **OpenCV (CV2):** A library of programming functions mainly aimed at real-time computer vision. In this project, OpenCV is utilized for image processing and face detection.
* **SIFT (Scale-Invarient Feature Transform****)** : SIFT is integrated within the OpenCV framework to detect and describe local features in images. It is crucial for identifying unique key points in faces that are invariant to image scale, rotation, and partially to changes in illumination.
* **Haar Cascade Classifier:** The Haar Cascade Classifier, also part of the OpenCV library, is employed for its efficient face detection capability. By utilizing pre-trained models like haarcascade\_frontalface\_default.xml, it can quickly identify faces within images
* **Matplotlib**: A plotting library for the Python programming language and its numerical mathematics extension NumPy. It provides an object-oriented API for embedding plots into applications
* **Python**: The programming language used to implement the system, known for its readability and rich ecosystem of libraries
* **NumPy** : This supports the data handling and computation needs of this project. NumPy is known for its efficient handling of large multi-dimensional arrays and matrices, providing a wide range of mathematical functions to operate on these arrays.

**5. Limitations and Challenges Involved**

* Dependency on image quality:

The system's performance heavily depends on the quality of the input images, including factors such as lighting, resolution, and the face's orientation

* Single-face Detection:

The current implementation assumes that each image contains a single face, which may not always be the case

* Variability in Facial Features:

Human faces exhibit a wide range of variability in terms of size, shape, colour, and expression. Capturing these nuances poses a significant challenge.

* Environment Conditions: The system's effectiveness can be influenced by environmental conditions, such as lighting and background.

**6. Visualizations**:

The system generates visualizations showing detected faces in images and the key points used for face recognition. These visualizations aid in understanding how the system processes and compares images.

**7. Applications:**

* **Security Systems:** For authentication in secure access systems
* **Surveillance:** In monitoring and identifying individuals in public or private spaces
* **Personal Identification:** In applications requiring user verification, like unlocking personal device

**8. Conclusion:**

The development of a face recognition system encapsulates the complexities and challenges of computer vision and pattern recognition. Despite its limitations, the system demonstrates the feasibility of using image processing and machine learning techniques for face recognition tasks. Future enhancements could focus on improving accuracy, handling multiple faces in a single image, and optimizing performance for real-time applications.

**9.References:**

1. Bradski, G., & Kaehler, A. (2000). OpenCV. Dr. Dobb’s journal of software tools, 3(2).

2. Singleton, D. EIGENFACE IMAGE PROCESSING USING LINEAR ALGEBRA.

3. Wu, J., Cui, Z., Sheng, V. S., Zhao, P., Su, D., & Gong, S. (2013). A Comparative Study of SIFT and its Variants. Measurement science review, 13(3), 122-131.

4. Yang, H., & Wang, X. A. (2016). Cascade classifier for face detection. Journal of Algorithms & Computational Technology, 10(3), 187-197.