Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 12, Issue 12, December 2023

Multi-Modal Biometric Authentication System Using Cnn

Prathamesh Shrinivas Shukla
Dept. of Computer and Communication Engineering
Manipal University Jaipur, Jaipur, Rajasthan, India

***Abstract*—: In practical applications, unimodal biometric systems rely on evidence from a single source of information for authentication. However, these systems encounter challenges, including noise in the sensed data arising from factors such as the repeated use of fingerprint sensors and intra-class variation. For instance, the reliability of a fingerprint-based system may be compromised due to variations in the sensed data caused by repeated sensor use.**

To address these limitations, the adoption of a multi-modal biometric authentication system becomes pivotal. This approach enhances the robustness and reliability of the authentication process by incorporating multiple biometric traits. The utilization of multiple modalities ensures that the system is better equipped to discern the presence of a live user at the data acquisition point, thereby mitigating the impact of potential challenges associated with unimodal systems.

Common examples of multimodal biometrics involve the fusion of different biometric modalities, such as face and fingerprint or iris and fingerprint. By integrating diverse biometric sources, a multimodal approach leverages the strengths of each modality, contributing to a more resilient and effective authentication system in real-world scenarios.

***Keywords*:** Multi-modal Biometric Authentication System; Convolution Neural Network; Face Recognition; Fingerprint Recognition

I. INTRODUCTION

A biometric system is designed to assess at least one physical or behavioral attribute, encompassing distinctive features like fingerprints, palm prints, facial characteristics, iris and retina patterns, ear structure, voice, signature, gait, and hand-vein data. These attributes are variably referred to as traits, indicators, identifiers, or modalities.

Functioning as an identification system, a biometric system utilizes diverse biometric features, examining physiological characteristics such as fingerprints, eye retinas and irises, voice patterns, facial features, and hand measurements for authentication. These systems, often termed as unimodal biometric systems, rely on the unique and intrinsic aspects of an individual's biological or behavioral characteristics to determine or verify their identity.

A multimodal biometric system integrates outcomes derived from multiple biometric characteristics to authenticate individuals. Compared to unimodal systems, multimodal biometric systems are considered more dependable since they incorporate several independent biometric modalities. Employing multimodal biometrics can lead to a significantly precise and secure identification system, addressing the limitations of unimodal systems, which may lack accuracy due to non-universality.

Unimodal biometrics are susceptible to inter-class similarities, a challenge particularly evident in facial recognition applications. In instances involving identical twins, the inherent resemblance between subjects poses a notable complication, wherein the imaging system may encounter difficulties in distinguishing between the two individuals. Unimodal biometric systems are quite vulnerable to spoof attacks where the data can be imitated or forged. For example, fingerprint recognition systems can be easily spoofed using rubber fingerprints. These reasons make it inevitable for modern systems to use multiple models.

II. RELATED WORK

[1] This study undertakes an examination and comparison of various biometric modalities, including Face, Iris, Ear, Fingerprints, Signature, and Voice. The findings suggest that 1.) Facial, Fingerprint, and Iris biometrics emerge as the most suitable for incorporation into a biometric authentication system. 2.) The integration of two or more biometric modalities is identified as a strategy to enhance the robustness of a biometric authentication system.

[2] This study focuses on the integration of face and iris recognition within a unified framework. The authors employed K-Nearest Neighbours (K-NN) classification for image categorization. However, the inherent limitation of K-NN, characterized by potential inaccuracies and the risk of erroneous classifications, prompted the authors to enhance the classification accuracy. This improvement was achieved by implementing Fuzzy K-Nearest Neighbours (FK-NN) as an alternative approach.

In reference [3], the authors developed an automated attendance system utilizing students' fingerprints. The procedure involved preprocessing the fingerprint images to identify and highlight distinctive minutiae features. Subsequently, these features were encoded into a binary template and stored in the database. The stored templates were then utilized for the classification of fingerprints in the attendance system.

In [4] the author describes the advantages and disadvantages of biometric authentication system.

In reference [5], the authors employed the Hamming distance algorithm for the classification of iris images. Remarkably, they achieved an accuracy rate of 98%, coupled with a False Rejection Rate (FRR) as low as 1.85%.

In reference [6], the authors utilized a Convolutional Neural Network (CNN) to conduct image classification on a limited

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 12, Issue 12, December 2023

dataset comprising 10 classes. Impressively, they attained a commendable accuracy of 94%.

III. PROPOSED ALGORITHM

A. Design Consideration

- The System should accept Fingerprint and Face from a dataset.
- The System should create a Neural Network to match fingerprint from the dataset.
- The System should use a Convolutional Neural Network (CNN) as main component of the System
- The System should have an accuracy of at-least 80 percent.

A. Flow Chart

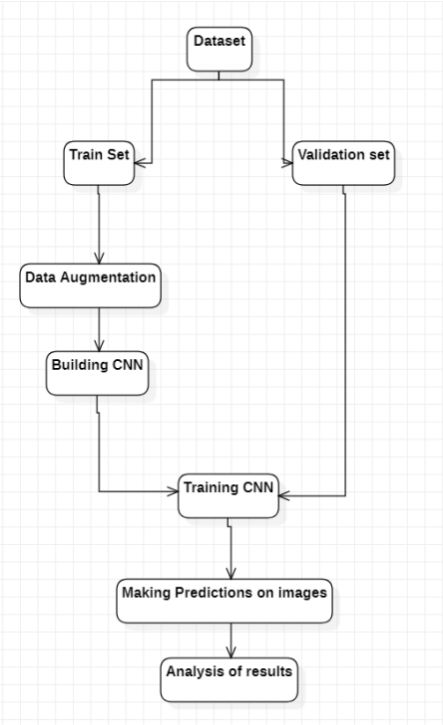

Figure 1: Working of the system.

IV. DESCRIPTION OF PROPOSED ALGORITHM

Aim of the proposed algorithm is to maximize the accuracy of the machine-learning models. The proposed algorithm (Convolution Neural Network) is used to create two models for face recognition and fingerprint recognition. The proposed algorithm is consists of three main parts.

Part 1: Convolution Layer:

A convolution layer transforms the input image to extract features from it. In this transformation, the image is convolved with a filter. A filter is a small matrix, with its height and width smaller than the image to be convolved. It is also known as a convolution matrix or convolution mask. This filter slides across the height and width of the image input and the dot product of the filter and the image are computed at every spatial position.

A convolution layer with an activation function ReLU was used to create the simulation. the rectifier or ReLU activation function is an activation function defined as the positive part of its argument:

$$f(x) = x^+ = \max(0, x)$$

where x is the input to a neuron.

eq. (1)

Part 2: Pooling Layer:

The pooling layer is used to reduce the size of the input image. In a convolutional neural network, a convolutional layer is usually followed by a pooling layer. A pooling layer is usually added to speed up computation and to make some of the detected features more robust. Pooling operation uses kernel and stride as well. In the example image below, a 2X2 filter is used for pooling the 4X4 input image of size, with a stride of 2. There are different types of pooling. Max pooling and average pooling are the most commonly used pooling methods a in a convolutional neural network.

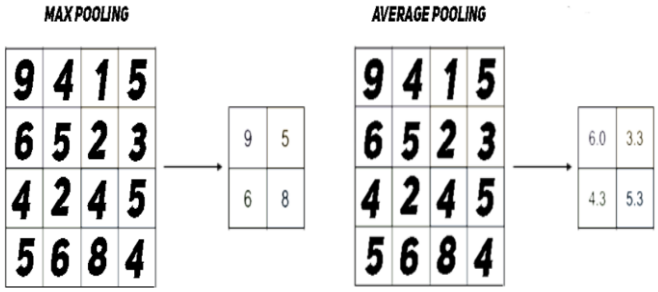

Fig 2: Max pooling and Average pooling layers.

Max pooling on left, Average pooling on the right Max Pooling: In max pooling, from each patch of a feature map, the maximum value is selected to create a reduced map. Average Pooling: In average pooling, from each patch of a feature map, the average value is selected to create a reduced map.

Part 3: Dense Layer:

Dense layers, also known as fully connected layers, in a Convolutional Neural Network (CNN) are layers where each neuron or node is connected to every neuron in the previous layer. These layers are responsible for learning global patterns and relationships in the input data. In contrast to convolutional layers that focus on local receptive fields and spatial hierarchies, dense layers aggregate information from the entire input.

In the context of a CNN, dense layers are typically used after the convolutional and pooling layers to make final predictions or classifications based on the extracted features. The dense layers serve as a classifier by learning how different features are correlated and contributing to the overall decision-making process.

V. PSEUDO CODE

Step 1: Import all the required libraries (TensorFlow, Numpy and Matplotlib)

Step 2: Import the dataset and split it into training and validation sets.

Step 3: Initialize a sequential model using TensorFlow.

Step 4: Add Conv2D Layer with ReLU activation function and add a MaxPooling Layer.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 12, Issue 12, December 2023

Step 5: Add another Conv2D layer with ReLU activation function with a MaxPooling Layer.
Step 6: Flatten the Layers.
Step 7: Add a dense layer of 128 nodes.
Step 8: Add a dense layer with the number of nodes equal to the number of classes in the dataset.
Step 9: Compile the model.
Step 10: Test the model.
Step 11: End.

VI. RESULTS

In this project I used two datasets for face and fingerprint each. Both the datasets had 10 classes and each class had 10 images of the same finger/face in different conditions. Some of the pictures are given below.

Fig 3: Subject has his mouth open.

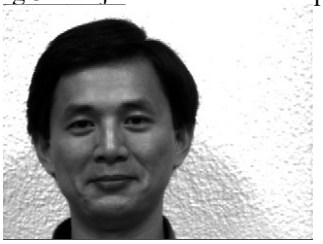

Fig 4: Subject us smiling

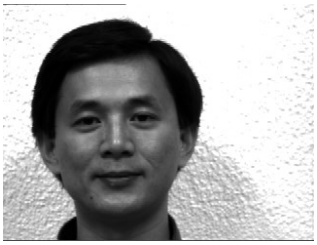

Fig 5: Subject has no expressions.

Fig 6: Fingerprint with noise

Fig 7: Clear Fingerprint

Fig 8: Partial Fingerprint

The above figures show the difference between all the images belonging to the same class.

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 318, 241, 128)	1280
max_pooling2d (MaxPooling2D)	(None, 159, 120, 128)	0
conv2d_1 (Conv2D)	(None, 157, 118, 128)	147584
max_pooling2d_1 (MaxPooling2D)	(None, 78, 59, 128)	0
global_max_pooling2d (GlobalMaxPooling2D)	(None, 128)	0
flatten (Flatten)	(None, 128)	0
dense (Dense)	(None, 128)	16512
dense_1 (Dense)	(None, 128)	16512
dense_2 (Dense)	(None, 10)	1290

Total params: 183178 (715.54 KB)
Trainable params: 183178 (715.54 KB)
Non-trainable params: 0 (0.00 Byte)

Fig 9: Model summary of Facial model.

Layer (type)	Output Shape	Param #
conv2d_9 (Conv2D)	(None, 386, 372, 128)	1280
max_pooling2d_9 (MaxPooling2D)	(None, 193, 186, 128)	0
conv2d_10 (Conv2D)	(None, 191, 184, 128)	147584
max_pooling2d_10 (MaxPooling2D)	(None, 95, 92, 128)	0
global_max_pooling2d_5 (GlobalMaxPooling2D)	(None, 128)	0
flatten_5 (Flatten)	(None, 128)	0
dense_10 (Dense)	(None, 128)	16512
dense_11 (Dense)	(None, 10)	1290

Total params: 166666 (651.04 KB)
Trainable params: 166666 (651.04 KB)
Non-trainable params: 0 (0.00 Byte)

Fig 10: Model summary of Fingerprint model.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 12, Issue 12, December 2023

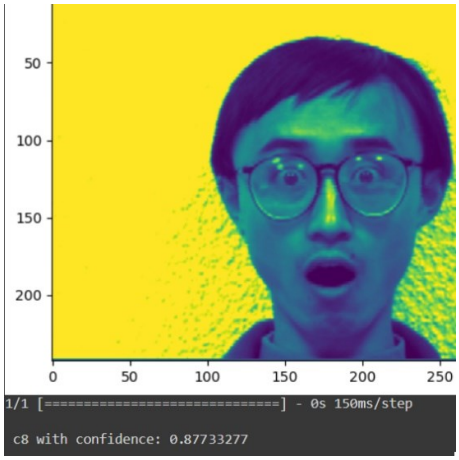

Fig 11: Face image detection at 87% accuracy

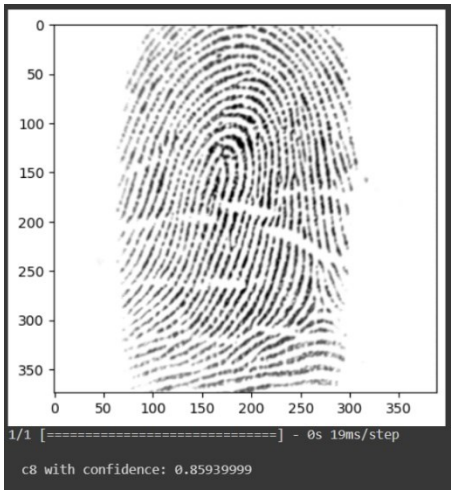

Fig 12: Fingerprint detection with 85% accuracy

Both the models, Fingerprint and Facial were able to attain an accuracy of 85% and 87% respectively. When passed a random image through the model.

VII. CONCLUSION AND FUTURE WORK

In this project, we employed unsupervised machine learning to match unknown fingerprints to classes within a dataset. Our approach involved the implementation of a Convolutional Neural Network (CNN) comprising two Convolutional layers with Rectified Linear Unit (ReLU) activation, two Max pooling layers, a GlobalMaxPooling layer, and two Dense layers. Notably, the fingerprint prediction model achieved a notable accuracy of 85%, while the Face model demonstrated a commendable accuracy of 87%. During testing, when comparing an image from the testing set with the training set, the model provided predictions with confidence scores of 0.85939999 and 0.87733277, as depicted in figures 11 and 12.

For future work, enhancing the robustness of Deep Learning algorithms and expanding the dataset size could further elevate accuracy and improve system security. Additionally, the incorporation of iris recognition, replacing or complementing face recognition, has the potential to fortify the system, ensuring a more resilient and comprehensive biometric authentication approach.

REFERENCES

[1] Jain, Anil & Ross, Arun & Prabhakar, Salil. (2004). An Introduction to Biometric Recognition. Circuits and Systems for Video Technology, IEEE Transactions on. 14. 4 - 20. 10.1109/TCSVT.2003.818349.
[2] Ammour, B. & Boubchir, Larbi & Bouden, Toufik & Ramdani, Messaoud. (2020). Face–Iris Multimodal Biometric Identification System. 9. 10.3390/electronics9010085.
[3] Rahman, Md. Mijanur. (2021). Study on Introducing Biometric Fingerprint Authentication in Automated Student Attendance System. 10.9734/bpi/nvst/v4/4580F.
[4] Kavita Gupta, 2017, Review Paper on Biometric Authentication, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) VIMPACT – 2017 (Volume 5 – Issue 23),
[5] Mr. Prasad M. Rajpure, Mr. Swapnesh S. Shinde, Mr. S. V. Khobragade, 2014, An Iris Authentication: Best Method of Biometric Authentication, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 03, Issue 05 (May 2014),
[6] Sharma, Atul and Phonsa, Gurbakash, Image Classification Using CNN (April 24, 2021). Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2021