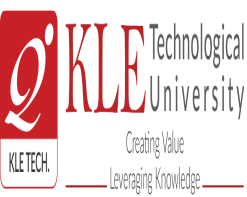
KLE Society's

KLE Technological University



**A Mini Project Report**

**On**

**Face recognition with anti-spoofing**

*submitted in partial fulfillment of the requirement for the degree of*

**Bachelor of Engineering**

**In**

**Computer Science and Engineering**

**Submitted By**

| **Soumya Katagihalli** | 01fe20bcs002 |
| --- | --- |
| **Neha Patil** | 01fe20bcs006 |
| **Sushir R Meti** | 01fe20bcs025 |
| **Srishti kadam** | 01fe20bcs010 |

**Under the guidance of**

**Dr. Karibasappa K.G**

.

SCHOOL OF COMPUTER SCIENCE & ENGINEERING

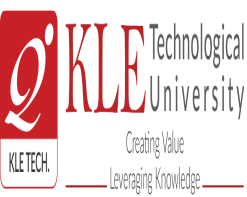
HUBLI–580 031 (India).

Academic year 2022-23

KLE Society's

KLE Technological University

2022 - 2023



SCHOOL OF COMPUTER SCIENCE & ENGINEERING

**CERTIFICATE**

This is to certify that Mini Project entitled FACE RECOGNITION WITH ANTI SPOOFING is a bonafide work carried out by the student team Ms. Soumya Kotresh Katagihalli- 01FE20BCS002, Ms. Neha Patil- 01FE20BCS006, Ms. Srishti Kadam 01FE20BCS010, Mr. Sushir Ramesh Meti- 01FE20BCS025, in partial fulfillment of completion of Fifth semester B. E. in Computer Science and Engineering during the year 2022 – 2023. The project report has been approved as it satisfies the academic requirement with respect to the project work prescribed for the above-said programme.

**Guide Head, SoCSE**

**Dr. Karibasappa K. G. Dr. Meena S.**

**External Viva:**

**Name of the Examiners Signature with date**

**1.**

**2.**

**ABSTRACT**

Despite great technological advancements in the field of security, the challenge of safeguarding private information is still a hurdle to overcome. We have now, technologically, reached a phase where almost all our daily activities are digital, right from buying groceries to advanced security systems. Security systems are also leaning towards being as digital as possible. This invites biometric systems and other similar services to provide their services. But just like a coin has two faces, developments also led to methods to cheat these systems and gain unauthorized access. This work aims to provide a solution one of such techniques by introducing an upgrade to the existing facial recognition system with an anti-spoofing system that only grants access if the user is registered and live (not spoofing).

| **Chapter No.** | **TABLE OF CONTENTS** | | | | | **Page No.** |
| --- | --- | --- | --- | --- | --- | --- |
| **1.** | **INTRODUCTION** | | | | | **1** |
|  | 1.1 | Preamble | | | | **.** |
|  | 1.2 | Motivation | | | | **.** |
|  | 1.3 | Objectives of the project | | | |  |
|  | 1.4 | Literature Survey (for identifying existing solutions) | | | |  |
|  | 1.5 | Problem Definition | | | |  |
| **2.** | **PROPOSED SYSTEM** | | | | | **.** |
|  | 2.1 | Description of the proposed system | | | |  |
|  | 2.2 | Description of Target Users | | | |  |
|  | 2.3 | Advantages/Applications of the Proposed System | | | |  |
|  | 2.4 | Scope | | | |  |
| **3.** | **SOFTWARE REQUIREMENT SPECIFICATION** | | | | |  |
|  | 3.1 | Overview of SRS | | | |  |
|  | 3.2 | Requirement Specifications (In brief write the meaning of functional requirements) | | | |  |
|  |  | 3.2.1 | | Functional Requirements ((In brief write the meaning of functional requirements) | |  |
|  |  | 3.2.2 | | Use case diagrams | |  |
|  |  | 3.2.3 | | Use Case descriptions using scenarios | |  |
|  |  | 3.2.4 | Nonfunctional Requirements | | |  |
|  |  |  | | 3.2.4.1 | Performance requirements |  |
|  |  |  | | 3.2.4.2 | Safety requirements |  |
|  |  |  | | 3.2.4.3 | Security Requirements |  |
|  |  |  | | 3.2.4.4 | Usability |  |
|  |  |  | |  |  |  |
|  | 3.3 | Software and Hardware requirement specifications | | | |  |
| **4** | **SYSTEM DESIGN** | | | | |  |
|  | 4.1 | The architecture of the system (explanation) | | | |  | |
|  | 4.1 | Class Diagram (with brief explanation) | | | |  | |
|  | 4.2 | Sequence diagram (if applicable with brief explanation) | | | |  | |
|  | 4.3 | ER diagram and schema (if applicable) | | | |  | |
|  | 4.4 | State transition diagram (if applicable) | | | |  | |
|  | 4.5 | The data structure used (if applicable) | | | |  | |
|  | 4.6 | Data Set Description (if applicable) | | | |  | |
| **5** | **IMPLEMENTATION** | | | | |  | |
|  | 5.1 | Proposed Methodology | | | |  | |
|  | 5.2 | Description of Modules | | | |  | |
| **6** | **TESTING** | | | | |  | |
|  | 6.1 | Test Plan and Test Cases  Acceptance of test plan & test cases  Unit test plan & test cases | | | |  | |
| **7** | **RESULTS & DISCUSSIONS** | | | | |  | |
| **8** | **CONCLUSION AND FUTURE SCOPE** | | | | |  |
| **9** | **References** | | | | |  |
| **10** | **Appendix** | | | | |  |
|  | A | Gantt Chart | | | |  |

1. **INTRODUCTION**
   1. **Preamble**

Despite significant technological developments, private information still needs to be kept secure from unauthorized access. Security services have evolved recently to the point that the entire system is now digital. This concept is made to resist spoofing attacks against various private data maintenance systems. A safe system needs liveness detection.

Based on different liveness detection algorithms, face anti-spoofing approaches are classed. To reinforce the authentication process and lessen this vulnerability, the administration might add a new security layer to the system known as the liveness detector or face spoofing detector. A facial recognition system, which is often used to authenticate users, is a technology that can compare a human face from a digital image or a video frame against a database of faces. However, false faces can launch spoof attacks against facial recognition systems. Face images, like those in portrait photos, can be used to readily mislead face recognition algorithms. This can happen through 2D assaults, such as flashing the system falsely obtained images or video, or through 3D attacks, where someone can put on a 3D mask and access the data. This will result in the loss of priceless data, financial loss, etc. Our key goal is to tackle this spoofing attack and strengthen the security of this architecture. These are employed widely. A secure system needs liveness detection to stop this form of spoofing. In this work, several face liveness identification methodologies are categorized based on the various liveness detection strategies. This classification makes it easier to understand different spoof attack scenarios and how they relate to the solutions developed. The major goal is to offer a straightforward route for a more secure face-liveness detection method. The applications of this system include an attendance system, secure locks for banks and home doors, and also to accelerate the investigations at crime scenes.

Before beginning to utilize it, the user scans and creates the only photos of people that are fed into the model—faces alone. For the aim of training the model for recognition, these photos (actual photographs) are employed. To train the spoofing assaults, the model is also fed fake photos taken with a phone. The test images will be classified as real or spoof based on the learning the model did during training. When a user or fraud attempts to access private information using the camera's interface, they try to identify their face; if successful, the system will display the result as real; if unsuccessful, the system will alert as a spoof attack.

**1.2 Motivation**

Strong security is essential in a society that is becoming more and more digital since it is growing harder and harder to keep sensitive information safe from hackers and unauthorized users. User authentication is thus very necessary for a reliable biometric system.

Traditional biometric techniques, such as fingerprint and face recognition, have sadly been shown to be vulnerable to spoofing attacks, in which a person attempts to pass as another by fabricating a biometric characteristic of the targeted user and presenting it to the input sensor to gain an unfair advantage. Among the other vulnerabilities, spoofing is the only one that relates to biometrics. The biggest problem with biometric authentication is probably this one. Because spoofing attacks take place at the sensor level and are not under the control of the biometric system's manufacturer, no digital protection techniques can be utilized to stop them. This makes the approach extremely easy to duplicate and highly likely to succeed. Pictures and videos are the most frequently used to trick face recognition systems since they are easy to use and inexpensive. It has been discovered that face recognition systems are susceptible to photo and video attacks. The problem is especially worrisome because so many individuals allow their images to be published online, especially on social networks. An attacker can locate numerous high-quality images and use them to attack with nothing more than the user's name. The administration of the system can implement a new security layer called the liveliness detector or face spoofing detector to strengthen the authentication procedure and minimize this vulnerability. Facial photographs, such as those in portrait shots, may easily be utilized to trick face recognition systems. This can occur through 2D attacks, such as flashing the system with fake graphics or video, or through 3D attacks, such as when someone dons a 3D mask and gains access to the data. As a result, irreplaceable data will be lost, as well as money and other resources. Our main objective is to thwart this spoofing attack and improve the architecture's security. These are often used. Liveness detection in a secure system must prevent this type of spoofing.

The goal is to develop non-intrusive countermeasures against spoofing attacks that can be integrated into existing face recognition systems without the need for additional hardware or human intervention.

* 1. **Objectives**
* To capture the facial images of the users and give each a unique identification number.
* To give each image a unique identification number.
* To detect the face of an individual while they are facing the camera.
* To check for the liveness of the person
* To pop up the results either spoof or real.

**1.4 Literature Survey**

Insight on face liveness detection: A systematic literature review. Published in December 2019. In this paper, Assaults are divided into two categories: indirect attacks and direct attacks. Hackers or other intrusive parties may carry out indirect assaults by altering the feature extractor (also known as the matcher) or the template database, for example. Several safeguards, including but not limited to antivirus software, firewalls, encryption, and intrusion detection, can prevent indirect assaults. On the other hand, direct attacks take place at the sensor level outside of the system's digital boundaries, making it impossible to foresee them using digital defense measures. Face anti-spoofing systems need the presence of a real photo, recorded video, false proof, etc. at the sensor (i.e. camera). Videos may often give more physiological proof, although photographs typically lack 3D information. This can be used as a static picture constraint in liveness detection.

Face Biometric Spoof Detection Method Using a Remote Photoplethysmography Signal. Published on 16 April 2022. They have employed signals in this model that can recognize a spoofing assault. In comparison to other detection techniques, such as 3D geometry cue-based methods or texture cue-based approaches, face spoofing detection utilizing rPPG signals offers a substantial advantage over 3D mask assault scenarios. The rPPG signal is frequently combined with 3D geometric information, which might counteract the benefit of simplicity of implementation. Therefore, the study's main goal was to increase the precision of replay attack detection using just the rPPG signal. Four separate attack scenarios, shot in three different settings, were the subject of video data collection. The following attack scenarios were to be picked up by our screening system for video integrity: Attacks include (1) light shaking; (2) horizontal and vertical photo bending; (3) light movement in the facial region. For increased accuracy, motion attacks and light movement attacks were anticipated.

Face anti-spoofing using neural networks published on 6th November 2019. The primary goal is to train distinct datasets for false faces and genuine faces, verify each dataset and then test each dataset using a different set. Using the training dataset, a convolutional neural network is trained. They gathered their dataset of genuine and fictitious faces (500 each) CNN is used, which is more effective than more conventional approaches like the motion-based method, the texture-based method, and the picture quality analysis method. The neural layers' flexibility is mostly to blame for the improved performance in spotting faked photos.

Face Detection and Recognition using OpenCV and Python published on 10th October 2020. Using Python and OpenCV, a deep learning programming language, the goal of this project is to build a system that uses the computer's camera to identify and recognize a person's face.

The OpenCV helps to recognize a person's frontal face and also produces XML documents for other locations, including body parts.

Two components will be the main emphasis of face detection and recognition using deep learning. The initial step requires accepting any pertinent picture as a solidary input, and the second step entails offering the best results or outputs for the image. The system's two most important libraries are Dlib and facial recognition. Using the dlib facial recognition framework would be the most straightforward way to organize the face assessment.

On June 6, 2021, Face Recognition Locker was released. OpenCV includes three face recognizers. The following are the names of those face recognizers and their OpenCV calls: Eigenfaces: createEigenFaceRecognizer cv2.face (). An algorithm called Eigenfaces Face Recognizer recognizes faces while taking into consideration the fact that not all facial features are equally important or helpful.

Fischer Faces cv2.face.createFisherFaceRecognizer (). The main components that distinguish one person from the others are carefully extracted using Fisher Faces' face recognizer algorithm.

Create an LBPH face recognizer with the command cv2.face.createLBPHFaceRecognizer (). Place a 3x3 window across the photo. Each time there is a movement, compare the center pixel to its neighboring pixels (each local area of the image). If the neighbors' intensity levels are less than or equal to the center pixel, indicate the neighbors with a 1 and the remainder with a 0.

**1.5 Problem Definition**

Face recognition is the most widely used biometric identification method in the modern world. This technique is very common from cell phone lock screens to home safes. One of the most popular applications, face recognition, has recently attracted a lot of attention and popularity. Numerous studies have been conducted on identifying a user from their facial appearance. The security of facial recognition technologies continues to be a major worry. However, this system, like any other, is susceptible to several ways by which one might break through the security and have access which is not meant for them, owing to man's never-ending hunger and curiosity. Spoofing may be used to do this in facial recognition. When facial spoofing occurs, it frequently goes by the name of a "presentation attack." According to the Biometrics Institute, it is a type of facial recognition spoofing that uses biometric information that has been illegally collected, either explicitly or overtly, from a person online or through compromised networks. Static 2D or static 3D assaults are two different ways that presentations might be attacked.

Attacks using static 2D presentation make use of flat, 2D items like images, paper, or masks. Surprisingly vulnerable to well-produced 2D media are facial recognition systems with minimum security measures. Furthermore, more advanced 2D assaults flash graphics in succession on tablet or smartphone screens to simulate real-time movement.

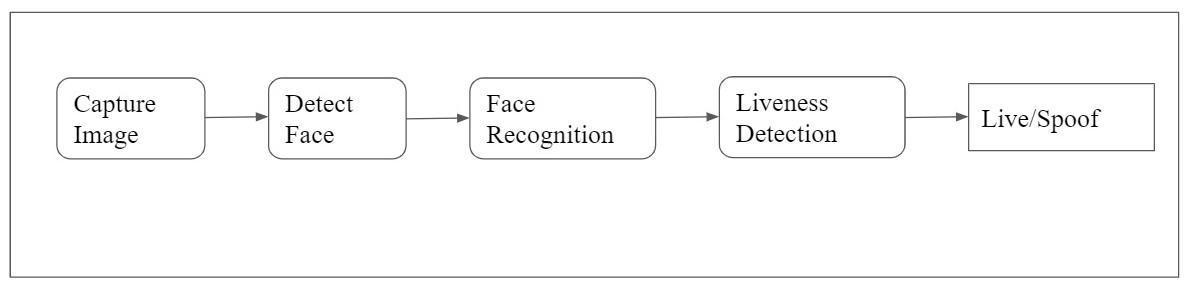
Attacks using static 3D technology go one step further by using 3D-printed masks, sculptures, or facial replicas. Bypassing more potent identification algorithms that rely on numerous face data points or even motions is made possible through this. Even robots that can create distinctive facial expressions are used in certain static 3D attacks.

Due to the technology required for 3D assaults, static 2D attacks are presently the more popular type of face recognition spoofing.

1. **PROPOSED SYSTEM**

**2.1 Description of Proposed System**

We build a presentation attack detection system (PAD) using anti-spoofing techniques and integrate it with the face recognition system.

****

**Fig 1: Block diagram of the proposed system**

This simple block diagram in Fig 1, gives a brief overview of the workings of the proposed system model.

Initially, the images are fed to the system and stored. As a result, the data set creation phase has been completed. The system is then trained with appropriate test and training data sets.

Then the system is put to the test with real-time inputs. Once the system captures the image, it will detect if there is a face in the image it has been fed. If yes, proceed with face detection of the one present in the input to the database If matched, the liveness of the input is going to be checked, and based on the result of the above 2 processes, the system provides the respective output based on the processing done.

**2.2 Description of target users**

The end users include a sizable percentage of smartphone users because many phones, including the most current iPhones, employ facial recognition to unlock the device. Law enforcement frequently employs face recognition technology to track down suspects and conduct additional illegal searches. A common sight at airports throughout the world is the growing number of passengers carrying biometric passports, which enable them to bypass the often-long lineups and proceed directly to the gate by passing through an automated ePassport inspection. Face recognition also has the advantage of biometric internet banking. Customers can authorize transactions by glancing at their computer or smartphone in place of one-time passwords. The consumer report claims that automakers are testing the use of face recognition to replace car keys. The car's starting and entry would no longer require a key, and the system would also remember the driver's preferred seat and mirror configurations as well as radio station presets. Educational institutions also value this method for employees and students to supplement the manual attendance system.

**2.3 Advantages of the proposed system**

* The system stores the faces that are recognized and automatically gives access or permits the user.
* Provide authorized access.
* Ease of use.
* Multiple face detection.
* Recognize the faces in real-time using live data.
* Checks for liveness and the model supports anti-spoofing.
* The applications here include the attendance system, bank, home lockers, and many more.

**3.SOFTWARE REQUIREMENT SPECIFICATION**

**3.1 Overview of SRS**

To build aFace recognition system which will be used as a means of authentication at a personal/high security level, certain algorithms need to be applied to overcome the spoofing attacks. In order to do this, Anti-spoofing technique is introduced which prevents the spoofing attacks.Liveness detection is necessary for a secure system to prevent this kind of spoofing. The Anti-spoofing method will overcome the image and video spoofing attacks. There are certain requirements for the same, for GUI we need concepts of web technology (HTML,javascript,css).

**3.2 Requirements Specifications**

Requirements specification is the process of defining the requirements for a product, system, or service. It is an important step in the development of any project, as it helps to ensure that the final product or service meets the needs and expectations of the users.

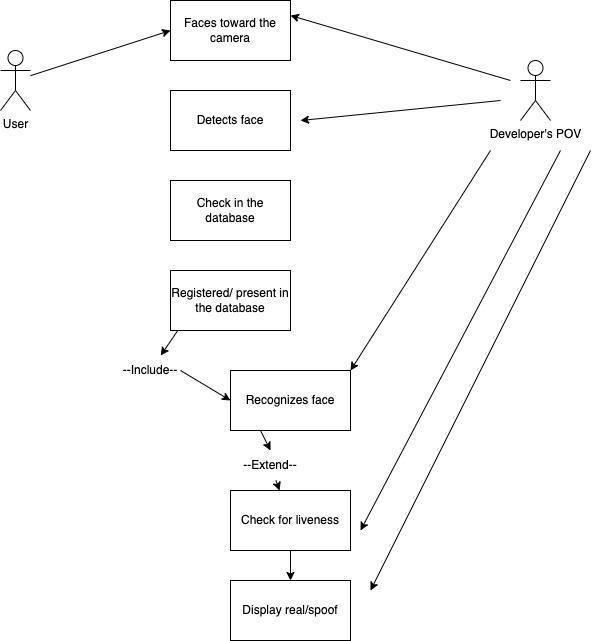
**3.2.1 Functional Requirements**

Functional requirements are specific actions or capabilities that a product, system, or service must be able to perform in order to meet the needs and expectations of the users. They describe the specific functionality that the product or system must provide in order to be successful. Our model’s functional requirements are listed below.

* This system shall provide GUI for interaction.
* This system shall capture face images of the users via webcam or external USB camera.
* This system shall detect the face of the user.
* This system shall check for a spoofing attack.
* This system shall give an alert message if a spoofing attack has been done.

**3.2.2 Use case diagram**

A use case diagram is a type of visual modeling tool that is used to represent the interactions between a system and the actors that interact with it. It is typically used in the early stages of software development to identify and define the functional requirements of a system.

****

**Fig 2: Use case diagram of the system**

The use case graphic up top in Fig 2, shows how our model functions. When a user faces the camera, the model, or the developer, recognizes the face and verifies that it is alive by comparing it to the dataset. If the user is permitted, the model will display the message as real; otherwise, it will display a warning message as “spoof”

**3.2.3 Use case diagram descriptions using scenarios**

| Use case | Developer |
| --- | --- |
| Primary Actor | Developer/trainer |
| Goal in context | to create a user-friendly application for face recognition. |
| Preconditions | Complete knowledge of how the system would work. |
| Trigger | An executable code. |
| Scenario | * Capture the images * Storing the dataset * Model training. |
| Expectations | * Any code error will be debugged. * Error occurring in downloading the dataset must be taken care of with enough memory space. |

| Use case | Real user |
| --- | --- |
| Primary Actor | Real user (Authorized person) |
| Goal in context | used for lockers, safes, and attendance systems. |
| Preconditions | To have a proper personal computer with all requirements |
| Trigger | Use the application by create and loading the frontal images of themselves. |
| Scenario | * Capture the frontal images. * Whenever in use, the user will scan their faces, to access the private data. * Access the private data. |
| Expectations | The user can access the private data as the system will detect the user as a real authorized person. |

| Use case | Unauthorized person |
| --- | --- |
| Primary Actor | Unauthorized person(spoof) |
| Goal in context | to access the private data of someone else, i.e., trying to attack the system. |
| Preconditions | to have images, videos, or 3D masks of someone else to attack the system. |
| Trigger | Show the images to the system as a spoof attack. |
| Scenario | Attack private information by spoofing. |
| Expectations | The system detects a spoof attack and denies access to sensitive information. |

**3.2.4 Non-Functional Requirements**

Non-functional requirements are characteristics or constraints of a product, system, or service that are not related to specific functions or capabilities. They describe the broader context in which the product or system will be used, and may include factors such as performance, security, usability, reliability, and maintainability.

* This system should be simple to understand and easier to deal with.
* This system should perform its process with accuracy and precision to avoid intruders gaining access to confidential data.
* This system should be secured in saving users’ privacy.

**3.2.4.2 Safety requirements**

As it is connected via LAN and MAN, an antivirus has been installed on the system for its safety.

**3.2.4.3 Security Requirements**

The main goal is to implement anti-spoofing techniques for major security purposes to defeat spoofing attacks. Data vulnerabilities are also highly possible. (Hackers have broken into databases containing facial scans).

* 1. **Software and Hardware requirement specifications**

1. Server side

* Operating System: Windows 7 or later versions
* Processor: Pentium 3.0 GHz or higher
* RAM: 8 GB or more
* Hard Drive: 10 GB or more

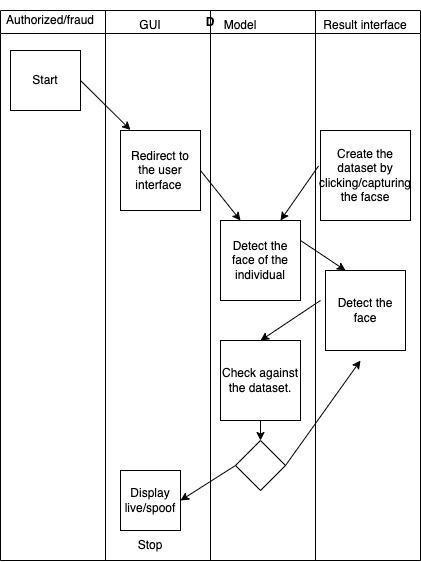
1. Client side

* Operating System: Windows 7 or above, MAC 10.12.6 or newer.
* Processor: Pentium 2.0 GHz or higher.
* RAM: 1 GB or more

1. **SYSTEM DESIGN**

**4.1 Architecture of the system**

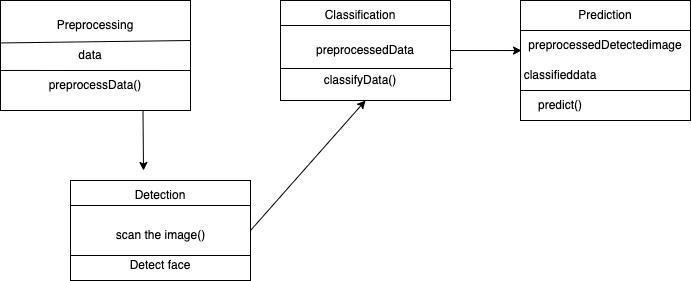
The model’s activity diagram.

****

**Fig 3: Activity diagram of the proposed system**

The above activity diagram in Fig 3, represents the functioning of our system. The people who own the private data in this system are still the end users. However, unauthorized users who want to attack the same data can engage in spoof attacks. In essence, people may record their faces and feed them to the model via the user interface provided by this system, allowing the model to learn and recognize the authorized person's face. The model looks for the user's face while they are facing the camera; it exclusively detects faces. When a face is found, the system compares it to the dataset to determine to whom it belongs. If a spoof attack is detected after this, the system will display the alert message as a spoof, and real if it is an authorized person. When it comes to convolutional architectures, we have used the MobileNet V2 architecture as it is a lightweight architecture to train the model.

**4.1 Class Diagram (with brief explanation)**

****

**Fig 4: Class diagram of the system**

Preprocessing is carried out for this reason so that the model can redirect and catch the backdrop or other images when taking the photographs. where the data is manually deleted. Our model receives this preprocessed data as input. The algorithm then classifies the identified person's picture using data from the dataset Whether the recognized person is an authorized person or not, future predictions are made. If a prediction is made by an authorized user, the system will notify as the genuine message; otherwise, it will alert as an unauthorized user. The class diagram for the same is shown in Fig 4.

**4.6 Data Set Description**

* The dataset generation is done using the Haar cascade classifier.
* The id is given to every authorized person.
* Every image in the dataset is given a unique id.
* The image frame i.e., the size of the image is 200 x 200 px.
* Under the Real folder and Spoof folder, folders of authorized persons are created respectively.
* These are read into two different folders i.e., train for training the data and

testfor testing.

* → The number of real images for the training dataset - 200

→ The number of spoof images for the training dataset - 200

→ The number of real images for testing dataset - 40

→ The number of real images for testing dataset - 40

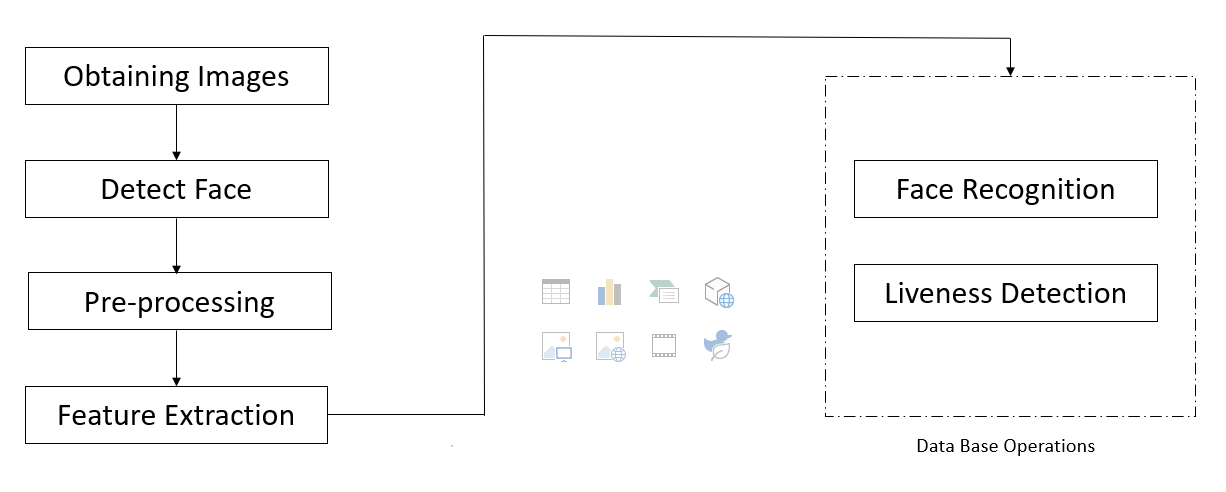
**5. Implementation**

**5.1. Proposed Methodology**

We have used the MobileNet V2 architecture for feature extraction. It is a neural network architecture that performs well on lightweight embedded devices. The architecture contains the initially fully convolution layer with 32 filters, followed by 19 residual bottleneck layers. Section 5.2, "Description of Modules," is the model's focal point.

Our project consists of modules. This is crucial to the project and to understanding coding principles. In the notion of software engineering, we regard it as a minor component of a system, but in our programming language, it is a little component of the program, sometimes referred to as a function, and makes up the main program. During the project, we could produce a lot of modules, which we then merged to make a system. The figure for the steps in the model is shown in Fig 5.

**5.1.1 Training stages**



**Fig 5: Stages involved in the entire system**

1. **Obtaining images**

A module called "Image Acquisition" is used to retrieve the image with the user ID. This is where we add images, we've taken using a web camera and save them to the database. Sixty photos of everyone are taken. Each picture is saved.

1. **Detect a face**

OpenCV has a built-in detector called detect Multiscale that may be used to find the area of interest (ROI) and give the coordinates of the detected face.

1. **Feature extraction**

Categorizing the images into their respective classes will need the outputs of the feature extraction process as the base inputs for it to further proceed.

1. **Face recognition**

The next and most crucial step is the classifier we will use to build the model for correctly categorizing the photos with labels. This module can compare and search against photos that already exist in the database. OpenCV comes with three built-in face recognizers:

* EigenFaces.
* FisherFaces.
* Local Binary Patterns Histograms (LBPH).

To generate our model in this case, we'll utilize the LBPH face recognizer.

**5. Liveness detection**

We are recognizing faces from the input picture using the Haar cascade classifier and the detectMultiscale() function, drawing a rectangle around the discovered face. The next task is to print the proper labels or names on the frames after the face has been accurately detected. To achieve this, we must employ the idea of a dictionary.

**6. TESTING**

**6.1 Test plan and test cases**

A testing plan is a document that outlines the strategy and approach for testing a product, system, or service. It is an important part of the software development process, as it helps to ensure that the final product or service meets the requirements and expectations of the users.

**Acceptance of test plan and test cases**

The final stage of software testing is acceptance testing, which is carried out after system testing and before the system is usable.

| Test ID | Test case description | Test steps | Test inputs | Expected results | Actual result | Pass/Fail |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Allowing the authorized person to access the data. | * Capture the image of the individual. * When a person faces the camera., the system has to classify it as a spoof or real. | Images | The system has to permit the user to access and alert as a real user | The alert message is given as “real” | Pass |

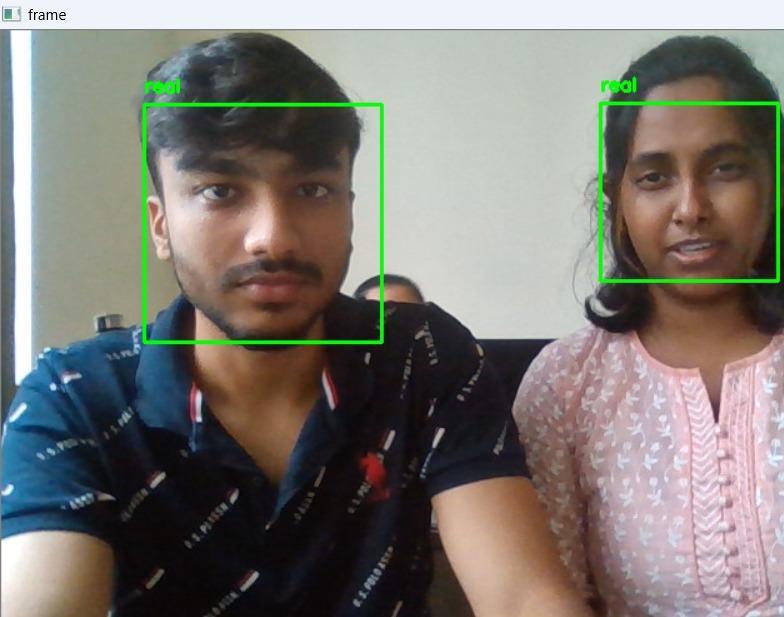
**Unit test plan and test cases**

Unit testing is a sort of software testing in which individual program components are tested.

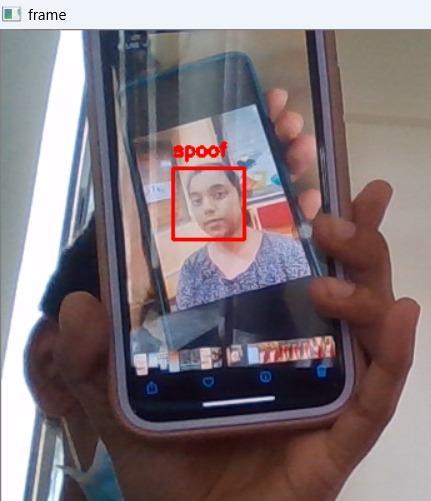
| Test ID | Test case description | Test steps | Test inputs | Expected results | Actual result | Pass/Fail |
| --- | --- | --- | --- | --- | --- | --- |
| 2 | preventing the unauthorized person from accessing the data. | * Capture the spoofed image of the individual. * when a person faces the camera with a spoofed image, the system has to classify it as a spoof or real. | Images | The system must not permit the user to access and alert as a spoofed user. | The alert message is given as a “spoof” | Pass |

**7. RESULTS AND DISCUSSIONS**

The model is fed frontal images of people. The model is trained with the same images. After the training is done, the model is ready to be used by all individuals. There are two results for spoof attacks and another one for authorized users. When the real user or authorized person faces the camera, the system has to alert the user and pop a message as “real user,” and the face is also marked with a green square.



**Fig 6: Classifying it as a Real image**



**Fig 7: Classifying it as a spoof image**

When an unauthorized user attempts to access private data, the system must detect it as a spoof attack, display the message "spoof attack," and mark the face with a green square.

**8. CONCLUSION AND FUTURE SCOPE**

A highly promising form of security system uses facial recognition technology since it is user-friendly and simple to integrate into gadgets. Additionally, it reduces vulnerability to high-quality replay attacks without the use of extra devices and some database requirements. Our model can precisely differentiate between an authorized person (real person) and an attack made by fraud based on the images of people categorized into real and spoofed which are given to the model while training.

Future scope includes improved image quality i.e., increasing the quality and resolution of input images can help to improve the accuracy and reliability of face anti-spoofing systems. Integration with other security measures: Face anti-spoofing systems can be more effective when used in combination with other security measures, such as password authentication or behavioral biometrics. Future work could focus on developing approaches for integrating these different security measures in a way that is seamless and easy for users, while also providing strong protection against spoofing attacks. This model can also be extended to overcome 3D mask attacks, and video spoofing attacks.

**9. REFERENCES**

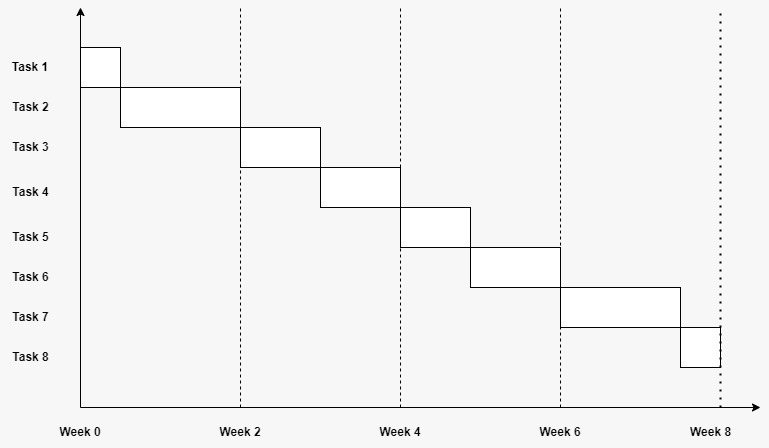
1. Bledsoe, W. W. The model method in facial recognition, Panoramic Research Inc., Palo Alto. CA, Technical Report, Technical Report PRI: 15, 1964.
2. Dhawanpatil, T., & Joglekar, B. , “Face Spoofing Detection using Multiscale Local Binary Pattern Approach”, IEEE, International Conference on Computing, Communication, Control and Automation, 2017, pp. 1-5.
3. Ratha, N.K., Connell, J.H., Bolle, R.M.: An analysis of minutiae matching strength. In: Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), pp. 223–228. Springer-Verlag (2001).
4. Jain,A.K.,Flynn,P.,Ross,A.A.(eds.):HandbookofBiometrics.Springer-Verlag(2008).
5. Li,S.Z.,Jain,A.K.(eds.):Hand book of Face Recognition. Springer-Verlag(2011).
6. McCool C, Marcel S, Hadid,A., Pietikainen,M., MatejkaP, Cernocky, J Poh N,Kittler J, Larcher, A., Levy, C., Matrouf, D., Bonastre, J.F. Tresadern, P Cootes T: Bi-modal person recognition on a mobile phone: using mobile phone data. In: IEEE ICME Workshop on Hot Topics in Mobile Multimedia (2012).
7. Li, Jiangwei, Yunhong Wang, Tieniu Tan, and Anil K. Jain. "Live face detection based on the analysis of fourier spectra." In Biometric Technology for Human Identification, vol. 5404, pp. 296-304. International Society for Optics and Photonics, 2004.
8. de Freitas ereira, Tiago, Andre Anjos, Joseario De artino, and Se astien arcel. B International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072 © 2022, IRJET | Impact Factor value: 7.529 | ISO 9001:2008 Certified Journal | Page 3858 TOP based countermeasure against face spoofing attacks." In Asian Conference on Computer Vision, pp. 121-132. Springer, Berlin, Heidelberg, 2012.
9. Wang, Tao, Jianwei Yang, Zhen Lei, Shengcai Liao, and Stan Z. Li. "Face liveness detection using 3D structure recovered from a single camera." In Biometrics (ICB), 2013 International Conference on, pp. 1-6. IEEE, 2013.
10. Ghorpade, Shruti, Dhanashri Gund, Swapnada Kadam, and Mr RA Jamadar. "Image Quality Assessment for Fake Biometric Detection: Application to Face and Fingerprint Recognition." International Journal of Emerging Technologies and Engineering (IJETE) Volume 2.
11. Gal all , Javier, Se astien arcel, and Julian Fierrez. "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition." IEEE transactions on image processing 23, no. 2 (2014): 710-724.
12. Wang, Tao, Jianwei Yang, Zhen Lei, Shengcai Liao, and Stan Z. Li. "Face liveness detection using 3D structure recovered from a single camera." In Biometrics (ICB), 2013 International Conference on, pp. 1-6. IEEE, 2013.
13. Kant C and Sharma N 2013 Fake face recognition using fusion of thermal image and skin elasticity International Journal for Computer Science and Information Security
14. Komulainen J, Hadid A and Pietikainen M 2013 Context based face anti-spoofing 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS)
15. X. Tan, Y. Li, J. Liu, L. Jiang, Face liveness detection from a single image with sparse low rank bilinear discriminative model, in Proceedings of the European Conference on Computer Vision (ECCV), LNCS, vol. 6316, Heraklion, Crete, Greece, (Springer, 2010), pp. 504–517
16. A. Anjos, M.M. Chakka and S. Marcel, Motionbased counter-measures to photo attacks in face recognition IET Biometrics, 3(3), 147–158 (2014)
17. M.M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristri, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S.Z. Li, W.R. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. Castrillon-Santana, J. Maatta, A. Hadid, M. Pietikainen, Competition on countermeasures to 2-D facial spoofing attacks, in International Joint Confer- ence on Biometrics (IJCB), Washington, DC., USA, 2011
18. Wu, H.Y., Rubinstein, M., Shih, E., Guttag, J., Durand, F., Freeman, W.T.: Eulerian video magnification for revealing subtle changes in the world. ACM Trans. Graph. (SIGGRAPH 2012) 31(4) (2012).
19. Chingovska,Anjos,A.,Marcel,S.:Antispoofing inaction:jointoperationwithaverification system. In: Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, Workshop on Biometrics (2013).

**10. APPENDIX**

Appendixes are often used to include technical details, data sets, graphs, charts, tables, or other materials that would be too lengthy or complex to include in the main body of the document. They can also be used to provide supporting evidence or examples to illustrate key points made in the main text.

1. **Gantt Chart**

A Gantt chart is a type of bar chart that is commonly used to illustrate the schedule of a project. It is named after Henry Gantt, an American engineer and management consultant who developed the chart in the early 20th century as a tool for visualizing and planning complex projects. In this Gantt chart represents project management to track the progress of a project, identify potential bottlenecks or delays, and adjust the project schedule as needed.

****

Phase 1: Generate the dataset.

Phase 2: Image Processing

Phase 3: Feature Extraction

Phase 4: Build a sample CNN model to classify images

Phase 5: Tuning hyperparameters for better accuracy.

Phase 6: Final Framework

Phase 7: Integration and results