

# FINGERPRINT DETECTION USING DEEP LEARNING

**Mrs. P. Jhansi Lakshmi<sup>1</sup>, A. Ramya Sri<sup>2</sup>, D. Bhanu Sri<sup>3</sup>, M. Rishitha<sup>4</sup>, J. Naga Lakshmi<sup>5</sup>**

Assistant Professor, Department of Computer Science & Engineering, Bapatla Women's Engineering College,  
Bapatla, INDIA<sup>1</sup>

B.Tech, Computer science & Engineering, Bapatla Women's Engineering College, Bapatla, INDIA<sup>2-5</sup>

**Abstract:** The system allows users to upload a dataset of fingerprint images, preprocess them, and train a CNN model for live vs. fake fingerprint detection. An alternative model using a simplified VGG16-like structure is also implemented for comparison purposes. Once trained, the models can predict the authenticity of a given fingerprint image with associated confidence scores. During prediction, the system applies multiple image processing techniques such as grayscale conversion, HSV transformation, and Canny edge detection to visualize intermediate steps and aid understanding. The trained models and their performance metrics, including accuracy and loss, are stored and can be visualized using built-in plotting functions. Additionally, a comparative analysis of CNN and VGG16 performance is provided through a bar chart. Overall, this system serves as a practical tool for demonstrating how deep learning models can be used in biometric security applications to combat spoofing attacks and enhance fingerprint authentication systems.

**Keywords:** Convolutional Neural Network (CNN), VGG16 Model, Spoof Detection, Image processing.

## I. INTRODUCTION

Fingerprint recognition is one of the most widely adopted biometric authentication techniques due to its uniqueness, permanence, and ease of acquisition. It has become an integral component in various applications, including mobile device security, access control systems, forensic investigations, and identity verification platforms. Traditional fingerprint recognition systems rely on handcrafted features and matching algorithms, which are often sensitive to variations in fingerprint quality, noise, and environmental conditions.

In recent years, the advent of deep learning has significantly advanced the field of fingerprint recognition. Deep learning models, particularly Convolutional Neural Networks (CNNs), have demonstrated exceptional capabilities in learning hierarchical representations directly from raw fingerprint images, outperforming traditional methods in terms of accuracy and robustness. These models can automatically learn complex patterns and features from large-scale datasets, making them highly effective in various fingerprint-related tasks such as classification, matching, and spoof detection.

Moreover, with the growing concerns over security and the increasing sophistication of spoofing attacks, deep learning-based approaches have also been employed for fingerprint liveness detection, aiming to distinguish between genuine fingerprints and fake ones created using materials like silicone, gelatin, or 2D prints. Such systems enhance the security of biometric authentication by ensuring the presence of a live user during the verification process.

## II. LITERATURE SURVEY

The integration of deep learning into fingerprint recognition and detection has attracted significant research attention in recent years. Several studies have demonstrated the superiority of deep learning models, particularly Convolutional Neural Networks (CNNs), over traditional fingerprint recognition methods that rely on minutiae extraction and pattern matching.

N. N. Ratha et al. (2001) explored traditional fingerprint recognition techniques, focusing on minutiae-based matching algorithms. While effective in controlled environments, these approaches often struggled with noise, distortion, and low-quality impressions, paving the way for more robust learning-based methods.

Tang et al. (2017) introduced a deep learning-based fingerprint classification framework using a CNN architecture that learns features directly from grayscale fingerprint images. Their method achieved high accuracy on benchmark datasets, significantly reducing the dependency on handcrafted features.

Deb et al. (2020) proposed a unified deep learning architecture that combines fingerprint recognition and liveness detection in a single framework. This holistic approach enhances security while reducing system complexity and computational overhead.

LivDet Competitions (2009–2023) have served as a benchmark for evaluating fingerprint liveness detection algorithms. Deep learning-based methods have consistently ranked among the top-performing solutions, showing continuous improvement in generalization to unseen spoof materials.

### III. IMPLEMENTATION

Fingerprint detection is a technique used in biometric systems to identify or verify an individual based on their fingerprint patterns. Traditional methods rely on hand-crafted features like ridges, minutiae, or texture patterns. However, these methods often struggle with noise, low-quality images, and spoof attacks. Deep learning, especially Convolutional Neural Networks (CNNs), revolutionized this area by automating feature extraction. Instead of manually designing filters, CNNs learn them directly from data, making them more robust to variations like rotation, translation, or image quality. This is especially important in liveness detection—distinguishing real fingerprints from spoofed ones made of materials like silicone or gelatin.

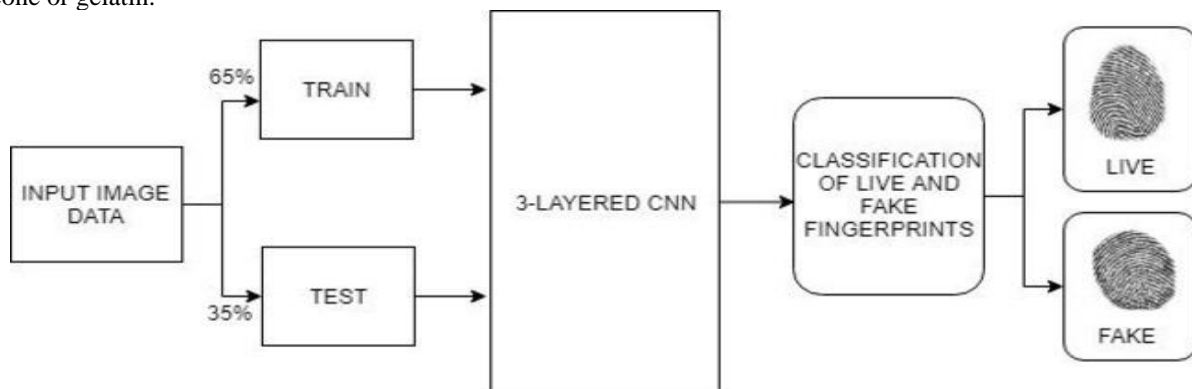


Fig.1 System Architecture

The diagram illustrates a fingerprint liveness detection system using a 3-layered Convolutional Neural Network (CNN). The input image data, consisting of both live and fake fingerprint samples, is first divided into training and testing sets. The training data is used to train the CNN model, and generate the CNN model and VGG16 model accuracy, which learns to extract and identify distinctive fingerprint features. Once trained, the model processes both training and test inputs to classify the fingerprints into two categories: live (genuine) and fake (spoofed). This approach enhances biometric security by accurately distinguishing real fingerprints from artificial ones. Finally it display the accuracy graph.

#### Role of CNN and VGG16 in Fingerprint Detection:

**CNN (Convolutional Neural Networks):** CNNs consist of layers that perform convolutions, pooling, and activation functions. These help in detecting edges, textures, and more complex features at different layers. A custom CNN can be designed from scratch for small or domain-specific datasets.

**VGG16:** This is a deep CNN architecture developed by the Visual Geometry Group at Oxford. It consists of 13 convolutional layers and 3 fully connected layers, known for its simplicity and effectiveness. In fingerprint detection, we use VGG16 as a feature extractor, especially when we have limited data, since it's already trained on millions of images.

### IV. MODULES AND LIBRARIES

**Tkinter:** Tkinter is Python's standard GUI library used to build interactive desktop applications. In a fingerprint detection system, Tkinter can be used to design the graphical user interface (GUI). This includes buttons for uploading fingerprint images, displaying results (live or fake), and initiating the detection process. It provides a user-friendly way to operate the deep learning model without needing to interact with code or command line.

**NumPy:** It is the fundamental library for numerical operations in Python. It plays a key role in deep learning projects by handling image data as arrays, manipulating pixel values, reshaping input for models, and performing mathematical computations. For fingerprint detection, NumPy is often used to process image arrays before feeding them into the CNN, and for handling model predictions.

**OpenCV (cv2):** cv2 from OpenCV is an essential module for image processing and computer vision tasks. It is used in fingerprint detection for reading images, converting them to grayscale, applying filters like Canny edge detection, and resizing them to the required input size (e.g., 224x224). It may also be used for HSV color conversion and image enhancements, which help improve model performance by emphasizing important features.

**Pickle:** It is used to serialize and save Python objects, such as trained models or preprocessing configurations. In a fingerprint detection system, after training a CNN model, you can use pickle to save the model or any preprocessing pipeline so that you can load and reuse it later for real-time predictions without retraining the model every time.

**Matplotlib, pyplot:** It is a popular plotting library used to visualize data and model performance. In this context, it can be used to plot training and validation accuracy/loss, confusion matrices, or even show the original and processed fingerprint images. It helps in understanding the model's learning curve and effectiveness in distinguishing between live and fake fingerprints.

**keras.utils.np\_utils:** This utility module from Keras contains functions like `to_categorical`, which is useful for converting class labels (like 0 and 1) into one-hot encoded vectors. One-hot encoding is essential when training CNNs for classification tasks such as distinguishing between live and fake fingerprints.

**keras.layers:** This module contains all the building blocks for CNNs, such as `Conv2D`, `MaxPooling2D`, `Flatten`, and `Dense` layers. These layers are used to build the 3-layered CNN architecture for fingerprint detection. Convolutional layers extract features, pooling layers reduce dimensionality, and dense layers perform classification.

**keras.models:** It provides the functionality to create, compile, and train deep learning models. It includes `Sequential` for building models layer by layer, and `load_model()` for loading pre-trained models. In fingerprint detection, this module helps define and manage the lifecycle of the CNN used to classify fingerprint images as live or fake.

**Adam Optimizer:** In fingerprint detection tasks, especially those involving Convolutional Neural Networks (CNNs), the dataset can be complex and feature-rich, with various patterns and textures. Adam is particularly well-suited for this because it automatically adjusts the learning rates, making the training process faster and more accurate without the need to manually tune learning rate parameters. This is useful in distinguishing subtle differences between live and fake fingerprints, which often requires precise feature learning.

**Image processing:** Fingerprint patterns are composed of fine ridges and valleys that define a person's unique biometric identity. Applying Canny edge detection to fingerprint images helps to highlight these structural features more clearly. This pre-processed image, when used as input to a deep learning model, helps the CNN focus on the most important parts of the fingerprint—improving its ability to distinguish between live (real) and fake (spoofed) fingerprints.

**TensorFlow:** In a fingerprint detection system, TensorFlow is used to build a model (like a 3-layered CNN or VGG16) that takes fingerprint images as input and learns to classify them. TensorFlow provides functionality for handling datasets, performing real-time augmentation (e.g., rotation, scaling), and compiling the model with optimizers like Adam and loss functions like categorical cross entropy. It also supports GPU acceleration, significantly reducing training time on large fingerprint datasets.

**Keras:** Fingerprint detection, especially liveness detection (distinguishing real vs. fake fingerprints), relies on learning intricate texture and ridge patterns. Keras offers the tools to easily define and train CNN models that can recognize such complex patterns. With just a few lines of code, you can build a powerful model, making Keras ideal for both beginners and experts working on biometric applications. Keras makes it easy to compile the model with optimizers like Adam and loss functions like categorical cross entropy. It also allows you to monitor metrics like accuracy during training. This is crucial for fingerprint detection, where high precision is needed to avoid misclassifying fake prints as real ones.

## V. RESULTS AND ANALYSIS

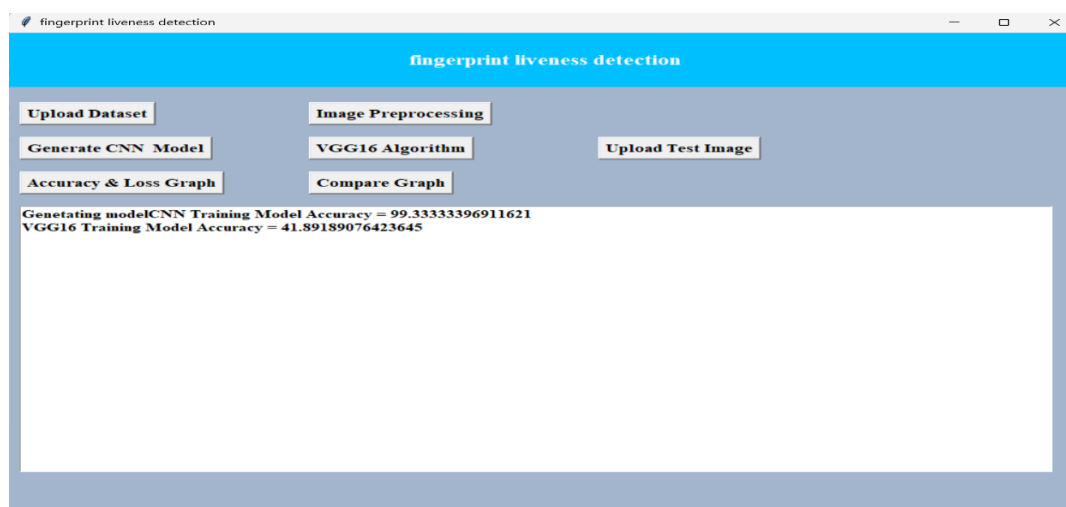


Fig.2 Upload dataset and generate CNN and VGG16 Model accuracy

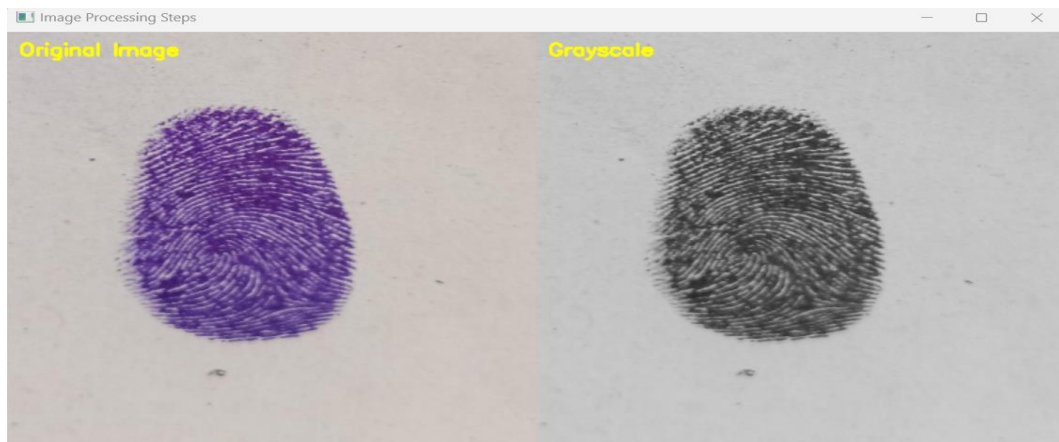


Fig.3 Image processing steps

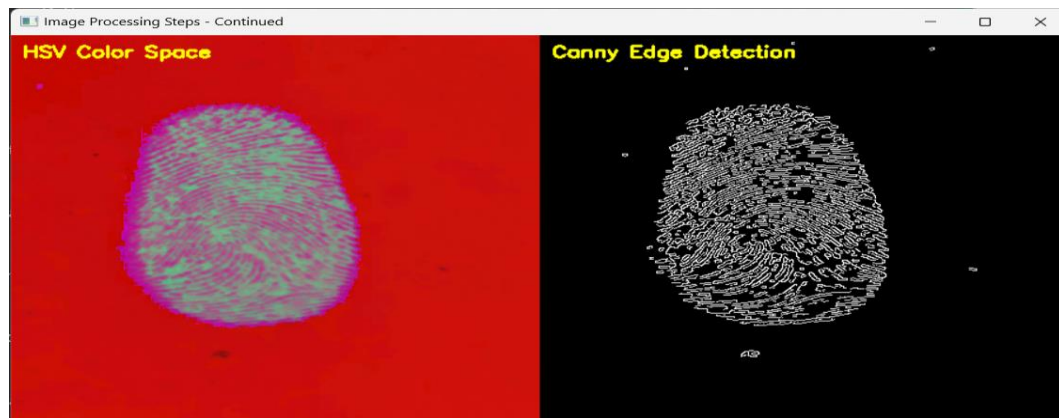


Fig.4 Filters to Classification of Image

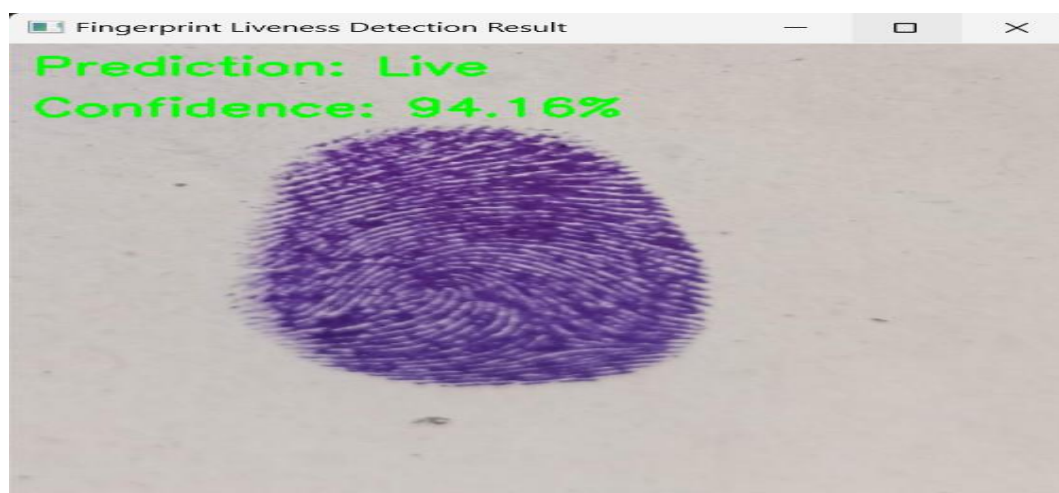


Fig.5 Fingerprint detection result

## VI. CONCLUSION AND THE FUTURE

Convolutional Neural Networks were used to detect false vs real fingerprints. Pre-trained CNNs can yield state-of-the-art results on benchmark datasets without requiring architecture or hyperparameter selection. We also showed that these models have good accuracy on very small training sets (400 samples). Additionally, no task-specific hand-engineered technique was used as in classical computer vision approaches. Despite the differences between images acquired from different sensors, we show that training a single classifier using all datasets helps to improve accuracy and robustness.



The application of deep learning in fingerprint detection presents several promising avenues for future research and development. One potential direction is the enhancement of model robustness against sophisticated spoofing attacks. As attackers develop more advanced methods using high-resolution materials and 3D printing technologies, it becomes essential to design deep learning models capable of distinguishing between increasingly realistic fake fingerprints and genuine ones. This can be achieved by incorporating multi-modal biometric data or additional sensor information, such as sweat pore activity or sub-dermal imaging.

### REFERENCES

- [1] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," *Future Generation Computer Systems*, vol. 28, no. 1, pp. 311–321, 2012.
- [2] Y. Chen, A. Jain, and S. Dass, "Fingerprint deformation for spoof detection," in *Biometric Symposium*, 2005, p. 21.
- [3] B. Tan and S. Schuckers, "Comparison of ridge-and intensity-based perspiration liveness detection methods in fingerprint scanners," in *Defense and Security Symposium*, vol. 6202. International Society for Optics and Photonics, 2006, pp. 62 020A–62 020A.
- [4] P. Coli, G. L. Marcialis, and F. Roli, "Fingerprint silicon replicas: static and dynamic features for vitality detection using an optical capture device," *International Journal of Image and Graphics*, vol. 8, no. 04, pp. 495–512, 2008.
- [5] P. D. Lapsley, J. A. Lee, D. F. Pare Jr, and N. Hoffman, "Anti-fraud biometric scanner that accurately detects blood flow," Apr. 7 1998, US Patent 5,737,439.
- [6] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers, "Livdet 2015 fingerprint liveness detection competition 2015," in *Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on*. IEEE, month 2015, pp. 1–6.
- [7] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger de- tection by skin distortion analysis," *Information Forensics and Security, IEEE Transactions on*, vol. 1, no. 3, pp. 360–373, 2006.
- [8] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in *Advances in Biometrics*. Springer, Berlin, Heidelberg, 2005, pp. 265–272.

### BIOGRAPHY



**P. Jhansi Lakshmi** working as Assistant Professor in Department of CSE, Bapatla Women's Engineering College. She completed her M. Tech in Computer Science Engineering from Gitam University, Visakhapatnam.



**A. Ramya Sri** B. Tech with Specialization of Computer Science and Engineering in Bapatla Women's Engineering College, Bapatla.



**D. Bhanu Sri** B. Tech with Specialization of Computer Science and Engineering in Bapatla Women's Engineering College, Bapatla.



**M. Rishitha** B. Tech with Specialization of Computer Science and Engineering in Bapatla Women's Engineering College, Bapatla.



**J. Naga Lakshmi** B. Tech with Specialization of Computer Science and Engineering in Bapatla Women's Engineering College, Bapatla.