**Face Recognition in the Context of Website Authentication**

**FACE DETECTION 🡪 FEATURE EXTRACTION 🡪 FACE RECOGNITION**

[PCA] Principal Component Analysis -----------------🡪 Algorithm

Dataset:

The dataset includes 13,668 pictures of 1409 persons, that is collected from internet resources such as https://www.kaggle.com/ and some volunteers’ images were

also included.

Face detection:

P. Viola & M. Jones (it is a machine learning object detection framework) is widely used for face detection because its ability to show high accuracy in detection

Facial landmark algorithm = this algorithm is used to calculate the distance between eyes , lips

Euclidean distance between each point and the other to get a vector

Classification algorithm - InceptionV3 Algorithm [9]. It is Google’s deep neural network for image recognition. It is trained on the ImageNet data set.

After the training on our dataset we got 2,047 features for each picture

Limitations –

 The model was not tested against common real-world challenges like partial occlusions (e.g., glasses, hats), different lighting, or extreme facial expressions, which are critical for face recognition in practical web-based systems.

 **Security and Privacy Considerations**: The paper does not address potential security issues related to face recognition, such as adversarial attacks, data breaches, or privacy concerns related to storing facial data. This is especially important for authentication systems where user data security is paramount.

**Face Anti-spoofing based on Convolutional Neural Networks**

**Database - The study uses the NUAA database there are 500 photos. The pictures within the database have been taken using well- known cameras and feature a decision of 640\*480 pixels for 15 subjects**

**The real class contains 5105 images (Table 1), and the spoof class has 7509.** **The study uses the 60:40 split**

**(Table 1) to split the data into 60% training and 40% for validation/ testing of the model.**

**CelebA- Spoof Dataset –**

**Quantity: CelebA-**

**Spoof has 625,537 images of 10,177 patients, a significant increase over the datasets that are currently available**

**For this experiment, a subset of the dataset was use**

**Algorithm –**

**First, the study uses face detection using Haar cascades from the OpenCV library to capture only the face from the rest of the image. Then apply data augmentation to increase the amount of data to improve the model performance. Grab Cut algorithm is used to remove the remaining noise in the images. Finally, convert all the images to black and white and resize them to 240 by 240 pixels.**

Observation - . It is noted that them Baseline CNN performance is higher than the other pipelines when benchmarked using NUAA datasets. However, benchmarked using the CelebA dataset, the baseline CNN performance decreased drastically CNN, AlexNet, and VGG16 are used for training and testing using the adopted dataset. The goal is to train the model to classify whether the provided face in a biometric system is genuine or spoof.

**Future work**

The future work for this experiment is to use a more sophisticated database to benchmark the model

**Face Anti-spoofing based on Motion Analysis**

Methods (A).

it is generally known that humans blink once every 2–4 seconds.

When there is a lot of movement in the foreground and no movement in the

background, the output is real; otherwise, the result is fake .

• Face Anti-spoofing based on Texture Analysis

Methods (B).

The approaches in this category presume that real faces’

surface qualities (e.g., pigments) differ from those of spoof

prints; thus, looking at skin texture and reflectance can aid

spoof detection

• Face Anti-spoofing based on General Image Quality

Assessment Methods (C).

a false image taken in an attack attempt will have a

different quality than a true sample obtained in the regular

operating situation

Quality variations might include colour and brightness

levels, information quantity, sharpness, structural deformities,

or natural look

• Face Anti-spoofing based on Hardware Methods (D).

* Face Anti-spoofing based on Deep learning.

Recent solutions to face anti-spoofing are CNN .Different authors have trained CNN architectures to recognise which images are genuine and faked .This technique assumes that the system would identify anything humans could not see with their naked eye.

**Anti-spoofing** **Techniques**

* Liveliness Detection Techniques
* Active liveliness Detection
* Use libraries like Dlib or OpenCV to detect facial landmarks (eyes, mouth, etc.) and track movements.
* **Action Verification – blinking eye**
* Passive liveliness Detection
* Images of printed faces or screen images often have a different texture when compared to live skin. You can analyze this using algorithms like Local Binary Patterns (LBP).
* By analyzing subtle movements
* **3D Depth Sensing**
* This involves machine learning models that estimate depth using monocular depth estimation techniques.
* Machnine Learning Techniques
* CNN
* fine-tune a pre-trained model (like MobileNetV2 or ResNet50) to perform liveness detection.
* Using Pre-trained models

**CelebA-Spoof**

* A large-scale dataset with over 625,000 images of real and spoofed faces.
* Contains multiple types of attacks (print, replay, 3D mask).
* Provides annotations for lighting conditions, spoofing mediums, and environments.

**MobileNetV2 for Anti-Spoofing)**

The pretrained **MobileNetV2** model for anti-spoofing can be structured as follows:

* **Input**: Face image or video frame.
* **Convolutional layers**: Extract features like texture, depth, and edges, which help differentiate real faces from spoofed ones.
* **Fully connected layers**: Use the extracted features for binary classification (real or spoof).
* **Output**: Binary decision (1 = real, 0 = spoofed).

Here’s how you can fine-tune it:

1. **Load Pretrained Model**: Use a MobileNetV2 model pretrained on a large dataset like **ImageNet**.
2. **Add Custom Layers**: Add fully connected layers for binary classification (real/spoof) at the end of the network.
3. **Freeze Initial Layers**: Freeze the early layers (up to a certain point) to retain the learned features and fine-tune the remaining layers.
4. **Train on Anti-Spoofing Dataset**: Fine-tune the network using an anti-spoofing dataset like **CelebA-Spoof**, **SiW**, or **CASIA-SURF**.

**FUTURE SCOPE**

**Enhanced Security with Multi-Factor Authentication (MFA)** can significantly improve the robustness of facial recognition systems by integrating biometric authentication with additional verification methods, such as OTPs or hardware tokens, reducing the chances of unauthorized access.

**Real-Time Surveillance and Monitoring** would enable continuous observation, detecting suspicious activities or spoofing attempts in real-time, making the system more proactive and responsive.

**Integration with IoT Devices** opens up possibilities for seamless authentication across a network of connected devices, such as smart locks or security cameras, creating a unified security system.

**Scalability and Cloud-Based Deployment** allows the system to handle large datasets and users, leveraging the computational power and storage of the cloud, which can dynamically scale to meet growing demands while ensuring efficient, distributed access control across global networks.

**Conclusion**

In conclusion, the work completed so far has focused on analyzing and understanding research papers related to facial recognition and anti-spoofing techniques. The detailed study of these papers has provided insights into the latest methodologies, challenges, and advancements in face recognition systems, which will guide the project's development. Moving forward, the focus will be on designing the system architecture, selecting appropriate datasets, and planning the implementation of machine learning models. By the next exam, the goal is to initiate the practical implementation, starting with data preprocessing and model selection, building a foundation for the facial authentication system with enhanced security features.