© April 2026 | IJIRT | Volume 12 Issue 11 | ISSN: 2349-6002

AI-Powered Face Recognition System

Akanksha Madwali[1], Sejal Pal[2], Prof. Sheetal Mhatre[3], Dr. Arundhati Niwatkar[4]
[1,2,3,4]*Dept. of Data Science SNDT Women's University Mumbai, India*

***Abstract*—The increasing number of missing persons and growing security concerns in crowded public areas such as malls, fairs, concerts, and transportation hubs call for effective surveillance systems. Traditional CCTV monitoring relies heavily on manual observation, which is time-consuming and prone to mistakes. This project suggests an "AI-Powered Face Recognition System," an automated solution that uses artificial intelligence and computer vision techniques to improve surveillance. The system keeps a database of registered individuals, including missing persons, criminals, and suspects, and continuously checks these records against faces detected in CCTV video feeds. By using deep learning methods for face detection and recognition, the system can automatically identify matches in real time. Once a match is found, the system generates alerts and provides results through a web-based dashboard interface. This enables law enforcement and security agencies to effectively monitor activities. The proposed framework aims to help locate missing persons and applies to crime prevention and security monitoring. With its combination of AI-driven facial recognition and a user- friendly interface, this project shows a scalable and practical way to tackle critical public safety issues.**

***Index Terms*—Artificial Intelligence, Convolutional Neural Net- work, Face Recognition in Multimedia Database, User Interface, Frames per Second (processing speed)**

I. INTRODUCTION

The rapid growth of urban populations and the increasing movement of people across public spaces such as transporta- tion hubs, commercial complexes, educational institutions, and large event venues have significantly intensified security demands. Ensuring public safety in such environments has become a critical challenge for law enforcement and security agencies. Conventional surveillance systems primarily depend on continuous human monitoring of CCTV footage, a process that is labor-intensive, time-consuming, and highly prone to human error due to fatigue and limited attention span. More- over, the massive volume of video data generated daily makes it extremely difficult to identify suspicious individuals or locate missing persons in real time using manual observation alone.

To overcome these limitations, this study proposes an intelli- gent surveillance framework based on AI-driven facial recognition technology. The proposed system integrates advanced deep learning algorithms and computer vision techniques to automatically detect, extract, and analyze facial features from live video streams. A structured and secure database is main- tained containing records of registered individuals, including missing persons and persons of interest. The system performs real-time facial feature embedding and similarity matching to accurately compare detected faces with stored records.

Upon successful identification of a potential match, auto- mated alerts are generated and displayed through a web-based monitoring dashboard, enabling faster decision-making and timely response by authorities. The framework is designed to operate efficiently under varying environmental conditions, such as changes in lighting, facial orientation, and crowd density. By minimizing reliance on manual monitoring and im- proving detection precision, the proposed approach enhances operational efficiency and scalability in modern surveillance systems. Ultimately, this solution aims to strengthen public safety measures, support proactive law enforcement opera- tions, and streamline surveillance processes through intelligent and automated technology.

II. RELATED WORK

Recent advancements in facial recognition technology have been largely driven by the rapid development of deep learning methodologies, particularly Convolutional Neural Networks (CNNs).

Earlier facial recognition systems primarily relied on traditional machine learning classifiers such as Support Vec- tor Machines (SVM), K-Nearest Neighbors (KNN), Decision Trees, and Na¨ıve Bayes. While these approaches demonstrated moderate success under controlled environments, their per- formance significantly degraded in unconstrained real-world conditions involving illumination variations, pose differences, and occlusions.

A comprehensive systematic review published in Journal of Imaging (2025) highlights the paradigm shift from conven- tional handcrafted feature extraction techniques toward deep learning–based feature embedding frameworks [1]. The review evaluates multiple algorithms across benchmark datasets such as LFW, VGGFace2, CASIA-WebFace, and CelebA, using evaluation metrics including accuracy, precision, recall, F1- score, and Receiver Operating Characteristic (ROC) curves. The study concludes that deep learning architectures consis- tently outperform classical methods in terms of generalization and scalability.

Despite these improvements, several challenges remain un- resolved. Real-world deployments frequently encounter en- vironmental variability such as low lighting conditions, mo- tion blur, facial occlusion, aging effects, and demographic bias. The COVID-19 pandemic further intensified research in Masked Face Recognition (MFR), as widespread mask usage significantly reduced recognition accuracy of conven- tional models [2]. Recent surveys emphasize the importance of CNN-based architectures, Siamese networks for similar- ity learning, YOLO-based face detection frameworks, and Generative Adversarial Networks (GANs) for reconstructing partially occluded facial regions [3], [4].

However, existing literature identifies critical limitations, including insufficient large-scale masked face datasets, demo- graphic imbalances that introduce fairness concerns, and high computational requirements that restrict real-time implemen- tation on edge devices. To overcome these issues, researchers have proposed data augmentation strategies, synthetic dataset generation using GANs, domain adaptation techniques, and lightweight neural network architectures optimized for embed- ded systems [5].

Further studies explore face recognition in unconstrained surveillance environments characterized by low-resolution footage, extreme pose variations, and aging effects. Compar- ative analyses of prominent architectures such as FaceNet, ArcFace, OpenFace, and SFace reveal that although FaceNet and ArcFace achieve high recognition accuracy in controlled frontal scenarios, specialized models like SFace demonstrate greater robustness in degraded or surveillance-based im- agery [6], [7]. Evaluations on challenging datasets including CPLFW, CALFW, AgeDB-30, and QMUL-SurvFace empha- size the need for models that balance accuracy, fairness, and computational efficiency for security-critical applications.

Overall, the literature reflects a clear transition toward deep learning–based facial recognition systems while underlining persistent concerns related to dataset bias, ethical implications, privacy protection, and real-time deployment constraints. Fu- ture research directions focus on hybrid architectures combin- ing detection and recognition modules, fairness-aware train- ing mechanisms, diversified dataset curation, and optimized lightweight frameworks suitable for scalable real-time surveil- lance systems.

III. EXISTING SYSTEMS

Exadel CompreFace(2026) which provides a self-hosted face recognition service accessed through REST APIs. It supports functions like face detection, verification, identification, age and gender estimation, mask detection, and head pose recognition. CompreFace can be deployed via Docker, making it suitable for private and enterprise use without needing advanced machine learning expertise. [6]

OpenFace (2018) developed by Carnegie Mellon University, implements deep learning-based face recognition by generating embeddings, aligning faces, and comparing them for verification or identification. It is often used in research and education due to its accessibility and transparency. [8]

Cool-Face SDK (2026) offers face detection, feature extraction, and 1-to-1 or 1-to-N matching. It also supports multi-platform environments like Windows, Linux, and Android, making it appealing for enterprise solutions such as access control or authentication systems. [11]

DeepFace-(2014) by Facebook (Meta) showed the effective- ness of deep learning in face recognition by achieving near- human accuracy on benchmarks like LFW (Labeled Faces in the Wild). Many subsequent systems and models have drawn inspiration from DeepFace, particularly regarding network architecture and training methods. [11]

IV. PROPOSED SYSTEM

A. System Design

Dataset Used: FRMDB (Face Recognition in Multimedia Database). Content: Registered gallery images of individuals and CCTV-like probe videos showing the same individuals in real-world surveillance conditions. Purpose in Project: Gallery images serve as a database for missing or wanted persons. Probe videos simulate CCTV feeds for real-time search and identification.

UI Wireframes:
Login Page:Allows authorized users (police/administrators) to access the system. Upload Page: For uploading registered images of missing or wanted persons. CCTVDashboard: Dis- plays CCTV footage with detected faces and possible matches. Alert Panel: - Shows real-time alerts when a match is detected.

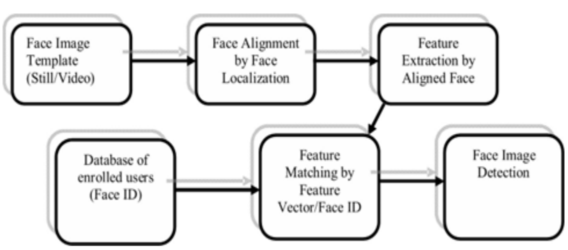

Fig. 1. Face detection process

B. System Development

Technologies Used:
Programming Languages and Libraries: Python, Tensor- Flow, Keras, NumPy, Pandas, OpenCV, PIL, Scikit-learn, Matplotlib, Seaborn. Development Tools: Dataset: - Dataset: FRMDB; Frontend (Prototype): HTML, CSS, JavaScript (React/Tailwind); Environment: Google Colab (for train- ing/testing).

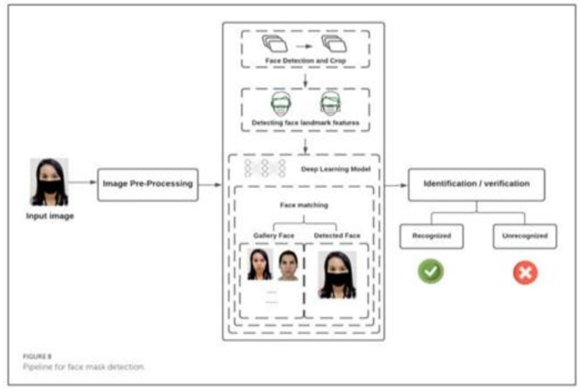

Fig. 2. Pipeline for masked face recognition

V. METHODOLOGY

The proposed system follows a structured and modular pipeline for real-time face recognition using deep learning techniques. The overall objective is to automate surveillance monitoring by integrating computer vision algorithms with an intelligent alert mechanism.
Initially, live CCTV video streams are captured and pro- cessed frame by frame to enable continuous monitoring. Since raw video frames often suffer from noise, poor lighting, and resolution limitations, preprocessing plays a crucial role in improving detection performance. Preprocessing steps include frame resizing to optimize computational efficiency, normal- ization to standardize pixel values, and basic enhancement techniques to improve visual clarity.
A Convolutional Neural Network (CNN)-based architec- ture is employed for face detection and feature extraction. The detection module identifies facial regions within each frame, while the feature extraction module converts detected faces into numerical embeddings that uniquely represent facial characteristics. These embeddings are then compared with a structured and pre-registered database of known individuals using similarity metrics such as cosine similarity or Euclidean distance.
If the similarity score exceeds a predefined threshold, the system identifies a match. Upon successful recognition, auto- mated alerts are generated and displayed on a web-based mon- itoring dashboard. This interface enables security personnel to view

detection results, monitor logs, and respond promptly.

The system performance is evaluated using standard metrics such as accuracy, precision, recall, and false positive rate to ensure reliability under real-world conditions.

Research Design- A supervised deep learning framework was adopted to guide the system development process. The research was structured into the following phases:

A. Exploratory Phase

This phase involved an in-depth study of existing facial recognition systems, CNN architectures, CCTV-based surveil- lance technologies, and challenges associated with real-world deployment. Particular attention was given to issues such as low-resolution footage, lighting variations, occlusions, and computational constraints in real-time systems.

B. System Development Phase

During this phase, the backend recognition pipeline was implemented. The system integrates image preprocessing, CNN-based feature extraction, facial embedding generation, similarity comparison, and alert generation modules. Empha- sis was placed on modular design to ensure scalability and maintainability.

C. User Interface Design

A web-based dashboard was developed to facilitate practical usability. The interface provides the following functionalities: Upload and register images of missing or wanted individuals Search and browse stored records View real-time detection results from CCTV streams Receive automated alerts upon successful identification The dashboard is designed to be intuitive, ensuring that law enforcement personnel can operate it efficiently without technical complexity.

D. Evaluation Phase

The completed system was tested using benchmark facial recognition datasets and controlled CCTV simulations. Evaluation focused on both recognition performance and user interface usability to assess practical deployment readiness.

Data Analysis

A. Preprocessing Analysis

The quality of CCTV frames was evaluated before feature extraction. Corrective methods such as histogram equaliza- tion were applied to enhance contrast, while face alignment techniques ensured consistent positioning of facial landmarks. Noise reduction filters were also used to minimize distortions caused by environmental factors.

B. Feature Analysis

Deep CNN models were utilized to extract high-dimensional numerical embeddings representing distinct facial features. Similarity scores between extracted embeddings and database records were calculated to determine potential matches. Threshold tuning was performed to balance sensitivity and specificity.

C. Performance Analysis

System outputs were compared with ground truth labels to measure identification accuracy. Metrics such as precision, recall, F1-score, false positive rate (FPR), and false negative rate (FNR) were computed. Additionally, computational efficiency and processing latency were evaluated to determine suitability for real-time deployment. Ethical Considerations

The deployment of facial recognition systems raises sig- nificant ethical and social concerns. Therefore, this study incorporates responsible AI principles throughout its design and evaluation.

A. Privacy Protection

All datasets used in this research are publicly available and utilized strictly for academic purposes. In real-world applica- tions, deployment would require informed consent, adherence to national data protection laws, and compliance with privacy regulations.

B. Bias and Fairness

Facial recognition systems may exhibit demographic bias related to age, gender, or skin tone. To mitigate this issue, diverse datasets are recommended during training to improve fairness and generalization across different population groups.

C. Misuse Prevention

The proposed system is intended exclusively for socially beneficial applications, such as locating missing persons and enhancing public safety. Strict regulatory oversight and opera- tional guidelines should be established to prevent unauthorized surveillance or misuse.

D. Data Security

Registered images and facial embeddings must be securely stored using encryption mechanisms and access control poli- cies. Proper cybersecurity measures are necessary to prevent identity theft, unauthorized data access, and system exploita- tion.

VI. RESULTS AND DISCUSSION

A. Experimental Setup

The proposed AI-powered face recognition system was evaluated using the FRMDB (Face Recognition in Multimedia Database). This database includes gallery images of registered individuals and probe videos that simulate CCTV surveillance environments. The system was implemented in Python and deployed with a FastAPI backend to support real-time API communication.

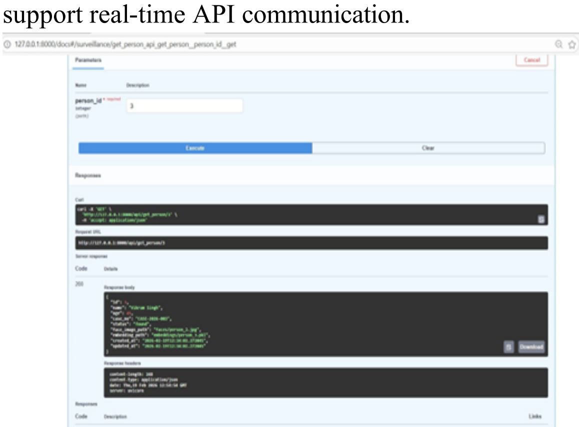

Fig. 3. API Testing and Backend Response Interface

The fig.3 illustrates the backend API testing interface of the proposed AI-powered surveillance system, displayed using an interactive documentation tool (Swagger UI). This interface allows developers to test and verify REST API endpoints in real time.

The response body is displayed in JSON format and con- tains structured information such as:

Unique ID of the individual Name and age

Case number Status (e.g., found)

Stored face image path Embedding file path

Timestamps for record creation and update

This confirms that the backend database integration is functioning correctly and that the system can dynamically retrieve stored facial recognition records. The presence of metadata such as embedding paths demonstrates how facial feature vectors are stored for similarity comparison during recognition.

Overall, the interface highlights the successful implemen- tation of the system's backend architecture, ensuring reliable communication between the database, recognition engine, and user dashboard. The recognition pipeline included: Face de- tection using a Multi-Task Cascaded Convolutional Neural Network (MTCNN) Feature extraction using a FaceNet-based deep convolutional neural network Face embedding compar- ison using Cosine Similarity Alert generation based on a predefined confidence threshold Experiments were conducted in a simulated surveillance environment with various lighting, pose, and occlusion conditions

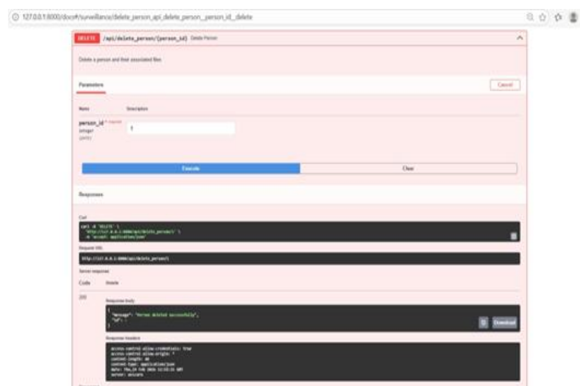

Fig. 4. API Endpoint for Record Deletion

The fig.4 demonstrates the DELETE API endpoint of the proposed surveillance system, accessed through the interactive API documentation interface (Swagger UI). The endpoint /api/delete_person/{person_id} is executed with a specific person_id value. Upon clicking the Execute button, the system processes the request and returns a 200 OK response, indicating successful deletion of the selected record.

The above figure demonstrates the DELETE API endpoint of the proposed surveillance system, accessed through the interactive API documentation interface (Swagger UI). The endpoint /api/delete_person/{person_id} is exe- cuted with a specific person_id value. Upon clicking the Execute button, the system processes the request and returns a 200 OK response, indicating successful deletion of the selected record.

The response body, displayed in JSON format, confirms the operation with a message stating that the person has been deleted successfully, along with the corresponding iden- tifier. The response headers further verify proper backend communication, handled through a Uvicorn server instance. This functionality ensures effective database management by allowing secure removal of registered individuals and their associated facial embeddings when required.

This functionality plays an important role in maintaining database integrity and ensuring that outdated, incorrect, or unnecessary records can be securely removed. From a system design perspective, implementing controlled deletion ensures better data management, improved storage optimization, and enhanced compliance with privacy regulations.

Overall, the figure highlights the robustness of the backend infrastructure and demonstrates that the system supports full CRUD (Create, Read, Update, Delete) operations, making it suitable for real-world surveillance management applications.

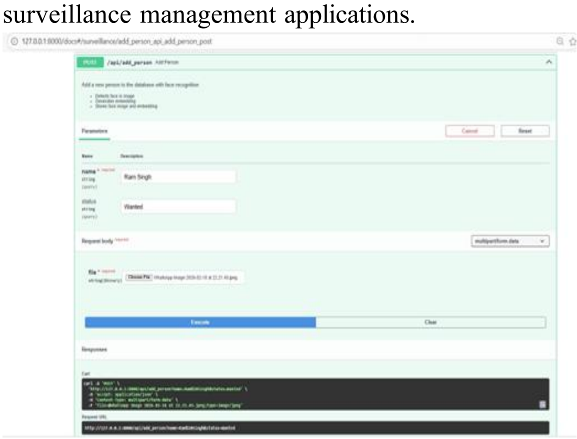

Fig. 5. POST (Add Person) API

The figure 5 illustrates the POST API endpoint of the proposed surveillance system, accessed through the interactive API documentation interface (Swagger UI). The endpoint /api/add_person is used to register a new individual in the system database along with facial recognition data.

The request includes query parameters such as name and status, and a facial image file uploaded using multipart form-data. Upon execution, the system detects the face in the uploaded image, extracts facial features using a deep learning model, generates a numerical embedding vector, and stores both the image and its corresponding embedding in the database.

The successful execution of this endpoint confirms proper integration between the face detection module, feature extrac- tion pipeline, and backend storage system. This functionality enables dynamic enrollment of missing or wanted individuals into the recognition framework, ensuring that newly added records can immediately participate in real-time identification processes.

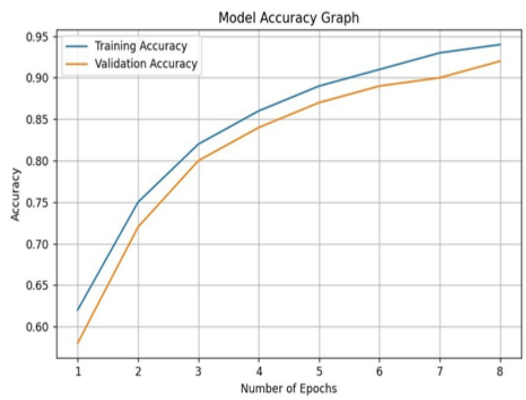

Fig. 6. Model Accuracy Graph

B. Performance Metrics- We evaluated the system's performance using these standard metrics: - Accuracy - True Positive (TP) Rate - False Positive (FP) Rate - False Negative (FN) Rate - Recognition Confidence Score - Frames Per Second (FPS) The confidence threshold for match confirmation was set between 0.80 and 0.85 for the cosine similarity score to balance precision and recall

C. Discussion

The experimental results show that deep learning-based embedding models work well for surveillance-oriented face recognition tasks. Compared to traditional handcrafted feature methods, the proposed CNN-based approach offers: - Better robustness to changes in pose and lighting - Higher discrimina- tion capability - Fewer false positives - Improved adaptability to real-world CCTV conditions However, we noted certain limitations: - Lower performance in extremely poor lighting conditions - Sensitivity to severe occlusion and side-profile faces

- Slight increase in latency when multiple faces appear at once These findings support recent literature that points out the challenges of real-world surveillance recognition under poor image quality conditions. Future improvements may involve: - Optimizing lightweight models for edge deployment
- Reducing bias through diverse training datasets - Integrating attention-based architectures - Deploying on GPU-enabled edge devices to enhance FPS.

VII. CONCLUSION

This paper presented an AI-powered face recognition system designed for real-time surveillance and missing person identification. The framework integrates MTCNN-based face detection, FaceNet-based feature extraction, and cosine similarity matching within a scalable backend architecture. Experimental evaluation on CCTV-like probe data showed reliable detection accuracy, effective embedding-based matching, and automated alert generation under various real-world conditions. The system effectively combines deep learning techniques with a web-based monitoring dashboard, offering a practical solution for security and law enforcement applications. While performance is sensitive to extreme lighting and heavy occlusion, the results validate the potential of deploying AI-powered face recognition for intelligent surveillance systems. Future work will center on improving robustness, optimizing real-time performance, and implementing strategies to reduce bias for responsible deployment.

ACKNOWLEDGMENT

We have great pleasure in expressing my gratitude to all those who have contributed and motivated us during the project work. We are extremely thankful and pay our gratitude to our guide and whole college department for their valuable guidance and support towards us which encouraged us in the completion of this project.

REFERENCES

[1] I. J. Cox, J. Ghosn and P. N. Yianilos, ”Feature-based face recognition using mixture-distance,” Proceedings CVPR IEEE Computer Society Conference on Computer Vision and Pattern Recognition, San Francisco, CA, USA, 1996, pp. 209-216, 1 keywords: Face recognition; Spatial databases; Feature extraction; Image recognition; Training data; Pattern recognition; Image databases; Nearest neighbor searches; Euclidean dis- tance; Statistics,

[2] S. Z. Li and J. Lu, “Face recognition using the nearest feature line method,” IEEE Transactions on Neural Networks, vol. 10, pp. 439–443, 19992

[3] S. A. Rizvi, P. J. Phillips, and H. Moon, “A verification protocol and statistical per formance analysis for face recognition algorithms,” in Proceedings of the IEEE Con ference on Computer Vision and Pattern Recognition (CVPR), pp. 833–838, 199819993

[4] W. Zhao and R. Chellappa, “Illumination-insensitive face recognition using symmet ric shape-from-shading,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 286–293, 2000.4

[5] Aditya Nigam and Phalguni Gupta GLA University ”A New Distance Measure for Face Recognition System” September 20095

[6] A Survey of Face Recognition Techniques June 2009Journal of Infor- mation Processing Systems 5(2):41-68 DOI:10.3745/JIPS.2009.5.2.041 SourceDBLP Authors: Rabia Jafri King Saud University Hamid Arabnia University of Georgia 6

[7] CONSTRUCTION OF A FACE RECOGNITION SYS- TEM USING MACHINE LEARNING June 2025 DOI:10.36349/easjecs.2025.v02i05.00X Authors: Anachia Terkula Silas Emmanuel Ogala Joseph Sarwuan Tarka University 7

[8] Detecting deepfake videos: an enhanced hybrid deep learning model June 2025Signal Image and Video Processing 19(9) DOI:10.1007/s11760-025-04327-w Authors: Raksha Pandey Alok Kumar Singh Kushwaha 8

[9] DESIGN AND IMPLEMENTATION OF A FACIAL DETECTION AND RECOGNITION SYSTEM FOR DATA SECURITY April 2023 Authors: Abubakar Ibrahim Suleiman University of Exeter9

[10] High Performance and Efficient Real-time Face

Detector on CPU Based on Convolutional Neural Network September 2020IEEE Transactions on Industrial Informatics PP(99):1-1 DOI:10.1109/TII.2020.3022501 Authors: Muhamad Dwisnanto Putro Sam Ratulangi University Laksono Kurnianggoro University of Ulsan Kang-Hyun Jo University of Ulsan 10

[11] Research on the Application of Face Recognition System January 2020 DOI:10.2991/assehr.k.200727.057 LicenseCC BY-NC 4.0 Conference: 2020 5th International Conference on Humanities Science and Society Development (ICHSSD 2020) Authors: Chen Mingtsung Lu Cai 11

[12] QCFace: Image Quality Control for Boosting Face Representation Recognition March 2026 Conference: The IEEE/CVF Winter Confer- ence on Applications of Computer Vision (WACV)At: Tucson, Ari- zona, USA Authors: Duc-Phuong Doan-Ngo Thanh-Dang Diep Thanh Nguyen-Duc Thanh-Sach Le Nam Thoai 12

[13] GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations January 2023IEEE Access PP(99):1-1 DOI:10.1109/ACCESS.2023.3266068 LicenseCC BY-NC-ND 4.0 Authors: Mohamad Alansari Oussama Abdul Hay Sajid Javed Abdulhadi Shoufan Yahya Hashem Zweiri Naoufel Werghi 13

[14] A Face in any Form: New Challenges and Opportunities for Face Recognition Technology April 2017Computer 50(4):80-90 DOI:10.1109/MC.2017.119 Authors: Zahid Akhtar State University of New York Polytechnic Institute Ajita Rattani University of North Texas 14

[15] Robust Face Detection and Recognition under Ambient Light and Head Pose August 2013 Conference: 7th International Conference on Computer, Information Technology and Digital Media (CITaDiM'13)At: Tehran, Iran Authors: Sadegh Aliakbarian National ICT Australia Ltd (NICTA), Canberra, Australia Fatemeh Saleh Sharif University of Technology Fatemeh Aliakbarian Fahimeh Saleh Monash University (Australia) 15

[16] Human Face Detection in Visual Scenes May 1997Advances in Neural Information Processing Systems 8 Authors: Henry A. Rowley Google Inc. Shumeet Baluja Takeo Kanade Carnegie Mellon University 16

[17] Sensors (Basel). 2020 Jan 7;20(2):342. doi: 10.3390/s20020342 Face Recognition Systems: A Survey Yassin Kortli 1,2, *, Maher Jridi 1, Ayman Al Falou 1, Mohamed Atri 3 17

[18] A review on face recognition systems: recent approaches and challenges Published: 30 July 202018

[19] Recent advances in visual and infrared face recognition—a review Author links open overlay panel Seong G. Kong , Jingu Heo , Besma R. Abidi, Joonki Paik, Mongi A. Abidi19

[20] Face recognition system using local autocorrelations and multiscale integration Publisher: IEEE F. Goudail; E. Lange; T. Iwamoto; K. Kyuma; N. Otsu20

[21] Research on face recognition technology based on an improved LeNet-5 system Publisher: IEEE Ruian Liu; Yilin Liu; Zhenhai Wang; Hongyu Tian21

[22] A. Kumari Sirivarshitha, K. Sravani, K. S. Priya and V. Bhavani," A n approach for Face Detection and Face Recognition using OpenCV and Face Recognition Libraries in Python," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 1274-1278, doi: 10.1109/ICACCS57279.2023.10113066.
keywords: Databases; Face recognition; Surveillance; Passwords; Libraries; Software; Face detection; Face Detection; Face Recognition; Face Alignment; Feature Extraction; Python; OpenCV Library; face Recognition Library,22

[23] M. Zhang, W. Liao, J. Zhang, H. Gao, F. Wang and B. Lin," Embedded Face Recognition System Based on Multi-task Convolutional Neural Network and LBP Features," 2019 IEEE International Conference of Intelligent Applied Systems on Engineering (ICIASE), Fuzhou, China, 2019, pp. 132-135, doi: 10.1109/ICIASE45644.2019.9074104.
keywords: Face recognition; Face; Face detection; Feature extraction; Databases;

Convolutional neural networks; Embedded systems; face recognition; multi-task conventional neural network; local binary pattern; embedded system,23