IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Fingerprint Spoof Detection Using Convolutional Neural Networks

[1]Shivaram A M, [2]Sharath Gowda P, [3]Shivakumar V, [4]K Prajwal, [5]Susheel Kumar S K

[1]Associate Professor, [2]Student, [3]Student,
[4]Student, [5]Student [1]Information Science and
Engineering,
[1]Sai Vidya Institute of Technology, Bangalore, Karnataka ,India

Abstract: With the growing use of authentication systems in the recent years, fingerprint spoof detection has become increasinglyimportant. In this model, we use Convolutional Neural Networks (CNN) for fingerprint spoof detection. Our system is trained on the datasets used in The Liveness Detection Competition of years 2009, 2011 and 2013, which comprise almost 50,000 real and fake fingerprints images. The CNN is pre-trained on natural images and fine-tuned with the fingerprint images, CCN with random weights, and a classical Local Binary Pattern approach. The project shows that pretrained CNNs can yield state-of-the-art results with no need for architecture or hyperparameter selection. Dataset Augmentation is used to increase the classifiers performance, not only for deep architectures but also for shallow ones. We also report good accuracy on very small training sets (400 samples) using these large pre-trained networks. The model achieves an overall rate of 97.1% of correctly classified samples - a relative improvement of 16% in test error when compared with the best previously published results.

Index Terms **-**Fingerprint recognition, Feature extraction, Convolutional neural network.

I. INTRODUCTION

The basic aim of biometrics is to automatically discriminate subjects in a reliable manner for a target application based on one or more signals derived from physical or behavioural traits, such as fingerprint, face, iris, voice, palm, or handwritten signature. Biometric technology presents several advantages over classical security methods based on either some information (PIN, Password, etc.) or physical devices (key, card etc.). However, providing to the sensor a fake physical biometric can be an easy way to overtake the systems security. Fingerprints, in particular, can be easily spoofed from common materials, such as gelatine, silicone, and wood glue. Therefore, a safe fingerprint system must correctly distinguish a spoof from an authentic finger. Different fingerprint spoof detection algorithms have been proposed, and they can be broadly divided into two approaches: hardware and software. Inthe hardware approach, a specific device is added to the sensor in order to detect particular properties of a living trait such as blood pressure, skin distortion, or odor. In the software approach, which is usedin this study, fake traits are detected once the sample has been acquired with a standard sensor.

II. LITERATURE SURVEY

The following journals and research papers were surveyed for the project. They provided information on the current state of pose estimation in general additionally other key areas of feature extraction and semantic segmentation regarding our project additionallythe various approaches taken to achieve the goal of real-time articulated pose estimation.

1. “Anti-spoofing method for fingerprint recognition using patch based deep learning machine”. The rapid threat of evil actions isone of the major challenges facing biometric frameworks today. Most vengeful entertainers use a common show attack technique

known as "satirizing" to get over biometric security measures. The main goal of a demonstration attack is to imitate legitimatelyauthorized objective casualties.

2. “Fingerprint based Gender Identification using Discrete Wavelet Transform and Gabor Filters”. Since the first moment of birth, we have tried to recognize our parents, and whenever they are around, we continuously acknowledge their presence by acknowledging their orientation—often without even realizing it. The words "biometrics" are derived from the Greek words "bio" (meaning "life") and "metric" (meaning "to quantify"). Fundamentally, during weeks 12 to 19, dermal edges (edge counts) are formed, and the ensuing distinct finger impression edge arrangement (finger impression) is fixed for all time.

3. “Fingerprint Spoofing Detection Using Machine Learning” Due to its flexibility and strength compared to conventional techniques like a secret phrase, biometric recognition systems are being used in many different ID sectors. Frameworks for biometric recognition are based on people's physiological and social attributes. Unique finger impressions are one of the most often used validation frameworks because they guarantee high ID exactness, are cost-effective, and can be used with enormousdatabases of images. These characteristics allow banks, criminology, medical services frameworks, participation, mobile phone recognizable proof, and other applications to use distinct finger impression acknowledgment frameworks. However, those structures are not immune to harmful attacks. This paper's goal is to discuss recent machine learning-based fingerprint identification systems and anti-spoofing techniques.

4. “Fingerprint generation and presentation attack detection using deep neural networks” Performance assessment is a necessary task in algorithm development. Since fingerprint recognition systems are deployed in many applications that require high accuracy, for example, banking, forensic, and national security, performance evaluation is exceptionally essential. In performance assessment, test databases have huge impacts on the outcome of an evaluation. The fingerprint generation networks are trained on 10,000 fingerprints selected from a private database. This database contains 15,150 impressions of 3,030 fingers. All fingerprints are captured by an optical sensor which produces 320×280 images with 500 dpi. All images are resized to be suitable for the network architectures. Algorithm creation requires the problem of performance evaluation.

III. METHODOLOGY

3.1 Basic Block Diagram

The fundamental block diagram in Figure 3.1.1 provides information about the relationships and connections among the different system components. As seen in the figure, an image is captured by a camera and then delivered to the system for processing. A basic block diagram for finger print detection includes several key components. It starts with an input image containing a person ina specific position.

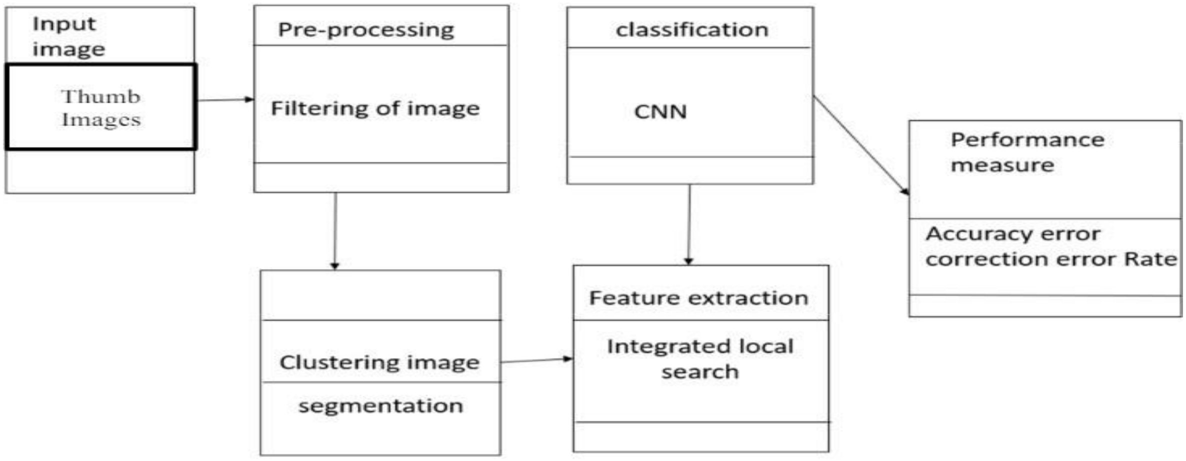

Figure 3.1.1: Block diagram

Block diagram is the boundary, which defines the system of interest in relation to the world around it. The actors, usually individualsinvolved with the system defined according to their roles. The use cases, which are the specific roles played by the actors within and around the system.

3.2 Image Collection

The dataset that we have used in this project is available publicly on the internet. The website has images of various types of fingerprints while we use the fingerprint spoofing dataset.

3.3 Image Preprocessing

Goal of pre-processing is an improvement of image data that reduces unwanted distortions and enhances some image features important for further image processing. Image pre-processing involves three main things: Gray scale conversion, Noise removal, Image enhancement

3.4 Grayscale conversion:

Grayscale image contains only brightness information. Each pixel value in grayscale image corresponds to an amount or quantity of light. The brightness graduation can be differentiated in grayscale image. Grayscale image measures only light intensity 8 bit image will have brightness variation from 0 to 255 where '0' represents black and '255' represent white. In grayscale conversion color image is converted into grayscale image shows. Grayscale images are easier and faster to process than colored images. All image processing technique are applied on grayscale image.

3.5 Noise Removal:

The objective of noise removal is to detect and remove unwanted noise from digital image. The difficulty is in deciding which features of an image are real and which are caused by noise. Noise is random variations in pixel values. We are using median filterto remove unwanted noise. Median filter is nonlinear filter, it leaves edges invariant. Median filter is implemented by sliding window of odd length. Each sample value is sorted by magnitude, the centermost value is median of sample within the window, is a filter output.

3.6 Image Enhancement:

The objective of image enhancement is to process an image to increase visibility of feature of interest. Here contrast enhancementis used to get better quality result.

IV. FLOW CHART

An input image of a fingerprinting in a specific stance is the first step in the flowchart for fingerprint detection. To identify important body parts, such joints, this image is processed using a posture detection model. To evaluate the pose, the angles between these crucial locations are computed after they have been detected.

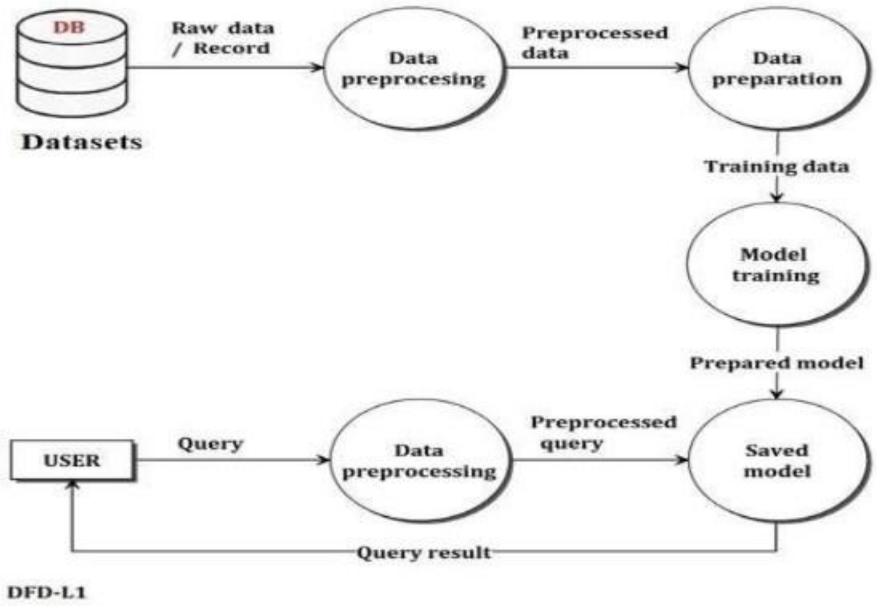

Figure 4.1: Flow chart

Subsequently, the position is evaluated to ascertain whether correction is required, based on predetermined criteria such as angles falling outside of a specific range. If the pose has to be corrected, a plan is made to change it, which can include moving some joints. After that, the correction is physically applied to the identified key spots to fix the stance. Lastly, the output image shows the adjusted pose. This flowchart shows the fundamental steps involved in identifying and adjusting human position, which may be applied to a variety of applications like animation, sports analysis, and fitness tracking.

V. USE CASE DIAGRAM

Fig 5.1 depicts the project's use case diagram-Virtual Assistance for Physical Fitness using Human Pose Estimation. this use case diagram illustrates the various interactions between the user and the system components involved in the procedure of human pose correction.

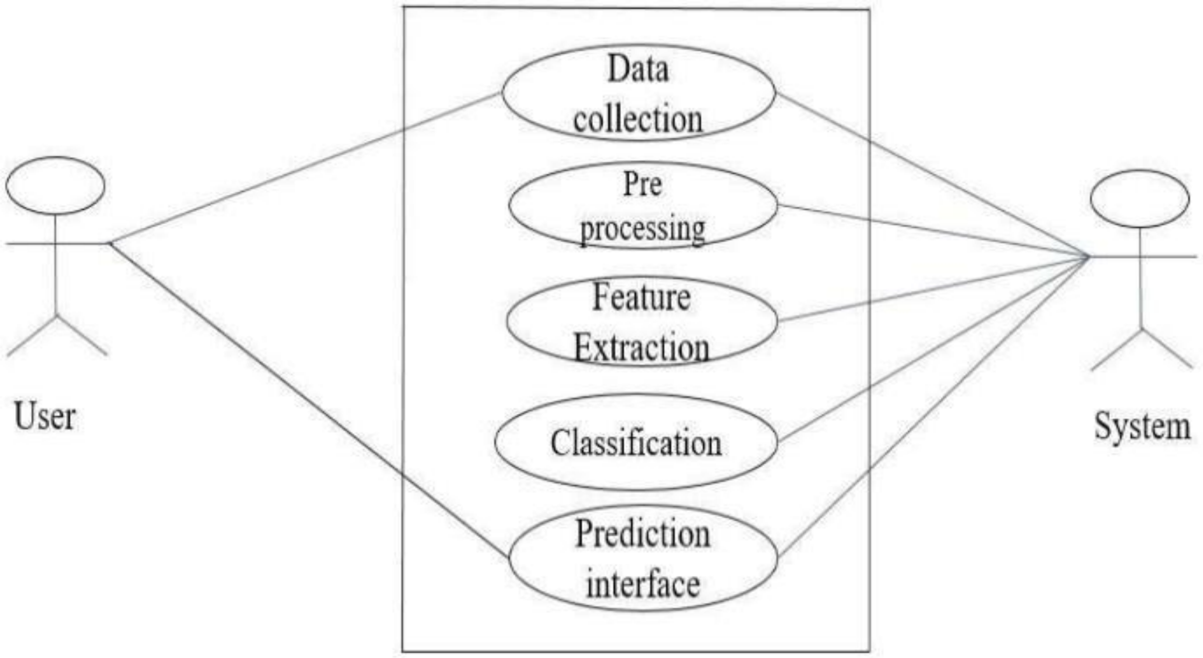

Figure 5.1: Use case diagram

Use case diagram is the boundary, which defines the system of interest in relation to the world around it. The actors, usuallyindividuals involved with the system defined according to their roles. The use cases, which are the specific roles played by the actors within and around the system.

VI. CONCLUSION

Our system will make it easier to do exercises without the need for a special trainer. Reduce injuries due to improper technique.By implementing the system into a website, and selecting the required exercise in the webpage thereby improving the accuracy of detecting the pose with much more precision which in turn helps better angle calculation for comparison. Feedback for correction will be in the form of audio through chatbot.

REFERENCES

[1] Ratha, N. K., Connell, J. H., & Bolle, R. M. (Eds.). (2007). Guide to Biometrics. Springer.

[2] Jain, A. K., Nandakumar, K., & Ross, A. (2008). Introduction to Biometrics. In Handbook of Fingerprint Recognition (2nd Ed.).Springer.

[3] Marasco, E., & Sansone, C. (2017). Fingerprint Spoofing Detection: A Review. IEEE Access, 5, 16824-16839.

[4] Derawi, M. O., Nickel, C., & Bours, P. (2012). Presentation Attack Detection for Fingerprint Recognition Systems: A Review.IET Biometrics, 1(2), 72-83..

[5] Ghiani, L., Marcialis, G. L., & Roli, F. (2017). Fingerprint Presentation Attack Detection through Quality Related Features.Pattern Recognition Letters, 88, 114-121.

[6] Galbally, J., Gomez-Barrero, M., Fierrez, J., & Ortega-Garcia, J. (2014). Fingerprint Spoofing Detection Based on QualityRelated Features. IEEE Transactions on Information Forensics and Security, 9(10), 1717-1729.