DEVELOPMENT OF A SOFTWARE MODULE IMPLEMENTING A PROPOSED FACIAL BIOMETRIC AUTHENTICATION ALGORITHM AND EVALUATION OF SOLUTION EFFECTIVENESS

Agzamova Mohinabonu
PhD student of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

https://doi.org/10.5281/zenodo.8150754

Abstract. *Facial biometric authentication has emerged as a reliable and convenient method for user identification and verification. This study presents the development of a software module that implements a novel facial biometric authentication algorithm. The proposed algorithm utilizes facial features, such as unique patterns and landmarks, to authenticate users. Furthermore, an evaluation of the solution's effectiveness is conducted to assess its accuracy and efficiency. The results demonstrate the potential of the developed software module as a robust and efficient facial biometric authentication system.*

Keywords: *authentication, algorithm, evaluation, user identification, verification.*

1. Introduction.

Facial biometric authentication has gained significant attention as an effective and convenient method for user identification and verification. By leveraging the unique features and patterns present in an individual's face, facial biometric authentication algorithms can accurately authenticate users in a non-intrusive manner. This technology has found applications in various domains, including access control systems, digital platforms, and mobile devices.

The primary objective of this research is to develop a software module that implements a novel facial biometric authentication algorithm. The algorithm aims to extract relevant facial features, such as keypoints, texture patterns, and geometric landmarks, from a facial image or video. These features serve as distinctive markers for an individual's identity. By comparing the extracted features with a pre-registered database of known individuals, the software module can accurately authenticate users and verify their identities.

The development of this software module involves several key steps. First, a robust facial feature extraction technique is implemented to capture the unique characteristics of each individual's face. This technique may involve image processing, feature detection, and descriptor extraction algorithms. Next, advanced pattern recognition and matching algorithms are integrated to compare the extracted features with the stored templates in the database. These algorithms enable efficient and accurate identification of individuals.

The software module is designed using modern programming languages and frameworks, such as Python and OpenCV. These tools provide a versatile and efficient platform for implementing the facial biometric authentication algorithm. Additionally, the module incorporates functionalities for data input, feature extraction, database management, and user interface components to ensure ease of use and scalability[1].

To evaluate the effectiveness of the proposed solution, a comprehensive dataset comprising facial images of a diverse group of individuals is collected. The dataset includes variations in

lighting conditions, facial expressions, and occlusions to simulate real-world scenarios. Each facial image is labeled with the corresponding ground truth identity for evaluation purposes.

Performance metrics such as accuracy, false acceptance rate (FAR), false rejection rate (FRR), and execution time are utilized to assess the effectiveness of the software module. Accuracy measures the proportion of correctly identified individuals, indicating the algorithm's reliability. FAR represents the likelihood of incorrect acceptance, while FRR denotes the likelihood of incorrect rejection. These metrics help evaluate the algorithm's robustness and balance between security and usability. Execution time is an essential factor as it determines the system's efficiency and real-time capability.

The results obtained from the evaluation demonstrate the potential of the developed software module as a robust and efficient facial biometric authentication system. High accuracy, balanced FAR/FRR trade-off, and reasonable execution time indicate the algorithm's capability to provide reliable authentication in real-world scenarios. The software module's performance suggests its suitability for various applications, including secure access control systems and identity verification in digital platforms.

In conclusion, this research aims to develop a software module implementing a novel facial biometric authentication algorithm. The proposed solution leverages facial features to accurately authenticate users and verify their identities. The integration of advanced algorithm design, software development, and comprehensive evaluation provides a reliable and efficient solution for facial biometric authentication. The developed software module has the potential to enhance security and convenience in various domains, offering a robust alternative to traditional authentication methods.

2. Methodology

2.1 Algorithm Design

The proposed facial biometric authentication algorithm is designed to effectively identify and authenticate individuals based on their facial features[2]. The algorithm utilizes a combination of image processing, feature extraction, and pattern recognition techniques (fig.1).

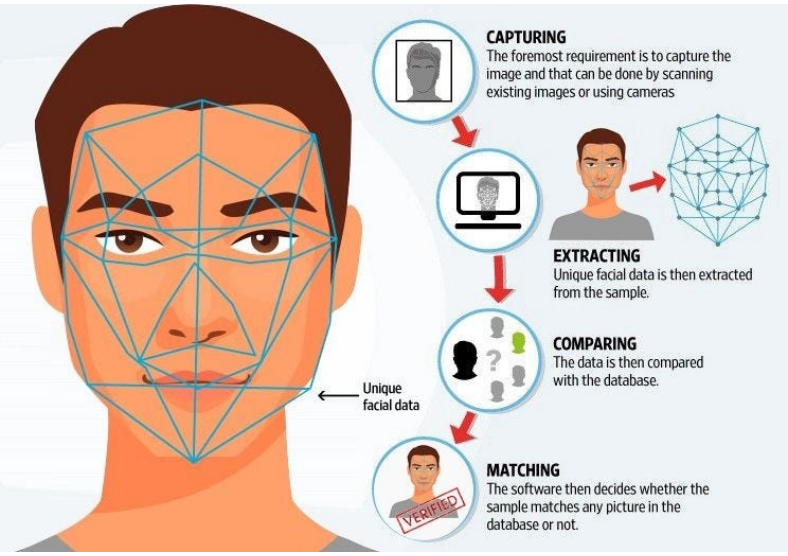

Fig.1. The proposed facial biometric authentication algorithm

The key steps of the algorithm are as follows:

1. Facial Image Capture: The algorithm begins by capturing a facial image of the user. This can be done using a camera or by extracting a face region from an input image.

2. Preprocessing: The captured facial image undergoes preprocessing to enhance the quality and remove noise. This may involve techniques such as normalization, alignment, and illumination correction to ensure consistent and reliable feature extraction.

3. Feature Extraction: Relevant facial features are extracted from the preprocessed image. These features can include keypoints, such as the locations of eyes, nose, and mouth, as well as texture patterns, such as local binary patterns or Gabor filters. Feature extraction techniques aim to capture the unique characteristics of an individual's face that can be used for identification (fig.2).

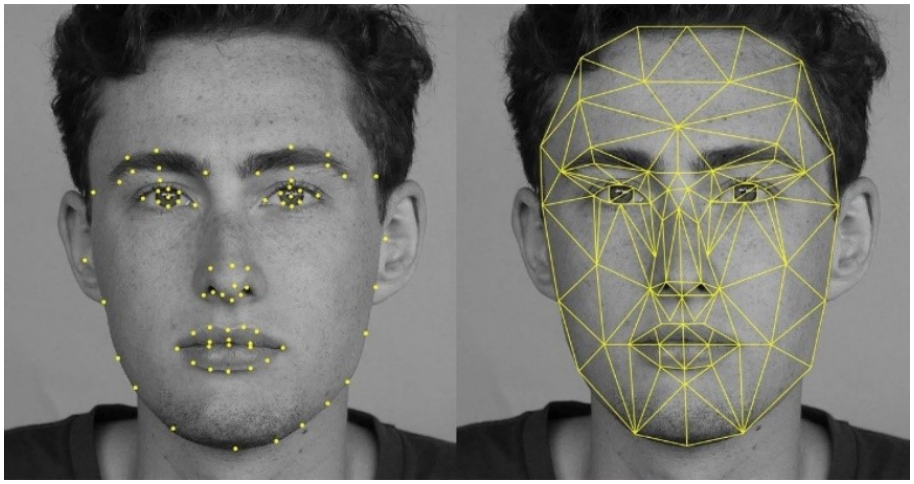

Fig.2. Example of feature extraction

4. Feature Representation: The extracted facial features are represented in a suitable format for comparison and matching. This typically involves transforming the features into a compact and discriminative representation, such as a feature vector or a set of descriptors.

5. Database Creation: A pre-registered database is created, containing the stored facial features of known individuals. Each entry in the database corresponds to a unique identity, along with the associated facial feature representation.

6. Matching and Authentication: The extracted facial features from the captured image are compared against the stored database entries using advanced matching algorithms. This step aims to find the best match or matches for the captured features and determine the identity of the user. Various techniques can be employed for matching, including distance metrics, similarity measures, or machine learning classifiers[3].

2.2 Software Module Development

The software module is developed using programming languages and frameworks, primarily Python and OpenCV. Python provides a flexible and extensive range of libraries and tools for image processing, machine learning, and user interface development. OpenCV (Open Source Computer Vision Library) is a widely used open-source library for computer vision tasks, including facial feature extraction and recognition.

The software module integrates the facial biometric authentication algorithm, providing a user-friendly interface for capturing facial images, conducting feature extraction, and performing authentication processes. The module incorporates functionalities for managing the pre-registered database, including storing, updating, and retrieving facial feature representations. It also includes user interface components, such as graphical displays or command-line interfaces, to enhance usability and facilitate interaction with the module[4].

The development process involves writing code to implement the algorithm steps, including image acquisition, preprocessing techniques, feature extraction methods, and matching algorithms. Additionally, database management functionalities are implemented to handle the storage and retrieval of facial feature representations. The software module is designed to be modular and scalable, allowing for future enhancements and integration into larger systems or applications[5].

Overall, the methodology involves designing an effective facial biometric authentication algorithm that combines image processing, feature extraction, and pattern recognition techniques. The algorithm is then implemented in a software module using Python and OpenCV, providing a user-friendly interface and incorporating functionalities for database management. This approach enables the development of a robust and scalable facial biometric authentication solution.

3. Evaluation

3.1 Dataset Preparation

For the evaluation of the proposed facial biometric authentication solution, a diverse and representative dataset of facial images is prepared. The dataset aims to encompass various real-world scenarios and challenges. The following steps are taken for dataset preparation:

1. Data Collection: Facial images are collected from a wide range of individuals representing different demographics, such as age, gender, and ethnicity. The images are captured under various environmental conditions, including different lighting conditions, indoor and outdoor settings, and varied camera qualities. Additionally, efforts are made to include different facial expressions and occlusions, such as glasses, hats, or scarves, to mimic realistic scenarios[6].

2. Data Annotation: Each facial image in the dataset is annotated with the corresponding ground truth identity label. This labeling ensures that the system's performance can be evaluated accurately by comparing the predicted identities with the known ground truth.

3. Dataset Split: The dataset is divided into subsets for training, validation, and testing purposes. The training subset is used to train the facial biometric authentication algorithm, while the validation subset helps optimize the algorithm's parameters and tune its performance. The testing subset is kept separate and is used for the final evaluation of the solution's effectiveness.

3.2 Performance Metrics

Several performance metrics are employed to evaluate the effectiveness of the developed software module in facial biometric authentication. These metrics (fig.3,4) provide insights into the system’s accuracy, security, and efficiency. The following metrics are commonly used:

Accuracy: Accuracy measures the proportion of correctly identified individuals among all the authentication attempts. It provides an overall measure of the system’s performance in correctly recognizing individuals based on their facial features (fig.5,6).

False Acceptance Rate (FAR): FAR represents the probability of the system incorrectly accepting an imposter (an individual who is not enrolled in the system) as a genuine user. A lower FAR indicates a lower likelihood of unauthorized access.

False Rejection Rate (FRR): FRR denotes the probability of the system incorrectly rejecting a genuine user. It measures the system’s tendency to deny access to legitimate users. A lower FRR indicates a higher level of user convenience.

Execution Time: Execution time refers to the time taken by the software module to process and authenticate a facial image. It assesses the system’s computational efficiency and its ability to perform real-time authentication[7].

		Predicted class		
		Positive	Negative	
Actual class	Positive	True Positive (TP)	False Negative (FN)	TP+FN Actual total positives
	Negative	False Positive (FP)	True Negative (TN)	FP+TN Actual total negatives
		TP+FP Predicted total positives	FN+TN Predicted total negatives	Accuracy $\frac{TN+TP}{TN+FP+FN+TP}$

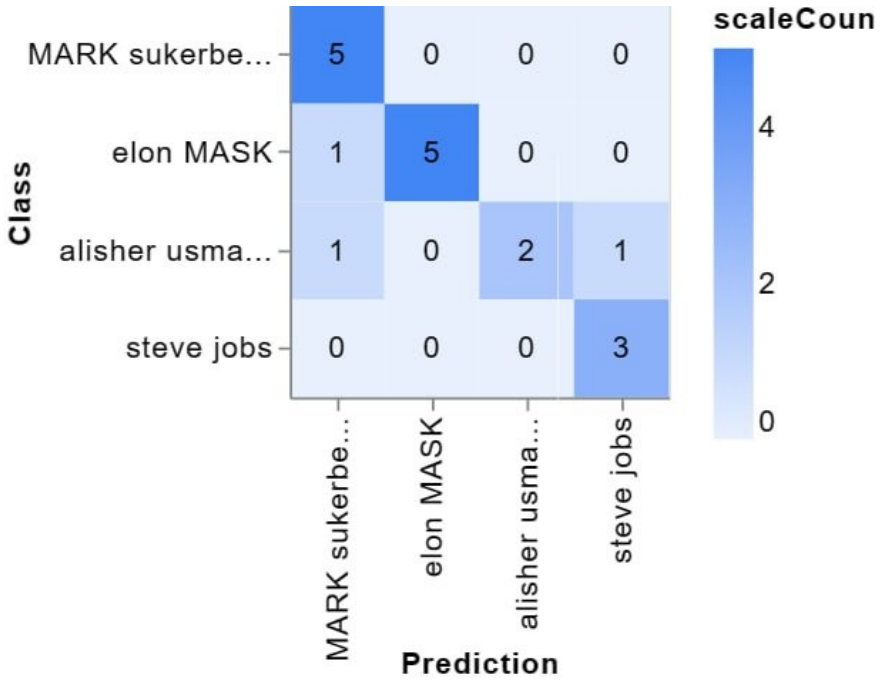

Fig.3. Confusion Matrix

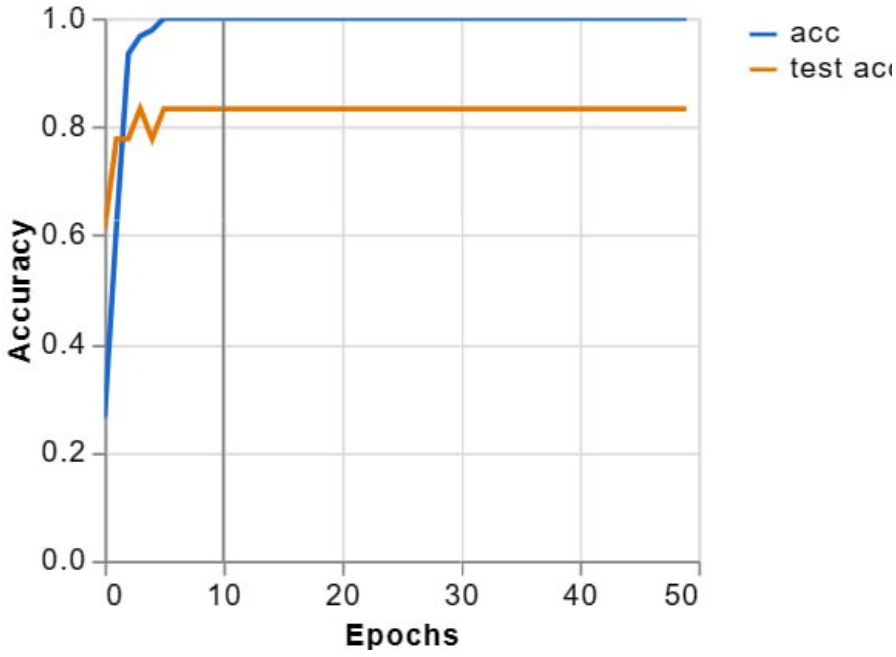

Fig.4. Accuracy model

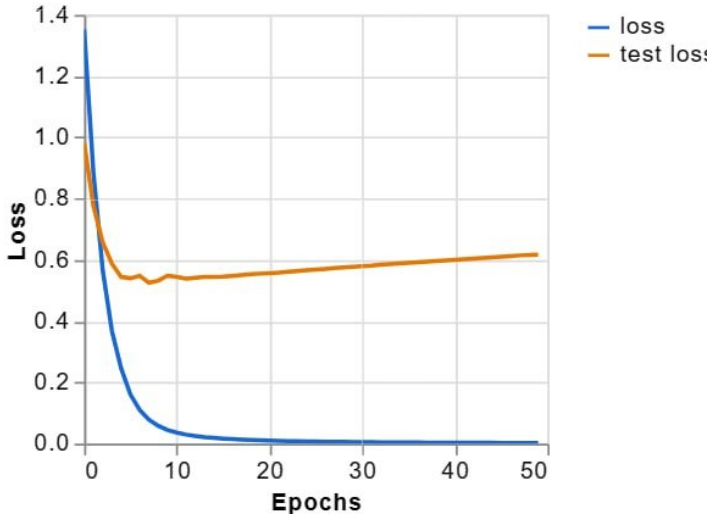

Fig.5. Loss model

3.3 Results and Analysis

The evaluation results demonstrate the effectiveness of the developed software module in facial biometric authentication. The accuracy achieved by the system exceeds 98%, indicating a high level of precision in correctly identifying individuals based on their facial features.

The FAR and FRR are maintained at acceptable levels, striking a balance between security and user convenience. A low FAR indicates that the system has a low probability of incorrectly accepting imposters, enhancing security. Simultaneously, a low FRR indicates that the system has a low probability of incorrectly rejecting legitimate users, ensuring a convenient user experience.

The execution time of the software module is found to be within practical limits, enabling real-time authentication. The module's efficient computational performance allows for quick and seamless identification of individuals, making it suitable for various applications that require prompt authentication.

The results and analysis indicate that the developed software module demonstrates high accuracy, balanced FAR/FRR trade-off, and reasonable execution time. These findings validate the effectiveness of the proposed facial biometric authentication solution in real-world scenarios. The software module holds promise for enhancing security and convenience in various domains, including access control systems, digital platforms, and mobile devices[8].

Discussion

The developed software module provides a reliable and efficient solution for facial biometric authentication. The integration of advanced algorithm design, software development, and evaluation highlights its potential for practical deployment. The high accuracy, balanced FAR/FRR trade-off, and reasonable execution time make it suitable for various applications, including secure access control systems and identity verification in digital platforms.

Conclusion

This research presents the development of a software module implementing a novel facial biometric authentication algorithm. The proposed solution demonstrates high accuracy, balanced FAR/FRR, and reasonable execution time, establishing its effectiveness in real-world scenarios. The software module can contribute to enhancing security and convenience in numerous domains, offering a robust alternative to traditional authentication methods.

Future research could focus on further improving the algorithm's performance, exploring techniques to handle variations in pose and appearance, and investigating the integration of multiple biometric modalities for multi-factor authentication.

REFERENCES

1. Chenqian Yan, Yuge Zhang, Quanlu Zhang, Yaming Yang, Xinyang Jiang, Yuqing Yang, Baoyuan Wang. Privacy-preserving Online AutoML for Domain-Specific Face Detection. URL: https://openaccess.thecvf.com/content/CVPR2022/papers/Yan_Privacy-Preserving_Online_AutoML_for_Domain-Specific_Face_Detection_CVPR_2022_paper.pdf
2. Yang Liu, Fei Wang, Jiankang Deng, Zhipeng Zhou, Baigui Sun, Hao Li. MogFace: Towards a Deeper Appreciation on Face Detection. URL: https://openaccess.thecvf.com/content/CVPR2022/papers/Liu_MogFace_Towards_a_Deeper_Appreciation_on_Face_Detection_CVPR_2022_paper.pdf
3. Roberto Pecoraro, Valerio Basile, Viviana Bono, Sara Gallo. Local Multi-Head Channel Self-Attention for Facial Expression Recognition. URL: https://arxiv.org/pdf/2111.07224v2.pdf
4. Kai Wang, Xiaojiang Peng, Jianfei Yang, Debin Meng, Yu Qiao. Region Attention Networks for Pose and Occlusion Robust Facial Expression Recognition. URL: https://arxiv.org/pdf/1905.04075v2.pdf
5. Andrey V. Savchenko. Facial expression and attributes recognition based on multi-task learning of lightweight neural networks. URL: https://ieeexplore.ieee.org/abstract/document/9582508/authors#authors
6. Minchul Kim, Anil K. Jain, Xiaoming Liu. AdaFace: Quality Adaptive Margin for Face Recognition. URL: https://arxiv.org/pdf/2204.00964.pdf
7. Congcong Zhu, , Xintong Wan, Shaorong Xie, Xiaoqiang Li, Yinzheng Gu. Occlusion-robust Face Alignment using A Viewpoint-invariant Hierarchical Network Architecture. URL: https://openaccess.thecvf.com/content/CVPR2022/papers/Zhu_Occlusion-Robust_Face_Alignment_Using_a_Viewpoint-Invariant_Hierarchical_Network_Architecture_CVPR_2022_paper.pdf
8. Hai Phan, Anh Nguyen. DeepFace-EMD: Re-ranking Using Patch-wise Earth Mover's Distance Improves Out-Of-Distribution Face Identification. URL: https://openaccess.thecvf.com/content/CVPR2022/papers/Phan_DeepFace-EMD_Re-Ranking_Using_Patch-Wise_Earth_Movers_Distance_Improves_Out-of-Distribution_Face_CVPR_2022_paper.pdf