JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURE ACCESS WITH A SMILE – FACIAL RECOGNITION ACCESS CONTROL

Bharath Gowda R, B.E Student, Department of Information Science and Engineering
Kuppa Shashank, B.E Student, Department of Information Science and Engineering
Piyush Nahar, B.E Student, Department of Information Science and Engineering
Sandeep R C, B.E Student, Department of Information Science and Engineering
Mr. Byre Gowda B K, Assistant Professor, Department of Information Science
Sir M Visvesvaraya Institute of Technology (Affiliated to VTU, Belagavi)
Bengaluru - 562157

Abstract : Biometrics are revolutionised by artificial intelligence algorithms that analyse and validate biological characteristics such as voice, locomotion, fingerprints, iris patterns, and face features. By removing specific components from biometric data, these algorithms improve system robustness, speed, and accuracy. AI's flexibility makes it possible for it to learn and grow over time, which is essential for changing security requirements. Real-time identification is enabled by the efficient handling of massive data volumes. Additionally, AI ensures reliability by mitigating issues such as environmental changes. The incorporation of artificial intelligence (AI)-powered biometrics reinforces security protocols across various domains, including law enforcement, finance, and access control. Improved security, faster procedures, and better user experiences across domains are all promised by this synergy between AI and biometrics.

I. INTRODUCTION

1.1 Development of AI

The path towards the creation of AI has been revolutionary, replete with important turning points and innovations in a variety of fields. AI began with the idea of "thinking machines" in the 1950s and has progressed from complex neural networks and algorithms to rule-based systems. Important developments include the creation of expert systems in the 1970s, the emergence of machine learning methods in the 1990s, and the discovery of Deep-Learning in the 2010s, which was made possible by the availability of Zeta Bytes and powerful computers. These achievements have accelerated the use of AI in many fields, including robotics, driverless cars, computer vision, and natural language processing. AI is still being developed, and its future direction is being shaped by ongoing research into topics like explainable AI, generative adversarial networks, and reinforcement Learning.

1.2 Biometrics

With the biometrics, people can be authenticated based on their distinct biological qualities, including voice, facial features, iris patterns, fingerprints, and behavioral tendencies. For a range of uses, such as financial transactions, healthcare, border security, and access control, it provides quick and safe identification verification. These distinctive characteristics are sensed and processed by biometric technologies, which then turn them into digital templates for comparison and authentication. Biometric systems now enable real-time identification and improved security measures thanks to advances in A.I and machine learning. These systems are precise, dependable, and adaptable. Biometrics is becoming widely used and is changing the face of identity management and identification in the digital era.

1.3 Neural Networks

Inspirited by the structure and functions of the human brain, the neural networks are a class of machine learning techniques. Neural networks are composed of interconnected nodes, or neurons, arranged in layers. These networks use a sequences of mathematical operations to interpret complex data inputs and produce responses. Sequence prediction, regression, classification, and pattern recognition are among the tasks which they excel in. Significant advances in computer visioning, processing of natural language , and speech recognition have been made possible by deep neural networks, which comprise several hidden layers. Through backpropagation, which adjusts weights by propagating errors backward, neural networks can learn and become more efficient over time. This process is known as neural network training.

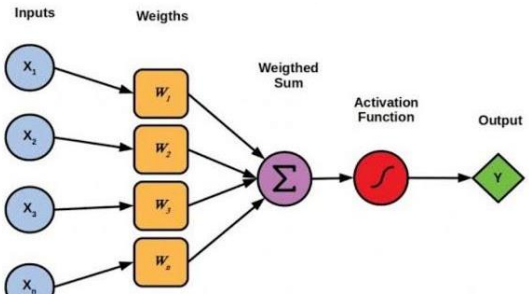

Fig 1.1 Perceptron Network

II. METHODLOGY

1. Tensorflow

Renowned for its adaptability, scalability, and extensive ecosystem, 'TensorFlow' is an open-source machine learning framework created by Google. With its user-friendly interface and large library, it makes the development and implementation of machine learning models easier. Tasks like photo recognition, "natural language ToolKit", and time series analysis are made easier by TensorFlow's support for multiple neural network topologies, such as transformers, recurrent neural networks (RNNs), and convolutional neural networks (CNNs). Effective execution on CPUs, GPUs, and specialised hardware such as TPUs is made possible by its computational graph abstraction. Researchers, developers, and organisations looking to leverage the power of machine learning choose TensorFlow because of its strong community, comprehensive documentation, and seamless interface with other technologies.

2. Convolutional Neural Networks (cnn)

CNNs, they are a kind of deep learning algorithm which are mainly employed for tasks involving image processing and recognition. CNNs are composed of several layers of neurons that process visual information in a hierarchical fashion, taking inspiration from the structure of the animal visual cortex. Important parts are pooling layers, which minimize spatial dimensions, convolutional layers, which extract information from input images, and fully linked layers, which carry classification or regression. Because CNNs can automatically learn and extract features from raw pixel data, they are excellent at tasks like object detection, facial recognition, and picture categorization.

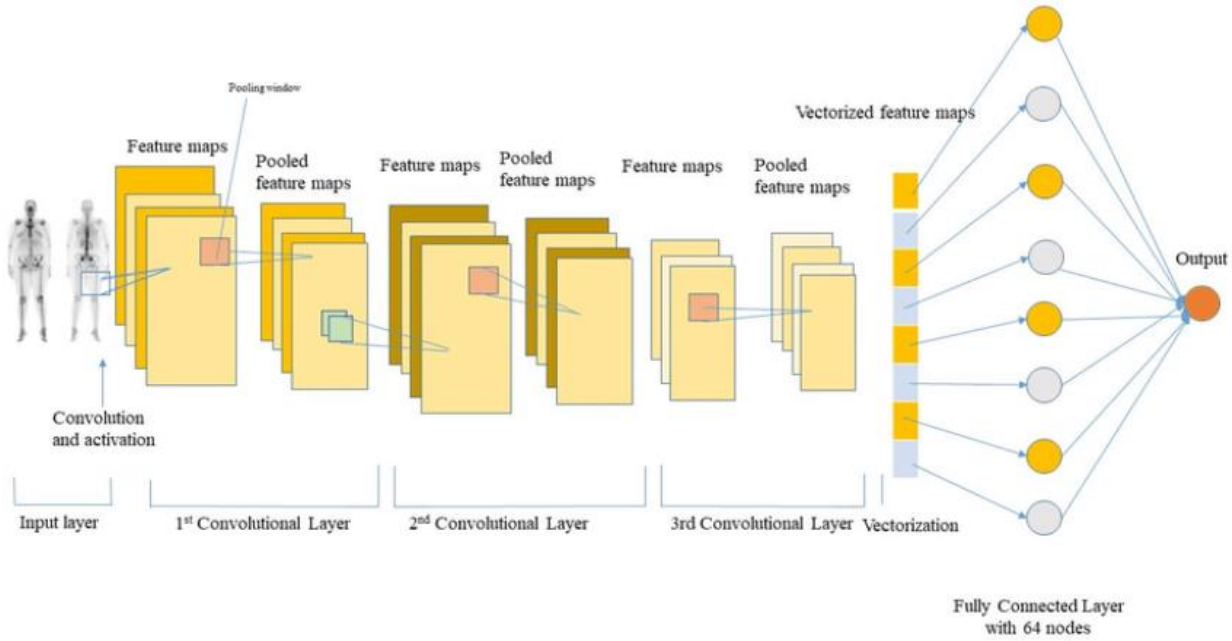

Fig 2.1 Layers of CNN

2.1. Steps involved in CNN

1. Input Layer: Data is fed into the network, typically in the form of pictures.
2. Convolutional Layer: This layer uses filters, sometimes referred to as kernels, to apply convolution operations to the input data. These filters identify different characteristics in the input pictures.
3. Activation Function: To add non-linearity and help the network learn intricate patterns, an activation function such as ReLU (Rectified Linear Activation) is used after convolution.
4. Pooling Layer: Feature maps produced by convolution have less spatial dimensions thanks to pooling layers. Max pooling and "average pooling" are two common pooling methods.
5. Flattening: The feature maps that are produced are flattened into a vector following numerous convolutional and pooling layers, readying them for input into fully connected layers.
6. Fully Connected Layer: Also referred to as dense layers, these layers allow for higher-order thinking by connecting all of the neurons in one layer to all of the neurons in the layer below.

7. Output Layer: The last layer generates the output of the network, usually in the form of probabilities for each class using a softmax activation function for classification tasks.
8. Loss Calculation: To determine how well a network is performing, the loss function calculates the difference between the expected output and the actual labels.
9. Backpropagation: The network's weights and biases are adjusted to minimise the loss when the erroneous signal from the "loss function" travels backward.
10. Optimisation: To enhance the performance of the model, iteratively updating the network parameters using optimisation techniques like Adam or "Stochastic Gradient Descent" (SGD) is used

III. System Overview

Access Control with Facial Recognition - An Android App. The functionality of the biometric system is as follows:

3.1 App Functionality:

3.1.1 User Enrollment:

Users can register themselves within the app. This might involve capturing their facial image under different luminance for better recognition accuracy. Secure storage of facial data is crucial, potentially on the device's Trusted Execution Environment (TEE) for added security.

3.1.2 Facial Recognition:

The app will utilize the device's camera to capture a live feed of the user's face. Google's ML Kit library offers facial detection capabilities for Android, allowing the app to identify faces within the camera frame. The captured facial data will be compared against the enrolled user database using a facial recognition algorithm.

3.1.3 Access Control:

Upon successful recognition, the app grants access to the designated resource (e.g., opening a door, accessing a secure area of the app). If facial recognition fails, the app might prompt for an alternative authentication method (PIN, password) for additional security.

3.2 Benefits:

- Enhanced security compared to traditional methods (key cards, passwords).
- Convenient and hands-free access control.
- Improved user experience with faster authentication.

3.3 Challenges:

- Accuracy of facial detection can be influenced by lighting variations, facial expressions, and occlusions (glasses, masks).
- Security concerns regarding user data storage and potential misuse of facial recognition technology.

3.4 Additional Considerations:

- The app should prioritize user privacy by ensuring secure storage and responsible use of facial data.
- Liveliness detection could be implemented to prevent spoofing attempts (using photos or videos).
- Consider integrating with existing access-control systems for wider implementation.

3.5 Development Tools:

- Android Studio (Integrated Development Environment)
- Android SDK (Software Development Kit)
- Google ML Kit for facial detection
- Secure storage libraries for user data

IV. Literature Survey

[1] The study undertaken by author Sameer Aqib Hashmi discusses the challenges of detecting faces in unconstrained environments and proposes a deep cascaded multi-task framework that utilizes deep learning techniques to improve face detection performance. The framework includes three stages of convolutional networks that can recognize faces and landmark locations such as eyes, nostrils, and mouth. The proposed framework outperformed other models, achieving a 73% accuracy rate and a 76% recall rate. The author also discusses the online hard sample mining method, which is used to improve the performance of the proposed framework. The paper provides a comprehensive overview of the experimental results and a summary of the findings. The author conducted experiments using various models, including MTCNN and Haar cascade, and compared their accuracy rates. The MTCNN model achieved a 99% accuracy rate, while the Haar cascade model achieved a 68% accuracy rate. Overall, Sameer Aqib Hashmi's proposed framework shows promising results in identifying faces in extreme conditions and provides valuable insights into the challenges of face detection in unconstrained environments.

[2] The paper by Shivam Singh and Prof. Graceline Jasmine discusses the proposed automated facial matching system that uses various algorithms for face detection, feature extraction, and recognition. The system is designed to be reliable, secure, and fast, and can be used in various applications and security systems. The challenges faced in implementing the system, include the challenges of laying transmission lines in places where the topography is bad. They propose a system that uses wireless communication to overcome this challenge. The paper concludes by stating that the proposed system is reliable, secure, and fast and can be used in various applications.

[3] The Study by Saud Haji and Asaf Varol on biometrics proposes that Biometrics refers to the identification of individuals through their unique biological or behavioural traits, including DNA, hand geometry, face, voice, hand signature, and keystrokes. These distinctive features are employed for authentication. Among biometric methods, facial recognition technology is gaining popularity. Genetic biometrics typically involves analysing physical characteristics like fingerprints, iris patterns, and veins to authenticate individuals. Instead of conventional bank cards, some Automated Teller Machines now use cameras to capture customer's faces, which are then compared to account holder photos in the bank's database for identity verification. This paper introduces a real-time Windows-based application system utilizing face recognition algorithms, feasible for various applications such as identity verification and commercial use. It incorporates Eigen and Local Binary Patterns face algorithms to enhance accuracy under varying lighting conditions.

[4] The authors, Pranav K B and Manikandan J describe the flow of the system, which includes multiple layers of convolutional operations, as well as a dropout layer to prevent overfitting. They also provide details on the dataset used for training and testing and the performance metrics used to evaluate the system. The results show that the system achieves high accuracy and fast execution times, making it suitable for real-time applications. The article concludes with a discussion of the limitations and future directions of the research. The research gives us a valuable insights into the development of a state-of-the-art face recognition system using deep learning techniques.

V. Future Enhancements

Integrating Advanced Biometric Modalities: Investigate the integration of biometric modalities other than fingerprint, face, and iris identification. Consider adding new modalities such as gait recognition, vein pattern recognition, or behavioral biometrics like keystroke dynamics to improve security and user identification.

Improvement of Convolutional Neural Networks (CNNs): Investigate improvements in CNN architectures and approaches for biometric recognition. Experiment with cutting-edge CNN designs such as ResNet, DenseNet, and EfficientNet to increase the accuracy, speed, and resilience of biometric identification and verification systems.

Multi-modal biometric systems: Create multi-modal biometric systems that integrate different biometric modalities for greater accuracy and dependability. Investigate fusion strategies, such as score-level fusion or decision-level fusion, to efficiently merge data from various biometric sources and improve recognition performance.

Adaptive and Transfer Learning: Use adaptive learning methods to constantly enhance the performance of biometric recognition systems over time. Detailed transfer learning techniques for using pre-trained CNN models on large-scale datasets and fine-tuning them for specific biometric recognition tasks, eliminating the requirement for huge annotated datasets and accelerating model training.

Privacy-safeguarding Biometric Authentication: Look into techniques for safeguarding biometric data's privacy and security. Investigate biometric cryptosystems, secure multi-party computing, and federated learning to enable biometric authentication without disclosing sensitive biometric information to unauthorized parties.

Real-time biometric authentication: Optimize biometric recognition algorithms and system architectures for real-time processing to support applications that require immediate user identification, such as access control systems, attendance monitoring, or mobile.

User Experience (UX) Optimization: Improve the user interfaces, feedback mechanisms, and error handling of biometric authentication systems. Conduct usability tests and get feedback from end users to identify problems and opportunities for improvement in the biometric authentication process.

Robustness to Adversarial assaults: Look into strategies for improving the resilience of biometric recognition systems against adversarial assaults and spoofing efforts. Investigate techniques such as adversarial training, data augmentation, and anomaly detection to identify and mitigate attacks on biometric authentication systems.

Ethical and Legal Considerations: Consider the ethical and legal implications of collecting, storing, and using biometric data. Comply with appropriate requirements, such as GDPR (General Data Protection Regulation) or biometric privacy laws, and incorporate privacy-by-design principles into the development of biometric authentication systems.

Design biometric authentication systems for scalability and deployment across several settings. Consider cloud-based architectures, containerization, or microservices for biometric authentication services that can be easily deployed, maintained, and scaled across multiple platforms and devices.

VI. Results And Conclusion

The development and implementation of a Real-Time Biometric Access-Control System using Facial Recognition is a complex but highly valuable endeavor. This project has been carefully planned, and throughout the planning process, various aspects have been considered, including hardware and software requirements, data security, user experience, and compliance with relevant regulations. The primary objective of this project is to enhance security by utilizing facial recognition as a biometric access control

system. A focus on user experience has been incorporated into the project planning to ensure that the system is intuitive and easy for users to interact with. Facial recognition should be quick and convenient, fostering seamless access for authorized individuals.

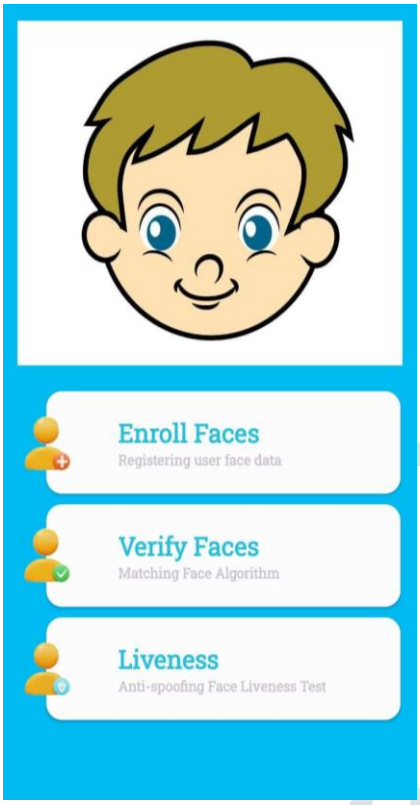

Fig 5.1 Home Page

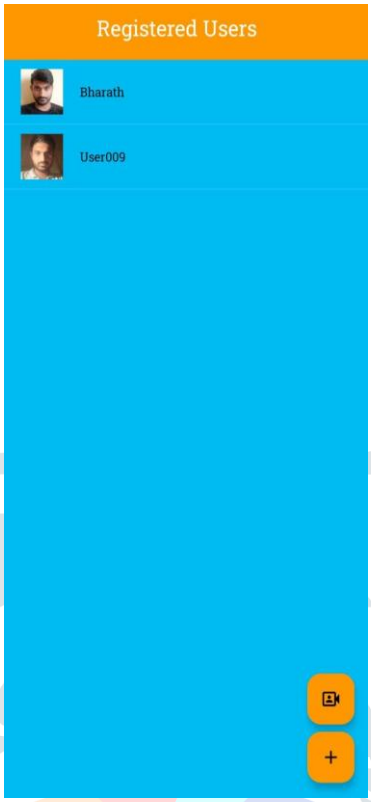

Fig 5.2 Registered Users

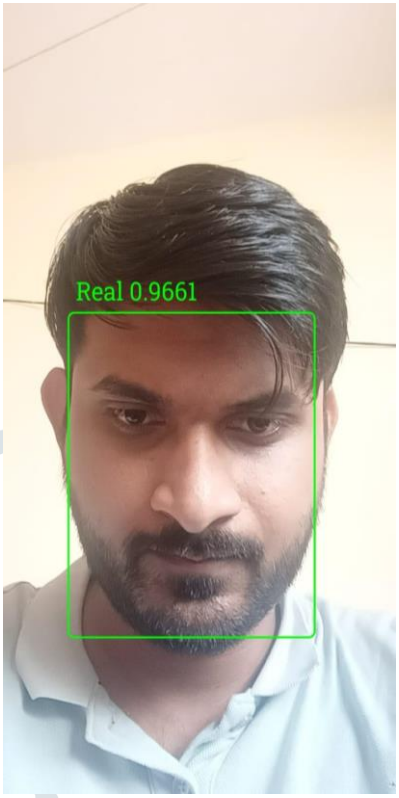

Fig 5.3 Camera Activity

Fig 5.4 Successful Recognition

Fig 5.5 Successful login

References

[1] *Face Detection in Extreme Condition: A Machine-learning Approach* Authors: Sameer Aqib Hashmi, Professor in the Dept. of ECE, North South University Basundhara, Dhaka, Bangladesh

[2] **"***Face Recognition System*" Authors: Shivam Singh and Prof. S. Graceline Jasmine from the Dept. of SCSE at Vellore Institute of Technology, Chennai, Tamil Nadu, India

[3] **"***Real-time Face Recognition System*" Authors: Saud Haji and Asaf Varol, Professors at College of Technology, Firat University, Elazig, Turkey

[4] **"**Design and Evaluation of a Real-time Facial Recognition System using Convolution Neural Networks Authors": Pranav K B and Manikandan J, Crucible of Research and Innovation, Department of ECE, PES University, Bangalore, India