FINGERPRINT AUTHENTICATION SYSTEM USING CONVOLUTION NEURAL NETWORKS WITH DATA AUGMENTATION

Mrs. Geetha N, Sandhya M , Sruthi Murali , Subha Sri Sangari G , Karthikeyan

Dept of Information Technology, Coimbatore Institution of Technology, Coimbatore

ABSTRACT

Biometrics technology determines the correct identity of a person by extracting human biological or behavioral characteristics data. As the possibility of hacking increases with the development of IT technology, interests in biometrics and authentication technology is greatly increasing currently. The most popular authentication technology is fingerprint recognition. In the first step, the inputted fingerprint image is subjected to a complicated preprocessing stage, and the fingerprint image is then classified. In the second step the feature points of the classified fingerprints are extracted and compared with the fingerprint feature points stored in a database. In this paper, we propose the use of a CNN model which extracts the pattern found within the local region of the inputted image, by convolving a template or filter over the inputted image pixels and outputting this as a feature map. In the third step, classification is done. The images are predicted accordingly as Live and Fake images and finally outputted in the CSV File Format. Finally Data augmentation is performed by artificially creating modified samples from the original ones. It is expected that the classifier will become more robust to small variations that may be found during the testing phase.

1. INTRODUCTION

1.1. MACHINE LEARNING:

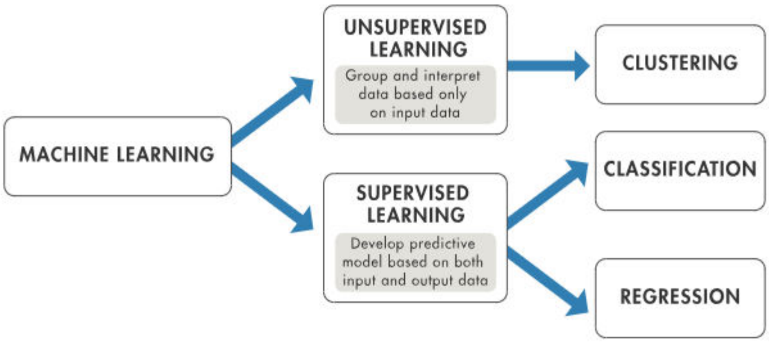
Machine learning is a subset of artificial intelligence in the field of computer science that often uses statistical techniques to give computers the ability to "learn" with data. Machine learning (ML) is a category of algorithm that allows software applications to become more accurate in predicting outcomes without being explicitly programmed. The basic premise of machine learning is to build algorithms that can receive input data and use statistical analysis to predict an output while updating outputs as new data becomes available.

Any technology user today has benefitted from machine learning: Facial recognition technology allows social media platforms to help users tag and share photos of friends. Optical character recognition (OCR) technology converts images of text into movable type. Recommendation engines, powered by machine learning, suggest what movies or television shows to watch next based on user preferences. Self-driving cars that rely on machine learning to navigate may soon be available to consumers.

1.2. MACHINE LEARNING METHODS:

In machine learning, tasks are generally classified into broad categories. These categories are based on how learning is received or how feedback on the learning is given to the system developed. Two of the most widely adopted machine learning methods:

- Supervised Learning.
- Unsupervised Learning.


MACHINE LEARNING
UNSUPERVISED LEARNING
Group and interpret data based only on input data
SUPERVISED LEARNING
Develop predictive model based on both input and output data
CLUSTERING
CLASSIFICATION
REGRESSION

1.2.1. Supervised Learning:

In supervised learning, the computer is provided with example inputs that are labeled with their desired outputs. The purpose of this method is for the algorithm to be able to "learn" by comparing its actual output with the "taught" outputs to find errors, and modify the model accordingly. Supervised learning therefore uses patterns to predict label values on additional unlabeled data.

Example : With supervised learning, an algorithm may be fed data with images of sharks labeled as fish and images of oceans labeled as water. By being trained on this data, the supervised learning algorithm should be able to later identify unlabeled shark images as fish and unlabeled ocean images as water.

Supervised learning uses classification and regression techniques to develop predictive models.

1. **Classification techniques** predict discrete responses.Classification models classify input data into categories. Typical applications include medical imaging, speech recognition, and credit scoring. Use classification if your data can be tagged, categorized, or separated into specific groups or classes. For example, applications for hand-writing recognition use classification to recognize letters and numbers. Common

algorithms for performing classification include SVM, boosted and bagged decision trees, k-nearest neighbor, Naïve Bayes, discriminant analysis, logistic regression, and neural networks.

2. **Regression techniques** predict continuous responses—for example, changes in temperature or fluctuations in power demand. Typical applications include electricity load forecasting and algorithmic trading.Common regression algorithms include linear model, non-linear model, regularization, step-wise regression, boosted and bagged decision trees,neural networks,

Advantages:

- Supervised learning is to use historical data to predict statistically likely future events.
- It may use historical stock market information to anticipate upcoming fluctuations, or be employed to filter out spam emails.

1.2.2. Unsupervised Learning:

In unsupervised learning, data is unlabeled, so the learning algorithm is left to find commonalities among its input data. As unlabeled data are more abundant than labeled data, machine learning methods that facilitate unsupervised learning are particularly valuable.The goal of unsupervised learning may be as straightforward as discovering hidden patterns within a dataset, but it may also have a goal of feature learning, which allows the computational machine to automatically discover the representations that are needed to classify raw data.

Unsupervised learning is commonly used for transactional data. You may have a large dataset of customers and their purchases, but as a human you will likely not be able to make sense of what similar attributes can be drawn from customer profiles and their types of purchases. With this data fed into an unsupervised learning algorithm, it may be determined that women of a certain age range who buy unscented soaps are likely to be allergetic, and therefore a marketing campaign related to allergy can be targeted to this audience in order to increase their number of purchases.

Unsupervised learning uses clustering techniques.

Clustering is the most common unsupervised learning technique. It is used for exploratory data analysis to find hidden patterns or groupings in data. Applications for cluster analysis include gene sequence analysis, market research, and object recognition.

Common algorithms for performing clustering include k-means and k-medoids, hierarchical clustering, Gaussian mixture models, hidden Markov models, self-organizing maps, fuzzy c-means clustering, and subtractive clustering.

Advantages:

- Without being told a "correct" answer, unsupervised learning methods can look at complex data that is more expansive and seemingly unrelated in order to organize it in potentially meaningful ways.

- Unsupervised learning is often used for anomaly detection including for fraudulent credit card purchases, and recommender systems that recommend what products to buy next.

1.3. CONVOLUTION NEURAL NETWORKS IN MACHINE LEARNING:

Convolutional Neural Networks[2] expect and preserve the spatial relationship between pixels by learning internal feature representations using small squares of input data. Feature are learned and used across the whole image, allowing for the objects in the images to be shifted or translated in the scene and still detectable by the network.

Building Blocks of Convolutional Neural Networks

There are three types of layers in a Convolutional Neural Network:

- Convolutional Layers.
- Pooling Layers.
- Fully-Connected Layers.

1.Convolutional Layers:

Convolutional layers are comprised of filters and feature maps.

Filters

The filters are the "neurons" of the layer. The have input weights and output a value. The input size is a fixed square called a patch or a receptive field. If the convolutional layer is an input layer, then the input patch will be pixel values. If the deeper in the network architecture, then the convolutional layer will take input from a feature map from the previous layer.

Feature Maps

The feature map is the output of one filter applied to the previous layer.A given filter is drawn across the entire previous layer, moved one pixel at a time. Each position results in an activation of the neuron and the output is collected in the feature map. You can see that if the receptive field is moved one pixel from activation to activation, then the field will overlap with the previous activation by (field width – 1) input values.

2.Pooling Layers

The pooling layers down-sample the previous layers feature map. Pooling layers follow a sequence of one or more convolutional layers and are intended to consolidate the features learned and expressed in the previous layers feature map. As such, pooling may be consider a technique to compress or generalize feature representations and generally reduce the overfitting of the training data by the model. They too have a receptive field, often much smaller than the convolutional layer. Also, the stride or number of inputs that the receptive field is moved for each activation is often equal to the size of the receptive field to avoid any overlap. Pooling layers are often very simple, taking the average or the maximum of the input value in order to create its own feature map.

3. Fully Connected Layers

Fully connected layers are the normal flat feed-forward neural network layer.These layers may have a non-linear activation function or a softmax activation in order to output probabilities of class predictions. Fully connected layers are used at the end of the network after feature extraction and consolidation has been performed by the convolutional and pooling layers. They are used to create final non-linear combinations of features and for making predictions by the network.

1.4. FINGERPRINT AUTHENTICATION SYSTEM:

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. a safe fingerprint system must correctly distinguish a spoof from an authentic finger. Approaches can be broadly classified into two categories: hardware and software. In the software approach, which is used in this study, fake traits are detected once the sample has been acquired with a standard sensor. Biometrics technology determines the correct identity of a person by extracting human biological or behavioral characteristics data. As the possibility of hacking increases with the development of IT technology, interests in biometrics and authentication technology is greatly increasing currently. The most popular authentication technology is fingerprint recognition. In the first step, the inputted fingerprint image is subjected to a complicated preprocessing stage, and the fingerprint image is then classified. In the second step the feature points of the classified fingerprints are extracted and compared with the fingerprint feature points stored in a database. In this paper, we propose the use of a CNN model which extracts the pattern found within the local region of the inputted image, by

convolving a template or filter over the inputted image pixels and outputting this as a feature map.In thethird step, classification is done.Finally Data augmentation is performed by artificially creating modified samples from the original ones. It is expected that the classifier will become more robust to small variations that may be found during the testing phase.

Advantages of the Existing Fingerprint Liveness Detection System is its

Scalability : Biometrics systems can be quite flexible and easily scalable. You can use higher versions of sensors and security systems based on your requirements.

Versatility:There are different types of biometrics scanners available today.

User Friendly System.

Disadvantages of the Existing Fingerprint Liveness Detection System is it increases the timing, measurement and complex algorithms, decrease acceptability. Can be fooled by artificial fingerprint and stolen password. Difficulty of distinguishing between the challenge-respond person and true owner.

2.LITERATURE SURVEY

2. 1. FAKE FINGERPRINT DETECTION BY SKIN DISTORTION ANALYSIS [1]

Attacking fingerprint-based biometric systems by presenting fake fingers at the sensor could be a serious threat for unattended applications. This work introduces a new approach for discriminating fake fingers from real ones, based on the analysis of skin distortion. The user is required to place a finger onto the scanner surface and to apply some pressure while rotating the finger in either clockwise or counter-clockwise direction (this particular movement has bee n chosen after some initial tests, as it seems quite easy for the user and it produces the right amount of distortion). A sequence of frames is acquired at a high frame rate during the movement and analyzed to extract relevant features related to skin distortion. Novel techniques for extracting, encoding and comparing skin distortion information are formally defined and systematically evaluated over a test set of real and fake fingers. The experimental results indicate the new approach to be a very promising technique for making fingerprint recognition systems more robust against fake-finger-based spoofing attempts.

This paper has an advantage of not requiring expensive additional hardware, provided that the fingerprint scanner is able to acquire images at a proper frame rate. The future works could be implementation and evaluation of alternative alignment techniques for the Distortion Code sequences; Experimentation on a larger user population.

2.2. IMAGE CLASSIFICATION BASED ON THE BOOST CONVOLUTION NETWORK[2]

Convolutional neural networks (CNNs), which are composed of multiple processing layers to learn the representations of data with multiple abstract levels, are the most successful machine learning models in recent years. However, these models can have millions of parameters and many layers, which are difficult to train, and sometimes several days or weeks are required to tune the parameters. Within this paper, we present the usage of a trained deep convolutional neural network model to extract the features of the images, and then, used the AdaBoost algorithm to assemble the Softmax classifiers into recognizable images. Compared with the original Boosting algorithm, AdaBoost replaces random sampling with weighted sampling to train data. In this way, focus is placed on training data that are difficult to process, which renders training more targeted. This method resulted in a 3% increase of accuracy of the trained CNN models, and dramatically reduced the retraining time cost, and thus, it has good application prospects.

The advantages could be this algorithm saves the training cost. AdaBoost can self-adjust weak classifiers after learning and is sensitive to noise data and outliers. In some tasks, it can efficiently resist overfitting. The disadvantages are it is necessary to know the lower limit of the learning performance of weak learners, which is difficult to do in reality. Boosting method algorithm may lead to the problem of learners focusing so much attention on some data that are extremely difficult to train (maybe noise data), in follow-up learning, the algorithm performance becomes unstable, which is overcame in AdaBoost Algorithm. Though it is a high performance computing algorithm, it still takes weeks to train a deep learning model.

2.3. IMAGE QUALITY ASSESSMENT FOR FAKE BIOMETRIC DETECTION [3]

To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this paper, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits. Its advantages is simple, fast, non-intrusive, user-friendly and cheap, all of them very desirable properties in a practical protection system.

2.4. A MULTICHANNEL APPROACH TO FINGERPRINT CLASSIFICATION [4]

Fingerprint classification provides an important indexing mechanism in a fingerprint database. An accurate and consistent classification can greatly reduce fingerprint matching time for a large database. We present a fingerprint classification algorithm which is able to achieve an accuracy better than previously reported in the literature. We classify fingerprints into five categories: whorl, right loop, left loop, arch, and tented arch. The algorithm uses a novel representation (FingerCode) and is based on a two-stage classifier to make a classification. It has been tested on 4000 images in the NIST-4 database. For the five-class problem, a classification accuracy of 90 percent is achieved (with a 1.8 percent rejection during the feature extraction phase). For the four-class problem (arch and tented arch combined into one class), we are able to achieve a classification accuracy of 94.8 percent (with 1.8 percent rejection). By incorporating a reject option at the classifier, the classification accuracy can be increased to 96 percent for the five-class classification task, and to 97.8 percent for the four-class classification task after a total of 32.5 percent of the images are rejected.

The advantages are algorithm is tested on the NIST-4 database and a very good performance has been achieved.This novel multichannel filter-based classification algorithm used here gives better accuracy than previously reported in the literature on the NIST-4 database.The disadvantage is that algorithm suffers from the requirement that the region of interest be correctly located, requiring the accurate detection of center point in the fingerprint image.

2.5. ALTERED FINGERPRINTS: ANALYSIS AND DETECTION (IEEE 2012) **[5]**

The distorted and imitated fingerprints are very hard to detect for any fingerprint image quality assessment algorithm that is based on analyzing local image quality. So, in this paper we consider the problem of automatic detection of alterations based on analyzing ridge orientation field and minutiae distribution.

Advantages are fast operational time and High true positive rate at low false positive rate**.** Disadvantages are independent development of AFISs by different manufacturers hindered the ability of the systems to be interoperable.Future work includes to determine the alteration type automatically so that appropriate counter measures can be taken.A matcher specialized for altered fingerprints can be developed to link them to unaltered mates in the database utilizing whatever information is available in the altered fingerprints**.**

3.PROBLEM DEFINITION:

3.1.EXISTING SYSTEM :

Liveness detection methods can be categorized as hardware or software-based whether the detection is performed through additional hardware or by processing the obtained image Hardware-based solutions work by measuring some physical characteristics (such as blood pressure, temperature, pulse, or pupil dilation, voluntary eye blink, among others) and have the disadvantage of being expensive and requiring intervention at the device level

Advantages are that biometrics systems can be quite flexible and easily scalable. You can use higher versions of sensors and security systems based on your requirements. There are different types of biometric scanners available. Disadvantages include in several of the existing procedures is the inclusion of the background in the liveness decision.Temperature liveness detection techniques lack in its ability to detect wafer thin silicon.We are not interested in assessing the liveness of the background (which should always be lifeless) but only in assessing the liveness of the fingerprint. Another methodological limitation is that models are designed and evaluated using fake samples of one type of material individually

3.2.PROPOSED SYSTEM :

Biometrics technology determines the correct identity of a person by extracting human biological or behavioral characteristics data. As the possibility of hacking increases with the development of IT technology, interests in biometrics and authentication technology is greatly increasing currently. The most popular authentication technology is fingerprint recognition. In the first step, the inputted fingerprint image is subjected to a complicated pre-processing stage, and the fingerprint image is then classified. In the second step the feature points of the classified fingerprints are extracted and compared with the fingerprint feature points stored in a database. In this paper, we propose the use of a CNN model which extracts the pattern found within the local region of the inputted image, by convolving a template or filter over the inputted image pixels and outputting this as a feature map. In the third step, classification is done using Softmax Classifier.Finally Data augmentation is performed by artificially creating modified samples from the original ones. It is expected that the classifier will become more robust to small variations that may be found during the testing phase.

Advantages are the Convolutional Networks presented the best performance. Dataset augmentation is helpful to prevent overfitting and increase accuracy .The main contributors for the good results achieved are the large models and datasets like images in their original sizes, augmented datasets, and large number of layers and filters in the convolutional networks. Disadvantage is that the Convolutional Networks are slower and more complex to design than other methodologies

3.3 OBJECTIVE:

Fingerprint liveness detection system can be defined as a system to detect if a fingerprint is a fake fingerprint or a real fingerprint. This gives output with greater accuracy due to use of Data Augmentation.

4. EXPERIMENTAL SETUP:

Datasets:

A spoof attack, a type of presentation attack, is the use of an artificial replica of a biometric used in an attempt to circumvent a system. “Liveness detection” is a method used to recognize a presentation attack.The goal is to compare biometric liveness detection methodologies using a standardized testing protocol and large quantities of spoof and live samples. The LivDet competitions[9] have been hosted in 2009, 2011, 2013, 2015, 2017 .We have used the 2009 th year fingerprint datasets. Our experiments were carried out on publicly available fingerprint liveness database for LivDet 2011 and 2013 competitions from Clarkson University - University of Cagliari [7]. For the LivDet 2011 database, four optical sensors, Biometrika, Digital Persona, ItalData, and Sagem were used to collect the fingerprints. Similarly, four optical sensors, Biometrika, Digital Persona, ItalData, and Swipe were used to collect fingerprints for the LivDet 2013 database.The corresponding spoof materials were chosen from body double, latex, PlayDoh, wood glue, gelatine, latex, ecoflex.

4.1.SOFTWARE SPECIFICATIONS:

The Software specifications include ,it is operated on Windows 10 operating system. The Software used in this project is Anaconda IDE Version 3.6 Spyder(36).The coding language used here is python.

4.2.SYSTEM DESIGN:

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. a safe fingerprint system must correctly distinguish a spoof from an authentic finger. Approaches can be broadly classified into two categories: hardware and software. In the software approach, which is used in this study, fake traits are detected once the sample has been acquired with a standard sensor. In this work, the pipelines used in training and testing can be broadly divided in four phases: pre-processing, feature extraction, classification and Data augmentation.

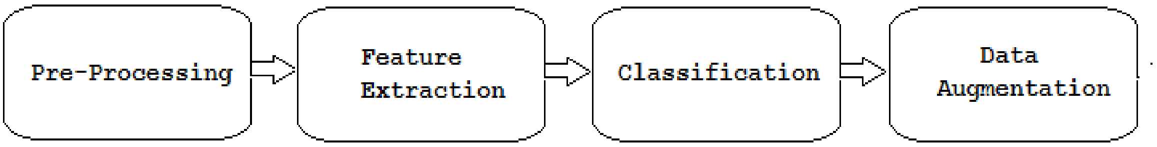


FIG.4.2.1 ARCHITECTURE FOR FINGERPRINT AUTHENTICATION SYSTEM

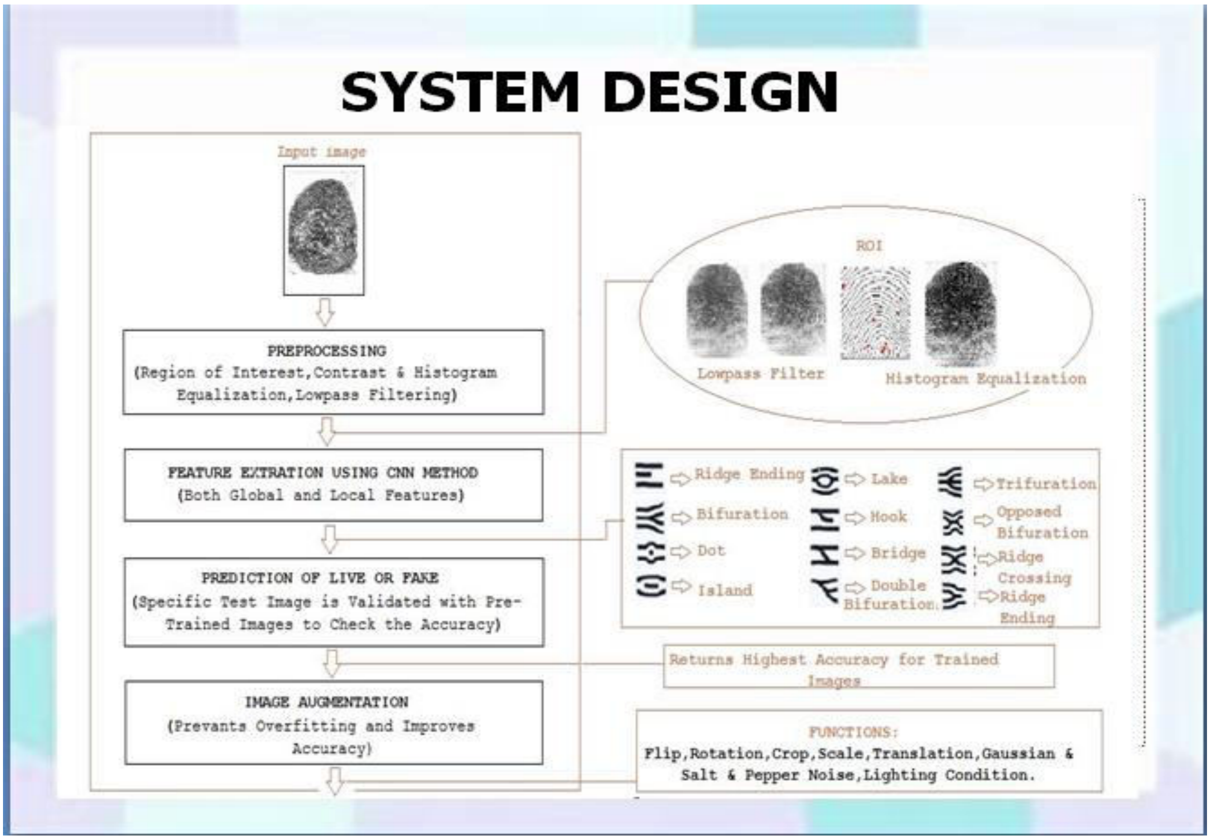
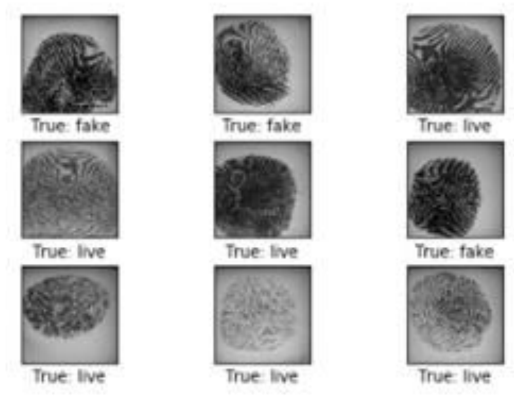

SYSTEM DESIGN
Input image
PREPROCESSING
(Region of Interest,Contrast & Histogram Equalization,Lowpass Filtering)
FEATURE EXTRATION USING CNN METHOD
(Both Global and Local Features)
PREDICTION OF LIVE OR FAKE
(Specific Test Image is Validated with Pre-Trained Images to Check the Accuracy)
IMAGE AUGMENTATION
(Prevants Overfitting and Improves Accuracy)
ROI
Lowpass Filter
Histogram Equalization
Ridge Ending
Bifuration
Dot
Island
Lake
Hook
Bridge
Double Bifuration
Trifuration
Opposed Bifuration
Ridge Crossing
Ridge Ending
Returns Highest Accuracy for Trained Images
FUNCTIONS:
Flip,Rotation,Crop,Scale,Translation,Gaussian & Salt & Pepper Noise,Lighting Condition.

FIG.4.2.2 SYSTEM DESIGN

4.3.RESULTS AND DISCUSSION:

4.3.1. Pre-processing:

Four pre-processing operations [8] were carried out: image reduction, bilateral filtering, media filtering and Gaussian filtering(Low Pass Filtering). The execution or non-execution of each operation in the final model is decided at validation time, that is, the combination of pre-processing operations that had the lowest validation error were included in the final model.



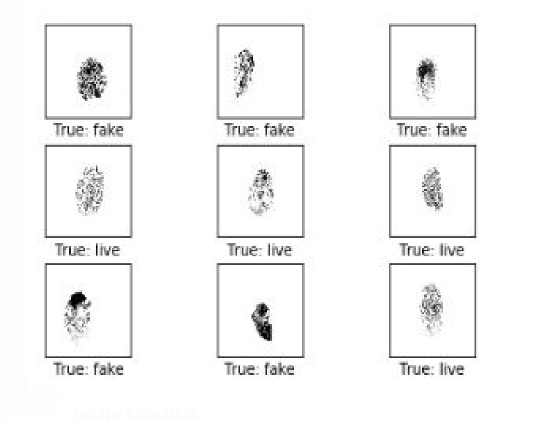


FIG 4.3.1.1 BEFORE PREPROCESSING FIG 4.3.1.2 AFTER PREPROCESSING

4.3.2. Feature Extraction:

The feature extractor that was tested was Convolutional Networks (CN) with random weights.A classical convolutional network is composed of alternating layers of convolution and local pooling (i.e., subsampling). The aim of a convolutional layer is to extract patterns found within local regions of the inputted images that are common throughout the dataset by convolving a template over the inputted image pixels and outputting this as a feature map c, for each filter in the layer.

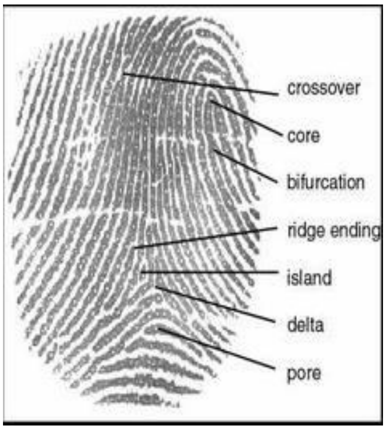
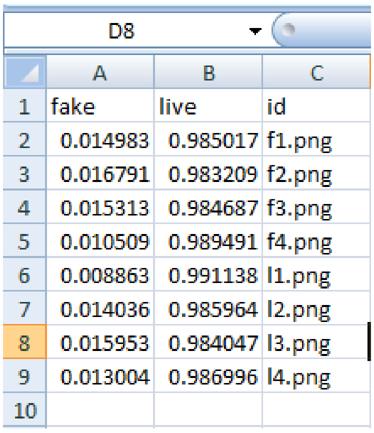


Fig.4.3.2.1 Possible features in fingerprint

4.3.3. Classification:

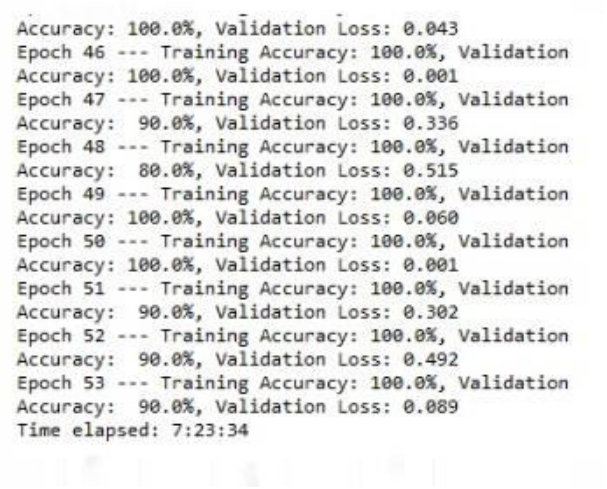
After the images in the dataset are completely trained ,they are set up for the next stage. The images are classified using softmax classifier[2] and are predicted accordingly as Live and Fake images. The results are finally displayed in the CSV File Format.



D8

	A	B	C
1	fake	live	id
2	0.014983	0.985017	f1.png
3	0.016791	0.983209	f2.png
4	0.015313	0.984687	f3.png
5	0.010509	0.989491	f4.png
6	0.008863	0.991138	l1.png
7	0.014036	0.985964	l2.png
8	0.015953	0.984047	l3.png
9	0.013004	0.986996	l4.png
10			

FIG: 4.3.3.1 CSV OUTPUT FILE CLASSIFICAION



```
Accuracy: 100.0%, Validation Loss: 0.043
Epoch 46 --- Training Accuracy: 100.0%, Validation
Accuracy: 100.0%, Validation Loss: 0.001
Epoch 47 --- Training Accuracy: 100.0%, Validation
Accuracy:  90.0%, Validation Loss: 0.336
Epoch 48 --- Training Accuracy: 100.0%, Validation
Accuracy:  80.0%, Validation Loss: 0.515
Epoch 49 --- Training Accuracy: 100.0%, Validation
Accuracy: 100.0%, Validation Loss: 0.060
Epoch 50 --- Training Accuracy: 100.0%, Validation
Accuracy: 100.0%, Validation Loss: 0.001
Epoch 51 --- Training Accuracy: 100.0%, Validation
Accuracy:  90.0%, Validation Loss: 0.302
Epoch 52 --- Training Accuracy: 100.0%, Validation
Accuracy:  90.0%, Validation Loss: 0.492
Epoch 53 --- Training Accuracy: 100.0%, Validation
Accuracy:  90.0%, Validation Loss: 0.089
Time elapsed: 7:23:34
```

FIG: TRAINING IMAGES AND VALIDATING THE ACCURACY

4.3.4.Data Augmentation:

Data Augmentation[8] is a technique that consists in artificially creating slightly modified samples from the original ones. Using them during training, it is expected that the classifier will become more robust against small variations that may be present in the data, forcing it to learn larger structures from each image of the dataset five smaller images with 80% of each dimension of the original images are extracted: four patches from each corner and one at the center. For each patch, horizontal reflections are created. As a result, we obtain a dataset that is 10 times larger than the original one. At test time, the classifier makes a prediction by averaging the individual predictions on the ten patches.

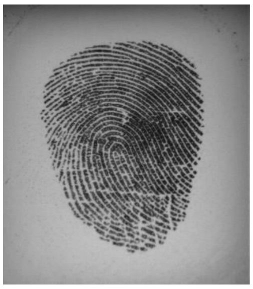


Fig.4.3.4.1 Original input image

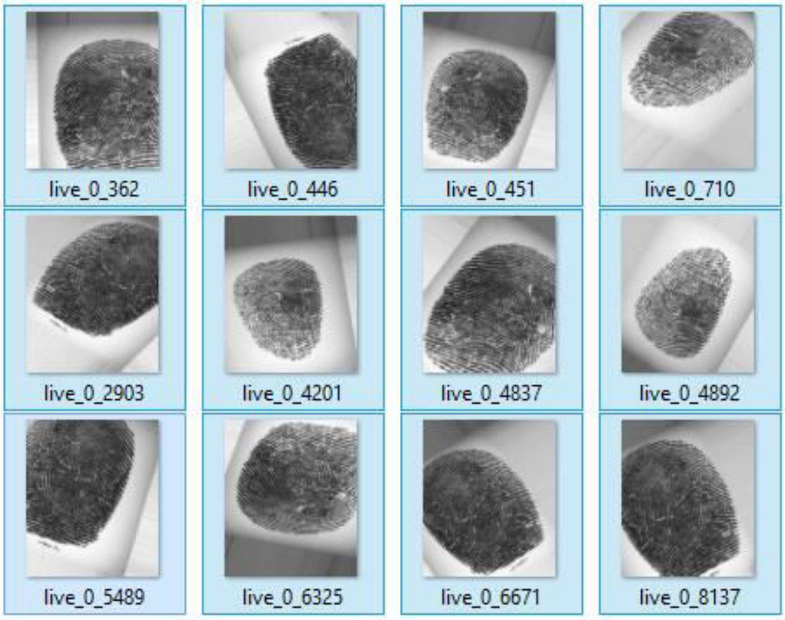
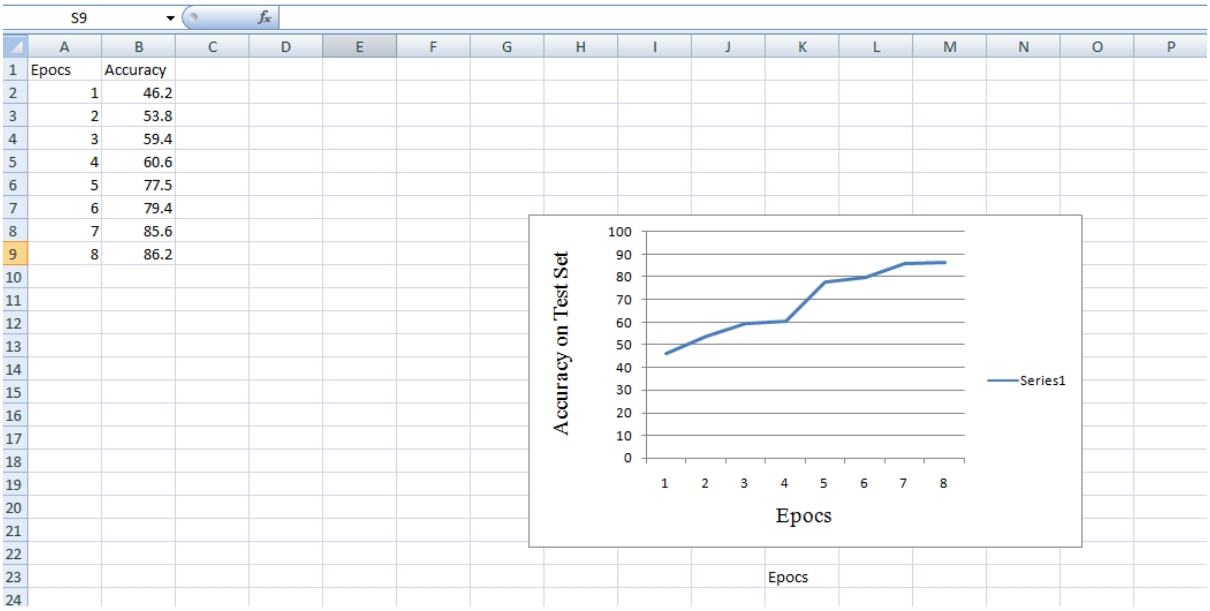


Fig.4.3.4..2 Augmented Image

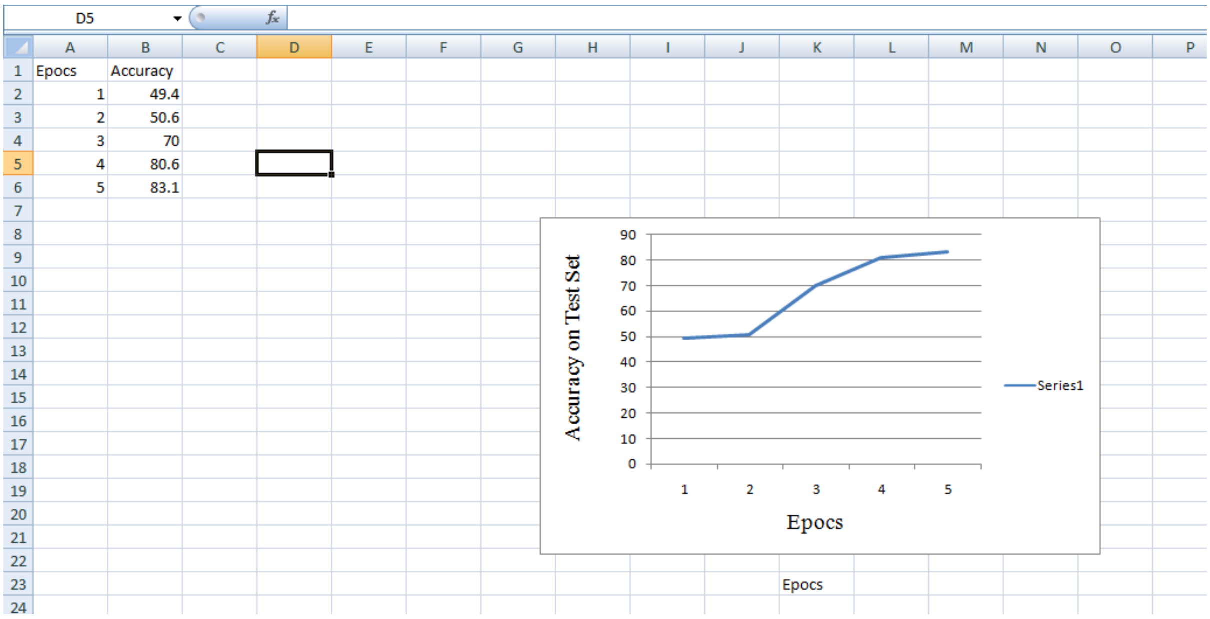
4.3.5 COMPARISON

The following two graphs denotes the accuracy of the test set before and after preprocessing and data augmentation. It shows that after preprocessing and data augmentation the test set accuracy increases within lesser epocs.



Epocs	Accuracy
1	46.2
2	53.8
3	59.4
4	60.6
5	77.5
6	79.4
7	85.6
8	86.2

FIG:4.3.4.1 . Before pre-processing results



Epocs	Accuracy
1	49.4
2	50.6
3	70
4	80.6
5	83.1

FIG:4.3.4.2 . After pre-processing and Data augmentation results

5.CONCLUSION AND FUTURE ENHANCEMENTS :

5.1.CONCLUSION:

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 small training sets (2000 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. This suggests that the effort required to design a liveness detection system (such as hyper-parameters fine tuning) can be significantly reduced if different datasets (and acquiring devices) are combined during the training of a single classifier. Dataset augmentation plays an important role in increasing accuracy and it is also simple to implement. We suggest that the method should always be considered for the training and prediction phases if time is not a major concern. Given the promising results provided by the technique, more types of image transformations should be included, such as color manipulation and multiple scales.

5.2.FUTURE ENHANCEMENTS:

Our experimental results demonstrate that the proposed quality feature based method is able to handle various spoofing materials and sensors consistently well over different datasets. Therefore, generality and robustness of the proposed approach is adequate for liveness detection of different spoof materials. Additionally, as proposed method requires a single image, it is more user-friendly, faster and computationally efficient. In future work, proposed liveness detection system can be integrated with quality assessment module of fingerprint recognition system. Effectiveness of other quality related features can also be evaluated for fingerprint liveness detection.

6. REFERENCES:

[1] Athos Antonelli, Raffaele Cappelli, Dario Maio, and Davide Maltoni, " FAKE FINGERPRINT DETECTION BY SKIN DISTORTION ANALYSIS", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY , 2006.

[2] , Shin-Jye Lee1 , Tonglin Chen2 , Lun Yu2 , Chin- Hui Lai3, "IMAGE CLASSIFICATION BASED ON THE BOOST CONVOLUTION NETWORK", IEEE ACCESS 2018.

[3] Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian Fierrez.," IMAGE QUALITY ASSESSMENT FOR FAKE BIOMETRIC DETECTION", IEEE 2014.

[4] Anil K. Jain, Fellow, IEEE, Salil Prabhakar, Student Member, IEEE, and Lin Hong, "A MULTI CHANNEL APPROACH TO FINGERPRINT CLASSIFICATION", IEEE TRANSACTIONS ,ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE. ,2007.

[5] , Adrian Lim Hooi Jinl, Ali Chekima', Jamal Ahmad Dargham', and Liau Chung Fan', "FINGERPRINT IDENTIFICATION AND RECOGNITION USING BACKPROPAGATION NEURAL NETWORK", IEEE 2012.

[6] L. Ghiani, A. Hadid, G.L. Marcialis, and F. Roli, "FINDERPRINT LIVENESS DETECTION USING BINARIZED STATISTICAL IMAGE FEATURES", in Biometrics: Theory, Application and Systems (BTAS), 2013 IEEE Sixth International Conference on, Sept 2013, pp. 1–6.

[7] D. Yambay, L. Ghiani, P. Denti, G.L. Marcialis, F. Roli, and S. Schuckers, "Livdet 2011,

FINGERPRINT LIVENESS DETECTION COMPETITION," in Biometrics (ICB), 2012 5th IAPR International Conference on, March 2012, pp. 208–215

[8] Rodrigo Frassetto Nogueira1 , Roberto de Alencar Lotufo2 , and Rubens Campos Machado3," FINGERPRINT LIVENESS DETECTION SYSTEM USING CONVOLUTION NEURAL NETWORKS",IEEE Transactions on Information Forensics and Security.

[9] Dataset Collection- http://livdet.org/registration.php