E-ISSN: 1115 – 8492 P-ISSN: 3027 –
MPRI-JNSAR | INTERNATIONAL JOURNAL OF NATURE AND SCIENCE ADVANCE RES.
VOL. 07 NO. 9 JANUARY, 2025

DESIGN AND IMPLEMENTATION OF A GENDER-BASED FACIAL RECOGNITION SYSTEM USING MACHINE LEARNING MODEL

OYETOSO MODUPEOLU OPEYEMI; BUSARI OLUKAYODE AYODEJI; AKANJI OLULEYE O.; & AFENIFERE YUSUF BABATUNDE

Department of Computer Engineering Technology, the Polytechnic, Ibadan, Oyo State, Nigeria

Corresponding Author:
modupeoyetoso@gmail.com

DOI: https://doi.org/10.70382/mejnsar.v7i9.032

Abstract

This paper presents a gender-based facial recognition system, which utilizes advanced machine learning algorithms and real-time image processing to address the challenges of accurate and efficient gender classification. The system leverages Convolutional Neural Networks (CNNs) for feature extraction and TensorFlow for training and optimization, ensuring high performance in various real-world conditions. OpenCV is integrated to enhance face detection and processing, enabling real-time recognition. This system offers applications in security, access control, and biometric authentication,

Keywords;
Machine learning, TensorFlow, Biometric authentication, Image processing, Convolutional Neural Networks (CNNs), Facial recognition, Gender classification.

reducing verification time and enhancing accuracy compared to traditional methods. The research discusses the significance of gender recognition in modern biometric systems and explores existing literature on the evolution and challenges of facial recognition technology. Despite its effectiveness, the system faces limitations, such as performance degradation with varying test images and slower processing speeds. Future work will focus on improving the system's robustness, handling scale and rotation variations, and transitioning to a network-based model for greater scalability and accessibility.

INTRODUCTION

Face recognition systems are pivotal in modern facial image processing applications, gaining prominence due to their versatility and growing applicability. These systems utilize biometric information, offering advantages over traditional methods like fingerprinting or iris scanning, particularly for non-collaborative individuals. They are widely used in metropolitan areas for crime prevention, video surveillance, and person verification, but remain a complex challenge due to factors such as illumination, occlusion, and varying imaging conditions (Rahman et al., 2015). Gender detection, an important application of face recognition, has gained attention in fields such as surveillance, criminology, psychology, and biometric authentication. While humans intuitively adapt to changes in facial appearance, machines require advanced algorithms to ensure reliable performance. Traditional "high-level feature-based" approaches, reliant on facial attributes like the distance between eyes or nose structure, often fail under uncontrolled conditions or ambiguous features. These limitations underscore the need for alternative methods. This research adopts a "pixel-level matching" approach, which improves gender detection accuracy irrespective of image quality, offering a solution to challenges posed by complex imaging conditions (Dey et al., 2013).

Biometric systems must also address significant security concerns, as their use in sensitive applications like passports and identification cards demands high reliability. Challenges such as identical twins or overlapping facial features further emphasize the importance of robust recognition systems. This paper aims to design and implement a reliable, scalable, and cost-effective gender-based facial recognition system, combining face detection, recognition, and gender identification techniques. By leveraging machine learning, the research strives to enhance the security and reliability of such systems while addressing the limitations of existing approaches.

SIGNIFICANCE OF THE SYSTEM

This paper aims to enhance security and efficiency by developing a system that uses face and gender recognition to reduce fraudulent activities and automate user verification. Unlike manual methods, which are time-consuming, error-prone, and vulnerable to misinformation, the system ensures accurate identification, supports data tracking, and maintains a secure database for timely interventions. It offers applications in surveillance, demographic studies, and user authentication, significantly reducing verification time and improving accuracy. By providing a reliable and scalable solution, this research addresses key challenges in biometric identification, ensuring high security and paving the way for future advancements in the field.

LITERATURE REVIEW

Facial recognition technology has evolved significantly over the past decades, transitioning from rudimentary manual identification methods to advanced, automated systems powered by artificial intelligence (AI). The inception of facial recognition as a formalized concept can be traced back to the 1960s when researchers such as Woody Bledsoe, Helen Chan Wolf, and Charles Bisson began experimenting with semi-automated systems for facial feature mapping. Gender-based facial recognition systems emerged as a specialized application within this field, addressing the need for systems that can not only identify individuals but also classify them based on gender. This innovation was driven by diverse applications in marketing, security, healthcare, and

personalized user experiences. Researchers began leveraging convolutional neural networks (CNNs) and other deep learning techniques to improve the accuracy of gender classification, achieving significant milestones in the 2010s (Zhang et al., 2017). Most of past researches has already implement many system such as;

Gender classification has become a critical application area in computer vision, with deep learning offering innovative solutions. Levi and Hassner (2015) utilized deep convolutional neural networks (CNNs) for gender classification, leveraging the Adience dataset annotated with age and gender labels. Their study demonstrated the efficacy of transfer learning, where pre-trained models on large-scale datasets like ImageNet significantly improved classification performance. Hyperparameter tuning further optimized the learning process. In the context of mobile applications, Howard et al. (2017) developed lightweight models for real-time gender recognition using MobileNet, a neural network architecture designed for computationally constrained environments. By incorporating model compression and quantization, the system achieved a balance between efficiency and accuracy. The model's performance was tested under various conditions, including differing lighting and backgrounds, simulating real-world usage.

Expanding the scope to multi-task learning, Huang et al. (2020) explored a system that integrated gender classification and emotion detection within a shared framework. By leveraging shared feature representations, the study demonstrated that synergistic learning improved the accuracy of both tasks. However, the increased complexity demanded significant computational resources, and the limited availability of annotated datasets posed overfitting risks. Recognizing ethical concerns in gender recognition systems, Wang et al. (2021) addressed demographic bias through adversarial debiasing techniques. Their research employed balanced datasets, bias-sensitive loss functions, and adversarial training to reduce biases in the training process. Fairness metrics revealed improved equity across demographic groups, though this often came at the cost of reduced overall accuracy.

Collectively, these studies highlight the advancements and challenges in gender classification using deep learning, emphasizing the importance of addressing dataset biases, ensuring fairness, and balancing performance with

computational efficiency. From enhancing real-time recognition on mobile devices to improving fairness and applying insights in retail analytics, these efforts pave the way for more robust and ethical applications of gender recognition systems.

METHODOLOGY

The gender-based facial recognition system employs a top-down approach, breaking down the overall functionality into structured components for clarity and efficiency. At its core, the system relies on advanced machine learning algorithms, specifically Convolutional Neural Networks (CNNs), to analyze and classify gender based on facial features. Built with TensorFlow for robust training and optimization, the system also integrates OpenCV for real-time image processing, enabling efficient facial detection and recognition. This combination ensures accurate and reliable gender classification, meeting the demands of modern security and access control applications. This design integrates advanced machine learning with real-time image processing to deliver a scalable and effective system for gender-based facial recognition.

Design Analysis

The system's modular design ensures seamless interaction among components, enhancing performance and maintainability. Key modules include:

a. **Input Module**: Captures facial images or video frames using cameras, producing grayscale or colored images.
b. **Preprocessing Module**: Prepares images through resizing, normalization, and color adjustments for uniformity and enhanced processing.
c. **Feature Extraction Module**: Extracts key facial features like eyes, nose, and mouth using techniques such as Haar Cascade or histogram-based methods.
d. **Recognition and Classification Module**: Utilizes CNNs to process features and classify gender, trained on diverse datasets to learn patterns associated with male and female faces.

Core Components and Architectures

i. **Convolutional Neural Network (CNN)**
   a. **Architecture**: This Includes convolutional layers for feature extraction, pooling layers for dimensionality reduction, and fully connected layers for final classification.
   b. **Training**: Leveraging TensorFlow, the CNN is trained with labeled datasets of male and female faces, optimizing through techniques like backpropagation and gradient descent.

ii. **Image Processing with OpenCV**
   a. **Face Detection**: Employs Haar Cascade classifiers or modern deep learning techniques to locate faces in images.
   b. **Facial Landmark Detection**: Identifies key landmarks (eyes, nose, mouth) for alignment and normalization before classification.

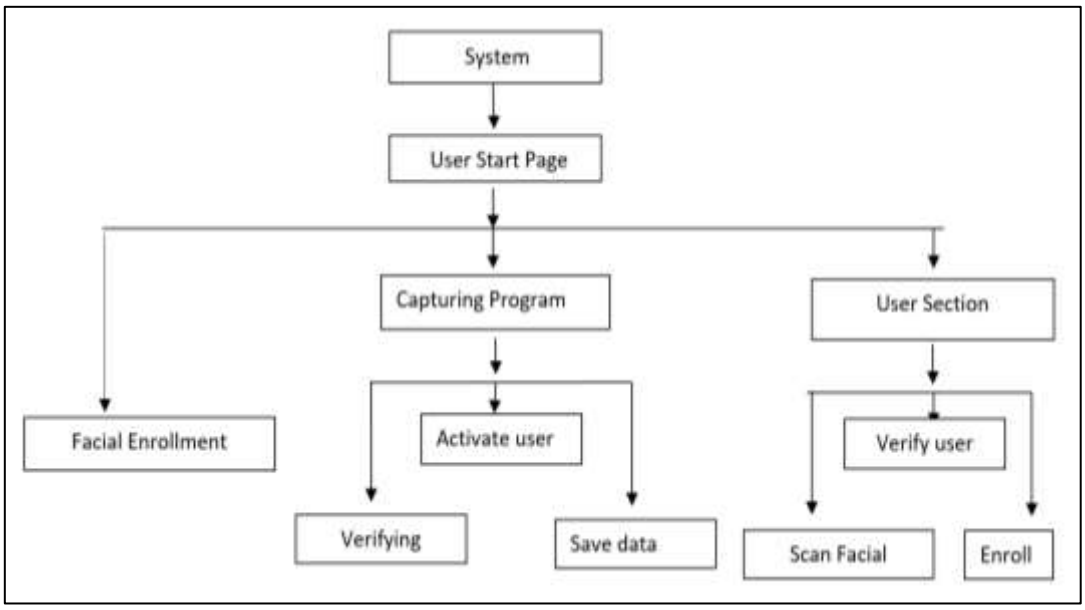

Figure 1: Top Down Design approach for the system

Brief Operation

This system consists of three modules, i.e. Processor module, Image Capture and Processing module and Verification and data saving module. The respective modules and their roles are explained below:

i. Processing Module: It forms the backbone of the system. It drives the control logic behind every functionality, some of which are mentioned below:

- Start the Program and initialize it and dependent modules.
- Check for interrupts, faults while the modules get initialized.
- Command the fingerprint module to function as requested by the software interface.

ii. Image Capture Module (ICM): The image capture module is essentially a picture upload module. It is an electronic device that process and uploaded image. Then a number of processing functions are applied to the scan and it is converted into a biometric template. Generally optical sensors are used, even though ultrasonic and capacitive sensors are also present.

iii. PC based Server-Client Software Management Module: The entire system is run from control software. The software on the server side consists of a database management and a GUI- based interactive. The SQL server is a local host and a system based database

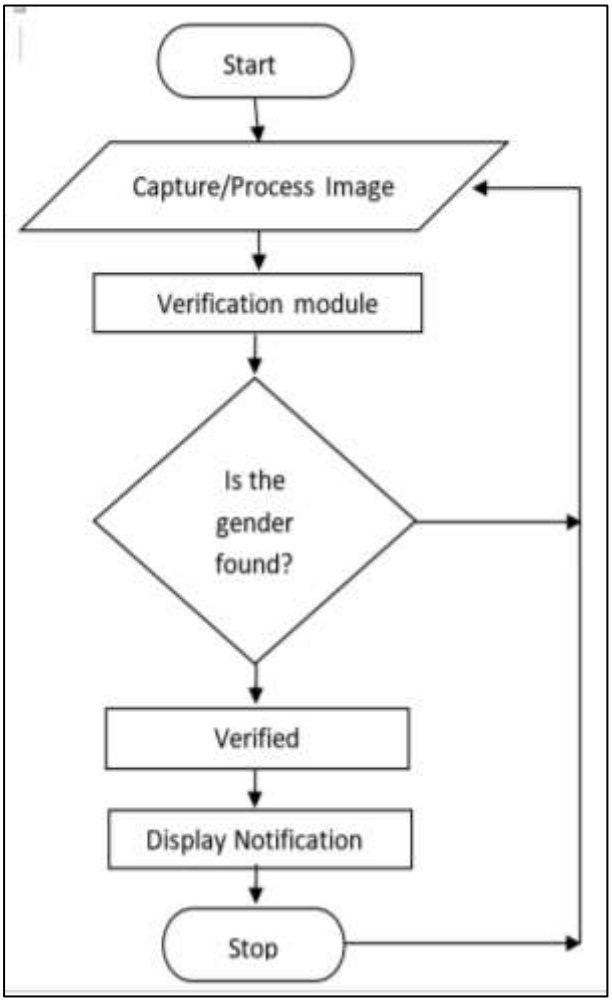

Figure 2: Flowchart of the System

Choice of Programming Language

The system was designed using common and popular window development technology which includes Python and MSSQL Server.

- **Python:** Python is used to implement the server side logic of the design. The reason for using this language is because of its fastness and easy way in creating web applications.
- **.NET Framework:** User Interface programs run on the .Net Framework which is an integral component of Windows that includes a virtual execution system called the Common Language Runtime (CLR) and a unified set of class libraries.
- **Local Dataset:** Local dataset is used in this project to stored needed image for processing and capturing model.
- **T-SQL:** Transaction Structured Query Language is used to write stored procedures embedded in the Microsoft SQL server.

RESULT PRESENTATION

As shown Figure 3, the first GUI to show is the main menu which has the different command button for each interface to work with;

Capturing Selection:

This button is used to navigate to the interface where the user selects the type of model of image processing model to be used in the enrollment and verification process.

Verification:

This button is used to navigate to the verification interface of the system, this interface consist of four important features, which are the; mark attendance, Create PDF, Student/fingerprint verification process, and the mail messaging features.

Enrollment:

This button is used to navigate to the enrollment interface, this is where all the data entry and fingerprint enrollment processing occurs.

Enrollment GUI:

This is Graphics User Interface (GUI) this interface is used to use to check the effectiveness of the fingerprint imagery and capturing.

Figure 3: Result Presentation I

As shown in fig. 4.1, the system create frames and cordinate mapping of genders, after been trained using image captured and processed using tensor flow sytem. The CNN which is the main controller of the system uses shapes and bone figure to identify and map together the identification.

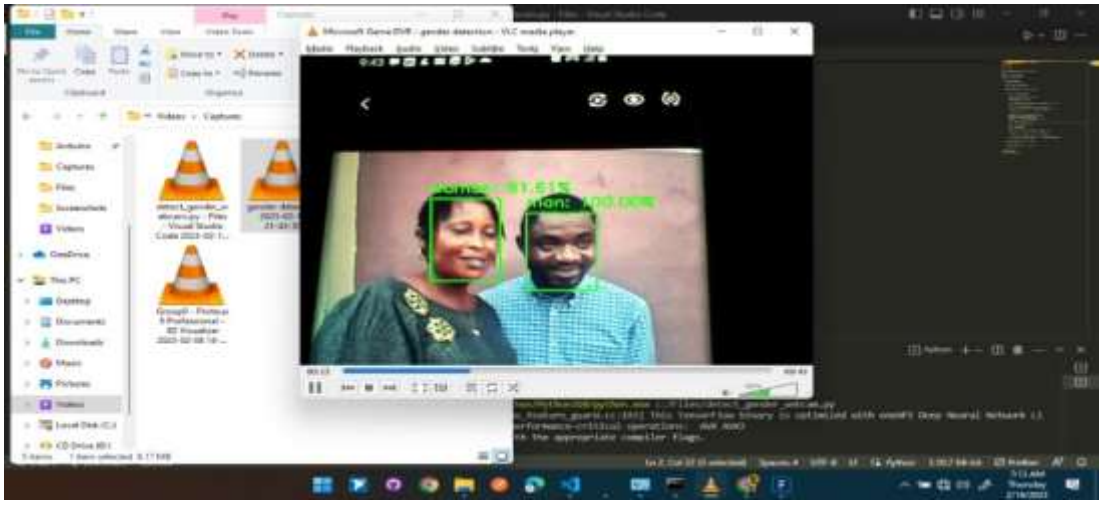

Figure 4: Result Presentation II

Figure 4 and 5 is showing another model of the result, video graphics is used to test the machine after been trained to recognice and verify images from any model of video or images.

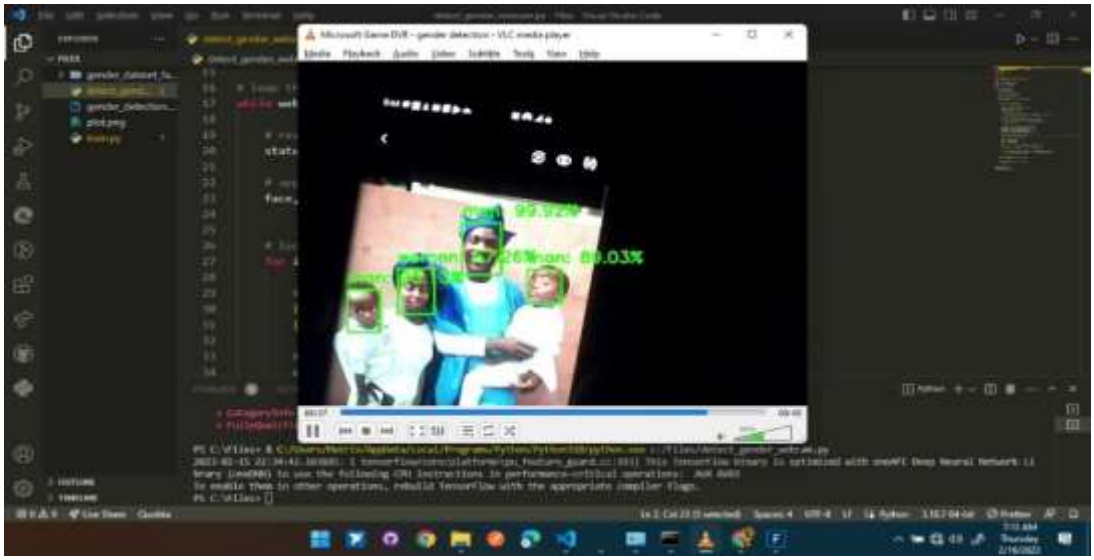

Figure 5: Result Presentation III

Algorithm of the system operation

The first process is to select the type/name of picture/image or use externa camera.

Enrolling Procedure

1. Enroll Start (ID); // Issue command to start enrolling over the past ID as parameter.
2. Upload or pick image
3. Analyzing Image

Verification

Verification is different from identification in a way that the person's identity is stored along with the fingerprint in a database.

Verifying Procedure:

1. Analyze or Process Image
2. Identify1_N
3. If (Xml== yes) > Verified ID
4. Else Invalid image

DISCUSSION

The system's primary goal is accurate gender classification, achieved through detection, preprocessing, and feature extraction. Once a face is detected and preprocessed, extracted features are processed by a Convolutional Neural Network (CNN), which assigns probabilities to each gender based on learned facial patterns. The predicted gender can be used in various applications, such as access control and security systems. Training is performed using TensorFlow, ensuring model optimization and reliable performance. OpenCV is integrated to enhance image detection and processing, enabling efficient real-time facial recognition. By combining TensorFlow's deep learning capabilities with OpenCV's robust image processing tools, the system delivers accurate and scalable gender classification, meeting the demands of modern security and access control applications.

CONCLUSION AND FUTURE WORK

Gender and image identification are reliable biometric systems due to the uniqueness and consistency of facial features. This project developed a gender detection system using machine learning and OpenCV for face detection, achieving decent accuracy. The system quickly identifies features and is adaptable for other object detection tasks. However, while it performs well under standard conditions, accuracy can decrease when test images differ significantly from training data, and the system is slow during calculation and matching. To enhance the study, improving model robustness through data augmentation and advanced transfer learning models like ResNet can boost accuracy. Optimizing processing speed with deep learning-based face detectors and model pruning ensures real-time efficiency. Addressing bias requires diverse datasets and fairness-aware techniques for equitable performance. Scalability can be improved with cloud-based models and API integration, while security can be strengthened with encryption and liveness detection. These enhancements will ensure a more accurate, efficient, and secure gender-based facial recognition system.

REFERENCES

Dey, E. K., Khan, M., & Ali, M. H. (2013). Computer Vision Based Gender Detection from Facial Image. LAP LAMBERT Academic Publishing.

Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., ... & Adam, H. (2017). MobileNets: Efficient convolutional neural networks for mobile vision applications. arXiv preprint arXiv:1704.04861.

Huang, G., Liu, Z., Maaten, L. V. D., & Weinberger, K. Q. (2020). Densely connected convolutional networks. Proceedings of the IEEE conference on computer vision and pattern recognition.

Levi, G., & Hassner, T. (2015). Age and gender classification using convolutional neural networks. Proceedings of the IEEE conference on computer vision and pattern recognition workshops.

Mollahosseini, A., Hasani, B., & Mahoor, M. H. (2016). AffectNet: A database for facial expression, valence, and arousal computing in the wild. IEEE Transactions on Affective Computing.

Rahman, M. M., Rahman, S., Dey, E. K., & Shoyaib, M. (2015). A gender recognition approach with an embedded preprocessing. International Journal of Information Technology and Computer Science (IJITCS), 7(7), 19.

Wang, Y., Zhao, Q., & Luo, Y. (2021). Adversarial debiasing for gender recognition systems. Advances in Neural Information Processing Systems, 34, 12345-12356.

Zhang, Z., Luo, P., Loy, C. C., & Tang, X. (2017). Facial landmark detection by deep multi-task learning. In European Conference on Computer Vision (pp. 94-108). Springer, Cham.

MEDITERRANEAN PUBLICATION AND RESEARCH INTERNATIONAL
E-ISSN: 1115 – 8492 P-ISSN: 3027 - 0693