

# Liveness Detection of Anti-spoofing Fingerprints using Machine learning

Mrs.Prabha S Naik<sup>1</sup>, Basavarajeshwari H<sup>2</sup>, Madan N.M<sup>3</sup>, Harshitha T.R<sup>4</sup>, Madanraj N<sup>5</sup>  
<sup>1,2,3,4,5</sup>Computer Science and Engineering M.S. Engineering College Bangalore, Karnataka

**Abstract—** With the growing use of biometric authentication systems in the recent years, spoof fingerprint detection has become increasingly important. In this study, we use Convolutional Neural Networks (CNN) for fingerprint liveness detection. Our system is evaluated 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. We compare four different models: two CNNs pre-trained on natural images and fine-tuned with the fingerprint images, CCN with random weights, and a classical Local Binary Pattern approach. We show that pre-trained 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. Our best 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. This model won the first prize in the Fingerprint Liveness Detection Competition (LivDet) 2015 with an overall accuracy of 95.5%.

## 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 liveness detection

algorithms have been proposed, and they can be broadly divided into two approaches: hardware and software. In the 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 used in this study, fake traits are detected once the sample has been acquired with a standard sensor.

Nowadays, biometric recognition systems have used in a variety of identification sectors, due to their convenience and robustness compared with conventional techniques such as a password. Biometrics recognition systems rely on the physiological and behavioural attributes of individuals. The fingerprint is one of the most frequently used authentication systems since they guarantee high identification accuracy, cost- effective, and can be applied to huge datasets of images. Those characteristics make fingerprint recognition systems deployed in many applications, such as attendance, smartphone identification, forensics, health-care systems, banks, etc. However, those systems are not aloof from malicious attacks

## EXISTING SYSTEM

- Authentication technologies are used in security awareness in many places, with increasing financial activities.
- Traditional authentication such as passwords, personal identification numbers, smart cards were largely unable to meet convenience, reliability and security requirements in a wide variety of applications.

## PROPOSED SYSTEM

- Fingerprint spoofing detection and identification have followed traditional CNN model. Basically, a CNN model requires a huge dataset so as to learn from the training dataset.

- The fingerprint database used in the proposed work which has fingerprint images of just many individuals. Hence, the proposed work has been implemented based on transfer learning model.
- The transfer learning is an approach where the model is pre-trained on a huge database of images and the knowledge gained by the model through those images is used for training another set of images. One of the major transfer learning models is ResNet-50.
- CNN's network design consists of multiple layers mentioned below. Convolutional neural networks are made up of different layers between the layers of input and output.
- These layers, known as the hidden layers, consist mainly of the Convolutional layer, Pooling layer and Fully connected layer. In our model, we used Convolutional layer and pooling layer.

## II. SYSTEM ARCHITECTURE

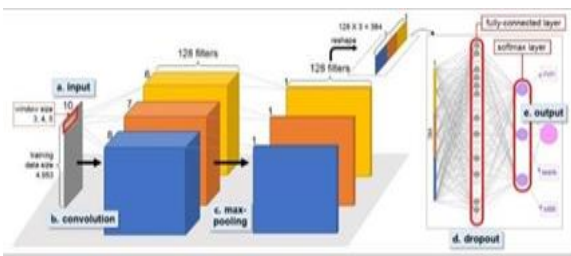


Fig 2.1: System Architecture

A Deep-CNN is type of a DNN consists of multiple hidden layers such as convolutional layer, RELU layer, Pooling layer and fully connected a normalized layer. CNN shares weights in the convolutional layer reducing the memory footprint and increases the performance of the network. The important features of CNN lie with the 3D volumes of neurons, local connectivity and shared weights

A feature map is produced by convolution layer through the convolution of different subregions of the input image with a learned kernel.

## III.METHODOLOGY

- The execution of this project as well as the compilation of the project report has been possible owing to the understanding and co-operation and help extended by numerous people.
- Though it is presumptuous on our part to assume that

a few grateful words are enough to describe the magnitude if help that has been extended to us, we shall attempt to express our gratitude to some of these eminent and knowledgeable persons.

## IV. IMPLEMENTATION

Implementation is the process of converting a new system design into an operational one. It is the key stage in achieving a successful new system. It must therefore be carefully planned and controlled. The implementation of a system is done after the development effort is completed.

### Module specification:

Module Specification is the way to improve the structural design by breaking down the system into modules and solving it as an independent task. By doing so the complexity is reduced and the modules can be tested independently. The number of modules for our model is three, namely pre- processing, identification, feature extraction and detection. So each phase signify the functionalities provided by the proposed system. In the data pre-processing phase noise removal using median filtering is done.

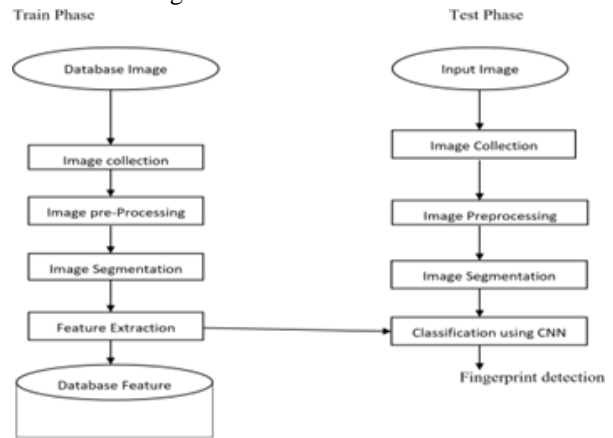


Fig 5.1.1 Module specification

The System design mainly consists of

- Image Collection
- Image Preprocessing
- Image Segmentation
- Feature Extraction
- Training
- Classification

### Image Collection:

The dataset that we have used in this project is available publicly on the internet ([https:// www. kaggle. com](https://www.kaggle.com)).

com/datasets). The website has images of various types of fingerprints while we use the fingerprint sooping dataset

#### 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 Segmentation

The next step after image pre-processing was to segment the cervical tumor area from the surrounding images. A black and white image was produced with its contrast adjusted to provide better segmentation.

#### Feature Extraction

Feature extraction plays an important role in extracting information present in given image. are using GLCM for texture image analysis. GLCM is used to capture spatial dependency between image pixels. GLCM works on gray level image matrix to capture most common feature such as contrast, entropy, energy, homogeneity

#### Training

Training dataset was created from images of known Cancer stages. Classifiers are trained on the created training dataset. Testing dataset is placed in a temporary folder. Predicted results from the test case, Plots classifiers graphs and add feature-sets to test case file, to make image processing models more accurate

#### Classification

The binary classifier which makes use of the hyper-plane which is also called as the decision boundary between two of the classes is called as Convolution Neural Network. Some of the problems are pattern recognition like texture classification makes use of CNN. Mapping of non-linear input data to the linear data provides good classification in high dimensional space in CNN. The marginal distance is maximized between different classes by CNN. Different Kernels are used to divide the classes. CNN is bas binarclassifier which determines hyper plane in dividing two classes.

### V. SYSTEM TESTING

Testing is the process of evaluating a system or its component(s) with the intent to find whether it satisfies

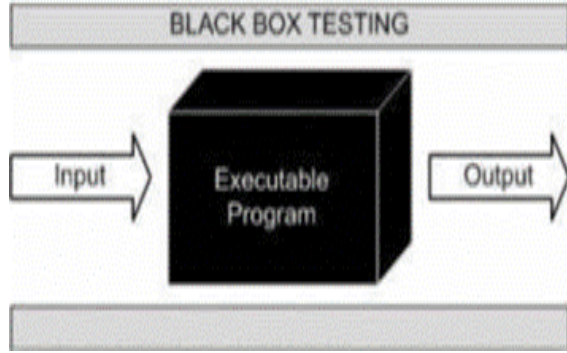
the specified requirements or not. Testing is executing a system to identify any gaps, errors, or missing requirements in contrary to the actual requirements. System testing of a software or hardware is a testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. System testing fails within the scope of black-box testing, and such, should require no knowledge of the inner design of the code or logic. As a rule, system testing takes, as its input, of all the 'integrated' software components that have passed integration testing and the software system itself integrated with any applicable software systems. The purpose of integration testing is to detect any inconsistencies between the software units that are integrated together. System testing is a more limited type of testing. It seeks to detect defects both within the inter- assemblages and within the system. System testing is performed on the entire system in the context of a Functional Requirement Specification (FRS) and/or a System Requirement Specification (SRS). System testing tests not only the design, but also the behavior and even the believed expectation of the customer. It is also intended to test up to and beyond the bounds defined in the software / hardware requirement specification. Before applying methods to design effective test cases, a software engineer must understand the basic principle that guides software testing. All the tests should be traceable to customer requirements

#### Types of testing

Software testing methods and traditionally divided into two: white-box and black-box testing. These two approaches are used to describe the point of view that a test engineer takes when designing test cases.

White-box testing: also known as clear box testing, glass box testing, transparent box testing and structural testing, by seeing the source code) tests internal structures or workings of a program, as opposed to the functionality exposed to the end-user.









Black box testing: The technique of testing without having any knowledge of the interior workings of the application is called black-box testing. The tester is oblivious to the system architecture and does not have access to the source code



5.1 Black –boxing testing

### VI.PERFORMANCE EVALUATION

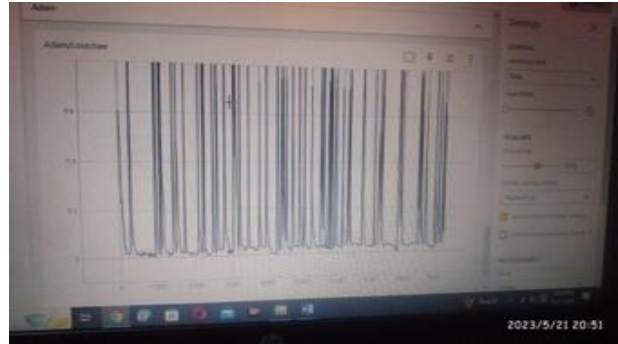
The performance evaluation in biometrics allows the developer to rapidly grasp the status of the current technology, as well as, to shorten the completion of commercialization. Also, this provides the reliability of the product to users and establishes a wide market. Especially for fingerprint recognition, the algorithm developers as well as users require objective and quantitative evaluation processes because the fingerprint recognition is the most unique technology in biometrics in the sense of various kinds of fingerprint sensors are being commercialized. The purpose of this research is to propose the process of performance evaluation, evaluation indices, and the presentation of result for fingerprint sensor modules. Four commercial fingerprint sensor modules have been tested and evaluated by comparing the quantitative measure of fingerprint image quality affected by environmental factors (temperature and humidity) and user factors (skin humidity and pressure). The result of this research is expected to be utilized for improvement of algorithms adapting to different fingerprint sensor modules.

	Optical	Capacitive	Tactile	Thermal
Company	A	B	C	D
DPI	500	250	403	500
Liveness Detection	X	O	X	X
Sensor				
Image				

6.1 Test sensor modules



6.2 Model Accuracy

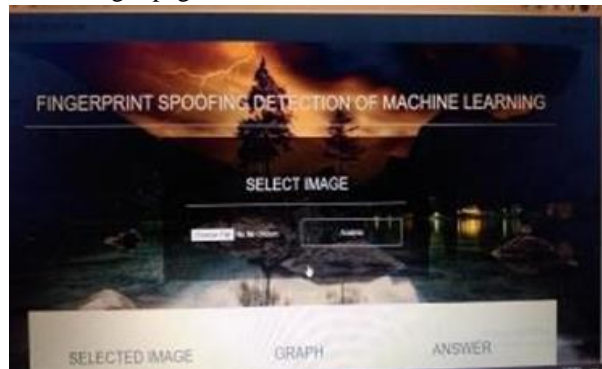


6.3 Model loss

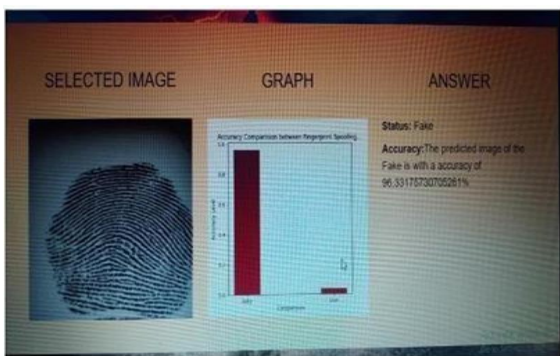
### VII. SCREENSHOTS AND RESULTS



7.1 User login page



7.2 Home page



7.3 Resulted graph

Forensics and Security, vol. 12, no. 9, pp. 2067–2077, 2017.

- [10] J. J. Engelsma, S. S. Arora, A. K. Jain, and N. G. Paulter, “Universal 3D wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1564–1578, 2018.

## REFERENCE

- [1] R. Gajawada, A. Popli, T. Chugh, A. Nambodiri, and A. K. Jain, “Universal Material Translator: Towards Spoof Fingerprint Generalization,” in *IEEE International Conference on Biometrics (ICB)*, 2019.
- [2] T. Chugh, K. Cao, and A. K. Jain, “Fingerprint Spoof Buster: Use of Minutiae-centered Patches,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2190–2202, 2018.
- [3] S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, Eds., “Handbook of Biometric Anti-Spoofing: Presentation Attack Detection”, 2nd ed. Springer, 2019.
- [4] ODNI, IARPA, “IARPA-BAA-16-04 (Thor),” <https://www.iarpa.gov/index.php/research-programs/odin/odin-baa>, 2016.
- [5] International Standards Organization, “ISO/IEC 30107-1:2016, Information Technology—Biometric Presentation Attack Detection—Part 1: Framework,” <https://www.iso.org/standard/53227.html>, 2016.
- [6] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of artificial gummy fingers on fingerprint systems,” in *Proc. SPIE*, vol. 4677, 2012, pp. 275–289.
- [7] K. Cao and A. K. Jain, “Hacking mobile phones using 2D Printed Fingerprints,” MSU Tech. report, MSU-CSE-16-2 <https://www.youtube.com/watch?v=fZJI BrMZXU>, 2016.
- [8] S. S. Arora, K. Cao, A. K. Jain, and N. G. Paulter, “Design and Fabrication of 3D Fingerprint Targets,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2284–2297, 2016.
- [9] S. S. Arora, A. K. Jain, and N. G. Paulter, “Gold Fingers: 3D Targets for Evaluating Capacitive Readers,” *IEEE Transactions on Information*