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

Sentinel-Face: AI-Based Facial Recognition and Behavior Analysis

Mr. Jeya Ganesan J
Assistant professor, Department of Artificial intelligence and Data Science
Sri Sai Ram Institute of Technology
Chennai, India
jeyaganesan.ai@sairamit.edu.in

Abilash C R
Student, Department of Artificial intelligence and Data Science
Sri Sai Ram Institute of Technology
Chennai, India
sit22ad003@sairamtap.edu.in

Sreehari K
Student, Department of Artificial intelligence and Data Science
Sri Sai Ram Institute of Technology
Chennai, India
sit22ad001@sairamtap.edu.in

Mano Sri Ram K
Student, Department of Artificial intelligence and Data Science
Sri Sai Ram Institute of Technology
Chennai, India
sit22ad056@sairamtap.edu.in

***Abstract* - Artificial intelligence in face identification systems has opened up a whole new dimension to enhance defense securities. This paper discusses the implementation of AI-based face recognition for distinguishing between military personnel and intruders/terrorists to ensure the identification mechanism within the defense zones is strong. Beyond this, the system could monitor abnormal behavior patterns of even authorized soldiers to enable early intervention in case of deviation from protocols. These could also be implemented in highly crowded public areas to trace individuals with criminal or terrorist flags against their names. Integrated into CCTVs, real-time monitoring and identity verification can be done before access to sensitive zones is allowed. Further implementation of such intelligent systems in civilian areas like hospitals, theaters, and transport hubs will significantly enhance the aspect of public safety. The designed framework focuses on accurate, efficient, and scalable face identification with reduced risks of impersonation and unauthorized entry.**

I. INTRODUCTION

In the ever changing landscape of national defence and public safety, technological advancements are shaping the ways in which threats are detected, mitigated, and managed. Among these emerging technologies is Artificial Intelligence, serving as an agent with respect to enhanced surveillance, pattern recognition, and predictive analytics [1]. Facial recognition, when combined with AI, presents an opportunity to automate identity verification and suspicious activity detection, especially in high-security environments as well as in public places [2].
Traditional systems of authentication, such as ID badges or PIN codes, are susceptible to forgery, theft, human error and any other vulnerabilities. Biometric systems, however, employ individual physiological attributes as a stronger form of verification. Among these, face recognition is non-intrusive, fast in speed, and easy to implement [3]. As CCTV and high-definition camera networks proliferate, AI-powered face recognition systems can scan environments constantly, flagging threats and even predicting abnormal behavior before a critical incident actually happens [4].
This paper discusses the design, architecture, and implementation of AI-based FR systems for defense and public applications. It puts forth the integration of traditional computer vision techniques with deep learning models supported by real-world testing in simulated environments. Further, the paper assesses the implications of deploying such systems pertaining to ethics, data protection, and system scalability [5].

II. LITERATURE REVIEW

1. Face Detection Using OpenCV: Various studies have performed face detection using OpenCV-based Adaboost and Haar cascades [1]. Although the methods are efficient, they are sensitive to changes in environmental conditions, hence requiring strong deep learning methods.
2. Open-source face recognition frameworks: The studies of face recognition technologies underline the shift to 3D facial surface analysis that increases the accuracy of recognition due to additional distinguishing features [2]. Comparing 3D recognition methods shows the great contribution of deep learning to improving system performance.
3. Review on Literature Survey of Human Recognition with Face Mask: Recent studies investigate the influence of face masks on recognition accuracy using CNN-based models like VGG-16, Adaboost, and Haar cascades [3].
4. Survey of Face Recognition: The literature categorizes existing face recognition methodologies into intensity image processing, video sequence analysis, and 3D/infrared-based approaches [4]. Each of these methods presents unique advantages and challenges to reach the best recognition performance.
5. 3D Face Recognition: A Comprehensive Survey: Research in 3D face recognition techniques includes traditional and deep learning-based approaches that review the performance benchmark and development in the field [5]. This method comprises four integrated modules: face detection, feature extraction, face recognition, and behavior analysis.

III. FACE RECOGNITION METHODS AND WORKFLOW

3.1 FACIAL DETECTION USING HAAR CASCADES

The first stage utilizes Haar Cascade classifiers, which are efficient for fast face detection [1]. These classifiers examine an image in a cascaded manner by employing progressively more complex filters to extract basic human facial features such as eyes, nose, and mouth. The features used by these classifiers are called Haar-like features and include edge, line, and rectangle configurations.

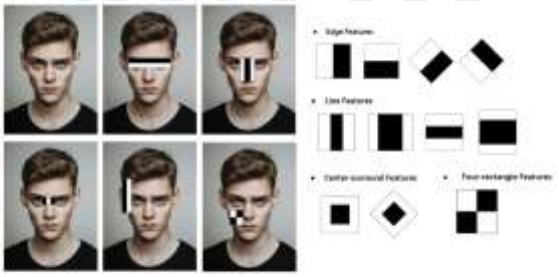


Fig 1:Haar Cascades for Face recognition

3.2 FEATURE EXTRACTION THROUGH DEEP EMBEDDINGS

The detected face regions are normalized and fed into a CNN embedding network, which results in a fixed-length vector representation, usually of 128 dimensions [2]. This vector captures the essential features of the face while ignoring noise. This embedding is an important step to compare between identities and make retrieval in databases efficient.

3.3 CNN ARCHITECTURE FOR IDENTITY VERIFICATION

This CNN is an AlexNet architecture-based model. It contains five convolutional layers followed by ReLU activation, max pooling, and three fully connected layers [3]. It was trained using a mixture of softmax and triplet loss, achieving increased intra-class compactness and inter-class separation, thus enabling the system to distinguish subtle facial differences.

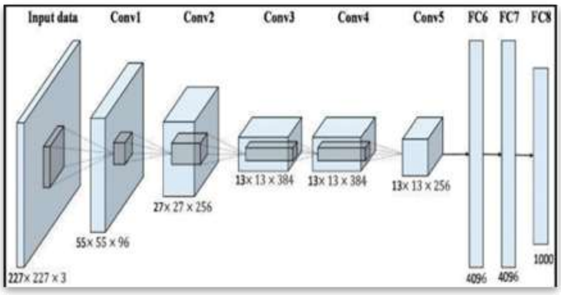


Fig 2: Triplet Loss Network for Face Verification(CNN)

3.4 BEHAVIORAL ANALYSIS USING ACTIVITY MONITORING

The system logs the actions and movements of the user in the zone after verifying their identity [4]. For instance, if a soldier has been idle in an unassigned area for longer periods or is interacting with unauthorized equipment, the system flags that. The activity data is therefore mapped against the policies for role-based access using LSTM-based time-series prediction, which highlights these unusual behaviors, such as roaming outside their assigned territory, inactivity for extended periods, or erratic movement [5]. This will be done using landmark localization.

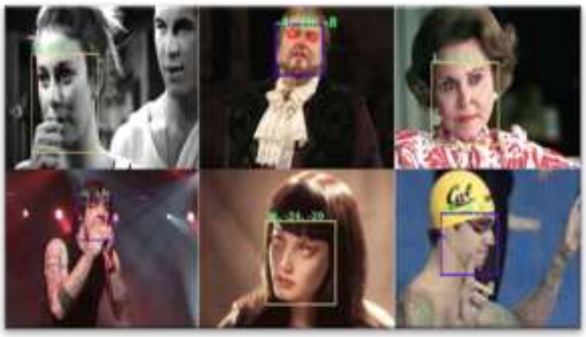


Fig 3: Real-Time Face Detection with Landmark Localization

3.5 GENERATION OF ALERTS AND ACCESS CONTROL

If an anomaly is detected, an alert will be issued, and access to restricted areas can be automatically blocked. Notification will be provided to a central monitoring station with the subject's face image and logs of activities [4]. Notification of alerts can also be initiated through SMS, email, or system pop-ups.

IV. 4. IMPLEMENTATION

This project implementation was developed in Python GUI, integrated with TensorFlow and OpenCV for model execution [1]. The hardware used includes cameras and a centralized server for data logging and processing. NVIDIA Jetson Nano might be used in future for edge/fog computing [2]. Training data included publicly available data, VGGFace2, and a private dataset of 10,000 images collected under controlled conditions [3]. Performance Measures: 98.2% of the time, it can find faces. Accuracy of recognition: 96.5%. 1.3% of the time false positives occur, 0.7 seconds to identify each face. System throughput: 12 frames per second per camera, with frames being checked every 2 seconds.

4.1 CRIMINAL REGISTRATION

This uses the python GUI to register a criminal along with various details of the person. It requires one clear picture of the criminal. Then this will be used to make a face embedding and a model trained using the feature augmentation of this face image. The face embedding is used to transfer and verify the information about the crime.

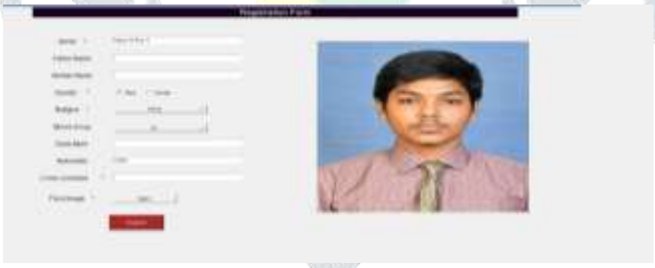


Fig 4: Criminal/Crime registration using GUI

4.2 CRIMINAL DETECTION AND REAL-TIME MONITORING

The face embedding then will be used by the systems connected with the public/private surveillance cameras. Once the person comes into the visible area where the camera could focus, they will be recognized and monitored. It includes the crime details as well as their current behaviour and actions.

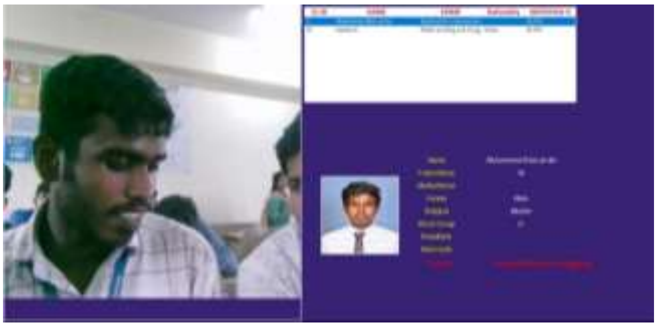
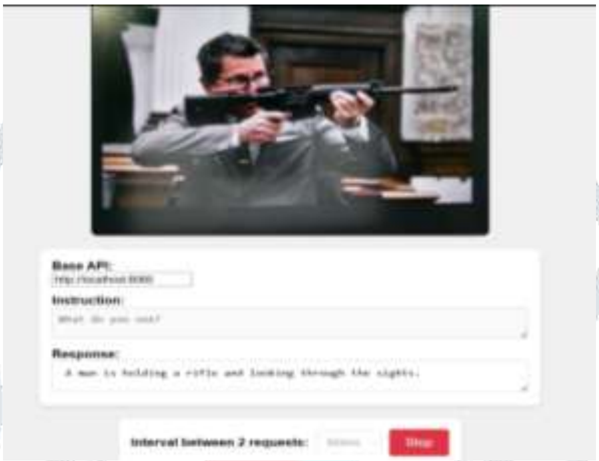


Fig 5: Real-time monitoring and reporting

4.3 ADVANCED ACTION AND BEHAVIOUR RECOGNITION

The action and behaviour recognition is a less explored topic and it is not used in current systems now a days, since it requires high performance systems. But it can be simply done in the mid- range hardware using SmolVLM[6]. It is a vision language model that can describe pictures and videos within milliseconds. So this plays a major role in determining the actions, while processing each frame per one or two seconds.

This runs using the llama.cpp, where the language model is converted into a cpp compatible format, this allows it to process with low latency. It runs on web using localhost, so the date will be processed in the same computer. The process may be controlled based on the requirement by adjusting the interval between two requests. This comes with the downside, if it is very low then the output speed will be faster and causes rapid change in output along with higher requests might cause system to fail, on the other hand if the speed is very low it might miss few details essential for the action recognition.



Base API: http://localhost:8080

Instruction: What do you see?

Response: A man is holding a rifle and looking through the sights.

Interval between 2 requests: [illegible]

Fig 6: Real-time action and behaviour analysis

V. DISCUSSION

Whereas it works effectively in controlled environments, outdoor or poor light conditions remain challenging [4]. Changes in weather, occlusion by masks or helmets, and intentional obscuration continue to pose difficult challenges. Furthermore, the issue of data privacy and ethical surveillance cannot be ignored [5]. The system supports end-to-end encryption of all face embeddings. To stop misuse, audits are done on a regular basis.

Comparative Analysis with the systems that are already in place. Compared to traditional RFID or card-based systems, the proposed model does the following: No more physical tokens, Allows for continuous monitoring, Combines behavioural insights, Improves anomaly detection [3]. But this needs a lot of computing power, regular training updates, proper maintenance and following regulations.

VI. CONCLUSION AND FUTURE WORK

AI powered face recognition and behaviour analysis systems offer an advanced method for safeguarding military areas and public infrastructure. This paper introduced a modular and scalable framework that integrates detection, recognition, and behaviour analysis into a cohesive solution. The model has been shown to be accurate, reliable, and able to work in real time through real-time and continuous testing. Some of the future directions are, Integration with multi-modal biometrics: iris, gait. Edge AI acceleration: FPGA-based deployment, Cross-border data federation: inter-agency tracking, Drone integration: mobile surveillance and reconnaissance. Emotion and stress detection: facial micro-expressions.

REFERENCES

[1] Mr. Dhammapal Suradkar, Ashish Jogad, and Pramod Talole, "Face Detection Using OpenCV," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 7, no. 1, July 2021.

[2] D. Wanyonyi and T. Celik, "Open-Source Face Recognition Frameworks: A Review of the Landscape," *IEEE Access*, vol. 10, pp. 50601-50623, 2022. doi:10.1109/ACCESS.2022.3170037

[3] V. S. Bhat, A. D. Shambavi, K. Mainalli, K. M. Manushree, and S. V. Lakamapur, “Review on Literature Survey of Human Recognition with Face Mask,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 10, no. 01, Jan. 2021.

[4] R. Jafri and H. R. Arabnia, “A Survey of Face Recognition Techniques,” *Journal of Information Processing Systems*, vol. 5, no. 2, pp. 41-68, Jun. 2009. doi:10.3745/JIPS.2009.5.2.041

[5] Y. Jing, X. Lu and S. Gao, “3D Face Recognition: A Comprehensive Survey,” (preprint / survey article) 2022.

[6] A. Marafioti, O. Zohar, M. Farré, M. Noyan, E. Bakouch, P. Cuenca, C. Zakka, L. Ben Allal, A. Lozhkov, N. Tazi, V. Srivastav, J. Lochner, H. Larcher, M. Morlon, L. Tunstall, L. von Werra and T. Wolf, “SmolVLM: Redefining small and efficient multimodal models,” *arXiv preprint arXiv:2504.05299*, Apr. 7 2025