Paper 1 - Face Recognition in the Context of Website Authentication

Authors -Mohamad Amir Dliwati , Dinesh Kumar

Year – 2021

Methodology:

- The paper focuses on developing a security system for website authentication using face recognition techniques based on machine learning and deep learning.
- The process includes three main tasks:
  - Face detection using the P. Viola & M. Jones method.
  - Feature extraction using various methods, including PCA.
  - Classification using algorithms like Decision Trees, Support Vector Machines (SVM), Random Forest, and deep learning techniques such as InceptionV3.
- The InceptionV3 algorithm was specifically used to classify faces, trained on a dataset collected from various sources.

Technologies Used:

- **Machine Learning & Deep Learning**: Principal Component Analysis (PCA), SVM, Logistic Regression, InceptionV3.
- **Programming**: Python.
- **Libraries**: TensorFlow, Scikit-learn.
- **Dataset**: Collected from internet resources, including Kaggle, containing 13,668 images of 1409 individuals.

Observations:

- Logistic Regression, when used with deep learning, performed better than traditional machine learning algorithms for face recognition.
- The dataset's diversity and complexity can influence the effectiveness of the face recognition system.

Remarks:

- The study demonstrates the superiority of deep learning-based methods (like Logistic Regression with deep learning) over traditional machine learning techniques for face recognition.
- Future work aims to improve accuracy by diversifying the dataset and exploring new deep learning architectures with hyperparameter tuning.

Paper 2 - Face Anti-spoofing Based on Convolutional Neural Networks

Author - Siyamdumisa Maphisa, Duncan Coulter

Year - 2022

- ## Methodology:
  - The study proposes an anti-spoofing model for face recognition systems using three different pipelines based on Convolutional Neural Networks (CNNs):

        - A baseline CNN with hyperparameter tuning.
        - An AlexNet-based CNN.
        - A VGG16-based CNN.
    - The pipelines are trained and tested using the NUAA and CelebA datasets to identify and prevent face spoofing attacks such as photo, video, and mask attacks.
    - Performance metrics like accuracy, precision, recall, F1 score, AUC, and ROC curve were used for evaluation.
    - Preprocessing steps included face detection using Haar cascades, data augmentation, noise removal using the GrabCut algorithm, and resizing images.
- **Technologies Used**:
    - **Deep Learning**: CNN, AlexNet, VGG16.
    - **Programming**: Python using Google Colaboratory and PyCharm.
    - **Libraries**: Keras, OpenCV, Scikit-learn.
    - **Datasets**: NUAA and CelebA datasets.
- **Observations**:
    - The Baseline CNN performed better on the NUAA dataset, while its performance decreased on the more complex CelebA dataset.
    - The VGG16 model showed consistent performance across both datasets, highlighting its robustness.
    - The complexity of the dataset affects the performance of the models, indicating a need for more sophisticated datasets for future benchmarking.
- **Remarks**:
    - The VGG16 architecture was found to be the most effective in this study.
    - The study suggests using more sophisticated databases and ensemble learning techniques in the future to enhance model performance.