**A Project report on**

### FAKE FACE DETECTOR

A Dissertation submitted to JNTU Hyderabad in partial fulfillment of the academic requirements for the award of the degree.

**Bachelor of Technology**

**in**

**Computer Science and Engineering**

Submitted by

K.LOKESH REDDY 19H51A0514 B.VISHNU VARSHITHA 19H51A0565 I.SUMANTH 19H51A05K4

Under the esteemed guidance of T.UPENDER

(Asst.Professor)



**Department of Computer Science and Engineering**

### CMR COLLEGE OF ENGINEERING & TECHNOLOGY

(An Autonomous Institution under UGC & JNTUH, Approved by AICTE, Permanently Affiliated to JNTUH, Accredited by NBA.)

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD - 501401.

### 2019- 2023

**CMR COLLEGE OF ENGINEERING & TECHNOLOGY**

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD – 501401

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**



### CERTIFICATE

This is to certify that the Major Project Phase-1 report entitled **"Fake Face Detector"** being submitted by K.Lokesh Reddy (19H51A0514), B.Vishnu Varshitha (19H51A0565), I.Sumanth (19H51A05K4) in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering** is a record of bonafide work carried out his/her under my guidance and supervision.

The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree.

**T.Upender Dr. Siva Skandha Sanagala**

**Asst,Professor Associate Professor and HOD**

**Dept. of CSE Dept. of CSE**

### ACKNOWLEDGEMENT

With great pleasure,we want to take this opportunity to express my heartfelt gratitude to all the people who helped in making this project work a grand success.

We are grateful to **T. Upender, Asst.Professor,** Department of Computer Science and Engineering for his valuable technical suggestions and guidance during the execution of this project work.

We would like to thank **Dr. Siva Skandha Sanagala,** Head of the Department of Computer Science and Engineering, CMR College of Engineering and Technology, who is the major driving forces to complete my project work successfully.

We are very grateful to **Dr. Vijaya Kumar Koppula**, Dean-Academic, CMR College of Engineering and Technology, for his constant support and motivation in carrying out the project work successfully.

We are highly indebted to **Dr. V A Narayana,** Principal, CMR College of Engineering and Technology, for giving permission to carry out this project in a successful and fruitful way.

We would like to thank the Teaching & Non- teaching staff of the Department of Computer Science and Engineering for their co-operation

We express our sincere thanks to **Mr. Ch. Gopal Reddy**, Secretary, CMR Group of Institutions, for his continuous care.

Finally, Weextend thanks to our parents who stood behind us at different stages of this Project. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project work.

K.LOKESHREDDY (19H51A0514) B.VISHNUVARSHITHA (19H51A0565)

I. SUMANTH (19H51A05K4)

**CHAPTER**

**TABLE OF CONTENTS**

**NO. TITLE PAGE NO.**

1. **INTRODUCTION** 1
   1. Problem Statement 2
   2. Research Objective 2
   3. Project Scope and Limitations 2
2. **BACKGROUND WORK** 3
   1. Face Liveness Detection Using De-focus
      1. Introduction 4
      2. Merits,Demerits, and Challenges 4
      3. Implementation 5
   2. Face Liveness Detection with Behavioural Confirmation 2.2.1.Introduction 6
      1. Merits,Demerits, and Challenges 6
      2. Implementation 6
   3. Face Detection using Viola Jones Algorithm
      1. Introduction 7
      2. Merits,Demerits, and Challenges 7
      3. Implementation 8
3. **RESULTS AND DISCUSSION**
   1. Comparison of Existing Solutions 10
   2. Data Collection 11
   3. Performance metrics 12
4. **CONCLUSION**
   1. Conclusion 15
5. **REFERENCES** 17

#### ABSTRACT

Face recognition is a widely used biometric approach. Face recognition technology has developed rapidly in recent years and it is more direct, user-friendly, and convenient compared to other methods. But face recognition systems are vulnerable to spoof attacks made by non-real faces. It is an easy way to spoof face recognition systems by facial pictures such as portrait photographs. A secure system needs liveness detection in order to guard against such spoofing. In this work, face liveness detection approaches are categorized based on the various types of techniques used for liveness detection. This categorization helps understand different spoof attack scenarios and their relation to the developed solutions. A review of the latest works regarding face liveness detection works is presented. The main aim is to provide a simple path for the future development of a novel and more secureface-liveness detection approach.

# CHAPTER 1

## INTRODUCTION

### CHAPTER 1 INTRODUCTION

#### Problem statement

Fake or manipulated photographs and videos are being generated enormously which are harder to detect by traditional means of software. Deep Learning can be employed to identify real or fake images/faces/videos efficiently. In this project, we propose an approach that takes an image as input and classifies it, using an effective system (the CNN model).The result of this project isthat the images are fed into the detector, and it will then detect whether the image that is fed into it is real or fake.

#### Research objective

Face recognition systems are becoming more useful than ever before. From face recognition on a smartphone, to face recognition for mass surveillance, face recognition systems are being utilized everywhere.However, face recognition systems are easily fooled by “spoofing” and “non-real” faces.Face recognition systems can be fooled simply by holding up a photo of a person (whether printed, on a smartphone, etc.) to the face recognition camera.In order to make face recognition systems more secure, we need to be able to detect such fake/non-real faces.

#### Project scope and limitations

Liveness detection in biometrics is the ability of a system to detect if a face (or other biometrics) is real (from a live person present at the point of capture) or fake (from a spoof artifact or lifeless body part).Liveness check uses algorithms that analyze date after they are collected from biometric scanners and readers to verify if the source is coming from a fake representation.

# CHAPTER 2

## BACKGROUND WORK

### CHAPTER 2 BACKGROUND WORK

#### Existing model – 1

**Face Liveness Detection Using De-focus**

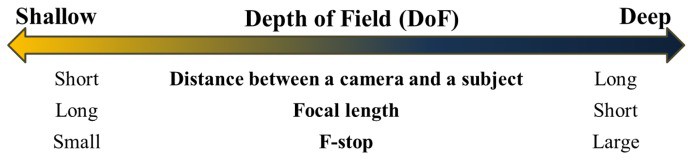
One of the main problems of applying FR technology is that the systems are especially vulnerable to attacks with spoofing faces (e.g., 2D pictures). To defend from these attacks and enhance the reliability of FR systems, many anti-spoofing approaches have been recently developed.

From two images sequentially taken at different focuses, three features, focus, power histogram, and gradient location and orientation histogram (GLOH), are extracted. Afterward, we detect forged faces through the feature-level fusion approach. For reliable performance verification, we develop two databases with a handheld digital camera and a webcam.

Current systems cannot distinguish fake faces from real faces and give approvals to forged faces. A new method to secure face identification systems from forged 2D photos.This method utilizes the camera function called variable focusing. By adjusting the focusing parameters, parts of the image that are not in focus become blurry. With this function, we can evaluate differences in the degree of focus between real faces and fake faces and use this information to detect face liveness. To evaluate our method, we organized two databases using a handheld digital camera and a webcam.

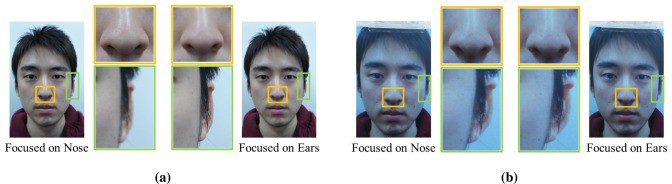
The degree of focus is determined by the depth of field (DoF), the range between the nearest and farthest objects in a given focal plane. Entities in the DoF are perceived to be sharp. In order to emphasize the effect of defocus, the DoF should be narrow.

When DoF is shallow enough to make the only partial area blurred, this method shows good results. However, at a deep DoF, the performance deteriorated.



Depending on the object or place of focus, the ear area might or might not be clear, as shown in (Figure a) Unlike real faces, 2D spoofing faces are flat. There is little difference in clarity, regardless of the focus (Figure b). We emphasize this characteristic in order to discriminate real faces from 2D faces.

When users utilize webcams and cameras embedded in cellular phones, they cannot accurately manipulate the DoF.



For evaluations, the following measures are used.

* False acceptance rate (FAR): the proportion of fake images misclassified as real.
* False rejection rate (FRR): the proportion of real images misclassified as fake.
* Total error rate (TER): the sum of FAR and FRR. *TER* = *FAR* + *FRR*
* Half total error rate (HTER): half of the TER. *HTER* = *TER*/2

In this paper, we set focus on the ears and nose and find the centers of the eyes manually. In order to apply our proposed method to security systems at low cost and with low-specification devices, like smartphones, facial components must be detected automatically.

Our experimental results show 3.29% HTER when the DoF of images is within 4 cm.

It has a limitation for being applied to camera-embedded security systems, such as smartphones, because of the manual processes to acquire the focused images and to detect facial components.

We will consider more robust countermeasures against videos and 3D attacks by analyzing textural and temporal characteristics.

#### Existing model – 2

**Face Liveness Detection with Behavioural Confirmation**

However, these approaches cause users inconvenience and rely on users' cooperation. For this reason, many researchers have attempted to develop non-intrusive methods.

Depending on the type of attack, methods can be categorized into three groups: 2D static attacks (facial photographs), 2D dynamic attacks (videos), and 3D attacks (masks).

Traditional face liveness detection methods use images that cover only the face area. However, the area around the face might include some useful features to distinguish real and fake face images. For example, replay attack images include phone edges and hand fingers. Therefore, we extended the region of interest (ROI) two times so that face images include face images and some background as well.

The dataset was split into a testing set and a training set within a proportion of 75% and 25% respectively. To train the liveness detection network, we applied the Adam optimization algorithm

For the evaluation of classification performance, the following statistical and machine learning metrics can be used: accuracy, confusion matrix, log-loss, Receiver operating characteristic (ROC) curves, precision and recall, F1-scores, and false positives per image. We evaluated our approach using F1-score: 𝐹1 = 2

∗(𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛∗𝑅𝑒𝑐𝑎𝑙𝑙 /𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛+𝑅𝑒𝑐𝑎𝑙𝑙 )

counted the total number of True Positives (TPs), False Negatives (FNs), and False Positives (FPs). Precision and Recall are calculated by the equations:

𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛 = 𝑇𝑃/ (𝑇𝑃+𝐹𝑃 )

𝑅𝑒𝑐𝑎𝑙𝑙 = 𝑇𝑃/( 𝑇𝑃+𝐹𝑁 )

To prevent biometric person authentication systems from replay and printed spoofing attacks a set of real face images and fake face images were collected and a face liveness detection model is trained on the constructed dataset.

The usage of face recognition techniques is increasing year after year because of their convenience, simplicity, and security. However, it can be easily attacked by spoofing attacks. The most widely used face spoofing attacks are prints attack, replay attack, and 3D mask attack

#### Existing model – 3 Face Detection using Viola Jones Algorithm

This algorithm is the foundation of the OpenCV library. It was developed by Paul Viola and Michael Jones in 2001. It allows the detection of images in real time.

#### How it works

There are two stages in this algorithm

1. Training
2. Detection

We’ll discuss Detection first

#### Detection

This algorithm is designed to look for **Frontal Faces.** The performance will be poor when it comes to detecting sideways, upwards, or downwards. The image is first converted into grayscale because it is easier to work and takes lesser data to process. This algorithm first finds the face on grayscale images then it finds the face location in the color image.

It outlines a rectangular box and searches for a face from the top-right corner left. It looks for haar-like features which we will be discussed later in this blog. The rectangular box right side after every step on the tile.

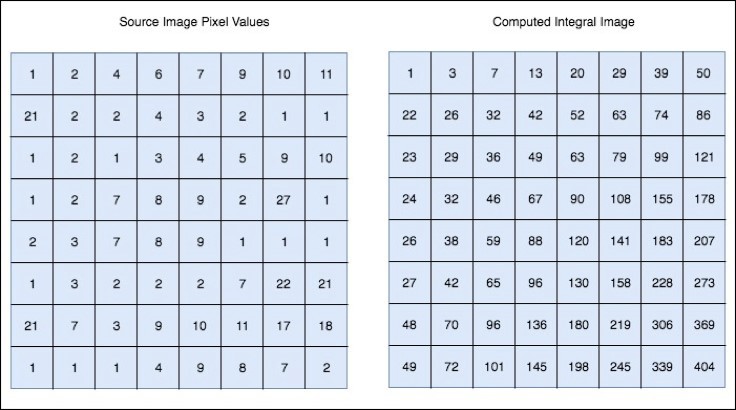
#### Limitations of the Viola-Jones Algorithm

Although, there are no major downsides to this algorithm that is why it is still very popular for recognizing faces in real-time applications. However, as we know, nothing is perfect in this world so some minor limitations of this framework are its inability to detect faces in certain scenarios like-

* If the face of a person is covered with a mask or something else, then Viola-Jones might not work perfectly in that case.
* If the faces are not oriented properly, then there is the possibility that this algorithm won't be able to detect those faces.

#### Implementation:

Each point in the integral image is a sum of the pixels above and left of the corresponding pixel in the source image. We use this because instead of doing additions for every pixel value for all features we use this to make use of a few subtractions to get the same result.



# CHAPTER 3

## RESULTS AND DISCUSSION

### CHAPTER 3 RESULTS AND DISCUSSION

#### Comparison of Existing solutions:

Here are the comparison of solutions based on half total error rate that is calculated

|  |  |
| --- | --- |
| **METHOD** | **HTER(%)** |
| Fine – tuned VGG-Face[19] | 4.30 |
| DPCNN[19] | 6.10 |
| Boulkenafet et al[20] | 2.90 |
| Boulkenafet et al[21] | 2.20 |
| Moire pattern[22] | 3.30 |
| Patch – based CNN[2] | 1.25 |
| Depth -based CNN[2] | 0.75 |
| Patch and depth CNN[2] | 0.72 |

#### Data Collection:

Liveness detection in biometrics is the ability of a system to detect if a fingerprint or face (or other biometrics) is real (from a live person present at the point of capture) or fake (from a spoof artifact or lifeless body part). It comprises a set of technical features to counter biometric spoofing attacks where a replica imitating a person’s unique biometrics (like a fingerprint mold or 3D mask made of silicone) is presented to the biometric scanner to deceive or bypass the identification and authentication steps given by the system.

Liveness check uses algorithms that analyze data - after they are collected from biometric scanners and readers - to verify if the source is coming from a fake representation. 2D static attacks are made with high-definition face pictures on flat paper, simple flat paper masks with holes.

**Presentation Attack Instruments (face)**

* 2D dynamic hacks are carried out with multiple photographs to be used in a sequence or a video replay via a low or high-quality (4K) screen. The high-definition screen is used to spoof low-resolution cameras. A video sequence with pictures can be used to answer basic challenge/response methods. The holes, in particular, allow for the eyes to blink. These 2D attacks are well documented.
* More recent 2D dynamic potential attacks can include 3D digital doubles or avatars (on a 2D screen) and deep fake puppets so named because they leverage deep learning processes.
* In 3D static attacks, impersonators use 3D prints, wax heads, or sculptures.
* IN 3D dynamic attacks, fraudsters can use masks in resin, latex, or silicone with holes for the eyes and other specific areas such as the mouth, lips, and eyes brows.

#### Performance Metrics:

1. For the evaluation of classification performance, the following statistical and machine learning metrics canbe used: accuracy, confusion matrix, log-loss, Receiver operating characteristic (ROC) curves, precision andrecall, F1-scores, and false positives.

We evaluated our approach using the F1-score:

𝐹**1 = 2** ∗**(**𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛∗𝑅𝑒𝑐𝑎𝑙𝑙**)/(**𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛**+**𝑅𝑒𝑐𝑎𝑙𝑙**)**

Where in order to calculate Precision and Recall, we applied our liveness detector on the 400-test real and fakeface images of 20 people and counted the total number of True Positives (TPs), False Negatives (FNs), andFalse Positives (FPs). Precision and Recall are calculated by the equations:

𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛 **=** 𝑇𝑃/(𝑇𝑃**+**𝐹𝑃)

𝑅𝑒𝑐𝑎𝑙𝑙 **=** 𝑇𝑃/(𝑇𝑃**+**𝐹𝑁)

#### Confusion Matrix:

In the field of Machine Learning and specifically the problem of Statistical Classification, a **confusion matrix**, also known as an error matrix, is a specific table layout that allows visualization of the performance of an algorithm, typically a supervised learning one (in unsupervised learning it is usually called a **matching matrix**). Each row of the matrix represents the instances in an actual class while each column represents the instances in a predicted class, or vice versa – both variants are found in the literature. The name stems from the fact that it makes it easy to see whether the system is confusing two classes (i.e. commonly mislabeling one as another).

**condition positive (P):** the number of real positive cases in the data

**condition negative (N):** the number of real negative cases in the data

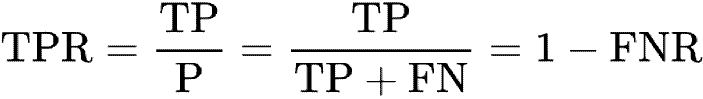
**true positive (TP**): A test result that correctly indicates the presence of a condition or characteristic

**true negative (TN):**A test result that correctly indicates the absence of a condition or characteristic

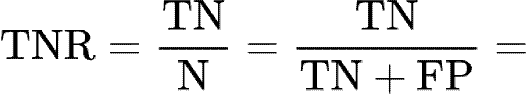
**false positive (FP):**A test result that wrongly indicates that a particular condition or attribute is present

**false negative (FN):**A test result that wrongly indicates that a particular condition or attribute is absent

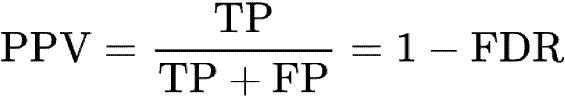
**TPR**(True Possitive Rate)



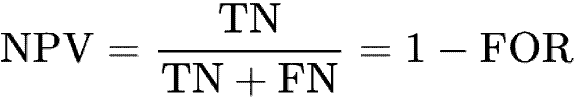
**TNR**(True Negative Rate)



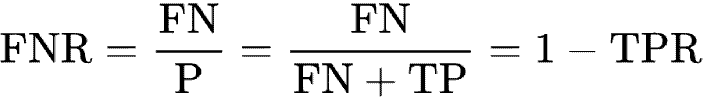
**PPV**(Positive Predictive Value)



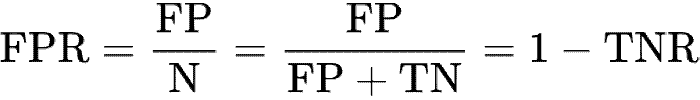
**NPV**(Negative Predictive Value)



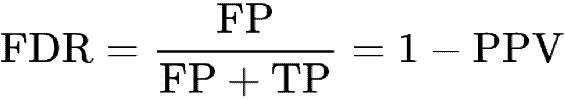
**FNR**(False Negative Rate)



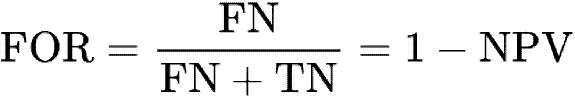
**FPR**(False Positive Rate)



**FDR**(False Discovery Rate)



**FOR**(False Omission Rate)



CHAPTER 4

## CONCLUSION

### CHAPTER 4 CONCLUSION

* At present, fake face image detection is a necessary procedure for the normal functioning of face recognition systems.
* Our project finally deals with:
  + Prevent static and dynamic 2D spoofs
  + Use images, not videos for detection
  + Required no interaction from the user
  + Detect Cell-phone
  + Detect multiple people

# CHAPTER 5

## REFERENCES

### CHAPTER 5 REFERENCES

*https://*[*www.ncbi.nlm.nih.gov/pmc/articles/PMC7514912/*](http://www.ncbi.nlm.nih.gov/pmc/articles/PMC7514912/)

https://koreascience.kr/article/JAKO202116954732832.pdf

https://[www.ncbi.nlm.nih.gov/pmc/articles/PMC4970178/](http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4970178/)

https://[www.ncbi.nlm.nih.gov/pmc/articles/PMC7597357/](http://www.ncbi.nlm.nih.gov/pmc/articles/PMC7597357/)

https://[www.ncbi.nlm.nih.gov/pmc/articles/PMC7514912/](http://www.ncbi.nlm.nih.gov/pmc/articles/PMC7514912/)

https://pyimagesearch.com/2019/03/11/liveness-detection-with-opencv/

https://towardsdatascience.com/anti-spoofing-techniques-for-face- recognition-solutions-4257c5b1dfc9

https://[www.ncbi.nlm.nih.gov/pmc/articles/PMC4327091/](http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4327091/)