International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on Multimodal Biometric System

Atharva Jadhav[1], *Sarvesh Gholap*[2], *Ashish Kambale*[3]

[1,2,3]Student, Department. Electronics and Telecommunications SCTR's Pune Institute of Computer Technology, Pune 43, Maharashtra, India
atharva4102001@gmail.com[1], sarveshgholap31@gmail.com[2], ashishkamble1221@gmail.com[3]

ABSTRACT:

Design of a biometric based attendance monitoring system for educational institutions to upgrade the current system of attendance into more efficient method has been a need of the current technical trend This requires the analysis of various authentication algorithms that are processed in the industry currently. Unlike the traditional system of attendance requiring manual entry in hard copy as well as the individual face detection of a student, the project focuses on multiple faces detection while during the hours of class. Thus, by researching efficient machine learning algorithms, a multimodal biometric system will aim at resolving t¬¬he flaws that existed in the current scenarios of manual verification while bringing attendance taking to a whole new level by automating most of the tasks. embarks importance of more accurate and faster techniques of biometric to aid to the ease of the requirement of ever growing and rapid technological advancements. The project manages to compare the existing methods of implementation of biometric authentication and analyse the accuracy and errors to conclude for the more efficient method that has been implemented thus far.

KEYWORDS: Feature Identification, Detection and Authorization, Machine Learning, Automatic Speech Recognition, Linear Binary Histogram Pattern, Convolutional Neural Networks, MFCC.

I. INTRODUCTION

Body measurements and computations known as bio-metrics are used to study human traits. The categorization of a biometric system is done as per the characteristics utilized for authentication. There are various methods for identification such as Face Recognition, Iris Recognition, Voice Recognition, Fingerprint Recognition, etc. As a result, so-called multi-factor authentication protocols were created, which make use of additional authentication procedures. Advanced biometrics are being used to accomplish a number of government initiatives, including e-passports, e-licenses, driver's border control, and national identifications.

1.1 Feature Identification

A multi-factor based Feature extraction system acts as an efficient method to account for authentication. Many different systems use numerous detection and recognition algorithms however the main parameter that affects majorly is the accuracy and the percentage of uncertainty. As a result Facial and Vocal traits are used. These charateristics, however are subject to exploitation, provide a higher degree of security. These use neural networks and deep learning algorithms.

1.2 Feature extraction

Feature extraction is where relevant features are extracted from the preprocessed biometric data. These features capture the unique characteristics of the individual's biometric trait and are used to represent the data in a more compact and informative manner. The choice of feature extraction techniques depends on the type of biometric trait being used.

1.3 Machine Learning

ML methods have been applied to many disciplines including image processing and biometrics. The two most popular machine learning strategies are supervised and unsupervised learning. For the purpose of training algorithms, labelled examples that resemble input with preferred output are used. With the aid of unsupervised learning, instances without historical labelling are learned. Unsupervised learning's two main goals are to find some structure in the data and to explore the data. The basis for

any biometrics method is some kind of matching methods which typically are one to one in case of verification and one to many in case of identification. With embedded ML in biometric systems, sometimes tedious tasks such as one to one or one to many matching tasks can be done automatically and seamlessly. In particular, Deep Learning (DL), a specific ML approach based on neural nets composed of many layers, has been used in different biometrics applications. DL methods exhibit the ability to create robust and reliable authentication models

II. LITERATURE REVIEW

2.1 Traditional biometrics

It refers to the use of physiological or behavioral characteristics of individuals for identification or authentication purposes. These biometric traits are inherent to individuals and are relatively stable over time. Some commonly used traditional biometrics include:

Fingerprint Recognition: This is one of the oldest and most widely used biometric modalities. It involves capturing and analyzing the unique patterns of ridges and valleys on an individual's fingertips.

1. Iris Recognition: Iris recognition involves capturing and analyzing the unique patterns present in the colored portion of the eye (the iris). The intricate and stable nature of iris patterns makes it a reliable biometric modality.
2. Face Recognition: Face recognition uses facial features, such as the arrangement of eyes, nose, mouth, and other facial characteristics, to identify or verify individuals. It can be performed using images or video sequences.
3. Voice Recognition: Voice recognition utilizes the distinctive vocal characteristics of individuals, including pitch, tone, and other speech patterns, to verify their identity. It involves analyzing voice samples for authentication purposes.
4. Hand Geometry: Hand geometry recognition analyzes the physical features and proportions of an individual's hand, including finger length, width, and knuckle placement, to establish identity.
5. Signature Recognition: Signature recognition involves analyzing the dynamic characteristics and unique features of an individual's signature for verification purposes. It can be used for both offline (static image) and online (capturing the signature process) verification.
6. Retina Recognition: Retina recognition involves capturing and analyzing the unique patterns of blood vessels at the back of the eye (the retina). It requires specialized imaging equipment and is considered highly accurate.

These traditional biometric modalities have been widely adopted in various applications, including access control systems, border control, time and attendance tracking, and forensic investigations. Each modality has its own strengths and weaknesses in terms of accuracy, usability, cost, and privacy considerations. Additionally, multimodal biometric systems combine multiple traditional biometric modalities to enhance overall performance and reliability.

2.2 Principal Component Analysis

PCA is based on a statistical procedure that uses an orthogonal transformation which transforms a set of correlated variables into a linearly different variables called principal components. The number of principal components is less than or equal to the number of original variables [2]. The basic formula relates to statistics, standard deviation, eigenvectors. The entire subject is based on a big set of data, that is to be analysed in terms of the relationships between the individual points in that data set [3].

PCA works by transforming the original feature space into a new coordinate system, where the first axis (principal component) captures the maximum variance in the data. The subsequent axes, called the second principal component, third principal component, and so on, capture the remaining variance in decreasing order.

Here's a step-by-step overview of how PCA works:

1. Standardize the data: PCA assumes that the data is centered around zero and has a unit variance. Therefore, it is important to standardize the dataset by subtracting the mean and dividing by the standard deviation for each feature.
2. Compute the covariance matrix: The covariance matrix measures the relationship between the different features in the dataset. It represents how changes in one variable are associated with changes in other variables.
3. Calculate the eigenvectors and eigenvalues: The eigenvectors represent the directions or axes of the new feature space, and the corresponding eigenvalues indicate the amount of variance explained by each eigenvector. The eigenvectors and eigenvalues are derived from the covariance matrix.
4. Select the principal components: The eigenvectors are ranked based on their corresponding eigenvalues, and the top-k eigenvectors are chosen to form the principal components. These principal components explain the most significant variance in the data.
5. Transform the data: The original dataset is projected onto the new coordinate system defined by the principal components. This transformation results in a new set of uncorrelated variables called the principal component scores.

2.3 Signal Processing

A project on Signal Processing, specifies the use of different DSP modules where each biometric trait is captured then features are extracted from that captured trait, based on that extracted features these traits are classified like “accept or reject”.

1. Signal acquisition: The first step is to use sensors or transducers to get the desired signal.
   The signal may be electrical, optical, or acoustic, among other things.
2. Preprocessing: To get rid of noise, artefacts, or undesired components, the signal is frequently put through preprocessing after it has been ac quired.
3. Filtering (using lowpass, highpass, or bandpass filters, for example), noise reduction, amplification, and resampling are a few preprocessing methods.
4. Feature extraction: To capture a signal's important qualities, pertinent features must be extracted from the signal.
5. Feature extraction techniques can include approaches like Fourier analysis, wavelet analysis timefrequency analysis, or statistical analysis, depending on theparticular application.

III. PROPOSED METHODOLOGY

3.1 Linear Binary Histogram Pattern

Real time detection and recognition is implemented using Linear Binary Histogram Pattern for implementing the proposed system for Phase 1 - Facial Recognition and CNN will be used for Phase 2 – Voice Authentication. These ML algorithms use a manual created database updated in real instances each time a new user is to be uploaded. The facial recognition system uses an auto-focus webcam for capturing the faces of individuals. Face detection here is handled by using python libraries and is implemented by the most efficient algorithm which is Local Binary Pattern Histogram. An experiment dataset of the group members is collected through a .py file. As and when faces are detected by the camera depending on the requirement of detection either the image or the video is tested. The LBP is a simple yet very efficient texture operator which labels the pixels based on a threshold value of the neighbourhood, each pixel is served as a binary number. It has further been determined that when LBP is combined with histograms of oriented gradients (HOG) descriptor, it improves the detection performance considerably on some datasets. Using the LBP combined with histograms we can represent the face images with a simple data vector[1].

3.2 Convolutional Neural Networks

CNN is a type of deep learning algorithm that has been applied to different of computer vision services, including voice recognition. The key idea behind CNN is to learn a set of filters (also known as convolution kernels) that can capture useful features from the input audio data[6].

CNN architecture:

Input Layer: to take the audio input

1. Convolutional Layer: produces a set of feature maps that capture different aspects of the audio data.
2. Activation Layer: an activation function (such as ReLU) is applied to the output of the convolutional layer, introducing non-linearity into the network.
3. Pooling Layer: down-sampling feature maps produced by the convolutional layer, to reduce the spatial dimensionality while preserving the important features.
4. Output Layer: This layer produces the final prediction of the network.

During the training process, the CNN learns to optimize the filter weights to minimize a loss function that measures the difference between the predicted output and the true output labels. The optimization process is typically done using stochastic gradient descent (SGD) or one of its variants.

The project has targeted dual functioning proposing a multitude modal of biometric authentication, it applies latest technology of computer vision and and Machine Learning. Figure 1 describes the overall block model of the above proposed system.

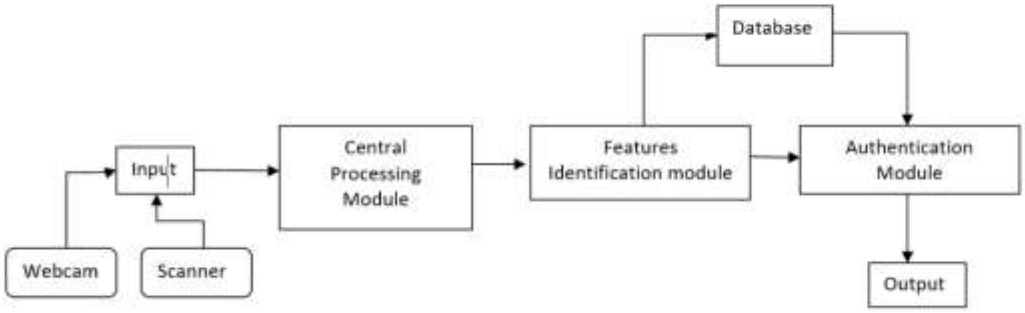


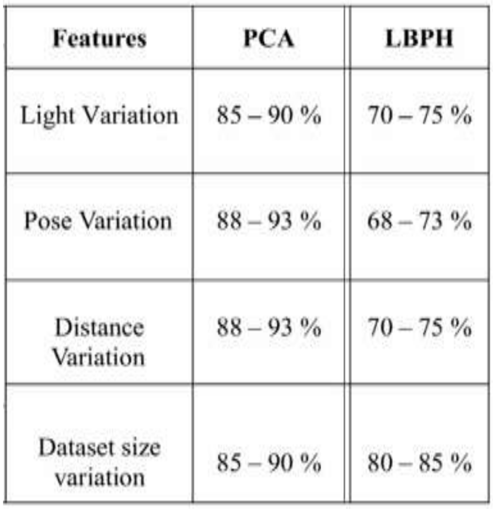
Figure 1: Block Diagram of the Complete system

As stated in the description the system uses dual input factor for detection and authentication through webcam and audio scanner. It allows live recognition of faces (multiple and individual) furthermore it assesses the audio input as given by the user to verify its authenticity.

Thereby increasing the efficiency of conventional biometric authentication systems.

The table below shows the comparative analysis of the PCA and LBPH algorithm based on a survey conducted by NFC Institute of Engineering and Fertilizers.[7].

.



Features	PCA	LBPH
Light Variation	85 – 90 %	70 – 75 %
Pose Variation	88 – 93 %	68 – 73 %
Distance Variation	88 – 93 %	70 – 75 %
Dataset size variation	85 – 90 %	80 – 85 %

Table 1: Comparative analysis of PCA, LBPH

FUTURE SCOPE

Further work can be done on this project to alert the student by sending SMS regarding the attendance. For this purpose, GSM module can be used. Currently we have developed a facial recognition system using LBPH method which gives result up to 71% correct. We can improve the face recognition algorithm by detecting the face in the dark light. Fingerprint detection system can be used as an alternative to the face detection in which each unique fingerprint will be scanned and attendance will be recorded.

CONCLUSION

The face detection and recognition and CNN algorithms were studied thoroughly taking number of the test results from different varying condition. For face recognition Local Binary Pattern Histogram method is used. After this the user is enrolled through a voice recorder where its authenticity is verified using a neural network model and authenticated by the face recognition, his name can be stored in a record and the same is displayed on successful verification. The paper discuss the survey of existing algorithms and methodologies for biometric authentication and derives the best among them based on several factors of differentiation.

REFERENCES

[1] Ms. Varsha Gupta and Mr. Dipesh Sharma, “A Study of Various Face Detection Methods” International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, pp. 6694-6697, May 2014.

[2] Jackson, J.E. (1991). A User's Guide to Principal Components (Wiley).

[3] Lindsay I Smith, A tutorial on Principal Components Analysis, February 26, 2002, page 2-8

[4] Nikhil Buduma, “Fundamentals of Deep Learning Designing Next-Generation Machine Intelligence Algorithms”, 1 st Edition, O’REILLY.

[5] A multimodal biometric system using fingerprint, face and speech AK Jain, L Hong, Y Kulkarni - 2nd Int'l Conf. AVBPA, 1999 - biometrics.cse.msu.edu

[6] IBM “Convolutional Neural Network” https://www.ibm.com/in-en/topics/convolutional-neural-networks

[7] “Comparative analysis of Face recognition methodologies and techniques” by NFC Institute of Engineering and Fertilizers, IEFR Journal of Scientific Research, Dec-2016