A Major Project Report on

**Convolutional Neural Network Approach for Bimodal (Face and Fingerprint) Biometric Identification System**

Submitted in partial fulfilment of the requirements for the award of the degree of

**Bachelor of Engineering**

in

**Department of Computer Engineering**

by

**Aditi Sangle         (19102023)**

**Vedang Gore        (19102065)**

**Zeal Punamiya     (19102031)**

**Soumyojyoti Dutta (19102014)**

Under the Guidance of

**HOD. Sachin Malave**

****

**Department of Computer Engineering**

A. P. Shah Institute of Technology

G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615

UNIVERSITY OF MUMBAI



A. P. SHAH INSTITUTE OF TECHNOLOGY, THANE

CERTIFICATE

This is to certify that the project entitled “Convolutional Neural Network Approach for Bimodal Biometric Identification System” is a bonafide work of **“Soumyojyoti Dutta ” (19102014), “Vedang Gore ” (19102065), “Aditi Sangle ” (19102023), “Zeal Punamiya ” (19102031)** submitted to the University of Mumbai in partial fulfilment of the requirement for the award of the degree of **Bachelor of Engineering** in **Computer Engineering**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Guide Project Coordinator

Prof. Rushikesh Nikam Prof. Rushikesh Nikam

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Head of Department Principal

Prof. Sachin Malave Dr. Uttam Kolekar

Date:

 A. P. SHAH INSTITUTE OF TECHNOLOGY, THANE

**Project Report Approval for B.E.**

This project report for Sem-VII entitled ***Convolutional Neural Network Approach for Bimodal Biometric Identification System*** by ***Soumyojyoti Dutta, Vedang Gore, Aditi Sangle and Zeal Punamiya*** is approved for the degree of ***Bachelor of Engineering*** in ***Computer Engineering***, ***2022-23***.

Examiner Name Signature

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:

Place:

**Declaration**

We declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Soumyojyoti Dutta 19102014)

(Vedang Gore 19102065)

(Aditi Sangle 19102023)

(Zeal Punamiya 20202031)

Date:

**Abstract**

Sometimes the process of machine learning is found to be difficult for analysing and computing the desired result. This generally happens when the dataset is relatively small. Therefore, we have considered taking images for faces as well as fingerprints. This is keenly effective security wise and training wise too. In this paper we focus on working on the learning ability of the Siamese neural network which is one of the most famous networks among the other convolutional networks. In this study, we investigate a technique for training Siamese neural networks, which use a special structure to prioritize input similarity. When the training is done, the model then has the ability to extend its prediction qualities not only to new classes, but also to unknown distribution sets as well. The base being a convolutional architecture, we are therefore able to get a much higher and stronger results in comparison to other deep neural networks. The purpose of this paper is affected by the inefficient accuracy provided when only one biometric system is used. For example, in the case of twins the face might be considered as same by the model; this would be a huge breach in the security of the whole state. In order to rectify it we take in face as well as fingerprint images which, for a twins case which works perfectly with high accuracy.

**CONTENTS**

1. Introduction 1
2. Literature Survey 3
3. Limitation of Existing System 7
4. Problem Statement, Objectives and Scope 8

4.1 Problem Statement 8

4.2 Objectives 9

4.3 Scope 9

1. Proposed System 10

5.1 Proposed System Overview 10

5.2 Design details 15

5.3 Methodology 19

1. Experimental Setup 20
2. Project Plan 23
3. Expected Outcome 24

References 23

**LIST OF FIGURES**

5.1.1 Architecture Diagram of the model 11

5.1.2 Data Flow Diagram (level 0) 12

5.1.3 Data Flow Diagram (level 1) 13

5.1.4 Sequence diagram………………………………………………………………………..14

5.2.1 labelled faces in the wild dataset sample image 15

5.2.2 Own biometric dataset sample image 1…………………………………………………..16

5.2.3 Own biometric dataset sample image 2………………………………………………….16

5.2.4 Own biometric dataset sample image 3…………………………………………………..16

5.2.5 Own biometric dataset sample image 4………………………………………………….16

5.2.6 Own biometric dataset sample image 5………………………………………………….17

5.2.7 Implementation Output 1………………………………………………………………..17

5.2.8 Implementation Output 2…………………………………………………………………18

5.2.9 Implementation Output 3………………………………………………………………….18

7.1 Gantt Chart…………………………………………………………………………………..23

**LIST OF TABLES**

2.1 Literature review Table 5

6.1.1 Hardware and software reduired……………………………………………………………….22

**CHAPTER 1**

**Introduction**

Devices that use biometric identification rely on physical traits such a fingerprint, face patterns, iris or retinal patterns to confirm a user's identity. Network logon is just one application where biometric authentication is gaining popularity. For the device to compare a fresh sample provided during the logon process to a biometric template or identifier (a sample known to be from the authorized user), it is necessary to store the information in a database. The two most often used techniques for biometric authentication are face recognition and fingerprint recognition. There are some locations where a higher level of protection is necessary that can be equipped with a face recognition and fingerprint recognition system. When you offer a physical aspect for authentication, biometric authentication is carried out by comparing it to a copy that has been stored, biometric authentication is carried out by comparing it to a copy that has been stored.

Fingerprint authentication is a type of biometric authentication that instantly verifies a user's identification by comparing their fingerprint to a template that has been stored. Due to the fact that each person has a distinct fingerprint, fingerprint scans are an inherent characteristic or "something you are," making them impossible to predict and challenging to change or falsify. By analyzing and comparing the dermal ridges on a person's fingers, fingerprint recognition enables verification or identification of that person. One of the earliest methods for automatically recognising individuals was fingerprint recognition, which is still one of the most widely used and reliable biometric methods today. To ascertain whether the reported identity of the person is accurate, it performs a one-to-one comparison. The submitted claim of identification is either rejected or accepted by a verification system.

Face recognition is a biometric identification technique that relies on body measurements—in this case, the face and head—to confirm a person's identity using their facial biometric pattern and data. The technique uses a collection of specific biometric information about each person's face and expression to identify, confirm, and/or authenticate them. Finding several instances of the same face in a database of training photos from an input image is the goal of face recognition. Face recognition is one of the areas of pattern recognition and computer vision study because it has so many real-world applications in the fields of biometrics, information security, access control, law enforcement, smart cards, and surveillance.

Multimodal biometric systems boost performance and resilience against imposters' attacks and environmental changes in order to get beyond the limitations associated with systems based on a single modality of biometric data. This system falls within the categories of hybrid, multi-instance, multi-sensor, multi-algorithm, and multi-modal systems. The system for multi-biometric recognition incorporates data from many biometric sources. The key benefit of a multimodal system over a standard single biometric is that it makes recognition more precise and safe. The remaining portion of the paper is divided as follows: A literature review is a brief summary of related studies. Our suggested algorithm's supporting procedures are referred to as the proposed system. Conclusion brings the proposed work to a close while Experimental results and discussion clarify the experimental results

**CHAPTER 2**

**Literature Survey**

There are many ways to implement face and fingerprint recognition. After discussing about several ways, we have chosen the Siamese Neural network. Many studies have been done on these biometric systems. According to Cherrat et al., 2017, The biometrics modalities are often unique, measurable or automatically validated or permanent. According to Borra, Reddy & Reddy, 2018, Fingerprint have become an essential biometric trait due to its uniqueness and invariant to every individual. This biometric modality is more used and more acceptable by users as the acquiring device is comparatively small. Moreover, the recognition accuracy is relatively much higher than the others biometric recognition system based on the retina, ear shape, iris, etc. Face recognition is a biometric recognition technology based on facial feature (human ofcourse) information (feature vectors) for identification or verification.

According to Mane & Shah, 2019, human and computer performance on facial identification is a research topic with both scientific research value and widely application prospects. The bimodal biometric recognition system combines any two biometric recognition system. The main advantage of multimodal system against traditional single biometric is the recognition process  we achieve is more secure and accurate (Unar, Seng & Abbasi, 2014). The advantage of using face and fingerprint is these things are more natural for recognizing and their deployment cost is relatively low.

Ross & Jain (2003) presented information fusion in a multimodal system at various levels, the performance of different normalization techniques and fusion rules in the context of a multimodal biometric system based on the face, fingerprint and hand -geometry features of a user. They also observed that multimodal systems utilizing user-specific weights perform better compared to systems that assign the same set of weights to the multiple biometric traits of all users. Yang & Zhang (2012) made experimental systems with a fusion of fingerprint and finger vein. These biometric features were extracted using a unified Gabor filter method. The feature level fusion is generated based on supervised local preserving correlation analysis framework. This work is evaluated using a database only of 600 fingerprints and finger veins respectively.

Son & Lee (2005) have been subjected a fusion of face and iris using reduced joint feature vector method. However, it is not verified on a large amount of data. Ross & Govindarajan (2005) presented multimodal biometric system that uses hand and face feature level fusion for biometric recognition purposes. Moreover, the experiments have been tested on both intra-modal and inter-modal fusion with R, G, B channels. But it does not accord eigen-coefficients of face and minutiae points of fingerprints, so still lacks significant accuracy. Ma, Popoola & Sun (2015) achieved a good fingerprint and finger vein identification system by concatenating the feature vectors. But, the accuracy of this technique is so less, it does not satisfy the requirements of  real-world applications. Huang et al. (2015) used adaptive face and ear recognition system(bimodal) based on sparse coding. Talking about Siamese neural network, Koch, Zemel & Salakhutdinov used Siamese neural network for one shot image recognition. Here, image representations were learnt via a supervised metric-based approach using Siamese neural network then reuse the network’s feature for one short learning without any re-training. Lake et al. approached the problem of one-shot learning by inverting a composition casual process, addressing one-shot learning for character recognition with a method called Hierarchical Bayesian Program Learning.

Table 2.1: Survey of Literature

|  |  |  |  |
| --- | --- | --- | --- |
| Authors | Title | Source | Abstract |
| El Mehdi Cherrat  Rachid Alaoui  Hassane Bouzahir | Multimodal Biometric Identification System Based on Advanced Cascading of Fingerprint and Finger vein Images and AND Rule at Decision Level Fusion | [link](https://www.researchgate.net/publication/336702890_Multimodal_Biometric_Identification_System_Based_on_Advanced_Cascading_of_Fingerprint_and_Finger_vein_Images_and_AND_Rule_at_Decision_Level_Fusion) | The multimodal identification system can integrate a variety of biometric characteristics. The main advantage of multibiometric system against traditional single biometric is achieving the recognition process more accurate and safe. In this paper, we will present a multimodal biometric recognition system that combines fingerprint and finger vein. The features in theses biometric traits are extracted to identify that individual is genuine or impostor using minutia points for fingerprint and Histogram of Oriented Gradient for finger vein |
| Subba Reddy Borra  Jagadeeswar Reddy  Edara Reddy | A broad survey on fingerprint recognition systems | [link](https://www.researchgate.net/publication/308708136_A_broad_survey_on_fingerprint_recognition_systems) | Fingerprints are extensively and effectively utilized for proof of identity in recent years. Mostly because of their originality, stability through life, a uniqueness among the people, public acceptance and their least risk of invasion. Fingerprint technology, which is a bio-metric system, is utilized to classify an individual based on their physical qualities. Fingerprint matching is the trendiest biometric technique utilized to provide authentication. |
| El Mehdi Cherrat  Rachid Alaoui  Hassane Bouzahir | Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images | [link](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7924518/) | In recent years, the need for security of personal data is becoming progressively important. In this regard, the identification system based on fusion of multibiometric is most recommended for significantly improving and achieving the high performance accuracy. The main purpose of this paper is to propose a hybrid system of combining the effect of tree efficient models: Convolutional neural network (CNN), Softmax and Random forest (RF) classifier based on multi-biometric fingerprint, finger-vein and face identification system. In conventional fingerprint system, image pre-processed is applied to separate the foreground and background region based on *K*-means and DBSCAN algorithm. |
| Arun Ross  Anil Jain | Information fusion in biometrics | [link](https://www.sciencedirect.com/science/article/abs/pii/S0167865503000795) | User [verification systems](https://www.sciencedirect.com/topics/computer-science/verification-system) that use a single [biometric](https://www.sciencedirect.com/topics/engineering/biometric) indicator often have to contend with noisy sensor data, restricted degrees of freedom, non-universality of the [biometric trait](https://www.sciencedirect.com/topics/computer-science/biometric-trait) and unacceptable error rates. Attempting to improve the performance of individual matchers in such situations may not prove to be effective because of these inherent problems. Multibiometric systems seek to alleviate some of these drawbacks by providing multiple evidences of the same identity. |
| Jinfeng Yang  Xu Zhang | Feature-level fusion of fingerprint and finger-vein for personal identification | [link](https://www.sciencedirect.com/science/article/abs/pii/S0167865511003771) | Multimodal biometrics based on feature-level fusion is a significant topic in personal identification research community. In this paper, a new fingerprint-vein based biometric method is proposed for making a finger more universal in biometrics. The fingerprint and finger-vein features are first exploited and extracted using a unified Gabor filter framework. Then, a novel supervised local-preserving canonical correlation analysis method (SLPCCAM) is proposed to generate fingerprint-vein feature vectors (FPVFVs) in feature-level fusion. Based on FPVFVs, the nearest neighborhood classifier is employed for personal identification finally. |
| Gregory Koch  Richard Zemel  Ruslan Salakhutdinov | Siamese Neural Networks for One-shot Image Recognition | [link](https://www.cs.cmu.edu/~rsalakhu/papers/oneshot1.pdf) | The process of learning good features for machine learning applications can be very computationally expensive and may prove difficult in cases where little data is available. A prototypical example of this is the one-shot learning setting, in which we must correctly make predictions given only a single example of each new class. In this paper, we explore a method for learning siamese neural networks which employ a unique structure to naturally rank similarity between inputs. |

**CHAPTER 3**

**Limitation of Existing system**

The existing systems are very much expensive.  It is often expensive to scale these systems as you will need to install hardware at every location. There is no alternative to investing in new hardware every time. For companies that have a primarily distributed workforce, with employees working on remote sites or massive production floors, disadvantages of biometric scanning become evident.

As, standalone system, accuracy of fingerprint is much lower than of facial recognition system. Fingerprint attendance systems are not as accurate as facial recognition systems.

Also, workers utilize tools and heavy machinery leading to wearing fingerprints for labor-intensive industries such as mining. It makes it difficult for machines to recognize the fingerprints leading to frustration. Workers have to fill out attendance sheets manually. Facial recognition systems are highly accurate as they do not depend on just set biometric attributes like fingerprints.

If a standalone is used,the face can be easily mimicked by using images of the respective person.

**CHAPTER 4**

**Problem Statement, Objectives and Scope**

**4.1 Problem Statement**

To propose a hybrid system of Neural Network: Siamese Convolutional neural network (CNN) based multi-biometric Fingerprint and face identification system.

The score provided by these systems is combined for improving Human identification not only in companies but also in other industries too where manual attendance or recognition is of utmost importance.

The need of authentication is the need of the hour. For security systems to work correctly identifying the person is very important. So in order to propose a hybrid bimodal model of siamese convolutional neural network to be used for the purpose of verifying the identity of a person using face and fingerprint data , this project is deployed.

To inaugurate a system which enhances the current traffic management by developing intelligent traffic lights based upon machine learning and artificial intelligence.

**4.2 Objectives**

* To offer an accurate matching compared with other systems based on bimodal characteristics.
* This is a bimodal biometric and makes use of two biometric indicators by personal identification systems for identifying the individuals. As compare to unimodal biometrics, bimodal provides  more authentication.
* To get accurate experimental results and demonstrate that our approach is significantly accurate against other approaches.
* To create an inexpensive, reliable option towards a passwordless future.
* Since there are not many systems available that can provide good efficiency and  accuracy we propose to have more than 99.99% of accuracy.

**4.3 Scope**

* This system is classified as multi-modal and hybrid systems.
* In order to overcome the limitation concerned unimodal biometric system, the multimodal biometric system increase the robustness and performance against the imposter`s attack and environment variations.
* The advantage of combining the fingerprint and face is its devices are less expensive and easier to deploy.
* Moreover, the face is one of the most natural methods to identify an individual, it does not restrict the movement of the person and its deployment cost is relatively low.
* The user will give an input image of face or fingerprint, the model will compare it with the predefined verification images and predict if the two images of the user are same or not.

**CHAPTER 5**

**Proposed System**

**5.1 Proposed system overview**

The Siamese nets were first introduced in the early 1990s by Bromley and LeCun to solve signature verification as an image matching problem (Bromley et al., 1993). A Siamese neural network consists of twin networks which accept distinct inputs but are joined by an energy function at the top. This function computes some metric between the highest level feature representation on each side. The parameters between the twin networks are tied. Weight tying guarantees that two extremely similar images could not possibly be mapped by their respective networks to very different locations in feature space because each network computes the same function.

We propose the use of a siamese convolutional neural network for the purpose of bimodal biometric verification. The two modes we use here are face and fingerprint.

Figure 5.1.1: Architecture Diagram of the model

Graphical user interface

Description automatically generated

Architecture Diagram of the model

An architectural diagram is a visual representation that maps out the physical implementation for components of a software system. It shows the general structure of the software system and the associations, limitations, and boundaries between each element.

The input images and anchor(verification) images of face are taken as input by the face model. The model then does feature extraction and encodes the images. The difference layer of the model then calculates by how much do these images differ which is then flattened by the fully connected flatten(dense) layer and then if the difference is less then we get a score greater than the threshold value and the face is verified as Yes(True). If the difference is greater then we get a score less than the threshold value and the face is verified as No(False).

The same process happens with the fingerprint input and anchor images and we get a value of either yes(True) or No(False). Then we apply the logical AND gate to verify if both the outputs are True or not and output it as the final result.

Data Flow Diagram

A Data Flow Diagram (DFD) is a graphical representation of the “flow” of data through an information system (as shown on the DFD flow chart Fig.2 & Fig.3), modeling its process aspects. Often it is a preliminary step used to create an overview of the system that can later be elaborated.

Figure 5.1.2: Data Flow Diagram (level 0)

Diagram

Description automatically generated

Level-0

Data collected from components that is face input 1, face input 2, fingerprint input 1 and fingerprint input 2 are sent to the respective Models, then the model gives the prediction and then AND gate is applied on the predictions of the models giving the final output .

**Text

Description automatically generated**

Figure 5.1.3: Data Flow Diagram (level 1)

Level-1

Data is collected from user in the form of images. This data is then sent to the respective Neural Network Model for intermediate processing. The verification status is predicted for both face and fingerprint data. AND gate is applied between the two predictions and the final output is recieved.

Sequence Diagram:

Figure 5.1.4 Sequence diagram

**Diagram

Description automatically generated**

**5.2** **Design details**

Dataset:

For implementation of this project we have made use of two datasets. The first one is the labelled faces in the wild dataset and the second dataset is our own dataset that we have created.

1. Labelled faces in the wild dataset:

The data set contains more than 13,000 images of faces collected from the web. Each face has been labeled with the name of the person pictured. 1680 of the people pictured have two or more distinct photos in the data set. The only constraint on these faces is that they were detected by the Viola-Jones face detector.

Figure 5.2.1: labelled faces in the wild dataset sample image



1. Our Own Biometric Dataset

Our biometric dataset consists of a total of 5151 images out of which 2410 images are face images and 2741 images are fingerprint images. The face images are of three subjects with subject1 having 729 face images, subject2 having 867 face images and subject3 having 814 face images. The fingerprint images contain fingerprint images of index finger of three subjects with at least 600 images each. There is also a set of 900 fingerprint images of random fingers from these subjects.

Figure 5.2.2: own biometric dataset sample image 1



Figure 5.2.3: own biometric dataset sample image 2



Figure 5.2.4: own biometric dataset sample image 3



Figure 5.2.5: own biometric dataset sample image 4



Figure 5.2.6: own biometric dataset sample image 5

A person smiling for the camera

Description automatically generated with low confidence

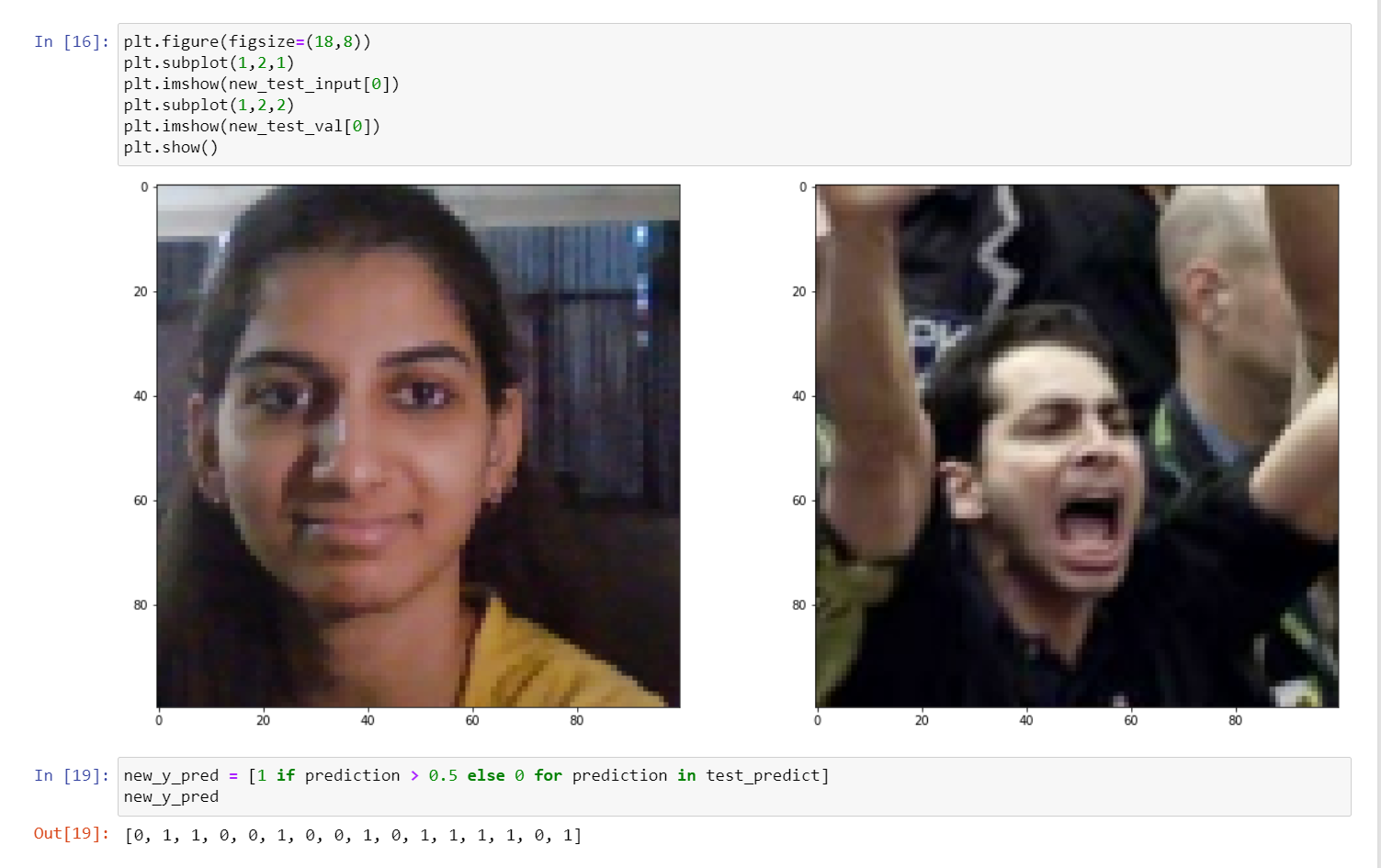
Figure 5.2.7: Implementation Output 1

Table

Description automatically generated

This is the summary of the layers of the embedding for the model

Figure 5.2.8: Implementation Output 2



This is how we get the predicted values for a test batch of face data

Figure 5.2.9: Implementation output 3



This is how we get the predicted values for a test batch of fingerprint data

**5.3 Methodology**

The user will provide a input image, The model will compare it with the verification image and calculate the difference between two images and if the difference is less than a particular threshold value, then the image will be verified as true and the user will be granted permission, if the difference is greater than threshold, this means that the two images are different. Hence, the person will not be verified and will be denied permission

Same will be applied for the fingerprint recognition system. The user will provide his/her fingerprint through fingerprint taker system and the fingerprint will be saved as images and will be compared to existing fingerprint images of the dataset by the model image and calculate the difference between two images and if the difference is less than a particular threshold value, then the image will be verified as true and the user will be granted permission, if the difference is greater than threshold, this means that the two images are different. Hence, the person will not be verified and will be denied permission.

Finally, we will combine both the outputs using logical AND gate. And show the output.

**CHAPTER 6**

**Experimental Setup**

* 1. **Software Requirements:**
* **Windows 7 or higher OS**
* **Jupyter Notebook:** Project Jupyter  is a project with goals to develop open-source software, open standards, and services for interactive computing across multiple programming languages. It was spun off from IPython in 2014 by Fernando Pérez and Brian Granger. Project Jupyter's name is a reference to the three core programming languages supported by Jupyter, which are Julia, Python and R. Its name and logo are an homage to Galileo's discovery of the moons of Jupiter, as documented in notebooks attributed to Galileo. Project Jupyter has developed and supported the interactive computing products Jupyter Notebook, JupyterHub, and JupyterLab. Jupyter is financially sponsored by NumFOCUS
* **Tensorflow.:** TensorFlow is a free and open-source software library for machine learning and artificial intelligence. It can be used across a range of tasks but has a particular focus on training and inference of deep neural networks. TensorFlow was developed by the Google Brain team for internal Google use in research and production. The initial version was released under the Apache License 2.0 in 2015. Google released the updated version of TensorFlow, named TensorFlow 2.0, in September 2019. TensorFlow can be used in a wide variety of programming languages, including Python, JavaScript, C++, and Java. This flexibility lends itself to a range of applications in many different sectors.
* **Python:** Python is one of the widely used programming languages for building systems that indulge in Image Processing as well as Machine Learning. Python provides amazingly powerful libraries and tools that help us in achieving the tasks efficiently
* **Scikit Learn:** Scikit-learn (formerly scikits.learn and also known as sklearn) is a free software machine learning library for the Python programming language. It features various classification, regression and clustering algorithms including support-vector machines, random forests, gradient boosting, k-means and DBSCAN, and is designed to interoperate with the Python numerical and scientific libraries NumPy and SciPy. Scikit-learn is a NumFOCUS fiscally sponsored project.
* **Software needed to activate the GPU:** CUDA (or Compute Unified Device Architecture) is a parallel computing platform and application programming interface (API) that allows software to use certain types of graphics processing units (GPUs) for general purpose processing, an approach called general-purpose computing on GPUs (GPGPU). CUDA is a software layer that gives direct access to the GPU's virtual instruction set and parallel computational elements, for the execution of compute kernels. CUDA is designed to work with programming languages such as C, C++, and Fortran. This accessibility makes it easier for specialists in parallel programming to use GPU resources, in contrast to prior APIs like Direct3D and OpenGL, which required advanced skills in graphics programming. CUDA-powered GPUs also support programming frameworks such as OpenMP, OpenACC and OpenCL; and HIP by compiling such code to CUDA. CUDA was created by Nvidia. When it was first introduced, the name was an acronym for Compute Unified Device Architecture, but Nvidia later dropped the common use of the acronym.
* **Google Colab(if gpu is unavailable):** Colaboratory, or “Colab” for short, is a product from Google Research. Colab allows anybody to write and execute arbitrary python code through the browser, and is especially well suited to machine learning, data analysis and education. More technically, Colab is a hosted Jupyter notebook service that requires no setup to use, while providing access free of charge to computing resources including GPUs.
* **Matplotlib:** Matplotlib is 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 using general-purpose GUI toolkits like Tkinter, wxPython, Qt, or GTK. There is also a procedural "pylab" interface based on a state machine (like OpenGL), designed to closely resemble that of MATLAB, though its use is discouraged.[3] SciPy makes use of Matplotlib.

**6.2 Hardware Requirements:**

* PC or laptop with x86-64 (64-bit) compatible processors
* A camera or webcam.
* Fingerprint scanner
* GPU for efficiency

|  |  |
| --- | --- |
| **Hardware Specification** |  |
| 1.Fingerprint Scanner | Futronic FS 80 |
| 2.GPU | Nvidia RTX 3060 |
| 3.Processor | AMD Ryzen 7 |
| **Software Specification** |  |
| 1. Nvidia CUDA | 11.2 |
| 2.Nvidia CuDNN | 8.1.0 |
| 3. FTR Scan software | - |
| 4. Tensorflow | 2.9 |

Table 6.1.1 Hardware and software requirments

**CHAPTER 7**

**Project Plan**

**Chart, funnel chart

Description automatically generated**

**7.1Gantt Chart**

**CHAPTER 8**

**Expected Outcome**

The model compares the input image to the verification image and calculates the difference between the two images. If the difference is less than a specific threshold value, the image is verified as true and the user is given permission. If the difference is greater than the threshold, the two images are different. Consequently, the individual won't be authenticated and won't be given permission.

The system for fingerprint recognition will function similarly. The user will submit his or her fingerprint by a fingerprint taker system, and the fingerprint will be saved as photos. The fingerprint images will be compared to the dataset's already-existing fingerprint images by the model image, and the difference between the two images will be calculated.

**References**

1. Cherrat EM, Alaoui R, Bouzahir H, Jenkal W. 2017. High-density salt-and-pepper noise

suppression using adaptive dual threshold decision based algorithm in fingerprint images.

In: 2017 Intelligent Systems and Computer Vision (ISCV). Fez: IEEE, 1–4.

1. Borra SR, Reddy GJ, Reddy ES. 2018. An efficient fingerprint identification using neural network and BAT algorithm. International Journal of Electrical & Computer Engineering 8(2):1194–1213DOI 10.11591/ijece.v8i2.pp1194-1213
2. Mane S, Shah G. 2019. Facial recognition, expression recognition, and gender identification. In: Balas V, Sharma N, Chakrabarti A, eds. Data Management, Analytics and Innovation. Singapore: Springer, 275–290.
3. Unar JA, Seng WC, Abbasi A. 2014. A review of biometric technology along with trends and prospects. Pattern Recognition 47(8):2673–2688 DOI 10.1016/j.patcog.2014.01.016.
4. Ross A, Jain A. 2003. Information fusion in biometrics. Pattern Recognition Letters 24(13):2115–2125 DOI 10.1016/S0167-8655(03)00079-5.
5. Yang J, Zhang X. 2012. Feature-level fusion of fingerprint and finger-vein for personal identification. Pattern Recognition Letters 33(5):623–628 DOI 10.1016/j.patrec.2011.11.002.
6. Son B, Lee Y. 2005. Biometric authentication system using reduced joint feature vector of iris and face. In: International Conference on Audio- and Video-Based Biometric Person Authentication. Berlin, Heidelberg: Springer, 513–522
7. Ross AA, Govindarajan R. 2005. Feature level fusion of hand and face biometrics. In: Biometric Technology for Human Identification II, Orlando, Florida, United States. Vol. 5779. International Society for Optics and Photonics, 196–205 DOI 10.1117/12.606093.
8. Ma H, Popoola OP, Sun S. 2015. Research of dual-modal decision level fusion for fingerprint and finger vein image. International Journal of Biometrics 7(3):271–285DOI 10.1504/IJBM.2015.071949.
9. Huang Z, Liu Y, Li X, Li J. 2015. An adaptive bimodal recognition framework using sparse coding for face and ear. Pattern Recognition Letters 53:69–76 DOI 10.1016/j.patrec.2014.10.009
10. Koch, Zemel & Salakhutdinov  Siamese neural network for one shot image recognition Lake, Brenden M, Salakhutdinov, Ruslan R, and Tenenbaum,Josh. One-shot learning by inverting a compositionalcausal process. In Advances in neural information processing systems, pp. 2526–2534, 2013