Deep Learning-Based Fingerprint Classification to Secure Biometric Devices from GAN Attacks

# Abstract

This paper presents a deep learning-based approach to classify fingerprint images into 'Real' or various levels of 'Altered' fingerprints. The goal is to enhance the security of biometric systems against spoofing attacks, particularly those generated using Generative Adversarial Networks (GANs). By training a Convolutional Neural Network (CNN) on a balanced dataset, we aim to detect tampered fingerprints with high accuracy. The system achieves a peak validation accuracy of 83%, demonstrating its potential as a secure pre-processing module in fingerprint authentication systems.

# 1. Introduction

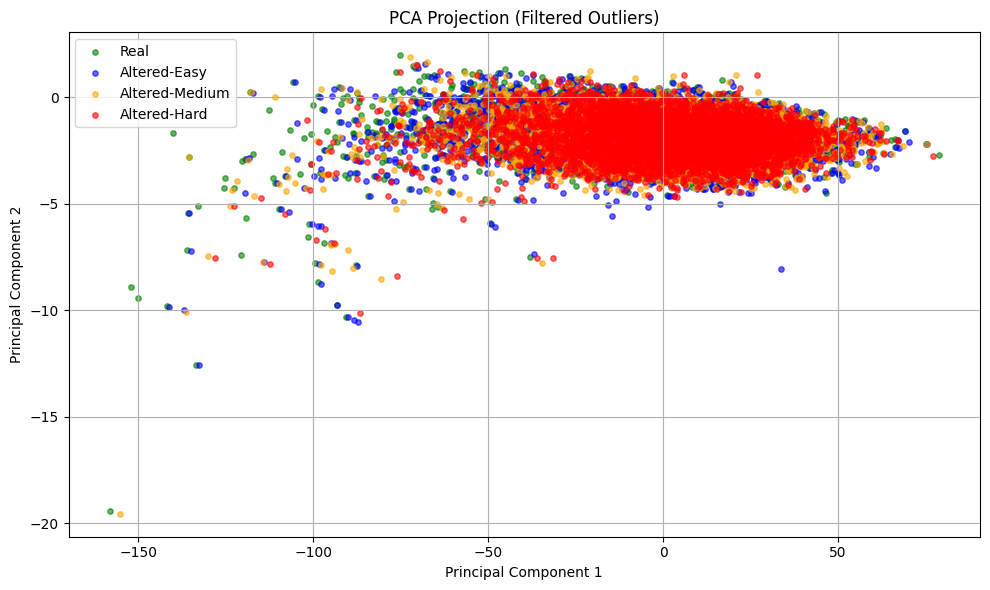
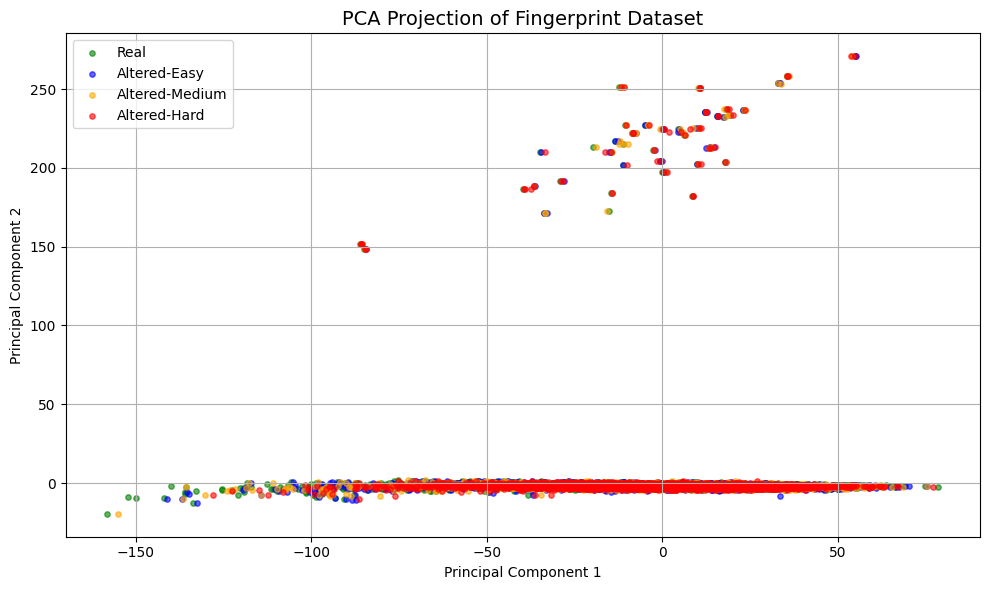
Biometric authentication systems are increasingly adopted for secure access control. However, these systems are vulnerable to spoofing attacks via generative models like GANs. In this work, we leverage a CNN-based model trained on a labeled dataset of fingerprint images, comprising both real and altered prints (categorized into easy, medium, and hard difficulty levels). The classifier acts as a safeguard by identifying manipulated or synthetic fingerprints prior to authentication, thus fortifying biometric devices.

# 2. Methodology

The proposed methodology follows a structured pipeline involving dataset preprocessing, model design, training, and evaluation. We begin by balancing the dataset using undersampling techniques to ensure fair learning. Next, we train a CNN model using PyTorch with a standard training-validation split. The model uses grayscale fingerprint images resized to 128×128 pixels and normalized to a range of -1 to 1.

## 2.1 Dataset and Preprocessing

The dataset comprises 6000 Real fingerprint images and 49,270 Altered images split into three difficulty levels: Easy (17,931), Medium (17,067), and Hard (14,272). To ensure class balance, 6000 images were randomly selected from each class. All images were converted to grayscale and resized to 128×128 pixels. The dataset was then split into training and validation sets (80:20 ratio).

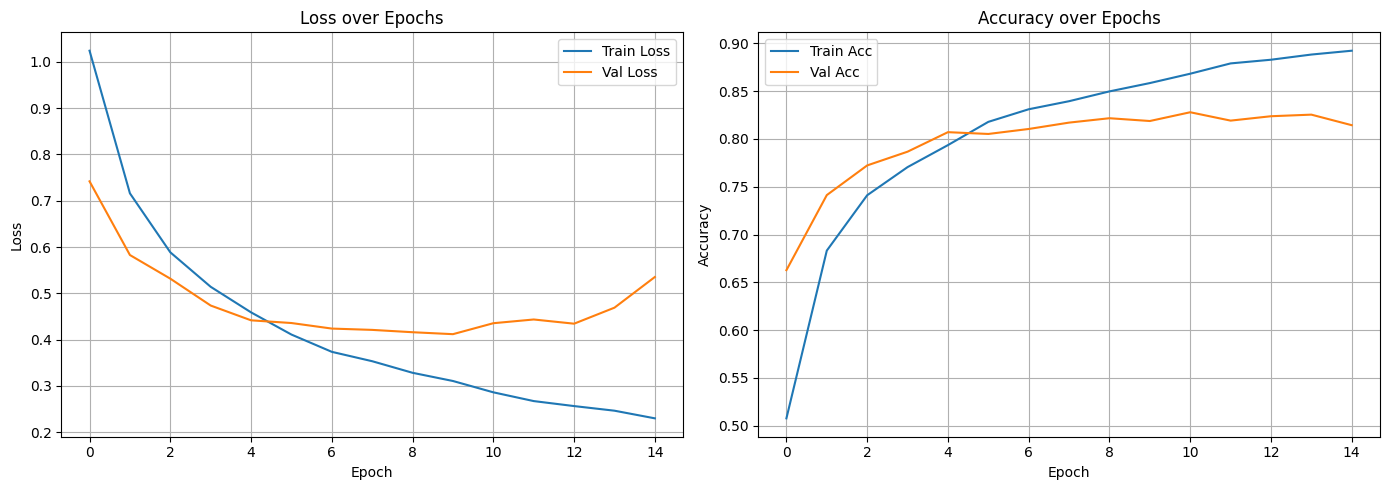


## 2.2 Model Architecture

The CNN model contains multiple convolutional, ReLU activation, batch normalization, and dropout layers followed by fully connected layers. The final output layer uses a softmax function to output probabilities for four classes. The model was trained using the Adam optimizer with cross-entropy loss over 15 epochs.

# 3. Results

The model was trained over 15 epochs and evaluated using accuracy and loss on the validation dataset. The table below summarizes the training and validation performance for each epoch.



## Training Metrics

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Epoch | Train Loss | Train Acc | Val Loss | Val Acc |
| 1 | 1.0244 | 0.5077 | 0.742 | 0.6627 |
| 2 | 0.716 | 0.6832 | 0.5827 | 0.7412 |
| 3 | 0.5885 | 0.7411 | 0.5316 | 0.7723 |
| 4 | 0.514 | 0.7705 | 0.4735 | 0.7867 |
| 5 | 0.4587 | 0.7935 | 0.4415 | 0.8071 |
| 6 | 0.4107 | 0.8179 | 0.4357 | 0.8052 |
| 7 | 0.3734 | 0.831 | 0.4237 | 0.8104 |
| 8 | 0.3531 | 0.8395 | 0.4208 | 0.8171 |
| 9 | 0.3281 | 0.8497 | 0.4158 | 0.8217 |
| 10 | 0.3103 | 0.8584 | 0.4116 | 0.8187 |
| 11 | 0.2859 | 0.8682 | 0.4353 | 0.8279 |
| 12 | 0.2669 | 0.879 | 0.4433 | 0.8192 |
| 13 | 0.2561 | 0.8829 | 0.4342 | 0.8237 |
| 14 | 0.2461 | 0.8883 | 0.4689 | 0.8254 |
| 15 | 0.2296 | 0.8923 | 0.5352 | 0.8144 |

# 4. Conclusion

The CNN-based fingerprint classifier achieved a maximum validation accuracy of 83%, demonstrating strong generalization and robustness against altered fingerprints. This model can act as a defense layer in biometric systems, effectively filtering out manipulated fingerprints potentially generated via GANs. Future work involves improving robustness with adversarial training and integrating this approach into real-world biometric authentication systems.