A MULTIMODAL COMBINED MACHINE LEARNING APPROACH FOR FINGERPRINT CLASSIFICATION

A.Thilagavathy[1], Ravin N Krishnan[2], C Sidhartha Reddy[3], Sode Bharath Chandra[4]

[1,2,3,4] R.M.K. Engineering College, Tamil Nadu, India
Email: [1] atv.cse@rmkec.ac.in, [2] ravi17234.cs@rmkec.ac.in, [3] sode17310.cs@rmkec.ac.in,
[4]sidh17309.cs@rmkec.ac.in

Abstract

Fingerprint identification is the most widely used biometric for a multitude of security applications ranging from phone unlocks to bank security. All modern systems use a machine learning approach based on a unique algorithmic - such as Support Vector Machines(SVM) , Convolutional Neural Networks(CNN) or Residual Convolutional Neural Network(RESCNN).Each and every algorithm is strong in some areas and weak in others. In our work we describe the output yielded using a new proposed algorithm that uses a trifecta combination, i.e three different algorithms are combined to maximise their individual strengths and cover each other's weaknesses. The algorithms we combine are a simple preprocessing algorithm, SVM and a trained convolutional neural network. First, the preprocessing algorithms smoothens, sharpens and filters the image, then an SVM is used to extract the minutiae (fingerprint features) which is finally classified using a trained CNN classifier. This new algorithmic approach will have enhanced accuracy, faster processing time and lower error than the traditional unilateral algorithmic approaches.

Key words: Machine Learning, Fingerprint

Introduction

Biometrics is human characteristics and features such as fingerprint, palmprint and eyes. Biometric identification has been around since the fourteenth century, where China introduced fingerprinting (one of the most common biometrics used even today) , by collecting the fingerprints of traders and their progeny to uniquely identify them. Biometrics have come a long way from then in terms of their relevance and importance in even the common man's life. The rise of radicalism and terrorism in the 21st century has led to paranoia and fear growing worldwide and consequently, increased draconian security measures and checks. This is troublesome because it trades customer comfort, experience and time for the feeling of added security. This is where biometric identification has been making rapid, unchecked expansion since it is simultaneously safe and efficient without affecting the customer invasively. For example, Airports around the world are committing to biometric identification since it can efficiently verify and board more than 200 passengers in less than 20 minutes using biometric identification.

Fingerprinting for the purpose of identification has been around since the 1880s.The earliest systems involved painstaking and time intensive verification of fingerprints against a physical database that was until the Henry Classification System came along. It makes fingerprint identification more efficient by giving every finger values based on ridge count, whorls etc and then using these values to group them. After this is done, upcoming searches are performed using minutiae. It is still used to this day in some cities in case cataclysms come to pass. The drawbacks of this system are that it is requires all ten fingers of a human to be documented correctly and it is best used to exclude people from matching, not finding an exact match. In the modern day, fingerprint identification is done by machine learning algorithms trained with minutiae .Minutiae are important features that can profess the uniqueness of a fingerprint .These include Support Vector Machines(SVM) , Convolutional Neural Networks(CNN) or Residual Convolutional Neural Network(RESCNN).Each and every algorithm is strong in some areas and weak in others. For example, residual convolutional neural networks are very accurate but take a large processing time , most normal convolutional neural networks are fast but susceptible to spoofing via presentation attacks etc.

In our work we propose a new algorithm that uses a trifecta combination,i.e three different algorithms are combined to maximise their individual strengths and cover each other's weaknesses. The algorithms we combine are a simple preprocessing algorithm, support vector machine and a convolutional neural network. The datasets used for training the convolutional neural network are from the LivDet database.The first step is preprocessing , where the fingerprint images are smoothened ,sharpened and filtered .Then these processed images are fed to the Support Vector Machine, which extracts the features(minutiae) and maps it onto a feature vector array. This array is fed to the convolutional neural network which then classifies the fingerprint. The results are reported to illustrate its superior efficiency and accuracy. This paper adheres to the structure: section 2 as literature survey, section 3 methodology , section 4 result, section 5 Conclusion and section 6 references.

Literature Survey

The authors in [1] have proposed a unique local descriptor for fingerprint liveness discernment. They do it by examining two features, intensity variance and binary gradient orientation. They calculate the odds of simultaneous occurrence of the features and feed it to a support vector machine (SVM) for classification. The effectiveness of their new system is demonstrated through having the best detection accuracy amongst existing local descriptors. However, this descriptor requires optimum lighting condition and sample quality to calculate intensity variance correctly, these optimum conditions are not always feasible in real world applications over a long span of time. In [2], the authors propose anti-spoofing via a deep residual network(DRN) combined with an extraction algorithm, adaptive learning and texture enhancement. Residual networks are used to reduce processing time, adaptive learning to adjust the learning rate as required and the extraction algorithm is used to remove invalid or unnecessary areas from the image, finally texture enhancement improves the generality of the classifier. This massive network shows best in class anti spoofing capabilities but its processing time is still too high.

The authors in [3] demonstrate liveness detection using convolutional neural networks(CNN) .They show top of the line results using a trained CNN with even minute training sets(400 samples) giving extremely high accuracy. However, this model cannot detect presentation attacks accurately enough. The authors in [4]propose a deep CNN using not just minutiae but also patches surrounding each minutiae to detect liveness. The minutiae is used for alignment of the patches. This is tested against multiple spoofing materials and scanners and yields commendable results. They also present a Graphical User Interface (GUI) which shows personnel the patches that are likely to be fake. However, this also requires high resolution and quality images to work effectively, which is not perennially feasible in real world scenarios.

The authors in [5] propose a deep residual CNN for fingerprint liveness detection. They utilise an improved resCNN using exclusively designed residual blocks to which can detect fingerprint liveness without excessive processing time and noise/reactions from overfitting. This also won FLD competition in 2017 due to its high accuracy. However ,even though the combination of high accuracy and low processing time is appealing,this model suffers from high false positive rate.

Methodology

We use minutiae based extraction combined with a preprocessing algorithm, Convolutional Neural Networks (CNN) and support vector machine (SVM) for fingerprint identification. Experimental results conducted on a publicly available database are reported to illustrate the superior efficiency and accuracy. Figure 1 depicts the architecture diagram of proposed workflow.

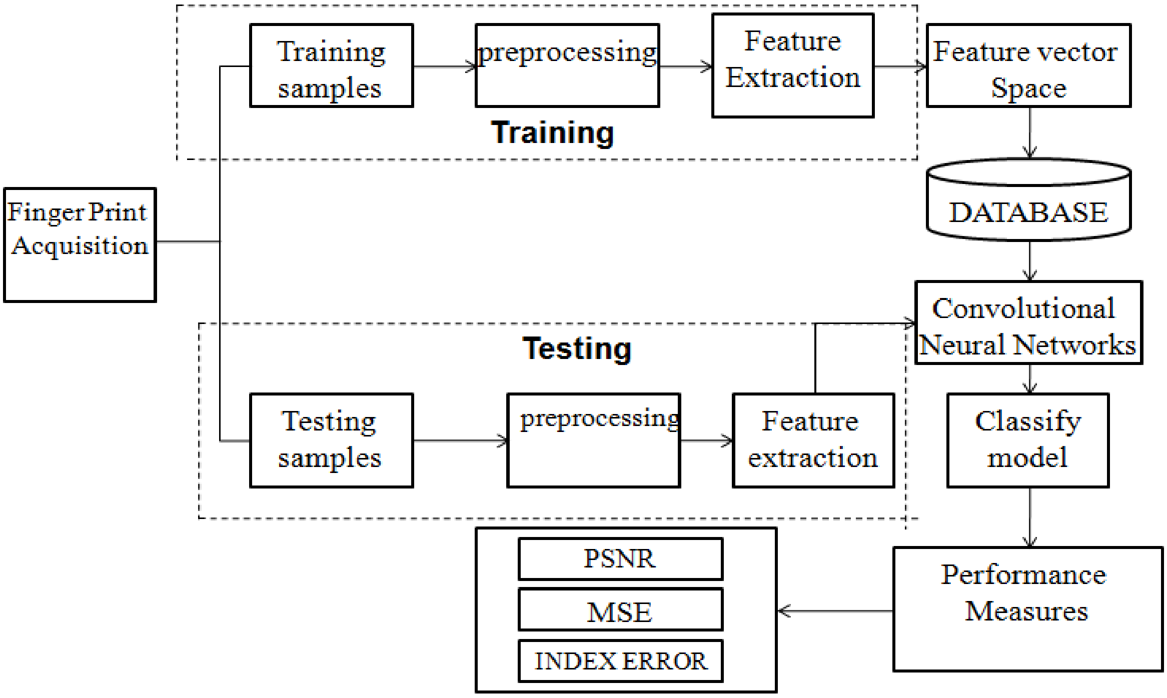


Figure 1: Architecture diagram of proposed workflow

This algorithm contains(i)a preprocessing algorithm that filters,smoothens and sharpens the image.(ii)support vector machine which extracts the minutiae and maps it into a feature vector array.(iii)Convolutional neural network which performs classification.

Our algorithm consists of 5 modules namely image acquisition, preprocessing, feature extraction, classification and performance evaluation. This is implemented in MATLAB.

3.1 Image Acquisition

Images are acquired from the livdet competition database which consists of several real fingerprints and multiple spoofs made from materials such as glass,silicon,clay etc.

- Preprocessing

The preprocessing algorithm helps in optimizing image quality by performing smoothening,sharpening and filtering operations on the image.

- Feature Extraction

The feature extraction is performed by Support Vector Machine and the feature is minutiae,that is ridge endings and ridge bifurcations.The SVM extracts the features and then maps them onto a feature vector array.

- Classification

First,the model is trained with labels in the training phase to aid in differentiation.Then,the convolutional neural network(CNN) is tested to verify its accuracy in classification.

- Performance evaluation

We evaluate the performance on the following parameters ,PSNR(Peak Signal to Noise Ratio),MSE(Mean Square Error) and index error.

Result

The fed input dataset consists of a collection of real images and their fakes made using a variety of materials such as silicon, glassetc. It is used to compare the accuracy of classification between the various algorithmic approaches. We have achieved the following graph which shows that the proposed algorithm performs classification with an accuracy of over 95%. Figure 2 shows the comparison result of proposed system with existing system. The proposed system is compared with the the existing DWT,SVM and Sobel operators. Figure 3 is the screenshot of Training GUI. Figure 4 shows the Database Creation. Figure 5 is the screenshot of Testing GUI. Figure 6 is the Extracting minutiae and in Figure 7 the User is Authenticated.

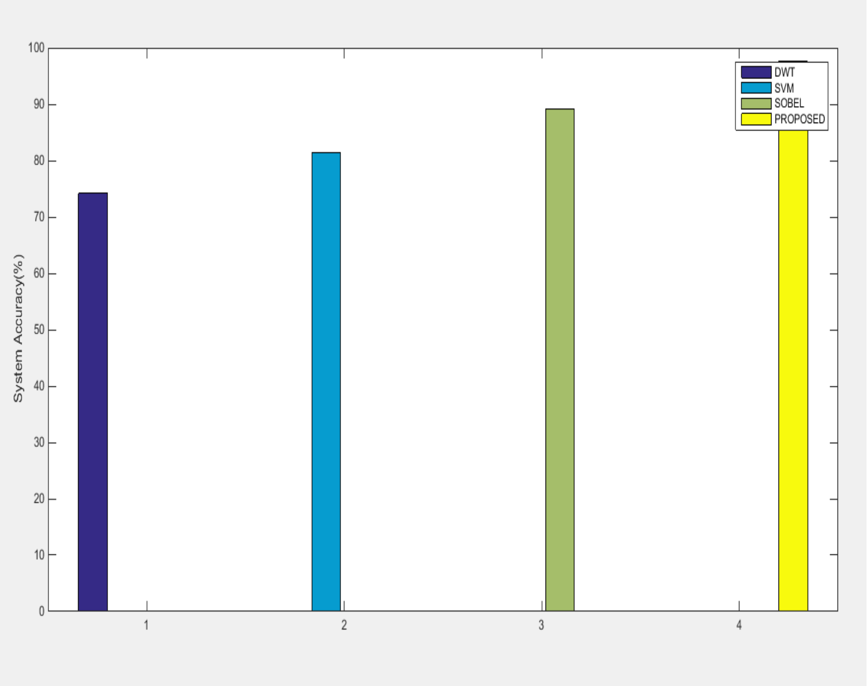


Figure 2: Comparison result of proposed system with existing system.

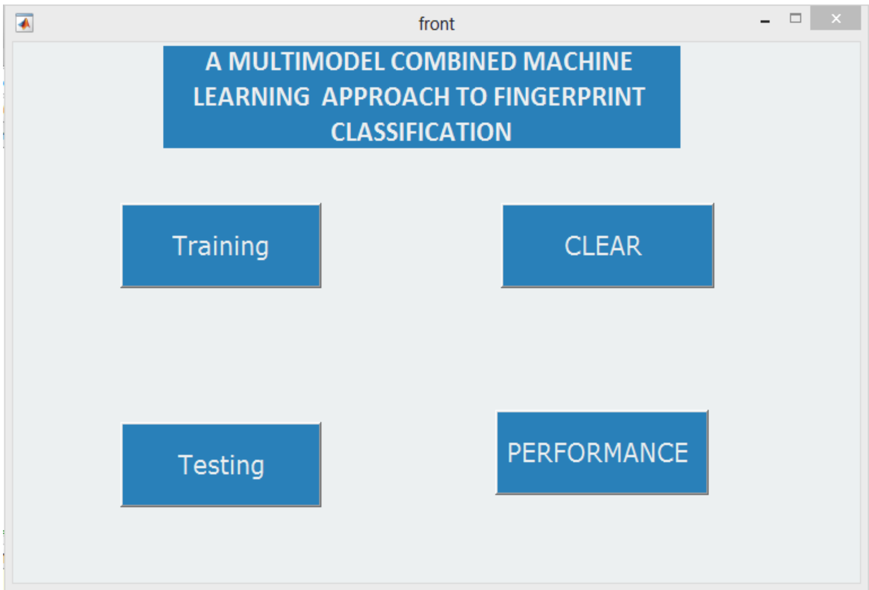

front
A MULTIMODEL COMBINED MACHINE LEARNING APPROACH TO FINGERPRINT CLASSIFICATION
Training
CLEAR
Testing
PERFORMANCE

Figure 3: TRAINING GUI.

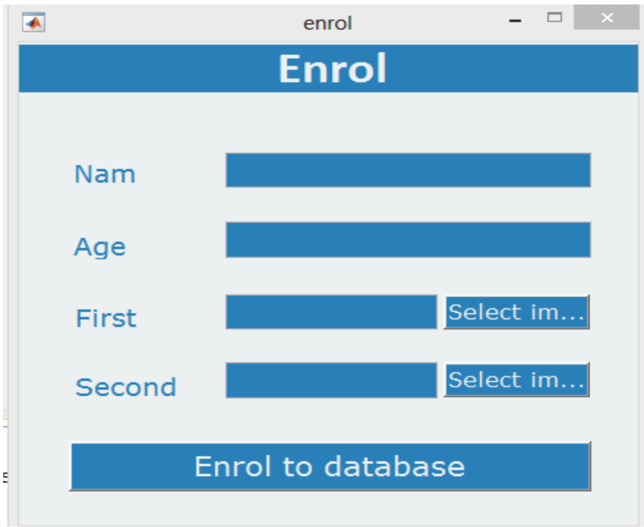


Figure 4: DATABASE CREATION.

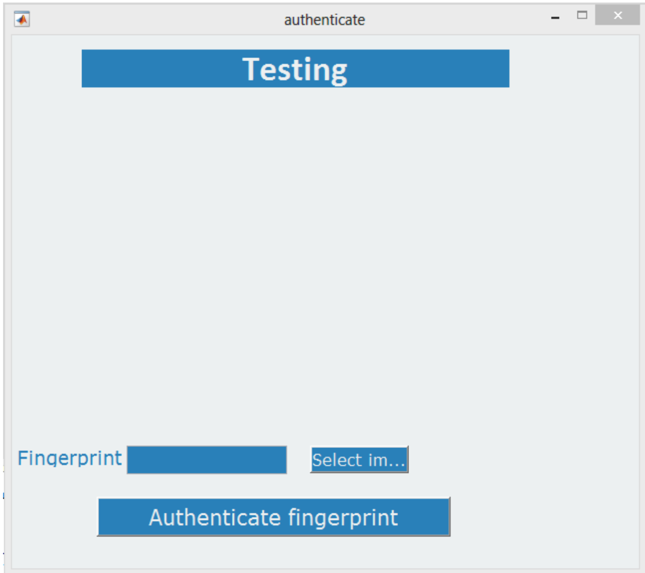


Figure 5: TESTING GUI

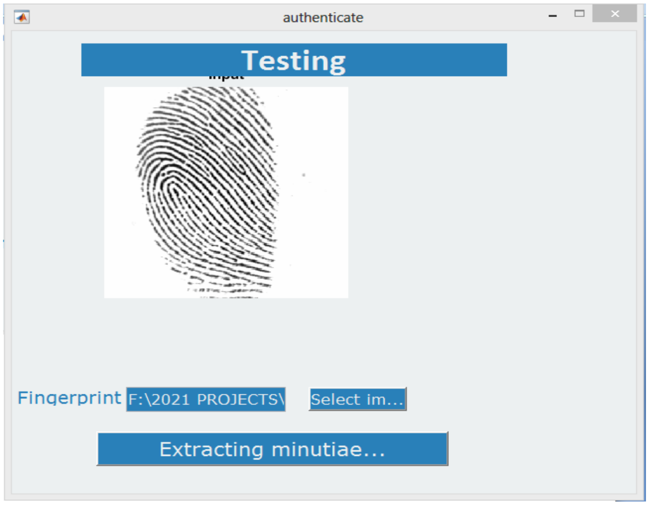
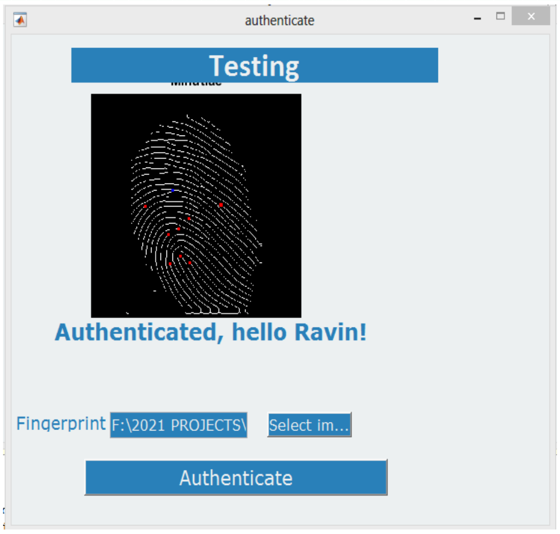


Figure 6: Extracting minutiae



Authenticated, hello Ravin!

Fingerprint F:\2021 PROJECTS\

Figure 7: User Authenticated

Conclusion

The result shows that a convolutional neural network balanced with support vector machines and a preprocessing algorithm is a highly efficient, accurate tool while simultaneously taking a low processing time and working with images from imperfectly oriented or illuminated sources. Combining CNN with SVM increases the accuracy to a standard higher than any one pure method. This displays its superiority to conventional unilateral algorithmic methods.

References

1. Z. Xia, C. Yuan, R. Lv, X. Sun, N. N. Xiong and Y. Shi, "A Novel Weber Local Binary Descriptor for Fingerprint Liveness Detection," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 4, pp. 1526-1536, April 2020, doi: 10.1109/TSMC.2018.2874281.
2. C. Yuan, Z. Xia, X. Sun and Q. M. J. Wu, "Deep Residual Network With Adaptive Learning Framework for Fingerprint Liveness Detection," in *IEEE Transactions on Cognitive and Developmental Systems*, vol. 12, no. 3, pp. 461-473, Sept. 2020, doi: 10.1109/TCDS.2019.2920364.
3. R. F. Nogueira, R. de AlencarLotufo and R. Campos Machado, "Fingerprint Liveness Detection Using Convolutional Neural Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1206-1213, June 2016, doi: 10.1109/TIFS.2016.2520880.
4. T. Chugh, K. Cao and A. K. Jain, "Fingerprint Spoof Buster: Use of Minutiae-Centered Patches," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2190-2202, Sept. 2018, doi: 10.1109/TIFS.2018.2812193.
5. Y. Zhang, D. Shi, X. Zhan, D. Cao, K. Zhu and Z. Li, "Slim-ResCNN: A Deep Residual Convolutional Neural Network for Fingerprint Liveness Detection," in *IEEE Access*, vol. 7, pp. 91476-91487, 2019, doi: 10.1109/ACCESS.2019.2927357.
6. S. Soviany, C. Soviany, S. Puşcoci, “Feature-level Data fusion for biometric mobile applications. A case study”, The 2019 International Conference on Security and Management (SAM'19), Las Vegas, USA, July 29 – August 1, 2019.
7. S. Soviany, S. Puşcoci, “A biometric security model with co-occurrence matrices for palmprint features”, ECAI 2019 - International Conference – 11th Edition Electronics, Computers and Artificial Intelligence, Piteşti, România, 27-29 June, 2019.
8. A. Jain, K. Nandakumar, A. Ross, “Score normalization in multimodal biometric systems, Pattern Recognition”, The Journal of the Pattern Recognition Society, 38 (2005).
9. D. Zhang, F. Song, Y. Xu, Z. Liang, Advanced Pattern Recognition Technologies with Applications to Biometrics, Medical Information Science Reference, IGI Global, 2009.
10. S. Soviany, S. Puşcoci, “A case study of data fusion for biometric applications”, The 7th IEEE International Conference on E-Health and Bioengineering - EHB 2019 Grigore T. Popa University of Medicine and Pharmacy, Iaşi, România, November 21-23, 2019.