Face Recognition with Convolutional Neural Networks for Enhanced Security

S. Nagendrudu, A. Sai Pavan, B. Sreekanth Rao, P. Narendra, S. Khaja Moinuddin
and O. Surya Arjun

Computer science and engineering, Santhiram engineering College, NH-40, Nandyal - 518501, Andhra Pradesh, India

Keywords: Network of Convolutional Neurons, Vector Machine Support, Rate of Recognition and Training Duration.

Abstract: Convolutional neural networks (CNNs) have become an effective tool for face recognition in the domain of access control, surveillance and identity verification. They are well suited for extracting and learning large amounts of hierarchical facial features and performing accurate and robust recognition under various condition which include variation in lighting conditions, pose and occlusion. This work presents the implementation of a CNN-based face recognition system implementing deep learning architectures such as FaceNet or VGG-Face for feature extraction and classification. Incorporating the technology into biometric security frameworks, the proposed system improves authentication reliability, reduces risks of unauthorized access and provides real-time monitoring capabilities. This work represents an overview of the applications of CNNs in biometric security as well as a scalable and efficient approach to modern facial recognition systems.

1 INTRODUCTION

Recognition of faces is a biometric authentication method that uses facial features to identify or authenticate a person. The method is widely used in security, surveillance, user authentication and social media applications. The problem in face recognition is related to variations in lighting, pose, expression, occlusion and aging.

The best-known face recognition machine learning approach is convolutional neural networks (CNNs), which automatically extract hierarchical features from image data. CNNs beat other face recognition methods in learning distinguishing characteristics from unprocessed pixel data.

A crucial area of human-computer interaction, face recognition has had a significant impact on the creation of artificial intelligence. Since the concept was proposed in 1960s, there are currently about five methods to implement face recognition, such as geometrical characteristic method, methods such as neural networks, hidden Markov models, elastic graph matching, and subspace analysis. Neural network-based methods are categorized as deep learning because they can extract more complex features like corner point and plane features, while the first four methods are generally categorized as shallow learning because they can only exploit certain basic features of images; the majority of them are based on artificial experience extraction of sample features.

As usual, CNN, Deep Belief Network (DBN), and Stacked Denoising Autoencoder (SDAE) are the neural networks that are mentioned while discussing facial recognition techniques. In other words, CNN may be used to directly input images and can withstand image deformations such as rotation, translation, and scaling. More significantly, CNN is capable of automatically extracting useful facial traits. When it comes to face recognition, CNN is by far the best option. LeCun used multilayer CNN to successfully handle 2D images in 1988. As computer hardware advanced, Hinton and Krazhevsky processed the ImageNet database in 2012 using deep CNN, and the results were better than before.

In addition to face recognition, CNN is frequently used for face verification, which has shown very good results. Face recognition Sun has conducted research and created the CNN-based DeepId method for face verification. Up till 2015, they had developed three DeepId versions. They have demonstrated that their

Nagendrudu, S., Pavan, A. S., Rao, B. S., Narendra, P., Moinuddin, S. K. and Arjun, O. S.
Face Recognition with Convolutional Neural Networks for Enhanced Security.
DOI: 10.5220/0013925500004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 5*, pages 219-223
ISBN: 978-989-758-777-1

DeepId techniques produce face verification results that surpass those of human eyes. CNN can be used as a feature extractor to extract useful features in addition to being a classifier to address two- or multi-class classification issues. In this work, we extract facial features using CNN.

2 LITERATURE REVIEW

A summary of current research and outcomes relevant to a particular subject. For facial recognition utilizing Convolutional Neural Networks and Support Vector Machines, this section will encompass important studies, methodologies, and advancements. Below is a fixed structure for a literature review on this topic:

- An Introduction to Facial Recognition Definition and Significance: A summary of facial recognition technology and how it is utilized in fields like security, surveillance, and personal identification. Challenges: A discussion on challenges that facial recognition technology faces, including lighting, pose, expression, and occlusions.
- Traditional Methods of Facial Recognition Eigenfaces & Fisher faces: Early methods using LDA (linear discriminant analysis) or PCA (principal component analysis). Local Binary Patterns: Texture-based methods for face recognition. Limitations: The limitations of traditional facial recognition methods for handling complex variations and the fluctuating impacts of lighting on these technologies.
- Deep Learning for Facial Recognition Introduction to CNNs: A discussion on CNNs and how they "extract" hierarchical features from images. Key Studies: An examination of landmark studies (e.g. Deep Face-Facebook, FaceNet-Google, DeepID x2), which contributed to modern facial recognition accuracy, or the field of facial recognition in general. Architectures: A discussion on common CNN architectures in facial recognition (i.e. VGG, Inception, ResNet). Deep Learning: Generative Adversarial Networks (GANs) and autoencoders have shown promise in identifying complex spatiotemporal correlations.

3 SYSTEM MODEL DESIGN

An arrangement of system model design wherein pre-training and target training stages are included and convolutional neural networks (CNNs) and support vector machines (SVMs) are used. Here is the system model design procedure illustrated from the Figure 1:

- **Pre-training Phase:** Pre-training Dataset: This is the initial dataset used to train the CNN. It helps the model learn general features that can be useful for a variety of tasks.
- **Pre-training CNN**: The CNN is pre-trained on the pre-training dataset to learn feature representations; the problem here is to make the weights of the network minimize the loss function.
- **Weight Transfer:** After pre-training, the learned weights of the CNN are transferred into the next stage (these weights comprise the feature representations learned in the pre-training phase).
- **Target Training Phase:** Target Training Dataset is the training dataset for the task in question. It may be smaller or more specialized than the pre - training dataset.
- **Train CNN:** After initializing the CNN with pre-trained weights, the CNN is further trained on the training data set corresponding to the task to adjust the feature representations according to the task.

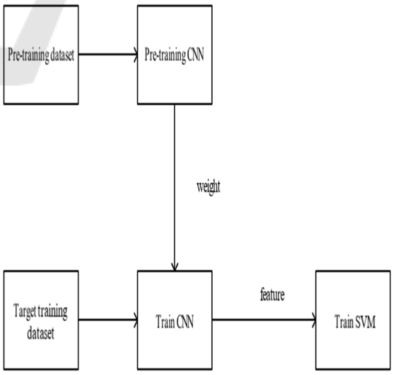

Figure 1: The whole training system framework.

- **Feature extraction:** After the CNN has been trained on the target data set its features are taken out of the CNN and these are representations of the data in the input.

- **Train SVM:** The features learned from the extracted images are then used to train a Support Vector Machine (SVM), a classifier that can be used to make predictions based on the features learned from the C.

A face recognition process using convolutional neural networks (CNNs) and support vector machines (SVMs).

- **Target Using Dataset:** Dataset gathering: gather a dataset of faces. The dataset should include different kinds of faces in different conditions (lighting, angle, expressions) so the model can generalize well.

- Preprocessing (preparing the images for normalization) usually just resizing and/or grayscale conversion or normalization of pixel values.

- **CNN (Convolutional Neural Network):** Feature extraction CNN is used to extract features from the face images. As you can see in the diagram below there are multiple layers, the convolutional, pooling and fully connected layers, learning hierarchical representations of the input images.

- The CNN training The CNN training on the face dataset. During the training, the CNN learns to identify features that are most important for distinguishing different faces.

- **Feature:** Feature vector The CNN after training outputs a feature vector for each input face image: the feature vector is a high dimensional representation of the face that contains all the necessary characteristics.

- **SVM (Support Vector Machine):** Trained SVM: The feature vectors that the CNN extracts are used to train an SVM classifier and the SVM learns to classify each of the feature vectors into different classes (with different people representing different classes). Results can be then compared against classification models to see which kind of image has better feature vectors.

- **Recognition:** Face Recognition Whenever a new face image is uploaded to the system the CNN extracts its feature vector and the SVM Classifies the image to recognize the person.

- **Lack:** How to cope with lack of data: If there is not enough training data, data augmentation (rotation, flipping, scaling) or transfer learning (using a pre-trained CNN on an already trained dataset such as ImageNet) can be used to **increase the performance of the model.**

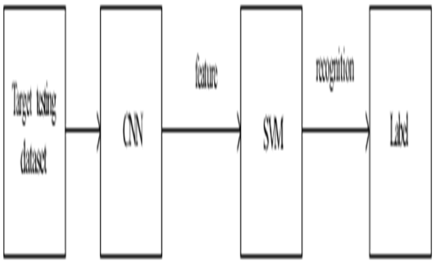

Figure 2: The testing framework.

3 METHODOLOGY

The above-mentioned techniques of face recognitions are explained in the reference. Geometrical characteristic method is one that extract geometric features like distance between key features or points of the face. Techniques such as PCA (Principal Component Analysis), LDA, etc. are used for face image dimension reduction and feature extraction through subspace analysis method. This technique uses a graph-based approach for matching facial features and allows some deformation in the face structure. The Hidden Markov Model (HMM) method is used for modelling the spatial and temporal variation in the face images. In the past, face recognition was done using simple neural networks like radial basis function (RBF) networks. Although these methods could extract more complex features but were limited due to the computational resources at that time. techniques, such as Fourier transforms and wavelet analysis, are used to identify anomalies in temporal data.

4 PROPOSED METHODOLOGY

4.1 CNN Feature Extraction

- **Pre-training:** To learn general facial traits, the CNN is pre-trained on a sizable auxiliary dataset called Casia-Webfaces.
- **Fine-tuning:** To extract more precise facial features, the pre-trained CNN is subsequently adjusted on the target dataset (FERET).

- **SVM classification:** An SVM uses the CNN's retrieved features as input for classification. To categorize facial features into distinct classes (individuals), the SVM is trained.

4.2 Methods of Optimization

Rectified Linear Units (ReLU): A CNN's activation function that boosts efficiency.
Weight Penalty: To avoid overfitting, L2 regularization is used.
Dropout: To enhance generalization, units are randomly dropped during training.
Enhancement of Data: To improve the diversity of training data, photos are flipped and added to the collection.

5 RESULTS AND DISCUSSIONS

the performance of the proposed face recognition system, which combines Convolutional Neural Networks (CNNs) for feature extraction and Support Vector Machines (SVMs) for classification. The experiments were conducted on the FERET and ORL datasets, and the results demonstrate the effectiveness of the proposed approach.

5.1 Recognition Performance of CNN

- The CNN was tested on six different configurations of the FERET dataset, with recognition rates ranging from 87.29% to 99.66%. The highest recognition rate was achieved with the "test samples135" configuration, which included images under varying lighting conditions and expressions.
- The recognition error rate was significantly low, with most configurations converging to an error rate of 0.03% after 50 epochs. This indicates that the CNN is highly effective in extracting discriminative features from face images.

5.2 CNN and SVM Recognition

Performance:

- When the features extracted by the CNN were used to train an SVM, the recognition rates improved further. For example, the recognition rate for "test samples123" increased from 98.25% (CNN alone) to 98.63% (CNN + SVM).
- The combination of CNN and SVM consistently outperformed the CNN alone across all dataset configurations, demonstrating the SVM's ability to better classify the extracted features.

5.3 Training Time

- The proposed system significantly reduced training time compared to traditional methods. For instance, the CNN + SVM approach achieved a recognition rate of 97.5% in just 28 seconds on the ORL dataset, whereas a traditional method (Global + Local Expansion ACNN) took 343 seconds to achieve a lower recognition rate of 93.30%.
- The use of pre-training with the Casia-Webfaces dataset contributed to faster convergence and reduced training time, highlighting the efficiency of the proposed method.

5.4 Data Augmentation

Data augmentation techniques, such as flipping images, were employed to increase the diversity of the training dataset. This approach helped improve the generalization ability of the model, leading to better performance on the testing dataset

6 CONCLUSIONS

In conclusion, the suggested face recognition system shows notable gains in recognition accuracy and training efficiency by combining CNNs for feature extraction and SVMs for classification. Compared to conventional techniques, the system drastically cuts down on training time while achieving high recognition rates some configurations can reach up to 99.83% accuracy. The system is suitable for real-world applications due to its resilience to changes in lighting, pose, and expression. To improve performance, future research might concentrate on investigating bigger datasets and further refining the CNN architecture. Overall, a potent method for face recognition that strikes a balance between high accuracy and computational efficiency is presented by the combination of CNNs and SVMs.

REFERENCES

Muhammad, Farooq Sumar, et al. "Key distribution scheme for preventing key reinstallation attack in wireless networks." *AIP Conference Proceedings.* Vol. 3028. No. 1. AIP Publishing, 2024.

Suman, Jani Venkata, et al. "Leveraging natural language processing in conversational AI agents to improve healthcare security." *Conversational Artificial Intelligence* (2024): 699-711.

Sumar, Mohammad Farooq, and V. Madhu Viswanathan. "A fast approach to encrypt and decrypt of video streams for secure channel transmission." *World Review of Science, Technology and Sustainable Development* 14.1 (2018): 11–28.

Muhammad, Farooq Sumar, Karthik Balasubramanian, and T. Sudhakar Babu. "A comprehensive research on video imaging techniques." *All Open Access, Bronze* (2019).

Muhammad, Farooq Sumar, and V. Madhu Viswanathan. "Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach." *The Journal of Supercomputing* 76.4 (2020): 2275–2288.

Devi, M. Sharmila, et al. "Extracting and Analyzing Features in Natural Language Processing for Deep Learning with English Language." *Journal of Research Publication and Reviews* 4.4 (2023): 497–502.

Devi, M. Sharmila, et al. "Machine Learning Based Classification and Clustering Analysis of Efficiency of Exercise Against Covid-19 Infection." *Journal of Algebraic Statistics* 13.3 (2022): 112–117.

Mandalapu, Sharmila Devi, et al. "Rainfall prediction using machine learning." *AIP Conference Proceedings.* Vol. 3028. No. 1. AIP Publishing, 2024.

Chaitanya, V. Lakshmi, et al. "Identification of traffic sign boards and voice assistance system for driving." *AIP Conference Proceedings.* Vol. 3028. No. 1. AIP Publishing, 2024.

Chaitanya, V. Lakshmi. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." *Journal of Algebraic Statistics* 13.2 (2022): 2477–2483.

Chaitanya, V. Lakshmi, and G. Vijaya Bhaskar. "Apriori vs Genetic algorithms for Identifying Frequent Item Sets." *International Journal of Innovative Research & Development* 3.6 (2014): 249–254.

Parumanacha Bhaskar, et al. "Incorporating Deep Learning Techniques to Estimate the Damage of Cars During the Accidents." *AIP Conference Proceedings.* Vol. 3028. No. 1. AIP Publishing, 2024.

Parumanacha Bhaskar, et al. "Cloud Computing Network in Remote Sensing-Based Climate Detection Using Machine Learning Algorithms." *Remote Sensing in Earth Systems Sciences* (Springer).

Parumanacha Bhaskar, et al. "Machine Learning Based Predictive Model for Closed Loop Air Filtering System." *Journal of Algebraic Statistics* 13.3 (2022): 416–423.

Paradiesi Subba Rao, "Detecting malicious Twitter bots using machine learning." *AIP Conf. Proc.* 3028, 020073 (2024), https://doi.org/10.1063/5.0212693

Paradiesi Subba Rao, "Morphed Image Detection using Structural Similarity Index Measure." *M6 Volume 48 Issue 4* (December 2024) https://powertechjournal.com

Mr. M.Amaraeswar Kumar, "Effective Feature Engineering Technique For Heart Disease Prediction With Machine Learning" in *International Journal of Engineering & Science Research*, Volume 14, Issue 2, April–2024 with ISSN 2277-2685.