International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-8, June 2020

Finger Vein Recognition Using Vgg-16 Cnn Algorithm

Ganugula Sri Harshan, Sudheer Rayudu, Krishnan Anush Bharadwaj, Saravanan K

Abstract*: With the advancement in the electronic technology, data identification and security is to be mainly considered as a factor in the security. Biometric recognition has been taken in to consideration for security purpose. Data security has to be done to prevent the system security from transmission of data by unauthorized users. Various authentications are taken in to consideration but most commonly focuses on finger print biometric system. Biometric recognition is taken in priority which is high safe and security oriented. Preprocessing, extraction and Equal Error rate are taken in to consideration. In this we are mainly focusing in finger vein authentication domains over the system implementation.

Keywords: LBP, Data Augmentation, Resnet, VGG-16, ERR, CNN.

I. INTRODUCTION

Many biometric systems have its own recognition, database and system model specification. On consideration of other recognition such as voice, finger print and facial expression but it is not secure. But with finger vein recognition, it is unique. Highlighting the system method by vein recognition [1]. Security and authenticate the system for providing security issues. Considering the other factors of authentication such as image or facial recognition makes it most difficult to consider with security factors. Use of finger vein has added advantage over all other systems [2]. Collecting number of datasets based on the vein recognition. Data sets organization on the basis of collected images. Implementing the system by use of certain algorithm techniques and feature extraction system [3]. Review on the problem of authentication and password management criteria has a lacked information security. On considering the security issues, pros and cons of the system have been protected [4]. Comparison on the basis of retrieval of data Identification of crime, password authentication this has been placed a major role. By pattern recognition, the image results were obtained [5].

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author
Ganugula Sri Harshan*, Department of Communication Engineering, VIT Vellore, Vellore, India. Email: harshan1823@gmail.com.
Sudheer Rayudu, Department of Communication Engineering, VIT Vellore, Vellore, India. Email: sudheerrayudu183@gmail.com.
Krishnan Anush Bharadwaj, Department of Communication Engineering, VIT Vellore, Vellore, India. Email: anushbharadwaj6798@gmail.com.
K. Saravanan,Professor,School of Electronics and Engineering, VIT Vellore, Vellore, India. Email: kasisaravanan@vit.ac.in

II. AUTHENTICATION SYSTEM USING BIOMETRIC

The authentication system based on biometric deals with the real time identity verification of a person using their behaviour or characteristic of a body. This system will collect the data of a body (i.e. iris or finger vein) scanned images and transfer them into digital data to store them in particular manner. By using different algorithm this data's can be trained and stored for further usage. This algorithm is used in matching patterns to match with the stored registered recognised data and then verify the identity of a particular person in safe and secure manner. In this two modes of process are done they are identification and verification modes. In identification mode initially the biometric of the person is taken and then stored in the database. Once the identification is done then in the verification mode the reorganization of a biometric is done. When the input data is collected it is allowed to compare the data with the stored database to predict the matching of the pattern using identification mode. In verification mode the same input data will be analysed to predict the matched finger vein has the same pattern of the person to prevent it from multiple usage.

III. PROPOSED SYSTEM

The finger vein reorganization system is considered as an image classification problem and can be performed using deep learning algorithm. Hence the CNN architecture can be used to perform this authentication system. To perform CNN, the required data should be collected using Data collection, data augmentation, pre-processing and feature extraction should be performed. Normally the feature extraction is performed using features of the trained data and the based upon that data the threshold values can be kept and then in testing part the value of the features will compared with the trained one to predict the verification system.

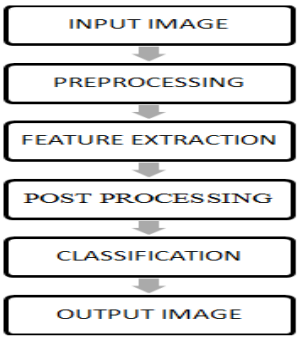

Fig 4.1: Basic Block Diagram of processing the input image

IV. ARCHITECTURE DIAGRAM OF PROPOSED SYSTEM IN REAL TIME

In this the User A and User B finger vein data are taken and stored in database. The features of both the users are taken and compared using CNN architecture to predict the matching.

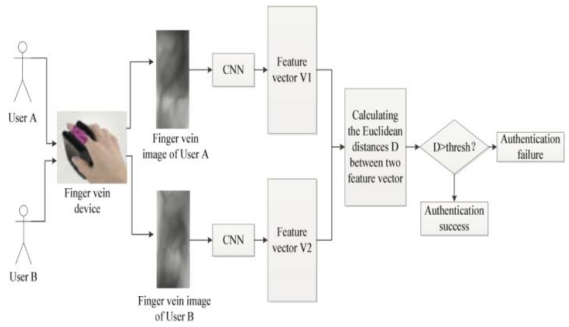

Fig 4.1: Block Diagram of Processing Image

V. MODEL DESCRIPTION

a. Data Collection:

The data collection deals with collecting the finger vein data of the various people. The images will be collected and the filter according to the dimension, size and format. Total data which are collected will be stored in database in one format.

b. Data Augmentation:

The Data augmentation is normally performed to change the dimension or direction of an image. Normally the 3-pixel images are in vertical direction and 5-pixels are in horizontal direction. Normally the data augmentation method is used to perform the padding, cropping of an image and then the horizontal flipping to achieve the neural network architecture.

c. Feature Extraction (LBP):

The local binary pattern algorithm is used to extract the feature values of an image which will be used to train the datasets in the neural network algorithm.

d. Resnet model (Transfer Learning):

In CNN architecture while training at certain condition adding the neural network will slow down the training process and also saturate the accuracy.

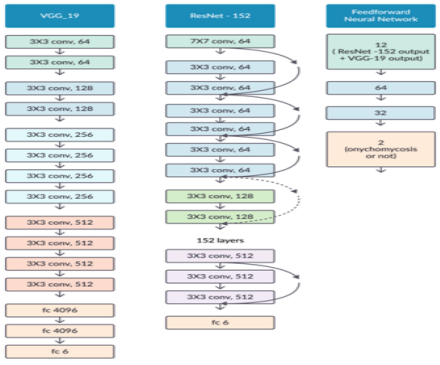

Fig 5.1: Resnet Model

e. VGG model:

The VGG-16 is a very deep convolutional neural network which has 138 millions of parameters. Training on this deep architecture needs large-scale datasets. However, our training data is much smaller than the ImageNet. So a pre-trained VGG-16 model was fine-tuned on our datasets. To mitigate this problem, ResNet incorporates identify shortcut connections which essentially skip the training of one or more layers — creating a residual block.

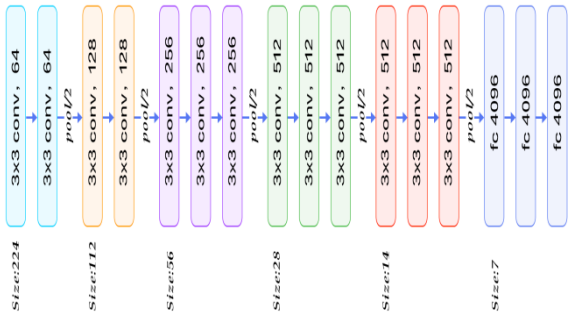

Fig 5.2: VGG Model

f. CNN Model:

The pre-trained CNN model can be treated as a feature extractor. A linear classifier can be built by using extracted features as input. On the other hand, the fine-tuning method is often carried out to fine-tune some high-level layers. Features in the early layers are more generic. While features in the later layers contain more specific information of original datasets. Freezing early layers can bring us general and useful features for many tasks. And fine-tuning following layers can generate more particular features existing in our datasets. In this we tried out VGG-16 model which will do fine tuning some layer for pre-trained model. It increases the accuracy when compared to previous convolution network.

VI. OUTPUTS

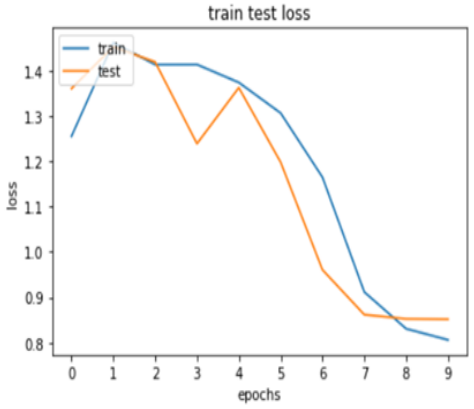

Fig 6.1: Loss in test and train data

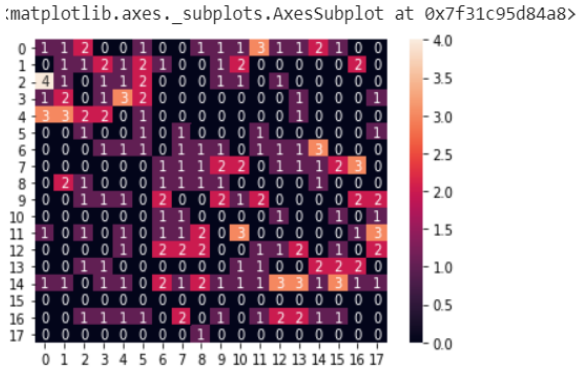

Fig 6.2: Feature Extraction On A Vein Image

VII. CONCLUSION

Novel method of CNN algorithm with VGG method of transfer learning algorithm is applied. The ResNet–16 dataset usage has helped to increase the efficiency with higher accuracy. Equal Error Rate also the accuracy is better for training and testing datasets. The practical and theoretical model of this algorithm have resulted us good accuracy for authentication of a person and we can conclude that this CNN model produce better accuracy than the other one.

REFERENCES

1.]. Kashif Shaheed, Hangang Liu, Gongping Yang, Imran Qureshi, Jie Gou and Yilong Yin, "A systematic review of finger vein recognition techniques", information 2018, MDPI, Basel, Switzerland, 2018
2. Rahul Dev and Ruqaiya Khanam, " Review of Finger Vein Feature Extraction Methods", International Conference on Computing, Communication and Automation (ICCCA2017), ISBN: 978-1-5090-6471-7, IEEE 2017
3. Chetana Hegde, Phanindra J, P Deepa Shenoy and L M Patnaik, " Human Authentication using Finger Knuckle Print", ACM, COMPUTE'11, March 25-26, Bangalore, Karnataka, India.2011.
4. P Gopinath and R Shivakumar, " A Review of Various Feature Extraction Methods on Finger Vein Images", IJARTET 2016
5. Rig Das, Emanuela Piciucco, Emanuele Maiorana and Patrizio Campisi, " Convolutional Neural network for Finger Vein Based Biometric Identification", , IEEE transactions on Information Forensics and Security, 2018
6. Huafeng Qin and Mounim A. EI-Yacoubi, " Deep representation based feature extraction and recovering for finger vein verification", IEEE Transactions on information forensics and security, Vol.12, No.8, August-2017.
7. Wenjie Liu, Weijun Li, Linjun Sun, Liping Zhang and Peng Chen, "Finger vein recognition based on deep learning", 12th IEEE conference on industrial electronics and applications (ICIEA), 2017.

AUTHORS PROFILE

Ganugula Sri Harshan is pursuing B. Tech in Electronics and Communication Engineering from VIT Vellore, TamilNadu.

Sudheer Rayudu is pursuing B. Tech in Electronics and Communication Engineering from VIT Vellore, TamilNadu.

Krishnan Anush Bharadwaj is pursuing B. Tech in Electronics and Communication Engineering from VIT Vellore, TamilNadu.

Dr. Saravanan K received M. Tech Degree in Electronics and Communication Engineering from Pondicherry Engineering College and Ph.D. from Anna University, Chennai. He is currently working as Professor in Department of Communication Engineering, VIT, Vellore. He published 12 papers in various National and International journals. His research interests are of Wireless Networks, Network Security, Device to Device communication and 5G.