Cnn Based Multimodel Biometric Authentication System Using Face And Fingerprint

[1.]Mr.E.Balraj[*],[2.]Mr.T.Dinesh,[3.]Mr.S.Deepan,[4.]Mr.N.Nattudurai,[5.]S.Ramamoorthi
[1.]*Assistant Professor, M.Kumarasamy College of Engineering, Karur,balrajbecs@gmail.com.*
[2.]*.UG Student, M.Kumarasamy College of Engineering, Karur, thirudinesh71@gmail.com*
[3]*.UG Student, M.Kumarasamy College of Engineering, Karur,,deepan968@gmail.com,*
[4]*.UG Student, M.Kumarasamy College of Engineering, Karur,nattudurai107@gmail.com,*
[5]*.UG Student, M.Kumarasamy College of Engineering, Karur,mailtoram011@gmail.com.*

Abstract

Multimodal biometric authentication methods have been introduced to provide accurate and safe solutions, integrating both soft and hard biometric schemes. This paper suggests a new hybrid strategy that guarantees the user's loyalty to the device, as well as checking whether the user has passed the biometric test as a regular or spoofed one. The suggested scheme is two modules: Module I combines fingerprint, and face recognition to suit the relevant databases, while module II incorporates models based on fingerprint, and face anti-spoofing convolutional neural networks (CNN) to identify spoof. The hash of a fingerprint is correlated with the fingerprint database at beginning level. Following a successful fingerprint match, it is checked on a fingerprint model based on CNN to check whether it is a fake or actual. A same process is repeated for the face recognition, and the system allows users to log in to the system based on cumulative proof. In the system introduced, utilizing Squeeze Net to provide accurate and reliable test results align with previous systems, challenging the restrictions of usual authentication and spoofing activities.

I. INTRODUCTION

Traditional methods such as passwords and tokens are used to safeguard our data and information. But it can be replicated, exchanged, misplaced, overlooked, hacked or faked. To prevent this security issue, we later used a biometric authentication scheme utilizing human biometric identities such as iris, thumb, voice recognition, fingerprint, facial recognition, retina, and finger veins, which can be classified as unimodeled systems because they depend on a common biometric source to identify all, hence it is difficult to spoof it.

Identification of fingerprints includes the analysis of two samples of traction ridge skin sensation from human fingers, palms or toes. A technology for facial recognition is a system that can determine or validate a person by capturing their image, or from a source of film. There are several forms identity verification systems work, but usually they function by comparing a specified image's chosen face expression with image stored in a database. It is also characterized as a Biometric Artificial Intelligence based research that can uniquely identify individuals by analysing behaviors based on the texture and shape of a person's face.

Neural networks is currently the most powerful machine learning algorithms for machines. Neural networks were shaped by the human brain's neural structures and, like in a human brain, the building blocks is labelled the Neuron. The current approach uses the multimodal biometric recognition system that combines fingerprint and face images using convolutionary neural network architecture.

2. LITERATURE SURVEY

Mohamed Hammad et al.[1] Suggested fingerprint and ECG-based multimodal biometric authentication schemes utilizing Q-Gaussian multi-support vector machine and neural convolution network. Two fusion algorithms built this system: a decision level fusion and a feature level fusion. This system offers the advantage of predicting liveness by detecting ECG signals which helps us to prevent spoof assaults. The feature extraction for every modalities are done by using CNN. To achieve the highest accuracy, they selected two layers from CNN. They applied QG-MSVM classifier to improve authentication performance in the system.

ISSN: 2233-7857 IJFGCN

D. Jagadiswary, D. Saraswady.[2] Proposed fused multimodal authentication system based on fingerprint, retina and finger vein that includes two modules: Conscription module and authentication module. Conscription module that integrating the biometric sensor to record the raw biometric data of individual. The feature extraction of fingerprint, retina and finger vein are fused using feature level fusion and the secret key is generated by using asymmetric cryptographic algorithm RSA. Authentication module, the users uniqueness are captured and validate whether it is genuine or spoofed.

N. Lalithamani and M. Sabrigiriraj.[3] Experimentation to generate palm and hand vein-based fuzzy vault for multi-biometric cryptosystem that consist of four phase: Pre-processing phase, feature extraction phase, fuzzy vault generation phase and recognition phase. Phase I resize the input image size to standard image size and then converted to double precision format. Phase II, the unique points are extracted from the palm and hand veins and it added with chaff point to generate the combined feature vector. Phase III, the secret key is generated depend on the number of feature vector points that form the fuzzy vault. Phase IV users palm and hand vein images are captured and extracted input future is compared with fuzzy vault if it matched, then it authenticate.

P Appala Naidu et al.[4] proposed "fingerprint and palm print multi-modal biometric security system" in which they identify the palm and the finger print and then the authentication process is carried out. They used three process in it to scan the finger print binarization, thinning and minute extraction. The binarization will be identifying the ridges of finger print, thinning will remove the repetitive pixels and minute extraction will be choosing the specific area of the images. After they have used fussy extraction to generate the secrete key and store in fuzzy vault. While user authenticate the same process is repeated and the key generated and the key stored are same then authentication will be success otherwise authentication will be failure.

ZhendongWu et al.[5] proposed "Multibiometric Fusion Authentication in Wireless Multimedia Environment Using Dynamic Bayesian Method" In this system they have used finger print and voice print to do the two- step authentication system. They have used they dynamic Bayesian method to recognize the voice print which has the higher level of accuracy. The voice print is compared with the voice which is stored in the authentication system and the stability will be gently increased.

3. PROPOSED SYSTEM

Architecture:

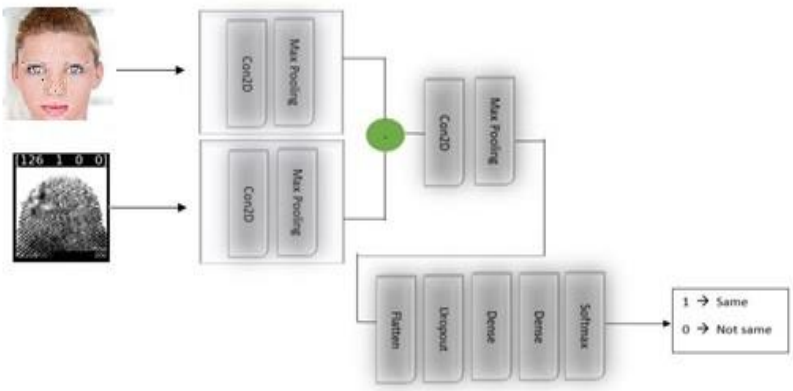

Figure1: Architecture of Proposed System

Layers in the proposed system:

I.Convolution layer:

Images are basically referred as pixel. Most of the values of the grayscale pixels are range between 0-255 and it consist of 6*6 matrix. For the coloured image is referred as RGB and it consist of 6*6*3 matrix. There are various layer like V1, V2, V3, V4, V5 and V6 that each and

every layers are responsible for finding information from the images and that layers are acting as filters. When the particular image is passed To the respective layer is responsible for finding vertical information. After that we can retransform the image by using Min-Max scaler in that we need to find the min value and the max value after that change the all min value to 0 and convert the max value to 255.

II. Max-Pooling Layer:

Max-pooling layer is basically referred as location invariant what is says that we should try to make our convolution neural network or kernel that are basically using should make automatically triggered where it able to detect the image. Usually after the convolution layer takes place after we can apply another filter called max-pooling filter and it can be of 3*3 or 2*2. The max pooling operation basically takes of the which of the value is higher in this pixel and it repeated for each and every pixels. The image has been properly detected because we are taking the high pixel values with the help of max-pooling filter.

III. Drop Out Layer:

When the Artificial neural network which is very deep that time we will understand that many weights and bytes parameters. When we have huge amount of weights and bytes parameter what will happen is that the Artificial neural network tense to overfit the dataset problem or particular use case. First we need to select our dropout ratio and the ratio is between 0<=p<=1. We need to select the subset of features in each and every hidden layer along with input features. According to the drop out ratio it randomly select the some activation function and it will deactivate it and it simultaneously moves to next layer and perform same function. And during backward propagation which ever neurons gets activated their weights will gets updated and every time features gets randomly selected and deactivate it.

IV. Flatten Layer:

The flatten layer is also called as fully connected layer. In this layer converting the pixel or data into a single dimensional array then the converted array is inputting to the next layer. In the flatten layer we need to create the single long feature vector using the output of the convolutional layer and the flattening is completed then the single long feature vector is pass through the artificial neural network as a input data and it has processed further.

4. RESULT COMPARISION

Table1 : Comparison of Proposed System with the existing system

Algorithms	Accuracy
FingerprintANN & FingerveinANN & FaceANN (Rajesh & Selvarajan)	99.23%
Fingerprint and Palmprint Multi-Modal Biometric Security System P Appala Naidu et al.	97.18%
Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint	99.12%
Proposed system using Convolutional neural network	99.58%

5. CONCLUSION

Multimodel biometric authentication device essentially is the combination of several human biometric identities. Compared to uni model biometric system, it is an efficient authentication method. The experiment results in the overall performance of the proposed multimodal system being higher than the other CNN-based multimodel biometric system. We may also infer from the results that we obtained that the effect of the pre-processed algorithm

improved the precision rate of the proposed method. Dropout technique plays an significant role in increasing the efficiency of the recogintion, it also helps to lower the system's error rate. Future research can be expanded further by accurately modeling feature extraction techniques and handling the database more efficiently and using different levels of fusion to perform biometric method.

REFERENCES

1. Mohamed hammad , yashu liu, and kuanquan wang, " Multimodal Biometric Authentication Systems using Convolution Neural Network Based on different level fusion of ECG and Fingerprint " , December 13, 2018.
2. D. Jagadiswarya, D. Saraswady, " Biometric Authentication using Fused Multimodal Biometric" , International Conference on Computational Modeling and Security ,2016.
3. N. Lalithamani and M. Sabrigiriraj, " Palm and hand vein-based fuzzy vault generation scheme for multibiometric cryptosystem, February 2015.
4. P Appala Naidu, CH GVN Prasad, Prasad B, Bhanuja Bodla, " Fingerprint and Palmprint Multi-Modal Biometric Security System" , 10 May 2017.
5. Zhendong Wu, Jiajia Yang, Jianwu Zhang, Hengli Yue, "Multibiometric Fusion Authentication in Wireless Multimedia Environment Using Dynamic Bayesian Method", 18 November 2018.
6. Saritha Reddy Venna, Ramesh Babu Inampudi, " MMBAS-NS: Multimodal Biometric Authentication System and Key Generation Algorithm for Network Security on Mobile Phones", January 2019
7. El mehdi Cherrat, Rachid Alaoui and Hassane Bouzahir, " Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images ", 6 January 2020.
8. Soleymani S, Dabouei A, Kazemi H, Dawson J, Nasrabadi NM, " Multi-level feature abstraction from convolutional neural networks for multimodal biometric identification",2018.
9. Park E, Kim W, Li Q, Kim J, Kim H," Fingerprint liveness detection using CNN features of random sample patches",2016.
10. Itqan KS, Syafeeza AR, Gong FG, Mustafa N, Wong YC, Ibrahim MM,"User identification system based on finger-vein patterns using Convolutional Neural Network", 2016.
11.E.Balraj,T.Abirami,"A multibiometric authentication system using fusion level techniques",Jan 2020.