SOFT COMPUTING FACE RECOGNITION SECURTIY SYSTEM

Mohit Aggarwal[1], Aditya Rawat[2], Akash Gupta[3], Umang Kant4

[1-3]CSE Department, Krishna Engineering College, Ghaziabad, U.P., India
[4]Asst. Professor CSE Department, Krishna Engineering College, Ghaziabad, U.P., India

---

Abstract- *This article presents a brief introduction to the fast-growing technology known as Soft Computing with its application in biometric recognition. Using the concepts of soft computing and biometric facial recognition we will focus on generating a Face Recognition Security System. The security system will help the user to check for the intruders. The system will grant the access only to the recognized individuals permitted by the user otherwise the system will generate an alert message with an image and will ask the certified user whether the grant the access or not.*

Key Words – Soft computing, Face recognition, features, database, extraction, recognition.

I. INTRODUCTION TO SOFT COMPUTING

Soft computing is a new approach to computing. It has ability to reason and learn in an environment of uncertainty, approximation and imprecision. The main aim of soft computing is to solve real world problems which are not solved by hard computing. Soft computing is used to develop intelligent reasonable machines to provide solutions to many real-world problems.

Soft computing is the recent buzz in today's era. It was given by Zadeh in 1992. Soft computing takes the human mind as role model. It uses fuzzy logic instead of Boolean algebra to find results and make systems which have high machine intelligence. Unlike hard computing which uses crisp systems, binary logic and numerical analysis, Soft computing is a mixture of fuzzy logic, probabilistic reasoning, artificial neural network, genetic algorithm, evolutionary computing and machine learning. Soft computing does not produce accurate result but it yields approximate and near about answers. Soft computing aims to solve the real-world problems with the reasonable less time and also with reasonable less resources and cost.

The various factors which makes Soft computing very much important are: -

- It generates its own programs.
- Can deal with noisy data.
- Programs learn by own.
- Applications are tolerant to imprecision, uncertainty and approximation.
- It uses human brain as its role model.

II. BRANCHES OF SOFT COMPUTING

Soft computing is the combination of Fuzzy Logic, Genetic Algorithm, Artificial Neural Networks, Machine Learning and probabilistic reasoning.

- **Fuzzy Logic:** Fuzzy Logic was given by Zadeh. He was a professor in University of California and showed that people do not need precise, numerical information. Fuzzy logic defines the intermediate and approximate values. Control field is the most significant area of fuzzy logic. Fuzzy control includes complex aircraft engines, industrial processes, automation transmission, missile guidance and many more.

- **Artificial Neural Network(ANN):** Artificial neural network is inspired by biological neural networks. In ANN the inputs and weights of the neurons are combined in a linear way. The results are fed into non-linear activation unit where they are compared with a threshold value. Neural networks are used to increase and optimize fuzzy logic-based systems by giving them the ability to learn. Learning is achieved by providing a training set along with learning algorithm. Neural network offer input-output mapping, nonlinearity, fault tolerance and adaptability.

- **Genetic Algorithms:** Genetic algorithms were given by John Holland at University of Michigan in 1960s. They are Search heuristic algorithm. Genetic algorithms are based on evolutionary ideas of natural selection and genetics. It operates on the concept of the fittest one wins. It is basically a model of machine learning which is inspired by the process of evolution in nature.

- **Probabilistic Reasoning:** It is used to deal with the uncertain and incomplete data in artificial intelligence. The main aim of probabilistic reasoning is to combine the capability of probability theory with the capability of deductive logic to exploit structure. It uses approaches like classical probability, uncertainty factors, fuzzy set theory.

- **Machine Learning:** Machine Learning is a branch of computer science that evolved from pattern recognition and computational learning theory. It exploits the study and construction of algorithms that can learn from these algorithms and make predictions based on data. It is a science of making computers act without being explicitly programmed.

III. APPLICATIONS OF SOFTCOMPUTING

- Pattern Recognition
- Diagnostics
- Automation Engineering
- Robotics
- Time Series analysis
- Natural Language Processing
- Biometrics
- Weather Forecasting
- Gaming and many more…

IV. INTRODUCTION TO BIOMETRIC RECOGNITION

Humans uses body characteristics such as face, voice, and gait for thousands of years to recognize each other. Alphonse Bertillon, chief of the criminal identification division of the local department in Paris, developed and then practiced the thought of using a variety of body measurements to spot criminals within the mid-19th century. Although biometrics emerged from its extensive use in enforcement to spot criminals, it's being increasingly used today to determine person recognition during a sizable amount of civilian applications. Any human physical and behavioral characteristics can be used as biometric as long as it satisfies the following requirements: -

- Universality
- Distinctiveness
- Permanence
- Collectability
- Performance
- Acceptability
- Circumvention

It operates on in two modes: -

- **Verification Modes**
  In this mode the system validates a person identity by comparing the captured biometric data with her own biometric templates stored in the database. In such systems an individual who desires to be recognized claims an identity usually via a personal identification number(PIN), a user name, or a smart card and the system performs a one on one comparison to determine whether the question is true or not.

- **Identification Mode**
  In this mode system recognizes an individual by searching the templates of all the users in the database for a match. It conducts a one to many comparisons to establish an individual's identity without the subject having to claim an identity.

V. VARIOUS TYPES OF BIOMETRICS

The match between a selected biometric and an application is decided depending upon the operational mode of the appliance and therefore the properties of the biometric characteristics. A brief introduction to the commonly used biometrics are:

- **DNA:** Deoxyribonucleic acid(DNA) is the one-dimensional(1-D) ultimate unique code for one's individuality except for the fact that identical twins have identical DNA patterns. It is however, currently used mostly in the context of forensic applications for person recognition. Three issues limit the utility of this biometrics for other applications: 1) contamination and sensitivity 2) automatic real time recognition issues 3) privacy issues.

- **Ear:** It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear aren't expected to be very distinctive in establishing the identity of a private.

- **Face:** Face recognition may be a no intrusive method and facial images are probably the foremost common biometric characteristics employed by humans to form a private recognition. The most popular approaches to face recognition are based on: 1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips, and chin, and their spatial relationships, 2) the overall analysis of the face image that represents a face as a weighted combination of a number of canonical faces. In order for a facial system to work well in practice it should automatically: 1) detect whether a face is present in the acquired image, 2) locate the face 3) acknowledge the face from a particular point.

- **Fingerprint:** A fingerprint is that the pattern of ridges and valleys on the surface of a fingertip, the formation of which is decided during the primary seven months of fetal development. The accuracy of the currently available fingerprint recognition systems is adequate for verification

systems involving a few hundred users. One problem with current fingerprint system is that they require a large amount of computational resources.

- **Retinal scan:** The retinal vasculature is rich in structure and is meant to be a characteristic of every individual and every eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image acquisition involves cooperation of the subject, entails contact with the eye-piece, and requires a conscious effort on the part of the user. All these factors adversely affect the general public acceptability of retinal biometric.

- **Voice:** Voice may be a combination of physiological and behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages that are used in the synthesis of the sound. Voice is also not very distinctive and appropriate for identification as voice of person changes with age and medical conditions.

VI. SYSTEM ARCHITECTURE

The Proposed system may be a standalone application that uses a centralized database to acknowledge human faces. During this application human faces are going to be captured by the webcam or camera and therefore the detected face is stored into database. The system constructed has the following modules as shown in Fig.1:

- Face Detector
- Face Feature Extractor
- Face Recognizer.

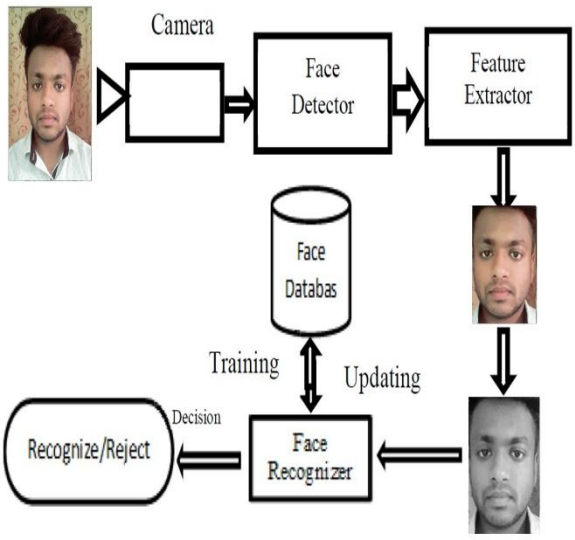

Figure 1. Architecture for face recognition system.

VII. IMPLEMENTATION AND WORKING OF THE SYSTEM

The whole face recognition security system will be implemented in the Python Language and OpenCV Library of python with the help of a training dataset and for alert message sending we will use a web-based messaging platform which will ask user for action to be taken via a web browser. The working or implementation is as follows: -

A. Face Detection: Face Detection is the prior step and the entry point of the face recognition process. This step is where the face image under consideration is presented to the face recognition system. To have an accurate detection of individual's face image, is one of the most important processes involved in face recognition system. When face image is exactly and accurately placed in the detection step, the other remaining recognition steps would not be so complicated.

Face Detection can capture a face image from different surrounding equipment. The face image can be a real time live video feed, an image file format that is located on either an optical disk. It can also be captured by a digital camera directly or it can be scanned from photo paper with the help of a scanner machine.

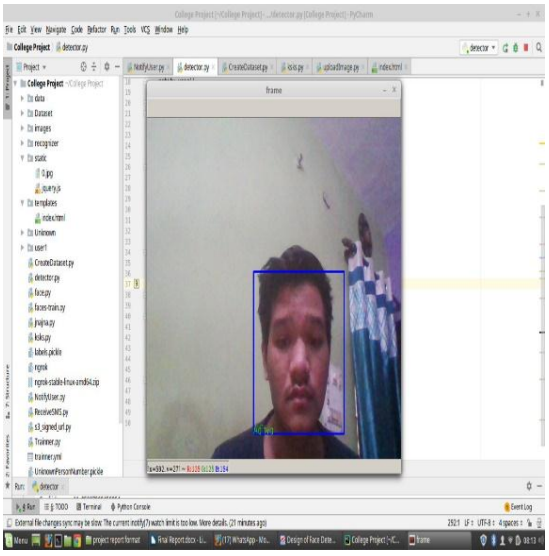

Figure 2. Real time video feed face detection done by web cam.

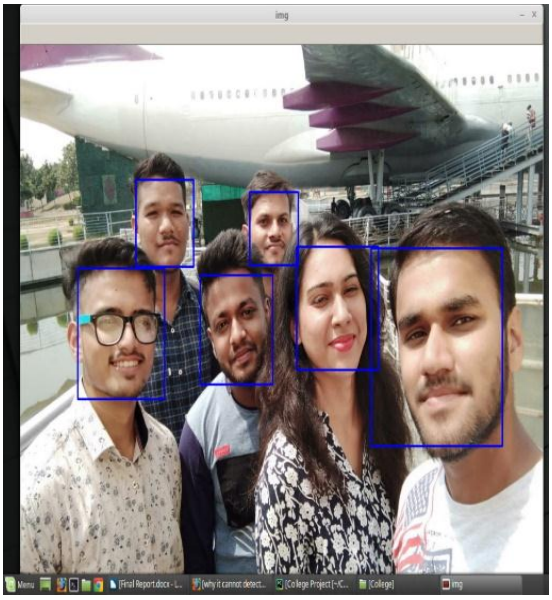

Figure 3. Face detection in a still image.

B. Feature Extraction: The aim of this step is to extract a compressed set of personal discriminating geometrical and biometrical features of the face image. After performing some pre-processing steps, the normalized face image is passed to the feature extraction section in order to find the key features that will be used for producing a feature vector that is sufficiently enough to characterize the face image.
A training set with face features will be used for this step and multiple images of the will be clicked by the system and stored in the database as shown in the figure-

Figure 4. Images clicked for feature extraction by the system to store in thee database.

C. **Feature Matching:** Feature matching is the real recognition process. The feature vector or geometrical features obtained from feature extraction is matched to individual's facial images already enrolled and stored in a database or a fie. In this step we can have different purposes, whether it is identification or verification. If identification takes place the image will be compared with all images in a database. But if it is verification the image will match to only one image in a database. Feature matching result will be predicted on this basis of the confidence value of detected face with the face store data in the database.

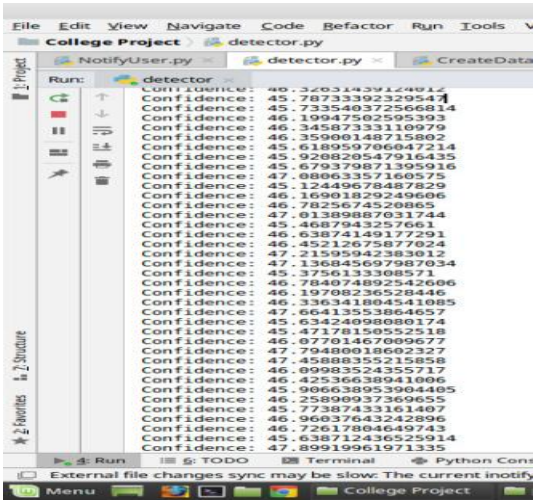

Figure 5. Confidence level value predicted with respect to the detected face.

D. Identification and Verification: This step is done after the feature matching is done by the system for the detected human face. The system will identify the face by looking through the database i.e. the particular face exists in the system or not and then verify it. This step is the main step of the security system. As shown in the figure the system identifies the user and verifies it by detecting face and displaying name "Aditya".

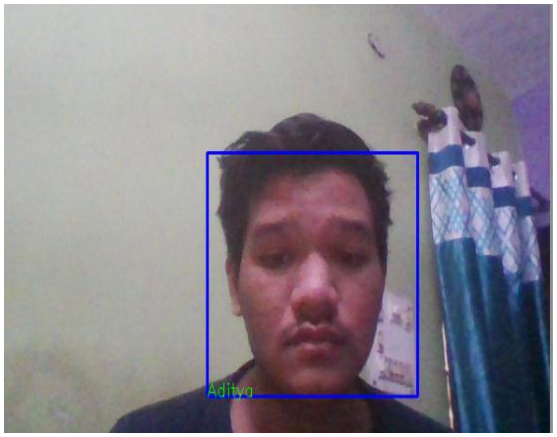

Figure 6. Detected face of the user is identified and verified by displaying of the name.

E. Granting/Restricting Access: In this step if the system finds the detected face details and features stored in the database it will grant access to the particular person.

On the other hand, if the system does not found the detected face details in the base and the system will generate an alert message that the particular person is not authorized to access and send it to system's certified user through a message sending medium with the image of the detected face and will ask the user whether to grant the access or restrict it with a single keyword i.e. Allow or Decline through a web page as shown in the figure-

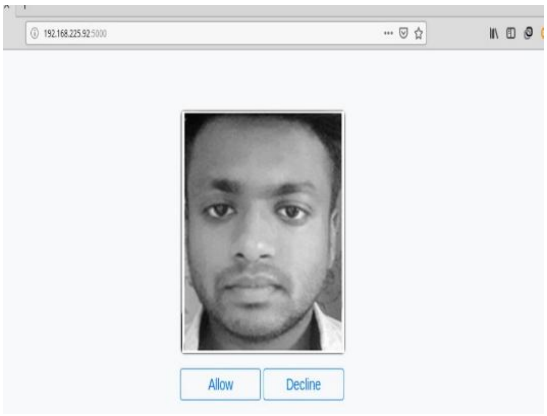

Figure 7. Unidentified face detected by system and an image alert message sent to the user.

VII. CONCLUSION

We have designed a real time automated face recognition security system which allows the user a cheap and efficient surveillance system which also reduces the time and resources that is required while surveil anting manually. This system uses the technology of face detection and recognition. The system also tells us whether the detected face or person is authorized or not and then only grant access to the premises. Various efficient algorithms are used in order to get the desired results. This system works well in the ideal conditions and further improvement can be made when the conditions are not ideal like proper illumination or lightning.

REFERENCES

[1]. Anil k. Jain, Arun Ross, Salil Prabhakar," An Introduction to Biometric Recognition", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004.

[2]. Dr. Uma Kumari," Soft Computing Applications: A perspective View", Proceedings of the 2nd International Conference on Communications and Electronics Systems (ICCES 2017).

[3]. Suad Haji, Asaf Varol, "Real time Face recognition System(RTFRS)", 4th International Symposium on Digital Forensics and Security (ISDFS' 16), 25-27 April 2016.

[4]. Dwi Ana Ratna Wati and Dika Abadianto, "Design of Face Detection and Recognition System for Smart Home Security Application.", 2017 2nd International conference on Information Technology.

[5]. Kazarian Artem, Teslyuk Vasyl, Tsmots Ivan, "Development of Face Recognition Module for A "Smart Home" System Using A Remote Server", IEEE CSIT, 2018 11-14 September, 2018.

[6]. RongBao Chen, ShiJie Zhang, "Video Based Face Recognition Technology for Automotive Security", IEEE 2010.