EasyChair Preprint

№ 7634

Introduction to Multimodal Biometrics Using OpenCV

Abhimanyu Kumar and Tarushi Singh

March 28, 2022

Introduction to Multimodal Biometrics using OpenCV

Abhimanyu Kumar
school of computer science and engineering(Galgotias University) Greater noida ,uttar predesh,India
abhimanyuk1212@gmail.com

Tarushi Singh
school of computer science and engineering(Galgotias University) Greater noida ,uttar predesh,India

***Abstract*— Biometrics is defined as analysis of people's unique physical and behavior wise characteristics. Biometric systems are used for identification of entity, controlling the access and find the identity of the personals who are under observations. Some commonly used biometrics are face, iris, fingerprints. Recognition of identity with the help of biometrics offer a lot of potential advantage over methods with knowledge. Uni modal biometrics is a widely tested biometric system nowadays but there are many issues that has been encountered with the system using mono modal biometrics. An extension of it is multi modal biometrics is been developed which extracts the features of multiple biometrics and using algorithms work on it to produce a fused modal and identifies the authorized entity using algorithm from that fused modal. Technology is so much broad now that biometric systems are able to provide knowledge based as well as token based systems. Confidential data can be access by only those individuals who are accurately identified by the biometric system. The modal will be working on multi biometric system. This modal will try extract features from multiple biometrics and try to fuse them to form it single identifiable character. The modal will consist of new algorithms which will help it to match the identity**

Keywords: Artificial Intelligence, Deep Learning, Machine Learning.

I. INTRODUCTION

Biometric are measurements or device which from the physical characteristics of a person or an individual detects its identity. Biometric can consists of face, fingerprints, iris and retina scan, palmprints, etc. Biometric is one of the important field in computer science which is used for authentication and controlling the access. Now it is found that authentication is more and more important for operating any type of things on computer networks so due to this reason an automatic personal authentication system was developed with the name of biometrics. There are mainly two types of biometrics Unimodal Biometric System and Multimodal Biometric System.

Unimodal Biometric System is a type of system which extracts features from single trait and finds the identity of the individual using that trait. Unimodal Biometric System faced several problems such as noisy data i.e. incorrect and inaccurate matching, intra class variation i.e. the data which has been extracted during the enrollment phase does not matches with the data collected during the verification phase, Interclass similarities i.e. if features of multiple entities collides, Non universality i.e. if some person doesn't able to provide their biometric due to disabilities, Spoofing i.e. if someone is imitates the data.
Due to all these disadvantages unimodal biometric system provided very poor performance which lead to evolution of biometric system which was merged with two or more biometrics and these modals were called as multimodal biometric system which is now been used for identification authorization and verification. Multimodal Biometric System provided high accuracy and security. Due to this reason, it is now being used in security system in bank, check cashing, credit card transaction and many other transaction system.

II. LITERATURE REVIEW

In He et al. in the year 2010, a modal with three biometrics was proposed with fingerprints, face and veins of the finger. The scoring was doing by Support Vector Machine scoring techniques. This system attained a very high accuracy of (GAR)mean of 0.99. [1] Pflug and Busch prepared a 2d and 3d modal of biometric from ear. This system used ear covering as the identification medium. [1] Huang et al. in the year 2013 proposed a modal with the help of face and ear and using feature level fusion to produce a conclusion identification score. [2] Gayatri Bokade with his team combined face and prints from palm. This modal obtained a fusion modal using fusion algorithm. GAR values produced by this modal was approves 82% using palm and using face it was approx 89 percent which on fusion produced a GAR values of 95% .[4] Md.Monwaret al. proposed a biometric modal with th help of face, ear and signature. The PCA(Principle Component analysis was used with rank level using logistic regression and borda count. [6] P. Kartik et al. used the biometrics face, speech and signature. The extraction was done with the help of PCA techinique along with linear discriminant analysis (LDA). For scoring method is done my sum rule. [3] S. Ribaric et al. used fingerprint, palmprints and face scan as the biometrics. Algorithms such as minmax, zscore and median double sigmoid, median-MAD for the feature extraction from the biometrics and then bayers based normalization was used to find the final score for identification.

[6] T Murakami et al. invented a multiple biometric with iris, face and fingerprint. This system usdbayes decision rule for extraction of features and permutation based indexing for producing the final score. [2] Z. Cheng et al. produces a multispectral face image using biometric system with four different fusion techniques these techniques were hidden markov modal , mean fusion, linear discriminant, k nearest neighbour. The team

concluded that the output from hidden markov modal seemed to be most reliable among all the four techniques. [3] A. P Yazdanpanahet al. used face and gait and used gabor wavelet with fusion technique and weighted sum and weighted product for producing the score.
[5] Mahesh P.K. et al. proposed a multimodal biometric using speech and palm print. The extraction method they used was Kernel PCA and Mel frequency Cepstral coefficient. The scoring level was determined by using weighted sum technique. [5] N Gargouri Ben Ayed et al. proposed a multimodal biometric system using fingerprint and face. They used gabor wavelet and local binary pattern with the fusion technique and the weighted sum procedure was used for finalizing the score for identification. [2] A.Kumar et al. discovered a multimodal system which was extracting features from face and ear using haar wavelet and scale invariant feature transform technique. [5] S. Jahanbin et al. proposed a new modal using face recognition using gabor wavelet. They first computed the gabor coefficient using the fused modal and used that coefficient to determine the final score.[4] F. Yang et al. proposed a multimodal biometric framework using fingerprint, palmprint and hand geometry using support vector machine for fusion and determined the matching score using that fused modal. [1] A. Bhattacharjee et al. proposed a multimodal biometric using iris and speech used Daubechies wavelet for extracting features and decision making was using feature level scoring technique.

III. FLOW OF ARCHITECTURE

1. A use case diagram is a graphical depiction of a user's possible interactions with a system. A use case diagram shows various use cases and different types of users the system has and will often be accompanied by other types of diagrams as well. The use cases are represented by either circles or ellipses.

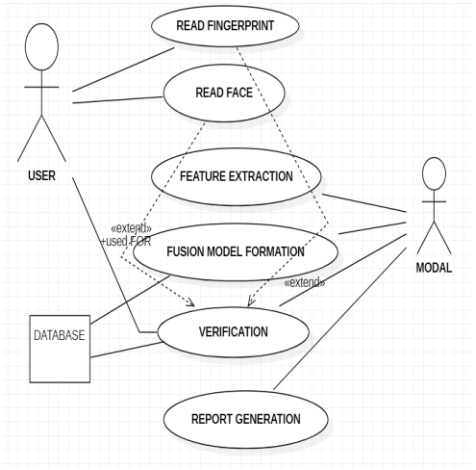

Figure1: Use case scenario

2. A data flow diagram shows the way information flows through a process or system. It includes data inputs and outputs, data stores, and the various subprocesses the data moves through. You can use these diagrams to map out an existing system and make it better or to plan out a new system for implementation.

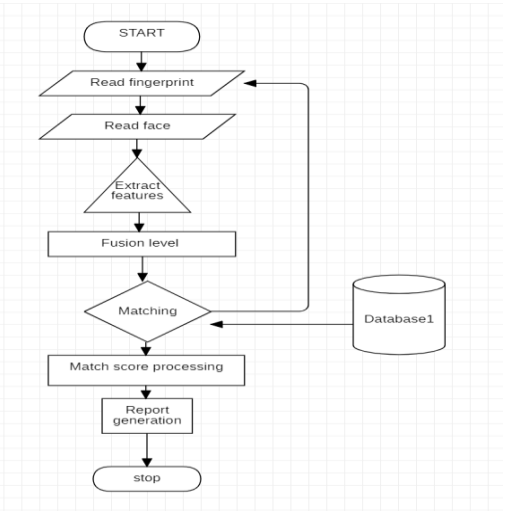

Figure 2: Data flow diagram

IV. FEATURES OF THE APPLICATION

Being an AI/ML model there are lot of library and modules used which we will show you below: -

OpenCV is a Python open source library utilized for PC vision in Artificial knowledge, Machine Learning, face acknowledgment, face location and so on.It represents Open Source Computer Vision Library. OpenCV is utilized to foster constant PC vision applications. It is fit for handling pictures and recordings to distinguish articles, faces, or in any event. .Right now OpenCV upholds a wide assortment of programming dialects like C++, Python, The LBPH utilizes 4 boundaries:
Radius: the sweep is utilized to fabricate the round nearby paired example and addresses the range around the focal pixel. It is generally set to 1. Neighbors: the quantity of test focuses to assemble the roundabout nearby twofold example. Remember: the more example focuses you incorporate, the higher the computational expense. It is generally set to 8. Lattice X: the quantity of cells the flat way. The more cells, the better the lattice, the higher the dimensionality of the subsequent component vector. It is typically set to 8. Network Y: the quantity of cells the upward way. The more cells, the better the network, the higher the dimensionality of the subsequent element vector. It is normally set to 8. Enter Haar classifiers, classifiers that were utilized in the principal ongoing face indicator. A Haar classifier, or a Haar course classifier, is an AI object location program that recognizes objects in a picture and video

V. Module Description for Face Recognition

1**.**Generate data set module :-

This module mainly gets the images of the person from the webcam and crop it in store it in the folder of the name the webcam attached to the system the webcam clicks the image of the face in front of it when the ‘s’ button in the keyboard of the person. This module follows different steps as follows
Step 1:- initialize the haarcascade_frontalface_default.xml

Step 2:- set the user ID and user input
Step 3:- gets the video from the video capture function save it into a path described in the save image function
Step 4:- it will convert the image into grayscale and get the coordinates of the location of the image in the picture using the code
cv2.rectangle(img, (x, y), (x + w, y + h), (0, 255, 0), 2)
Step 5:- when as button of your keyboard is pressed the camera captures the image and save it into the location for the path of the image of that ID with the name of the person.

2.Train module:-

This module is required to train the data set the data set and obtains the filename training.yml.
Step 1:- It will extract all the IDs of the faces and create a list of it
Step 2:- It creats faces and names using Numpy Arrays
Step 3:- it will initialized the classifier and classify the modal
Step 4:- based on the classification the module trains the modal
When the modal is trained a file training is produced with extension .yml with all the trained data. The training is based on LBPH FaceRecognizer which is a part of cv2 library.

3.Recognize module :-

User to detect and recognize the correct face recognize we need to initialize the haarcascade frontal face default XML. This module creates a recognizer using the lbph face recognizer. Using this object the body will read the training.yml file. Just step this module will perform are
Step 1: the body will create a list of all the names of the person in his allies in the data set corresponding to their Id-1 as their index
Step 2: the module will read the image which is to be checked and it will convert it into a grayscale
Step 3: the fade cascade class will detect Gray image and scale it according to the given value and then the module will create a rectangle around the face detected
Step 4: Using recognizer.predict the module will recognize the idea of the person
Step 5: if the ID is found the module will print the name of the person created the rectangle created the idea is not found or not predicted it will

VI. **Module Description for Face Recognition**

1.Removedot module:

This module will take the 2 fingerprints that are to be matched one from the database and another from the person whose fingerprint is to be matched and it will do the following steps for the preprocessing of the fingerprintsThis module basically works as preprocessing module
Step 1: It enhances the image using numpy array and and select the rich structures only which are to be matched select the rich structures only which
Step 2: Remove all the impurities from the fingerprint and and noisy data which doesn't have any work in case of recognizing the fingerprint and matching them
Step 3: stores the 2 fingerprints after doing all these 2 processes as the result of the module

2.Get_descriptors module:

This module will take this module will take the returned images that are pre processed from the remove door module and it will extract features from that images that are to be matched or those features can define that fingerprint is of that person. It performs following steps to extract features from the preprocessed fingerprintThis module works as a feature extraction module
Step 1: First it sets a threshold value that is needed to compare the values of the fingerprint that is in the saved in the dataset with the verification Bank of fingerprint if it is equal to or above the threshold the fingerprints are matched for this purpose a threshold value is found from the fingerprint saved in the data set
Step 2: the 2 fingerprint using the remove dot function are already pre processed now thinning of the fingerprint is done that is basically some part are extracted from where identifiable characters are generated
Step 3: now using those identifiable character key points are extracted in our project the key points are extracted using Harris corner extraction feature detector
Step 4: both key points from the 2 preprocessed fingerprints are stored as a return of this module

3.main_matching:

This module will take the extracted features from the last module that is get descriptor module and it will match the key points that is returned in that module and subsequently find the matching score
Step 1: Store the key points of the fingerprints in a variable
Step 2: then draw the keypoint map for calculating the score
Step 3: use match.distance for matching the key points of the fingerprints
Step 4: if the calculated score is greater than the threshold score then the system should print that the fingerprint is of the person that is to be identified else the system is the system will show that the fingerprint is not the intended fingerprint or simply the fingerprints are not matched.
If a person is satisfied by both face recognition and fingerprint verification the system that is using this technique will allow the person to get access to his system else it will deny the access

VII. **Conslusion**

To the extent that far as our insight is concerned, the OpenCV library is continuously beneficial, has better execution for face detection and recognition. It also infers that with OpenCV, it's more intelligent to collect affirmation applications for the IOT stage. Note that solitary HOG computation has been examined while checking for various computations, for instance, the Haar course, it works longer, yet turns out extra exhaustively, assuming there are a part of photos later on for a few, it is reasonable to consider using this technique. Regardless, the design reasoning also the vital reasons for making an application affirmation, were discussed. Haar Cascade

Classifier works better which has the best precision when diverged from some different estimations like LBP, etc.,

VIII. Future Scope

We purposed LBPH for picture detectiont and face recognition in the observation camera in a particular region. Having gotten great outcomes from different trial dissects of this method, they additionally give legitimate outcomes to impediment, present variety. In this way, the proposed framework permits acknowledgment and Showing of appearances in a controlled climate. As AI is very significant these days, there are numerous regions where this work can be extended. In executing this venture, we have recognized a few regions for development, for example, Limitations of distance, the development of calculations and camera characteristics, even utilizing DNN procedures.

Exactness can be worked on in the future, which is all the more straightforwardly identified with our work. The system had a lot of difficulties while playing with lights so it can be worked out in the future another works that can be done in the future is combining the result of this biometric with other biometric And create a multimodal biometric system.

IX. Reference

1. A Comparative Analysis of Biometrics Types: Literature Review, by Mohammad Al Rousan and Benedetto Intrigila, 2020.
2. An Overview Of Multimodal Biometrics, P.S Sanjekar and J.B. Patil, 2013.
3. Literature review on multimodal biometrics, S. Arunarani and R. Gobinath, 2018.
4. A review of biometric technology along with trends and prospects, J.A.Unar, Woo Chaw Seng and Almas Abbasi, 2014.
5. Multimodal Biometric system using Iris and Fingerprint, Nabil Hezil, Amir Benzaoui, Boukrouche Abdelhani, 2013.
6. The Basics of Information Security (Second Edition), Jason Andress, 2014.