INTERNATIONAL JOURNAL
FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Face Authentication using MTCNN and FaceNet

Anjali Pandit[1], Ritesh Nikalje[2], Neha Vishwakarma[3], Vaishnavi Vishwasrao[4], Prof. Trupti Khose[5]

Department of Information Technology, Dhole Patil College of Engineering, Pune

Abstract: Advancements in facial recognition are on the rise after the recent breakthroughs in deep learning technologies and the extensive training datasets. But still, the practical application of facial recognition for authentication purposes faces some difficulties and problems when dealing with variations that are observed in real-world scenarios, including variations in facial poses, varying angles, lightning conditions and potential obstructions. In order to resolve these challenges, this paper presents an innovative deep learning API, which combines the capabilities of MTCNN and FaceNet, to overcome these limitations. Building upon the foundations of MTCNN and FaceNet, we have developed an API capable of verifying the identity of users through a two-step verification process. The system utilizes MTCNN for precise face detection and FaceNet for facial feature extraction that has the ability to directly map facial images into a compact Euclidean space in which spatial distances directly reflect facial similarity, and then storing this data securely within a MongoDB database. We have used the cutting-edge Deep Face model, developed by Facebook's AI research team. Its reliable deep learning capabilities have helped us in achieving exceptional accuracy in the user's verification process. This system serves to provides a superior level of user authentication, effectively reducing the risk of an unauthorized access while optimizing the user experience. Even though there is still some room for improvement within our experiment, we are committed to providing a comprehensive summary of our findings and an exploration of the challenges on the horizon.

Keywords: Facial recognition, Deep learning, Authentication, MTCNN, FaceNet, MongoDB database, User authentication, Unauthorized access, User experience

I. INTRODUCTION

In an era where digital security is paramount, the demand for robust authentication systems has never been more pressing. Traditional methods relying solely on passwords and email verifications are increasingly vulnerable to sophisticated cyber threats. To address this, our research project endeavours to design and implement an advanced authentication system, leveraging the power of facial recognition technology. By integrating the Multi-Task Cascaded Convolutional Networks (MTCNN) for precise face detection and FaceNet for accurate facial feature extraction, we aim to create a two-step verification process that not only fortifies security but also enhances the user experience.

Facial recognition technology has emerged as a cutting-edge solution, offering a unique and biometrically secure method for user authentication. MTCNN, known for its efficiency in detecting facial landmarks, forms the initial stage of our system. Subsequently, FaceNet, a state-of-the-art deep learning model developed by Google, takes charge of mapping facial features into a compact Euclidean space, providing a reliable and unique representation for each individual. The fusion of these technologies aims to mitigate the vulnerabilities associated with traditional authentication methods and significantly elevate the level of security.

This project delves into the intricacies of facial recognition, exploring the challenges posed by variations in facial expressions, poses, and lighting conditions. By conducting a comprehensive examination of MTCNN and FaceNet, we seek to understand their synergistic potential in crafting an authentication system that balances accuracy, efficiency, and user-friendliness. The outcomes of this research contribute not only to the academic understanding of biometric security but also offer practical insights for the implementation of facial recognition-based authentication systems in real-world scenarios.

As we navigate through the details of our research methodology, literature review, this paper aims to provide a comprehensive view of our endeavours, shedding light on the advancements made and challenges encountered in the pursuit of a more secure digital landscape.

II. LITERATURE REVIEW

This literature survey examines existing research on two-step verification systems employing facial recognition. This section critically reviews relevant scholarly works, focusing on the integration of MTCNN (Multi-Task Cascaded Convolutional Networks) and FaceNet algorithms. By synthesizing knowledge from previous research, this literature survey seeks to identify gaps in current understanding, highlight emerging trends, and inform the research framework, ultimately contributing to the ongoing discourse on the efficacy of facial recognition in bolstering cybersecurity measures.

TABLE NO. 1 LITERATURE REVIEW

Sr. No	Paper Name	Author, Year of Publishing Journals	Work
1.	Research on Face Detection Technology Based on MTCNN.	Ning Zhang, Junmin Luo, and Wuqi Gao, 2020, In IEEE International Conference on Computer Network, Electronic and Automation (ICCNEA).	In this paper, they mainly focus on the application of MTCNN in face detection. The authors learned a lot about computer vision and they learned how to make computers recognize faces in images and what measures should be taken to make face detection even better in the future.
2.	The Research and Analysis of Different Face Recognition Algorithms.	Wang Xiang, 2022. Journal of Physics: Conference Series. CONF-CIAP 2022.	In this paper, the author discussed the principles of five algorithms used in the face recognition field and the merits and weaknesses of each algorithm. They came to a conclusion that the combination of algorithms like MTCNN and FaceNet have more accurate judgments of human faces than the single algorithm.
3.	Face Recognition Based on MTCNN and Integrated Application of FaceNet and LBP Method.	Zaiye Yang, Wei Ge, Zheng Zhang, 2020, In IEEE 2nd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM)	In this paper, they aim to improve the robustness of illumination on the basis of MTCNN and FaceNet. They talk about how parallel connection of LBP and FaceNet improves the face recognition accuracy. They used Markus Weber's face database and ORL to experiment with the enhanced model.
4.	Face Recognition Based on MTCNN and FaceNet.	Rongrong Jin, Hao Li, Jing Pan, Wenxi Ma, and Jingyu Lin, 2021, Association for the Advancement of Artificial Intelligence	In this paper the authors introduce a multi-task cascaded CNN framework that enhances face detection and recognition. They demonstrate the superior performance in face alignment benchmarks, and joint face alignment learning. Their approach employs a unified embedding method for face verification, which simplifies the setup and improves performance compared to other techniques.

III. METHODOLOGY

The research methodology for our project involves a structured approach to developing, testing, and evaluating the facial recognition system.

The following sections outline the key methodological aspects of this project:

A. Data Collection and Preprocessing

Data collection is a crucial aspect of this research, involving the acquisition of facial image datasets to train and test the system.

Data preprocessing techniques will be applied, including image normalization, feature extraction, and quality control, to ensure the data's relevance and quality.

B. MTCNN (Multi-task Cascaded Convolutional Networks) Algorithm

MTCNN is a multi-stage algorithm designed for real-time face detection. It consists of three cascaded networks: the P-Net, R-Net, and O-Net. The P-Net is responsible for generating candidate regions for faces, the R-Net refines these candidates and filters out false positives, and the O-Net further refines the face bounding boxes and extracts facial landmarks. This multi-stage approach ensures high precision in detecting faces under various conditions, such as scale, pose, and occlusion.

MTCNN's remarkable accuracy and efficiency make it a valuable component of our project. It provides the system with the ability to locate and extract facial regions, setting the stage for the subsequent face recognition phase.

C. FaceNet Algorithm

FaceNet is a deep convolutional neural network (CNN) designed to generate facial embeddings, also known as face embeddings. These embeddings represent a person's unique facial characteristics as numerical vectors. FaceNet's architecture is trained on a large dataset of face images, enabling it to map faces into a multi-dimensional space where similar faces are positioned closer together, and dissimilar faces are farther apart. This Euclidean space of face embeddings makes it possible to quantify the similarity between two faces.

In our project, FaceNet calculates face embeddings for each individual user during the enrolment phase. These embeddings serve as a unique and compact representation of the user's face, which can be stored in a MongoDB feature store. During authentication requests, FaceNet is used to generate embeddings for the captured face, which are then compared to the stored embeddings in the feature store.

The FaceNet algorithm's accuracy, coupled with its ability to capture subtle facial details, plays a pivotal role in ensuring reliable and secure user verification within our system.

D. Authentication system workflow

The heart of our project lies in its robust authentication system. This system employs advanced techniques and technologies to ensure that access to restricted areas, applications, or devices is granted only to authorized users.

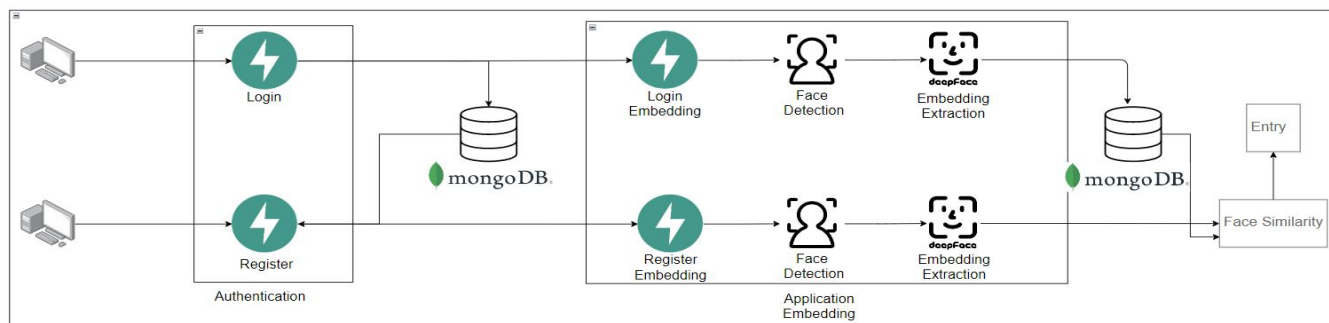The authentication process involves several key steps:

Fig .1. Authentication system workflow

1) *Face Detection:* The process begins with face detection, where the MTCNN (Multi-task Cascaded Convolutional Networks) algorithm comes into play. MTCNN locates and extracts faces within an image or video frame. It identifies the facial regions of interest, providing a focused area for subsequent processing.
2) *Face Embeddings:* Following face detection, the FaceNet algorithm generates face embeddings for each individual. These embeddings serve as unique representations of users' faces in the form of numerical vectors. The embeddings are then stored in a MongoDB feature store for quick retrieval during authentication requests.
3) *User Verification:* When a user seeks access to a secure area or system, their face is captured, and FaceNet generates embeddings for the captured face. The system then performs a similarity comparison between the user's face embeddings and those stored in the feature store. This comparison is based on Cosine Similarity, a measure of the cosine of the angle between two non-zero vectors.
4) *Access Decision:* The Cosine Similarity score determines whether the captured face matches the stored face embeddings within an acceptable threshold. If the similarity score exceeds the threshold, access is granted, and the user is verified. If the score falls below the threshold, the authentication request is denied.

5) *Cosine Similarity:* Cosine Similarity is a vital component of the authentication system, serving as the metric to assess the likeness of face embeddings. It measures the cosine of the angle between two non-zero vectors and produces a score between -1 (dissimilar) and 1 (identical). The system's access decision threshold can be adjusted to balance security and convenience.

The project's authentication system ensures a high level of security by verifying users' identities through their facial features. By combining precise face detection and FaceNet's powerful face recognition capabilities, this system offers a reliable and efficient means of access control, making it suitable for a wide range of applications and environments.

E. Testing and Validation

Rigorous testing procedures will be conducted to validate the system's performance. This includes testing under various conditions, assessing real-time response, and evaluating accuracy.

The methodology integrates user testing to ensure the system's user-friendliness and reliability.

F. Benchmarking and Comparison

The research methodology includes benchmarking the developed system against existing facial recognition technologies, both traditional and advanced.

Comparative analysis will be performed to assess the system's superiority and identify areas of improvement.

G. Ethical Considerations

The methodology encompasses ethical considerations related to data privacy, security, and compliance with regulatory standards.

IV.CONCLUSIONS

Our project presents an innovative system leveraging the power of MTCNN and FaceNet. This system excels in balancing high-security requirements with user-friendliness. MTCNN demonstrates its effectiveness in accurate face detection, while FaceNet's capability to extract unique facial features ensures reliable recognition.

The two-step verification process added an extra layer of security. This project signifies a significant advancement in the realm of biometrics and security systems. It highlights the potential of deep learning in safeguarding critical access points. Our project contributes to the development of more secure and user-centric authentication systems in the digital age, addressing the increasing need for robust identity verification.

While challenges, such as dataset quality and robustness against facial alterations, exist, the future roadmap involves system refinement, dataset expansion, and addressing ethical implications.

REFERENCES

[1] Ning Zhang, Junmin Luo, and Wuqi Gao. Research on Face Detection Technology Based on MTCNN. 2020. In IEEE International Conference on Computer Network, Electronic and Automation (ICCNEA).

[2] Zaiye Yang, Wei Ge, Zheng Zhang. Face Recognition Based on MTCNN and Integrated Application of FaceNet and LBP Method. 2020. In IEEE 2nd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM).

[3] Edwin Jose, Greeshma M., Mithun Haridas T. P., Supriya M. H. Face Recognition based Surveillance System Using FaceNet and MTCNN on Jetson TX2. 2019. In IEEE 5th International Conference on Advanced Computing & Communication Systems (ICACCS).

[4] Wang Xiang. The Research and Analysis of Different Face Recognition Algorithms. 2022. Journal of Physics: Conference Series 2386 (2022) 012036.

[5] Narayana Darapaneni, Aruna Kumari Evoori, Vijaya Bava Vemuri, Thangaselvi Arichandrapandian, Karthikeyan G, Anwesh Reddy Paduri, Dhivakar Babu, Jayadev Madhavan. Automatic Face Detection and Recognition for Attendance Maintenance. 2020. In IEEE International Conference on Industrial and Information Systems (ICIIS).

[6] De Rosal Ignatius Moses Setiadi, Heru agus Santoso, Atika Sari, Eko Hari Rachmawanto. Face Recognition using FaceNet (Survey, Performance Test, and Comparison) .2019 Fourth International Conference on Informatics and Computing (ICIC).

[7] Wang Aihua. Design and optimization of two-step verification scheme for form data. 2021. Journal of Physics: Conference Series 1883 (2021) 012092 doi:10.1088/1742- 6596/1883/1/012092

[8] Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, Lior Wolf. DeepFace: Closing the Gap to Human-Level Performance in Face Verification. 2014. IEEE Conference on Computer Vision and Pattern Recognition.

[9] Zhou Chun-rong. Research on Face Recognition Technology Based on Deep Learning. 2020. IEEE International Conference on Industrial Application of Artificial Intelligence (IAAI).

[10] NehaCharandas Titre, Antara Bhattacharya. Access Data Privacy Management Control in MongoDB. 2018. IEEE international conference on system, computation, automation and networking (icscan).

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)