International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1200-1203 www.ijaem.net ISSN: 2395-5252

Facial Recognition Using FES Algorithm

[1]P. Matheswaran, [2]T. Guru Prasad, [3]M. Akash Chandran, [4]K. Matheshwaran

[1]*Assistant Professor, K. Ramakrishnan College of Technology*
[2,3,4]*UG Student, K. Ramakrishnan College of Technology*

Submitted: 15-04-2022 Revised: 27-04-2022 Accepted: 30-04-2022

ABSTRACT

Face recognition technology is a type of biometric technology that identifies a person's facial features through images of their faces. It collects images and then processes them automatically through algorithms such as Fisherface, Eigenface, SURF. This paper demonstrates the related research of face recognition from different perspectives. It also describes the development stages and the related technologies of face recognition. We innovate the research of face recognition for real conditions, also some specific evaluation standard for improved security and a general database to store facial data. Face recognitions has become the future and has many potential application prospects which also includes FACIAL RECOGNITION USING FES. We will be studying the implementation of variousalgorithmsinthe field of securevoting methodology, since each vote matters. One vote can make a major difference thus, we have two levels of verification which will used for the voters in our proposed system. The first stage is UID Verification using Government Proofs, second stage of verification includes the use of various algorithms for facial recognition and verification. These two-stage verification enhances the security features of existing facial recognition and verification.

I. INTRODUCTION

- Facial recognition is a category of biometric software which works by matching the facial features.
- There are two levels of verification which were used for the voters in our proposed system. The first is UID verification, second level of verification includes the use of various algorithms for facial recognition.
- The face plays a vital role in social interactions. As a form of identifying people, facial recognition is increasingly trending worldwide as an exceptionally safe and reliable security technology. Because of its high level of security and reliability, it is gaining considerable attention from corporate and government organizations.
- Furthermore, unlike other biometric security solutions such as palmprints and fingerprints, FR systems are able to capture biometric measurements of a person from a distance without interacting with them.
- Many organizations refer to this technology as a crime deterrent since it can identify people with criminal records or other legal issues. Therefore, this technology is becoming essential for numerous residential buildings and corporate organizations especially in voting system.
- Using this technique, you can recognize a human face and then compare it with previously recorded. This feature increases the significance of the method and makes it widely applicable. It is developed with user-friendly features and operations that include different nodal points of the face. There are approximately 80 to 90 unique nodal points of a face. FR measures these nodal points by creating a code called the faceprint, which identifies aspects such as the distance between the eyes, the length of the jawline, the shape of the cheekbones, and the depth of the eyes. These codes are created using Eigenface Algorithm which in turn creates eigenvectors. Systems based on 2D graphics are now available on 3D graphics, which improves accuracy and reliability.
- Biometrics refers to the measurement and statistical analysis of biological data. Utilizing biological features like the face, iris, and retina, biometric systems identify individuals through authentication. Face Recognition is only used here.
- Thus, FR has become a popular topic in computer science related to biometrics and machine learning. A major goal of machine learning is to develop algorithms for

performing a task-machine learning related to the field of computational statistics and mathematical optimization. Machine learning algorithms consume a great deal of resources, so it would be better if they were run in a distributed environment such as cloud computing, fog computing, or edge computing.

- In cloud computing, shared resources such as services, applications, storage, servers, and networks are utilized to maximize efficiency and achieve economies of scale.
- Facial Recognition has multiple algorithms to implement like CNN (Convolution Neural Network),

II. LITERATURE REVIEW:

Since a great deal of development has been made in machine learning, the computing environment, and recognition systems, many researchers are pioneering the concept of pattern recognition and identification with different biometrics through the use of a variety of building mining models.

Diaa Salama AbdELminaam, Abdulrhman M. Almansori, Mohamed Taha and ElsayedBadr proposed a complete Facial Recognition system using transfer learning in fog computing and cloud computing. To overcome the occlusions, expressions, illuminations, and pose conditions. Deep convolutional neural networks (DCNN) are proposed. The experimental results confirm that the proposed method is superior to all other algorithms. The suggested algorithm is more accurate (99.06%), more precise (99.12%), more recall (99.07%), and more specific (99.10%) than the comparison algorithms. In addition to the proposed algorithm, other popular machine learning algorithms, such as the DT, KNN, and SVM algorithms, were also tested on three standard benchmark datasets to demonstrate the proposed DCNN's efficiency and effectiveness.In terms of the input image, FR encounters many difficulties and challenges such as different facial expressions, subjects wearing hats or glasses, and varying brightness levels.

M.A.O. Vasilescu and D. Terzopoulos applied a concept of multilinear algebra, a higher-order tensor algebra, to separate these factors (such as different facial geometries, expressions, head poses, and lighting conditions) and derive an optimal representation of facial images. TensorFaces' representation results in higher facial recognition rates than standard Eigenfaces. (Pending…..)

Faizan Ahmad, Aaima Najam and Zeeshan Ahmed evaluated different methods of face detection and recognition, as an initial step to video surveillance, built a complete solution for image-based face detection and recognition with high accuracy. Tests on various face-rich databases in terms of subjects, pose, emotions, race, and light have led to a proposed solution. However, the proposed system has false detections in facial features. A complicated dataset is required for this system.

SerignModouBah and FangMing proposed an improved face recognition algorithm in attendance management system. Using the Local Binary Pattern (LBP) algorithm together with advanced image processing techniques such as Contrast Adjustment, Bilateral Filter, Histogram Equalization, and Image Blending, the research paper presents a new method for improving the LBP codes, and ultimately improving face recognition accuracy. In this proposed system for every nodal points in the human face, a histogram with all possible labels is constructed. The technique can be used in an application that can be implemented in a real-life environment since it is very accurate and robust. Researchers have not examined the issue of occlusions and mask faces in facial recognition

The system Jiashu HE proposed influences the glass factor in face recognition systems. Data collection and accuracy testing are the two steps in the study. A variety of situations are used to collect data on human faces, such as clear glasses, glasses with water, and glasses with mist. In order to further analyze the collected data, an existing state-of-the-art face detection and recognition system built on MTCNN and Inception V1 deep nets is tested. By comparing real-time disturbed images with the frontal ones, it fails to determine if two images belong to the same person.

Huilin Ge , Yuewei Dai , Zhiyu Zhu , Biao Wang proposed a Robust face recognition based on multi-task convolutional neural network. Face recognition is not that accurate due to issues such as unclear face images, large illumination changes, and complex backgrounds in the background, which are dealt with using multi-task convolutional neural network (MTCNN) for face detection and recognition algorithm. Increasing accuracy and reducing false detections can not only reduce the waste of human resources and improve efficiency, but also ensure the security of people and property, ensure the safety of property and increase the security of people. A PSNR of 1.24 dB is the average of this technique, and it is 0.94 dB higher than that of Faster R-CNN. A SSIM value of 10.7% is the average of MTCNN, and it is 8.7% higher than R-

CNN. AUC of MTCNN is 97.56%, while that of R-CNN is 91.24%, and that of Faster R-CNN is 92.01%. For the face images with defective features, MTCNN still has the best effect.

Pranav K B and ManikandanJ proposed a Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks. Face recognition systems for various applications have been bolstered by high-speed processors and high-resolution cameras.Depending on the application, face recognition systems use offline data or real-time input.Based on standard datasets and real-time inputs, respectively, the proposed system achieved maximum recognition accuracies of 98.75% and 98.00%.

III. ALGORITHM

Face recognition is a function that humans perform automatically and practically without thinking about it. Despite this seemingly simple task, a computer is faced with many variables that can impair the accuracy of the methods, such as illumination variation, low resolution, and occlusion.

Face recognition is the process of recognizing a person based on their facial image in computer science. The new methods and the quality of the current videos/cameras have made it very popular in the last two decades.

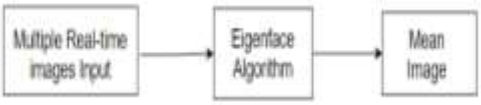
- The goal of face detection is to locate faces (facial size and nodal points) in an image and extract them for use by the face recognition algorithm.
- Using facial images that have been extracted are generally converted to grayscale, the face recognition algorithm determines what characteristics best describe the image.

Two modes,

- Verifying or authenticating a facial image is basically a comparison between the input facial image and the facial image related to the person requiring authentication. It is basically a 1X1 comparison.
- Face recognition or identification involves comparing the input facial image with the facial images from a dataset with the intention of finding the user that matches that face. It is basically an 1XN comparison.

1.1. EIGENFACE

- An algorithm called Eigenface is capable of recognizing and detecting faces based on their variance in a set of images.
- The algorithm lets the camera capture multiple images in a shorter period so that mean imageis picked for better image quality.
- As a result, the mean image is the image that has all the facial features the algorithm demands.

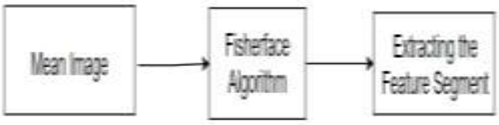


Limitation:

- It works with faces as a whole image instead of dismantling the facial structure as nodes and symmetry, and it cannot take into account any of the specific features of the face, such as the eyes, nose, lips and so on.

1.2. Fisherface

- Fisherfaces identifies individual differences based on principal components.
- In Fisherfaces, your image will not be affected by noise or blurring.
- Fisherfaces can also do pattern recognition, but it does faster and accurate recognition when compared to Eigenface, thus Fissherface is used for pattern recognition.

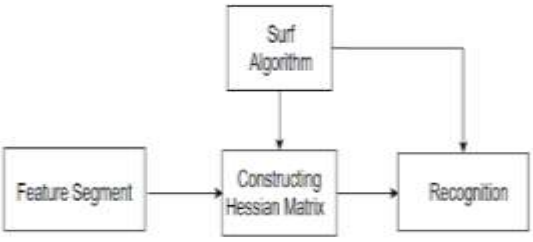


Limitation:

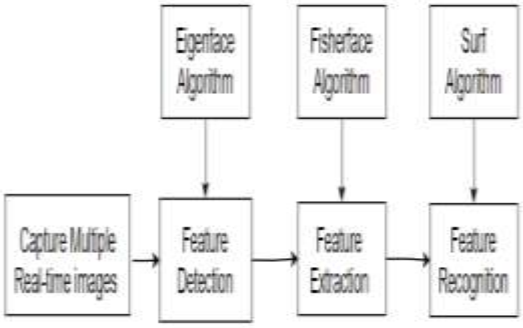
- The illumination is generated to identify the mean image and complete the verification.

1.3. SURF

- SURF stands for Speeded Up Robust Features.
- Steps of the SURF algorithm are divided into three sections: detecting interest points, describing interest points, and matching interest points.
- A Hessian matrix detector is used to detect interest points.



2. System Architecture



3. Smart Voting System through Facial Recognition Using FES Algorithm:

Implementing the Facial Recognition technology in Voting system as there is no software involved in the Voting system.

3.1. Existing System:

The existing system verifies and authenticates users manually. The security system can easily be bypassed since it offers poor security. Electronic verification is not yet incorporated in the security enhancement side.

Limitations of Facial Recognition in existing system:

1. Older system has a problem in which similar facial structure can bypass the authentication.
2. The existing system has limited security which in turn is less secure. It also has a slower processing speed which consumes more time than expected.
3. Proposed system that overcomes limitations like use of efficient algorithms to increase speed and security of the voting system.

3.2. Proposed System:

The proposed system involves a software that has two levels of security verification, User ID verification such as Aadhar Card or any other government proof verification is done at stage one. Stage two offers facial recognition which is innovation that has been added in order to improve and enhance security features of the system. A web based application is developed for the system.

Working Principle:

1. The camera captures the image of the user in multiple frames and the mean image is finally obtained by the use of the **Eigenface** algorithm.
2. The obtained image will be used for segmentation purposes (obtaining nodal points in a human face) through the **Fisherface** algorithm.
3. **SURF** uses the segmented image to construct a hessian matrix by identifying the nodal points such as eyes, nose, lips which in turn produces dimensions of facial symmetry and stores the obtained values in a matrix format.
4. The same process (1,2,3) is repeated on the photo fetched from a government proof provided at stage one of verification.
5. The matrix generated on the user id photo and the user's real-time image is validated and verified for the user's identity verification.
6. If the matrices values are the same, the user is authorized into the system.

IV. RESULT:

Thus, Eigenface algorithm is capable of recognizing and detecting faces based on their variance in a set of images. Eigenface can extract the MEAN image from multiple image input. Even though the fisherface is capable of recognizing but and illumination is generated while detecting the MEAN image with the Pre-defined image. Fisherface algorithm is used mainly for extracting the facial segment i.e., extracts the enlarged image of facial features for better performance. Whereas, the surf algorithm detects the nodal points and constructs the HESSIAN MATRIX. The hessian matrix is a mathematically generated value which can be used for comparison.

An web based application is developed for smart voting system using FES algorithnm (F-Fisherface, E-Eigenface, S-Surf algorithms). Initially, system captures Multiple real time images and the multiple image is inputted to Eigenface to select the MEAN image, the mean image is inputted to Fisherface algorithm to extract the facial segments. Finally, Surf constructs the facial segment and contructs the HESSIAN matrix to generate a matrix containing mathematical value. The Matrix is compared with pre-defined database image to verify the voter. The system prompts the compared result wheather the voter is a valid or invalid.

V. CONCLUSION:

The facial recognition includes multiple algorithms like Convolution neural network, Multi-tasks convolution neural network, etc.., We have utilized EigenFace, Fisherface, and Surf algorithm for facial detection and recognition. Each of those algorithm can perform entire facial recognition process. But, some of the non-advantageous features in the algorithm makes it inefficient. Inspite of that we utilized the efficient feature within the algorithm to get the accurate results.