TITLE OF PROJECT:

Biometric Student Access Control For SPU

MODULE:

SIGNAL AND IMAGE PROCESSING (NSIP73116)

Cecil Plaatjies 202000942

Ryan Isaacs 202001716

Department of Computer Sciences, Sol Plaatje University,

Kimberley South Africa

Abstract

In the following paper we explore, discuss, implement and test biometric systems. We explored two type of biometrics; Facial recognition and fingerprint recognition. The end goal was to bring a new type of idea regarding access control at Sol Plaatjie University to try an ease and expand the access control systems.

Introduction

A problem I have experienced at SPU was forgetting\ losing my student card and then not being able to have access to the buildings and facilities on campus. Access control at SPU is one dimensional, such that we can only gain access to facilities using student cards. We feel like this can be improved with a simple solution using some technologies using biometric recognition.

This paper review will help us to understand the type of work we will be doing as well as guiding us to the different methods we will encounter. We will also see problems we might encounter in the project.

This is important as it will set the foundation to the rest of our project.

Literature review:

Paper Contributions

Researchers working in the field of biometrics (face recognition) who attempts to address the issues posed by facial beautification, e.g face retouching, facial plastic surgery and facial cosmetics (Rathgeb, 2019)

This article states both the advantages and disadvantages in general and giving methods on how Sol Plaatje University can tighten the security on campus. It gives ways on how SPU can improve the campus access system by making use of biometric technique (facial, fingerprint recognition). (Tlape, 2019)

They don’t really give much information in this paper besides the fact that the paper gives us a good method on how to extract a person’s best features of fingerprint images, by using the SSO and GA method and algorithm. (Ahmed, 2020)

This paper states all the security risks that an organization can face when unauthorized persons are not using biometric method and also if those persons having access to organizations property. (Li Yang, 2019)

This article gives security and performance analysis of the proposed scheme in terms of computing, storage, communications, and power overhead. Analysis of the proposed scheme demonstrates the feasibility of devices with limited resources while maintaining secure communication between IoT devices. (AboDoma, 2021)

This paper contributes to biometric by proposing to combine multispectral biometric data processing with powerful deep learning techniques, and techniques such as convolutional and recurrent neural networks (CNN and RNN). The machine-learning techniques are being used more often in this paper, e.g used as supporting tool to give decision support for a user. (Lai, 2022)

We see that this paper describes how people transition from access their houses via traditional e.g with keys, security cards and passwords patterns to the modern style, by using, face recognition using deep learning technique are being introduced with Internet of Thing (IoT) integration to create efficient access control systems. The paper also informs as that using IoT and biometric is far better and its stress and safer. (Syafeeza, 2019)

This paper explains how facial recognition systems work and clarifies methods and goals for face recognition, face verification, and face identification. It turns out that systems that analyze and classify facial features are not part of facial recognition systems because they do not verify or predict an individual's identity. It is also explained in this article.

We also see aspects of facial recognition systems like enrollment databases, training datasets, and match threshold settings (Partnership on AI, 2020)

The paper showed the implantation of facial recognition in security systems. The algorithm that used was implemented and tested in MATLAB. Also, that the results

showed that the PCA algorithm is less accurate than that ICA in some cases. (Bazama, 2021)

The following were discussed in the article face detection and face recognition. The face detector achieved 89.6% accuracy using the Honda dataset. Also, this article proposes a biometric system for usage in an open environment with no constrains that use a modified YOLO-Face approach in conjunction with a classification scheme to improve detection accuracy while minimizing computation time. We also offer a categorization architecture that combines a CNN and supervised learning algorithm. (Suarez, n.d.)

Gaps

In this paper we see that after facial beautification are being applied to individuals, especially females, their facial appearance looks very attractive, but the negative part is that face recognition systems are finding it difficult to recognize an individual after they undergo facial beautification. (Rathgeb, 2019)

In this paper we see that SPU are making use of student/lecture cards for them to access the premises. Biometric were recommended to be used rather than those cards. They didn't address the fact as to how they will work with biometric at the access points. (Tlape, 2019)

Correct Verification Rate (CVR) was 99,334% and it indicates that the model or method used to identify a person's fingerprint it's a good model or method used. The False Acceptance Rate (FAR),(00.0) and False Rejection Rate (FRR),(0.00666) is very low in this case, it must increase or being removed (Ahmed, 2020)

Organization not using biometric, leaves them open for various attacks and security threats. (Li Yang, 2019)

We see that the system in company is open or is vulnerable for easy hacking in the paper and private information were being disclose. (AboDoma, 2021)

To perform an exhaustive hyper-parameter search by an individual are being delayed or extended by the long training process. So, we need to find a way to speed up the training process. (Lai, 2022)

The efficiency in image processing must be improved. Using a module such as Raspberry Pi 3 where the processing time for coding was long. So process the image taken and act, then the instructions executing time will take less time. (Syafeeza, 2019)

We see that the following factors influence the performance of these systems; including subjects in the photographs used in biometric systems, how the images are collected, time they are stored, processing methods they go through, and the goals for which they are used. (Partnership on AI, 2020)

It's stated in the paper that they took only 10 photos, as only 10 people are allowed in to protect the security of the system. Also, that the accuracy of the face recognition still needs improvement. (Bazama, 2021)

We see that in different practical cases, the handcrafted approaches of VJ, LBP, and HOG perform on its best, but in very complicated scenarios, their performance deteriorates or degrade. (Syafeeza, 2019)

We can use a better algorithm (RBM Algorithm) that will allow us to take in more than 10 photos and people in the exam system. The fingerprint will be added to this system as improved efficiency (Bazama, 2021)

Since the handcrafted approaches of VJ, LBP, and HOG only performs on its best in less complicated scenarios, we can use, the YOLO-Face performs better in contexts with big changes in lighting, position variations, occlusion, and other factors. It will ensure a better output as well (Suarez, n.d.)

Limitation

According to RATHGEB C. one of the biggest limitations facial recognition systems can face is alterations to the face such as makeup beautification or plastic surgery that changes a person's appearance. Facial plastic surgery is the medical alteration of one's face that aims to correct features of the face and is a permanent type of alteration. (Given this there is an easy way to work around this problem, after permanent facial alteration system will have to be retained to recognize that person). Facial cosmetics is quite the opposite, where it is a non-permanent alteration but can still change from day to day as there is many different styles of cosmetics. (Rathgeb, 2019)

The main changes that affect the accuracy of the facial recognition systems are (Rathgeb, 2019):

-Face thinning
-Reduced baggy eyelids
-Changing shape of eyebrows
-And reduced dark spots in the face

The current access control system implemented at SPU is the use of access cards. This method is effective enough to sustain the university (Tlape, 2019). Even though it is working the system is very one dimensional and can greatly improve by using multiple methods at one time. This will mean that students and staff are not limited to one way of accessing the facilities.

In a case where the student is unable to use one access method there will be an alternative. (Tlape, 2019)

New Knowledge

We can resolve this by feeding the face recognition system real time facial images of a person before and after the undergo facial beautification. Equate these two images and then they system should be able to recognize a person. In the case of facial cosmetics, females can just limit the amount of make-up they put on their faces for the system to recognize them. (Rathgeb, 2019)

SPU can have both options (finger and facial recognition) at all access points, so students and lectures can just choose which biometric option they will use to access the campus. (Tlape, 2019)

Since CVR has 99,334% and that it's a good model to correctly identify a person's fingerprint, we can cancel/remove/eliminate FAR and FRR since it does have a significant impact on a individual's fingerprint recognition. (Ahmed, 2020)

We would suggest for any organization to make use of biometric. (Li Yang, 2019)

One of the solutions we can come up with is the fact the bluetooth must be of to avoid being hack (Bluetooth links all devices). (AboDoma, 2021)

A way to save time when performing hyper parameter tuning on large data sets is to pre-augment your data set, when building the binaries instead of using on the fly augmentation. (Lai, 2022)

We can maybe use a module different than Raspberry Pi 3, maybe Banana Pi M5, since it's a better module. The processing time is better, hence its time efficient. (Syafeeza, 2019)

We can simply change or remove some factors like the way the images are collected and the time the images are stored to ensure that it doesn't has an impact on the processing of the image. (Bazama, 2021)

We can use a better algorithm (RBM Algorithm) that will allow us to take in more than 10 photos and people in the exam system. The fingerprint will be added to this system to create a multi-dimensional system (Olszewska, 2016)

Since the handcrafted approaches of VJ, LBP, and HOG only performs on its best in less complicated scenarios, we can use, the YOLO-Face performs better in contexts with big changes in lighting, position variations, occlusion, and other factors. It will ensure a better output as well (Suarez, n.d.)

Proposed Methodology

Deep Neural networks (Rathgeb, 2019)

Genetic Algorithm (Ahmed, 2020) Steps:

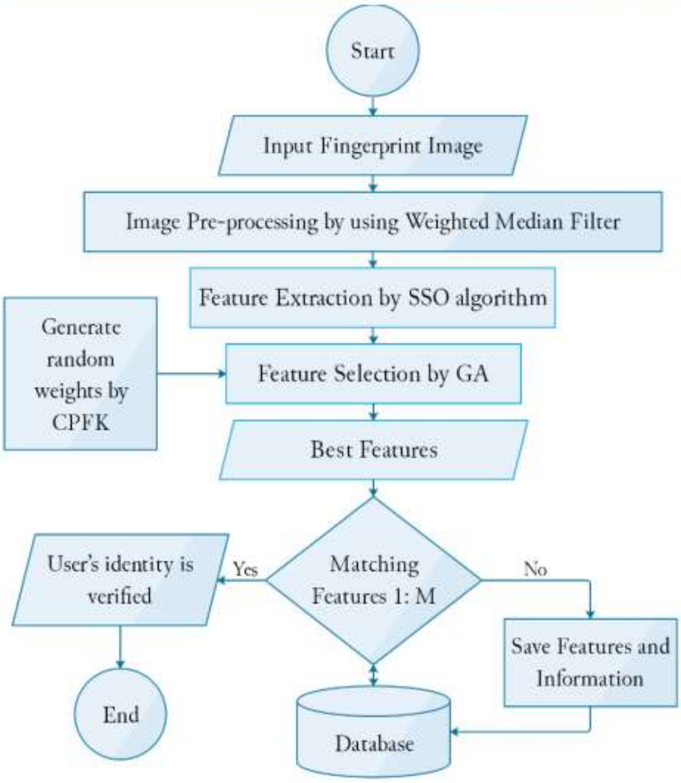

Start
Input Fingerprint Image
Image Pre-processing by using Weighted Median Filter
Feature Extraction by SSO algorithm
Generate random weights by CPFK
Feature Selection by GA
Best Features
User's identity is verified
Yes
Matching Features 1: M
No
Save Features and Information
End
Database

Fig. 1. Flowchart of the proposed model.

Enrolment stage – this is the stage where the data/images are collected and stored in the database

Image Pre-processing: Using weighted median

Feature extraction: Using algorithm features are extracted from the image and then the best feature are selected for the next step

Matching process – this is the process when the algorithm used the best features extracted from the two images to then compare and match two images.

Figure 1: (Ahmed, 2020)

Proposed methodology.

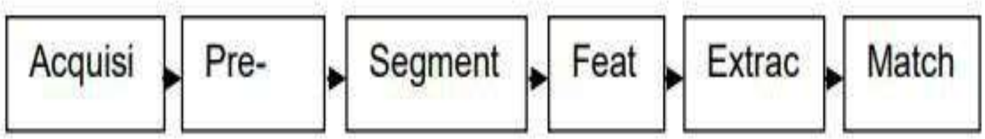


Figure 2 : (Tlape, 2019)

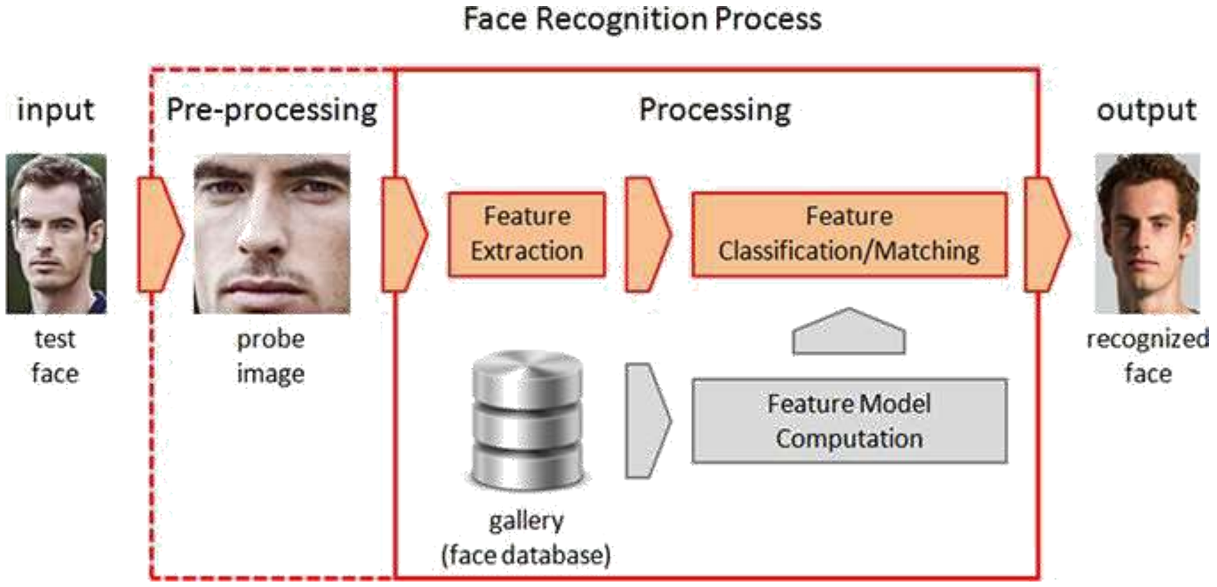


Figure 3: (Olszewska, 2016)

The methodology we intend to use is a deep learning method that makes use of the structure mentioned above. In the first step we will acquire images of a person to use as training in our layers for the CNN. The images will then be pre-processed making them clear and removing any degradation in the images.

Next the images will be segmented, which will break them down and take out only the information we will need in the images to further use in our system. After which we will write an algorithm that will extract the feature, we will use to then match with the features of our images collect in the data base. The final step will be to match an image take in real time with an image that is stored in the database based on the features extracted.

3. The Implemented method and analysis

-Clearly specify the methodology and its working principles in detail.

3.1 The following is an explanation on the method we used for biometric system named facial recognition:

We ended up using the Holistic Approach for our facial recognition system.

Holistic Approach

This approach is when we use the entire features of the face as an input, features like the nose, mouth, eyes (iris) and ears as well. To perform face identification, holistic face recognition makes use of global data, features, or information from faces. These features can be extracted through the pixel information of the image.

Different techniques can be seen as holistic approaches such as principle component analysis (PCA), Independent component Analysis (ICA), Linear Discriminate Analysis (LDA) and the Noise Model. In this project we implemented the holistic approach using principle component analysis.

The principal component analysis (PCA) is an algorithms in biometrics that is a statistical method which uses orthogonal transformation to change observations of correlated variables to values of linearly uncorrelated variables. PCA is also a tool that can reduce multidimensional data to lower dimensions without losing most of the information.

A full-face recognition system is made up of different operations. Each action or operation is important and contributes to the system's main purpose, which is to effectively detect a face.

One of the setbacks of this approach is that it cannot handle images that are small.

The main working principles in face recognition are listed as follows:

- Face detection
- Face tracking
- Face verification
- Face recognition

Working principles of facial recognition explained:

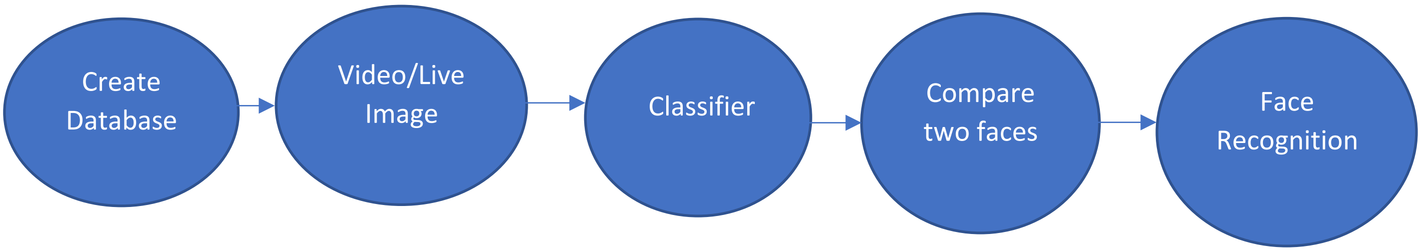
Face detection is the starting process of facial recognition. Face detection is an Artificial intelligence computer technology that uses computer vision to identify the faces of people in videos, images and in our case real time video feeds. Detection is the foundation to facial recognition because without being able to detect a face, there is no way to authenticate it.

The next step is to be able to **track the identified facial area**. This process further adds to face detection by identifying the location of the face in a particular frame at a particular time. This allows the facial area to be highlighted or segmented continuously throughout a video or live feed.

Step 3, **face verification** is when you are now comparing the highlighted facial area with some base image sorted in a database and conclude whether these faces match one another.

Running all these processes together then forms the final process being **face recognition** as you can find the location of a face, track the face, and finally identify who the face really belongs to.

Below is the flow diagram:



3.2 The following is an explanation on the method we used for biometric system named fingerprint recognition:

Methodology for fingerprint recognition - K nearest neighbour

K nearest neighbour also known as KNN, is a supervised machine learning algorithm that is easy to understand, since it uses labelled data, and it's also easy implemented for classification problems. Hence, we decided to use this method in our fingerprint recognition system. Also, KNN is commonly used, because of its low-cost and high accuracy

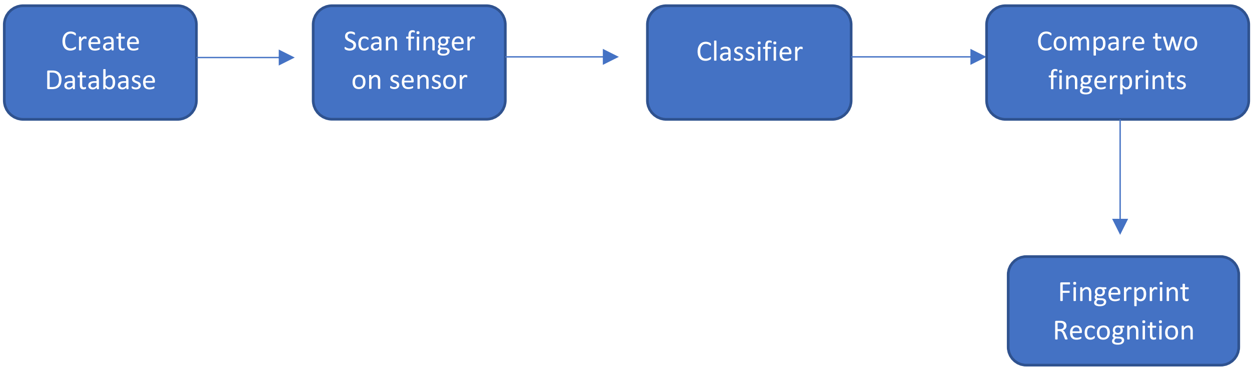
The KNN algorithm is a method for classifying objects using on closest example in the training phase. In the case of our fingerprint recognition system, we give one input image (sample image), then compute as many key points and descriptors on that image as we can.

We used the Sokoto Coventry Fingerprint Dataset (SOCOFing) for our fingerprint model. 6,000 fingerprint photos from 600 African participants make up the collection, which also includes synthetically altered copies with three distinct levels of alteration for obliteration, central rotation, and z-cut. Unique attributes include labels for gender, hand, and finger names.

The main working principles in fingerprint recognition are listed as follows:

The KNN system will then take images one at a time from the database, compute its key points and descriptors. Thereafter it will compare and match the key points from the sample image and the database image, by finding the euclidean distance between them in each image. And chooses an image that has the most matching key points and descriptors. Or the image that's key points have the smallest distance from the key points in the sample image.

Below is the flow diagram:

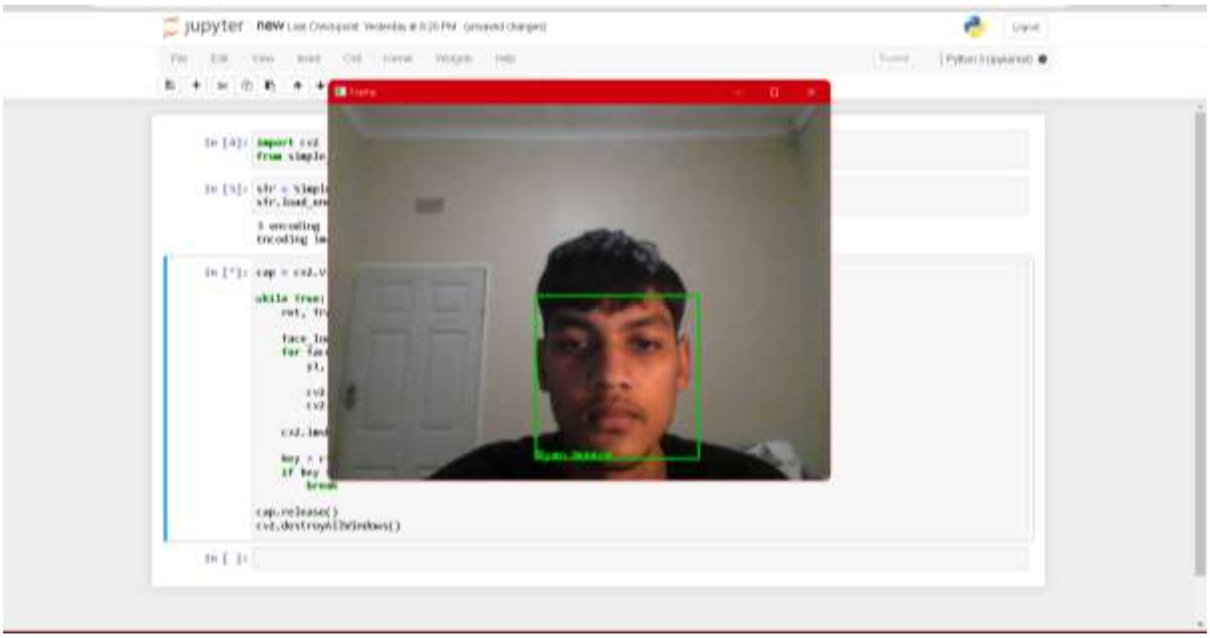


4. Experiment, results, and discussion

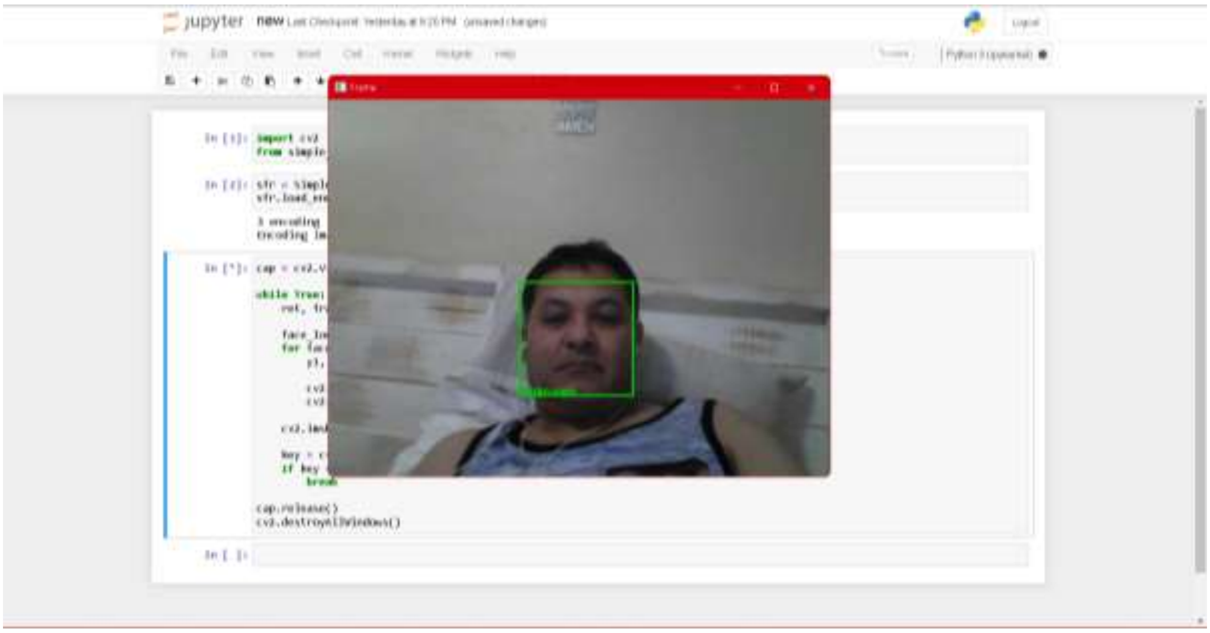
4.1 Facial Recognition

Face recognition code output

The output shows that the code can detect the face of Ryan Isaacs, who is in the database but when someone who is not recognized because they are not registered it will print unknown.


jupyter new Last Checkpoint: Yesterday at 8:20 PM (unsaved changes)
Logout
File Edit View Insert Cell Kernel Widgets Help
Trusted
Python 3 (ipykernel)
Frame

```
In [4]: import cv2
        from simple
In [5]: sfr = Simple
        sfr.load_en
        3 encoding
        Encoding im
In [*]: cap = cv2.V

        while True:
            ret, fr

            face_lo
            for fac
                y1,

                cv2
                cv2

            cv2.ims

            key = c
            if key
                break

        cap.release()
        cv2.destroyAllWindows()
In [ ]:
```


jupyter new Last Checkpoint: Yesterday at 8:20 PM (unsaved changes)
Logout
File Edit View Insert Cell Kernel Widgets Help
Trusted
Python 3 (ipykernel)
Frame

```
In [1]: import cv2
        from simple
In [2]: sfr = Simple
        sfr.load_en
        3 encoding
        Encoding im
In [*]: cap = cv2.V

        while True:
            ret, fr

            face_lo
            for fac
                y1,

                cv2
                cv2

            cv2.ims

            key = c
            if key
                break

        cap.release()
        cv2.destroyAllWindows()
In [ ]:
```

-**<u>Description of experiment.</u>**

So, to begin with we first going to create a database with all the images of the individuals we want our model or system to correctly recognize. In this case, we have images stored in our data with heading “Ryan”, “Cecil” and “Gary”.

We than write line of code that allows us to take a real time picture of a person and then runs through the entire database. It compares images in database with the real time picture. If the features of the person in the live feed match the features in the database image the model will display a live video with their face highlighted and their name displayed. If stored image and real time image doesn't match, the model will simply display "unknown".

-**What are the different experimental parameters that may be considered during the experiment, should be clearly written, and explained why?**

-Distance between individuals face and camera.
The system recognizing a person more accurately depends on how far or near a person's face is from the camera. For instance, if an individual is close and directly in-front of the camera, camera will easily recognize the face. The opposite is also true, it will be difficult for system to recognize a person if they are a bit further from the camera. (Uliyan, 2020)

-Features
Facial recognition systems rely heavily on features of a face to classify a person but since we are using a Holistic approach, we will use all details of an individuals faces as the features to recognise the person. (Bazama, 2021)

-Beautification or facial cosmetics
It is important for individuals not to put on a lot of make-up, especially females. Make-up can either upgrade or hide facial features. The system will easily recognize a persons face with light make-up and will find it a bit challenging or difficult to recognize a person with heavy make-up on their face. (Bazama, 2021)

-Testing environment (Lightning, time of the day)
Testing and real time implementation is not the same, hence the system might be able to correctly identify a person during testing but might be unable to identify a person in real time application. Lightning and time (what time it is in the day) must also be considered when a system tries to recognize an individual. During the day, lightning is better and the accuracy of system recognizing a person is higher comparing to night times where lightning is not enough, and recognition accuracy is low.

-A person's facial expression and wearing masks or not
It will be much easier for the system or model to identify a person when he/she isn't wearing a much, because all features will be visible to the camera when performing the process, compared to when a person wearing a mask and hiding most facial fractures.

Facial expressions depend on an individual’s current emotion. Whenever a person makes any other facial expression than the normal facial expression, system will also find it difficult to recognize or identify a person, because the facial features are being reshape and some features are not even properly displayed. These are all factors to be considered when performing the experiment.

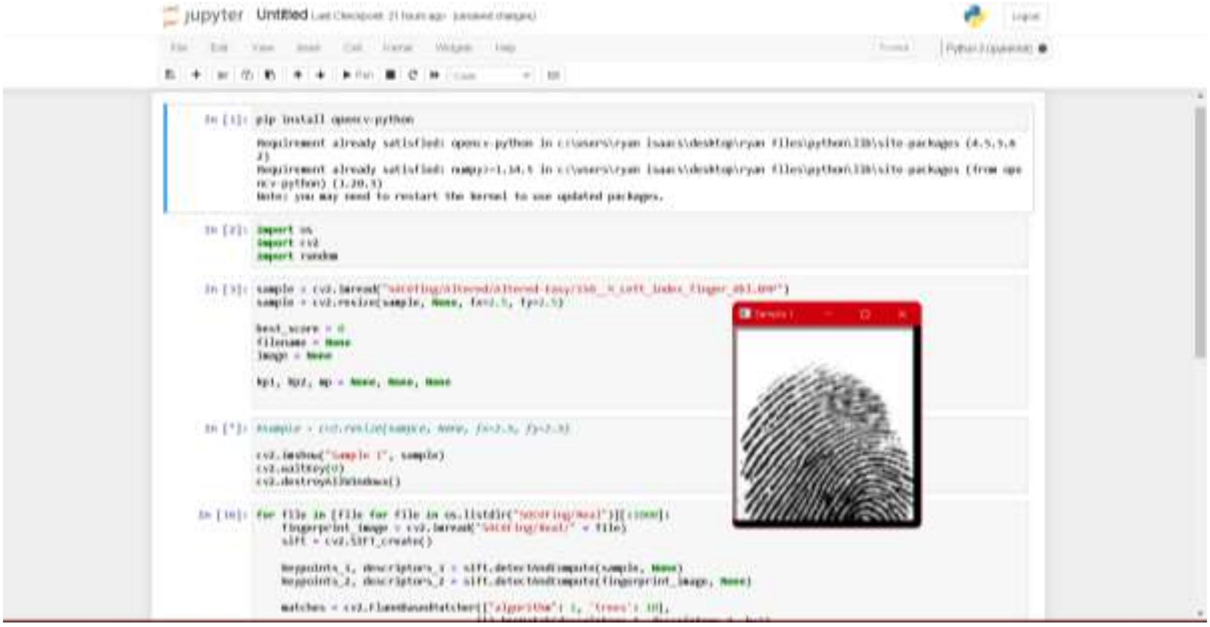
Result analysis Compared

The holistic approach is a good middle ground between the 3 approaches (hybrid, feature based and holistic approaches). The Holistic approach is much better than the feature-based approach because it considers all the details of the persons face in the image and not just basic features like eyes, nose, mouth. Even though the hybrid method produces better results, the holistic method is easier to implement and understand, compared to the hybrid approach, which will take longer to run and implement.

4.2 Fingerprint recognition

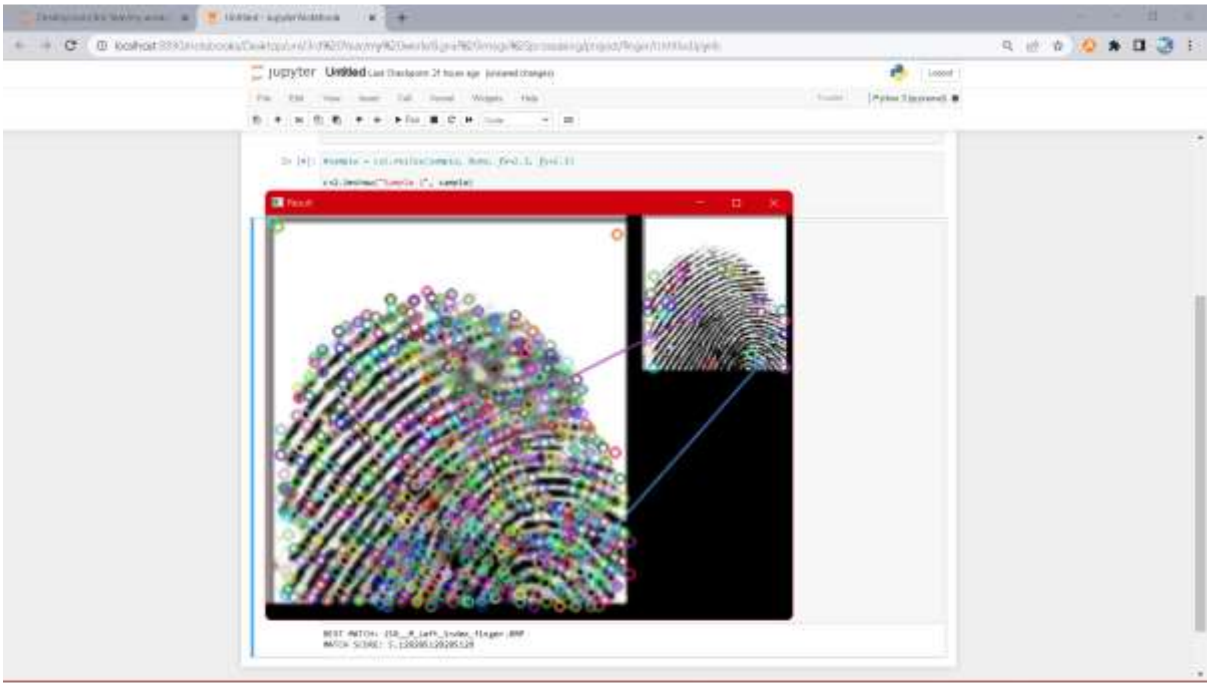
Fingerprint Matching output

The next screen shot shows the output of the sample image being used in the test.



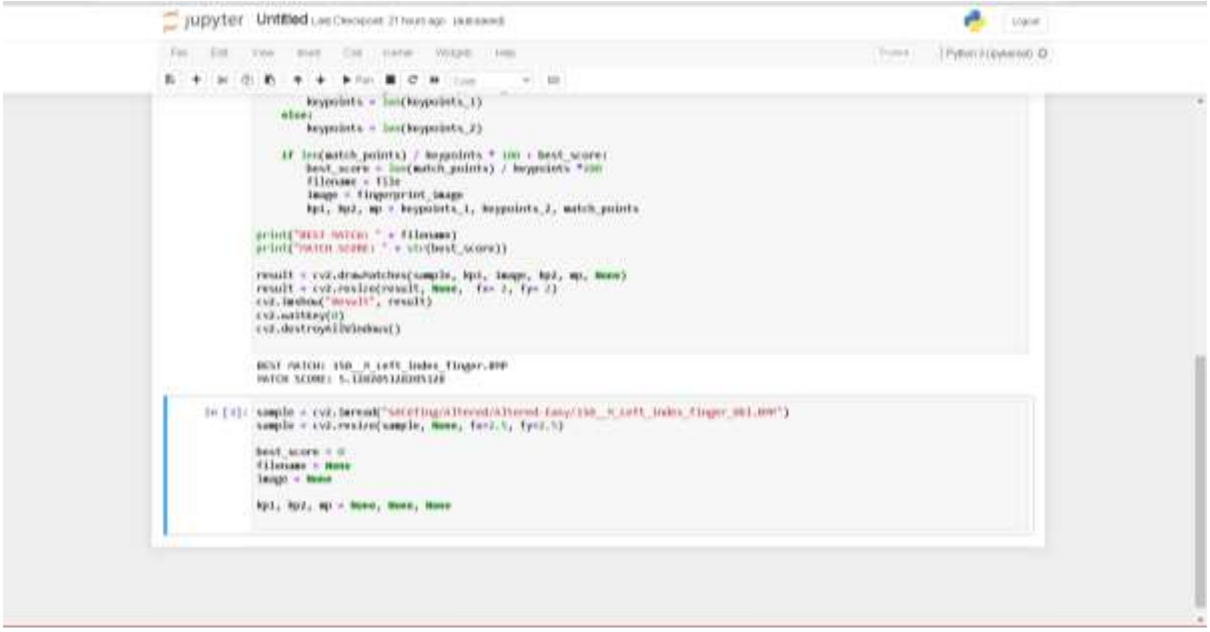
```
In [1]: pip install opencv-python
        Requirement already satisfied: opencv-python in c:\users\ryan isaacs\desktop\ryan files\python\lib\site-packages (4.5.5.6
        2)
        Requirement already satisfied: numpy>=1.14.5 in c:\users\ryan isaacs\desktop\ryan files\python\lib\site-packages (from ope
        ncv-python) (1.20.3)
        Note: you may need to restart the kernel to use updated packages.

In [2]: import os
        import cv2
        import random

In [3]: sample = cv2.imread("SOCOFing/Altered/Altered-Easy/150__M_Left_index_finger_Obl.BMP")
        sample = cv2.resize(sample, None, fx=2.5, fy=2.5)

        best_score = 0
        filename = None
        image = None

        kp1, kp2, mp = None, None, None

In [*]: #sample = cv2.resize(sample, None, fx=2.5, fy=2.5)

        cv2.imshow("Sample 1", sample)
        cv2.waitKey(0)
        cv2.destroyAllWindows()

In [10]: for file in [file for file in os.listdir("SOCOFing/Real")][:1000]:
             fingerprint_image = cv2.imread("SOCOFing/Real/" + file)
             sift = cv2.SIFT_create()

             keypoints_1, descriptors_1 = sift.detectAndCompute(sample, None)
             keypoints_2, descriptors_2 = sift.detectAndCompute(fingerprint_image, None)

             matches = cv2.FlannBasedMatcher({"algorithm": 1, "trees": 10},
```

Now the next output shows us all the key points and descriptors on the sample image and the image from the database and how they are matched. It also shows the name of the matched fingerprint and the score percentage of how much the fingerprints match



```
In [*]: #sample = cv2.resize(sample, None, fx=2.5, fy=2.5)
        cv2.imshow("Sample 1", sample)
```

```
BEST MATCH: 150__M_Left_index_finger.BMP
MATCH SCORE: 5.128205128205128
```



```
            keypoints = len(keypoints_1)
        else:
            keypoints = len(keypoints_2)

        if len(match_points) / keypoints * 100 > best_score:
            best_score = len(match_points) / keypoints *100
            filename = file
            image = fingerprint_image
            kp1, kp2, mp = keypoints_1, keypoints_2, match_points

print("BEST MATCH: " + filename)
print("MATCH SCORE: " + str(best_score))

result = cv2.drawMatches(sample, kp1, image, kp2, mp, None)
result = cv2.resize(result, None,  fx= 2, fy= 2)
cv2.imshow("Result", result)
cv2.waitKey(0)
cv2.destroyAllWindows()
```

```
BEST MATCH: 150__M_Left_index_finger.BMP
MATCH SCORE: 5.128205128205128
```

```
In [1]: sample = cv2.imread("SOCOFing/Altered/Altered-Easy/150__M_Left_index_finger_Obl.BMP")
        sample = cv2.resize(sample, None, fx=2.5, fy=2.5)

        best_score = 0
        filename = None
        image = None

        kp1, kp2, mp = None, None, None
```

The code was able to correctly identify the real image from the sample given.

Experiment, results and discussion

Fingerprint recognition groups and classifies prints based on is characteristics, this means that the main parameters used by fingerprint recognition models are the ridges and curve patterns in someone's fingerprint. The shape and build of an individual's finger can also play a big role in some results. (Uliyan, 2020)

Even though fingerprints are unique, two fingerprints recorded after each other can differ because of the roughness of the skin, the way the finger is applied to the scanner. A scan can also be inaccurate because of water present on a finger. Also, a person's finger being clean or not plays a role

The KNN model is much simpler and easy to understand and implement compared to CNNs and deep learning models. The basic parameters taken by KNNs are the number of k neighbours and the distance algorithm. (Ahmed, 2020)

One big disadvantage of KNN models over different algorithms is the real time computation. CNNs/deep learning generally take much less time to train and compute results. But since the sample size is relatively small for this project it.

Conclusion

Our research consisted of 4 steps in which we proposed our project to create a biometric access control system for SPU. We then conducted some background research in the form of a literature review to broaden and gain some knowledge on the concept of biometrics. From the research we did we the chose our preferred methodology and models that we would implement in our project. We chose to do a Holistic feature approach to in our facial recognition and a KNN for the fingerprint recognition (Uliyan, 2020)

When comparing our research to previous work, we saw that not many articles /papers had work implementing both face and fingerprint recognition together. They rather focused on one topic or the other. We have only seen one published paper regarding SPUs access control system. This is the main reasons our paper can be unique. (Tlape, 2019)

If SPU was to adopt the system, then the implications that could follow would be that student cards might be phased out, it could bring about more vandalism in the university (hardware will be costly to replace in this case), the varsity would have pay Ryan and Cecil lots of money, also many would say privacy is violated with such systems. Some positive implications can be that it is very safe due to the unique nature of biometrics, using biometrics is also very easy and quick.

Matching scores for the fingerprint recognition was quite low although it got the prediction correct this still show that the system need to be optimized. Hence in future work we can work on creating a much more accurate system and add more features, like maybe voice recognition or hand recognition. Basically, creating many ways of authenticating yourself to the university.

Complete References

1. AboDoma, N., Shaaban, E. and Mostafa, A., 2021. Adaptive time-bound access control for internet of things in fog computing architecture. *International Journal of Computers and Applications*, pp.1-12.

2. Ahmed, B.T. and Abdulhameed, O.Y., 2020. Fingerprint recognition based on shark smell optimization and genetic algorithm. *International Journal of Advances in Intelligent Informatics*, *6*(2), pp.123-134.

3. Bazama, A., Mansur, F. and Alsharef, N., 2021. Security System by Face Recognition. *AlQalam Journal of Medical and Applied Sciences*, *4*(2), pp.58-67.

4. Lai, K. (2022). Biometric-Enabled Decision Support Platform with Risk Assessment (Unpublished
doctoral thesis). University of Calgary, Calgary, AB.)
http://hdl.handle.net/1880/114302
doctoral thesis

5. Yang, L., Yuan, X., He, W., Ellis, J. and Land, J., 2019, February. Cybersecurity education with pogil: Experiences with access control instruction. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 6, No. 2, pp. 14-14).

6. Olszewska, J.I., 2016. Automated face recognition: Challenges and solutions. *Pattern Recognition-Analysis and Applications*, pp.59-79.

7. Leslie, D., 2020. Understanding bias in facial recognition technologies. *arXiv preprint arXiv:2010.07023*.

8. Rathgeb, C., Dantcheva, A. and Busch, C., 2019. Impact and detection of facial beautification in face recognition: An overview. *IEEE Access*, *7*, pp.152667-152678.

9. Sanchez-Moreno, A.S., Olivares-Mercado, J., Hernandez-Suarez, A., Toscano-Medina, K., Sanchez-Perez, G. and Benitez-Garcia, G., 2021. Efficient face recognition system for operating in unconstrained environments. *Journal of Imaging*, *7*(9), p.161.

10. Radzi, S.A., Alif, M.M.F., Athirah, Y.N., Jaafar, A.S., Norihan, A.H. and Saleha, M.S., 2020. IoT based facial recognition door access control home security system using raspberry pi. *International Journal of Power Electronics and Drive Systems*, *11*(1), p.417.

11. Tlape, O.P.L., 2019. *Investigating the effectiveness of the access control system at Sol Plaatje University, in Kimberley, Northern Cape Province* (Doctoral dissertation, North-West University (South Africa)).

12. Dai, P., Yang, Y., Wang, M. and Yan, R., 2019. Combination of DNN and improved KNN for indoor location fingerprinting. *Wireless Communications and Mobile Computing*, *2019*.

13. Yuan, Z., Zha, X. and Zhang, X., 2020. Adaptive multi-type fingerprint indoor positioning and localization method based on multi-task learning and weight coefficients K-nearest neighbor. *Sensors*, *20*(18), p.5416.

14. Uliyan, D.M., Sadeghi, S. and Jalab, H.A., 2020. Anti-spoofing method for fingerprint recognition using patch based deep learning machine. *Engineering Science and Technology, an International Journal*, *23*(2), pp.264-273.